ANNALES DE L'INSTITUT FOURIER

GEORGES GRAS

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

Annales de l'institut Fourier, tome 23, n° 3 (1973), p. 1-48

<http://www.numdam.org/item?id=AIF_1973__23_3_1_0>

Ann. Inst. Fourier, Grenoble
23,3 (1973), 1-48

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

par Georges GRAS

TABLE DES MATIERES

Pages

Fascicule 4, tome 23 :

Pages

Introduction.

Soit K/k une extension de corps de nombres à groupe de Galois cyclique d'ordre premier l. La théorie des genres conduit à la formule de Chevalley dite des "l-classes ambiges" (i.e. invariantes par le groupe de Galois). Cette formule ne fournit qu'un diviseur du nombre de classes d'idéaux du corps K et il est naturel de se demander s'il existe des l-classes non invariantes par $\mathrm{Gal}(K/k)$. On peut se convaincre facilement que de telles classes existent :

Le cas $l = 2$, $k = \mathbf{Q}$, est bien connu, et la structure du 2-groupe des classes de K peut se déterminer grâce aux méthodes de Rédei et Reichardt, Hasse, Bauer et Shanks ([30], [3], [32]) ;

Le cas $l = 3$, $k = \mathbf{Q}$, a été étudié par Bauer qui a donné une formule pour le 3-rang du groupe des classes ([4]).

Il faut noter qu'aucun de ces auteurs ne se réfère aux travaux de Inaba ([18]) injustement tombés dans l'oubli et que nous avons découvert par hasard une fois le présent travail achevé (seuls Fröhlich et Kobayashi, à notre connaissance, les citent sans pour autant insister sur le contenu). En fait, Inaba est sans doute le premier à avoir étudié le problème dans toute sa généralité et fourni un exemple numérique de classe non invariante dans le cas cubique.

Le cas cyclique de degré l^n sur $\mathbf{Q}$ a été étudié par Fröhlich grâce à d'autres méthodes que celles employées ici (principalement [9]). Les résultats sont tout à fait explicites et sont à rapprocher de ceux du chapitre VI (A – § 2 et 3).

Dans ce travail nous avons considéré d'emblée le cas des extensions cycliques relatives de degré premier l ; les résultats obtenus généralisent et simplifient ceux déjà cités. Ils permettent, d'une part, une détermination effective du l-groupe des classes d'une extension K/k donnée et, d'autre part, de retrouver des résultats connus (obtenus souvent par d'autres méthodes) et d'étudier des problèmes nouveaux.

Plan de travail.

Les chapitres I et II contiennent les résultats classiques (que nous avons empruntés, pour la plupart, à [31]) 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 [5]), et se termine par l'énoncé de propriétés des symboles locaux, particulières au cadre dans lequel nous nous plaçons.

Dans le chapitre IV, nous établissons la "formule de Chevalley" pour le cas restreint. 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 l'action de la norme dans K/k. Ces propriétés sont liées de façon naturelle au "théorème des normes de Hasse" que nous traduisons en terme de symboles locaux (symbole de Hilbert).

Des calculs du même type de ceux que l'on doit faire pour démontrer la "formule des classes ambiges" 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 (à paraître dans le Fascicule 4, Tome 23) sont destinés à une exploitation des résultats précédents, le chapitre VI étant plus spécialement réservé au cas $k = \mathbf{Q}$ et à des exemples numériques. Par exemple, lorsque le discriminant d'une extension cyclique K/Q de degré l est divisible par t nombres premiers distincts il y a $(l-1)^{t-1}$ 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.

Je tiens à remercier ici, le Professeur Claude Chabauty, Président du Jury, Jacques Martinet, qui a dirigé mes recherches, Jean-Jacques Payan, pour les encouragements qu'il m'a prodigués et le Professeur Jean-Louis Koszul qui a bien voulu me proposer un sujet de seconde thèse.

CHAPITRE I

GENERALITES SUR LES EXTENSIONS DE CORPS DE NOMBRES (1)

A. Corps de nombres.

1. *Généralités.*

Soit K un corps de nombres (i.e. une extension finie du corps des rationnels Q). Il existe r_1 Q-isomorphismes réels de K dans C et $2r_2$ Q-isomorphismes complexes, conjugués deux par deux. Le degré $[K : Q]$ 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 Q-isomorphismes réels de K dans C et soit sgn la fonction signe sur 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 s'il 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 est noté K^{*+}.

Soit A_K l'anneau des entiers de K (i.e. la clôture intégrale de 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 Z-rang de E_K est égal à $r_1 + r_2 - 1$.

Le groupe des idéaux fractionnaires de A_K est noté $\mathfrak{J}(K)$ et le sous-groupe des idéaux principaux (au sens habituel) est noté $\mathfrak{J}_0'(K)$. Le sous-groupe de $\mathfrak{J}_0'(K)$ formé des idéaux engendrés par un nombre totalement positif est le groupe des idéaux principaux au *sens restreint* et est noté $\mathfrak{J}_0(K)$. 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

$$\mathfrak{Cl}'(K) = \mathfrak{J}(K)/\mathfrak{J}_0'(K) \text{ (resp. } \mathfrak{Cl}(K) = \mathfrak{J}(K)/\mathfrak{J}_0(K)).$$

(1) Les Chapitres V et VI paraîtront dans le fascicule 4 du même tome.

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 1.1. – Les deux notions d'idéal principal 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 $r_1 + r_2$ Q-isomorphismes de K dans C non conjugués deux à deux. 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 premier fini ou non et nous réserverons le mot idéal pour désigner un idéal premier au sens habituel.*

3. *Complétions d'un corps de nombres.*

Soit $\mathfrak{P}$ une place de K ; on désigne par $K_{\mathfrak{P}}$ le 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 $\mathbf{Q}_p$ ($p\mathbf{Z} = \mathfrak{P} \cap \mathbf{Z}$). Si $\mathfrak{P}$ est un idéal premier à l'infini $K_{\mathfrak{P}}$ est égal à **R** ou à **C**. 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 de $K_{\mathfrak{P}}$, $\overline{\mathfrak{P}}$ 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, k^{*+}, A_k, E_k, $\mathcal{J}(k)$, $\mathcal{J}'_0(k)$, $\mathcal{J}_0(k)$, $\mathcal{H}'(k)$ et $\mathcal{H}(k)$.

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

Ayant défini S_k et S_K, il faut remarquer que l'on a l'inclusion $\operatorname{Ker} S_k \subset \operatorname{Ker} S_K$ mais qu'il n'y a pas égalité en général. Citons une propriété des homomorphismes S_k et S_K qui nous sera utile par la suite :

PROPOSITION 1.1. — *Soit* K/k *cyclique 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) alors $l = 2$ et $\operatorname{Gal}(K_i/k_i)$ 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 :

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

σ désignant un générateur de $\operatorname{Gal}(K/k)$.

Posons $S_K(u) = (\ldots ; \varepsilon_i^{(1)}, \ldots, \varepsilon_i^{(l)}; \ldots)$, $i = 1, \ldots, \rho_1$, et $S_K(v) = (\ldots ; \eta_i^{(1)}, \ldots, \eta_i^{(l)}; \ldots)$; $S_K(v^{\sigma-1}) =$

$$= (\ldots ; \eta_i^{(1)}\eta_i^{(2)}, \ldots, \eta_i^{(l)}\eta_i^{(1)}; \ldots),$$

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 l équations : $\eta_i^{(k)}\eta_i^{(k+1)} = \varepsilon_i^{(k)}$ (l'indice k étant défini modulo l) ; le rang de ce système est égal à $l - 1$ et il admet une solution dès que la relation $\prod_{k=1}^{l} \varepsilon_i^{(k)} = 1$, 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.

Nous supposons désormais K/k galoisienne.

DEFINITIONS 1.1. — *Soit $K_{\mathfrak{P}}$ le 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 $\mathfrak{p}$ de k qui ne dépend que de $\mathfrak{P}$. On dit que $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$.*

Soit $\mathfrak{p}$ une place de k ; nous dirons que $\mathfrak{p}$ est ramifiée dans K/k si $\mathfrak{p}$ est un idéal premier ramifié au sens habituel ou si $\mathfrak{p}$ est un idéal à l'infini associé à un corps k_i réel pour lequel K_i est imaginaire.

2. *Groupes de ramification* ([1] et [31]).

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 $i \geqslant -1$, on désigne par H_i le sous-groupe de H_{-1} formé des éléments σ tels que $v_{\mathfrak{P}}(x^{\sigma} - x) \geqslant i + 1$ pour tout $x \in A_{K_{\mathfrak{P}}}$ On rappelle que dans le cas totalement ramifié, π désignant une uniformisante quelconque dans $K_{\mathfrak{P}}$, $\pi^{\sigma-1} \in 1 + \mathfrak{P}^i$, $i \geqslant 0$, 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 $l^{\text{èmes}}$ 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 $\mathbf{F}_l$-espaces vectoriels de dimension 1 de L^*/L^{*l} : soit $\alpha \in L^*$ dont l'image dans L^*/L^{*l} engendre un tel sous-espace ; alors il lui correspond l'extension $E = L(\sqrt[l]{\alpha})$.

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

PROPOSITION 1.2. – *Soit* $E = L(\sqrt[l]{\alpha})$, $\alpha \in L^*$, *une extension de Kummer de degré premier l et soit* $\mathfrak{P}$ *un idéal premier de* L :

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

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

iii) *si* $v_{\mathfrak{P}}(\alpha) \equiv 0 \mod l$ *et si* $\mathfrak{P}$ *divise* lA_L, *alors* $\mathfrak{P}$ *est non ramifié dans* E/L *si et seulement si la congruence* $\alpha \equiv \xi^l \mod \mathfrak{P}^\lambda$ *est soluble dans* L (α *étant choisi premier à* $\mathfrak{P}$) *avec* $\lambda = lv_{\mathfrak{P}}(1-\zeta)$. *Dans le cas contraire, on a* $t_{\mathfrak{P}} = lv_{\mathfrak{P}}(1-\zeta) - \lambda_{\mathfrak{P}}$, *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 1.2. – *On note* :

P_0 *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

$$R = P_0 \cup P_1 \cup P_2 \cup P_\infty.$$

CHAPITRE II

LOIS DE RECIPROCITE

A. Cas local.

1. *Rappels* (*d'après* [31])

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 $\overline{x}$ est son image dans $E^*/N_{F/E}F^*$, on pose

$$(x, F/E) = \omega(\overline{x})$$

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 2.1. – L'isomorphisme de réciprocité pour les corps **R** et **C** est le suivant :

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

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) :

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

qui ne dépend pas du choix de θ.

Lorsque L est égal à **R** ou à **C** on définit encore le symbole de Hilbert par la même formule.

PROPOSITION 2.1. — *Le symbole de Hilbert a les propriétés suivantes :*

i) $(aa', b)_{\mathfrak{P}} = (a, b)_{\mathfrak{P}} (a', b)_{\mathfrak{P}}$,

ii) $(a, bb')_{\mathfrak{P}} = (a, b)_{\mathfrak{P}} (a, b')_{\mathfrak{P}}$,

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

iv) $(a, b)_{\mathfrak{P}} (b, a)_{\mathfrak{P}} = 1$.

B. Cas global.

1. *Rappels* ([2] et [31]).

Cette fois L désigne un corps de nombres. On considère, dans le produit $\prod_{\mathfrak{P}} L_{\mathfrak{P}}^*$, où $\mathfrak{P}$ parcourt l'ensemble des places de L, le sous-ensemble des familles $\{x_{\mathfrak{P}}\}_{\mathfrak{P}}$, $x_{\mathfrak{P}} \in L_{\mathfrak{P}}^*$, pour lesquelles $x_{\mathfrak{P}}$ est une unité pour presque tout $\mathfrak{P}$: 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 $\mathfrak{P}'$ une place quelconque au-dessus de $\mathfrak{P}$ dans E. On note $H_{\mathfrak{P}}$ le groupe de décomposition de $\mathfrak{P}$ dans E/L.

Les isomorphismes de réciprocité :

$$f_{\mathfrak{P}} : L_{\mathfrak{P}}^*/NE_{\mathfrak{P}'}^* \to H_{\mathfrak{P}} \subset H,$$

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

$$f : I_L \to H,$$

définie par $f(x) = \prod_{\mathfrak{P}} f_{\mathfrak{P}}(\overline{x}_{\mathfrak{P}})$; 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 $(a, b)_{\mathfrak{q}}$ a un sens dans tout complété puisque l'on a convenu d'identifier L a un sous-corps de $L_{\mathfrak{q}}$. 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 $\prod_{\mathfrak{q}} f_{\mathfrak{q}}(\overline{b}) = 1$ ce qui conduit immédiatement à la formule dite du produit :

$$\prod_{\mathfrak{q}} (a, b)_{\mathfrak{q}} = 1.$$

C. Calculs explicites des symboles. (dans le cas du degré premier l).

1. *Notations.*

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

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

2. *Résultats explicites (d'après [31], proposition 8, p. 217, proposition 5, p. 236).*

PROPOSITION 2.2. — *Si la caractéristique p est différente de l, $\overline{L}_{\mathfrak{q}}^*$ contient le groupe des racines $l^{\text{èmes}}$ de l'unité et on a*

$$q_{\mathfrak{q}}((a, b)_{\mathfrak{q}}) = q_{\mathfrak{q}}(c)^{\frac{\overline{q}-1}{l}}$$

avec

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

PROPOSITION 2.3. — *On suppose $p = l$ et E/L totalement ramifiée en $\mathfrak{R}$. Soit π une uniformisante de $L_{\mathfrak{q}}(\theta)$ et soit $M = \pi^{\sigma-1} - 1$.*

Lorsque b *est congru à* 1 modulo $\mathfrak{P}^{t\mathfrak{P}}$, *le nombre* $c = \dfrac{b-1}{\mathrm{Tr}(\mathrm{M})}$ *est entier dans* $\mathrm{L}_{\mathfrak{P}}$ *et vérifie* $c \equiv -\dfrac{b-1}{\mathrm{N}(\mathrm{M})} \equiv -\dfrac{b-1}{\mathrm{M}^l}$ modulo π.

On a alors : $(a, b)_{\mathfrak{P}} = \zeta_\sigma^{\mathrm{S}_{\mathfrak{P}}(q_{\mathfrak{P}}(c))}$.

PROPOSITION 2.4. — *On suppose* $p = l$. *Soit* $a \in \mathrm{L}^*$; *si* $b \in \mathrm{L}^*$ *est congru à* 1 modulo $\mathfrak{P}^{l\nu_{\mathfrak{P}}(1-\zeta_\sigma)}$, *le nombre* $c = \dfrac{b-1}{l(\zeta_\sigma - 1)}$ *est entier dans* $\mathrm{L}_{\mathfrak{P}}$ *et on a* :

$$(a, b)_{\mathfrak{P}} = \zeta_\sigma^{\nu_{\mathfrak{P}}(a)\mathrm{S}_{\mathfrak{P}}(q_{\mathfrak{P}}(c))}.$$

PROPOSITION 2.5. — *Soit* $\mathfrak{P}$ *une place à l'infini. Si* $\mathrm{L}_{\mathfrak{P}} = \mathbf{C}$ *alors* $(a, b)_{\mathfrak{P}} = 1$; *si* $\mathrm{L}_{\mathfrak{P}} = \mathbf{R}$, *nécessairement* $l = 2$ *et dans ce cas* $(a, b)_{\mathfrak{P}} = -1$ *si et seulement si* a *et* b *sont négatifs dans* $\mathrm{L}_{\mathfrak{P}}$.

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 $l^{\text{èmes}}$ 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 $\mathbf{Z}_l[G]$-modules.

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

Les éléments $e_\chi = d^{-1} \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma$ constituent un système complet d'idempotents orthogonaux de $\mathbf{Z}_l[G]$; 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 $\mathbf{Z}_l[G]$-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 $\mathbf{Z}_l[G]$-module.

PROPOSITION 3.1. — *Soit* $\chi \in G^*$ *et soit* M *un* $\mathbf{Z}_l[G]$*-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* $e \in \mathbf{Z}_l[G]$ *vérifie* $e(s - \chi(s)) = 0$ *pour tout* $s \in G$, *alors* $e = \lambda e_\chi$, $\lambda \in \mathbf{Z}_l$,

iii) *quels que soient* $n \geqslant 1$, $\chi \in G^*$ *et* $s \in G$, *il existe* $a \in \mathbf{Z}$ *et* $e \in \mathbf{Z}[G]$ *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 $x^s = \prod_{\chi'} x^{se_{\chi'}} = \prod_{\chi'} x^{\chi'(s)e_{\chi'}} = \prod_{\chi'} x^{\chi(s)e_{\chi'}}$ 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 $e = \sum_s a_s s$, $a_s \in \mathbf{Z}_l$, on aura $ee_\chi = \sum_s a_s s e_\chi = \left(\sum_s a_s \chi(s)\right) e_\chi$ qui est de la forme λe_χ , $\lambda \in \mathbf{Z}_l$.

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

DEFINITION 3.1. — *Lorsque* G *opère sur le groupe des racines* $l^{\text{èmes}}$ *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* $l^{\text{ème}}$ ζ *de l'unité. L'application qui associe à s l'unique élément* $\theta(a)$ *de* U *qui est congru à a modulo l, est un caractère injectif de* G *à valeurs dans* $\mathbf{Z}_l$: *on le note* χ^* *et on note* e^* *l'idempotent* e_{χ^*}.

La relation $\zeta^s = \zeta^{\chi^*(s)}$ pour tout $s \in G$ entraîne alors $\zeta^{e^*} = \zeta$ (on applique la proposition 3.1 au groupe des racines $l^{\text{èmes}}$ 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 $l^{\text{ème}}$ de l'unité,

k' et K' les composés $k\mathbf{Q}(\zeta)$ et $\mathrm{KQ}(\zeta)$. On pose $G = \mathrm{Gal}(K'/K)$ et $H = \mathrm{Gal}(K'/k')$; les groupes $\mathrm{Gal}(k'/k)$ et $\mathrm{Gal}(K/k)$ sont respectivement isomorphes à G et H par restriction. Enfin G est un groupe cyclique dont l'ordre d divise $l - 1$.

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-$\mathbf{F}_l$-espace de dimension 1 de k'^*/k'^{*l}. Soit q l'homomorphisme canonique $q : k'^* \to k'^*/k'^{*l}$; posons $\mathfrak{X} = k'^*/k'^{*l}$, $\mathfrak{X}$ peut être considéré comme un $\mathbf{Z}_l[G]$-module. On vient donc de définir une application canonique de l'ensemble des extensions abéliennes de degré l de k dans l'espace projectif $\mathbf{P}(\mathfrak{X})$.

Soit $\mathfrak{X}^* = \mathfrak{X}^{e^*} = \{q(\alpha) \in \mathfrak{X},\ q(\alpha)^s = q(\alpha)^{\chi(s)}$ pour tout $s \in G\}$; $\mathfrak{X}^*$ est un sous-$\mathbf{F}_l$-espace vectoriel de $\mathfrak{X}$ et on peut considérer $\mathbf{P}(\mathfrak{X}^*)$ comme un sous-espace de $\mathbf{P}(\mathfrak{X})$; on a alors le résultat suivant :

THEOREME 3.1. — *L'application qui associe à* K/k *un point de* $\mathbf{P}(\mathfrak{X})$ *est une bijection de l'ensemble des extensions abéliennes de degré* l *de* k *sur* $\mathbf{P}(\mathfrak{X}^*)$.

Démonstration. — Soit K une extension abélienne de degré l de k et soit $\alpha \in k'$ tel que $K' = k'(\sqrt[l]{\alpha})$; 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 $q(\alpha)^h$, $h \in \mathbf{Z}$ convenable, car K'/k est galoisienne ; on a donc $\theta^{\varphi - h} \in k'$, où θ est une racine du polynôme $X^l - \alpha$. Soit $\sigma \in H$, $\sigma \neq 1$; comme φ et σ commutent (K'/k est abélienne) on obtient :

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

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

Montrons maintenant que si $q(\gamma)$ représente un élément de $\mathbf{P}(\mathfrak{X}^*)$ alors l'extension $K' = k'(\sqrt[l]{\gamma})$ est de la forme Kk' avec K abélienne de degré l de k. Il est équivalent de démontrer que $k'(\sqrt[l]{\gamma})$ est abélienne sur k. La condition $q(\gamma)^s = q(\gamma)^{\chi^*(s)}$, 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_0 un générateur de G ; d'après la proposition 3.1, il existe $a_0 \in \mathbf{Z}$ et $e_0 \in \mathbf{Z}[G]$ tels que $a_0 \equiv \chi^*(s_0)$ modulo l et $e_0(s_0 - a_0) \equiv 0$ modulo l^n.

On sait que $q(\gamma) = q(\gamma)^{e^*} = q(\gamma)^{e_0}$ donc $\gamma = \gamma^{e_0} u^l$, $u \in k'$. Posons $\alpha = \gamma u^{-l}$ et soit θ une racine du polynôme $X^l - \alpha$ ($K' = k'(\theta)$). On aura ainsi $\alpha^{s_0 - a_0} = \gamma^{e_0(s_0 - a_0)} = \mu^{l^n}$, $\mu \in k'$, ce qui conduit immédiatement à l'existence de a et b entiers tels que $\alpha^{s-a} = u^{l^n}$ et $\alpha^{t-b} = v^{l^n}$, $u, v \in k'$. Comme toute racine $l^{\text{ème}}$ de l'unité est puissance l^{n-1}-ème dans k' par définition de n, on peut écrire $\theta^{\varphi - a} = u^{l^{n-1}}$ et $\theta^{\psi - b} = v^{l^{n-1}}$, ce qui conduit aux relations

$$\theta^{\varphi\psi} = \theta^{ab} v^{al^{n-1}} u^{tl^{n-1}} \quad \text{et} \quad \theta^{\psi\varphi} = \theta^{ab} u^{bl^{n-1}} v^{sl^{n-1}} ;$$

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

$$\zeta = \zeta^{e_0} = (v^{(a-s)e_0} u^{(t-b)e_0})^{l^{n-1}} ;$$

or $(a - s)\, e_0 \equiv (t - b)\, e_0 \equiv 0$ 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* $\mathbf{P}(\mathfrak{X}^*)$.

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 $K' = k'(\sqrt[l]{\alpha})$ (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 $\bar{a}$ les élements du quotient $\bar{\mathcal{J}}(k') = \mathcal{J}(k')/\mathcal{J}(k')^l$, qui est un $\mathbf{Z}_l[G]$-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 pour lesquels le groupe de décomposition dans k'/k est réduit à l'élément neutre.

PROPOSITION 3.2. – *L'idéal* $\alpha A_{k'}$ *vérifie la relation :*

$$\overline{\alpha A_{k'}} = \prod_{\mathfrak{P} \in \mathfrak{D}} \overline{\mathfrak{P}}^{e^* x_{\mathfrak{P}}}, \quad x_{\mathfrak{P}} \in \mathbf{Z}.$$

Démonstration. – Soit $e \in \mathbf{Z}[G]$ congru à e^* modulo l ; alors $q(\alpha) = q(\alpha)^{e^*} = q(\alpha)^e$ soit $\alpha = \alpha^e u^l$, $u \in k'$; $\alpha A_{k'} = (\alpha A_{k'})^e (u A_{k'})^l$ ce qui entraîne $\overline{\alpha A_{k'}} = \overline{(\alpha A_{k'})^e} = \overline{\alpha A_{k'}}^{e^*}$. Si on écrit

$$\alpha A_{k'} = \prod_{\mathfrak{P}} \mathfrak{P}^{y_{\mathfrak{P}}}, \quad y_{\mathfrak{P}} \in \mathbf{Z}[G],$$

les idéaux $\mathfrak{P}$ étant non conjugués deux à deux, on aura

$$\overline{\alpha A_{k'}} = \prod_{\mathfrak{P}} \overline{\mathfrak{P}}^{y_{\mathfrak{P}}} = \prod_{\mathfrak{P}} \overline{\mathfrak{P}}^{y_{\mathfrak{P}} e^*} = \prod_{\mathfrak{P}} \overline{\mathfrak{P}}^{e^* x_{\mathfrak{P}}}, \quad x_{\mathfrak{P}} \in \mathbf{Z}.$$

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 $\overline{\mathfrak{P}}^{e^* s} = \overline{\mathfrak{P}}^{e^*} = \overline{\mathfrak{P}}^{e^* \chi^*(s)}$; comme on a par hypothèse $s \neq 1$, il en résulte que $\chi^*(s) \neq 1$ et on obtient $\overline{\mathfrak{P}}^{e^*} = \overline{1}$.

COROLLAIRE 3.1. – *L'ensemble* $P_0 \cup P_1$ *(cf. Définition 1.2) 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*).*

Remarque 3.1. – 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 $(1 - \zeta)A_{k'} = \mathfrak{P}^{a_{\mathfrak{P}}} \mathfrak{U}$, $\mathfrak{U}$ premier à $\mathfrak{P}$,

$$(1 - \zeta^s)A_{k'} = \mathfrak{P}^{s a_{\mathfrak{P}}} \mathfrak{U}^s ;$$

or $1 - \zeta^s = (1 - \zeta)\varepsilon$, ε unité, et $(1 - \zeta)A_{k'} = \mathfrak{P}^{s a_{\mathfrak{P}}} \mathfrak{U}^s$; il en résulte que $v_{\mathfrak{P}s}(1 - \zeta) = a_{\mathfrak{P}}$.

Supposons qu'il existe $\xi \in k'$ tel que $\alpha \equiv \xi^l \bmod \mathfrak{P}^\lambda$, alors $\alpha^s \equiv \xi^{sl} \bmod \mathfrak{P}^{s\lambda}$, soit $\alpha^g u^l \equiv \xi^{sl} \bmod \mathfrak{P}^{s\lambda}$ (g entier convenable), ce qui s'écrit $\alpha^g \equiv \xi'^l \bmod \mathfrak{P}^{s\lambda}$ (car α est premier à $\mathfrak{P}$ et ses conjugués),

soit $\alpha \equiv \xi'^{l} \bmod \mathfrak{P}^{s\lambda}$; 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 1.2) 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 2.5 qui permet un calcul effectif immédiat.

ii) si $\mathfrak{P}$ est un idéal premier qui ne divise pas l, on utilise la proposition 2.2 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 2.4 : $(\alpha, a)_{\mathfrak{p}} = \zeta^{\nu_{\mathfrak{P}}(a) S_{\mathfrak{P}}(q_{\mathfrak{P}}(c))}$, $c = \dfrac{\alpha - 1}{l(\zeta - 1)}$, en choisissant le nombre α congru à 1 modulo $l(\zeta - 1)$ (ce qui est possible d'après le cas (iii) de la Proposition 1.2).

iii)$_2$ $\mathfrak{P} \in P_1$, on applique la proposition 2.4 :

$$(\alpha, a)_{\mathfrak{p}} = \zeta^{\nu_{\mathfrak{P}}(\alpha) S_{\mathfrak{P}}(q_{\mathfrak{P}}(c))}, \quad c = \frac{a - 1}{l(\zeta - 1)},$$

en supposant a congru à 1 modulo $l(\zeta - 1)$.

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

PROPOSITION 3.3. – *Si* $\mathfrak{P} \in P_2$ *alors :*

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

si a est congru à 1 *modulo* $\mathfrak{P}^{t_{\mathfrak{P}}}$ *et* α *choisi congru à* 1 *modulo* $\mathfrak{P}^{\lambda_{\mathfrak{P}}}$.

Démontrons ce résultat à partir de l'énoncé de la proposition 2.3. On sait que $M \in \mathfrak{P}^{t\mathfrak{q}}$, $M \notin \mathfrak{P}^{t\mathfrak{q}+1}$ (théorie de la ramification supérieure) et que $Tr_{K'/k'}(M) \equiv -N_{K'/k'}(M) \equiv -M^l$ modulo $\pi^{t\mathfrak{q}+1}$ (on utilise le lemme 5 p. 91 de [31] et le fait que $\pi^{\sigma-1} \equiv 1 \bmod \pi^{t\mathfrak{q}}$). Posons $\xi = \pi^{\sigma-1}$, alors $M = \xi - 1 = \varphi\pi^{t\mathfrak{q}}$, φ unité $\mathfrak{P}$-adique ; on aura $M^l = (\xi - 1)^l = \varphi^l\pi^{lt\mathfrak{q}}$.

Posons $\theta = 1 + \pi^{\lambda\mathfrak{q}}\varepsilon$, ε unité ; alors

$$\left(\frac{\theta - 1}{\varepsilon}\right)^{\sigma-1} = (\pi^{\lambda\mathfrak{q}})^{\sigma-1} = \xi^{\lambda\mathfrak{q}} = 1 + \lambda_{\mathfrak{q}}\varphi\pi^{t\mathfrak{q}} \bmod \pi^{t\mathfrak{q}+1}$$

et

$$(\xi^{\lambda\mathfrak{q}} - 1)^l \equiv \lambda^l\,\varphi^l\pi^{lt\mathfrak{q}} \bmod \pi^{l(t\mathfrak{q}+1)},$$

d'où la relation $\left(\left(\frac{\theta - 1}{\varepsilon}\right)^{\sigma-1} - 1\right)^l \equiv \lambda_{\mathfrak{q}}^l M^l \bmod \pi^{l(t\mathfrak{q}+1)}$. Comme $\lambda_{\mathfrak{q}}$ est premier à l (proposition 1.2), on est ramené au calcul de $\left(\left(\frac{\theta - 1}{\varepsilon}\right)^{\sigma-1} - 1\right)^l$ modulo $\pi^{l(t\mathfrak{q}+1)}$.

On a

$$\left(\frac{\theta - 1}{\varepsilon}\right)^{\sigma-1} - 1 = \frac{\zeta\theta - 1}{\theta - 1}\,\varepsilon^{1-\sigma} - 1 = \frac{(\zeta\theta - 1)\varepsilon^{1-\sigma} - \theta + 1}{\theta - 1},$$

or $\varepsilon^{1-\sigma} \equiv 1 \bmod \pi^{t\mathfrak{q}+1}$ et $\frac{\zeta\theta - 1}{\theta - 1} \equiv 1 \bmod \pi^{t\mathfrak{q}}$, donc

$$\frac{(\zeta\theta - 1)\varepsilon^{1-\sigma} - \theta + 1}{\theta - 1} \equiv \frac{\zeta\theta - \theta}{\theta - 1} \bmod \pi^{t\mathfrak{q}+1} ;$$

on en déduit que $\left(\left(\frac{\theta - 1}{\varepsilon}\right)^{\sigma-1} - 1\right)^l \equiv \lambda_{\mathfrak{q}}^l M^l \equiv \frac{(\zeta - 1)^l\theta^l}{(\theta - 1)^l} \bmod \pi^{l(t\mathfrak{q}+1)}$, ce qui s'écrit encore $M^l \equiv \frac{(\zeta - 1)^l\alpha}{\lambda_{\mathfrak{q}}(\theta - 1)^l} \bmod \pi^{l(t\mathfrak{q}+1)}$, soit $M^l \equiv \frac{(\zeta - 1)^l}{\lambda_{\mathfrak{q}}(\theta - 1)^l}$ (car $\alpha \equiv 1 \bmod \pi^{l\lambda\mathfrak{q}}$).

Montrons enfin que $(\theta - 1)^l \equiv \alpha - 1 \bmod \pi^{la_{\mathfrak{q}}}$, avec

$$a_{\mathfrak{q}} = v_{\mathfrak{q}}(1 - \zeta) ;$$

on a $\alpha - 1 = \theta^l - 1 = \prod_{k=1}^{l} (\theta - \zeta^k)$ 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 $l a_{\mathfrak{P}}$; d'où $\alpha - 1 \equiv (\theta - 1)^l \bmod \pi^{t+\lambda_{\mathfrak{P}} l}$. Finalement :

$-\dfrac{a-1}{\mathrm{M}^l} \equiv -\dfrac{\lambda_{\mathfrak{P}}(a-1)\ (\alpha-1)}{(\zeta-1)^l}$ modulo $\pi^{t_{\mathfrak{P}}}$, c'est-à-dire que $\dfrac{a-1}{\mathrm{Tr}(\mathrm{M})}$ est congru à $\dfrac{\lambda_{\mathfrak{P}}(a-1)\ (\alpha-1)}{l(\zeta-1)}$ modulo $\mathfrak{P}$.

2. *Propriété fondamentale du symbole* $(\alpha, a)_{\mathfrak{P}}$.

On a le résultat suivant :

PROPOSITION 3.4. — *Soit $\mathfrak{P}$ une place quelconque de k' ; le symbole $(\alpha, a)_{\mathfrak{P}}$, $a \in k^*$, $\alpha \in k'^*$ tel que $q(\alpha) \in \mathfrak{X}^*$, ne dépend que de la place $\mathfrak{p}$ de k en dessous de $\mathfrak{P}$.*

Démonstration. — On peut supposer que $\mathfrak{P}$ est un idéal premier de k' et que l est différent de 2 car autrement la proposition est triviale.

Soit $\mathfrak{P}^s$ un conjugué de $\mathfrak{P}$. Supposons d'abord que $\mathfrak{P}$ ne divise pas l. Soit g un entier congru à $\chi^*(s)$ modulo l ; la proposition 3.2 montre que $g v_{\mathfrak{P}} s(\alpha) \equiv v_{\mathfrak{P}}(\alpha) \bmod l$; on a

$$(\alpha, a)_{\mathfrak{P}} \equiv (\alpha^{v_{\mathfrak{P}}(a)} a^{-v_{\mathfrak{P}}(\alpha)})^{\frac{\bar{q}-1}{l}} \bmod \mathfrak{P}$$

soit

$$(\alpha, a)^s_{\mathfrak{P}} = (\alpha, a)^g_{\mathfrak{P}} \equiv (\alpha^{g v_{\mathfrak{P}}(a)} a^{-v_{\mathfrak{P}}(\alpha)})^{\frac{\bar{q}-1}{l}} \bmod \mathfrak{P}^s,$$

$$(\alpha, a)^g_{\mathfrak{P}} \equiv (\alpha^{v_{\mathfrak{P}}(a)} a^{-v_{\mathfrak{P}} s(\alpha)})^{\frac{\bar{q}-1}{l} g} \bmod \mathfrak{P}^s \ ;$$

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

Supposons maintenant que $\mathfrak{P}$ divise l.

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

$$c^s \equiv c_s \mod \mathfrak{P}^s \ ;$$

les différentes expressions possibles pour c sont :

$$\frac{a-1}{l(\zeta-1)}\, v_{\mathfrak{P}}(\alpha)\,,$$

$$\frac{\alpha-1}{l(\zeta-1)}\, v_{\mathfrak{P}}(a)\,,$$

$$\frac{\lambda_{\mathfrak{P}}(a-1)\,(a-1)}{l(\zeta-1)}\,,$$

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

Remarque 3.2. – Sous les hypothèses de la proposition précédente on peut sans inconvénient noter le symbole $(\alpha, a)_{\mathfrak{P}}$ par $(\alpha, a)_{\mathfrak{p}}$.

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, $\mathcal{J}(K)$, $\mathcal{J}'_0(K)$, $\mathcal{J}_0(K)$, $\mathcal{H}'(K)$ et $\mathcal{H}(K)$ (resp S_k, A_k, E_k, $\mathcal{J}(k)$, $\mathcal{J}'_0(k)$, $\mathcal{J}_0(k)$, $\mathcal{H}'(k)$ 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

$$\mathcal{J}_0 = \mathcal{J} \cap \mathcal{J}_0(K).$$

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 $\nu = 1 + \sigma + \ldots + \sigma^{l-1}$. 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 :

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

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

THEOREME 4.1. – *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 ($E_k^+ = E_k \cap \mathrm{Ker}\ S_k$). Alors :*

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

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 $l = 2$ et posons :

$$\overline{K^*} = \{\alpha \in K^*,\ S_K(N\alpha) = 1\},\ \overline{E_K} = \{\varepsilon \in E_K,\ S_K(N\varepsilon) = 1\},$$

$$E_k^{++} = \{\varepsilon \in E_k,\ S_K(\varepsilon) = 1\} \quad \text{et} \quad \Gamma = \{\alpha \in K^*,\ N\alpha \in E_k\}.$$

LEMME 4.1. – *On a les suites exactes :*

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

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

Les homomorphismes θ, μ, φ et ψ sont ainsi définis : si $\mathrm{Cl}'(\mathfrak{A}) \in \mathcal{H}_1'$ alors $\mathfrak{A}^{\sigma-1} = \alpha A_K$, $\alpha \in K^*$; $\mu(\mathrm{cl}'(\mathfrak{A}))$ est alors l'image de $S_K(\alpha)$ dans $S_K(\Gamma)/S_K(E_K K^{*\sigma-1})$; on pose $\theta(\mathrm{cl}(\mathfrak{A})) = \mathrm{cl}'(\mathfrak{A})$, on a donc

$$\mathrm{Ker}\ \theta = \{\mathrm{cl}(\gamma A_K),\ S_K(\gamma^{\sigma-1}) \in S_K(E_K)\}$$

et à $\mathrm{cl}(\gamma A_K)$ 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 $\overline{K}^*/\mathrm{Ker}\ S_K$ la classe $\mathrm{cl}(\gamma A_K)$.

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

On obtient alors :

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

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

LEMME 4.2. – *On a les suites exactes :*

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

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

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

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

Le lemme 4.2 conduit à l'expression :

$$|\mathcal{H}_1| = |\mathcal{H}'_1| \frac{|\overline{K}^*|}{|\mathrm{Ker}\ S_K|\ |S_K(E_k \cap NK^*)|} =$$

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

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

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 $\mathcal{J}'_0(k)/\mathcal{J}_0(k) \cong S_k(k^*)/S_k(E_k)$, 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 4.1. – *Lorsque k est égal à* $\mathbf{Q}$ *(ou à un corps quadratique réel avec $l = 2$ et $|\mathcal{H}(k)| = 1$), $|\mathcal{H}_1| = l^{t-1}$, t étant le nombre d'idéaux premiers ramifiés dans* K/k.

COROLLAIRE 4.2. – *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 :

$$1 \to \mathcal{H}_1^0 \to \mathcal{H}_1 \to E_k^{+} \cap NK^*/NE_K^{+} \to 1\,,$$

où $\mathcal{H}_1^0$ désigne le sous-groupe de $\mathcal{H}_1$ formé des classes des idéaux de K invariants par H : soit $\mathrm{cl}(\mathfrak{A}) \in \mathcal{H}_1$, 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 1.1) ; l'application qui associe à $\mathrm{cl}(\mathfrak{A}) \in \mathcal{H}_1$ l'image de ε dans $E_k^{+} \cap NK^*/NE_K^{+}$ est un homomorphisme surjectif dont le noyau est $\mathcal{H}_1^0$ (vérification immédiate).

Par exemple, si $k = \mathbf{Q}$ et si K est une extension quadratique de $\mathbf{Q}$, 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 4.1. – On a la relation suivante :

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

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 [19] p. 192 ainsi que le théorème 94 de Hilbert ([17])).

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

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

$$1 \to \mathcal{H}_R \cap \mathrm{Im}\, j \to \mathrm{Im}\, j \to \mathcal{H}_1^0/\mathcal{H}_R \to 1.$$

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 :

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

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

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

On rappelle que σ est un générateur de H (groupe cyclique d'ordre l).

PROPOSITION 4.1. –

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

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

iii) lorsque $M^\nu = \{1\}$ *on a pour tout* $n \geqslant 0$ *la relation*

$$M^{(n)} = M_{n(l-1)}.$$

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 $l = 2$, 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 (ce qui provient du fait que $(\sigma - 1)^l \equiv 0 \bmod l\mathbf{Z}[H]$).

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

$$1 + X + \ldots + X^{l-1} = (X-1)^{l-1} - lA(X),$$

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

$$\nu = (\sigma - 1)^{l-1} - lA(\sigma) \text{ dans } \mathbf{Z}[H] ;$$

vérifions que dans $\mathbf{Z}_l[H]$, $A(\sigma)$ est inversible :

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

$$U(X)\ (X^l - 1) + V(X)\ A(X) = 1 ;$$

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 $\mathbf{Z}_l[X]$ à condition d'écrire la relation précédente sous la forme $U(X)\ (X^l - 1) + V(X)\ A(X) = l^n$, $n \geqslant 0$, 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 $\mathbf{F}_l[X]$ la relation

$$\overline{U}(X)\ (X^l - \overline{1}) = -\overline{V}(X)\ \overline{A}(X) ;$$

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 $\mathbf{Z}_l[H]$, $V(\sigma)\ A(\sigma) = 1$.

Si le $\mathbf{Z}_l[H]$-module M est annulé par ν, on a, pour tout $h \in M$, $h^{(\sigma-1)^{l-1}} = h^{lA(\sigma)}$, soit pour tout $n \geqslant 1$, $h^{(\sigma-1)^{n(l-1)}} = h^{l^n A^n(\sigma)}$, ce qui montre que $h^{(\sigma-1)^{n(l-1)}} = 1$ si et seulement si $h^{l^n} = 1$, d'où l'assertion (iii).

PROPOSITION 4.2. — *Soit* R_q *le* l^q*-rang de* M *(i.e. la dimension sur* $\mathbf{F}_l$ *de l'espace vectoriel* $M^{l^{q-1}}/M^{l^q}$*) ; alors* R_q *est égal à la dimension sur* $\mathbf{F}_l$ *de* $M^{(q)}/M^{(q-1)}$.

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

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

COROLLAIRE 4.3. – *On suppose* $M^{\nu} = \{1\}$. *Soit* n *le plus petit entier tel que* $M_n = M$; *on pose* $n = a(l-1) + b$, $a \geqslant 0$, $0 \leqslant b < l-1$. *Si les quotients* M_{i+1}/M_i *sont d'ordre* l *pour* $0 \leqslant i < n$, *alors on a l'isomorphisme :*

$$M \simeq (\mathbf{Z}/l^{a+1}\mathbf{Z})^b \times (\mathbf{Z}/l^a\mathbf{Z})^{l-1-b}.$$

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

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

est donc égal à $\dfrac{|M^{C_q}/M^{l^q}|}{|M^{(q)}/\{1\}|} = \dfrac{|M|}{|M^{l^q}|\,|M^{(q)}|}$. Comme M est fini, on a $h_q(A) = 1$ ([31] p. 142), quel que soit $q \geqslant 1$; d'où :

$$\frac{|M^{(q)}|}{|M^{(q-1)}|} = \frac{|M^{l^{q-1}}|}{|M^{l^q}|}$$

ce qui démontre la première partie de la proposition. La seconde partie résulte de la relation (proposition 4.1, (iii)) :

$$M^{(q)}/M^{(q-1)} = M_{q(l-1)}/M_{(q-1)(l-1)}.$$

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

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

d'où l'isomorphisme.

PROPOSITION 4.3. – *Soit* M *tel que* $M^{\nu} \neq \{1\}$. *Soit* n *le plus petit entier tel que* $M_n = M$; *on pose* $n = a(l-1) + b$, $0 \leqslant b < l-1$. *On suppose que* $|M_{i+1}/M_i| = l$ *pour* $0 \leqslant i < n$. *Alors on a* $n \geqslant 2$ *et :*

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

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

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

Remarque 4.2. – Si $l = 2$ il ne reste que les possibilités

$$M \simeq \mathbf{Z}/2^n\mathbf{Z} \ (n \geqslant 2) \quad \text{ou} \quad M \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

Démonstration. –

LEMME 4.3. – *Pour tout* $q \geqslant 1$ *on a la suite exacte d'espaces vectoriels :*

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

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

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

$$M_1 \cap M_n^{l^{q-1}}/M_n^{l^q} \cap M_1 \subset \mathrm{Ker}(\sigma - 1),$$

l'inclusion inverse étant triviale.

LEMME 4.4. – *Si* $n \neq l$ *alors le l-rang de* M *est égal au l-rang de* M_{n-1}.

Supposons d'abord $n \geqslant l + 1$.

Soit $x \in M_{n-1} \backslash M_{n-2}$ (ce qui a un sens car on a $n \geqslant l + 1 \geqslant 3$) 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 $B(\sigma) \in \mathbf{Z}_l[H]$ tel que $(\sigma - 1)^{n-2} = B(\sigma)(\sigma - 1)^{l-1}$ et en posant $z = x^{B(\sigma)}$ on obtient $y = z^{(\sigma-1)^{l-1}}$. Comme $M_{n-1} = M^{\sigma-1}$ on a $M_{n-1}^{\nu} = \{1\}$ donc, ici $z^{\nu} = 1$ et $z^{(\sigma-1)^{l-1}} = z^{lA(\sigma)}$ ce qui montre que $y \in M^l$; l'hypothèse $|M_1| = l$ entraîne alors l'inclusion $M_1 \subset M^l$. Le lemme 4.3 appliqué avec $q = 1$ donne alors l'isomorphisme

$$M_n/M_n^l \simeq M_{n-1}/M_{n-1}^l.$$

Si on suppose maintenant $n \leqslant l - 1$, on aura $M_{n-1} \simeq (\mathbf{Z}/l\mathbf{Z})^{n-1}$ (corollaire 4.3 appliqué à M_{n-1}), or la relation $\nu = (\sigma - 1)^{l-1} - lA(\sigma)$ conduit à

$$M_n^{\nu} = M^{(\sigma-1)^{l-1} - lA(\sigma)} = M_n^l$$

car,

$$M_n^{(\sigma-1)^{l-1}} = \{1\} ;$$

donc comme $M_n^{\nu} = M_1$ on a $M_n^l = M_1$ et nécessairement M est isomorphe à $(\mathbf{Z}/l^2\mathbf{Z}) \times (\mathbf{Z}/l\mathbf{Z})^{n-2}$ $(n \geqslant 2)$. D'où le lemme.

Démonstration de la proposition. — Les cas (i) et (ii) se déduisent immédiatement du lemme 4.4.

Remarquons que pour $j \leqslant i$ on a, avec des notations évidentes, $(M_i)_j = M_j$; on peut donc appliquer les résultats du corollaire 4.3. à M_{n-1}.

Supposons $n \geqslant l + 1$. Le lemme 4.3 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 4.4 et la remarque ci-dessus montrent que, pour $q \leqslant \left[\frac{n-1}{l-1}\right]$, les l^q-rangs de M et M_{n-1} sont égaux à $l - 1$.

Posons $n - 1 = a'(l - 1) + b'$, $0 \leqslant b' < l - 1$

$$\left(\text{on a } a' = \left[\frac{n-1}{l-1}\right]\right).$$

Le lemme 4.3 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 $l^{a'+1}$-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 $x^{\nu} = x^{(\sigma-1)^{l-1}} x^{-lA(\sigma)}$;

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

$x' \in M_{n-(l-1)} = M_{(a'-1)(l-1)+b'+1} \subset M_{a'(l-1)}$; or

$$M_{a'(l-1)} = (M_{n-1})_{a'(l-1)} = (M_{n-1})^{(a')}.$$

Comme $x \notin M_{n-1}$, on a $x^{l^{a'+1}} \neq 1$ soit $x''^{l^{a'}} \neq 1$. 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 $n \geqslant l+1$), 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 4.3. – Les résultats précédents s'appliquent au H-module $\mathcal{H}(K)$. La filtration $\{M_i\}_{i\geqslant 0}$ associée à $M = \mathcal{H}(K)$ est particulièrement importante pour l'étude de $\mathcal{H}(K)$; posons :

$$\mathcal{H}_i = \{h \in \mathcal{H}(K)\,,\ h^{(\sigma-1)^i} = 1\}$$

et $$\mathcal{H}^{(n)} = \{h \in \mathcal{H}(K)\,,\ h^{l^n} = 1\}\,,\ i \geqslant 0\,,\ n \geqslant 0.$$

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

i) *$\widetilde{\mathcal{H}}$ 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 $\mathbf{F}_l[H]$-modules :*

$$1 \to N\mathcal{J}_0/(N\mathcal{J} \cap \mathcal{J}_0(k))^l \to N\mathcal{J} \cap N\mathcal{J}_0(K)/(N\mathcal{J} \cap \mathcal{J}_0(k))^l$$

$$\xrightarrow{\bar{\varphi}} \widetilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1 \to 1\,,$$

où $$\mathcal{J}_0 = \mathcal{J} \cap \mathcal{J}_0(K).$$

Remarque 4.4. – D'après un résultat connu ([27], 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* $N\mathcal{J} \cap N\mathcal{J}_0(K)$ *dans* $\widetilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1$.

Soit $\mathfrak{a} \in N\mathcal{J} \cap N\mathcal{J}_0(K)$; il existe $\mathfrak{A}_0 \in \mathcal{J}$ et $\alpha \in K^{*+}$ tels que $\mathfrak{a} = N\mathfrak{A}_0 = N(\alpha A_K)$; l'idéal $\mathfrak{A}_0 \alpha^{-1} A_K$ étant de norme A_k, il existe $\mathfrak{A} \in \mathcal{J}(K)$ [1] tel que :

$$\mathfrak{A}_0 = \alpha A_K \mathfrak{A}^{\sigma-1}. \tag{1}$$

On note $\varphi(\mathfrak{a})$ l'image de la classe de $\mathfrak{A}$ dans $\widetilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1$. Montrons que $\varphi(\mathfrak{a})$ ne dépend pas des choix effectués. Si $\mathfrak{a} = N\mathfrak{A}'_0 = N(\alpha' A_K)$, $\mathfrak{A}'_0 \in \mathcal{J}$, $\alpha' \in K^{*+}$, 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 :

$$\mathfrak{A}'_0 = \mathfrak{A}_0 \mathfrak{b}^{\sigma-1}, \tag{2}$$

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

au couple $(\mathfrak{A}'_0, \alpha')$ est associé un idéal $\mathfrak{A}'$ tel que :

$$\mathfrak{A}'_0 = \alpha' A_K \mathfrak{A}'^{\sigma-1}. \tag{4}$$

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 $\widetilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1$. On a bien un homomorphisme et on vérifie qu'il est surjectif.

b) *Définition de* $\overline{\varphi}$.

Soit $\mathfrak{a}_0 \in N\mathcal{J} \cap \mathcal{J}_0(k)$, $\mathfrak{a}_0 = N\mathfrak{A}_0 = \alpha_0 A_k$ avec $\mathfrak{A}_0 \in \mathcal{J}$, $\alpha_0 \in k^{*+}$; posons $\mathfrak{a} = \mathfrak{a}_0^l$, alors $\mathfrak{a} = N(\alpha_0 A_K) = N(\alpha_0 A_K)$; comme $\mathfrak{a}_0 = N\mathfrak{A}_0$

[1] On vérifie facilement qu'il suffit de choisir $\mathfrak{A}$ modulo $j(\mathcal{J}(k))$ pour que sa classe soit dans $\mathcal{H}(K)$.

on aura $\alpha_0 A_K = (N\mathfrak{A}_0)A_K = \mathfrak{A}_0^{\nu} \in \mathcal{J}$ (car $\mathcal{J}$ est un H-module), on aura aussi $\alpha_0 A_K \in \mathcal{J}_0(K)$ car α_0 est dans K^{*+}. On obtient la relation $\alpha_0 A_K = \alpha_0 A_K \mathfrak{A}'^{\sigma-1}$ avec $\mathfrak{A}' = A_K$; donc $\mathrm{Ker}\,\varphi$ contient $(N\mathcal{J} \cap \mathcal{J}_0(k))^l$, d'où $\bar{\varphi}$ par passage au quotient.

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

Si $\mathfrak{a} \in N\mathcal{J}_0$, $\mathfrak{a} = N(\alpha A_K)$ 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 $\mathfrak{a} \in N\mathcal{J} \cap N\mathcal{J}_0(K)$, $\mathfrak{a} = N\mathfrak{A}_0 = N(\alpha A_K)$, $\mathfrak{A}_0 \in \mathcal{J}$ et $\alpha \in K^{*+}$; $\mathfrak{A}_0 = \alpha A_K \mathfrak{A}^{1-\sigma}$, 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 $\mathfrak{A}'^{\sigma-1}$ sous la forme γA_K (on a alors $\gamma \in K^{*+}$ et $N\gamma \in E_k^+$). On a donc $\alpha A_K = \mathfrak{A}_0 \mathfrak{A}_1^{\sigma-1} \beta^{\sigma-1} \gamma A_K$, d'où $(\gamma^{-1}\alpha\beta^{1-\sigma})A_K = \mathfrak{A}_0 \mathfrak{A}_1^{\sigma-1}$; comme $\mathfrak{A}_0$ et $\mathfrak{A}_1$ sont dans $\mathcal{J}$, on a $\mathfrak{A}_0 \mathfrak{A}_1^{\sigma-1} = (\gamma^{-1}\alpha\beta^{1-\sigma})A_K \in \mathcal{J}_0$, 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 $N\mathcal{J}_0$.

Remarque 4.5. – 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 4.2, le terme $\widetilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1$ doit être remplacé par un terme de la forme $\widetilde{\mathcal{H}}/\mathcal{H}_{\mathcal{J}}\mathcal{H}_1$ 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 $|\widetilde{\mathcal{H}}/\mathcal{H}|$ généralisant ainsi l'expression de $|\mathcal{H}_1|$ (théorème 4.1) (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 4.2. On pose $I_0 = N\mathcal{J} \cap \mathcal{J}_0(k)$ et on considère la suite exacte :

$$1 \to E_k^+ \to k^{*+} \xrightarrow{\psi} \mathcal{J}_0(k) \to 1.$$

DEFINITION 4.1. – *On pose :*

$$\Lambda = \psi^{-1}(I_0) ;$$

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

$$q : \Lambda \to \Lambda/\Lambda^l.$$

b) *Résultats préliminaires.*

PROPOSITION 4.4. – *On a les suites exactes de F_l-espaces vectoriels suivantes :*

$$1 \to N\mathcal{J}_0/I_0^l \to I_0 \cap N\mathcal{J}_0(K)/I_0^l \to \mathfrak{Je}/\mathfrak{Je}\mathfrak{Je}_1 \to 1$$

$$1 \to \Lambda \cap NK^*/\Lambda^l(E_k^+ \cap NK^*) \to I_0 \cap N\mathcal{J}_0(K)/I_0^l \to 1$$

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

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

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

Démonstration. – La première suite n'est autre que celle du théorème 4.2, compte tenu de l'égalité (utilisant la proposition 1.1, (i)) : $I_0 \cap N\mathcal{J}_0(K) = N\mathcal{J} \cap N\mathcal{J}_0(K)$. Ceci étant, soit $x \in \Lambda \cap NK^*$; considérons xA_k, puis l'image de xA_k dans $I_0 \cap N\mathcal{J}_0(K)/I_0^l$ (ce qui a un sens car $xA_k \in I_0$ par définition et, en écrivant $x = N\alpha$, on peut, d'après la proposition 1.1, supposer $\alpha \in K^{*+}$, d'où

$$xA_k = N(\alpha A_K) \in N\mathcal{J}_0(K)) ;$$

montrons que l'homomorphisme ainsi défini est surjectif : si xA_k est dans $I_0 \cap N\mathcal{J}_0(K)$, 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 1.1) donc $\varepsilon \in E_k^+$, $x\varepsilon^{-1} \in \Lambda \cap NK^*$ et $x\varepsilon^{-1}A_k = xA_k$. Montrons maintenant l'injectivité.

Si $xA_k \in I_0^l$ il existe $y \in \Lambda$ tel que $yA_k \in I_0$ et $xA_k = (yA_k)^l$. On a donc $x = y^l\varepsilon'$, $\varepsilon' \in E_k^+$; comme $x \in NK^*$ on aura $\varepsilon' \in NK^* \cap E_k^+$ et $x \in \Lambda^l(E_k^+ \cap NK^*)$. Inversement, si $x = y^l\varepsilon'$, $y \in \Lambda$, $\varepsilon' \in E_k^+ \cap NK^*$, alors $xA_k = (yA_k)^l$ avec $yA_k \in I_0$, soit $xA_k \in I_0^l$. D'où l'isomorphisme.

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

$$\Lambda \cap \mathrm{NK}^*/\Lambda^l \to \Lambda \cap \mathrm{NK}^*/\Lambda^l\,(\mathrm{E}_k^+ \cap \mathrm{NK}^*) \to 1$$

dont le noyau s'identifie au quotient $\mathrm{E}_k^+ \cap \mathrm{NK}^*/\Lambda^l \cap (\mathrm{E}_k^+ \cap \mathrm{NK}^*)$; or $\Lambda^l \cap \mathrm{E}_k^+ \cap \mathrm{NK}^* = \Lambda^l \cap \mathrm{E}_k^+ = (\mathrm{E}_k^+)^l$. Pour les deux dernières suites, on considère les homomorphismes canoniques surjectifs :

$$\Lambda/\Lambda^l \to \Lambda/\Lambda \cap \mathrm{NK}^* \to 1$$

et $\mathrm{E}_k^+/\mathrm{E}_k^{+l} \to \mathrm{E}_k^+/\mathrm{E}_k^+ \cap \mathrm{NK}^* \to 1$ dont les noyaux sont respectivement $\Lambda \cap \mathrm{NK}^*/\Lambda^l$ et $\mathrm{E}_k^+ \cap \mathrm{NK}^*/\mathrm{E}_k^{+l}$.

PROPOSITION 4.5. — *On a les suites exactes (on suppose toujours* $\mathcal{J} \cap \mathcal{J}(\mathrm{K})^{\sigma-1} = \mathcal{J}^{\sigma-1}$) :

$$1 \to \mathrm{N}\mathcal{J}/\mathrm{I}_0 \to \mathrm{N}\mathcal{H} \to 1\,,$$

$$1 \to \mathrm{N}\mathcal{J}_0 \to \mathrm{N}\mathcal{J} \to \mathcal{H}/\mathcal{H}^{\sigma-1} \to 1\,,$$

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

$$1 \to \mathrm{E}_k^+/\mathrm{E}_k^{+l} \to \Lambda/\Lambda^l \to \mathrm{I}_0/\mathrm{I}_0^l \to 1.$$

Démonstration. — La première resulte de la définition de $\mathrm{N} : \mathcal{H}(\mathrm{K}) \to \mathcal{H}(k)$.

Pour la seconde, soit $\mathfrak{A} \in \mathcal{J}$; à $\mathrm{N}\mathfrak{A}$ on associe l'image de la classe de $\mathfrak{A}$ dans $\mathcal{H}/\mathcal{H}^{\sigma-1}$; si $\mathfrak{B} \in \mathcal{J}$ est tel que $\mathrm{N}\mathfrak{A} = \mathrm{N}\mathfrak{B}$ 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 $\mathcal{J} \cap \mathcal{J}(\mathrm{K})^{\sigma-1} = \mathcal{J}^{\sigma-1}$ et les classes de $\mathfrak{A}$ et $\mathfrak{B}$ sont équivalentes modulo $\mathcal{H}^{\sigma-1}$. Si la classe de $\mathfrak{A}$ est dans $\mathcal{H}^{\sigma-1}$, il existe $\mathfrak{B} \in \mathcal{J}$ et $\alpha \in \mathrm{K}^{*+}$ tels que $\mathfrak{A} = \mathfrak{B}^{\sigma-1}\alpha\mathrm{A}_\mathrm{K}$ et $\mathrm{N}\mathfrak{A} = \mathrm{N}(\alpha\mathrm{A}_\mathrm{K})$; or $\mathfrak{A} \in \mathcal{J}$ et $\mathfrak{B}^{\sigma-1} \in \mathcal{J}$ donc $\alpha\mathrm{A}_\mathrm{K} \in \mathcal{J}$ donc $\alpha\mathrm{A}_\mathrm{K} \in \mathcal{J}_0$ et $\mathrm{N}\mathfrak{A} \in \mathrm{N}\mathcal{J}_0$, la réciproque étant évidente.

La troisième est immédiate.

La dernière suite exacte découle de la suite exacte

$$1 \to \mathrm{E}_k^+ \to \Lambda \xrightarrow{\psi} \mathrm{I}_0 \to 1\,,$$

compte tenu du fait que $\Lambda^l \cap \mathrm{E}_k^+ = \mathrm{E}_k^{+l}$.

PROPOSITION 4.6. – *L'ordre du quotient* $\widetilde{\mathfrak{H}}/\mathfrak{H}$ *est donné par la formule* :

$$|\widetilde{\mathfrak{H}}/\mathfrak{H}| = \frac{|\mathfrak{H}(k)|\ |\Lambda \cap \mathrm{NK}^*/\Lambda^l|}{|\mathrm{N}\mathfrak{H}|\ |\Lambda/\Lambda^l|}\, l^{t-1}.$$

Démonstration. – La proposition 4.4 conduit à l'expression

$$|\widetilde{\mathfrak{H}}/\mathfrak{H}\mathfrak{H}_1| = \frac{|\Lambda \cap \mathrm{NK}^*/\Lambda^l|}{|\mathrm{N}\mathcal{J}_0/\mathrm{I}_0^l|\ |\mathrm{E}_k^+ \cap \mathrm{NK}^*/\mathrm{E}_k^{+l}|}.$$

On remarque que l'on a $\mathrm{I}_0^l \subset \mathrm{N}\mathcal{J}_0$; alors

$$(\mathrm{N}\mathcal{J} : \mathrm{I}_0^l) = (\mathrm{N}\mathcal{J} : \mathrm{N}\mathcal{J}_0)\ (\mathrm{N}\mathcal{J}_0 : \mathrm{I}_0^l) = (\mathrm{N}\mathcal{J} : \mathrm{I}_0)\ (\mathrm{I}_0 : \mathrm{I}_0^l),$$

ce qui montre (en utilisant la proposition 4.5) que :

$$|\mathrm{N}\mathcal{J}_0/\mathrm{I}_0^l| = \frac{|\mathrm{N}\mathfrak{H}|\ |\mathrm{I}_0/\mathrm{I}_0^l|}{|\mathfrak{H}_1 \cap \mathfrak{H}|} = \frac{|\mathrm{N}\mathfrak{H}|\ |\Lambda/\Lambda^l|}{|\mathfrak{H}_1 \cap \mathfrak{H}|\ |\mathrm{E}_k^+/\mathrm{E}_k^{+l}|},$$

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

$$|\widetilde{\mathfrak{H}}/\mathfrak{H}\mathfrak{H}_1| = \frac{|\mathfrak{H}_1 \cap \mathfrak{H}|}{|\mathrm{N}\mathfrak{H}|}\ \frac{|\Lambda \cap \mathrm{NK}^*/\Lambda^l|}{|\Lambda/\Lambda^l|}\ \frac{|\mathrm{E}_k^+/\mathrm{E}_k^{+l}|}{|\mathrm{E}_k^+ \cap \mathrm{NK}^*/\mathrm{E}_k^{+l}|}$$

$$= \frac{|\mathfrak{H}_1 \cap \mathfrak{H}|}{|\mathrm{N}\mathfrak{H}|}\ \frac{|\Lambda \cap \mathrm{NK}^*/\Lambda^l|}{|\Lambda/\Lambda^l|}\ |\mathrm{E}_k^+/\mathrm{E}_k^+ \cap \mathrm{NK}^*|$$

(cf. proposition 4.4.).

Comme $\widetilde{\mathfrak{H}}$ contient $\mathfrak{H}\mathfrak{H}_1$ on aura

$$(\widetilde{\mathfrak{H}} : \mathfrak{H}) = (\widetilde{\mathfrak{H}} : \mathfrak{H}\mathfrak{H}_1)\ (\mathfrak{H}\mathfrak{H}_1 : \mathfrak{H})$$

d'où

$$|\widetilde{\mathfrak{H}}/\mathfrak{H}| = |\widetilde{\mathfrak{H}}/\mathfrak{H}\mathfrak{H}_1|\ |\mathfrak{H}\mathfrak{H}_1/\mathfrak{H}| = \frac{|\widetilde{\mathfrak{H}}/\mathfrak{H}\mathfrak{H}_1|\ |\mathfrak{H}\mathfrak{H}_1/\mathfrak{H}|}{|\mathfrak{H}_1|}\ |\mathfrak{H}_1| =$$

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

compte tenu de la formule donnant $|\mathfrak{H}_1|$ (théorème 4.1) et de la suite exacte $1 \to \mathfrak{H}_1 \cap \mathfrak{H} \to \mathfrak{H}_1 \to \mathfrak{H}\mathfrak{H}_1/\mathfrak{H} \to 1$.

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

c) *Calcul de* $\dfrac{|\Lambda \cap \mathrm{NK}^*/\Lambda^l|}{|\Lambda/\Lambda^l|}$.

PROPOSITION 4.7. – *Soit* $q(a_1), \ldots, q(a_n)$ *une base du* $\mathbf{F}_l$*-espace vectoriel* Λ/Λ^l, $a_i \in \Lambda$. *Le nombre* $\dfrac{|\Lambda/\Lambda^l|}{|\Lambda \cap \mathrm{NK}^*/\Lambda^l|}$ *est égal à* l^r *où* r *est le rang du système linéaire homogène défini sur* $\mathbf{F}_l$ *par les* t *équations :* $\prod_{i=1}^{n} (\alpha, a_i)_{\mathfrak{p}}^{x_i} = 1$ *pour tout idéal premier* $\mathfrak{p}$ *ramifié dans* K/k, α *étant un nombre de* k' *tel que* $\mathrm{K}' = k'(\sqrt[l]{\alpha})$.

En outre, on a les relations : $0 \leqslant r \leqslant t-1$ *pour* $t \geqslant 1$ *et* $r = 0$ *si* $t = 0$.

Démonstration. – Considérons l'extension K'/k', K' et k' étant les corps obtenus par adjonction à K et k des racines $l^{\text{èmes}}$ 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 $\mathrm{K}'_{\mathfrak{P}}/k'_{\mathfrak{P}}$, $\mathfrak{P}$ décrivant l'ensemble des places de k' ([2]) ; en vertu de la proposition 2.1, (iii), si $\mathrm{K}' = k'(\sqrt[l]{\alpha})$, a sera norme locale partout, si et seulement si $(\alpha, a)_{\mathfrak{P}} = 1$ pour toute place $\mathfrak{P}$ de k', ou encore, si et seulement si $(\alpha, a)_{\mathfrak{p}} = 1$ pour toute place $\mathfrak{p}$ de k (remarque 3.2).

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 $\mathfrak{P}$ au-dessus de $\mathfrak{p}$ dans k'/k est ramifié (resp. inerte, décomposé) dans K'/k'.

Si $l = 2$ et si $\mathfrak{p}$ est une place à l'infini, le symbole $(\alpha, a)_{\mathfrak{p}}$ ne peut valoir -1, que si $k_{\mathfrak{p}} = \mathbf{R}$ 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 $\mathrm{K}_{\mathfrak{p}} = k_{\mathfrak{p}}$ et tout nombre est norme.

Supposons $\mathfrak{p}$ inerte dans K/k ; on sait que $a \in \Lambda$, donc $aA_k \in N\mathfrak{J}$ et aA_k, est la norme d'un idéal $\mathfrak{A}'$ de K' ; il en résulte pour tout $\mathfrak{P}$ au dessus de $\mathfrak{p}$ dans k'/k $v_{\mathfrak{P}}(aA_{k'}) \equiv 0 \bmod l$; l'extension locale en $\mathfrak{P}$, $K'_{\mathfrak{P}}/k'_{\mathfrak{P}}$ étant non ramifiée, ces conditions suffisent à montrer que $(\alpha, a)_{\mathfrak{p}} = 1$ (compte tenu du fait que dans le cas local non ramifié toute unité est norme).

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

$$\Lambda \cap NK^*/\Lambda^l \simeq \{(x_1, \ldots, x_n) \in \mathbf{F}_l^n, \prod_{i=1}^{n} a_i^{x_i} \in NK^*\},$$

donc $\Lambda \cap NK^*/\Lambda^l$ 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 (2.B.2) s'écrit pour tout i, $\prod_{\mathfrak{P}} (\alpha, a_i)_{\mathfrak{P}} = 1$ soit $\prod_{\mathfrak{p}} (\alpha, a_i)_{\mathfrak{p}}^{\delta_{\mathfrak{p}}} = 1$; 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 $r \leqslant t - 1$. Si $t = 0$ on vérifie directement que "r est nul" dans la formule.

Remarque 4.6. – Les n relations $\prod_{\mathfrak{p}} (\alpha, a_i)_{\mathfrak{p}}^{\delta_{\mathfrak{p}}} = 1$ évitent, dans la pratique, le calcul de n symboles.

THEOREME 4.3. – *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 $\Lambda = \psi^{-1}(N\mathcal{J} \cap \mathcal{J}_0(k))$ le groupe de nombres associé à $\mathcal{J}$ et soit $q(a_1), \ldots, q(a_n)$ une $\mathbf{F}_l$-base de Λ/Λ^l, $a_i \in \Lambda$; alors :*

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

où $t \geqslant 0$ est le nombre d'idéaux premiers ramifiés dans K/k, et où r, vérifiant en outre $r \leqslant t - 1$, est le rang du système linéaire homogène sur $\mathbf{F}_l$:

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

COROLLAIRE 4.4. — *Pour tout* $i \geqslant 0$ *on obtient pour* $\mathcal{H} = \mathcal{H}_i$:

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

3. *Algorithme général.*

Les théorèmes 4.2 et 4.3 permettent de définir une sorte d'algorithme pour la détermination de $\mathcal{H}(K)$, par construction d'une suite croissante $\{\mathcal{J}_i\}_{i\geqslant 1}$, associée à la filtration $\{\mathcal{H}_i\}_{i\geqslant 1}$, et vérifiant les hypothèses du théorème 4.2, ainsi que de la suite $\{\Lambda_i\}_{i\geqslant 1}$ correspondante (définition 4.1).

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 4.3 et construit à partir de $\Lambda_0 = E_k^+$).

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 4.2, qui permet de construire $\widetilde{\mathcal{H}}_{i-1} = \mathcal{H}_i$ comme classes des idéaux $\mathfrak{A}'$ vérifiant :

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

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 4.4 :

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

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

Remarque 4.7. – 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 (cf. remarque 4.4) ; 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 4.8. – Lorsque $t = 0$ ou 1, seuls le théorème 4.2 et la relation $|\mathcal{H}_{i+1}/\mathcal{H}_i| = \dfrac{|\mathcal{H}(k)|}{|N\mathcal{H}_i|}$ sont utilisés car tous les éléments d'un groupe Λ sont normes (le rang r est toujours nul).

Exemple 4.1. – Soit $k = Q(\sqrt{-23})$ et $l = 3$; 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 $\widetilde{k}$ (le sous-corps quadratique de k' distinct de k et de $Q(j)$) ; on a $\alpha^{s+1} = 163^3$ ce qui fait que l'extension K/k associée (déduite de $K' = k'(\sqrt[3]{\alpha})$) est cyclique de degré 3 et que K/Q est diédrale ([10]).

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 $\mathfrak{p}'_{163}A_K = \mathfrak{P}'^3$.

Détermination de $\mathcal{H}(K)$. – On a $|\mathcal{H}_1| = |\mathcal{H}(k)|3^{t-1} = 9$ (Théorème 4.1) et $\mathcal{H}_1$ est engendré par les classes des idéaux invariants (Corollaire 4.2) donc par les classes de $\mathfrak{P}$, $\mathfrak{P}'$ et $\mathfrak{p}_2 A_K$; on aura :

$$\mathcal{J}_1 = \langle \mathfrak{P}, \mathfrak{P}' \ \mathfrak{p}_2 A_K \rangle$$

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

$$I_0 = N\mathcal{J}_1 \cap \mathcal{J}_0(k) = \langle \mathfrak{p}_{163}^3 , \mathfrak{p}_{163}'^3 , \mathfrak{p}_{163}\mathfrak{p}'_{163'} , \left(\frac{3+\sqrt{-23}}{2}\right)\rangle ,$$

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

$$I_0 = \langle \mathfrak{p}_{163}^3 , (163)\,A_k , \left(\frac{3+\sqrt{-23}}{2}\right) A_k\rangle$$

et, en posant $\mathfrak{p}_{163}^3 = \alpha_0 A_k$ on obtient $\Lambda_1 = \langle \alpha_0 , 163 , \frac{3+\sqrt{-23}}{2}\rangle$.

Calculons le symbole $(\alpha , 163)_{\mathfrak{P}}$. On a $\alpha = 163\,\beta, \beta = 28 + 3\sqrt{69}$ donc $(\alpha , 163)_{\mathfrak{P}} = (\beta , 163)_{\mathfrak{P}}$; soit $\mathfrak{P}$ 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 $3\sqrt{69} \equiv 28 \bmod \mathfrak{P}$ soit $(\beta , 163)_{\mathfrak{P}} \equiv (\beta)^{54} \equiv 56^{54}$ modulo $\mathfrak{P}$; si on avait $(\beta , 163)_{\mathfrak{P}} = 1$ on aurait $56^{54} \equiv 1$ modulo 163, ce qui n'est car 56 n'est pas reste cubique modulo 163.

Le rang r_1 est égal à 1 et on a $|\mathcal{H}_2/\mathcal{H}_1| = \dfrac{3}{|N\mathcal{H}_1|}$; or

$$N\mathcal{H}_1 = \langle \mathrm{cl}(\mathfrak{p}_{163}) , \mathrm{cl}(\mathfrak{p}'_{163}) , \mathrm{cl}(\mathfrak{p}_2^3)\rangle = \langle \mathrm{cl}(\mathfrak{p}_{163})\rangle ,$$

comme $\mathfrak{p}_{163}$ n'est pas principal on a $|N\mathcal{H}_1| = 3$; d'où $\mathcal{H}(K) = \mathcal{H}_1$.

Exemple 4.2. – Soit $k = Q(\sqrt{-111})$; 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 :

$$\mathfrak{p}_2^8 = \left(\frac{5+3\sqrt{-111}}{2}\right) A_k .$$

On considère alors l'extension $K = k(\sqrt{\theta})$ avec $\theta = \dfrac{5+3\sqrt{-111}}{2}$.

On vérifie en utilisant la proposition 1.2 que K/k est non ramifiée (K/Q est biquadratique : $K = Q(\sqrt{-3} , \sqrt{37})$).

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

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

On trouve

$$N\left[\frac{-2+2\sqrt{-111}+\dfrac{5+\sqrt{-111}}{2}\sqrt{\theta}}{2}\right]=-\left(\frac{9-\sqrt{-111}}{2}\right)^2$$

et on vérifie que le nombre entre crochets α'' est tel 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 $\left(\dfrac{\alpha''}{\dfrac{9-\sqrt{-111}}{2}}\right)A_K=\mathfrak{P}_3^{\sigma-1}$ et $\mathfrak{A}=\mathfrak{P}_3$.

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

$$N\mathfrak{J}_1=\langle \mathfrak{p}_2^2, \mathfrak{p}_3\rangle \text{ et } N\mathfrak{J}_1\cap \mathfrak{J}_0(k)=\langle \mathfrak{p}_3^2\rangle.$$

On obtient alors $N\mathfrak{H}\mathfrak{e}_1=\langle \mathrm{cl}\,\mathfrak{p}_2^2\rangle$ qui est d'ordre 4 ; ainsi

$$|\mathfrak{H}\mathfrak{e}_2/\mathfrak{H}\mathfrak{e}_1|=\frac{8}{2|N\mathfrak{H}\mathfrak{e}_1|}=1$$

et $\mathfrak{H}\mathfrak{e}(K)=\mathfrak{H}\mathfrak{e}_1$ (on peut conduire aussi les calculs dans $K/Q(\sqrt{-3})$ avec $k=Q(\sqrt{-3})$; dans ce cas $|\mathfrak{H}\mathfrak{e}_1|=2$ et $\mathfrak{H}\mathfrak{e}(K)=\mathfrak{H}\mathfrak{e}_2$ et il résulte du corollaire 4.3 que $\mathfrak{H}\mathfrak{e}(K)$ est cyclique d'ordre 4 : $\mathfrak{H}\mathfrak{e}(K)$ est engendré par la classe de $\mathfrak{p}_2 A_K$, $\mathfrak{p}_2$ relatif à $k=Q(\sqrt{-111})$) ; cf. [25].

4. *Cas du corps des rationnels : caractérisation du groupe* Λ_1.

Dans le cas où $k=Q$, l'expression de $|\widetilde{\mathfrak{H}\mathfrak{e}}/\mathfrak{H}\mathfrak{e}|$ est alors :

$$|\widetilde{\mathfrak{H}\mathfrak{e}}/\mathfrak{H}\mathfrak{e}|=l^{t-1-r}.$$

Soit $\mathfrak{H}\mathfrak{e}=\mathfrak{H}\mathfrak{e}_1$; comme $E_Q^+=\{1\}$, il résulte du corollaire 4.2 que $\mathfrak{H}\mathfrak{e}_1$ est engendré par les classes des idéaux premiers ramifiés dans K/Q : si $p_1,\ldots,p_t$ sont les nombres premiers ramifiés dans K/Q, on obtient pour Λ (relativement à $\mathfrak{H}\mathfrak{e}=\mathfrak{H}\mathfrak{e}_1$) le groupe engendré par $p_1,\ldots,p_t$ et noté :

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

Remarque 4.9. – 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 $t \geqslant 2$. Des exemples on été donnés dans [11] et [12].

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

Note. – Les chapitres V et VI (cf. table des matières) paraîtront dans le Fascicule 4 (Tome 23) des Annales de l'Institut Fourier.

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, Uber die kubischen Klassenkörper zyklischer kubischer Zahlkörper, Dissertation, Karlsruhe Universität (1970).

[5] L. BOUVIER et J.J. PAYAN, Construction de certaines extensions de degré p, Séminaire de théorie des nombres de Grenoble (1972).

[6] L. BOUVIER, Table des 2-rang, 4-rang et 8-rang du 2-groupe des classes d'idéaux au sens restreint de $\mathbf{Q}(\sqrt{m})\ldots$, *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] A. FRÖHLICH, The generalization of a theorem of L. Rédei's, Qart. Jour. of math. Oxford (2), 5 (1954), 13-140.

[10] G. GRAS, Extensions abéliennes non ramifiées de degré premier d'un corps quadratique, *Bull. Soc. Math. France,* 100 (1972).

[11] 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.

[12] G. GRAS, Etude du l-groupe des classes des extensions cycliques de degré l, Sém. Delange-Pisot-Poitou, 13^e année, (1971-1972), n° 20.

[13] M.N. GRAS, Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de Q (à paraître au journal de Crelle).

[14] H. HASSE, Über die Klassenzahl des Körpers $P(\sqrt{-p})$ mit einer Primzahl $p \equiv 1 \mod 2^3$, Aequationes math. 3 (1969).

[15] H. HASSE, Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$, *J. of Number theory.*, 1 (1969), 231-234.

[16] H. HASSE, Über die Teilbarkeit durch 2^3 der Klassenzahl imaginärquadratischer Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, *j.f.d.r.u.a. Math.*, 241 (1970).

[17] D. HILBERT, Théorie des corps de nombres algébriques, trad. T. Got et A. Levy, Hermann, (1913).

[18] E. INABA, Uber die Struktur der l-klassengruppe zyklischer Zahlkörper von Primzahlgrad l, *J. Fac. Sci. Univ. Tokyo,* Sect. I 4 (1940), 61-115.

[19] K. IWASAWA, A note on the group of units of an algebraic Number Field, *J. Math. Pures et App.*, 35 (1956), 189-192.

[20] P. KAPLAN, Divisibilité par 8 du nombre de classes des corps quadratiques réels dont le 2-sous-groupe des classes est cyclique, Note, *C.R.A.S.*, t. 275, 887-890.

[21] P. KAPLAN, Divisibilité par 8 du nombre de classes des corps quadratiques dont le 2-sous-groupe des classes est cyclique et réciprocité biquadratique, à paraître au *J. Math. Soc. of Japan.*

[22] H. KISILEVSKY, Some results related to Hilbert's Theorem 94, *J. of Number theory,* 2 (1970), 199-206.

[23] S. KOBAYASHI, On the l-dimension of the ideal class group of Kummer extensions of a certain type, *J. Fac. Sci. Univ. Tokyo,* Sect. IA, Vol. 18 N° 2, 399-404.

[24] S. KOBAYASHI, On the 3-rank of the ideal class group of certain pure cubic fields (à paraître).

[25] T. KUBOTA, Uber den bizyklischen biquadratischen Zahlkorper Nagoya Math. J. 10-12 (1956), 65-85.

[26] S.N. KURODA, On the Class Number of Imaginary quadratic Number Fields, *Proceedings of Japan Academy,* 8, 1965.

[27] S. LANG, Algebraic Number Theory, Addison-Wesley Pub. comp., New York 1970.

[28] H.W. LEOPOLDT, Zur Geschlechtertheorie in abelschen Zahlkörpern, Math. Nachr., 9 (1953), 351-362.

[29] J.J. PAYAN, Sur les classes ambiges et les ordres monogènes d'une extension cyclique de degré premier impair sur **Q** ou sur un corps quadratique imaginaire, à paraître à Arkiv för mathematik.

[30] 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).

[31] J.P. SERRE, Corps locaux, Act. Sc. et ind., Paris 1962.

[32] D. SHANKS, Gauss's Ternary form reduction and the 2-Sylow sub-group, *Math. of computation,* 25 (1971), 837-853.

[33] O. TAUSSKY, A remark concerning Hilbert's Theorem 94, *J.f.d.r.u. a. Math.,* 239/240 (1970), 435-438.

Manuscrit reçu le 8 janvier 1973
accepté par C. Chabauty

Georges GRAS
Institut de Mathématiques Pures
B.P. 116
38402 – St-Martin-d'hères.
(Université scientifique et médicale
de Grenoble I)