

ANNALES DE L'INSTITUT FOURIER

JACQUES MARTINET

**Sur l'arithmétique des extensions galoisiennes à
groupe de Galois diédral d'ordre $2p$**

Annales de l'institut Fourier, tome 19, n° 1 (1969), p. 1-80

http://www.numdam.org/item?id=AIF_1969__19_1_1_0

© Annales de l'institut Fourier, 1969, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (<http://annalif.ujf-grenoble.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

SUR L'ARITHMÉTIQUE DES EXTENSIONS GALOISIENNES A GROUPE DE GALOIS DIEDRAL D'ORDRE $2p$

par Jacques MARTINET

Introduction.

Hilbert, dans son célèbre rapport sur la théorie des nombres algébriques [10], donne l'énoncé suivant :

“Une extension abélienne K de degré M dont le discriminant D est premier avec M possède une base normale” (Théorème 132).

Ce théorème peut s'énoncer sous la forme suivante : si une extension abélienne K des rationnels de groupe de Galois G a un discriminant premier avec son degré, l'anneau des entiers de K est un $\mathbb{Z}[G]$ -module libre.

En fait, l'énoncé de Hilbert est encore vrai lorsqu'on remplace la condition : “ D est premier avec M ” par la condition moins restrictive : “l'extension $K/\mathbb{Q}$ est modérément ramifiée” ; sa démonstration s'adapte aisément à ce cas. On peut trouver une autre démonstration dans l'article de Leopoldt (Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, Théorème 8 [12]) ; le résultat sur les extensions modérément ramifiées y est un cas particulier de son “Hauptsatz”, théorème de structure sur les extensions abéliennes absolues, valable sans hypothèse sur la ramification. Dans tous les cas, les démonstrations se font en plongeant l'extension dans un corps cyclotomique, ce qui ne permet pas d'étendre facilement le résultat aux extensions non abéliennes.

Le résultat le plus important de ce travail est :

Soit N une extension galoisienne du corps $\mathbb{Q}$ des rationnels, dont le groupe de Galois G est un groupe diédral d'ordre $2p$, p premier impair. Alors, si l'extension $N/\mathbb{Q}$ est modérément ramifiée, l'anneau des entiers de N est un $\mathbb{Z}[G]$ -module libre. (Théorème VI.6).

D'autre part, on démontre (Théorème II.1) :

Soient A un anneau de Dedekind, K son corps des fractions, L une extension galoisienne de K , de groupe de Galois G , B la clôture intégrale de A dans L . Alors, B est un module projectif sur $A[G]$ si et seulement si l'extension L/K est modérément ramifiée.

Ainsi, l'intérêt des résultats précédents est lié au problème de l'existence de $\mathbb{Z}[G]$ -modules projectifs de type fini non libres, G étant un groupe fini, abélien ou diédral d'ordre $2p$. Ce problème est posé par H. Cartan et S. Eilenberg (Homological algebra [5]), et a été étudié par D.S. Rim. Soit G un groupe fini. On dit que deux $\mathbb{Z}[G]$ -modules projectifs de type fini P et P' sont équivalents s'il existe deux modules libres de type fini L et L' tels que $P \oplus L$ soit isomorphe à $P' \oplus L'$. La loi de composition $(P, P') \longrightarrow P \oplus P'$ munit l'ensemble quotient $P(G)$ d'une structure de groupe. Le résultat de D.S. Rim s'énonce alors de la façon suivante :

Si G est un groupe cyclique d'ordre premier p , $P(G)$ est isomorphe au groupe des classes d'idéaux du corps des racines p -ièmes de l'unité. Il est bien connu que pour certaines valeurs de p , par exemple $p = 23$, ce dernier groupe n'est pas réduit à l'élément neutre.

On possède un résultat analogue dans le cas où G est un groupe diédral d'ordre $2p$: M. P. Lee (Integral representations of dihedral groups of order $2p$ [11]) a montré que $P(G)$ était alors isomorphe au groupe des classes d'idéaux du sous-corps réel maximal du corps des racines p -ièmes de l'unité. On connaît des nombres premiers p , par exemple $p = 257$, pour lesquels ce dernier groupe n'est pas réduit à l'élément neutre. On trouve d'autres exemples dans l'article de Ankeny-Chowla-Hasse (On the class number of the maximal real subfield of a cyclotomic field [1]).

Plan du travail.

Le premier chapitre rappelle des résultats connus concernant les modules sur les anneaux de Dedekind. On a insisté sur l'étude des réseaux : pour deux réseaux X et X' d'un espace vectoriel V , relativement à un anneau de Dedekind A , on définit une fonction $\chi(X, X')$ à valeurs dans le groupe des idéaux inversibles de A . Lorsque V est

muni d'une forme bilinéaire non dégénérée, on sait en outre définir le discriminant d'un réseau (voir J.P. Serre, Corps locaux, Chapitre III [20]). On peut alors, soit en utilisant la fonction χ , soit au moyen de calculs de discriminants, étudier si un réseau est un module libre sur A , ce qui permet de démontrer le "critère d'Artin" (Questions de base minimale dans la théorie des nombres algébriques [2]). Ces méthodes jouent un rôle important dans le chapitre IV.

On étudie dans le second chapitre les modules sur l'algèbre $A[G]$ d'un groupe fini G , A désignant un anneau de Dedekind. On démontre le théorème II.1 cité plus haut, et on étend la notion de base normale à des extensions supposées seulement séparables.

Dans le troisième chapitre, et dans toute la suite, on considère un anneau de Dedekind A , de corps des fractions κ , et une extension galoisienne N de κ ayant pour groupe de Galois G un groupe diédral d'ordre $2p$. On détermine le discriminant de l'extension N/κ . On étudie la structure de l'anneau des entiers de N comme module sur l'anneau des entiers de k , k désignant la sous extension de N quadratique sur κ .

Le quatrième chapitre est fondamental pour la suite. On étudie l'arithmétique d'une sous extension K de κ , de degré p sur κ , par la "méthode de Kummer". Notons κ' l'extension de κ obtenue par adjonction d'une racine primitive p -ième de l'unité ω , et H le sous-groupe d'ordre p de G ; on forme les "résolvantes de Lagrange" $\langle \theta, \chi \rangle = \sum_{\sigma \in H} \chi(\sigma^{-1}) (\sigma\theta)$, associées à un élément θ de K et à un caractère χ de H à valeurs dans le groupe multiplicatif de κ' . Les résolvantes de Lagrange permettent de définir une sous-extension $\tilde{k}$ de $N(\omega)$, contenue dans $k(\omega)$. On ramène l'étude des entiers de K à celle d'idéaux de $\tilde{k}$ qui sont associés à K et à un caractère χ . Nous les appelons "idéaux essentiels de K relativement à χ ". L'étude de ces idéaux conduit directement aux résultats du chapitre suivant.

Dans le cinquième chapitre, on étudie les entiers de K . On prouve en particulier que, si A est un anneau principal et si pA est un idéal maximal de A , le A -module des entiers de K possède une base du type $1, \varphi, \psi, \sigma^i \varphi + \sigma^{-i} \varphi, \sigma^i \psi + \sigma^{-i} \psi \left(1 \leq i \leq \frac{p-3}{2} \right)$, σ désignant un élément d'ordre p de G .

Le but du dernier chapitre est la démonstration du théorème VI.6, cité dans l'introduction. Supposons N/κ modérément ramifiée. Lorsque A est un anneau principal, dans lequel pA est un idéal maximal, on prouve que le A -module des entiers de K possède une base normale dans le sens du chapitre II. Lorsque A est l'anneau $\mathbb{Z}$ des entiers rationnels, on construit une base normale d'entiers de $N/\mathbb{Q}$ à l'aide d'une base normale d'entiers de $K/\mathbb{Q}$, qui existe d'après le résultat précédent, et d'une base normale d'entiers de $k/\mathbb{Q}$.

CHAPITRE I

ANNEAUX DE DEDEKIND

1. Propriétés générales.

Les définitions et les résultats de ce chapitre peuvent être trouvés dans les ouvrages suivants :

- a) Bourbaki, Algèbre Commutative, Chapitre VII [4].
- b) J.P. Serre, Corps Locaux, Chapitres I, III, IV [20].
- c) Samuel-Zariski, Commutative Algebra, Volume I, Chapitre V [19].

Rappelons qu'on appelle *anneau de Dedekind* un anneau commutatif, unitaire, qui est noethérien, intégralement clos, et dans lequel tout idéal premier non nul est maximal.

Soit A un anneau de Dedekind, K son corps des fractions, L une extension finie de K , B la clôture intégrale de A dans L . On sait que B est un anneau de Dedekind (cf. Bourbaki, Algèbre Commutative, Ch. VII, § 2, n° 5 corollaire 3 de la proposition V). Nous supposons en outre l'extension L/K séparable ; il résulte de cette hypothèse que B est un A -module de type fini (C.L., Ch. I, §).

DEFINITION I.1. — Soit $\mathfrak{P}$ un idéal premier non nul de A ; l'idéal $\mathfrak{P}B$ de B s'écrit $\mathfrak{P}B = \prod_{\mathfrak{P}'|\mathfrak{P}} \mathfrak{P}'^{e_{\mathfrak{P}'}}$. L'entier $e_{\mathfrak{P}'}$ est appelé l'indice de ramification de $\mathfrak{P}'$; l'entier $f_{\mathfrak{P}'} = [B/\mathfrak{P}' : A/\mathfrak{P}]$ est appelé le degré résiduel de $\mathfrak{P}'$. L'extension L/K est dite *modérément ramifiée* en $\mathfrak{P}'$ si :

- 1) $B/\mathfrak{P}'$ est une extension séparable de $A/\mathfrak{P}$
- 2) la caractéristique de $A/\mathfrak{P}$ ne divise pas $e_{\mathfrak{P}'}$.

L'extension L/K est dite *modérément ramifiée* en un idéal non nul $\mathfrak{A}$ de A si elle est modérément ramifiée en tout facteur premier de $\mathfrak{A}$ dans B . L'extension L/K est dite *modérément ramifiée* si elle est modérément ramifiée en tout idéal premier non nul de B .

2. Modules de type fini sur un anneau de Dedekind.

Dans ce paragraphe, A désigne un anneau de Dedekind, K son corps des fractions, et M un A -module de type fini. Rappelons qu'on appelle *rang* de M , et l'on note $rg(M)$, l'entier $n = \dim_K M \otimes_A K$.

THEOREME I.1. — *Supposons M sans torsion, de rang $n > 0$.*

a) *M est projectif*

b) *Il existe des idéaux non nuls $\mathfrak{u}_1, \dots, \mathfrak{u}_n$ de A , tels que M soit isomorphe à la somme directe $\bigoplus_{i=1}^n \mathfrak{u}_i$.*

c) *Si $M' = \bigoplus_{i=1}^n \mathfrak{u}'_i$, les $\mathfrak{u}'_i$ étant des idéaux fractionnaires non nuls de A , M et M' sont des A -modules isomorphes si et seulement si $(\prod \mathfrak{u}_i)(\prod \mathfrak{u}'_i)^{-1}$ est un idéal principal de A (cf. Bourbaki, Algèbre Commutative, Ch. VII, § 4, n° 10, prop. 22 et 24 et exercice 19).*

Il résulte du théorème ci-dessus que, étant donné un A -module M de type fini, sans torsion de rang $n > 0$, on peut trouver un idéal $\mathfrak{u}$ tel que $M \simeq A^{n-1} \oplus \mathfrak{u}$, et que, si $\mathfrak{u}'$ est un idéal de A pour lequel $M \simeq A^{n-1} \oplus \mathfrak{u}'$, $\mathfrak{u}$ et $\mathfrak{u}'$ sont équivalents. Cela nous permet de poser la

DEFINITION I.2. — *Etant donné un A -module M , de type fini, sans torsion, de rang $n > 0$, on appelle classe de M , et l'on note $cl_A(M)$ (ou $cl(M)$ lorsque aucune confusion n'est à craindre) la classe d'un idéal $\mathfrak{u}$ de A tel que M est isomorphe à la somme directe $A^{n-1} \oplus \mathfrak{u}$. On convient que, si M est réduit à 0, sa classe est la classe des idéaux principaux de A .*

On montre facilement que, étant donnée une suite exacte $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$, où M', M, M'' sont des A -modules de type fini, sans torsion, $cl(M) = cl(M') cl(M'')$.

Supposons maintenant que A ne soit pas un corps. Les A -modules de torsion de type fini sont les A -modules de longueur finie. Soit $\mathcal{C}_A$ cette catégorie ; si $M \in \mathcal{C}_A$, M possède une suite de Jordan-Hölder $0 = M_0 \subset M_1 \subset \dots \subset M_m = M$, chaque quotient M_{i-1}/M_i étant isomorphe à un module $A/\mathfrak{P}_i$, où $\mathfrak{P}_i$ est un idéal maximal de A . La suite des $A/\mathfrak{P}_i$, à une permutation près des entiers $1, \dots, m$, ne dépend que de M .

DEFINITION I.3. — On pose $\chi_A(M) = \prod_{i=1}^m \mathfrak{P}_i$.

L'application χ_A de $\mathfrak{C}_A$ dans le groupe des idéaux fractionnaires non nuls de A est multiplicative dans le sens suivant : si $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ est une suite exacte,

$$\chi_A(M) = \chi_A(M') \chi_A(M'').$$

Si $\mathfrak{u}$ est un idéal non nul de A , $A/\mathfrak{u} \in \mathfrak{C}_A$ et $\chi_A(A/\mathfrak{u}) = \mathfrak{u}$ (C. L. Ch. I, § 5).

THEOREME I.2. — Soit L une extension séparable de K , B la clôture intégrale de A dans L , $M \in \mathfrak{C}_B$. Alors, $M \in \mathfrak{C}_A$, et

$$\chi_A(M) = N_{L/K}(\chi_B(M)),$$

$N_{L/K}$ désignant la norme de L par rapport à K . En d'autres termes, $\chi_A = N_{L/K} \circ \chi_B$. (C.L. Ch. I, § 5, Prop. 12).

DEFINITION I.4. — Soit $M \in \mathfrak{C}_A$. On appelle classe de M , et l'on note $cl(M)$, la classe de l'idéal $\chi_A(M)$. Clairement, $cl(M)$ est multiplicative : si $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ est une suite exacte où $M', M, M'' \in \mathfrak{C}_A$, $cl(M) = cl(M') cl(M'')$.

3. Réseaux.

Dans ce paragraphe, A est un anneau de Dedekind, K son corps des fractions, et V un K -espace vectoriel de dimension n .

DEFINITION I.5. — On appelle réseau de V (par rapport à A) un sous- A -module de type fini de V , de rang n .

Si X est un réseau de V , il est facile de voir qu'on peut trouver deux réseaux L_1 et L_2 de V , qui sont des A -modules libres, et qui vérifient en outre $L_1 \subset X \subset L_2$.

Si X_1 et X_2 sont deux réseaux de V , et si $X_1 \subset X_2$, X_2/X_1 est un module de longueur finie.

PROPOSITION I.1. — Soient X_1 et X_2 deux réseaux de V , et soit X_3 un réseau de V , inclus dans $X_1 \cap X_2$. Alors, $\chi_A(X_1/X_3) \cdot \chi_A(X_2/X_3)^{-1}$ ne dépend pas du choix de X_3 (C.L. Ch. III, § 1, lemme 1).

DEFINITION I.6. — On note $\chi_A(X_1, X_2)$ (ou $\chi(X_1, X_2)$ lorsque aucune confusion n'est à craindre) l'idéal

$$\chi_A(X_1/X_3) \chi_A(X_2/X_3)^{-1}.$$

Remarques :

1) $\chi(X_1, X_1) = A$; si $X_2 \subset X_1$, $\chi(X_1, X_2) = \chi_A(X_1/X_2)$.

2) Si X_1, X_2, X_3 sont trois réseaux de V ,

$$\chi(X_1, X_2) \chi(X_2, X_3) \chi(X_3, X_1) = A$$

(C.L. Ch. III, § 1, Prop. 1).

3) Un réseau est un A -module de type fini, sans torsion. On peut donc définir la classe d'un réseau (définition I.2).

THEOREME I.3. — Soient X_1 et X_2 deux réseaux de V . Alors,

$$cl(X_2) = cl(\chi(X_1, X_2)) cl(X_1)$$

Démonstration. — Le théorème I.1 entraîne qu'il existe des éléments $x_1, \dots, x_n$ de V et un idéal non nul $\mathfrak{u}$ de A tels que $X_2 = Ax_1 + \dots + Ax_{n-1} + \mathfrak{u}x_n$, la somme étant directe. Notons L le réseau $Ax_1 + \dots + Ax_n$ de V , qui est un A -module libre. Comme $\chi(L, X_2) = \chi(L/X_2) = \chi(A/\mathfrak{u}) = \mathfrak{u}$,

$$cl(X_2) = cl(\mathfrak{u}) = cl(\chi(L, X_2)),$$

et le théorème est démontré dans le cas où $X_1 = L$.

Si X_1 est un réseau libre de V , $\chi(X_1, L)$ est un idéal principal (C.L. Ch. I, § 5, lemme 3). On a alors $\chi(X_1, X_2) = \chi(X_1, L) \chi(L, X_2)$, d'où $cl(X_2) = cl(\chi(X_1, X_2))$. Dans le cas général, soit X_3 un réseau libre de V . La formule $\chi(X_1, X_2) = \chi(X_3, X_2) \chi(X_3, X_1)^{-1}$ entraîne l'égalité $cl(\chi(X_1, X_2)) = cl(X_2) cl(X_1)^{-1}$, qui n'est autre que le résultat cherché.

Nous supposons maintenant V muni d'une forme bilinéaire non dégénérée T . Pour un réseau X de V , on sait définir le discriminant

de X par rapport à T (C.L. Ch. III, § 2). C'est un idéal fractionnaire de A , noté $\Delta_T(X)$. Si X et X' sont deux réseaux de V , leurs discriminants sont reliés par la formule :

$$\Delta_T(X') = \Delta_T(X) \chi(X, X')^2 \quad (\text{C.L. Ch. III, § 2, Prop. 5}).$$

On déduit alors immédiatement du théorème I.3 et de la formule ci-dessus le

THEOREME I.4. (Théorème d'Artin). — *Soient X et X' deux réseaux de V , $\mathfrak{u}$ l'idéal fractionnaire de A vérifiant $\Delta_T(X') = \Delta_T(X) \mathfrak{u}^2$. Alors,*

$$cl(X') = cl(X) \cdot cl(\mathfrak{u}).$$

COROLLAIRE. — *Soit X un réseau de V , $x_1, \dots, x_n$ des éléments de X linéairement indépendants sur K , L le réseau $Ax_1 + \dots + Ax_n$. Pour que X soit un A -module libre, il faut et il suffit que le quotient des discriminants de X et de L soit le carré d'un idéal principal.*

Remarque. — L'énoncé ci-dessus a été donné par Artin [2], dans le cas où V est une extension finie L du corps des fractions K de A , X la clôture intégrale de A dans L , et T la trace définie par l'extension L/K .

4. Discriminants dans les extensions séparables.

Dans les paragraphes IV et V, on considère un anneau de Dedekind A , de corps des fractions, K , et une extension séparable L de K , de degré fini n . On désigne par B la clôture intégrale de A dans L . B est un réseau de L par rapport à A . Soit T la forme bilinéaire

$$(x, y) \longrightarrow \text{Tr}_{L/K}(xy).$$

Elle est non dégénérée. Si X est un réseau de L (par rapport à A), on notera $\Delta_{L/K}(X)$ (ou $\Delta(X)$ lorsque aucune confusion n'est à craindre) le discriminant de X par rapport à T . Le discriminant $\Delta_{L/K}(B)$ de B est appelé le discriminant de l'extension ; on écrira souvent $\Delta(L/K)$ au lieu de $\Delta_{L/K}(B)$. Si X est un réseau de L ,

$$\Delta(X) = \Delta(L/K) \chi_A(B, X)^2 .$$

Un cas particulier important est celui où X est un idéal fractionnaire de B .

THEOREME I.5. — Soit $\mathfrak{u}$ un idéal fractionnaire non nul de B .

$$i) \Delta(\mathfrak{u}) = \Delta(L/K) N_{L/K}(\mathfrak{u})^2$$

$$ii) cl_A(\mathfrak{u}) = cl_A(B) cl_A(N_{L/K}(\mathfrak{u})) .$$

Démonstration :

i) Si $a \in K^*$, on a $N_{L/K}(a\mathfrak{u}) = a^n N_{L/K}(\mathfrak{u})$ et $\Delta(a\mathfrak{u}) = a^{2n} \Delta(\mathfrak{u})$. On est donc ramené au cas où $\mathfrak{u} \subset B$. Alors,

$$\Delta_{L/K}(\mathfrak{u}) = \Delta(L/K) \chi_A(B, \mathfrak{u})^2 \quad (\S \text{ III}). \text{ Comme } \mathfrak{u} \subset B ,$$

$$\begin{aligned} \chi_A(B, \mathfrak{u}) &= \chi_A(B/\mathfrak{u}) = N_{L/K} \circ \chi_B(B/\mathfrak{u}) \quad (\text{Théorème I.2}) \\ &= N_{L/K}(\mathfrak{u}) . \end{aligned}$$

ii) résulte immédiatement de i) et du théorème d'Artin (Théorème I.4).

5. La différentielle.

On conserve dans ce paragraphe les notations du § IV. Rappelons que l'ensemble B^* des $x \in L$ vérifiant $\text{Tr}_{L/K}(xB) \subset B$ est un idéal fractionnaire de B contenant B (C.L., Ch. III, § 3). L'idéal inverse B^{*-1} , qui est donc un idéal entier de B , s'appelle la différentielle de l'extension, nous le noterons $\mathcal{O}_{B/A}$ ou $\mathcal{O}_{L/K}$ lorsque aucune confusion n'est à craindre. Rappelons simplement les deux résultats suivants :

THEOREME I.6. — Soit $\mathfrak{B}$ (resp. $\mathfrak{u}$) un idéal fractionnaire de B (resp. de A) ; alors, $\text{Tr}_{L/K}(\mathfrak{B}) \subset \mathfrak{u} \iff \mathfrak{B} \subset \mathfrak{u} \mathcal{O}_{B/A}^{-1}$. (cf. C.L., Ch. III, § 3, prop. 7).

THEOREME I.7. — Soit $\mathfrak{Q}'$ un idéal premier non nul de B , $\mathfrak{Q} = \mathfrak{Q}' \cap A$.

$$i) L/K \text{ est non ramifiée en } \mathfrak{Q}' \iff \mathfrak{Q}' \text{ ne divise pas } \mathcal{O}_{L/K} .$$

ii) L/K est non ramifiée en $\mathfrak{R} \iff \mathfrak{R}$ ne divise pas $\Delta(L/K)$.

iii) Soit e l'indice de ramification de $\mathfrak{R}'$ par rapport à $\mathfrak{R}$. Alors, l'exposant de $\mathfrak{R}'$ dans $\mathcal{O}_{L/K}$ est au moins égal à $e - 1$, et est égal à $e - 1$ si et seulement si l'extension L/K est modérément ramifiée en $\mathfrak{R}'$.

(cf. C.L., Ch. III, § 5, théorème I pour les assertions i) et ii), et Samuel-Zariski, Commutative Algebra, Ch. V, théorème 28 pour l'assertion iii)).

Le théorème I.7 permet de calculer le discriminant d'une extension modérément ramifiée. Dans le cas où L/K est galoisienne de groupe de Galois G , et où les extensions résiduelles sont séparables, on peut calculer le discriminant en faisant intervenir la suite des groupes de ramification. Etant donné un idéal premier non nul $\mathfrak{R}'$ de B , nous noterons $G_i(\mathfrak{R}')$ (ou G_i lorsque aucune confusion n'est à craindre) la suite des groupes de ramification, l'indice i variant de -1 à $+\infty$, $G_{-1}(\mathfrak{R}')$ désignant le groupe de décomposition de $\mathfrak{R}'$, et $G_0(\mathfrak{R}')$ le groupe d'inertie de $\mathfrak{R}'$ (C.L., Ch. I, § 7 et Ch. IV, § 1).

6. Extensions de Kummer.

Dans ce paragraphe, on se donne un anneau de Dedekind A , de corps des fractions K , un nombre premier p , et une extension cyclique L de K , de degré p . On suppose la caractéristique de K distincte de p , et que K contient les racines p -ièmes de l'unité. Comme A est intégralement clos, A lui-même contient les racines p -ièmes de l'unité.

On sait ([3], Ch. V, § 11, n° 6, prop. 6) qu'il existe $\theta \in L$, tel que $L = K(\theta)$ et $\theta^p \in K$. On peut même supposer que θ est un élément de l'anneau B des éléments de L entiers sur K . Alors, $\alpha = \theta^p \in K \cap B = A$.

On peut déterminer le discriminant de l'extension L/K . Nous énoncerons seulement le théorème suivant, dans lequel les notations sont celles qui ont été introduites ci-dessus :

THEOREME I.8. — Soit $\mathfrak{R}$ un idéal maximal de A , ne divisant pas pA , et soit n l'exposant de $\mathfrak{R}$ dans α . Alors, l'extension L/K est modérément ramifiée en $\mathfrak{R}$, et est ramifiée si et seulement si p ne divise pas n .

Comme $\mathfrak{Q}$ ne divise pas pA , la caractéristique de $A/\mathfrak{Q}$ est distincte de p . On en déduit immédiatement que L/K est modérément ramifiée. La suite du théorème se démontre par des arguments standards, analogues à ceux utilisés par Hecke ([9], Ch. V, § 39, Satz 118) pour prouver le résultat dans le cas où A est un anneau d'entiers algébriques.

CHAPITRE II

MODULES SUR L'ALGÈBRE D'UN GROUPE

Sauf mention expresse du contraire, les modules considérés dans ce chapitre sont des modules à gauche.

1. Caractérisation des modules projectifs.

Dans ce paragraphe, A désigne un anneau commutatif, et G un groupe fini.

Soit M un $A[G]$ -module, et soit M_0 le A -module sous-jacent à M . $A[G] \otimes_A M_0$ est muni d'une structure de $A[G]$ -module à gauche lorsqu'on fait opérer G par $s(t \otimes x) = st \otimes x$ pour tout $x \in M_0$, et tout s , tout t de G . Nous considérons la suite exacte de $A[G]$ -modules :

$$0 \rightarrow \text{Ker } \pi \rightarrow A[G] \otimes_A M_0 \rightarrow M \rightarrow 0,$$

où π est défini par $\pi(s \otimes x) = sx$.

DEFINITION II.1. — *On dit que M est un $A[G]$ -module relativement projectif si cette suite exacte est scindée.*

PROPOSITION II.1. — *Les conditions suivantes sont équivalentes :*

- i) M est un $A[G]$ -module relativement projectif,
- ii) Il existe $f \in \text{End}_A(M)$, tel que $\sum_{s \in G} sf(s^{-1}x) = x$, quel que soit $x \in M$.

La proposition II.1 est démontrée dans [5], chapitre XII, lorsque $A = \mathbb{Z}$; la démonstration s'étend sans changement au cas d'un anneau commutatif quelconque.

COROLLAIRE. — *Si M est un $A[G]$ -module relativement projectif, M , considéré comme $\mathbb{Z}[G]$ -module, est relativement projectif.*

En effet, le A -endomorphisme f de la condition ii) est un Z -endomorphisme.

PROPOSITION II.2. — *Soit M un $A[G]$ -module. Les conditions suivantes sont équivalentes :*

- i) M est un $A[G]$ -module projectif.
- ii) M est un $A[G]$ -module relativement projectif, et un A -module projectif.

Pour une démonstration, voir [18], proposition 2-3.

Soient maintenant B un anneau commutatif, G un groupe fini d'automorphismes de B , A l'anneau des invariants de G . B est muni naturellement d'une structure de $A[G]$ -module. On définit l'application trace (en abrégé Tr) par $\text{Tr } x = \sum_{s \in G} sx$, pour tout $x \in B$. L'application $x \rightarrow \text{Tr } x$ est un A -homomorphisme de B dans A (donc un élément de $\text{End}_A(B)$), et $\text{Tr}(B)$ est un idéal de A .

PROPOSITION II.3. — *Les conditions suivantes sont équivalentes :*

- i) B est un $A[G]$ -module relativement projectif.
- ii) $\text{Tr}(B) = A$.

Démonstration :

i) $\implies$ ii).

L'anneau B , considéré comme $Z[G]$ -module, est relativement projectif (Proposition II.1, corollaire), donc cohomologiquement trivial. En particulier, $\hat{H}^0(G, B) = 0$.

Comme $\hat{H}^0(G, B) = A/\text{Tr}(B)$, $\text{Tr}(B) = A$.

ii) $\implies$ i).

Si $\text{Tr}(B) = A$, il existe $\theta \in B$, tel que $\text{Tr}(\theta) = 1$. Posons $f(x) = \theta x$. L'application f est un A -endomorphisme de B et l'on a :

$$\sum_{s \in G} sf(s^{-1}x) = \sum_{s \in G} s(\theta s^{-1}x) = \sum_{s \in G} s\theta \cdot x = \text{Tr}(\theta) \cdot x = x.$$

B est donc un $A[G]$ -module relativement projectif (Proposition II.2).

Nous allons appliquer ce résultat au cas où G est le groupe de Galois d'une extension galoisienne.

2. Anneau des entiers d'une extension galoisienne.

THEOREME II.1. — Soient A un anneau de Dedekind, K son corps des fractions, L une extension galoisienne de K de degré fini, G son groupe de Galois, B la clôture intégrale de A dans L .

Les conditions suivantes sont équivalentes :

- i) B est un $A[G]$ -module projectif.
- ii) $\text{Tr}_{L/K}(B) = A$
- iii) L/K est modérément ramifiée (Ch. I, § II, définition I.2).

Démonstration :

i) $\Longleftrightarrow$ ii).

L'anneau B est un A -module de type fini, car L/K est séparable, et sans torsion, donc projectif (Théorème I.1, a). D'après la proposition II.1, i) équivaut à la condition B est un $A[G]$ -module relativement projectif ; l'équivalence de i) et de ii) résulte alors de la proposition II.3, compte tenu de ce que $\text{Tr}(B)$, au sens de cette proposition, n'est autre que $\text{Tr}_{L/K}(B)$.

ii) $\Longleftrightarrow$ iii).

L'idéal $\text{Tr}_{L/K}(B)$ est distinct de A si et seulement s'il est contenu dans un idéal maximal $\mathfrak{P}$ de A . Pour que $\text{Tr}_{L/K}(B)$ soit contenu dans $\mathfrak{P}$, il faut et il suffit que $\mathfrak{P}B$ divise $\mathcal{O}_{B/A}$ (Théorème I.6). Dans B , $\mathfrak{P}$ se décompose en un produit d'idéaux premiers sous la forme

$\mathfrak{P}B = \left(\prod_{i=1}^g \mathfrak{P}'_i \right)^e$. Mais $\mathfrak{P}B | \mathcal{O}_{B/A} \Longleftrightarrow \mathfrak{P}'_i{}^e | \mathcal{O}_{B/A}$ pour tout $i \Longleftrightarrow L/K$

n'est pas modérément ramifiée en $\mathfrak{P}'_i$ (théorème I.7), C.Q.F.D.

Remarque. — Lorsque L/K est simplement supposée séparable, la condition “ L/K est modérément ramifiée” implique encore que l'on a $\text{Tr}_{L/K}(B) = A$: cela résulte immédiatement de la démonstration ci-dessus. Mais la réciproque est inexacte : prenons $K = \mathbb{Q}$, $A = \mathbb{Z}$; soit L une extension cubique de $\mathbb{Q}$, non galoisienne, telle que 3 ne se ramifie pas dans L , mais telle que 2 se décompose sous la forme $2B = \mathfrak{P}^2\mathfrak{P}'$, avec $\mathfrak{P} \neq \mathfrak{P}'$. Alors, L/K n'est pas modérément ramifiée, mais $\text{Tr}_{L/K}(B) = \mathbb{Z}$. On construit aisément un tel exemple à l'aide des méthodes de [13].

Le théorème II.1 donne des conditions nécessaires pour que B soit un $A[G]$ -module libre. Ces conditions ne sont pas suffisantes : d'une part, il peut se faire que B ne soit pas A -libre, et, même lorsque B est un A -module libre, B peut ne pas être $A[G]$ -libre. (Pour un exemple, voir [13], chapitre 3, § 8, remarque).

3. Notions de base normale.

Dans ce paragraphe, on se donne une extension séparable finie L/K . On pose $n = [L : K]$. Lorsque L/K est galoisienne, on note G son groupe de Galois. Plus généralement, pour une extension galoisienne quelconque L'/K' , le groupe de Galois de L'/K' sera noté $\text{Gal}(L'/K')$.

On se donne en outre un sous-anneau B de L , ayant L pour corps des fractions, et l'on pose $A = B \cap K$.

Rappelons d'abord la définition usuelle des bases normales.

DEFINITION II.2. — Soit L/K galoisienne. S'il existe $\theta \in B$, tel que tout $\varphi \in B$ s'écrive sous la forme $\varphi = \sum_{s \in G} a(s) (s\theta)$, avec $a(s) \in A$, on dit que $(s\theta)_{s \in G}$ est une base normale de B/A (ou une A -base normale de B). Cela s'exprime également en disant que B est un $A[G]$ -module libre, avec θ comme $A[G]$ -base.

Cas particulier.

$B = L$. Alors, $A = K$ et l'on a le

THEOREME DE LA BASE NORMALE. — L/K possède toujours des bases normales. En d'autres termes, L est un $K[G]$ -module libre. (cf. [3], Ch. V, § 10, n° 8, Théorème 5).

Nous aurons besoin au cours de ce travail d'une notion plus générale de base normale, valable pour une extension séparable finie. C'est l'objet de la définition suivante :

DEFINITION II.3. — Soit L/K une extension séparable finie, Ω une clôture séparable de L , N la plus petite extension de L contenue dans

Ω , qui soit galoisienne sur K (en abrégé, on dira que N est une clôture galoisienne de L/K). Une A -base $\theta_1, \dots, \theta_n$ de B est dite normale s'il existe un système $\tau_{i(1 \leq i \leq n)}$ de représentants des classes à droite de $\text{Gal}(N/K)$ modulo $\text{Gal}(N/L)$ et une base normale $(\sigma \tau_i \theta')_{\substack{\sigma \in \text{Gal}(N/L) \\ 1 \leq i \leq n}}$

de N/K , tels que

$$\theta_i = \text{Tr}_{N/L}(\tau_i \theta') = \sum_{\sigma \in \text{Gal}(N/L)} (\sigma \tau_i \theta').$$

Il est clair que cette définition ne dépend pas du choix de la clôture galoisienne N de L/K , et qu'elle généralise la définition II.2 correspondant à $N = L$.

PROPOSITION II.4.

- i) Si B/A possède une base normale, $\text{Tr}_{L/K}(B) = A$.
- ii) Si B/A possède une base normale, les composantes d'un élément de A dans cette base sont égales.

Démonstration. — Soit $\theta_1, \dots, \theta_n$ une A -base normale de B , N une clôture galoisienne de L/K . Avec les notations de la définition II.3, $\theta_i = \text{Tr}_{N/L}(\tau_i \theta') = \sum_{\sigma \in H} \sigma \tau_i \theta'$. On peut écrire

$$1 = \sum_{i=1}^n a_i \theta_i = \sum_{i, \sigma} a_i \sigma \tau_i \theta'.$$

Comme 1 est invariant par $\text{Gal}(N/K)$, les éléments a_i sont égaux à a_1 . On a donc

$$1 = a_1 \left(\sum_{i=1}^n \theta_i \right).$$

Si $a \in A$, $a = (aa_1) \left(\sum_{i=1}^n \theta_i \right)$, ce qui prouve l'assertion ii). De plus,

l'égalité $1 = a_1 \sum_{i=1}^n \theta_i$ prouve que $\sum_{i=1}^n \theta_i$ est un élément inversible de A . Pour tout i ,

$$\text{Tr}_{L/K}(\theta_i) = \text{Tr}_{N/L}(\tau_i \theta') = \sum_{i, \sigma} \sigma \tau_i \theta' = \sum \theta_i.$$

Il en résulte que $\text{Tr}_{L/K}(\theta_i)$ est un élément inversible de A , ce qui prouve i).

PROPOSITION II.5. — *Supposons L/K galoisienne, de groupe de Galois G , et soit L' un corps intermédiaire entre K et L ; posons $B' = B \cap L'$. On désigne par H le sous-groupe de G auquel appartient L' et par $(s_i)_{1 \leq i \leq n}$ un système de représentants des classes à droite de $G \bmod H$. Alors, si θ est une $A[G]$ -base de B , les éléments $\text{Tr}_{L/L'}(s_i \theta)$ de B' constituent une A -base normale de B' .*

Démonstration. — Il est clair que, pour tout i , $\text{Tr}_{L/L'}(s_i \theta)$ est un élément de B' . Un élément φ de B' s'écrit de manière unique sous la forme $\varphi = \sum_{\substack{t \in H \\ 1 \leq i \leq n}} a(t, i) (ts_i \theta)$, les $a(t, i)$ étant des éléments de A .

Comme φ est invariant par les éléments de H , on a pour tout i , $a(t, i) = a(1, i)$. Par conséquent, $\varphi = \sum_{1 \leq i \leq n} a(1, i) \left(\sum_{t \in H} ts_i \theta \right)$, ce qui prouve que les éléments $\text{Tr}_{L/L'}(s_i \theta)$ de B' constituent une base du A -module B' .

Il reste à voir que les $\text{Tr}_{L/L'}(s_i \theta)$ sont en fait une base normale de B'/A . Soit N' la clôture galoisienne de L'/K dans L . Le raisonnement ci-dessus appliqué à $B \cap N'$ permet de ramener la démonstration de la proposition II.5 au cas où L est une clôture galoisienne de L'/K ; c'est alors une conséquence immédiate de la définition II.3.

4. Bases normales dans les extensions décomposées.

Dans ce paragraphe, on se donne un corps κ , une extension galoisienne N de κ , de degré fini n , de groupe de Galois G , un sous-anneau A_N de N , ayant N pour corps des fractions ; on pose $A_L = A_N \cap L$ pour tout corps L intermédiaire entre κ et N , et $A_K = A$.

DEFINITION II.4. — *Soit k une extension intermédiaire entre κ et N , galoisienne sur κ . On dit que l'extension N/κ se décompose sur k s'il existe une extension K intermédiaire entre κ et N , linéairement disjointe de k sur κ , telle que $N = k(K)$. (voir [17], § III).*

Si H (resp. g) désigne le sous-groupe de G ayant k (resp. K) pour corps des invariants, H est distingué dans G , et il existe une section $s : G/H \rightarrow G$ de l'application canonique $q : G \rightarrow G/H$, telle que $s(G/H) = g$. On traduit cela en disant que le groupe G est produit semi-direct de H et de g .

Dans le théorème suivant, nous adoptons les notations ci-dessus.

THEOREME II.2. — *Supposons que A_N possède une A -base normale. Il en est alors de même de A_k (voir prop. II.5). Si ω désigne un élément de A_k dont les conjugués forment une base normale de A_k/A , il existe $\theta \in A_N$, dont les conjugués forment une base normale de A_N/A , et tel que $\text{Tr}_{N/k}(\theta) = \omega$.*

Démonstration. — Le groupe de Galois de k/κ est canoniquement isomorphe par restriction à g . Soit θ' une $A[G]$ -base de A_N . Posons $\omega' = \text{Tr}_{N/k}(\theta')$; ω' est une $A[g]$ -base de A_k (proposition II.5). Puisque ω et ω' sont deux $A[g]$ -bases de A_k , il existe un élément inversible u de $A[g]$ tel que $\omega = u\omega'$. Soit $\theta = u\theta'$. Du fait que u est inversible dans $A[g]$, donc dans $A[G]$, θ est une $A[G]$ -base de A_N .

D'autre part, $\text{Tr}_{N/k}(\theta) = \sum_{s \in H} s(u\theta')$. Ecrivons $u = \sum_{t \in g} a(t)t$, où $a(t) \in A$. Alors,

$$\begin{aligned} \text{Tr}_{N/k}(\theta) &= \sum_{\substack{s \in H \\ t \in g}} sa(t)t\theta' = \sum_{t \in g} a(t)t \sum_{s \in H} (t^{-1}st)\theta' \\ &= \sum_{t \in g} a(t)t \left(\sum_{s \in H} s\theta' \right) = u\omega' = \omega, \end{aligned}$$

et θ répond à la question.

PROPOSITION II.6. — *Supposons que A_k et A_K possèdent des A -bases normales. Alors, l'extension N/κ est modérément ramifiée.*

Démonstration. — Il résulte de la proposition II.4, i) que l'on a $\text{Tr}_{K/\kappa}(A_K) = A$, $\text{Tr}_{k/\kappa}(A_k) = A$. Soient alors φ et ω des éléments de A_K et A_k vérifiant $\text{Tr}_{K/\kappa}(\varphi) = 1$, $\text{Tr}_{k/\kappa}(\omega) = 1$. L'élément $\omega\varphi$ de A_N vérifie $\text{Tr}_{N/\kappa}(\omega\varphi) = 1$, ce qui prouve que N/κ est modérément ramifiée (Théorème II.1).

5. Bases quasi-normales.

On se donne dans ce paragraphe une extension séparable finie L/K , avec $[L : K] = n$; B désigne un sous-anneau de L , ayant L pour corps des fractions, et l'on pose $A = B \cap K$.

DEFINITION II.5. — On appelle *base quasi-normale de B sur A* , ou *A -base quasi-normale de B* , une A -base de B du type $1, \theta_2, \dots, \theta_n$, vérifiant la propriété suivante : il existe une clôture galoisienne N de L/K , une base normale $(s\theta)_{s \in \text{Gal}(N/K)}$ de N/K , et un système $(s_i)_{1 \leq i \leq n}$ de représentants des classes à droite de $\text{Gal}(N/K)$ modulo $\text{Gal}(N/L)$, tels que pour $2 \leq i \leq n$, $\theta_i = \text{Tr}_{N/L}(s_i \theta)$.

Il est clair que, si B admet une A -base normale $\theta_1, \dots, \theta_n$, $1, \theta_2, \dots, \theta_n$ est une A -base quasi-normale de B (en effet, on a vu dans le courant de la démonstration de la proposition II.5 que $\sum_{i=1}^n \theta_i$ est un élément inversible de A).

Réciproquement, si B admet une A -base quasi-normale, B peut ne pas admettre de A -base normale, même si $\text{Tr}_{L/K}(B) = A$. (Pour un exemple voir [13], Chapitre III, § 8, remarque).

La notion de base quasi-normale est intéressante parce qu'on peut chercher de telles bases, même lorsque la condition $\text{Tr}_{L/K}(B) = A$ n'est pas réalisée.

On peut par exemple montrer le

THEOREME. — Soit K/Q une extension cyclique de degré premier des rationnels, A l'anneau des entiers de K . Alors, A possède toujours des Z -bases quasi-normales.

(cf. [15], Chapitre III, § 2, corollaire du théorème 8).

Le cas d'une extension de degré premier dont la clôture galoisienne a pour groupe de Galois le groupe non abélien d'ordre $2p$ sera examiné au chapitre V de ce travail.

6. Résultats généraux sur les $A[G]$ -modules.

Dans ce paragraphe, on se donne un anneau de Dedekind A , de corps des fractions K , et un groupe fini G , dont l'ordre n n'est pas divisible par la caractéristique de K . On désigne par M un $A[G]$ -module projectif de type fini. On pose $n = \text{card } G$, et l'on note n' le rang du A -module M ($n' = \dim_K M \otimes_A K$). R.G. Swan ([21]) a démontré le

THEOREME. — *Supposons que $M \otimes_A K$ soit un $K[G]$ -module libre. Alors :*

1) *n est un diviseur de n' ; posons $r = \frac{n'}{n}$.*

2) *Si $r > 0$, $M \simeq A[G]^{r-1} \oplus I$, où I est un idéal projectif de $A[G]$.*

3) *Si $\mathfrak{u}$ désigne un idéal non nul de A , on peut toujours choisir I de façon à ce que $I \cap A$ soit étranger à $\mathfrak{u}$.*

L'hypothèse que $M \otimes_A K$ est $K[G]$ -libre est réalisée dans les deux cas suivants :

a) Les facteurs premiers de l'ordre de G ne sont pas inversible dans A (Swan, loc. cit.).

b) M est la clôture intégrale de A dans une extension galoisienne de K , ayant G pour groupe de Galois. En effet, $M \otimes_A K$ est alors visiblement isomorphe comme $A[G]$ -module à L , et le théorème de la base normale (§ 3) montre que L est $K[G]$ -libre.

On montre à partir du théorème de Swan, le

COROLLAIRE. — *Soit A un anneau de Dedekind semi-local (donc principal), K son corps des fractions, L une extension galoisienne de K , de groupe de Galois G , B la clôture intégrale de A dans L .*

Si la caractéristique de K ne divise pas l'ordre de G , B est un $A[G]$ -module libre.

En effet, on a $B \simeq I$, où I est un idéal projectif de $A[G]$. Notons $\mathfrak{P}_1, \dots, \mathfrak{P}_n$ les idéaux maximaux de A , et posons $\mathfrak{u} = \mathfrak{P}_1 \dots \mathfrak{P}_n$. On peut choisir I de façon que $I \cap A$ soit étranger à $\mathfrak{u}$; on en déduit alors que $I \cap A = A$, donc que $I = A[G]$.

Remarque. — Un cas particulier de ce corollaire a été donné par E. Noether ([15]).

CHAPITRE III

PROPRIETES DES EXTENSIONS DONT LE GROUPE DE GALOIS EST UN GROUPE DIEDRAL D'ORDRE $2p$

1. Notations.

Dans tout ce chapitre, on se donne un anneau de Dedekind A , de corps des fractions κ , et un nombre premier impair p .

On suppose la caractéristique de κ distincte de p .

On se donne en outre une extension galoisienne N de κ , de degré $2p$, de groupe de Galois G . On suppose que G est un groupe diédral. Il peut être défini par deux générateurs σ_0 et τ_0 , liés par relations $\sigma_0^p = 1$, $\tau_0^2 = 1$, $\sigma_0 \tau_0 = \tau_0 \sigma_0^{-1}$. G contient un sous-groupe d'ordre p , soit H ; on note k le sous-corps de N fixe par H ; c'est une extension quadratique de κ . Soit K une sous-extension de degré p de N , et g le sous-groupe de G qui lui "appartient". K/κ n'est pas une extension galoisienne. Les conjugués de K sont les p corps σK ($\sigma \in H$), appartenant aux sous-groupes $\sigma g \sigma^{-1}$ de G .

Pour toute extension L de κ , nous noterons A_L la clôture intégrale de A dans L . Nous faisons sur A l'hypothèse supplémentaire suivante :

Les corps résiduels de A sont des corps parfaits. Il résulte de cette hypothèse que, pour toute extension L de κ , de degré fini, les corps résiduels de A_L sont des corps parfaits.

Si L_1 et $L_2 \subset L_1$ sont des extensions finies de κ , nous noterons $\mathcal{O}_{L_1/L_2}$ la différentielle de A_{L_1} par rapport à A_{L_2} , et $\Delta(L_1/L_2)$ le discriminant de A_{L_1} par rapport à A_{L_2} .

On posera $\Delta(k/\kappa) = d$, $\Delta(K/\kappa) = D$, $\Delta(N/k) = \mathcal{O}$,

$$\Delta(N/K) = \delta, \Delta(N/\kappa) = \bar{D}.$$

Enfin, pour toute extension L de κ , nous noterons L' le corps obtenu en adjoignant à L les racines p -ièmes de l'unité. Nous poserons pour alléger l'écriture $A' = A_{\kappa'}$.

2. Hypothèses supplémentaires sur l'anneau A.

Nous n'obtiendrons des résultats simples qu'en faisant des hypothèses supplémentaires sur l'anneau A. Le plus souvent nous supposons que A vérifie les hypothèses suivantes :

Hypothèse (H). — p est inversible dans A, ou pA est un produit d'idéaux maximaux distincts.

Hypothèse (H'). — Le polynôme $\sum_{i=0}^{p-1} X^i$ est un polynôme irréductible de $\kappa[X]$.

PROPOSITION III.1. — *Pour que A vérifie l'hypothèse (H), il faut et il suffit que, pour tout idéal premier non nul $\mathfrak{P}$ de A, divisant pA , A soit un anneau de valuation discrète d'idéal maximal pA .*

La démonstration de cette proposition est immédiate.

PROPOSITION III.2.

a) *Si l'hypothèse (H) est vérifiée, et si p n'est pas inversible dans A l'hypothèse (H') est vérifiée.*

b) *Soit $\omega \neq 1$ une racine p -ième de l'unité. Si les hypothèses (H) et (H') sont vérifiées, $A' = A[\omega]$, et le discriminant $\Delta(\kappa'/\kappa)$ est l'idéal $p^{p-2}A$.*

Démonstration :

a) Puisque p n'est pas inversible dans A, pA possède un facteur premier $\mathfrak{P}$. Soit $f(x) = x^{p-1} + \dots + x + 1$. On a $f(x) = \frac{x^p - 1}{x - 1}$,

d'où $f(x + 1) = x^{p-1} + \sum_{k=1}^{p-1} C_p^k x^{p-k-1}$; il est clair que $f(x + 1)$ est un polynôme d'Eisenstein, d'où a) ;

b) Il suffit de faire la démonstration lorsque A est un anneau de valuation discrète. Soit $\mathfrak{P}$ son idéal maximal ; si $\mathfrak{P} | pA$, il résulte de a) que $A' = A[\omega - 1]$, donc $A' = A[\omega]$. D'autre part,

$$f'(x) = \frac{px^{p-1}(x-1) - (x^p-1)}{(x-1)^2},$$

donc $f'(\omega) = \frac{p\omega^{p-1}}{\omega-1}$. Donc, si $\mathfrak{A}$ ne divise pas pA , $f'(\omega)$ est une unité de A' , ce qui entraîne $A' = A[\omega]$. La différentielle est alors $\mathcal{O}_{A'/A} = f'(\omega)A'$ (C.L., Ch. I, § 6, prop. 17). Le discriminant de κ'/κ est $N_{\kappa'/\kappa} \left(\frac{pA'}{\omega-1} \right) = p^{p-2} A$.

3. Ramification dans N des idéaux premiers de A .

Nous étudions les diverses possibilités qu'ont les idéaux de A de se ramifier dans N , et nous calculons les discriminants de N et de ses sous-corps. Rappelons que, $\mathfrak{A}'$ désignant un idéal maximal de A_N , on note $G_i(\mathfrak{A}')$ (resp. $H_i(\mathfrak{A}')$) la suite des groupes de ramification de $\mathfrak{A}'$ dans G (resp. H) (Ch. I, § V).

PROPOSITION III.3. — *Soit $\mathfrak{A}$ un idéal premier non nul de A ne divisant pas pA , ramifié dans k , et définissons $\mathfrak{A}'$ par $\mathfrak{A}A_k = \mathfrak{A}'^2$. Alors $\mathfrak{A}'$ est dans N un produit de p idéaux premiers distincts.*

Démonstration. — N/k étant cyclique de degré p , la décomposition de $\mathfrak{A}'$ dans N ne peut prendre que l'une des formes suivantes :

- i) $\mathfrak{A}'A_N$ reste premier
- ii) $\mathfrak{A}'A_N = \mathfrak{A}'''^p$
- iii) $\mathfrak{A}'A_N = \mathfrak{A}_1'' \dots \mathfrak{A}_p''$, les $\mathfrak{A}_i''$ étant distincts.

Nous allons montrer successivement l'impossibilité de i) et de ii).

i) Si $\mathfrak{A}'$ reste premier, $G_{-1}(\mathfrak{A}') = G$, $H_{-1}(\mathfrak{A}') = H$, $H_0(\mathfrak{A}') = 1_H$. Comme N/κ est ramifiée en $\mathfrak{A}$, $G_0(\mathfrak{A}')$ n'est pas réduit à l'élément neutre. Mais $G_0(\mathfrak{A}') \cap H = H_0(\mathfrak{A}')$. (C.L., Ch. IV, § 1, Prop. 2). Donc, $G_0(\mathfrak{A}')$ est un sous-groupe d'ordre 2 de G ; mais cela est impossible, car $G_0(\mathfrak{A}')$ doit être distingué dans $G_{-1}(\mathfrak{A}') = G$.

ii) Supposons que l'on ait $\mathfrak{R}'A_N = \mathfrak{R}''^p$. L'extension $N/\mathfrak{K}$ est alors totalement ramifiée en $\mathfrak{R}$, ce qui entraîne $G_{-1}(\mathfrak{R}'') = G_0(\mathfrak{R}'') = G$. Mais N/k est modérément ramifiée en $\mathfrak{R}'$: en effet, comme $\mathfrak{R}$ ne divise pas pA , la caractéristique de $A/\mathfrak{R}$, donc aussi celle de $A_k/\mathfrak{R}'$, est distincte de p , et ne peut donc pas diviser l'indice de ramification de $\mathfrak{R}''$ par rapport à $\mathfrak{R}'$, qui est égal à p . On a donc $H_1(\mathfrak{R}'') = 1_H$, ce qui prouve que $G_1(\mathfrak{R}'')$ est un sous-groupe de G dont l'ordre est au plus 2 (car $G_1(\mathfrak{R}'') \cap H = H_1(\mathfrak{R}'')$). Comme $G_1(\mathfrak{R}'')$ est un sous-groupe distingué de $G_{-1} = G$ (C.L. Ch. IV, § 1), on a nécessairement $G_1(\mathfrak{R}'') = 1$. Mais on sait que G_0/G_1 est un groupe cyclique (C.L. Ch. IV, § 2, corollaire 1 de la proposition 7), ce qui conduit à une contradiction, car G_0/G_1 est isomorphe à G .

Remarque. — La démonstration de l'impossibilité de i) n'utilise pas le fait que $\mathfrak{R}$ ne divise pas pA .

PROPOSITION III.4. — Soit $\mathfrak{R}$ un idéal premier non nul de A , divisant pA , totalement ramifié dans N ; écrivons $\mathfrak{R}A_N = \mathfrak{R}''^{2p}$. Soit G_i (resp. H_i) la suite des groupes de ramification de $\mathfrak{R}''$ dans G (resp. H), et soit t l'entier pour lequel $G_t \neq \{1\}$, $G_{t+1} = \{1\}$. Alors, t est impair, au moins égal à 1, et $G_i = H_i$ pour $i \geq 1$.

Démonstration. — Comme $N/\mathfrak{K}$ est totalement ramifiée en $\mathfrak{R}$, $G_1 = G_0 = G$. Comme $A/\mathfrak{R}$ est de caractéristique p , les G_i , pour $i \geq 1$, sont des p -groupes. Comme $H_i = G_i \cap H$, $G_i = H_i$ pour $i \geq 1$. L'extension N/k n'étant pas modérément ramifiée en $\mathfrak{R}''$, H_1 n'est pas réduit à l'élément neutre, ce qui montre l'inégalité $t \geq 1$. Il reste à voir que t est impair. Pour cela, nous utiliserons le lemme suivant (C.L. Ch. IV, § 1, Prop. 2).

LEMME. — Soit L_1/L_2 une extension galoisienne, B un anneau de Dedekind ayant L_1 pour corps des fractions, $\mathfrak{R}$ un idéal premier non nul de B , G_i la suite des groupes de ramification de $\mathfrak{R}$. Soit $s \in G_0$, $s' \in G_i$, $s' \notin G_{i+1}$, avec $i \geq 1$. Alors,

$$ss's^{-1}s'^{-1} \in G_{i+1} \iff s'' \in G_1$$

(C.L. Ch. IV, § 2, Prop. 9, Cor. 1).

Nous allons appliquer ce lemme en prenant pour s un élément τ d'ordre 2 de G , et pour s' un élément σ de G_t , autre que l'élément neutre (un tel élément existe, par définition de t). Comme σ est d'ordre p dans G , $\tau\sigma\tau^{-1}\sigma^{-1} = \sigma^{-2} \neq 1$. Donc, $\tau\sigma\tau^{-1}\sigma^{-1} \notin G_{t+1}$, d'où l'on déduit que $\tau^t \notin G_1$, ce qui implique que t est impair.

Pour calculer le discriminant de N/k , nous aurons besoin de majorer l'entier t défini dans la proposition précédente. Nous parviendrons à ce but en utilisant l'hypothèse (H) et le lemme suivant :

LEMME III.1. — Soit A un anneau de Dedekind, K son corps des fractions, L une extension cyclique de K , de degré p . On suppose la caractéristique de K différente de p . Soit $\mathfrak{Q}$ un idéal premier non nul de A , totalement ramifié dans L , $\mathfrak{Q}'$ l'idéal de L au-dessus de $\mathfrak{Q}$, G_i la suite des groupes de ramification de $\mathfrak{Q}'$, t l'entier pour lequel $G_t \neq (1)$, $G_{t+1} = (1)$. On suppose que $\mathfrak{Q} | pA$, et l'on appelle e l'exposant de $\mathfrak{Q}$ dans pA ; alors, $1 \leq t \leq \left\lfloor \frac{pe}{p-1} \right\rfloor$, $[x]$ désignant la partie entière du nombre rationnel x .

Démonstration. — Comme $\mathfrak{Q}_{A_{L'}} = \mathfrak{Q}'^p$, L'/K' n'est pas modérément ramifiée en $\mathfrak{Q}$; donc, $t \geq 1$. Comme on ne change pas la suite des groupes de ramification de $\mathfrak{Q}'$ en localisant en $\mathfrak{Q}$, on peut supposer que A est un anneau de valuation discrète, d'idéal maximal $\mathfrak{Q}$. Comme $\text{Tr}_{L'/K'}(1) = p$, et $pA = \mathfrak{Q}^e$, $\text{Tr}_{L'/K'}(A_{L'}) \supset \mathfrak{Q}^e$. D'autre part, la différentielle $\mathcal{O}_{L'/K'}$ est $\mathcal{O}_{L'/K'} = \mathcal{O}'^{(t+1)(p-1)}$. (C.L. Ch. IV, § 1, Prop. 4). On a les implications suivantes :

$$\begin{aligned} t > \left\lfloor \frac{pe}{p-1} \right\rfloor &\implies t > \frac{pe}{p-1} \implies (t+1)(p-1) > pe + p - 1 \\ &\implies (t+1)(p-1) \geq p(e+1) \implies \\ &\qquad\qquad\qquad \mathfrak{Q}^{e+1} | \mathcal{O}_{L'/K'} \\ &\qquad\qquad\qquad (\text{car } \mathfrak{Q}^{e+1} A_{L'} = \mathfrak{Q}'^{p(e+1)}) \\ &\implies A_{L'} \subset \mathfrak{Q}^{e+1} \mathcal{O}_{L'/K'}^{-1} \\ &\implies \text{Tr}_{L'/K'}(A_{L'}) \subset \mathfrak{Q}^{e+1} \end{aligned}$$

(Ch. I, § V, Théorème I.6), ce qui contredit $\text{Tr}_{L'/K'}(A_{L'}) \supset \mathfrak{Q}^e$.

Nous sommes maintenant en mesure de préciser le discriminant de N/k , lorsque A vérifie l'hypothèse (H).

THEOREME III.1. — *Supposons l'hypothèse (H) vérifiée. Le discriminant $\mathcal{O}$ de N/k est alors la puissance $(p - 1)$ -ième d'un idéal $\mathfrak{Z}$ de A . Plus précisément,*

$$\mathfrak{Z} = \mathfrak{u} \left(\prod_{\substack{\mathfrak{P} \text{ ramifié dans} \\ \mathfrak{P} \nmid pA \ N/k \\ \mathfrak{P} \nmid d}} \mathfrak{P} \right) \left(\prod_{\substack{\mathfrak{P} \text{ ramifié dans} \\ \mathfrak{P} \mid pA \ N/k \\ \mathfrak{P} \nmid d}} \mathfrak{P}^2 \right) \left(\prod_{\substack{\mathfrak{P} \text{ totalement} \\ \text{ramifié} \\ \text{dans } N/k}} \mathfrak{P} \right),$$

$\mathfrak{u}$ désignant un idéal entier de A , produit d'idéaux premiers distincts de A totalement ramifiés (donc divisant pA) ; de plus, $\mathfrak{u} = A$ si $p \geq 5$.

Démonstration. — Il est clair qu'il suffit de démontrer le théorème lorsque A est un anneau de valuation discrète, en distinguant plusieurs cas suivant la ramification dans N de l'idéal maximal $\mathfrak{P}$ de A . Comme N/k est galoisienne, la différentielle $\mathcal{O}_{N/k}$ est un idéal de N , invariant par G . Par conséquent, si $\mathfrak{P}$ se décompose dans k sous la forme $\mathfrak{P}A_k = \mathfrak{P}_1 \mathfrak{P}_2$, $\mathfrak{P}_1$ et $\mathfrak{P}_2$ ont même exposant dans $\mathcal{O}$.

Cas 1.

$\mathfrak{P}$ ne divise pas pA . On voit (Proposition III.3) que, si $\mathfrak{P}$ se ramifie dans k , $\mathfrak{P}$ et $\mathcal{O}$ sont étrangers.

On est donc ramené à la situation suivante : $\mathfrak{P}$ ne divise pas dA , et, $\mathfrak{P}_1$ désignant un idéal de A_k au-dessus de $\mathfrak{P}$, $\mathfrak{P}_1 A_N = \mathfrak{P}'^p$. Comme N/k est modérément ramifiée en $\mathfrak{P}_1$ (car, $\mathfrak{P}_1$ ne divisant pas pA , la caractéristique de $A/\mathfrak{P}_1$ est distincte de p), l'exposant de $\mathfrak{P}_1$ dans $\mathcal{O}$ est égal à $p - 1$. Les idéaux de A_k au-dessus de $\mathfrak{P}$ ayant même exposant dans $\mathcal{O}$, $\mathcal{O} = \mathfrak{P}^{p-1}$.

Cas 2.

$\mathfrak{P} \mid pA$, $\mathfrak{P} \nmid dA$. Si $\mathfrak{P}$ ne se ramifie pas dans N , $\mathfrak{P}$ et $\mathcal{O}$ sont premiers entre eux. Si $\mathfrak{P}$ se ramifie dans N , et si $\mathfrak{P}_1$ désigne un idéal premier de A_k au-dessus de $\mathfrak{P}$, $\mathfrak{P}_1 A_N = \mathfrak{P}'^p$. L'exposant de $\mathfrak{P}_1$ dans $\mathcal{O}$ est $(t + 1)(p - 1)$, où t est l'entier pour lequel $H_t(\mathfrak{P}') \neq (1)$,

$H_{t+1}(\mathfrak{R}') = (1)$. On peut alors appliquer le lemme III.1, avec $e = 1$, car $\mathfrak{R}_1 | pA_k$, $\mathfrak{R}_1^2 \nmid pA_k$. On a donc $1 \leq t \leq \left\lfloor \frac{p}{p-1} \right\rfloor$, d'où $t = 1$, car $p \leq 3$.

L'exposant de $\mathfrak{R}_1$ dans $\mathcal{O}$ est donc $2(p-1)$, ce qui entraîne l'égalité

$$\mathcal{O} = \mathfrak{R}^{2(p-1)}.$$

Cas 3.

$\mathfrak{R} | pA$ et $\mathfrak{R} | dA$. Si $\mathfrak{R}$ n'est pas totalement ramifié, $\mathfrak{R}$ et $\mathcal{O}$ sont premiers entre eux. Supposons donc $\mathfrak{R}$ totalement ramifié, et posons $\mathfrak{R}A_k = \mathfrak{R}'^2$, $\mathfrak{R}'A_N = \mathfrak{R}''^p$. Avec les notations introduites dans le cas 2, $\mathcal{O} = \mathfrak{R}'^{(t+1)(p-1)}$. On sait que t est impair et ≥ 1 (proposition III.4). On peut donc écrire $\mathcal{O} = \mathfrak{R}'^{\frac{t+1}{2}(p-1)}$, ou encore $\mathcal{O} = \mathfrak{R}^{(p-1)} \mathfrak{u}^{p-1}$, avec $\mathfrak{u} = \mathfrak{R}'^{\frac{t-1}{2}}$. Mais $\mathfrak{R}A_k = \mathfrak{R}'^2$; donc, $\mathfrak{R}'^2 | pA_k$, $\mathfrak{R}'^3 \nmid pA_k$. On peut donc appliquer le lemme III.1, avec $e = 2$. On en déduit l'inégalité $t \leq \left\lfloor \frac{2p}{p-1} \right\rfloor$. Si $p = 3$, $\frac{2p}{p-1} = 3$; on a donc $t = 1$ ou $t = 3$, d'où $\mathfrak{u} = \mathfrak{R}$ ou $\mathfrak{u} = A$. Si $p \geq 5$, $\left\lfloor \frac{2p}{p-1} \right\rfloor = \left\lfloor 2 + \frac{2}{p-1} \right\rfloor = 2$; comme t est impair, $t = 1$, et $\mathfrak{u} = A$, ce qui achève de prouver le théorème.

Remarque 1. — Lorsque $p = 3$, l'éventualité $\mathfrak{u} \neq A$ se présente effectivement : c'est le "cas 9" dans [13].

Remarque 2. — Nous verrons au cours du chapitre IV comment calculer effectivement $\mathcal{O}$.

Remarque 3. — Si l'hypothèse (H) n'est pas vérifiée, pour tout idéal premier non nul $\mathfrak{R}'$ de A_k , l'exposant de $\mathfrak{R}'$ dans $\mathcal{O}$ est encore égal à $(p-1)(t+1)$, et $\mathcal{O}$ est donc toujours la puissance $(p-1)$ -ième d'un idéal $\mathfrak{Z}$ de A_k . Mais $\mathfrak{Z}$ est plus nécessairement un idéal de A .

COROLLAIRE.

$\bar{D} = d^p \mathfrak{Z}^{2(p-1)}$. En effet,

$$\bar{D} = \Delta(k/\kappa)^p N_{k/\kappa}(\omega) = d^p \omega^2 = d^p \mathfrak{Z}^{2(p-1)}$$

4. Ramification dans K.

PROPOSITION III.5. — (Ramification dans A_N des idéaux premiers de A_K).

Soit $\mathfrak{R}$ un idéal premier non nul de A , $\mathfrak{P}_i$ les idéaux premiers de A_K au-dessus de $\mathfrak{R}$. Alors, δ est divisible par l'un des $\mathfrak{P}_i$ si et seulement si $\mathfrak{R} \mid d$, et, si cette dernière condition est réalisée, un et un seul des $\mathfrak{P}_i$ divise δ . De plus, $N_{K/\kappa}(\delta) = d$.

Démonstration. — On peut supposer pour faire la démonstration que A est un anneau de valuation discrète. Si ω_1, ω_2 est une A -base de A_K , ω_1, ω_2 est une A_K -base d'un sous-anneau de A_N , car k et K sont linéairement disjointes. Il en résulte que $\delta \mid d$. Donc, si l'un des $\mathfrak{P}_i \mid \delta$, il divise aussi d et, par conséquent $\mathfrak{R} \mid d$.

Supposons donc que $\mathfrak{R} \mid d$. Si $\mathfrak{R} \mid \mathfrak{Z}$, $\mathfrak{R}A_N = \mathfrak{R}'^{2p}$, (cf. Théorème III.1) $\mathfrak{R}A_K = \mathfrak{R}'_1$, avec $\mathfrak{R}'_1 = \mathfrak{R}' \cap A_K$. De plus, $\mathfrak{R} \mid pA$ (Proposition III.3). Les extensions N/K et k/κ sont alors totalement et modérément ramifiées en $\mathfrak{R}$. On a donc $\delta = \mathfrak{R}_1$, $d = \mathfrak{R}$, et $d = N_{K/\kappa}(\delta)$, car, $\mathfrak{R}_1$ étant du premier degré, $N_{K/\kappa}(\mathfrak{R}_1) = \mathfrak{R}$. Supposons maintenant que $\mathfrak{R} \nmid \mathfrak{Z}$. On a alors $\mathfrak{R}A_K = \mathfrak{R}'^2$, $\mathfrak{R}'A_N = \prod_{\sigma \in H} \mathfrak{R}'_\sigma$, avec $\mathfrak{R}'_\sigma = \sigma \mathfrak{R}'_1$ (Pro-

position III.3). Les groupes de décomposition des $\mathfrak{R}'_\sigma$ sont des groupes d'ordre 2, conjugués de l'un d'entre eux. Quitte à modifier l'indexation des $\mathfrak{R}'_\sigma$, on peut supposer que K est le corps de décomposition de $\mathfrak{R}'_1$. Posons $\mathfrak{R}_1 = \mathfrak{R}'_1 \cap A_K$, $\mathfrak{R}_\sigma = N_{N/K}(\mathfrak{R}'_\sigma)$. Alors, dans K , $\mathfrak{R}A_K = \mathfrak{R}_1 \prod_{\sigma \neq 1} \mathfrak{R}_\sigma^2$,

le produit étant calculé pour σ parcourant les classes de conjugaison de H par G . $\mathfrak{R}_1$ se ramifie dans N , les $\mathfrak{R}_\sigma$ se décomposent pour $\sigma \neq 1$. Donc, $\mathfrak{R}_1 \mid \delta$, $\mathfrak{R}_\sigma \nmid \delta$ pour $\sigma \neq 1$. Lorsqu'on complète A , le complété $\hat{N}$ de N s'identifie à un produit de p corps quadratiques, et la clôture intégrale de A dans chacun de ces corps est un anneau de valuation discrète ayant pour idéal maximal le complété $\hat{\mathfrak{R}}'_i$ de $\mathfrak{R}'_i$ (C.L. Ch. II,

§ 3, Théorème I). L'égalité $d = N_{K/\kappa}(\delta)$ résulte alors de C.L., Ch. III, § 4, corollaire de la proposition 10.

THEOREME III.2. — *On suppose que A vérifie l'hypothèse (H).*

$$i) D = d^{\frac{p-1}{2}} \mathfrak{J}^{p-1}.$$

ii) *Un idéal maximal $\mathfrak{Q}$ de A se ramifie dans K si et seulement si $\mathfrak{Q} \mid D$. Si $\mathfrak{Q} \mid \mathfrak{J}$, $\mathfrak{Q}$ devient dans K la puissance p -ième d'un idéal premier. Si $\mathfrak{Q} \nmid d$, $\mathfrak{Q} \nmid \mathfrak{J}$, $\mathfrak{Q}$ se décompose dans K sous la forme $\mathfrak{Q}A_K = \mathfrak{P}_1 \mathfrak{P}_2 \dots \mathfrak{P}_{\frac{p+1}{2}}^2$, les $\mathfrak{P}_i$ étant des idéaux premiers de A_K deux à deux distincts.*

Démonstration :

$$i) \bar{D} = d^p \mathfrak{J}^{2(p-1)} = D^2 N_{K/\kappa}(\delta). \text{ On a donc}$$

$$D^2 = d^{p-1} \mathfrak{J}^{2(p-1)}, \text{ d'où } i).$$

ii) Le fait que les seuls idéaux de A ramifiés dans K sont ceux qui divisent D est évident ; le reste du théorème résulte trivialement des calculs effectués au cours des démonstrations des propositions III.3 et III.5.

5. Structure du A_k -module A_N .

THEOREME III.3. — *On suppose que A vérifie l'hypothèse (H).*

Alors, si A_K et A_k sont des A-modules libres, A_N est un A_k -module libre ; en particulier, si A est principal, A_N est A_k -libre.

La démonstration de ce théorème s'appuiera sur le

LEMME III.2. — *Soit L une extension quadratique séparable de κ , B la clôture intégrale de A dans L. Alors, si B est un A-module libre, la différentielle $\mathcal{O}_{L/\kappa}$ est un idéal principal de B.*

Démonstration du lemme :

Cas 1.

La caractéristique de κ est différente de 2. On peut écrire $L = \kappa(\theta)$, avec $\theta^2 = m \in \kappa$. Le discriminant du réseau $A + A\theta$ de L est égal à $4m$; comme B est A -libre, $d/(4m)$ est le carré d'un idéal principal de A (Théorème d'Artin). Comme $4m = (2\theta)^2$ et $d = \mathfrak{O}_{L/\kappa}^2$, $\mathfrak{O}_{L/\kappa}$ est bien un idéal principal de B .

Cas 2.

κ est de caractéristique 2. Comme L/κ est séparable, on peut écrire $L = \kappa(\theta)$, θ étant racine d'une équation $x^2 + ax + b = 0$, dans laquelle $a \neq 0$. Le discriminant du réseau $A + A\theta$ de L est $4b - a^2 = a^2$, ce qui prouve que d/a^2 est le carré d'un idéal principal de A , donc que $\mathfrak{O}_{L/\kappa}$ est un idéal principal de A .

Démonstration du théorème. — Soit $\omega_1, \dots, \omega_p$ une A -base de A_K . Le réseau $A_K \omega_1 + \dots + A_K \omega_p$ de N par rapport à A_K a pour discriminant $D = d^{\frac{p-1}{2}} \mathfrak{F}^{p-1}$. Le discriminant de A_N par rapport à A_K est $\mathfrak{F}^{p-1}$. Le quotient de ces deux discriminants est $d^{\frac{p-1}{2}}$, ce qu'on peut encore écrire $\mathfrak{O}_{K/\kappa}^{p-1} = \left((\mathfrak{O}_{K/\kappa})^{\frac{p-1}{2}} \right)^2$. Comme $\mathfrak{O}_{K/\kappa}$ est un idéal principal, le théorème d'Artin montre que A_N est un A_K -module libre.

Si A est principal, A_K et A_K , qui sont des A -modules de type fini, sans torsion, sont libres et A_N est bien un A_K -module libre.

Remarque 1. — Le théorème d'Artin montre que, si A_K est un A -module libre, A_N est un A_K -module libre si et seulement si d/δ est le carré d'un idéal principal de A_K . Cette condition peut ne pas être réalisée, même si A est principal. Pour un exemple, voir [13], Ch. II, § 2, exemple.

Remarque 2. — Le problème de la recherche de bases de A_N/A_K est traité dans [14], lorsque $p = 3$, A étant l'anneau $\mathbb{Z}$ des entiers rationnels.

Le tableau suivant résume les décompositions possibles dans k , N et K d'un idéal premier non nul de A .

Idéal maximal $\mathfrak{P}$ de A	Décomposition dans A_k	Décomposition dans A_N	Décomposition dans A_K
$\mathfrak{P} \mid d$ $\mathfrak{P} \mid \mathfrak{F} \implies \mathfrak{P} \mid pA$	$\mathfrak{P}'^2$	$\mathfrak{P}'^{2p}_1$	$\mathfrak{P}_1^p$
$\mathfrak{P} \mid d$ $\mathfrak{P} \nmid \mathfrak{F}$	$\mathfrak{P}'^2$	$\mathfrak{P}'^2_1 \dots \mathfrak{P}'^2_p$	$\mathfrak{P}_1 \mathfrak{P}_2 \dots \mathfrak{P}_{\frac{p+1}{2}}^2$
$\mathfrak{P} \nmid d$ $\mathfrak{P} \mid \mathfrak{F}$	$\mathfrak{P}'$	$\mathfrak{P}'^p_1$	$\mathfrak{P}_1^p$
	$\mathfrak{P}'\mathfrak{P}''$	$\mathfrak{P}'^p_1 \mathfrak{P}''^p_1$	
$\mathfrak{P}$ non ramifié dans N	$\mathfrak{P}'$	$\mathfrak{P}_1^{(1)}$	$\mathfrak{P}_1$
		$\mathfrak{P}'_1 \dots \mathfrak{P}'^{(2)}_p$	$\mathfrak{P}_1 \mathfrak{P}_2 \dots \mathfrak{P}_{\frac{p+1}{2}}^{(3)}$
	$\mathfrak{P}'\mathfrak{P}''$	$\mathfrak{P}'_1 \mathfrak{P}''_1$	$\mathfrak{P}_1$
		$\mathfrak{P}'_1 \dots \mathfrak{P}'_p \mathfrak{P}''_1 \dots \mathfrak{P}''_p$	$\mathfrak{P}_1 \dots \mathfrak{P}_p$

⁽¹⁾ Cette éventualité ne peut pas se produire lorsque $A/\mathfrak{P}$ est un corps quasi-fini (en particulier fini). C'est par exemple le cas lorsque A est l'anneau des entiers d'un corps de nombres. Par contre, $\mathfrak{P}$ reste premier lorsque A est un anneau de polynôme à une variable sur un corps, et N provient d'une extension du corps des constantes.

⁽²⁾ Les idéaux $\mathfrak{P}'_1, \dots, \mathfrak{P}'_p$ sont de degré 2.

⁽³⁾ On peut supposer que $\mathfrak{P}_1$ est de degré 1, $\mathfrak{P}_2, \dots, \mathfrak{P}_{\frac{p+1}{2}}$ étant de degré 2.

L'idéal $\mathfrak{P}_1$ reste alors premier dans A_N , devenant de degré 2. Les idéaux $\mathfrak{P}_2, \dots, \mathfrak{P}_{\frac{p+1}{2}}$, au contraire, se décomposent dans A_N en un produit de deux idéaux premiers du second degré.

CHAPITRE IV

ADJONCTION DES RACINES DE L'UNITÉ

On conserve les notations du chapitre III. Dans tout ce chapitre, nous supposons en outre que κ vérifie l'hypothèse (H'). Rappelons que, pour un corps L , L' désigne l'extension de L obtenue en adjoignant à L les racines p -ièmes de l'unité. L'hypothèse (H') signifie que l'on a $[\kappa' : \kappa] = p - 1$.

Nous supposerons en outre que κ n'est pas de caractéristique 2.

1. Le corps N' .

DEFINITION IV.1. — On désigne par κ'_0 la sous-extension de κ'/κ de degré $\frac{p-1}{2}$ sur κ .

On a donc $[\kappa' : \kappa'_0] = 2$. Nous poserons, pour alléger l'écriture, $A_{\kappa'} = A'$ et $A_{\kappa'_0} = A'_0$.

Remarque. — Si $\kappa = \mathbb{Q}$, κ'_0 est le sous-corps réel maximal de $\mathbb{Q}'$.

Nous allons maintenant distinguer deux cas, selon que k et κ' sont ou ne sont pas des extensions linéairement disjointes de κ ; mais, dans tous les cas, nous notons G' le groupe de Galois de N'/κ .

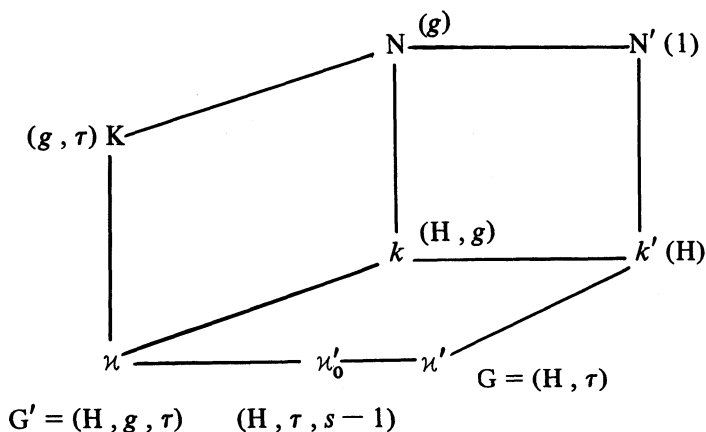
Cas A. k n'est pas un sous-corps de κ' .

Le groupe de Galois de N'/κ' est canoniquement isomorphe par restriction au groupe de Galois G de N/κ ; dans cet isomorphisme, le groupe de Galois de N'/k' a pour image H . Nous convenons de noter encore G le groupe de Galois de N'/κ' et H celui de N'/k' . Nous notons τ l'élément d'ordre 2 de G laissant fixe K' , et g le groupe de Galois de N'/N . Le groupe g est canoniquement isomorphe par restriction au groupe de Galois de κ'/κ ; il est donc cyclique d'ordre $p - 1$. Pour tout $i \not\equiv 0 \pmod{p}$, il existe un élément et un seul de g ,

noté s_i , vérifiant $s_i \omega = \omega^i$ pour toute racine p -ième de l'unité ω de N' .

L'application $i \rightarrow s_i$ est un isomorphisme de $(\mathbb{Z}/p\mathbb{Z})^*$ sur g . Le groupe G' est isomorphe au produit direct de G et g , et g est le centre de G' .

Le graphique suivant résume la situation. A côté de chaque corps figure le sous-groupe de G' auquel il appartient :



On peut définir G' par trois générateurs : σ_0 engendrant H , s engendrant g , et τ , et six relations :

$$\begin{aligned} \sigma_0^p &= 1 & \tau^2 &= 1 & s^{p-1} &= 1 \\ \tau \sigma_0 &= \sigma_0^{-1} \tau & s \sigma_0 &= \sigma_0 s & \tau s &= s \tau. \end{aligned}$$

Dans la suite, nous serons amenés à distinguer 2 cas suivant que p est congru à 1 ou $-1 \pmod{4}$. Ces cas seront notés respectivement A_1 et A_2 .

Cas B. k est un sous-corps de ν' .

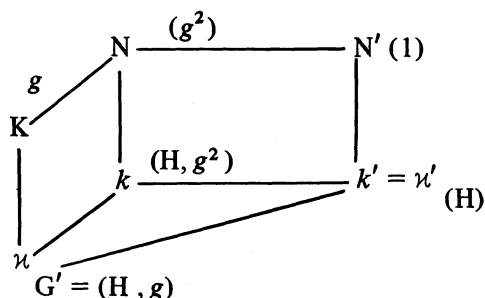
On a alors $k' = \nu'$. Le groupe de Galois de N'/k' est canoniquement isomorphe par restriction au groupe de Galois H de N/k ; on notera encore H le groupe de Galois de N'/k' . Le groupe de Galois g de N'/K est canoniquement isomorphe par restriction au groupe

de Galois de κ'/κ . On notera encore s_i ses éléments, s_i étant caractérisé par $s_i \omega = \omega^i$ pour toute racine p -ième de l'unité ω . Le groupe G' est produit semi-direct de son sous-groupe distingué H par g , ce dernier opérant sur H par $s h s^{-1} = h$ si $s \in g^2$, $s h s^{-1} = h^{-1}$ si $s \in g$, $s \notin g^2$. Il résulte de cette remarque que le centre de G' est cette fois g^2 (ensemble des carrés des éléments de g), et a N pour corps des invariants. Le groupe g lui-même n'est pas distingué dans G' .

Si $p \equiv 1 \pmod{4}$, G' ne contient aucun sous-groupe isomorphe à G , car les éléments d'ordre 2 de G' sont visiblement dans g^2 , donc dans le centre de G' . Ce cas sera désigné dans la suite par "*cas B₁*".

Si $p \equiv 3 \pmod{4}$, g contient un élément d'ordre 2, à savoir s_{-1} , qui n'est pas dans le centre de G' . Le sous-groupe de G' engendré par H et s_{-1} , est isomorphe à G . Son corps des invariants est le sous-corps κ'_0 de κ' de degré $\frac{p-1}{2}$ sur κ . Ce cas sera désigné par "*cas B₂*".

Le graphique suivant résume la situation. A côté de chaque corps figure le sous-groupe de G' auquel il appartient :



On peut définir G' par deux générateurs : σ_0 engendrant H et s engendrant g , et trois relations :

$$\sigma_0^p = 1 \quad s^{p-1} = 1 \quad s\sigma = \sigma^{-1}s.$$

Remarque 1. — Dans le cas B, k est le corps $\kappa(\sqrt[p]{(-1)^{\frac{p-1}{2}}})$.

Remarque 2. — Dans le cas B_1 , k est un sous-corps de κ'_0 . Dans le cas B_2 , k n'est pas inclus dans κ'_0 , et κ' est le corps composé de k et de κ'_0 .

2. Résolvantes de Lagrange.

Notons H^* le groupe des caractères de H à valeurs dans le groupe multiplicatif de κ' ; c'est un groupe d'ordre p . Désignons par χ_0 le caractère trivial; on a donc $\chi_0(\sigma) = 1$ pour tout $\sigma \in H$.

DEFINITION IV.2. — Soit $\theta \in N'$, $\chi \in H^*$. On appelle *résolvante de Lagrange de θ et de χ* , et l'on note $\langle \theta, \chi \rangle$ l'expression :

$$\langle \theta, \chi \rangle = \sum_{\sigma \in H} \chi(\sigma^{-1}) (\sigma\theta).$$

Pour pouvoir écrire commodément les formules relatives aux résolvantes de Lagrange, nous introduisons la

DEFINITION IV.3. — Soit i un entier, $i \not\equiv 0 \pmod{p}$. On appelle *i' l'entier défini de la manière suivante :*

- Dans le cas A, $i' = i$
- Dans le cas B, $i' = i$ si i est reste quadratique mod p
 $i' = -i$ si i n'est pas reste quadratique.

Remarque. — si $\sigma \in H$

$$s_i \sigma = \sigma s_i \quad \text{si} \quad i = i', \quad s_i \sigma = \sigma^{-1} s_i \quad \text{si} \quad i = -i'.$$

PROPOSITION IV.1. — On a les formules suivantes :

- (a) $\langle \theta, \chi_0 \rangle = \text{Tr}_{N'/k'}(\theta)$
- (b) $\sigma \langle \theta, \chi \rangle = \langle \sigma\theta, \chi \rangle = \chi(\sigma) \langle \theta, \chi \rangle$ pour tout $\sigma \in H$
- (c) $\theta = \frac{1}{p} \sum_{\chi \in H^*} \langle \theta, \chi \rangle \chi = \frac{1}{p} \left(\text{Tr}_{N'/k'} \theta + \sum_{\chi \neq \chi_0} \langle \theta, \chi \rangle \chi \right)$
- (d) si $\theta \in K$, $s_i \langle \theta, \chi \rangle = \langle \theta, \chi^{i'} \rangle$

(e) Dans le cas A, si $\theta \in K$, $\tau < \theta$, $\chi > = < \theta, \chi^{-1} >$

(f) Dans le cas A, si $\theta \in K$, $\tau s_{-1} < \theta$, $\chi > = < \theta, \chi >$

La démonstration de ces formules découle simplement des définitions et de la remarque suivant la définition IV.3.

PROPOSITION IV.2 — Soit $\theta \in N$.

Les conditions suivantes sont équivalentes :

i) $(\sigma\theta)_{\sigma \in H}$ est une k -base normale de N .

ii) $< \theta, \chi > \neq 0$ pour tout $\chi \in H^*$.

De plus, il existe des $\theta \in K$ tels que $(\sigma\theta)_{\sigma \in H}$ soit une k -base normale de N .

Pour une démonstration, voir [17], § III, lemme 5.

Remarque. — Si $\theta \in K$ vérifie les conditions équivalentes de la proposition IV.2, $\text{Tr}_{K/k}(\theta) \neq 0$, et $K = \kappa(\theta)$. Réciproquement, dans les cas A et B_1 , les conditions $\text{Tr}_{K/k}(\theta) \neq 0$ et $K = \kappa(\theta)$ entraînent que $(\sigma\theta)_{\sigma \in H}$ est une base normale de N/k . Mais ceci n'est pas exact dans le cas B_2 .

3. Le corps $\tilde{k}$.

DEFINITION IV.4. — $\tilde{k}$ désigne l'extension de κ engendrée par les puissances p -ième des résolvantes de Lagrange des éléments de K .

Remarque. — Cette définition est conforme à celle de [13], Chapitre I, § 1, ainsi qu'à celle de [17], § III, comme il est facile de le voir.

La proposition suivante caractérise l'extension $\tilde{k}$ parmi les sous-extensions de N' .

PROPOSITION IV.3. — Soit θ_0 un élément de K , tel que les $(\sigma\theta_0)_{\sigma \in H}$ forment une base normale de N/k , et soit χ_0 le caractère trivial.

a) Pour tout $\chi \neq \chi_0$, $\langle \theta_0, \chi \rangle^p$ est un élément primitif de l'extension $\tilde{k}/\mathfrak{N}$.

b) Dans les cas A et B_1 , les $\langle \theta_0, \chi \rangle^p$, $\chi \in H^*$, $\chi \neq \chi_0$, sont les éléments conjugués de $\tilde{k}/\mathfrak{N}$; dans le cas B_2 , χ_1 désignant un caractère non trivial, les $\langle \theta, \chi \rangle^p$ sont conjugués de $\langle \theta, \chi_1 \rangle^p$ ou de $\langle \theta, \chi_1^{-1} \rangle^p$, $\langle \theta, \chi_1 \rangle^p$ et $\langle \theta, \chi_1^{-1} \rangle^p$ n'étant pas eux-mêmes conjugués.

c) Dans les cas B_1 (resp. B_2), on a $\tilde{k} = \mathfrak{N}'$ (resp. $\tilde{k} = \mathfrak{N}'_0$).

d) Dans le cas A, $\tilde{k}$ est le sous-corps de k' fixe par $s_{-1}\tau$.

e) Dans tous les cas, $\tilde{k}$ est une extension de $\mathfrak{N}'_0$.

Pour prouver cette proposition, nous établissons auparavant le

LEMME IV.1. — Soit θ_0 un élément de K , tel que les $(\sigma\theta_0)_{\sigma \in H}$ constituent une k -base normale de N , et soient χ et χ' deux caractères distincts; alors les éléments $\langle \theta_0, \chi \rangle^p$ et $\langle \theta_0, \chi' \rangle^p$ de $\tilde{k}$ sont distincts.

Démonstration du lemme. — Supposons que l'on ait

$$\langle \theta_0, \chi \rangle^p = \langle \theta_0, \chi' \rangle^p.$$

Alors, il existe une racine p -ième de l'unité ω telle que l'on ait dans N' l'égalité $\langle \theta_0, \chi \rangle = \omega \langle \theta_0, \chi' \rangle$. En faisant opérer H , et en utilisant la proposition IV.1, b), on voit que cette égalité entraîne que l'on a l'égalité $\chi(\sigma) = \chi'(\sigma)$ pour tout $\sigma \in H$, d'où $\chi = \chi'$.

Démonstration de la proposition IV.3. — La proposition IV.1, b) montre que, dans tous les cas, $\tilde{k}$ est un sous-corps de k' . Étudions d'abord le cas A. La formule (f) de la proposition IV.1 montre immédiatement que $\tilde{k}$ est fixe par $s_{-1}\tau$; on en déduit l'inégalité $[\tilde{k} : \mathfrak{N}] \leq p - 1$. La formule (d) de la proposition IV.1 peut s'écrire dans le cas A sous la forme $s_i \langle \theta, \chi \rangle = \langle \theta, \chi' \rangle$; appliquée à un caractère $\chi_1 \neq \chi_0$, elle montre que les $\langle \theta, \chi \rangle^p$, $\chi \neq \chi_0$ sont conjugués de l'un d'entre eux. Le lemme IV.1, entraîne alors que l'on a $[\tilde{k} : \mathfrak{N}] \geq p - 1$, ce qui prouve (a), (b) et la première partie de l'assertion (d) dans le cas A. De plus, on voit que le groupe de Galois de $\tilde{k}/\mathfrak{N}$ est canoniquement isomorphe par restriction à g , d'où le fait que $\tilde{k}/\mathfrak{N}$ est cyclique de degré $p - 1$.

Enfin, (e) résulte de ce que κ'_0 est fixe à la fois par τ et s_{-1} .

Etudions maintenant les cas B_1 . Comme $p \equiv 1 \pmod{4}$, l'application $i \longrightarrow i'$ est un automorphisme de $(\mathbb{Z}/p\mathbb{Z})^*$.

La formule $s_i \langle \theta, \chi \rangle = \langle \theta, \chi^{i'} \rangle$ permet de montrer comme ci-dessus que les $\langle \theta, \chi \rangle^p$, $\chi \neq \chi_0$, sont distincts. La démonstration se poursuit alors comme dans le cas A.

Il reste à étudier le cas B_2 . Si i est reste quadratique modulo p , $i' = i$, et $s_i \langle \theta_0, \chi \rangle = \langle \theta_0, \chi^i \rangle$. Comme il y a $\frac{p-1}{2}$ reste quadratique modulo p , $[\tilde{k} : \theta] \geq \frac{p-1}{2}$. Mais $s_{-1} \langle \theta, \chi \rangle = \langle \theta, \chi \rangle$ quels que soient θ et χ . On a donc $\tilde{k} \subset \kappa'_0$, d'où $\tilde{k} = \kappa'_0$; il ne reste plus qu'à prouver l'assertion (b), et cela ne présente aucune difficulté.

PROPOSITION IV.4. — Soit $\theta \in K$ et soient χ et $\chi' \in H^*$.

a) si $\langle \theta, \chi\chi' \rangle \neq 0$, $\frac{\langle \theta, \chi \rangle \langle \theta, \chi' \rangle}{\langle \theta, \chi\chi' \rangle} \in \tilde{k}$. En particulier, si $\langle \theta, \chi \rangle \neq 0$, $\frac{\langle \theta, \chi^i \rangle}{\langle \theta, \chi \rangle^i} \in \tilde{k}$.

b) si θ' est un autre élément de K , et si $\langle \theta, \chi \rangle \neq 0$, alors $\frac{\langle \theta', \chi \rangle}{\langle \theta, \chi \rangle}$ est un élément de $\tilde{k}$.

La démonstration résulte immédiatement de la détermination de $\tilde{k}$ effectuée dans la proposition IV.3.

PROPOSITION IV.5. — Soit $\theta_0 \in K$, formant avec ses conjugués une base normale de N/k . Alors, l'application $\chi \longrightarrow \langle \theta_0, \chi \rangle^p$ définit par passage au quotient un isomorphisme de H^* sur un sous-groupe de $\tilde{k}^*/\tilde{k}^{*p}$, et cet isomorphisme ne dépend pas du choix de θ_0 .

Démonstration. — Le fait que l'application $\chi \longrightarrow \langle \theta_0, \chi \rangle^p$ de H^* dans $\tilde{k}^*/\tilde{k}^{*p}$ est un homomorphisme résulte de la proposition IV.4,a) ; le fait que cette application ne dépende pas du choix de θ_0 résulte de la proposition IV.4,b) ; enfin, le lemme IV.1 prouve que l'application est injective.

PROPOSITION IV.6. — Soit ω une racine primitive p -ième de l'unité, et soit φ un élément primitif de $k/\mathfrak{K}$, tel que $\varphi^2 \in \mathfrak{K}$. Alors, dans le cas A, $\tilde{k} = \mathfrak{K}((\omega - \omega^{-1})\varphi)$.

Démonstration.

$$\tau s_{-1}(\omega - \omega^{-1})\varphi = s_{-1}(\omega - \omega^{-1}) \cdot \tau\varphi = (\omega^{-1} - \omega) \cdot (-\varphi) = (\omega - \omega^{-1})\varphi.$$

Donc, $(\omega - \omega^{-1})\varphi \in \tilde{k}$. Comme $[(\omega - \omega^{-1})\varphi]^2$ est visiblement un élément primitif de $\mathfrak{K}'_0/\mathfrak{K}$, et que $(\omega - \omega^{-1})\varphi$ change de signe par s_{-1} , $(\omega - \omega^{-1})\varphi \notin \mathfrak{K}'_0$. Donc, $(\omega - \omega^{-1})\varphi$ est bien un élément primitif de $\tilde{k}/\mathfrak{K}$.

Remarque sur le corps $\tilde{k}$. — Il résulte de la détermination de $\tilde{k}$ faite dans les propositions IV.3 et IV.6 que $\tilde{k}$ ne dépend que de k , dans le sens suivant : si N_1 est une extension de $\mathfrak{K}$, galoisienne, non abélienne, de degré $2p$, et si K_1 est un sous-corps de degré p de N_1 , les puissances p -ièmes des résolvantes de Lagrange des éléments de K_1 engendrent le même corps que les puissances p -ièmes des résolvantes de Lagrange des éléments de K . Cela justifie a posteriori la notation $\tilde{k}$.

4. Discriminant de $\tilde{k}$.

Dans ce paragraphe, on suppose que A vérifie l'hypothèse (H). Bien entendu, on suppose toujours que $\mathfrak{K}$ vérifie l'hypothèse (H'). Rappelons qu'on a posé $A_{\mathfrak{K}'} = A'$, $A_{\mathfrak{K}'_0} = A'_0$. Nous poserons en outre $A_{\tilde{k}} = \tilde{A}$.

PROPOSITION IV.7. — Soit $\mathfrak{P}'_0$ un idéal premier non nul de A'_0 , $\mathfrak{P} = \mathfrak{P}'_0 \cap A$.

a) Si $\mathfrak{P} \nmid pA$, l'exposant de $\mathfrak{P}'_0$ dans $\Delta(\tilde{k}/\mathfrak{K}'_0)$ est égal à l'exposant de $\mathfrak{P}$ dans d .

b) Si $\mathfrak{P} \mid pA$, l'exposant de $\mathfrak{P}'_0$ dans $\Delta(\tilde{k}/\mathfrak{K}'_0)$ est égal à 1 si $\mathfrak{P} \nmid d$ ou si $p \equiv 1 \pmod{4}$, à 0 si $\mathfrak{P} \mid d$ et $p \equiv 3 \pmod{4}$.

Démonstration :

1. Cas B_2 .

On a $\tilde{k} = \kappa'_0$, et $\Delta(\tilde{k}/\kappa'_0) = A'_0$. Comme $p \equiv 3 \pmod{4}$, $k = \kappa(\sqrt{-p})$ et $d = p$. Donc, si $\mathfrak{R} \nmid pA$, $\mathfrak{R} \nmid d$ et a) est vérifiée. Si $\mathfrak{R} \mid pA$, on a évidemment $\mathfrak{R} \mid d$, car $d = pA$, et $p \equiv 3 \pmod{4}$, d'où b).

2. Cas B_1 .

Nous remarquons que $A' = A'_0[\omega]$. En effet,

$$\Delta_{\kappa'/\kappa'_0}(A'_0 + A'_0\omega) = (\omega - \omega^{-1})^2$$

est un idéal premier de A'_0 . Comme $A'_0[\omega] \subset A'$, $A' = A'_0[\omega]$.

Si $\mathfrak{R} \nmid pA$, $\mathfrak{R}'_0$ ne se ramifie pas dans $\tilde{A}$ (car $\tilde{A} = A'$, et

$$\mathfrak{R}'_0 \nmid (\omega - \omega^{-1})^2),$$

et $\mathfrak{R}'_0 \nmid d$, car $d = pA$.

Si $\mathfrak{R} \mid pA$, $\mathfrak{R}'_0$ se ramifie. A cause de l'hypothèse (H), $\mathfrak{R} \mid d$, $\mathfrak{R}^2 \nmid d$, et $\mathfrak{R}'_0 \mid (\omega - \omega^{-1})^2$, $\mathfrak{R}'_0{}^2 \nmid (\omega - \omega^{-1})^2$. Comme $p \equiv 1 \pmod{4}$, l'exposant de $\mathfrak{R}'_0$ dans $\Delta(\tilde{k}/\kappa'_0)$ a bien la valeur cherchée.

3. Cas A.

On se ramène immédiatement au cas où A est un anneau de valuation discrète, ayant $\mathfrak{R}$ pour idéal maximal.

a) Si $\mathfrak{R} \nmid pA$, $\Delta(\kappa'/\kappa) = A$. Comme $\mathfrak{R}$ ne se ramifie pas dans κ' , $\Delta(k'/\kappa') = d$. On a donc $\Delta(k'/\kappa) = N_{\kappa'/\kappa}(d) = d^{p-1}$. Mais $k' = \tilde{k}(\omega)$.

Donc, $\Delta(\tilde{k}/k) = \tilde{A}$, et $\Delta(\tilde{k}/\kappa)^2 = d^{p-1}$. On a donc $\Delta(\tilde{k}/\kappa) = d^{\frac{p-1}{2}}$ et

$\Delta(\tilde{k}/\kappa) = N_{\kappa'_0/\kappa}(\Delta(\tilde{k}/\kappa'_0)) \Delta(\kappa'_0/\kappa)^{\frac{p-1}{2}}$, ce qui entraîne

$$N_{\kappa'_0/\kappa}(\Delta(\tilde{k}/\kappa'_0)) = d^{\frac{p-1}{2}}.$$

Comme $\tilde{k}/\kappa$ est galoisienne, les différents idéaux de A'_0 ont même exposant dans $\Delta(\tilde{k}/\kappa'_0)$. On a donc $N_{\kappa'_0/\kappa}(\Delta(\tilde{k}/\kappa'_0)) = \Delta(\tilde{k}/\kappa'_0)^{\frac{p-1}{2}}$, d'où $\Delta(\tilde{k}/\kappa'_0) = d$, ce qui prouve a).

b) Si $\mathcal{R} \mid pA$, alors $\mathcal{R} = pA$, à cause de l'hypothèse (H). Le corps $A/\mathcal{R}$ est de caractéristique p ; donc, $\tilde{k}/\kappa'_0$ est modérément ramifiée. L'exposant de $\mathcal{R}'_0$ dans $\Delta(\tilde{k}/\kappa'_0)$ est par conséquent 0 ou 1. On peut écrire $A_k = A[\sqrt{m}]$, pour un m convenable. Si $\mathcal{R} \nmid d$, $\mathcal{R} \nmid m$. L'exposant de $\mathcal{R}'_0$ dans $m(\omega - \omega^{-1})^2$ est alors égal à 1. L'exposant de $\mathcal{R}'_0$ dans $\Delta(\tilde{k}/\kappa'_0)$ ne peut alors être égal qu'à 1. Si $\mathcal{R} \mid d$, l'exposant de $\mathcal{R}'_0$ dans m est alors $\frac{p-1}{2}$ (car $\mathcal{R} \mid m$, $\mathcal{R}^2 \nmid m$). L'exposant de $\mathcal{R}'_0$

dans $m(\omega - \omega^{-1})^2$ est égal à $\frac{p-1}{2} + 1 = \frac{p+1}{2}$, et a même parité que l'exposant de $\mathcal{R}'_0$ dans $\Delta(\tilde{k}/\kappa'_0)$ (car $m(\omega - \omega^{-1})^2$ est le discriminant du réseau $A'_0 + A'_0(\omega - \omega^{-1})\sqrt{m}$ contenu dans $\tilde{A}$). L'exposant cherché vaut donc 1 si $p \equiv 1 \pmod{4}$, 0 si $p \equiv 3 \pmod{4}$.

Grâce à la proposition précédente, on peut donner une expression du discriminant $\Delta(\tilde{k}/\kappa'_0)$. On trouve facilement dans le cas :

$$\text{cas } A_1 (p \equiv 1 \pmod{4}) : \Delta(\tilde{k}/\kappa'_0) = d \prod_{\mathfrak{r}'_0 \mid pA'_0} \mathcal{R}'_0 \prod_{\substack{\mathfrak{r}'_0 \mid pA'_0 \\ \mathfrak{r}'_0 \nmid dA'_0}} \mathcal{R}'_0^{-\frac{p-1}{2}}$$

$$\text{cas } A_2 (p \equiv 3 \pmod{4}) : \Delta(\tilde{k}/\kappa'_0) = d \prod_{\substack{\mathfrak{r}'_0 \mid pA'_0 \\ \mathfrak{r}'_0 \nmid dA'_0}} \mathcal{R}'_0 \prod_{\mathfrak{r}'_0 \mid pA'_0} \mathcal{R}'_0^{-\frac{p-1}{2}}$$

Afin d'obtenir une écriture unique valable dans les cas A_1 et A_2 ,

$$\text{nous posons } t(p) = \begin{cases} \frac{p-1}{4} & \text{si } p \equiv 1 \pmod{4} \\ \frac{p+1}{4} & \text{si } p \equiv 3 \pmod{4}. \end{cases}$$

Comme $\prod_{\mathfrak{r}'_0 \mid pA'_0} \mathcal{R}'_0$ est l'idéal principal $(\omega - \omega^{-1})^2 A'_0$, on trouve la formule suivante :

$$\Delta(\tilde{k}/\kappa'_0) = d(\omega - \omega^{-1})^2 \left(\prod_{\substack{\mathfrak{r}'_0 \mid pA'_0 \\ \mathfrak{r}'_0 \nmid dA'_0}} \mathcal{R}'_0 \right)^{-2t(p)}$$

Nous allons appliquer les calculs de discriminants ci-dessus à l'étude de $\tilde{A}$ considéré comme A'_0 -module. Rappelons, qu'étant donné

un réseau X relativement à un anneau de Dedekind A , on a défini la classe de ce réseau ($\text{Cl}(X)$, ou $\text{cl}_A(X)$ si l'on désire préciser A) (Chapitre I, définition I.3). Si A' est un anneau de Dedekind contenant A , qui est un A -module de type fini, et si h est une classe d'idéaux de A , on associe à h une classe d'idéaux de A' de la façon suivante : on prend un idéal $\mathfrak{u}$ de h , et on associe à h la classe dans A' de l'idéal $(\mathfrak{u}A')$. Avec cette convention, on peut énoncer le

THEOREME IV.1.

a) Dans le cas B , $\tilde{A}$ est un A'_0 -module libre.

b) Dans le cas A ,

$$\text{cl}_{A'_0}(\tilde{A}) = \text{cl}_A(A_k) \text{cl}_{A'_0} \left(\begin{array}{c|c} \prod \mathfrak{P}'_0 & \\ \hline \mathfrak{x}'_0 & pA'_0 \\ \mathfrak{x}'_0 & dA'_0 \end{array} \right)^{-1(p)}$$

c) Si A est un anneau principal, et si l'une des hypothèses suivantes est réalisée :

1) p est inversible dans A .

2) pA est un idéal maximal de A .

Alors, $\tilde{A}$ est un A'_0 -module libre.

Démonstration :

a) Dans le cas B_2 , $\tilde{k} = \kappa'_0$ et $\tilde{A} = A'_0$; il n'y a donc rien à démontrer. Dans le cas B_1 , $\tilde{k} = \kappa'$, $\tilde{A} = A'$. On vérifie facilement que $A' = A'_0[\omega]$, ce qui montre que A' est un A'_0 -module libre, ayant pour base $(1, \omega)$.

b) On écrit $k = \kappa(\varphi)$, où φ est tel que $\varphi^2 = m \in \mathfrak{u}$ et l'on pose $\varphi' = (\omega - \omega^{-1})\varphi$. On a alors $\tilde{k} = \kappa'_0(\varphi')$ (Proposition IV.6) ; de plus, $X = A'_0 + A'_0\varphi'$ est un réseau libre de $\tilde{k}$ par rapport à A'_0 , dont le discriminant est $\Delta(X) = 4\varphi^2 = 4m(\omega - \omega^{-1})^2$. Par ailleurs $A + A\varphi$ est un réseau libre de k par rapport à A , de discriminant $4\varphi^2 = 4m$. Le quotient $d/4m$ est le carré d'un idéal fractionnaire $\mathfrak{u}$ de A , et le théorème I.4 (théorème d'Artin) montre que $\text{cl}_A(A_k) = \text{cl}_A(\mathfrak{u})$.

De même, le quotient $\frac{\Delta(\tilde{k}/\kappa'_0)}{\Delta(X)}$ est le carré d'un idéal fractionnaire $\mathfrak{B}$ de A'_0 , et le théorème d'Artin montre que $\text{cl}_{A'_0}(\tilde{A}) = \text{Cl}_{A'_0}(\mathfrak{B})$. En

utilisant le calcul du discriminant de $\tilde{k}$ par rapport à κ'_0 , on trouve $\mathfrak{z}^2 = \frac{d}{4m} \left(\prod_{\substack{\mathfrak{x}'_0 | pA'_0 \\ \mathfrak{x}'_0 | dA'_0}} \mathfrak{D}'_0 \right)^{-2t}$, d'où $\mathfrak{z} = \mathfrak{u} \left(\prod_{\substack{\mathfrak{x}'_0 | pA'_0 \\ \mathfrak{x}'_0 | dA'_0}} \mathfrak{D}'_0 \right)^{-t}$, ce qui démontre b).

c) La formule b) montre que l'on a toujours $cl_{A'_0}(\tilde{A}) = cl_A(A_k)$ lorsque les idéaux premiers de A'_0 au-dessus des facteurs premiers de pA sont principaux. Cette condition est vérifiée lorsque p est inversible dans A , et aussi lorsque pA est un idéal maximal de A : en effet, dans ce cas $pA'_0 = \mathfrak{D}'_0^{\frac{p-1}{2}}$, où $\mathfrak{D}'_0$ est l'idéal principal $(\omega - \omega^{-1})^2 A'_0$.

Lorsque A est en outre principal, A_k est un A -module libre, et $\tilde{A}$ est par conséquent un A'_0 -module libre.

5. Idéaux essentiels.

Soit A' un anneau de Dedekind, n un entier positif, et $\mathfrak{u}$ un idéal fractionnaire non nul de A' . Il est clair que $\mathfrak{u}$ s'écrit de manière unique sous la forme $\mathfrak{u} = \mathfrak{u}_0^n \mathfrak{u}_1^1 \mathfrak{u}_2^2 \dots \mathfrak{u}_{n-1}^{n-1}$, où $\mathfrak{u}_0$ est un idéal fractionnaire de A' , et les $\mathfrak{u}_i (1 \leq i \leq n-1)$ sont des idéaux entiers de A' , premiers entre eux deux à deux, et sans facteurs carrés. Nous allons appliquer cette remarque pour associer à K des idéaux de $\tilde{k}$.

Pour cela, nous nous donnons un $\theta \in K$, tel que les $(\sigma\theta)_{\sigma \in H}$ forment une k -base normale de N (un tel θ existe, d'après la proposition IV.2). A tout $\chi \in H^*$, nous associons le nombre $\alpha(\chi) = \langle \theta, \chi \rangle^p$; c'est un élément non nul de $\tilde{k}$. (proposition IV.2).

L'idéal principal $\alpha(\chi)$ s'écrit de manière unique sous la forme $\alpha(\chi) = \mathfrak{z}(\chi)^p \prod_{i=1}^{p-1} \mathfrak{u}_{(i)}(\chi)^i$, où $\mathfrak{z}$ est un idéal fractionnaire de $\tilde{k}$, et où les $\mathfrak{u}_{(i)}(\chi)$ sont des idéaux entiers de $\tilde{k}$, premiers entre eux deux à deux, sans facteurs carrés.

Soit $\theta' \in K$, formant avec ses conjugués une k -base normale de N ; écrivons $\alpha'(\chi) = \langle \theta', \chi \rangle^p$. On décompose de même $\alpha'(\chi)$ sous la forme

$$\alpha'(\chi) = \mathfrak{A}'(\chi)^p \prod_{i=1}^{p-1} \mathfrak{u}'_{(i)}(\chi)^i.$$

D'après la proposition IV.4, b) on peut trouver $\lambda(\chi) \neq 0$, $\lambda(\chi) \in \tilde{k}$, tel que $\langle \theta', \chi \rangle = \lambda(\chi) \langle \theta, \chi \rangle$. On a donc $\alpha'(\chi) = \lambda(\chi)^p \alpha(\chi)$, d'où

$$(\lambda(\chi) \mathfrak{A}'(\chi))^p \prod_{i=1}^{p-1} \mathfrak{u}'_{(i)}(\chi)^i = \mathfrak{A}(\chi)^p \prod_{i=1}^{p-1} \mathfrak{u}_{(i)}(\chi)^i.$$

Il en résulte que les $\mathfrak{u}'_{(i)}(\chi)$ sont égaux aux $\mathfrak{u}_{(i)}(\chi)$, et que $\mathfrak{A}'(\chi)$ est un idéal équivalent à $\mathfrak{A}(\chi)$. Nous avons donc prouvé la

PROPOSITION IV.8. — *Les idéaux $\mathfrak{u}_{(i)}(\chi)$ et la classe de $\mathfrak{A}(\chi)$ sont des invariants du corps K.*

DEFINITION IV.5. — *Les idéaux $\mathfrak{u}_{(i)}(\chi)$ et $\mathfrak{A}(\chi)$ s'appellent les idéaux essentiels du corps K relativement au caractère χ . (voir A. Châtelet, [6] et [7]).*

Remarque. — Lorsque $\chi = \chi_0$, $\alpha(\chi_0) \in \tilde{k}^p$. On a donc dans ce cas $\mathfrak{u}_{(i)}(\chi_0) = A$, et $cl(\mathfrak{A}(\chi_0)) = 1$. Ce cas étant sans intérêt, nous n'en considérons plus que les idéaux essentiels associés à un caractère non trivial de H^* . Rappelons qu'on a associé à tout entier i , $i \not\equiv 0 \pmod{p}$, un entier i' (Définition IV.3). Pour étudier de plus près les idéaux essentiels, nous introduisons deux nouvelles définitions :

DEFINITION IV.6. — *Pour tout entier i , on désigne par $\bar{i}$ l'entier vérifiant $\bar{i} \equiv i \pmod{p}$, et $0 \leq \bar{i} \leq p-1$.*

DEFINITION IV.7. — *Pour tout entier i , $i \not\equiv 0 \pmod{p}$, on désigne par i^* l'entier vérifiant $ii^* \equiv 1 \pmod{p}$, et $1 \leq i^* \leq p-1$.*

PROPOSITION IV.9.

$$\mathfrak{u}_{(i)}(\chi) = \mathfrak{u}_{(1)}(\chi^{i^*})$$

Démonstration :

$$\alpha(\chi) = \mathfrak{A}(\chi)^p \prod_{i=1}^{p-1} \mathfrak{u}_{(i)}(\chi)^i.$$

Pour tout $j \not\equiv 0 \pmod p$, on a

$$\alpha(\chi^j) = \Re(\chi^j)^p \prod_{i=1}^{p-1} \mathfrak{u}_{(i)}(\chi^j)^i = \Re(\chi^j)^p \prod_{i=1}^{p-1} \mathfrak{u}_{(ij)}(\chi^j)^{\bar{ij}}$$

Mais on a vu (proposition IV.4,a) que $\beta_i(\chi) = \frac{\langle \theta, \chi^i \rangle}{\langle \theta, \chi \rangle^i}$ était un élément de $\tilde{k}$. On a donc :

$$\begin{aligned} \alpha(\chi^j) &= \beta_j(\chi)^p \alpha(\chi)^j = (\beta_j(\chi) \Re(\chi)^j)^p \prod_{i=1}^{p-1} \mathfrak{u}_{(i)}(\chi)^{\bar{ij}} \\ &= \left(\beta_j(\chi) \Re(\chi)^j \prod_{i=1}^{p-1} \mathfrak{u}_{(i)}(\chi)^{\frac{ij - \bar{ij}}{p}} \right)^p \prod_{i=1}^{p-1} \mathfrak{u}_{(i)}(\chi)^{\bar{ij}}. \end{aligned}$$

On déduit des deux expressions trouvées pour $\alpha(\chi^j)$ l'égalité $\mathfrak{u}_{(i)}(\chi) = \mathfrak{u}_{(ij)}(\chi^j)$ pour tout i , tout j , $i, j \not\equiv 0 \pmod p$. En faisant $j = i^*$ dans cette égalité, on obtient le résultat cherché. Nous écrivons pour simplifier $\mathfrak{u}_{(1)}(\chi) = (\chi)$. Avec cette convention, on peut énoncer le

COROLLAIRE. — *La décomposition de $\alpha(\chi)$ en idéaux essentiels est :*

$$\alpha(\chi) = \Re(\chi)^p \prod_{i=1}^{p-1} \mathfrak{u}(\chi^{i^*})^i = \Re(\chi)^p \prod_{i=1}^{p-1} \mathfrak{u}(\chi^i)^{i^*}$$

PROPOSITION IV.10. — *Pour tout $i \not\equiv 0 \pmod p$, $s_i \mathfrak{u}(\chi) = \mathfrak{u}(\chi^{i'})$ et $s_i \Re(\chi) = \Re(\chi^{i'})$.*

Démonstration. — On a vu (Proposition IV.1,3) que

$$s_i \langle \theta, \chi \rangle = \langle \theta, \chi^{i'} \rangle.$$

On a donc $s_i \alpha(\chi) = \alpha(\chi^{i'})$. On en déduit l'égalité

$$\Re(\chi^{i'})^p \prod_{j=1}^{p-1} \mathfrak{u}(\chi^{jj'})^{j^*} = (s_i \Re(\chi))^p \prod_{j=1}^{p-1} s_j \mathfrak{u}(\chi^j)^{j^*},$$

et l'unicité de la décomposition en idéaux essentiels entraîne le résultat cherché.

PROPOSITION IV.11. — *La décomposition de $\alpha(\chi)$ en idéaux essentiels peut se mettre sous la forme suivante :*

Dans le cas A, $\alpha(\chi) = \Re(\chi)^p \prod_{i=1}^{p-1} s_i \mathfrak{u}(\chi)^{i*}$

Dans le cas B₁, $\alpha(\chi) = \Re(\chi)^p \prod_{i=1}^{p-1} s_i \mathfrak{u}(\chi)^{i'*}$

Dans le cas B₂, $\alpha(\chi) = \Re(\chi)^p \prod_{\left(\frac{i}{p}\right)=1} (s_i \mathfrak{u}(\chi))^{i*} (s_i \mathfrak{u}(\chi^{-1}))^{p-i*}$.

Démonstration. — Dans le cas A, $i = i'$, donc $\mathfrak{u}(\chi^i) = s_i \mathfrak{u}(\chi)$.

Dans le cas B₁, $i' = \left(\frac{i}{p}\right)i$. Comme $\left(\frac{-1}{p}\right) = +1$, i' parcourt tous les entiers $\not\equiv 0$ modulo p lorsque i varie de 1 à $p-1$.

$$\begin{aligned} \text{Or } \mathfrak{u}(\chi^{i'}) &= s_{i'} \mathfrak{u}(\chi) ; \text{ donc, } \alpha(\chi) = \Re(\chi)^p \prod_{i=1}^{p-1} \mathfrak{u}(\chi^{i'})^{i'*} \\ &= \Re(\chi)^p \prod_{i=1}^{p-1} s_i \mathfrak{u}(\chi)^{i'*} . \end{aligned}$$

Dans le cas B₂, i' parcourt uniquement les classes modulo p qui sont des carrés lorsque i parcourt $(\mathbb{Z}/p\mathbb{Z})^*$.

si $\left(\frac{i}{p}\right) = +1$, on a $\mathfrak{u}(\chi^i) = s_i \mathfrak{u}(\chi)$, car $i = i'$.

si $\left(\frac{i}{p}\right) = -1$, on a $\mathfrak{u}(\chi^i) = s_i \mathfrak{u}(\chi^{-1})$, car $i = -i'$.

$$\text{On a donc } \alpha(\chi) = \Re(\chi)^p \prod_{\left(\frac{i}{p}\right)=+1} s_i \mathfrak{u}(\chi)^{i*} \prod_{\left(\frac{i}{p}\right)=-1} s_i \mathfrak{u}(\chi^{-1})^{i*} .$$

En changeant i en $-i$ dans le dernier produit, on obtient le résultat cherché, compte tenu de ce que $(-i)^* = p - i^*$.

Remarque. — Vue la définition de i' , la formule

$$\alpha(\chi) = \Re(\chi)^p \prod_{i=1}^{p-1} s_i \mathfrak{u}(\chi)^{i'*}$$

est correcte dans les cas A et B₁.

Application à l'étude de la ramification dans N.

PROPOSITION IV.12. — On suppose que A vérifie l'hypothèse (H).

Soit $\mathfrak{Q}$ un idéal premier non nul de A, ne divisant pas pA . Les propositions suivantes sont équivalentes :

i) $\mathfrak{Q} \mid \mathfrak{F}$ (voir théorème III.1).

ii) $\mathfrak{Q} \mid \prod_{x \neq x_0} u(x)$.

Démonstration. — On a les équivalences suivantes, χ désignant un élément de H^* distinct de χ_0 : $\mathfrak{Q} \mid \mathfrak{F} \iff$ tout facteur premier de $\mathfrak{Q}$ dans k est dans N la puissance p -ième d'un idéal premier $\iff$ tout facteur premier de $\mathfrak{Q}$ dans k est produit de puissances p -ième d'idéaux de N' (car $p \nmid [N' : N]$).

$\iff$ tout facteur premier de $\mathfrak{Q}$ dans k' est la puissance p -ième d'un idéal de N' (car $p \nmid [k' : k]$)

$\iff$ l'exposant dans $\alpha(\chi)$ des facteurs premiers de $\mathfrak{Q}$ dans k' n'est pas divisible par p (théorème I.8)

$\iff \mathfrak{Q} \mid \prod_{i=1}^{p-1} u(\chi^i)^{i^*}$

$\iff \mathfrak{Q} \mid \prod_{i=1}^{p-1} u(\chi^i)$

$\iff \mathfrak{Q} \mid \prod_{x \neq x_0} u(x)$.

COROLLAIRE. — Si $\mathfrak{Q} \mid \mathfrak{F}$, $\mathfrak{Q} \nmid pA$, $\mathfrak{Q}$ est complètement décomposé dans $\tilde{k}$.

En effet, si $\mathfrak{Q}$ n'est pas complètement décomposée dans $\tilde{k}$, il existe un facteur premier $\tilde{\mathfrak{Q}}$ de $\mathfrak{Q}$ dans $\tilde{k}$ dont le groupe de décomposition n'est pas réduit à l'élément neutre. Il existe donc un entier $i \not\equiv 1 \pmod p$ ($i \not\equiv \pm 1 \pmod p$ dans le cas B_2) pour lequel $s_i \tilde{\mathfrak{Q}} = \tilde{\mathfrak{Q}}$. Comme $s_i \tilde{\mathfrak{Q}} \mid s_i u(\chi)$, $\tilde{\mathfrak{Q}} \mid s_i u(\chi) = u(\chi^i)$. Comme $i' \not\equiv 1 \pmod p$ $u(\chi)$ et $u(\chi^i)$ sont premiers entre eux, ce qui conduit à une contradiction.

Remarque 1. — Le fait que les facteurs premiers de $\prod_{x \neq x_0} \mathfrak{u}(\chi)$

doivent être complètement décomposés entraîne en particulier que $\prod \mathfrak{u}(\chi)$ est premier au discriminant $\tilde{d}$ de $\tilde{k}/\kappa$. Dans le cas A, en calculant $\tilde{d}$ par la formule $\tilde{d} = \Delta(\kappa'_0/\kappa)^2 N_{\kappa'_0/\kappa}(\Delta(\tilde{k}/\kappa'_0))$, on retrouve le fait que les facteurs premiers communs à d et à $\mathfrak{F}$ doivent diviser pA (voir proposition III.3).

Remarque 2. — Comme $\Delta(\kappa'_0/\kappa) = p^{\frac{p-3}{2}} A$, $\tilde{d}$ ne peut être premier à p que si $p = 3$.

Le calcul de $\Delta(\tilde{k}/\kappa'_0)$ fait dans la proposition IV.7 montre qu'en outre p doit diviser d . Le cas particulier où p et $\prod_x \mathfrak{u}(\chi)$ ne sont pas premiers entre eux peut se produire : c'est le "cas 9" de [13]. Les idéaux essentiels donnent ainsi une interprétation du rôle particulier joué par $p = 3$, déjà rencontré auparavant (Chapitre III, remarque 1 suivant le théorème III.1).

6. Le réseau M_1 .

Nous définissons un espace vectoriel V sur κ de la manière suivante : dans les cas A et B_1 , nous posons $V = \tilde{k}$; dans le cas B_2 , nous posons $V = \tilde{k} \times \tilde{k} = \kappa'_0 \times \kappa'_0$. Il résulte de la détermination de $\tilde{k}$ (Proposition IV.3) que $\dim_{\kappa} V = p - 1$.

L'espace V est muni naturellement d'une structure de κ'_0 -espace vectoriel. Lorsque nous parlerons d'un réseau de V , nous préciserons s'il s'agit d'un réseau relativement à A ou à A'_0 . Clairement, un réseau relativement à A'_0 peut être considéré comme un réseau relativement à A .

Pour étudier les entiers de K , nous aurons besoin d'introduire un réseau par rapport à A'_0 noté M_1 .

DEFINITION IV.8. — *Donnons nous un élément $\theta \in K$ qui constitue avec ses conjugués une base normale de N/k , et un caractère $\chi \in H^*$, qui n'est pas le caractère trivial. On désigne par $M_1(\chi)$ (ou*

M_1 pour simplifier) l'ensemble $\mathfrak{K}(\chi)^{-1}$ dans les cas A et B_1 ,

$$\mathfrak{K}(\chi)^{-1} \oplus \mathfrak{K}(\chi^{-1})^{-1}$$

dans le cas B_2 .

Il est clair que M_1 est un réseau de V par rapport à A'_0 et à A . Considérons l'idéal $\prod_{x \neq x_0} \mathfrak{u}(\chi)$ de $\tilde{k}$. Il s'identifie dans le cas B_2 (resp. dans les cas A et B_1) à l'idéal $N_{\tilde{k}/\kappa}[\mathfrak{u}(\chi) \mathfrak{u}(\chi^{-1})]$ (resp. $N_{\tilde{k}/\kappa}[\mathfrak{u}(\chi)]$) étendu à $\tilde{A}$. Vues les conventions usuelles faites sur les idéaux, il peut être considéré comme un idéal de chacun des corps intermédiaires entre κ et $\tilde{k}$, donc en particulier comme un idéal de κ'_0 . Compte tenu de cette remarque, on peut énoncer le

THEOREME IV.2. — Si A vérifie l'hypothèse (H), alors

$$cl_{A'_0}(M_1) = cl_{A'_0}(\tilde{A}) cl_{A'_0}\left(\prod_{x \neq x_0} \mathfrak{u}(\chi)\right).$$

Démonstration. — Dans le cas B_2 , $cl_{A'_0}(\tilde{A}) = 1$,

et
$$M_1 = \mathfrak{K}(\chi)^{-1} \oplus \mathfrak{K}(\chi^{-1})^{-1}.$$

Il résulte du théorème I.1,c) que l'on a

$$cl_{A'_0}(M_1) = cl_{A'_0}[\mathfrak{K}(\chi) \mathfrak{K}(\chi^{-1})]^{-1}.$$

En utilisant les propositions IV.10 et IV.11 on voit que la décomposition en idéaux essentiels de $\alpha(\chi) = \langle \theta, \chi \rangle^p$ est :

$$\alpha(\chi) = \mathfrak{K}(\chi)^p \prod_{\left(\frac{i}{p}\right)=+1} \mathfrak{u}(\chi^{-i})^{i*} \mathfrak{u}(\chi^i)^{p-i*}.$$

De même,
$$\alpha(\chi^{-1}) = \mathfrak{K}(\chi^{-1})^p \prod_{\left(\frac{i}{p}\right)=+1} \mathfrak{u}(\chi^{-i})^{i*} \mathfrak{u}(\chi^i)^{p-i*}$$

Comme $\alpha(\chi) \alpha(\chi^{-1})$ est la puissance p -ième d'un élément $\beta_{-1}(\chi)$ de $\tilde{k}$, on a :

$$\beta_{-1}(\chi) = \mathfrak{K}(\chi) \mathfrak{K}(\chi^{-1}) \prod_{\left(\frac{i}{p}\right)=+1} \mathfrak{u}(\chi^i) \mathfrak{u}(\chi^{-i}),$$

ce qui démontre le théorème dans le cas B_2 .

Dans les cas A et B₁, la classe de M₁ est donnée par la formule :

$$cl_{A'_0}(M_1) = cl_{A'_0}(\tilde{A}) cl_{A'_0}[N_{\tilde{\kappa}/\kappa'_0}(\mathfrak{N}(\chi)^{-1})]$$

(Théorème I.5,ii).

Comme la norme relativement à κ'_0 de $\alpha(\chi)$ est la puissance p -ième d'un élément $\beta_{-1}(\chi)$ de κ'_0 , la décomposition en idéaux essentiels entraîne la formule :

$$\beta_{-1}(\chi)^p = N_{\tilde{\kappa}/\kappa'_0}(\mathfrak{N}(\chi))^p \prod_{i=1} N_{\tilde{\kappa}/\kappa'_0}(\mathfrak{u}(\chi^i))^{i^*}$$

Mais $s_{-1}(\chi) = \mathfrak{u}(\chi^{-1})$ (proposition IV.10) ; donc,

$$N_{\tilde{\kappa}/\kappa'_0}(\mathfrak{u}(\chi)) = N_{\tilde{\kappa}/\kappa'_0}(\mathfrak{u}(\chi^{-1})).$$

On peut donc écrire l'égalité précédente sous la forme :

$$\begin{aligned} \beta_{-1}(\chi)^p &= N_{\tilde{\kappa}/\kappa'_0}(\mathfrak{N}(\chi))^p \prod_{i=1}^{\frac{p-1}{2}} N_{\tilde{\kappa}/\kappa'_0}(\mathfrak{u}(\chi^i))^{i^*} \mathfrak{u}(\chi^i)^{p-i^*} \\ &= N_{\tilde{\kappa}/\kappa'_0}(\mathfrak{N}(\chi))^p \prod_{i=1}^{\frac{p-1}{2}} N_{\tilde{\kappa}/\kappa'_0}(\mathfrak{u}(\chi^i))^p, \end{aligned}$$

qui entraîne immédiatement le résultat cherché.

COROLLAIRE.

a) Supposons que A soit un anneau principal, et que l'une des conditions suivantes soient réalisées :

- i) p est inversible dans A
- ii) pA est un idéal maximal de A.

Alors, M₁ est un A'₀-module libre.

b) Dans le cas B, M₁ est un A'₀-module libre dès que A est principal.

Démonstration. — L'idéal $\prod_{x \neq x_0} \mathfrak{u}(\chi)$, considéré comme idéal de A, est égal à $N_{\tilde{\kappa}/\kappa}(\mathfrak{u}(\chi))$ dans les cas A et B₁, et à $N_{\tilde{\kappa}/\kappa}(\mathfrak{u}(\chi) \cdot \mathfrak{u}(\chi^{-1}))$

dans le cas B_2 . C'est donc toujours un idéal principal. Comme $\tilde{A}$ est A'_0 -libre dans le cas B, on a prouvé b) et il reste à montrer a) dans le cas A ; cela résulte du théorème IV.1,c).

7. Cas où κ est le corps Q des rationnels.

Lorsque κ est le corps Q des rationnels, un certain nombre de résultats de ce chapitre peuvent être exprimés plus simplement, et rattachés à des notions connues. Dans ce paragraphe, nous examinons les plus importants.

Q contient l'anneau Z des entiers. Comme pZ est un idéal maximal, Z vérifie l'hypothèse (H), et, par conséquent, Q vérifie l'hypothèse (H'). En fait, S désignant une partie multiplicative de Z ne contenant pas 0, $A = S^{-1}Z$ vérifie aussi l'hypothèse (H).

Rappelons que, si L est une extension de degré fini des rationnels, on peut associer à L un discriminant qui est un nombre entier, positif ou négatif, $\Delta(L/Q)$. L'idéal de Z engendré par ce nombre coïncide avec le discriminant de la clôture intégrale B de Z dans L par rapport à Z défini dans le chapitre I, § 4. Dans ce paragraphe, d , D et $\bar{D}$ désigneront les nombres, discriminants de k , K et N respectivement.

PROPOSITION IV.13. — Soit f l'entier positif tel que $\mathfrak{F} = fZ$ (voir chapitre III, Théorème II.1). Alors :

$$a) D = d^{\frac{p-1}{2}} f^{p-1}$$

$$b) \bar{D} = d^p f^{2(p-1)}$$

Démonstration. — Il résulte des résultats du chapitre III que les formules ci-dessus sont vraies au signe près.

Pour les démontrer, nous nous appuyerons sur le résultat suivant (voir [8]) : si L est un corps de nombres ayant r_1 conjugués réels et $2r_2$ conjugués imaginaires, le discriminant de L a le signe de $(-1)^{r_2}$.

Si $d > 0$, les membres de droite de a) et b) sont des nombres positifs. Le corps k est réel, et N , qui est une extension cyclique de degré impair d'un corps totalement réel est aussi un corps totalement

réel ; il en est de même de K , qui est contenu dans N . On a donc $D > 0$ et $\bar{D} > 0$, d'où a) et b) lorsque $d > 0$.

Si $d < 0$, k est un corps imaginaire ; il en est donc de même de N , et N est donc totalement imaginaire. N ayant $2p$ conjugués imaginaires, $\bar{D}$ a le signe $(-1)^p$. On a donc $\bar{D} < 0$; comme $d < 0$, b) est démontrée dans tous les cas. D'autre part, N possède un sous-corps réel de degré p , et un seul, faute de quoi il serait réel. K possède donc un conjugué réel. Il en résulte que D le signe $(-1)^{\frac{p-1}{2}}$, et c'est aussi le signe de $d^{\frac{p-1}{2}}$, c.q.f.d.

PROPOSITION IV.14. — Si A est un anneau $S^{-1}Z$, $\tilde{A}$ et M_1 sont des A'_0 -modules libres.

En effet, A est principal, et p est un élément inversible de A si $pZ \cap S \neq \emptyset$, ou engendre un idéal maximal de A si $pZ \cap S = \emptyset$. La proposition résulte alors immédiatement du théorème IV.1, c, et du corollaire du théorème IV.2.

PROPOSITION IV.15. — On suppose que $A = Z$. Soit q un nombre premier $\neq p$, ne divisant pas d . Pour que q soit complètement décomposé dans $\tilde{k}$, il faut et il suffit que l'on ait $\left(\frac{d}{q}\right) \equiv q \pmod{p}$.

Dans le cas B_1 , cette condition équivaut à $q \equiv 1 \pmod{p}$;

Dans le cas B_2 , cette condition équivaut à $q \equiv \pm 1 \pmod{p}$.

Démonstration. — Pour prouver la proposition précédente, nous utiliserons les propriétés de la substitution de Frobenius à valeurs dans le groupe de Galois de k'/Q (C.L., Ch. I, § 8). Pour une extension abélienne L/Q des rationnels, et un nombre premier q non ramifié dans L , nous notons F_q la substitution de Frobenius attachée à q : on a donc, pour tout idéal premier $\mathfrak{X}$ de L au-dessus de q la congruence $F_q(x) \equiv x^q \pmod{\mathfrak{X}}$ quel que soit l'entier x de L . Il résulte de C.L., Ch. I, § 8 que :

a) Si $L = Q'$, F_q est définie pour tout $q \neq p$, et n'est autre que l'élément de $\text{Gal}(Q'/Q)$ que nous avons noté s_q .

b) Si L est une extension quadratique k de Q , de discriminant d , F_q est définie pour tout q ne divisant pas d , et, en identifiant le groupe de Galois de k/Q au sous-groupe $\{\pm 1\}$ de Q^* , est égale au symbole de reste quadratique (d/q) .

Rappelons qu'un nombre premier q de Q est complètement décomposé dans une extension abélienne L de Q si et seulement si sa substitution de Frobenius F_q est l'élément neutre du groupe de Galois de L/Q .

Dans le cas B_1 , comme $\tilde{k} = Q'$ et $F_q = s_q$, q est complètement décomposé dans $\tilde{k}$ si et seulement si $q \equiv 1 \pmod{p}$. Comme q est aussi complètement décomposé dans k , on a aussi $(d/q) = +1$, d'où $q \equiv (d/q) \pmod{p}$, et réciproquement, on vérifie sans peine que $q \equiv (d/q) \pmod{p}$ entraîne $q \equiv 1 \pmod{p}$.

Dans le cas B_2 , $\tilde{k} = Q'_0$. Le groupe de Galois de $\tilde{k}/Q$ s'identifie au quotient du groupe que nous avons noté g par son sous-groupe d'ordre 2, et F_q est l'image de s_q dans ce quotient. Cela entraîne que q est complètement décomposé dans $\tilde{k}$ si et seulement si $s_q = s_1$ ou s_{-1} , c'est-à-dire si $q \equiv \pm 1 \pmod{p}$. Comme $d = -p$, il n'est pas difficile de vérifier que cette condition équivaut à $q \equiv (d/q) \pmod{p}$.

Dans le cas A , on remarque que q , qui ne divise ni d ni p , est non ramifié dans k' . Le groupe de Galois de k'/Q s'identifie au produit direct du groupe de Galois $\{\pm 1\}$ de k/Q et du groupe de Galois g de Q'/Q . Soit F_q la substitution de Frobenius de q à valeur dans le groupe de Galois de k'/Q . Sa composante dans le facteur $\{\pm 1\}$ est (d/q) , et celle dans g est s_q . Dire que q est complètement décomposé dans $\tilde{k}$ revient à dire que l'on est dans un des cas suivants : ou $s_q = (d/q) = +1$, ou $s_q = (d/q) = -1$. Il est clair que cette condition peut encore s'écrire $q \equiv (d/q) \pmod{p}$, C.Q.F.D.

COROLLAIRE 1. — Soit q un nombre premier. Si q divise le produit $\prod_{x \neq x_0} u(x)$, q vérifie une des conditions suivantes :

i) $q = p = 3$ et $d \equiv -3 \pmod{9}$

ii) $q \neq p$ et $q \equiv \left(\frac{d}{p}\right) \pmod{p}$.

Démonstration. — Lorsque $q \neq p$, cela résulte de la proposition ci-dessus et du corollaire de la proposition IV.12. Le cas $q = p$ ne peut se produire que si $p = 3$, car q ne doit pas diviser le discriminant $\tilde{d}$ de $\tilde{k}$. On a alors $\tilde{d} = -3d$. Comme 3 est complètement décomposé dans $\tilde{k}$, $\tilde{d} \equiv 1 \pmod{3}$, ce qui entraîne $d \equiv -3 \pmod{9}$.

COROLLAIRE 2. — *Soit q un nombre premier distinct de p . Si q divise f , $q \equiv (d/q) \pmod{p}$.*

Cela résulte du corollaire de la proposition IV.12 et de la proposition IV.15.

CHAPITRE V

ENTIERS DE K

Nous supposons toujours que les hypothèses (H) et (H') sont vérifiées (Chapitre III, § 2).

Dans ce chapitre, nous étudions l'anneau A_K des entiers de K considéré comme A-module. Nous étudions aussi l'existence de A-bases de A_K du type $1, \varphi, \psi, \sigma^i \varphi + \sigma^{-i} \varphi, \sigma^i \psi + \sigma^{-i} \psi$ ($1 \leq i \leq \frac{p-3}{2}$).

Nous verrons au chapitre VI comment on peut, dans certains cas, construire des bases normales de A_K/A et de A_N/A à partir d'une telle base.

Nous nous donnons dans ce chapitre un élément $\theta_0 \in K$, tel que les $(\sigma \theta_0)_{\sigma \in H}$ forment une k-base normale de N, et un $\chi_1 \in H^*$, $\chi_1 \neq \chi_0$.

1. Passage de K à V.

Rappelons qu'on a défini (Chapitre IV, § 6) un espace vectoriel V sur κ . On a vu comment associer à θ_0 et à χ_1 un réseau M_1 de V, en posant $M_1 = \mathfrak{K}(\chi_1)^{-1}$ dans les cas A et B_1 , $M_1 = \mathfrak{K}(\chi_1)^{-1} \oplus \mathfrak{K}(\chi_1^{-1})^{-1}$ dans le cas B_2 .

DEFINITION V.1. — On pose, pour tout $\theta \in K$, $f(\theta) = \frac{\langle \theta, \chi_1 \rangle}{\langle \theta_0, \chi_1 \rangle}$ dans les cas A et B_1 , $f(\theta) = \left(\frac{\langle \theta, \chi_1 \rangle}{\langle \theta_0, \chi_1 \rangle}, \frac{\langle \theta, \chi_1^{-1} \rangle}{\langle \theta_0, \chi_1^{-1} \rangle} \right)$ dans le cas B_2 .

Il résulte de la définition de V (Ch. IV, § VI) que quel que soit $\theta \in K$, $f(\theta)$ est un élément de V.

PROPOSITION V.1. — $f : K \longrightarrow V$ est un homomorphisme surjectif d'espaces vectoriels sur κ , de noyau κ .

Démonstration. — Les formules

$$\langle \theta + \theta', \chi \rangle = \langle \theta, \chi \rangle + \langle \theta', \chi \rangle \text{ et } \langle \lambda \theta, \chi \rangle = \lambda \langle \theta, \chi \rangle$$

pour $\theta, \theta' \in K, \lambda \in \kappa, \chi \in H^*$ montrent que f est κ -linéaire.

De plus, $f(\theta)$ est évidemment nul pour tout $\theta \in \kappa$. Réciproquement, si $\theta \in K$ vérifie $f(\theta) = 0$, on a $\langle \theta, \chi \rangle = 0$ pour tout $\chi \neq \chi_0$, car les $\langle \theta, \chi \rangle, \chi \neq \chi_0$, sont conjugués de $\langle \theta, \chi_1 \rangle$ (resp. de $\langle \theta, \chi_1 \rangle$ ou $\langle \theta, \chi_1^{-1} \rangle$) dans les cas A et B₁ (resp. dans le cas B₂). On a donc $\text{Ker } f = \kappa$. Comme $\dim_{\kappa} V = p - 1$, on déduit du calcul de $\text{Ker } f$ que f est surjectif.

PROPOSITION V.2.

a) Si X est un réseau de K par rapport à A , $f(X)$ est un réseau de V par rapport à A .

$$b) \text{cl}_A(X) = \text{cl}_A(f(X)) \text{cl}_A(\kappa \cap X).$$

Démonstration :

a) $\kappa f(X) = f(\kappa X) = f(K) = V$; comme X est un A -module de type fini, $f(X)$ est aussi de type fini sur A ; c'est donc un réseau de V relativement à A .

b) Il résulte de la proposition V.1 que la suite

$$0 \longrightarrow \kappa \cap X \longrightarrow X \longrightarrow f(X) \longrightarrow 0$$

est exacte. Les termes de cette suite sont des A -modules de type fini sans-torsion, d'où b) (voir Chapitre I, définition I.2 et théorème I.1).

COROLLAIRE.

$$\text{cl}_A(A_K) = \text{cl}_A(f(A_K)).$$

PROPOSITION V.3. — Entre les réseaux M_1 et $f(A_K)$ de V , on a la double inclusion : $pM_1 \subset f(A_K) \subset M_1$.

Démonstration :

a) $f(A_K) \subset M_1$. Soit $\theta \in A_K$ et $\chi \neq \chi_0$. La résolvante $\langle \theta, \chi \rangle$ est un élément de N' entier sur A . Posons $\lambda(\chi) = \frac{\langle \theta, \chi \rangle}{\langle \theta_0, \chi \rangle}$. Alors,

$\langle \theta, \chi \rangle^p \tilde{A} = [\lambda(\chi) \mathfrak{K}(\chi)]^p \prod_{i=1}^{p-1} \mathfrak{u}(\chi^i)^{i*}$ est un idéal entier de $\tilde{A}$.

Comme $\prod \mathfrak{u}(\chi^i)^{i*}$ n'est pas divisible par la puissance p -ième d'un idéal premier de $\tilde{A}$, $\lambda(\chi) \mathfrak{K}(\chi)$ est un idéal entier de $\tilde{A}$. On a donc $\lambda(\chi) \in \mathfrak{K}(\chi)^{-1}$ pour tout $\chi \neq \chi_0$, ce qui prouve a).

b) $pM_1 \subset f(A_K)$. Soit λ dans les cas A et B_1 (Resp. (λ, μ) dans le cas B_2) un élément de pM_1 . Soit $\chi \neq \chi_0$ et i tel que $\chi = \chi_1^i$. On définit $\lambda(\chi)$ de la façon suivante : dans les cas A et B_1 , on pose

$$\lambda(\chi) = s_i \lambda ; \text{ dans le cas } B_2, \text{ on pose } \begin{cases} \lambda(\chi) = s_i \mu \text{ si } \left(\frac{i}{p}\right) = -1 \\ \lambda(\chi) = s_i \lambda \text{ si } \left(\frac{i}{p}\right) = +1 \end{cases}$$

Posons $\theta = \frac{1}{p} \sum_{\chi \neq \chi_0} \lambda(\chi) \langle \theta_0, \chi \rangle$. Il est clair que $\theta \in K$. De plus,

$p\theta \in pA_K$: en effet, pour tout χ , $\lambda(\chi) \in p\mathfrak{K}(\chi)^{-1}$ car $\lambda(\chi)$ est conjugué de λ ou de μ . Il en résulte que θ est un élément de A_K , et l'on vérifie immédiatement que $f(\theta) = \lambda$ (Resp. $f(\theta) = (\lambda, \mu)$), ce qui prouve b).

Remarque. — Grâce aux propositions V.3 et V.4, il est parfois possible de déterminer $cl(A_K)$ sans déterminer $f(A_K)$. En effet on a calculé (théorème IV.1 et IV.2) la classe de M_1 considéré comme A'_0 -module.

Il est facile d'en déduire la classe de M_1 considéré comme A -module. D'autre part, la proposition V.3 montre que $\chi_A(M_1/f(A_K))$ est un idéal entier, divisant $\chi_A(M_1/pM_1)$, et $\chi_A(M_1/pM_1)$ est égal à l'idéal $p^{p-1}A$ de A .

Supposons que pA soit dans A un produit d'idéaux premiers principaux (c'est par exemple le cas si p est inversible dans A , ou si pA lui-même est un idéal premier). Alors, les idéaux divisant $p^{p-1}A$ sont tous principaux. On en déduit que $\chi_A(M_1/f(A_K))$ est un idéal principal, d'où $cl(f(A_K)) = cl(M_1)$.

Nous allons maintenant montrer comment on peut construire effectivement une décomposition de A_K en somme directe d'idéaux de A à partir d'une telle décomposition de $f(A_K)$.

THEOREME V.1. — Soient $x_1, \dots, x_{p-1} \in f(A_K)$ et I un idéal fractionnaire de A contenant A , tel que

$$f(A_K) = Ax_1 + \dots + Ax_{p-2} + Ix_{p-1}.$$

Soient $\theta_1, \dots, \theta_{p-1}$ des éléments de A_K , tels que $f(\theta_i) = x_i$. Alors,

$$A_K = A + A\theta_1 + \dots + A\theta_{p-2} + I\theta_{p-1}.$$

Démonstration. — Considérons la suite exacte

$$0 \longrightarrow A \longrightarrow A_K \xrightarrow{f} f(A_K) \longrightarrow 0.$$

Comme $f(A_K)$ est un A -module projectif (théorème I.1), cette suite est scindée. Soit $g : f(A_K) \longrightarrow A_K$ une section de f , et posons $\theta'_i = g(x_i)$. Il est évident que le A -module A_K s'écrit sous la forme $A_K = A + A\theta'_1 + \dots + A\theta'_{p-2} + I\theta'_{p-1}$, la somme étant directe. Comme $f(\theta_i) = x_i$, $f(\theta_i - \theta'_i) = 0$. On en déduit que pour tout i , $\theta_i - \theta'_i \in \mathfrak{N} \cap A_K = A$, ce qui achève la démonstration du théorème.

Remarque 1. — On retrouve le fait que $cl(A_K) = cl(f(A_K))$, la valeur commune étant la classe de l'idéal I .

Remarque 2. — Pour appliquer pratiquement le théorème, il faut connaître $f(A_K)$. La détermination de $f(A_K)$ pourrait être faite par les méthodes de [13], en utilisant le théorème I.8 et d'autres résultats plus généraux sur la ramification dans les extensions de Kummer.

2. Etude de A_K au moyen du A'_0 -module $f(A_K)$.

PROPOSITION V.4. — Soit X un réseau de K . Pour que $f(X)$ soit un réseau de V par rapport à A'_0 , il faut et il suffit que X vérifie la condition suivante :

quels que soient $\theta \in X$ et $\sigma \in H$, $\sigma\theta + \sigma^{-1}\theta \in X + \mathfrak{N}$.

Démonstration. — Puisque X est un réseau de K , $f(X)$ est un réseau de V par rapport à A (Proposition V.2). Dire que $f(X)$ est un réseau de V par rapport à A'_0 revient à dire que $f(X)$ est stable pour le produit par des éléments de A'_0 . Or, on a vu (Proposition III.2)

que, ω désignant une racine p -ième de l'unité autre que 1, $1, \omega, \dots, \omega^{p-2}$ était une A -base de A' . Cela entraîne que (ω^i) ($1 \leq i \leq p-1$) est une A -base normale de A' donc que $(\omega^i + \omega^{-i})$ ($1 \leq i \leq \frac{p-1}{2}$) est une A -base normale de A'_0 . Comme $\omega^i + \omega^{-i}$ peut s'exprimer sous forme de polynôme en $\omega + \omega^{-1}$, dire que $f(X)$ est un A'_0 -module revient à dire que $f(X)$ est stable par le produit par $\omega + \omega^{-1}$. Soit $\theta \in X$.

La proposition IV.1,b) montre immédiatement la formule suivante, où l'on a posé $\omega = \chi_1(\sigma)$:

$$f(\sigma\theta + \sigma^{-1}\theta) = (\omega + \omega^{-1})f(\theta).$$

Il est alors clair que $f(X)$ est stable par $(\omega + \omega^{-1})$ si et seulement si X est stable par $\sigma + \sigma^{-1}$ modulo $\mathfrak{u} \cap X$.

Nous allons appliquer la proposition précédente à la recherche de bases particulières du A -module A_K .

DEFINITION V.2. — Soit σ un générateur de H . On dira qu'un couple (φ, ψ) d'éléments de A_K est une H -base de A_K si les p -éléments $1, \varphi, \psi, \sigma^i\varphi + \sigma^{-i}\varphi, \sigma^i\psi + \sigma^{-i}\psi$ ($1 \leq i \leq \frac{p-3}{2}$) forment une base du A -module A_K . On dira aussi que la base de A_K ainsi construite est une H -base.

Remarque. — La sous-algèbre de $A[H]$ engendrée par les $\sigma^i + \sigma^{-i}$ ($1 \leq i \leq \frac{p-3}{2}$) ne dépend pas du choix de σ . Par conséquent, le fait qu'un couple (φ, ψ) soit une H -base de A_K ne dépend pas non plus du choix du générateur σ de H .

THEOREME V.2. — Pour qu'un couple (φ, ψ) d'éléments de A_K soit une H -base de A_K , il faut et il suffit que le couple $(f(\varphi), f(\psi))$ de $f(A_K)$ soit une base de $f(A_K)$ comme A'_0 -module.

Démonstration. — Pour tout élément θ de A_K et tout élément σ de H , $(\sigma + \sigma^{-1})\theta$ est un élément de A_K . Cela prouve que $f(A_K)$ est un réseau de V par rapport à A'_0 (Proposition V.4).

Le théorème V.2 résulte alors immédiatement du théorème V.1.

THEOREME V.3. — *Supposons que A soit un anneau principal, et que l'une des conditions suivantes soit vérifiée :*

- i) p est inversible dans A
- ii) pA est un idéal maximal de A .

Alors, A_K possède des H-bases.

Démonstration. — Les inclusions $pM_1 \subset f(A_K) \subset M_1$ (proposition V.3) montrent que $\chi_{A'_0}(M_1/f(A_K))$ est un idéal entier de A'_0 , qui divise $\chi_{A'_0}(M_1/pM_1) = (pA'_0)^2$. Lorsque p est inversible dans A ,

$$\chi_{A'_0}(M_1/f(A_K)) = A'_0.$$

Lorsque p n'est pas inversible dans A , $pA'_0 = ((\omega - \omega^{-1})^2 A'_0)^{\frac{p-1}{2}}$. Donc, les facteurs de $(pA'_0)^2$ sont principaux. Dans tous les cas, $\chi_{A'_0}(M_1/f(A_K))$ est un idéal principal. Il en résulte que $f(A_K)$ et M_1 sont des A'_0 -modules isomorphes. Mais on sait (Théorème IV.2, corollaire) que, sous les hypothèses du théorème V.3, M_1 est un A'_0 -module libre. Il en est donc de même de $f(A_K)$, c.q.f.d.

CHAPITRE VI

BASES NORMALES

On conserve les notations des chapitres III, IV et V. On suppose que la caractéristique de κ ne divise pas $2p$. On désigne encore par σ un générateur de H , et par $\{1, \tau\}$ le groupe de Galois de N/K .

1. Etude du $A[G]$ -module A_N .

PROPOSITION VI.1. — *Soit M un sous- $A[G]$ -module projectif de A_N , contenant A_K et A_k , et soient φ et ψ deux éléments de A_K ayant une même trace sur κ . Alors, il existe un élément θ de M , vérifiant $\text{Tr}_{N/K}(\theta) = \varphi$, $\text{Tr}_{N/K}(\sigma\theta) = \psi$. De plus, deux choix de θ diffèrent d'un élément λ de A_k , de trace sur κ nulle.*

Démonstration. — Tout d'abord, si θ et θ' sont deux solutions de notre problème, leur différence λ vérifie $\lambda + \tau\lambda = 0$, $\sigma\lambda + \tau\sigma\lambda = 0$, d'où l'on déduit $\sigma^2\lambda + \tau\lambda = 0$, et, par différence, $\lambda = \sigma^2\lambda$. On a donc $\lambda \in A_k$, et $\text{Tr}_{k/\kappa}(\lambda) = \lambda + \tau\lambda = 0$.

Nous montrons maintenant l'existence d'un θ vérifiant $\text{Tr}_{N/K}(\theta) = \varphi$, $\text{Tr}_{N/K}(\sigma\theta) = \psi$. Pour faire cette démonstration, nous utilisons le fait que M , qui est un $A[G]$ -module projectif, est un $Z[G]$ -module relativement projectif, donc cohomologiquement trivial, en remarquant que l'ensemble des éléments de M fixes par τ (resp. par H) n'est autre que A_K (resp. A_k).

a) *Démonstration dans le cas $\varphi = 0$.*

Dans ce cas, $\text{Tr}_{K/\kappa}(\psi) = 0$. Comme $\hat{H}^0(\{1, \tau\}, M) = 0$, il existe $u \in M$ tel que $\psi = u + \tau u$. Mais

$$(1 + \tau)\text{Tr}_{N/k}(u) = \text{Tr}_{N/k}(1 + \tau)u = \text{Tr}_{N/k}(u) = \text{Tr}_{K/\kappa}(\psi) = 0.$$

Comme $\hat{H}_0(\{1, \tau\}, A_k) = 0$, il existe $v \in A_k$ tel que $\text{Tr}_{N/k}(u) = v - \tau v$.

Comme $\hat{H}^0(H, M) = 0$, il existe $w \in M$ tel que $v = \text{Tr}_{N/k}(w)$. Alors,

$\text{Tr}_{N/K}(u - (w - \tau w) = v - \tau v - (v - \tau v) = 0$. Comme $\hat{H}_0(H, M) = 0$, il existe $\theta' \in M$ vérifiant $u - (w - \tau w) = \sigma\theta' - \sigma^{-1}\theta'$. Posons $\theta = \theta' - \tau\theta'$. L'élément θ que nous venons de définir est un élément de M , ayant une trace sur K nulle. De plus,

$$\begin{aligned}\text{Tr}_{N/K}(\sigma\theta) &= (1 + \tau)(\sigma\theta' - \sigma\tau\theta') = (1 + \tau)(\sigma - \tau\sigma^{-1})\theta' \\ &= (1 + \tau)(\sigma - \sigma^{-1})\theta' = (1 + \tau)(u - (w - \tau w)) \\ &= (1 + \tau)w = \psi.\end{aligned}$$

b) *Démonstration dans le cas général.*

Comme $\hat{H}^0(\{1, \tau\}, M) = 0$, on peut trouver un élément θ' de M tel que $\text{Tr}_{N/K}(\theta') = \varphi$. Posons $\psi' = \text{Tr}_{N/K}(\sigma\theta')$. Alors,

$$\begin{aligned}\text{Tr}_{K/k}(\psi - \psi') &= \text{Tr}_{K/k}(\psi) - \text{Tr}_{N/K}(\sigma\theta') = \text{Tr}_{K/k}(\psi) - \text{Tr}_{N/K}(\theta') \\ &= \text{Tr}_{K/k}(\psi) - \text{Tr}_{K/k}(\varphi) = 0.\end{aligned}$$

Il résulte de a) que l'on peut trouver un élément θ'' de M vérifiant $\text{Tr}_{N/K}(\theta'') = 0$, $\text{Tr}_{N/K}(\sigma\theta'') = \psi - \psi'$. Posons $\theta = \theta' + \theta''$. Il est immédiat que l'on a $\text{Tr}_{N/K}(\theta) = \varphi$, et $\text{Tr}_{N/K}(\sigma\theta) = \psi$.

COROLLAIRE 1. — *Supposons l'extension N/k modérément ramifiée, et soient φ et ψ deux éléments de A_K , ayant même trace sur k . Alors, il existe $\theta \in A_N$, vérifiant $\text{Tr}_{N/K}(\theta) = \varphi$, $\text{Tr}_{N/K}(\sigma\theta) = \psi$, et deux choix de θ différent d'un élément de A_k , de trace sur k nulle.*

En effet, puisque N/k est modérément ramifiée, A_N est un $A[G]$ -module projectif (Théorème II.1) auquel on peut appliquer la proposition VI.1.

COROLLAIRE 2. — *Soient φ et ψ deux éléments de K ayant même trace sur k . Alors, il existe un élément θ de N , vérifiant $\text{Tr}_{N/K}(\theta) = \varphi$, $\text{Tr}_{N/K}(\sigma\theta) = \psi$, et deux choix de θ différent d'un élément de k de trace sur k nulle.*

Ce corollaire résulte du corollaire 1, appliqué en prenant $A = k$.

PROPOSITION VI.2. — *Soit M un sous- $A[G]$ -module projectif de A_N , contenant A_K et A_k . Alors, $M = A_N$, et l'extension N/k est modérément ramifiée.*

Démonstration. — Soit $\theta \in A_N$. Posons

$$\varphi = \text{Tr}_{N/K}(\theta), \quad \psi = \text{Tr}_{N/K}(\sigma\theta).$$

Il est clair que les traces sur κ de φ et de ψ sont égales. D'après la proposition VI.1, il existe un élément θ' de M vérifiant $\text{Tr}_{N/K}(\theta') = \varphi$, $\text{Tr}_{N/K}(\sigma\theta') = \psi$. Posons $\lambda = \theta - \theta'$. D'après le corollaire 2 de la proposition VI.1, $\lambda \in k$. Comme θ et θ' appartiennent à A_N ,

$$\lambda \in A_N \cap k = A_k,$$

donc à M . Il en résulte que $\theta = \lambda + \theta'$ appartient à M , ce qui entraîne la première assertion. La seconde assertion résulte alors de la première et du théorème II.1.

THEOREME VI.1. — (Critère de base normale).

Soit $\theta \in A_N$. Si le A -module $A[G]\theta$ contient A_K et A_k , $A[G]\theta = A_N$; autrement dit, θ et ses conjugués forment une A -base normale de A_N .

Démonstration. — Le A -module $A[G]\theta$ est un $A[G]$ -module libre, donc projectif, et qui contient A_K et A_k . D'après la proposition VI.2, $A[G]\theta = A_N$.

Remarque. — Soit $T : A_N \longrightarrow A_K \times A_K$ l'application définie par $T(\theta) = (\text{Tr}_{N/K}(\theta), \text{Tr}_{N/K}(\sigma\theta))$, et soit $T' : A_K \times A_K \longrightarrow A$ l'application définie par $T'(\varphi, \psi) = \text{Tr}_{K/\kappa}(\varphi - \psi)$.

Supposons l'extension N/κ modérément ramifiée. Il résulte de la proposition VI.1, corollaire 1, que la suite de modules et d'applications $0 \longrightarrow A_k^0 \longrightarrow A_N \xrightarrow{T} A_K \times A_K \xrightarrow{T'} A \longrightarrow 0$ est exacte, A_k^0 désignant l'ensemble des éléments de A_k de trace nulle. On en déduit, entre les classes des A -modules A_k^0 , A_N , et A_K la relation $cl(A_N) = cl(A_k^0) cl(A_K)^2$. La suite exacte

$$0 \longrightarrow A_k^0 \longrightarrow A_k \xrightarrow{\text{Tr}_{k/\kappa}} A \longrightarrow 0$$

montre en outre que $cl(A_k^0) = cl(A_k)$, d'où la relation :

$$cl(A_N) = cl(A_k) cl(A_K)^2.$$

On peut démontrer cette relation à l'aide des méthodes du chapitre III. On doit alors supposer que A vérifie l'hypothèse (H), mais, on démontre alors l'égalité ci-dessus sans supposer que l'extension $N/\mathcal{K}$ est modérément ramifiée.

2. Bases normales de A_K .

PROPOSITION VI.3. — *On suppose que A_K possède une H-base, et que A vérifie l'une des hypothèses suivantes :*

- i) p est inversible dans A
- ii) pA est un idéal maximal de A ,

Alors :

- a) A_K possède une H-base (φ, ψ) où $\text{Tr}_{K/\mathcal{K}}(\varphi) = \text{Tr}_{K/\mathcal{K}}(\psi)$.
- b) Si K est modérément ramifiée en p , A_K possède une H-base (φ, ψ) , où $\text{Tr}_{K/\mathcal{K}}(\varphi) = \text{Tr}_{K/\mathcal{K}}(\psi) = 1$.

Démonstration. — Soit (φ', ψ') une H-base de A_K , $T = \text{Tr}_{K/\mathcal{K}}(\varphi')$, $U = \text{Tr}_{K/\mathcal{K}}(\psi')$. Si p est inversible dans A , posons $\varphi = \varphi' + \frac{1-T}{p}$, $\psi = \psi' + \frac{1-U}{p}$. Il est évident que (φ, ψ) est encore une H-base de A_K , et que $\text{Tr}_{K/\mathcal{K}}(\varphi) = \text{Tr}_{K/\mathcal{K}}(\psi) = 1$.

Si pA est un idéal maximal de A et si $K/\mathcal{K}$ n'est pas modérément ramifiée en p , alors $\text{Tr}_{K/\mathcal{K}}(A_K) \neq A$ (Théorème II.1). Comme

$$\text{Tr}_{K/\mathcal{K}}(A_K) \supset pA,$$

et que pA est maximal, $\text{Tr}_{K/\mathcal{K}}(A_K) = pA$. Il en résulte que T et U sont des éléments de pA . Posons $\varphi = \varphi' - \frac{T}{p}$, $\psi = \psi' - \frac{U}{p}$. Alors, (φ, ψ) est clairement une H-base de A_K et $\text{Tr}_{K/\mathcal{K}}(\varphi) = \text{Tr}_{K/\mathcal{K}}(\psi) = 0$.

Si pA est maximal et si $K/\mathcal{K}$ est modérément ramifiée en p ,

$$\text{Tr}_{K/\mathcal{K}}(A_K) = A$$

(Théorème II.1). Alors, $\text{Tr}_{K/\mathcal{K}}(1) = p$, $\text{Tr}_{K/\mathcal{K}}(\varphi') = T$, $\text{Tr}_{K/\mathcal{K}}(\psi') = U$,

$\text{Tr}_{K/\kappa}(\sigma^i \varphi' + \sigma^{-i} \varphi') = 2T$, $\text{Tr}_{K/\kappa}(\sigma^i \psi' + \sigma^{-i} \psi') = 2U$. L'idéal $\text{Tr}_{K/\kappa}(A_K)$ de A est donc engendré par les éléments p , T et U de A . Il en résulte que l'un au moins des nombres T , U (T par exemple) n'appartient pas à pA . On peut trouver des éléments a et b de A , tels que $aT + bp = 1$. Posons $\psi'' = \psi' - aU\varphi - bU + 1$. Il est clair que (φ', ψ'') est une H-base de A_K , et que

$$\text{Tr}_{K/\kappa}(\psi'') = U - aUT - bUp + p = p.$$

Soient alors

$$\begin{aligned}\varphi &= a\varphi' + b\psi'' \\ \psi &= (a - p)\varphi' + (b + T)\psi''.\end{aligned}$$

$$\sigma^i \varphi + \sigma^{-i} \varphi = a(\sigma^i \varphi' + \sigma^{-i} \varphi') + b(\sigma^i \psi'' + \sigma^{-i} \psi'')$$

$\sigma^i \psi + \sigma^{-i} \psi = (a - p)(\sigma^i \varphi' + \sigma^{-i} \varphi') + (b + T)(\sigma^i \psi'' + \sigma^{-i} \psi'')$; on peut donc exprimer φ , ψ , $\sigma^i \varphi + \sigma^{-i} \varphi$, $\sigma^i \psi + \sigma^{-i} \psi$ en fonction de φ' , ψ' , $\sigma^i \varphi' + \sigma^{-i} \varphi'$, $\sigma^i \psi' + \sigma^{-i} \psi'$ à l'aide de combinaisons linéaires à coefficients dans A .

Mais $\begin{pmatrix} a & b \\ a - p & b + T \end{pmatrix} \in \text{SL}(2, A)$. Il en résulte bien que $1, \varphi, \psi, \sigma^i \varphi + \sigma^{-i} \varphi, \sigma^i \psi + \sigma^{-i} \psi$ ($1 \leq i \leq \frac{p-3}{2}$) est une A-base de A_K , donc que (φ, ψ) est une H-base.

De plus, $\text{Tr}_{K/\kappa}(\varphi) = aT + bp = 1$

et $\text{Tr}_{K/\kappa}(\psi) = (a - p)T + (b + T)p = 1$,

ce qui prouve que (φ, ψ) est une H-base répondant à la question.

PROPOSITION VI.4. — Si A_K possède une H-base (φ, ψ) , où

$$\text{Tr}_{K/\kappa}(\varphi) = \text{Tr}_{K/\kappa}(\psi),$$

A_K possède une base quasi-normale. (Définition II.4). Si, de plus, N/κ est modérément ramifiée, A_K possède une base quasi-normale $(1, \theta, \dots, \theta_{p-1})$, telle que θ_i s'écrit sous la forme $\text{Tr}_{N/K}(\sigma^i \theta)$, avec $\theta \in A_N$.

Démonstration. — D'après la proposition VI.1, corollaire 2, il existe un $\theta \in N$, tel que $\theta + \tau\theta = \varphi$, $\sigma\theta + \tau\sigma\theta = \psi$. Posons

$$\theta_i = \sigma^i \theta + \tau \sigma^i \theta .$$

Montrons que 1 forme avec $p - 1$ des éléments θ_i une A-base de A_K .

On a $\varphi = \theta_0$, $\psi = \theta_1$, $\sigma^i \varphi + \sigma^{-i} \varphi = \theta_i + \theta_{-i}$,

$\sigma^i \psi + \sigma^{-i} \psi = \theta_{i+1} + \theta_{1-i}$. Les p éléments de la H-base (φ, ψ) de A_K s'expriment par les formules ci-dessus en fonction de 1 et des θ_i ($i \not\equiv -\frac{p-1}{2} \pmod{p}$).

Réciproquement, ces mêmes formules permettent de calculer de proche en proche les θ_i ($i \not\equiv -\frac{p-1}{2} \pmod{p}$) en fonction des éléments de la H-base (φ, ψ) . Donc, $1, \theta_0, \theta_1, \theta_{-1}, \dots, \theta_{\frac{p-3}{2}}, \theta_{\frac{p-1}{2}}$ est une A-base de A_K . La formule $\sum \theta_i = \text{Tr}_{N/K}(\theta)$ (voir proposition II.4) montre que 1 forme avec $(p - 1)$ éléments quelconques pris parmi les θ_i une base quasi-normale de A_K/A .

Si N/K est modérément ramifiée, la proposition VI.1, corollaire 1, montre qu'on peut prendre $\theta \in A_N$, c.q.f.d.

THEOREME VI.2. — *Soit A un anneau principal ; supposons que A vérifie l'une des hypothèses suivantes :*

- i) p est inversible dans A, et $[\kappa' : \kappa] = p - 1$
- ii) pA est un idéal maximal de A.

Alors :

- a) A_K possède des A-bases quasi-normales
- b) Si K/κ est modérément ramifiée en p , A_K possède des A-bases normales.
- c) Si N/κ est modérément ramifiée, A_K possède des bases normales formées à partir d'un élément de A_N .

Démonstration :

a) Le théorème V.3 montre que A_K possède des H-bases. La proposition VI.3,a) montre que A_K possède une H-base (φ, ψ) , où $\text{Tr}_{K/\kappa}(\varphi) = \text{Tr}_{K/\kappa}(\psi)$. La proposition VI.4 prouve alors que A_K possède une A-base quasi-normale formée avec un $\theta \in N$, pour lequel

$$\text{Tr}_{N/K}(\theta) = \text{Tr}_{K/\kappa}(\varphi) .$$

b) Si en outre K/κ est modérément ramifiée en p , la proposition VI.1,b, montre qu'on peut prendre $\text{Tr}_{K/\kappa}(\varphi) = 1$. Il est clair que, dans ces conditions, θ engendre une A -base normale de A_K .

c) Si N/κ est modérément ramifiée, la proposition VI.4 montre que θ peut être pris dans A_N .

Exemples. — Le théorème VI.2 s'applique en particulier lorsque $A = \mathbb{Z}$, ou, plus généralement, lorsque $A = S^{-1}\mathbb{Z}$, S étant une partie multiplicative de $\mathbb{Z}$ ne contenant pas 0.

Si A est l'anneau des entiers d'un corps de nombre dans lequel p reste premier et si A est principal, le théorème VI.1 s'applique encore.

Lorsque p ne reste pas premier dans A , mais ne se ramifie pas, ou encore lorsque A n'est plus principal, on peut encore essayer de déterminer le réseau $f(A_K)$ et d'étudier l'existence des H -bases. Par contre, si p se ramifie dans A , l'hypothèse (H) n'est plus vérifiée, et les résultats des chapitres IV et V ne s'appliquent plus.

THEOREME VI.3. — *Supposons que p soit inversible dans A . Les propositions suivantes sont équivalentes :*

- i) A_N est $A[G]$ -libre
- ii) A_K et A_κ possèdent des A -bases normales.

Démonstration :

i) $\implies$ ii). C'est la proposition II.4.

ii) $\implies$ i). Puisque A_K et A_κ possèdent des A -bases normales, l'extension N/κ est modérément ramifiée (proposition II.6). Il en résulte que A_K possède une A -base normale obtenue à partir d'un élément θ de A_N , (Théorème VI.2,c). Quitte à multiplier θ par une unité de A , on peut supposer que $\text{Tr}_{N/\kappa}(\theta) = 1$. On peut de même supposer que A_κ possède une base normale $(\omega, \tau\omega)$ avec

$$\text{Tr}_{\kappa/\kappa}(\omega) = \omega + \tau\omega = 1.$$

Alors, $\text{Tr}_{N/\kappa}(\theta) - \omega$ est un entier de A_κ de trace sur κ nulle. On peut donc écrire cet entier sous la forme $\text{Tr}_{N/\kappa}(\theta) - \omega = a(\omega - \tau\omega)$

avec $a \in A$. Posons $\theta' = \theta - \frac{a}{p}(\omega - \tau\omega)$; il est clair que

$$\text{Tr}_{N/K}(\theta') = \text{Tr}_{N/K}(\theta), \quad \text{et que} \quad \text{Tr}_{N/K}(\theta') = \omega.$$

Le A -module $A[G]\theta'$ contient donc A_K et A_K . Il en résulte (Théorème VI.1) que θ' est une $A[G]$ -base de A_N , c.q.f.d.

3. Propriétés de l'algèbre $A[G]$.

PROPOSITION VI.5. — Soit $u \in \mathfrak{K}[G]$. Si, pour tout i ,

$$(1 + \tau)\sigma^i u \in A[G],$$

il existe $v \in A[G]$, tel que $(1 + \tau)\sigma^i v = (1 + \tau)\sigma^i u$.

Démonstration. — Ecrivons $u = \sum_{j \bmod p} (a_j + a'_j \tau) \sigma^j$, où les a_j et a'_j sont des éléments de $\mathfrak{K}$. Alors,

$$(1 + \tau)\sigma^i u = \sum_{j \bmod p} (a_{j-i} + a'_{j+i}) (1 + \tau)\sigma^j.$$

Comme $(1 + \tau)\sigma^i u$ est un élément de $A[G]$, les $a_{j-i} + a'_{j+i}$ sont des éléments de A quels que soient i et j . On déduit de cette remarque que, pour tout i , $a_0 + a'_i \in A$ et $a_0 - a_i \in A$. Posons $h_i = a_i - a_0$, $h'_i = a_i + a_0$, et soit $v = \sum_{j \bmod p} (h_j + h'_j \tau) \sigma^j$. Il est clair que $v \in A[G]$, et que $(1 + \tau)\sigma^i v = (1 + \tau)\sigma^i u$.

DEFINITION VI.1. — Dans $A[G]$, on note T l'élément $\sum_{i \bmod p} \sigma^i$ et T' l'élément $(1 - \tau)T$.

On voit immédiatement que T et T' sont des éléments du centre de $A[G]$; en particulier $T' = T(1 - \tau)$. Si $u = \sum_{i \bmod p} (a_i + a'_i \tau) \sigma^i$ est un élément de $A[G]$, un calcul facile montre que

$$uT' = T'u = \left(\sum_{i \bmod p} a_i - b_i \right) T'.$$

On voit donc que le sous-ensemble AT' de $A[G]$ est un idéal bilatère de $A[G]$.

DEFINITION VI.2. — On désigne par $\mathcal{A}$ l'algèbre $A[G]/AT'$.

Nous aurons besoin d'étudier les éléments inversibles de $A[G]$ et de $\mathcal{A}$. Remarquons que $A[G]$ et $\mathcal{A}$ sont des anneaux noethériens, car ce sont des A -modules de type fini. On en déduit qu'un élément de $A[G]$ ou de $\mathcal{A}$ inversible à droite ou à gauche est inversible; c'est-à-dire possède un inverse à gauche et à droite unique (Bourbaki, Algèbre, Ch. VIII, § 2, exercices 7 et 8, [3]).

Soit f l'application de G dans A définie par $f(\sigma) = +1$ et $f(\tau) = -1$; cette application se prolonge en un homomorphisme de A algèbres de $A[G]$ sur A , que nous notons encore f .

Il est clair que f est nul sur l'idéal AT' de $A[G]$.

DEFINITION VI.3. — On note $\bar{f}$ l'homomorphisme de $\mathcal{A}$ dans A déduit de f par passage au quotient.

PROPOSITION VI.6. — Soit $u = \sum_{i \bmod p} (a_i + a'_i \tau) \sigma^i$ un élément de $A[G]$. Si l'image $\bar{u}$ de u dans $\mathcal{A}$ est un élément inversible de $\mathcal{A}$, alors $\sum_{i \bmod p} (a_i - a'_i) \sigma^i$ est un élément inversible de A .

Démonstration. — En effet, la quantité $\sum_{i \bmod p} (a_i - a'_i) \sigma^i$ n'est autre que l'image de $\bar{u}$ par l'homomorphisme $\bar{f}$.

PROPOSITION VI.7. — Soit r un entier vérifiant $0 \leq r \leq p-1$. Définissons deux suites d'entier $h_i^{(r)}$ et $h'_i{}^{(r)}$ ($0 \leq i \leq p-1$) par : $h_i^{(r)} = 1$ pour $0 \leq i \leq r$, $h_i^{(r)} = 0$ pour $r+1 \leq i \leq p-1$, $h_0'^{(r)} = 0$, $h_i'^{(r)} = -1$ pour $1 \leq i \leq r$, $h_i'^{(r)} = 0$ pour $r+1 \leq i \leq p-1$. Notons $u^{(r)}$ l'élément $\sum_{i=0}^{p-1} (h_i^{(r)} + h_i'^{(r)} \tau) \sigma^i$ de $A[G]$. Alors, si $r \neq \frac{p-1}{2}$, l'image dans $\mathcal{A}$ de $u^{(r)}$ est un élément inversible de $\mathcal{A}$.

Démonstration. — Puisque $r \not\equiv \frac{p-1}{2} \pmod{p}$, $2r+1$ est inversible modulo p . On peut donc trouver deux entiers positifs n et a tels que $n(2r+1) = ap - r$. Dans $A[G]$, on a l'identité

$$\left(\sum_{i=-r}^{i=+r} \sigma^i\right) \left(\sum_{j=1}^n \sigma^{(2r+1)j}\right) = \sum_{i=r+1}^{pa} \sigma^i = aT - \sum_{i=1}^r \sigma^i$$

On en déduit l'identité :

$$\begin{aligned} & \left(1 + (1 - \tau) \sum_{i=1}^r \sigma^i\right) \left(1 + (1 - \tau) \sum_{i=1}^n \sigma^{(2r+1)i}\right) \\ &= 1 + (1 - \tau) \left[\sum_{i=1}^r \sigma^i + \sum_{i=1}^n \sigma^{(2r+1)i} \right. \\ & \quad + \left(\sum_{i=1}^r \sigma^i\right) \left(\sum_{i=1}^n \sigma^{(2r+1)i}\right) \\ & \quad \left. + \left(\sum_{i=-r}^{-1} \sigma^i\right) \left(\sum_{i=1}^n \sigma^{(2r+1)i}\right) \right] \\ &= 1 + (1 - \tau)aT = 1 + aT' \equiv 1 \pmod{AT'}. \end{aligned}$$

$1 + (1 - \tau) \sum_{i=1}^r \sigma^i$ est donc inversible à droite dans $A[G]/AT'$.

4. Propriétés des bases normales de A_K .

Pour tout $\theta \in N$, on note $\theta_i = \sigma^i \theta + \tau \sigma^i \theta$.

PROPOSITION VI.8. — Soit θ_i ($i \pmod p$) une base normale de A_K . Il existe $\theta' \in N$, tel que $\theta'_i = \theta_i$, et qui forme avec ses conjugués une base normale de $N/\mathcal{N}$.

Démonstration. — Supposons qu'il y ait entre θ et ses conjugués une relation $\sum_{j \pmod p} a_j \sigma^j \theta + a'_j \tau \sigma^j \theta = 0$, avec des coefficients a_j , a'_j non tous nuls. En faisant opérer $(1 + \tau)\sigma^i$, on trouve, pour tout i , tout j , $\sum_{j \pmod p} (a_{j-i} + a'_{j+i}) (1 + \tau)\sigma^i \theta = 0$, ce qui entraîne

$$a_{j-i} + a'_{j+i} = 0$$

quels que soient i et j . On déduit immédiatement de ces relations les égalités $a_i = a_0$ et $a'_i = -a_0$ quel que soit i . La relation entre θ et ses conjugués est donc nécessairement de la forme $a_0 T'\theta = 0$. Soit alors λ un élément non nul de k , vérifiant $\text{Tr}_{k/k}(\lambda) = 0$. Posons $\theta' = \theta + \lambda$. Il est clair que $\theta_i = \theta'_i$. De plus,

$$T'\theta' = (1 - \tau) \sum_{i \bmod p} \sigma^i \theta' = 2p\lambda$$

n'est pas nul, car on a supposé la caractéristique de κ distincte de 2 et de p .

Donnons-nous un élément θ de N , tel que les $(\theta_i)_{i \bmod p}$ soient une base normale de A_K , et soit $u \in A[G]$. Si θ' est un autre élément de N tel que $\theta'_i = \theta_i$, alors, $(\theta - \theta')_i = 0$. Il résulte de la proposition VI.1 que $\lambda = \theta - \theta'$ est un élément de A_K , de trace sur κ nulle. Alors, pour tout i , $(u\theta)_i - (u\theta')_i = (u(\theta - \theta'))_i = (u\lambda)_i = 0$. Par conséquent le p -uplet $(u\theta)_i (i \bmod p)$ de A_K ne dépend pas du choix de θ définissant la base normale (θ_i) de A_K . De même, si v est un élément de $A[G]$ ayant même image que u dans $\mathcal{A}$,

$$(u\theta)_i - (v\theta)_i = ((u - v)\theta)_i = (1 + \tau)\sigma^i(u - v)\theta = (1 + \tau)(u - v)\theta = 0,$$

car $(1 + \tau)(u - v) = 0$.

Ce qui précède montre que, à tout élément $\bar{u} \in \mathcal{A}$ et à toute base normale B de A_K , on peut associer un p -uplet d'éléments de A_K , noté $\bar{u}(B)$ et défini de la manière suivante : on choisit $\theta \in N$, tel que $B = (\theta_i)_{i \bmod p}$, et un élément u de $A[G]$ ayant $\bar{u}$ pour image dans $\mathcal{A}$, et l'on pose $\bar{u}(B) = ((u\theta)_i)_{i \bmod p}$.

PROPOSITION VI.9. — Soit B une base normale de A_K . L'application qui à un élément $\bar{u}$ de $\mathcal{A}$ associe le p -uplet $\bar{u}(B)$ d'éléments de A_K établit une bijection entre l'ensemble des éléments inversibles de $\mathcal{A}$ et l'ensemble des bases normales de A_K .

Démonstration. — Nous choisissons un θ de N , tel que

$$B = (\theta_i)_{i \bmod p}$$

et qui soit une $\kappa[G]$ -base de N (proposition VI.8).

a) Si $\bar{u}$ est inversible dans A , $\bar{u}(B)$ est une base normale. En effet, soit u un représentant de $\bar{u}$ dans $A[G]$. Nous devons montrer que l'ensemble $(u\theta)_i (i \bmod p)$ est une A -base de A_K . La formule $(u\theta)_i = (1 + \tau)\sigma^i u\theta$ montre que l'on peut exprimer les $(u\theta)_i$ en fonction des θ_i . Mais, comme $\bar{u}$ est inversible dans $\mathcal{A}$, il existe $v \in A[G]$ et $a \in A$ tels que $vu = 1 + aT'$. Alors,

$$(vu\theta)_i = \theta_i + (aT'\theta)_i = \theta_i$$

car $(T'\theta)_i = (1 + \tau)\sigma^i T'\theta = (1 + \tau)T'\sigma^i \theta = 0$; cela montre que θ_i , qui s'écrit sous la forme $(1 + \tau)\sigma^i v(u\theta)$ peut être exprimé comme combinaison linéaire à coefficients dans A des $(u\theta)_i$.

b) L'application $\bar{u} \longrightarrow \bar{u}(B)$ est surjective.

En effet, soit B' une base normale de A_K , et soit θ' une $\kappa[G]$ -base de N telle que $B' = \theta'_i$. Il existe deux éléments u et u' de $\kappa[G]$, inverses l'un de l'autre, tels que $\theta' = u\theta$, $\theta = u'\theta'$. En exprimant $\theta'_i = (1 + \tau)\sigma^i u\theta$ en fonction des θ_i , on voit que, pour tout i , $(1 + \tau)\sigma^i u \in A[G]$. De même, pour tout i , $(1 + \tau)\sigma^i u' \in A[G]$. Il existe donc des éléments v et v' de $A[G]$ vérifiant

$$(1 + \tau)\sigma^i u = (1 + \tau)\sigma^i v$$

et $(1 + \tau)\sigma^i u' = (1 + \tau)\sigma^i v'$ pour tout i (proposition VI.5). On a donc $\theta'_i = (v\theta)_i$, ce qui s'écrit, en notant $\bar{v}$ l'image de v dans $\mathcal{A}$, $B' = \bar{v}(B)$. Mais u et v d'une part, u' et v' d'autre part diffèrent d'un élément de $\kappa T'$. On en déduit que $vv' - uu'$ est un élément de $\kappa T' \cap A[G] = AT'$, donc que $vv' - 1 \in AT'$, c'est-à-dire que v est inversible dans $\mathcal{A}$.

c) L'application $\bar{u} \longrightarrow \bar{u}(B)$ est injective.

En effet, soit $\bar{u}$ et $\bar{v}$ deux éléments de $\mathcal{A}$ tels que $\bar{u}(B) = \bar{v}(B)$, et soient u et v des représentants dans $A[G]$ de $\bar{u}$ et de $\bar{v}$. Pour tout i , $(1 + \tau)\sigma^i u\theta = (1 + \tau)\sigma^i v\theta$. Comme θ est une $\kappa[G]$ -base de N , on a $(1 + \tau)\sigma^i (u - v) = 0$ pour tout i , ce qui entraîne que $u - v \in AT'$, donc que $\bar{u} = \bar{v}$, c.q.f.d.

On suppose maintenant que p n'est pas inversible dans A et que N/κ est modérément ramifiée en p (c'est-à-dire en tout idéal premier non nul $\mathfrak{Q}$ divisant pA). On pose $S = \bigcap_{\mathfrak{Q} \mid pA} (A - \mathfrak{Q})$. S est donc une partie multiplicative de A , et $S^{-1}A$ est un anneau de Dedekind semi-

local. On notera A_p cet anneau. Pour toute extension L de $\mathcal{K}$,

$$(A_p)_L = S^{-1} A_L.$$

Soient φ et ψ deux éléments de A_K , ayant même trace sur $\mathcal{K}$. La proposition VI.1 montre qu'il existe un θ de $(A_p)_N$, tel que $\varphi = \text{Tr}_{N/K}(\theta)$, $\psi = \text{Tr}_{N/K}(\sigma\theta)$. Si $\theta' \in (A_p)_N$ vérifie $\text{Tr}_{N/K}(\theta') = \varphi$, $\text{Tr}_{N/K}(\sigma\theta') = \psi$, $\theta' - \theta = \lambda$, où $\lambda \in (A_p)_K$ et $\text{Tr}_{K/K}(\lambda) = 0$ (Proposition VI.1). Donc,

$$\text{Tr}_{N/K}(\theta') - \text{Tr}_{N/K}(\theta) = \text{Tr}_{N/K}(\theta' - \theta) = p\lambda \in p(A_K).$$

On voit donc qu'à tout couple (φ, ψ) de A_K , tel que $\text{Tr}_{K/K}(\varphi) = \text{Tr}_{K/K}(\psi)$ est associé un élément de $(A_p)_K/p(A_p)_K$, à savoir la classe dans $(A_p)_K$ modulo $p(A_p)_K$ de $\text{Tr}_{N/K}(\theta)$, où θ est un élément de $(A_p)_N$, vérifiant $\theta + \tau\theta = \varphi$, $\sigma\theta + \tau\sigma\theta = \psi$.

Si $(\theta_i)_{i \bmod p}$ est une A -base normale de A_K on a $\theta_i = \sigma^i\theta + \tau\sigma^i\theta$ pour un θ de $(A_p)_N$. La construction précédente, faite en prenant $(\varphi, \psi) = (\theta_0, \theta_1)$, associe à la base normale $B = (\theta_i)_{i \bmod p}$ un élément bien déterminé de $(A_p)_K/p(A_p)_K$, noté $g(B)$.

THEOREME VI.4. — Soit B une A -base normale de A_K . Alors, quel que soit l'idéal premier $\mathfrak{P}$ de A divisant pA ,

$$(1 - \tau)g(B) \notin \mathfrak{P}(A_p)_K/p(A_p)_K.$$

Démonstration. — Comme B est une A -base normale de A_K , B est aussi une A_p -base normale de $(A_p)_K$. On peut donc, pour faire la démonstration, supposer que $A = A_p$. L'extension $N/\mathcal{K}$ est alors modérément ramifiée (en p , par hypothèse, en 2, car 2 est inversible dans A). Comme A est semi-local, A_N est un $A[G]$ -module libre (Ch. II, § 6). Soit donc θ' une $A[G]$ -base de A_N . L'élément $\text{Tr}_{N/K}(\theta')$ de A_K est une $A[G/H]$ -base de A_K . Il en résulte que, pour tout idéal premier $\mathfrak{P}$ de A divisant pA , $(1 - \tau)\text{Tr}_{N/K}(\theta') \notin \mathfrak{P}A_K$.

Notons B' la base normale $(\theta'_i)_{i \bmod p}$ de A_K . Ce qui précède montre que, pour tout idéal premier $\mathfrak{P}$ de A divisant pA ,

$$(1 - \tau)g(B') \notin \mathfrak{P}A_K/pA_K.$$

La proposition VI.9 montre qu'il existe un élément inversible $\bar{u}$ de $\mathcal{A}$ pour lequel $B' = \bar{u}(B)$. Soit $u = \sum_{j \bmod p} (a_j + a'_j\tau)\sigma^j$ un représen-

tant de u dans $A[G]$. Nous avons :

$$\mathrm{Tr}_{N/k}(\theta') = \left(\sum_{j \bmod p} a_j \right) \mathrm{Tr}_{N/k}(\theta) + \left(\sum_{j \bmod p} a'_j \right) \tau \mathrm{Tr}_{N/k}(\theta).$$

On en déduit que

$$g(B') = \left(\sum a_j \right) g(B) + \left(\sum a'_j \right) \tau g(B),$$

$$\text{d'où} \quad (1 - \tau) g(B') = \left(\sum_{j \bmod p} a_j - a'_j \right) (1 - \tau) g(B),$$

et cette dernière égalité entraîne le résultat cherché.

5. Construction des $A[G]$ -bases de A_N .

Nous arrivons maintenant aux théorèmes essentiels de ce travail. Nous rappelons dans les énoncés toutes les hypothèses nécessaires.

THEOREME VI.5. — *Soit A un anneau principal, κ son corps des fractions. On suppose que la caractéristique de κ ne divise pas $2p$, et que A/pA est un corps à p éléments. Soit N/κ une extension de degré $2p$ de κ , galoisienne, non abélienne, de groupe de Galois G , K un sous-corps de degré p de N , k le sous-corps quadratique de N , A_k , A_K et A_N les clôtures intégrales de A dans k , K et N respectivement. Alors, si A_K et A_k possèdent des A -bases normales, A_N est $A[G]$ -libre.*

Démonstration du théorème. — On peut supposer que les éléments des A -bases normales de A_K et A_k qui nous sont données ont une trace sur κ égale à 1. Soit donc $(\omega, \tau\omega)$ une A -base normale de A_k . Alors, $\omega + \tau\omega = 1$. Comme A_K et A_k possèdent des A -bases normales, N/κ est modérément ramifiée (Proposition II.6). A_K possède donc une A -base normale $(\theta_i)_{i \bmod p}$ où $\theta_i = \sigma^i \theta + \tau \sigma^i \theta$, θ étant un élément de A_N . Soit $\lambda = \mathrm{Tr}_{N/k}(\theta)$. Alors,

$$\lambda + \tau\lambda = \mathrm{Tr}_{N/k}(\theta) = \mathrm{Tr}_{K/k}(\theta_i) = 1.$$

Mais A_K/pA_k contient p^2 éléments. Les $\mu \in A_k$, vérifiant $\mu + \tau\mu \equiv 1$

mod pA_k se répartissent en p classes modulo pA_k , dont $(p-1)$ classes pour lesquelles $\mu - \tau\mu \notin pA_k$. Posons $\theta^{(r)} = u^{(r)}\theta$, $u^{(r)}$ étant l'élément de $A[G]$ défini dans la proposition VI.7.

Comme $\sum_{i \bmod p} h_i^{(r)} + h_i'^{(r)} = 1$, $\text{Tr}_{N/k}(\theta^{(r)}) = 1$, d'où $\text{Tr}_{K/k}(\theta_i^{(r)}) = 1$.

Comme $\sum_{i \bmod p} h_i^{(r)} - h_i'^{(r)} = 2r + 1$, $\lambda_r = \text{Tr}_{N/k}(\theta^{(r)})$ prend les $p-1$ valeurs modulo pA_k pour lesquelles $\lambda_r + \tau\lambda_r = 1$, $\lambda_r - \tau\lambda_r \notin pA_k$. Pour un r convenable, on a donc $\lambda_r - \tau\lambda_r \equiv \omega - \tau\omega \bmod pA_k$. Quitte à remplacer $\theta^{(r)}$ par $\theta^{(r)} + \mu$, pour un μ convenable de A_k , de trace sur k nulle, on peut supposer que $\lambda_r - \tau\lambda_r = \omega - \tau\omega$. Comme $\lambda_r + \tau\lambda_r = 1 = \omega + \tau\omega$, on a alors $\lambda_r = \omega$. Il en résulte que le A -module engendré par $\theta^{(r)}$ et ses conjugués contient A_K et A_k , donc coïncide avec A_N (Théorème VI.2), c.q.f.d.

Nous étudions maintenant des cas particuliers où k est le corps des rationnels.

THEOREME VI.6. — (Théorème de la base normale). *Soit N une extension galoisienne non abélienne de degré $2p$ du corps Q des rationnels, G son groupe de Galois, Z l'anneau des entiers rationnels, S une partie multiplicative de Z , ne contenant pas 0, A le sous-anneau $S^{-1}Z$ de Q , B la clôture intégrale de A dans N . On suppose l'extension N/Q modérément ramifiée (par rapport à l'anneau A). Alors, B est un $A[G]$ -module libre.*

Démonstration. — Soit k le sous-corps quadratique de N , et m l'entier sans facteur carré tel que $k = Q(\sqrt{m})$. Puisque N/Q est modérément ramifiée, il en est de même de k/Q . Cela entraîne que $\frac{1 + \sqrt{m}}{2}$, $\frac{1 - \sqrt{m}}{2}$ est une A -base normale de l'anneau A_k des éléments de k entier sur A : c'est bien connu si $m \equiv 1 \bmod 4$, et, si $m \not\equiv 1 \bmod 4$, 2 est certainement inversible dans A , sinon, k/Q ne serait pas modérément ramifiée. Par conséquent, A_k possède des A -bases normales.

D'autre part, A est un anneau principal ; si $pZ \cap S \neq \emptyset$, p est inversible dans A . Si $pZ \cap S = \emptyset$, pA est un idéal maximal. Nous sommes alors dans les conditions d'application du théorème VI.1.

K désignant un sous-corps de degré p de N , et A_K l'anneau des éléments de K entiers sur A , A_K possède des A -bases normales. Si p est inversible dans A , le théorème VI.6 résulte immédiatement du théorème VI.3. Si p n'est pas inversible dans A , A/pA est alors isomorphe à $\mathbb{Z}/p\mathbb{Z}$, et le théorème VI.6 résulte du théorème VI.5.

Appendice

Monsieur Jean-Pierre Serre m'a fait remarquer que la plupart des arguments du chapitre VI de ce travail s'appliquent à un $A[G]$ -module M de type fini, de rang 1 (c'est-à-dire tel que $M \otimes_A \kappa$ soit un $\kappa[G]$ -module libre avec un générateur), éventuellement projectif. En fait, seuls le théorème VI.3 et le paragraphe V devraient être remaniés ; partout ailleurs, le fait que le module M soit l'anneau des entiers du corps N n'intervient plus, sinon pour utiliser le théorème V.3 ; c'est finalement ce théorème qui est essentiel pour démontrer les théorèmes VI.5 et VI.6.

Index des définitions

	Chapitre	Paragraphe
Base normale	II	III
Base quasi-normale	II	V
Classe (d'un module)	I	II
Décomposée (extension)	II	IV
H-base	V	II
Hypothèses (H) et (H')	III	II
Idéaux essentiels	IV	V
Ramifiée (extension non —, extension modérément —)	I	I
Relativement projectif (module)	II	V
Réseau	I	III
Résolvante de Lagrange	IV	II

Index des notations

Nous reproduisons ici les principales notations utilisées dans les chapitres III à VI.

	Chapitre	Paragraphe
A, A_L	III	I
$A_k, A_K, A_N, \dots$ cf. k, K, N ,		
A, A'_0	IV	I
$\tilde{A}$	IV	IV
$d, D, \mathcal{O}, \delta, \bar{D}$	III	I
$\Delta(L/K), \mathcal{O}_{L/K}$	I	IV et V
$f(\theta)$	V	I
$\mathfrak{F}$	III	III
g, G	III	I
G'	IV	I
H	III	I
H^*	IV	II
i'	IV	II
$\bar{i}, i^*$	IV	V
$\mathfrak{u}, k, K$	III	I
$\mathfrak{u}', k', K'$	III	I
$\mathfrak{u}'_0$	IV	I
χ_A	I	III et IV
χ_0	IV	II
M_1	IV	VI
N	III	I
N'	III	I
T, T'	VI	III

BIBLIOGRAPHIE

- [1] ANKENY, CHOWLA, HASSE, "On the class number of the maximal real subfield of a cyclotomic field", *Jour. reine angew. Math.* 217 (1965) 217-220.
- [2] E. ARTIN, "Questions de base minimale dans la théorie des nombres algébriques", *Colloque du C.N.R.S. Algèbre et théorie des nombres*. Paris (1949) 19-20.
- [3] N. BOURBAKI, "Algèbre" Chapitre V et VIII, Paris (1959).
- [4] N. BOURBAKI, "Algèbre commutative" Chapitre VII, Paris (1965).
- [5] H. CARTAN, S. EILENBERG, "Homological Algebra", Princeton (1956).
- [6] A. CHATELET, "Arithmétique des corps abéliens du troisième degré", *Annales scientifiques de l'E.N.S.* 63 (1946) 109-160.
- [7] A. CHATELET, "Idéaux principaux dans les corps circulaires", *Colloque du C.N.R.S. Algèbre et théorie des nombres*. Paris (1949) 103-106.
- [8] H. HASSE, "Zahlentheorie", Berlin (1963).
- [9] E. HECKE, "Vorlesungen über die Theorie der algebraischen Zahlen", Leipzig (1923), Réimpression : New-York (1948).
- [10] D. HILBERT, "Théorie des corps de nombres algébriques", Paris (1913).
- [11] M. P. LEE, "Integral representations of dihedral groups of order $2p$ ", *Trans. Amer. Math. Soc.* 110 (1964) 213-231.
- [12] H.W. LEOPOLDT, "Über die Hauptordnung der ganzen Elementen eines abelschen Zahlkörpers", *Jour. reine angew. Math.* 201 (1959) 119-149.
- [13] J. MARTINET et J.J. PAYAN, "Sur les extensions cubiques non galoisiennes des rationnels et leur clôture galoisienne", *Jour. reine angew. Math.* 228 (1967) 15-37.
- [14] J. MARTINET et J.J. PAYAN, "Sur les bases d'entiers des extensions galoisiennes et non abéliennes de degré 6 des rationnels", *Jour. reine angew. Math.* 229 (1968) 29-33.

- [15] E. NOETHER, "Normal basis bei Körpern ohne höhere Verzweigung", *Jour. reine angew. Math.* 167 (1932) 147-152.
- [16] J.J. PAYAN, "Contribution à l'étude des corps abéliens absolus de degré premier impair", *Annales de l'institut Fourier* (1965) 133-199.
- [17] J.J. PAYAN, "Critère de décomposition d'une extension de Kummer sur un sous-corps du corps de base", *Annales de l'E.N.S.* (à paraître).
- [18] D.S. RIM, "Modules over finite groups", *Ann. of Math.* 69 (1959) 700-712.
- [19] P. SAMUEL, O. ZARISKI, "Commutative algebra", Volume 1.
- [20] J.P. SERRE, "Corps locaux", Paris, Hermann (1962).
- [21] R.G. SWANN, "Induced representations and projective modules". *Ann. of Math.* 71 (1960) 552-578.

(Thèse, Fac. Sciences, Grenoble 1968)

Jacques MARTINET
Département de Mathématiques
Faculté des Sciences
33-Bordeaux