Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l

Georges Gras

THÈSE

présentée

A L'UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE
DE GRENOBLE

pour obtenir

LE GRADE DE DOCTEUR ÈS SCIENCES MATHÉMATIQUES

par

Georges GRAS

SUR LES ℓ-CLASSES D'IDEAUX DANS LES EXTENSIONS CYCLIQUES RELATIVES DE DEGRE PREMIER ℓ

Soutenue le 9 novembre 1972 devant la Commission d'examen

C. CHABAUTY Président

J.L. KOSZUL
J. MARTINET Examinateurs
J.J. PAYAN

THÈSE

présentée

A L'UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE
DE GRENOBLE

pour obtenir

LE GRADE DE DOCTEUR ÈS SCIENCES MATHÉMATIQUES

par

Georges GRAS

SUR LES ℓ-CLASSES D'IDEAUX DANS LES EXTENSIONS CYCLIQUES RELATIVES DE DEGRE PREMIER ℓ

Soutenue le 9 novembre 1972 devant la Commission d'examen

C. CHABAUTY Président

J.L. KOSZUL
J. MARTINET Examinateurs
J.J. PAYAN

TABLE DES MATIERES

.../...

.../...

J'exprime ici toute ma reconnaissance au Professeur Claude CHABAUTY, Président du Jury. Ma dette envers lui est immense.

Jean-Jacques PAYAN et Jacques MARTINET m'ont constamment communiqué leur enthousiasme pour l'Arithmétique et ce dernier a patiemment dirigé mes recherches. Leurs remarques et leurs suggestions concernant, entre autres, mon manuscrit m'ont été précieuses. Je leur adresse mes vifs remerciements.

Le Professeur Jean-Louis KOSZUL a bien voulu choisir mon second sujet et être membre du jury. Je l'en remercie très sincèrement.

Je remercie également Madame GUTTIN-LOMBARD et Messieurs GAUDE et GIRARD qui ont accepté avec gentillesse de mettre leurs compétences au service de la réalisation matérielle de ce travail.

INTRODUCTION

L'étude du groupe des classes d'idéaux de l'anneau des entiers d'un corps de nombres ne procède d'aucune méthode générale, et, de ce fait, on connait une multitude de résultats isolés utilisant chacun des techniques particulières : les types de résultats les plus importants, et connus parfois depuis assez longtemps, sont constitués par :

(i) des formules analytiques (complexes ou p-adiques) du nombre de classes, utilisant les unités du corps et sa fonction zêta, ce qui fait qu'elles conduisent rarement à des calculs explicites (sauf lorsqu'on connait un algorithme pour la détermination des unités : par exemple, dans les extensions cubiques cycliques de $\mathbb{Q}$ (algorithme de Hasse) pour lesquelles on trouvera dans [11] des illustrations directes). De toute façon, ces formules ne donnent jamais une idée de la structure du groupe des classes, lorsque celle-ci n'est pas triviale.

(ii) des algorithmes donnant le nombre de classes et la structure du groupe des classes : le seul algorithme couramment utilisé dans la pratique concerne les extensions quadratiques de $\mathbb{Q}$ (A. Châtelet, L'arithmétique des corps quadratiques, Institut de Mathématiques de Genève 9 (1962)) ; d'autres, comme celui de [21] et, plus récemment, celui de [23] permettent une étude directe du 2-groupe des classes d'un corps quadratique.

(iii) la "théorie des genres" (dans les extensions cycliques) qui conduit, par exemple, à la formule dite des "classes ambiges" (i.e. invariantes par le groupe de Galois) et qui fournit un diviseur de l'ordre du groupe des classes et une approche de sa structure.

(iv) des arguments purement algébriques, concernant l'opération d'un groupe de Galois sur le groupe des classes, qui montrent que certains groupes ne peuvent réaliser le groupe des classes en question. Ils sont intéressants mais ne font pas intervenir l'arithmétique du corps en général.

(v) les travaux d'Iwasawa sur les Γ-extensions et de Leopoldt sur le "Spiegelungsatz" ainsi que les nombreux résultats trouvés par d'autres auteurs et issus de ces travaux.

On ne peut citer ici tous les résultats ni toutes les remarques publiés, on peut seulement constater que la plupart d'entre eux concernent :

a) le groupe des classes des corps quadratiques,

b) le groupe des classes des corps cyclotomiques,

c) la p-participation au nombre de classes de certaines extensions, pour des nombres premiers p particuliers,

d) des investigations des situations décrites dans les points (iii) et (v) précédents,

e) des études numériques.

Une étude qui ne semblait pas avoir été abordée systématiquement jusqu'alors était celle du ℓ-sous-groupe de Sylow du groupe des classes d'une extension cyclique de degré premier ℓ (hormis le problème des "classes ambiges").

L'idée d'entreprendre cette étude est née d'une question de Jacques Martinet concernant l'existence, dans une extension cubique cyclique de $\mathbb{Q}$, de classes d'ordre 3 non invariantes par le groupe de Galois. Nous avions d'ailleurs résolu sommairement ce problème par l'affirmative (cf. J. Martinet, A propos de classes d'idéaux, Séminaire de Théorie des Nombres, 5, Nov. 71, Bordeaux), prouvant ainsi qu'il était soluble par des voies arithmétiques. L'intérêt fut renouvellé lorsque nous avons eu connaissance de travaux, antérieurs,

de Bauer (H. Bauer, [4], Math. Review, n°1946, vol. 43, n°2, fév. 1972) résolvant aussi, et indépendamment, le cas cubique cyclique sur $\mathbb{Q}$ (au moins en ce qui concerne l'étude du 3-rang du groupe des classes). Nous nous devons enfin de signaler un article de Inaba (Über die Struktur der ℓ-Klassengruppe zyklischer Zahlkörper von Primzahlgrad ℓ, jour. of the Fac. of Sc. Imp. of Tokyo, Sect. I.4, 1940 (61-115)), injustement tombé dans l'oubli (il est totalement ignoré dans les travaux de Bauer ainsi que dans les articles postérieurs à 1940 ; seul Fröhlich le mentionne dans un article (The generalization of a theorem of L. Redei's, Quart. Jour. of Math. Oxford (2), 5(1954), 13-140) sans insister sur le contenu) ; nous l'avons découvert par hasard une fois le présent travail terminé. Il contient sans doute le premier exemple de classes exceptionnelles (i.e. non invariantes par le groupe de Galois) (corps cubiques de discriminant $(9.73)^2$) et utilise une méthode qui est à rapprocher de celle développée dans le chapitre IV (tout en étant à la fois bien plus complexe et plus restrictive).

Dans ce travail, nous avons considéré d'emblée le cas des extensions cycliques relatives de degré premier ℓ mettant alors en évidence l'importance, d'une part, du "théorème des normes" de Hasse et, d'autre part, de la théorie du corps de classes sous la forme des lois de réciprocité globale ; les résultats obtenus généralisent et simplifient ceux déjà cités constituant ainsi une méthode d'étude très générale de ce genre de problème.

PLAN DU TRAVAIL

Les chapitres I et II contiennent les résultats classiques (que nous avons empruntés, pour la plupart, à [22]) sur lesquels reposent les résultats des chapitres suivants.

Le chapitre III commence par une méthode de construction des extensions cycliques K/k de degré premier ℓ, via la théorie de Kummer (dont on trouvera une généralisation dans : L. Bouvier et J.J. Payan, Construction de cer-

taines extensions de degré p , Exposé au Séminaire de théorie des Nombres de Grenoble, 1971-72) et se termine par l'énoncé de propriétés des symboles locaux, particulières au cadre dans lequel nous nous plaçons.

Dans le chapitre IV, nous redonnons des indications sur le groupe des classes invariantes par $H = Gal(K/k)$. Nous abordons ensuite l'étude (algébrique) de la structure du ℓ-groupe des classes $\mathcal{H}(K)$ de K ; pour cela nous introduisons une filtration $\{\mathcal{H}_i\}_{i\geq 0}$ de sous-groupes de $\mathcal{H}(K)$ qui permet un "dévissage" canonique de $\mathcal{H}(K)$ considéré comme H-module. Le théorème IV.2 constitue alors une étape importante dans l'étude que nous avons en vue car il ramène l'étude de la filtration $\{\mathcal{H}_i\}_{i\geq 0}$ à celle de propriétés plus simples concernant :

α) les groupes des idéaux de K et k ,

β) l'action de la norme dans K/k .

Le point β) introduit alors de façon naturelle les symboles locaux (symbole de Hilbert) et le théorème des normes de Hasse.

Des calculs du même type de ceux que l'on doit faire pour démontrer la "formule des classes ambiges" (C. Chevalley [7] pp. 402-406) nous conduisent à une expression (théorème IV.3) qui constitue, en un sens, une généralisation de la formule de Chevalley et qui permet une étude effective des groupes $\mathcal{H}_i$ donc de $\mathcal{H}(K)$ et de sa structure.

Les deux derniers chapitres sont destinés à une exploitation des résultats précédents, le chapitre VI étant plus spécialement réservé au cas $k = \mathbb{Q}$ et a des exemples numériques. Par exemple, lorsque le discriminant d'une extension cyclique $K/\mathbb{Q}$ de degré ℓ est divisible par t nombres premiers distincts il y a $(\ell-1)^{t-1}$ corps ayant pour discriminant celui de K ; nous obtenons alors pour $t = 2,3$ des relations entre les groupes des classes de ces corps.

En annexe, nous donnons quelques tables numériques obtenues à partir de nos méthodes.

CHAPITRE I

GENERALITES SUR LES EXTENSIONS DE CORPS DE NOMBRES

A. Corps de nombres

1. Généralités.

Soit K un corps de nombres (i.e. une extension finie du corps des rationnels $\mathbb{Q}$). Il existe r_1 $\mathbb{Q}$-isomorphismes réels de K dans $\mathbb{C}$ et $2r_2$ $\mathbb{Q}$-isomorphismes complexes, conjugués deux à deux. Le degré $[K:\mathbb{Q}]$ est alors égal à r_1+2r_2 .

Définissons l'homomorphisme S_K (signature) de K^* dans $\{-1,+1\}^{r_1}$: soient $\tau_1,\ldots,\tau_{r_1}$ les $\mathbb{Q}$-isomorphismes réels de K dans $\mathbb{C}$ et sgn la fonction signe sur $\mathbb{R}$; on pose :

$$S_K(\alpha) = (\mathrm{sgn}(\alpha^{\tau_1}),\ldots,\mathrm{sgn}(\alpha^{\tau_{r_1}})) .$$

On démontre ([7]) que S_K est surjectif. Un élément α de K^* est dit totalement positif si α est dans le noyau de S_K ou si le corps K est totalement imaginaire ; le sous-groupe de K^* formé des éléments totalement positifs sera noté K^{*+} .

Soit A_K l'anneau des entiers de K (i.e. la clôture intégrale de $\mathbb{Z}$ dans K) et soit E_K le groupe des unités de K (i.e. le groupe des éléments inversibles de A_K) ; on sait, d'après le théorème de Dirichlet, que le $\mathbb{Z}$-rang de E_K est égal à r_1+r_2-1 .

Le groupe des idéaux fractionnaires de A_K est noté $\mathcal{J}(K)$ et le sous-

groupe des idéaux principaux (au sens habituel) est noté $\mathcal{J}'_0(K)$. Le sous-groupe de $\mathcal{J}'_0(K)$ formé des idéaux engendrés par un nombre totalement positif est le groupe des idéaux principaux au sens restreint et est noté $\mathcal{J}_0(K)$. On a alors la notion de classes d'idéaux : le groupe des classes d'idéaux au sens ordinaire (resp. au sens restreint) est, par définition, le groupe $\mathcal{H}'(K) = \mathcal{J}(K)/\mathcal{J}'_0(K)$ (resp. $\mathcal{H}(K) = \mathcal{J}(K)/\mathcal{J}_0(K)$).

Dans toute la suite, un idéal principal (resp. une classe d'idéaux) sera, sauf mention contraire, un idéal principal au sens restreint (resp. une classe d'idéaux au sens restreint).

Remarque I.1.- Les notions d'idéal principal au sens habituel et au sens restreint coïncident si et seulement si la restriction de S_K à E_K est surjective.

2. Places d'un corps de nombres.

L'ensemble des valeurs absolues d'un corps de nombres K est constitué des valeurs absolues non archimédiennes, associées aux idéaux premiers $\mathfrak{P}$ de A_K , et des valeurs absolues archimédiennes associées aux r_1+r_2 $\mathbb{Q}$-isomorphismes de K dans $\mathbb{C}$ non conjugués deux à deux ([5]). Nous dirons, en suivant Hasse, que les valeurs absolues archimédiennes sont associées aux idéaux premiers à l'infini $\mathfrak{P}_{\infty_1}, \ldots, \mathfrak{P}_{\infty_{r_1+r_2}}$; nous dirons que $\mathfrak{P}$ est une place lorsque $\mathfrak{P}$ désigne un idéal fini ou non et nous réserverons le mot idéal pour désigner un idéal fini au sens habituel.

3. Complétions d'un corps de nombres.

Soit $\mathfrak{P}$ une place de K ; on désigne par $K_{\mathfrak{P}}$ un complété de K pour la topologie définie par la valeur absolue associée à $\mathfrak{P}$. Si $\mathfrak{P}$ est un idéal premier, $K_{\mathfrak{P}}$ est un corps local contenant le corps des nombres p-adiques $\mathbb{Q}_p$ ($p\mathbb{Z} = \mathfrak{P}\cap\mathbb{Z}$) . Si $\mathfrak{P}$ est un idéal premier à l'infini alors $K_{\mathfrak{P}}$ est égal à $\mathbb{R}$ ou à $\mathbb{C}$. Dans la suite, nous identifions K à un sous-corps de $K_{\mathfrak{P}}$.

Lorsque $\mathfrak{P}$ est un idéal premier, on note $v_{\mathfrak{P}}$ la fonction valuation $\mathfrak{P}$-adique associée, $A_{K_{\mathfrak{P}}}$ l'anneau des entiers ($A_{K_{\mathfrak{P}}} = \{x \in K_{\mathfrak{P}}, v_{\mathfrak{P}}(x) \geq 0\}$), $\overline{\mathfrak{P}}$ l'idéal maximal de $A_{K_{\mathfrak{P}}}$, $\overline{K}_{\mathfrak{P}} = A_{K_{\mathfrak{P}}}/\overline{\mathfrak{P}}$ le corps résiduel et $q_{\mathfrak{P}}$ l'homomorphisme canonique $q_{\mathfrak{P}} : A_{K_{\mathfrak{P}}} \to \overline{K}_{\mathfrak{P}}$. Le corps résiduel $\overline{K}_{\mathfrak{P}}$ est un corps fini de caractéristique p.

Comme nous avons identifié K à un sous-corps de $K_{\mathfrak{P}}$, la fonction $v_{\mathfrak{P}}$ est définie sur K et le corps résiduel $\overline{K}_{\mathfrak{P}}$ est canoniquement isomorphe au quotient $A_K/\mathfrak{P}$.

B. Extensions

1. Définitions et notations.

Soit k un sous-corps de K. On définit de façon analogue :

$$S_k, \quad k^{*+}, \quad A_k, \quad E_k, \quad \mathcal{J}(k), \quad \mathcal{J}'_o(k), \quad \mathcal{J}_o(k), \quad \mathcal{H}'(k) \quad \text{et} \quad \mathcal{H}(k).$$

Si K/k est une extension galoisienne, chaque conjugué k_i de k dans $\mathbb{C}$ est contenu dans $[K:k]$ conjugués K_i de K confondus ; on supposera que pour $1 \leq i \leq \rho_1$ les corps K_i et k_i sont réels et que pour $\rho_1 < i \leq \rho_1+\rho_2$ les corps K_i sont imaginaires et les corps k_i réels ($\rho_1+\rho_2$ désignant le nombre de conjugués réels de k dans $\mathbb{C}$).

Ayant défini S_k et S_K, il faut remarquer que pour $a \in k^*$, les quantités $S_k(a)$ et $S_K(a)$ sont distinctes en général ; par contre, on a l'inclusion :

$$\text{Ker } S_k \subset \text{Ker } S_K .$$

Donnons quelques propriétés des homomorphismes S_k et S_K qui nous seront utiles par la suite :

PROPOSITION I.1.- Soit K/k galoisienne de degré premier ℓ et soit N la norme dans K/k ; alors :

(i) $N(K^{*+}) \subset k^{*+}$,

(ii) tout élément α de k^{*+} qui est norme dans K/k , est norme d'un élément de K^{*+} .

Démonstration.-

(i) Soit $\alpha \in K^{*+}$; pour connaître la signature (dans k) de $N\alpha$, il suffit de déterminer les signes des normes des conjugués α_i de α dans les extensions K_i/k_i correspondantes, et lorsque k_i est réel :

si K_i est réel, $N_{K_i/k_i}(\alpha_i)$ est positif comme produit de nombres positifs appartenant à K_i . Si K_i est imaginaire (et k_i réel) c'est que $\ell = 2$ et que $Gal(K_i/k_i)$ contient la conjugaison complexe ; $N_{K_i/k_i}(\alpha_i)$ s'écrit $u\bar{u}$ (produit d'un nombre complexe par le nombre complexe conjugué) qui est positif.

(ii) Soit $u \in K^*$ tel que $Nu = \alpha$; il revient au même de démontrer qu'il existe $v \in K^*$ tel que :

$$S_K(uv^{\sigma-1}) = 1 \quad ,$$

σ désignant un générateur de $Gal(K/k)$.

Posons $S_K(u) = (\ldots;\varepsilon_i^{(1)},\ldots,\varepsilon_i^{(\ell)};\ldots)$, $i = 1,\ldots,\rho_1$, et $S_K(v) = (\ldots;\eta_i^{(1)},\ldots,\eta_i^{(\ell)};\ldots)$; $S_K(v^{\sigma-1}) = (\ldots;\eta_i^{(1)}\eta_i^{(2)},\ldots,\eta_i^{(\ell)}\eta_i^{(1)};\ldots)$, soit $S_K(uv^{\sigma-1}) = 1$, si et seulement si on peut résoudre, pour $i = 1,2,\ldots,\rho_1$ le système linéaire défini par les relations :

$$\eta_i^{(k)}\eta_i^{(k+1)} = \varepsilon_i^{(k)} \quad \text{(l'indice } k \text{ étant défini modulo } \ell\text{)} \ ;$$

le rang de ce système est égal à $\ell-1$ et il admet une solution dès que la relation $\prod_{k=1}^{\ell} \varepsilon_i^{(k)} = 1$, entre les seconds membres, est satisfaite ; or l'hypothèse $Nu \in k^{*+}$ entraîne précisément ces relations. Ainsi v existe compte tenu du fait que S_K est surjectif.

DEFINITION I.1.- Soit $K_{\mathfrak{P}}$ un complété de K pour la valeur absolue associée à la place $\mathfrak{P}$; $K_{\mathfrak{P}}$ contient un corps qui s'identifie au complété $k_{\mathfrak{p}}$ de k relativement à une place $\mathfrak{p}$ qui ne dépend que de $\mathfrak{P}$. On dit que $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$.

Nous supposons désormais K/k galoisienne.

2. Décomposition des places dans K/k .

Soit $\mathfrak{p}$ une place de k ; les notions de décomposition, ramification et inertie sont bien connues lorsque $\mathfrak{p}$ est un idéal premier. Lorsque $\mathfrak{p}$ est un idéal à l'infini soit k_i le conjugué de k associé à $\mathfrak{p}$; nous dirons que $\mathfrak{p}$ est décomposé (resp. ramifié, inerte) dans K/k si k_i et K_i sont réels (resp. k_i est réel et K_i imaginaire, k_i et K_i sont imaginaires).

3. Groupes de ramification ([1] et [22]).

Soit H le groupe de Galois de K/k ; soient $\mathfrak{P}$ un idéal premier dans K et $\mathfrak{p}$ l'idéal premier en-dessous de $\mathfrak{P}$ dans k . On sait que le groupe de Galois de l'extension locale $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ ne dépend que de $\mathfrak{p}$ et s'identifie canoniquement au groupe de décomposition H_{-1} de $\mathfrak{p}$ dans K/k ([1]). Pour $i \geq -1$, on désigne par H_i le sous-groupe de H_{-1} formé des éléments σ tels que $v_{\mathfrak{P}}(x^{\sigma}-x) \geq i+1$ pour tout $x \in A_{K_{\mathfrak{P}}}$. On rappelle que dans le cas totalement ramifié, π désignant une uniformisante quelconque dans $K_{\mathfrak{P}}$, $\pi^{\sigma-1} \in 1 + \mathfrak{P}^i$, $i \geq 0$, si et seulement si $\sigma \in H_i$.

Enfin, il existe un entier $t_{\mathfrak{p}}$, ne dépendant que de $\mathfrak{p}$, tel que $H_{t_{\mathfrak{p}}} \neq \{1\}$ et $H_{t_{\mathfrak{p}}+1} = \{1\}$.

C. Théorie de Kummer
(Cas cyclique de degré premier ℓ)

Soit L un corps de nombres contenant les racines $\ell^{\text{èmes}}$ de l'unité. On rappelle que l'ensemble des extensions E de L cycliques de degré premier ℓ est canoniquement isomorphe à l'ensemble des sous-$\mathbb{F}_\ell$-espaces vec-

toriels de dimension 1 de $L^*/L^{*\ell}$: soit $\alpha \in L^*$ dont l'image dans $L^*/L^{*\ell}$ engendre un tel sous-espace ; alors il lui correspond l'extension $E = L(\sqrt[\ell]{\alpha})$.

Le résultat suivant résume alors la théorie de la ramification dans une extension de Kummer :

PROPOSITION I.2.- Soit $E = L(\sqrt[\ell]{\alpha})$, $\alpha \in L^*$, une extension de Kummer de degré premier ℓ et soit $\mathfrak{P}$ un idéal premier de L :

(i) si $v_{\mathfrak{P}}(\alpha) \equiv 0 \bmod \ell$ et si $\mathfrak{P}$ est premier à ℓA_L , alors $\mathfrak{P}$ est non ramifié dans E/L ,

(ii) si $v_{\mathfrak{P}}(\alpha) \not\equiv 0 \bmod \ell$, alors $\mathfrak{P}$ se ramifie dans E/L et $t_{\mathfrak{P}} = \ell v_{\mathfrak{P}}(1-\zeta)$, en désignant par ζ une racine primitive $\ell^{\text{ème}}$ de l'unité,

(iii) si $v_{\mathfrak{P}}(\alpha) \equiv 0 \bmod \ell$ et si $\mathfrak{P}$ divise ℓA_L , alors $\mathfrak{P}$ est non ramifié dans E/L si et seulement si la congruence $\alpha \equiv \xi^{\ell} \bmod \mathfrak{P}^{\lambda}$ est soluble dans L (α étant choisi premier à $\mathfrak{P}$) avec $\lambda = \ell v_{\mathfrak{P}}(1-\zeta)$. Dans le cas contraire, on a $t_{\mathfrak{P}} = \ell v_{\mathfrak{P}}(1-\zeta) - \lambda_{\mathfrak{P}}$, où $\lambda_{\mathfrak{P}}$ est l'entier maximum pour lequel la congruence précédente est soluble dans L ; dans ce cas l'entier $t_{\mathfrak{P}}$ est premier à ℓ .

On définit alors les ensembles de places $\mathfrak{P}$ de L suivants :

DEFINITION I.2.- On note :

P_o l'ensemble des idéaux premiers ramifiés dans E/L et premiers à ℓA_L ,

P_1 l'ensemble des idéaux premiers $\mathfrak{P}$ ramifiés dans E/L qui divisent ℓA_L et tels que $v_{\mathfrak{P}}(\alpha) \not\equiv 0$ modulo ℓ ,

P_2 l'ensemble des idéaux premiers $\mathfrak{P}$ ramifiés dans E/L qui divisent ℓA_L et tels que $v_{\mathfrak{P}}(\alpha) \equiv 0$ modulo ℓ ,

P_∞ l'ensemble des places à l'infini ramifiées dans E/L .

Ces ensembles de places sont disjoints ; on pose

$R = P_o \cup P_1 \cup P_2 \cup P_\infty$.

CHAPITRE II

LOIS DE RECIPROCITE

A. Cas local

1. Rappels (d'après [22]).

Soit L un corps local et soit L_s une clôture séparable de L ; on désigne alors par L^a l'extension abélienne maximale de L dans L_s. Pour toute extension intermédiaire F/E ($L \subset E \subset F \subset L^a$ et F/L finie) il existe un isomorphisme de réciprocité :

$$\omega : E^*/N_{F/E}F^* \to \mathrm{Gal}(F/E) \ ;$$

si $x \in E^*$ et si $\bar{x}$ est son image dans $E^*/N_{F/E}F^*$, on pose $(x,F/E) = \omega(\bar{x})$ et on montre que ce symbole a les propriétés suivantes :

(i) $(xx',F/E) = (x,F/E)(x',F/E)$,

(ii) $(x,F/E) = 1$ si et seulement si $x \in N_{F/E}F^*$.

Remarque II.1.- L'isomorphisme de réciprocité pour les corps $\mathbb{R}$ et $\mathbb{C}$ est le suivant :

$$\mathbb{R}^*/N\mathbb{C}^* \to \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \ ,$$

la classe des nombres négatifs ayant pour image la conjugaison complexe.

2. Symbole de Hilbert.

Soit L un corps local à corps résiduel fini et soit $\mathfrak{P}$ l'idéal de la valuation discrète de L. On suppose que L contient les racines $n^{\text{èmes}}$ de

l'unité (n entier supérieur ou égal à 2). Pour tout couple $(a,b) \in L^* \times L^*$ on définit le symbole (symbole de Hilbert) :

$$(a,b)_\wp = \theta^{\sigma-1} \quad , \quad \sigma = (b, L(\sqrt[n]{a})/L) \quad , \quad \theta^n = a \ ,$$

qui ne dépend pas du choix de θ .

Lorsque L est égal à $\mathbb{R}$ ou à $\mathbb{C}$ on définit encore le symbole de Hilbert par la même formule.

PROPOSITION II.1.- Le symbole de Hilbert a les propriétés suivantes :

(i) $(aa',b)_\wp = (a,b)_\wp (a',b)_\wp$,

(ii) $(a,bb')_\wp = (a,b)_\wp (a,b')_\wp$,

(iii) pour que $(a,b)_\wp = 1$ il faut et il suffit que b soit une norme dans l'extension $L(\sqrt[n]{a})/L$,

(iv) $(a,b)_\wp (b,a)_\wp = 1$.

B. Cas global

1. Rappels ([2] et [22]).

Cette fois L désigne un corps de nombres. On considère, dans le produit $\prod_\wp L_\wp^*$, où $\wp$ parcourt l'ensemble des places de L , le sous-ensemble des familles $\{x_\wp\}_\wp$, $x_\wp \in L_\wp^*$, pour lesquelles $x_\wp$ est une unité pour presque tout $\wp$: on obtient le groupe des idèles de L , I_L ; on considère que L^* est plongé dans I_L (plongement diagonal).

Soit E une extension abélienne finie de L de groupe de Galois H et soit $\wp'$ une place quelconque au-dessus de $\wp$ dans E . On note $H_\wp$ le groupe de décomposition de $\wp$ dans E/L .

Les isomorphismes de réciprocité :

$$f_\wp : L_\wp/NE_{\wp'} \to H_\wp \subset H ,$$

sont à valeurs dans $H_\wp$. Soit alors $x = \{x_\wp\}_\wp$ un idèle de L ; les $f_\wp(\bar{x}_\wp)$ sont presque tous égaux à 1 et on peut considérer l'application, dite de réciprocité globale :

$$f : I_L \to H ,$$

définie par $f(x) = \overline{\prod_\wp} f_\wp(\bar{x}_\wp)$; on obtient alors :

LOI DE RECIPROCITE D'ARTIN.- L'application f est surjective et son noyau est engendré par L^* et par $N_{E/L}(I_E)$.

2. Application au symbole de Hilbert.

Supposons que L contienne les racines $n^{\text{èmes}}$ de l'unité. Soient $a,b \in L^*$; le symbole de Hilbert $(a,b)_\wp$ a un sens dans tout complété puisque l'on a convenu d'identifier L a un sous-corps de $L_\wp$. La loi de réciprocité globale appliquée à l'extension $L(\sqrt[n]{a})/L$ donne, pour tout $b \in L^* \subset I_L$, $f(b) = 1$ soit $\overline{\prod_\wp} f_\wp(\bar{b}) = 1$ ce qui conduit immédiatement à la formule dite du produit :

$$\overline{\prod_\wp} (a,b)_\wp = 1 .$$

C. Calculs explicites des symboles

(dans le cas du degré premier ℓ)

1. Notations.

Soit L un corps de nombres contenant les racines $\ell^{\text{èmes}}$ de l'unité, ℓ désignant un nombre premier, et soit $\wp$ un idéal premier de L . On pose $q = \text{Card}(\bar{L}_\wp)$; on désigne par p la caractéristique de $\bar{L}_\wp$ et par $S_\wp$ la trace dans l'extension résiduelle $\bar{L}_\wp/\mathbb{F}_p$.

Si $a \in L^*$, on désigne par E l'extension de Kummer $L(\sqrt[\ell]{a})$. Soit θ une racine $\ell^{\text{ème}}$ de a et soit σ un générateur du groupe de Galois de E/L ; $\theta^{\sigma-1}$ est une racine $\ell^{\text{ème}}$ de l'unité ζ_σ indépendante du choix de θ.

2. Résultats explicites (d'après [22]).

PROPOSITION II.2.- Si la caractéristique p est différente de ℓ, $\overline{L}_\wp^*$ contient le groupe des racines $\ell^{\text{èmes}}$ de l'unité et on a

$$q_\wp((a,b)_\wp) = q_\wp(c)^{\frac{q-1}{\ell}}$$

avec

$$c = (-1)^{v_\wp(a)v_\wp(b)} a^{v_\wp(b)} b^{-v_\wp(a)} .$$

PROPOSITION II.3.- On suppose $p = \ell$ et E/L totalement ramifiée en $\wp$. Soit π une uniformisante de $L_\wp(\theta)$ et soit $M = \pi^{\sigma-1}-1$. Lorsque b est congru à 1 modulo $\wp^{t_\wp}$, le nombre $c = \frac{b-1}{Tr(M)}$ est entier dans $L_\wp$ et vérifie $c \equiv -\frac{b-1}{N(M)} \equiv -\frac{b-1}{M^\ell}$ modulo π.

On a alors : $(a,b)_\wp = \zeta_\sigma^{S_\wp(q_\wp(c))}$.

PROPOSITION II.4.- On suppose $p = \ell$. Soit $a \in L^*$; si $b \in L^*$ est congru à 1 modulo $\wp^{\ell v_\wp(1-\zeta_\sigma)}$, le nombre $c = \frac{b-1}{\ell(\zeta_\sigma-1)}$ est entier dans $L_\wp$ et on a :

$$(a,b)_\wp = \zeta_\sigma^{v_\wp(a)\, S_\wp(q_\wp(c))} .$$

PROPOSITION II.5.- Soit $\wp$ une place à l'infini. Si $L_\wp = \mathbb{C}$ alors $(a,b)_\wp = 1$; si $L_\wp = \mathbb{R}$, nécessairement $\ell = 2$ et dans ce cas $(a,b)_\wp = -1$ si et seulement si a et b sont négatifs dans $L_\wp$.

CHAPITRE III

CONSTRUCTION DES EXTENSIONS CYCLIQUES DE DEGRE PREMIER ℓ

On se propose de décrire, dans ce chapitre, l'ensemble des extensions cycliques de degré premier ℓ d'un corps de nombres k ne contenant pas nécessairement les racines $\ell^{\text{èmes}}$ de l'unité et de particulariser certains résultats des chapitres précédents à ces extensions (notamment en ce qui concerne le symbole de Hilbert).

A. Rappels sur certains $\mathbb{Z}_\ell[G]$-modules

Soit G un groupe abélien fini d'ordre d diviseur de $\ell-1$. Soit $\mathbb{Z}_\ell$ l'anneau des entiers ℓ-adiques ; on sait que $\mathbb{Z}_\ell$ contient le sous-groupe multiplicatif des racines $(\ell-1)^{\text{èmes}}$ de l'unité, noté U, et que l'homomorphisme canonique $\theta : \mathbb{Z}_\ell \to \mathbb{F}_\ell$ identifie U et $\mathbb{F}_\ell^*$. Soit G^* le groupe des caractères de G ; comme G est d'ordre diviseur de $\ell-1$ on peut supposer que les éléments de G^* sont à valeurs dans $\mathbb{Z}_\ell$.

Les éléments $e_\chi = d^{-1} \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma$ constituent un système complet d'idempotents orthogonaux de $\mathbb{Z}_\ell[G]$; c'est-à-dire que :

(i) $1 = \sum_{\chi \in G^*} e_\chi$,

(ii) $e_\chi e_{\chi'} = 0$ pour $\chi \neq \chi'$,

(iii) $e_\chi^2 = e_\chi$ pour tout $\chi \in G^*$,

(iv) $e_\chi(s-\chi(s)) = 0$ pour tout $\chi \in G^*$ et tout $s \in G$.

Soit M un $\mathbb{Z}_\ell[G]$-module ; on a alors la décomposition :

$$M = \prod_{\chi \in G^*} M^{e_\chi} ;$$

en particulier tout G-module dont l'exposant (en tant que groupe abélien) est une puissance de ℓ peut être muni canoniquement d'une structure de $\mathbb{Z}_\ell[G]$-module.

PROPOSITION III.1.- *Soit* $\chi \in G^*$ *et soit* M *un* $\mathbb{Z}_\ell[G]$*-module* :

(i) *soit* $x \in M$; *alors* $x^{s-\chi(s)} = 1$ *pour tout* $s \in G$ *si et seulement si* $x = x^{e_\chi}$,

(ii) *si* $e \in \mathbb{Z}_\ell[G]$ *vérifie* $e(s-\chi(s)) = 0$ *pour tout* $s \in G$, *alors* $e = \lambda e_\chi$, $\lambda \in \mathbb{Z}_\ell$,

(iii) *quels que soient* $n \geq 1$, $\chi \in G^*$ *et* $s \in G$, *il existe* $a \in \mathbb{Z}$ *et* $e \in \mathbb{Z}[G]$ *tels que* : a *soit congru à* $\chi(s)$ *modulo* ℓ , e *soit congru à* e_χ *modulo* ℓ *et* $e(s-a)$ *soit congru à* 0 *modulo* ℓ^n .

Démonstration.-

(i) Si $x^s = x^{\chi(s)}$ on aura $x^s = \frac{}{|\chi'|} x^{se_{\chi'}} = \frac{}{|\chi'|} x^{\chi'(s)e_{\chi'}}$, ce qui donne $x^{e_{\chi'}(\chi'(s)-\chi(s))} = 1$ pour tout $\chi' \in G^*$ et tout $s \in G$; pour $\chi' \neq \chi$ on obtient $x^{e_{\chi'}} = 1$, d'où $x = x^{e_\chi}$.

(ii) D'après ce qui précède on aura $e = ee_\chi$ et en écrivant $e = \sum_s a_s s$, $a_s \in \mathbb{Z}_\ell$, on aura $ee_\chi = \sum_s a_s s e_\chi = (\sum_s a_s \chi(s))e_\chi$ qui est de la forme λe_χ , $\lambda \in \mathbb{Z}_\ell$.

(iii) Il suffit de prendre $a \in \mathbb{Z}$ congru à $\chi(s)$ modulo ℓ^n et e congru à e_χ modulo $\ell^n \mathbb{Z}_\ell[G]$.

DEFINITION III.1.- *Lorsque* G *opère sur le groupe des racines* $\ell^{\text{èmes}}$ *de l'unité (par exemple lorsque* G *est un groupe de Galois convenable), pour tout* $s \in G$ *il existe un entier* a *(défini modulo* ℓ*) tel que* $\zeta^s = \zeta^a$ *pour toute racine* $\ell^{\text{ème}}$ ζ *de l'unité. L'application qui associé à* s *l'unique élément* $\theta(a)$ *de* U *qui est congru à* a *modulo* ℓ , *est un caractère de* G *à valeurs dans* $\mathbb{Z}_\ell$: *on le note* χ^* *et on note* e^* *l'idempotent* e_{χ^*} .

La relation $\zeta^s = \zeta^{\varkappa^*(s)}$ entraîne alors $\zeta^{e^*} = \zeta$ (on applique la proposition III.1 au groupe des racines $\ell^{\text{èmes}}$ de l'unité).

B. Description des extensions cycliques de degré premier ℓ .

Soient k un corps de nombres et K une extension abélienne de degré premier ℓ de k . Soient ζ une racine primitive $\ell^{\text{ème}}$ de l'unité, k' et K' les composés $k\mathbb{Q}(\zeta)$ et $K\mathbb{Q}(\zeta)$. On pose $G = \text{Gal}(K'/K)$ et $H = \text{Gal}(K'/k')$; les groupes $\text{Gal}(k'/k)$ et $\text{Gal}(K/k)$ sont respectivement isomorphes à G et H par restriction. Enfin G est un groupe cyclique dont l'ordre d divise $\ell-1$.

1. Critère de décomposition.

A l'extension K/k on peut associer de façon canonique l'extension de Kummer K'/k' qui est canoniquement associée à un sous-$\mathbb{F}_\ell$-espace de dimension 1 de $k'^*/k'^{*\ell}$. Soit q l'homomorphisme canonique $q : k'^* \to k'^*/k'^{*\ell}$; posons $\mathfrak{X} = k'^*/k'^{*\ell}$, $\mathfrak{X}$ peut être considéré comme un $\mathbb{Z}_\ell[G]$-module. On vient donc de définir une application canonique de l'ensemble des extensions abéliennes de degré ℓ de k dans l'espace projectif $\mathbb{P}(\mathfrak{X})$.

Soit $\mathfrak{X}^* = \mathfrak{X}^{e^*} = \{q(\alpha) \in \mathfrak{X}\ ,\ q(\alpha)^s = q(\alpha)^{\varkappa(s)}\}$; $\mathfrak{X}^*$ est un sous-$\mathbb{F}_\ell$-espace vectoriel de $\mathfrak{X}$ et on peut considérer $\mathbb{P}(\mathfrak{X}^*)$ comme un sous-espace de $\mathbb{P}(\mathfrak{X})$; on a alors le résultat suivant :

THEOREME III.1.- <u>L'application qui associe à</u> K/k <u>un point de</u> $\mathbb{P}(\mathfrak{X})$ <u>est une bijection de l'ensemble des extensions abéliennes de degré</u> ℓ <u>de</u> k <u>sur</u> $\mathbb{P}(\mathfrak{X}^*)$.

<u>Démonstration</u>.- Soit K une extension abélienne de degré ℓ de k

et soit $\alpha \in k'$ tel que $K' = k'(\sqrt[\ell]{\alpha})$; si φ est un k-isomorphisme de K', dont la restriction à k' est notée s, il est nécessaire que $q(\alpha^s)$ soit de la forme $q(\alpha)^h$, $h \in \mathbb{Z}$ convenable, car K'/k est galoisienne ; on a donc $\theta^{\varphi-h} \in k'$, où θ est une racine du polynôme $X^\ell - \alpha$. Soit $\sigma \in H$, $\sigma \neq 1$; comme φ et σ commutent (K'/k est abélienne) on obtient :

$$\theta^{(\varphi-h)\sigma} = \theta^{\varphi-h} \quad \text{et} \quad \theta^{\sigma(\varphi-h)} = (\zeta\theta)^{\varphi-h}, \quad \zeta \neq 1 ;$$

ce qui conduit à $\zeta^{\varphi-h} = 1$ soit $\zeta^{s-h} = 1$; donc h est congru à $\varkappa^*(s)$ modulo ℓ, par définition de $\varkappa^*$, et $q(\alpha)^{s-\varkappa^*(s)} = 1$, soit $q(\alpha) \in \mathfrak{X}^*$.

Montrons maintenant que si $q(\gamma)$ représente un élément de $\mathbb{P}(\mathfrak{X}^*)$ alors l'extension $K' = k'(\sqrt[\ell]{\gamma})$ est de la forme Kk' avec K abélienne de degré ℓ de k. Il est équivalent de démontrer que $k'(\sqrt[\ell]{\gamma})$ est abélienne sur k. La condition $q(\gamma)^s = q(\gamma)^{\varkappa^*(s)}$, pour tout $s \in G$, montre que K' est galoisienne sur k et on est ramené à montrer que deux k-automorphismes quelconques φ et ψ de K' commutent. Soient s et t les restrictions de φ et ψ à k'. Soit n le plus grand entier pour lequel k' contient les racines ℓ^n-èmes de l'unité. Soit s_o un générateur de G ; d'après la proposition III.1, il existe $a_o \in \mathbb{Z}$ et $e_o \in \mathbb{Z}[G]$ tels que $a_o \equiv \varkappa^*(s_o)$ modulo ℓ et $e_o(s_o - a_o) \equiv 0$ modulo ℓ^n.

On sait que $q(\gamma) = q(\gamma)^{e^*} = q(\gamma)^{e_o}$ donc $\gamma = \gamma^{e_o} u^\ell$, $u \in k'$. Posons $\alpha = \gamma u^{-\ell}$ et soit θ une racine du polynôme $X^\ell - \alpha$ (on a $K' = k'(\theta)$) On aura ainsi $\alpha^{s_o - a_o} = \gamma^{e_o(s_o-a_o)} = \mu^{\ell^n}$, $\mu \in k'$, ce qui conduit immédiatement à l'existence de a et b entiers tels que $\alpha^{s-a} = u^{\ell^n}$ et $\alpha^{t-b} = v^{\ell^n}$, $u, v \in k'$. Comme toute racine $\ell^{\text{ème}}$ de l'unité est puissance ℓ^{n-1}-ème dans k' par définition de n, on peut écrire $\theta^{\varphi-a} = u^{\ell^{n-1}}$ et $\theta^{\psi-b} = v^{\ell^{n-1}}$, ce qui conduit aux relations

$$\theta^{\varphi\psi} = \theta^{ab} v^{a\ell^{n-1}} u^{t\ell^{n-1}} \quad \text{et} \quad \theta^{\psi\varphi} = \theta^{ab} u^{b\ell^{n-1}} v^{s\ell^{n-1}} ;$$

or $\theta^{\ell\varphi\psi} = \alpha^{\varphi\psi} = \alpha^{\psi\varphi}$ (φ et ψ commutent sur k'), soit $(v^{a-s} u^{t-b})^{\ell^n} = 1$. Si $(v^{a-s} u^{t-b})^{\ell^{n-1}} = 1$ on obtient $\theta^{\varphi\psi} = \theta^{\psi\varphi}$ sinon $(v^{a-s} u^{t-b})^{\ell^{n-1}} = \zeta$ avec $\zeta^\ell = 1$, $\zeta \neq 1$. On sait que $\zeta^{e^*} = \zeta$, soit $\zeta = \zeta^{e_o} = (v^{(a-s)e_o} u^{(t-b)e_o})^{\ell^{n-1}}$; or $(a-s)e_o \equiv (t-b)e_o \equiv 0$ modulo ℓ et

ζ serait puissance ℓ^n-ème dans k', ce qui est absurde. Comme φ et ψ sont déterminés par leur action sur ζ et θ, on a bien $\varphi\psi = \psi\varphi$.

2. Etude de $\mathbb{P}(\mathfrak{X}^*)$.

Soit K/k une extension abélienne de degré premier ℓ, soit K'/k' l'extension de Kummer associée et soit $\alpha \in k'$ un nombre tel que $K' = k'(\sqrt[\ell]{\alpha})$ (on sait que $q(\alpha) \in \mathfrak{X}^*$).

Soit $A_{k'}$ (resp. $\mathcal{J}(k')$) l'anneau des entiers de k' (resp. le groupe des idéaux fractionnaires de k'). On notera $\bar{\alpha}$ les éléments du quotient $\overline{\mathcal{J}}(k') = \mathcal{J}(k')/\mathcal{J}(k')^\ell$, qui est un $\mathbb{Z}_\ell[G]$-module.

Dans l'ensemble des idéaux premiers de k' la conjugaison relativement à k'/k est une relation d'équivalence ; soit alors $\mathcal{D}$ un système exact de représentants des classes des idéaux premiers totalement décomposés dans k'/k

PROPOSITION III.2.- L'idéal $\alpha A_{k'}$ vérifie la relation :

$$\overline{\alpha A_{k'}} = \overline{\Big|\Big|_{\mathfrak{P}\in\mathcal{D}}} \; \overline{\mathfrak{P}}^{e^* x_{\mathfrak{P}}} \quad , \quad x_{\mathfrak{P}} \in \mathbb{Z} .$$

Démonstration.- Soit $e \in \mathbb{Z}[G]$ congru à e^* modulo ℓ ; alors $q(\alpha) = q(\alpha)^{e^*} = q(\alpha)^e$ soit $\alpha = \alpha^e u^\ell$, $u \in k'$; $\alpha A_{k'} = (\alpha A_{k'})^e (u A_{k'})^\ell$ ce qui entraîne $\overline{\alpha A_{k'}} = (\alpha A_{k'})^e = \overline{\alpha A_{k'}}^{e^*}$. Si on écrit $\alpha A_{k'} = \Big|\Big|_{\mathfrak{P}} \mathfrak{P}^{y_{\mathfrak{P}}}$, $y_{\mathfrak{P}} \in \mathbb{Z}[G]$, les idéaux $\mathfrak{P}$ étant non conjugués deux à deux, on aura

$$\overline{\alpha A_{k'}} = \overline{\Big|\Big|_{\mathfrak{P}}} \; \overline{\mathfrak{P}}^{y_{\mathfrak{P}}} = \overline{\Big|\Big|_{\mathfrak{P}}} \; \overline{\mathfrak{P}}^{y_{\mathfrak{P}} e^*} = \overline{\Big|\Big|_{\mathfrak{P}}} \; \overline{\mathfrak{P}}^{e^* x_{\mathfrak{P}}} \quad , \quad x_{\mathfrak{P}} \in \mathbb{Z} .$$

Reste à montrer que si $\mathfrak{P}$ n'est pas totalement décomposé dans k'/k alors $\overline{\mathfrak{P}}^{e^* x_{\mathfrak{P}}} = \overline{1}$. Soit $s \neq 1$, s appartenant au groupe de décomposition pour $\mathfrak{P}$ dans k'/k ; alors $\mathfrak{P}^s = \mathfrak{P}$ et $\overline{\mathfrak{P}}^{e^* s} = \overline{\mathfrak{P}}^{e^*} = \overline{\mathfrak{P}}^{e^* \varkappa^*(s)}$; comme on a par hypothèse $s \neq 1$, il en résulte que $\varkappa^*(s) \neq 1$ et on obtient $\overline{\mathfrak{P}}^{e^*} = \overline{1}$.

COROLLAIRE III.1.- L'ensemble $P_o \cup P_1$ (cf. Définition I.2) est égal à l'ensemble formé par les idéaux $\mathfrak{P}$ et leurs conjugués pour lesquels $x_{\mathfrak{P}} \not\equiv 0$ modulo ℓ (ils sont totalement décomposés dans k'/k).

Nous conservons dans la suite les notations P_o , P_1 , P_2 et P_∞ caractérisant les différentes sortes de places ramifiées dans l'extension K'/k' .

Remarque III.1.- Pour tout $s \in G$ on a $t_{\mathfrak{P}s} = t_{\mathfrak{P}}$ et $v_{\mathfrak{P}s}(1-\zeta) = v_{\mathfrak{P}}(1-\zeta)$ (et, lorsque $\mathfrak{P} \in P_2$, $\lambda_{\mathfrak{P}^s} = \lambda_{\mathfrak{P}}$) relativement à K'/k' .

En effet, si $(1-\zeta)A_{k'} = \mathfrak{P}^{a_{\mathfrak{P}}}\mathfrak{A}$, $\mathfrak{A}$ premier à $\mathfrak{P}$, $(1-\zeta^s)A_{k'} = \mathfrak{P}^{sa_{\mathfrak{P}}}\mathfrak{A}^s$; or $1-\zeta^s = (1-\zeta)\varepsilon$, ε unité, et $(1-\zeta)A_{k'} = \mathfrak{P}^{sa_{\mathfrak{P}}}\mathfrak{A}^s$; il en résulte que $v_{\mathfrak{P}s}(1-\zeta) = a_{\mathfrak{P}}$.

Supposons qu'il existe $\xi \in k'$ tel que $\alpha \equiv \xi^{\ell} \bmod \mathfrak{P}^{\lambda}$, alors $\alpha^s \equiv \xi^{s\ell} \bmod \mathfrak{P}^{s\lambda}$, soit $\alpha^g u^{\ell} \equiv \xi^{s\ell} \bmod \mathfrak{P}^{s\lambda}$ (g entier convenable), ce qui s'écrit $\alpha^g \equiv \xi'^{\ell} \bmod \mathfrak{P}^{s\lambda}$ (car α est premier à $\mathfrak{P}$ et ses conjugués), soit $\alpha \equiv \xi''^{\ell} \bmod \mathfrak{P}^{s\lambda}$; lorsque $\mathfrak{P} \in P_2$, le maximum pour λ sera le même quel que soit $s \in G$. L'expression même de $t_{\mathfrak{P}}$ (Proposition I.2) permet de conclure.

C. Etude du symbole $(\alpha,a)_{\mathfrak{P}}$

Nous aurons besoin dans le chapitre IV du symbole $(\alpha,a)_{\mathfrak{P}}$, pour $a \in k^*$, $\alpha \in k'^*$ vérifiant $q(\alpha) \in \mathfrak{X}^*$. Nous en donnons ici les propriétés essentielles.

1. Calcul effectif de $(\alpha,a)_{\mathfrak{P}}$.

Distinguons plusieurs cas :

(i) si $\mathfrak{P}$ est une place à l'infini, on utilise la proposition II.5 qui permet un calcul effectif immédiat.

(ii) si $\mathfrak{P}$ est un idéal premier qui ne divise pas ℓ , on utilise la proposition II.2 qui conduit aussi à un calcul effectif.

(iii) si $\mathfrak{P}$ est un idéal premier qui divise ℓ , il y a encore trois possibilités :

$(iii)_1$ $\mathfrak{p}$ est non ramifié ; on applique la proposition II.4 : $(\alpha,a)_{\mathfrak{p}} = \zeta^{v_{\mathfrak{p}}(a)S_{\mathfrak{p}}(q_{\mathfrak{p}}(c))}$, $c = \frac{\alpha-1}{\ell(\zeta-1)}$, en choisissant le nombre α congru à 1 modulo $\ell(\zeta-1)$.

$(iii)_2$ $\mathfrak{p} \in P_1$, on applique la proposition II.4 : $(\alpha,a)_{\mathfrak{p}} = \zeta^{v_{\mathfrak{p}}(\alpha)S_{\mathfrak{p}}(q_{\mathfrak{p}}(c))}$, $c = \frac{a-1}{\ell(\zeta-1)}$, en supposant a congru à 1 modulo $\ell(\zeta-1)$.

$(iii)_3$ $\mathfrak{p} \in P_2$, on obtient dans ce cas :

PROPOSITION III.3.- <u>Si</u> $\mathfrak{p} \in P_2$ <u>alors</u> :

$$(\alpha,a)_{\mathfrak{p}} = \zeta^{S_{\mathfrak{p}}(q_{\mathfrak{p}}(\frac{\lambda_{\mathfrak{p}}(\alpha-1)(a-1)}{\ell(\zeta-1)}))}$$

<u>si</u> a <u>est congru à</u> 1 <u>modulo</u> $\mathfrak{p}^{t_{\mathfrak{p}}}$.

Démontrons ce résultat à partir de l'énoncé de la proposition II.3. On sait que $M \in \mathfrak{p}^{t_{\mathfrak{p}}}$, $M \notin \mathfrak{p}^{t_{\mathfrak{p}}+1}$ (théorie de la ramification supérieure) et que $Tr_{K'/k'}(M) \equiv -N_{K'/k'}(M) \equiv -M^{\ell}$ modulo $\pi^{t_{\mathfrak{p}}+1}$ (on utilise le lemme 5 p. 91 de [22] et le fait que $\pi^{\sigma-1} \equiv 1 \bmod \pi^{t_{\mathfrak{p}}}$) . Posons $\xi = \pi^{\sigma-1}$, alors $M = \xi-1 = \varphi\pi^{t_{\mathfrak{p}}}$, φ unité $\mathfrak{p}$-adique ; on aura $M^{\ell} = (\xi-1)^{\ell} = \varphi^{\ell}\pi^{\ell t_{\mathfrak{p}}}$.

Posons $\theta = 1+\pi^{\lambda_{\mathfrak{p}}}\epsilon$, ϵ unité ; alors

$$(\frac{\theta-1}{\epsilon})^{\sigma-1} = (\pi^{\lambda_{\mathfrak{p}}})^{\sigma-1} = \xi^{\lambda_{\mathfrak{p}}} \equiv 1 + \lambda_{\mathfrak{p}}\varphi\pi^{t_{\mathfrak{p}}} \bmod \pi^{t_{\mathfrak{p}}+1}$$

et

$$(\xi^{\lambda_{\mathfrak{p}}}-1)^{\ell} \equiv \lambda_{\mathfrak{p}}^{\ell}\varphi^{\ell}\pi^{\ell t_{\mathfrak{p}}} \bmod \pi^{\ell(t_{\mathfrak{p}}+1)} ,$$

d'où la relation $((\frac{\theta-1}{\epsilon})^{\sigma-1}-1)^{\ell} \equiv \lambda_{\mathfrak{p}}^{\ell}M^{\ell} \bmod \pi^{\ell(t_{\mathfrak{p}}+1)}$. Comme $\lambda_{\mathfrak{p}}$ est premier à ℓ (proposition I.2), on est ramené au calcul de $((\frac{\theta-1}{\epsilon})^{\sigma-1}-1)^{\ell}$ modulo $\pi^{\ell(t_{\mathfrak{p}}+1)}$.

On a donc $(\frac{\theta-1}{\epsilon})^{\sigma-1}-1 = \frac{\zeta\theta-1}{\theta-1}\epsilon^{1-\sigma}-1 = \frac{(\zeta\theta-1)\epsilon^{1-\sigma}-\theta+1}{\theta-1}$, or $\epsilon^{1-\sigma} \equiv 1 \bmod \pi^{t_{\mathfrak{p}}+1}$ et $\frac{\zeta\theta-1}{\theta-1} \equiv 1 \bmod \pi^{t_{\mathfrak{p}}}$, donc

$$\frac{(\zeta\theta-1)\epsilon^{1-\sigma}-\theta+1}{\theta-1} \equiv \frac{\zeta\theta-\theta}{\theta-1} \bmod \pi^{t_{\mathfrak{p}}+1} ;$$

comme $\frac{(\zeta-1)\theta}{\theta-1} \in (\pi)^{t_\wp}$ on en déduit que $((\frac{\theta-1}{\varepsilon})^{\sigma-1}-1)^{\ell} \equiv \lambda_\wp^{\ell} M^{\ell} \equiv \frac{(\zeta-1)^{\ell}\theta^{\ell}}{(\theta-1)^{\ell}}$ mod $\pi^{\ell(t_\wp+1)}$, ce qui s'écrit encore $M^{\ell} \equiv \frac{(\zeta-1)^{\ell}\alpha}{\lambda_\wp(\theta-1)^{\ell}}$ mod $\pi^{\ell(t_\wp+1)}$, soit $M^{\ell} \equiv \frac{(\zeta-1)^{\ell}}{\lambda_\wp(\theta-1)^{\ell}}$ (car $\alpha \equiv 1 \bmod \pi^{\ell\lambda_\wp}$).

Montrons enfin que $(\theta-1)^{\ell} \equiv \alpha-1 \bmod \pi^{\ell a_\wp}$, avec $a_\wp = v_\wp(1-\zeta)$; on a $\alpha-1 = \theta^{\ell}-1 = \prod_{k=1}^{\ell}(\theta-\zeta^k)$ et pour $k \neq k'$, $\theta-\zeta^k = \theta-1+1-\zeta^k$; or la valuation de $\theta-1$ est strictement plus petite que celle de $1-\zeta^k$ qui est égale à $\ell a_\wp$; d'où $\alpha-1 \equiv (\theta-1)^{\ell} \bmod \pi^{t+\lambda_\wp\ell}$. Finalement :

$-\frac{a-1}{M^{\ell}} \equiv -\frac{\lambda_\wp(a-1)(\alpha-1)}{(\zeta-1)^{\ell}}$ modulo $\pi^{t_\wp}$, c'est-à-dire que $\frac{a-1}{Tr(M)}$ est congru à $\frac{\lambda_\wp(a-1)(\alpha-1)}{\ell(\zeta-1)}$ modulo $\wp$.

2. Propriété fondamentale du symbole $(\alpha,a)_\wp$.

On a le résultat suivant :

PROPOSITION III.4.- Soit $\wp$ une place quelconque de k' ; le symbole $(\alpha,a)_\wp$, $a \in k^*$, $\alpha \in k'^*$ tel que $q(\alpha) \in \mathfrak{X}^*$, ne dépend que de la place $\mathfrak{p}$ de k en dessous de $\wp$.

Démonstration.- On peut supposer que $\wp$ est un idéal premier de k' et que ℓ est différent de 2 car autrement la proposition est triviale.

Soit $\wp^s$ un conjugué de $\wp$. Supposons d'abord que $\wp$ ne divise pas ℓ. Soit g un entier congru à $\varkappa^*(s)$ modulo ℓ ; la proposition III.2 montre que $gv_{\wp^s}(\alpha) \equiv v_\wp(\alpha) \bmod \ell$; on a

$$(\alpha,a)_\wp \equiv (\alpha^{v_\wp(a)} a^{-v_\wp(\alpha)})^{\frac{q-1}{\ell}} \bmod \wp$$

soit

$$(\alpha,a)_\wp^s = (\alpha,a)_\wp^g \equiv (\alpha^{gv_\wp(a)} a^{-v_\wp(\alpha)})^{\frac{q-1}{\ell}} \bmod \wp^s,$$

$$(\alpha,a)_\wp^g \equiv (\alpha^{v_\wp(a)} a^{-v_{\wp^s}(\alpha)})^{\frac{q-1}{\ell}g} \bmod \wp^s ;$$

or on a précisément $(\alpha,a)_{\wp^s} \equiv (\alpha^{v_\wp(\alpha)} a^{-v_{\wp^s}(\alpha)})^{\frac{q-1}{\ell}} \bmod \wp^s$, d'où l'égalité des symboles, compte tenu du fait que ce sont des racines $\ell^{\text{èmes}}$ de l'unité et que $\wp$ ne divise pas ℓ .

Supposons maintenant que $\wp$ divise ℓ .

Le symbole $(\alpha,a)_\wp$ est de la forme $\zeta^{S_\wp(q_\wp(c))}$, $c \in k'$ convenable. On remarque ([22] p. 223) que $S_\wp$ ne dépend pas de $\wp$; par conséquent, $S_\wp(q_\wp(c)) = q_\wp(S(c))$ et il existe $q \in \mathbb{Z}$ tel que $S(c) \equiv q \bmod \wp$; posons $(\alpha,a)_{\wp^s} = \zeta^{S(q_{\wp^s}(c_s))}$; il existe $q_s \in \mathbb{Z}$ vérifiant $S(c_s) \equiv q_s \bmod \wp$ et on remarque que $(S(c))^s = S(c^s) \equiv q \bmod \wp^s$; il suffit donc de démontrer la relation

$$c^s \equiv c_s \bmod \wp^s \ ;$$

les différentes expressions possibles pour c sont :

$$\frac{a-1}{\ell(\zeta-1)} v_\wp(\alpha) \ ,$$

$$\frac{\alpha-1}{\ell(\zeta-1)} v_\wp(a) \ ,$$

$$\frac{\lambda_\wp(a-1)(\alpha-1)}{\ell(\zeta-1)} \ ,$$

pour chacune d'elles on vérifie directement la relation ci-dessus.

Remarque III.2.- Sous les hypothèses de la proposition précédente on peut sans inconvénient noter le symbole $(\alpha,a)_\wp$ par $(\alpha,a)_p$.

CHAPITRE IV

ETUDE DU ℓ-GROUPE DES CLASSES D'UNE EXTENSION CYCLIQUE DE DEGRE PREMIER ℓ D'UN CORPS k

Soit K/k une extension cyclique de degré premier ℓ ; soient H le groupe de Galois de K/k et σ un générateur de H .Les notations S_K , A_K , E_K , $\mathcal{J}(K)$, $\mathcal{J}'_o(K)$, $\mathcal{J}_o(K)$, $\mathcal{H}'(K)$ et $\mathcal{H}(K)$ (resp S_k , A_k , E_k , $\mathcal{J}(k)$, $\mathcal{J}'_o(k)$, $\mathcal{J}_o(k)$, $\mathcal{H}'(k)$ et $\mathcal{H}(k)$) ont été définies dans le chapitre I.

Si $\mathcal{J}$ est un sous-groupe quelconque de $\mathcal{J}(K)$ on pose $\mathcal{J}_o = \mathcal{J} \cap \mathcal{J}_o(K)$. On note N l'application norme de $\mathcal{J}(K)$ dans $\mathcal{J}(k)$ et on note encore N l'application de $\mathcal{H}(K)$ dans $\mathcal{H}(k)$ qui se déduit de la précédente par passage aux classes. On pose $\nu = 1+\sigma+\ldots+\sigma^{\ell-1}$. On note j l'homomorphisme extension des idéaux de $\mathcal{J}(k)$ dans $\mathcal{J}(K)$ ainsi que l'application de $\mathcal{H}(k)$ dans $\mathcal{H}(K)$ qui s'en déduit : on rappelle que l'action de $j \circ N$ est identique à celle de ν (sur $\mathcal{J}(K)$ et $\mathcal{H}(K)$).

A. Propriétés élémentaires de $\mathcal{H}(K)$.

1. Classes invariantes dans K/k .

Une ℓ-classe $h \in \mathcal{H}(K)$ est dite invariante (ou "ambige") si elle est fixe par tout élément de H . On notera par la suite $\mathcal{H}_1$ le sous-groupe de $\mathcal{H}(K)$ formé des classes invariantes par H .

Une formule (dite, usuellement, "formule des classes ambiges") donnée par C. Chevalley ([7]) permet de calculer $\mathcal{H}'_1$, le nombre de ℓ-classes au sens ordinaire invariantes par H :

$$|\mathcal{H}'_1| = \frac{|\mathcal{H}'(k)|\,\ell^{t'-1}}{(E_k : E_k \cap NK^*)} ,$$

où t' est le nombre de places ramifiées dans K/k .

THEOREME IV.1.- Soit t le nombre d'idéaux premiers ramifiés dans K/k et soit E_k^+ le sous-groupe de E_k formé des unités totalement positives de k $(E_k^+ = E_k \cap \operatorname{Ker} S_k)$. Alors :

$$|\mathcal{H}_1| = \frac{|\mathcal{H}(k)|\,\ell^{t-1}}{(E_k^+ : E_k^+ \cap NK^*)} .$$

Démonstration.- Lorsque ℓ est impair, les notions de ℓ-classes au sens ordinaire et au sens restreint coïncident et $t' = t$; la formule de Chevalley convient donc, compte tenu du fait que dans ce cas $(E_k^+ : E_k^+ \cap NK^*) = (E_k : E_k \cap NK^*)$.

Supposons maintenant $\ell = 2$ et posons : $\overline{K^*} = \{\alpha \in K^*, S_K(N\alpha) = 1\}$, $\overline{E_K} = \{\varepsilon \in E_K, S_K(N\varepsilon) = 1\}$, $E_k^{++} = \{\varepsilon \in E_k, S_K(\varepsilon) = 1\}$ et $\Gamma = \{\alpha \in K^*, N\alpha \in E_k\}$.

LEMME IV.1.- On a les suites exactes :

$$1 \to \operatorname{Ker}\theta \to \mathcal{H}_1 \xrightarrow{\theta} \mathcal{H}'_1 \xrightarrow{\mu} S_K(\Gamma)/S_K(E_K K^{*\sigma-1}) \to 1 ,$$

$$1 \to \overline{E}_K/E_K^+ \to \overline{K}^*/\operatorname{Ker} S_K \xrightarrow{\varphi} \operatorname{Ker}\theta \xrightarrow{\psi} S_K(\overline{E}_K)/S_K(NE_K) \to 1 ,$$

où les homomorphismes θ , μ , φ et ψ sont ainsi définis : si $Cl'(\mathfrak{A}) \in \mathcal{H}'_1$ alors $\mathfrak{A}^{\sigma-1} = \alpha A_K$, $\alpha \in K^*$; $\mu(cl'(\mathfrak{A}))$ est alors l'image de $S(\alpha)$ dans $S_K(\Gamma)/S_K(E_K K^{*\sigma-1})$; on pose $\theta(cl(\mathfrak{A})) = cl'(\mathfrak{A})$, on a donc $\operatorname{Ker}\theta = \{cl(\gamma A_K), S_K(\gamma^{\sigma-1}) \in S_K(E_K)\}$ et à $cl(\gamma A_K)$ l'homomorphisme ψ associe l'image de $S_K(\gamma^{\sigma-1})$ dans $S_K(\overline{E}_K)/S_K(NE_K)$; enfin, l'homomorphisme φ associe à l'image de γ dans $\overline{K}^*/\operatorname{Ker} S_K$ la classe $cl(\gamma A_K)$.

On vérifie que les définitions précédentes ont un sens, l'exactitude des suites proposées est alors une conséquence immédiate des définitions.

On obtient alors :

$$|\mathcal{H}_1| = |\mathcal{H}'_1| \frac{|\mathrm{Ker}\ \theta|}{|S_K(\Gamma)/S_K(E_K K^{*\sigma-1})|} = |\mathcal{H}'_1| \frac{|\bar{K}^*|}{|\mathrm{Ker}\ S_K|} \frac{|S_K(\bar{E}_K)|}{|S_K(NE_K)|} \frac{|E_K^+|}{|\bar{E}_K|} \frac{|S_K(E_K K^{*\sigma-1}|}{|S_K(\Gamma)|}$$

LEMME IV.2.- On a les suites exactes :

$$1 \to S_K(E_K) \to S_K(E_K K^{*\sigma-1}) \to S_K(K^{*\sigma-1})/S_K(\bar{E}_K) \to 1 ,$$

$$1 \to S_K(K^{*\sigma-1}) \to S_K(\Gamma) \to S_K(E_k \cap NK^*) \to 1 ,$$

$$1 \to S_K(\bar{E}_K) \to S_K(E_K) \to S_K(NE_K) \to 1 ,$$

$$1 \to E_k^{++}/E_k^{++} \cap NK^* \to E_k/E_k \cap NK^* \to S_K(E_k)/S_K(E_k \cap NK^*) \to 1 .$$

Le lemme IV.2 conduit immédiatement à l'expression :

$$|\mathcal{H}_1| = |\mathcal{H}'_1| \frac{|\bar{K}^*|}{|\mathrm{Ker}\ S_K|\ |S_K(E_k \cap NK^*)|} = \frac{|\mathcal{H}'(k)|\, 2^{t'-1}}{(E_k^{++}:E_k^{++} \cap NK^*)} \frac{|S_K(\bar{K})|}{|S_K(E_k)|} ,$$

(en utilisant la formule de Chevalley et compte tenu des isomorphismes $\bar{K}^*/\mathrm{Ker}\ S_K \simeq S_K(\bar{K})$ et $\bar{E}_K/E_K^+ \simeq S_K(\bar{E}_K)$) ; un calcul direct montre que $|S_K(\bar{K})| = 2^{\rho_1}$.

Reste à exprimer $|\mathcal{H}'(k)|$ en fonction de $|\mathcal{H}(k)|$; on considère pour cela la suite exacte :

$$1 \to \mathcal{J}'_0(k)/\mathcal{J}_0(k) \to \mathcal{J}(k)/\mathcal{J}_0(k) \to \mathcal{J}(k)/\mathcal{J}'_0(k) \to 1$$

qui donne $|\mathcal{H}'(k)| = \dfrac{|\mathcal{H}(k)|}{|\mathcal{J}'_0(k)/\mathcal{J}_0(k)|}$.

On a alors $\mathcal{J}'_0(k)/\mathcal{J}_0(k) \simeq S_k(k)/S_k(E_k)$, d'où

$$|\mathcal{H}_1| = \frac{|\mathcal{H}(k)|\ 2^{t'-1}\ 2^{\rho_1}}{(E_k^{++}:E_k^{++} \cap NK^*)\ |S_k(k)|} \frac{|S_k(E_k)|}{|S_K(E_k)|} = |\mathcal{H}(k)| \frac{2^{t'-1} 2^{\rho_1}}{(E_k^{++}:E_k^{++} \cap NK^*) 2^{\rho_1+\rho_2}} \frac{|S_k(E_k)|}{|S_K(E_k)|}$$

$$= |\mathcal{H}(k)| \frac{2^{t-1}}{(E_k^{++}:E_k^{++} \cap NK^*)} \frac{|S_k(E_k)|}{|S_K(E_k)|} .$$

On remarque alors que $E_k^+ \cap NK^* = E_k^{++} \cap NK^*$: si K_i est imaginaire et k_i réel, la norme d'un nombre quelconque est positive dans k_i et ε_i est positive ; si K_i et k_i sont réels alors ε_i est positive dans k car ε est positive dans K .

On a donc :

$$(E_k^{++} : E_k^{++} \cap NK^*) = (E_k^{++} : E_k^+)(E_k^+ : E_k^+ \cap NK^*)$$

et les deux suites exactes :

$$1 \to E_k^+ \to E_k \to S_k(E_k) \to 1 ,$$

$$1 \to E_k^{++} \to E_k \to S_K(E_k) \to 1 ,$$

conduisent immédiatement au résultat.

COROLLAIRE IV.1- Lorsque k est égal à $\mathbb{Q}$ ou à un corps quadratique réel principal, $|\mathcal{H}_1| = \ell^{t-1}$, t étant le nombre d'idéaux premiers ramifiés dans K/k .

COROLLAIRE IV.2- Lorsque $E_k^+ \subset N(E_K^+)$, E_K^+ désignant le groupe des unités totalement positives de K , on peut engendrer $\mathcal{H}_1$ par des classes d'idéaux invariants, donc des classes d'idéaux premiers ramifiés dans K/k et par des classes d'idéaux de k étendus à K .

On a la suite exacte :

$$1 \to \mathcal{H}_1^o \to \mathcal{H}_1 \to E_k^+ \cap NK^*/NE_K^+ \to 1 ,$$

où $\mathcal{H}_1^o$ désigne le sous-groupe de $\mathcal{H}_1$ formé des classes des idéaux de K invariants par H : soit $cl(\mathfrak{A}) \in \mathcal{H}_1$, il existe $\alpha \in K^{*+}$ tel que $\mathfrak{A}^{\sigma-1} = \alpha A_K$ et $N\alpha$ est une unité ε de k totalement positive (proposition I.1) ; l'application qui associe à $cl(\mathfrak{A}) \in \mathcal{H}_1$ l'image de ε dans $E_k^+ \cap NK^*/NE_K^+$ est un homomorphisme surjectif dont le noyau est $\mathcal{H}_1^o$ (vérification immédiate).

Par exemple, si $k = \mathbb{Q}$ et si K est une extension quadratique de $\mathbb{Q}$, le corollaire précédent s'applique : on a $E_k = \{\pm 1\}$ donc $E_k^+ = \{1\}$ et le groupe $\mathcal{H}_1$ est engendré par les classes des idéaux premiers ramifiés.

Remarque IV.1.- On a la relation suivante :

$$|\mathrm{Ker}\ j| = \frac{|\mathcal{H}_R|\,|E_k^+/NE_K^+|}{|\mathrm{Im}\ j \cap \mathcal{H}_R|\,\ell^{t-1}} ,$$

où $\mathcal{H}_R$ est le sous-groupe de $\mathcal{H}(K)$ engendré par les classes des idéaux premiers ramifiés dans K/k (pour $t = 0$, on retrouve l'énoncé de [16] p. 192 ainsi que le théorème 94 de Hilbert ([15])).

Cette relation se démontre en considérant la suite exacte ci-dessus ainsi que les deux suivantes (triviales) :

$$1 \to \mathrm{Ker}\ j \to \mathcal{H}(k) \xrightarrow{j} \mathrm{Im}\ j \to 1 ,$$

$$1 \to \mathcal{H}_R \cap \mathrm{Im}\ j \to \mathrm{Im}\ j \to \mathcal{H}_1^{o}/\mathcal{H}_R \to 1 .$$

2. Etude d'une filtration associée à certains H-modules.

Comme $\mathcal{H}(K)$ est un ℓ-groupe abélien fini muni d'une structure de H-module, on est amené à étudier la structure de tels H-modules.

Soit donc M un ℓ-groupe abélien fini muni d'une structure de H-module. On pose :

$$M_i = \{h \in M ,\ h^{(\sigma-1)^i} = 1\} ,$$

$$M^{(n)} = \{h \in M ,\ h^{\ell^n} = 1\} ,$$

pour tout $i \geq 0$ et tout $n \geq 0$.

PROPOSITION IV.1.-

(i) On a $M_i \subset M_{i+1}$ et $M_i = M_{i+1}$ si et seulement si $M_i = M$, $i \geq 0$;

(ii) les ordres des groupes M_{i+1}/M_i décroissent vers 1 ;

(iii) lorsque $M^{\vee} = \{1\}$ on a pour tout $n \geq 0$ la relation $M^{(n)} = M_{n(\ell-1)}$.

Remarquons que cette proposition précise l'un des problèmes que nous avons en vue et qui concerne l'existence de classes "exceptionnelles" (i.e.

non invariantes) : de telles classes existeront si et seulement si $M_1 \neq M_2$ (avec $M = \mathcal{H}(K)$) et pour $\ell = 2$, une classe d'ordre 2 ne pourra être exceptionnelle que pour $M^{\nu} \neq \{1\}$.

Démonstration.- Si $h^{(\sigma-1)^i} = 1$ alors $h^{(\sigma-1)^{i+1}} = 1$ et $M_i \subset M_{i+1}$; on a $M_{i+1}^{\sigma-1} \subset M_i$; l'application $h \to h^{\sigma-1}$ donne par passage au quotient un homomorphisme de M_{i+1}/M_i dans M_i/M_{i-1} qui est injectif ; d'où les assertions (i) et (ii) compte tenu du fait que le H-module M est de la forme M_i pour i suffisamment grand.

Le polynôme $(X-1)^{\ell-1} - (X^{\ell-1}+\ldots+X+1)$ est le polynôme nul modulo $\ell\mathbb{Z}[X]$; il existe donc $A \in \mathbb{Z}[X]$ tel que

$$1 + X + \ldots + X^{\ell-1} = (X-1)^{\ell-1} - \ell A(X) ,$$

ce qui montre que $A(1) = -1$ et que

$$\nu = (\sigma-1)^{\ell-1} - \ell A(\sigma) \quad \text{dans} \quad \mathbb{Z}[H] ;$$

vérifions que dans $\mathbb{Z}_\ell[H]$, $A(\sigma)$ est inversible :

Dans $\mathbb{Q}_\ell[X]$ le théorème de Bezout, appliqué aux polynômes premiers entre eux $X^{\ell}-1$ et $A(X)$, montre l'existence de U et $V \in \mathbb{Q}_\ell[X]$ tels que

$$U(X)(X^{\ell}-1) + V(X)A(X) = 1 ;$$

on sait que l'on peut supposer le degré de V strictement inférieur à ℓ. Ce choix étant fait on peut encore supposer que U et V sont dans $\mathbb{Z}_\ell[X]$ à condition d'écrire la relation précédente sous la forme $U(X)(X^{\ell}-1)+V(X)A(X) = \ell^n$, $n \geq 0$, et de supposer que les coefficients de U et V ne sont pas tous divisibles par ℓ. Si n était strictement positif on aurait dans $\mathbb{F}_\ell[X]$ la relation $\overline{U}(X)(X^{\ell}-\overline{1}) = -\overline{V}(X)\overline{A}(X)$; or $\overline{A}(\overline{1}) = -\overline{1}$ et $\overline{V}$ ne peut pas être le polynôme nul, par conséquent $\overline{V}(X)$ admettrait $\overline{1}$ comme racine multiple d'ordre ℓ et serait de degré ℓ au moins, ce qui est absurde. On a donc, dans $\mathbb{Z}_\ell[H]$, $V(\sigma)A(\sigma) = 1$.

Le $\mathbb{Z}_\ell[H]$-module M étant annulé par ν, on a, pour tout $h \in M$, $h^{(\sigma-1)^{\ell-1}} = h^{\ell A(\sigma)}$, soit pour tout $n \geq 1$, $h^{(\sigma-1)^{n(\ell-1)}} = h^{\ell^n A^n(\sigma)}$, ce qui montre que $h^{(\sigma-1)^{n(\ell-1)}} = 1$ si et seulement si $h^{\ell^n} = 1$, d'où l'assertion.

PROPOSITION IV.2.- Soit R_q le ℓ^q-rang de M (i.e. la dimension sur $\mathbb{F}_\ell$ de l'espace vectoriel $M^{\ell^{q-1}}/M^{\ell^q}$) ; alors R_q est égal à la dimension sur $\mathbb{F}_\ell$ de $M^{(q)}/M^{(q-1)}$.

Si $M^\nu = \{1\}$, alors on a la relation

$$\ell^{R_q} = \prod_{i=(q-1)(\ell-1)}^{q(\ell-1)-1} |M_{i+1}/M_i| \quad .$$

COROLLAIRE IV.3.- On suppose $M^\nu = \{1\}$. Soit n le plus petit entier tel que $M_n = M$; on pose $n = a(\ell-1)+b$, $a \geq 0$, $0 \leq b < \ell-1$. Si les quotients M_{i+1}/M_i sont d'ordre ℓ alors on a l'isomorphisme :

$$M \simeq (\mathbb{Z}/\ell^{a+1}\mathbb{Z})^b \times (\mathbb{Z}/\ell^a\mathbb{Z})^{\ell-1-b} \quad .$$

Démonstration.- Considérons le groupe cyclique $C_q = \mathbb{Z}/\ell^q\mathbb{Z}$ opérant trivialement sur M ; le quotient de Herbrand :

$$h_q(A) = \frac{|\hat{H}^0(C_q, M)|}{|\hat{H}^1(C_q, M)|} \quad ,$$

est donc égal à $\dfrac{|M^{C_q}/M^{\ell^q}|}{|M^{(q)}/\{1\}|} = \dfrac{|M|}{|M^{\ell^q}||M^{(q)}|}$. Comme M est fini, on a $h_q(A) = 1$ ([22] p. 142), quel que soit $q \geq 1$; d'où :

$$\frac{|M^{(q)}|}{|M^{(q-1)}|} = \frac{|M^{\ell^{q-1}}|}{|M^{\ell^q}|} \quad ,$$

ce qui démontre la première partie de la proposition. La seconde partie résulte de la relation (proposition IV.1, (iii)) :

$$M^{(q)}/M^{(q-1)} = M_{q(\ell-1)}/M_{(q-1)(\ell-1)} \quad .$$

Le corollaire se démontre en calculant les ℓ^q-rangs : pour $q \leq a$, $\ell^{R_q} = \prod_{i=(q-1)(\ell-1)}^{q(\ell-1)-1} |M_{i+1}/M_i| = \ell^{\ell-1}$; pour $q = a+1$, on a

$$\ell^{R_{a+1}} = \prod_{i=a(\ell-1)}^{a(\ell-1)+\ell-2} |M_{i+1}/M_i| = \prod_{i=a(\ell-1)}^{n-1} |M_{i+1}/M_i| = \ell^b \quad ,$$

d'où l'isomorphisme.

PROPOSITION IV.3.- Soit M tel que $M^{\nu} \neq \{1\}$. Soit n le plus petit entier tel que $M_n = M$; on pose $n = a(\ell-1) + b$, $0 \leq b < \ell-1$. On suppose que $|M_{i+1}/M_i| = \ell$ pour $0 \leq i < n$.

(i) si $n < \ell$, alors $M \simeq (\mathbb{Z}/\ell^2\mathbb{Z}) \times (\mathbb{Z}/\ell\mathbb{Z})^{n-2}$;

(ii) si $n = \ell$, alors $M \simeq (\mathbb{Z}/\ell\mathbb{Z})^{\ell}$ ou bien $M \simeq (\mathbb{Z}/\ell^2\mathbb{Z}) \times (\mathbb{Z}/\ell\mathbb{Z})^{\ell-2}$;

(iii) si $n > \ell$, alors $M \simeq (\mathbb{Z}/\ell^{a+1}\mathbb{Z})^{b} \times (\mathbb{Z}/\ell^{a}\mathbb{Z})^{\ell-1-b}$.

Remarque IV.2.- Si $\ell = 2$ il ne reste que les possibilités $M \simeq \mathbb{Z}/\ell^n\mathbb{Z}$ ou $M \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Si $\ell = 3$, le cas (i) ne peut avoir lieu que pour $n = 2$.

Démonstration.-

LEMME IV.3.- Pour tout $q \geq 1$ on a la suite exacte d'espaces vectoriels :

$$1 \to M_1/M_n^{\ell^q} \cap M_1 \to M_n^{\ell^{q-1}}/M_n^{\ell^q} \xrightarrow{\sigma-1} M_{n-1}^{\ell^{q-1}}/M_{n-1}^{\ell^q} \to 1 .$$

On a, pour $0 \leq i < n$, $M_{i+1}^{\sigma-1} = M_i$: en effet, la suite exacte $1 \to M_1 \to M_{i+1} \xrightarrow{\sigma-1} M_{i+1}^{\sigma-1} \to 1$ montre que $|M_{i+1}/M_{i+1}^{\sigma-1}| = |M_1/\{1\}| = \ell$; comme $M_{i+1}^{\sigma-1} \subset M_i$ et que $|M_{i+1}/M_i| = \ell$ on a bien $M_{i+1}^{\sigma-1} = M_i$; d'où la surjectivité dans la suite proposée.

Détermination du noyau : soit $x \in M_n^{\ell^{q-1}}$ tel que $x^{\sigma-1} = y^{\ell^q}$, $y \in M_{n-1}$. Il existe $z \in M_n$ tel que $y = z^{\sigma-1}$ et $x^{\sigma-1} = z^{\ell^q(\sigma-1)}$; par suite $(xz^{-\ell^q})^{\sigma-1} = 1$ et $xz^{-\ell^q} \in M_1$ d'où l'inclusion $M_1/M_n^{\ell^q} \cap M_1 \subset \mathrm{Ker}(\sigma-1)$, l'inclusion inverse étant triviale.

LEMME IV.4.- Si $n \geq \ell+1$ alors le ℓ-rang de M est égal au ℓ-rang de M_{n-1} .

Soit $x \in M_{n-1} \setminus M_{n-2}$ (ce qui a un sens car on a $n \geq \ell+1 \geq 3$) et soit $y = x^{(\sigma-1)^{n-2}}$; on a $y \in M_1$ et $y \neq 1$ à cause du choix de x . Il existe $B(\sigma) \in \mathbb{Z}_{\ell}[H]$ tel que $(\sigma-1)^{n-2} = B(\sigma)(\sigma-1)^{\ell-1}$ et en posant $z = x^{B(\sigma)}$

on obtient $y = z^{(\sigma-1)^{\ell-1}}$. Comme $M_{n-1} = M^{\sigma-1}$ on a $M_{n-1}^{\nu} = \{1\}$ donc, ici, $z^{\nu} = 1$ et $z^{(\sigma-1)^{\ell-1}} = z^{\ell A(\sigma)}$, ce qui montre que $y \in M^{\ell}$; l'hypothèse $|M_1| = \ell$ entraîne alors l'inclusion $M_1 \subset M^{\ell}$. Le lemme IV.3 appliqué avec $q = 1$ achève la démonstration du lemme IV.4.

Remarquons que pour $j \leq i$ on a, avec des notations évidentes, $(M_i)_j = M_j$; on peut donc appliquer les résultats du corollaire IV.3 à M_{n-1} . Pour $n \leq \ell$ la conclusion est immédiate (vu que $M^{\nu} \neq \{1\}$) .

Supposons $n \geq \ell+1$. Le lemme IV.3 montre que le ℓ^q-rang de M est supérieur ou égal à celui de M_{n-1} (d'une unité au plus) ; comme le ℓ^q-rang d'un groupe est fonction décroissante de q , le lemme IV.4 et la remarque ci-dessus montrent que, pour $q \leq [\frac{n-1}{\ell-1}]$, les ℓ^q-rangs de M et M_{n-1} sont égaux à $\ell-1$.

Posons $n-1 = a'(\ell-1)+b'$, $0 \leq b' < \ell-1$ (on a $a' = [\frac{n-1}{\ell-1}]$) . Le lemme IV.3 montre qu'il y a trois possibilités :

(i) $b' = 0$, nécessairement $R_{a'+1}(M) = 1$ et $R_{a'+1}(M_{n-1}) = 0$,

(ii) $b' > 0$ et les $\ell^{a'+1}$-rangs de M et M_{n-1} vérifient :

$$R_{a'+1}(M) = R_{a'+1}(M_{n-1}) + 1 ,$$

(iii) $b' > 0$, $R_{a'+1}(M) = R_{a'+1}(M_{n-1})$ et $R_{a'+2}(M) = 1$.

La proposition est démontrée si l'on démontre que le cas (iii) est impossible :

soit $x \in M$, $x \notin M_{n-1}$, $x^{\nu} \in M_1$ et $x^{\nu} = x^{(\sigma-1)^{\ell-1}} x^{-\ell A(\sigma)}$;

posons $x' = x^{(\sigma-1)^{\ell-1}}$ et $x'' = x^{-\ell A(\sigma)}$;

$x' \in M_{n-(\ell-1)} = M_{(a'-1)(\ell-1)+b'+1} \subset M_{a'(\ell-1)}$; or $M_{a'(\ell-1)} = (M_{n-1})_{a'(\ell-1)} = (M_{n-1})^{(a')}$. Comme $x \notin M_{n-1}$, on a $x^{\ell^{a'+1}} \neq 1$ soit $x''^{\ell^{a'}} \neq 1$. En résumé on a obtenu $x' \in (M_{n-1})^{(a')}$ et $x'' \notin (M_{n-1})^{(a')}$; comme $x^{\nu} \in M_1$ et que a' est non nul (on a supposé $n \geq \ell+1$) on a $x^{\nu} \in (M_{n-1})^{(a')}$ soit $x'' = x^{\nu} x'^{-1} \in (M_{n-1})^{(a')}$ ce qui est absurde.

Remarque IV.3.- Les résultats précédents s'appliquent au H-module $\mathcal{H}(K)$. La filtration $\{M_i\}_{i \geq 0}$ associée à $M = \mathcal{H}(K)$ est particulièrement importante

à cause des résultats suivants ; posons : $\mathcal{H}_i = \{h \in \mathcal{H}(K), h^{(\sigma-1)^i} = 1\}$ et $\mathcal{H}^{(n)} = \{h \in \mathcal{H}(K), h^{\ell^n} = 1\}$, $i \geq 0$, $n \geq 0$.

B. Résultats généraux concernant la structure de $\mathcal{H}(K)$

On rappelle que $\mathcal{H}(K)$ désigne le ℓ-sous-groupe de Sylow du groupe des classes au sens restreint de K .

1. Démonstration d'un résultat préliminaire.

THEOREME IV.2.- Soit $\mathcal{H}$ un sous-H-module de $\mathcal{H}(K)$ et soit $\tilde{\mathcal{H}}$ l'ensemble formé par les $h \in \mathcal{H}(K)$ tels que $h^{\sigma-1} \in \mathcal{H}$;

(i) $\tilde{\mathcal{H}}$ est un sous-H-module de $\mathcal{H}(K)$ qui contient $\mathcal{H}$ et $\mathcal{H}_1$.

(ii) pour tout sous-H-module $\mathcal{J}$ de $\mathcal{J}(K)$ dont l'image dans $\mathcal{H}(K)$ est égale à $\mathcal{H}$ et qui est tel que $\mathcal{J} \cap \mathcal{J}(K)^{\sigma-1} = \mathcal{J}^{\sigma-1}$ on a la suite exacte de $\mathbb{F}_\ell[H]$-modules :

$$1 \to N\mathcal{J}_o/(N\mathcal{J} \cap \mathcal{J}_o(k))^\ell \to N\mathcal{J} \cap N\mathcal{J}_o(K)/(N\mathcal{J} \cap \mathcal{J}_o(k))^\ell \xrightarrow{\bar{\varphi}} \tilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1 \to 1 ,$$

où $\mathcal{J}_o = \mathcal{J} \cap \mathcal{J}_o(K)$.

Remarque IV.4.- D'après un résultat connu ([19], chap. VIII, §4) on sait que toute classe d'idéaux (au sens restreint) contient un idéal premier. Représentons tout élément de $\mathcal{H}$ par un idéal premier ; alors le H-module $\mathcal{J}$ engendré par ces idéaux vérifie la condition $\mathcal{J} \cap \mathcal{J}(K)^{\sigma-1} = \mathcal{J}^{\sigma-1}$.

Démonstration du théorème.- L'assertion (i) est évidente ; étudions maintenant la partie (ii) :

a) Définition d'un homomorphisme φ de $N\mathcal{J} \cap N\mathcal{J}_o(K)$ dans $\tilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1$.

Soit $\alpha \in N\mathcal{J} \cap N\mathcal{J}_o(K)$; il existe $\mathfrak{A}_o \in \mathcal{J}$ et $\alpha \in K^{*+}$ tels que $\alpha = N\mathfrak{A}_o = N(\alpha A_K)$; l'idéal $\mathfrak{A}_o \alpha^{-1} A_K$ étant de norme A_k , il existe $\mathfrak{A} \in \mathcal{J}(K)$

tel que :

$$(1) \qquad \mathfrak{A}_o = \alpha A_K \mathfrak{A}^{\sigma-1} .$$

On note $\varphi(\mathfrak{a})$ l'image de la classe de $\mathfrak{A}$ dans $\tilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1$. Montrons que $\varphi(\mathfrak{a})$ ne dépend pas des choix effectués. Si $\mathfrak{a} = N\mathfrak{A}'_o = N(\alpha' A_K)$, $\mathfrak{A}'_o \in \mathcal{J}$, $\alpha' \in K^{*+}$, alors, en vertu de l'hypothèse $\mathcal{J} \cap \mathcal{J}(K)^{\sigma-1} = \mathcal{J}^{\sigma-1}$, il existe $\mathfrak{b} \in \mathcal{J}$ et $\mathfrak{c} \in \mathcal{J}(K)$ tels que :

$$(2) \qquad \mathfrak{A}'_o = \mathfrak{A}_o \mathfrak{b}^{\sigma-1} ,$$

$$(3) \qquad \alpha' A_K = \alpha A_K \mathfrak{c}^{\sigma-1} ;$$

au couple $(\mathfrak{A}'_o, \alpha')$ est associé un idéal $\mathfrak{A}'$ tel que :

$$(4) \qquad \mathfrak{A}'_o = \alpha' A_K \mathfrak{A}'^{\sigma-1} .$$

Les quatre relations ci-dessus conduisent à la relation

$$\mathfrak{A}^{\sigma-1} \mathfrak{A}'^{1-\sigma} \mathfrak{b}^{\sigma-1} = \alpha' \alpha^{-1} A_K ,$$

qui montre que la classe de l'idéal $\mathfrak{A}\mathfrak{A}'^{-1}\mathfrak{b}$ est dans $\mathcal{H}_1$; comme $\mathfrak{b} \in \mathcal{J}$, $\mathfrak{A}$ et $\mathfrak{A}'$ ont la même image dans $\tilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1$. On a bien un homomorphisme et on vérifie qu'il est surjectif.

b) Définition de $\bar{\varphi}$.

Soit $\mathfrak{a}_o \in N\mathcal{J} \cap \mathcal{J}_o(k)$, $\mathfrak{a}_o = N\mathfrak{A}_o = \alpha_o A_k$ avec $\mathfrak{A}_o \in \mathcal{J}$, $\alpha_o \in k^{*+}$; posons $\mathfrak{a} = \mathfrak{a}_o^{\ell}$, alors $\mathfrak{a} = N(\mathfrak{a}_o A_K) = N(\alpha_o A_K)$; comme $\mathfrak{a}_o = N\mathfrak{A}_o$ on aura $\mathfrak{a}_o A_K = (N\mathfrak{A}_o) A_K = \mathfrak{A}_o^{\nu} \in \mathcal{J}$ (car $\mathcal{J}$ est un H-module), on aura aussi $\alpha_o A_K \in \mathcal{J}_o(K)$ car α_o est dans K^{*+} . On obtient la relation $\mathfrak{a}_o A_K = \alpha_o A_K \mathfrak{A}'^{\sigma-1}$ avec $\mathfrak{A}' = A_K$; donc Ker φ contient $(N\mathcal{J} \cap \mathcal{J}_o(k))^{\ell}$, d'où $\bar{\varphi}$ par passage au quotient.

c) Noyau de $\bar{\varphi}$.

Si $\mathfrak{a} \in N\mathcal{J}_o$, $\mathfrak{a} = N(\alpha A_K)$ avec $\alpha A_K \in \mathcal{J}$ et $\alpha \in K^{*+}$ on a alors $\alpha A_K = \alpha A_K (A_K)^{\sigma-1}$ et $\varphi(\mathfrak{a}) = 1$.

Réciproquement, soit $\mathfrak{a} \in N\mathcal{J} \cap N\mathcal{J}_o(K)$, $\mathfrak{a} = N\mathfrak{A}_o = N(\alpha A_K)$, $\mathfrak{A}_o \in \mathcal{J}$ et $\alpha \in K^{*+}$; $\mathfrak{A}_o = \alpha A_K \mathfrak{A}^{1-\sigma}$, la classe de $\mathfrak{A}$ étant dans $\mathcal{H}\mathcal{H}_1$. Il existe

$\beta \in K^{*+}$, $\mathfrak{A}_1 \in \mathcal{J}$ et $\mathfrak{A}'_1 \in \mathcal{J}(K)$ (tel que cl $\mathfrak{A}'_1 \in \mathcal{H}_1$) vérifiant $\mathfrak{A} = \mathfrak{A}_1\mathfrak{A}'_1\beta A_K$; alors $\mathfrak{A}^{\sigma-1} = \mathfrak{A}_1^{\sigma-1}\mathfrak{A}'^{\sigma-1}_1\beta^{\sigma-1}A_K$, soit $\mathfrak{A}^{\sigma-1} = \mathfrak{A}_1^{\sigma-1}\beta^{\sigma-1}\gamma A_K$ en écrivant $\mathfrak{A}'^{\sigma-1}_1$ sous la forme γA_K (on a alors $\gamma \in K^{*+}$ et $N\gamma \in E_k^+$) . On a donc $\alpha A_K = \mathfrak{A}_o\mathfrak{A}_1^{\sigma-1}\beta^{\sigma-1}\gamma A_K$, d'où $(\gamma^{-1}\alpha\beta^{1-\sigma})A_K = \mathfrak{A}_o\mathfrak{A}_1^{\sigma-1}$; comme $\mathfrak{A}_o$ et $\mathfrak{A}_1$ sont dans $\mathcal{J}$, on a $\mathfrak{A}_o\mathfrak{A}_1^{\sigma-1} = (\gamma^{-1}\alpha\beta^{1-\sigma})A_K \in \mathcal{J}_o$, d'où $N(\gamma^{-1}\alpha\beta^{1-\sigma}A_K) = N(\alpha A_K) = \mathfrak{a}$ et $\mathfrak{a}$ est bien un élément de $N\mathcal{J}_o$.

Remarque IV.5.- Lorsque l'hypothèse $\mathcal{J}\cap\mathcal{J}(K)^{\sigma-1} = \mathcal{J}^{\sigma-1}$ n'est pas vérifiée, on démontre sans difficulté que, dans la suite exacte du théorème IV.2, le terme $\tilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1$ doit être remplacé par un terme de la forme $\tilde{\mathcal{H}}/\mathcal{H}_{\mathcal{J}}\mathcal{H}_1$ où $\mathcal{H}_{\mathcal{J}}$ désigne l'ensemble des classes des idéaux $\mathfrak{b} \in \mathcal{J}(K)$ tels que $\mathfrak{b}^{\sigma-1} \in \mathcal{J}$ (on a $\mathcal{H} \subset \mathcal{H}_{\mathcal{J}}$ mais pas égalité en général).

2. Généralisation de la "formule des classes ambiges".

Nous avons en vue une formule explicite donnant la valeur de $|\tilde{\mathcal{H}}/\mathcal{H}|$ généralisant ainsi l'expression de $|\mathcal{H}_1|$ (théorème IV.1) (laquelle correspond à $\mathcal{H} = \{1\}$). Pour cela, nous allons chercher à remplacer les groupes d'idéaux qui interviennent dans la suite exacte du théorème précédent par des groupes de nombres convenables.

a) Définition du groupe Λ .

Les notations et hypothèses sont celles du théorème IV.2. On pose $I_o = N\mathcal{J}\cap\mathcal{J}_o(k)$ et on considère la suite exacte :

$$1 \to E_k^+ \to k^{*+} \xrightarrow{\psi} \mathcal{J}_o(k) \to 1 \ .$$

DEFINITION IV.1.- On pose :

$$\Lambda = \psi^{-1}(I_o) \ ;$$

c'est un sous-groupe de k^{*+} qui contient E_k^+ . On désigne par q l'homomorphisme canonique :

$$q : \Lambda \to \Lambda/\Lambda^{\ell} \ .$$

b) Résultats préliminaires.-

PROPOSITION IV.4- On a les suites exactes de $\mathbb{F}_\ell$-espaces vectoriels suivantes :

$$1 \to N\mathcal{J}_o/I_o^\ell \to I_o \cap N\mathcal{J}_o(K)/I_o^\ell \to \tilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1 \to 1$$

$$1 \to \Lambda \cap NK^*/\Lambda^\ell(E_k^+ \cap NK^*) \to I_o \cap N\mathcal{J}_o(K)/I_o^\ell \to 1$$

$$1 \to E_k^+ \cap NK^*/E_k^{+\ell} \to \Lambda \cap NK^*/\Lambda^\ell \to \Lambda \cap NK^*/\Lambda^\ell(E_k^+ \cap NK^*) \to 1$$

$$1 \to \Lambda \cap NK^*/\Lambda^\ell \to \Lambda/\Lambda^\ell \to \Lambda/\Lambda \cap NK^* \to 1$$

$$1 \to E_k^+ \cap NK^*/E_k^{+\ell} \to E_k^+/E_k^{+\ell} \to E_k^+/E_k^+ \cap NK^* \to 1 .$$

Démonstration.- La première suite n'est autre que celle du théorème IV.2, compte tenu de l'égalité (utilisant la proposition I.1,(i)) : $I_o \cap N\mathcal{J}_o(K) = N\mathcal{J} \cap N\mathcal{J}_o(K)$. Ceci étant, soit $x \in \Lambda \cap NK^*$; considérons xA_k , puis l'image de xA_k dans $I_o \cap N\mathcal{J}_o(K)/I_o^\ell$ (ce qui a un sens car $xA_k \in I_o$ $(x \in k^{*+})$ par définition et en écrivant $x = N\alpha$ on peut, d'après la proposition I.1, supposer $\alpha \in K^{*+}$, d'où $xA_k = N(\alpha A_K) \in N\mathcal{J}_o(K)$) ; montrons que l'homomorphisme ainsi défini est surjectif : si xA_k est dans $I_o \cap N\mathcal{J}_o(K)$, on peut supposer $x \in \Lambda$ et il existe $\alpha \in K^{*+}$ tel que $xA_k = N(\alpha A_K)$, soit $x = \varepsilon N\alpha$, $\varepsilon \in E_k$; on a $S_k(N\alpha) = 1$ (Proposition I.1) donc $\varepsilon \in E_k^+$, $x\varepsilon^{-1} \in \Lambda \cap NK^*$ et $x\varepsilon^{-1}A_k = xA_k$.

Si $xA_k \in I_o^\ell$, il existe $y \in \Lambda$ tel que $yA_k \in I_o$ et $xA_k = (yA_k)^\ell$. On a donc $x = y^\ell\varepsilon'$, $\varepsilon' \in E_k^+$; comme $x \in NK^*$ on aura $\varepsilon' \in NK^* \cap E_k^+$ et $x \in \Lambda^\ell(E_k^+ \cap NK^*)$.

Inversement, si $x = y^\ell\varepsilon'$, $y \in \Lambda$, $\varepsilon' \in E_k^+ \cap NK^*$, alors $xA_k = (yA_k)^\ell$ avec $yA_k \in I_o$, soit $xA_k \in I_o^\ell$. D'où l'exactitude de la seconde suite.

Pour la troisième, on considère l'homomorphisme canonique surjectif :

$$\Lambda \cap NK^*/\Lambda^\ell \to \Lambda \cap NK^*/\Lambda^\ell(E_k^+ \cap NK^*) \to 1$$

dont le noyau s'identifie au quotient $E_k^+ \cap NK^*/\Lambda^\ell \cap (E_k^+ \cap NK^*)$; or $\Lambda^\ell \cap E_k^+ \cap NK^* = \Lambda^\ell \cap E_k^+ = (E_k^+)^\ell$. Pour les deux dernières suites exactes, on considère les homomorphismes canoniques surjectifs :

$$\Lambda/\Lambda^\ell \to \Lambda/\Lambda \cap NK^* \to 1$$

et $E_k^+/E_k^{+\ell} \to E_k^+/E_k^+ \cap NK^* \to 1$ dont les noyaux sont respectivement $\Lambda \cap NK^*/\Lambda^\ell$ et $E_k^+ \cap NK^*/E_k^{+\ell}$.

PROPOSITION IV.5.- On a les suites exactes :

$$1 \to N\mathcal{J}/I_o \to N\mathfrak{H} \to 1 ,$$

$$1 \to N\mathcal{J}_o \to N\mathcal{J} \to \mathfrak{H}/\mathfrak{H}^{\sigma-1} \to 1 ,$$

$$1 \to \mathfrak{H}_1 \cap \mathfrak{H} \to \mathfrak{H} \xrightarrow{\sigma-1} \mathfrak{H}^{\sigma-1} \to 1 ,$$

$$1 \to E_k^+/E_k^{+\ell} \to \Lambda/\Lambda^\ell \to I_o/I_o^\ell \to 1 .$$

Démonstration.- La première résulte de la définition de $N : \mathfrak{H}(K) \to \mathfrak{H}(k)$.

Pour la seconde, soit $\mathfrak{A} \in \mathcal{J}$; à $N\mathfrak{A}$ on associe l'image de la classe de $\mathfrak{A}$ dans $\mathfrak{H}/\mathfrak{H}^{\sigma-1}$; si $\mathfrak{B} \in \mathcal{J}$ est tel que $N\mathfrak{A} = N\mathfrak{B}$ on sait qu'il existe $\mathfrak{A}'$ tel que $\mathfrak{B} = \mathfrak{A}\mathfrak{A}'^{\sigma-1}$; par conséquent $\mathfrak{A}'^{\sigma-1} \in \mathcal{J}$, on peut donc supposer $\mathfrak{A}' \in \mathcal{J}$ grâce à l'hypothèse $\mathcal{J} \cap \mathcal{J}(K)^{\sigma-1} = \mathcal{J}^{\sigma-1}$ et les classes de $\mathfrak{A}$ et $\mathfrak{B}$ sont équivalentes modulo $\mathfrak{H}^{\sigma-1}$. Si la classe de $\mathfrak{A}$ est dans $\mathfrak{H}^{\sigma-1}$, il existe $\mathfrak{B} \in \mathcal{J}$ et $\alpha \in K^{*+}$ tels que $\mathfrak{A} = \mathfrak{B}^{\sigma-1}\alpha A_K$ et $N\mathfrak{A} = N(\alpha A_K)$; or $\mathfrak{A} \in \mathcal{J}$ et $\mathfrak{B}^{\sigma-1} \in \mathcal{J}$ donc $\alpha A_K \in \mathcal{J}$ donc $\alpha A_K \in \mathcal{J}_o$ et $N\mathfrak{A} \in N\mathcal{J}_o$, la réciproque étant évidente.

La troisième est immédiate.

La dernière suite exacte découle de la suite exacte

$$1 \to E_k^+ \to \Lambda \xrightarrow{\Psi} I_o \to 1 ,$$

compte tenu du fait que $\Lambda^\ell \cap E_k^+ = E_k^{+\ell}$.

PROPOSITION IV.6.- L'ordre du quotient $\tilde{\mathfrak{H}}/\mathfrak{H}$ est donné par la formule :

$$|\tilde{\mathfrak{H}}/\mathfrak{H}| = \frac{|\mathfrak{H}(k)| \; |\Lambda \cap NK^*/\Lambda^\ell|}{|N\mathfrak{H}| \; |\Lambda/\Lambda^\ell|} \ell^{t-1} .$$

Démonstration.- La proposition IV.4 conduit à l'expression

$|\tilde{\mathfrak{H}}/\mathfrak{H}\mathfrak{H}_1| = \dfrac{|\Lambda \cap NK^*/\Lambda^\ell|}{|N\mathcal{J}_o/I_o^\ell| \; |E_k^+ \cap NK^*/E_k^{+\ell}|}$. On remarque que :

$(N\mathcal{J}:I_o^{\ell}) = (N\mathcal{J}:N\mathcal{J}_o)(N\mathcal{J}_o:I_o^{\ell}) = (N\mathcal{J}:I_o)(I_o:I_o^{\ell})$ qui montre (en utilisant la proposition IV.5) que

$$|N\mathcal{J}_o/I_o^{\ell}| = \frac{|N\mathfrak{H}|\ |I_o/I_o^{\ell}|}{|\mathfrak{H}_1\cap\mathfrak{H}|} = \frac{|N\mathfrak{H}|\ |\Lambda/\Lambda^{\ell}|}{|\mathfrak{H}_1\cap\mathfrak{H}|\,|E_k^{+}/E_k^{+\ell}|}\ ,$$

d'où une autre expression de $|\tilde{\mathfrak{H}}/\mathfrak{H}\mathfrak{H}_1|$:

$$|\tilde{\mathfrak{H}}/\mathfrak{H}\mathfrak{H}_1| = \frac{|\mathfrak{H}_1\cap\mathfrak{H}|}{|N\mathfrak{H}|}\ \frac{|\Lambda\cap NK^*/\Lambda^{\ell}|}{|\Lambda/\Lambda^{\ell}|}\ \frac{|E_k^{+}/E_k^{+\ell}|}{|E_k^{+}\cap NK^*/E_k^{+\ell}|}$$

$$= \frac{|\mathfrak{H}_1\cap\mathfrak{H}|}{|N\mathfrak{H}|}\ \frac{|\Lambda\cap NK^*/\Lambda^{\ell}|}{|\Lambda/\Lambda^{\ell}|}\ |E_k^{+}/E_k^{+}\cap NK^*| \quad \text{(cf. proposition IV.4)}.$$

Comme $\tilde{\mathfrak{H}}$ contient $\mathfrak{H}\mathfrak{H}_1$ on aura $(\tilde{\mathfrak{H}}:\mathfrak{H}) = (\tilde{\mathfrak{H}}:\mathfrak{H}\mathfrak{H}_1)(\mathfrak{H}\mathfrak{H}_1:\mathfrak{H})$ d'où

$$|\tilde{\mathfrak{H}}/\mathfrak{H}| = |\tilde{\mathfrak{H}}/\mathfrak{H}\mathfrak{H}_1|\,|\mathfrak{H}\mathfrak{H}_1/\mathfrak{H}| = \frac{|\tilde{\mathfrak{H}}/\mathfrak{H}\mathfrak{H}_1|\,|\mathfrak{H}\mathfrak{H}_1/\mathfrak{H}|}{|\mathfrak{H}_1|}\,|\mathfrak{H}_1| = \frac{|\mathfrak{H}(k)|}{|N\mathfrak{H}|}\ \frac{|\Lambda\cap NK^*/\Lambda^{\ell}|}{|\Lambda/\Lambda^{\ell}|}\ \ell^{t-1}$$

compte tenu de la formule donnant $|\mathfrak{H}_1|$ (théorème IV.1) et de la suite exacte $1 \to \mathfrak{H}_1\cap\mathfrak{H} \to \mathfrak{H} \to \mathfrak{H}\mathfrak{H}_1/\mathfrak{H}_1 \to 1$.

Reste à donner une méthode de calcul du terme $\frac{|\Lambda\cap NK^*/\Lambda^{\ell}|}{|\Lambda/\Lambda^{\ell}|}$ qui dépend essentiellement de la nature du groupe des normes NK^* .

c) <u>Calcul de</u> $\frac{|\Lambda\cap NK^*/\Lambda^{\ell}|}{|\Lambda/\Lambda^{\ell}|}$.

PROPOSITION IV.7.- <u>Soit</u> $q(a_1),\ldots,q(a_n)$ <u>une base du</u> $\mathbb{F}_{\ell}$<u>-espace vectoriel</u> Λ/Λ^{ℓ} , $a_i \in \Lambda$. <u>Le nombre</u> $\frac{|\Lambda/\Lambda^{\ell}|}{|\Lambda\cap NK^*/\Lambda^{\ell}|}$ <u>est égal à</u> ℓ^r <u>où</u> r <u>est le rang du système linéaire homogène défini sur</u> $\mathbb{F}_{\ell}$ <u>par les</u> t <u>équations</u> : $\prod_{i=1}^{n} (\alpha,a_i)_{\mathfrak{p}}^{x_i} = 1$ <u>pour tout idéal</u> $\mathfrak{p}$ <u>ramifié dans</u> K/k , α <u>étant un nombre de</u> k' <u>tel que</u> $K' = k'(\sqrt[\ell]{\alpha})$.

<u>En outre, on a les relations</u> : $0 \le r \le t-1$ <u>pour</u> $t \ge 1$ <u>et</u> $r = 0$ <u>si</u> $t = 0$.

<u>Démonstration</u>.- Considérons l'extension K'/k' , K' et k' étant les corps obtenus par adjonction à K et k des racines $\ell^{\text{èmes}}$ de l'unité. Comme

$d = [k':k]$ est premier à ℓ , il en résulte qu'un nombre $a \in k$ est une norme dans K/k si et seulement s'il est norme dans K'/k' . L'extension K'/k' étant cyclique, le théorème des normes de Hasse s'applique et montre que a est norme dans K'/k' si et seulement s'il est norme dans toute extension locale $K'_{\wp'}/k'_{\wp}$, $\wp$ décrivant l'ensemble des places de k' ([2]) ; en vertu de la proposition II.1, (iii), si $K' = k'(\sqrt[\ell]{\alpha})$, a sera norme locale partout, si et seulement si $(\alpha,a)_{\wp} = 1$ pour toute place $\wp$ de k' , ou encore, si et seulement si $(\alpha,a)_{\mathfrak{p}} = 1$ pour toute place $\mathfrak{p}$ de k (remarque III.2).

Le fait que d soit premier à ℓ entraîne qu'un idéal premier $\mathfrak{p}$ de k est ramifié (resp. inerte, décomposé) dans K/k si et seulement si tout idéal premier $\wp$ au-dessus de $\mathfrak{p}$ dans k'/k est ramifié (resp. inerte, décomposé) dans K'/k' .

Si $\ell = 2$ et si $\mathfrak{p}$ est une place à l'infini, le symbole $(\alpha,a)_{\mathfrak{p}}$ ne peut valoir -1 , que si $k_{\mathfrak{p}} = \mathbb{R}$ et si α et a sont négatifs ; or ici, $\Lambda \subset k^{*+}$, donc si $a \in \Lambda$ on a $(\alpha,a)_{\mathfrak{p}} = 1$.

Revenons maintenant au cas où $\mathfrak{p}$ est un idéal premier : si $\mathfrak{p}$ est décomposé dans K/k , alors $K_{\mathfrak{p}} = k_{\mathfrak{p}}$ et tout nombre est norme. Supposons $\mathfrak{p}$ inerte dans K/k ; on sait que pour tout $\wp$ au-dessus de $\mathfrak{p}$ dans k' on a $v_{\wp}(\alpha) \equiv 0$ modulo ℓ (proposition I.2) ; de plus, $a \in \Lambda$, donc $aA_k \in N\mathcal{J}$ et $aA_{k'}$ est la norme d'un idéal $\mathfrak{A}'$ de K' ; il en résulte $v_{\wp}(aA_{k'}) \equiv 0 \bmod \ell$; l'extension locale en $\wp$, $K'_{\wp}/k'_{\wp}$ étant non ramifiée, ces conditions suffisent à montrer que $(\alpha,a)_{\wp} = 1$ (compte tenu du fait que dans le cas local non ramifié toute unité est norme).

Donc si $q(a) \in \Lambda/\Lambda^{\ell}$, $a \in \Lambda$, $q(a)$ est un élément de $\Lambda \cap NK^*/\Lambda^{\ell}$ si et seulement si $(\alpha,a)_{\mathfrak{p}} = 1$ pour tout idéal $\mathfrak{p}$ de k ramifié dans K/k . On remarque enfin que l'on a l'isomorphisme :

$$\Lambda \cap NK^*/\Lambda^{\ell} \simeq \{(x_1,\dots,x_n) \in \mathbb{F}_{\ell}^n \ , \ \prod_{i=1}^{n} a_i^{x_i} \in NK^*\} \ ,$$

donc $\Lambda \cap NK^*/\Lambda^{\ell}$ est isomorphe à l'espace des solutions du système homogène proposé ; ce qui achève la démonstration de la première partie de la proposition.

Soit $\delta_{\mathfrak{p}}$ le nombre d'idéaux premiers au-dessus de $\mathfrak{p}$ dans k' ; la formule du produit (II.B.2) s'écrit pour tout i , $\overline{|\ |}_{\mathfrak{P}}(\alpha,a_i)_{\mathfrak{P}} = 1$ soit $\overline{|\ |}_{\mathfrak{p}}(\alpha,a_i)_{\mathfrak{p}}^{\delta_{\mathfrak{p}}} = 1$; en vertu de ce qui précède, on peut supposer que $\mathfrak{p}$ parcourt l'ensemble des idéaux premiers ramifiés dans K/k ; les $\delta_{\mathfrak{p}}$ étant premiers à ℓ , les t équations du système sont linéairement dépendantes et on a $r \leq t-1$. Si $t = 0$ on vérifie directement que "r est nul" dans la formule.

Remarque IV.6.- Les n relations $\overline{|\ |}_{\mathfrak{p}}(\alpha,a_i)_{\mathfrak{p}}^{\delta_{\mathfrak{p}}} = 1$ évitent, dans la pratique, le calcul de n symboles.

THEOREME IV.3.- Soit $\mathcal{H}$ un sous-H-module de $\mathcal{H}(K)$; soit $\mathcal{J}$ un sous-H-module de $\mathcal{J}(K)$ dont l'image dans $\mathcal{H}(K)$ soit égale à $\mathcal{H}$ et tel que $\mathcal{J}\cap\mathcal{J}(K)^{\sigma-1} = \mathcal{J}^{\sigma-1}$; soit $\Lambda = \psi^{-1}(N\mathcal{J}\cap\mathcal{J}_o(k))$ le groupe de nombres associé à $\mathcal{J}$ et soit $q(a_1),\ldots,q(a_n)$ une $\mathbb{F}_\ell$-base de Λ/Λ^ℓ ; alors :

$$|\tilde{\mathcal{H}}/\mathcal{H}| = \frac{|\mathcal{H}(k)|}{|N\mathcal{H}|}\,\ell^{t-1-r} ,$$

où $t \geq 0$ est le nombre d'idéaux ramifiés dans K/k , et où r , vérifiant en outre $r \leq t-1$, est le rang du système linéaire homogène sur $\mathbb{F}_\ell$:

$$\prod_{i=1}^{n} \overline{|\ |}_{\mathfrak{p}}(\alpha,a_i)_{\mathfrak{p}}^{x_i} = 1 \ , \quad \mathfrak{p} \text{ ramifié dans } K/k .$$

COROLLAIRE IV.4.- Pour tout $i \geq 0$ on obtient pour $\mathcal{H} = \mathcal{H}_i$:

$$|\mathcal{H}_{i+1}/\mathcal{H}_i| = \frac{|\mathcal{H}(k)|}{|N\mathcal{H}_i|}\,\ell^{t-1-r} .$$

3. Algorithme général.

Les théorèmes IV.2 et IV.3 permettent de définir une sorte d'algorithme pour la détermination de $\mathcal{H}(K)$ par construction d'une suite croissante $\{\mathcal{J}_i\}_{i\geq 1}$, associée à la filtration $\{\mathcal{H}_i\}_{i\geq 1}$, et vérifiant les hypothèses du théorème IV.2, ainsi que de la suite $\{\Lambda_i\}_{i\geq 1}$ correspondante (définition IV.1).

De façon précise, $\mathcal{J}_1$ est engendré par les idéaux suivants :

(i) des idéaux invariants : idéaux premiers ramifiés dans K/k et idéaux de A_k dont les classes engendrent $\mathcal{H}(k)$ et que l'on étend à A_K ;

(ii) des idéaux $\mathfrak{A}$ de K tels que $\mathfrak{A}^{\sigma-1} = \alpha A_K$, que l'on obtient en résolvant l'équation $N\alpha = \varepsilon$, pour $\varepsilon \in E_k^+ \cap NK^*$ (les unités ε qui sont normes dans K/k étant trouvées au moyen du système linéaire défini dans le théorème IV.3 et construit à partir de $\Lambda_o = E_k^+$) .

Supposons avoir déterminé $\mathcal{J}_{i-1}$, Λ_{i-1} ($\mathcal{H}_{i-1}$ étant alors l'image de $\mathcal{J}_{i-1}$ dans $\mathcal{H}(K)$ et $|\mathcal{H}_{i-1}|$ étant connu) ; le système linéaire associé à Λ_{i-1} donne un ensemble de solutions indépendantes : "a" , telles que $aA_k = N\mathfrak{A} = N(\alpha A_K)$, $\mathfrak{A} \in \mathcal{J}_{i-1}$, $\alpha \in K^*$; on utilise alors l'homomorphisme φ défini dans le théorème IV.2, qui permet de construire $\tilde{\mathcal{H}}_{i-1} = \mathcal{H}_i$ comme classes des idéaux $\mathfrak{A}'$ vérifiant :

$$\alpha A_K = \mathfrak{A}\mathfrak{A}'^{\sigma-1} \quad .$$

Le groupe $\mathcal{J}_i$ sera engendré par $\mathcal{J}_{i-1}$ et par ces idéaux $\mathfrak{A}'$; Λ_i s'en déduit trivialement, quant à $|\mathcal{H}_i|$ on utilise la formule du corollaire IV.4 :

$$|\mathcal{H}_i/\mathcal{H}_{i-1}| = \frac{|\mathcal{H}(k)|}{|N\mathcal{H}_{i-1}|}\, \ell^{t-1-r_{i-1}} ,$$

($N\mathcal{H}_{i-1}$ étant déterminé à partir des $N\mathfrak{A}$, $\mathfrak{A} \in \mathcal{J}_{i-1}$) .

Remarque IV.7.- Nous n'avons pas parlé de la condition $\mathcal{J} \cap \mathcal{J}(K)^{\sigma-1} = \mathcal{J}^{\sigma-1}$; il suffit, pour la vérifier, de se ramener à des groupes $\mathcal{J}$ engendrés par des idéaux premiers :

En effet dans la relation $\alpha A_K = \mathfrak{A}\mathfrak{A}'^{\sigma-1}$ la classe de $\mathfrak{A}'$ contient des idéaux premiers ([19]) ; soit $\mathfrak{p}$ un tel idéal, il existe $\gamma \in K^{*+}$ tel que $\mathfrak{A}' = \mathfrak{p}\gamma A_K$ et $\alpha A_K = \mathfrak{A}\mathfrak{p}^{\sigma-1}\gamma^{\sigma-1}A_K$, d'où $\alpha\gamma^{1-\sigma}A_K = \mathfrak{A}\mathfrak{p}^{\sigma-1}$; on a toujours $N(\alpha\gamma^{1-\sigma}) = N(\alpha) = N\mathfrak{A}$, d'où la remarque.

Remarque IV.8.- Lorsque $t = 0$ ou 1 , seul le théorème IV.2 est utilisé car tous les éléments d'un groupe Λ sont normes (le rang r est toujours nul).

Exemple IV.1.- Soit $k = \mathbb{Q}(\sqrt{-23})$; on vérifie que le nombre de classes est 3 et que la classe de $\mathfrak{p}_2$ (idéal premier au-dessus de 2) engendre $\mathcal{H}(k)$.

Soit $\alpha = 163(28+3\sqrt{69})$; α est un élément de k' et en fait de $\tilde{k}$ (le sous-corps quadratique de k' distinct de k et de $\mathbb{Q}(j)$) ; on a bien $\alpha^{s+1} = 163^3$ ce qui fait que l'extension K/k associée est cyclique de degré 3 et que $K/\mathbb{Q}$ est diédrale ([9]) .

On remarque que 163 est totalement décomposé dans k' et que 3 est non ramifié dans K/k ($\alpha \equiv 1$ modulo $3\sqrt{-3}$) ; il y a donc deux idéaux premiers ramifiés dans K/k : $\mathfrak{p}_{163}$ et $\mathfrak{p}'_{163}$, au-dessus de 163 dans k . Posons $\mathfrak{p}_{163}A_K = \mathfrak{P}^3$ et $\mathfrak{p}'_{136}A_K = \mathfrak{P}'^3$.

Détermination de $\mathcal{H}(K)$.- On a $|\mathcal{H}_1| = |\mathcal{H}(k)|3^{t-1} = 9$ (Théorème IV.1) et $\mathcal{H}_1$ est engendré par les classes des idéaux invariants (Corollaire IV.2) donc par les classes de $\mathfrak{P}$, $\mathfrak{P}'$ et $\mathfrak{p}_2A_K$; on aura :

$$\mathcal{J}_1 = \langle \mathfrak{P}, \mathfrak{P}', \mathfrak{p}_2A_K \rangle$$

$$N\mathcal{J}_1 = \langle \mathfrak{p}_{163}, \mathfrak{p}'_{163}, \mathfrak{p}_2^3 \rangle \quad \text{avec} \quad \mathfrak{p}_2^3 = (\tfrac{3+\sqrt{-23}}{2})A_k \ ;$$

$$I_o = N\mathcal{J}_1 \cap \mathcal{J}_o(k) = \langle \mathfrak{p}_{163}^3, \mathfrak{p}'^3_{163}, \mathfrak{p}_{163}\mathfrak{p}'_{163}, (\tfrac{3+\sqrt{-23}}{2}) \rangle \ ;$$

car on vérifie que $\mathfrak{p}_{163}$ n'est pas principal, d'où

$$I_o = \langle \mathfrak{p}_{163}^3, (163)A_k, (\tfrac{3+\sqrt{-23}}{2})A_k \rangle$$

et, en posant $\mathfrak{p}_{163}^3 = \alpha_o A_k$ on obtient $\Lambda_1 = \langle \alpha_o, 163, \frac{3+\sqrt{-23}}{2} \rangle$.

Calculons le symbole $(\alpha,163)_\wp$. On a $\alpha = 163\,\beta$, $\beta = 28 + 3\sqrt{69}$ donc $(\alpha,163)_\wp = (\beta,163)_\wp$; soit $\wp$ un des quatre idéaux au-dessus de 163 dans k' qui ne divise pas β , il divisera $\beta^s = 28-3\sqrt{69}$ et on aura $3\sqrt{69} \equiv 28 \bmod \wp$ soit $(\beta,163)_\wp \equiv (\beta)^{54} \equiv 56^{54}$ modulo $\wp$; si on avait $(\beta,163)_\wp = 1$ on aurait $56^{54} \equiv 1$ modulo 163, ce qui n'est pas car 56 n'est pas reste cubique modulo 163.

Le rang r_1 est égal à 1 et on a $|\mathcal{H}_2/\mathcal{H}_1| = \frac{3}{|N\mathcal{H}_1|}$; or $N\mathcal{H}_1 = \langle cl(\mathfrak{p}_{163}), cl(\mathfrak{p}'_{163}), cl(\mathfrak{p}_2^3) \rangle = \langle cl(\mathfrak{p}_{163}) \rangle$, comme $\mathfrak{p}_{163}$ n'est pas principal

on a $|N\mathcal{H}_1| = 3$; d'où $\mathcal{H}(K) = \mathcal{H}_1$.

Exemple IV.2.- Soit $k = \mathbb{Q}(\sqrt{-111})$; on vérifie que $\mathcal{H}(k)$ est cyclique d'ordre 8 et est engendré par la classe de $\mathfrak{p}_2$ (idéal premier au-dessus de 2) ; on a :

$$\mathfrak{p}_2^8 = \frac{5+3\sqrt{-111}}{2} .$$

On considère alors l'extension $K = k(\sqrt{\theta})$ avec $\theta = \frac{5+3\sqrt{-111}}{2}$. On vérifie en utilisant la proposition I.2 que K/k est non ramifiée ($K/\mathbb{Q}$ est aussi biquadratique : $K = \mathbb{Q}(\sqrt{-3},\sqrt{37})$) .

On aura $|\mathcal{H}_1| = \frac{8}{2} = 4$ et si $\mathfrak{A}$ engendre un élément de $\mathcal{H}_1$, $\mathfrak{A}^{\sigma-1} = \alpha A_K$ avec $N\alpha \in E_k = \{-1,+1\}$, comme -1 est norme il suffit de résoudre

$$N\alpha' = -1 .$$

On trouve $N\left[\frac{-2+2\sqrt{-111}+\frac{5+\sqrt{-111}}{2}\sqrt{\theta}}{2}\right] = -\left(\frac{9-\sqrt{-111}}{2}\right)^2$ et on vérifie que

$(\alpha')A_K = \mathfrak{P}_3^2(\mathfrak{p}_2 A_K)^4$ où $\mathfrak{P}_3$ est un idéal premier au-dessus de $\mathfrak{p}_3$ dans K avec $N\mathfrak{P}_3 = \mathfrak{p}_3$. Ceci conduit à $\left(\frac{\alpha'}{\frac{9-\sqrt{-111}}{2}}\right)A_K = \mathfrak{P}_3^{\sigma-1}$ et $\mathfrak{A} = \mathfrak{P}_3$.

On a donc $\mathcal{J}_1 = \langle \mathfrak{p}_2 A_K, \mathfrak{P}_3, \mathfrak{P}_3^{\sigma} \rangle$

$$N\mathcal{J}_1 = \langle \mathfrak{p}_2^2, \mathfrak{p}_3 \rangle \quad \text{et} \quad N\mathcal{J}_1 \cap \mathcal{J}_o(k) = \langle \mathfrak{p}_3^2 \rangle .$$

On obtient alors $N\mathcal{H}_1 = \langle \mathrm{cl}\ \mathfrak{p}_2^2 \rangle$ qui est d'ordre 4 ; ainsi $|\mathcal{H}_2/\mathcal{H}_1| = \frac{8}{2|N\mathcal{H}_1|} = 1$ et $\mathcal{H}(K) = \mathcal{H}_1$ (on peut conduire aussi les calculs dans $K/\mathbb{Q}(\sqrt{-3})$ avec $k = \mathbb{Q}(\sqrt{-3})$; dans ce cas $|\mathcal{H}_1| = 2$ et $\mathcal{H}(K) = \mathcal{H}_2$ et il résulte du corollaire IV.3 que $\mathcal{H}(K)$ est cyclique d'ordre 4 : $\mathcal{H}(K)$ est engendré par la classe de $\mathfrak{p}_2 A_K$, $\mathfrak{p}_2$ relatif à $k = \mathbb{Q}(\sqrt{-111})$) ; cf. Résultats du Kubota, Über den bizyklischen biquadratischen Zahlkörper, Nagoya Math. J. 10-12 (1956), 65-85.

4. Cas du corps des rationnels : définition du groupe Λ_1 .

Dans le cas où $k = \mathbb{Q}$, l'expression de $|\tilde{\mathcal{H}}/\mathcal{H}|$ est alors :

$$|\tilde{\mathcal{H}}/\mathcal{H}| = \ell^{t-1-r} .$$

Soit $\mathcal{H} = \mathcal{H}_1$; comme $E_{\mathbb{Q}}^{+} = \{1\}$, il résulte du corollaire IV.2 que $\mathcal{H}_1$ est engendré par les classes des idéaux premiers ramifiés dans $K/\mathbb{Q}$; si $p_1, \ldots, p_t$ sont les nombres premiers ramifiés dans $K/\mathbb{Q}$, on obtient pour Λ (relativement à $\mathcal{H} = \mathcal{H}_1$) le groupe engendré par $p_1, \ldots, p_t$ et noté :

$$\Lambda_1 = \langle p_1, p_2, \ldots, p_t \rangle .$$

Remarque IV.9.- L'existence de classes d'ordre ℓ , non invariantes par H est équivalente à la condition $|\mathcal{H}_2/\mathcal{H}_1| > 1$ soit $r < t-1$; il est donc nécessaire d'avoir $t \geq 2$. Des exemples on été donnés dans [10] .

Dans le chapitre VI, nous donnons d'autres exemples numériques et, en annexe, des tables numériques.

CHAPITRE V

APPLICATION DES RESULTATS DU CHAPITRE PRECEDENT

A. Généralisation d'un théorème de Kisilewsky ([17])

Les propositions IV.2 et IV.3 peuvent s'appliquer à $M = \mathcal{H}(K)$, si et seulement si $|\mathcal{H}_1| = \ell$ (les quotients $\mathcal{H}_{i+1}/\mathcal{H}_i$ étant nécessairement d'ordre ℓ pour $i < n$).

Le théorème IV.1 nous donne :

$$|\mathcal{H}_1| = \frac{|\mathcal{H}(k)|\,\ell^{t-1}}{(E_k^+ : E_k^+ \cap NK^*)} ,$$

et la condition $|\mathcal{H}_1| = \ell$ se produit dans les trois cas suivants (compte tenu du théorème IV.3 appliqué à $\Lambda = E_k^+$) :

(i) $|\mathcal{H}(k)| = 1$, $t \geq 2$, $(E_k^+ : E_k^+ \cap NK^*) = \ell^{t-2}$,

(ii) $|\mathcal{H}(k)| = \ell$, $t \geq 1$, $(E_k^+ : E_k^+ \cap NK^*) = \ell^{t-1}$,

(iii) $|\mathcal{H}(k)| = \ell^2$ et $t = 0$.

Si $k = \mathbb{Q}$ et ℓ impair, il ne subsiste que le cas (i) avec $t = 2$.

Si k est un corps quadratique avec $\mathcal{H}(k) \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ et si K/k est non ramifiée, on retrouve un résultat énoncé (dans [17]) dans un cas particulier.

B. Problème de O. Taussky

Supposons K/k non ramifiée pour les idéaux ; le théorème 94 de Hilbert ([15]) affirme qu'un idéal de k devient principal dans K/k ; si $\mathcal{H}(K)$ est le ℓ-groupe des classes de K , $N\mathcal{H}(K)$ est d'indice ℓ dans $\mathcal{H}(k)$ (théorie du corps de classes).

O. Taussky a donné la définition suivante ([24]) :

L'extension K/k est dite de type A si $N\mathcal{H}(K)\cap \mathrm{Ker}\ j \neq \{1\}$, sinon elle est dite de type B .

Si $\mathcal{H}$ est un sous-H-module de $\mathcal{H}(K)$, on a $|\tilde{\mathcal{H}}/\mathcal{H}| = \dfrac{|\mathcal{H}(k)|}{|N\mathcal{H}|\ell}$ (théorème IV.3), soit $|\tilde{\mathcal{H}}/\mathcal{H}| = \dfrac{|\mathcal{H}_1|}{|N\mathcal{H}|}$ (théorème IV.1)

$$= \frac{|\mathcal{H}_1|}{|\mathcal{H}^\nu|}\ \frac{|\mathcal{H}^\nu|}{|N\mathcal{H}|}\ ;$$

la suite exacte $1 \to \mathrm{Ker}\ j\cap N\mathcal{H} \to N\mathcal{H} \xrightarrow{j} \mathcal{H}^\nu \to 1$ donne

$$|\tilde{\mathcal{H}}/\mathcal{H}| = \frac{|\mathcal{H}_1|}{|\mathcal{H}^\nu|\,|\mathrm{Ker}\ j\cap N\mathcal{H}|} = \frac{|\hat{H}^0(H,\mathcal{H})|}{|\mathrm{Ker}\ j\cap N\mathcal{H}|}\ ,$$

en désignant par $\hat{H}^i$ la cohomologie modifiée de Tate. Appliqué à $\mathcal{H} = \mathcal{H}(K)$ on retrouve un résultat de [17] (démontré dans le cas cyclique de degré quelconque) : à savoir que la condition B équivaut à la condition : $|\hat{H}^0(H,\mathcal{H}(K))| = 1$

C. Résultats sur les corps quadratiques

1. Comparaison des 4-rangs de $\mathbb{Q}(\sqrt{m})$ et de $\mathbb{Q}(\sqrt{-m})$ ([8]).

Soit m un entier sans facteurs carrés. Posons $K = \mathbb{Q}(\sqrt{m})$ et $\hat{K} = \mathbb{Q}(\sqrt{-m})$ et réservons la notation $\hat{}$ pour toute quantité qui concerne le corps $\hat{K}$.

Soient $p_1,\ldots,p_{t^*}$ les nombres premiers impairs ramifiés dans $K/\mathbb{Q}$ (ils se ramifient aussi dans $\hat{K}/\mathbb{Q}$). Si 2 ne divise pas m , il est nécessairement ramifié dans K ou dans $\hat{K}$ (et dans l'un des deux seulement), sinon il

est ramifié dans les deux corps.

D'après les corollaires IV.1 et IV.2, les ordres des groupes de classes invariantes sont respectivement :

$$|\mathcal{H}_1| = 2^{t-1} \quad \text{et} \quad |\hat{\mathcal{H}}_1| = 2^{\hat{t}-1} \ ;$$

les groupes $\mathcal{H}_1$ et $\hat{\mathcal{H}}_1$ étant engendrés par les classes des idéaux premiers ramifiés. Les groupes Λ et $\hat{\Lambda}$ associés sont donc :

$$\Lambda = \langle p_1,\ldots,p_{t^*}\rangle \ , \ \hat{\Lambda} = \langle p_1,\ldots,p_{t^*},2\rangle \quad \text{ou vice-versa,}$$

lorsque m est impair ;

$$\Lambda = \hat{\Lambda} = \langle p_1,\ldots,p_{t^*},2\rangle \quad \text{lorsque 2 divise } m \ .$$

Soient A et $\hat{A}$ les matrices (carrées) des systèmes linéaires associés aux groupes Λ et $\hat{\Lambda}$ (cf. théorème IV.3).

Les propositions IV.1 et IV.2 et le corollaire IV.4 ramènent la comparaison des 4-rangs R_2 et $\hat{R}_2$ de K et $\hat{K}$ à la comparaison des rangs r et $\hat{r}$ des matrices A et $\hat{A}$: en effet, on obtient immédiatement la relation :

$$R_2-\hat{R}_2 = t-\hat{t}+\hat{r}-r \ .$$

Posons pour $1 \le i,j \le t^*$:

$$(m,p_i)_{p_j} = (-1)^{a_{ji}} \ , \quad (-m,p_i)_{p_j} = (-1)^{\hat{a}_{ji}} \ ;$$

$$(m,p_i)_2 = (-1)^{\varepsilon_i} \ , \quad (-m,p_i)_2 = (-1)^{\hat{\varepsilon}_i} \ ;$$

$$(m,2)_{p_i} = (-1)^{\eta_i} \ , \quad (-m,2)_{p_i} = (-1)^{\hat{\eta}_i} \ ;$$

$$(m,2)_2 = (-1)^{\eta_o} \ , \quad (-m,2)_2 = (-1)^{\hat{\eta}_o}$$

et $\delta_i = \dfrac{p_i-1}{2}$ (les quantités a_{ji} , ε_i , η_i , η_o , δ_i ,... étant définies modulo 2) .

On pose enfin $m = 2d$ si 2 divise m , $m = d$ sinon et on peut supposer $d \equiv 1$ modulo 4 quitte à échanger les rôles de m et de $-m$ une fois pour toutes. La formule du produit conduit alors à :

$$(-1)^{\sum \delta_i} = \operatorname{sgn}(d) \quad (\text{noté } (-1)^{\delta_o}) \ .$$

LEMME V.1.- On a les relations :

(i) $a_{ij} + a_{ji} = \delta_i \delta_j$ pour $i \neq j$,

(ii) $\hat{a}_{ij} = a_{ij}$ pour $i \neq j$,

(iii) $\hat{a}_{ii} = a_{ii} + \delta_i$,

(iv) $\hat{\epsilon}_i = \epsilon_i + \delta_i$, $\hat{\eta}_i = \eta_i$ et $\hat{\eta}_o = \eta_o$.

La première exprime la loi de réciprocité quadratique appliquée aux nombres p_i et p_j : $\left(\frac{p_i}{p_j}\right)\left(\frac{p_j}{p_i}\right) = (-1)^{\frac{p_i-1}{2}\,\frac{p_j-1}{2}}$ (symboles de Legendre) ; les deux suivantes résultent du calcul du symbole $(-1,p_i)_{p_j}$: si $i \neq j$, $(-1,p_i)_{p_j} = 1$ et $(-1,p_i)_{p_i} = (-1)^{\delta_i}$. La dernière résulte des relations : $(-1,p_i)_2 = (-1)^{\delta_i}$ et $(-1,2)_{p_i} = (-1,2)_2 = 1$.

On pose :

$$B = \begin{pmatrix} a_{11} & \cdots & a_{1t^*} \\ & & \\ a_{t^*1} & \cdots & a_{t^*t^*} \end{pmatrix} \quad , \quad M = \begin{pmatrix} 1 & & & \delta_1 \\ & \ddots & & \vdots \\ & & 1 & \delta_{t^*} \\ & & & 1 \end{pmatrix} \quad ,$$

$$\Delta = \begin{pmatrix} \delta_1\delta_1 & \cdots & \delta_1\delta_{t^*} \\ & & \\ \delta_{t^*}\delta_1 & \cdots & \delta_{t^*}\delta_{t^*} \end{pmatrix} \quad , \qquad D = \begin{pmatrix} \delta_1 & & 0 \\ & \ddots & \\ 0 & & \delta_{t^*} \end{pmatrix} \quad ,$$

$\hat{B} = B + D$, $\hat{C} = {}^tB + \Delta$ et $C = \hat{C} + D$ (ce sont des matrices carrées de dimension $t^* \times t^*$).

Le lemme précédent (assertion (i)) montre que :

$$\hat{C} = \hat{B} = {}^tB + \Delta \ .$$

a) Cas où 2 ne divise pas m . (on rappelle que $m = d \equiv 1 \bmod 4$).

Le nombre 2 étant non ramifié dans K et ramifié dans $\hat{K}$ on a :

$$A = B \quad , \qquad \hat{A} = \begin{pmatrix} & \hat{B} & & \eta_1 \\ & & & \vdots \\ & & & \eta_{t^*} \\ \delta_1 & \cdots & \delta_{t^*} & \eta_o \end{pmatrix} \text{ et } M\hat{A} = \begin{pmatrix} & {}^tB & & \eta_1 + \delta_1\eta_o \\ & & & \vdots \\ & & & \eta_{t^*} + \delta_{t^*}\eta_o \\ \delta_1 & \cdots & \delta_{t^*} & \eta_o \end{pmatrix}$$

(i) Cas $m > 0$. On a $(m,m)_{p_i} = (-1,m)_{p_i}(-m,m)_{p_i} = (-1)^{\delta_i}$ car m est norme dans $\mathbb{Q}(\sqrt{-m})$; donc la somme des colonnes de B est formée des δ_i ; de plus les sommes $\sum_i \eta_i + \eta_o$ et $\delta_o = \sum_i \delta_i$ sont nulles, par conséquent, la somme des lignes de $M\hat{A}$ est la ligne nulle et $\hat{r} = r$ ou $r+1$, soit

$$-1 \leq R_2 - \hat{R}_2 \leq 0 \ .$$

(ii) Cas $m < 0$. Dans ce cas, la somme δ_o est égale à 1 et, la somme des lignes de B étant nulle, on peut remplacer la t^*-ème colonne de $M\hat{A}$ par la colonne $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$; il en résulte immédiatement que $\hat{r} = r+1$ ou $r+2$ soit :

$$0 \leq R_2 - \hat{R}_2 \leq 1 \ .$$

b) Cas où 2 divise m . On aura

$$A = \begin{pmatrix} & & \eta_1 \\ & B & \vdots \\ & & \eta_{t^*} \\ \varepsilon_1 \cdots \varepsilon_{t^*} & & \eta_o \end{pmatrix} \quad \text{et} \quad \hat{A} = \begin{pmatrix} & & \eta_1 \\ & \hat{B} & \vdots \\ & & \eta_{t^*} \\ \varepsilon_1+\delta_1 \cdots \varepsilon_{t^*}+\delta_{t^*} & & \eta_o \end{pmatrix} \ .$$

(i) Cas $m > 0$. La somme des colonnes de la matrice A est constituée des symboles $(m,|m|)_{p_i}$ et $(m,|m|)_2$.

On a $(m,|m|)_{p_i} = (m,m)_{p_i} = (-1)^{\delta_i}$ et $(m,m)_2 = 1$.

Compte tenu de ces relations et du fait que la somme des lignes de A est nulle, le rang r est égal au rang des matrices :

$$A_1 = \begin{pmatrix} & \delta_1 \\ B & \vdots \\ & \delta_{t^*} \end{pmatrix} \quad \text{et} \quad A_1 {}^tM = \begin{pmatrix} & \delta_1 \\ B+\Delta & \vdots \\ & \delta_{t^*} \end{pmatrix} \ ;$$

or $A_1{}^tM = \begin{pmatrix} {}^t\hat{B} & \begin{matrix}\delta_1\\ \vdots\\ \delta_{t^*}\end{matrix} \end{pmatrix}$ et $\hat{A}$ a même rang que $\hat{B}$ (en effet la somme des lignes et la somme des colonnes de $\hat{A}$ sont nulles). On aura, dans ce cas, $r = \hat{r}$ ou $r = \hat{r}+1$ soit encore :

$$-1 \leq R_2 - \hat{R}_2 \leq 0 .$$

(ii) Cas $m < 0$. On échange les rôles des matrices A et $\hat{A}$: la somme des colonnes de $\hat{A}$ est constituée des symboles $(-m,-m)_{p_i}$ et $(-m,-m)_2$; or $(-m,-m)_{p_i} = (-1)^{\delta_i}$ et $(-m,-m)_2 = -1$; on vérifie que, de la même manière A a même rang que B et que $\hat{A}$ a même rang que les matrices :

$$\hat{A}_1 = \begin{pmatrix} \hat{B} & \begin{matrix}\delta_1\\ \vdots\\ \delta_{t^*}\end{matrix} \end{pmatrix} \quad \text{et} \quad \hat{A}_1{}^tM = \begin{pmatrix} \hat{B}+\Delta & \begin{matrix}\delta_1\\ \vdots\\ \delta_{t^*}\end{matrix} \end{pmatrix}$$

soit $\hat{A}_1{}^tM = \begin{pmatrix} {}^tB & \begin{matrix}\delta_1\\ \vdots\\ \delta_{t^*}\end{matrix} \end{pmatrix}$; d'où la conclusion :

$$0 \leq R_2 - \hat{R}_2 \leq 1 .$$

On peut alors énoncer le résultat (obtenu dans [8] par dénombrement d'extensions non ramifiées et, ici, comme conséquence des lois de réciprocité quadratique) :

PROPOSITION V.1.- Soit m un entier sans facteurs carrés avec $m \equiv 1 \bmod 4$ si 2 ne divise pas m et $\frac{m}{2} \equiv 1$ modulo 4 si 2 divise m . Les 4-rangs R_2 et $\hat{R}_2$ de $\mathbb{Q}(\sqrt{m})$ et de $\mathbb{Q}(\sqrt{-m})$ diffèrent d'une unité au plus. De façon plus précise : $R_2 \leq \hat{R}_2 \leq R_2+1$ pour $m > 0$; $R_2-1 \leq \hat{R}_2 \leq R_2$ pour $m < 0$.

2. Corps quadratiques ayant un 4-rang donné ([6]).

PROPOSITION V.2.- *Soit* $m \in \mathbb{Z}$ *un entier sans facteurs carrés, soit* p *un nombre premier congru à* 1 *modulo* 4 *et ne divisant pas* m . *On pose* $K = \mathbb{Q}(\sqrt{m})$ *et* $\hat{K} = \mathbb{Q}(\sqrt{pm})$; *on note* $p_1,\dots,p_t$ *les nombres premiers ramifiés dans* $K/\mathbb{Q}$ (*dans* $\hat{K}/\mathbb{Q}$, $p_1,\dots,p_t$, p *se ramifient et ce sont les seuls*).

Si $\left(\frac{p_i}{p}\right) = 1$ *pour tout* i , $1 \le i \le t$, *les* 4-*rangs* R_2 *et* $\hat{R}_2$ *de* $\mathcal{H}(K)$ *et* $\mathcal{H}(\hat{K})$ *vérifient* :

$$\hat{R}_2 = R_2 + 1 \ .$$

Démonstration.- A K est associé $\Lambda = \langle p_1,\dots,p_t\rangle$ et à $\hat{K}$ est associé $\hat{\Lambda} = \langle p_1,\dots,p_t,p\rangle$. Posons $(-1)^{\varepsilon_{ij}} = (p,p_j)_{p_i}$; les matrices associées à Λ et $\hat{\Lambda}$ sont respectivement :

$$A = \begin{pmatrix} (m,p_1)_{p_1} & \dots & (m,p_t)_{p_1} \\ (m,p_1)_{p_2} & \dots & (m,p_t)_{p_2} \\ \dots & \dots & \dots \\ (m,p_1)_{p_t} & \dots & (m,p_t)_{p_t} \end{pmatrix}, \hat{A} = \begin{pmatrix} \varepsilon_{11}+(m,p_1)_{p_1} & \dots & \varepsilon_{1t}+(m,p_t)_{p_1} & (pm,p)_{p_1} \\ \varepsilon_{21}+(m,p_1)_{p_2} & \dots & \varepsilon_{2t}+(m,p_t)_{p_2} & (pm,p)_{p_2} \\ \dots & \dots & \dots & \dots \\ \varepsilon_{t1}+(m,p_1)_{p_t} & \dots & \varepsilon_{tt}+(m,p_t)_{p_t} & (pm,p)_{p_t} \\ (pm,p_1)_p & \dots & (pm,p_t)_p & (pm,p)_p \end{pmatrix}$$

Pour $i \neq j$, $(-1)^{\varepsilon_{ij}} = (p,p_j)_{p_i} = 1$,

pour $p_i \neq 2$, $(-1)^{\varepsilon_{ii}} = \left(\frac{p}{p_i}\right) = (-1)^{\frac{p-1}{2}\frac{p_i-1}{2}} \left(\frac{p_i}{p}\right) = \left(\frac{p_i}{p}\right)$ car $p \equiv 1\ (4)$;

si $p_i = 2$, $(-1)^{\varepsilon_{ii}} = (p,2)_2 = (-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right) = \left(\frac{p_i}{p}\right)$.

Si $\left(\frac{p_i}{p}\right) = 1$ pour tout i on aura

$$\hat{A} = \begin{pmatrix} & & (pm,p)_{p_1} \\ & A & \vdots \\ & & (pm,p)_{p_t} \\ (pm,p_1)_p & \dots & (pm,p)_p \end{pmatrix} \ ;$$

or $(pm,p)_{p_i} = (p,p)_{p_i}(m,p)_{p_i} = \left(\frac{p}{p_i}\right) = 1$ pour tout i ,

$$(pm,p_i)_p = (p,p_i)_p(m,p_i)_p = \left(\frac{p_i}{p}\right) = 1 \quad \text{pour tout } i \ ,$$

et enfin $(pm,p)_p = (p,p)_p(m,p)_p = (-1)^{\frac{p-1}{2}} \left(\frac{m}{p}\right) = 1$;

$$\hat{A} = \begin{pmatrix} & & 0 \\ & A & \vdots \\ 0 & \ldots & 0 \end{pmatrix}$$ et les rangs de A et $\hat{A}$ sont égaux.

On aura donc pour K : $|\mathcal{H}_2/\mathcal{H}_1| = 2^{t-1-r}$ et pour $\hat{K}$: $|\hat{\mathcal{H}}_2/\hat{\mathcal{H}}_1| = 2^{\hat{t}-1-\hat{r}} = 2^{t-r}$ d'où la relation $\hat{R}_2 = R_2+1$.

On peut donc construire une infinité de corps quadratiques ayant un 4-rang donné.

3. Corps quadratiques ayant un 2^n-rang non nul.

PROPOSITION V.3.- Soient a,b,m,n des entiers positifs non nuls. Soit $\lambda = 1$ si a est impair, 2 sinon. On pose :

$$\lambda^2 a 2^n - mb^2 = m'y^2 \ ,$$

avec les hypothèses suivantes :

(i) $(a,b) = (a,m) = 1$,

(ii) m et m' sont plus grands que 1 et sans facteurs carrés.

Alors le 2^{n+1}-rang du corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{-mm'})$ est non nul.

Démonstration.- On vérifie que $(m,m') = 1$, ainsi, d'après (ii), mm' est un entier sans facteur carré et est divisible par deux nombres premiers distincts au moins.

Soient $p_1,\ldots,p_t$ les nombres premiers ramifiés dans $K/\mathbb{Q}$ $(t \geq 2)$.

LEMME V.2.- Posons $\alpha = \frac{mb+y\sqrt{-mm'}}{\lambda}$; alors α est un entier et l'idéal αA_K est de la forme $\mathfrak{M}\mathfrak{A}^{2^n}$, où $\mathfrak{A}$ est un idéal entier de norme $a\mathbb{Z}$, $\mathfrak{M}$ un produit d'idéaux premiers ramifiés ; $\mathfrak{M}$ et $\mathfrak{A}$ sont premiers entre eux.

On a $\mathrm{Irr}(\alpha) = X^2 - \frac{2mb}{\lambda}X + ma^{2^n}$; α est donc entier. On remarque que $(\frac{2mb}{\lambda}, ma^{2^n}) = m$, l'idéal αA_K est sans facteur rationnel et est donc de la forme voulue. Il en résulte aussi que $\mathfrak{A}$ est produit d'idéaux premiers décomposés non conjugués deux à deux.

LEMME V.3.- Le rang r_1 de la matrice A_1 associée à $\Lambda_1 = \langle p_1, \ldots, p_t \rangle$ vérifie l'inégalité : $r_1 \leq t-2$.

En effet, $mm' = N(\sqrt{-mm'})$ et $m = N(\frac{\alpha}{a^{2^{n-1}}})$; par conséquent, m' et m sont des éléments de $\Lambda_1 \setminus \Lambda_1^2$ qui sont normes ; étant premiers entre eux et non carrés, ils définissent deux solutions non triviales indépendantes du système linéaire associé à Λ_1 .

Fin de la démonstration de la proposition.- Si $n = 1$ le lemme précédent achève la démonstration : $|\mathcal{H}_2/\mathcal{H}_1| \geq 2$ et R_2 est non nul.

Supposons $n > 1$ et montrons par récurrence sur $i \in \{2,3,\ldots,n\}$ qu'il existe une suite de groupes $\mathcal{J}_i$ et Λ_i (relatifs à la détermination de $\mathcal{H}_i$) vérifiant le système d'hypothèses suivant :

$$\mathcal{J}_i = \langle p_1, \ldots, p_t, \mathfrak{A}^{2^{n+1-i}}, \mathfrak{A}_1, \ldots, \mathfrak{A}_{n_i} \rangle ,$$

$$\Lambda_i = \langle p_1, \ldots, p_t, a^{2^{n+1-i}}, a_1, \ldots, a_{n_i} \rangle ,$$

la matrice du système associé à Λ_i étant de la forme

$$A_i = \left(C_1^i \ldots C_t^i 0 D_1^i \ldots D_{n_i}^i \right) \qquad (t+1+n_i \text{ colonnes}) ;$$

enfin le rang r_i de A_i vérifiant : $r_i \leq t-2$.

Vérification pour $i = 2$: on a $\Lambda_1 = \langle p_1, \ldots, p_t \rangle$, l'espace des solutions x du système $A_1.x = 0$ est de dimension $t-r_1$; on complète les deux solutions indépendantes relatives à m et m' par $t-r_1-2$ autres solutions convenables. On applique alors l'algorithme défini dans IV.3 avec les hypothèses supplémentaires expliquées dans la remarque IV.4 :

on a $mm'\mathbb{Z} = N(\sqrt{-mm'}\,A_K) = N(\mathfrak{M})$, avec $\mathfrak{M} = \overline{\prod_{p_i \mid mm'} p_i} \in \mathcal{J}_1$; donc

$(\sqrt{-mm'})A_K = \mathfrak{M}\mathfrak{a}'^{\sigma-1}$ avec, ici, $\mathfrak{a}' = A_K$.

De même $m\mathbb{Z} = N(\mathfrak{M}_1) = N(\frac{\alpha}{a^{2^{n-1}}})$ avec $\mathfrak{M}_1 = \overline{\prod_{\mathfrak{p}_i | m} \mathfrak{p}_i} \in \mathcal{J}_1$ et $(\frac{\alpha}{a^{2^{n-1}}})A_K = \mathfrak{M}_1 \mathfrak{a}'^{1-\sigma}_1$, soit $\mathfrak{a}'^{1-\sigma}_1 = \frac{\mathfrak{M}_1 \mathfrak{a}^{2^n}}{\mathfrak{M}_1 \mathfrak{a}^{2^{n-1}} \mathfrak{a}^{2^{n-1}\sigma}} = (\mathfrak{a}^{1-\sigma})^{2^{n-1}}$ où l'on peut prendre $\mathfrak{a}' = \mathfrak{a}^{2^{n-1}}$. On aura :

$$\mathcal{J}_2 = \langle \mathfrak{p}_1, \ldots, \mathfrak{p}_t, \mathfrak{a}^{2^{n-1}}, \mathfrak{a}_1, \ldots, \mathfrak{a}_{t-2-r_1} \rangle ,$$

$$\Lambda_2 = \langle p_1, \ldots, p_t, a^{2^{n-1}}, a_1, \ldots, a_{n_2} \rangle , \quad n_2 = t-2-r_1 ,$$

$$A_2 = \left(C_1^2 \ldots C_t^2 0 D_1^2 \ldots D_{n_2}^2 \right) = \left((A_1) 0 D_1^2 \ldots D_{n_2}^2 \right) ;$$

on aura bien $r_2 \leq r_1 + n_2 = r_1 + t - 2 - r_1 = t - 2$.

On peut admettre que :

$$\mathcal{J}_{i-1} = \langle \mathfrak{p}_1, \ldots, \mathfrak{p}_t, \mathfrak{a}^{2^{n+2-i}}, \mathfrak{a}_1, \ldots, \mathfrak{a}_{n_{i-1}} \rangle$$

$$\Lambda_{i-1} = \langle p_1, \ldots, p_t, a^{2^{n+2-i}}, a_1, \ldots, a_{n_{i-1}} \rangle$$

$$A_{i-1} = \left((A_{i-2}) D_{n_{i-2}+1} \ldots D_{n_{i-1}} \right) \quad \text{avec} \quad r_{i-1} \leq t-2$$

et $n_{i-1} - n_{i-2} = t-2-r_{i-2}$.

Les solutions $(x,0,\ldots,0)$ telles que $A_{i-2}.x = 0$ constituent un sous-espace $\mathcal{S}$ de dimension $t+1+n_{i-2}$ que l'on complète par un système de $t-2-r_{i-2}$ solutions convenables. En comparant $\mathcal{J}_{i-2}$ et $\mathcal{J}_{i-1}$ on constate que les idéaux $\mathfrak{a}'$ obtenus à partir des équations "$(\beta) = \mathfrak{a}\mathfrak{a}'^{1-\sigma}$" , $\mathfrak{a} \in \mathcal{J}_{i-1}$ sont de la forme

$$\mathfrak{a}^{2^{n+1-i}} , \mathfrak{a}_1 , \ldots , \mathfrak{a}_{n_{i-1}} , \mathfrak{a}_{n_{i-1}+1} , \ldots , \mathfrak{a}_{n_i}$$

avec $n_i = n_{i-1} + (t-2-r_{i-1})$; d'où :

$$\mathcal{J}_i = \langle \mathfrak{p}_1, \ldots, \mathfrak{p}_t, \mathfrak{a}^{2^{n+1-i}}, \mathfrak{a}_1, \ldots, \mathfrak{a}_{n_i} \rangle ,$$

$$\Lambda_i = \langle p_1, \ldots, p_t, a^{2^{n+1-i}}, a_1, \ldots, a_{n_i} \rangle ,$$

$$A_i = \left(C_1^1 \ldots C_t^1 \; 0 \; D_1^{i-1} \ldots D_{n_{i-1}}^{i-1} \; D_{n_{i-1}+1}^{i} \ldots D_{n_i}^{i} \right)$$

(la t+1-ème colonne est nulle tant que l'on a $n+1-i \geq 1$)

$$= \left((A_{i-1} \; D_{n_{i-1}+1} \ldots D_{n_i} \right) \quad \text{qui est telle que}$$

$r_i \leq r_{i-1}+n_i-n_{i-1} = r_{i-1}+t-2-r_{i-1} = t-2$.

Le procédé existe donc pour $i \in \{2,3,\ldots,n\}$; au rang $n+1$ on ne peut rien dire car la $t+1$-ème colonne de la matrice A_{n+1} n'est pas nécessairement nulle. On a donc (proposition IV.2) :

$$2^{R_{n+1}} = |\mathcal{H}_{n+1}/\mathcal{H}_n| = 2^{t-1-r_n} \geq 2 .$$

COROLLAIRE V.1.- Quel que soit n , il existe une infinité de corps quadratiques imaginaires ayant un 2^n-rang non nul. De façon précise, lorsque a est un nombre premier, l'intervalle $[1, \frac{\lambda a^{2^{n-1}}}{\sqrt{m}}]$ contient $N(n,a,m)$ entiers sans facteurs carrés tels que le 2^{n+1}-rang de $\mathbb{Q}(\sqrt{-d})$ soit non nul, avec :

$$N(n,a,m) = \frac{\lambda a^{2^{n-1}-1}(a-1)}{\sqrt{m}} - \delta \quad , \quad 0 \leq \delta \leq 4 .$$

Démonstration.-

LEMME V.4.- Pour n , a et m fixés, l'équation en $b > 0$, $y > 0$: $\lambda^2 a^{2^n} - mb^2 = y^2$ a au plus δ' solution ($\delta' = 1$ si $m \neq 3$, $\delta' = 3$ si $m = 3$).

On a $a^{2^n} = N(\frac{y+b\sqrt{-m}}{\lambda})$ dans $\mathbb{Q}(\sqrt{-m})/\mathbb{Q}$; $\beta = \frac{y+b\sqrt{-m}}{\lambda}$ est entier (il suffit de regarder $\mathrm{Irr}(\beta)$) et $(\beta) = \mathfrak{p}^{2^n}$, $\mathfrak{p}$ étant un idéal premier (puisque a est premier). Si (y',b') est une autre solution on aura $(\frac{y'\pm b'\sqrt{-m}}{\lambda}) = \mathfrak{p}^{2^n}$ soit $\frac{y'\pm b'\sqrt{-m}}{\lambda} = \varepsilon\beta$, ε unité ; d'où le lemme.

LEMME V.5.- Lorsque m' est plus grand que 1 , l'équation en $b > 0$, $y > 0$: $\lambda^2 a^{2^n} - mb^2 = m'y^2$ admet une solution au plus.

Même type de raisonnement que précédemment en utilisant le lemme V.1.

Par conséquent, lorsque $\lambda^2 a^{2^n} - mb^2$ est positif (c'est-à-dire que $1 \leq b < \frac{\lambda a^{2^{n-1}}}{\sqrt{m}}$) il y a autant de valeurs m' différentes que de valeurs de b premières avec a (sauf, éventuellement, $\delta' = 1$ ou 3 valeurs de b donnant $m' = 1$) ; dans l'intervalle $[1, \frac{\lambda a^{2^{n-1}}}{\sqrt{m}}]$ il y a $[\frac{\lambda a^{2^{n-1}}}{a\sqrt{m}}]$ multiples de a d'où $N(n,a,m) = [\frac{\lambda a^{2^{n-1}}}{\sqrt{m}}] - [\frac{\lambda a^{2^{n-1}}}{a\sqrt{m}}] - \delta'$. L'expression de l'énoncé s'en déduit immédiatement, ainsi que la première partie de la proposition.

Exemple V.1.- Soient $n = 2$, $a = 5$, $m = 2$; on aura $14 \leq N(2,5,2) \leq 16$. On trouve pour mm' les valeurs : 94, 226, 466, 574, 674, 766, 926, 994, 1054, 1106, 1186, 1214, 1234, 1246 ; les corps $\mathbb{Q}(\sqrt{-mm'})$ auront un 8-rang non nul.

Remarque V.1.- L'expression $\lambda^2 a^{2^n} - mb^2 = m'y^2$ est celle utilisée dans [18] lorsque $y = 1$. Le fait d'avoir, ici, y quelconque permet de montrer que tous les corps $\mathbb{Q}(\sqrt{-d})$ ayant un 2^{n+1}-rang non nul (d produit de deux facteurs premiers au moins) sont obtenus par ce procédé.

PROPOSITION V.4.- Soient a,b,m,n des entiers positifs non nuls. Soit $\lambda = 1$ si a est impair, 2 sinon. On pose :

$$mb^2 \pm \lambda^2 a^{2^n} = m'y^2 ,$$

avec les hypothèses suivantes :

(i) $(a,b) = (a,m) = 1$,

(ii) m et m' sont plus grands que 1 et sans facteurs carrés ,

(iii) l'unité fondamentale de $\mathbb{Q}(\sqrt{mm'})$ est de norme -1 .

Alors le 2^{n+1}-rang du corps quadratique réel $K = \mathbb{Q}(\sqrt{mm'})$ est non nul .

La démonstration est analogue à celle de la proposition V.5. Cependant la condition (iii) est nécessaire pour que mm' soit norme d'un nombre α tel que l'idéal $\mathfrak{U}'$ vérifiant $\alpha A_K = \mathfrak{M}\mathfrak{U}'^{1-\sigma}$, soit l'idéal unité : on a $-mm' = N(\sqrt{mm'})$ d'où $N(\varepsilon\sqrt{mm'}) = mm'$ si $N\varepsilon = -1$. La condition $-1 \in NK^*$ est d'ailleurs insuffisante car elle n'entraîne pas nécessairement $\mathfrak{U}' = A_K$, en

effet :

Exemple V.2.- Soient $n = 3$, $m = 13$, $b = 9$, alors $mb^2-4a^8 = 29$; -1 est norme mais $|\mathcal{H}(K)| = 4$ avec $R_1 = R_2 = 1$ et $R_3 = 0$.

4. Autres exemples avec $\ell = 2$.

Dans ce paragraphe, nous allons montrer que certains résultats connus sur les corps quadratiques (et qui utilisent aussi les symboles locaux) découlent naturellement des méthodes exposées ici.

PROPOSITION V.5. (Hasse [13] et [14])- Soient p et $q \neq 2$ deux nombres premiers distincts tels que $pq \equiv 2$ ou $3 \bmod 4$; soit $K = \mathbb{Q}(\sqrt{-pq})$ et soit $\{1,\theta\}$ une $\mathbb{Z}$-base de A_K , alors :

(i) $\mathcal{H}(K)$ est cyclique,

(ii) si le symbole de Legendre $\left(\frac{p}{q}\right)$ est égal à -1 alors $|\mathcal{H}(K)| = 2$,

(iii) si $\left(\frac{p}{q}\right) = 1$, il existe $x,y,z \in \mathbb{Z}$, $z > 0$, $(x,y,z) = 1$, tels que $pz^2 = N(x+y\theta)$; si $\left(\frac{z}{p}\right) = -1$ alors $|\mathcal{H}(K)| = 2^2$, sinon $|\mathcal{H}(K)|$ est divisible par 2^3 .

Démonstration.- Les nombres premiers ramifiés sont p et q (2 n'est ramifié que lorsque $p = 2$) et le groupe Λ associé à $\mathcal{H}_1$ est donc $\Lambda_1 = \langle p,q \rangle$; la matrice du système étant (en notation multiplicative) :

$$A = \begin{pmatrix} (-pq,p)_p & (-pq,q)_p \\ (-pq,p)_q & (-pq,q)_q \end{pmatrix} = \begin{pmatrix} \left(\frac{p}{q}\right) & \left(\frac{p}{q}\right) \\ \left(\frac{p}{q}\right) & \left(\frac{p}{q}\right) \end{pmatrix} ;$$

si $\left(\frac{p}{q}\right) = -1$ le rang de A est $r = 1$ et $\mathcal{H}(K) = \mathcal{H}_1$, d'où (ii) . Supposons maintenant que $\left(\frac{p}{q}\right) = 1$: le rang de A est nul. Pour déterminer un groupe d'idéaux $\mathcal{J}$ associé à $\mathcal{H}_2$ il faut résoudre les équations :

$$p = N\alpha \quad \text{et} \quad q = N\beta \quad , \quad \alpha,\beta \in K^* ;$$

en fait la relation $N(\sqrt{-pq}) = pq$ montre qu'il suffit d'une seule équation

$(p = N\alpha)$. On a donc

$$pz^2 = N(x+y\theta) \quad , \quad x,y,z \in \mathbb{Z} \quad , \quad (x,y,z) = 1 \ ;$$

on constate sans peine que

$$(x+y\theta)A_K = \mathfrak{A}^2\mathfrak{p} \quad \text{avec} \quad \mathfrak{p}^2 = p\mathbb{Z}$$

et $\mathfrak{A}^{1+\sigma} = z\mathbb{Z}$; il existe $\mathfrak{A}'$ tel que $(\frac{x+y\theta}{z})A_K = \mathfrak{p}\,\mathfrak{A}'^{1-\sigma}$ soit $\mathfrak{A}'^{1-\sigma} = \frac{\mathfrak{A}^2}{zA_K} = \mathfrak{A}^{1-\sigma}$. On peut donc prendre $\mathfrak{A}' = \mathfrak{A}$ et $N\mathfrak{A} = z$. Il en résulte que $\mathcal{J} = \langle \mathfrak{p}, \mathfrak{q}, \mathfrak{A}, \mathfrak{A}^\sigma \rangle$ et que le groupe Λ associé est $\Lambda = \langle p,q,z \rangle$; la matrice B correspondante est donc $B = \begin{pmatrix} 1 & 1 & \left(\frac{z}{p}\right) \\ & & \\ 1 & 1 & \left(\frac{z}{p}\right) \end{pmatrix}$: si $\left(\frac{z}{p}\right) = -1$ le rang de B est 1 et $\mathcal{H}_2 = \mathcal{H}(K)$, si $\left(\frac{z}{p}\right) = +1$ le rang de B est nul et $|\mathcal{H}_2/\mathcal{H}_1| = |\mathcal{H}_3/\mathcal{H}_2| = 2$, d'où l'assertion (iii).

Remarque V.2.- Le procédé peut alors se continuer (cf. chapitre VI : "Algorithme pour $\ell = 2$", valable pour un corps quadratique quelconque).

PROPOSITION V.6. (Hasse [12])- Soit p congru à 1 modulo 8 ; alors il existe x et y positifs tels que $p = 2x^2 - y^2$. Si on a $x \equiv 1$ modulo 4 , $|\mathcal{H}(\mathbb{Q}(\sqrt{-p}))|$ est divisible par 8 .

Démonstration.- On aura $\Lambda_1 = \langle p,2 \rangle$ car 2 est ramifié dans $\mathbb{Q}(\sqrt{-p})/\mathbb{Q}$; la matrice associée sera

$$\begin{pmatrix} (-p,p)_p & (-p,2)_p \\ & \\ (-p,p)_2 & (-p,2)_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ & \\ 1 & 1 \end{pmatrix} \quad \text{de rang nul.}$$

Comme $p = N(\sqrt{-p})$, il suffit de traduire le fait que 2 est norme : or p étant décomposé dans $\mathbb{Q}(\sqrt{2})$, qui est principal et dont l'unité fondamentale est de norme -1 , on peut écrire $-p = y^2 - 2x^2$, x,y positifs premiers à p . On a donc $2x^2 = y^2 + p$; ceci conduit à la relation

$$(\frac{y+\sqrt{-p}}{x})A_K = \mathfrak{p}_2\mathfrak{A}^{\sigma-1} \quad , \text{ avec } \mathfrak{p}_2^2 = (2)A_K \text{ et } N\mathfrak{A} = (x) \ .$$

On obtient alors $\Lambda_2 = \langle p,2,x\rangle$ avec pour matrice associée :

$$\begin{pmatrix} 1 & 1 & (-p,x)_p \\ 1 & 1 & (-p,x)_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & (-1)^{\frac{x-1}{2}} \\ 1 & 1 & (-1)^{\frac{x-1}{2}} \end{pmatrix}$$, d'où la proposition.

PROPOSITION V.7.- Soit p premier impair ; alors $|\mathcal{H}(\mathbb{Q}(\sqrt{2p}))| = 2$ si et seulement si $p \not\equiv 1$ modulo 8 . Lorsque $p \equiv 1$ modulo 8 alors $|\mathcal{H}(\mathbb{Q}(\sqrt{2p}))|$ est divisible par 8 si et seulement si $p \equiv 1$ mod 16 et dans l'écriture $p = x^2+2y^2$, y est divisible par 4 (sinon ce nombre est égal à 4).

Démonstration.- On aura $\mathcal{J}_1 = \langle \mathfrak{p}_2, \mathfrak{p}_p\rangle$ et $\Lambda_1 = \langle 2,p\rangle$ la matrice associée sera alors :

$$A_1 = \begin{pmatrix} (2p,2)_2 & (2p,p)_2 \\ (2p,2)_p & (2p,p)_p \end{pmatrix} = \begin{pmatrix} (-1)^{\frac{p^2-1}{8}} & (-1)^{\frac{p^2-1}{8}+\frac{p-1}{2}} \\ (-1)^{\frac{p^2-1}{8}} & (-1)^{\frac{p^2-1}{8}+\frac{p-1}{2}} \end{pmatrix}$$

on a alors $\mathcal{H}_2 = \mathcal{H}_1$ si et seulement si l'un des 4 symboles est différent de 1 donc si et seulement si $p \equiv 3,5$ ou 7 modulo 8 .

Supposons $p \equiv 1$ modulo 8 , alors $A_1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ et $|\mathcal{H}_2| = 2|\mathcal{H}_1| = 4$. Il en résulte aussi que p est décomposé dans les corps $\mathbb{Q}(\sqrt{-2})$ et $\mathbb{Q}(\sqrt{2})$ et qu'il existe des entiers u , v , x et y tels que

$$-p = u^2-2v^2 \quad \text{et} \quad p = x^2+2y^2$$

ce qui entraîne

$$(2v)^2-2p = 2u^2 \quad \text{et} \quad p^2-2py^2 = px^2$$

où l'on peut supposer $(p,y) = 1$ et $(u,v) = 1$.

On a $(2v+\sqrt{2p})A_k = \mathfrak{p}_2\mathfrak{U}^2$ où $\mathfrak{U}$ est un idéal entier de norme u et, de même $(p+y\sqrt{2p})A_k = \mathfrak{p}_p\mathfrak{U}'^2$ avec $\mathfrak{U}'$ entier de norme x . On a déjà vu que cela entraînait $\mathcal{J}_2 = \langle \mathfrak{p}_2, \mathfrak{p}_p, \mathfrak{U}, \mathfrak{U}', \mathfrak{U}^\sigma, \mathfrak{U}'^\sigma\rangle$ et $\Lambda_2 = \langle 2,p,u,x\rangle$ dont la matrice

associée est $\begin{pmatrix} 1 & 1 & (2p,u)_2 & (2p,x)_2 \\ 1 & 1 & (2p,u)_p & (2p,x)_p \end{pmatrix} = \begin{pmatrix} 1 & 1 & (-1)^{\frac{u^2-1}{8}} & (-1)^{\frac{x^2-1}{8}} \\ 1 & 1 & \left(\frac{u}{p}\right) & \left(\frac{x}{p}\right) \end{pmatrix}$

$$= \begin{pmatrix} 1 & 1 & (-1)^{\frac{u^2-1}{8}} & (-1)^{\frac{x^2-1}{8}} \\ 1 & 1 & (-1)^{\frac{u^2-1}{8}} & (-1)^{\frac{x^2-1}{8}} \end{pmatrix}$$

grâce à la formule du produit ; le fait que $u^2 \equiv 1\ (16)$ et $x^2 \equiv 1\ (16)$ est équivalent à $y \equiv 0\ (4)$ et $p \equiv 1 \bmod 16$, d'où la proposition.

Remarque V.3.- Les résultats précédents sont connus de P. Kaplan qui en a donné une démonstration élémentaire à partir de l'étude des formes quadratiques ("Divisibilité par 8 du nombre de classes des corps quadratiques dont le 2-sous-groupe des classes est cyclique et réciprocité biquadratique", à paraître à Journal of the Math. Soc. or Japan).

CHAPITRE VI

METHODES EFFECTIVES - RESULTATS NUMERIQUES

A. Etude du cas $k = \mathbb{Q}$

1. Construction des extensions cycliques de degré ℓ de $\mathbb{Q}$.

Nous reprenons ici l'étude générale du chapitre III (paragraphe B) avec ℓ premier impair.

A $K/\mathbb{Q}$ est associée l'extension de Kummer $K'/\mathbb{Q}'$ définie par $K' = \mathbb{Q}'(\sqrt[\ell]{\alpha})$ où le nombre α choisi est tel que $q(\alpha) \in \mathfrak{x}^*$. Les seules places qui peuvent se ramifier dans $K'/\mathbb{Q}'$ sont :

les idéaux premiers totalement décomposés dans $\mathbb{Q}'/\mathbb{Q}$,
l'idéal premier $\mathfrak{P}_o = (1-\zeta)$ au-dessus de ℓ dans $\mathbb{Q}'$.

PROPOSITION VI.1.- Choisissons α congru à 1 modulo $\mathfrak{P}_o$; alors ℓ est ramifié dans $K'/\mathbb{Q}'$ (donc dans $K/\mathbb{Q}$) si et seulement si la quantité

$$w = \frac{\alpha-1}{1-\zeta}$$

est première à $\mathfrak{P}_o$.

Démonstration.- Si ℓ est ramifié, c'est que l'entier maximum λ tel que l'on ait $\alpha \equiv \xi^\ell \bmod \mathfrak{P}_o^\lambda$ dans $\mathbb{Q}'$ vérifie $\lambda < \ell$ (cf. proposition I.2) ; on a donc $\alpha = \xi^\ell + (1-\zeta)^\lambda w_1$ avec de plus $\xi \equiv 1 \bmod \mathfrak{P}_o$;
$\alpha = (1+(1-\zeta)A)^\ell + (1-\zeta)^\lambda w_1$, ce qui est de la forme $\alpha = 1 + (1-\zeta)^\lambda w'$ avec w' premier à $\mathfrak{P}_o$.

Soit s un générateur de $G = Gal(\mathbb{Q}'/\mathbb{Q})$ et soit g un entier tel que $\alpha^s = \alpha^g u^\ell$, $u \in \mathbb{Q}'$. On obtient :

$$1 + (1-\zeta^g)^\lambda w'^s = (1+(1-\zeta)^\lambda w')^g u^\ell \quad ,$$

$$1 + (1-\zeta^g)^\lambda w'^s \equiv (1+(1-\zeta)^\lambda w')^g \mod \mathfrak{p}_o^{\lambda+1} \quad ,$$

$$1 + (1-\zeta^g)^\lambda w'^s \equiv 1 + gw'(1-\zeta)^\lambda \quad " \quad ,$$

$$(1-\zeta)^\lambda (1+\zeta+\ldots+\zeta^{g-1})^\lambda w'^s \equiv gw'(1-\zeta)^\lambda \quad " \quad ,$$

$$(1+\zeta+\ldots+\zeta^{g-1})^\lambda \equiv g \mod \mathfrak{p}_o$$

(on a, en effet, $w'^s \equiv w' \mod \mathfrak{p}_o$ car G opère trivialement sur $A_{\mathbb{Q}'}/\mathfrak{p}_o$) ; finalement, $g^\lambda \equiv g \mod \ell$ entraîne $\lambda = 1$ et $w' = w$ puisque $1 \leq \lambda < \ell$; w est donc premier à $\mathfrak{p}_o$.

La réciproque est immédiate car alors la congruence $\alpha \equiv \xi^\ell \mod \mathfrak{p}_o^\ell$ est manifestement insoluble.

La proposition III.2 nous montre que :

$$\overline{\alpha A_{\mathbb{Q}'}} = \overline{\prod_{\mathfrak{p} \in P}} \ \overline{\mathfrak{p}}^{e^* x_\mathfrak{p}} \quad , \quad x_\mathfrak{p} \in \mathbb{Z} \ ;$$

on est donc amené à introduire l'ensemble $\mathbb{V}$ suivant :

DEFINITION VI.1.- Soit $t \geq 1$ et soit $\mathbb{V}$ le quotient de l'ensemble des t-uples $(v_1,\ldots,v_t) \in \mathbb{F}_\ell^t$ avec les v_i tous non nuls, par la relation d'équivalence définissant l'espace projectif $\mathbb{P}(\mathbb{F}_\ell^t)$.

On peut alors associer à $q(\alpha)$ un point de $\mathbb{V}$ de la manière suivante :

(i) si ℓ est non ramifié dans $K/\mathbb{Q}$ on associe le t-uple $(v_1,\ldots,v_t) \in \mathbb{F}_\ell^t$ défini par $v_i \equiv v_{\mathfrak{p}_i}(\alpha)$ avec $\mathfrak{p}_i \in \mathfrak{P}$ (on rappelle que $\mathfrak{P}$ est un système d'idéaux premiers non conjugués deux à deux représentant les idéaux qui peuvent se ramifier dans $K'/\mathbb{Q}'$) ;

(ii) si ℓ est ramifié dans $K/\mathbb{Q}$ on associe le t-uple $(v_1,\ldots,v_{t-1},v_t) \in \mathbb{F}_\ell^t$ défini par $v_i \equiv v_{\mathfrak{p}_i}(\alpha)$ pour $1 \leq i \leq t-1$, $\mathfrak{p}_i \in \mathfrak{P}$

et $v_t \equiv \frac{\alpha-1}{1-\zeta_o}$ modulo $\mathfrak{P}_o$.

On définit, de cette manière, une application de $\mathbb{P}(\mathfrak{X}^*)$ dans $\mathbb{V}$ qui dépend du choix de $\mathfrak{D}$ et, lorsque ℓ est ramifié, du choix de la racine primitive $\ell^{\text{ème}}$ de l'unité ζ_o .

PROPOSITION VI.2.- L'application définie ci-dessus est bijective.

Ce résultat provient, par exemple, du fait que l'on peut dénombrer l'ensemble des extensions cycliques de degré ℓ ramifiées en t places données (en l'occurence ce nombre est égal à $(\ell-1)^{t-1}$) .

2. Systèmes linéaires associés aux groupes Λ .

Soient $p_1,\ldots,p_t$ les nombres premiers ramifiés dans $K/\mathbb{Q}$; si ℓ est ramifié on posera $\ell = p_t$.

Soit Λ le groupe de nombres associé à un quotient $\tilde{\mathcal{H}}/\mathcal{H}$ (notations du théorème IV.3). Etant donnée une base de Λ/Λ^{ℓ} de la forme $q(a_1),\ldots,q(a_n)$ on fera l'hypothèse suivante (non restrictive car on peut s'y ramener par un choix convenable du H-module $\mathcal{J}$ associé à $\mathcal{H}$) :

HYPOTHESE VI.1.- On a pour $\bar{t} \leq t$: $a_1 = p_1,\ldots,a_{\bar{t}} = p_{\bar{t}}$, et les nombres $a_{\bar{t}+1},\ldots,a_n$ ne sont divisibles par aucun des nombres premiers $p_1,\ldots,p_t$ ramifiés dans $K/\mathbb{Q}$.

DEFINITION VI.2.- Soit $\mathfrak{P}$ un idéal premier dans $\mathbb{Q}'$; on note $n_{\mathfrak{P}}$ le nombre de conjugués distincts de $\mathfrak{P}$ dans $\mathbb{Q}'/\mathbb{Q}$ et on pose pour $a \in \mathbb{Q}$:

$$[a]_{\mathfrak{P}} = (p,a)_{\mathfrak{P}} \quad , \quad (p) = \mathfrak{P}\cap\mathbb{Z} \quad , \quad \mathfrak{P} \neq \mathfrak{P}_o$$

$$[a]_{\mathfrak{P}_o} = (\zeta_o,a)_{\mathfrak{P}_o} \quad \text{sinon.}$$

On a alors le lemme suivant :

LEMME VI.1.- Soit $p = p_i$ et soit $a \in \mathbb{Q}$, a premier à p_i ; alors

$$(\alpha,a)_{p_i} = [a]_{\wp_i}^{-v_i n_{\wp_i}} .$$

Si $p_i \neq \ell$ on a $(\alpha,a)_{p_i} = (\alpha,a)_{\wp_i}$ et

$$(\alpha,a)_{\wp_i} \equiv \left(\alpha^{v_{\wp_i}(a)}\, a^{-v_{\wp_i}(\alpha)}\right)^{\frac{p_i-1}{\ell}} \text{ modulo } \wp_i \equiv \left(a^{-v_i}\right)^{\frac{p_i-1}{\ell}} \text{ modulo } \wp_i ;$$

or $[a]_{\wp_i} = (p_i,a)_{\wp_i}$ et $n_{\wp_i} = \ell-1$;

$$(p_i,a)_{\wp_i} \equiv \left(p_i^{v_{\wp_i}(a)}\, a^{-v_{\wp_i}(p_i)}\right)^{\frac{p_i-1}{\ell}} \text{ modulo } \wp_i \equiv \left(a^{-1}\right)^{\frac{p_i-1}{\ell}} \text{ modulo } \wp_i ,$$

d'où le lemme dans ce cas .

Si $p_i = p_t = \ell$ on a $(\alpha,a)_\ell = \zeta_o^{S_{\wp_o} q_{\wp_o} \left(\frac{\lambda_{\wp_o}(\alpha-1)(a-1)}{\ell(\zeta_o-1)}\right)}$ et, de même

$(\zeta_o,a)_{\wp_o} = \zeta_o^{S_{\wp_o} q_{\wp_o} \left(\frac{\lambda_{\wp_o}(\zeta_o-1)(a-1)}{\ell(\zeta_o-1}\right)}$; on a alors $v_t \equiv \frac{\alpha-1}{1-\zeta_o}$ et $n_{\wp_o} = 1$; le lemme en résulte alors immédiatement.

Remarque VI.1.- Les calculs effectifs du chapitre III, paragraphe C montrent que si l'on pose

$$a^{\ell-1} = 1 + \mu\ell ,$$

alors

$$(\alpha,a)_{\wp_o} = \zeta_o^{\mu v_t}$$

lorsque $\ell = p_t$ est ramifié (on a, en effet, $S_{\wp_o}$ = identité , $\lambda_{\wp_o} = 1$ d'après la proposition VI.1).

Posons, pour simplifier l'écriture,

$$n_i = n_{\wp_i} , \quad [a]_i = [a]_{\wp_i} , \quad \wp_i \in \mathcal{P} \quad \text{et} \quad (\alpha,a_i)_j = (\alpha,a_i)_{\wp_j} .$$

THEOREME VI.1.- Soit Λ un groupe de nombres associé au quotient $\tilde{\mathcal{H}}/\mathcal{H}$ et soit $q(a_1),\ldots,q(a_n)$ une base de Λ/Λ^{ℓ} vérifiant l'hypothèse VI.1 ; le système linéaire $\prod_{i=1}^{n} (\alpha,a_i)_j^{x_i} = 1$, $1 \le j \le t$ s'écrit (pour ℓ impair) :

$$\begin{cases} \prod_{i=1}^{n} [a_i]_j^{v_j x_i} \prod_{k=1}^{t} [a_j]_k^{-v_k x_j} = 1 \quad , \quad 1 \le j \le \bar{t} \\ \prod_{i=1}^{n} [a_i]_j^{x_i} = 1 \quad , \quad \bar{t}+1 \le j \le t \quad , \end{cases}$$

où l'on a posé $[a]_{\wp} = (p,a)_{\wp}$, $p\mathbb{Z} = \wp\cap\mathbb{Z}$, $\wp \neq \wp_o$, $[a]_{\wp_o} = (\zeta_o,a)_{\wp_o}$.

Démonstration.- Le système $\prod_{i=1}^{n} (\alpha,a_i)_j^{x_i} = 1$ s'écrit

$$\prod_{i=1}^{\bar{t}} (\alpha,a_i)_j^{x_i} \prod_{i\ge\bar{t}} (\alpha,a_i)_j^{x_i} = 1 \ ;$$

pour $i > \bar{t}$, a_i est premier à tous les p_j , $j = 1,\ldots,t$ donc $(\alpha,a_i)_j = [a_i]_j^{-n_j v_j}$. On aura donc pour $j \le \bar{t}$:

$$\prod_{i=1}^{n} (\alpha,a_i)_j^{x_i} = \prod_{\substack{i=1 \\ i\neq j}}^{\bar{t}} (\alpha,a_i)_j^{x_i} (\alpha,a_j)_j^{x_j} \prod_{i>\bar{t}} (\alpha,a_i)_j^{x_i} = 1$$

$$= \prod_{\substack{i=1 \\ i\neq j}}^{\bar{t}} [a_i]_j^{-n_j v_j x_i} (\alpha,a_j)_j^{x_j} \prod_{i>\bar{t}} [a_i]_j^{-n_j v_j x_i} = 1$$

Calcul de $(\alpha,a_j)_j$ $(j \le \bar{t})$:

La formule du produit donne $\prod_{|\wp|} (\alpha,a_j)_{\wp} = 1$, ou encore $\prod_{\substack{|\wp| \\ \text{ramifié}}} (\alpha,a_j)_{\wp} = 1$, soit $\prod_{k=1}^{t} (\alpha,a_j)_k^{n_k} = 1$;

$$(\alpha,a_j)_j = \prod_{\substack{k=1 \\ k\neq j}}^{t} (\alpha,a_j)_k^{-n_k/n_j} = \prod_{\substack{k=1 \\ k\neq j}}^{t} [a_j]_k^{n_k^2 v_k/n_j} \quad .$$

Or $n_i = 1$ ou $\ell-1$; par conséquent, on aura $n_k^2 \equiv 1$ et $1/n_j \equiv n_j$ modulo ℓ et :

$$(\alpha, a_j)_j = \prod_{\substack{k=1 \\ k\neq j}}^{t} [a_j]_k^{n_j v_k} .$$

Il vient alors pour la $j^{\text{ème}}$ ligne du système :

$$\prod_{\substack{i=1 \\ i\neq j}}^{n} [a_i]_j^{-n_j v_j x_i} \prod_{\substack{k=1 \\ k\neq j}}^{t} [a_j]_k^{n_j v_k x_j} = 1 \text{ , soit } \prod_{\substack{i=1 \\ i\neq j}}^{n} [a_i]_j^{v_j x_i} \prod_{\substack{k=1 \\ k\neq j}}^{t} [a_j]_k^{-v_k x_j} = 1 \text{ , } j \leq \bar{t}$$

Pour $j > \bar{t}$, l'hypothèse a_i premier avec p_j est vérifiée pour tout i et on obtient :

$$\prod_{i=1}^{n} (\alpha, a_i)_j^{x_i} = \prod_{i=1}^{n} [a_i]_j^{-n_j v_j x_i} = 1$$

soit encore

$$\prod_{i=1}^{n} [a_i]_j^{x_i} = 1 \quad , \quad j > \bar{t} .$$

COROLLAIRE VI.1.- Lorsque $\mathcal{H}$ contient $\mathcal{H}_1$, on peut toujours supposer que $a_1 = p_1, \ldots, a_t = p_t$ et l'expression du système devient :

$$\prod_{i=1}^{t} [p_i]_j^{v_j x_i} [p_j]_i^{-v_i x_j} \prod_{i=t+1}^{n} [a_i]_j^{v_j x_i} = 1 \quad , \quad 1 \leq j \leq t .$$

COROLLAIRE VI.2.- Lorsque $\mathcal{H} = \mathcal{H}_1$ le groupe Λ est égal à $\langle p_1, p_2, \ldots, p_t \rangle$ et le système est alors :

$$\prod_{i=1}^{t} [p_i]_j^{v_j x_i} [p_j]_i^{-v_i x_j} = 1 \quad , \quad 1 \leq j \leq t .$$

THEOREME VI.2.- Lorsque ℓ est égal à 2 , il existe $m \in \mathbb{Z}$ tel que $K = \mathbb{Q}(\sqrt{m})$ et le système associé à Λ est $\prod_{i=1}^{n} (m, a_i)_j^{x_i} = 1$, $1 \leq j \leq t$ avec les formules :

$$(a,b)_p = (-1)^{\frac{p-1}{2} v_p(a) v_p(b)} \left(\frac{b'}{p}\right)^{v_p(a)} \left(\frac{a'}{p}\right)^{v_p(b)} \quad \text{(Symboles de Legendre)}$$

où $a' = \frac{a}{p^{v_p(a)}}$, $b' = \frac{b}{p^{v_p(b)}}$, $p \neq 2$,

$$(2,a)_2 = (-1)^{\frac{a^2-1}{8}} \quad \text{si } a \text{ est impair,}$$

$$(a,b)_2 = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} \quad \text{si } a \text{ et } b \text{ sont impairs .}$$

Remarque VI.2.- Si r_i désigne le rang du système linéaire associé à la détermination de $|\mathfrak{H}_{i+1}/\mathfrak{H}_i|$, la proposition IV.2 montre que

$$\ell^{R_1} = \prod_{i=0}^{\ell-2} |\mathfrak{H}_{i+1}/\mathfrak{H}_i| = \prod_{i=0}^{\ell-2} \ell^{t-1-r_i} \text{ , soit :}$$

$$R_1 = (\ell-1)(t-1) - \sum_{i=1}^{\ell-2} r_i$$

(cf. remarque de [20] p. 361 ainsi que : Fröhlich, the generalization of a theorem of L. Rédei's, quart. J. of Math. 5, 1954 et les références p. 140).

3. Etude du cas $\mathfrak{H} = \mathfrak{H}_1$.

La dimension du quotient $\mathfrak{H}_2/\mathfrak{H}_1$ est égale à $t-1-r$ où r est le rang du système

$$(S) : \prod_{i=1}^{t} [p_i]_j^{v_j x_i} [p_j]_i^{-v_i x_j} = 1 , \quad 1 \leq j \leq t .$$

PROPOSITION VI.3.- Le rang r du système (S) est égal à 0 si et seulement si p_i est congru à une puissance $\ell^{\text{ème}}$ modulo p_j pour tout i , j , $i \neq j$, en remplaçant cette condition par p_i congru à 1 modulo ℓ^2 lorsque $p_t = \ell$. En outre, lorsque $r = 0$ relativement à $K/\mathbb{Q}$, on a $r = 0$ relativement aux $(\ell-1)^{t-1}$ extensions ayant même discriminant que $K/\mathbb{Q}$.

Démonstration.- La dernière partie de la proposition est évidente car la nullité de r ne dépend pas du système $\{v_1,\dots,v_t\}$ considéré.

On aura $r = 0$ si et seulement si $[p_i]_j = 1$ pour tout i , j , $i \neq j$; si $p_j \neq \ell$ on a

$$[p_i]_j = (p_j, p_i)_{\wp_j} \equiv (1/p_i)^{\frac{p_j-1}{\ell}} \quad \text{modulo } \wp_j \ ,$$

d'où l'assertion ; si $p_j = \ell$ alors

$$[p_i]_j = (\zeta_o, p_i)_{\wp_o} = \zeta_o^{\frac{p_i-1}{\ell}} \ .$$

PROPOSITION VI.4.- Lorsque $t = 2$ on a les résultats suivants :

(i) l'ordre des groupes $\mathcal{H}_2$ est le même pour les $\ell-1$ extensions $K/\mathbb{Q}$ ramifiées en p_1 , p_2 ;

(ii) si r est égal à 0 (ce qui équivaut à la condition $\mathcal{H}_2/\mathcal{H}_1 \neq \{1\}$) soit p un nombre premier décomposé dans $K/\mathbb{Q}$ tel que l'un des symboles $[p]_{\wp_1}$, $[p]_{\wp_2}$ soit différent de 1 ; alors $\mathcal{H}(K)$ est le ℓ-sous-groupe de Sylow du H-module engendré par la classe d'un idéal premier $\mathfrak{p}$ au-dessus de p dans K .

Démonstration.- Pour $t = 2$ le système (S) s'écrit :

$$\begin{cases} [p_2]_1^{v_1 x_2}\ [p_1]_2^{-v_2 x_1} = 1 \\ [p_1]_2^{v_2 x_1}\ [p_2]_1^{-v_1 x_2} = 1 \ , \end{cases}$$

Posons $[p_i]_j = \zeta_o^{a_{ij}}$; on obtient alors en notation additive le système :

$$\begin{cases} -a_{12} v_2 x_1 + a_{21} v_1 x_2 = 0 \\ a_{12} v_2 x_1 - a_{21} v_1 x_2 = 0 \end{cases}$$

dont le rang ne dépend pas des nombres v_i car ceux-ci sont non nuls par hypothèse.

D'où l'assertion (i) .

Supposons maintenant $r = 0$. Il existe q premier à ℓ tel que la classe de $\mathfrak{p}^q$ est d'ordre une puissance de ℓ dans $H(K)$. Considérons $\mathcal{J} = \langle \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}^q, \mathfrak{p}^{q\sigma}, \ldots, \mathfrak{p}^{q\sigma^{\ell-1}} \rangle$ où $\mathfrak{p}_1$, $\mathfrak{p}_2$ désignent les deux idéaux premiers ramifiés dans $K/\mathbb{Q}$. Soit $\mathcal{H}$ l'image de $\mathcal{J}$ dans le groupe des classes de K ; on a en fait $\mathcal{H} \subset H(K)$.

On vérifie que $\mathcal{J} \cap \mathcal{J}(K)^{\sigma-1} = \mathcal{J}^{\sigma-1}$; on peut alors appliquer les théorèmes IV.2 et IV.3 : on aura $|\tilde{\mathcal{H}}/\mathcal{H}| = \ell^{t-1-r'} = \ell^{1-r'}$ où r' est le rang du système associé au groupe :

$$\Lambda = \langle p_1, p_2, p^q \rangle ;$$

or l'hypothèse faite sur p entraîne $r' = 1$ soit $\tilde{\mathcal{H}} = \mathcal{H}$; il en résulte alors que $H(K) = \mathcal{H}$. Soit h la classe de $\mathfrak{p}^q$; elle est différente de 1 sinon on aurait $H(K) = \mathcal{H}_1$ (ce qui est contraire à l'hypothèse) ; par conséquent, le générateur h_1 de $\mathcal{H}_1$ est de la forme $h^{(\sigma-1)^\lambda}$ pour λ convenable et $H(K)$ est bien le H-module engendré par h.

Le résultat (i) devient faux en général lorsque t est strictement plus grand que 2 :

Exemple VI.1.- Soit $\ell = 3$; considérons les 4 corps cubiques de discriminant $(7.163.271)^2$; la matrice du système linéaire associé au groupe $\Lambda = \langle 7, 163, 271 \rangle$ est de la forme :

$$\begin{pmatrix} v_2+v_3 & 2v_1 & 2v_1 \\ 2v_2 & v_1-v_3 & v_2 \\ 2v_3 & v_3 & v_1-v_2 \end{pmatrix}$$

Pour $v_1 = 1$, $v_2 = v_3 = 2$ la matrice du système est $\begin{pmatrix} 1 & 2 & 2 \\ 1 & 2 & 2 \\ 1 & 2 & 2 \end{pmatrix}$ et est de rang 1 et le corps correspondant a un 3-rang égal à 3 ; on vérifie que dans tous les autres cas la matrice obtenue est de rang 2 ; les trois autres corps ont donc un 3-rang égal à 2.

On peut donner une classification des ensembles $\{p_1, \ldots, p_t\}$ pour t donné de la manière suivante :

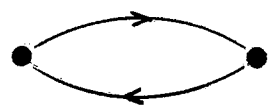
DEFINITION VI.3.- Graphe associé à l'ensemble $\{p_1,\ldots,p_t\}$.

Le graphe associé à $\{p_1,\ldots,p_t\}$ est constitué de t sommets $S_1,\ldots,S_t$ et des arêtes orientées $S_i \rightharpoonup S_j$, où (i,j) , $i \neq j$, parcourt l'ensemble des couples pour lesquels $[p_i]_j = 1$ (Définition VI.2). Ce graphe est donc associé à l'ensemble des $(\ell-1)^{t-1}$ extensions $K/\mathbb{Q}$ de discriminant donné.

Lorsque t augmente le nombre de systèmes possibles, relativement à $\mathcal{H} = \mathcal{H}_1$ (i.e. $\Lambda = \langle p_1,\ldots,p_t\rangle$) ,est rapidement très grand (les $[p_i]_j$ pouvant prendre toutes valeurs) et l'étude du rang en fonction du t-uple $(v_1,\ldots,v_t)$ complexe ; l'étude du graphe associé semble simplifier la situation : nous donnons les résultats pour $\ell = 3$, $t = 2$ et 3 (la démonstration n'étant qu'une vérification fastidieuse). Posons $\delta = a_{12}a_{23}a_{31} - a_{13}a_{32}a_{21}$ (on rappelle que $[p_i]_j = \zeta_o^{a_{ij}}$).

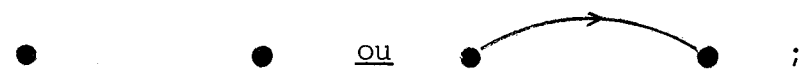
PROPOSITION VI.5.- a) Si $\ell = 3$ et $t = 2$ alors :

(i) $R_1 = 2$ pour les deux corps si le graphe associé est :



;

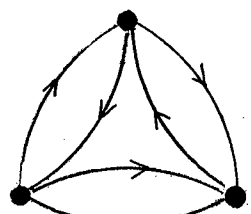
(ii) $R_1 = 1$ pour les deux corps si le graphe associé est :



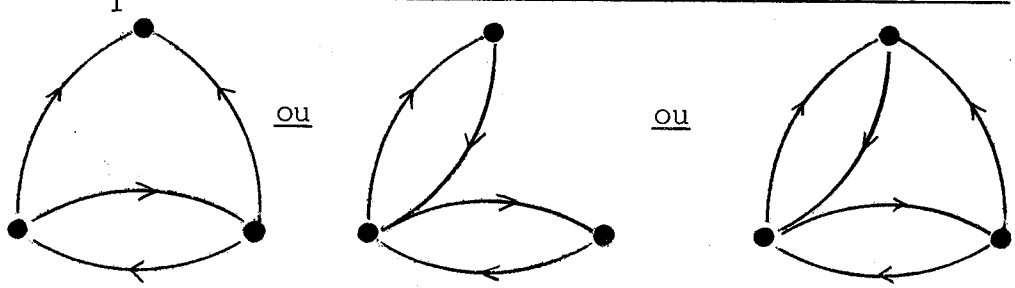
ou ;

b) Si $\ell = 3$ et $t = 3$ alors :

(i) $R_1 = 4$ pour les quatre corps si le graphe associé est :

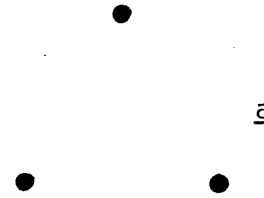


(ii) $R_1 = 3$ pour les quatre corps si le graphe associé est :

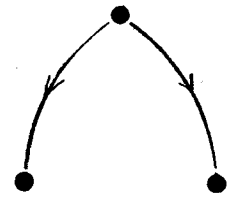


ou ou ;

(iii) $R_1 = 3$ pour un corps et $R_1 = 2$ pour les trois autres si le graphe associé est :

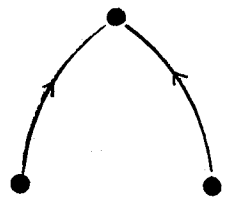


avec $\delta = 0$, ou

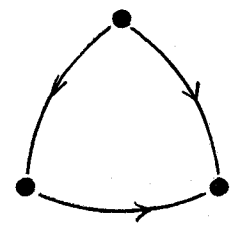


;

(iv) $R_1 = 3$ pour deux corps et $R_1 = 2$ pour les deux autres si le graphe associé est

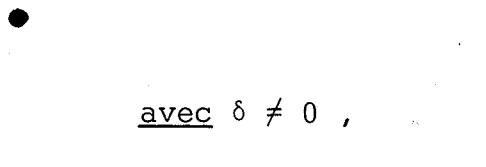


ou

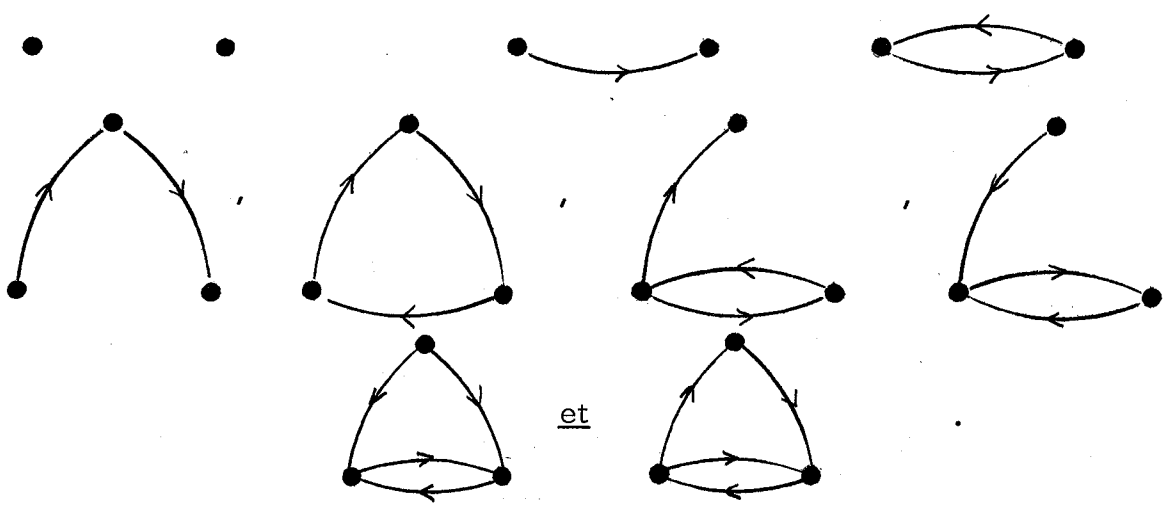


;

(v) $R_1 = 2$ pour les quatre corps dans les autres cas, i.e. pour les graphes suivants :



avec $\delta \neq 0$,



et

Remarque VI.3.- Pour $\ell = 3$ et $t = 3$ on peut donner un exemple des 17 situations possibles, à savoir (dans l'ordre des graphes ci-dessus) :

(i) : (7,181,673) ; (ii) : (13,103,223) , (7,181,463) et (7,181,223) ;

(iii) : (7,163,271) , (7,13,163) ;

(iv) : (7,13,43) , (7,43,97) ;

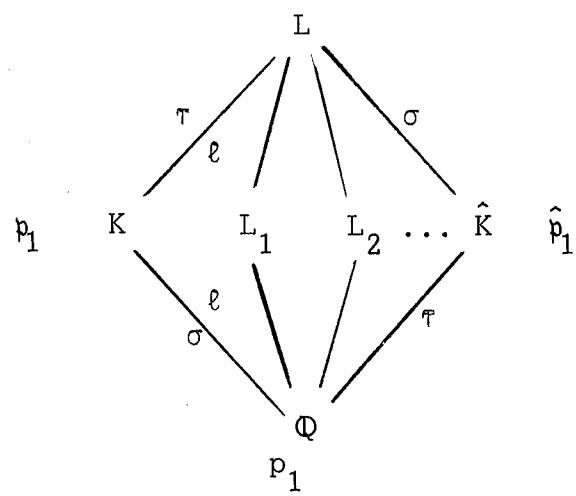
(v) : (7,31,67) , (7,31,37) , (7,37,181) , (7,13,31) , (7,13,73) , (7,73,181) , (7,43,181) , (7,13,223) , (7,19,181) .

4. Etude du cas $t = 2$.

Considérons le cas ℓ impair et $t = 2$. Soient p_1 , p_2 les nombres premiers ramifiés dans les $\ell-1$ extensions K_i cycliques de degré ℓ de $\mathbb{Q}$ de discriminant commun. On suppose qu'il y a des classes exceptionnelles ; donc, d'après les propositions VI.3 et VI.4 on a $|\mathfrak{H}_2| = \ell^2$ pour les $\ell-1$ corps K_i et les symboles $[p_1]_{p_2}$ et $[p_2]_{p_1}$ sont égaux à 1 .

PROPOSITION VI.6.- Soit K l'un des corps K_i . On suppose que pour ce corps $|\mathfrak{H}_3/\mathfrak{H}_2| = \ell$. Alors il en est de même pour les $\ell-2$ autres corps K_i distincts de K .

Démonstration.- Soit $\hat{K}$ l'un des $\ell-2$ corps K_i distincts de K et soit L le composé de K et $\hat{K}$; alors L contient les $\ell-1$ corps K_i ainsi que le corps L_1 (resp. L_2) qui est l'extension cyclique de degré ℓ de $\mathbb{Q}$ dans laquelle p_1 (resp. p_2) est le seul nombre premier ramifié. Soit $\mathfrak{p}_1$ (resp. $\hat{\mathfrak{p}}_1$) l'idéal premier au-dessus de p_1 dans K (resp. $\hat{K}$) . On note enfin par σ (resp. τ) un générateur de $\mathrm{Gal}(L/\hat{K})$ (resp. $\mathrm{Gal}(L/K)$) .



LEMME 1.- (i) Les extensions L/K et $L/\hat{K}$ sont non ramifiées.

(ii) $\mathfrak{p}_1$ (resp. $\hat{\mathfrak{p}}_1$) est décomposé dans L/K (resp. $L/\hat{K}$) .

Le (i) est trivial et le (ii) résulte du fait que $[p_1]_{p_2} = 1$, donc que p_1 est décomposé dans L_2 .

Soit $\alpha \in K$ de norme p_1 , alors $\alpha A_K = p_1 \mathfrak{A}^{\sigma-1}$ et on peut supposer que $\mathfrak{A}$ est un idéal premier de K (remarque IV.7) :

$$\alpha A_K = p_1 q_1^{\sigma-1}$$

D'après les hypothèses faites $q_1 = Nq_1$ est norme d'un élément de K donc les symboles $[q_1]_{p_1}$ et $[q_1]_{p_2}$ sont égaux à 1 (c'est-à-dire que q_1 est totalement décomposé dans $L/\mathbb{Q}$) .

LEMME 2.- Le nombre α est norme dans L/K .

Il suffit de le vérifier localement. Soit $\mathfrak{p}$ un idéal premier dans K . Le cas $\mathfrak{p}$ décomposé dans L/K étant trivial, on peut supposer $\mathfrak{p}$ inerte dans L/K et figurant dans la décomposition de αA_K (sinon α est une unité en $\mathfrak{p}$ donc norme, car L/K est non ramifiée) ; nécessairement $\mathfrak{p} = q_1$ (ou q_1^{σ}) , or ceci est absurde car q_1 est totalement décomposé dans $L/\mathbb{Q}$.

On pose $\alpha = N_{L/K}\varphi$, $\varphi \in L$. Soit $\mathfrak{P}$ un idéal premier au-dessus de p_1 dans L ; on a $N_{L/\mathbb{Q}}\varphi = p_1$ donc $\varphi A_L = \mathfrak{P}\mathfrak{A}_1$ avec $N_{L/\mathbb{Q}}\mathfrak{A}_1 = \mathbb{Z}$; il en résulte facilement que $\mathfrak{A}_1$ est de la forme $\mathfrak{A}_1 = \mathfrak{A}^{\sigma-1}\hat{\mathfrak{A}}^{\tau-1}$ (car $\hat{H}_o(\mathrm{Gal}(L/\mathbb{Q}), \mathcal{J}(L)) = \{1\}$ et $\mathfrak{A}_1 \in \mathcal{J}(L)^I$ où I est l'idéal d'augmentation de $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$ (cf. [22] chap.VIII)), $\mathfrak{A}$ et $\hat{\mathfrak{A}}$ idéaux de L . Soit $\hat{\mathfrak{Q}}$ un idéal premier de L équivalent à $\hat{\mathfrak{A}}$: $\hat{\mathfrak{A}} = \hat{\mathfrak{Q}}(\hat{\gamma})$, $\hat{\gamma} \in L$; on a

$$N_{L/\hat{K}}(\varphi\hat{\gamma}^{1-\tau}A_L) = \hat{p}_1 \ (N_{L/\hat{K}}\hat{\mathfrak{Q}})^{\tau-1}$$

soit $\hat{\alpha}A_{\hat{K}} = \hat{p}_1 \hat{q}^{\hat{f}(\tau-1)}$ où $\hat{q}^{\hat{f}} = N_{L/\hat{K}}\hat{\mathfrak{Q}}$ et où $\hat{\alpha} = N_{L/\hat{K}}(\varphi\hat{\gamma}^{1-\tau})$. La proposition sera démontrée si on montre que $\hat{q}^{f\hat{f}} = N_{\hat{K}/\mathbb{Q}}\hat{q}^{\hat{f}}$ est norme d'un élément de $\hat{K}$:

Si $\hat{q}$ est inerte dans $L/\hat{K}$, $\hat{f} = \ell$ et $\hat{q}^{f\hat{f}} \in N(\hat{K})$. Si $\hat{q}$ est inerte ou ramifié dans $\hat{K}/\mathbb{Q}$ alors $\hat{q}^{\tau-1} = A_{\hat{K}}$. Supposons $\hat{q}$ totalement décomposé dans $L/\mathbb{Q}$. Alors $\hat{q}$ est décomposé dans L_1 et dans L_2 , donc les sym-

boles $[\hat{q}]_{p_1}$ et $[\hat{q}]_{p_2}$ valent 1 et $\hat{q}$ est norme dans $\hat{K}/\Phi$.

COROLLAIRE VI.3.- Lorsque $\ell = 3$ (et $t = 2$) il y a deux corps K_i et l'un admet une classe d'ordre 9 si et seulement si l'autre a la même propriété.

Voir à ce sujet la table 3 en annexe et aussi l'exemple VI.7.

5. La relation de dépendance des classes invariantes ($\ell > 2$).

On sait que les classes invariantes sont représentées par les idéaux premiers ramifiés $\mathfrak{p}_1,\ldots,\mathfrak{p}_t$ dans K/Φ et que, d'après le théorème IV.1, il existe une relation :

$$(1) \qquad \mathfrak{p}_1^{x_1^o}\ldots\mathfrak{p}_t^{x_t^o} = (\alpha)A_K \quad ,$$

x_i^o non tous congrus à 0 modulo ℓ , $(x_1^o,\ldots,x_t^o)$ unique à multiplication près par $\lambda \not\equiv 0$ modulo ℓ .

On a donc $N\alpha = \prod_{i=1}^{t} p_i^{x_i^o}$ et par conséquent le système

(S) : $\prod_{i=1}^{t} (\alpha,\mathfrak{p}_i)_{p_j}^{x_i} = 1$, $1 \le j \le t$ (associé à $\Lambda_1 = \langle p_1,\ldots,p_t\rangle$) , dont le rang est $r_1 \le t-1$, admet la solution $(x_1^o,\ldots,x_t^o)$. En particulier, si $r_1 = t-1$ le système donne la relation de dépendance en question. Si $r_1 < t-1$, le système ci-dessus est insuffisant ; il faut utiliser des méthodes plus directes par exemple comme celle de [11] qui illuste en fait le "théorème 92" de Hilbert ([15]) : partant d'une unité quelconque $\eta \neq \pm 1$ (par exemple l'unité "cyclotomique") on écrit

$$\eta = \psi^{(\sigma-1)^r} \quad , \ r \ge 1 \ ,$$

r étant supposé maximum et ψA_K entier sans facteur rationnel ; on vérifie sans difficulté que

$$\psi A_K = \prod_{i=1}^{t} \mathfrak{p}_i^{x_i^o}$$

est la relation non triviale cherchée (cf. [11] pour la recherche pratique de ψ).

Soit $\mathfrak{f}$ le conducteur du corps ($\mathfrak{f} = p_1 \dots p_{t-1} \ell^2$ ou $p_1 \dots p_t$ selon que ℓ est ramifié ou non) ; on pose $1^* = 2$ (resp. $1^* = 1$) si ℓ est ramifié (resp. non ramifié) . Le cas

$$(x_1^o, \dots, x_t^o) = (1, \dots, 1, 1^*)$$

est particulièrement intéressant à cause du fait suivant (cf. Payan, Sur les classes ambiges et les ordres monogènes d'une extension cyclique de degré premier impair sur $\mathbb{Q}$ ou sur un corps quadratique imaginaire, à paraître à Arkiv för mathematik) :

PROPOSITION VI.7.- Si l'anneau des entiers de K est monogène (i.e. $A_K = \mathbb{Z}[\theta]$, $\theta \in A_K$) il est nécessaire que la relation (1) soit :

$$p_1 \dots p_{t-1} p_t^{1^*} = \alpha A_K \ .$$

Démonstration.- Si $A_K = \mathbb{Z}[\theta]$, le polynôme irréductible de θ a pour discriminant le discriminant du corps soit

$$N_{K/\mathbb{Q}}\left(\prod_{i=1}^{\ell-1} (\theta - \theta^{\sigma^i})\right) = \mathfrak{f}^{\ell-1} \ ;$$

on a alors

$$\prod_{i=1}^{\ell-1} (\theta - \theta^{\sigma^i}) A_K = (p_1 \dots p_{t-1} p_t^{1^*})^{\ell-1} \ ,$$

d'où la proposition.

COROLLAIRE VI.4.- Pour que $A_K = \mathbb{Z}[\theta]$ il est nécessaire que (S) admette la solution $(1, \dots, 1, 1^*)$.

COROLLAIRE VI.5.- Supposons $t = 2$.

(i) si le graphe associé à $\{p_1, p_2\}$ est : ● ● alors l'un au plus des corps associés peut admettre une base d'entiers $\{1, \theta, \dots, \theta^{\ell-1}\}$,

(ii) si le graphe associé est ● ⟶ ● alors aucun des $\ell-1$ corps n'admet une base $\{1, \theta, \dots, \theta^{\ell-1}\}$.

La matrice associée est :

$$A = \begin{pmatrix} -a_{12}v_2 & a_{21}v_1 \\ a_{12}v_2 & -a_{21}v_1 \end{pmatrix} \quad ;$$

dans le cas (i) on a $a_{12} \neq 0$ et $a_{21} \neq 0$; par conséquent $(1,1^*)$ est solution si et seulement si

$$a_{12}v_2 = a_{21}v_1.1^* \quad ,$$

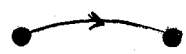
soit $v_2 = \frac{a_{21}}{a_{12}} v_1.1^*$, ce qui se produit pour un corps et un seul.

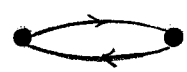
Dans le cas (ii) on a, par exemple, $a_{21} = 0$ et $a_{12} \neq 0$, soit $A = \begin{pmatrix} -a_{12}v_2 & 0 \\ a_{12}v_2 & 0 \end{pmatrix}$ et $(1,1^*)$ ne peut être solution du système homogène associé.

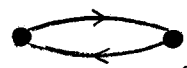
Exemples (ℓ=3) (pour la définition de "a et b" se reporter à la proposition VI.8, partie B).-

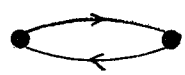
(i) $\{3,7\}$ (graphe : ● ●) ; un corps et un seul admet une base $\{1,\theta,\theta^2\}$ (a=3, b=1 pour ce corps, a=4, b=2 pour l'autre),

(ii) $\{3,13\}$ (graphe : ● ●) ; aucun corps n'admet de base $\{1,\theta,\theta^2\}$,

(iii) $\{3,19)$ (graphe : ) ;

(iv) $\{3,307\}$ (graphe : ) ; les deux corps admettent une base $\{1,\theta,\theta^2\}$: pour le corps défini par a = 35 , b = 1 c'est évident (θ racine de $X^3 - 3.307X - 307.35$) pour le corps défini par a = 19 , b = 17 on prend θ racine du polynôme $X^3 - 7.3.307\,X - 649.307$ (cf. [11]) ,

(v) $\{3,73\}$ (graphe : ) ; l'un des corps est défini par a = 17 , b = 1 (d'où une base $\{1,\theta,\theta^2\}$) et l'autre par a = 10 , b = 8 (il est bien connu que lorsque a et b sont pairs , il n'y a pas de bases $\{1,\theta,\theta^2\}$) ,

(vi) $\{3,271\}$ (graphe : ) ; pour un corps on a a = 28 , b = 10

(donc pas de base $\{1,\theta,\theta^2\}$) et pour l'autre, $a = 1$, $b = 19$; le polynôme $X^3 - 3.271X - 271$ montre que $\mathfrak{p}_{271}$ est principal, donc il n'y a pas de base $\{1,\theta,\theta^2\}$.

Remarquons enfin que pour $t > 2$ une étude systématique conduirait à des énoncés plus compliqués mais du même type que celui du corollaire VI.5.

Lorsque $(1,\ldots,1,1^*)$ est solution, il n'y a pas nécessairement de base d'entiers $\{1,\theta,\ldots,\theta^{\ell-1}\}$; une condition nécessaire et suffisante permettant un test effectif pratique semble ne pas exister vu que dans [11] il est démontré un critère pour $\ell = 3$ portant sur des équations diophantiennes du 3^e degré, à savoir :

"(i) soit $\mathfrak{f}$ un conducteur d'extension cubique cyclique de $\mathbb{Q}$; si $\mathfrak{f}$ est de la forme

$$\mathfrak{f} = \frac{\alpha^2+27}{4\gamma^3} \quad \text{ou} \quad \mathfrak{f} = \frac{27\alpha^2+1}{4\gamma^3} ,$$

α et $\gamma \in \mathbb{Z}$ premiers entre eux, il existe un corps $K(\alpha,\gamma,\mathfrak{f})$ de conducteur $\mathfrak{f}$ admettant une base d'entiers $\{1,\theta,\theta^2\}$.

(ii) Toutes les extensions cubiques cycliques admettant une base d'entiers $\{1,\theta,\theta^2\}$ sont de la forme $K(\alpha,\gamma,\mathfrak{f})$" .

B. Algorithmes et illustrations

1. Algorithme pour $\ell = 2$.

Soit m un entier sans facteurs carrés et soient $p_1,\ldots,p_t$ les nombres premiers ramifiés dans $K = \mathbb{Q}(\sqrt{m})$. La détermination de $\mathcal{H}(K)$ se ramène à la détermination de deux suites croissantes $\mathcal{J}_i$ et Λ_i , $i \geq 1$, vérifiant les hypothèses des théorèmes IV.2 et IV.3.

On peut toujours supposer que $\mathcal{J}_i$ est engendré par des idéaux premiers

de degré 1 pour tout i (cf. remarque IV.7).

Dans la pratique, il suffit de connaître $\Lambda_{i-1} = \langle p_1,\dots,p_t,q_1,\dots,q_n\rangle$ car $\mathcal{J}_{i-1}$ s'en déduit sans ambiguité. Les nombres q_j se déterminent alors de la façon suivante :

LEMME VI.2.- Soit $\Lambda_{i-1} = \langle p_1,\dots,p_t,q_1,\dots,q_n\rangle$. Soit $\{1,\theta\}$ une $\mathbb{Z}$-base de A_K ($\theta = \sqrt{m}$ si $m \equiv 2$ ou $3 \bmod 4$, $\theta = \frac{1+\sqrt{m}}{2}$ sinon).

Pour a parcourant un ensemble de solutions indépendantes du système "$a \in \Lambda_{i-1} \cap NK^*$ ", on résout l'équation :

$$az^2 = N(x+y\theta) \quad , \quad x,y,z \in \mathbb{Z} \quad , \quad (z,x,y) = 1 \ ,$$

avec $z = 1$ ou z premier ; Λ_i est alors obtenu par adjonction à Λ_{i-1} des solutions z qui sont des nombres premiers.

En effet, si $a = N(x+y\theta)$ (en supposant a sans facteurs carrés), $x,y \in \mathbb{Z}$, c'est qu'il existe un idéal $\mathfrak{A} \in \mathcal{J}_{i-1}$ de norme a qui est principal ; l'idéal $\mathfrak{A}'$ correspondant est par exemple A_K . S'il existe p_o premier tel que $ap_o^2 = N(x+y\theta)$, $(p_o,x,y) = 1$ c'est que $(x+y\theta)A_K$ est de la forme $\mathfrak{A}\mathfrak{p}_o^2$ avec $\mathfrak{A} \in \mathcal{J}$ et $N\mathfrak{A} = a\mathbb{Z}$; d'où $(\frac{x+y\theta}{p_o})A_K = \mathfrak{A}\mathfrak{p}_o^{1-\sigma}$ et en posant $\alpha = \frac{x+y\theta}{p_o}$ on obtient la solution $\mathfrak{A}' = \mathfrak{p}_o$, d'où le lemme.

Remarque VI.4.- Il est clair que les groupes $\mathcal{J}_i$ satisfont à la condition $\mathcal{J} \cap \mathcal{J}(K)^{\sigma-1} = \mathcal{J}^{\sigma-1}$. L'hypothèse $\mathcal{J}$ engendré par des idéaux premiers n'étant pas nécessaire pour un exemple traité "à la main" (il faut alors vérifier à chaque pas l'hypothèse $\mathcal{J}(K)^{\sigma-1} \cap \mathcal{J} = \mathcal{J}^{\sigma-1}$, elle est par contre indispensable pour un calcul systématique (sur ordinateur).

Remarque VI.5.- L'algorithme ci-dessus est valable pour ℓ quelconque sans changement (sauf en ce qui concerne l'expression de la norme).

Exemple VI.2.- Soit $K = \mathbb{Q}(\sqrt{-146})$. On aura $\mathcal{J}_1 = \langle \mathfrak{p}_2, \mathfrak{p}_{73}\rangle$ et $\Lambda_1 = \langle 2,73\rangle$ dont la matrice associée est $A_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$; d'où $|H_2/H_1| = 2$.

Comme $\mathfrak{p}_2\mathfrak{p}_{73}$ est principal il suffit de résoudre l'équation

$2z^2 = x^2 + 146y^2$ dont une solution est $x = 4$, $y = 1$ et $z = 9$; on a :

$$\mathcal{J}_2 = \langle \mathfrak{p}_2, \mathfrak{p}_{73}, \mathfrak{p}_3^2, \mathfrak{p}_3^{2\sigma} \rangle \quad \text{et} \quad \Lambda_2 = \langle 2, 73, 3^2 \rangle$$

et évidemment $A_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$; ainsi $|\mathcal{H}_3/\mathcal{H}_2| = 2$.

On écrit $9 = N(3) = N(\mathfrak{p}_3^2)$ qui conduit à $(3) = \mathfrak{p}_3^2 \mathfrak{A}'^{\sigma-1}$ avec $\mathfrak{A}' = \mathfrak{p}_3$, d'où :

$$\mathcal{J}_3 = \langle \mathfrak{p}_2, \mathfrak{p}_{73}, \mathfrak{p}_3, \mathfrak{p}_3^{\sigma} \rangle \quad \text{et} \quad \Lambda_3 = \langle 2, 73, 3 \rangle \ ;$$

$A_3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$, car 3 est un carré modulo 73 , et $|\mathcal{H}_4/\mathcal{H}_3| = 2$. On trouve alors $3.7^2 = 1^2 + 146.1^2$ soit :

$$\mathcal{J}_4 = \langle \mathfrak{p}_2, \mathfrak{p}_{73}, \mathfrak{p}_3, \mathfrak{p}_3^{\sigma}, \mathfrak{p}_7, \mathfrak{p}_7^{\sigma} \rangle \quad \text{et} \quad \Lambda_4 = \langle 2, 73, 3, 7 \rangle \ .$$

Cette fois $\left(\frac{7}{73}\right) = -1$ ainsi A_4 est de rang 1 et $\mathcal{H}_5 = \mathcal{H}_4 = \mathcal{H}(K)$ et $\mathcal{H}(K)$ est cyclique d'ordre 16.

Exemple VI.3.- Soit $K = \mathbb{Q}(\sqrt{226})$. On aura $\mathcal{J}_1 = \langle \mathfrak{p}_2, \mathfrak{p}_{113} \rangle$ et $\Lambda_1 = \langle 2, 113 \rangle$; on vérifie que $A_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$; -1 étant norme et $N(\sqrt{226})$ étant égal à -226 il suffit de résoudre l'équation :

$$2z^2 = x^2 - 226y^2 \ ;$$

on trouve $(z,x,y) = (9,7,1)$ soit :

$$\mathcal{J}_2 = \langle \mathfrak{p}_2, \mathfrak{p}_{113}, \mathfrak{p}_3^2, \mathfrak{p}_3^{2\sigma} \rangle \ , \quad \Lambda_2 = \langle 2, 113, 3^2 \rangle \ ,$$

$A_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, finalement :

$$\mathcal{J}_3 = \langle \mathfrak{p}_2, \mathfrak{p}_{113}, \mathfrak{p}_3, \mathfrak{p}_3^{\sigma} \rangle \quad \text{et} \quad \Lambda_3 = \langle 2, 113, 3 \rangle \ .$$

On vérifie que $\left(\frac{3}{113}\right) = -1$, c'est-à-dire que $\mathcal{H}(K) = \mathcal{H}_3$ est cyclique d'ordre 8 .

Remarque VI.6.- Il existe d'autres algorithmes pour la détermination des 2-classes d'idéaux d'un corps quadratique (sans calcul du nombre de classes du corps) : principalement celui de Shanks ([23]). Celui que nous venons de définir

donne, sans calculs supplémentaires, la structure du 2-groupe des classes (on peut considérer que c'est pratiquement celui de Shanks (qui est issu de la théorie des formes quadratiques) transposé dans le langage des classes d'idéaux).

2. Etude du cas $\ell = 3$.

La remarque VI.2 montre que le 3-rang d'une extension cubique cyclique de $\mathbb{Q}$ est : $R_1 = 2(t-1) - r_1$, où r_1 est le rang du système linéaire attaché au groupe $\Lambda = \langle p_1, \ldots, p_t \rangle$.

Nous donnons en annexe une table des corps cubiques cycliques pour lesquels $R_1 = 2(t-1)$, avec $t = 2, 3,$ et 4 , $p_i < 10\ 000$ pour $1 \leq i \leq t$.

a) Rappelons la construction des extensions cubiques cycliques de $\mathbb{Q}$ de discriminant donné :

Les résultats du chapitre III montrent que si $p_1, \ldots, p_{t^*}$ sont les nombres premiers ramifiés dans $K/\mathbb{Q}$ et distincts de $\ell = 3$, un nombre α vérifiant $q(\alpha) \in \mathfrak{X}^*$ sera de la forme

$$\alpha = \beta D \quad \text{avec} \quad D = p_1 . p_2 \ldots p_{t^*}$$

où β est, dans $\mathbb{Q}' = \mathbb{Q}(j)$, un entier de norme D .

On peut écrire $\beta = \frac{a'+b'\sqrt{-3}}{2}$ (a', b' entiers de même parité) avec $a' \equiv -1 \bmod 3$ (afin d'avoir $\alpha \equiv 1 \bmod \wp_o = (1-j)$) . Si 3 est non ramifié il faut éventuellement multiplier β par j ou j^2 de telle manière que α vérifie :

$$\alpha \equiv 1 \bmod (1-j)^3 \quad \text{(Proposition VI.1)} .$$

Dans ce cas, on a $\beta \equiv 1 \bmod 3$ soit $\beta = \frac{a+3b\sqrt{-3}}{2}$ et $D = \frac{a^2+27b^2}{4}$.

Si 3 est ramifié, on aura au contraire $\beta = \frac{a+b\sqrt{-3}}{2}$ avec $a \equiv -1 \bmod 3$ et $b \not\equiv 0 \bmod 3$ et $D = \frac{a^2+3b^2}{4}$.

Soit alors $\theta = \sqrt[3]{\alpha}$; on a $K' = \mathbb{Q}'(\theta)$ et on vérifie que $\mathrm{Tr}_{K'/K}(\theta)$ est un élément primitif dans l'extension $K/\mathbb{Q}$. Son polynôme irréductible est alors ([9]) :

$$X^3 - 3DX - aD .$$

Résumons la situation dans la proposition suivante :

PROPOSITION VI.8.- Soient $p_1,\dots,p_t$, $p_i \equiv 1 \bmod 3$ si $p_i \neq 3$; les 2^{t-1} extensions cubiques cycliques de $\mathbb{Q}$ admettant les p_i comme nombres premiers ramifiés, sont définies par les polynômes suivants :

$$X^3 - 3DX - aD \quad , \quad D = p_1 \dots p_t = \frac{a^2+27b^2}{4}$$

si 3 est non ramifié dans l'extension (ou encore $X^3-DX-bD$) ;

$$X^3 - 3DX - aD \quad , \quad D = p_1 \dots p_{t*} = \frac{a^2+3b^2}{4} \quad ,$$

b non divisible par 3 , lorsque $p_t = 3$ est ramifié.

Remarque VI.7.- Le cas $\ell = 5$ peut se traiter d'une manière analogue en ce qui concerne la recherche d'un polynôme (cf. [9] p. 182) .

b) Exemples (avec $t = 2$ et $r_1 = 0$) .

Exemple VI.4.- Corps cubiques de discriminant $(7.181)^2$.

(i) Corps défini par le polynôme : $X^3 - 3.7.181X - 71.7.181$. Soit θ une racine de ce polynôme ; le nombre $\alpha = 181 + \theta + 5\theta^\sigma$ est de norme 181.17^3 et son polynôme irréductible est :

$$X^3 - 3.181X^2 + 181.6.17X - 181.17^3 \quad ;$$

il en résulte $\alpha A_K = \mathfrak{p}_{181}\mathfrak{p}_{17}\mathfrak{p}_{17}^{2\sigma}$ ($\mathfrak{p}_{181}^3 = 181\mathbb{Z}$, $N\mathfrak{p}_{17} = 17\mathbb{Z}$) et $\left(\frac{\alpha}{17}\right) A_K = \mathfrak{p}_{181}\mathfrak{p}_{17}^{\sigma(1-\sigma)}$. Par conséquent, le groupe $\mathcal{J}_2$ contiendra $\mathfrak{p}_{181}$, $\mathfrak{p}_7$ et $\mathfrak{p}_{17}$ et Λ_2 contiendra 181, 7 et 17 ; or 17 n'est pas reste cubique modulo 7 et ceci suffit pour pouvoir affirmer que $r_2 = 1$ et donc que $|\mathcal{H}_3/\mathcal{H}_2| = 1$ ($\mathcal{H}(K)$ est donc isomorphe à $(\mathbb{Z}/3\mathbb{Z})^2$) .

(ii) Corps défini par le polynôme $X^3 - 3.7.181X - 64.7.181$. On trouve un entier α dont le polynôme irréductible est : $X^3-49X^2-308.7X+7.(24)^3$; on vérifie que $\alpha A_K = \mathfrak{p}_7\mathfrak{p}_2^2\mathfrak{p}_2^{7\sigma}\mathfrak{p}_3^3$ et par un raisonnement analogue au précédent on montre que $r_2 = 1$.

Exemple VI.5.- Corps cubiques de discriminant $(7.673)^2$.

(i) Corps défini par le polynôme $X^3 - 3\,7.673X - 113.7.673$. Si θ est une racine de ce polynôme, les nombres $\alpha_1 \quad \frac{13.7+\theta}{3}$ et $\alpha_2 = \frac{673+5\theta+5\theta'}{3}$ sont des entiers dont les polynômes irréductibles sont respectivement :

$$X^3 - 13.7X^2 + 170.7X - 7 \quad \text{et} \quad X^3 - 673X^2 + 66.673X - 3^3.673 .$$

On a $\alpha_1 A_K = \mathfrak{p}_7$ et $\alpha_2 A_K = \mathfrak{p}_{673}\mathfrak{p}_3^3$ et les idéaux $\alpha_1 A_K$ et $\left(\frac{\alpha_2}{3}\right)A_K$ sont de la forme :

$$\alpha_1 A_K = \mathfrak{p}_7 A_K^{\sigma-1} \quad , \quad \frac{\alpha_2}{3} A_K = \mathfrak{p}_{673}(\mathfrak{p}_3^{2+\sigma})^{1-\sigma}$$

On peut donc écrire $\mathcal{J}_2 = \langle \mathfrak{p}_7, \mathfrak{p}_{673}, \mathfrak{p}_3^{2+\sigma}, \mathfrak{p}_3^{\sigma(2+\sigma)}, \mathfrak{p}_3^{\sigma^2(2+\sigma)} \rangle$ et $\Lambda_2 = \langle 7, 673, 3^3 \rangle$; le rang r_2 est alors nul et $|\mathcal{H}_3/\mathcal{H}_2| = 3$.

Ecrivons maintenant que 3^3 est norme : $3^3\mathbb{Z} = N(3) = N(\mathfrak{p}_3^{2+\sigma})$ soit $3A_K = \mathfrak{p}_3^{2+\sigma}\mathfrak{p}_3^{(\sigma+1)(\sigma-1)}$; d'où

$$\mathcal{J}_3 = \langle \mathfrak{p}_7, \mathfrak{p}_{673}, \mathfrak{p}_3^{\sigma+2}, \ldots, \mathfrak{p}_3^{\sigma+1}, \ldots \rangle = \langle \mathfrak{p}_7, \mathfrak{p}_{673}, \mathfrak{p}_3, \mathfrak{p}_3^{\sigma}, \mathfrak{p}_3^{\sigma^2} \rangle$$

et $\Lambda_3 = \langle 7, 673, 3 \rangle$; 3 n'étant pas reste cubique modulo 7 il en résulte $r_3 = 1$ et $|\mathcal{H}_4/\mathcal{H}_3| = 1$. On obtient que $|\mathcal{H}(K)| = 27$ et que $\mathcal{H}(K)$ est isomorphe à $(\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ (cf. corollaire IV.3).

Utilisons l'assertion (ii) de la proposition VI.4 ; le nombre premier 3 est décomposé dans $K/\mathbb{Q}$ et le symbole $[3]_7$ est différent de 1 : $\mathcal{H}(K)$ est engendré par $h = Cl(\mathfrak{p}_3)$ et on a la relation :

$$h^3 = Cl(\mathfrak{p}_{673})^2 \quad , \quad \text{avec} \quad Cl(\mathfrak{p}_{673}) \neq 1$$

puisque $\mathfrak{p}_7$ est principal.

(ii) Corps défini par le polynôme $X^3 - 3.7.673X - 76.7.673$. Considérons les nombres :

$$\alpha_1 = 12.7 + 8\theta + 3\theta' \quad \text{et} \quad \alpha_2 = \frac{673+6\theta+2\theta'}{3}$$

dont les polynômes irréductibles sont :

et
$$X^3 - 36.7X^2 - 3.7^2.4567X + 7.(73.4)^3$$
$$X^3 - 673X^2 - 673.3.53X + 673 \quad ;$$

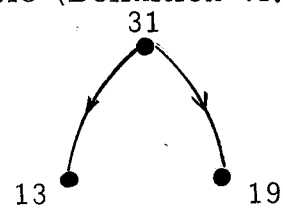
ce qui donne :

$$(\alpha_1)A_K = \mathfrak{p}_7\mathfrak{p}_{73}^3\mathfrak{p}_2^6 \quad \text{et} \quad (\alpha_2)A_K = \mathfrak{p}_{673} \quad .$$

On a $\left(\frac{\alpha_1}{4.73}\right)A_K = \mathfrak{p}_7\mathfrak{p}_{73}^{(1-\sigma)(2+\sigma)}\mathfrak{p}_2^{2(1-\sigma)(2+\sigma)}$ et $(\alpha_2)A_K = \mathfrak{p}_{673}A_K^{1-\sigma}$, d'où :

$\mathcal{J}_2 = \langle \mathfrak{p}_7, \mathfrak{p}_{673}, (\mathfrak{p}_2^2\mathfrak{p}_{73})^{2+\sigma}, \ldots \rangle$ et $\Lambda_2 = \langle 7, 673, 292^3 \rangle$; r_2 est nul et $|\mathcal{H}_3/\mathcal{H}_2| = 3$; alors $\mathcal{J}_3 = \langle \mathfrak{p}_7, \mathfrak{p}_{673}, \mathfrak{p}_2^2\mathfrak{p}_{73}, \ldots \rangle$ et $\Lambda_3 = \langle 7, 673, 292 \rangle$; on vérifie que 292 n'est pas reste cubique modulo 7 , donc $r_3 = 1$ et $|\mathcal{H}(K)| = 27$ comme dans le cas (i) (la structure étant la même).

Exemple VI.6.- Considérons les 4 corps cubiques de discriminant $(13.19.31)^2$; le graphe associé (Définition VI.3) est le suivant :



donc d'après la proposition VI.5, pour 3 des corps on aura $R_1 = 2$ (c'est-à-dire que $|\mathcal{H}(K)| = |\mathcal{H}_1| = 9$) et pour le dernier on aura $R_1 = 3$. On vérifie facilement que c'est pour le corps K défini par $a = 170$, $b = 8$ ($\frac{a^2+27b^2}{4} = 13.19.31$, cf. Proposition VI.8) donc par le polynôme $X^3 - 13.19.31X - 8.13.19.31$; le triplet (v_1, v_2, v_3) associé étant ici $(1,1,1)$ relativement au choix des idéaux premiers au-dessus de 13, 19 et 31 :

$$\mathfrak{P}_{13} = (3-j^2) \quad , \quad \mathfrak{P}_{19} = (3-2j^2) \quad \text{et} \quad \mathfrak{P}_{31} = (5-j^2)$$

(cf. Définition VI.1) et pour $\alpha = \frac{-170+24\sqrt{-3}}{2} = -73 + 24j = j(3-j^2)(3-2j^2)(5-j^2)$, on trouve immédiatement :

$$(\alpha,13)_{13} = j \quad , \quad (\alpha,13)_{19} = j \quad , \quad (\alpha,13)_{31} = j \quad ,$$
$$(\alpha,19)_{13} = j^2 \quad , \quad (\alpha,19)_{19} = j^2 \quad , \quad (\alpha,19)_{31} = j^2 \quad ,$$
$$(\alpha,31)_{13} = 1 \quad , \quad (\alpha,31)_{19} = 1 \quad , \quad (\alpha,31)_{31} = 1 \quad ,$$
$$(\alpha,2)_{13} = j \quad , \quad (\alpha,2)_{19} = j^2 \quad , \quad (\alpha,2)_{31} = 1 \quad ;$$

La matrice associée au groupe $\Lambda_1 = \langle 13,19,31\rangle$ est donc

$$\begin{pmatrix} 1 & 2 & 0 \\ 1 & 2 & 0 \\ 1 & 2 & 0 \end{pmatrix}$$

de rang 1 , comme prévu ; on doit donc chercher α_1 et α_2 de K tels que $N\alpha_1 = 31$ et $N\alpha_2 = 13.19$; on montre que le polynôme irréductible de $\varphi = \frac{1439-16\theta-18\theta'}{3}$ où θ est une racine de $X^3-3DX-170D$ $(D = 13.19.31)$, est : $X^3 - 1439X^2 - 55041X - 1$ et qu'un entier α tel que $\alpha^{\sigma-1} = \varphi$ (théorème 90 de Hilbert : $\alpha = 1+\varphi+\varphi\varphi'$) est de norme $13^2.19^2.31$ on a donc la relation $\mathfrak{p}_{31}\mathfrak{p}_{13}^2\mathfrak{p}_{19}^2 \sim 1$ et il suffit de considérer la solution $N\theta = 8.13.19.31$ obtenue à partir du polynôme $X^3 - DX - 8D$ (proposition VI.8) qui conduit à $\frac{\theta}{2} A_K = \mathfrak{p}_{13}\mathfrak{p}_{19}\mathfrak{p}_{31}\mathfrak{p}_2^{(1-\sigma)(2+\sigma)}$ et $N\mathfrak{p}_2^{2+\sigma} = 8$, d'où le groupe $\Lambda_2 = \langle 13,19,31,8\rangle$ qui montre que

$$|\mathcyr{H}_3/\mathcyr{H}_2| = 3 .$$

Au stade suivant on aura évidemment $\Lambda_3 = \langle 13,19,31,2\rangle$, la matrice associée étant :

$$\begin{pmatrix} 1 & 2 & 0 & 1 \\ 1 & 2 & 0 & 2 \\ 1 & 2 & 0 & 0 \end{pmatrix} ;$$

son rang est 2 , d'où $|\mathcyr{H}_4/\mathcyr{H}_3| = 1$. La proposition IV.2 entraîne que $\mathcyr{H}(K) \simeq (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})^2$.

Remarque VI.8.- L'exemple ci-dessus montre que l'on ne peut pas obtenir pour $t \geq 3$ un énoncé simple donnant la structure de $\mathcyr{H}(K)$ (contrairement au cas $t = 2$, cf.corollaire IV.3) ; toutes les situations "intermédiaires" semblent être possibles.

Nous allons terminer par un exemple qui montre que la proposition VI.6 n'est pas généralisable en ce qui concerne la comparaison des groupes $\mathcyr{H}_i$, $i > 3$, des corps ayant même discriminant (et avec $t = 2$) :

Exemple VI.7.- On considère les deux corps cubiques de discriminant $(37.991)^2 = (36\ 667)^2$. On vérifie facilement qu'il y a des classes exception-

nelles $(R_1 = 2)$.

Soit K le corps défini par $a = 295$, $b = 47$ et soit $\hat{K}$ le corps défini par $a = 376$, $b = 14$.

(i) Etude de K .

Si θ est une racine de $X^3 - 3DX - aD$, $D = 37.991$, on vérifie que :

$$\alpha_1 = \frac{1}{3}(37.8 + 6\theta + \theta^\sigma)$$

et

$$\alpha_2 = \frac{1}{3}(991.7 + 17\theta + 15\theta^\sigma)$$

ont respectivement pour polynômes irréductibles :

$$X^3 - 37.8X^2 - 37.13.727X - 37.5^6$$

et

$$X^3 - 991.7X^2 + 991.2^6.7.29X - 991(5.29)^3 .$$

Il en résulte que $\alpha_1 A_K = \mathfrak{p}_{37}\mathfrak{p}_5^6$ et $\alpha_2 A_K = \mathfrak{p}_5^3\mathfrak{p}_{29}^{2+\sigma}$; le groupe $\mathcal{J}_2$ sera donc égal à :

$$\mathcal{J}_2 = \langle \mathfrak{p}_{37}, \mathfrak{p}_{991}, \mathfrak{p}_5^{2(2+\sigma)}, \mathfrak{p}_5^{2+\sigma}\mathfrak{p}_{29}^{1+\sigma}, \ldots \rangle = \langle \mathfrak{p}_{37}, \mathfrak{p}_{991}, \mathfrak{p}_5^{2+\sigma}, \mathfrak{p}_{29}, \ldots \rangle$$

soit $\Lambda_2 = \langle 37, 991, 5^3, 29 \rangle$; 29 étant reste cubique modulo 37 et 991 il en résulte que $|\mathcal{H}_3/\mathcal{H}_2| = 3$.

Au stade suivant $\mathcal{J}_3$ contiendra $\mathfrak{p}_5$ et 5 n'étant pas reste cubique modulo 37 on aura $\mathcal{H}_4 = \mathcal{H}_3$ d'où

$$\mathcal{H}(K) \simeq \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} .$$

(ii) Etude de $\hat{K}$.

On vérifie que l'entier ψ , de polynôme irréductible $X^3+DX^2+13DX-D$, est un entier de $\hat{K}$; il en résulte que $\mathfrak{p}_{37}\mathfrak{p}_{991}$ est principal, ce qui permet d'écrire :

$$\Lambda_1 = \langle \mathfrak{p}_{991} \rangle .$$

Soient θ et ϑ des racines des polynômes

$$X^3 - 3DX - aD \qquad (a = 376)$$

et

$$X^3 - DX - bD \qquad (b = 14) ,$$

on sait que l'on peut écrire :

$$\theta = \vartheta - \vartheta^{\sigma}$$

à condition de définir la conjugaison σ par l'expression

$$\vartheta^{\sigma} = -\frac{3}{a}\vartheta^2 + \frac{9b-a}{2a}\vartheta + \frac{2D}{a} \quad .$$

On considère enfin l'entier φ défini par :

$$\varphi = \frac{1}{3}(11.991 + 42\theta + \theta^{\sigma^2})$$

dont le polynôme irréductible est :

$$X^3 - 11.991X^2 + 2^5.3^2.5.13.991X - 991(2^2.7^2)^3 \quad ;$$

si on définit $\mathfrak{p}_2$ et $\mathfrak{p}_7$ par la relation

$$\vartheta A_K = \mathfrak{p}_2\mathfrak{p}_7 \ ,$$

on vérifie sans difficulté que :

$$\varphi A_K = \mathfrak{p}_{991}\mathfrak{p}_2^{3(\sigma+\sigma^2)}\mathfrak{p}_7^6 \ ,$$

et par conséquent, il existe un nombre φ' tel que

$$\varphi' A_K = \mathfrak{p}_{991}\mathfrak{p}_2^{3(\sigma+\sigma^2)-6} \quad \text{(on prend } \varphi' = \frac{\varphi}{\vartheta^6}\text{)} \quad .$$

On aura successivement :

$$\mathcal{J}_1 = \langle \mathfrak{p}_{991} \rangle \ , \qquad \Lambda_1 = \langle 991 \rangle \ ,$$

$$\mathcal{J}_2 = \langle \mathfrak{p}_{991}, \mathfrak{p}_2^{3(2+\sigma)}, \ldots \rangle \ , \qquad \Lambda_2 = \langle 991, 2^9 \rangle$$

$$\mathcal{J}_3 = \langle \mathfrak{p}_{991}, \mathfrak{p}_2^{3(2+\sigma)}, \mathfrak{p}_2^{3(1+\sigma)} \rangle = \langle \mathfrak{p}_{991}, \mathfrak{p}_2^3, \ldots \rangle \ , \ \Lambda_3 = \langle 991, 2^3 \rangle$$

$$\mathcal{J}_4 = \langle \mathfrak{p}_{991}, \mathfrak{p}_2^{2+\sigma}, \mathfrak{p}_2^3, \ldots \rangle \quad \text{qui est équivalent à}$$

$$\langle \mathfrak{p}_{991}, \mathfrak{p}_2^{2+\sigma}, \mathfrak{p}_7^3, \ldots \rangle \ , \qquad \Lambda_4 = \langle 991, 2^3, 7^3 \rangle \ ,$$

ceci afin de satisfaire à la condition :

$$\mathcal{J} \cap \mathcal{J}(\hat{K})^{\sigma-1} = \mathcal{J}^{\sigma-1} \ ;$$

$$\mathcal{J}_5 = \langle \mathfrak{p}_{991}, \mathfrak{p}_2^{2+\sigma}, \mathfrak{p}_7^3, \mathfrak{p}_2^{1+\sigma}, \mathfrak{p}_7^{2+\sigma}, \ldots \rangle \quad \text{équivalent à}$$

$$\langle \mathfrak{p}_{991}, \mathfrak{p}_2, \ldots \rangle \quad \text{soit} \qquad \Lambda_5 = \langle 991, 2 \rangle \ .$$

Or 2 n'est pas reste cubique modulo 37 donc $|\mathcal{H}_6/\mathcal{H}_5| = 1$ ce qui fait que la structure de $\mathcal{H}(\hat{K})$ est donnée par :

$$\mathcal{H}(\hat{K}) \simeq \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \ .$$

oo0oo

TABLES NUMERIQUES

1. Table 1.

Table des corps cubiques définis par p_1 et $p_2 < 1000$ et pour lesquels $|\mathcal{H}_3| = 9$ (le 3-rang est donc maximum (= 2) et ceci a lieu pour les deux corps de même discriminant).

2. Tables 2.

Tables analogues à la table 1 pour $\ell = 5$ et $\ell = 7$.

3. Table 3.

Exemples de couples (p_1, p_2) figurant dans la table 1 précédente pour lesquels l'un des corps cubiques possède une classe d'ordre 9 (donc les deux d'après la proposition VI.6).

Nous définissons les corps par l'intermédiaire de a et b tels que $D = \frac{a^2+27b^2}{4} = p_1.p_2$. Pour p_1 , puis de la même manière pour p_2 , nous donnons les coefficients d'un polynôme irréductible d'un entier φ_i tel que $|N\varphi_i| = p_i n^3$, $|Tr(\varphi_i \varphi_i^{\sigma})| = p_i s$ et $|Tr\ \varphi_i| = p_i t$. Les idéaux $\mathfrak{A}_i$ sont définis par l'égalité

$$(\varphi_i)A_K = p_i \mathfrak{A}_i^{1-\sigma} ;$$

la conclusion sur la structure de $\mathcal{H}(K)$ s'en déduit dans presque tous les cas (la présence d'une * indique que $\mathcal{H}(K)$ contient au moins un sous-groupe de la forme indiquée).

4. Table 4.

Exemples de corps cubiques tels que $\mathcal{H}(K) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (pour $t = 2$).

5. Table 5.

Table des corps cubiques définis par p_1 , p_2 et $p_3 < 1000$ et pour lesquels le 3-rang du groupe des classes est maximum (i.e. $R_1 = 4$). Ceci a alors lieu pour les 4 corps de même discriminant.

TABLE 1

3, 73	619	283	619	643	829	883	643	829
271	829	337	631	733	283,313	379,409	823	859
307	883	349	661	199,211	349	463	853	919
523	37,103	409	769	313	499	541	997	643,859
577	421	433	151,211	397	619	601	523,547	883
613	433	631	283	661	691	691	661	661,727
757	487	673	331	733	307,313	733	673	853
919	739	757	367	859	421	877	709	877
991	991	769	409	211,307	499	937	739	673,757
7,181	43,193	823	433	367	523	397,523	757	769
223	409	859	547	223,277	739	613	541,739	787
337	457	877	607	283	919	631	757	997
421	613	97,313	691	439	313,349	907	853	691,757
463	643	337	727	661	463	919	547,619	823
673	61,163	433	877	787	577	409,523	571,607	859
769	241	463	157,337	859	607	571	661	907
811	277	601	373	919	331,409	421,499	709	937
853	313	997	379	229,283	547	691	757	709,727
883	487	103,409	439	457	727	829	787	751
13,103	613	439	487	241,271	877	433,571	859	727,823
229	877	823	601	379	937	631	577,619	919
421	907	919	727	457	337,499	739	757	733,859
499	67,193	991	787	751	811	751	811	991
619	283	109,199	877	787	349,661	787	991	739,967
853	349	373	883	829	709	439,727	601,811	751,811
859	643	709	991	859	877	733	823	967
19,151	661	997	163,313	877	967	457,673	607,643	757,907
277	937	127,349	349	271,487	367,439	829	823	991
373	997	421	379	571	733	877	937	811,919
487	73,103	619	757	661	739	977	613,643	823,919
577	241	643	823	769	937	463,547	811	877,967
691	313	673	181,331	823	373,457	643	829	997
733	439	757	397	919	577	733	907	907,919
31,163	709	139,199	673	967	613	487,499	619,643	919,991
271	883	277	823	277,397	769	499,523	751	967,991
349	79, 97	373	859	541	787	577	631,661	997
373	157	601	193,409	757				

TABLES 2

$\ell = 5$

5,251	991	941	751	631
601	41,191	191,941	941	601,761
11,241	571	211,251	271,571	641,661
661	61,761	811	991	701,911
31,191	131,331	241,701	331,751	821,881
211	571	251,331	401,421	941,991

$\ell = 7$

127,449	197,211	883	449,827	673,757
743	337,673	379,827	617,953	757,911

TABLE 3

$p_1 \cdot p_2$	a	b	n	s	t	$\mathfrak{A}_1$	n	s	t	$\mathfrak{A}_2$	$\mathfrak{H}(K)$
7.673	113	15	1	2.5.17	13	(1)	3^3	2.83	1	$p_3^{2+\sigma}$	(9,3)
	76	22	$2^6.73^3$	3.7.4567	$2^2.3^2$	$(p_2^2 p_{73})^{2+\sigma}$	1	3.53	1	(1)	(9,3)
7.769	92	22	2^6	677	$2^2.5$	$p_2^{2(2+\sigma)}$	$2^6.31^3$	$2^2.3^2.31$	3	$p_2^2 p_{31}$	(9,3)
	43	27	3^3	2.11.19	17	$p_3^{2+\sigma}$	1	2	1	(1)	(9,3)
37.991	376	14	$2^6.13^3$	$2^2.13.3^4$	23	$p_2^2 p_{13}$	$2^6.7^6$	$2^5.3^2.5.13$	11	$p_2^{2+\sigma} p_7^{2(2+\sigma)}$	(27,9)
	295	47	5^6	13.727	2^3	$p_5^{2(2+\sigma)}$	$5^3.29^3$	$2^6.7.29$	7	$p_5^{2+\sigma} p_{29}$	(9.3)
67.643	343	45	$3^3.5^3.29^3$	$2^4.3.2029$	5	$p_3(p_5 p_{29})^{2+\sigma}$	173^3	$3^2.19.137$	$2^2.3$	$p_{173}^{2+\sigma}$	(9,3)
	143	75	19^3	$2^3.43.3^2$	3.5	$p_{19}^{2+\sigma}$	$5^3.13^3$	$2^6.3^3$	3	$(p_5 p_{13})^{2+\sigma}$	(9,3)
73.241	262	8	2^3	17	2	$p_2^{2+\sigma}$	1	17	1	(1)	(9,3)
	143	43	17^3	$7^2.17$	2.7	p_{17}	17^3	$7^2.17$	7	p_{17}	(9,3)*
79.157	173	27	3^6	$3^4.29$	11	$p_3^{2+\sigma}$	83^3	$3^2.653$	$2^2.3$	$p_{83}^{2+\sigma}$	(9,3)
	65	41	11^3	1201	2^2	$p_{11}^{2+\sigma}$	5^6	3.5^4	2^2	$p_5^{2+\sigma}$	(9,3)
79.349	328	10	$2^9.5^6$	$2^3.3541$	3.11	$p_2^3 p_5^{2(2+\sigma)}$	$2^{12}.19^3$	$2^3.3.5.17.31$	3^3	$p_2^{5+\sigma} p_{19}^{2+\sigma}$	(9,3)
	301	27	$7^3.23^3$	2.3.7.23.71	$3^2.11$	$p_7 p_{23}$	$7^3.23^3$	12659	17	$p_7^{2+\sigma} p_{23}^{2+\sigma}$	(9,3)*
79.409	331	27	223^3	23.223	31	p_{223}	89^3	$2^2.5.401$	11	$p_{89}^{2+\sigma}$	(9,3)*
	196	58	2^{12}	$2^3.37$	5	$p_2^{5+\sigma}$	2^{18}	$2^3.5.17$	1	$p_2^{9+3\sigma}$	(9,3)
79.631	433	21	7^6	$2^2.5^2.229$	1	$p_7^{2(2+\sigma)}$	23^3	$2.7^2.13$	7	$p_{23}^{2+\sigma}$	(9,3)
	298	64	$2^9.59^3$	2.59.661	3.5	$p_2^{5+2\sigma} p_{59}$	$2^6.19^3$	$2^4.5^2.37$	3^2	$p_2^{2+\sigma} p_{19}^{2+\sigma}$	(9,3)*
79.757	368	62	$2^6.23^3$	$2^2.23.11.37$	5	$p_2^2 p_{23}$	11^6	8069	1	$p_{11}^{2(2+\sigma)}$	(9,3)
	125	91	61^3	$2^2.3.5^2.11$	3^3	$p_{61}^{2+\sigma}$	$5^6.13^3$	$3.5^4.19$	$2^2.3$	$p_5^{2+\sigma} p_{13}^{2+\sigma}$	(9,3)*
97.337	142	64	1	3.139	1	(1)	2^6	$2^4.5$	1	$p_2^{2+\sigma}$	(9,3)
	47	69	3^3	2.23	3	$p_3^{2+\sigma}$	$3^3.29^3$	$2^2.3.29$	7	$p_3 p_{29}$	(9,3)
103.409	404	14	13^3	499	7	$p_{13}^{2+\sigma}$	$7^3.31^3$	11.31.67	3.5	$p_{31} \cdot p_7^{2+\sigma}$	(9,3)*
	1	79	13^3	$2^3.7.13$	7	p_{13}	13^3	$2^3.13$	1	p_{13}	(9,3)*
139.277	353	33	107^3	$3^2.7.173$	$2^3.3$	$p_{107}^{2+\sigma}$	89^3	2.3.11.19.53	$3^2.5$	$p_{89}^{2+\sigma}$	(9,3)
	245	59	5^3	2.4987	17	$p_5^{2+\sigma}$	7^6	3.733	2^3	$p_7^{2(2+\sigma)}$	(9,3)
139.373	244	74	$2^6.23^3$	$2^5.19.23$	19	$p_2^{2+\sigma} p_{23}$	$2^6.23^3$	$2^5.13.23$	13	$p_2^{2+\sigma} p_{23}$	(9,3)*
	55	87	$3^3.5^6$	$5^3.7$	2^2	$p_3^{2+\sigma} p_5^{2+\sigma}$	5^6	61	1	$p_5^{2(2+\sigma)}$	(9,3)
151.433	343	73	$7^3.23^3$	13.4157	3.13	$p_7^{2+\sigma} p_{23}^{2+\sigma}$	$7^3.67^3$	$2^2.5.67.73$	3^3	$p_7^{2+\sigma} p_{67}$	(9,3)*
	305	79	67^3	$11^2.23$	5	$p_{67}^{2+\sigma}$	5^3	661	1	$p_5^{2+\sigma}$	(9,3)

TABLE 4

3, 73	13,103	619	487	79,433	757
271	229	829	613	673	139,199
307	421	883	877	769	601
523	499	37,103	907	823	619
577	619	421	67,193	859	631
613	853	433	283	877	661
757	19,151	487	349	97,313	769
919	277	739	661	433	151,211
991	373	43,193	937	463	283
7,181	487	409	997	103,439	331
223	19,577	457	73,103	919	367
337	691	613	313	991	409
421	733	643	439	109,199	547
463	31,163	61,163	709	373	607
811	271	241	883	997	691
853	349	277	79, 97	127,349	727
883	373	313	283	421	877
			337	643	

TABLE 5

3	271	919	61	163	313	139	373	769	283	313	349
3	307	523	61	241	877	139	631	661	307	421	499
3	307	919	67	193	643	151	211	367	307	499	523
3	523	757	67	283	349	151	283	691	307	523	739
3	577	757	73	103	439	151	331	409	349	661	877
3	577	991	79	97	337	151	331	547	349	877	967
3	757	991	79	97	433	151	331	727	367	439	733
3	919	991	79	157	337	151	331	877	379	463	733
7	181	673	79	157	877	157	373	787	379	691	937
7	337	811	79	283	349	157	373	883	397	613	907
7	673	769	79	349	877	157	379	601	397	631	919
13	421	499	79	433	631	157	379	877	397	907	919
13	499	853	79	631	859	157	439	727	433	571	787
19	151	691	79	673	757	163	313	349	457	673	997
19	373	577	79	673	769	199	733	859	457	877	997
31	163	349	97	313	463	241	379	877	523	673	757
31	373	883	103	823	919	241	457	829	577	757	991
37	103	991	103	919	991	241	457	877	691	757	907
37	433	739	127	619	643	271	571	661	727	823	919
43	193	409	127	673	757	271	823	919	877	967	997
43	613	643	139	199	661	277	541	757			

BIBLIOGRAPHIE

[1] - E. ARTIN - Algebraic Numbers and algebraic Functions, Lectures notes by I. Adamson, Gordon and Breach, New York, 1967.

[2] - E. ARTIN and J. TATE - Class Field Theory, Benjamin, New York, 1967.

[3] - H. BAUER - Die 2-Klassenzahlen spezieller quadratischer Zahlkörper, J.f.d.r.u.a.Math., 252 (1972).

[4] - H. BAUER - Über die kubischen Klassenkörper zyklischer kubischer Zahlkörper, Dissertation, Karlsruhe Universität (1970).

[5] - Z. BOREVICH and I. SHAFAREVICH - Number Theory, Academic Press, New York, 1966.

[6] - L. BOUVIER - Table des 2-rang, 4-rang et 8-rang du 2-groupe des classes d'idéaux au sens restreint de $\mathbb{Q}(\sqrt{m})$..., L'Ens. Math. II^{e} série, t. XVIII, 1, 1972, 37-45.

[7] - C. CHEVALLEY - Sur la théorie du corps de classes dans les corps finis et les corps locaux, Jour. of the Fac. of Sc., Tokyo, Vol.II, Part 9 (1933).

[8] - P. DAMEY et J.J. PAYAN - Existence et construction des extensions galoisiennes et non abéliennes de degré 8 d'un corps de caractéristique différente de 2, J.f.d.r.u.a. Math., B. 244 (1970).

[9] - G. GRAS - Extensions abéliennes non ramifiées de degré premier d'un corps quadratique, Bull. Soc. Math. France, 100 (1972).

[10] - G. GRAS - Sur le ℓ-groupe des classes des extensions cycliques de degré premier ℓ, Note C.R.A.S., t. 274 (1972), 1145-1148.

[11] - M.N. GRAS - Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbb{Q}$; bases d'entiers (à paraître).

[12] - H. HASSE - Über die Klassenzahl des Körpers $P(\sqrt{-p})$ mit einer Primzahl $p \equiv 1 \bmod 2^3$, Aequationes math. 3 (1969).

[13] - H. HASSE - Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$, J. of Number theory., 1 (1969), 231-234.

[14] - H. HASSE - Über die Teilbarkeit durch 2^3 der Klassenzahl imaginär-quadratischer Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, j.f.d.r.u.a.Math., 241 (1970).

[15] - D. HILBERT - Théorie des corps de nombres algébriques, trad. T. Got et A. Levy, Hermann, 1913.

[16] - K. IWASAWA - A note on the group of units of an algebraic Number Field, J. Math. Pures et App., 35 (1956), 189-192.

[17] - H. KISILEVSKY - Some results related to Hilbert's Theorem 94, J. of Number theory, 2 (1970), 199-206.

[18] - S.N. KURODA - On the Class Number of Imaginary quadratic Number Fields, Proceedings of Japan Academy, 8, 1965.

[19] - S. LANG - Algebraic Number Theory, Addison- Wesley Pub. comp., New York 1970.

[20] - H.W. LEOPOLDT - Zur Geschlechtertheorie in abelschen Zahlkörpern, Math. Nachr., 9 (1953), 351-362.

[21] - L. REDEI und H. REICHARDT - Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, J.f.d.r.u.a. Math., 170 (1933).

[22] - J.P. SERRE - Corps locaux, Act. Sc. et ind., Paris 1962.

[23] - D. SHANKS - Gauss's Ternary form reduction and the 2-Sylow subgroup, Math. of computation, 25(1971), 837-853.

[24] - O. TAUSSKY - A remark concerning Hilbert's Theorem 94, J.f.d.r.u.a. Math., 239/240 (1970), 435-438.

VU,

Grenoble, le

Le président de la thèse,

C. CHABAUTY

VU, et permis d'imprimer

Grenoble, le

Le président de l'Université
scientifique et médicale,

LISTE DES PROFESSEURS

Président : Monsieur Michel SOUTIF
Vice-Président : Monsieur Gabriel CAU

PROFESSEURS TITULAIRES

MM.	ANGLES D'AURIAC Paul	Mécanique des fluides
	ARNAUD Georges	Clinique des maladies infectieuses
	ARNAUD Paul	Chimie
	AUBERT Guy	Physique
	AYANT Yves	Physique approfondie
Mme	BARBIER Marie-Jeanne	Electrochimie
MM.	BARBIER Jean-Claude	Physique expérimentale
	BARBIER Reynold	Géologie appliquée
	BARJON Robert	Physique nucléaire
	BARNOUD Fernand	Biosynthèse de la cellulose
	BARRA Jean-René	Statistiques
	BARRIE Joseph	Clinique chirurgicale
	BENOIT Jean	Radioélectricité
	BERNARD Alain	Mathématiques Pures
	BESSON Jean	Electrochimie
	BEZES Henri	Chirurgie générale
	BLAMBERT Maurice	Mathématiques Pures
	BOLLIET Louis	Informatique (IUT B)
	BONNET Georges	Electrotechnique
	BONNET Jean-Louis	Clinique ophtalmologique
	BONNET-EYMARD Joseph	Pathologie médicale
	BONNIER Etienne	Electrochimie Electrométallurgie
	BOUCHERLE André	Chimie et Toxicologie
	BOUCHEZ Robert	Physique nucléaire
	BOUSSARD Jean-Claude	Mathématiques Appliquées
	BRAVARD Yves	Géographie
	BRISSONNEAU Pierre	Physique du Solide
	BUYLE-BODIN Maurice	Electronique
	CABANAC Jean	Pathologie chirurgicale
	CABANEL Guy	Clinique rhumatologique et hydrologie
	CALAS François	Anatomie
	CARRAZ Gilbert	Biologie animale et pharmacodynamie
	CAU Gabriel	Médecine légale et Toxicologie
	CAUQUIS Georges	Chimie organique
	CHABAUTY Claude	Mathématiques Pures
	CHARACHON Robert	Oto-Rhino-Laryngologie
	CHATEAU Robert	Thérapeutique
	CHENE Marcel	Chimie papetière
	COEUR André	Pharmacie chimique
	CONTAMIN Robert	Clinique gynécologique
	COUDERC Pierre	Anatomie Pathologique
	CRAYA Antoine	Mécanique
Mme	DEBELMAS Anne-Marie	Matière médicale
MM.	DEBELMAS Jacques	Géologie générale
	DEGRANGE Charles	Zoologie
	DESRE Pierre	Métallurgie
	DESSAUX Georges	Physiologie animale
	DODU Jacques	Mécanique appliquée
	DOLIQUE Jean-Michel	Physique des plasmas
	DREYFUS Bernard	Thermodynamique
	DUCROS Pierre	Cristallographie
	DUGOIS Pierre	Clinique de Dermatologie et Syphiligraphie
	FAU René	Clinique neuro-psychiatrique
	FELICI Noël	Electrostatique
	GAGNAIRE Didier	Chimie physique
	GALLISSOT François	Mathématiques Pures
	GALVANI Octave	Mathématiques Pures
	GASTINEL Noël	Analyse numérique
	GEINDRE Michel	Electroradiologie
	GERBER Robert	Mathématiques Pures
	GIRAUD Pierre	Géologie
	KLEIN Joseph	Mathématiques Pures
Mme	KOFLER Lucie	Botanique et Physiologie végétale
MM.	KOSZUL Jean-Louis	Mathématiques Pures
	KRAVTCHENKO Julien	Mécanique
	KUNTZMANN Jean	Mathématiques Appliquées
	LACAZE Albert	Thermodynamique
	LACHARME Jean	Biologie végétale
	LAJZEROWICZ Joseph	Physique
	LATREILLE René	Chirurgie générale
	LATURAZE Jean	Biochimie pharmaceutique
	LAURENT Pierre	Mathématiques Appliquées
	LEDRU Jean	Clinique médicale B
	LLIBOUTRY Louis	Géophysique
	LOUP Jean	Géographie
Mlle	LUTZ Elisabeth	Mathématiques Pures
	MALGRANGE Bernard	Mathématiques Pures
	MALINAS Yves	Clinique obstétricale
	MARTIN-NOEL Pierre	Somélogie médicale
	MASSEPORT Jean	Géographie
	MAZARE Yves	Clinique médicale A
	MICHEL Robert	Minéralogie et Pétrographie
	MOURIQUAND Claude	Histologie
	MOUSSA André	Chimie nucléaire
	NEEL Louis	Physique du Solide
	OZENDA Paul	Botanique
	PAUTHENET René	Electrotechnique
	PAYAN Jean-Jacques	Mathématiques Pures
	PEBAY-PEYROULA Jean-Claude	Physique
	PERRET René	Servomécanismes
	PILLET Emile	Physique industrielle
	RASSAT André	Chimie systématique
	RENARD Michel	Thermodynamique
	REULOS René	Physique industrielle
	RINALDI Renaud	Physique
	ROGET Jean	Clinique de pédiatrie et de puériculture
	SANTON Lucien	Mécanique
	SEIGNEURIN Raymond	Microbiologie et Hygiène
	SENGEL Philippe	Zoologie
	SILBERT Robert	Mécanique des fluides
	SOUTIF Michel	Physique générale
	TANCHE Maurice	Physiologie
	TRAYNARD Philippe	Chimie générale
	VAILLAND François	Zoologie
	VALENTIN Jacques	Physique Nucléaire
	VAUQUOIS Bernard	Calcul électronique
Mme	VERAIN Alice	Pharmacie galénique
M.	VERAIN André	Physique
Mme	VEYRET Germaine	Géographie
MM.	VEYRET Paul	Géographie
	VIGNAIS Pierre	Biochimie médicale
	YOCCOZ Jean	Physique nucléaire théorique

PROFESSEURS ASSOCIES

MM.	BULLEMER Bernhard	Physique

PROFESSEURS SANS CHAIRE

MM.	BEAUDOING André	Pédiatrie
Mme	BERTRANDIAS Françoise	Mathématiques Pures
MM.	BERTRANDIAS Jean-Paul	Mathématiques appliquées
	BIAREZ Jean-Pierre	Mécanique
	BONNETAIN Lucien	Chimie minérale
Mme	BONNIER Jane	Chimie générale
MM.	CARLIER Georges	Biologie végétale
	COHEN Joseph	Electrotechnique
	COUMES André	Radioélectricité
	DEPASSEL Roger	Mécanique des Fluides
	DEPORTES Charles	Chimie minérale
	GAUTHIER Yves	Sciences biologiques
	GAVEND Michel	Pharmacologie
	GERMAIN Jean Pierre	Mécanique
	GIDON Paul	Géologie et Minéralogie
	GLENAT René	Chimie organique
	HACQUES Gérard	Calcul numérique
	JANIN Bernard	Géographie
Mme	KAHANE Josette	Physique
MM.	MULLER Jean-Michel	Thérapeutique
	PERRIAUX Jean-Jacques	Géologie et minéralogie
	POULOUJADOFF Michel	Electrotechnique
	REBECQ Jacques	Biologie (CUS)
	REVOL Michel	Urologie
	REYMOND Jean-Charles	Chirurgie générale
	ROBERT André	Chimie papetière
	DE ROUGEMONT Jacques	Neurochirurgie
	SARRAZIN Roger	Anatomie et chirurgie
	SARROT-REYNAULD Jean	Géologie
	SIBILLE Robert	Construction Mécanique
	SIROT Louis	Chirurgie générale
Mme	SOUTIF Jeanne	Physique générale

MAITRES DE CONFERENCES ET MAITRES DE CONFERENCES AGREGES

Mlle	AGNIUS-DELORD Claudine	Physique pharmaceutique
	ALARY Josette	Chimie analytique
MM.	AMBLARD Pierre	Dermatologie
	AMBROISE-THOMAS Pierre	Parasitologie
	ARMAND Yves	Chimie
	BEGUIN Claude	Chimie organique
	BELORIZKY Elie	Physique
	BENZAKEN Claude	Mathématiques Appliquées
	BILLET Jean	Géographie
	BLIMAN Samuel	Electronique (EIE)
	BLOCH Daniel	Electrotechnique
Mme	BOUCHE Liane	Mathématiques (CUS)
MM.	BOUCHET Yves	Anatomie
	BOUVARD Maurice	Mécanique des Fluides
	BRODEAU François	Mathématiques (IUT B)
	BRUGEL Lucien	Energétique
	BUISSON Roger	Physique
	BUTEL Jean	Orthopédie
	CHAMBAZ Edmond	Biochimie médicale
	CHAMPETIER Jean	Anatomie et organogénèse
	CHIAVERINA Jean	Biologie appliquée (EFP)
	CHIBON Pierre	Biologie animale
	COHEN-ADDAD Jean-Pierre	Spectrométrie physique
	COLOMB Maurice	Biochimie médicale
	CONTE René	Physique
	COULOMB Max	Radiologie
	CROUZET Guy	Radiologie
	DURAND Francis	Métallurgie
	DUSSAUD René	Mathématiques (CUS)
Mme	ETERRADOSSI Jacqueline	Physiologie
MM.	FAURE Jacques	Médecine légale
	GENSAC Pierre	Botanique
	GIDON Maurice	Géologie
	GRIFFITHS Michaël	Mathématiques Appliquées
	GROULADE Joseph	Biochimie médicale
	HOLLARD Daniel	Hématologie
	HUGONOT Robert	Hygiène et Médecine préventive
	IDELMAN Simon	Physiologie animale
	IVANES Marcel	Electricité
	JALBERT Pierre	Histologie
	JOLY Jean-René	Mathématiques Pures
	JOUBERT Jean-Claude	Physique du Solide
	JULLIEN Pierre	Mathématiques Pures
	KAHANE André	Physique générale
	KUHN Gérard	Physique
	LACOUME Jean-Louis	Physique
Mme	LAJZEROWICZ Jeannine	Physique
MM.	LANCIA Roland	Physique atomique
	LE JUNTER Noël	Electronique
	LEROY Philippe	Mathématiques
	LOISEAUX Jean-Marie	Physique Nucléaire
	LONGEQUEUE Jean-Pierre	Physique Nucléaire
	LUU DUC Cuong	Chimie Organique
	MACHE Régis	Physiologie végétale
	MAGNIN Robert	Hygiène et Médecine préventive
	MARECHAL Jean	Mécanique
	MARTIN-BOUYER Michel	Chimie (CUS)
	MAYNARD Roger	Physique du Solide
	MICHOULIER Jean	Physique (I.U.T. "A")
	MICOUD Max	Maladies infectieuses
	MOREAU René	Hydraulique (INP)
	NEGRE Robert	Mécanique
	PARAMELLE Bernard	Pneumologie
	PECCOUD François	Analyse (IUT B)
	PEFFEN René	Métallurgie
	PELMONT Jean	Physiologie animale
	PERRET Jean	Neurologie
	PERRIN Louis	Pathologie expérimentale
	PFISTER Jean-Claude	Physique du Solide
	PHELIP Xavier	Rhumatologie
Mlle	PIERY Yvette	Biologie animale
MM.	RACHAIL Michel	Médecine Interne
	RACINET Claude	Gynécologie et obstétrique
	RENAUD Maurice	Chimie
	RICHARD Lucien	Botanique
Mme	RINAUDO Marguerite	Chimie macromoléculaire
MM.	ROMIER Guy	Mathématiques (IUT B)
	SHOM Jean Claude	Chimie Générale
	STIEGLITZ Paul	Anesthésiologie
	STOEBNER Pierre	Anatomie pathologique
	VAN CUTSEM Bernard	Mathématiques Appliquées
	VEILLON Gérard	Mathématiques Appliquées (INP)
	VIALON Pierre	Géologie
	VOOG Robert	Médecine Interne
	VROUSSOS Constantin	Radiologie
	ZADWORNY François	Electronique

MAITRES DE CONFERENCES ASSOCIES

MM.	BOUDOURIS Georges	Radioélectricité
	CHEEKE John	Thermodynamique
	YACOUB Mahmoud	Médecine légale

CHARGES DE FONCTIONS DE MAITRES DE CONFERENCES

Mme	BERIEL Hélène	Physiologie
Mme	RENAUDET Jacqueline	Microbiologie

Fait le 30 Mai 1972