PUBLICATIONS DE L'INSTITUT DE MATHÉMATIQUE
DE L'UNIVERSITÉ DE NANCAGO

VIII

JEAN-PIERRE SERRE

Corps locaux

Troisième édition, corrigée

HERMANN

AVERTISSEMENT

à la troisième édition

Cette édition est la reproduction photographique de la première; toutefois, la bibliographie a été augmentée et un certain nombre d'erreurs typographiques ont été corrigées.

ISBN 2 7056 1296 3

TABLE DES MATIÈRES

PREMIÈRE PARTIE

CORPS LOCAUX (GÉNÉRALITÉS)

CHAPITRE I

ANNEAUX DE VALUATION DISCRÈTE ET ANNEAUX DE DEDEKIND

§ 1. *Définition des anneaux de valuation discrète*

Un anneau A est appelé un *anneau de valuation discrète* si c'est un anneau principal (Bourbaki, *Alg.*, Chap. VII), et s'il possède un idéal premier non nul $\mathfrak{m}(A)$ et un seul.

[On rappelle qu'un idéal $\mathfrak{p}$ d'un anneau commutatif A est dit *premier* si l'anneau quotient $A/\mathfrak{p}$ est intègre.]

Le corps $A/\mathfrak{m}(A)$ s'appelle le *corps résiduel* de A. Les éléments inversibles de A sont ceux qui n'appartiennent pas à $\mathfrak{m}(A)$; ils forment un groupe multiplicatif; on les appelle parfois les *unités* de A (ou du corps des fractions de A) : nous utiliserons rarement cette terminologie, qui peut prêter à confusion.

Dans un anneau principal, les idéaux premiers non nuls sont les idéaux de la forme πA, où π est un élément irréductible. La définition ci-dessus revient donc à dire que A possède un élément irréductible et un seul, à la multiplication par un élément inversible près; un tel élément est appelé une *uniformisante* de A.

Les idéaux non nuls de A sont de la forme $\mathfrak{m}(A)^n = \pi^n A$, où π est une uniformisante. Si $x \neq 0$ est un élément A, on peut écrire $x = \pi^n u$, avec $n \in \mathbf{N}$, et u inversible; l'entier n est appelé la *valuation* (ou *l'ordre*) de x, et noté $v(x)$; il ne dépend pas du choix de π.

Soit K le corps des fractions de A, et soit K^* le groupe multiplicatif des éléments non nuls de K. Si $x = a/b$ est un élément de K^*, on peut encore écrire x sous la forme $\pi^n u$, avec $n \in \mathbf{Z}$ cette fois, et poser $v(x) = n$. On vérifie immédiatement les propriétés suivantes :

a) *L'application* $v : K^* \to \mathbf{Z}$ *est un homomorphisme surjectif.*

b) *On a* $v(x+y) \geqslant \mathrm{Inf}\,(v(x), v(y))$.

(Il est commode de convenir que $v(0) = +\infty$.)

La connaissance de la fonction v détermine l'anneau A : c'est l'ensemble des $x \in K$ tels que $v(x) \geqslant 0$; de même $\mathfrak{m}(A)$ est l'ensemble des $x \in K$ tels que $v(x) > 0$. On aurait donc pu partir de v. De façon précise :

PROPOSITION 1. *Soit* K *un corps, et soit* $v : K^* \to \mathbf{Z}$ *un homomorphisme vérifiant les propriétés* a) *et* b). *L'ensemble* A *des* $x \in K$ *tels que* $v(x) \geqslant 0$ *est un anneau de valuation discrète, dont* v *est la valuation associée.*

En effet, soit π un élément tel que $v(\pi) = 1$. Tout $x \in A$ s'écrit sous la forme $x = \pi^n u$, avec $n = v(x)$, et $v(u) = 0$, c'est-à-dire u inversible. Tout idéal non nul de A est donc de la forme $\pi^n A$, avec $n \geqslant 0$, ce qui montre bien que A est un anneau de valuation discrète.

Exemples d'anneaux de valuation discrète.

1) Soit p un nombre premier, et soit $\mathbf{Z}_{(p)}$ le sous-ensemble du corps $\mathbf{Q}$ des rationnels formé des fractions r/s, où s n'est pas divisible par p; c'est un anneau de valuation discrète de corps résiduel le corps $\mathbf{F}_p$ à p éléments. Si v_p désigne la valuation associée, $v_p(x)$ n'est autre que l'exposant de p dans la décomposition de x en facteurs premiers.

Un procédé analogue s'applique à tout anneau principal (et même à tout anneau de Dedekind, cf. § 3).

2) Soit k un corps, et soit $k((T))$ le corps des *séries formelles à une variable* sur k. Pour toute série formelle non nulle

$$f(T) = \sum_{n \geqslant n_0} a_n T^n, \qquad a_{n_0} \neq 0,$$

on définit l'*ordre* $v(f)$ de f comme l'entier n_0 (cf. Bourbaki, *Alg.*, Chap. IV). On obtient ainsi une valuation discrète de $k((T))$, dont l'anneau de valuation est $k[[T]]$, ensemble des séries formelles à exposants $\geqslant 0$; son corps résiduel est k.

3) Soit V une variété algébrique normale, de dimension n, et soit W une sous-variété irréductible de V, de dimension $n - 1$. Soit $A_{V/W}$ l'anneau local de V en W (c'est-à-dire l'ensemble des fonctions rationnelles f sur V qui sont définies en au moins un point de W). L'hypothèse de normalité montre que $A_{V/W}$ est un anneau intégralement clos; l'hypothèse sur les dimensions montre que c'est un anneau local de dimension 1; c'est donc un anneau de valuation discrète (cf. § 2, prop. 3); son corps résiduel est le corps des fonctions rationnelles sur W. Si v_W désigne la valuation associée, et si f est une fonction rationnelle sur V, l'entier $v_W(f)$ est appelé l'« ordre » de f en W; c'est la multiplicité de W dans le diviseur des zéros et des pôles de f.

4) Soit S une *surface de Riemann* (c'est-à-dire une variété analytique complexe de dimension 1), et soit $P \in S$. L'anneau $\mathfrak{O}_P$ des fonctions holomorphes sur un voisinage (non précisé) de P est un anneau de valuation discrète, isomorphe au sous-anneau de $\mathbf{C}[[T]]$ formé des séries convergentes; son corps résiduel est $\mathbf{C}$.

§ 2. Caractérisations des anneaux de valuation discrète

PROPOSITION 2. *Soit* A *un anneau commutatif. Pour que* A *soit un anneau de valuation discrète, il faut et il suffit que ce soit un anneau local noethérien, et que son idéal maximal soit engendré par un élément non nilpotent.*

[On rappelle qu'un anneau A est dit *local* s'il possède un seul idéal maximal, *noethérien* si toute suite croissante d'idéaux de A est stationnaire (ou, ce qui revient au même, si tout idéal de A est engendré par un nombre fini d'éléments).]

Il est clair qu'un anneau de valuation discrète vérifie les propriétés de l'énoncé. Inversement, supposons que A vérifie ces propriétés, et soit π un générateur de l'idéal maximal $\mathfrak{m}(A)$ de A. Soit $\mathfrak{u}$ l'idéal de l'anneau A formé des éléments x tels que $x\pi^m = 0$ pour m assez grand; puisque A est noethérien, $\mathfrak{n}$ est de type fini, et on en conclut qu'il existe un N fixe tel que $x\pi^N = 0$ pour tout $x \in \mathfrak{n}$. Ceci étant, nous allons prouver que l'intersection des puissances $\mathfrak{m}(A)^n$ est réduite à 0 (c'est là en fait un résultat valable dans tout anneau local noethérien, cf. Bourbaki, *Alg. comm.*, Chap. III, § 3). Soit $y \in \bigcap \mathfrak{m}(A)^n$; on peut écrire $y = \pi^n x_n$ pour tout n, d'où

$$\pi^n(x_n - \pi x_{n+1}) = 0, \qquad \text{et} \qquad x_n - \pi x_{n+1} \in \mathfrak{u}.$$

La suite des idéaux $\mathfrak{n} + Ax_n$ étant croissante, on en conclut que $x_{n+1} \in \mathfrak{n} + Ax_n$ pour n grand, d'où $x_{n+1} = z + tx_n$, $z \in \mathfrak{n}$, et comme $x_n = \pi x_{n+1} + z'$, $z' \in \mathfrak{n}$, on en tire $(1 - \pi t)x_{n+1} \in \mathfrak{n}$; mais $1 - \pi t$ n'appartient pas à $\mathfrak{m}(A)$, donc est inversible (A étant local); on en conclut que x_{n+1} appartient à $\mathfrak{u}$ pour n assez grand, et, en prenant $n + 1 \geqslant N$, on voit que $y = \pi^{n+1}x_{n+1}$ est nul, ce qui achève de prouver que

$$\bigcap \mathfrak{m}(A)^n = 0.$$

Par hypothèse, aucun des $\mathfrak{m}(A)^n$ n'est nul. Si y est un élément non nul de A, y peut donc s'écrire sous la forme $\pi^n u$, avec u non dans $\mathfrak{m}(A)$, c'est-à-dire u inversible.

Cette écriture est visiblement unique; elle montre déjà que A est intègre. De plus, si l'on pose $n = v(y)$, on vérifie sans difficultés que la fonction v se prolonge en une valuation discrète du corps des fractions de A dont l'anneau de valuation est A, c.q.f.d.

Remarque. Lorsque l'on sait d'avance que A est intègre (ce qui est fréquent dans les applications), on a $\mathfrak{u} = 0$, $\pi x_n = x_{n+1}$, et la démonstration ci-dessus se simplifie notablement.

PROPOSITION 3. *Soit* A *un anneau intègre noethérien. Pour que* A *soit un anneau de valuation discrète, il faut et il suffit qu'il vérifie les deux conditions suivantes*:

(*i*) A *est intégralement clos.*

(*ii*) A *possède un idéal premier non nul et un seul.*

[On rappelle qu'un élément x d'un anneau contenant A est dit *entier* sur A s'il vérifie une équation « de dépendance intégrale » :

$$(*) \qquad x^n + a_1x^{n-1} + \cdots + a_n = 0, \qquad \text{avec} \quad a_i \in A.$$

On dit que A est *intégralement fermé* dans un anneau B le contenant si tout élément de B qui est entier sur A appartient à A. On dit que A est *intégralement clos* s'il est intègre et s'il est intégralement fermé dans son corps des fractions. Cf. Bourbaki, *Alg. comm.*, Chap. V, § 1.]

Il est clair qu'un anneau de valuation discrète vérifie (*ii*). Montrons qu'il vérifie (*i*). Soit K le corps des fractions de A, et soit x un élément de K vérifiant une équation du type (*), et supposons x non dans A. Cela signifie que $v(x) = -m$, avec $m > 0$. Dans l'équation (*), le premier terme a pour valuation $-nm$, alors que la valuation des autres est $\geqslant -(n-1)m$, qui est $> -m$; c'est une contradiction, d'après le lemme suivant :

LEMME 1. *Soit* A *un anneau de valuation discrète, et soient x_i des éléments de son corps des fractions tels que $v(x_i) > v(x_1)$ pour $i \geqslant 2$. On a alors*

$$x_1 + x_2 + \cdots + x_n \neq 0.$$

Quitte à diviser par x_1, on peut supposer $x_1 = 1$, d'où $v(x_i) \geqslant 1$ pour $i \geqslant 2$, c'est-à-dire $x_i \in \mathfrak{m}(A)$; comme $x_1 \notin \mathfrak{m}(A)$, on en déduit $x_1 + \cdots + x_n \notin \mathfrak{m}(A)$ ce qui démontre le lemme.

[Cette démonstration prouve en outre que l'élément $x_1 + \cdots + x_n$ a même valuation que x_1.]

Montrons maintenant qu'un anneau intègre et noethérien A qui vérifie (*i*) et (*ii*) est un anneau de valuation discrète. La condition (*ii*) montre que A est un anneau local dont l'idéal maximal $\mathfrak{m}$ est $\neq 0$. Soit $\mathfrak{m}'$ l'ensemble des $x \in K$ tels que $x\mathfrak{m} \subset A$ (c'est-à-dire $xy \in A$ pour tout $y \in \mathfrak{m}$); c'est un sous-A-module de K contenant A. Si y est un élément non nul de $\mathfrak{m}$, on a évidemment $\mathfrak{m}' \subset y^{-1}A$, et comme A est noethérien, ceci montre que $\mathfrak{m}'$ est un A-module de type fini (c'est ce qu'on appelle un « idéal fractionnaire » de K par rapport à A). Soit $\mathfrak{m}.\mathfrak{m}'$ le produit de $\mathfrak{m}$ et de $\mathfrak{m}'$, c'est-à-dire l'ensemble des $\sum x_i y_i$, $x_i \in \mathfrak{m}$, $y_i \in \mathfrak{m}'$; par définition de $\mathfrak{m}'$, on a $\mathfrak{m}.\mathfrak{m}' \subset A$; d'autre part, puisque $A \subset \mathfrak{m}'$, on a $\mathfrak{m}.\mathfrak{m}' \supset \mathfrak{m}$; puisque $\mathfrak{m}.\mathfrak{m}'$ est un idéal, on a donc, soit $\mathfrak{m}.\mathfrak{m}' = \mathfrak{m}$, soit $\mathfrak{m}.\mathfrak{m}' = A$. On va successivement montrer :

I. *Si* $\mathfrak{m}.\mathfrak{m}' = A$, *l'idéal* $\mathfrak{m}$ *est principal.*

II. *Si* $\mathfrak{m}.\mathfrak{m}' = \mathfrak{m}$, *et si* (*i*) *est vérifiée, on a* $\mathfrak{m}' = A$.

III. *Si* (*ii*) *est vérifiée, on a* $\mathfrak{m}' \neq A$.

En combinant II et III, on verra alors que $\mathfrak{m}.\mathfrak{m}' = \mathfrak{m}$ est impossible, d'où, d'après I, le fait que $\mathfrak{m}$ est principal, donc que A est un anneau de valuation discrète (prop. 2).

Reste à démontrer les assertions I, II, III.

Démonstration de I.

Si $\mathfrak{m}.\mathfrak{m}' = A$, on a une relation $\sum x_i y_i = 1$, avec $x_i \in \mathfrak{m}$, $y_i \in \mathfrak{m}'$. Les produits $x_i y_i$ appartiennent tous à A; l'un au moins, soit xy, n'appartient pas à $\mathfrak{m}$, donc est un élément inversible u. Remplaçant x par xu^{-1}, on obtient une relation $xy = 1$, avec $x \in \mathfrak{m}$ et $y \in \mathfrak{m}'$. Si $z \in \mathfrak{m}$, on a $z = x(yz)$, avec $yz \in A$ puisque $y \in \mathfrak{m}'$; donc z est un multiple de x, ce qui montre bien que $\mathfrak{m}$ est un idéal principal, engendré par x.

Démonstration de II.

Supposons que $\mathfrak{m}.\mathfrak{m}' = \mathfrak{m}$, et soit $x \in \mathfrak{m}'$. On a donc $x\mathfrak{m} \subset \mathfrak{m}$, d'où, en itérant, $x^n\mathfrak{m} \subset \mathfrak{m}$ pour tout n, c'est-à-dire $x^n \in \mathfrak{m}'$. Soit a_n le sous-A-module de K engendré par les

puissances $\{1, x, \ldots, x^n\}$ de x; on a $\mathfrak{a}_n \subset \mathfrak{a}_{n+1}$, et tous les $\mathfrak{a}_n$ sont contenus dans le A-module de type fini $\mathfrak{m}'$. Puisque A est noethérien, on a donc $\mathfrak{a}_{n-1} = \mathfrak{a}_n$ pour n grand, c'est-à-dire $x^n \in \mathfrak{a}_{n-1}$. On peut alors écrire $x^n = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$, $b_i \in A$, ce qui montre que x est entier sur A. La condition (i) entraîne alors $x \in A$, donc $\mathfrak{m}' = A$.

Démonstration de III.

Soit x un élément non nul de $\mathfrak{m}$, et formons l'anneau A_x des fractions de la forme y/x^n, avec $y \in A$, et $n \geqslant 0$ arbitraire. La condition (*ii*) entraîne $A_x = K$. En effet, sinon, A_x ne serait pas un corps, et contiendrait un idéal maximal non nul, soit $\mathfrak{p}$; comme x est inversible dans A_x, on aurait $x \notin \mathfrak{p}$, ce qui montre que $\mathfrak{p} \cap A \neq \mathfrak{m}$. D'autre part, si y/x^n est un élément non nul de $\mathfrak{p}$, on a $y \in \mathfrak{p} \cap A$, d'où $\mathfrak{p} \cap A \neq 0$. Enfin, puisque $\mathfrak{p}$ est premier, il en est de même de $\mathfrak{p} \cap A$, ce qui est contraire à (*ii*).

Ainsi, tout élément de K s'écrit y/x^n; appliquons ceci à $1/z$, avec $z \neq 0$, et $z \in A$. On obtient $1/z = y/x^n$, d'où $x^n = yz \in zA$. Tout élément de $\mathfrak{m}$ a donc une puissance qui appartient à l'idéal zA. Soient $x_1, \ldots, x_k$ des générateurs de $\mathfrak{m}$, et soit n assez grand pour que $x_i^n \in zA$ pour tout i; si l'on choisit $N > k(n-1)$, tous les monômes en les x_i de degré total N contiennent en facteur un x_i^n, donc appartiennent à zA; comme l'idéal $\mathfrak{m}^N$ est engendré par ces monômes, on a $\mathfrak{m}^N \subset zA$. Appliquons ceci avec $z \in \mathfrak{m}$. On en conclut qu'il existe un plus petit entier $N \geqslant 1$ tel que $\mathfrak{m}^N \subset zA$; choisissons $y \in \mathfrak{m}^{N-1}$, $y \notin zA$ (on pose $\mathfrak{m}^0 = A$, par convention). On a alors $my \subset zA$, d'où $y/z \in \mathfrak{m}'$, et $y/z \notin A$, ce qui prouve bien que $\mathfrak{m}' \neq A$ et achève la démonstration.

Remarque. La construction de $\mathfrak{m}'$ n'utilise pas les hypothèses faites sur A et $\mathfrak{m}$; pour tout idéal non nul $\mathfrak{a}$ d'un anneau intègre A, on peut définir $\mathfrak{a}'$ comme l'ensemble des $x \in K$ tels que $x\mathfrak{a} \subset A$; si A est noethérien, c'est un idéal fractionnaire. Lorsque $\mathfrak{a}\mathfrak{a}' = A$, on dit que $\mathfrak{a}$ est *inversible*. La démonstration de I prouve que, dans un anneau local, tout idéal inversible est principal.

§ 3. *Anneaux de Dedekind*

Rappel. Soit A un anneau intègre, de corps des fractions K, et soit S une partie de A stable pour la multiplication et contenant 1 (une telle partie sera appelée *multiplicative*); on suppose en outre que 0 n'appartient pas à S. L'ensemble des éléments de K de la forme x/s, $x \in A$, $s \in S$ est un anneau que l'on note $S^{-1}A$. L'application $\mathfrak{p}' \to \mathfrak{p}' \cap A$ est une bijection de l'ensemble des idéaux premiers de $S^{-1}A$ sur l'ensemble des idéaux premiers de A ne rencontrant pas S.

Ceci s'applique notamment lorsque $S = A - \mathfrak{p}$, où $\mathfrak{p}$ est un idéal premier de A. L'anneau $S^{-1}A$ correspondant se note $A_{\mathfrak{p}}$; c'est un anneau local d'idéal maximal $\mathfrak{p}A_{\mathfrak{p}}$ et de corps résiduel le corps des fractions de $A/\mathfrak{p}$; les idéaux premiers de $A_{\mathfrak{p}}$ correspondant aux idéaux premiers de A contenus dans $\mathfrak{p}$. On dit que $A_{\mathfrak{p}}$ est le *localisé de* A *en* $\mathfrak{p}$ (ou *pour* $\mathfrak{p}$), cf. Bourbaki, *Alg. comm.*, Chap. II, § 2.

PROPOSITION 4. *Si* A *est un anneau intègre noethérien, les deux propriétés suivantes sont équivalentes* :

(i) *Pour tout idéal premier* $\mathfrak{p} \neq 0$ *de* A, $A_{\mathfrak{p}}$ *est un anneau de valuation discrète.*

(ii) A *est intégralement clos et de dimension* $\leqslant 1$.

[Un anneau intègre A est dit de dimension $\leqslant 1$ si tout idéal premier non nul de A est maximal; il revient au même de dire que, si $\mathfrak{p}$ et $\mathfrak{p}'$ sont deux idéaux premiers de A tels que $\mathfrak{p} \subset \mathfrak{p}'$, on a $\mathfrak{p} = 0$ ou $\mathfrak{p} = \mathfrak{p}'$.]

(i) *entraîne* (ii) : Si $\mathfrak{p} \subset \mathfrak{p}'$, alors $A_{\mathfrak{p}'}$ contient l'idéal premier $\mathfrak{p}A_{\mathfrak{p}'}$, ce qui entraîne $\mathfrak{p} = 0$ ou $\mathfrak{p} = \mathfrak{p}'$ (cf. prop. 3, (*ii*)). D'autre part, si a est entier sur A, il est *a fortiori* entier sur chaque $A_{\mathfrak{p}}$, et d'après la prop. 3, (*i*), il appartient à tous les $A_{\mathfrak{p}}$. Si l'on écrit a sous la forme $a = b/c$, avec $b, c \in A$ et $c \neq 0$, et si $\mathfrak{a}$ est l'idéal des $x \in A$ tels que $xb \in cA$, l'idéal $\mathfrak{a}$ n'est contenu dans aucun idéal premier $\mathfrak{p}$, d'où $\mathfrak{a} = A$ et $a \in A$.

(ii) *entraîne* (i) : Il est clair que les $A_{\mathfrak{p}}$ vérifient la condition (*ii*) de la prop. 3, et il suffit donc de prouver qu'ils sont intégralement clos. Soit x un élément entier sur $A_{\mathfrak{p}}$. En faisant apparaître un dénominateur commun des coefficients de l'équation de dépendance intégrale de x sur $A_{\mathfrak{p}}$, on peut écrire celle-ci sous la forme :

$$sx^n + a_1x^{n-1} + \cdots + a_n = 0, \qquad \text{avec} \quad a_i \in A, \quad s \in A - \mathfrak{p}.$$

Multipliant par s^{n-1}, on obtient une équation de dépendance intégrale de sx sur A, ce qui entraîne $sx \in A$, d'où $x \in A_{\mathfrak{p}}$.

Remarque. La démonstration ci-dessus établit en fait le résultat suivant :

Soit A *un sous-anneau d'un corps* K, *et soit* S *une partie multiplicative de* A *ne contenant pas* 0. *Pour qu'un élément de* K *soit entier sur* $S^{-1}A$, *il faut et il suffit qu'il soit de la forme* a'/s *où* a' *est entier sur* A, *et où* s *appartient à* S.

(Le passage aux anneaux de fractions commute à la fermeture intégrale.)

DÉFINITION. *Un anneau intègre, noethérien, et qui possède les deux propriétés équivalentes de la proposition* 4, *est appelé un anneau de Dedekind.*

Exemples: Tout anneau principal est un anneau de Dedekind. L'anneau des entiers d'un corps de nombres algébriques est un anneau de Dedekind (appliquer la prop. 9 ci-après à l'anneau $\mathbf{Z}$). Si V est une variété algébrique affine, définie sur un corps algébriquement clos k, l'anneau de coordonnées $k[V]$ de V est un anneau de Dedekind si et seulement si V est non singulière, irréductible, et de dimension $\leqslant 1$.

PROPOSITION 5. *Dans un anneau de Dedekind, tout idéal fractionnaire non nul est inversible.*

[Si K est le corps des fractions de A, un idéal fractionnaire $\mathfrak{a}$ de A est un sous-A-module de type fini de K. On dit que $\mathfrak{a}$ est inversible s'il existe $\mathfrak{a}' \subset K$ avec $\mathfrak{a}.\mathfrak{a}' = A$.]

Dans un anneau de valuation discrète, un idéal fractionnaire est de la forme $\pi^n A$, où $n \in \mathbf{Z}$, et est donc inversible. La proposition en résulte par localisation, compte tenu de :

$$(\mathfrak{a}.\mathfrak{b})_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}}\,\mathfrak{b}_{\mathfrak{p}}; \quad (\mathfrak{a} + \mathfrak{b})_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}} + \mathfrak{b}_{\mathfrak{p}}; \quad (\mathfrak{a} : \mathfrak{b})_{\mathfrak{p}} = (\mathfrak{a}_{\mathfrak{p}} : \mathfrak{b}_{\mathfrak{p}}) \quad \text{si } \mathfrak{b} \text{ est de type fini.}$$

[$(\mathfrak{a} : \mathfrak{b})$ désigne l'idéal des x de K tels que $x\mathfrak{b} \subset \mathfrak{a}$. Si $\mathfrak{a}' = (A : \mathfrak{a})$, dire que $\mathfrak{a}$ est inversible revient à dire que $\mathfrak{a}.\mathfrak{a}' = A$.]

COROLLAIRE. *Les idéaux fractionnaires non nuls d'un anneau de Dedekind forment un groupe pour la multiplication.*

Ce groupe est appelé le *groupe des idéaux* de l'anneau.

PROPOSITION 6. *Si $x \in A$, $x \neq 0$, il n'y a qu'un nombre fini d'idéaux premiers contenant x.*

En effet les idéaux contenant x vérifient la condition de chaîne descendante : si $Ax \subset \mathfrak{a} \subset \mathfrak{a}' \subset A$, on a $Ax^{-1} \supset \mathfrak{a}^{-1} \supset \mathfrak{a}'^{-1} \supset A$ et A est noethérien.

Il en résulte que si $x \in \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k, \ldots$, la suite

$$\mathfrak{p}_1 \supset \mathfrak{p}_1 \cap \mathfrak{p}_2 \supset \cdots \supset \mathfrak{p}_1 \cap \mathfrak{p}_3 \cap \cdots \cap \mathfrak{p}_k \supset \cdots$$

est stationnaire, ce qui veut dire que, à partir d'un certain rang, on a

$$\mathfrak{p}_i \supset \mathfrak{p}_1 \cap \mathfrak{p}_3 \cdots \cap \mathfrak{p}_k \supset \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_k$$

ce qui, comme les $\mathfrak{p}_\alpha$ sont premiers, montre que $\mathfrak{p}_i$ est l'un des $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$.

COROLLAIRE. *Si on note $v_\mathfrak{p}$ la valuation de* K *définie par* $A_\mathfrak{p}$, *pour tout $x \in K^*$, les nombres $v_\mathfrak{p}(x)$ sont presque tous nuls* (i. e. nuls sauf un nombre fini).

Soit maintenant $\mathfrak{a}$ un idéal fractionnaire quelconque de A; il n'est contenu que dans un nombre fini d'idéaux premiers $\mathfrak{p}$. L'image $\mathfrak{a}_\mathfrak{p}$ de $\mathfrak{a}$ dans $A_\mathfrak{p}$ est de la forme $\mathfrak{a}_\mathfrak{p} = (\mathfrak{p}A_\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{a})}$ où les $v_\mathfrak{p}(\mathfrak{a})$ sont des entiers rationnels presque tous nuls.

Si l'on considère l'idéal $\mathfrak{a}_1 = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}$ et l'idéal $\mathfrak{a}_2$ des x tels que $v_\mathfrak{p}(x) \geqslant v_\mathfrak{p}(\mathfrak{a})$ pour tout $\mathfrak{p}$, les trois idéaux $\mathfrak{a}$, $\mathfrak{a}_1$ et $\mathfrak{a}_2$ sont égaux *localement* (i. e. ont les mêmes images dans tous les $A_\mathfrak{p}$). Un raisonnement facile montre alors qu'ils sont égaux, d'où :

PROPOSITION 7. *Tout idéal fractionnaire $\mathfrak{a}$ de* A *s'écrit de manière unique sous la forme* :

$$\mathfrak{a} = \prod \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})},$$

où les $v_\mathfrak{p}(\mathfrak{a})$ sont des entiers presque tous nuls.

On a les formules suivantes, conséquences immédiates de la proposition précédente :

$$v_\mathfrak{p}(\mathfrak{a}.\mathfrak{b}) = v_\mathfrak{p}(\mathfrak{a}) + v_\mathfrak{p}(\mathfrak{b})$$
$$v_\mathfrak{p}((\mathfrak{b} : \mathfrak{a})) = v_\mathfrak{p}(\mathfrak{b}.\mathfrak{a}^{-1}) = v_\mathfrak{p}(\mathfrak{b}) - v_\mathfrak{p}(\mathfrak{a})$$
$$v_\mathfrak{p}(\mathfrak{a} + \mathfrak{b}) = \mathrm{Inf}\,(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b}))$$
$$v_\mathfrak{p}(x\mathrm{A}) = v_\mathfrak{p}(x).$$

De plus :

LEMME D'APPROXIMATION. *Soit k un entier. Pour tout i, $1 \leqslant i \leqslant k$, soient $\mathfrak{p}_i$ des idéaux premiers de* A *distincts deux à deux, x_i des éléments de* K, *et n_i des entiers. Il existe alors $x \in K$ tel que $v_{\mathfrak{p}_i}(x - x_i) \geqslant n_i$ pour tout i, et $v_\mathfrak{q}(x) \geqslant 0$ pour $\mathfrak{q} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_k$.*

Supposons d'abord que les x_i appartiennent à A, et cherchons une solution x appartenant à A. Par linéarité, on peut supposer que $x_2 = \cdots = x_k = 0$. Quitte à augmenter les n_i, on peut également supposer que ceux-ci sont $\geqslant 0$. Posons

$$\mathfrak{a} = \mathfrak{p}_1^{n_1} + \mathfrak{p}_2^{n_2} \ldots \mathfrak{p}_k^{n_k}.$$

On a $v_\mathfrak{p}(\mathfrak{a}) = 0$ pour tout $\mathfrak{p}$, d'où $\mathfrak{a} = A$. On en conclut que

$$x_1 = x + y, \qquad \text{avec} \qquad y \in \mathfrak{p}_1^{n_1}, \quad x \in \mathfrak{p}_2^{n_2} \ldots \mathfrak{p}_k^{n_k},$$

et l'élément x vérifie les propriétés voulues.

Dans le cas général, on pose $x_i = a_i/s$, avec $a_i \in A$, $s \in A$, $s \neq 0$, et $x = a/s$. L'élément a doit vérifier les conditions :

$$\begin{aligned} &v_{\mathfrak{p}_i}(a - a_i) \geqslant n_i + v_{\mathfrak{p}_i}(s), \qquad 1 \leqslant i \leqslant k, \\ &v_\mathfrak{q}(a) \geqslant v_\mathfrak{q}(s) \qquad \text{pour} \quad \mathfrak{q} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_k. \end{aligned}$$

Ces conditions sont du type envisagé ci-dessus (il faut adjoindre à la famille $\{\mathfrak{p}_i\}$ les idéaux premiers $\mathfrak{q}$ tels que $v_\mathfrak{q}(s) > 0$); d'où l'existence de a, ce qui achève de démontrer le lemme.

COROLLAIRE. *Un anneau de Dedekind qui n'a qu'un nombre fini d'idéaux premiers est principal.*

Il suffit de montrer que tous les idéaux premiers sont principaux. Or si $\mathfrak{p}$ est l'un d'entre eux, il existe $x \in A$ avec $v_\mathfrak{p}(x) = 1$ et $v_\mathfrak{q}(x) = 0$ pour $\mathfrak{q} \neq \mathfrak{p}$, c'est-à-dire tel que $xA = \mathfrak{p}$.

§ 4. *Extensions*

Dans tout ce paragraphe, on se donne un corps K et une extension de degré fini L de K; son degré [L : K] sera noté n.

On se donne également un anneau A, noethérien et intégralement clos, de corps des fractions K. On note B la *fermeture intégrale* de A dans L (c'est-à-dire l'ensemble des éléments de L qui sont entiers sur A). D'après la remarque qui suit la proposition 4, on a $K.B = L$. En particulier, le corps des fractions de B est L.

Nous ferons dans ce qui suit l'hypothèse suivante :

(F) *L'anneau* B *est un* A*-module de type fini.*

Cette hypothèse entraîne que B est un anneau noethérien intégralement clos.

PROPOSITION 8. *L'hypothèse* (F) *est vérifiée lorsque* L/K *est une extension séparable.*

Soit $\mathrm{Tr} : L \to K$ l'application *trace* (Bourbaki, *Alg.*, Chap. V, § 10, n° 6). On sait (*loc. cit.*, prop. 12) que $\mathrm{Tr}(xy)$ est une forme K-bilinéaire symétrique non dégénérée sur L. Si x appartient à B, les conjugués de x par rapport à K (dans une extension convenable de L) sont entiers sur A, et il en est de même de $\mathrm{Tr}(x)$ qui est leur somme; comme $\mathrm{Tr}(x) \in K$, on en conclut que $\mathrm{Tr}(x) \in A$.

Soit alors $\{e_i\}$ une base de L sur K, avec $e_i \in B$, et soit V le A-module libre engendré

par les e_i. Pour tout sous-A-module M de L, soit M* l'ensemble des $x \in L$ tels que $\mathrm{Tr}(xy) \in A$ pour tout $y \in M$. On a évidemment :

$$V \subset B \subset B^* \subset V^*.$$

Comme V* est le module libre engendré par la base duale de e_i (par rapport à la forme bilinéaire $\mathrm{Tr}(xy)$), on en conclut bien que B est un module de type fini.

Remarques. 1) Le même raisonnement montre que B* est un B-module de type fini, c'est-à-dire un idéal fractionnaire de B. Son inverse s'appelle la *différente* de B sur A, cf. Chap. III, § 3.

2) On peut montrer que l'hypothèse (F) est vérifiée lorsque A est une algèbre de type fini sur un corps (cf. Bourbaki, *Alg. comm.*, Chap. V), ou lorsque A est un anneau de valuation discrète complet (cf. Chap. II, § 2).

PROPOSITION 9. *Si* A *est de Dedekind,* B *est de Dedekind.*

On sait déjà, grâce à l'hypothèse (F), que B est noethérien intégralement clos. D'après la proposition 4, il nous suffit donc de montrer que B est de dimension $\leqslant 1$. Soit $\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \mathfrak{P}_2$ une chaîne d'idéaux premiers distincts de B. Le lemme suivant montre que les $\mathfrak{P}_i \cap A$ sont distincts (ce qui contredit le fait que A est de dimension $\leqslant 1$) :

LEMME 2. *Soient* A *et* B *deux anneaux, avec* $A \subset B$, *et* B *entier sur* A. *Si* $\mathfrak{P} \subset \mathfrak{Q}$ *sont deux idéaux premiers de* B *tels que* $\mathfrak{P} \cap A = \mathfrak{Q} \cap A$, *on a* $\mathfrak{P} = \mathfrak{Q}$.

Passant au quotient par $\mathfrak{P}$, on peut supposer que $\mathfrak{P} = 0$. Si $\mathfrak{Q} \neq \mathfrak{P}$, il existe un élément non nul $x \in \mathfrak{Q}$. Soit

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \qquad a_i \in A,$$

son équation minimale sur A. On a $a_0 \neq 0$, et a_0 appartient à l'idéal de B engendré par x, donc à $\mathfrak{Q} \cap A = \mathfrak{P} \cap A$, ce qui est absurde.

Remarque. On peut montrer que la proposition 9 reste valable même lorsque l'hypothèse (F) n'est pas vérifiée (cf. Bourbaki, *Alg. comm.*, Chap. VII).

Conservons les hypothèses de la prop. 9. Si $\mathfrak{P}$ est un idéal premier non nul de B, et si $\mathfrak{p} = \mathfrak{P} \cap A$, on dira que $\mathfrak{P}$ *divise* $\mathfrak{p}$ (ou que $\mathfrak{P}$ est « au-dessus » de $\mathfrak{p}$), et on écrira $\mathfrak{P}|\mathfrak{p}$. Cette relation équivaut aussi à dire que $\mathfrak{P}$ *contient* l'idéal $\mathfrak{p}B$ de B engendré par $\mathfrak{p}$. On notera $e_{\mathfrak{P}}$ l'exposant de $\mathfrak{P}$ dans la décomposition en idéaux premiers de $\mathfrak{p}B$. On a donc :

$$e_{\mathfrak{P}} = v_{\mathfrak{P}}(\mathfrak{p}B), \qquad \mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}.$$

L'entier $e_{\mathfrak{P}}$ est appelé *l'indice de ramification* de $\mathfrak{P}$ dans l'extension L/K.

D'autre part, si $\mathfrak{P}$ divise $\mathfrak{p}$, le corps $B/\mathfrak{P}$ est une extension du corps $A/\mathfrak{p}$. Comme B est de type fini sur A, $B/\mathfrak{P}$ est une extension de degré fini de $A/\mathfrak{p}$. Le degré de cette

extension est appelé le *degré résiduel* de $\mathfrak{P}$ dans l'extension L/K, et noté $f_{\mathfrak{P}}$. On a donc :

$$f_{\mathfrak{P}} = [B/\mathfrak{P} : A/\mathfrak{p}].$$

[Quand on veut préciser K, on écrit $e_{\mathfrak{P}/\mathfrak{p}}$ et $f_{\mathfrak{P}/\mathfrak{p}}$ au lieu de $e_{\mathfrak{P}}$ et $f_{\mathfrak{P}}$.]

Lorsqu'il y a un seul idéal premier $\mathfrak{P}$ qui divise $\mathfrak{p}$, et que $f_{\mathfrak{P}} = 1$, on dit que L/K est *totalement ramifiée* en $\mathfrak{p}$.

Lorsque $e_{\mathfrak{P}} = 1$ et que $B/\mathfrak{P}$ est séparable sur $A/\mathfrak{p}$, on dit que L/K est *non ramifiée* en $\mathfrak{P}$. Si L/K est non ramifiée pour tous les idéaux premiers $\mathfrak{P}$ divisant $\mathfrak{p}$, on dit que L/K est non ramifiée au-dessus de $\mathfrak{p}$ (ou « en $\mathfrak{p}$ »), cf. Chap. III, § 5.

PROPOSITION 10. *Soit $\mathfrak{p}$ un idéal premier non nul de* A. *L'anneau* $B/\mathfrak{p}B$ *est une* $A/\mathfrak{p}$*-algèbre de degré* $n = [L : K]$, *isomorphe au produit* $\prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}}$. *On a la formule :*

$$n = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}.$$

Soit $S = A - \mathfrak{p}$, soit $A' = S^{-1}A$, et soit $B' = S^{-1}B$. L'anneau $A' = A_{\mathfrak{p}}$ est un anneau de valuation discrète, et B' est sa fermeture intégrale dans L (cf. la remarque suivant la prop. 4). On a $A'/\mathfrak{p}A' = A/\mathfrak{p}$, et l'on voit facilement que $B'/\mathfrak{p}B' = B/\mathfrak{p}B$. Comme A' est principal, l'hypothèse (F) montre que B' est un module libre de rang $n = [L : K]$ et $B'/\mathfrak{p}B'$ est libre de rang n sur $A'/\mathfrak{p}A'$. On voit donc bien que $B/\mathfrak{p}B$ est une algèbre de degré n.

Puisque $\mathfrak{p}B = \bigcap \mathfrak{P}^{e_{\mathfrak{P}}}$, l'application canonique

$$B/\mathfrak{p}B \to \prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}}$$

est injective; le lemme d'approximation montre qu'elle est surjective; c'est donc un isomorphisme. En comparant les degrés, on voit que n est égal à la somme des degrés

$$n_{\mathfrak{P}} = [B/\mathfrak{P}^{e_{\mathfrak{P}}} : A/\mathfrak{p}].$$

On a $n_{\mathfrak{P}} = \sum_{i=0}^{i=e_{\mathfrak{P}}-1} [\mathfrak{P}^i/\mathfrak{P}^{i+1} : A/\mathfrak{p}] = e_{\mathfrak{P}} \cdot [B/\mathfrak{P} : A/\mathfrak{p}] = e_{\mathfrak{P}} f_{\mathfrak{P}}$, ce qui achève de démontrer la proposition.

COROLLAIRE. *Le nombre des idéaux premiers $\mathfrak{P}$ de* B *qui divisent un idéal premier $\mathfrak{p}$ de* A *est compris entre* 1 *et* n. *Si* A *n'a qu'un nombre fini d'idéaux premiers, il en est de même de* B (qui est donc principal).

Remarque. Lorsque l'hypothèse (F) n'est pas vérifiée, la somme des $e_{\mathfrak{P}} f_{\mathfrak{P}}$ est encore égale au degré de $B/\mathfrak{p}B$, mais ce degré peut être $< n$.

Soit $\mathfrak{P}$ un idéal premier non nul de B, et soit $\mathfrak{p} = A \cap \mathfrak{P}$. Il est clair que

$v_{\mathfrak{P}}(x) = e_{\mathfrak{P}} v_{\mathfrak{p}}(x)$ si $x \in K$. On dit (par abus de langage) que la valuation $v_{\mathfrak{P}}$ *prolonge* la valuation $v_{\mathfrak{p}}$ avec l'indice $e_{\mathfrak{P}}$. Réciproquement :

PROPOSITION 11. *Soit w une valuation discrète de* L *qui prolonge $v_{\mathfrak{p}}$ avec l'indice e. Il existe alors un diviseur premier $\mathfrak{P}$ de $\mathfrak{p}$ tel que $w = v_{\mathfrak{P}}$ et $e = e_{\mathfrak{P}}$.*

Soit W l'anneau de w, et soit $\mathfrak{N}$ son idéal maximal. Cet anneau est intégralement clos, de corps des fractions L, et contient A; il contient donc B. Soit $\mathfrak{P} = \mathfrak{N} \cap B$. On a évidemment $\mathfrak{P} \cap A = \mathfrak{p}$, d'où $\mathfrak{P}$ divise $\mathfrak{p}$. L'anneau W contient donc $B_{\mathfrak{P}}$. Mais on vérifie tout de suite que tout anneau de valuation discrète est un sous-anneau *maximal* de son corps des fractions. On a donc $W = B_{\mathfrak{P}}$, d'où $w = v_{\mathfrak{P}}$ et $e = e_{\mathfrak{P}}$.

§ 5. *Les homomorphismes de norme et d'injection*

On garde les hypothèses du paragraphe précédent. On note I_A et I_B les groupes des idéaux de A et de B. On va définir deux homomorphismes

$$i : I_A \to I_B$$
$$N : I_B \to I_A.$$

Comme I_A (resp I_B) est le groupe libre engendré par les idéaux premiers non nuls $\mathfrak{p}$ de A (resp $\mathfrak{P}$ de B), il suffit de définir $i(\mathfrak{p})$ et $N(\mathfrak{P})$. On pose :

$$i(\mathfrak{p}) = \mathfrak{p}B = \prod_{\mathfrak{P}\,|\,\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}$$
$$N(\mathfrak{P}) = \mathfrak{p}^{f_{\mathfrak{P}}} \quad \text{si} \quad \mathfrak{P}|\mathfrak{p}.$$

D'après la proposition 10, on a $N(i(\mathfrak{a})) = \mathfrak{a}^n$ pour tout $\mathfrak{a} \in I_A$. L'homomorphisme i fait correspondre à un idéal $\mathfrak{a}$ de A l'idéal $\mathfrak{a}B$ engendré par $\mathfrak{a}$.

Ces deux homomorphismes peuvent s'interpréter de façon plus suggestive au moyen de « groupes de Grothendieck » convenables :

Soit $\mathcal{C}_A$ la catégorie des A-modules de longueur finie. Si $M \in \mathcal{C}_A$ et si M est de longueur m, M possède une suite de Jordan-Hölder :

$$0 = M_0 \subset M_1 \subset \ldots \subset M_m = M,$$

chaque M_i/M_{i-1} étant isomorphe à un A-module simple, c'est-à-dire à un quotient $A/\mathfrak{p}_i$, où $\mathfrak{p}_i$ est un idéal premier non nul de A (on écarte le cas trivial où $A = K$). D'après le théorème de Jordan-Hölder, la suite des $A/\mathfrak{p}_i$ ne dépend, à une permutation près, que de M, et l'on peut poser :

$$\chi_A(M) = \prod \mathfrak{p}_i.$$

Exemple: Lorsque $M = \mathfrak{b}/\mathfrak{a}$, où $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux fractionnaires non nuls tels que $\mathfrak{a} \subset \mathfrak{b}$, on vérifie tout de suite que $\chi_A(M) = \mathfrak{a}.\mathfrak{b}^{-1}$. En particulier, $\chi_A(A/\mathfrak{a}) = \mathfrak{a}$ si $\mathfrak{a} \subset A$.

L'application $\chi_A : \mathcal{C}_A \to I_A$ est « multiplicative » : si l'on a une suite exacte :

$$0 \to M' \to M \to M'' \to 0$$

de A-modules de longueur finie, on a $\chi_A(M) = \chi_A(M')\chi_A(M'')$. Réciproquement, toute application multiplicative $f : \mathcal{C}_A \to G$, où G est un groupe commutatif, se met de façon unique sous la forme $g \circ \chi_A$, où g est un homomorphisme de I_A dans G (il suffit de définir $g(\mathfrak{p})$ comme $f(A/\mathfrak{p})$). En d'autres termes χ_A identifie le « *groupe de Grothendieck* » de $\mathcal{C}_A$ au groupe I_A.

Définissons de même $\mathcal{C}_B$ et $\chi_B : \mathcal{C}_B \to I_B$. Il est clair que tout B-module de longueur finie est de longueur finie sur A. On définit ainsi un foncteur exact $\mathcal{C}_B \to \mathcal{C}_A$, d'où un homomorphisme de I_B dans I_A. Cet homomorphisme n'est autre que la *norme*. En d'autres termes :

PROPOSITION 12. *Si* M *est un* B*-module de longueur finie, on a* $\chi_A(M) = N(\chi_B(M))$.

Par linéarité, il suffit de considérer le cas où $M = B/\mathfrak{P}$, auquel cas cela résulte de la définition de la norme.

D'autre part, tout A-module de longueur finie M définit par produit tensoriel avec B un module M_B de longueur finie. Le foncteur $\mathcal{C}_A \to \mathcal{C}_B$ ainsi défini est encore exact (par localisation, on se ramène au cas où A est principal, et B est alors un A-module libre). D'où également un homomorphisme $I_A \to I_B$ qui cette fois coïncide avec l'injection :

PROPOSITION 13. *Si* M *est un* A*-module de longueur finie, on a* $\chi_B(M_B) = i(\chi_A(M))$.

Par linéarité, il suffit de considérer le cas où $M = A/\mathfrak{p}$, d'où $M_B = B/\mathfrak{p}B$, et la proposition est évidente.

La proposition suivante montre que la restriction de N aux idéaux *principaux* de B coïncide avec l'application usuelle de norme définie dans Bourbaki, *Alg.*, Chap. V :

PROPOSITION 14. *Si* $x \in L$, *on a* $N(xB) = N_{L/K}(x)A$.

On peut supposer que x est entier sur A et en localisant que A est principal. L'anneau B est alors un A-module libre de rang n. Soit u_x la multiplication par x dans B. On a : $N_{L/K}(x) = \det(u_x)$ et $N(xB) = \chi_A(B/xB) = \chi_A(\operatorname{Coker} u_x)$. On est donc ramené au :

LEMME 3. *Soient* A *un anneau principal et* $u : A^n \to A^n$ *une application linéaire telle que* $\det(u) \neq 0$. *Alors* $\det(u)A = \chi_A(\operatorname{Coker} u)$.

L'idéal $\det(u)A$ ne changeant pas lorsqu'on multiplie u par une application linéaire inversible, on peut se ramener par le théorème des diviseurs élémentaires (Bourbaki, *Alg.*, Chap. VII, § 4, n° 5, prop. 4) au cas où u est diagonal. La démonstration se fait alors par récurrence sur n, le cas $n = 1$ étant la propriété déjà remarquée : $\chi_A(A/a) = a$.

§ 6. *Exemple : extensions monogènes*

Dans ce paragraphe, nous nous placerons de nouveau dans le *cas local*. Soit donc A un anneau local de corps résiduel k. Soit n un entier $\geqslant 1$, et soit $f \in A[X]$ un polynôme unitaire de degré n. Soit B_f l'anneau quotient de A[X] par l'idéal principal (f)

engendré par f. C'est une A-algèbre, libre et de type fini sur A, admettant pour base $|1, X, \ldots, X^{n-1}|$. Nous allons tout d'abord déterminer ses idéaux maximaux. Pour cela, notons $\mathfrak{m}$ l'idéal maximal de A, et posons $\overline{B}_f = B_f/\mathfrak{m}B_f = A[X]/(\mathfrak{m}, f)$. Si l'on note $\bar{f}$ l'image de f dans $k[X]$ par réduction mod. $\mathfrak{m}$, on a donc :

$$\overline{B}_f = k[X]/(\bar{f}).$$

Soit $\bar{f} = \prod_{i\in I} \varphi_i^{e_i}$ la décomposition en facteurs irréductibles du polynôme $\bar{f}$ dans $k[X]$, et, pour chaque i, choisissons un polynôme $g_i \in A[X]$ tel que $\bar{g}_i = \varphi_i$. Avec ces notations, on a :

LEMME 4. *Soit* $\mathfrak{m}_i = (\mathfrak{m}, g_i)$ *l'idéal de* B_f *engendré par* $\mathfrak{m}$ *et l'image canonique de* g_i *dans* B_f; *les idéaux* $\mathfrak{m}_i$, $i \in I$, *sont maximaux, deux à deux distincts, et tout idéal maximal de* B_f *est égal à l'un d'eux. Le quotient* $B_f/\mathfrak{m}_i$ *est isomorphe au corps* $k_i = k[X]/(\varphi_i)$.

Par définition, $\mathfrak{m}_i$ est image réciproque dans B_f de l'idéal $\overline{\mathfrak{m}}_i$ de $\overline{B}_f$ engendré par φ_i; comme $\overline{B}_f/(\varphi_i) = k_i = k[X]/(\varphi_i)$, il est clair que $\mathfrak{m}_i$ est maximal et que $B_f/\mathfrak{m}_i = k_i$. Pour montrer que tout idéal maximal $\mathfrak{u}$ de B_f est égal à l'un des $\mathfrak{m}_i$, il suffit de prouver que $\mathfrak{u}$ contient $\mathfrak{m}$ (car alors $\mathfrak{u}$ sera l'image réciproque de l'un des idéaux maximaux (φ_i) de $\overline{B}_f$). Or, sinon, on aurait $\mathfrak{u} + \mathfrak{m}B_f = B_f$, et comme B_f est un A-module de type fini, le lemme de Nakayama (Bourbaki, *Alg.*, Chap. VIII, § 6, n° 3) montrerait que $\mathfrak{u} = B_f$, ce qui est absurde.

Supposons maintenant que A soit un *anneau de valuation discrète*; nous allons donner deux cas particuliers dans lesquels on peut affirmer que B_f est lui aussi un anneau de valuation discrète.

(i) *Cas non ramifié.*

PROPOSITION 15. *Si* A *est un anneau de valuation discrète, et si* $\bar{f}$ *est irréductible,* B_f *est un anneau de valuation discrète d'idéal maximal* $\mathfrak{m}B_f$, *de corps résiduel* $k[X]/(\bar{f})$.

D'après le lemme 4, B_f est un anneau local, d'idéal maximal $\mathfrak{m}B_f$, et de corps résiduel $k[X]/(\bar{f})$. De plus, si π engendre $\mathfrak{m}$, l'image de π dans B_f engendre $\mathfrak{m}B_f$ et n'est pas un élément nilpotent. D'après la proposition 2, B_f est un anneau de valuation discrète, c.q.f.d.

COROLLAIRE 1. *Si* K *est le corps des fractions de* A, *le polynôme* f *est irréductible dans* K[X]. *Si de plus* L *désigne le corps* K[X]/(f), *l'anneau* B_f *est la fermeture intégrale de* A *dans* L.

On a $K[X]/(f) = B_f \otimes_A K$. Comme B_f est intègre, on en conclut que $B_f \otimes_A K$ l'est aussi, donc que $K[X]/(f)$ est un corps. Comme B_f est intégralement clos et admet pour corps des fractions L, c'est bien la fermeture intégrale de A dans L.

COROLLAIRE 2. *Si* $\bar{f}$ *est un polynôme séparable, l'extension* L/K *est non ramifiée.*

C'est clair.

La proposition 15 admet la réciproque suivante :

PROPOSITION 16. *Soit* A *un anneau de valuation discrète, de corps des fractions* K, *et soit* L *une extension finie de degré* n *de* K. *Soit* B *la fermeture intégrale de* A *dans* L. *Supposons*

que B *soit un anneau de valuation discrète, et que le corps résiduel* $\mathbf{L}$ *de* B *soit une extension monogène de degré n du corps résiduel* $k = \mathbf{K}$ *de* A. *Soit x un élément de* B *dont l'image* $\bar{x}$ *dans* $\mathbf{L}$ *engendre* $\mathbf{L}$ *sur k, et soit f le polynôme caractéristique de x sur* K. *Alors l'homomorphisme de* A[X] *dans* B *qui applique* X *sur x définit par passage au quotient un isomorphisme de* B_f *sur* B.

Les coefficients de f sont entiers sur A et appartiennent à K; comme A est intégralement clos, ils appartiennent à A. De plus, on a $f(x) =_{\mathfrak{p}} 0$, ce qui montre que l'application $A[X] \to B$ définie par x se factorise bien en $A[X] \to B_f \to B$. D'autre part, on a $\bar{f}(\bar{x}) = 0$; comme $\bar{x}$ est de degré n sur k, on en conclut que $\bar{f}$ est le polynôme minimal de $\bar{x}$ sur k, donc est irréductible. On est alors dans les conditions d'application du corollaire 1 ci-dessus, et la proposition en résulte aussitôt.

(ii) *Cas totalement ramifié.*

PROPOSITION 17. *Supposons que* A *soit un anneau de valuation discrète, et que f soit de la forme suivante*:

$$f = X^n + a_1X^{n-1} + \cdots + a_n, \quad a_i \in \mathfrak{m}, \quad a_n \notin \mathfrak{m}^2.$$

Alors B_f *est un anneau de valuation discrète, d'idéal maximal engendré par l'image x de* X, *et de corps résiduel k.*

[Un polynôme de la forme ci-dessus est appelé un « polynôme d'Eisenstein ».]

On a $\bar{f} = X^n$. Le lemme 4 montre donc que B_f est un anneau local d'idéal maximal engendré par $(\mathfrak{m}, x)$. De plus, l'élément $\pi = a_n$ est une uniformisante de A. Comme :

$$-\pi = x^n + a_1x^{n-1} + \cdots + a_{n-1}x,$$

on voit que π appartient à l'idéal (x), et on en conclut que $(\mathfrak{m}, x) = (x)$. Comme π n'est pas nilpotent, il en est de même de x, et la proposition 2 montre bien que B_f est un anneau de valuation discrète, c.q.f.d.

On en déduit comme précédemment :

COROLLAIRE. *Le polynôme f est irréductible dans* K[X], *et si* $L = K[X]/(f)$, *l'anneau* B_f *est la fermeture intégrale de* A *dans* L.

Ici encore, on a une réciproque :

PROPOSITION 18. *Soit* A *un anneau de valuation discrète, de corps des fractions* K, *et soit* L *une extension finie de degré n de* K. *Soit* B *la fermeture intégrale de* A *dans* L. *Supposons que* B *soit un anneau de valuation discrète, et que la valuation associée prolonge celle de* A *avec l'indice de ramification n. Soit x une uniformisante de* B, *et soit f le polynôme caractéristique de x sur* K. *Alors f est un polynôme d'Eisenstein, et l'homomorphisme de* A[X] *dans* B *qui applique* X *sur x définit par passage au quotient un isomorphisme de* B_f *sur* B.

On voit comme dans le cas (i) que les coefficients de f appartiennent à A. Écrivons alors f sous la forme :

$$f = a_0X^n + \cdots + a_n, \qquad a_i \in A, \quad a_0 = 1.$$

Puisque $f(x) = 0$, on a :

$$a_0 x^n + \cdots + a_n = 0.$$

Soit w la valuation discrète associée à B. On a $w(x) = 1$, et $w(a) \equiv 0 \bmod. n$ si $a \in A$. Soit $r = \mathrm{Inf}\,(w(a_i x^{n-i}))$, $0 \leqslant i \leqslant n$. D'après le lemme 1 du § 1, il existe deux entiers i et j, avec $0 \leqslant i < j \leqslant n$, tels que

$$r = w(a_i x^{n-i}) = w(a_j x^{n-j}).$$

On en tire $j - i = w(a_j/a_i) \equiv 0 \bmod. n$, ce qui n'est possible que si $i = 0$, $j = n$, d'où $r = n$, $w(a_n) = n$, $w(a_i) \geqslant n - i$ pour tout $i \geqslant 1$; le polynôme f est donc un polynôme d'Eisenstein, et la proposition résulte alors du corollaire à la proposition 17.

Exercice. Les notations étant celles du lemme 4, montrer que, si $e_i = 1$, l'anneau local $(B_f)_{m_i}$ correspondant est un anneau de valuation discrète.

§ 7. *Extensions galoisiennes*

Nous revenons maintenant aux hypothèses et notations des paragraphes 4 et 5, et nous supposons en outre que L/K est une extension *galoisienne*. Son groupe de Galois sera noté G(L/K).

PROPOSITION 19. *Le groupe* G(L/K) *opère transitivement sur l'ensemble des idéaux premiers* $\mathfrak{P}$ *de* B *divisant un idéal premier donné* $\mathfrak{p}$ *de* A.

Soit $\mathfrak{P}|\mathfrak{p}$, et supposons qu'il existe un idéal premier $\mathfrak{P}'$ de B au-dessus de $\mathfrak{p}$ distinct des $s(\mathfrak{P})$, $s \in G(L/K)$. D'après le lemme d'approximation, il existe $a \in \mathfrak{P}'$, $a \notin s(\mathfrak{P})$ pour tout s. Si $x = N_{L/K}(a)$, on a $x \in A$, et $x = \prod s(a)$, d'où $x \notin \mathfrak{P}$, $x \in \mathfrak{P}'$, ce qui est absurde puisque $\mathfrak{P} \cap A = \mathfrak{P}' \cap A$.

COROLLAIRE. *Soit* $\mathfrak{p}$ *un idéal premier non nul de* A. *Les entiers* $e_{\mathfrak{P}}$ *et* $f_{\mathfrak{P}}$ (*pour* $\mathfrak{P}$ *divisant* $\mathfrak{p}$) *ne dépendent que de* $\mathfrak{p}$. *Si on les note* $e_{\mathfrak{p}}$, $f_{\mathfrak{p}}$, *et si* $g_{\mathfrak{p}}$ *est le nombre des idéaux premiers* $\mathfrak{P}|\mathfrak{p}$, *on a*

$$n = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}.$$

C'est évident.

Le sous-groupe de G(L/K) formé des s tels que $s(\mathfrak{P}) = \mathfrak{P}$ s'appelle le *groupe de décomposition* de $\mathfrak{P}$ dans L/K; nous le noterons $D_{\mathfrak{P}}(L/K)$, ou parfois simplement D. Si $\mathfrak{P}'$ est un autre idéal premier de B au-dessus du même idéal $\mathfrak{p}$ de A, la proposition 19 montre que $D_{\mathfrak{P}'}(L/K)$ est conjugué de $D_{\mathfrak{P}}(L/K)$. L'indice de D dans G(L/K) est égal au nombre $g_{\mathfrak{p}}$ des idéaux premiers de B divisant $\mathfrak{p}$.

Fixons maintenant l'idéal $\mathfrak{P}$, et écrivons G, D, e, f, g au lieu de G(L/K), $D_{\mathfrak{P}}(L/K)$, $e_{\mathfrak{p}}$, $f_{\mathfrak{p}}$, $g_{\mathfrak{p}}$. Le groupe D correspond par la théorie de Galois à une extension K_D de K contenue dans L; cette extension n'est galoisienne que si D est invariant dans G. On a :

$$[K_D : K] = g, \qquad [L : K_D] = ef, \qquad G(L/K_D) = D.$$

Si E est un corps intermédiaire entre K et L, soit $B_E = E \cap B$ la fermeture intégrale de A dans E, soit $\mathfrak{P}_E = \mathfrak{P} \cap B_E$, et soit $\bar{E}$ le corps résiduel $B_E/\mathfrak{P}_E$. Ceci s'applique notamment à K et L, et définit les corps $\bar{K}$ et $\bar{L}$. Si $s \in D$, s définit par passage au quotient un $\bar{K}$-automorphisme $\bar{s}$ de $\bar{L}$. Nous obtenons ainsi un homomorphisme

$$\varepsilon : D \to G(\bar{L}/\bar{K})$$

dont le noyau est appelé le *groupe d'inertie* de $\mathfrak{P}$, et noté $T_{\mathfrak{P}}(L/K)$, ou simplement T. Il lui correspond une extension galoisienne K_T/K_D, du groupe de Galois D/T; on a $G(L/K_T) = T$.

PROPOSITION 20. *L'extension résiduelle* $\bar{L}/\bar{K}$ *est quasi-galoisienne* (« normale » au sens de Bourbaki, *Alg.*, Chap. V, § 6), *et l'homomorphisme*

$$\varepsilon : D \to G(\bar{L}/\bar{K})$$

définit un isomorphisme de D/T *sur* $G(\bar{L}/\bar{K})$.

Montrons d'abord que $\bar{L}/\bar{K}$ est quasi-galoisienne. Soit $\bar{a} \in \bar{L}$, et soit $a \in B$ un représentant de $\bar{a}$. Soit $P(X) = \prod(X - s(a))$, où s parcourt G; c'est un polynôme unitaire à coefficients dans A, qui admet a pour racine. Le polynôme réduit $\bar{P}(X)$ a pour racines les $\overline{s(a)}$; ceci suffit à prouver que $\bar{L}$ est quasi-galoisienne sur $\bar{K}$, cf. Bourbaki, *loc. cit.*, cor. 3 à la prop. 9. Passons maintenant à ε. Choisissons pour $\bar{a}$ un élément primitif de la plus grande extension séparable $\bar{L}_s$ de $\bar{K}$ contenue dans $\bar{L}$; le « lemme d'approximation » du § 3 montre qu'il existe un représentant a de $\bar{a}$ qui appartient à tous les idéaux premiers $s(\mathfrak{P})$, $s \notin D$. Formons comme ci-dessus le polynôme $P = \prod(X - s(a))$. Les racines non nulles de $\bar{P}(X)$ sont de la forme $s(\bar{a})$, avec $s \in D$; on en conclut que tout conjugué de $\bar{a}$ est égal à l'un des $s(\bar{a})$, avec $s \in D$, ce qui démontre la surjectivité de ε, d'où la proposition.

Nous noterons $\bar{L}_s$ la plus grande extension séparable de $\bar{K}$ contenue dans $\bar{L}$. D'après ce qui précède, c'est une extension galoisienne de K, de groupe de Galois D/T. Nous poserons :

$$f_0 = [\bar{L}_s : \bar{K}] = [\bar{L} : \bar{K}]_s, \qquad p^t = [\bar{L} : \bar{L}_s] = [\bar{L} : \bar{K}]_i.$$

On a :

$$f = f_0 p^t.$$

PROPOSITION 21. *Les notations étant comme ci-dessus, soient* w, w_T, w_D, v *les valuations discrètes définies par les idéaux* $\mathfrak{P}$, $\mathfrak{P}_T$, $\mathfrak{P}_D$, $\mathfrak{p}$. *Alors*:

a) $[L : K_T] = ep^t$, $[K_T : K_D] = f_0$, $[K_D : K] = g$.

b) w *prolonge* w_T *avec l'indice* e, w_T *et* w_D *prolongent* v *avec l'indice* 1.

c) $\bar{K}_T = \bar{L}_s$, $\bar{K}_D = \bar{K}$. *En particulier* $[\bar{L} : \bar{K}_T] = p^t$, $[\bar{K}_T : \bar{K}_D] = f_0$, $[\bar{K}_D : \bar{K}] = 1$.

On sait que l'ordre de D est ef, et l'on vient de voir que celui de D/T est f_0; celui de T est donc ep^t, ce qui démontre *a*).

D'autre part, appliquons au groupe T la proposition 20. On en conclut que $\bar{L}$ est radiciel sur $\bar{K}_T$. En particulier, tout élément $x \in \bar{L}_s$ est radiciel sur $\bar{K}_T$; comme x est séparable sur $\bar{K}$ qui est contenu dans $\bar{K}_T$, cela montre que $x \in \bar{K}_T$. Donc $\bar{K}_T$

contient L_0, et l'on a $[L : K_T] \leqslant p^r$, i. e. $f(L/K_T) \leqslant p^r$; d'autre part, il est clair que $e(L/K_T) \leqslant e$. Comme $[L : K_T] = ep^r$, on a nécessairement $L = K_T$ et $e(L/K_T) = e$, ce qui démontre *b*), et la première formule de *c*). La seconde résulte de la prop. 20, appliquée au groupe D/T opérant sur B_T, c.q.f.d.

COROLLAIRE. *Si L/K est séparable, c'est une extension galoisienne de groupe de Galois* D/T, *et l'on a* $K_T = L$, $[L : K_T] = e$, $[K_T : K_D] = f$, $[K_D : K] = g$.

En effet, on a alors $p^r = 1$.

Remarque. L'extension résiduelle L/K est séparable dans chacun des cas suivants (qui couvrent la plupart des applications) :

1) K est parfait.

2) L'ordre du groupe d'inertie T est premier à la caractéristique p du corps résiduel K (on a vu en effet que l'ordre de ce groupe est divisible par p^r).

Les hypothèses étant celles de la proposition 21, soit E un sous-corps de L contenant K; les groupes D(L/E) et T(L/E) sont bien définis; de même, lorsque E/K est galoisienne, les groupes D(E/K) et T(E/K) sont bien définis.

PROPOSITION 22. *a*) *On a* $D(L/E) = D(L/K) \cap G(L/E)$ *et*

$$T(L/E) = T(L/K) \cap G(L/E).$$

b) *Si* E/K *est galoisienne, le diagramme ci-dessous est commutatif, et ses lignes et ses colonnes sont exactes*:

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & T(L/E) & \to & T(L/K) & \to & T(E/K) & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & D(L/E) & \to & D(L/K) & \to & D(E/K) & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & G(L/E) & \to & G(L/K) & \to & G(E/K) & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

L'assertion *a*) est immédiate, ainsi que la commutativité du diagramme *b*). L'exactitude des colonnes résulte de la proposition 20, et celle de la troisième ligne de la théorie de Galois appliquée aux corps résiduels L, E, K. Si $s \in D(E/K)$, il existe $t \in G(L/K)$ qui induit s sur E; les idéaux $\mathfrak{P}$ et $t(\mathfrak{P})$ ont même restriction à E; d'après la proposition 19, il existe donc $t' \in G(L/E)$ tel que $t't(\mathfrak{P}) = \mathfrak{P}$; l'élément $t't$ appartient à D(L/K) et induit s sur L, ce qui montre que $D(L/K) \to D(E/K)$ est surjective. La deuxième ligne du diagramme est donc exacte, et un petit raisonnement formel montre que cela entraîne l'exactitude de la première ligne, c.q.f.d.

Remarque. Lorsque l'on veut étudier les groupes de décomposition, ou d'inertie, au-dessus d'un idéal premier $\mathfrak{p}$ donné de A, on peut si l'on veut remplacer A par

l'anneau de valuation discrète $A_\mathfrak{p}$; cette réduction au cas local peut être poussée plus loin : on peut même remplacer $A_\mathfrak{p}$ par son *complété* (cf. Chap. II).

§ 8. *Substitution de Frobenius*

Soit L/K une extension galoisienne, soit A un anneau de Dedekind de corps des fractions K, et soit B sa fermeture intégrale dans L. Soit $\mathfrak{P}$ un idéal premier de B, non nul, et soit $\mathfrak{p} = \mathfrak{P} \cap A$. Supposons que L/K soit *non ramifié* en $\mathfrak{P}$, et que $A/\mathfrak{p}$ soit un *corps fini* à q éléments. Le groupe d'inertie $T_\mathfrak{P}(L/K)$ est alors réduit à $\{1\}$, et le groupe de décomposition $D_\mathfrak{P}(L/K)$ s'identifie au groupe de Galois de l'extension résiduelle $\mathbf{L}/\mathbf{K}$. Puisque $\mathbf{K} = \mathbf{F}_q$, ce dernier groupe est un groupe cyclique, engendré par l'application $x \to x^q$ (cf. Bourbaki, *Alg.*, Chap. V, § 11). Soit $s_\mathfrak{P}$ l'élément de $D_\mathfrak{P}(L/K)$ correspondant à ce générateur; il est caractérisé par la propriété suivante :

$$s_\mathfrak{P}(b) \equiv b^q \bmod. \mathfrak{P} \qquad \textit{pour tout} \quad b \in B.$$

L'élément $s_\mathfrak{P}$ est appelé la *substitution de Frobenius* de $\mathfrak{P}$ (ou attachée à $\mathfrak{P}$). Sa définition montre que c'est un générateur du groupe de décomposition de $\mathfrak{P}$; son ordre est égal à $f_\mathfrak{P}$. On la note souvent $(\mathfrak{P}, L/K)$. Elle jouit de propriétés fonctorielles dont voici deux échantillons (on en verra un troisième au Chap. VII, § 8) :

Proposition 23. *Soit* E *un sous-corps de* L *contenant* K, *et soit* $\mathfrak{P}_E = \mathfrak{P} \cap E$. *Alors:*

a) *On a* $(\mathfrak{P}, L/E) = (\mathfrak{P}, L/K)^f$, *avec* $f = [E : K]$.

b) *Si* E *est galoisienne sur* K, *l'image de* $(\mathfrak{P}, L/K)$ *dans* $G(E/K)$ *est égale à* $(\mathfrak{P}_E, E/K)$.

La démonstration est immédiate.

Revenons à une extension L/K; si $t \in G(L/K)$, on a (par transport de structure) la formule :

$$(t(\mathfrak{P}),\ L/K) = t(\mathfrak{P},\ L/K)t^{-1}.$$

En particulier, *si* $G(L/K)$ *est abélien*, $(\mathfrak{P}, L/K)$ ne dépend que de $\mathfrak{p} = \mathfrak{P} \cap A$, c'est le *symbole d'Artin* de $\mathfrak{p}$, noté $(\mathfrak{p}, L/K)$. On définit par linéarité le symbole d'Artin de tout idéal $\mathfrak{a}$ de A ne contenant aucun $\mathfrak{p}$ ramifié, et on le note encore $(\mathfrak{a}, L/K)$ [on trouve également dans la littérature la notation $\left(\frac{L/K}{\mathfrak{a}}\right)$, ou simplement $\left(\frac{L}{\mathfrak{a}}\right)$].

Citons sans démonstration la célèbre :

Loi de réciprocité d'Artin (cf. [3]). *Soit* L *une extension abélienne finie d'un corps de nombres* K, *soit* A *l'anneau des entiers de* K, *et soient* $\mathfrak{p}_i$ *les idéaux premiers de* A *ramifiés dans* L/K. *Il existe alors des nombres entiers* $n_i \geqslant 1$ *tels que les conditions*:

(i) $v_{\mathfrak{p}_i}(x - 1) \geqslant n_i$ *pour tout* i,

(ii) x *est* > 0 *dans tout plongement réel de* K *qui n'est pas induit par un plongement réel de* L, *entraînent* $(x\mathrm{A}, L/K) = 1$.

De plus, tout élément s *de* $G(L/K)$ *est de la forme* $(\mathfrak{a}, L/K)$ *pour un idéal* $\mathfrak{a}$ *convenable* (en fait, on a même $s = (\mathfrak{p}, L/K)$ pour une infinité d'idéaux premiers $\mathfrak{p}$ de A).

Exemple. Soit n un entier $\geqslant 1$, soit $K = \mathbf{Q}$, et soit $L = \mathbf{Q}(\zeta_n)$ le corps des racines n-ièmes de l'unité. Le groupe de Galois $G(L/K)$ est un sous-groupe $G'(n)$ du groupe $G(n)$ des éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$ (cf. Bourbaki, *Alg.*, Chap. V, § 11); si $x \in G'(n)$, l'automorphisme σ_x associé à x transforme une racine ζ_n de l'unité en sa puissance x-ième. Si $(p, n) = 1$, on voit facilement (par exemple en utilisant les résultats du Chap. IV, § 4) que p est non ramifié, et que le symbole d'Artin $(p, L/K)$ est égal à σ_p. On en conclut par linéarité que *le symbole d'Artin d'un entier positif m premier à n est égal à* σ_m. Il en résulte tout d'abord que $G'(n) = G(n)$, c'est-à-dire que

$$[L : K] = \varphi(n)$$

(irréductibilité du polynôme cyclotomique). De plus, si $m > 0$, et si $m \equiv 1 \bmod n$, on a $(m, L/K) = 1$, ce qui vérifie la loi de réciprocité d'Artin dans ce cas. [Le fait que $s = (p, L/K)$ pour une infinité de nombres premiers p équivaut au théorème de Dirichlet sur les nombres premiers appartenant à une progression arithmétique.]

Une fois le symbole d'Artin déterminé dans $\mathbf{Q}(\zeta_n)/\mathbf{Q}$, la proposition 23 le fournit pour tout sous-corps E de $\mathbf{Q}(\zeta_n)$. Un tel corps est abélien sur $\mathbf{Q}$. Inversement, tout corps abélien sur $\mathbf{Q}$ peut être obtenu de cette manière (théorème de Kronecker-Weber). En particulier, tout corps quadratique $\mathbf{Q}(\sqrt{d})$ peut se plonger dans un corps $\mathbf{Q}(\zeta_n)$ convenable; ce résultat peut d'ailleurs se vérifier élémentairement par diverses méthodes (sommes de Gauss, par exemple). On a donc un procédé pour déterminer le symbole d'Artin $(p, \mathbf{Q}(\sqrt{d})/\mathbf{Q})$; en comparant le résultat avec celui que donne un calcul direct, on obtient la *loi de réciprocité quadratique*. Pour plus de détails, voir Hasse [34], § 27, ou H. Weyl [68], Chap. III, § 11.

CHAPITRE II

COMPLÉTION

§ 1. *Valeurs absolues et topologie définies par une valuation discrète*

Soit K un corps muni d'une valuation discrète v d'anneau A. Si a est un nombre réel, avec $0 < a < 1$, posons

$$\|x\| = a^{v(x)} \quad \text{pour} \quad x \neq 0 \quad \text{et} \quad \|0\| = 0.$$

On a alors les formules :

$$\begin{aligned} &\|x.y\| = \|x\| \cdot \|y\| \\ &\|x + y\| \leqslant \sup\,(\|x\|, \|y\|) \\ &\|x\| = 0 \quad \text{si et seulement si} \quad x = 0. \end{aligned}$$

On voit donc que $\|x\|$ est une *valeur absolue* sur K, au sens de Bourbaki, *Top. gén.*, Chap. IX, § 3; c'est même une valeur absolue *ultramétrique*. Inversement, on montre facilement que toute valeur absolue ultramétrique d'un corps K est de la forme $a^{v(x)}$, où v est une valuation *réelle* de K, c'est-à-dire une valuation dont le groupe des ordres est un sous-groupe additif de $\mathbf{R}$. Quant aux valeurs absolues non ultramétriques, on démontre (Ostrowski) qu'elles sont de la forme :

$$\|x\| = |f(x)|^c, \qquad \text{avec} \qquad 0 < c \leqslant 1,$$

où f ; $K \to \mathbf{C}$ est un isomorphisme de K sur un sous-corps du corps des nombres complexes.

Revenons maintenant au cas où v est discrète, et soit $\hat{K}$ le *complété* de K pour la topologie définie par sa valeur absolue (topologie qui ne dépend pas du nombre a choisi). On sait (Bourbaki, *loc. cit.*) que $\hat{K}$ est un corps valué, dont la valeur absolue prolonge celle de K. Si l'on l'écrit sous la forme

$$\|x\| = a^{\hat{v}(x)}, \qquad x \in \hat{K},$$

la fonction $\hat{v}(x)$ est à valeurs entières, et l'on vérifie tout de suite que c'est une valuation discrète sur $\hat{K}$, dont l'anneau de valuation est l'adhérence $\hat{A}$ de A dans $\hat{K}$. Si π est une uniformisante locale de A, les idéaux $\pi^n A$ forment une base de voisinages de zéro dans K, donc aussi dans A, ce qui montre que la topologie de A coïncide avec sa topologie naturelle d'*anneau local*; on a donc :

$$\hat{A} = \varprojlim A/\pi^n A \quad \text{(limite projective)}.$$

L'élément π est uniformisante locale de $\hat{A}$, et l'on a $\hat{A}/\pi^n\hat{A} = A/\pi^n A$. En particulier les corps résiduels de A et de $\hat{A}$ coïncident.

PROPOSITION 1. *Pour que* K *soit localement compact, il faut et il suffit qu'il soit complet et que son corps résiduel* $K = A/\pi A$ *soit un corps fini.*

Si K est localement compact, il est complet. De plus, comme les $\pi^n A$ forment un système fondamental de voisinages fermés de 0, l'un d'eux est compact, et par homothétie on voit que A est compact. Le quotient $K = A/\pi A$, étant à la fois compact et discret, est nécessairement fini.

Réciproquement, si K est fini, les $A/\pi^n A$ sont finis, donc $\hat{A}$, étant limite projective de groupes finis, est compact; si en outre K est complet, on a $A = \hat{A}$, et K est bien localement compact.

Exemples. 1) Le corps $\mathbf{Q}_p$, complété de $\mathbf{Q}$ pour la topologie définie par la valuation p-adique, est un corps localement compact de corps résiduel $\mathbf{F}_p$.

2) Si F est un corps fini, le corps de séries formelles F((T)) est localement compact.

Lorsque K vérifie les conditions de la prop. 1, il y a une façon canonique de choisir le nombre a : on prend $a = q^{-1}$, où q est le nombre d'éléments du corps résiduel K. La valeur absolue correspondante est dite *normalisée*. La proposition suivante en donne une caractérisation « analytique » :

PROPOSITION 2. *Soit* K *un corps vérifiant les conditions de la prop.* 1, *et soit* μ *une mesure de Haar du groupe additif localement compact* K. *Pour toute partie mesurable* E *de* K, *et pour tout* $x \in K$, *on a alors*

$$\mu(xE) = \|x\|\mu(E),$$

où $\|x\|$ *désigne la valeur absolue normalisée de* x.

On peut supposer $x \neq 0$; l'homothétie $y \to xy$ est alors un automorphisme du groupe additif de K, donc transforme la mesure de Haar μ en un de ses multiples $\chi(x).\mu$, et il s'agit de voir que le multiplicateur $\chi(x)$ est égal à $\|x\|$. Puisque $\chi(x)$ et $\|x\|$ sont multiplicatifs, on peut supposer $x \in A$. Si l'on prend alors $E = A$, on voit que E est réunion de $(A : xA)$ classes modulo xE, d'où $\mu(E) = (A : xA).\mu(xE)$, et $\chi(x) = 1/(A : xA)$. Comme $(A : xA)$ est égal à $q^{v(x)}$, on trouve bien

$$\chi(x) = q^{-v(x)} = \|x\|, \qquad \text{c.q.f.d.}$$

Remarque. On peut effectuer la même normalisation pour un corps valué localement compact K dont la valuation n'est pas ultramétrique; d'après le théorème d'Ostrowski cité plus haut, on a $K = \mathbf{R}$ ou $K = \mathbf{C}$; dans le premier cas on trouve la valeur absolue usuelle, et dans le second cas son carré (qui n'est d'ailleurs pas une valeur absolue au sens strict, car elle ne vérifie pas l'inégalité triangulaire). Ces normalisations sont indispensables pour la *formule du produit*: soit K un corps de nombres, et soit P l'ensemble des valeurs absolues normalisées de K (ultramétriques ou non ultramétriques); on a alors

$$\prod_{\mathfrak{p}\in P} \|x\|_{\mathfrak{p}} = 1 \quad \text{pour tout } x \in K^*$$

(le produit infini a un sens, car presque tout les termes qui y figurent sont égaux à 1). Pour démontrer cette formule, on la vérifie d'abord pour $K = \mathbf{Q}$, par un calcul direct; on se sert ensuite du résultat suivant (équivalent, dans le cas ultramétrique, à la formule $\sum e_i f_i = n$) :

$$\|N_{K/\mathbf{Q}}(x)\|_p = \prod_{\mathfrak{p}\mid p} \|x\|_{\mathfrak{p}}, \quad x \in K^*.$$

Une formule analogue est valable pour les corps de fonctions algébriques d'une variable.

§ 2. *Extensions d'un corps complet*

PROPOSITION 3. *Soit* K *un corps muni d'une valuation discrète* v *d'anneau* A, *et complet pour la topologie définie par* v. *Soit* L/K *une extension finie de* K, *et soit* B *la fermeture intégrale de* A *dans* L (*cf.* Chap. I, § 4). *Alors* B *est un anneau de valuation discrète; c'est un* A*-module libre de rang* $n = [L : K]$, *et* L *est complet pour la topologie définie par* B.

Commençons par le cas où L/K est *séparable*. La condition (F) du Chap. I, § 4 est alors automatiquement vérifiée; comme A est principal, il s'ensuit que B est un A-module libre de rang n. Soient $\mathfrak{P}_i$ les idéaux premiers de B, et soient w_i les valuations correspondantes. Chaque w_i définit, comme au § précédent, une *norme* sur L, qui en fait un *espace vectoriel topologique* séparé sur K; comme K est complet, il s'ensuit (cf. Bourbaki, *Esp. Vect. Top.*, Chap. I, § 2, th. 2) que la topologie $\mathfrak{T}_i$ définie par w_i est en fait la topologie produit de L (identifié à K^n), et ne dépend donc pas de i. Mais w_i est déterminée par $\mathfrak{T}_i$: l'anneau de w_i est l'ensemble des x tels que x^{-n} ne tende pas vers zéro pour $\mathfrak{T}_i$. Il s'ensuit que l'ensemble des w_i est réduit à un seul élément, ce qui montre que B est un anneau de valuation discrète. Comme K est complet, il en est de même de K^n, donc aussi de L. Une fois ce cas traité, un argument de « dévissage » évident permet de se ramener au cas où L/K est *radicielle*. Il existe alors une puissance q de l'exposant caractéristique telle que $x^q \in K$ pour tout $x \in L$. Posons $v'(x) = v(x^q)$; l'application $v' : L^* \to \mathbf{Z}$ est un homomorphisme. Si m désigne le générateur positif du sous-groupe $v'(L^*)$, la fonction $w = \frac{1}{m} v$ est une valuation discrète de L. Il est immédiat que son anneau de valuation est B; le même argument

que ci-dessus montre que la topologie définie par w coïncide avec celle de K^n, et fait en particulier de L un corps *complet*. Reste à prouver que B est un A-module de type fini. Soit π une uniformisante de A, et soit $\overline{B} = B/\pi B$. Soient b_i des éléments de B dont les images $\overline{b}_i$ dans $\overline{B}$ sont linéairement indépendantes sur $\overline{K} = A/\pi A$. Les b_i sont linéairement indépendants sur A; en effet, si l'on avait une relation $\sum a_i b_i = 0$ non triviale, on pourrait supposer que l'un au moins des a_i n'est pas divisible par π, et en réduisant mod. πB, on obtiendrait une relation entre les $\overline{b}_i$. En particulier, le nombre des b_i est $\leqslant n$. Supposons maintenant que les $\overline{b}_i$ forment une *base* de $\overline{B}$ et soit E le sous-A-module de B engendré par les b_i. Tout $b \in B$ s'écrit donc $b = b_0 + \pi b_1$, avec $b_0 \in E$ et $b_1 \in B$; en appliquant ceci à b_1, et en itérant, on en conclut que b s'écrit sous la forme :

$$b = b_0 + \pi b_1 + \pi^2 b_2 + \cdots, \qquad b_i \in E,$$

et comme A est complet, ceci montre que $b \in E$, c.q.f.d.

COROLLAIRE 1. *Si e* (resp. f) *désigne l'indice de ramification* (resp. *le degré résiduel*) *de* L *sur* K, *on a* $ef = n$.

Cela résulte de la proposition 10 du Chap. I, qui est applicable puisque l'on a démontré que B est un A-module de type fini.

COROLLAIRE 2. *Il existe une valuation w et une seule de* L *qui prolonge v.*

Cela ne fait que reformuler une partie de la proposition.

COROLLAIRE 3. *Deux éléments de* L *conjugués sur* K *ont même valuation.*

Quitte à augmenter L, on peut la supposer quasi-galoisienne. Si $s \in G(L/K)$, $w \circ s$ prolonge v, donc coïncide avec w (cor. 2); comme les conjugués de $x \in L$ ne sont autres que les $s(x)$, $s \in G(L/K)$, le corollaire en résulte.

COROLLAIRE 4. *On a* $w(x) = \frac{1}{f} v(N_{L/K}(x))$ *pour tout* $x \in L$.

Ici encore, on peut se ramener au cas où L/K est quasi-galoisien, auquel cas notre assertion résulte du corollaire 3. [On pourrait tout aussi bien appliquer directement la proposition 14 du Chap. I.]

En termes de *valeurs absolues*, le corollaire 4 signifie que la topologie de L peut être définie par la norme

$$\|x\|_L = \|N_{L/K}(x)\|_K.$$

On observera que, si K est localement compact, et si $\| \ \|_K$ est normalisée, il en est de même de $\| \ \|_L$.

Remarque. Il est possible de prendre la formule ci-dessus comme *définition* de $\| \ \|_L$; on doit alors prouver directement que c'est une valeur absolue ultramétrique, ce qui se fait au moyen du « lemme de Hensel » (cf. van der Waerden [65], § 77); on peut aussi se servir de l'existence d'au moins une valuation prolongeant v, ce

qui est un fait général (cf. Bourbaki, *Alg. comm.*, Chap. VI). Ces méthodes ont l'avantage de s'appliquer aux « valuations de rang 1 » non nécessairement discrètes.

Exercices.

1) Soit E/K une extension galoisienne finie d'un corps complet K. On prolonge à E la valuation de K. Soit $x \in E$, et soit $\{x_1, ..., x_n\}$ l'ensemble des conjugués de x sur K, avec $x = x_1$. Soit $y \in E$ tel que $\|y - x\| < \|y - x_i\|$ pour $i \geqslant 2$. Montrer que x appartient au corps $K(y)$.

(Remarquer que, si x_i est conjugué de x sur $K(y)$, on a $\|y - x\| = \|y - x_i\|$ d'après le corollaire 3.)

2) Soit K un corps complet, et soit $f(X) \in K[X]$ un polynôme irréductible et séparable de degré n. Soit L/K l'extension de degré n définie par f. Montrer que, pour tout polynôme $h(X)$ de degré n assez voisin de f, $h(X)$ est irréductible et l'extension L_h/K définie par h est isomorphe à L.

(Appliquer l'exercice 1 aux racines x_i de f et à une racine y de h.)

3) Les hypothèses étant celles de la prop. 3, montrer directement que B est un A-module de type fini en utilisant l'exer. 8 de Bourbaki, *Alg.*, Chap. VII, § 3.

4) Soit K un corps complet pour une valuation discrète v, et soit Ω une clôture algébrique de K.

(*a*) Soit S l'ensemble des sous-extensions E de Ω telles que, pour toute sous-extension finie E' de E, on ait $e(E'/K) = 1$. Montrer que S possède des éléments maximaux. Si K_0 est l'un d'eux, montrer que v se prolonge en une valuation discrète de K_0, et que le corps résiduel de K_0 est la clôture algébrique de celui de K (utiliser la prop. 15 du Chap. I).

(*b*) Soit L/K une extension totalement ramifiée contenue dans Ω, et soit K_0/K une extension de K vérifiant les propriétés de (*a*). Montrer que L et K_0 sont linéairement disjointes sur K. Si L/K est galoisienne de groupe de Galois G, en déduire que l'extension L_0/K_0, avec $L_0 = K_0L$, est galoisienne de groupe de Galois G.

§ 3. Extension et complétion

THÉORÈME 1. *Soit* L/K *une extension de degré fini* n, *soit* v *une valuation discrète de* K, *soit* A *l'anneau de* v, *et soit* B *la fermeture intégrale de* A *dans* L. *On suppose que* B *est un* A*-module de type fini. Soient* w_i *les différents prolongements de* v *à* L, *et soient* e_i, f_i *les nombres correspondants* (*cf.* Chap. I, § 4). *Soient* $\hat{K}$ *et* $\hat{L}_i$ *les complétés de* K *et* L *pour* v *et les* w_i.

(i) *Le corps* $\hat{L}_i$ *est une extension de* $\hat{K}$ *de degré* $n_i = e_i f_i$.

(ii) *La valuation* $\hat{w}_i$ *est l'unique valuation de* $\hat{L}_i$ *prolongeant la valuation* $\hat{v}$; *on a*

$$e_i = e(\hat{L}_i/\hat{K}) \qquad et \qquad f_i = f(\hat{L}_i/\hat{K}).$$

(iii) *L'homomorphisme canonique* $\varphi : L \otimes_K \hat{K} \to \prod_i \hat{L}_i$ *est un isomorphisme.*

L'assertion (ii) est évidente, compte tenu du § 2, et elle entraîne l'assertion (i). D'autre part, la topologie produit fait de $\prod \hat{L}_i$ un espace vectoriel topologique séparé de dimension n sur $\hat{K}$; d'après le lemme d'approximation (Chap. I, § 3) $\varphi(L)$ est dense dans $\prod \hat{L}_i$, donc aussi $\varphi(L \otimes_K \hat{K})$. Il s'ensuit (cf. Bourbaki, *Esp. Vect. Top.*, Chap. I, § 2, cor. 1 au th. 2) que φ est surjectif, donc bijectif, puisque $L \otimes_K \hat{K}$ et $\prod \hat{L}_i$ sont tous deux des espaces vectoriels de dimension n sur $\hat{K}$.

COROLLAIRE 1. *Les corps* $\hat{L}_i$ *ne sont autres que les composés des extensions* $\hat{K}$ *et* L *de* K.

On sait en effet (cf. Bourbaki, *Alg.*, Chap. VIII, § 8) que ces composés sont les corps quotients du produit tensoriel $L_K \otimes \hat{K}$.

COROLLAIRE 2. *Si* $x \in L$, *le polynôme caractéristique* F *de* x *dans* L/K *est égal au produit des polynômes caractéristiques* F_i *de* x *dans les* $\hat{L}_i/\hat{K}$. *En particulier, si l'on note* Tr *et* N (*resp.* Tr_i *et* N_i) *la trace et la norme dans* L/K (*resp. dans* $\hat{L}_i/\hat{K}$), *on a*:

$$Tr(x) = \sum Tr_i(x), \qquad N(x) = \prod N_i(x).$$

Le polynôme F est aussi le polynôme caractéristique de x dans la $\hat{K}$-algèbre $L \otimes_K \hat{K}$. La formule $F = \prod F_i$ résulte donc de l'isomorphisme (iii) et les formules sur $Tr(x)$ et $N(x)$ s'en déduisent immédiatement (cf. Bourbaki, *Alg.*, Chap. VIII, § 12, n° 2).

COROLLAIRE 3. *Si* L/K *est séparable* (*auquel cas l'hypothèse de finitude faite sur* B *est automatiquement vérifiée*), *les* $\hat{L}_i/\hat{K}$ *le sont aussi.*

En effet, on a $\hat{L}_i = L\hat{K}$.

COROLLAIRE 4. *Si* L/K *est galoisienne de groupe de Galois* G, *et si* D_i *désigne le groupe de décomposition de* w_i *dans* G (*cf.* Chap. I, § 7), *l'extension* $\hat{L}_i/\hat{K}$ *est galoisienne de groupe de Galois* D_i.

Tout élément de D_i se prolonge par continuité en un $\hat{K}$-automorphisme de $\hat{L}_i$, et comme l'ordre de D_i est égal à $[\hat{L}_i : \hat{K}]$, la proposition en résulte.

(L'isomorphisme $\varphi : L \otimes_K \hat{K} \to \prod \hat{L}_i$ ne fait alors qu'exprimer la décomposition de $L \otimes_K \hat{K}$, considérée comme « algèbre galoisienne » au sens de Hasse.)

Passons maintenant aux anneaux de valuation eux-mêmes :

PROPOSITION 4. *Les hypothèses et notations étant celles du théorème* 1, *soit* B_i *l'anneau de la valuation* w_i. *L'homomorphisme canonique*

$$\varphi : B \otimes_A \hat{A} \to \prod_i \hat{B}_i$$

est alors un isomorphisme.

Les deux membres sont des $\hat{A}$-modules libres de rang n. Pour montrer que φ est bijectif, il suffit donc de voir qu'il en est ainsi lorsqu'on réduit modulo l'idéal maximal $\hat{m}$ de $\hat{A}$. Pour le premier membre, on trouve B/mB, et pour le second $\prod B/\mathfrak{m}_i^{e_i}B$ ($\mathfrak{m}$ et $\mathfrak{m}_i$ désignant les idéaux de v et des w_i), d'où aussitôt le résultat.

Remarque. L'anneau $B \otimes_A \hat{A}$ n'est autre que le *complété* $\hat{B}$ de B pour la topologie naturelle de l'anneau semi-local B. Sa décomposition en facteurs directs $\hat{B}_i$ est un cas particulier d'une propriété générale des anneaux semi-locaux (cf. Bourbaki, *Alg. comm.*, Chap. III, § 2, n° 12).

Exercices.

1) Soit K un corps muni d'une valuation discrète v d'anneau A. On suppose que toute extension radicielle finie L/K vérifie la condition (F) du Chap. I, § 4, vis-à-vis de A. Montrer que $\hat{K}$ est alors une extension séparable de K. (Utiliser le th. 1 de Bourbaki, *Alg.*, Chap. VIII, § 7.)

2) On garde les hypothèses et notations du th. 1, à cela près que l'on remplace l'hypothèse « B est de type fini sur A » par « B n'est pas de type fini sur A ». Montrer que (i) et (ii) restent valables, que φ est surjectif, et que son noyau est un idéal nilpotent non nul de $L \otimes_K \hat{K}$.

§ 4. *Structure des anneaux de valuation discrète complets. Cas d'égale caractéristique*

Soit A un anneau de valuation discrète complet, de corps des fractions K, de corps résiduel $\mathbf{K}$. Soit un S système de représentants de $\mathbf{K}$ dans A, et soit π une uniformisante de A.

PROPOSITION 5. *Tout élément $a \in A$ s'écrit de façon unique comme série convergente :*

$$(*) \qquad a = \sum_{n=0}^{\infty} s_n \pi^n, \qquad \text{avec} \quad s_n \in S.$$

Tout élément $x \in K$ s'écrit de même :

$$x = \sum_{n \gg -\infty} s_n \pi^n, \qquad \text{avec} \quad s_n \in S,$$

la série ne comportant qu'un nombre fini de termes à exposants négatifs.

La seconde partie résulte de la première par homothétie. Soit donc $a \in A$; par hypothèse, il existe $s_0 \in S$ tel que $a - s_0 \equiv 0 \bmod \pi$; si l'on écrit $a = s_0 + \pi a_1$, en appliquant ce qui précède à a_1, on trouve $s_1 \in S$ tel que

$$a = s_0 + s_1\pi + a_2\pi^2,$$

et ainsi de suite. La série $\sum s_n \pi^n$ converge vers a et l'on voit facilement que c'est la seule. Inversement, toute série de la forme $\sum s_n \pi^n$ est convergente, puisque son terme général tend vers zéro et que A est complet.

Exemple. Si $A = \mathbf{Z}_p$, on peut prendre pour S l'ensemble des entiers i tels que $0 \leqslant i < p$; on peut aussi, et c'est préférable, prendre pour S la réunion de $\{0\}$ et de l'ensemble des racines $(p-1)$-ièmes de l'unité, cf. prop. 8.

La proposition 5 montre que l'addition et la multiplication dans A sont déterminées par les décompositions de $s + s'$ et ss' sous la forme $(*)$. En particulier, *si* S *est un sous-corps de* K (nécessairement isomorphe à $\mathbf{K}$), l'anneau A s'identifie à l'anneau $\mathbf{K}[[T]]$ des séries formelles à coefficients dans $\mathbf{K}$. Ceci n'est évidemment possible que si K et $\mathbf{K}$ ont même caractéristique. Inversement :

THÉORÈME 2. *Soit* A *un anneau de valuation discrète complet, de corps résiduel* K. *Supposons que* A *et* K *aient même caractéristique, et que* K *soit parfait. Alors* A *est isomorphe à* K[[T]].

[En fait, ce résultat vaut même si K n'est pas parfait, voir plus loin.]

Tout revient à montrer que A contient un système de représentants qui est un corps. Nous distinguerons deux cas, suivant la caractéristique de K :

(i) *La caractéristique de* K *est* 0.

L'existence d'un corps de représentants est alors vraie pour des anneaux locaux nettement plus généraux que les anneaux de valuation discrète. De façon précise :

PROPOSITION 6. *Soit* A *un anneau local séparé et complet pour la topologie définie par une suite décroissante d'idéaux* $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots$ *telle que* $\mathfrak{a}_n . \mathfrak{a}_m \subset \mathfrak{a}_{n+m}$. *Supposons que* $K = A/\mathfrak{a}_1$ *soit un corps de caractéristique zéro. Il existe alors dans* A *un système de représentants de* K *qui est un corps.*

[Noter que la première hypothèse sur A est vérifiée si A est un anneau local noethérien, complet pour sa topologie naturelle d'anneau local.]

Comme $\mathbf{Z} \to A \to K$ est injective, l'homomorphisme $\mathbf{Z} \to A$ se prolonge à $\mathbf{Q}$, et l'on voit que A contient $\mathbf{Q}$. D'après le théorème de Zorn il existe un sous-corps maximal S de A; si $\bar{S}$ désigne son image dans K, nous allons montrer que $\bar{S} = K$.

Tout d'abord, montrons que K est *algébrique* sur $\bar{S}$; sinon, en effet, il existerait $a \in A$ dont l'image $\bar{a}$ dans K est transcendante sur $\bar{S}$; le sous-anneau S[a] de A s'applique sur $\bar{S}[\bar{a}]$, donc est isomorphe à S[X], et $S[a] \cap \mathfrak{a}_1 = 0$; on en conclut que A contient le corps S(a) des fonctions rationnelles en a, ce qui est contraire au caractère maximal de S.

Montrons maintenant que $K = \bar{S}$. Soit $\lambda \in K$, et soit $\bar{f}(X)$ son polynôme minimal sur $\bar{S}$; puisque la caractéristique est 0, λ est racine simple de $\bar{f}$. Soit $f \in S[X]$ le polynôme correspondant par l'isomorphisme $\bar{S} \to S$. D'après la proposition 7 ci-après, il existe $x \in A$ tel que $\bar{x} = \lambda$ et $f(x) = 0$, et l'on peut relever $\bar{S}[\lambda]$ dans A en envoyant λ sur x; vu le caractère maximal de S, on a donc $\lambda \in \bar{S}$, ce qui montre bien que $K = \bar{S}$.

Il nous reste à démontrer la proposition suivante, qui est un cas particulier du « lemme de Hensel » (Bourbaki, *Alg. comm.*, Chap. III) :

PROPOSITION 7. *Soit* A *un anneau local séparé et complet pour la topologie définie par une suite décroissante d'idéaux* $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots$ *telle que* $\mathfrak{a}_n . \mathfrak{a}_m \subset \mathfrak{a}_{n+m}$. *Supposons que* $\mathfrak{a}_1$ *soit l'idéal maximal de* A, *et soit* $K = A/\mathfrak{a}_1$. *Soit* $f(X)$ *un polynôme à coefficients dans* A *tel que le polynôme réduit* $\bar{f} \in K[X]$ *ait une racine simple* λ *dans* K. *Il existe alors une racine* x *de* f *dans* A, *et une seule, telle que* $\bar{x} = \lambda$.

Si x répond à la question, on a $f(X) = (X - x)g(X)$, avec $\bar{g}(\lambda) \neq 0$; si x' est une autre solution du problème, en faisant $X = x'$, on obtient $0 = (x' - x)g(x')$. Comme $g(x')$ admet $\bar{g}(\lambda)$ pour réduction mod. $\mathfrak{a}_1$, $g(x')$ est inversible, et l'on a $x = x'$, ce qui démontre l'unicité de la solution.

Pour prouver son existence, on emploie la méthode d'approximation de Newton. Soit $x_1 \in A$ tel que $\bar{x}_1 = \lambda$; on a $f(x_1) \equiv 0$ mod. $\mathfrak{a}_1$.

Supposons avoir trouvé $x_n \in A$ tel que $\bar{x}_n = \lambda$, $f(x_n) \equiv 0 \bmod \mathfrak{a}_n$, et montrons que l'on peut trouver $x_{n+1} \in A$, $x_{n+1} \equiv x_n \bmod \mathfrak{a}_n$ et $f(x_{n+1}) \equiv 0 \bmod \mathfrak{a}_{n+1}$. Cela démontrera le lemme en posant $x = \lim x_n$. Pour trouver x_{n+1}, on écrit $x_{n+1} = x_n + h$, avec $h \in \mathfrak{a}_n$, et on applique la formule de Taylor :

$$f(x_{n+1}) = f(x_n) + h.f'(x_n) + h^2.y, \qquad \text{avec} \quad y \in A.$$

On a $h^2.y \in \mathfrak{a}_n.\mathfrak{a}_n \subset \mathfrak{a}_{n+1}$, et l'on voit que tout revient à trouver $h \in \mathfrak{a}_n$ tel que

$$f(x_n) + h.f'(x_n) \equiv 0 \bmod \mathfrak{a}_{n+1}.$$

Mais puisque λ est racine simple de $\bar{f}$, on a $\bar{f}'(\lambda) \neq 0$, et $f'(x_n)$ est *inversible* dans A; comme $f(x_n) \in \mathfrak{a}_n$, l'équation ci-dessus se résout, c.q.f.d.

Le théorème 2 est donc établi en caractéristique zéro.

(ii) *Les corps* K *et* $\mathbf{K}$ *sont de caractéristique* $p \neq 0$.

Ici encore, on va obtenir un résultat pour des anneaux nettement plus généraux.

Nous dirons qu'un anneau A de caractéristique p est *parfait* si l'endomorphisme $x \to x^p$ de A est un *automorphisme*. Tout élément $x \in A$ a donc une racine p-ième unique, notée $x^{p^{-1}}$. Lorsque A est un corps, on retrouve la définition habituelle d'un corps parfait.

PROPOSITION 8. *Soit* A *un anneau séparé et complet pour la topologie définie par une suite décroissante d'idéaux* $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots$ *telle que* $\mathfrak{a}_n.\mathfrak{a}_m \subset \mathfrak{a}_{n+m}$. *On suppose que l'anneau* $\mathbf{K} = A/\mathfrak{a}_1$ *est un anneau parfait de caractéristique* p. *Alors*:

(i) *Il existe un système de représentants* $f : \mathbf{K} \to A$ *et un seul qui commute à la puissance* p*-ième*: $f(\lambda^p) = f(\lambda)^p$.

(ii) *Pour que* $a \in A$ *appartienne à* $S = f(\mathbf{K})$, *il faut et il suffit que* a *soit une puissance* p^n*-ième pour tout* $n \geqslant 0$.

(iii) *Ce système de représentants est multiplicatif, i.e. on a* $f(\lambda\mu) = f(\lambda).f(\mu)$ *pour* $\lambda, \mu \in \mathbf{K}$.

(iv) *Si* A *est de caractéristique* p, *ce système de représentants est additif, i.e.* $f(\lambda + \mu) = f(\lambda) + f(\mu)$.

Soit $\lambda \in \mathbf{K}$; pour tout $n \geqslant 0$, désignons par L_n l'image réciproque de $\lambda^{p^{-n}}$ dans A, et par U_n l'ensemble des x^{p^n}, $x \in L_n$; les U_n sont contenus dans la classe L_0 de λ, et forment une famille décroissante. Nous allons voir qu'ils forment une *base de filtre de Cauchy* dans A. En effet, si $a = x^{p^n}$ et $b = y^{p^n}$ on démontre par récurrence sur n que $a \equiv b \bmod \mathfrak{a}_{n+1}$, en utilisant le lemme suivant :

LEMME 1. *Si* $a \equiv b \bmod \mathfrak{a}_n$ *on a* $a^p \equiv b^p \bmod \mathfrak{a}_{n+1}$.

Ce lemme résulte de la formule du binôme, compte tenu de ce que $p \in \mathfrak{a}_1$, d'où $p\mathfrak{a}_n \subset \mathfrak{a}_{n+1}$.

Puisque les U_n forment une base de filtre de Cauchy et que A est complet, on peut poser $f(\lambda) = \lim U_n$. C'est un système de représentants. Si $\lambda = \mu^p$, l'opération de puissance p-ième dans A applique $U_n(\mu)$ dans $U_{n+1}(\lambda)$, et, en passant à

la limite, elle applique $f(\mu)$ sur $f(\lambda)$, ce qui montre bien que f commute à la puissance p-ième. Inversement, si f' est un système de représentants vérifiant cette propriété, $f'(\lambda)$ est une puissance p^n-ième pour tout n, donc $f'(\lambda) \in U_n(\lambda)$ pour tout n; comme les U_n forment une base de filtre de Cauchy, ceci entraîne l'unicité de f', et en même temps le fait que l'intersection des U_n est non vide, et égale à $f(\lambda)$, d'où (i) et (ii).

Pour (iii) on remarque que, si x et y sont des puissances p^n-ièmes pour tout n, il en est de même de xy; même raisonnement pour (iv), en tenant compte de ce que $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ si A est de caractéristique p.

Le système de représentants de la proposition 8 est appelé *système de représentants multiplicatifs*, en raison de la propriété (iii).

L'application de la proposition 8 au théorème 2 est immédiate : si K est un corps parfait, et si A est de caractéristique p, les propriétés (iii) et (iv) montrent que $S = f(K)$ est un corps. On voit en outre que c'est le *seul*. [Lorsque K n'est pas parfait, on peut montrer qu'il existe encore un corps de représentants S, mais ce corps n'est plus unique en général : on peut relever arbitrairement les éléments d'une « p-base » de K. Pour plus de détails sur ces questions et celles traitées au § suivant, voir Cohen [18] et Roquette [52].]

Exercice. Soit k un corps parfait de caractéristique p. Montrer que toute extension radicielle finie de $k((T))$ est isomorphe à une extension de la forme $k((T^{q^{-1}}))$, où q est une puissance de p.

§ 5. *Structure des anneaux de valuation discrète complets. Cas d'inégale caractéristique*

Soit A un anneau de valuation discrète complet, de corps des fractions K, de corps résiduel K. Supposons que les caractéristiques de A et de K soient différentes, c'est-à-dire que A soit de caractéristique zéro et K de caractéristique $p \neq 0$. On peut alors identifier $\mathbf{Z}$ à un sous-anneau de A, et $p \in \mathbf{Z}$ à un élément, noté encore p, de A. Puisque p donne zéro dans K, on a $v(p) \geqslant 1$, v désignant la valuation discrète attachée à A. L'entier $e = v(p)$ est appelé *l'indice de ramification absolu* de A. On observera que l'injection $\mathbf{Z} \to A$ se prolonge par continuité en une injection de l'anneau $\mathbf{Z}_p$ des entiers p-adiques dans A; lorsque le corps des restes K est un corps fini à $q = p^f$ éléments, la proposition 5 montre que A est un $\mathbf{Z}_p$-module libre de rang $n = ef$, et K est une extension de degré n du corps p-adique $\mathbf{Q}_p$; l'entier e s'interprète alors comme indice de ramification de l'extension $K/\mathbf{Q}_p$, ce qui justifie le terme d'« indice de ramification absolu ».

Revenant au cas général, nous dirons que A est *absolument non ramifié* si $e = 1$, c'est-à-dire si p est une uniformisante locale de A. C'est pour ces anneaux que l'on a un théorème de structure :

THÉORÈME 3. *Pour tout corps parfait k de caractéristique p, il existe un anneau de valuation discrète complet et un seul (à un isomorphisme unique près) qui est absolument non ramifié et admet k pour corps résiduel.*

Cet anneau sera désigné par $W(k)$ dans ce qui suit. Il est « unique » au sens suivant : si A_1 et A_2 vérifient tous deux les conditions du théorème, il existe un isomorphisme $g : A_1 \to A_2$ *et un seul* qui rend commutatif le diagramme :

$$\begin{array}{ccc} A_1 & \xrightarrow{g} & A_2 \\ & \searrow^{k} \swarrow & \end{array}$$

Dans le cas ramifié, on a :

THÉORÈME 4. *Soit* A *un anneau de valuation discrète complet, d'inégale caractéristique, et de corps résiduel parfait k. Soit e son indice de ramification absolu. Il existe alors un homomorphisme et un seul de* $W(k)$ *dans* A *qui rend commutatif le diagramme :*

$$\begin{array}{ccc} W(k) & \longrightarrow & A \\ & \searrow^{k} \swarrow & \end{array}$$

Cet homomorphisme est injectif, et A *est un* $W(k)$*-module libre de rang égal à e.*

[En appliquant la proposition 18 du Chap. I, on voit donc que A s'obtient en adjoignant à $W(k)$ un élément π vérifiant une « équation d'Eisenstein » :

$$\pi^e + a_1\pi^{e-1} + \cdots + a_e = 0, \qquad a_i \in W(k),$$

les a_i étant divisibles par p, et a_e n'étant pas divisible par p^2. Inversement, d'après la prop. 17 du Chap. I, une telle équation définit bien une extension totalement ramifiée de $W(k)$ de degré e.]

On va démontrer les théorèmes 3 et 4 par une méthode due à Lazard ([42], [43]). Ici, encore on obtiendra des résultats pour des anneaux plus généraux que les anneaux de valuation discrète : les anneaux munis d'une filtration $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots$ vérifiant les hypothèses de la prop. 8; un tel anneau sera appelé un p-anneau. On dira qu'un p-anneau A est *strict* (Lazard dit « p-adique », mais ce terme peut prêter à confusion) si la filtration $\mathfrak{a}_n$ de A est sa filtration p-adique (i. e. $\mathfrak{a}_n = p^n A$) et si p est non diviseur de zéro dans A. Un p-anneau a toujours un système de représentants multiplicatifs $f : A/\mathfrak{a}_1 \to A$ (cf. prop. 8), et pour toute suite d'éléments $\alpha_0, \ldots, \alpha_n, \ldots$, de $A/\mathfrak{a}_1$, la série

$$(**) \qquad \sum_{i=0}^{\infty} f(\alpha_i) \cdot p^i$$

converge vers un élément $a \in A$. Lorsque A est strict, on voit, en raisonnant comme dans la prop. 5, que tout élément $a \in A$ se met d'une façon et d'une seule sous la forme d'une série du type $(**)$; les α_i qui figurent dans cette série seront appelés les *coordonnées* de a.

Exemple de p-anneau strict. Soit X_α une famille d'indéterminées, et soit S l'anneau des $p^{-\infty}$-polynômes en les X_α à coefficients entiers, c'est-à-dire la réunion des anneaux $\mathbf{Z}[X_\alpha^{p^{-n}}]$ pour tous les n. Si l'on munit S de la filtration p-adique $|p^n S|_{n \geqslant 0}$ et que

l'on complète, on obtient un p-anneau strict, que nous noterons $\hat{S} = \hat{\mathbf{Z}}[X_\iota^{p^{-\infty}}]$. L'anneau résiduel $\hat{S}/p\hat{S}$ n'est pas autre chose que l'anneau $\mathbf{F}_p[X_\iota^{p^{-\infty}}]$; c'est bien un anneau parfait de caractéristique p. On notera que les X_n sont des représentants multiplicatifs dans $\hat{S}$ puisqu'ils admettent une racine p^n-ième pour tout n.

Appliquons ceci au cas où les indéterminées sont $X_0, \ldots, X_n, \ldots$, et $Y_0, \ldots, Y_n, \ldots$; dans l'anneau $\hat{\mathbf{Z}}[X_\iota^{p^{-\infty}}, Y_\iota^{p^{-\infty}}]$ ainsi obtenu, considérons les deux éléments

$$x = \sum_{i=0}^{\infty} X_i p^i \qquad \text{et} \qquad y = \sum_{i=0}^{\infty} Y_i p^i.$$

Si $*$ désigne l'une des opérations $+$, $\times$, $-$, le composé $x * y$ est un élément de l'anneau, donc peut s'écrire de façon unique sous la forme :

$$x * y = \sum_{i=0}^{\infty} f(Q_i^*) \cdot p^i, \qquad \text{avec} \qquad Q_i^* \in \mathbf{F}_p[X_\iota^{p^{-\infty}}, Y_\iota^{p^{-\infty}}].$$

Les Q_i^* sont des $p^{-\infty}$-polynômes à coefficients dans le corps premier $\mathbf{F}_p$; on peut parler de la *valeur* d'un tel polynôme lorsque ses arguments sont pris dans un anneau parfait k de caractéristique p. Nous allons voir que ces fonctions permettent de déterminer la structure d'un p-anneau strict. De façon précise :

PROPOSITION 9. *Soit* A *un p-anneau d'anneau résiduel k et soit $f : k \to A$ le système de représentants multiplicatifs de* A. *Soient $\{\alpha_i\}$ et $\{\beta_i\}$ deux suites d'éléments de k. On a alors*

$$\sum_{i=0}^{\infty} f(\alpha_i) \cdot p^i * \sum_{i=0}^{\infty} f(\beta_i) \cdot p^i = \sum_{i=0}^{\infty} f(\gamma_i) \cdot p^i$$

avec $\gamma_i = Q_i^*(\alpha_0, \alpha_1, \ldots; \beta_0, \beta_1, \ldots)$.

On voit tout de suite qu'il existe un homomorphisme θ de $\mathbf{Z}[X_\iota^{p^{-\infty}}, Y_\iota^{p^{-\infty}}]$ dans A qui applique X_i sur $f(\alpha_i)$ et Y_i sur $f(\beta_i)$. Cet homomorphisme se prolonge par continuité au complété $\hat{S} = \hat{\mathbf{Z}}[X_\iota^{p^{-\infty}}, Y_\iota^{p^{-\infty}}]$, et applique $x = \sum_{i=0}^{\infty} X_i p^i$ sur $a = \sum_{i=0}^{\infty} f(\alpha_i) \cdot p^i$, et de même pour y. Si l'on passe aux anneaux résiduels, θ définit un homomorphisme $\bar{\theta} : \mathbf{F}_p[X_\iota^{p^{-\infty}}, Y_\iota^{p^{-\infty}}] \to k$ qui applique les X_i sur les α_i et les Y_j sur les β_j. De plus θ commute aux représentants multiplicatifs (c'est là une propriété générale des homomorphismes de p-anneaux, qui provient de la caractérisation des représentants multiplicatifs comme puissances p^n-ièmes pour tout n). On a alors :

$$\begin{aligned} \sum f(\alpha_i) \cdot p^i * \sum f(\beta_i) \cdot p^i &= \theta(x) * \theta(y) = \theta(x * y) \\ &= \sum \theta(f(Q_i^*)) \cdot p^i \\ &= \sum f(\bar{\theta}(Q_i^*)) \cdot p^i \end{aligned}$$

ce qui démontre la proposition, puisque $\bar{\theta}(Q_i^*)$ n'est autre que γ_i.

PROPOSITION 10. *Soient* A *et* A′ *deux p-anneaux d'anneaux résiduels k et k′, et supposons que* A *soit strict. Pour tout homomorphisme* $\varphi : k \to k'$ *il existe alors un homomorphisme* $g : A \to A'$ *et un seul rendant commutatif le diagramme :*

$$\begin{array}{ccc} A & \xrightarrow{g} & A' \\ \downarrow & & \downarrow \\ k & \xrightarrow{\varphi} & k'. \end{array}$$

On a déjà remarqué que tout homomorphisme de A dans A′ commute aux systèmes de représentants multiplicatifs. Si $a \in A$ est un élément de coordonnées $\{\alpha_i\}$, on devra avoir :

$$g(a) = \sum_{i=0}^{\infty} g(f_A(\alpha_i)).p^i = \sum_{i=0}^{\infty} f_{A'}(\varphi(\alpha_i)).p^i,$$

ce qui démontre l'unicité de g. Pour avoir son existence, on prend la formule précédente pour définition, et la prop. 9 montre que c'est bien un homomorphisme d'anneaux.

COROLLAIRE. *Deux p-anneaux stricts ayant même anneau résiduel sont canoniquement isomorphes.*

LEMME 2. *Soit* $\varphi : k \to k'$ *un homomorphisme surjectif, les anneaux k et k′ étant des anneaux parfaits de caractéristique p. S'il existe un p-anneau strict* A *d'anneau résiduel k, il existe aussi un p-anneau strict* A′ *d'anneau résiduel k′.*

Nous allons définir A′ comme un quotient de A. Si a et b sont deux éléments de A de coordonnées α_i, β_i dans k, nous dirons que $a \equiv b$ si $\varphi(\alpha_i) = \varphi(\beta_i)$ pour tout i. Si $a \equiv a'$ et $b \equiv b'$, la prop. 9 montre que $a * b \equiv a' * b'$, et le quotient A′ de A par la relation d'équivalence que l'on vient de définir est un anneau. Si $x \in A'$ provient d'un élément $a \in A$ de coordonnées α_i, les $\xi_i = \varphi(\alpha_i)$ ne dépendent que de x, ce sont les *coordonnées* de x; toute suite $(\xi_0, \xi_1, \ldots)$ d'éléments de k' forme les coordonnées d'un élément $x' \in A'$ déterminé de façon unique. La multiplication par p dans A′ transforme l'élément de coordonnées $(\xi_0, \xi_1, \ldots)$ en celui de coordonnées $(0, \xi_0, \xi_1, \ldots)$. Il en résulte que p est non diviseur de zéro dans A′ et que $\bigcap p^n A' = 0$; la topologie p-adique de A′ est donc séparée; comme A′ est quotient de A, A′ est complet. Enfin, on voit tout de suite que l'application qui à x' fait correspondre sa première coordonnée ξ_0 est un isomorphisme de A'/pA' sur k', ce qui achève de montrer que A′ est un p-anneau strict d'anneau résiduel k'.

THÉORÈME 5. *Pour tout anneau parfait k de caractéristique p, il existe un p-anneau strict* $W(k)$ *et un seul dont l'anneau résiduel soit k.*

L'unicité a déjà été démontrée. Occupons-nous de l'existence : si k est de la forme $\mathbf{F}_p[X_\alpha^{p^{-\infty}}]$, pour une famille quelconque d'indéterminées X_α, on prend $W(k) = \hat{\mathbf{Z}}[X_\alpha^{p^{-\infty}}]$, cf. plus haut. Le cas général se déduit de là en appliquant le

lemme 2, et en remarquant que tout anneau parfait est quotient d'un anneau du type $\mathbf{F}_p[X_\alpha^{p^{-\infty}}]$.

La prop. 10 montre que $W(k)$ est un *foncteur* en k. De façon plus précise, on a un isomorphisme $\mathrm{Hom}(k, k') = \mathrm{Hom}(W(k), W(k'))$.

Démonstration des théorèmes 3 et 4.

Le théorème 3 est un cas particulier du théorème 5, si l'on remarque qu'un anneau de valuation discrète complet, absolument non ramifié, et de corps résiduel parfait k, n'est pas autre chose qu'un p-anneau strict d'anneau résiduel k. Dans le th. 4, l'existence et l'unicité de l'homomorphisme $g : W(k) \to A$ résultent de la prop. 10, en remarquant que A est un p-anneau. L'homomorphisme g est injectif, puisque A est de caractéristique zéro; enfin, si π est une uniformisante locale de A, un raisonnement analogue à celui de la prop. 5 montre que tout élément de A se met de manière unique sous la forme :

$$a = \sum_{i=0}^{\infty} \sum_{j=0}^{j=e-1} f(\alpha_{ij}) \cdot \pi^j p^i, \qquad \alpha_{ij} \in k,$$

d'où le fait que $\{1, \pi, \ldots, \pi^{e-1}\}$ est une base de A considéré comme $W(k)$-module (ce qui résulte aussi de la proposition 18 du Chap. I).

Remarque. Les fonctions Q_i^* qui définissent les opérations de $W(k)$ font effectivement intervenir les racines p^n-ièmes des X_α et des Y_α. Si l'on veut des polynômes au sens usuel, il faut définir les coordonnées α_i d'un élément a par la formule :

$$a = \sum_{i=0}^{\infty} f(\alpha_i)^{p^{-i}} p^i.$$

On est alors conduit à introduire les « vecteurs de Witt » qui font l'object du § suivant.

§ 6. *Vecteurs de Witt*

Soit p un nombre premier, soit $(X_0, \ldots, X_n, \ldots)$ une suite d'indéterminées, et considérons les polynômes suivants (appelés « polynômes de Witt ») :

$$W_0 = X_0$$
$$W_1 = X_0^p + pX_1$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$W_n = \sum_{i=0}^{i=n} p^i X_i^{p^{n-i}} = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Si l'on note Z' l'anneau $Z[p^{-1}]$, il est clair que l'on peut exprimer les X_l comme des polynômes par rapport aux W_l à coefficients dans Z' :

$$X_0 = W_0, \qquad X_1 = p^{-1}W_1 - W_0^p, \ \ldots, \text{ etc.}$$

Soit maintenant $(Y_0, \ldots, Y_n, \ldots)$ une autre suite d'indéterminées.

THÉORÈME 5. *Pour tout* $\Phi \in Z[X, Y]$, *il existe une suite* $(\varphi_0, \ldots, \varphi_n, \ldots)$ *d'éléments de* $Z[X_0, \ldots, X_n, \ldots; Y_0, \ldots, Y_n, \ldots]$ *et une seule telle que l'on ait* :

$$W_n(\varphi_0, \ldots, \varphi_n, \ldots) = \Phi(W_n(X_0, \ldots), W_n(Y_0, \ldots)), \quad n = 0, 1, \ldots$$

L'existence et l'unicité des φ_l sont évidentes *dans l'anneau des polynômes à coefficients dans* Z'; tout revient donc à montrer que les coefficients des φ_l n'ont pas de dénominateur, autrement dit, sont des éléments de Z. Ce fait peut se prouver directement (cf. Witt [73]). Mais il est plus commode, suivant Lazard (*loc. cit.*), de la déduire des résultats du § précédent :

Plaçons-nous de nouveau dans l'anneau $\hat{S} = \hat{Z}[X_l^{p^{-\infty}}, Y_l^{p^{-\infty}}]$, et posons :

$$x' = \sum_{i=0}^{\infty} X_l^{p^{-i}} p^i$$

$$y' = \sum_{i=0}^{\infty} Y_l^{p^{-i}} p^i.$$

Puisque $\Phi(x', y')$ est un élément de $\hat{S}$, on peut l'écrire de façon unique sous la forme :

$$\Phi(x', y') = \sum_{i=0}^{\infty} f(\bar{\psi}_l)^{p^{-i}} p^i, \qquad \bar{\psi}_l \in F_p[X_l^{p^{-\infty}}, Y_l^{p^{-\infty}}].$$

Notons ψ_l un représentant de $\bar{\psi}_l$ dans l'anneau $\hat{S}$. On va prouver à la fois que *les* φ_l *sont à coefficients entiers, et qu'ils sont congrus* mod. p *aux* ψ_l.

On a tout d'abord la congruence évidente :

$$\Phi\left(\sum_{i \leqslant n} X_l^{p^{-i}} p^i, \ \sum_{i \leqslant n} Y_l^{p^{-i}} p^i\right) \equiv \sum_{i \leqslant n} f(\bar{\psi}_l(X, Y))^{p^{-i}} p^i \text{ mod. } p^{n+1}.$$

Remplaçant X_l et Y_l par $X_l^{p^n}$ et $Y_l^{p^n}$ (ce qui définit un automorphisme de $\hat{S}$), on obtient :

$$\Phi(W_n(X), (W_n(Y)) \equiv \sum_{i \leqslant n} f(\bar{\psi}_l(X^{p^n}, Y^{p^n}))^{p^{-i}} p^i \text{ mod. } p^{n+1}.$$

Mais, on a $\bar{\psi}_l(X^{p^n}, Y^{p^n}) = \bar{\psi}_l(X, Y)^{p^n}$ puisque les coefficients de $\bar{\psi}_l$ appartiennent au corps F_p. Comme f commute à la puissance p-ième, on voit que la congruence précédente peut s'écrire :

$$W_n(\varphi_0, \ldots, \varphi_n) \equiv \sum_{i \leqslant n} f(\bar{\psi}_l)^{p^{n-i}} p^i \text{ mod. } p^{n+1}.$$

Mais $f(\overline{\psi_i}) \equiv \psi_i \bmod. p$, d'où $f(\overline{\psi_i})^{p^{n-i}} \equiv \psi_i^{p^{n-i}} \bmod. p^{n-i+1}$ (cf. § 3, lemme 1). On obtient donc :

$$W_n(\varphi_0, \ldots, \varphi_n) \equiv W_n(\psi_0, \ldots, \psi_n) \bmod. p^{n+1}.$$

En raisonnant par récurrence sur n, on peut supposer que φ_i est à coefficients entiers pour $i < n$, et congru mod. p à ψ_i (ou encore, quitte à changer ψ_i, on peut supposer que $\psi_i = \varphi_i$ pour $i < n$). On déduit donc de la congruence précédente :

$$p^n \varphi_n \equiv p^n \psi_n \bmod. p^{n+1},$$

d'où à la fois le fait que φ_n est à coefficients entiers, et que $\varphi_n \equiv \psi_n \bmod. p$, c.q.f.d.

Notons maintenant $S_0, \ldots, S_n, \ldots$, (resp. $P_0, \ldots, P_n, \ldots$) les polynômes $\varphi_0, \ldots, \varphi_n$ associés par le procédé du th. 5 au polynôme

$$\Phi(X, Y) = X + Y \text{ (resp. } \Phi(X, Y) = X.Y).$$

Si A est un anneau commutatif quelconque, et si $\mathfrak{a} = (a_0, \ldots, a_n, \ldots)$, $\mathfrak{b} = (b_0, \ldots, b_n, \ldots)$ sont des éléments de $A^{\mathbb{N}}$ (« vecteurs de Witt à coefficients dans A »), on posera :

$$\mathfrak{a} + \mathfrak{b} = (S_0(a, b), \ldots, S_n(a, b), \ldots)$$
$$\mathfrak{a}.\mathfrak{b} = (P_0(a, b), \ldots, P_n(a, b), \ldots).$$

THÉORÈME 6. *Les lois de composition définies ci-dessus font de* $A^{\mathbb{N}}$ *un anneau commutatif à élément unité, appelé l'anneau des vecteurs de Witt à coefficients dans* A, *et noté* W(A).

Remarquons tout d'abord que, si l'on fait correspondre à un vecteur de Witt $\mathfrak{a} = (a_0, \ldots, a_n, \ldots)$ l'élément de l'anneau produit $A^{\mathbb{N}}$ qui a pour coordonnées les $W_n(a)$, on obtient un homomorphisme

$$W_* : W(A) \to A^{\mathbb{N}},$$

par définition même des polynômes S et P.

L'homomorphisme W_* est un isomorphisme si p est inversible dans A, et dans ce cas on voit bien que W(A) est un anneau commutatif d'élément unité $1 = (1, 0, \ldots, 0, \ldots)$. Mais, si le théorème est établi pour un anneau A, il l'est aussi pour tout sous-anneau et tout quotient. Comme il est vrai pour tout anneau de polynômes $\mathbf{Z}'[T_\alpha]$, il l'est pour $\mathbf{Z}[T_\alpha]$, donc pour tout anneau, c.q.f.d.

Exemples.

On a

$$S_0(a, b) = a_0 + b_0, \qquad S_1(a, b) = a_1 + b_1 + \frac{a_0^p + b_0^p - (a_0 + b_0)^p}{p},$$
$$P_0(a, b) = a_0.b_0, \qquad P_1(a, b) = b_0^p a_1 + b_1 a_0^p + p a_1 b_1.$$

Au lieu de considérer des vecteurs de longueur infinie, on peut se borner à considérer des vecteurs $(a_0, \ldots, a_{n-1})$ à n composantes. Comme les polynômes φ_i ne font intervenir que les variables d'indice $\leqslant i$, on en conclut que ces vecteurs forment un

anneau $W_n(A)$, quotient de $W(A)$, que l'on appelle *l'anneau des vecteurs de Witt de longueur n*. On a $W_1(A) = A$. L'anneau $W(A)$ est *limite projective* des anneaux $W_n(A)$, pour $n \to +\infty$.

Les applications V *et* r.

Si $\mathfrak{a} = (a_0, \ldots, a_n, \ldots)$ est un vecteur de Witt, on définit le vecteur $V\mathfrak{a}$ par la formule :

$$V\mathfrak{a} = (0, a_0, \ldots, a_{n-1}, \ldots) \quad (\text{« décalage »}).$$

L'application $V : W(A) \to W(A)$ est *additive*. En effet, il suffit de le vérifier lorsque p est inversible dans A, et l'homomorphisme

$$W_* : W(A) \to A^{\mathbb{N}}$$

transforme alors V en l'application qui fait passer de $(w_0, w_1, \ldots)$ à $(0, pw_0, \ldots)$.

Par passage au quotient, on déduit de V une application additive de $W_n(A)$ dans $W_{n+1}(A)$. On a des suites exactes :

$$0 \to W_k(A) \xrightarrow{V^r} W_{k+r}(A) \to W_r(A) \to 0.$$

Si $x \in A$, on pose :

$$r(x) = (x, 0, \ldots, 0, \ldots).$$

On définit ainsi une application $r : A \to W(A)$. Lorsque p est inversible dans A, W_* transforme r en l'application qui fait passer de x à $(x, x^p, \ldots, x^{p^n}, \ldots)$. On en déduit par le même raisonnement que ci-dessus, les formules :

$$r(xy) = r(x).r(y), \qquad x, y \in A$$

$$(a_0, a_1, \ldots) = \sum_{n=0}^{\infty} V^n(r(a_n)), \qquad a_i \in A$$

$$r(x).(a_0, \ldots) = (xa_0, x^p a_1, \ldots, x^{p^n} a_n, \ldots), \qquad x, a_i \in A.$$

THÉORÈME 7. *Si k est un anneau parfait de caractéristique p, $W(k)$ est un p-anneau strict d'anneau résiduel k.*

Soit H le p-anneau strict d'anneau residuel k, et soit $f : k \to H$ le système de représentants multiplicatifs de H. A un vecteur de Witt $\mathfrak{a} = (a_0, \ldots, a_n, \ldots)$, associons l'élément $\theta(\mathfrak{a}) \in H$ défini par :

$$\theta(\mathfrak{a}) = \sum_{i=0}^{\infty} f(a_i)^{p^{-i}} p^i.$$

Les formules :

$$\theta(\mathfrak{a} + \mathfrak{b}) = \theta(\mathfrak{a}) + \theta(\mathfrak{b}), \qquad \theta(\mathfrak{a}.\mathfrak{b}) = \theta(\mathfrak{a}).\theta(\mathfrak{b})$$

sont vraies lorsque $H = \hat{S}$, $\mathfrak{a} = (X_0, \ldots)$, $\mathfrak{b} = (Y_0, \ldots)$, on l'a vu au cours de la

démonstration du théorème 5. Il en résulte facilement qu'elles sont vraies sans restriction sur $\mathfrak{a}$ et $\mathfrak{b}$, autrement dit que θ est un homomorphisme d'anneaux. Comme θ est bijectif, on voit finalement que c'est un *isomorphisme* de W(A) sur H, ce qui démontre le théorème.

COROLLAIRE. *On a* $W(\mathbf{F}_p) = \mathbf{Z}_p$ *et* $W_n(\mathbf{F}_p) = \mathbf{Z}/p^n\mathbf{Z}$.

En effet, l'anneau $\mathbf{Z}_p$ des entiers p-adiques est un p-anneau strict d'anneau résiduel le corps premier $\mathbf{F}_p$.

L'application F.

Supposons que k soit un anneau de caractéristique p (non nécessairement parfait). L'application $x \to x^p$ est un homomorphisme de k dans k. Elle définit donc une application $F : W(k) \to W(k)$, donnée par la formule :

$$F(a_0, a_1, \ldots) = (a_0^p, a_1^p, \ldots)$$

qui est un homomorphisme d'anneaux.

On a de plus *l'identité* $VF = FV = p$. En effet, il suffit de vérifier cette identité lorsque k est parfait; en appliquant alors l'isomorphisme θ défini ci-dessus, on trouve :

$$\theta(FV\mathfrak{a}) = \sum_{i=0}^{\infty} f(a_i)^{p^{-i}} p^{i+1} = p\theta(\mathfrak{a}) = \theta(p\mathfrak{a}),$$

ce qui montre bien que $FV = VF = p$.

Remarque. Dans le langage des *schémas* de Grothendieck, les constructions précédentes reviennent à définir pour, chaque entier n, un *schéma d'anneaux* W_n, affine et de type fini sur Spec(Z). Pour tout anneau A, l'anneau $W_n(A)$ n'est autre que l'ensemble des *points de* W_n *à valeurs dans* A.

DEUXIÈME PARTIE

RAMIFICATION

CHAPITRE III

DISCRIMINANT ET DIFFÉRENTE

Dans tout ce chapitre, A désigne un anneau de Dedekind, de corps des fractions K.

§ 1. *Réseaux*

Soit V un K-espace vectoriel de dimension finie. On appelle *réseau* de V (par rapport à A) un sous-A-module X de V engendrant V, et de type fini sur A. Si A est principal, il revient au même de dire que X est un A-module libre de rang égal à $[V : K]$; on peut souvent se ramener à ce cas en localisant, c'est-à-dire en remplaçant A par $A_\mathfrak{p}$ et X par $A_\mathfrak{p}X = X_\mathfrak{p}$.

Soient X_1 et X_2 deux réseaux de V; si $X_2 \subset X_1$, le module X_1/X_2 est un module de longueur finie, et l'on a défini au Chap. I, § 5 son invariant $\chi(X_1/X_2)$ qui est un idéal non nul de A. Nous allons étendre cette définition au cas général :

LEMME 1. *Soient* X_1 *et* X_2 *deux réseaux de* V; *l'idéal fractionnaire* $\chi(X_1/X_3)\cdot\chi(X_2/X_3)^{-1}$, *défini pour tout réseau* $X_3 \subset X_1 \cap X_2$, *ne dépend que de* X_1 *et* X_2.

En effet, si l'on pose $X_4 = X_1 \cap X_2$, la suite exacte :

$$0 \to X_4/X_3 \to X_1/X_3 \to X_1/X_4 \to 0$$

montre que $\chi(X_1/X_3) = \chi(X_4/X_3)\cdot\chi(X_1/X_4)$, et de même :

$$\chi(X_2/X_3) = \chi(X_4/X_3)\cdot\chi(X_2/X_4).$$

On en tire :

$$\chi(X_1/X_3)\cdot\chi(X_2/X_3)^{-1} = \chi(X_1/X_4)\cdot\chi(X_2/X_4)^{-1}, \qquad \text{c.q.f.d.}$$

On peut donc associer à X_1 et X_2 l'idéal fractionnaire non nul

$$\chi(X_1, X_2) = \chi(X_1/X_3)\cdot\chi(X_2/X_3)^{-1} \qquad \text{pour } X_4 \subset X_1 \cap X_2.$$

PROPOSITION 1. *On a les formules suivantes* :

(*a*) $\chi(X_1, X_2).\chi(X_2, X_3).\chi(X_3, X_1) = 1$.

(*b*) $\chi(X_1, X_2).\chi(X_2, X_1) = 1$.

(*c*) $\chi(X_1, X_2) = \chi(X_1/X_2)$ *si* $X_1 \supset X_2$.

(Par abus d'écriture, on note 1 l'élément unité du groupe des idéaux fractionnaires non nuls de A, c'est-à-dire l'idéal A.)

La formule (*a*) se démontre en choisissant un réseau X contenu dans $X_1 \cap X_2 \cap X_3$, et en écrivant $\chi(X_i, X_j)$ sous la forme $\chi(X_i/X).\chi(X_j/X)^{-1}$. Les formules (*b*) et (*c*) sont triviales.

PROPOSITION 2. *Si u est un* K*-automorphisme de* V, *et si* X *est un réseau de* V, *on a* $\chi(X, uX) = (\det(u))$ (idéal principal engendré par $\det(u)$).

(On a noté *u*X le transformé de X par *u*.)

En localisant, et en multipliant *u* par une constante, on se ramène au cas où $X = A^n$, et où $uX \subset X$, auquel cas la proposition résulte du lemme 3 du Chap I, § 5.

La proposition précédente suggère la définition directe suivante de l'idéal $\chi(X, X')$:

Soit $n = [V : K]$, et soit $W = \bigwedge^n V$; c'est un espace vectoriel de dimension 1 sur K. A tout réseau X de V faisons correspondre $X_W = \bigwedge^n X$, qui s'identifie à un réseau de W; comme $[W : K] = 1$, si D et D′ sont deux réseaux de W, il existe un idéal fractionnaire non nul a de K et un seul tel que $D' = aD$ (c'est d'ailleurs $\chi(D, D')$). En appliquant ceci à $D = X_W$, $D' = X'_W$, on obtient un idéal *qui n'est autre que* $\chi(X, X')$: c'est immédiat par localisation, en appliquant la proposition 2.

§ 2. *Discriminant d'un réseau par rapport à une forme bilinéaire*

Nous supposerons maintenant que l'espace vectoriel V est muni d'une *forme bilinéaire non dégénérée* $T(x, y)$.

Soit $n = [V : K]$. On sait que T se prolonge en une forme bilinéaire non dégénérée (que nous noterons encore T) sur l'algèbre extérieure de V, et en particulier sur $W = \bigwedge^n V$. Cette forme donne en fait un isomorphisme.

$$T : W \otimes_K W \to K.$$

Soit X un réseau de V, et soit X_W sa puissance extérieure n-ième, identifiée à un réseau de W. L'image de $X_W \otimes_A X_W$ par T est un *idéal fractionnaire non nul* de K, qui s'appelle le *discriminant de* X *par rapport à* T; nous le noterons $\mathfrak{d}_{X,T}$ ou seulement $\mathfrak{d}_X$ si cela ne prête pas à confusion.

Remarque. La définition précédente montre que $\mathfrak{d}_X$ est isomorphe comme A-module à $X_W \otimes_A X_W$; sa classe d'idéaux (modulo les idéaux principaux) est donc un *carré*.

PROPOSITION 3. *Si* X *est un* A*-module libre de base* $S = \{e_1, \ldots, e_n\}$, *l'idéal* $\mathfrak{d}_{X,T}$ *est l'idéal principal engendré par le discriminant* $D_T(S)$ *de* S (*au sens de Bourbaki, Alg.*, Chap. IX, § 2).

[On rappelle que $D_T(S) = \det(T(e_i, e_j))$.]

En effet, on sait que dans ce cas X_W est un A-module libre de base $\{e\}$, avec $e = e_1 \wedge \cdots \wedge e_n$, et que $T(e, e) = D_T(S)$, cf. Bourbaki, *loc. cit.* L'image de $X_W \otimes_A X_W$ dans K est donc bien engendrée par $D_T(S)$.

Remarque. Quitte à localiser, on aurait pu prendre la formule $\mathfrak{d}_{X,T} = (\det(T(e_i, e_j)))$ pour *définition* de $\mathfrak{d}_{X,T}$.

PROPOSITION 4. *Soit* X *un réseau de* V, *et soit* X_T^* *l'ensemble des* $y \in V$ *tels que* $T(x, y) \in A$ *pour tout* $x \in V$. *Alors* X_T^* *est un réseau de* V, *et l'on a* :

$$\mathfrak{d}_{X,T} = \chi(X_T^*, X).$$

En localisant, on se ramène au cas où X est libre de base $\{e_i\}$; alors X_T^* est libre de base la base $\{e_i^*\}$ définie par les relations

$$T(e_i, e_j^*) = \delta_{ij} \qquad \text{cf. Bourbaki, } \textit{loc. cit.}, \text{ p. 22.}$$

Si l'on écrit $e_i = \sum x_{ij} e_j^*$, la proposition 2 montre que $\chi(X_T^*, X) = (\det(x_{ij}))$. Comme $T(e_i, e_j) = x_{ji}$, on obtient la formule cherchée.

Enfin, la proposition suivante montre comment $\mathfrak{d}_{X,T}$ varie avec X :

PROPOSITION 5. *Si* X *et* X′ *sont deux réseaux de* V, *on a* :

$$\mathfrak{d}_{X',T} = \mathfrak{d}_{X,T} \cdot \chi(X, X')^2.$$

Soit $\mathfrak{a} = \chi(X, X')$. On a vu au § 1 que $X'_W = \mathfrak{a} . X_W$ dans W; l'image par l'isomorphisme $T : W \otimes W \to K$ de $X'_W \otimes X'_W$ est donc égale au produit de $\mathfrak{a}^2$ par l'image de $X_W \otimes X_W$, ce qui démontre la proposition.

COROLLAIRE. *Si* $X' \subset X$, *on a* $\mathfrak{d}_{X',T} = \mathfrak{d}_{X,T}\mathfrak{a}^2$, *où* $\mathfrak{a}$ *est un idéal de* A; *on a* $\mathfrak{a} = 1$ *si et seulement si* $X' = X$.

On prend $\mathfrak{a} = \chi(X/X')$; il est clair que $\mathfrak{a} = 1$ si et seulement si $X = X'$.

§ 3. *Discriminant et différente d'une extension séparable*

Soit L une extension finie et séparable du corps K. On sait que l'homomorphisme

$$\mathrm{Tr} : L \to K$$

est surjectif, et que la forme bilinéaire $\mathrm{Tr}(xy)$ est non dégénérée sur L. On peut donc appliquer les définitions et résultats du § précédent à cette forme bilinéaire; en particulier, le *discriminant* d'un réseau de L (par rapport à A) est défini; si ce réseau est un A-module libre de base $\{e_i\}$, son discriminant est l'idéal engendré par $\det(\mathrm{Tr}(e_i e_j))$, et l'on sait (Bourbaki, *Alg.*, Chap. V, § 10, prop. 12) que l'on a :

$$\det(\mathrm{Tr}(e_i e_j)) = (\det(\sigma(e_i)))^2,$$

σ parcourant l'ensemble des K-isomorphismes de L dans une clôture algébrique de K.

Ceci s'applique notamment à la fermeture intégrale B de A dans L; la proposition 8 du Chapitre I montre en effet que c'est bien un réseau de L. Le discriminant correspondant sera noté $\mathfrak{d}_{B/A}$, ou parfois $\mathfrak{d}_{L/K}$ (lorsqu'aucune confusion sur A n'est possible).

Soit B^* l'ensemble des $y \in L$ tels que $\mathrm{Tr}(xy) \in A$ pour tout $x \in B$; c'est le réseau noté B_1^* au § précédent. On l'appelle la *codifférente* de B sur A (ou encore la « différente inverse »). C'est un sous-B-module de L; on voit tout de suite que c'est le plus grand sous-B-module E de L tel que $\mathrm{Tr}(E) \subset A$. En particulier, comme $\mathrm{Tr}(B) \subset A$, on a $B \subset B^*$. La codifférente est donc un idéal fractionnaire de L par rapport à B; son inverse s'appelle la *différente* de B sur A (ou de l'extension L/K), et se note $\mathfrak{D}_{B/A}$ ou $\mathfrak{D}_{L/K}$; c'est un idéal non nul de B. Différente et discriminant sont reliés par la proposition suivante :

PROPOSITION 6. *On a* $\mathfrak{d}_{B/A} = \chi_A(B^*/B) = N_{L/K}(\mathfrak{D}_{B/A})$.

L'égalité $\mathfrak{d}_{B/A} = \chi_A(B^*/B)$ résulte de la proposition 4. D'autre part, on a $\chi_B(B^*/B) = \mathfrak{D}_{B/A}$, et l'on sait que $\chi_A = N_{L/K} \circ \chi_B$, cf. Chap. I, § 5, prop. 12.

COROLLAIRE. *Le discriminant* $\mathfrak{d}_{B/A}$ *est contenu dans* A.

Remarque. La proposition précédente montre que la différente détermine le discriminant; la réciproque n'est pas vraie en général (sauf toutefois s'il n'y a qu'un seul idéal premier de B au-dessus de tout idéal premier de A, ce qui est justement le cas lorsque l'on complète).

PROPOSITION 7. *Soit* $\mathfrak{a}$ (*resp.* $\mathfrak{b}$) *un idéal fractionnaire de* K (*resp.* L) *relativement à* A (*resp.* B). *Les deux propriétés suivantes sont alors équivalentes*:

(i) $\mathrm{Tr}(\mathfrak{b}) \subset \mathfrak{a}$.

(ii) $\mathfrak{b} \subset \mathfrak{a}.\mathfrak{D}_{B/A}^{-1}$.

Le cas $\mathfrak{a} = 0$ est trivial. Lorsque $\mathfrak{a} \neq 0$. la proposition résulte des équivalences suivantes (qui sont immédiates) :

$$\mathrm{Tr}(\mathfrak{b}) \subset \mathfrak{a} \iff \mathfrak{a}^{-1}\mathrm{Tr}(\mathfrak{b}) \subset A \iff \mathrm{Tr}(\mathfrak{a}^{-1}\mathfrak{b}) \subset A \iff \mathfrak{a}^{-1}\mathfrak{b} \subset \mathfrak{D}_{B/A}^{-1} \iff \mathfrak{b} \subset \mathfrak{a}.\mathfrak{D}_{B/A}^{-1}.$$

Il est clair que la propriété énoncée dans la proposition 7 *caractérise* la différente.

§ 4. *Propriétés élémentaires de la différente et du discriminant.*

On conserve les notations du § précédent : L désigne une extension finie séparable de K, et B la fermeture intégrale de A dans L.

(i) *Transitivité.*

PROPOSITION 8. *Soit* M/L *une extension séparable de degré fini n, et soit* C *la fermeture intégrale de* A *dans* M. *On a*:

$$\mathfrak{D}_{C/A} = \mathfrak{D}_{C/B}.\mathfrak{D}_{B/A} \qquad \textit{et} \qquad \mathfrak{d}_{C/A} = (\mathfrak{d}_{B/A})^n.N_{L/K}(\mathfrak{d}_{C/B}).$$

Posons $\theta = \mathrm{Tr}_{M/K}$, $\theta' = \mathrm{Tr}_{L/K}$, $\theta'' = \mathrm{Tr}_{M/L}$; on a $\theta = \theta' \circ \theta''$. Soit $\mathfrak{c}$ un idéal fractionnaire de M par rapport à C. Les équivalences suivantes sont immédiates :

$$\mathfrak{c} \subset \mathfrak{D}_{C/B}^{-1} \iff \theta''(\mathfrak{c}) \subset B \iff \mathfrak{D}_{B/A}^{-1}.\theta''(\mathfrak{c}) \subset \mathfrak{D}_{B/A}^{-1} \iff \theta'(\mathfrak{D}_{B/A}^{-1}.\theta''(\mathfrak{c})) \subset A$$
$$\iff \theta(\mathfrak{D}_{B/A}^{-1}.\mathfrak{c}) \subset A \iff \mathfrak{D}_{B/A}^{-1}.\mathfrak{c} \subset \mathfrak{D}_{C/A}^{-1} \iff \mathfrak{c} \subset \mathfrak{D}_{B/A}.\mathfrak{D}_{C/A}^{-1}.$$

En comparant, on voit que $\mathfrak{D}_{C/B}^{-1} = \mathfrak{D}_{B/A}.\mathfrak{D}_{C/A}^{-1}$, d'où la formule relative à la différente. En appliquant $N_{M/K}$ aux deux membres, on obtient celle relative aux discriminants.

(ii) *Localisation.*

PROPOSITION 9. *Si* S *est une partie muliplicative de* A, *on a* :

$$S^{-1}\mathfrak{D}_{B/A} = \mathfrak{D}_{S^{-1}B/S^{-1}A} \qquad \textit{et} \qquad S^{-1}\mathfrak{d}_{B/A} = \mathfrak{d}_{S^{-1}B/S^{-1}A}.$$

Vu la formule $(S^{-1}\mathfrak{b})^{-1} = S^{-1}\mathfrak{b}^{-1}$, plusieurs fois utilisée au Chap. I, il suffit de montrer que $S^{-1}B^* = (S^{-1}B)^*$. Or, si $x = s^{-1}y$, avec $s \in S$, $y \in B^*$, on a

$$\mathrm{Tr}(x) = s^{-1}\mathrm{Tr}(y) \in S^{-1}A;$$

comme $S^{-1}B^*$ contient $S^{-1}B$ et est un idéal fractionnaire, ceci montre que $S^{-1}B^* \subset (S^{-1}B)^*$. En sens inverse, soient b_i des générateurs de B, et soit $x \in (S^{-1}B)^*$; on a $\mathrm{Tr}(xb_i) \in S^{-1}A$, d'où $\mathrm{Tr}(xb_i) = s^{-1}a_i$, avec $a_i \in A$ (les b_i étant en nombre fini), et $sx \in B^*$, ce qui démontre l'inclusion opposée.

(iii) *Complétion.*

PROPOSITION 10. *Soit* $\mathfrak{P}$ *un idéal premier de* B, *et soit* $\mathfrak{p} = \mathfrak{P} \cap A$. *Soit* $\hat{\mathfrak{D}}_{\mathfrak{P}}$ *l'idéal du complété* $\hat{B}_{\mathfrak{P}}$ *engendré par la différente* $\mathfrak{D}_{B/A}$; *l'idéal* $\hat{\mathfrak{D}}_{\mathfrak{P}}$ *est alors la différente de l'anneau* $\hat{B}_{\mathfrak{P}}$ *par rapport à l'anneau* $\hat{A}_{\mathfrak{p}}$.

(En d'autres termes, l'exposant de $\mathfrak{P}$ dans $\mathfrak{D}_{B/A}$ est égal à l'exposant de $\mathfrak{P}\hat{B}_{\mathfrak{P}}$ dans la différente de $\hat{B}_{\mathfrak{P}}$ sur $\hat{A}_{\mathfrak{p}}$: la différente « se conserve par complétion ».)

En appliquant la proposition 9 avec $S = A - \mathfrak{p}$, on se ramène au cas où A est un *anneau de valuation discrète*; nous noterons $\hat{A}$ (resp. $\hat{K}$) son complété (resp. celui du corps K). De même, si $(\mathfrak{P}_i)_{i \in I}$ est la famille des idéaux premiers de B au-dessus de $\mathfrak{p}$, nous noterons $\hat{B}_i$ (resp. L_i) le complété de B (resp. de L) pour la valuation définie par $\mathfrak{P}_i$.

Plaçons-nous d'abord dans la $\hat{K}$-algèbre $L \otimes_K \hat{K} = \hat{L}$; soit $\hat{B} = B \otimes_A \hat{A}$; c'est un $\hat{A}$-réseau de $\hat{L}$. La forme $\mathrm{Tr}(xy)$ est une forme bilinéaire non dégénérée sur $\hat{L}$, déduite par extension des scalaires de la forme analogue sur L. On en déduit facilement (par exemple en prenant une base) que le réseau dual $(\hat{B})^*$ de $\hat{B}$ s'obtient par extension des scalaires à partir du réseau $B^* = \mathfrak{D}_{B/A}^{-1}$. En d'autres termes, on a :

$$(\hat{B})^* = (B^*)\hat{} = B^* \otimes_A \hat{A}.$$

Mais d'autre part, nous savons (cf. Chap. II, § 2) que $L\otimes_K\hat{K} = \prod_{i\in I}\hat{L}_i$ et que $B\otimes_A\hat{A} = \prod_{i\in I}\hat{B}_i$; si l'on note Tr_i la trace dans l'extension $\hat{L}_i/\hat{K}$, la forme bilinéaire $\mathrm{Tr}(xy)$ sur $\hat{L}$ est somme directe des formes bilinéaires $\mathrm{Tr}_i(xy)$ sur les $\hat{L}_i$. La formule évidente :

$$\Big(\prod_{i\in I} X_i\Big)^* = \prod_{i\in I}(X_i)^*,$$

appliquée à $X_i = \hat{B}_i$, montre alors que $(\hat{B})^* = \prod_{i\in I}(\hat{B}_i^*)$. En d'autres termes, *la codifférente de* B *par rapport à* A *engendre dans chacun des* $\hat{L}_i$ *la codifférente de* $\hat{B}_i$ *par rapport à* $\hat{A}$; en prenant les inverses, on obtient le même résultat pour la différente, c.q.f.d.

COROLLAIRE. *Soit* $\hat{\mathfrak{d}}$ *l'idéal de* $\hat{A}_\mathfrak{p}$ *engendré par le discriminant* $\mathfrak{d}_{B/A}$ *et soit* $\mathfrak{d}_\mathfrak{P}$ *le discriminant de* $\hat{B}_\mathfrak{P}$ *par rapport à* $\hat{A}_\mathfrak{p}$. *On a* :

$$\hat{\mathfrak{d}} = \prod_{\mathfrak{P}\mid\mathfrak{p}} \mathfrak{d}_\mathfrak{P}.$$

Cela résulte de la proposition 10, en prenant la norme.

Exercice. Soit C un sous-anneau de B, contenant A, et ayant même corps des fractions que B.

a) Montrer que, parmi tous les idéaux de B contenus dans C, il en existe un plus grand, qui est l'annulateur du C-module B/C; on le notera $\mathfrak{f}_{C/B}$ (c'est le « conducteur » de B dans C).

b) Montrer que $\mathfrak{f}_{C/B} = (B^* : C^*)$, autrement dit que $\mathfrak{f}_{C/B}$ est l'ensemble des $x\in L$ tels que $xC^*\subset B^*$.

c) On suppose que C^*, considéré comme C-idéal fractionnaire, est inversible; soit $\mathfrak{c}$ son inverse (on a donc $\mathfrak{c}C^* = C$). Déduire de *b*) la formule :

$$\mathfrak{f}_{C/B} = \mathfrak{c}.\mathfrak{D}_{B/A}^{-1}.$$

§ 5. *Extensions non ramifiées*

On conserve les notations et hypothèses des §§ 3 et 4.

THÉORÈME 1. *Soit* $\mathfrak{P}$ *un idéal premier de* B, *et soit* $\mathfrak{p} = \mathfrak{P}\cap A$. *Pour que l'extension* L/K *soit non ramifiée en* $\mathfrak{P}$ (*cf.* Chap. I, § 4), *il faut et il suffit que* $\mathfrak{P}$ *ne divise pas la différente* $\mathfrak{D}_{B/A}$.

Les propositions 9 et 10 permettent de se ramener au cas où A est un anneau de valuation discrète complet, de corps résiduel k; dans ce cas, B est lui aussi un anneau de valuation discrète. Dire que $\mathfrak{P}$ est non ramifié, équivaut alors à dire que $B/\mathfrak{p}B$ est un corps (autrement dit que $e_\mathfrak{P} = 1$), et que ce corps est extension séparable de k.

Soit $\{x_i\}$ une base de B sur A, et soit $d = \det(\mathrm{Tr}(x_ix_j))$; on sait que $\mathfrak{d}_{B/A}$ est l'idéal principal engendré par d. Pour que $\mathfrak{P}$ soit non ramifié, il est donc nécessaire et suffisant que $\mathfrak{p}$ ne divise pas d, c'est-à-dire que l'image $\overline{d}$ de d dans k soit non nulle. Or, si l'on pose $\overline{B} = B/\mathfrak{p}B$, les images $\overline{x}_i$ des x_i dans $\overline{B}$ forment une base de $\overline{B}$ et le discri-

minant de cette base est égal à $\overline{d}$. D'après un résultat connu (Bourbaki, *Alg.*, Chap. IX, § 2, prop. 5), la condition $\overline{d} \neq 0$ équivaut donc à dire que $\overline{B}$ est une k-algèbre séparable, et comme c'est un anneau local, cela revient bien à dire que c'est un corps, et que ce corps est extension séparable de k, c.q.f.d.

COROLLAIRE 1. *Soit* $\mathfrak{p}$ *un idéal premier de* A. *Pour que* L/K *soit non ramifiée en* $\mathfrak{p}$, *il faut et il suffit que* $\mathfrak{p}$ *ne divise pas le discriminant* $\mathfrak{d}_{B/A}$.

Cela résulte du fait que $\mathfrak{d}_{B/A} = N(\mathfrak{D}_{B/A})$.

COROLLAIRE 2. *Presque tous les idéaux premiers de* B (*ou de* A) *sont non ramifiés dans l'extension* L/K.

C'est évident.

On va maintenant examiner d'un peu plus près la structure des extensions non ramifiées, en nous bornant au cas où A *est un anneau de valuation discrète complet*; on notera k son corps résiduel.

THÉORÈME 2. *Soit* k'/k *une extension séparable finie. Il existe alors une extension finie non ramifiée* K'/K *dont l'extension résiduelle correspondante est isomorphe à* k'/k; *cette extension est unique, à un isomorphisme unique près. Elle est galoisienne si et seulement si* k'/k *l'est.*

Puisque k'/k est finie et séparable, elle est monogène. Soit ξ un générateur de cette extension, et soit φ son polynôme minimal sur k; il est de degré $n = [k' : k]$. Soit $f \in A[X]$ un polynôme unitaire dont la réduction $\overline{f}$ mod. $\mathfrak{p}$ est égale à φ. D'après la proposition 15 du chapitre I, l'anneau $A' = A[X]/(f)$ est un anneau de valuation discrète, non ramifié sur A, et d'extension résiduelle k'/k. Son corps des fractions est le corps K' cherché, ce qui démontre la première partie du théorème. Les autres assertions (qui, elles, font intervenir de façon essentielle le fait que A est *complet*) résultent du théorème plus précis suivant :

THÉORÈME 3. *Soit* K'/K *une extension finie non ramifiée de* K, *d'extension résiduelle* k'/k, *et soit* K''/K *une extension finie quelconque, d'extension résiduelle* k''/k. *L'ensemble des* K-*isomorphismes de* K' *dans* K'' *correspond alors bijectivement* (*par réduction*) *à l'ensemble des* k-*isomorphismes de* k' *dans* k''.

Convenons de noter $\mathrm{Hom}^{al}(B, C)$ l'ensemble des homomorphismes d'algèbres de B dans C. Si l'on désigne par A' et A'' les fermetures intégrales de A dans K' et K'' respectivement, on a évidemment :

$$\mathrm{Hom}^{al}_{K}(K', K'') = \mathrm{Hom}^{al}_{A}(A', A''),$$

et il s'agit de montrer que l'homomorphisme canonique

$$\theta : \mathrm{Hom}^{al}_{A}(A', A'') \to \mathrm{Hom}^{al}_{k}(k', k'')$$

est bijectif.

D'après la proposition 16 du Chapitre I, il existe $x \in A'$ tel que, si $n = [K' : K]$, les éléments $\{1, x, \ldots, x^{n-1}\}$ forment une base de A' sur A; de plus, si f désigne le polynôme caractéristique de x, la réduction $\overline{f}$ de f est le polynôme caractéristique de l'image $\overline{x}$ de x dans k'. Il s'ensuit que les éléments de $\mathrm{Hom}^{al}_{A}(A', A'')$ (resp. de $\mathrm{Hom}^{al}_{k}(k', k'')$) correspondent biunivoquement aux éléments $a'' \in A''$ (resp. $\xi'' \in k''$)

tels que $f(a'') = 0$ (resp. tels que $\overline{f}(\xi'') = 0$); quant à l'application θ, elle correspond à la réduction $a'' \to \xi'' = \overline{a}''$. Tout revient donc à montrer qu'une racine de $\overline{f}$ dans k'' se relève de façon unique en une racine de f dans A'', ce qui est une conséquence de la proposition 7 du Chapitre II (noter que toutes les racines de $\overline{f}$ sont simples, puisque ce polynôme est irréductible et séparable sur k).

COROLLAIRE 1. *Soit k_s la clôture séparable de k (i.e. la plus grande extension séparable de k contenue dans une clôture algébrique de k), et soit K_{nr} la limite inductive des extensions non ramifiées de K correspondant aux sous-extensions finies de k_s. Le corps K_{nr} est galoisien sur K, de corps résiduel k_s, et l'on a* : $G(K_{nr}/K) = G(k_s/k)$.

C'est clair.

L'extension K_{nr} s'appelle, pour des raisons évidentes, l'extension maximale non ramifiée de K. Elle est unique, à isomorphisme près. Si par exemple k est un corps fini, $G(k_s/k)$ est isomorphe au complété $\hat{\mathbf{Z}}$ de $\mathbf{Z}$ pour la topologie des sous-groupes d'indice fini, et il en est de même de $G(K_{nr}/K)$.

COROLLAIRE 2. *Soit K''/K une extension finie, d'extension résiduelle k''/k. Les sous-extensions K'/K de K''/K qui sont non ramifiées sur K correspondent biunivoquement aux sous-extensions k'/k de k''/k qui sont séparables.*

C'est clair.

COROLLAIRE 3. *Les hypothèses étant celles du corollaire 2, il existe un sous-corps non ramifié maximal K'/K contenu dans K''. Son corps résiduel k' est la plus grande extension séparable de k contenue dans k''. On a $e(K''/K') = e(K''/K), f(K''/K') = [k'' : k]_i$ et $f(K'/K) = [k'' : k]_s$.*

Cela résulte du corollaire 2.

[On applique le plus souvent le corollaire 3 dans le cas où k'' est séparable sur k; on obtient alors un corps intermédiaire K' tel que K''/K' soit totalement ramifié ($f = 1$), et K'/K non ramifié.]

Remarques. 1) Lorsque K et k ont même caractéristique, K est isomorphe à $k((T))$ (cf. Chapitre II, § 4, où nous avons donné la démonstration lorsque k est parfait); si k' est une extension finie séparable de k, l'extension non ramifiée correspondante est $K' = k'((T)) = k' \otimes_k K$. Lorsque k est un corps parfait de caractéristique $p > 0$, on a de même $K' = W(k') \otimes_{W(k)} K$, où $W(k)$ désigne l'anneau des vecteurs de Witt à coefficients dans k.

2) Les résultats de ce paragraphe s'étendent aux anneaux locaux noethériens complets quelconques; le lecteur pourra se reporter au séminaire de Grothendieck ([29], § 1).

§ 6. *Calcul de la différente et du discriminant*

On conserve les notations et hypothèses des §§ 3 et 4.

PROPOSITION 11. *Soit $n = [L : K]$ et soit C un sous-anneau de B, contenant A, et admettant une A-base formée des puissances x^i, $0 \leqslant i \leqslant n - 1$, d'un élément x. Soit f le polynôme caractéristique de x. Alors* :

(i) *On a* $f \in A[X]$.

(ii) *Le* A*-module* C^* *est un module libre, admettant pour base les* $x^i/f'(x)$, $0 \leqslant i \leqslant n-1$, *où* $f'(X)$ *désigne la dérivée de* $f(X)$.

Les coefficients de f sont entiers sur A, et appartiennent à K; ils appartiennent donc à A, ce qui démontre (i). (Noter que l'anneau C est isomorphe à l'anneau $B_f = A[X]/(f)$, cf. Chap. I, § 6.)

Pour démontrer (ii) on va se servir du résultat suivant :

LEMME 2 (Euler). *On a* $\mathrm{Tr}\,(x^i/f'(x)) = 0$ *si* $0 \leqslant i \leqslant n-2$, *et* $\mathrm{Tr}\,(x^{n-1}/f'(x)) = 1$.

Soient x_k, $k = 1, \ldots, n$, les conjugués de x dans une extension convenable de L. Il faut calculer les sommes $\sum_k (x_k)^i/f'(x_k)$. Or on a l'identité :

$$(*) \qquad \frac{1}{f(T)} = \sum_{k=1}^{k=n} \frac{1}{f'(x_k)(T - x_k)}.$$

[Décomposer la fonction rationnelle $\frac{1}{f(T)}$ en somme d'« éléments simples » $a_k/(T - x_k)$, et déterminer les a_k par le procédé usuel.]

Si l'on développe $\frac{1}{f(T)}$ en série de puissances en $1/T$, le terme de plus bas degré est $1/T^n$, et en comparant avec le développement du membre de droite de (*) on obtient bien les formules cherchées.

Revenons maintenant à la proposition 11; il suffit de montrer que la matrice $r_{ij} = \mathrm{Tr}\,(x^i.x^j/f'(x))$ est inversible dans $GL(n, A)$. Or le lemme 2 montre que $r_{ij} = 0$ si $i + j \leqslant n-2$, et $r_{ij} = 1$ si $i + j = n - 1$; pour $i + j \geqslant n$, on a

$$r_{ij} = \mathrm{Tr}\,(x^n.x^{i+j-n}/f'(x)),$$

et comme x^n est combinaison linéaire à coefficients dans A des x^i, $0 \leqslant i < n$, ceci montre par récurrence que $r_{ij} \in A$. Le calcul du déterminant d'une matrice triangulaire donne alors $\det(r_{ij}) = (-1)^{n(n-1)/2}$, c.q.f.d.

Conservons les hypothèses de la proposition 11. L'ensemble r des éléments $t \in C$ tels que $tB \subset C$ est un idéal à la fois dans C et dans B, qu'on appelle le *conducteur* de B dans C.

COROLLAIRE 1. *Avec les hypothèses et notations précédentes, on a* :

$$\mathfrak{r} = f'(x).\mathfrak{D}_{B/A}^{-1}.$$

Posons, pour simplifier l'écriture, $b = f'(x)$. Si $t \in L$, on a les équivalences suivantes :

$$t \in \mathfrak{r} \iff tB \subset C \iff b^{-1}tB \subset C^* \iff \mathrm{Tr}\,(b^{-1}tB) \subset A \iff b^{-1}t \in \mathfrak{D}_{B/A}^{-1} \iff t \in b.\mathfrak{D}_{B/A}^{-1},$$

d'où le corollaire.

COROLLAIRE 2. *La différente $\mathfrak{D}_{B/A}$ divise l'idéal principal $(f'(x))$. Pour que ces deux idéaux soient égaux, il faut et il suffit que* B = C (c'est-à-dire que B = A[x]).

La première assertion résulte de la formule $(f'(x)) = r.\mathfrak{D}_{B/A}$. Cette même formule montre que $\mathfrak{D}_{B/A} = (f'(x))$ si et seulement si $r = 1$, c'est-à-dire si B = C, d'où la seconde assertion.

Le corollaire 2 permet de calculer la différente $\mathfrak{D}_{B/A}$ lorsque B est de la forme A[x]; on va donner une condition pour qu'il en soit ainsi :

PROPOSITION 12. *Supposons que* B (*donc aussi* A) *soit un anneau de valuation discrète ; si on note* $\overline{L}$ *et* $\overline{K}$ *les corps résiduels de ces deux anneaux, supposons en outre que l'extension* $\overline{L}/\overline{K}$ *soit séparable. Il existe alors une base de* B *formée des puissances* $\{1, x, \ldots, x^{n-1}\}$ *d'un élément* x.

(Cette proposition s'applique notamment lorsque A est un anneau de valuation discrète *complet* dont le corps résiduel est *parfait.*)

Soit e l'indice de ramification de L/K, et soit $f = [\overline{L} : \overline{K}]$. On a $n = ef$. Soit π une uniformisante de B, et soit x un élément de B dont la classe dans $\overline{L}$ est un élément primitif de l'extension $\overline{L}/\overline{K}$.

LEMME 3. *Les produits* $x^i\pi^j$, $0 \leqslant i < f$, $0 \leqslant j < e$, *forment une base du* A*-module* B.

Le nombre de ces produits est ef; pour voir qu'ils forment une base de B, il suffit donc de montrer qu'ils *engendrent* B, et même qu'ils engendrent B/$\mathfrak{p}$B, où $\mathfrak{p}$ est l'idéal maximal de A. Or on a $\mathfrak{p}B = \pi^e B$. Il suffit donc de montrer que si ces éléments engendrent B mod. π^m, avec $m < e$, ils engendrent B mod. π^{m+1}, ce qui est immédiat.

LEMME 4. *On peut choisir l'élément* x *de telle sorte qu'il existe un polynôme unitaire* R(X), *de degré* f, *à coefficients dans* A, *tel que* R(x) *soit une uniformisante de* B.

Faisons d'abord un choix quelconque de x, et soit $\bar{x}$ sa classe dans $\overline{L}$; par hypothèse, on a $\overline{L} = \overline{K}(\bar{x})$, et $\bar{x}$ vérifie une équation $\overline{R}(\bar{x}) = 0$, où $\overline{R}$ est un polynôme unitaire sur $\overline{K}$ de degré f; on peut relever $\overline{R}$ en un polynôme unitaire R sur l'anneau A. Puisque l'image de R(x) dans $\overline{L}$ est nulle, on a $w(R(x)) \geqslant 1$, où w désigne la valuation de B. S'il y a égalité l'élément x vérifie les conclusions du lemme; sinon, on a $w(R(x)) \geqslant 2$. Soit h un élément de valuation 1, et formons $R(x + h)$; la formule de Taylor donne :

$$R(x + h) = R(x) + h.R'(x) + h^2.b, \qquad \text{avec} \qquad b \in B.$$

Comme $\overline{L}/\overline{K}$ est séparable, on a $\overline{R}'(\bar{x}) \neq 0$, ce qui montre que $R'(x)$ est inversible, et que $h.R'(x)$ a pour valuation 1; comme les autres termes de $R(x + h)$ ont une valuation $\geqslant 2$, on voit que $w(R(x + h)) = 1$, et l'élément $x + h$ est l'élément cherché.

Nous pouvons maintenant achever la démonstration de la proposition 12. Si nous choisissons un élément x vérifiant les hypothèses du lemme 4, et si nous posons $\pi = R(x)$, le lemme 3 montre que les produits $x^i R(x)^j$, $0 \leqslant i < f$, $0 \leqslant j < e$, forment une base de B; donc B = A[x], et comme x vérifie une équation unitaire de degré n, ceci suffit à prouver que $\{1, x, \ldots, x^{n-1}\}$ forme une base.

Remarque. La proposition 12 ne s'étend pas au cas où l'on suppose seulement que A est un anneau de valuation discrète, cf. Exerc. 3.

PROPOSITION 13. *Soit $\mathfrak{P}$ un idéal premier non nul de* B, *soit* $\mathfrak{p} = \mathfrak{P} \cap A$, *soient* $L_{\mathfrak{P}}$ *et* $K_{\mathfrak{p}}$ *les corps résiduels correspondants. On suppose que l'extension résiduelle* $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ *est séparable. Alors l'exposant de* $\mathfrak{P}$ *dans la différente* $\mathfrak{D}_{B/A}$ *est supérieur ou égal à* $e_{\mathfrak{P}} - 1$ ($e_{\mathfrak{P}}$ désignant l'indice de ramification), *l'égalité ayant lieu si et seulement si et seulement si* $e_{\mathfrak{P}}$ *est premier à la caractéristique du corps résiduel* $K_{\mathfrak{p}}$.

En localisant et complétant, on se ramène au cas où A et B sont des anneaux de valuation discrète complets; en utilisant le corollaire 3 au théorème 3, on peut en outre supposer que L/K est totalement ramifiée. Si π est une uniformisante de L, on sait (cf. Chap. I, § 6) que π vérifie une équation d'Eisenstein $f(\pi) = 0$, avec

$$f = X^e + a_1 X^{e-1} + \cdots + a_e, \qquad a_i \in \mathfrak{p}, \qquad e = e_{\mathfrak{P}} = [L : K].$$

De plus, on a $B = A[\pi]$, ce qui permet d'appliquer le corollaire 2 à la proposition 11 : la différente $\mathfrak{D}_{B/A}$ est engendrée par $f'(\pi)$. Or, on a :

$$f'(\pi) = \sum_{i=0}^{i=e-1} (e - i) a_i \pi^{e-i-1}, \qquad \text{avec } a_0 = 1.$$

Soit w la valuation discrète associée à B. On a $w(\pi) = 1$ et
$w((e - i)\, a_i \pi^{e-i-1}) \equiv -i - 1 \pmod{e}$ si $(e - i) a_i \neq 0$.
Cela montre que les termes non nuls de $f'(\pi)$ ont des valuations *distinctes* (puisque distinctes modulo e). D'où :

$$(*)\quad w(f'(\pi)) = \operatorname*{Inf}_{0 \leqslant i < e} w((e - i)\, a_i \pi^{e-i-1}).$$

Le terme correspondant à $i = 0$ donne $e - 1 + w(e)$; ceux correspondant à $i \geqslant 1$ sont $\geqslant e$. On voit donc que $w(f'(\pi)) \geqslant e - 1$ et qu'il y a égalité si et seulement si $w(e) = 0$, *i.e.* si e est premier à la caractéristique résiduelle, cqfd.

Remarque. La formule (*), appliquée en prenant $i = 0$, donne :

$$w(f'(\pi)) \leqslant e - 1 + w(e).$$

On en déduit une *borne supérieure* pour l'exposant de $\mathfrak{P}$ dans la différente $\mathfrak{D}_{B/A}$. Cette borne est due à Hensel (*J. Crelle* 113 (1894)) lorsque $K = \mathbf{Q}$; elle avait été conjecturée par Dedekind. Quant à la valeur exacte de l'exposant en question, elle dépend des *groupes de ramification* de l'extension, cf. chap. IV, prop. 4.

Exercices. 1) Les hypothèses étant celles de la prop. 12, montrer que, si $B = A[x]$, et si y est assez voisin de x, on a $B = A[y]$.

2) Dans le cas général, soit $\mathfrak{P}$ un idéal premier de B, tel que l'extension résiduelle correspondante soit séparable. Montrer qu'il existe $x \in B$, engendrant l'extension L/K, et tel que le conducteur $\mathfrak{r}$ de B dans $A[x]$ soit premier à $\mathfrak{P}$ (appliquer la prop. 12 et l'exer. 1 ci-dessus aux complétés de B et de A).

3) Supposons que A soit un anneau de valuation discrète, et que B soit « complètement décomposé », c'est-à-dire qu'il existe $n = [L : K]$ idéaux premiers de B au-dessus de l'idéal premier $\mathfrak{p}$ de A. Montrer que, pour qu'il existe $x \in B$ tel que $B = A[x]$, il faut et il suffit que l'on ait $n \leqslant \mathrm{Card}(\overline{K})$, où $\overline{K}$ est le corps résiduel de A.

§ 7. *Une caractérisation différentielle de la différente*

Soit B une A-algèbre commutative quelconque. L'application $(x, y) \to xy$ définit un homomorphisme

$$\theta : B \otimes_A B \to B$$

Soit I son noyau, et posons $\Omega_A(B) = I/I^2 = I \otimes_{B \otimes_A B} B$; on obtient ainsi un B-module, qui s'appelle le module des A-*différentielles de l'anneau* B (cette définition est due à E. Kähler). Si l'on note dx l'image de $x \otimes 1 - 1 \otimes x$ dans I/I^2, tout élément de $\Omega_A(B)$ s'écrit sous la forme $\sum y_i\, dx_i$, et l'on a :

$$d(xy) = x\, dy + y\, dx$$
$$da = 0 \quad \text{si} \quad a \in A.$$

Le module $\Omega_A(B)$ est d'ailleurs *universel* pour les propriétés précédentes (cf. [12], exposé 13, ainsi que [46]).

Proposition 14. *Soit* A *un anneau de Dedekind, de corps des fractions* K; *soit* L *une extension séparable finie de* K, *et soit* B *la fermeture intégrale de* A *dans* L. *On suppose que, pour tout idéal premier* $\mathfrak{P}$ *de* B, *l'extension résiduelle correspondante est séparable. Le* B-*module* $\Omega_A(B)$ *est alors un* B-*module monogène, dont l'annulateur est la différente* $\mathfrak{D}_{B/A}$.

On démontre facilement que, si A' est une A-algèbre commutative quelconque, et si $B' = B \otimes_A A'$, on a $\Omega_{A'}(B') = \Omega_A(B) \otimes_A A'$. Il en résulte que le module des différentielles « se conserve » par localisation et complétion, ce qui nous ramène au cas où A est un anneau de valuation discrète complet. D'après la proposition 12, on a alors $B = A[X]/(f)$, où f est un polynôme unitaire. Si x désigne l'image de X dans B, on en déduit ([12], *loc. cit.*) que $\Omega_A(B)$ est engendré par dx, et que l'annulateur de dx est $f'(x)$. D'autre part, d'après le corollaire 2 à la proposition 11, $\mathfrak{D}_{B/A}$ est l'idéal principal engendré par $f'(x)$, d'où la proposition.

Remarque. Il serait intéressant d'obtenir une démonstration plus directe de la proposition précédente, et également d'étudier les « parties principales d'ordre m » $P_m(B/A) = (B \otimes_A B)/I^{m+1}$.

Exercices. 1) Les hypothèses étant celles de la proposition 14, montrer qu'il existe un élément $x \in B$ tel que dx engendre $\Omega_A(B)$.

2) Traduire la proposition 14 et l'exercice 1 en termes de dérivations.

3) Donner un exemple d'extension séparable L/K admettant une extension résiduelle $\overline{L}/\overline{K}$ qui est radicielle de hauteur 1 et non monogène. Montrer que, pour une telle extension, $\Omega_A(B)$ n'est pas monogène.

CHAPITRE IV

GROUPES DE RAMIFICATION

Notations

Dans ce chapitre, K désigne un corps muni d'une *valuation discrète* v_K pour laquelle il est *complet*. On note A_K l'anneau de valuation correspondant, $\mathfrak{p}_K$ son idéal maximal, $\mathbf{K} = A_K/\mathfrak{p}_K$ son corps résiduel et $U_K = A_K - \mathfrak{p}_K$ le groupe multiplicatif des éléments inversibles de A_K.

Si L est une extension séparable finie de K, on note A_L la fermeture intégrale de A_K dans L; c'est un anneau de valuation discrète complet (Chap. II, § 2); on définit comme ci-dessus v_L, $\mathfrak{p}_L$, U_L, $\mathbf{L}$. *Nous supposerons toujours que l'extension résiduelle* $\mathbf{L}/\mathbf{K}$ *est séparable.* L'indice de ramification de $\mathfrak{p}_L$ dans L/K sera noté $e_{L/K}$, et son degré résiduel sera noté $f_{L/K}$; on a $e_{L/K} \cdot f_{L/K} = [L : K]$, cf. Chap. I, § 4.

§ 1. *Définition des groupes de ramification, et premières propriétés*

Soit L/K une extension *galoisienne* (vérifiant les hypothèses ci-dessus) et soit $G = G(L/K)$ son groupe de Galois. Le groupe G opère sur l'anneau A_L; on sait (Chap. III, § 6, prop. 12) qu'il existe un élément $x \in A_L$ qui engendre A_L considéré comme A_K-algèbre.

LEMME 1. *Soit* $s \in G$, *et soit* i *un entier* $\geqslant -1$. *Les trois conditions suivantes sont équivalentes* :

a) s *opère trivialement sur l'anneau quotient* $A_L/\mathfrak{p}_L^{i+1}$.

b) $v_L(s(a) - a) \geqslant i + 1$ *pour tout* $a \in A_L$.

c) $v_L(s(x) - x) \geqslant i + 1$.

L'équivalence de (*a*) et (*b*) est triviale; d'autre part, l'image x_i de x dans $A_L/\mathfrak{p}_L^{i+1} = A_i$ engendre A_i, considéré comme A_K-algèbre. Donc, pour que s opère trivialement sur A_i, il faut et il suffit que $s(x_i) = x_i$, ce qui montre l'équivalence de (*a*) et de (*c*).

PROPOSITION 1. *Pour tout entier* $i \geqslant -1$, *soit* G_i *l'ensemble des* $s \in G$ *qui vérifient les conditions* (*a*), (*b*), (*c*) *du lemme* 1. *Les* G_i *forment une suite décroissante de sous-groupes invariants de* G. *On a* $G_i = \{1\}$ *pour* i *assez grand,* G_0 *est le sous-groupe d'inertie de* G (*cf.* Chap. I, § 7), *et* $G_{-1} = G$.

La condition (*a*) montre que les G_i sont des sous-groupes invariants de G, qui décroissent évidemment avec i. La condition (*c*) montre que, si

$$i \geqslant \sup\,(v_L(s(x) - x)),$$

pour $s \neq 1$, on a $G_i = \{1\}$. Les autres assertions sont évidentes.

Le groupe G_i s'appelle le *i-ième groupe de ramification de* G (ou de L/K). Les groupes de ramification définissent une *filtration* du groupe G (au sens de Bourbaki, *Alg. comm.*, Chap. III, § 2); le quotient G/G_0 n'est autre que le groupe de Galois $G(\bar{L}/K)$ de l'extension résiduelle $\bar{L}/\bar{K}$ (cf. Chap. I, § 7); les quotients G_i/G_{i+1}, $i \geqslant 0$, seront étudiés au paragraphe suivant.

L'élément x désignant toujours un générateur de la A_K-algèbre A_L, nous définirons une *fonction i_G sur* G par la formule :

$$i_G(s) = v_L(s(x) - x).$$

Si $s \neq 1$, $i_G(s)$ est un entier $\geqslant 0$; on a $i_G(1) = +\infty$. La fonction i_G jouit des propriétés suivantes :

$$i_G(s) \geqslant i + 1 \iff s \in G_i$$
$$i_G(tst^{-1}) = i_G(s)$$
$$i_G(st) \geqslant \mathrm{Inf}\,(i_G(s),\ i_G(t)).$$

La première propriété ne fait qu'exprimer la définition de G_i; elle montre que i_G ne dépend pas du choix du générateur x, et que *la connaissance de i_G est équivalente à celle des* G_i (dans la terminologie de Bourbaki, *loc. cit.*, i_G est égale à la *fonction d'ordre* de la filtration (G_i), augmentée d'une unité). Les deux autres propriétés résultent de la première, et du fait que les G_i sont des sous-groupes invariants de G.

Soit maintenant H un *sous-groupe* de G, et soit K′ la sous-extension de L correspondant à H. On a $G(L/K') = H$, et nous allons voir que les groupes de ramification de G déterminent ceux de H :

PROPOSITION 2. *On a* $H_i = G_i \cap H$, *et* $i_H(s) = i_G(s)$ *pour tout* $s \in H$.

C'est évident par exemple en utilisant la condition (*a*) du lemme 1.

COROLLAIRE. *Soit* K_r *la plus grande extension non ramifiée de* K *contenue dans* L, *et soit* H *le sous-groupe de* G *correspondant. Le groupe* H *est égal au groupe d'inertie* G_0, *et les groupes de ramification de* G *d'indice* $\geqslant 0$ *sont égaux à ceux de* H.

Le fait que $H = G_0$ a été démontré au Chap. I, § 7. Comme $G_i \subset G_0$ pour $i \geqslant 0$, la proposition 2 montre bien que $G_i = H_i$.

Remarque. L'extension L/K_r est *totalement ramifiée*; le corollaire précédent ramène donc l'étude des groupes de ramification « supérieurs » (d'indice $i \geqslant 0$) à celle du cas totalement ramifié; c'est la méthode que nous suivrons au § 2.

Supposons en outre que H soit un *sous-groupe invariant* de G, de sorte que G/H s'identifie au groupe de Galois de K'/K. Nous allons voir que les groupes de ramification de G déterminent ceux de G/H; le résultat s'énonce de façon simple en termes de la fonction i :

PROPOSITION 3. *On a* $i_{G/H}(\sigma) = \frac{1}{e'} \sum_{s \to \sigma} i_G(s)$ *pour tout* $\sigma \in G/H$, *avec* $e' = e_{L/K'}$.

Démonstration (d'après J. Tate). Pour $\sigma = 1$, les deux membres sont égaux à $+\infty$, et la formule est vraie. Supposons donc $\sigma \neq 1$. Soit x (resp. y) un générateur de la A_K-algèbre A_L (resp. $A_{K'}$). Par définition, $e' . i_{G/H}(\sigma) = v_L(\sigma(y) - y)$, et $i_G(s) = v_L(s(x) - x)$. Si l'on choisit un $s \in G$ ayant pour image σ, les autres éléments de G ayant pour image σ sont de la forme st, $t \in H$. Tout revient donc à montrer que *les éléments*

$$a = s(y) - y \qquad et \qquad b = \prod_{t \in H} (st(x) - x)$$

engendrent le même idéal dans A_L.

Soit $f \in A_{K'}[X]$ l'équation minimale de x par rapport au corps intermédiaire K'. On a $f(X) = \prod_{t \in H} (X - t(x))$. Désignons par $s(f)$ le polynôme déduit de f en transformant chacun de ses coefficients par s. On a évidemment :

$$s(f)(X) = \prod_{t \in H} (X - st(x)).$$

Comme $s(f) - f$ a tous ses coefficients divisibles par $s(y) - y$, on en conclut que $s(y) - y = a$ divise $s(f)(x) - f(x) = s(f)(x) = \pm b$.

Reste à montrer que b divise a. Pour cela, écrivons y comme polynôme en x, à coefficients dans A_K : $y = g(x)$. Le polynôme $g(X) - y$ a pour racine x, et a tous ses coefficients dans $A_{K'}$; il est donc divisible par le polynôme f introduit ci-dessus, et l'on a :

$$g(X) - y = f(X) . h(X), \qquad \text{avec} \qquad h \in A_{K'}[X].$$

En transformant cette équation par s, et en faisant $X = x$ dans le résultat, on obtient :

$$y - s(y) = s(f)(x) . s(h)(x),$$

ce qui montre bien que b divise a, et achève la démonstration.

COROLLAIRE. *Si* $H = G_j$ *pour un entier* $j \geqslant 0$, *on a* $(G/H)_i = G_i/H$ *pour* $i \leqslant j$, *et* $(G/H)_i = \{1\}$ *pour* $i \geqslant j$.

Les G_i/H, $i \leqslant j$, forment une filtration décroissante de G/H. Si $\sigma \in G/H$, $\sigma \neq 1$, il existe donc un $i < j$ et un seul tel que $\sigma \in G_i/H$, $\sigma \notin G_{i+1}/H$. Si $s \in G$ a pour

image σ, il est clair que l'on a $s \in G_i$, $s \notin G_{i+1}$, d'où $i_G(s) = i + 1$. De plus, puisque $H \subset G_0$, l'extension L/K' est totalement ramifiée, et $e_{L/K'}$ est égal à l'ordre de H. La proposition 3 montre alors que $i_{G/H}(\sigma) = i + 1$, ce qui prouve que la filtration des G_i/H coïncide avec celle des $(G/H)_i$ pour $i \leqslant j$. Comme d'autre part $(G/H)_j = G_j/H = |1|$, on a bien $(G/H)_i = |1|$ pour $i \geqslant j$.

Remarque. Dans le cas général, la proposition 3 permet encore de démontrer que les groupes de ramification de G/H sont les images de ceux de G, *mais il faut en modifier la numérotation.* Nous reviendrons là-dessus au § 3.

Nous allons maintenant utiliser les groupes de ramification pour déterminer la *différente* d'une sous-extension de L/K :

PROPOSITION 4. *Si $\mathfrak{D}_{L/K}$ désigne la différente de l'extension* L/K, *on a* :

$$v_L(\mathfrak{D}_{L/K}) = \sum_{s \neq 1} i_G(s) = \sum_{i=0}^{i=\infty} (\text{Card } (G_i) - 1).$$

[Ici, et dans toute la suite, on note Card (S) le nombre d'éléments d'un ensemble fini S. On notera que Card $(G_i) - 1 = 0$ pour i assez grand, ce qui donne un sens à la somme infinie.]

Désignons encore par x un générateur de A_L sur A_K, et soit f le polynôme minimal de x sur K. D'après le corollaire 2 à la proposition 11 du Chapitre III, $\mathfrak{D}_{L/K}$ est engendré par $f'(x)$. Mais on a $f(X) = \prod_{s \in G} (X - s(x))$, d'où :

$$f'(x) = \prod_{s \neq 1} (x - s(x)),$$

et

$$v_L(\mathfrak{D}_{L/K}) = v_L(f'(x)) = \sum_{s \neq 1} i_G(s),$$

ce qui démontre la première formule.

Pour démontrer la seconde, posons $r_i = \text{Card } (G_i) - 1$, et remarquons que la fonction i_G est égale à i sur $G_{i-1} - G_i$. On a donc :

$$\sum_{\neq 1} i_G(s) = \sum_{i=0}^{i=\infty} i(r_{i-1} - r_i) = (r_0 - r_1) + 2(r_1 - r_2) + 3(r_2 - r_3) + \cdots$$
$$= r_0 + r_1 + r_2 + \cdots, \qquad \text{c.q.f.d.}$$

COROLLAIRE. *Si* K' *est une sous-extension de* L, *correspondant au sous-groupe* H *de* G, *on a* :

$$v_{K'}(\mathfrak{D}_{K'/K}) = \frac{1}{e'} \sum_{s \notin H} i_G(s), \qquad \textit{avec} \quad e' = e_{L/K'}.$$

En effet, d'après la proposition 4, on a :

$$v_L(\mathfrak{D}_{L/K}) = \sum_{s \neq 1} i_G(s), \qquad v_L(\mathfrak{D}_{L/K'}) = \sum_{\substack{s \neq 1 \\ s \in H}} i_G(s),$$

et on conclut en appliquant la transitivité de la différente (Chap. III, § 4, prop. 8).

Remarques. 1) Lorsqu'on ne suppose plus l'extension résiduelle L/K séparable, on est conduit à *dédoubler* la suite G_n des groupes de ramification (cf. Samuel-Zariski [53], I, Chap. V, § 10). J'ignore s'il est possible d'étendre à ce cas les propositions 3 et 4.

2) La « globalisation » des définitions et des résultats de ce Chapitre ne présente aucune difficulté. De façon précise, soit A un anneau de Dedekind de corps des fractions E, soit B sa fermeture intégrale dans une extension galoisienne F de E, de groupe de Galois G, et soit $\mathfrak{P}$ un idéal premier de B; soit $\mathfrak{p} = \mathfrak{P} \cap A$. On sait (Chap. II, § 3) que le *groupe de décomposition* $D_{\mathfrak{P}}$ de $\mathfrak{P}$ est le groupe de Galois de l'extension des corps complétés $\hat{L}_{\mathfrak{P}}/\hat{K}_{\mathfrak{p}}$; si l'extension résiduelle correspondante est séparable, on peut appliquer les définitions ci-dessus à cette extension, et définir les *groupes de ramification* $G_i(\mathfrak{P})$ *de* G *relativement à* $\mathfrak{P}$; ce sont des sous-groupes invariants du groupe de décomposition $D_{\mathfrak{P}}$. Il est facile de voir que :

$$s \in G_i(\mathfrak{P}) \iff s(x) \equiv x \mod \mathfrak{P}^{i+1} \qquad \textit{pour tout} \quad x \in B.$$

La proposition 2 montre que, si $H \subset G$, on a $H_i(\mathfrak{P}) = H \cap G_i(\mathfrak{P})$. On peut traduire de même les propositions 3 et 4 et, plus généralement, tous les résultats de ce chapitre; nous nous en dispenserons.

Exercice. Soit L/K une extension galoisienne totalement ramifiée, et soit L_0/K_0 une extension déduite de la précédente par le procédé de l'exer. 4 du Chap. II, § 2. Montrer que les groupes de ramification de L/K coïncident avec ceux de $\hat{L}_0/\hat{K}_0$.

[On ramène ainsi l'étude des groupes de ramification au cas où le corps résiduel est algébriquement clos.]

§ 2. *Les quotients* G_i/G_{i+1}, $i \geqslant 0$

On conserve les notations et les hypothèses du paragraphe 1, et l'on désigne par K_r la plus grande extension non ramifiée de K contenue dans L (cf. corollaire à la proposition 2).

On note π une uniformisante de L.

PROPOSITION 5. *Soit i un entier* $\geqslant 0$. *Pour qu'un élément s du groupe d'inertie* G_0 *appartienne à* G_i, *il faut et il suffit que l'on ait*:

$$s(\pi)/\pi \equiv 1 \mod \mathfrak{p}_L^i.$$

En remplaçant G par G_0 et K par K_r, on se ramène au cas d'une extension

totalement ramifiée. D'après la proposition 18 du Chapitre I, § 6, l'élément π est alors un générateur de la A_K-algèbre A_L. On a donc :

$$\begin{aligned} i_G(s) &= v_L(s(\pi) - \pi) \\ &= 1 + v_L(s(\pi)/\pi - 1), \qquad \text{puisque} \quad v_L(\pi) = 1, \end{aligned}$$

d'où la proposition.

Définissons maintenant une *filtration* sur le groupe U_L des éléments inversibles de A_L, en posant :

$$\begin{aligned} U_L^{(0)} &= U_L \\ U_L^{(i)} &= 1 + \mathfrak{p}_L^i \qquad \text{pour} \quad i \geqslant 1. \end{aligned}$$

On vérifie tout de suite que l'on obtient ainsi une suite décroissante de sous-groupes fermés de U_L; ces sous-groupes forment une base de voisinages de 1 dans la topologie induite sur U_L par L^*; comme U_L est fermé, donc complet, on a :

$$U_L = \varprojlim U_L/U_L^{(i)}$$

[Dans toute la suite, nous écrirons U_L^i au lieu de $U_L^{(i)}$, sauf lorsqu'il y aura risque de confusion avec l'ensemble des puissances i-ièmes des éléments de U_L.]

PROPOSITION 6. (*a*) *On a* $U_L^0/U_L^1 = \bar{L}^*$ (*groupe multiplicatif du corps résiduel* $\bar{L}$). (*b*) *Pour* $i \geqslant 1$, *le groupe* U_L^i/U_L^{i+1} *est canoniquement isomorphe au groupe* $\mathfrak{p}_L^i/\mathfrak{p}_L^{i+1}$, *lui-même isomorphe* (*non canoniquement*) *au groupe additif du corps résiduel* $\bar{L}$.

L'assertion (*a*) est triviale. Pour démontrer (*b*), on fait correspondre à tout $x \in \mathfrak{p}_L^i$ l'élément $1 + x$ de U_L^i, et l'on vérifie immédiatement que l'on obtient ainsi, par passage au quotient, un isomorphisme de $\mathfrak{p}_L^i/\mathfrak{p}_L^{i+1}$ sur U_L^i/U_L^{i+1}. Comme de plus $\mathfrak{p}_L^i/\mathfrak{p}_L^{i+1}$ est un espace vectoriel de dimension 1 sur $\bar{L}$, cela démontre (*b*).

Remarque. La somme directe des $\mathfrak{p}_L^i/\mathfrak{p}_L^{i+1}$ est munie de façon naturelle d'une structure de $\bar{L}$-algèbre graduée (c'est l'algèbre graduée associée à la filtration $\mathfrak{p}_L$-adique de A_L, cf. Bourbaki, *Alg. comm.*, Chap. III, § 2). En particulier, si l'on pose $\Omega_L = \mathfrak{p}_L/\mathfrak{p}_L^2$, on a une application canonique de la puissance tensorielle i-ième Ω_L^i de Ω_L dans $\mathfrak{p}_L^i/\mathfrak{p}_L^{i+1}$; on vérifie tout de suite que cette application est un isomorphisme. On peut donc identifier *canoniquement* U_L^i/U_L^{i+1} *à* Ω_L^i.

Revenons maintenant aux groupes de ramification. La proposition 5 peut se traduire par l'équivalence :

$$s \in G_i \iff s(\pi)/\pi \in U_L^i.$$

De façon plus précise :

PROPOSITION 7. *L'application qui, à* $s \in G_i$, *fait correspondre* $s(\pi)/\pi$, *définit par passage au quotient un isomorphisme* θ_i *du groupe quotient* G_i/G_{i+1} *sur un sous-groupe du groupe* U_L^i/U_L^{i+1}. *Cet isomorphisme ne dépend pas du choix de l'uniformisante* π.

Si π' est une autre uniformisante, on a $\pi' = \pi u$, avec $u \in U_L$, d'où

$$s(\pi')/\pi' = s(\pi)/\pi \,.\, s(u)/u.$$

Si $s \in G_i$, on a $s(u) \equiv u \bmod \mathfrak{p}_L^{i+1}$ d'où $s(u)/u \equiv 1 \bmod U_L^{i+1}$, ce qui montre bien que θ_i ne dépend pas du choix de π. Si s, $t \in G_i$, on peut écrire :

$$st(\pi)/\pi = s(\pi)/\pi \cdot t(\pi)/\pi \cdot s(u)/u, \qquad \text{avec} \qquad u = t(\pi)/\pi.$$

Puisque u est dans U_L, on a $s(u)/u \equiv 1 \bmod U_L^{i+1}$ comme ci-dessus, et on en tire :

$$st(\pi)/\pi \equiv s(\pi)/\pi \cdot t(\pi)/\pi \mod U_L^{i+1},$$

ce qui montre que θ_i est un homomorphisme. Le fait qu'il soit injectif est trivial.

[Explicitons la définition de θ_i :

Si $s \in G_0$, on a $s\pi = u\pi$, avec $u \in U_L$, et $\theta_0(s) = \bar{u} \in \bar{L}^*$. Si $s \in G_i$, $i \geqslant 1$, on a $s\pi = \pi(1 + a)$, avec $a \in \mathfrak{p}_L$, et $\theta_i(s)$ est égal à la classe de a dans $\mathfrak{p}_L/\mathfrak{p}_L^{i+1}$.]

Remarque. On verra au Chapitre suivant que, *pour certaines valeurs de i*, on peut caractériser l'image de θ_i dans U_L^i/U_L^{i+1} comme le noyau d'une application déduite de la norme $N_{L/K}$, par passage au quotient.

COROLLAIRE 1. *Le groupe G_0/G_1 est un groupe cyclique, appliqué isomorphiquement par θ_0 sur un sous-groupe du groupe des racines de l'unité contenues dans $\bar{L}$. Son ordre est premier à la caractéristique du corps résiduel $\bar{L}$.*

En effet, $U_L/U_L^1 = \bar{L}^*$, ce qui montre que $\theta_0(G_0/G_1)$ est un sous-groupe fini du groupe des racines de l'unité de $\bar{L}$; le fait qu'il soit cyclique et d'ordre premier à la caractéristique de $\bar{L}$ en résulte (cf. Bourbaki, *Alg.*, Chap. V, § 11, n° 1).

COROLLAIRE 2. *Si la caractéristique de $\bar{L}$ est nulle, on a $G_1 = \{1\}$, et le groupe G_0 est cyclique.*

En effet, si $i \geqslant 1$, U_L^i/U_L^{i+1} est isomorphe à $\bar{L}$, qui n'admet aucun sous-groupe fini non réduit à 0. On a donc $G_i = G_{i+1}$, et comme $G_i = \{1\}$ pour i grand, on a bien $G_1 = \{1\}$, et $G_0 = G_0/G_1$ est cyclique d'après le corollaire 1.

COROLLAIRE 3. *Si la caractéristique de $\bar{L}$ est $p \neq 0$, les quotients G_i/G_{i+1}, $i \geqslant 1$, sont des groupes abéliens, produits directs de groupes cycliques d'ordre p. Le groupe G_1 est un p-groupe.*

(Rappelons qu'on appelle *p-groupe* tout groupe fini dont l'ordre est une puissance de p.)

En effet, pour $i \geqslant 1$, U_L^i/U_L^{i+1} est isomorphe au groupe additif de $\bar{L}$, et tout sous-groupe de $\bar{L}$ est un espace vectoriel sur le corps à p éléments $\mathbf{F}_p$, donc est somme directe de groupes cycliques d'ordre p. Comme l'ordre de G_1 est égal au produit des ordres des G_i/G_{i+1}, pour $i \geqslant 1$, on voit bien que G_1 est un p-groupe.

COROLLAIRE 4. *Si la caractéristique de $\bar{L}$ est $p \neq 0$, le groupe d'inertie G_0 possède la propriété suivante:*

(R_p)-C'est le produit semi-direct d'un sous-groupe cyclique d'ordre premier à p par un sous-groupe invariant d'ordre une puissance de p.

D'après les corollaires 1 et 3, G_1 est un p-groupe, et G_0/G_1 est cyclique d'ordre premier à p; tout revient donc à montrer qu'il existe un sous-groupe H de G_0 qui se projette isomorphiquement sur G_0/G_1. C'est là une propriété générale des extensions de groupes finis dont les ordres sont premiers entre eux (cf. par exemple M. Hall [3], th. 15. 2. 2). En voici une démonstration directe :

Soit s un élément de G_0 dont l'image dans G_0/G_1 engendre G_0/G_1. Soit e_0 l'ordre de G_0/G_1, et soit p^n celui de G_1. Comme p est premier à e_0, il existe un entier $N \neq 0$ tel que $p^N \equiv 1 \bmod. e_0$; quitte à remplacer N par un de ses multiples, on peut en outre supposer que $N \geqslant n$. Posons alors :

$$t = s^{p^N}.$$

On a $t^{e_0} = s^{e_0 p^N} = 1$, puisque $e_0 p^N$ est multiple de l'ordre de G_0. D'autre part, comme $p^N \equiv 1 \bmod. e_0$, l'image de t dans G_0/G_1 est égale à celle de s. Il s'ensuit que le sous-groupe H de G_0 engendré par t est cyclique d'ordre e_0 et se projette isomorphiquement sur G_0/G_1, c.q.f.d.

Remarque. Inversement, on peut montrer que *tout groupe vérifiant* (R_p) *est groupe d'inertie* pour une extension du type considéré ici. Il serait intéressant d'aller plus loin, et de donner une caractérisation du groupe G_0, *muni de la filtration des* G_i, mais cela paraît beaucoup plus difficile.

COROLLAIRE 5. *Le groupe* G_0 *est résoluble. Si* $\mathbf{K}$ *est un corps fini, il en est de même de* G.

La première assertion est triviale. La seconde résulte de la première, et du fait que $G/G_0 = G(\mathbf{L}/\mathbf{K})$ est cyclique si $\mathbf{K}$ est fini.

Indiquons une application simple du corollaire 2 :

PROPOSITION 8. *Soit* k *un corps algébriquement clos de caractéristique zéro, et soit* $K = k((T))$. *La clôture algébrique* K_a *du corps* K *est réunion des corps* $K_n = k((T^{1/n}))$, *pour n entier* $\geqslant 1$.

Soit $L \subset K_a$ une extension galoisienne finie de K, de groupe de Galois G. Puisque $\mathbf{K} = k$ est algébriquement clos, on a $G = G_0$; le corollaire 2 montre donc que G est cyclique. Soit L' une autre extension galoisienne finie de K, contenue dans K_a, et dont le degré est un multiple de celui de L. Comme l'extension composée L'L est cyclique, le groupe G(L'L/L') est contenu dans le groupe G(L'L/L), ce qui montre que L est contenue dans L'. Appliquant ce résultat avec $L' = K_n$, pour n convenable, on voit que L est contenu dans la réunion des K_n, d'où la proposition.

COROLLAIRE. *Le groupe de Galois* $G(K_a/K)$ *est isomorphe à* $\hat{\mathbf{Z}}$.

C'est immédiat.

Remarque. La proposition 8 peut être considérée comme l'analogue formel du « théorème de Puiseux ».

Nous allons maintenant donner quelques propriétés des *commutateurs* vis-à-vis de la filtration (G_i), cf. Speiser [61].

Tout d'abord, puisque G_i et G_{i+1} sont invariants dans G_0, le groupe G_0 opère sur G_i/G_{i+1} par automorphismes intérieurs. Nous allons déterminer ces opérations :

PROPOSITION 9. *Soit* $s \in G_0$, *et soit* $\tau \in G_i/G_{i+1}$, $i \geqslant 1$. *On a*

$$\theta_i(s\tau s^{-1}) = \theta_0(s)^i \theta_i(\tau).$$

[Cette formule a un sens, car $\theta_i(\tau)$ appartient à $\mathfrak{p}_L^i/\mathfrak{p}_L^{i+1}$ qui est un espace vectoriel de dimension 1 sur $\bar{L}$, et $\theta_0(s)$ est un élément du groupe multiplicatif de $\bar{L}$.]

Soit $t \in G_i$ un représentant de τ. On écrira dans ce qui suit $\theta_i(t)$ au lieu de $\theta_i(\tau)$. Soit $\pi' = s^{-1}(\pi)$. On a $t(\pi') = \pi'(1 + a)$, avec $a \in \mathfrak{p}_L^i$, et $\theta_i(t)$ est la classe $\bar{a}$ de a mod. $\mathfrak{p}_L^{i+1}$. Appliquant s à cette équation, on trouve :

$$sts^{-1}(\pi) = st(\pi') = \pi(1 + s(a)),$$

ce qui montre que $\theta_i(sts^{-1})$ est la classe de $s(a)$ mod. $\mathfrak{p}_L^{i+1}$. Mais on peut écrire $a = b\pi^i$, d'où, si $s(\pi) = u\pi$, $s(a) = s(b)u^i\pi^i$, et comme $s(b) \equiv b$ mod. $\mathfrak{p}_L$, et $\bar{u} = \theta_0(s)$, on voit bien que la classe de $s(a)$ est égale au produit de $\theta_0(s)^i$ par la classe de a, c.q.f.d.

COROLLAIRE 1. *Si* $s \in G_0$ *et* $t \in G_i$, $i \geqslant 1$, *on a* $sts^{-1}t^{-1} \in G_{i+1}$ *si et seulement si* $s^i \in G_1$ *ou* $t \in G_{i+1}$.

En effet, $sts^{-1}t^{-1} \in G_{i+1}$ équivaut à $sts^{-1} \equiv t$ mod. G_{i+1}, lequel équivaut à

$$\theta_i(sts^{-1}) = \theta_i(t),$$

d'où le résultat, d'après la proposition.

COROLLAIRE 2. *Supposons* G *abélien, et soit* e_0 *l'ordre de* G_0/G_1. *Si* i *est un entier non divisible par* e_0, *on a* $G_i = G_{i+1}$.

En effet, si $t \in G_i$, et si s est un élément de G_0 qui engendre G_0/G_1, on applique le corollaire 1. Comme s_i n'appartient pas à G_1, on a $t \in G_{i+1}$.

Passons maintenant au commutateur $sts^{-1}t^{-1}$, avec $s \in G_i$, $t \in G_j$ et $i, j \geqslant 1$:

PROPOSITION 10. *Si* $s \in G_i$, $t \in G_j$, *et* $i, j \geqslant 1$, *on a* $sts^{-1}t^{-1} \in G_{i+j+1}$.

Nous démontrerons en même temps le résultat suivant :

PROPOSITION 11. *Les entiers* $i \geqslant 1$ *tels que* $G_i \neq G_{i+1}$ *sont congrus entre eux* mod. p.

(On note p la caractéristique du corps résiduel $\bar{L}$.)

Commençons par établir un résultat plus faible :

LEMME 2. *Sous les hypothèses de la proposition* 10, *on a* $sts^{-1}t^{-1} \in G_{i+j}$ *et*

$$\theta_{i+j}(sts^{-1}t^{-1}) = (j - i)\,\theta_i(s)\,\theta_j(t).$$

[Cette formule a un sens, car on a remarqué plus haut que la somme directe des $\mathfrak{p}_L^i/\mathfrak{p}_L^{i+1}$ admet une structure naturelle de $\bar{L}$-algèbre graduée.]

Posons $s(\pi) = \pi(1 + a)$, $t(\pi) = \pi(1 + b)$, $a \in \mathfrak{p}_L^i$, $b \in \mathfrak{p}_L^j$. On en tire :

$$st(\pi) = \pi(1 + a)\,(1 + s(b)) = \pi(1 + c),$$

avec $c = a + s(b) + a.s(b)$.

De même : $ts(\pi) = \pi(1 + d)$, avec $d = b + t(a) + b.t(a)$.
Posons $a = \alpha\pi^i$, $b = \beta\pi^j$, $\alpha, \beta \in A_L$. On a :

$$s(b) = s(\beta)\, s(\pi)^j = s(\beta)\, \pi^j (1 + a)^j.$$

Puisque $s \in G_i$, on a $s(\beta) \equiv \beta \bmod \mathfrak{p}_L^{i+1}$, et puisque $a \in \mathfrak{p}_L^i$, on a

$$(1 + a)^j \equiv 1 + ja \bmod \mathfrak{p}_L^{i+1} \quad \text{(et même mod. } \mathfrak{p}_L^{2i}).$$

On en tire :

$$\begin{aligned} s(b) &\equiv \beta\pi^j(1 + ja) \bmod \mathfrak{p}_L^{i+j+1} \\ &\equiv b + j.ab \quad \bmod \mathfrak{p}_L^{i+j+1} \end{aligned}$$

d'où :

$$c \equiv a + b + (j + 1)ab \bmod \mathfrak{p}_L^{i+j+1},$$

et de même :

$$d \equiv a + b + (i + 1)ab \bmod \mathfrak{p}_L^{i+j+1}.$$

Posons $\pi' = ts(\pi)$. On a :

$$\begin{aligned} sts^{-1}t^{-1}(\pi') &= st(\pi) = \pi(1 + c) = \pi'(1 + c)(1 + d)^{-1} \\ &= \pi'(1 + e), \end{aligned}$$

avec $e = (c - d)/(1 + d) \equiv (j - i)ab \bmod \mathfrak{p}_L^{i+j+1}$.

On en conclut tout d'abord que $sts^{-1}t^{-1}$ appartient à G_{i+j}; de plus, comme la classe de a (resp. b, resp. e) est égale à $\theta_i(s)$ (resp. $\theta_j(t)$, resp. $\theta_{i+j}(sts^{-1}t^{-1})$), on voit bien que l'on a

$$\theta_{i+j}(sts^{-1}t^{-1}) = (j - i)\theta_i(s)\theta_j(t), \qquad \text{c.q.f.d.}$$

Démontrons maintenant la proposition 11. Si $G_1 = \{1\}$, il n'y a rien à démontrer. Sinon, soit j le plus grand entier tel que $G_j \neq \{1\}$; on a $G_{j+1} = \{1\}$. Soit i un entier $\geqslant 1$ tel que $G_i \neq G_{i+1}$; il nous faut montrer que $j \equiv i \bmod p$. Soit s (resp. t) un élément de G_i (resp. G_j) n'appartenant pas à G_{i+1} (resp. G_{j+1}). D'après le lemme 2, le commutateur $sts^{-1}t^{-1}$ appartient à G_{i+j}; il est donc égal à 1, et $\theta_{i+j}(sts^{-1}t^{-1}) = 0$. Comme $\theta_i(s)$ et $\theta_j(t)$ sont non nuls, le lemme 2 montre que $j - i \equiv 0 \bmod p$, c.q.f.d.

Passons à la proposition 10. Si $s \in G_{i+1}$, ou $t \in G_{j+1}$, le lemme 2 montre que $sts^{-1}t^{-1} \in G_{i+j+1}$. Sinon, d'après la proposition 11, on a $j \equiv i \bmod p$, et le lemme 2 montre que $\theta_{i+j}(sts^{-1}t^{-1}) = 0$, ce qui signifie bien que $sts^{-1}t^{-1}$ appartient à G_{i+j+1}, et achève la démonstration.

Remarques. 1) Lorsque G est *abélien*, on peut démontrer des congruences plus précises que celles données par la proposition 11. Nous reviendrons là-dessus au § 3 ainsi qu'au Chap. VI.

2) Le fait que $s \in G_i$, $t \in G_j$ entraîne $sts^{-1}t^{-1} \in G_{i+j}$ est un cas particulier de résultats de Lazard ([44], Chap. I, n° 3) sur les groupes filtrés. Dans sa terminologie, la proposition 10 signifie que *l'algèbre de Lie* $gr(G_1) = \sum_{i \geqslant 1} G_i/G_{i+1}$ *est abélienne.*

Exercices. 1) Si G' est un groupe quotient de $G = G(L/K)$, montrer que G'_0 et G'_1 sont les images dans G' de G_0 et de G_1. En déduire (par passage à la limite) une définition de G_0 et de G_1 lorsque G est le groupe de Galois d'une extension infinie.

2) On suppose que $\overline{K}$ est un corps parfait. Soit K_s la clôture séparable de K, et soit

$$G = G(K_s/K)$$

son groupe de Galois. On définit par passage à la limite les sous-groupes G_0 et G_1 de G (cf. exer. 1).

a) Soit $\overline{K}_s$ la clôture séparable (ou algébrique, c'est la même chose) du corps $\overline{K}$. Montrer que $G/G_0 = G(\overline{K}_s/\overline{K})$.

b) Pour tout entier $n \geqslant 1$, soit E_n l'ensemble des racines n-ièmes de l'unité de $\overline{K}_s$. Si m divise n, soit $f_{mn} : E_n \to E_m$ l'homomorphisme $x \to x^{n/m}$, et soit E la limite projective du système (E_n, f_{mn}). Montrer que G_0/G_1 est isomorphe (canoniquement) à E. En déduire qu'il est isomorphe (non canoniquement) au produit $\prod \mathbf{Z}_q$ des groupes d'entiers q-adiques, q parcourant l'ensemble des nombres premiers distincts de la caractéristique de $\overline{K}$. Montrer que l'isomorphisme $G_0/G_1 = E$ est compatible avec les opérations de G/G_0 sur G_0/G_1 et sur E.

c) Déduire de ce qui précède la structure du groupe G/G_1 lorsque $\overline{K}$ est un corps fini.

3) On suppose que la caractéristique de $\overline{K}$ est $p \neq 0$. On pose $e = v_L(p)$ (indice de ramification absolu de L).

a) Soit $s \in G_i$, $i \geqslant 1$; soit $s(\pi) = \pi(1 + a)$, avec $a \in \mathfrak{p}_L$. Posons $\varphi = s - 1$; c'est une application K-linéaire de L dans L. Montrer que $\varphi(x) \equiv jax \mod \mathfrak{p}_L^{i+j+1}$ si $x \in \mathfrak{p}_L^j$.

b) On pose $\psi = s^p - 1$. Montrer, en utilisant la formule du binôme, que pour tout $x \in \mathfrak{p}_L$, on a :

(i)	$\psi(x) \equiv pjax \mod \mathfrak{p}_L^{i+j+e+1}$	si	$i > e/(p-1)$,
(ii)	$\psi(x) \equiv pjax + j(1 - i^{p-1})a^p x \mod \mathfrak{p}_L^{i+j+e+1}$	si	$i = e/(p-1)$,
(iii)	$\psi(x) \equiv j(1 - i^{p-1})\, a^p x \mod \mathfrak{p}_L^{j+pi+1}$	si	$i < e/(p-1)$.

c) On suppose que $i > e/(p-1)$ et que $s \notin G_{i+1}$. Déduire de *b*) que $s^p \in G_{i+e}$ et $s^p \notin G_{i+e+1}$. En déduire une contradiction avec le fait que s est d'ordre une puissance de p, d'où $G_i = |1|$ si $i > e/(p-1)$.

d) Montrer, par un raisonnement analogue, que lorsque $i = e/(p-1)$, le groupe G_i est soit égal à $|1|$, soit cyclique d'ordre p, ce dernier cas n'étant possible que si $i \equiv 0 \mod p$.

e) Si $i < e/(p-1)$, et si $i \not\equiv 0 \mod p$, montrer que $s^p \in G_{pi+1}$. Si $i \equiv 0 \mod p$, montrer que $s^p \in G_{pi}$ et que $\theta_{pi}(s^p) = 0_i(s)^p$; en déduire que, pour une telle valeur de i, le groupe G_i/G_{i+1} est soit réduit à $|1|$, soit cyclique d'ordre p, ce dernier cas ne pouvant se présenter que s'il existe un entier $h > 0$ tel que $p^h i = e/(p-1)$.

f) Montrer que, si les entiers $i \geqslant 1$ tels que $G_i \neq G_{i+1}$ sont congrus à 0 mod. p (cf. prop. 11), les entiers en question sont de la forme $p^k i_0$, $1 \leqslant k \leqslant h$, avec $p^h i_0 = e/(p-1)$, et le groupe G_1 est cyclique d'ordre p^h.

4) On suppose que K contient une racine primitive p-ième de l'unité. Soit L l'extension de K obtenue au moyen de l'équation $x^p = \pi$. Montrer que L est une extension cyclique totalement ramifiée de K. Montrer que, si s est un générateur de son groupe de Galois, on a $s \in G_i$, $s \notin G_{i+1}$ pour $i = e/(p-1)$, e désignant l'indice de ramification absolu de L (cf. exer. 3, *d*)).

5) Soit e_K l'indice de ramification absolu de K, soit n un entier $\geqslant 1$, avec $n < pe_K/(p-1)$, et $(n, p) = 1$, et soit $y \in K$ un élément de valuation $-n$.

(*a*) Montrer que l'équation (dite *d'Artin-Schreier*)

$$x^p - x = y$$

est irréductible sur K, et définit une extension L/K qui est cyclique de degré p. (On montrera que, si x est racine de cette équation, les autres racines sont de la forme $x + z_i$ $(0 \leqslant i < p)$, avec $z_i \in A_L$ et $z_i \equiv i \bmod. \mathfrak{p}_L$.)

(*b*) Soit $G = G(L/K)$. Montrer que $G_n = G$, et $G_{n+1} = \{1\}$.

[Pour davantage de détails sur les exercices 3, 4, 5, cf. Ore [49] et MacKenzie-Whaples [45].]

6) En utilisant l'expression de la différente au moyen des groupes de ramification, donner une nouvelle démonstration de la proposition 13 du Chapitre III.

7) Soit k un corps algébriquement clos de caractéristique zéro, et soit E le corps des séries formelles $\sum c_r T^r$, où les coefficients c_r appartiennent à k, et où les exposants r sont des nombres *rationnels* tendant vers $+\infty$. Montrer que E est algébriquement clos. (On observera que E est le complété de la clôture algébrique de $k((T))$, d'après la proposition 8.)

8) Soit k un corps valué complet algébriquement clos de caractéristique zéro, et soit $k\{\{T\}\}$ le corps des fractions de l'anneau des séries convergentes à coefficients dans k. Montrer que la clôture algébrique de $k\{\{T\}\}$ est réunion des corps $k\{\{T^{1/n}\}\}$.

§ 3. *Les fonctions* φ *et* ψ *et le théorème de Herbrand*

On conserve les hypothèses et notations des deux paragraphes précédents. Si u est un nombre réel $\geqslant -1$, on note G_u le groupe de ramification G_i, où i est le plus petit entier $\geqslant u$. On a donc :

$$s \in G_u \Longleftrightarrow i_G(s) \geqslant u + 1.$$

On pose :

$$\varphi(u) = \int_0^u \frac{dt}{(G_0 : G_t)}.$$

Lorsque $-1 \leqslant t \leqslant 0$, on convient que $(G_0 : G_t)$ représente l'inverse de $(G_t : G_0)$ c'est-à-dire 1 pour $-1 < t \leqslant 0$. La fonction φ est donc égale à u entre -1 et 0.

[Lorsqu'on veut préciser l'extension L/K, on écrit $\varphi_{L/K}$ au lieu de φ.]

Il est facile d'expliciter la fonction φ : si $m \leqslant u \leqslant m+1$, où m est un entier positif, on a :

$$\varphi(u) = \frac{1}{g_0}(g_1 + \cdots + g_m + (u-m)\, g_{m+1}), \qquad \text{avec} \quad g_i = \operatorname{Card}(G_i).$$

En particulier, $\varphi(m) + 1 = \dfrac{1}{g_0} \sum_{i=0}^{i=m} g_i$.

Proposition 12. (*a*) *La fonction* φ *est continue, linéaire par morceaux, croissante, concave.*

(*b*) *On a* $\varphi(0) = 0$.

(*c*) *Si l'on désigne par* φ'_d *et* φ'_g *les dérivées à droite et à gauche de* φ, *on a*:

$\varphi'_g(u) = \varphi'_d(u) = 1/(G_0 : G_u)$ *si* u *n'est pas entier,*
$\varphi'_g(u) = 1/(G_0 : G_u)$ *et* $\varphi'_d(u) = 1/(G_0 : G_{u+1})$ *si* u *est entier.*

La vérification est immédiate. On notera que ces propriétés suffisent à caractériser φ.

L'application φ est un homéomorphisme de la demi-droite $[-1, +\infty[$ sur elle-même. Nous noterons ψ (ou $\psi_{L/K}$) l'application réciproque.

PROPOSITION 13. (*a*) *La fonction* ψ *est continue, linéaire par morceaux, croissante, convexe.*

(*b*) *On a* $\psi(0) = 0$.

(*c*) *Si* $v = \varphi(u)$, *on a* $\psi'_g(v) = 1/\varphi'_g(u)$, $\psi'_d(v) = 1/\varphi'_d(u)$. (*En particulier,* ψ'_g *et* ψ'_d *ne prennent que des valeurs entières.*)

(*d*) *Si* v *est entier, il en est de même de* $u = \psi(v)$.

Les propriétés (*a*), (*b*), (*c*) sont immédiates. Pour prouver (*d*), soit m un entier tel que $m \leqslant u \leqslant m + 1$. On a :

$$g_0 v = g_1 + \cdots + g_m + (u - m) g_{m+1}.$$

Comme G_{m+1} est contenu dans $G_0, \ldots, G_m$, son ordre g_{m+1} divise $g_0, \ldots, g_m$. On en déduit que $u - m$ est entier, d'où le fait que u lui-même est entier, c.q.f.d.

Nous pouvons maintenant définir la *numérotation supérieure* des groupes de ramification. On pose :

$$G^v = G_{\psi(v)} \qquad \text{ou encore} \qquad G^{\varphi(u)} = G_u.$$

On a $G^{-1} = G$, $G^0 = G_0$, $G^v = \{1\}$ pour v assez grand. La connaissance des G^v équivaut à celle des G_u: en effet, on vérifie facilement que $\psi(v) = \int_0^v (G^0 : G^w)\, dw$.

La détermination des groupes de ramification d'un groupe quotient s'énonce alors ainsi :

PROPOSITION 14. *Si* H *est un sous-groupe invariant de* G, *on a* $(G/H)^v = G^v H/H$ *pour tout* v.

(En d'autres termes, lorsqu'on emploie la numérotation supérieure, les groupes de ramification de G/H sont les images de ceux de G; la notation supérieure est adaptée aux quotients, tout comme la notation inférieure est adaptée aux sous-groupes.)

Soit K′ le sous-corps de L correspondant à H; on a :

PROPOSITION 15. *Les fonctions* φ *et* ψ *vérifient les formules de transitivité* :

$$\varphi_{L/K} = \varphi_{K'/K} \circ \varphi_{L/K'} \qquad \text{et} \qquad \psi_{L/K} = \psi_{L/K'} \circ \psi_{K'/K}.$$

Nous allons d'abord démontrer quelques lemmes :

LEMME 3. $\varphi_{L/K}(u) = \frac{1}{g_0} \sum_{s \in G} \mathrm{Inf}(i_G(s), u+1) - 1$.

Soit $\theta(u)$ la fonction définie par le membre de droite; c'est une fonction continue, linéaire par morceaux, et qui s'annule pour $u = 0$. Si $m < u < m+1$, où m est entier, la dérivée $\theta'(u)$ est égale au nombre des $s \in G$ tels que $i_G(s) \geqslant m+2$, multiplié par $1/g_0$; on a donc $\theta'(u) = 1/(G_0 : G_{m+1})$, et comme c'est aussi la valeur de $\varphi'(u)$, on en conclut que les fonctions θ et φ coïncident.

LEMME 4. *Soit $\sigma \in G/H$, et soit $j(\sigma)$ la borne supérieure des entiers $i_G(s)$, s parcourant l'ensemble des éléments de* G *ayant σ pour image dans* G/H. *On a*:

$$i_{G/H}(\sigma) - 1 = \varphi_{L/K'}(j(\sigma) - 1).$$

Soit $s \in G$ un élément ayant pour image σ et tel que $i_G(s) = j(\sigma)$. Posons $m = i_G(s)$. Si $t \in H$ appartient à H_{m-1}, on a $i_G(t) \geqslant m$, d'où $i_G(st) \geqslant m$, et $i_G(st) = m$. Si d'autre part t n'appartient pas à H_{m-1}, on a $i_G(t) < m$, et $i_G(st) = i_G(t)$. Dans les deux cas, on a $i_G(st) = \mathrm{Inf}(i_G(t), m)$. Appliquant la proposition 3 du § 1, on obtient:

$$i_{G/H}(\sigma) = \frac{1}{e_{L/K'}} \sum_{t \in H} \mathrm{Inf}(i_G(t), m).$$

Mais on a $i_G(t) = i_H(t)$, et $e_{L/K'} = \mathrm{Card}(H_0)$. En appliquant le lemme 3 au groupe H, on trouve :

$$i_{G/H}(\sigma) = 1 + \varphi_{L/K'}(m-1), \qquad \text{c.q.f.d.}$$

LEMME 5. *On a $G_u H/H = (G/H)_v$, avec $v = \varphi_{L/K'}(u)$.*

(C'est là ce qu'on appelle usuellement le « théorème de Herbrand ».)

Conservons les notations du lemme précédent. On a les équivalences :

$$\sigma \in G_u H/H \iff j(\sigma) - 1 \geqslant u \iff \varphi_{L/K'}(j(\sigma) - 1) \geqslant \varphi_{L/K'}(u)$$
$$\iff i_{G/H}(\sigma) - 1 \geqslant \varphi_{L/K'}(u) \iff \sigma \in (G/H)_v, \quad \text{c.q.f.d.}$$

Démonstration de la proposition 15. Soit u non entier $\geqslant -1$. La dérivée de la fonction composée $\varphi_{K'/K} \circ \varphi_{L/K'}$ est égale à

$$\varphi'_{K'/K}(v) \cdot \varphi'_{L/K'}(u), \qquad \text{avec} \quad v = \varphi_{L/K'}(u).$$

On peut donc l'écrire sous la forme :

$$(\mathrm{Card}\,(G/H)_v / e_{K'/K}) \cdot (\mathrm{Card}\,(H_u)/e_{L/K'}).$$

En appliquant le lemme 5, on voit que cette expression est égale à $\mathrm{Card}\,(G_u)/e_{L/K}$, c'est-à-dire à la dérivée $\varphi'_{L/K}(u)$, ce qui montre l'égalité cherchée. La formule relative aux fonctions ψ résulte de la précédente.

Démonstration de la proposition 14. On a :

$$(G/H)^v = (G/H)_x \qquad \text{avec} \quad x = \psi_{K'/K}(v).$$

D'après le lemme 5, on a $(G/H)_x = G_w H/H$, avec $w = \psi_{L/K'}(x) = \psi_{L/K}(v)$ d'après la proposition 15. On a donc $G_w = G^v$, c.q.f.d.

Remarques. 1) Soit L/K une extension galoisienne infinie, et soit G son groupe de Galois. On peut définir G^v comme $\varprojlim G(L'/K)^v$, L' parcourant l'ensemble des sous-extensions galoisiennes finies de L. Les G^v forment encore une filtration de G; cette filtration est *continue à gauche*: $G^v = \bigcap_{w<v} G^w$. On dit que v est un « saut » pour la filtration (G^v) si $G^v \neq G^{v+\varepsilon}$ pour tout $\varepsilon > 0$. Même lorsque L/K est finie, *un saut n'est pas nécessairement entier* (cf. exer. 2).

2) Soit E une sous-extension de l'extension galoisienne L/K (cette dernière étant supposée à extension résiduelle séparable, comme toujours). On définit $\varphi_{E/K}$ comme $\varphi_{L/K} \circ \psi_{L/E}$; la proposition 15 montre que cette définition est indépendante de l'extension L choisie, et que les $\varphi_{E/K}$ vérifient les mêmes formules de transitivité que les $\varphi_{L/K}$.

3) La double numérotation des groupes de ramification peut aussi se présenter de la façon suivante :

Soit $\Gamma_L = L^*/U_L$ le groupe des ordres de L, et soit $\mathbf{R}_L = \Gamma_L \otimes \mathbf{R}$. L'isomorphisme canonique $\Gamma_L = \mathbf{Z}$ identifie $\mathbf{R}_L$ à $\mathbf{R}$; soit T_L l'image de $[-1, +\infty[$ par cet isomorphisme. Il est naturel de considérer que les groupes G_u sont *indexés par des éléments u de* T_L (on a utilisé la valuation v_L de L pour les définir). De même, on interprète $\varphi_{L/K}$ comme un *isomorphisme de l'ensemble ordonné* T_L *sur l'ensemble ordonné* T_K et $\psi_{L/K}$ comme l'isomorphisme réciproque. De ce point de vue, la numérotation supérieure revient simplement à indexer les groupes de ramification *par les éléments de* T_K. La proposition 15 montre que les $(T_L, \varphi_{L/K})$ forment un système transitif d'isomorphismes. On peut en profiter pour définir un ensemble ordonné unique :

$$T = \varprojlim (T_L, \varphi_{L/L'}) = \varinjlim (T_L, \psi_{L/L'}),$$

où L parcourt l'ensemble des sous-extensions finies d'une extension galoisienne donnée E/K. Un élément t de T est par définition un système $(t_L)_{L \subset E}$, avec $t_L \in T_L$ et $\varphi_{L/L'}(t_L) = t_{L'}$ si $L \supset L'$. Si maintenant G est le groupe de Galois d'une extension L/L', on pose :

$$G(t) = G_{t_L} = G^{t_{L'}}, \qquad \text{pour tout} \quad t \in T.$$

Si H est un sous-groupe de G, on a $H(t) = H \cap G(t)$, et si H est invariant, on a $(G/H)(t) = G(t)H/H$: *l'indexation des groupes de ramification par* T *est compatible à la fois avec le passage au sous-groupe, et avec le passage au quotient.*

La numérotation supérieure est particulièrement intéressante dans le cas abélien, à cause du résultat suivant :

THÉORÈME (Hasse-Arf). *Si* G *est un groupe abélien, et si* v *est un saut de la filtration* $\{G^i\}$, *alors* v *est entier.*

[En d'autres termes, si $G_i \neq G_{i+1}$, $\varphi(i)$ est entier.]

Pour la démonstration, voir Chap. V, § 7.

Remarque. Le théorème ci-dessus a été d'abord démontré par Hasse (cf. [32] et [33]) dans le cas d'un corps résiduel fini (voir aussi Chap. XV, § 2). Le cas général est dû à Arf [2]; on en trouvera une autre démonstration, basée sur la structure de groupe proalgébrique du groupe des unités, dans [59]. Voir aussi Sen [106], ainsi que Cassels-Fröhlich, [75], p. 157.

Exemple. Supposons que G soit cyclique d'ordre p^n, p étant la caractéristique de K et soit $G(i)$ le sous-groupe de G d'ordre p^{n-i}. Le théorème de Hasse-Arf revient à dire qu'il existe des entiers

$$i_0, i_1, \ldots, i_{n-1},$$

strictement positifs, et tels que les groupes de ramification de G soient donnés par les formules :

$$\begin{aligned}
G_0 = \cdots = G_{i_0} = G = G^0 = \cdots = G^{i_0}, \\
G_{i_0+1} = \cdots = G_{i_0+pi_1} = G(1) = G^{i_0+1} = \cdots = G^{i_0+i_1}, \\
G_{i_0+pi_1+1} = \cdots = G_{i_0+pi_1+p^2i_2} = G(2) = G^{i_0+i_1+1} = \cdots = G^{i_0+i_1+i_2}, \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
G_{i_0+pi_1+\cdots+p^{n-1}i_{n-1}+1} = \{1\} = G^{i_0+\cdots+i_{n-1}+1}.
\end{aligned}$$

Exercices: 1) Comme application du théorème de Herbrand, retrouver les formules

$$G_1H/H = (G/H)_1, \qquad G_0H/H = (G/H)_0,$$

ainsi que le corollaire à la proposition 3 du § 1.

2) Soit $G = \{\pm 1, \pm i, \pm j, \pm k\}$ le groupe quaternionien, et soit $C = \{\pm 1\}$ son centre. On suppose que G est groupe de Galois d'une extension L/K totalement ramifiée et que $G_4 = \{1\}$ (c'est effectivement possible, cf. [57], n° 5). Montrer que l'on a alors $G = G_0 = G_1$, $C = G_2 = G_3$. En déduire les formules :

$$G^v = G \quad \text{pour} \quad v \leqslant 1, \qquad G^v = C \quad \text{pour} \quad 1 < v \leqslant 3/2, \qquad G^v = \{1\} \quad \text{pour} \quad v > 3/2,$$

3) Montrer que, si le théorème de Hasse-Arf est vrai pour tout groupe cyclique d'ordre une puissance d'un nombre premier, il l'est pour tout groupe (utiliser le cor. 2 à la prop. 9. ainsi que le théorème de Herbrand).

§ 4. *Exemple: extensions cyclotomiques du corps* $\mathbf{Q}_p$

Nous allons étudier les corps obtenus en adjoignant à $\mathbf{Q}_p$ les racines de l'unité. Commençons par celles d'ordre premier à p. On a le résultat général suivant :

PROPOSITION 16. *Soit* K *un corps complet pour une valuation discrète, et de corps résiduel* $k = \mathbf{F}_q$, *avec* $q = p^f$. *Soit* n *un entier premier à* p. *Soit* K_n (*resp.* k_n) *le corps obtenu en adjoignant à* K (*resp.* k) *les racines* n*-ièmes de l'unité. Le corps* K_n *est une extension non ramifiée de*

K, *d'extension résiduelle* k_n/k. *On a* $A_{K_n} = A_K[z]$, *où* z *est une racine primitive* n*-ième de l'unité. Le groupe de Galois* $G(K_n/K)$ *s'identifie au groupe* $G(k_n/k)$. *Il est cyclique, et admet un générateur* s *tel que* $s(z) = z^q$ *pour toute racine* n*-ième de l'unité* z.

Soit L l'extension non ramifiée de K admettant pour extension résiduelle l'extension k_n/k (cf. Chap. III, § 5), et soit S l'ensemble des représentants multiplicatifs de L (cf. Chap. II, § 4). Soit ζ une racine primitive n-ième de l'unité dans k_n, et soit z son représentant multiplicatif. Il est clair que z est une racine primitive n-ième de l'unité; comme ζ engendre k_n/k, z engendre la A_K-algèbre A_L, et *a fortiori* l'extension L/K. Donc $L = K_n$, et l'on voit que $G(K_n/K) = G(k_n/k)$ est engendré par un élément s tel que $s(a) \equiv a^q$ pour tout $a \in A_L$. Si $z \in S$, on a encore $s(z) \in S$, et comme $s(z) \equiv z^q$, cela entraîne $s(z) = z^q$, ce qui achève de prouver la proposition.

COROLLAIRE 1. *Le degré* $[K_n : K]$ *est égal au plus petit entier* $r \geqslant 1$ *tel que* $q^r \equiv 1 \bmod. n$.

En effet, r est le plus petit entier tel que $s^r = 1$.

COROLLAIRE 2. *L'extension maximale non ramifiée* K_{ar} *de* K *s'obtient en adjoignant à* K *toutes les racines de l'unité d'ordre premier à* p. *Son groupe de Galois s'identifie au groupe* $\hat{\mathbf{Z}}$; *il admet un générateur* s *tel que* $s(z) = z^q$ *pour toute racine de l'unité* z *d'ordre premier à* p.

Cela résulte de la proposition 16, par passage à la limite sur n, en observant que la réunion des k_n est la clôture algébrique de k.

Remarque. L'élément s n'est autre que le *symbole d'Artin de* $\mathfrak{p}_K$, au sens du Chap. I, § 8.

Passons maintenant aux racines de l'unité d'ordre $n = p^m$, où m est un entier $\geqslant 1$; nous nous limitons cette fois au cas du corps $\mathbf{Q}_p$.

PROPOSITION 17. *Soit* K_n *le corps obtenu en adjoignant à* $K = \mathbf{Q}_p$ *une racine primitive* n*-ième* z *de l'unité, avec* $n = p^m$. *Alors*:

(i) *On a* $[K_n : K] = \varphi(n) = (p - 1)\, p^{m-1}$.

(ii) *Le groupe de Galois* $G(K_n/K)$ *s'identifie au groupe* $G(n)$ *des éléments inversibles de* $\mathbf{Z}/n\mathbf{Z}$.

(iii) *Le corps* K_n *est totalement ramifié sur le corps* K. *L'élément* $\pi = z - 1$ *est une uniformisante de* K_n, *et* $A_{K_n} = A_K[z]$.

On sait *a priori* (cf. Bourbaki, *Alg.*, Chap. V, § 11) que $G(K_n/K)$ s'identifie à un sous-groupe de $G(n)$; comme l'ordre de $G(n)$ est $\varphi(n)$, on voit que les assertions (i) et (ii) sont équivalentes.

D'autre part, soit $u = z^{p^{m-1}}$; comme c'est une racine primitive p-ième de l'unité, on a $u^{p-1} + u^{p-2} + \cdots + 1 = 0$, d'où :

$$z^{(p-1)p^{m-1}} + z^{(p-2)p^{m-1}} + \cdots + 1 = 0.$$

Si l'on note F le polynôme du membre de gauche, on voit que π est racine de l'équation $F(1 + X) = 0$. C'est là une *équation d'Eisenstein* de degré $\varphi(n)$. En effet, son terme constant est égal à $F(1) = p$, et la réduction mod. p de cette équation est égale à $X^{\varphi(n)}$, comme on le montre tout de suite. En appliquant la proposition 18 du Chap. I, on voit à la fois que $[K_n : K] = \varphi(n)$, que π est une uniformisante de K_n, et que A_{K_n} est engendré par π (ou, ce qui revient au même, par z), c.q.f.d.

Nous allons maintenant déterminer les *groupes de ramification* du groupe

$$G = G(K_n/K).$$

Si v est un entier compris entre 0 et m, nous noterons $G(n)^v$ le sous-groupe de $G(n)$ formé des éléments a tels que $a \equiv 1 \bmod p^v$. Le groupe $G(n)/G(n)^v$ s'identifie au groupe $G(p^v)$, c'est-à-dire au groupe de Galois de l'extension K_{p^v}/K; on a donc $G(n)^v = G(K_n/K_{p^v})$.

PROPOSITION 18. *Les groupes de ramification* G_u *de* $G(K_n/K)$ *sont les suivants* :

$$\begin{array}{lll} & G_0 = G, & \\ si & 1 \leqslant u \leqslant p-1, & G_u = G(n)^1 \\ si & p \leqslant u \leqslant p^2-1, & G_u = G(n)^2 \\ & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ si & p^{m-1} \leqslant u, & G_u = G(n)^m = \{1\}. \end{array}$$

Soit $a \in G(n)$ un élément distinct de 1, et soit s_a l'élément correspondant de G. Soit v le plus grand entier tel que $a \equiv 1 \bmod p^v$; on a $a \in G(n)^v$ et $a \notin G(n)^{v+1}$. D'autre part :

$$i_G(s_a) = v_{K_n}(s_a(z) - z) = v_{K_n}(z^a - z) = v_{K_n}(z^{a-1} - 1).$$

Comme z^{a-1} est une racine primitive p^{m-v}-ième de l'unité, $z^{a-1} - 1$ est une uniformisante du corps $K_{p^{m-v}}$. On en déduit :

$$i_G(s_a) = [K_n : K_{p^{m-v}}] = \text{Card}\,(G(n)^{m-v}) = p^v.$$

Si alors on a $p^{k-1} \leqslant u \leqslant p^k - 1$, on voit que l'élément s_a appartient à G_u si et seulement si $v \geqslant k$, ce qui montre bien que $G_u = G(n)^v$, c.q.f.d.

COROLLAIRE. *Les sauts de la filtration* (G^v) *sont entiers. On a de plus* :

$$G^v = G(n)^v \quad \textit{pour} \quad 0 \leqslant v \leqslant m, \quad \textit{et} \quad G^v = \{1\} \quad \textit{pour} \quad v \geqslant m.$$

Les sauts de la filtration G_u ont lieu pour $u = p^k - 1$, avec $0 \leqslant k \leqslant m - 1$ (le cas $p = 2$ fait exception : 0 n'est pas un saut). Tout revient donc à prouver que $\varphi_{L/K}(p^k - 1) = k$ pour $k = 0, 1, \ldots, m-1$, ce qui ne présente pas de difficultés.

Remarques. 1) Le résultat précédent peut s'énoncer de façon plus suggestive *en passant à la limite sur m*, c'est-à-dire en introduisant le corps K_{p^∞} réunion des K_{p^m}. Le groupe de Galois de K_{p^∞} sur K est la limite projective des groupes

$$G(p^m) = (\mathbf{Z}/p^m\mathbf{Z})^*;$$

comme la limite projective des $\mathbf{Z}/p^m\mathbf{Z}$ est le groupe $\mathbf{Z}_p$ des entiers p-adiques, la limite des $G(p^m)$ s'identifie de façon naturelle au groupe U_p *des éléments inversibles de* $\mathbf{Z}_p$. Si $\alpha \in U_p$, l'élément $s_\alpha \in G(K_{p^\infty}/K)$ associé à α transforme une racine p^m-ième de l'unité z en z^α, l'exponentielle ayant un sens évident. Le groupe U_p est filtré par les U_p^n comme

il a été dit au § 2; on prolonge cette filtration aux valeurs non entières v de l'indice en posant $U_p^v = U_p^n$ si n est le plus petit entier $\geqslant v$. Le corollaire ci-dessus montre alors que *l'isomorphisme canonique de* U_p *sur* $G(K_{p^\infty}/K)$ *transforme la filtration* U_p^v *de* U_p *en la filtration de* $G(K_{p^\infty}/K)$ *formée des groupes de ramification* (avec la notation supérieure).

2) Si l'on adjoint à $K = \mathbf{Q}_p$ *toutes* les racines de l'unité, on obtient l'extension composée des extensions K_{nr} et K_{p^∞}; comme ces extensions sont linéairement disjointes sur K (l'une étant totalement ramifiée, et l'autre non ramifiée), le groupe de Galois de leur composée $K_{nr}K_{p^\infty}$ sur K est isomorphe au produit des groupes de Galois $G(K_{nr}/K)$ et $G(K_{p^\infty}/K)$, c'est-à-dire à $\hat{\mathbf{Z}} \times U_p$. Nous verrons au Chap. XIV, § 7, que $K_{nr}K_{p^\infty}$ est en fait *l'extension abélienne maximale de* K.

CHAPITRE V

LA NORME

Soit L/K une extension galoisienne vérifiant les hypothèses du Chapitre IV. La norme $N = N_{L/K}$ est un homomorphisme du groupe multiplicatif L^* dans le groupe multiplicatif K^*; elle applique U_L dans U_K, et l'on a $v_K(Nx) = fv_L(x)$, avec $f = [\bar{L} : \bar{K}]$. On a donc un diagramme commutatif :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L & \longrightarrow & L^* & \longrightarrow & \mathbf{Z} & \longrightarrow & 0 \\ & & \mathrm{N}\downarrow & & \mathrm{N}\downarrow & & f\downarrow & & \\ 0 & \longrightarrow & U_K & \longrightarrow & K^* & \longrightarrow & \mathbf{Z} & \longrightarrow & 0. \end{array}$$

Nous nous proposons, en suivant Hasse [33], de déterminer l'effet de N sur la filtration des U_L^i (resp. des U_K^i); nous nous bornerons aux résultats indépendants de toute hypothèse sur les corps résiduels. Le cas d'un corps résiduel fini (ou plus généralement quasi-fini) sera traité au Chapitre XV.

Notation. Si v est un nombre réel $\geqslant 0$, on note U_L^v le groupe U_L^n, où n est le plus petit entier $\geqslant v$.

§ 1. Lemmes

Les deux lemmes suivants sont utiles lorsqu'on veut comparer des groupes filtrés :

LEMME 1. *Soit*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ & & f'\downarrow & & f\downarrow & & f''\downarrow & & \\ 0 & \longrightarrow & B' & \longrightarrow & B & \longrightarrow & B'' & \longrightarrow & 0 \end{array}$$

un diagramme commutatif dont les lignes sont exactes. On a alors une suite exacte :

$$0 \to \mathrm{Ker}\, f' \to \mathrm{Ker}\, f \to \mathrm{Ker}\, f'' \xrightarrow{\varphi} \mathrm{Coker}\, f' \to \mathrm{Coker}\, f \to \mathrm{Coker}\, f'' \to 0.$$

[On rappelle que $\mathrm{Ker}\, f = f^{-1}(0)$ est le *noyau* de f, et que $\mathrm{Coker}\, f = \mathrm{B}/f(\mathrm{A})$ est son *conoyau*.]

Si $a'' \in \mathrm{Ker}\, f''$, on choisit un élément $a \in \mathrm{A}$ se projetant en a''; $f(a)$ est un élément de B d'image nulle dans B''; il existe donc un élément $b' \in \mathrm{B}'$ dont l'image dans B est égale à $f(a)$; la classe de b' ne dépend pas du choix de a, et si on la note $\varphi(a'')$, φ est un homomorphisme de $\mathrm{Ker}\, f''$ dans $\mathrm{Coker}\, f'$. Les autres applications intervenant dans la suite exacte se définissent de façon évidente; quant à l'exactitude elle-même, elle ne présente pas de difficultés (cf. Cartan-Eilenberg [13], p. 40, ainsi que Bourbaki, *Alg. comm.*, Chap. I, § 1).

LEMME 2. *Soit* A (*resp.* A') *un groupe abélien muni d'une suite décroissante de sous-groupes* A_n (*resp.* A'_n). *Supposons que* $\mathrm{A}_0 = \mathrm{A}$, $\mathrm{A}'_0 = \mathrm{A}'$, *et que* A *et* A' *soient séparés et complets pour les topologies définies par* A_n *et* A'_n (en d'autres termes, les homomorphismes canoniques $\mathrm{A} \to \varprojlim \mathrm{A}/\mathrm{A}_n$ et $\mathrm{A}' \to \varprojlim \mathrm{A}'/\mathrm{A}'_n$ sont bijectifs). *Soit* $u : \mathrm{A} \to \mathrm{A}'$ *un homomorphisme appliquant* A_n *dans* A'_n *pour tout* n. *Si les homomorphismes*

$$u_n : \mathrm{A}_n/\mathrm{A}_{n+1} \to \mathrm{A}'_n/\mathrm{A}'_{n+1}$$

définis par u *sont tous injectifs* (*resp. surjectifs*), *il en est de même de* u.

Rappelons brièvement la démonstration de ce résultat (cf. Bourbaki, *Alg. comm.*, Chap. III, § 2) :

Si les u_n sont injectifs, on a $\mathrm{Ker}(u) \cap \mathrm{A}_n = \mathrm{Ker}(u) \cap \mathrm{A}_{n+1}$, d'où par récurrence sur n, $\mathrm{Ker}(u) \subset \mathrm{A}_n$ pour tout n, et comme $\bigcap \mathrm{A}_n$ est réduit à $\{0\}$ (A étant séparé), on voit bien que u est injectif.

Supposons les u_n surjectifs, et soit $a' \in \mathrm{A}' = \mathrm{A}'_0$. Il existe $a_0 \in \mathrm{A}_0$ et $a'_1 \in \mathrm{A}'_1$ tels que $u(a_0) = a' - a'_1$. De même, utilisant la surjectivité de u_1, on voit qu'il existe $a_1 \in \mathrm{A}_1$ et $a'_2 \in \mathrm{A}'_2$ tels que $u(a_1) = a'_1 - a'_2$. On construit de même a_2, a_3, ..., et a'_2, a'_4, ... Comme A est complet, la série $a_0 + a_1 + \cdots$ converge vers un élément $a \in \mathrm{A}$. On a $u(a) - a' \in \mathrm{A}'_n$ pour tout n, d'où $u(a) = a'$, c.q.f.d.

§ 2. *Le cas non ramifié*

PROPOSITION 1. *Si* L/K *est non ramifiée*, N *applique* U_L^n *dans* U_K^n *pour tout* n.

Soit $x = 1 + y$, avec $y \in \mathfrak{p}_\mathrm{L}^n$. On a $s(x) = 1 + s(y)$ pour tout $s \in \mathrm{G}$, et $s(y) \in \mathfrak{p}_\mathrm{L}^n$. On en tire :

$$(*) \qquad \mathrm{N}x = \prod_{s \in \mathrm{G}} (1 + s(y)) \equiv 1 + \sum_{s \in \mathrm{G}} s(y) \mod \mathfrak{p}_\mathrm{L}^{n+1}.$$

Mais, puisque L/K est non ramifiée, $\mathfrak{p}_\mathrm{L}^n \cap \mathrm{K} = \mathfrak{p}_\mathrm{K}^n$, et on a donc bien $\mathrm{N}x \equiv 1 \mod \mathfrak{p}_\mathrm{K}^n$, c.q.f.d.

L'application N définit par passage au quotient des applications

$$\mathrm{N}_n : \mathrm{U}_\mathrm{L}^n/\mathrm{U}_\mathrm{L}^{n+1} \to \mathrm{U}_\mathrm{K}^n/\mathrm{U}_\mathrm{K}^{n+1}$$

que l'on va déterminer. Pour cela, rappelons (cf. Chap. IV, § 2) que $\mathrm{U}_\mathrm{L}/\mathrm{U}_\mathrm{L}^1$ s'iden-

tifie au groupe multiplicatif $\overline{L}^*$ du corps résiduel $\overline{L}$, et que U_L^n/U_L^{n+1} ($n \geqslant 1$) s'identifie à $\mathfrak{p}_L^n/\mathfrak{p}_L^{n+1}$, qui est un espace vectoriel de dimension 1 sur $\overline{L}$, que nous noterons aussi Ω_L^n. Comme L/K est non ramifié, on voit tout de suite que Ω_L^n s'identifie canoniquement à $\overline{L} \otimes_K \Omega_K^n$. Compte tenu de ces identifications, on a :

PROPOSITION 2. *Supposons l'extension* L/K *non ramifiée. Alors*

(*i*) *L'application* $N_0 : \overline{L}^* \to \overline{K}^*$ *n'est autre que la norme dans l'extension résiduelle* $\overline{L}/\overline{K}$.

(*ii*) *Pour* $n \geqslant 1$, *l'application* $N_n : \overline{L} \otimes_K \Omega_K^n \to \Omega_K^n$ *n'est autre que l'application*

$$1 \otimes \mathrm{Tr}_{\overline{L}/\overline{K}}.$$

L'assertion (*i*) est triviale. L'assertion (*ii*) résulte de la formule (*) démontrée ci-dessus.

PROPOSITION 3. *a*) *On a* $N(U_L^n) = U_K^n$ *pour tout* $n \geqslant 1$.

b) *Le groupe* U_K/NU_L *est isomorphe au groupe* $\overline{K}^*/N\overline{L}^*$.

c) *Le groupe* K^*/NL^* *est isomorphe à* $\mathbf{Z}/f\mathbf{Z} \times \overline{K}^*/N\overline{L}^*$, *avec* $f = [L : K] = [\overline{L} : \overline{K}]$.

On sait que la trace est surjective dans toute extension séparable; la proposition 2 montre donc que N_n est surjective pour $n \geqslant 1$, et en appliquant le lemme 2 à $N : U_L^1 \to U_K^n$, on en déduit (*a*).

On applique ensuite le lemme 1 au diagramme commutatif :

$$\begin{array}{ccccccc} 0 & \longrightarrow & U_L^1 & \longrightarrow & U_L & \longrightarrow & \overline{L}^* \longrightarrow 0 \\ & & \downarrow N & & \downarrow N & & \downarrow N \\ 0 & \longrightarrow & U_K^1 & \longrightarrow & U_K & \longrightarrow & \overline{K}^* \longrightarrow 0. \end{array}$$

On en déduit (*b*).

Enfin, le choix d'une uniformisante π de K permet d'identifier K^* à $\mathbf{Z} \times U_K$, et L^* à $\mathbf{Z} \times U_L$, ces identifications étant compatibles avec les opérations de G. On en déduit (*c*).

COROLLAIRE. *Les trois conditions suivantes sont équivalentes* :

(1) $(K^* : NL^*) = f$.

(2) $U_K = NU_L$.

(3) $\overline{K}^* = N\overline{L}^*$.

C'est évident.

Remarques. 1) La condition (3) est satisfaite lorsque $\overline{K}$ est un corps *fini* (ou plus généralement quasi-fini, cf. Chap. XIII).

2) Si v est un nombre réel $\geqslant 0$, la proposition 1 montre que $N(U_L^1)$ est contenu dans U_K^v, l'égalité ayant lieu si $v > 0$.

Exercice. Étendre les propositions 1, 2, 3 au cas d'une extension non ramifiée qui n'est pas galoisienne.

§ 3. *Le cas cyclique d'ordre premier, totalement ramifié*

On suppose dans ce paragraphe que G est un groupe cyclique d'ordre premier l, et que L/K est totalement ramifiée (on a donc $\overline{L} = \overline{K}$). On note π une uniformisante de L.

Soit s un générateur de G, et posons $t = i(s) - 1$, cf. Chap. IV, § 1. Les groupes de ramification de G sont les suivants :

$$G = G_0 = \cdots = G_t$$
$$\{1\} = G_{t+1} = \cdots .$$

D'après le Chap. IV, § 2, on a $t \neq 0$ si et seulement si l est égal à la caractéristique de $\overline{K}$, caractéristique que l'on désignera par p.

La fonction ψ du Chap. IV, § 5, s'écrit ici :

$$\psi(x) = \begin{cases} x & \text{si} \quad x \leqslant t \\ t + l(x - t) & \text{si} \quad x \geqslant t. \end{cases}$$

LEMME 3. *La différente* $\mathfrak{D}$ *de l'extension* L/K *est égale à* $\mathfrak{p}_L^m$, *avec* $m = (t+1)(l-1)$.

Cela résulte de la proposition 4 du Chap. IV.

LEMME 4. *Pour tout entier* $n \geqslant 0$, *on a* $\mathrm{Tr}(\mathfrak{p}_L^n) = \mathfrak{p}_K^r$, *avec* $m = (t+1)(l-1)$, *et* $r = [(m+n)/l]$.

[On rappelle que le symbole $[x]$ désigne la *partie entière* du nombre réel x, c'est-à-dire le plus grand entier $\leqslant x$.]

Puisque la trace est A_K-linéaire, $\mathrm{Tr}(\mathfrak{p}_L^n)$ est un idéal de A_K. Si r est un entier, la proposition 7 du Chap. III montre que $\mathrm{Tr}(\mathfrak{p}_L^n) \subset \mathfrak{p}_K^r$ si et seulement si

$$\mathfrak{p}_L^n \subset \mathfrak{p}_K^r . \mathfrak{D}^{-1} = \mathfrak{p}_L^{lr-m}$$

c'est-à-dire si $r \leqslant (m+n)/l$, c.q.f.d.

LEMME 5. *Si* $x \in \mathfrak{p}_L^n$, *on a* :

$$(**) \qquad N(1+x) \equiv 1 + \mathrm{Tr}(x) + N(x) \mod \mathrm{Tr}(\mathfrak{p}_L^{2n}).$$

Il est commode, pour le calcul qui suit, d'utiliser la notation exponentielle pour le groupe G, autrement dit de noter x^s le transformé de x par $s \in G$. On a par définition :

$$N(1+x) = \prod_{s \in G} (1 + x^s)$$

et, en développant :

$$N(1+x) = \sum x^u$$

où u parcourt l'ensemble des éléments de l'algèbre de groupe $\mathbf{Z}[G]$ qui sont de la forme $u = s_1 + \cdots + s_k$, les s_i étant eux-mêmes des éléments de G, deux à deux distincts. On pose $k = n(u)$: c'est l'augmentation de u. Les u d'augmentation 0, 1,

et l donnent respectivement les termes 1, $\mathrm{Tr}(x)$, et $\mathrm{N}(x)$ de la formule à démontrer. Tout revient donc à prouver que la somme des autres termes appartient à $\mathrm{Tr}(\mathfrak{p}_L^{s_n})$. Or, soit s un générateur de G. Si $u = us$, l'élément u est nécessairement multiple de la norme N, donc d'augmentation 0 ou l. Si donc $2 \leqslant n(u) \leqslant l - 1$, on a $u \neq us$. Groupant ensemble les $s^i u$, $0 \leqslant i \leqslant l - 1$, on obtient $\mathrm{Tr}(x^u)$; comme $n(u) \geqslant 2$, on a $x^u \in \mathfrak{p}_L^{s_n}$, d'où $\mathrm{Tr}(x^u) \in \mathrm{Tr}(\mathfrak{p}_L^{s_n})$, ce qui achève la démonstration.

PROPOSITION 4. *Pour tout entier $n \geqslant 0$, on a* $\mathrm{N}(U_L^{\psi(n)}) \subset U_K^n$ *et* $\mathrm{N}(U_L^{\psi(n)+1}) \subset U_K^{n+1}$.

Nous démontrerons cette proposition un peu plus loin. Notons tout de suite qu'elle permet de définir, par passage au quotient, des homomorphismes

$$\mathrm{N}_n : U_L^{\psi(n)}/U_L^{\psi(n)+1} \to U_K^n/U_K^{n+1} \quad (n \geqslant 0).$$

Pour préciser ces homomorphismes, on identifiera comme d'habitude U_K/U_K^1 (resp. U_L/U_L^1) à $\mathbf{K}^*$ (resp. à $\mathbf{L}^* = \mathbf{K}^*$), ainsi que U_K^n/U_K^{n+1} (resp. U_L^n/U_L^{n+1}) à $\mathbf{K}$ (resp. à $\mathbf{L} = \mathbf{K}$), ces derniers isomorphismes provenant eux-mêmes du choix d'une uniformisante π' (resp. π) de L (resp. K). Compte tenu de ces identifications, on a :

PROPOSITION 5. (i) *Pour $n = 0$, l'application $\mathrm{N}_0 : \mathbf{K}^* \to \mathbf{K}^*$ est donnée par $\mathrm{N}_0(\xi) = \xi^l$. Si $t \neq 0$, cette application est injective. Si $t = 0$, son noyau est cyclique d'ordre l, et égal à l'image de G par l'application $\theta_0 : G \to U_L/U_L^1$ définie au Chap.* IV, § 2.

(ii) *Pour $1 \leqslant n < t$, l'application $\mathrm{N}_n : \mathbf{K} \to \mathbf{K}$ est donnée par $\mathrm{N}_n(\xi) = \alpha_n \xi^p$, avec $\alpha_n \in \mathbf{K}^*$; elle est injective.*

(iii) *Pour $1 \leqslant n = t$, l'application $\mathrm{N}_n : \mathbf{K} \to \mathbf{K}$ est donnée par $\mathrm{N}_n(\xi) = \alpha\xi^p + \beta\xi$, avec $\alpha, \beta \in \mathbf{K}^*$. Son noyau est cyclique d'ordre $p = l$, et égal à $\theta_t(G)$, où $\theta_t : G \to U_L^t/U_L^{t+1}$ est l'application définie au Chap.* IV, § 2.

(iv) *Pour $n > t$, l'application $\mathrm{N}_n : \mathbf{K} \to \mathbf{K}$ est donnée par $\mathrm{N}_n(\xi) = \beta_n \xi$, avec $\beta_n \in \mathbf{K}^*$; elle est bijective.*

On va démonter simultanément les propositions 4 et 5. Il y a quatre cas à considérer :

(i) *On a $n = 0$.*

Il est trivial que $\mathrm{N}(U_L) \subset U_K$, $\mathrm{N}(U_L^1) \subset U_K^1$, et que $\mathrm{N}_0(\xi) = \xi^l$. Si $t \neq 0$, on a $l = p$, et N_0 est injective. Si $t = 0$, on a $l \neq p$, et le noyau de N_0 est d'ordre $\leqslant l$; mais $\theta_0(G)$ est formé des classes dans $\mathbf{K}^*$ des $s(\pi)/\pi$, et on a évidemment $\mathrm{N}(s(\pi)/\pi) = 1$, ce qui prouve que $\theta_0(G)$ est contenu dans $\mathrm{Ker}(\mathrm{N}_0)$, et lui est donc égal.

(ii) *On a $1 \leqslant n < t$.*

Puisque $t \geqslant 1$, on a $l = p$. De plus $\psi(n) = n$. Soit alors $x \in \mathfrak{p}_L^n$; on a $\mathrm{N}(x) \in \mathfrak{p}_K^n$ puisque $v_L = v_K \circ \mathrm{N}$. D'après le lemme 4, on a $\mathrm{Tr}(x) \in \mathfrak{p}_K^r$, avec

$$r = \left[\frac{(t+1)(l-1)+n}{l}\right] = \left[n + 2 - \frac{2}{l}\right] \geqslant n + 1.$$

Un calcul analogue montre que $\mathrm{Tr}(\mathfrak{p}_L^{s_n}) \in \mathfrak{p}_K^{n+1}$. D'après le lemme 5, on a donc :

$$\mathrm{N}(1 + x) \equiv 1 + \mathrm{N}(x) \mod \mathfrak{p}_K^{n+1}.$$

Comme $N(x) \in \mathfrak{p}_K^n$, cette formule montre bien que N applique U_L^n dans U_K^n et U_L^{n+1} dans U_K^{n+1}. De plus, si l'on pose $x = u\pi^n$, on a $N(x) \equiv u^p N(\pi)^n \bmod. \mathfrak{p}_K^{n+1}$, et, en posant $N(\pi)^n = a_n \pi'^n$, ceci donne :

$$N(1 + u\pi^n) \equiv 1 + a_n u^p \pi'^n \bmod. \mathfrak{p}_K^{n+1}$$

d'où $N_n(\xi) = \alpha_n \xi^p$, α_n désignant l'image de a_n dans K^*.

(iii) *On a* $1 \leqslant n = t$.

Ici encore, $l = p$, et $\psi(t) = t$. Soit $x \in \mathfrak{p}_L^t$. Un calcul analogue au précédent montre que :

$$N(1 + x) \equiv 1 + \mathrm{Tr}(x) + N(x) \bmod. \mathfrak{p}_K^{t+1}.$$

D'après le lemme 4, on a $\mathrm{Tr}(x) \in \mathfrak{p}_K^t$, et $\mathrm{Tr}(x) \in \mathfrak{p}_K^{t+1}$ si $x \in \mathfrak{p}_L^{t+1}$. Il en résulte bien que N applique U_L^t dans U_K^t et U_L^{t+1} dans U_K^{t+1}. Pour déterminer N_t, il suffit de calculer $N(1 + u\pi^t)$, avec $u \in A_K$; si l'on pose $\mathrm{Tr}(\pi^t) = b\pi'^t$ et $N(\pi)^t = a\pi'^t$, on obtient :

$$N(1 + u\pi^t) \equiv 1 + (bu + au^p)\,\pi'^t \bmod. \mathfrak{p}_K^{t+1}$$

c'est-à-dire $N_t(\xi) = \beta\xi + \alpha\xi^p$, α et β désignant les images de a et de b dans K. Il est clair que $\alpha \neq 0$. Si β était nul, N_t serait injectif; or son noyau contient $\theta_t(G)$ qui est cyclique d'ordre p (cela se voit comme dans le cas (i)); donc $\beta \neq 0$, et comme le noyau de N_t est d'ordre $\leqslant p$, cela achève de démontrer la proposition 5 dans le cas considéré.

(iv) *On a* $n \geqslant t$.

Ici $\psi(n) = t + l(n - t)$. Si $x \in \mathfrak{p}_L^{\psi(n)}$, le lemme 4 montre que $\mathrm{Tr}(x) \in \mathfrak{p}_K^n$, et comme $N(x) \in \mathfrak{p}_K^{\psi(n)}$ qui est contenu dans $\mathfrak{p}_K^{n+1}$, on obtient la formule :

$$N(1 + x) \equiv 1 + \mathrm{Tr}(x) \bmod. \mathfrak{p}_K^{n+1}.$$

On en conclut, comme précédemment, que N applique $U_L^{\psi(n)}$ dans U_K^n, $U_L^{\psi(n)+1}$ dans U_K^{n+1}, et que $N_n(\xi) = \beta_n \xi$. Si l'on avait $\beta_n = 0$, on aurait $\mathrm{Tr}(\mathfrak{p}_L^{\psi(n)}) \subset \mathfrak{p}_K^{n+1}$, ce qui serait en contradiction avec le lemme 4. On a donc $\beta_n \neq 0$, ce qui achève la démonstration des propositions 4 et 5.

Corollaire 1. *L'homomorphisme* N_n *est injectif pour tout* n, *sauf pour* $n = t$, *auquel cas on a une suite exacte* :

$$0 \longrightarrow G \xrightarrow{\theta_t} U_L^t/U_L^{t+1} \xrightarrow{N_t} U_K^t/U_K^{t+1}.$$

C'est évident.

Corollaire 2. *L'homomorphisme* N_n *est surjectif pour* $n > t$, *et, si* K *est parfait, pour* $n < t$. *Si* K *est algébriquement clos, il est surjectif pour tout* n.

C'est évident.

Corollaire 3. *On a* $N(U_L^{\psi(n)}) = U_K^n$ *pour* $n > t$, *et* $N(U_L^{\psi(n)+1}) = U_K^{n+1}$ *pour* $n \geqslant t$. *Lorsque* K *est algébriquement clos, ces égalités ont lieu pour tout* n.

On filtre $U_L^{\psi(n)}$ par les $U_L^{\psi(m)}$, et U_K^n par les U_K^m; par passage au quotient, on en déduit des homomorphismes

$$U_L^{\psi(m)}/U_L^{\psi(m+1)} \to U_K^m/U_K^{m+1}$$

qui sont composés de N_m et de la projection canonique

$$U_L^{\psi(m)}/U_L^{\psi(m+1)} \to U_L^{\psi(m)}/U_L^{\psi(m)+1}.$$

Si $m > t$, le corollaire 2 montre que ces homomorphismes sont surjectifs, et le lemme 2 montre alors que $N : U_L^{\psi(n)} \to U_K^n$ est surjectif. On raisonne de même si K est algébriquement clos et n quelconque. Quant à la formule $N(U_L^{\psi(n)+1}) = U_K^{n+1}$, elle résulte simplement de la proposition 4, et du fait que $U_L^{\psi(n)+1}$ contient $U_L^{\psi(n+1)}$.

COROLLAIRE 4. *On a* $N(U_L^{\psi(v)}) = U_K^v$ *si* v *est un nombre réel* $> t$ *ou si* K *est algébriquement clos.*

En effet, supposons que $n < v \leqslant n + 1$, où n est un entier. On a

$$\psi(n) < \psi(v) \leqslant \psi(n + 1).$$

Si m est le plus petit entier $\geqslant \psi(v)$, on en déduit :

$$\psi(n) + 1 \leqslant m \leqslant \psi(n + 1).$$

On a $U_K^v = U_K^{n+1}$, $U_L^{\psi(v)} = U_L^m$, et le cor. 3 montre que $NU_L^m = U_K^{n+1}$, c.q.f.d.

COROLLAIRE 5. *Si* $t = 0$, $\mathrm{Coker}(N_t) = K^*/K^{*l}$. *Si* $t \neq 0$, $\mathrm{Coker}(N_t)$ *est isomorphe à* $K/\wp(K)$, *avec* $\wp(\xi) = \xi^p - \xi$.

Si $t = 0$, on a vu que $N_t(\xi) = \xi^l$, d'où la première assertion. Si $t \neq 0$, il nous faut montrer que $\mathrm{Coker}(N_t)$ est isomorphe à $\mathrm{Coker}(\wp)$. Or, on a :

$$N_t(\xi) = \alpha\xi^p + \beta\xi, \qquad \text{avec} \qquad \alpha,\ \beta \neq 0$$

et de plus il existe un élément non nul η dans le noyau de N_t. On peut donc écrire :

$$N_t(\xi) = \alpha\eta^p((\xi/\eta)^p - \xi/\eta) = \gamma\wp(\xi/\eta) \qquad (\gamma \neq 0),$$

d'où $\mathrm{Im}(N_t) = \gamma\mathrm{Im}(\wp)$, ce qui démontre le résultat cherché.

COROLLAIRE 6. *Si* K *est parfait,* $N : U_L/U_L^n \to U_K/U_K^n$ *est un isomorphisme pour tout* $n \leqslant t$.

D'après les corollaires 1 et 2, N_n est surjectif pour $n < t$. Le corollaire en résulte par récurrence sur n, en utilisant le lemme 1.

COROLLAIRE 7. *Si* K *est parfait, les trois homomorphismes canoniques suivants sont des isomorphismes* :

$$\mathrm{Coker}(N_t) \leftarrow U_K^t/N(U_L^t) \to U_K/NU_L \to K^*/NL^*$$

a) On applique le lemme 1 au diagramme:

$$\begin{array}{ccccccc} 0 & \longrightarrow & U_L^{i+1} & \longrightarrow & U_L^i & \longrightarrow & U_L^i/U_L^{i+1} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & U_K^{i+1} & \longrightarrow & U_K^i & \longrightarrow & U_K^i/U_K^{i+1} \longrightarrow 0. \end{array}$$

Comme $N(U_L^{i+1}) = U_K^{i+1}$, on en déduit bien que $U_K^i/N(U_L^i) \to \mathrm{Coker}(N_i)$ est un isomorphisme.

b) On applique le lemme 1 au diagramme :

$$\begin{array}{ccccccc} 0 & \longrightarrow & U_L^i & \longrightarrow & U_L & \longrightarrow & U_L/U_L^i \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & U_K^i & \longrightarrow & U_K & \longrightarrow & U_K/U_K^i \longrightarrow 0. \end{array}$$

Compte tenu du corollaire 6, on en déduit bien que $U_K^i/N(U_L^i) \to U_K/NU_L$ est un isomorphisme.

c) On applique le lemme 1 au diagramme :

$$\begin{array}{ccccccc} 0 & \longrightarrow & U_L & \longrightarrow & L^* & \longrightarrow & \mathbf{Z} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & f \downarrow \\ 0 & \longrightarrow & U_K & \longrightarrow & K^* & \longrightarrow & \mathbf{Z} \longrightarrow 0. \end{array}$$

Comme $f = 1$, on en déduit bien que $U_K/NU_L \to K^*/NL^*$ est un isomorphisme.

Remarque. Lorsque $\mathbf{K}$ est un corps fini, on montre facilement que $\mathbf{K}^*/\mathbf{K}^{*l}$ (resp. $\mathbf{K}/\wp(\mathbf{K})$) est cyclique d'ordre l si l est premier à la caractéristique p de $\mathbf{K}$ (resp. si $l = p$). Combinant les corollaires 5 et 7, on en déduit que K^*/NL^* *est cyclique d'ordre* l; nous reviendrons là-dessus au Chap. XIII.

§ 4. *Extension du corps résiduel dans une extension totalement ramifiée*

Soit L/K une extension finie totalement ramifiée. Nous supposerons que son corps résiduel $\mathbf{L} = \mathbf{K}$ est un corps *parfait.*

Soit $\mathbf{K}'$ une extension finie de $\mathbf{K}$, et soit K' l'extension non ramifiée de K correspondante (cf. Chap. III, § 5). Les extensions L/K et K'/K sont *linéairement disjointes.* En effet, si l'on note L' leur composé, on a $e(L'/K) \geqslant e(L/K) = [L : K]$ et

$$f(L'/L) \geqslant f(K'/K) = [K' : K]$$

d'où

$$[L' : K] \geqslant [L : K].[K' : K].$$

On peut donc identifier L' à $K' \otimes_K L$, et l'on voit que L'/L est non ramifiée, et d'extension résiduelle $\mathbf{K}'/\mathbf{K}$. Nous dirons que L'/K' *se déduit de* L/K *par extension du corps*

résiduel de K *à* K'. C'est là une opération analogue à celle de *l'extension du corps de base* en géométrie algébrique (c'est même plus qu'une analogie, cf. Greenberg [25]). Soit π_K (resp. π_L) une uniformisante de K (resp. L); c'est aussi une uniformisante de K' (resp. L'). Supposons à partir de maintenant que L/K soit *galoisienne*, de groupe de Galois G; il en est alors de même de L'/K', et les groupes de ramification de G et les homomorphismes θ_i du Chap. IV sont *les mêmes* pour L/K et L'/K' (on est tenté de dire que ce sont des invariants « géométriques »).

Considérons plus particulièrement le cas où G est *cyclique de degré premier l*. Pour tout $n \geqslant 0$, on a des homomorphismes

$$N_n : U_L^{\psi(n)}/U_L^{\psi(n)+1} \to U_K^n/U_K^{n+1}$$
$$N'_n : U_{L'}^{\psi(n)}/U_{L'}^{\psi(n)+1} \to U_{K'}^n/U_{K'}^{n+1}.$$

Occupons-nous seulement du cas $n \geqslant 1$ (le cas $n = 0$ se traite de même). Au moyen des uniformisantes π_K et π_L, on peut identifier les quatre groupes ci-dessus à K, K, K' et K' respectivement. Les homomorphismes N_n et N'_n sont ainsi transformés en des homomorphismes

$$N_n : K \to K$$
$$N'_n : K' \to K'.$$

Ces homomorphismes sont des polynômes (de degré 1 ou p, suivant la valeur de n) dont les coefficients ont été déterminés au cours de la démonstration des propositions 4 et 5. Cette détermination montre que les coefficients en question *sont les mêmes pour* N_n *et* N'_n [dans le langage de la géométrie algébrique, cela signifie qu'on a pour chaque $n \geqslant 1$ un homomorphisme $v_n : G_a \to G_a$ rationnel sur K, et que N'_n est la restriction de v_n aux points de G_a rationnels sur K' — pour $n = 0$, le groupe additif G_a est remplacé par le groupe multiplicatif G_m]. Voici une application simple de cette remarque :

PROPOSITION 6. *Sous les hypothèses ci-dessus, soit x un élément de* K*. *Il existe alors une extension* K'/K, *de degré* $\leqslant l$, *telle que x soit une norme dans l'extension étendue* L'/K' *correspondante.*

D'après le corollaire 7 à la prop. 5, on peut supposer que $x \in U_K^1$. Dans ce cas, pour que x soit une norme, il faut et il suffit que sa classe ξ dans U_K^1/U_K^{1+1} soit de la forme $N_l(\eta)$, avec $\eta \in U_L^1/U_L^{1+1}$. Or, comme le degré de N_l est l, il existe un tel η dans une extension K'/K de degré $\leqslant l$; l'image de x dans Coker (N'_l) est alors nulle, et en appliquant à nouveau le cor. 7 à la prop. 5, on voit que x est une norme dans L'/K', c.q.f.d.

Remarque. La démonstration ci-dessus prouve en fait que, si x n'est pas une norme, l'extension K'/K est unique et c'est une extension cyclique de degré l.

Lorsqu'on passe à la limite sur K', on obtient comme limite inductive des corps K' (resp. L') le corps K_{nr} (resp. L_{nr}) *extension maximale non ramifiée de* K (*resp.* L); ici encore $L_{nr} = L \otimes_K K_{nr}$.

COROLLAIRE. *Sous les hypothèses ci-dessus, on a* $N(L_{nr}^*) = K_{nr}^*$.

En effet, si $x \in K_{nr}^*$, il existe une extension finie K_0/K telle que x appartienne à l'extension K_0 correspondante. En appliquant la proposition 6 à L_0/K_0 et à x, on voit alors bien que $x \in N(L_{nr}^*)$.

[*Variante.* Comme les corps résiduels des complétés $\hat{L}_{nr}$ et $\hat{K}_{nr}$ sont algébriquement clos, le cor. 3 à la prop. 5 montre qu'il existe $y \in \hat{L}_{nr}^*$ tel que $Ny = x$. Comme y est limite d'éléments de L_{nr}^*, on en déduit que, pour tout entier v, il existe $z_v \in L_{nr}^*$ tel que $Nz_v = x.u_v$, avec $u_v \in U_{\hat{K}_{nr}}$. Si $v \geqslant t + 1$, u_v est une norme (cor. 2 à la prop. 5), donc x est aussi une norme.]

Les extensions de K_{nr} qui sont de la forme L_{nr} donnent « essentiellement toutes » les extensions de K_{nr}. Pour préciser ce point, démontrons d'abord le lemme général suivant :

LEMME 6. *Soit* L *un corps, réunion d'une famille filtrante croissante de sous-corps* $\{L_i\}_{i \in I}$, *et soit* M *une extension de* L, *de degré fini* n. *Il existe alors un indice* $i \in I$ *et une extension* M_i *de* L_i, *de degré* n, *linéairement disjointe de* L *sur* L_i, *et telle que* $M_iL = M$. *Si* M_i *et* M_j *vérifient toutes deux ces conditions, il existe* $k \geqslant i, j$ *tel que* $M_iL_k = M_jL_k$. *Si* M *est séparable* (*resp. galoisienne*), M_i *peut être choisie séparable* (*resp. galoisienne*) *sur* L_i.

(En d'autres termes, les extensions finies de L sont limites inductives d'extensions finies des L_i.)

Soit $\{m_\alpha\}$, $\alpha = 1, \ldots, n$, une base de M sur L; on a

$$m_\alpha . m_\beta = \sum c_{\alpha\beta}^\gamma m_\gamma, \qquad \text{avec } c_{\alpha\beta}^\gamma \in L.$$

On choisit i assez grand pour que les $c_{\alpha\beta}^\gamma$ appartiennent à L_i. L'algèbre M_i définie par ces constantes de structure est évidemment telle que $M_i \otimes_{L_i} L = M$; c'est donc un corps, vérifiant les conditions cherchées. L'assertion concernant l'unicité se démontre de même. Si M/L est séparable, les m_α sont linéairement indépendants sur $L^{p^{-1}}$, donc *a fortiori* sur $L_i^{p^{-1}}$, ce qui montre que M_i/L_i est séparable. Enfin, si M/L est galoisien, les transformés $s(M_i)$ de M_i par les éléments $s \in G(M/L)$ sont tels que $s(M_i)L = M$; il existe donc $j \geqslant i$ tel que $s(M_i).L_j = M_iL_j$, et en posant $M_j = M_iL_j$, on obtient une extension galoisienne M_j/L_j répondant à la question.

LEMME 7. *Soit* K *un corps complet pour une valuation discrète, et de corps résiduel* $\mathbf{K}$ *parfait. Soit* K_{nr} *l'extension maximale non ramifiée de* K, *et soit* E *une extension finie de* K_{nr}, *de degré* n. *Il existe alors une sous-extension finie* K' *de* K_{nr} *et une extension* E'/K' *de degré* n, *linéairement disjointe de* K_{nr} *sur* K', *et telle que* $E = E' . K_{nr}$. *L'extension* E'/K' *est alors totalement ramifiée, et* E *s'identifie à* E'_{nr}. *Si* E *est séparable* (*resp. galoisienne*), *on peut choisir* E'/K' *séparable* (*resp. galoisienne*).

Le corps résiduel $\mathbf{K}_{nr}$ de K_{nr} est une clôture algébrique de $\mathbf{K}$. Soit $\{\mathbf{K}_i\}_{i \in I}$ l'ensemble des sous-extensions finies de $\mathbf{K}_{nr}$, et soit $\{K_i\}_{i \in I}$ l'ensemble des sous-extensions correspondantes de K_{nr}. La famille $\{K_i\}$ vérifie les hypothèses du lemme 6. L'existence de E'/K' en résulte. Le fait que E' soit linéairement disjointe de K_{nr} montre que son corps résiduel est égal à $\mathbf{K}$ (sinon en effet E' contiendrait une extension non ramifiée K''/K' distincte de L', et ne serait pas linéairement disjointe

de K_{nr}); on a donc $E'_{nr} = E$. Les autres assertions du lemme sont conséquences de celles du lemme 6.

Nous pouvons maintenant démontrer le résultat que nous avions en vue :

PROPOSITION 7. *Soit* K *un corps complet pour une valuation discrète, et de corps résiduel* $\mathbf{K}$ *parfait. Soit* K_{nr} *l'extension maximale non ramifiée de* K, *et soient* $F \supset E \supset K_{nr}$ *deux extensions finies de* K_{nr}, *avec* F/E *séparable. On a alors* $N(F^*) = E^*$.

Quitte à augmenter F, on peut supposer que F/E est galoisienne. D'après le lemme 7, il existe une sous-extension finie K′ de K_{nr} telle que $F = F'_{nr}$, $E = E'_{nr}$, où $F' \supset E' \supset K'$ sont linéairement disjoints de $K_{nr} = K'_{nr}$ sur K′, et où F′/E′ est galoisienne. Comme $\mathbf{F}' = \mathbf{E}' = \mathbf{K}'$, l'extension F′/E′ est totalement ramifiée et son groupe de Galois est donc résoluble (Chap. IV, § 2); par dévissage on est ramené au cas où il est cyclique de degré premier, auquel cas la proposition résulte du corollaire à la proposition 6.

Exercice. Montrer que la prop. 7 reste valable lorsqu'on supprime l'hypothèse de séparabilité sur F/E. (Traiter directement le cas radiciel, en s'aidant du théorème de structure du Chap. II, § 4.)

§ 5. *Polynômes multiplicatifs et polynômes additifs*

Soit k un corps, d'exposant caractéristique p. Un polynôme $P \in k[X]$ est dit *multiplicatif* si $P(XY) = P(X).P(Y)$, X et Y étant deux indéterminées, et si $P(1) = 1$. Un tel polynôme est nécessairement un *monôme* X^h; on posera $h = d(P)$. De plus, si $h = h_0 p^r$, avec $(h_0, p) = 1$, on dira que h_0 est le *degré séparable de* P, et on le notera $d_s(P)$. Le noyau de l'homomorphisme

$$P : k^* \to k^*$$

est l'ensemble des racines $d_s(P)$-ièmes de l'unité contenues dans k; c'est un groupe fini d'ordre divisant $d_s(P)$. Si P et Q sont deux polynômes multiplicatifs, il en est de même de leur composé $P \circ Q$, et l'on a

$$d(P \circ Q) = d(P).d(Q), \qquad d_s(P \circ Q) = d_s(P).d_s(Q).$$

Un polynôme $P \in k[X]$ est dit *additif* si $P(X + Y) = P(X) + P(Y)$. Si k est de caractéristique zéro, on a $P(X) = aX$, $a \in k$. Sinon, on vérifie facilement que P est combinaison linéaire de monômes X^{p^h} à exposants puissances de p. Si $P \neq 0$, on peut l'écrire de façon unique sous la forme :

$$P = X^{p^h} P', \qquad \text{avec} \qquad P' = a_0 X + \cdots + a_k X^{p^k}, \qquad a_0,\ a_k \neq 0.$$

Le degré $d(P)$ de P est égal à p^{h+k}; l'entier p^k est appelé le *degré séparable* de P, et noté $d_s(P)$.

Le noyau de l'homomorphisme

$$P : k \to k$$

est égal à celui de P'; c'est un sous-groupe additif de k d'ordre divisant $d_s(P)$. De plus, comme P' est séparable, on peut écrire (dans la clôture algébrique de k) :

$$P' = a_k \prod_{P(\xi)=0} (X - \xi)$$

ce qui montre que le noyau de P est d'ordre $d_s(P)$ si k contient les racines de P'. Si P et Q sont deux polynômes additifs, il en est de même de $P \circ Q$, et

$$d(P \circ Q) = d(P).d(Q), \qquad d_s(P \circ Q) = d_s(P).d_s(Q).$$

[Les polynômes additifs ne sont autres que les k-endomorphismes du groupe algébrique G_a; ils forment un anneau dont la structure a été étudiée par Ore [50]; voir aussi Whaples [69, 70].]

§ 6. *Le cas galoisien totalement ramifié*

Dans ce paragraphe, on suppose que l'extension L/K est galoisienne et totalement ramifiée. On a donc $\bar{L} = \bar{K}$. On note ψ la fonction définie au Chap. IV, § 3.

PROPOSITION 8. *Pour tout entier* $n \geqslant 0$, *on a* $N(U_L^{\psi(n)}) \subset U_K^n$ *et* $N(U_L^{\psi(n)+1}) \subset U_K^{n+1}$.

Nous démontrerons cette proposition un peu plus loin.

Comme dans le cas cyclique de degré premier, la proposition 8 permet de définir des homomorphismes :

$$N_0 : K^* \to K^*$$
$$N_n : K \to K, \quad n \geqslant 1.$$

PROPOSITION 9. *Pour* $n = 0$ (*resp.* $n \neq 0$), *l'homomorphisme* N_n *est induit par un polynôme multiplicatif* (*resp. additif*) *non constant* P_n *tel que* :

$$d(P_n) = \mathrm{Card}\,(G_{\psi(n)}) \qquad \text{et} \qquad d_s(P_n) = (G_{\psi(n)} : G_{\psi(n)+1}) = \psi'_d(n)/\psi'_g(n).$$

La suite :

$$0 \longrightarrow G_{\psi(n)}/G_{\psi(n)+1} \xrightarrow{\theta} U_L^{\psi(n)}/U_L^{\psi(n)+1} \xrightarrow{N_n} U_K^n/U_K^{n+1}$$

est exacte.

[L'homomorphisme θ fait correspondre à $s \in G_{\psi(n)}$ la classe de $s(\pi)/\pi$, où π est une uniformisante de L, cf. Chap. IV, § 2.]

Nous raisonnerons par récurrence sur l'ordre de G. Le cas $G = \{1\}$ est trivial. Si $G \neq \{1\}$, comme c'est un groupe résoluble (Chap. IV, § 2), il admet un quotient cyclique d'ordre premier. Il existe donc une sous-extension K'/K de L/K telle que K'/K soit cyclique d'ordre premier l. D'après l'hypothèse de récurrence (resp. les propositions 4 et 5), les propositions à démontrer sont vraies pour L/K' (resp. pour K'/K). Si l'on pose :

$$n' = \psi_{K'/K}(n), \qquad n'' = \psi_{L/K'}(n'),$$

on a donc :

$$N_{L/K'}(U_L^{v'}) \subset U_{K'}^{v'} \qquad \text{et} \qquad N_{K'/K}(U_{K'}^{v'}) \subset U_K^v$$

d'où, puisque $N_{L/K} = N_{K'/K} \circ N_{L/K'}$, $N(U_L^{v'}) \subset U_K^v$, ce qui démontre la première des inclusions de la prop. 8, puisque $\psi_{L/K} = \psi_{L/K'} \circ \psi_{K'/K}$. La seconde inclusion se démontre de même.

En ce qui concerne la proposition 9, on remarque que N_n se factorise en :

$$U_L^{v'}/U_L^{v'+1} \xrightarrow{N''} U_{K'}^{v'}/U_{K'}^{v'+1} \xrightarrow{N'} U_K^v/U_K^{v+1}$$

où N'' et N' sont définis respectivement par $N_{L/K'}$ et $N_{K'/K}$. Si N'' et N' sont induits par les polynômes multiplicatifs (resp. additifs) P'' et P', N_n est donc induit par leur composé $P_n = P' \circ P''$, qui est bien multiplicatif (resp. additif). Le degré séparable d du polynôme P_n est égal au produit des degrés séparables d' et d'' de P' et P''. L'hypothèse de récurrence, appliquée à l'extension L/K', montre que

$$d'' = (\psi_{L/K'})'_{d/g}(n')$$

en convenant de noter $f'_{d/g}$ le quotient f'_d/f'_g de la dérivée à droite par la dérivée à gauche. On a de même :

$$d' = (\psi_{K'/K})'_{d/g}(n).$$

Comme $\psi_{L/K} = \psi_{L/K'} \circ \psi_{K'/K}$, la formule donnant la dérivée d'une fonction composée montre que l'on a :

$$d = (\psi_{L/K})'_{d/g}(n).$$

Compte tenu des propriétés de ψ (cf. Chap. IV, § 3, prop. 12 et 13), ceci peut aussi s'écrire :

$$d = (G_{\psi(n)} : G_{\psi(n)+1}).$$

On démontre de même la formule :

$$d(P_n) = \text{Card } (G_{\psi(n)}).$$

D'autre part, d'après ce qui a été dit au § 5, le noyau de N_n est d'ordre un diviseur de $d_s(P_n)$; comme $N(s(\pi)/\pi) = 1$, ce noyau contient l'image de θ, image dont l'ordre est justement $d_s(P_n)$, on vient de le voir. On a donc bien $\text{Im}\,(\theta) = \text{Ker}\,(N_n)$, ce qui achève la démonstration.

COROLLAIRE 1. *N_n est injectif si et seulement si $G_{\psi(n)} = G_{\psi(n)+1}$.*

C'est évident.

COROLLAIRE 2. *N_n est surjectif dans chacun des trois cas suivants :*

(i) *K est algébriquement clos,*

(ii) *K est parfait, et $G_{\psi(n)} = G_{\psi(n)+1}$,*

(iii) $G_{\psi(n)} = \{1\}$.

En effet, dans le cas (i), P_n est un polynôme non constant, dans le cas (ii), $P_n = cX^{p^n}$, et dans le cas (iii), $P_n = cX$.

COROLLAIRE 3. *On a* $N(U_L^{\psi(n)}) = U_K^n$ *si* $G_{\psi(n)} = \{1\}$, *et* $N(U_L^{\psi(n)+1}) = U_K^{n+1}$ *si* $G_{\psi(n+1)} = \{1\}$. *Lorsque* K *est algébriquement clos, ces égalités ont lieu pour tout* $n \geqslant 0$.

La démonstration est la même que celle du corollaire 3 dn § 3.

COROLLAIRE 4. *Soit* v *un nombre réel* $\geqslant 0$. *On a* $N(U_L^{\psi(v)}) = U_K^v$ *si* $G_{\psi(v)} = \{1\}$, *ou bien si* K *est algébriquement clos.*

Même démonstration que pour le corollaire 4 du § 3.

Remarques. 1) Nous avons procédé par « dévissage », à partir du cas cyclique de degré premier; on peut aussi opérer directement, comme le fait Hasse [33].
2) Si K est fini, les conditions de la proposition 9 ne suffisent pas nécessairement à déterminer les polynômes P_n. Toutefois, il existe un choix des P_n qui est invariant par extension résiduelle (cela résulte de la démonstration), et ce choix est évidemment unique; les polynômes P_n correspondants seront dits *canoniques*.

La proposition 6 s'étend d'elle-même au cas considéré ici. Nous nous bornerons à l'énoncer :

PROPOSITION 10. *Supposons* K *parfait, et soit* $x \in K^*$. *Il existe alors une extension* K'/K *de degré* $\leqslant [L : K]$, *telle que* x *soit une norme dans l'extension étendue* L'/K' *correspondante.*

Cette proposition apporte une précision supplémentaire à la prop. 7 du § 4.

Exercice. En supposant K parfait, étendre les résultats de ce § au cas d'une extension finie L/K quelconque.

§ 7. *Application : démonstration du théorème de Hasse-Arf*

Il s'agit du théorème suivant (cf. Chap. IV, § 3) :

THÉORÈME 1. *Soit* K *un corps complet pour une valuation discrète, soit* L *une extension abélienne finie de* K, *de groupe de Galois* G; *on suppose que l'extension résiduelle* $\bar{L}/\bar{K}$ *est séparable. Si* v *est un saut de la filtration* $\{G^v\}$ *de* G, *alors* v *est entier.*

(Dire que v est un *saut* signifie par définition que $G^{v+\varepsilon} \neq G^v$ pour tout $\varepsilon > 0$.)

L'énoncé ci-dessus utilise la numérotation *supérieure* des groupes de ramification. Si l'on traduit en termes de la numérotation *inférieure*, on obtient :

THÉORÈME 1'. *Les hypothèses étant celles du théorème* 1, *si* μ *est un entier tel que*

$$G_\mu \neq G_{\mu+1}$$

alors $\varphi_{L/K}(\mu)$ *est un entier.*

La proposition suivante est un cas particulier du théorème 1' :

PROPOSITION 11. *Soit* L/K *une extension cyclique, totalement ramifiée, de groupe de Galois* G, *et soit* μ *le plus grand entier tel que* $G_\mu \neq \{1\}$. *Alors* $\varphi_{L/K}(\mu)$ *est un entier.*

Inversement, cette proposition *entraîne* le théorème 1. En effet, soit L/K une extension vérifiant les hypothèses du théorème 1, et soit v un saut de la filtration $\{G_v\}$. Quitte à remplacer G par son sous-groupe d'inertie, on peut supposer que L/K est totalement ramifiée. Posons $G' = G_v$ et soit G'' le groupe de ramification suivant (on a donc $G'' = G_{v+\varepsilon}$ pour tout $\varepsilon > 0$ assez petit). Par hypothèse, $G' \neq G''$. Décomposant G/G'' en produit de groupes cycliques, on voit qu'il existe un groupe quotient cyclique H de G/G'' tel que l'image H' de G' dans H soit $\neq \{1\}$. Le groupe H est groupe de Galois d'une sous-extension L'/K de L/K. D'après le théorème de Herbrand, on a $H_v = H'$ et $H_{v+\varepsilon} = \{1\}$ pour tout $\varepsilon > 0$, et la prop. 11 montre donc que v est un entier, c.q.f.d.

Reste donc à *démontrer la proposition* 11. Nous noterons w la valuation discrète de L, et nous choisirons une uniformisante π de L. Nous poserons

$$r = \text{Card } (G), \qquad r' = \text{Card } (G_1), \qquad k = r/r'.$$

Nous ferons choix d'un générateur s de G; le groupe G_1 est alors engendré par $\sigma = s^k$. Nous utiliserons la notation exponentielle x^s pour désigner $s(x)$. Enfin, nous supposerons que le corps résiduel $K = \bar{L}$ *n'est pas le corps premier* : on peut toujours se ramener à ce cas, quitte à faire une extension du corps résiduel, cf. § 4.

Soit V l'ensemble des $x \in L^*$ tels que $Nx = 1$. D'après un résultat classique de Hilbert (cf. Bourbaki, *Alg.*, Chap. V, § 11, th. 3) V est l'ensemble des y^{s-1}, $y \in L^*$. Soit W le sous-groupe de V formé des y^{s-1} avec $y \in U_L$.

Lemme 8. *Le groupe* V/W *est cyclique.*

En effet, l'application $y \to y^{s-1}$ définit par passage au quotient un homomorphisme de $L^*/U_L = \mathbf{Z}$ *sur* V/W.

[En fait, V/W est isomorphe à G, cf. exer.]

Soit m un entier $\geqslant 0$. Nous poserons :

$$V_m = V \cap U_L^m, \qquad W_m = W \cap U_L^m.$$

On a $W_m \subset V_m$; le groupe V_m/W_m s'identifie à un sous-groupe de V/W, et les V_m/W_m forment une filtration décroissante de V/W.

Lemme 9. *On a* $V_m = W_m$ *pour* m *assez grand.*

Soit t un élément de L tel que $\text{Tr}(t) = 1$, et soit $m_0 = -w(t)$. Soit $x \in V_m$, avec $m > m_0$; nous allons montrer que x appartient à W_m. Formons la « résolvante de Lagrange-Hilbert » (Bourbaki, *loc. cit.*) :

$$y = \sum_{i=0}^{i=r-1} x^{1+s+\cdots+s^{i-1}} . t^i.$$

Puisque $\text{Tr}(t) = 1$, on peut écrire :

$$y - 1 = \sum_{i=0}^{i=r-1} (x^{1+s+\cdots+s^{i-1}} - 1) . t^i$$

d'où $w(y-1) > 0$ et $y \in U_L^1$. Comme $Nx = 1$, on a $y^{1-s} = x$, ce qui montre bien que x appartient à W_m.

Nous allons maintenant nous occuper des quotients successifs $V_m/V_{m+1}W_m$ de la filtration $\{V_n/W_n\}$.

LEMME 10. *Si $\varphi(m)$ est entier et si $G_m = G_{m+1}$, alors $V_m = V_{m+1}$.*

Posons $n = \varphi(m)$, de telle sorte qu'on a $m = \psi(n)$. Soit $x \in V_m$, et soit $\bar{x}$ l'image de x dans U_L^m/U_L^{m+1}. Il est clair que $\bar{x}$ appartient au noyau de l'homomorphisme

$$N_n : U_L^m/U_L^{m+1} \to U_K^n/U_K^{n+1}$$

défini au paragraphe précédent. D'après la proposition 9, le noyau de N_n est isomorphe à G_n/G_{n+1}, donc nul. On a alors $\bar{x} = 0$, i.e. $x \in V_{m+1}$.

LEMME 11. *Soit m un entier $\geqslant 1$. Si l'image de W_m dans U_L^m/U_L^{m+1} est non nulle, cette image est égale à U_L^m/U_L^{m+1} tout entier.*

Soit x un élément de W_m n'appartenant pas à U_L^{m+1}. On a $x = y^{s-1}$, avec $y \in U_L$. Quitte à multiplier y par un élément de U_K (ce qui ne change pas y^{s-1}), on peut supposer que $y \in U_L^1$, autrement dit que $y = 1 + z$, avec $w(z) \geqslant 1$. Pour tout $a \in A_K$, posons $y_a = 1 + az$ et $x_a = y_a^{s-1}$. On a :

$$x_a - 1 = \frac{s(y_a) - y_a}{y_a} = \frac{a(s(y) - y)}{y_a} = a\frac{y}{y_a}(x - 1).$$

Comme $y/y_a \in U_L^1$, on voit que x_a appartient à W_m, et que son image $\bar{x}_a$ dans U_L^m/U_L^{m+1} est égale à $\bar{a}.\bar{x}$, où $\bar{a}$ désigne l'image de a dans $K = \bar{L}$; comme tout élément de U_L^m/U_L^{m+1} est de la forme $\bar{a}.\bar{x}$, cela démontre le lemme.

LEMME 12. *Soit n un entier tel que $G_{\psi(n+1)} = \{1\}$. Soit m un entier tel que*

$$n < \varphi(m) < n + 1.$$

Alors les images de V_m et de W_m dans U_L^m/U_L^{m+1} sont toutes deux égales à U_L^m/U_L^{m+1}.

Soit $\bar{x} \in U_L^m/U_L^{m+1}$, et soit $x \in U_L^m$ un représentant de $\bar{x}$. On a

$$\psi(n) < m < \psi(n+1), \qquad \text{d'où } m \geqslant \psi(n) + 1.$$

D'après la prop. 8, on a $Nx \in U_K^{n+1}$, et le cor. 3 à la prop. 9 montre qu'il existe $y \in U_L^{\psi(n+1)}$ tel que $Ny = Nx$. En posant $x' = xy^{-1}$, on trouve un représentant de $\bar{x}$ qui appartient à V. Le groupe V_m s'envoie donc bien *sur* U_L^m/U_L^{m+1}. Quant à W_m, son image dans U_L^m/U_L^{m+1} est un sous-groupe H_m de ce groupe; comme V_m/W_m est cyclique (puisque sous-groupe de V/W), le quotient de U_L^m/U_L^{m+1} par H_m est également cyclique. Mais U_L^m/U_L^{m+1} est isomorphe au groupe additif K, et ce dernier *n'est pas* un groupe cyclique, puisqu'on a pris la précaution de supposer que K n'est pas le corps premier. On a donc nécessairement $H_m \neq 0$, et le lemme précédent montre que $H_m = U_L^m/U_L^{m+1}$, ce qui démontre le lemme.

LEMME 13. *Soit m un entier, et soit $n+1$ le plus petit entier $\geqslant \varphi(m)$. Si $G_{\psi(n+1)} = \{1\}$, on a $V_m = W_m$.*

Montrons d'abord que $V_m = V_{m+1}W_m$. Si $\varphi(m)$ est entier, on a $n+1 = \varphi(m)$, $\psi(n+1) = m$, et notre assertion résulte du lemme 10. Si $\varphi(m)$ n'est pas entier, on a $n < \varphi(m) < n+1$, et le lemme 12 montre que V_m et W_m ont même image dans U_L^m/U_L^{m+1}, d'où évidemment $V_m = V_{m+1}W_m$.

En appliquant ce qui précède à $m+1$, on trouve $V_{m+1} = V_{m+2}W_{m+1}$, d'où $V_m = V_{m+2}W_m$, et de proche en proche $V_m = V_{m+k}W_m$ pour tout $k \geqslant 0$. Si l'on prend k assez grand, on a $V_{m+k} = W_{m+k}$ (lemme 9), d'où $V_m = W_{m+k}W_m = W_m$, ce qui démontre le lemme.

Nous pouvons maintenant démontrer la proposition 11. Supposons que $\varphi(\mu)$ ne soit pas entier, et soit $\nu+1$ le plus petit entier $\geqslant \varphi(\mu)$. On a $\mu < \psi(\nu+1)$, d'où $G_{\psi(\nu+1)} = \{1\}$, et d'après le lemme précédent on a $V_\mu = W_\mu$. Soit $\sigma = s^k$ le générateur de G_μ défini au début de la démonstration, et posons $x = \pi^{\sigma-1}$. Il est clair que x appartient à V_μ; puisque $V_\mu = W_\mu$, il existe donc $y \in U_L$ tel que $\pi^{\sigma-1} = y^{s-1}$. Mais l'on a :

$$\sigma - 1 = (s-1)(1 + s + \cdots + s^{k-1})$$

et en posant $z = y^{-1}\pi^{1+s+\cdots+s^{k-1}}$, on trouve $z^{s-1} = 1$, d'où $z \in K^*$. Comme L/K est totalement ramifiée, on en déduit $w(z) \equiv 0 \pmod{r}$; comme $w(y) = 0$, $w(\pi) = 1$, cela donne $k \equiv 0 \pmod{r}$, ce qui est absurde, c.q.f.d.

Exercice. On conserve les notations et les hypothèses de la démonstration de la prop. 11.

a) Montrer que, si $\varphi(m)$ est entier, on a $W_m \subset V_{m+1}$, et V_m/V_{m+1} est isomorphe à G_m/G_{m+1}.

b) Montrer que, si $\varphi(m)$ n'est pas entier, on a $V_m = V_{m+1}W_m$.

c) Montrer que l'application $t \to \pi^{t-1}$ définit par passage au quotient un isomorphisme du groupe G filtré par les $\{G_n\}$ sur le groupe V/W filtré par les $\{V_n/W_n\}$.

CHAPITRE VI

REPRÉSENTATION D'ARTIN

§ 1. *Représentations et caractères*

(Il s'agit d'un rappel de définitions et de résultats bien connus. Pour les démonstrations, le lecteur pourra par exemple consulter M. Hall [30], Chap. XVI.)

Soit G un groupe fini, d'ordre g. Une fonction f sur G, à valeurs complexes, est dite *centrale* si $f(sts^{-1}) = f(t)$ pour $s, t \in G$. Soit V un espace vectoriel de dimension finie sur $\mathbf{C}$, et soit $\mathbf{GL}(V)$ le groupe des automorphismes de V; on appelle *représentation linéaire* de G dans V un homomorphisme $\rho : G \to \mathbf{GL}(V)$. Si $s \in G$, $\rho(s)$ est un endomorphisme de V, et sa *trace* $\mathrm{Tr}(\rho(s))$ est définie. On posera

$$\chi_\rho(s) = \mathrm{Tr}(\rho(s)).$$

La fonction χ_ρ est une fonction centrale sur G, que l'on appelle le *caractère* de la représentation ρ; elle détermine ρ à un isomorphisme près. On a $\chi_\rho(s^{-1}) = \overline{\chi_\rho(s)}$. L'entier $\chi(1)$ est appelé le *degré* de ρ; c'est la dimension de V.

La fonction constante égale à 1 sera notée 1_G ou simplement 1. C'est le caractère de la représentation *unité* de G (dim. $V = 1$ et $\rho(s) = 1$ pour tout $s \in G$).

Le caractère de la représentation *régulière* de G sera noté r_G. On a $r_G(1) = g$, $r_G(s) = 0$ pour $s \neq 1$. La représentation unité se plonge dans la représentation régulière; le quotient s'appelle la représentation *d'augmentation* de G; son caractère sera noté u_G. On a $r_G = u_G + 1_G$.

Un caractère χ est dit *irréductible* si la représentation correspondante est *irréductible*. Toute fonction centrale φ s'écrit de manière unique comme combinaison linéaire

$$\varphi = \sum c_\chi \chi, \qquad c_\chi \in \mathbf{C}$$

de caractères irréductibles. Pour que φ soit le caractère d'une représentation linéaire de G, il faut et il suffit que les c_χ soient des entiers $\geqslant 0$.

Les coefficients c_χ peuvent se calculer de la manière suivante : posons, si φ et ψ sont deux fonctions centrales sur G,

$$(\varphi, \psi) = \frac{1}{g} \sum_{s \in G} \varphi(s)\, \overline{\psi(s)}.$$

On a alors $(\chi, \chi) = 1$, $(\chi, \chi') = 0$ si χ et χ' sont des caractères irréductibles distincts d'où :

$$c_\chi = (\varphi, \chi).$$

(En d'autres termes, les caractères irréductibles χ forment une base orthonormale de l'espace hilbertien des fonctions centrales.) On a par exemple $r_G = \sum_\chi \chi(1)\,\chi$, $u_G = \sum_{\chi \neq 1} \chi(1)\,\chi$.

Soit maintenant $\alpha : H \to G$ un homomorphisme d'un groupe fini H dans le groupe G. Si φ est une fonction centrale sur G, la fonction $\alpha^*(\varphi) = \varphi \circ \alpha$ est une fonction centrale sur H; si φ est le caractère d'une représentation linéaire $\rho : G \to \mathbf{GL}(V)$, $\alpha^*(\varphi)$ est le caractère de la représentation $\rho \circ \alpha : H \to \mathbf{GL}(V)$. En sens inverse, soit ψ une fonction centrale sur H. On montre qu'il existe une fonction centrale $\alpha_*(\psi)$ sur G, et une seule, telle que l'on ait l'identité (dite « de Frobenius »)

$$(\varphi, \alpha_*(\psi)) = (\alpha^*(\varphi), \psi)$$

pour toute fonction centrale φ sur G. Si ψ est le caractère d'une représentation linéaire de H dans V, $\alpha_*(\psi)$ est le caractère de la représentation $\mathbf{C}[G] \otimes_{\mathbf{C}[H]} V$, obtenue à partir de V par extension des scalaires (représentation « induite »).

Nous appliquerons principalement ceci aux deux cas particuliers suivants :

a) H *est un sous-groupe de* G, *et* α *est l'injection canonique de* H *dans* G.

On écrit alors $\varphi|H$ (ou même simplement φ) au lieu de $\alpha^*(\varphi)$, et ψ^* au lieu de $\alpha_*(\psi)$ (fonction *induite*). Si $s \in G$, on a :

$$\psi^*(s) = \sum_{t \in G/H} \psi(tst^{-1})$$

en convenant que

$$\psi(tst^{-1}) = 0 \qquad \text{si } tst^{-1} \notin H.$$

b) G *est un quotient* H/N *de* H, *et* α *est la projection canonique de* H *sur* H/N. On écrit alors φ au lieu de $\alpha^*(\varphi)$, et $\psi^{\natural}$ au lieu de $\alpha_*(\psi)$. Si $s \in H/N$, on a :

$$\psi^{\natural}(s) = \frac{1}{\text{Card }(N)} \sum_{t \mapsto s} \psi(t).$$

Nous aurons à utiliser le résultat suivant :

THÉORÈME DE BRAUER. *Tout caractère d'un groupe fini* G *est combinaison* **Z***-linéaire de caractères* χ_i^* *induits par des caractères* χ_i *de degré* 1 *de sous-groupes* H_i *de* G.
(Un caractère de degré 1 d'un groupe H est simplement un homomorphisme de H dans le groupe multiplicatif $\mathbf{C}^*$.)

Pour la démonstration, voir Brauer-Tate [11].

§ 2. *Représentation d'Artin*

Soit L/K une extension galoisienne finie, de groupe de Galois G, vérifiant les hypothèses des chapitres IV et V. On posera $f = [L : K]$. Si s est un élément de G distinct de 1, on a défini au Chap. IV, § 1 l'entier positif $i_G(s)$. Posons :

$$a_G(s) = -f.i_G(s) \qquad \text{si } s \neq 1$$

$$a_G(1) = f\sum_{s\neq 1} i_G(s).$$

On a donc :

$$\sum_{s\in G} a_G(s) = 0, \quad \text{c'est-à-dire} \quad (a_G, 1_G) = 0.$$

THÉORÈME 1. *La fonction a_G est le caractère d'une représentation linéaire du groupe* G.

Il est clair que a_G est une fonction centrale. On peut donc l'écrire :

$$a_G = \sum c_\chi \chi$$

où χ parcourt l'ensemble des caractères irréductibles de G. On a :

$$c_\chi = (a_G, \chi) = \frac{1}{g}\sum_{s\in G} a_G(s)\chi(s^{-1})$$

$$= \frac{1}{g}\sum_{s\in G} a_G(s^{-1})\,\chi(s)$$

et comme $a_G(s^{-1}) = a_G(s)$, on voit que $c_\chi = (\chi, a_G)$.

De façon générale, si φ est une fonction centrale sur G, on posera :

$$f(\varphi) = (\varphi, a_G).$$

Le théorème 1 peut donc se reformuler de la manière suivante :

THÉORÈME 1'. *$f(\chi)$ est un entier $\geqslant 0$ si χ est un caractère de* G.

Avant de démontrer ces deux théorèmes, nous allons établir un certain nombre de propriétés des $f(\chi)$ et de a_G.

PROPOSITION 1. *La fonction a_G est égale à la fonction induite $(a_{G_0})^*$ par la fonction correspondante du groupe d'inertie G_0.*

Comme G_0 est invariant dans G, on a $(a_{G_0})^*(s) = 0 = a_G(s)$ si $s \notin G_0$. Si $s \in G_0$, $s \neq 1$, on a :

$$(a_{G_0})^*(s) = \sum_{t\in G/G_0} a_{G_0}(tst^{-1}) = -\sum_{t\in G/G_0} i_{G_0}(tst^{-1})$$

$$= -f.i_G(s) = a_G(s).$$

Le cas de $s = 1$ se traite de même.

[Cette proposition permettrait, si on le désirait, de ramener les théorèmes 1 et 1' au cas *totalement ramifié* $G = G_0$.]

PROPOSITION 2. *Soit* G_i *le* i*-ième groupe de ramification de* G, *soit* u_i *le caractère de la représentation d'augmentation de* G_i, *et soit* u_i^* *le caractère de* G *induit par* u_i. *On a* :

$$a_G = \sum_{i=0}^{\infty} \frac{1}{(G_0 : G_i)} u_i^*.$$

Posons $g_i = \text{Card}(G_i)$. Le raisonnement fait ci-dessus montre que $u_i^*(s) = 0$ si $s \notin G_i$, $u_i^*(s) = -g/g_i = -f.g_0/g_i$ si $s \in G_i$, $s \neq 1$, et $\sum_{s \in G} u_i^*(s) = 0$. Si alors $s \in G_k - G_{k+1}$, la somme de droite vaut $-f(k+1)$, et il en est de même de $a_G(s)$. Pour $s = 1$, l'égalité provient de ce que les deux membres sont orthogonaux à 1_G.

Si φ est une fonction centrale sur G, nous poserons :

$$\varphi(G_i) = \frac{1}{g_i} \sum_{s \in G_i} \varphi(s), \qquad g_i = \text{Card}(G_i).$$

COROLLAIRE 1. *Si* φ *est une fonction centrale sur* G, *on a* :

$$f(\varphi) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} (\varphi(1) - \varphi(G_i)).$$

Cela résulte de la proposition 2, compte tenu de ce que :

$$(\varphi, u_i^*) = (\varphi | G_i, u_i) = \varphi(1) - \varphi(G_i).$$

COROLLAIRE 2. *Si* χ *est un caractère de* G, $f(\chi)$ *est un nombre rationnel positif.*

En effet, la proposition 2 montre que $g_0 a_G$ est le caractère d'une représentation linéaire de G; donc $g_0 . f(\chi)$ est un entier $\geqslant 0$.

PROPOSITION 3. *Si* N *est un sous-groupe invariant du groupe* G, *on a* :

$$a_{G/N} = (a_G)^N.$$

Cela résulte de la proposition 3 du Chapitre IV.

COROLLAIRE. *Si* φ *est une fonction centrale sur* G/N, *et si* φ' *est la fonction centrale sur* G *correspondante, on a* $f(\varphi) = f(\varphi')$.

En effet $f(\varphi) = (\varphi, a_G^N) = (\varphi', a_G) = f(\varphi')$.

PROPOSITION 4. *Soit* H *un sous-groupe de* G *correspondant à la sous-extension* K'/K, *et soit* $\mathfrak{d}_{K'/K}$ *le discriminant de* K'/K. *On a* :

$$a_G | H = \lambda r_H + f_{K'/K} . a_H, \qquad \text{avec } \lambda = v_K(\mathfrak{d}_{K'/K}).$$

(On rappelle que r_H désigne le caractère de la représentation *régulière* de H.)

Si s est un élément de H distinct de 1, on a :

$$a_G(s) = -f_{L/K} i_G(s), \qquad a_H(s) = -f_{L/K'} i_H(s), \qquad r_H(s) = 0,$$

et comme $i_G(s) = i_H(s)$, cela donne bien

$$a_G(s) = \lambda r_H(s) + f_{K'/K} a_H(s).$$

Prenons maintenant $s = 1$. On a tout d'abord :

$$a_G(1) = f_{L/K} v_L(\mathfrak{D}_{L/K}) = v_K(\mathfrak{d}_{L/K})$$

d'après la proposition 4 du Chap. IV. De même, $a_H(1) = v_{K'}(\mathfrak{d}_{L/K'})$. La formule à démontrer s'écrit donc :

$$v_K(\mathfrak{d}_{L/K}) = [L : K']\, v_K(\mathfrak{d}_{K'/K}) + f_{K'/K} v_{K'}(\mathfrak{d}_{L/K'}),$$

et elle résulte de la formule de transitivité du discriminant (Chap. III, prop. 8) :

$$\mathfrak{d}_{L/K} = (\mathfrak{d}_{K'/K})^{[L : K']} . N_{K'/K}(\mathfrak{d}_{L/K'}).$$

COROLLAIRE. *Soit ψ un caractère de* H, *et soit ψ^* le caractère de* G *induit par ψ. On a :*

$$f(\psi^*) = v_K(\mathfrak{d}_{K'/K})\, \psi(1) + f_{K'/K} f(\psi).$$

En effet :

$$\begin{aligned} f(\psi^*) &= (\psi^*,\ a_G) = (\psi,\ a_G|H) \\ &= (\psi,\ r_H) + f_{K'/K}(\psi,\ a_H) \\ &= \lambda\psi(1) + f_{K'/K} f(\psi), \qquad \text{avec } \lambda = v_K(\mathfrak{d}_{K'/K}). \end{aligned}$$

PROPOSITION 5. *Soit χ un caractère de degré* 1 *de* G. *Soit c_χ le plus grand entier tel que la restriction de χ au groupe de ramification G_{c_χ} ne soit pas le caractère unité (si $\chi = 1_G$, on prend $c_\chi = -1$). On a alors :*

$$f(\chi) = \varphi_{L/K}(c_\chi) + 1.$$

(Pour la définition de la fonction $\varphi_{L/K}$, voir Chap. IV, § 3.)
Si $i \leqslant c_\chi$, on a $\chi(G_i) = 0$, d'où $\chi(1) - \chi(G_i) = 1$; si $i > c_\chi$, on a $\chi(G_i) = 1$, d'où $\chi(1) - \chi(G_i) = 0$. En appliquant le corollaire 1 à la proposition 2, on obtient donc :

$$f(\chi) = \sum_{i=0}^{i=c_\chi} \frac{g_i}{g_0} = \varphi_{L/K}(c_\chi) + 1.$$

COROLLAIRE. *Soit* H *le noyau de χ, soit* K' *la sous-extension de* L/K *correspondant à* H, *et soit c'_χ le plus grand entier tel que $(G/H)_{c'_\chi} \neq \{1\}$. On a $f(\chi) = \varphi_{K'/K}(c'_\chi) + 1$, et c'est un entier $\geqslant 0$.*

(Si H = G, on pose $c'_\chi = -1$.)

Le théorème de Herbrand (Chap. IV, lemme 5) montre que $c'_\chi = \varphi_{L/K'}(c_\chi)$. La formule $f(\chi) = \varphi_{K'/K}(c'_\chi) + 1$ résulte donc simplement de la transitivité des fonctions φ. Le fait que $\varphi_{K'/K}(c'_\chi)$ soit un entier résulte du théorème de Hasse-Arf (Chap. IV, § 3), puisque G/H est abélien.

Démonstration des théorèmes 1 *et* 1'. Il s'agit de prouver que, si χ est un caractère de G, $f(\chi)$ est un entier positif. On sait déjà (cor. 2 à la prop. 2) que c'est un nombre rationnel positif; reste à montrer que c'est un entier. D'après le théorème de Brauer rappelé au § 1, on a $\chi = \sum n_i \chi_i^*$, $n_i \in \mathbf{Z}$, les χ_i étant des caractères de degré 1 de sous-groupes H_i de G. On est donc ramené à montrer que $f(\chi^*)$ est entier si χ est un caractère de degré 1; or, sous ces hypothèses, $f(\chi)$ est entier (cor. à la prop. 5), et il en est donc de même de $f(\chi^*)$, d'après le corollaire de la proposition 4, c.q.f.d.

Remarques. 1) Le théorème 1 et sa démonstration sont dus à Artin [6], à cela près qu'il devait supposer le corps résiduel K *fini*, le théorème de Hasse-Arf n'étant alors démontré que dans ce cas. De plus, comme il ne disposait pas du théorème de Brauer, Artin commençait par se ramener au cas $G = G_1$, grâce à un théorème de Speiser (cf. Chap. IV, cor. 2 à la prop. 9); le groupe G étant un p-groupe, il est alors facile de prouver que tout caractère irréductible de G est induit par un caractère de degré 1 d'un sous-groupe, ce qui démontre (et précise) le théorème de Brauer dans ce cas particulier.

2) Comme on l'a vu, la démonstration du théorème d'Artin utilise de façon essentielle celui de Hasse-Arf; inversement, on déduit facilement le théorème de Hasse-Arf de celui d'Artin.

Terminologie. La représentation dont le théorème 1 affirme l'existence s'appelle la *représentation d'Artin* du groupe G attachée à l'extension L/K. On notera qu'elle n'est définie que par l'intermédiaire de son caractère, c'est-à-dire à un isomorphisme près; il serait très intéressant d'en obtenir une description directe; nous reviendrons là-dessus au § 4.

Si χ est un caractère de G, l'idéal $\mathfrak{p}_K^{f(\chi)}$ est appelé le *conducteur* de χ, et noté $\mathfrak{f}(\chi)$. Lorsque χ est un caractère de degré 1, correspondant à une sous-extension cyclique K'/K, et lorsque K est fini, $\mathfrak{f}(\chi)$ est bien le conducteur de l'extension K'/K, au sens de la théorie du corps de classes local (cf. Chap. XV); il en est de même si K est algébriquement clos (cf. [59], n° 3.7). Lorsque χ est un caractère irréductible de degré > 1, on n'a aucune interprétation de ce genre pour $\mathfrak{f}(\chi)$.

Exercice. Soit G^i le i-ième groupe de ramification de G en numérotation supérieure, et soit v_i^* le caractère de G induit par le caractère de la représentation d'augmentation de G^i.

a) Montrer que $a_G = \dfrac{1}{g_0} \sum_{n=0}^{\infty} v_{n/g_0}^*$.

b) Lorsque G est abélien, montrer que $a_G = \sum_{n=0}^{\infty} v_n^*$.

§ 3. *Globalisation*

Elle ne présente aucune difficulté. Indiquons rapidement comment on procède :

Soit L/K une extension finie galoisienne, de groupe de Galois G, soit A un anneau de Dedekind de corps des fractions K, et soit B sa fermeture intégrale dans L. On supposera que, si $\mathfrak{P}$ est un idéal premier non nul de B au-dessus d'un idéal premier $\mathfrak{p}$ de A, le corps résiduel $\mathbf{L}_{\mathfrak{P}} = \mathrm{B}/\mathfrak{P}$ est *séparable* sur $\mathbf{K}_{\mathfrak{p}} = \mathrm{A}/\mathfrak{p}$. Sous ces hypothèses, le complété $\hat{\mathrm{L}}_{\mathfrak{P}}$ est galoisien sur $\hat{\mathrm{K}}_{\mathfrak{p}}$, le groupe de Galois étant le groupe de décomposition $\mathrm{D}_{\mathfrak{P}}$. On peut appliquer à l'extension $\hat{\mathrm{L}}_{\mathfrak{P}}/\hat{\mathrm{K}}_{\mathfrak{p}}$ et au groupe $\mathrm{D}_{\mathfrak{P}}$ les définitions et les résultats des paragraphes 1 et 2. La fonction a correspondante sera notée $a_{\mathfrak{P}}$; elle est définie *a priori* sur $\mathrm{D}_{\mathfrak{P}}$, mais on la prolonge par zéro à G tout entier. On pose :

$$a_{\mathfrak{p}} = \sum_{\mathfrak{P}|\mathfrak{p}} a_{\mathfrak{P}}.$$

On vérifie tout de suite que $a_{\mathfrak{p}}$ est égale à $(a_{\mathfrak{P}})^*$, pour un choix quelconque de $\mathfrak{P}$ au-dessus de $\mathfrak{p}$. Il s'ensuit que $a_{\mathfrak{p}}$ est le caractère d'une représentation de G (que l'on appelle la *représentation d'Artin* attachée à $\mathfrak{p}$ et à l'extension L/K), et que cette représentation est induite par la représentation d'Artin de l'un des groupes de décomposition $\mathrm{D}_{\mathfrak{P}}$, pour $\mathfrak{P}|\mathfrak{p}$. Si χ est un caractère de G, on pose :

$$f(\chi, \mathfrak{p}) = (\chi, a_{\mathfrak{p}}) = f(\chi|\mathrm{D}_{\mathfrak{P}}).$$

Si $\mathfrak{p}$ est non ramifié, on a évidemment $f(\chi, \mathfrak{p}) = 0$. On peut donc former l'idéal produit :

$$\mathfrak{f}(\chi) = \prod_{\mathfrak{p}} \mathfrak{p}^{f(\chi, \mathfrak{p})}$$

que l'on appelle le *conducteur* du caractère χ; lorsque l'on veut préciser davantage, on écrit $\mathfrak{f}(\chi, \mathrm{L}/\mathrm{K})$ au lieu de $\mathfrak{f}(\chi)$. Les propriétés démontrées au § 2 se traduisent de la manière suivante :

PROPOSITION 6. (*a*) $\mathfrak{f}(\chi + \chi') = \mathfrak{f}(\chi).\mathfrak{f}(\chi')$, $\mathfrak{f}(1) = (1)$.
(*b*) *Si* K'/K *est une sous-extension de* L/K, *correspondant au sous-groupe* H *de* G, *et si* ψ *est un caractère de* H, *on a* :

$$\mathfrak{f}(\psi^*, \mathrm{L}/\mathrm{K}) = \mathfrak{d}_{\mathrm{K}'/\mathrm{K}}^{\psi(1)}.\mathrm{N}_{\mathrm{K}'/\mathrm{K}}(\mathfrak{f}(\psi, \mathrm{L}/\mathrm{K}')).$$

(*c*) *Si* K'/K *est galoisienne, et si* χ *est un caractère de* G/H, *on a* :

$$\mathfrak{f}(\chi, \mathrm{L}/\mathrm{K}) = \mathfrak{f}(\chi, \mathrm{K}'/\mathrm{K}).$$

Appliquons (*b*) au cas où $\psi = 1_{\mathrm{H}}$; le caractère induit ψ^* sera noté $s_{\mathrm{G/H}}$; c'est le caractère de la représentation de G définie par les opérations de G sur l'espace homogène G/H. Comme $\mathfrak{f}(\psi) = (1)$, on obtient :

COROLLAIRE 1. *On a* $\mathfrak{d}_{\mathrm{K}'/\mathrm{K}} = \mathfrak{f}(s_{\mathrm{G/H}}, \mathrm{L}/\mathrm{K})$.

En décomposant $s_{G/H}$ en combinaison linéaire de caractères irréductibles, on en déduit une *décomposition du discriminant* $\mathfrak{d}_{K'/K}$ *en produit de conducteurs*. Si par exemple $H = |1|$, on a $s_{G/H} = r_G$, et l'on obtient la « Führerdiskriminantenproduktformel » d'Artin et Hasse :

COROLLAIRE 2. *On a* $\mathfrak{d}_{L/K} = \prod f(\chi)^{\chi(1)}$, *où* χ *parcourt l'ensemble des caractères irréductibles de* G.

Si G est *abélien*, cette formule devient tout simplement :

$$\mathfrak{d}_{L/K} = \prod f(\chi).$$

Le cas des corps de nombres. Supposons que K soit un corps de nombres (c'est-à-dire une extension finie de $\mathbf{Q}$), et que A soit l'anneau des entiers de K. Considérons l'idéal de $\mathbf{Z}$ défini par la formule :

$$c(\chi,\ L/K) = \mathfrak{d}_{K/0}^{\chi(1)} . N_{K/0}(f(\chi,\ L/K)).$$

Il est engendré par un entier > 0, que nous noterons $c(\chi, L/K)$. En appliquant la prop. 6, et la transitivité du discriminant, on voit qu'il vérifie les propriétés suivantes :

(a) $\quad c(\chi + \chi', L/K) = c(\chi, L/K) . c(\chi', L/K), \qquad c(1, L/K) = |d_{K/0}|$

(b) $\quad c(\psi^*, L/K) = c(\psi, L/K')$

(c) $\quad c(\chi, L/K) = c(\chi, K'/K)$

les notations étant celles de la prop. 6.

Ces propriétés d'invariance sont identiques à celles des fonctions L d'Artin (cf. [5]) ; en fait, $c(\chi, L/K)$ intervient dans le terme « exponentiel » de l'équation fonctionnelle de $L(\chi, L/K)$, cf. [5], n° 7.

§ 4. *Représentations d'Artin et homologie (cas des courbes algébriques)*

Soit k un corps algébriquement clos de caractéristique p, soit Y une courbe algébrique projective, non singulière, connexe, définie sur k, et soit G un groupe fini d'automorphismes de Y. Soit $X = Y/G$ la courbe quotient. Soit L (resp. K) le corps des fonctions rationnelles sur Y (resp. sur X) ; l'extension L/K est galoisienne, de groupe de Galois G. De plus, chaque point $Q \in Y$ a un anneau local qui est un anneau de valuation discrète, de corps des fractions L, de corps résiduel k ; soit v_Q la valuation correspondante. On définit de même v_P si $P \in X$. Le sous-groupe D_Q de G formé des $s \in G$ tels que $s(Q) = Q$ est appelé le *groupe de décomposition* de Q ; si $\hat{L}_Q$ (resp. $\hat{K}_P$) est le complété de L (resp. K) pour la valuation v_Q (resp. v_P), l'extension $\hat{L}_Q/\hat{K}_P$ est galoisienne de groupe de Galois D_Q (la situation est analogue à celle du § 3, et pourrait d'ailleurs s'y ramener). On peut appliquer à $\hat{L}_Q/\hat{K}_P$ les constructions du § 2, et l'on obtient des fonctions i et a, que l'on note i_Q et a_Q. Si t est une uniformisante locale en Q, on a donc :

$$i_Q(s) = v_Q(s(t) - t) \qquad \text{si } s \in D_Q, \qquad s \neq 1.$$

On peut ici donner une interprétation *géométrique* de $i_G(s)$: si Γ_s désigne le graphe de s dans $Y \times Y$, $i_Q(s)$ est égal à la multiplicité de $Q \times Q$ dans l'intersection $\Delta . \Gamma_s$, (Δ désignant la diagonale de Y); la vérification est immédiate.

Comme au § 3, on étend a_Q par 0 en dehors de D_Q, et l'on pose :

$$a_P = \sum_{Q \to P} a_Q \qquad \text{pour tout } P \in X.$$

Si l'on choisit un point $Q \in Y$ au-dessus de X, on vérifie que $a_P = (a_Q)^*$; donc a_P est le caractère d'une représentation de G, que l'on appelle la *représentation d'Artin* attachée à P.

On va maintenant *interpréter homologiquement la somme directe des représentations d'Artin correspondant aux divers points* $P \in X$. Soit l un nombre premier fixé, distinct de p. On définit avec Weil ([66], voir aussi [57], n° 5) les *groupes d'homologie l-adiques* de Y : $H_0(Y)$, $H_1(Y)$, $H_2(Y)$, en prenant $H_0(Y) = H_2(Y) = \mathbf{Z}_l$, et $H_1(Y) = T_l(J)$ (groupe de Tate de la jacobienne J de Y). Ce sont des $\mathbf{Z}_l$-modules libres de type fini, sur lesquels opère le groupe G. Ils définissent donc des représentations, dont nous noterons les caractères h_i, $i = 0, 1, 2$. Nous poserons $h = h_0 - h_1 + h_2$. L'entier $E(Y) = h(1)$ est la *caractéristique d'Euler-Poincaré* de Y; si g_Y est le genre de Y, on a $E(Y) = 2 - 2g_Y$. On définit de même E(X).

PROPOSITION 7. *Avec les notations ci-dessus, on a*

$$h = E(X) . r_G - \sum_{P \in X} a_P.$$

Pour $s \neq 1$, on doit montrer que $h(s) = -\sum a_P(s) = \sum i_Q(s)$, et comme $\sum i_Q(s) = \deg(\Delta . \Gamma_s)$, la formule n'est qu'un cas particulier de la *formule de Lefschetz* (cf. par exemple [40], p. 161). Pour $s = 1$, c'est la formule de Hurwitz.

COROLLAIRE. *On a* $\sum_{P \in X} a_P = h_1 + E(X) . r_G - 2 . 1_G$.

En effet, on a $h_0 = h_2 = 1_G$.

Remarque. Les résultats qui précèdent sont dus à Weil, au langage près (cf. [66], § V). Ils montrent notamment que la somme des représentations d'Artin A_P attachées aux divers points P de X est *rationnelle sur* $\mathbf{Q}_l$ (c'est-à-dire peut être réalisée par une représentation matricielle à coefficients dans $\mathbf{Q}_l$); cela suggère que chaque A_P doit être rationnelle sur $\mathbf{Q}_l$, $l \neq p$, et c'est effectivement ce que l'on peut démontrer, sans même que l'on ait à se borner au cas d'égale caractéristique, cf. [57], [78]. Par contre, ni la représentation H_1, ni les représentations d'Artin ne sont en général rationnelles sur Q (cf. [57], n° 4 et 6), ce qui ôte l'espoir de trouver une définition « triviale » de ces représentations.

TROISIÈME PARTIE

COHOMOLOGIE DES GROUPES

-

CHAPITRE VII

GÉNÉRALITÉS

Ce chapitre et le suivant sont consacrés à des rappels de définitions et de résultats sur l'homologie et la cohomologie des groupes; pour plus de détails, le lecteur se reportera à Cartan-Eilenberg [13], Grothendieck [26] ou Lang [93].

§ 1. *G-modules*

Soit G un groupe, noté multiplicativement, et soit A un groupe abélien, noté additivement. On dit que G *opère à gauche sur* A si l'on s'est donné un homomorphisme $G \to \mathrm{Aut}(A)$, où Aut (A) désigne le groupe des automorphismes de A. Il revient au même de se donner une application $(s, x) \to s.x$ de $G \times A$ dans A vérifiant les identités :

$$1.a = a$$
$$s.(a + a') = s.a + s.a'$$
$$(s.t).a = s.(t.a).$$

Dans ces conditions, si Λ désigne l'algèbre $\mathbf{Z}[G]$ du groupe G sur $\mathbf{Z}$, on munit A d'une structure de Λ-module unitaire à gauche en posant :

$$(\Sigma n_s s)a = \Sigma n_s(s.a).$$

Inversement, si A est un Λ-module unitaire à gauche (nous dirons plus brièvement un Λ-module), le groupe G opère par $a \to s.a$ sur A, cf. Bourbaki, *Alg.*, Chap. II, § 7, n° 9. Au lieu de dire « Λ-module », nous dirons souvent « G-module ».

Si A et A′ sont deux G-modules, une application $f : A \to A'$ est appelée un G-*homomorphisme* (ou parfois simplement un *homomorphisme*) si c'est un homomorphisme de groupes abéliens, et si elle commute aux opérations de G (ce qui revient à dire que c'est un homomorphisme de Λ-modules). Les G-homomorphismes forment un groupe noté $\mathrm{Hom}_G(A, A')$. Pour ces homomorphismes, les G-modules forment une *catégorie abélienne* au sens de Grothendieck [26]. Comme dans toute catégorie abélienne, on a la notion d'objet *projectif* et d'objet *injectif* : un G-module

A est dit projectif si le foncteur $\mathrm{Hom}_G(A, A')$ est exact par rapport à A'; un G-module A' est dit injectif si le foncteur $\mathrm{Hom}_G(A, A')$ est exact par rapport à A. A côté de ces notions (souvent trop restrictives pour les applications), on est amené à introduire les notions suivantes :

Un G-module A sera dit *induit* s'il est de la forme $\Lambda \otimes X$, où X est un groupe abélien (le produit tensoriel étant pris sur $\mathbf{Z}$). Il revient au même de dire que A contient un sous-groupe X tel que $A = \sum_{s \in G} s.X$, la somme étant *directe*. Tout G-module *est quotient d'un module induit*. De façon plus précise, soit A un G-module, et soit A_0 le groupe abélien sous-jacent à A; formons le G-module induit $\Lambda \otimes A_0$. Tout élément de $\Lambda \otimes A_0$ est somme d'éléments de la forme $s \otimes x$, $x \in A_0$, $s \in G$, et en appliquant un tel élément sur $s.x \in A$, on définit un homomorphisme

$$\pi : \Lambda \otimes A_0 \to A.$$

Il est clair que π est un G-*homomorphisme surjectif*; de plus, si l'on pose $\varphi(a) = 1 \otimes a$, on a $\pi \circ \varphi = 1$ (mais, bien entendu, φ n'est pas un G-homomorphisme si $A \neq 0$) On a ainsi une *façon canonique* d'écrire un G-module comme quotient d'un G-module induit. Si π identifie A à un facteur direct de $\Lambda \otimes A_0$ (comme G-module), on dit que A est *relativement projectif* (c'est ce que Cartan-Eilenberg appellent « faiblement » projectif dans [13], Chap. X, § 8 — ce sont les modules $(\Lambda, \mathbf{Z})$-projectifs dans la théorie relative de Hochschild [35]). Les modules relativement projectifs peuvent aussi être caractérisés comme les *facteurs directs des modules induits*.

Remarque. Si A et B sont deux G-modules, on peut munir $A \otimes B$ d'une structure de G-module grâce à la formule :

$$s.(a \otimes b) = s.a \otimes s.b.$$

En particulier, $\Lambda \otimes A$ est muni d'une telle structure de G-module. Le G-module obtenu *est isomorphe* à $\Lambda \otimes A_0$: en effet, on vérifie facilement que $s \otimes a \to s \otimes s.a$ se prolonge en un G-isomorphisme de $\Lambda \otimes A_0$ sur $\Lambda \otimes A$. Dans la suite, cela nous permettra d'écrire à volonté $\Lambda \otimes A$ ou $\Lambda \otimes A_0$.

Dualement, un G-module A sera dit *co-induit* s'il est de la forme $\mathrm{Hom}_{\mathbf{Z}}(\Lambda, X)$, où X est un groupe abélien. On montre comme ci-dessus que tout G-module A se plonge canoniquement dans le G-module co-induit $\mathrm{Hom}_{\mathbf{Z}}(\Lambda, A_0)$. Les facteurs directs de modules co-induits seront appelés *relativement injectifs* (ce sont les modules « faiblement » injectifs de Cartan-Eilenberg, *loc. cit.*). Lorsque G est *fini*, on voit tout de suite que $\mathrm{Hom}_{\mathbf{Z}}(\Lambda, X)$ est isomorphe à $\Lambda \otimes_{\mathbf{Z}} X$, de sorte que les notions de modules induits et co-induits coïncident; il en est de même des notions de modules relativement injectifs et relativement projectifs (cf. [13], p. 233, prop. 1.1).

Exercice. Soit k un anneau commutatif. Dans la définition des G-modules, remplacer le groupe abélien A par un k-module, et $\mathbf{Z}[G]$ par $k[G]$. Comment définit-on les modules induits et co-induits dans ce cadre?

§ 2. *Cohomologie des groupes*

Soit A un G-module, et soit A^G le sous-groupe de A formé des éléments invariants par G. Si $f : A \to B$ est un G-homomorphisme, f applique A^G dans B^G; on peut donc parler du *foncteur* A^G. C'est un foncteur additif exact à gauche : si l'on a une suite exacte de G-modules

$$0 \to A \to A' \to A''$$

la suite de groupes abéliens

$$0 \to A^G \to A'^G \to A''^G$$

est encore exacte.

Les *foncteurs dérivés droits* du foncteur A^G sont, par définition, les groupes de cohomologie de G à coefficients dans A; on les note $H^q(G, A)$, $q \geqslant 0$. Rappelons brièvement comment on peut les calculer :

Notons tout d'abord que A^G peut être identifié à $\mathrm{Hom}_G(\mathbf{Z}, A)$, le groupe $\mathbf{Z}$ étant considéré comme un G-module à opérateurs triviaux ($s.n = n$ pour tout $s \in G$). On a donc $H^q(G, A) = \mathrm{Ext}^q(\mathbf{Z}, A)$, puisque les Ext^q sont les foncteurs dérivés du foncteur $\mathrm{Hom} = \mathrm{Hom}_G$. Choisissons alors une résolution du G-module $\mathbf{Z}$ par des G-modules projectifs, c'est-à-dire une suite exacte :

$$\cdots \to P_i \to P_{i-1} \to \cdots \to P_0 \to \mathbf{Z} \to 0$$

où les P_i sont projectifs (par exemple libres sur A). Si l'on pose $K^i = \mathrm{Hom}_G(P_i, A)$, les K^i forment un complexe de cochaînes K, et l'on a :

$$H^q(G, A) = H^q(K)$$

ce qui donne un procédé de calcul de ces groupes; nous donnerons au paragraphe suivant une résolution libre explicite, la résolution « standard ». On doit considérer les $H^q(G, A)$ non pas seulement comme une suite de foncteurs, mais comme un « foncteur cohomologique » (cf. Grothendieck [26], n° 2.1); cela signifie que, pour chaque suite exacte de G-modules

$$0 \to A \to B \to C \to 0$$

et pour chaque entier $q \geqslant 0$, on a un homomorphisme

$$\delta : H^q(G, C) \to H^{q+1}(G, A)$$

tel que la suite (dite « suite exacte de cohomologie ») :

$$\cdots \to H^q(G, B) \to H^q(G, C) \xrightarrow{\delta} H^{q+1}(G, A) \to H^{q+1}(G, B) \to \cdots$$

soit exacte; de plus les δ dépendent « fonctoriellement » de la suite exacte donnée, en un sens évident. On écrit souvent d au lieu de δ.

Les propriétés suivantes caractérisent le foncteur cohomologique $\{H^q(G, \ ), \delta\}$:

(i) *On a* $H^0(G, A) = A^G$.

(ii) *On a* $H^q(G, A) = 0$ *si* $q \geqslant 1$, *et si* A *est injectif.*

[C'est là une caractérisation générale des foncteurs dérivés.]

On peut renforcer (ii) :

PROPOSITION 1. *Si* A *est relativement injectif, on a* $H^q(G, A) = 0$ *pour tout* $q \geqslant 1$.

Comme A est facteur direct d'un module co-induit, on est tout de suite ramené au cas où A lui-même est co-induit, c'est-à-dire où $A = \mathrm{Hom}_S(\Lambda, X)$, X étant un groupe abélien. Si B est un Λ-module, on a alors $\mathrm{Hom}_\Lambda(B, A) = \mathrm{Hom}_S(B, X)$. En appliquant cette formule au complexe introduit ci-dessus, on voit que

$$K^i = \mathrm{Hom}_S(P_i, X)$$

et $H^q(K)$ n'est donc pas autre chose que $\mathrm{Ext}^q_S(\mathbf{Z}, X)$, qui est évidemment nul pour $q \geqslant 1$.

COROLLAIRE. *Si* $0 \to A \to A^* \to A' \to 0$ *est une suite exacte de* G*-modules, avec* A^* *co-induit, on a*

$$H^q(G, A') = H^{q+1}(G, A) \qquad \textit{pour } q \geqslant 1.$$

Cela résulte de la suite exacte de cohomologie.

Le corollaire ci-dessus permet de « décaler » les groupes de cohomologie; on peut par exemple prendre $A^* = \mathrm{Hom}_{\mathbf{Z}}(\Lambda, A)$ cf. § 1.

§ 3. *Calcul de la cohomologie au moyen de cochaînes*

On obtient une résolution libre de $\mathbf{Z}$ en prenant pour G-module P_i le $\mathbf{Z}$-module libre L_i ayant pour base les systèmes $(g_0, \ldots, g_i)$ de $i + 1$ éléments de G, et en faisant opérer G sur L_i par translations :

$$s.(g_0, \ldots, g_i) = (sg_0, \ldots, sg_i).$$

L'homomorphisme $d : L_i \to L_{i-1}$ est défini par la formule

$$(*) \qquad d(g_0, \ldots, g_i) = \sum_{j=0}^{j=i} (-1)^j (g_0, \ldots, \hat{g}_j, \ldots, g_i)$$

où le symbole $\hat{}$ signifie que la lettre au-dessus duquel il se trouve doit être omise.

L'homomorphisme $L_0 \to \mathbf{Z}$ est défini par la condition d'appliquer chaque (g_0) sur $1 \in \mathbf{Z}$. Le fait que la suite $\cdots \to L_1 \to L_0 \to \mathbf{Z} \to 0$ ainsi obtenue soit exacte est bien connu (un simplexe est acyclique).

Si l'on choisit les L_j comme on vient de dire, un élément de $K^i = \mathrm{Hom}_\Lambda(L_i, A)$ s'identifie à une fonction $f(g_0, \ldots, g_i)$ définie sur $G \times G \times \cdots \times G$, à valeurs dans A, et qui vérifie la condition de « covariance » :

$$f(s.g_0, \ldots, s.g_i) = s.f(g_0, \ldots, g_i).$$

Le cobord de f est défini par une formule, transposée de (*), qu'il est inutile d'expliciter.

Une cochaîne covariante f est bien déterminée par sa restriction aux systèmes de la forme $(1, g_1, g_1g_2, \ldots, g_1 \ldots g_i)$. On est ainsi conduit à interpréter les éléments de K^i comme des « cochaînes non homogènes », qui sont des fonctions $f(g_1, \ldots, g_i)$ de i arguments, à valeurs dans A, et où le cobord df est donné par la formule suivante :

$$(**) \quad df(g_1, \ldots, g_{i+1}) = g_1 . f(g_2, \ldots, g_{i+1}) + \sum_{j=1}^{j=i} (-1)^j f(g_1, \ldots, g_j g_{j+1}, \ldots, g_{i+1}) + (-1)^{i+1} f(g_1, \ldots, g_i).$$

Le groupe $H^1(G, A)$.

La formule (**) montre qu'un 1-cocycle est une application f de G dans A vérifiant l'identité

$$f(gg') = g.f(g') + f(g).$$

On dit que f est un *homomorphisme croisé*. Un homomorphisme croisé est un cobord s'il existe $a \in A$ tel que $f(g) = g.a - a$ pour tout $g \in G$.

Lorsque G opère trivialement sur A, on a donc $H^1(G, A) = \mathrm{Hom}(G, A)$.

Le groupe $H^2(G, A)$.

Un 2-cocycle est une application f de $G \times G$ dans A vérifiant l'identité :

$$g.f(g', g'') - f(gg', g'') + f(g, g'g'') - f(g, g') = 0.$$

On dit que c'est un *système de facteurs*.

De telles fonctions se rencontrent dans la classification des *extensions de* G *par* A :

Soit E un groupe contenant A comme sous-groupe invariant, le quotient étant G; le groupe G opère alors par automorphismes intérieurs sur A (on suppose A commutatif, bien entendu), ce qui fournit un premier *invariant* de l'extension. Ces opérateurs étant connus, soit $s : G \to E$ une section (un « système de représentants »); si g, g' sont dans G, il est clair que $s(g).s(g')$ et $s(g.g')$ sont dans la même classe modulo A, et il existe donc un élément $f(g, g')$ de A tel que l'on ait :

$$s(g).s(g') = f(g, g').s(gg').$$

Il est clair que la connaissance de f permet d'écrire la loi de composition de E; en exprimant l'associativité de cette loi, on trouve, après un petit calcul, que f est un *système de facteurs*. Changer s modifie f par un cobord, et l'on peut construire une extension correspondant à un système de facteurs donné. On en conclut (voir les détails dans [13], Chap. XIV, § 4) que $H^2(G, A)$ *est l'ensemble des classes d'extensions de* G *par* A (les opérations de G sur A étant fixées).

Exercice. Soit f une cochaîne de degré n. On pose :

$$Tf(g_1, \ldots, g_n) = g_1 \ldots g_n . f(g_n^{-1}, \ldots, g_1^{-1}).$$

Démontrer l'identité $T(df) = (-1)^{n+1} d(Tf)$. En déduire que, si f est un cocycle, Tf est un cocycle cohomologue à f (resp. $-f$) si $\deg(f) \equiv 0, 3 \bmod 4$ (resp. si $\deg(f) \equiv 1, 2 \bmod 4$). Vérifier directement ce résultat si $\deg(f) \leqslant 2$.

§ 4. *Homologie*

Soit A un G-module, et soit DA le sous-groupe de A engendré par les $s.a - a$, $a \in A$, $s \in G$. Le quotient A/DA sera noté A_G; c'est le plus grand module quotient de A sur lequel G opère trivialement (alors que A^G est le plus grand sous-module jouissant de la même propriété).

Le foncteur A_G est additif, et exact à droite. Ses foncteurs dérivés gauches sont, par définition, les groupes d'homologie de G à coefficients dans A, notés $H_q(G, A)$. Ils forment un « foncteur homologique ». On a $H_0(G, A) = A_G = \mathbf{Z} \otimes_\Lambda A$, et $H_q(G, A) = \mathrm{Tor}_q^\Lambda(\mathbf{Z}, A)$. Si $\{P_i\}$ est une résolution projective de Z, les $H_q(G, A)$ s'identifient aux groupes d'homologie du complexe formé par les $P_i \otimes_\Lambda A$.

[Dans une formule du type $B \otimes_\Lambda A$, on considère B comme Λ-*module à droite* en posant $b.s = s^{-1}.b$.]

Le foncteur homologique $\{H_q(G, \ ), \partial\}$ est caractérisé par les deux propriétés suivantes :

(i) *On a* $H_0(G, A) = A_G$.

(ii) *On a* $H_q(G, A) = 0$ *si* $q \geqslant 1$ *et si* A *est projectif.*

Proposition 2. *Si* A *est relativement projectif, on a* $H_q(G, A) = 0$ *pour tout* $q \geqslant 1$.

La démonstration est tout à fait analogue à celle de la prop. 1. En particulier, un module *induit* a une homologie triviale, ce qui permet ici encore d'utiliser des méthodes de « décalage ».

La résolution libre de Z donnée au § précédent permet aussi une description explicite du complexe $L \otimes_\Lambda A$ des $L_i \otimes_\Lambda A$, donc aussi des $H_q(G, A)$. Le résultat est le suivant :

Un élément $x \in L_q \otimes_\Lambda A$ peut être identifié à une fonction $x(g_1, \ldots, g_q)$, à valeurs dans A, nulle pour presque tous les systèmes $(g_1, \ldots, g_q)$ (i. e. sauf pour un nombre fini d'entre eux). Le bord d est donné par la formule suivante :

$$\begin{aligned} dx(g_1, \ldots, g_{q-1}) = &\sum_{g \in G} g^{-1} x(g, g_1, \ldots, g_{q-1}) \\ &+ \sum_{j=1}^{j=q-1} (-1)^j \sum_{g \in G} x(g_1, \ldots, g_j g, g^{-1}, g_{j+1}, \ldots, g_{q-1}) \\ &+ (-1)^q \sum_{g \in G} x(g_1, g_2, \ldots, g_{q-1}, g). \end{aligned}$$

Lorsque $A = \mathbf{Z}$, sur lequel le groupe G opère trivialement, on a $H_1(G, \mathbf{Z}) = G/G'$ (G' désignant le groupe des commutateurs de G), cf. [13], p. 190. Comme cet isomorphisme jouera un rôle important dans la suite, nous allons rappeler brièvement comment on le définit :

Soit $\Lambda = \mathbf{Z}[G]$ l'algèbre de groupe de G, et soit $\pi : \Lambda \to \mathbf{Z}$ l'homomorphisme *d'augmentation*, c'est-à-dire l'homomorphisme qui applique $\sum n_s s \in \Lambda$ sur $\sum n_s \in \mathbf{Z}$.

Soit I_G le noyau de π; c'est le sous-groupe de Λ engendré par les éléments $i_s = s - 1$, pour s parcourant G. Si A est un G-module quelconque, on a par définition $H_0(G, A) = A/I_G A$. Considérons alors la suite exacte :

$$0 \to I_G \to \Lambda \xrightarrow{\pi} \mathbf{Z} \to 0.$$

On a $H_0(G, I_G) = I_G/I_G^2$, et l'image de $H_0(G, I_G)$ dans $H_0(G, \Lambda)$ est nulle. Comme d'autre part Λ est libre, on a $H_1(G, \Lambda) = 0$. La suite exacte d'homologie donne alors un isomorphisme

$$d : H_1(G, \mathbf{Z}) \to H_0(G, I_G) = I_G/I_G^2.$$

D'autre part, on vérifie tout de suite (cf. [13], *loc. cit.*) que $s \to i_s$ définit par passage au quotient un isomorphisme θ de G/G' sur I_G/I_G^2. On peut donc identifier $H_1(G, \mathbf{Z})$ et G/G' au moyen de l'isomorphisme $\theta^{-1} \circ d$, et c'est ce que nous ferons désormais.

§ 5. *Changement de groupe*

Soient G et G' deux groupes, soit $f : G' \to G$ un homomorphisme, et soit A un G-module. Si l'on pose :

$$s' . a = f(s') . a, \qquad s' \in G', \quad a \in A,$$

on munit A d'une structure de G'-module, que l'on notera f^*A (ou simplement A si cela ne prête pas à confusion). Il est clair que A^G est un sous-groupe de $(f^*A)^{G'}$. Cela définit un morphisme du foncteur $H^0(G, A)$ dans le foncteur $H^0(G', f^*A)$; comme les $H^q(G', f^*A)$ forment un foncteur cohomologique (par rapport à A), la propriété universelle des foncteurs dérivés (cf. par exemple Grothendieck [26], n°s 2. 2, 2. 3) montre que le morphisme ci-dessus se prolonge en un morphisme du foncteur cohomologique $\{H^q(G, \ ), \delta\}$ dans le foncteur cohomologique

$$\{H^q(G', f^* \ ), \delta\}.$$

En particulier, on a pour chaque entier $q \geqslant 0$, et pour chaque G-module A, un homomorphisme

$$H^q(G, A) \to H^q(G', A)$$

noté le plus souvent f_q^*.

Plus généralement, considérons un G'-module A', et une application additive $g : A \to A'$. On dira que f et g sont *compatibles* lorsque $g(f(s') . a) = s' . g(a)$ pour $s' \in G'$, $a \in A$, ce qui revient à dire que g est un *G'-homomorphisme de* f^*A *dans* A'. L'application g définit donc un homomorphisme

$$H^q(G', f^*A) \to H^q(G', A')$$

et en le composant avec l'homomorphisme obtenu ci-dessus, on obtient un homomorphisme

$$(f, g)_q^* : H^q(G, A) \to H^q(G', A')$$

qui est dit *associé* au couple (f, g); l'expression de cet homomorphisme au moyen de cochaînes standard est immédiate.

Exemples. 1) Si H est un sous-groupe de G, on peut prendre pour f *l'injection* de H dans G. On obtient ainsi des homomorphismes

$$H^q(G, A) \to H^q(H, A)$$

que nous appellerons homomorphismes de *restriction*, et que nous noterons Res.

2) Soit H un sous-groupe invariant de G. Le groupe A^H est un G/H -module, et les homomorphismes $G \to G/H$, $A^H \to A$ sont compatibles. On obtient ainsi des homomorphismes

$$H^q(G/H, A^H) \to H^q(G, A)$$

que nous appellerons homomorphismes d'*inflation*, et que nous noterons Inf.

On procède de même avec l'homologie. On a des homomorphismes

$$H_q(G', f^*A) \to H_q(G, A).$$

Lorsque H est un sous-groupe de G, et que l'on prend pour f l'injection de H dans G, on obtient des homomorphismes

$$H_q(H, A) \to H_q(G, A)$$

appelés homomorphismes de *corestriction* et notés Cor.

Revenons à la cohomologie. Considérons le cas où $G = G'$, $A = A'$, l'application $f : G \to G$ étant l'automorphisme intérieur $s \to tst^{-1}$, et $g : A \to A$ étant $a \to t^{-1}a$. On vérifie tout de suite que ces deux applications sont compatibles, et elles définissent donc par passage à la cohomologie des automorphismes σ_t des $H^q(G, A)$. En fait :

PROPOSITION 3. *Les automorphismes σ_t sont égaux à l'identité.*

Les σ_t constituent un automorphisme du foncteur cohomologique $\{H^q(G, \ ), \delta\}$; cet automorphisme est l'identité en dimension zéro, c'est clair. Il est donc l'identité en toute dimension d'après un résultat général (cf. Cartan-Eilenberg [13], Chap. III, ou Grothendieck [26], n° 2. 2).

[*Démonstration directe.* On raisonne par récurrence sur q, le cas $q = 0$ étant trivial. On plonge A dans un module co-induit A^*; soit $B = A^*/A$. On a le diagramme commutatif :

$$\begin{array}{ccccc} H^q(G, B) & \xrightarrow{\delta} & H^{q+1}(G, A) & \longrightarrow & 0 \\ \downarrow{\scriptstyle \sigma_t} & & \downarrow{\scriptstyle \sigma_t} & & \\ H^q(G, B) & \xrightarrow{\delta} & H^{q+1}(G, A) & \longrightarrow & 0. \end{array}$$

Comme σ_t est l'identité sur $H^q(G, B)$ d'après l'hypothèse de récurrence, il en résulte bien que c'est l'identité sur $H^{q+1}(G, A)$.]

Exercice. Soit H un sous-groupe de G, et soit B un H-module. Soit B^* le groupe des applications φ de G dans B telles que $\varphi(hs) = h\varphi(s)$ pour tout $h \in H$; montrer que $B^* = \mathrm{Hom}_{\mathbf{Z}[H]}(\mathbf{Z}[G], B)$. On fait de B^* un G-module en posant $(s\varphi)(g) = \varphi(gs)$. Soit $\theta : B^* \to B$ l'homomorphisme défini par $\theta(\varphi) = \varphi(1)$. Montrer que θ est compatible avec l'injection $H \to G$. Montrer que les homomorphismes

$$H^q(G, B^*) \to H^q(H, B)$$

associés à ce couple d'applications sont des *isomorphismes*.
[Noter que, si B est co-induit pour H, B^* est co-induit pour G; en déduire que $H^q(G, B^*) = 0$ si $q \geqslant 1$, et si B est co-induit. Conclure en remarquant que $H^q(G, B^*)$ est un foncteur cohomologique par rapport au H-module B.]

§ 6. *Une suite exacte*

Soit G un groupe, soit H un sous-groupe invariant de G, et soit A un G-module. On a défini au § précédent les homomorphismes

$$\mathrm{Res} : H^q(G, A) \to H^q(H, A)$$
$$\mathrm{Inf} : H^q(G/H, A^H) \to H^q(G, A).$$

PROPOSITION 4. *La suite ci-dessous est exacte* :

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^1(G, A) \xrightarrow{\mathrm{Res}} H^1(H, A).$$

Il est clair que $\mathrm{Res} \circ \mathrm{Inf} = 0$ (regarder sur les cochaînes, par exemple). Il y a donc deux choses à démontrer :

1. *Exactitude en* $H^1(G/H, A^H)$. Soit $f : G/H \to A^H$ un cocycle équivalent à 0 dans $H^1(G, A)$. Il existe $a \in A$ tel que $f(s) = sa - a$ (par abus de langage on identifie f avec l'application de G dans A constante sur les classes modulo H qui relève f). Mais $f(s)$ ne dépend que de la classe de s modulo H, ce qui montre que $sa - a = sta - a$ pour tout $t \in H$, c'est-à-dire que $ta = a$. Alors $a \in A^H$, et f est cohomologue à 0 dans $H^1(G/H, A^H)$.

2. *Exactitude en* $H^1(G, A)$. Soit f un cocycle $G \to A$, supposons que la restriction de f à H soit cohomologue à 0, i.e. qu'il existe $a \in A$ tel que $f(t) = ta - a$ pour tout $t \in H$. En retranchant de f le cobord $g(s) = sa - a$, on se ramène au cas où $f(t) = 0$ pour $t \in H$. La formule $f(st) = f(s) + sf(t)$ où l'on prend t dans H, montre alors que f est constante sur les classes modulo H. Appliquant à nouveau cette formule avec cette fois $s \in H$, et tenant compte de ce que H est invariant, on voit que $f(st) = sf(t)$, ce qui entraîne que $f(t)$ est invariant par H. Donc f est un cocycle de G/H à valeurs dans A^H, c.q.f.d.

La proposition suivante généralise la proposition 4 :

PROPOSITION 5. *Soit q un entier $\geqslant 1$. Supposons que $H^i(H, A) = 0$ pour*

$$1 \leqslant i \leqslant q - 1.$$

La suite ci-dessous est alors exacte :

$$0 \longrightarrow H^q(G/H, A^H) \xrightarrow{\text{Inf}} H^q(G, A) \xrightarrow{\text{Res}} H^q(H, A).$$

(Dans l'étude du groupe de Brauer, nous aurons à appliquer cette proposition pour $q = 2$; l'hypothèse est alors que $H^1(H, A) = 0$.)

COROLLAIRE. $\text{Inf} : H^i(G/H, A^H) \to H^i(G, A)$ *est un isomorphisme pour* $i \leqslant q - 1$.

Démonstration de la proposition 5. On raisonne par récurrence sur q, le cas $q = 1$ n'étant autre que la proposition 4. Supposons donc $q \geqslant 2$. Soit $B = \text{Hom}(\mathbf{Z}[G], A)$ le module co-induit associé canoniquement à A; un élément de b s'identifie à une fonction φ sur G à valeurs dans A, et l'on a $s\varphi(t) = \varphi(ts)$. Si $a \in A$, on pose $\varphi_a(t) = t.a$; on obtient ainsi un G-homomorphisme injectif de A dans B; si $C = B/A$, on a la suite exacte de G-modules :

$$0 \to A \to B \to C \to 0.$$

Le module B est co-induit pour G; il l'est aussi pour H, car $\mathbf{Z}[G]$ est $\mathbf{Z}[H]$-libre, donc s'écrit $\mathbf{Z}[H] \otimes M$ (M étant un groupe abélien), et $B = \text{Hom}(\mathbf{Z}[H], \text{Hom}(M, A))$. De plus comme $H^1(H, A) = 0$, on a la suite exacte

$$0 \to A^H \to B^H \to C^H \to 0$$

et $B^H = \text{Hom}(\mathbf{Z}[G/H], A)$ est G/H-induit.

Considérons alors le diagramme suivant :

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^{q-1}(G/H, C^H) & \longrightarrow & H^{q-1}(G, C) & \longrightarrow & H^{q-1}(H, C) \\ & & \downarrow\delta & & \downarrow\delta & & \downarrow\delta \\ 0 & \longrightarrow & H^q(G/H, A^H) & \longrightarrow & H^q(G, A) & \longrightarrow & H^q(H, A). \end{array}$$

Ce diagramme est commutatif, cela se voit sans difficulté. Les flèches verticales sont les cobords définis par les suites exactes écrites ci-dessus; comme B est co-induit pour G et H, et que B^H est co-induit pour G/H, ces cobords sont des isomorphismes. Pour la même raison, C vérifie l'hypothèse de récurrence (avec $q - 1$ au lieu de q). La première ligne du diagramme est donc exacte, et il en est de même de la deuxième, c.q.f.d.

Remarque. En appliquant la prop. 3, on peut montrer que G/H opère sur tous les $H^i(H, A)$, ce qui fait que l'on peut parler des groupes $H^j(G/H, H^i(H, A))$. La suite exacte de la prop. 5 peut se prolonger en la suite exacte :

$$0 \to H^q(G/H, A^H) \to H^q(G, A) \to H^q(H, A)^{G/H} \to H^{q+1}(G/H, A^H) \to H^{q+1}(G, A).$$

Cela se voit, soit par décalage (mais c'est assez pénible), soit en appliquant la *suite spectrale des extensions de groupes* (cf. [13], p. 351, ou [37]).

§ 7. *Sous-groupes d'indice fini*

Soit H un sous-groupe d'un groupe G et soit G un A-module. On a défini au § 5 des homomorphismes de restriction

$$\mathrm{Res} : \mathrm{H}^q(\mathrm{G}, \mathrm{A}) \to \mathrm{H}^q(\mathrm{H}, \mathrm{A}).$$

Supposons maintenant que H soit un *sous-groupe d'indice fini* de G. On va définir des homomorphismes en sens inverse

$$\mathrm{Cor} : \mathrm{H}^q(\mathrm{H}, \mathrm{A}) \to \mathrm{H}^q(\mathrm{G}, \mathrm{A})$$

appelés homomorphismes de *corestriction*.

Commençons par le cas $q = 0$. Si $a \in \mathrm{A}^{\mathrm{H}}$, et si $s \in \mathrm{G}$, l'élément sa ne dépend évidemment que la *classe à gauche* de s mod. H; comme par hypothèse G/H est fini, on peut former la somme :

$$\mathrm{N}_{\mathrm{G/H}}(a) = \sum_{s \in \mathrm{G/H}} sa,$$

que l'on appellera la *norme* de a. On vérifie tout de suite que $\mathrm{N}_{\mathrm{G/H}}(a)$ est invariant par G, et l'on a ainsi défini un homomorphisme

$$\mathrm{N}_{\mathrm{G/H}} : \mathrm{H}^0(\mathrm{H}, \mathrm{A}) \to \mathrm{H}^0(\mathrm{G}, \mathrm{A}).$$

C'est la corestriction en dimension 0. On la prolonge de façon unique en un homomorphisme du foncteur cohomologique $\{\mathrm{H}^q(\mathrm{H}, f^*\ ), \delta\}$ dans le foncteur cohomologique $\{\mathrm{H}^q(\mathrm{G},\ ), \delta\}$. C'est possible, car le premier foncteur est « effaçable » en dimension $\geqslant 1$, au sens de Grothendieck [26], n° 2. 2 (en effet, si A est co-induit pour G, on sait qu'il est co-induit pour H, et l'on a bien $\mathrm{H}^q(\mathrm{H}, \mathrm{A}) = 0$ pour $q \geqslant 1$). On a donc bien défini

$$\mathrm{Cor} : \mathrm{H}^q(\mathrm{H}, \mathrm{A}) \to \mathrm{H}^q(\mathrm{G}, \mathrm{A}).$$

[Pour une définition plus explicite, voir Cartan-Eilenberg [13], p. 254, ainsi que Eckmann [22].]

PROPOSITION 6. *Si* $n = \mathrm{Card}\,(\mathrm{G/H})$, *on a* $\mathrm{Cor} \circ \mathrm{Res} = n$.

Pour $q = 0$, cela signifie que, si $a \in \mathrm{A}^{\mathrm{G}}$, on a $\mathrm{N}_{\mathrm{G/H}}(a) = na$, ce qui est clair. Le cas général se ramène par décalage au cas $q = 0$.

Passons maintenant à l'homologie. Si $a \in \mathrm{A}$, et si s et s' sont dans la même *classe à gauche* mod. H, les images de $s^{-1}a$ et $s'^{-1}a$ dans A_{H} coïncident. L'expression

$$\mathrm{N}'_{\mathrm{G/H}}(a) = \sum_{s \in \mathrm{G/H}} s^{-1}a$$

a donc un sens dans A_H, et l'on obtient ainsi un homomorphisme

$$N'_{G/H} : A_G \to A_H$$

que nous appellerons la *restriction*, et que nous noterons Res. On le prolonge comme ci-dessus en un homomorphisme du foncteur homologique $\{H_q(G, \ ), \partial\}$ dans le foncteur homologique $\{H_q(H, f^* \ ), \partial\}$, homomorphisme noté encore Res. On a une proposition duale de la prop. 6.

Exercices. 1. Les hypothèses étant celles de la proposition 6, soit q un entier tel que $H^q(H, A) = 0$. Montrer que $nx = 0$ pour tout $x \in H^q(G, A)$.

2. Soit $G = \mathbf{PSL}(2, \mathbf{Z})$ le *groupe modulaire*, et soit A un G-module. Montrer que, pour tout $q \geqslant 2$, et tout $x \in H^q(G, A)$, on a $6x = 0$. (Appliquer l'exercice 1 en remarquant que G contient un sous-groupe libre d'indice 6.)

3. Soit A un G-module, et soit $A^* = \mathrm{Hom}_{\mathbf{Z}[H]}(\mathbf{Z}[G], A)$ le G-module défini en exercice au § 5. Si $\varphi \in A^*$, montrer que $s^{-1}\varphi(s)$ ne dépend que de la classe de s mod. H. En supposant H d'indice fini dans G, former la somme $\pi(\varphi) = \sum_{s \in G/H} s^{-1}\varphi(s)$, et montrer qu'elle définit un G-homomorphisme $\pi : A^* \to A$. En déduire des homomorphismes $H^q(G, A^*) \to H^q(G, A)$, et, en les combinant avec l'isomorphisme $H^q(G, A^*) = H^q(H, A)$, montrer que l'on obtient la corestriction.

§ 8. *Le transfert*

Soient encore G un groupe et H un *sous-groupe d'indice fini* de G. Appliquons les définitions du § 7 au G-module $\mathbf{Z}$ (sur lequel G opère trivialement), et à l'entier $q = 1$. On obtient un homomorphisme

$$\mathrm{Res} : H_1(G, \mathbf{Z}) \to H_1(H, \mathbf{Z}).$$

Or, on a vu au § 4 que $H_1(G, \mathbf{Z})$ s'identifie à G/G', et de même $H_1(H, \mathbf{Z})$ s'identifie à H/H'. Il s'ensuit que Res s'identifie à un homomorphisme

$$\mathrm{Ver} : G/G' \to H/H',$$

appelé *transfert* (« Verlagerung » dans la terminologie allemande), et que nous nous proposons d'expliciter.

Soit I_G le noyau de $\mathbf{Z}[G] \to \mathbf{Z}$. Par définition même de Res, on a le diagramme commutatif :

$$\begin{array}{ccc} H_1(G, \mathbf{Z}) & \xrightarrow{\partial} & H_0(G, I_G) = I_G/I_G^2 \\ \mathrm{Res}\downarrow & & \downarrow N \\ H_1(H, \mathbf{Z}) & \xrightarrow{\partial} & H_0(H, I_G) = I_G/I_H I_G. \end{array}$$

Comme d'autre part $\mathbf{Z}[H]$ se plonge dans $\mathbf{Z}[G]$ de façon compatible avec les opérations de H, on a le diagramme commutatif :

$$\begin{array}{ccc} H_1(H, \mathbf{Z}) & \xrightarrow{\partial} & I_G/I_H I_G \\ \mathrm{id.}\uparrow & & \uparrow \\ H_1(H, \mathbf{Z}) & \xrightarrow{\partial} & I_H/I_H^2. \end{array}$$

Dans ces deux diagrammes, les opérations ∂ sont injectives, puisque $\mathbf{Z}[H]$ et $\mathbf{Z}[G]$ sont des modules induits. On peut donc les utiliser pour expliciter

$$\mathrm{Res} : H_1(G, \mathbf{Z}) \to H_1(H, \mathbf{Z}).$$

Si l'on remplace $H_1(G, \mathbf{Z})$ par G/G' et $H_1(H, \mathbf{Z})$ par H/H', on a le diagramme commutatif suivant :

$$\begin{array}{ccccc} G/G' & \xrightarrow{\approx} & I_G/I_G^2 & \xrightarrow{N} & \\ \mathrm{Ver}\downarrow & & & & I_G/I_H I_G. \\ H/H' & \xrightarrow{\approx} & I_H/I_H^2 & \nearrow & \end{array}$$

Il n'y a plus maintenant qu'à calculer : soit $s \in G$; l'image de s dans I_G/I_G^2 est $i_s = s - 1$. Si les s_t forment un système de représentants des *classes à droite* mod. H, $N(i_s)$ est la classe de $\Sigma s_t(s-1)$ mod. $I_H I_G$. Mais, pour chaque t, il existe un indice $j(t)$, et un élément $x_t \in H$ tels que :

$$s_t s = x_t s_{j(t)}.$$

On peut donc écrire :

$$\begin{aligned} N(i_s) &\equiv \Sigma x_t s_{j(t)} - \Sigma s_{j(t)} && \text{mod. } I_H I_G \\ &\equiv \Sigma(x_t - 1) s_{j(t)} && \text{mod. } I_H I_G \\ &\equiv \Sigma(x_t - 1) && \text{mod. } I_H I_G \end{aligned}$$

Posons alors $x = \prod x_t$. L'image de x dans $I_G/I_H I_G$ est égale à la classe de $\sum(x_t - 1)$. Il en résulte que l'image de x dans H/H' est égale au transfert de l'image de s dans G/G'. En changeant légèrement les notations, ceci donne :

PROPOSITION 7. *Soit* $\theta : H\backslash G \to G$ *un système de représentants de l'espace homogène* $H\backslash G$ *des classes à droite de* G mod. H. *Pour tout* $s \in G$ *et* $t \in H\backslash G$, *soit* $x_{t,s}$, *l'élément de* H *défini par la formule* :

$$\theta(t).s = x_{t,s}.\theta(t.s).$$

Le transfert $\mathrm{Ver} : G/G' \to H/H'$ *est alors donné par passage au quotient à partir de l'application* $s \to \prod_t x_{t,s}$.

On retrouve bien la définition classique du transfert, cf. par exemple M. Hall [30], p. 202.

On peut pousser davantage le calcul précédent :

Soit S le sous-groupe de G engendré par l'élément s, et faisons opérer S à droite sur l'espace homogène $H\backslash G$. Les orbites sont les doubles classes $W \in H\backslash G/S$. Dans chaque double classe, choisissons un élément x, et soit f_x l'ordre de l'orbite correspondante (c'est-à-dire le plus petit entier f strictement positif tel que $x.s^f \equiv x$ mod. H). Il est clair que, lorsque x parcourt les représentants des doubles classes, les éléments x, $x.s$, $x.s^2$, ..., $x.s^{f_x-1}$ forment un système de représentants de $H\backslash G$.

Pour déterminer le transfert au moyen de ce système de représentants, il faut écrire

chaque produit $xs^e.s$ sous la forme $y.t$, avec $y \in H$ et t représentant. Or $x.s^{e+1}$ est un représentant, sauf si $e = f_x - 1$, auquel cas, par définition de f_x, on a

$$x.s^{f_x} \equiv x \text{ mod. } H.$$

Ainsi, dans le calcul de Ver (s), les seuls facteurs non nécessairement égaux à 1 sont ceux qui correspondent aux produits $x.s^{f_x-1}.s$, et ceux-ci sont égaux à $x.s^{f_x}.x^{-1}$. D'où :

PROPOSITION 8. *Soit x_i un système de représentants des doubles classes HxS, et pour chaque i, soit $f_i = f_{x_i}$ défini comme ci-dessus. On a alors :*

$$\text{Ver } (s) = \prod x_i.s^{f_i}.x_i^{-1} \text{ mod. } H'.$$

Application (Artin [4]). Soit L/K une extension galoisienne, de groupe de Galois G, et soit A un anneau de Dedekind de corps des fractions K, dont les corps résiduels soient des corps finis. Si L_a/K désigne la plus grande extension abélienne de K contenue dans L, le symbole $(\mathfrak{a}, L_a/K)$ est défini pour tout idéal $\mathfrak{a}$ de A non ramifié dans L (cf. Chap. I, § 8) ; c'est un élément de G/G'. D'autre part, soit K' une extension de K intermédiaire entre K et L, et soit L'_a la plus grande extension abélienne de K' contenue dans L; si $\mathfrak{a}'$ désigne l'idéal engendré par $\mathfrak{a}$ dans la fermeture intégrale de A dans K', le symbole $(\mathfrak{a}', L'_a/K')$ est bien défini, et appartient à H/H', avec $H = G(L/K')$. On a alors la formule :

$$\text{Ver } ((\mathfrak{a}, L_a/K)) = (\mathfrak{a}', L'_a/K').$$

[Par linéarité, on peut supposer que $\mathfrak{a} = \mathfrak{p}$ est premier; on choisit alors $\mathfrak{P}$ premier dans L au-dessus de $\mathfrak{p}$, et l'on pose $s = (\mathfrak{P}, L/K)$; il est clair que $(\mathfrak{a}, L_a/K)$ n'est autre que l'image canonique de s dans G/G', et l'on est ramené à calculer Ver (s). Cela se fait au moyen de la proposition 8, en remarquant que les doubles classes Hx_iS correspondent bijectivement aux idéaux premiers $\mathfrak{p}'_i$ de K' au-dessus de $\mathfrak{p}$. Chaque terme $x_i.s^{f_i}.x_i^{-1}$ n'est autre que $(\mathfrak{p}'_i, L'_a/K')$, d'après la proposition 22 du chapitre I. On trouve bien

$$\text{Ver } (s) = \prod (\mathfrak{p}'_i, L'_a/K') = (\mathfrak{a}', L'_a/K')$$

puisque $\mathfrak{a}' = \prod \mathfrak{p}'_i$, c.q.f.d.]

Remarque. Si G a un nombre fini de générateurs, et si H = G', on peut montrer que le transfert Ver : $G/G' \to H/H'$ est nul (cf. Artin-Tate [8], p. 189). Combiné avec ce qui précède, et avec la loi de réciprocité d'Artin, ce résultat donne le « Hauptidealsatz », cf. Artin [4].

Exercice. Soit H un sous-groupe d'indice fini d'un groupe G, et soit $\chi : H \to \mathbf{C}^*$ une représentation linéaire de degré 1 de H. Soit $s \to M_s$ la représentation linéaire de G *induite* par χ (cf. Chap. VI, § 1). Montrer que l'on a :

$$\det (M_s) = \varepsilon(s).\chi(\text{Ver}(s)),$$

où $\varepsilon(s)$ est la signature de la permutation de G/H définie par s.

ANNEXE

Cohomologie non abélienne

Soit G un groupe, et soit A un groupe sur lequel G opère à gauche. Jusqu'à présent, nous n'avons considéré que le cas où A est abélien. Nous allons maintenant abandonner cette hypothèse et montrer que l'on peut encore définir $H^0(G, A)$ et $H^1(G, A)$ et démontrer un « morceau » de suite exacte.

Nous écrirons A multiplicativement. On définit tout d'abord $H^0(G, A)$ comme le groupe A^G des éléments de A invariants par G (i. e. $s(a) = a$ pour tout $s \in G$). D'autre part, on appelle *cocycle* une application de G dans A notée a_s telle que $a_{st} = a_t . s(a_t)$; on dit que a_s et b_s sont cohomologues s'il existe $a \in A$ tel que $b_s = a^{-1} . a_s . s(a)$ pour tout s de G. Cette relation est une relation d'équivalence dans l'ensemble des cocycles, et l'ensemble quotient, muni de la structure définie par la donnée de la classe d'équivalence du cocycle identique (c'est-à-dire d'une structure « d'ensemble pointé »), sera appelé *ensemble de cohomologie de* G *à valeurs dans* A et noté $H^1(G, A)$. Cette définition coïncide bien dans le cas où A est abélien avec la définition habituelle, à ceci près qu'on ne retient de la structure de groupe de $H^1(G, A)$ que la donnée de l'élément unité (c'est-à-dire, pour parler savamment, la structure d'*ensemble pointé* sous-jacente à la structure de groupe).

Les objets $H^0(G, A)$ et $H^1(G, A)$ sont des foncteurs en A : Si $f : A \to B$ est un homomorphisme de G-modules non abéliens, i. e. un homomorphisme de groupes qui commute aux opérations de G, on définit

$$f_0 : H^0(G, A) \to H^0(G, B)$$
$$f_1 : H^1(G, A) \to H^1(G, B)$$

de la manière suivante : f_0 est la restriction à A^G de f, l'image de f_0 étant évidemment composée d'invariants de B; si nous considérons maintenant un cocycle de A, on obtient en le composant avec f un cocycle de B, et cette opération est compatible avec les équivalences nécessaires; f_0 est un homomorphisme de groupes, f_1 envoie la classe d'équivalence du cocycle unité de A sur son homologue dans B, c'est un « morphisme d'ensembles pointés ».

On appelle noyau d'un morphisme d'ensembles pointés l'image inverse de l'élément distingué de l'image. Cette définition permet aussitôt de généraliser la notion de suite exacte à des ensembles pointés.

Soit (*) $1 \to A \xrightarrow{i} B \xrightarrow{p} C \to 1$ une suite exacte de G-modules non abéliens,

A étant invariant dans B. On définit un opérateur *cobord* δ : $H^0(G, C) \to H^1(G, A)$ de la manière suivante :

Soit $c \in C^G$. Choisissons un $b \in B$ tel que $pb = c$. L'élément c étant invariant par G, et la suite (*) étant exacte, on a $s(b) \equiv b \pmod{A}$ pour tout $s \in G$. Ceci permet de définir $a_s : G \to A$ par $a_s = b^{-1}s(b)$. Nous allons montrer successivement que a_s est un cocycle de A, et que si l'on choisit un autre élément b' de B tel que $pb = c$, on remplace ce cocycle par un cocycle cohomologue, ce qui achèvera de définir δ.

On a : $$a_{st} = b^{-1}st(b) = b^{-1}s(b)\, s(b^{-1}t(b)) = a_s.s(a_t).$$

Si $pb' = pb = c$, il existe $a \in A$ tel que $b' = ba$, et si on note a'_s le cocycle défini à l'aide de b', on a :

$$a'_s = a^{-1}b^{-1}s(b)s(a) = a^{-1}a_s s(a) \text{ qui est cohomologue à } a_s.$$

Remarquons que cet opérateur cobord coïncide dans le cas abélien avec l'opérateur cobord habituel.

Supposons maintenant A *contenu dans le centre de* B. On va définir Δ : $H^1(G, C) \to H^2(G, A)$, ce dernier étant l'ensemble pointé sous-jacent au groupe $H^2(G, A)$ défini à la manière habituelle, A étant abélien. Soient donc c_s un cocycle de C et $b_s \in B$ tel que $p(b_s) = c_s$. On a comme précédemment $b_{st} \equiv b_s.s(b_t) \pmod{A}$ pour tous $s, t \in G$, ce qui permet de définir un élément $a_{s,t} \in A$ par $a_{s,t} = b_s.s(b_t).b_{st}^{-1}$. On se propose de montrer maintenant que $a_{s,t}$ est un 2-cocycle de A et que sa classe dans $H^2(G, A)$ ne dépend ni du choix de c_s dans sa classe de cohomologie, ni du choix de b_s dans $p^{-1}(c_s)$, ce qui permettra de définir Δ par passage aux quotients.

Pour montrer que $a_{s,t}$ est un 2-cocycle de A, on doit vérifier que :

$$s(a_{t,u})a_{s,tu} = a_{st,u}a_{s,t}$$

soit, comme A est abélien, $a_{s,t}^{-1}a_{s,tu}a_{st,u}^{-1}s(a_{t,u}) = 1$. Explicitons :

$$b_{st}s(b_t)^{-1}b_s^{-1}b_s s(b_{tu})b_{stu}^{-1}b_{stu}st(b_u)^{-1}b_{tu}^{-1}s(a_{t,u}) = b_{st}s(b_t)^{-1}s(b_{tu})st(b_u)^{-1}b_{st}^{-1}s(a_{t,u}).$$

Mais $s(a_{t,u}) = s(b_t)st(b_u)s(b_{tu}^{-1})$ est dans le centre de B. La formule à démontrer peut alors s'écrire

$$b_{st}s(b_t)^{-1}s(b_t)st(b_u)s(b_{tu}^{-1})s(b_{tu})st(b_u)^{-1}b_{st}^{-1} = 1,$$

ce qui est évident.

D'autre part, si nous remplaçons c_s par un cocycle homologue $c'_s = c^{-1}c_s s(c)$, on peut relever c'_s en $b'_s = b^{-1}b_s s(b)$ où $b \in B$ est tel que $pb = c$. Montrons que $a_{s,t}$ ne change pas :

On a :

$$a'_{s,t} = b'_s s(b'_t)b'^{-1}_{st} = b^{-1}b_s s(b)s(b^{-1})s(b_t)st(b)st(b)^{-1}b_{st}^{-1}b = b^{-1}a_{s,t}b = a_{s,t}.$$

Si nous modifions le choix de b_s, nous le remplaçons par $b'_s = a_s b_s$ où $a_s \in A$. Le

cocycle $a_{s,t}$ est alors remplacé par $a'_{s,t} = a_s b_s s(a_t) b_t b_{st}^{-1} a_{st}^{-1}$ qui, A étant dans le centre de B, s'écrit :

$$a'_{s,t} = a_s s(a_t) a_{st}^{-1} a_{s,t}$$

et c'est bien un cocycle cohomologue à $a_{s,t}$.

L'application $\Delta : H^1(G, C) \to H^2(G, A)$ est donc définie.

PROPOSITION 1. *Soit* $1 \to A \xrightarrow{i} B \xrightarrow{p} C \to 1$ *une suite exacte de* G*-modules non commutatifs. La suite d'ensembles pointés ci-dessous est alors exacte :*

$$1 \to H^0(G, A) \xrightarrow{i_0} H^0(G, B) \xrightarrow{p_0} H^0(G, C) \xrightarrow{\delta} H^1(G, A) \xrightarrow{i_1} H^1(G, B) \xrightarrow{p_1} H^1(G, C).$$

PROPOSITION 2. *Soit* $1 \to A \to B \to C \to 1$ *une suite exacte de* G*-modules non commutatifs* A *étant dans le centre de* B. *La suite d'ensembles pointés ci-dessous est alors exacte :*

$$1 \to H^0(G, A) \xrightarrow{i_0} H^0(G, B) \xrightarrow{p_0} H^0(G, C) \xrightarrow{\delta} H^1(G, A) \xrightarrow{i_1} H^1(G, B) \xrightarrow{p_1} H^1(G, C) \xrightarrow{\Delta} H^2(G, A).$$

La démonstration consiste en une série de vérifications :

1. *Exactitude en* $H^0(G, A)$. Triviale.

2. *Exactitude en* $H^0(G, B)$. On a $p_0 \circ i_0 = 1$ par fonctorialité (ici, « 1 » désigne l'application constante égale à 1, et non l'application identique). Réciproquement, si $b \in B^G$ est annulé par p_0, on a $b \in A \cap B^G = i_0(A^G)$.

3. *Exactitude en* $H^0(G, C)$. Dire que $c \in G^G$ est dans $p_0(B^G)$, c'est dire qu'on peut le remonter dans B en un invariant. Dire que $\delta(c) = 1$, c'est également dire que B peut se remonter en un invariant, d'après la définition de δ.

4. *Exactitude en* $H^1(G, A)$. Soit a_s un cocycle de A. La classe de a_s est annulée par i_0 s'il existe $b \in B$ tel que $a_s = b^{-1} s(b)$. Ceci est en tout cas vrai si a_s est dans l'image de δ, par définition de cette dernière. Inversement, si $a_s = b^{-1} s(b)$, on a $p(b) \in C^G$, et $\delta p(b)$ est la classe de a_s.

5. *Exactitude en* $H^1(G, B)$. On a par fonctorialité $p_1 \circ i_1 = 1$. Réciproquement, il est évident qu'un cocycle de B cohomologue à 1 « en projection dans C » est cohomologue dans B à un cocycle de A.

6. *Exactitude en* $H^1(G, C)$ *lorsque* A *est dans le centre de* B. La définition montre que $\Delta \circ p_1 = 1$. Inversement, soit c_s un cocycle de C appartenant au noyau de Δ; on a $c_s = p(b_s)$, et le 2-cocycle $a_{s,t} = b_s s(b_t) b_{st}^{-1}$ est cohomologue à zéro, c'est-à-dire de la forme $a_s s(a_t) a_{st}^{-1}$; en remplaçant b_s par $a_s^{-1} b_s$, on se ramène au cas où $a_{s,t} = 1$, ce qui signifie que b_s est un cocycle de B d'image c_s, et achève la démonstration.

Remarques. 1. On peut, au moyen du groupe de Brauer, donner des exemples où *l'image de* Δ *n'est pas un sous-groupe de* $H^2(G, A)$.

2. La proposition précédente donne une caractérisation du noyau de Δ, mais ne permet pas de dire sous quelles conditions deux éléments de $H^1(G, C)$ ont même image dans $H^2(G, A)$ cf. [113]. La situation est la même en théorie des faisceaux, cf. par exemple Grothendieck [27] et Frenkel [24]; il existe d'ailleurs une « algèbre homologique non abélienne » qui englobe ces diverses théories, cf. Giraud [80].

CHAPITRE VIII

COHOMOLOGIE DES GROUPES FINIS

§ 1. *Les groupes de cohomologie modifiés*

Soit G un groupe fini. Dans l'algèbre $\mathbf{Z}[G]$, l'élément $\sum_{s \in G} s$ sera appelé la *norme*, et sera noté N. Pour tout G-module A, l'élément N définit un endomorphisme

$$N : A \to A$$

par la formule $Na = \sum_{s \in G} s.a$. Si I_G désigne *l'idéal d'augmentation* de $\mathbf{Z}[G]$ (i.e. l'ensemble des combinaisons linéaires des $s - 1$, $s \in G$), on a évidemment

$$I_G A \subset \mathrm{Ker}(N) \qquad \text{et} \qquad \mathrm{Im}(N) \subset A^G.$$

Comme $H_0(G, A) = A/I_G A$ et $H^0(G, A) = A^G$, il s'ensuit que N définit par passage au quotient un homomorphisme

$$N^* : H_0(G, A) \to H^0(G, A).$$

On posera :

$$\hat{H}_0(G, A) = \mathrm{Ker}(N^*), \qquad \hat{H}^0(G, A) = \mathrm{Coker}(N^*).$$

Autrement dit, en notant ${}_N A$ le noyau de N opérant dans A :

$$\hat{H}_0(G, A) = {}_N A/I_G A$$
$$\hat{H}^0(G, A) = A^G/NA.$$

PROPOSITION 1. *Si* A *est relativement projectif,* $\hat{H}_0(G, A)$ *et* $\hat{H}^0(G, A)$ *sont nuls.*

(Rappelons que « relativement projectif » est équivalent à « relativement injectif », puisque G est fini.)

Il suffit de le démontrer pour A induit. Donnons la démonstration pour $\hat{H}^0$.

On a $A = \sum_{s \in G} sX$, X étant un sous-groupe de A, et la somme étant directe. Tout $a \in A$ s'écrit donc de façon unique sous la forme $a = \Sigma s(x_s)$, $x_s \in X$. On voit tout de suite que a est invariant par G si et seulement si tous les x_s sont égaux, c'est-à-dire si l'on peut écrire $a = Nx$, avec $x \in X$. On a donc $A^G = NA$, d'où $\hat{H}^0(G, A) = 0$.

Soit maintenant $0 \to A \to B \to C \to 0$ une suite exacte de G-modules. On vérifie aisément que le diagramme

$$\begin{array}{ccccccccc} H_1(G, C) & \longrightarrow & H_0(G, A) & \longrightarrow & H_0(G, B) & \longrightarrow & H_0(G, C) & \longrightarrow & 0 \\ \downarrow & & \downarrow N_A^* & & \downarrow N_B^* & & \downarrow N_C^* & & \downarrow \\ 0 & \longrightarrow & H^0(G, A) & \longrightarrow & H^0(G, B) & \longrightarrow & H^0(G, C) & \longrightarrow & H^1(G, A) \end{array}$$

est commutatif (on a noté N_A^* l'homomorphisme N^* relatif à A, et de même pour B et C).

On sait (cf. Cartan-Eilenberg [13], V. 10. 1) qu'un tel diagramme définit canoniquement un homomorphisme

$$\delta : \mathrm{Ker}\,(N_C^*) \to \mathrm{Coker}\,(N_A^*).$$

[Rappelons la définition de cet homomorphisme : si $c \in \mathrm{Ker}(N_C^*)$, on relève c en $b \in H_0(G, B)$; l'élément $N_B^*(b)$ provient d'un élément $a \in H^0(G, A)$, et l'image $\bar{a}$ de a dans $\mathrm{Coker}(N_A^*)$ est égale par définition à $\delta(c)$. On vérifie qu'elle ne dépend pas du choix de b.]

Comme $\mathrm{Ker}\,(N_C^*) = \hat{H}_0(G, C)$ et $\mathrm{Coker}\,(N_A^*) = \hat{H}^0(G, A)$, on a ainsi défini un homomorphisme

$$\delta : \hat{H}_0(G, C) \to \hat{H}^0(G, A).$$

De plus, d'après Cartan-Eilenberg (*loc. cit.*), le diagramme ci-dessus donne naissance à une suite exacte :

$$\cdots \to H_1(G, C) \to \hat{H}_0(G, A) \to \hat{H}_0(G, B) \to \hat{H}_0(G, C) \xrightarrow{\delta} \hat{H}^0(G, A)$$
$$\to \hat{H}^0(G, B) \to \hat{H}^0(G, C) \to H^1(G, A) \to \cdots$$

On est ainsi conduit, avec Tate, à définir des *groupes de cohomologie à exposants positifs ou négatifs* au moyen des formules :

$$\begin{aligned} \hat{H}^n(G, A) &= H^n(G, A) && \text{si } n \geqslant 1 \\ \hat{H}^0(G, A) &= A^G/NA \\ \hat{H}^{-1}(G, A) &= {}_NA/I_GA \\ \hat{H}^{-n}(G, A) &= H_{n-1}(G, A) && \text{si } n \geqslant 2. \end{aligned}$$

Ces groupes $\hat{H}^n$ forment de façon naturelle, on l'a vu, un *foncteur cohomologique*, défini en toute dimension. On a de plus $\hat{H}^n(G, A) = 0$ pour tout n lorsque A est relativement projectif (cf. prop. 1 pour $n = 0, -1$, ainsi que le Chap. VII pour les autres valeurs de n). Il s'ensuit que ce foncteur est *effaçable* et *coeffaçable* en toute dimension, au sens de Grothendieck [26], n° 2. 2. De façon précise :

a) Tout G-module se plonge dans un G-module induit A*, et l'on a

$$\hat{H}^q(G, A) = \hat{H}^{q-1}(G, A^*/A) \qquad \text{pour tout } q \in \mathbf{Z}.$$

b) Tout G-module A est quotient d'un G-module induit A_* par un sous-G-module A', et l'on a :

$$\hat{H}^q(G, A) = \hat{H}^{q+1}(G, A') \qquad \text{pour tout } q \in \mathbf{Z}.$$

On peut de plus choisir A* et A_* de telle sorte que A soit facteur direct (comme Z-module) dans A*, et A' facteur direct dans A_*, cf. Chap. VII, § 1.

Remarque. Les propriétés de « décalage » précédentes pourraient être utilisées pour donner une définition récurrente des groupes $\hat{H}^q(G, A)$. C'est essentiellement le point de vue de Chevalley [17].

§ 2. *Restriction et corestriction*

Soit H un sous-groupe du groupe fini G, et soit A un G-module. On a défini au Chap. VII, § 5 les homomorphismes de *restriction* :

$$\mathrm{Res} : H^q(G, A) \to H^q(H, A).$$

Pour $q = 0$, cet homomorphisme n'est autre que l'injection canonique de A^G dans A^H; comme $N_G = N_{G/H} \circ N_H$, on a $N_G A \subset N_H A$, et par passage au quotient, on obtient un homomorphisme

$$\mathrm{Res} : \hat{H}^0(G, A) \to \hat{H}^0(H, A).$$

Passons maintenant aux $\hat{H}^{-n}$, avec $n \geqslant 1$. Tout d'abord, si $n \geqslant 2$, on a $\hat{H}^{-n} = H_{n-1}$, et l'on a défini au Chap. VII, § 7 l'homomorphisme de restriction. Pour $n = 1$, il faut vérifier que cet homomorphisme passe au quotient, ce qui est immédiat. En résumé, *on a défini pour tout* $q \in \mathbf{Z}$ *un homomorphisme*

$$\mathrm{Res} : \hat{H}^q(G, A) \to \hat{H}^q(H, A).$$

La proposition suivante montre que cette définition est « raisonnable » :

PROPOSITION 2. *Les applications* Res *forment un morphisme de foncteurs cohomologiques.*
(En d'autres termes, ces applications commutent avec le cobord.)

Soit $0 \to A \to B \to C \to 0$ une suite exacte de G-modules. On doit vérifier la commutativité du diagramme :

$$\begin{array}{ccc} \hat{H}^q(G, C) & \xrightarrow{\delta} & \hat{H}^{q+1}(G, A) \\ \mathrm{Res}\downarrow & & \mathrm{Res}\downarrow \\ \hat{H}^q(H, C) & \xrightarrow{\delta} & \hat{H}^{q+1}(H, A). \end{array}$$

Lorsque $q \geqslant 0$, cela résulte de la définition de Res donnée au Chap. VII, § 5; lorsque $q \leqslant -2$, cela résulte du Chap. VII, § 7. Reste le cas $q = -1$, où l'on a $\hat{H}^q(G, C) = {}_NC/I_GC$, $\hat{H}^{q+1}(G, A) = A^G/NA$, ... Explicitons le calcul dans ce cas :

Soit $c \in {}_NC$ un représentant d'un élément $\bar{c} \in \hat{H}^{-1}(G, C)$. On relève c en $b \in B$, et on prend $N_G(b)$; c'est un élément de A^G, dont la classe mod. N_GA est égale à $\delta(\bar{c})$. La classe de $N_G(b)$ mod. N_HA est donc égale à $\mathrm{Res} \circ \delta(\bar{c})$. D'autre part Res $(\bar{c})$ est donné par la classe de $\Sigma s_i c$, où les s_i sont des représentants des classes à droite mod. H; on relève cet élément en $\Sigma s_i b$, et $\delta \circ \mathrm{Res}\,(\bar{c})$ est représenté par $N_H(\Sigma s_i b)$, ce qui est visiblement égal à $N_G(b)$, c.q.f.d.

Remarque. La proposition précédente montre que Res est *l'unique foncteur cohomologique qui coïncide en degré* 0 *avec l'application de* A^G/N_GA *dans* A^H/N_HA *induite par l'injection* $A^G \to A^H$.

On procède exactement de même pour la *corestriction*

$$\mathrm{Cor} : \hat{H}^q(H, A) \to \hat{H}^q(G, A).$$

En dimensions $q \geqslant 0$, on la définit comme au Chap. VII, § 7, et en dimensions $q \leqslant -1$, on la définit comme au Chap. VII, § 5. Le raisonnement de la proposition 2 se dualise et donne :

PROPOSITION 3. *Les applications* Cor *forment un morphisme de foncteurs cohomologiques.*

Plus précisément, Cor *est l'unique foncteur cohomologique qui coïncide en degré* -1 *avec l'application de* ${}_NA/I_HA$ *dans* ${}_NA/I_GA$ *induite par l'injection de* ${}_NA$ *dans* ${}_NA$.

En degré zéro, Cor est induite par l'application $N_{G/H} : A^H \to A^G$.

PROPOSITION 4. *Si* $n = \mathrm{Card}\,(G/H)$, *on a* $\mathrm{Cor} \circ \mathrm{Res} = n$.

Cela résulte de la prop. 6 du Chap. VII, et de la proposition analogue pour l'homologie.

[*Démonstration directe* : Si f_n désigne la multiplication par n, le morphisme de foncteurs cohomologiques $\mathrm{Cor} \circ \mathrm{Res} - f_n$ est nul en dimension 0 (vérification triviale), donc partout.]

COROLLAIRE 1. *Si* g *est l'ordre du groupe* G, *tous les groupes* $\hat{H}^q(G, A)$ *sont annulés par* g.

On applique la prop. 4 avec $H = \{1\}$, en remarquant que les $\hat{H}^q(H, A)$ sont tous nuls.

COROLLAIRE 2. *Si* A *est un* G*-module de type fini sur* Z, *les* $\hat{H}^q(G, A)$ *sont des groupes finis.*

En effet, la définition de ces groupes au moyen de cochaînes (ou de chaînes) montre que ce sont des groupes de type fini; comme, d'après le corollaire 1, ce sont des groupes de torsion, ce sont des groupes finis.

§ 3. *Cup-produits*

Soient A et B deux G-modules, et soit $A \otimes B$ leur produit tensoriel (sur l'anneau $\mathbf{Z}$, comme toujours). On fait de $A \otimes B$ un G-module en posant :

$$s.(a \otimes b) = s.a \otimes s.b$$

et en prolongeant par linéarité.

Ceci étant posé, on a :

PROPOSITION 5. *Soit* G *un groupe fini. Il existe une famille et une seule d'homomorphismes*

$$\hat{H}^p(G, A) \otimes \hat{H}^q(G, B) \to \hat{H}^{p+q}(G, A \otimes B)$$

notés $(a, b) \to a.b$, *qui sont définis pour tout couple d'entiers* (p, q) *et tout couple de* G*-modules* A, B, *et qui vérifient les quatre propriétés suivantes :*

(i) *Ces homomorphismes sont des morphismes de foncteurs, lorsqu'on considère les deux membres comme des bifoncteurs covariants en* (A, B).

(ii) *Pour* $p = q = 0$, *le cup-produit* $a.b$ *s'obtient par passage au quotient à partir de l'application évidente* $A^G \otimes B^G \to (A \otimes B)^G$.

(iii) *Si* $0 \to A \to A' \to A'' \to 0$ *est une suite exacte de* G*-modules et si la suite*

$$0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0$$

est exacte, on a pour tous $a'' \in \hat{H}^p(G, A'')$ *et* $b \in \hat{H}^q(G, B)$:

$$(\delta a'').b = \delta(a''.b)$$

où les deux membres sont des éléments de $\hat{H}^{p+q+1}(G, A \otimes B)$.

(iv) *Si* $0 \to B \to B' \to B'' \to 0$ *est une suite exacte de* G*-modules et si la suite*

$$0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0$$

est aussi exacte, on a, pour tous $a \in \hat{H}^p(G, A)$ *et* $b'' \in \hat{H}^q(G, B'')$:

$$a.(\delta b'') = (-1)^p \delta(a.b'')$$

où les deux membres sont dans $\hat{H}^{p+q+1}(G, A \otimes B)$.

Les propriétés (iii) et (iv) permettent d'utiliser la méthode de « décalage »; l'unicité du produit en résulte. Quant à l'existence, elle se démontre en définissant un produit sur les cochaînes (ou plus précisément sur une « résolution complète ») : voir Cartan-Eilenberg [13], Chap. XII.

Nous renvoyons également à Cartan-Eilenberg pour les nombreuses formules relatives au cup-produit (en particulier celles qui font intervenir Res et Cor). Nous mentionnerons seulement les deux suivantes (immédiates par décalage);

(v) *On a* $(a.b).c = a.(b.c)$ *modulo l'identification de* $(A \otimes B) \otimes C$ *et de* $A \otimes (B \otimes C)$.

(vi) *On a* $a.b = (-1)^{\dim(a).\dim(b)} b.a$ *modulo l'identification de* $A \otimes B$ *avec* $B \otimes A$.

On a quelquefois à considérer un autre type de cup-produit (qui se déduit d'ailleurs du précédent) :

Soient A, B, C trois G-modules, et soit $\varphi : A \times B \to C$ une application **Z**-bilinéaire *invariante par* G, c'est-à-dire telle que $\varphi(s.a, s.b) = s.\varphi(a, b)$ pour $s \in G$, $a \in A$, $b \in B$. L'application φ définit un G-homomorphisme

$$\Phi : A \otimes B \to C.$$

Si $a \in \hat{H}^p(G, A)$, $b \in \hat{H}^q(G, B)$, on a $a.b \in \hat{H}^{p+q}(G, A \otimes B)$, et on peut prendre l'image de $a.b$ par Φ. C'est un élément de $\hat{H}^{p+q}(G, C)$, que l'on appellera encore le *cup-produit de a et b relativement à* φ, et que l'on notera $a._{\varphi} b$ (ou même $a.b$, lorsqu'il n'y aura pas d'ambiguïté sur φ).

§ 4. *Cohomologie des groupes cycliques finis. Quotient de Herbrand*

Soit G un groupe cyclique d'ordre fini n, et faisons choix d'un *générateur* s de G. Dans l'algèbre **Z**[G], considérons les deux éléments suivants :

$$N = \sum_{t \in G} t = \sum_{i=0}^{i=n-1} s^i$$
$$D = s - 1.$$

Soit K le complexe de cochaînes défini de la façon suivante :

$$\begin{cases} K^i = \mathbf{Z}[G] \text{ pour tout } i \\ d : K^i \to K^{i+1} \text{ est la multiplication par D (resp. par N) si } i \text{ est pair (resp. impair).} \end{cases}$$

Pour tout G-module A, posons $K(A) = K \otimes_{\mathbf{Z}[G]} A$. On a :

$$\begin{cases} K^i(A) = A \text{ pour tout } i \\ d : K^i(A) \to K^{i+1}(A) \text{ est la multiplication par D (resp. par N) si } i \text{ est pair (resp. impair).} \end{cases}$$

Si $0 \to A \to B \to C \to 0$ est une suite exacte de G-modules, on a la suite exacte de complexes :

$$0 \to K(A) \to K(B) \to K(C) \to 0$$

d'où une suite exacte de cohomologie, et en particulier un opérateur cobord δ.

PROPOSITION 6. *Le foncteur cohomologique* $\{H^q(K(\ )), \delta\}$ *est isomorphe au foncteur* $\{\hat{H}^q(G, \ ), \delta\}$.

Il est tout d'abord clair que $\hat{H}^0(G, A) = H^0(K(A))$, $\hat{H}^{-1}(G, A) = H^1(K(A))$, et que l'opérateur cobord δ reliant H^0 à H^{-1} est le même. Il en résulte que

$$H^q(K(A)) = 0$$

pour $q = 0,1$ lorsque A est relativement projectif, donc pour toute valeur de q (car les $H^q(K(A))$ ne dépendent visiblement que de la parité de q). Ceci suffit à assurer que le foncteur $|H^q(K(\ )), \delta|$ est isomorphe au foncteur $|\hat{H}^q(G, \ ), \delta|$.

COROLLAIRE. *Les groupes* $\hat{H}^q(G, A)$ *ne dépendent que de la parité de* q.

(En d'autres termes, la cohomologie d'un groupe cyclique est *périodique de période* 2.)

De façon explicite, on a :

$$\hat{H}^q(G, A) = \mathrm{Ker}(D)/\mathrm{Im}(N) = A^G/NA \qquad \text{pour } q \equiv 0 \bmod 2$$
$$\hat{H}^q(G, A) = \mathrm{Ker}(N)/\mathrm{Im}(D) = {}_NA/DA \qquad \text{pour } q \equiv 1 \bmod 2.$$

Remarque. Les isomorphismes ci-dessus *dépendent du choix du générateur* s (car l'opérateur cobord du complexe K en dépend). On peut aussi mettre ce fait en évidence de la manière suivante : le choix de s définit un *caractère* $\chi_s : G \to \mathbf{Q}/\mathbf{Z}$ tel que $\chi_s(s) = \frac{1}{n}$, et le cobord de la suite exacte :

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0$$

transforme χ_s en un élément $\theta_s = \delta\chi_s$ de $H^2(G, \mathbf{Z})$. Les *isomorphismes de périodicité* définis ci-dessus :

$$\hat{H}^q(G, A) \to \hat{H}^{q+2}(G, A)$$

sont donnés par le cup-produit avec θ_s : cela résulte, par exemple, des formules de cup-produit données dans Cartan-Eilenberg [13], p. 252. En particulier, l'isomorphisme $A^G/NA \to H^2(G, A)$ fait correspondre à a l'élément $a.\theta_s$; on voit bien ainsi que cet isomorphisme dépend du choix de s.

Nous allons maintenant changer légèrement la définition du complexe K(A) : nous le considèrerons comme *gradué par les entiers mod.* 2. Nous écrirons $H^0(A)$ et $H^1(A)$ au lieu de $H^0(K(A))$ et $H^1(K(A))$; on a $H^0(A) = A_G/NA$, $H^1(A) = {}_NA/DA$. Si

$$0 \to A \to B \to C \to 0$$

est une suite exacte de G-modules, la suite exacte de cohomologie s'écrit sous forme d'*hexagone exact* :

$$\begin{array}{ccccc} & & H^0(A) & \to & H^0(B) & & \\ & \nearrow & & & & \searrow & \\ H^1(C) & & & & & & H^0(C). \\ & \nwarrow & & & & \swarrow & \\ & & H^1(B) & \leftarrow & H^1(A) & & \end{array}$$

Supposons alors que $H^0(A)$ et $H^1(A)$ soient des groupes *finis*, et soient $h_0(A)$ et $h_1(A)$ leurs ordres. Le quotient

$$h(A) = h_0(A)/h_1(A)$$

est appelé le *quotient de Herbrand* de A. Vu ce qui précède, c'est le quotient des ordres

des groupes de cohomologie du complexe K(A); il est donc analogue à une caractéristique d'Euler-Poincaré.

[On peut préciser cette analogie en se plaçant dans le cadre des catégories abéliennes. On suppose que A parcourt les G-objets d'une catégorie abélienne $\mathcal{C}$, et l'on se donne une sous-catégorie $\mathcal{D}$ de $\mathcal{C}$; si l'on suppose que $H^0(A)$ et $H^1(A)$ appartiennent à $\mathcal{D}$, on définit $h(A)$ comme $H^0(A) - H^1(A)$, cette différence ayant un sens dans le *groupe de Grothendieck* $K(\mathcal{D})$ associé à $\mathcal{D}$. Ici, $\mathcal{D}$ est la catégorie des groupes abéliens finis, et $K(\mathcal{D})$ est le groupe multiplicatif des nombres rationnels > 0, cf. Chap. I, § 5. On pourrait évidemment considérer d'autres catégories, par exemple celle des espaces vectoriels de dimension finie, celle des groupes quasi-algébriques, etc.]

PROPOSITION 7. *Soit* $0 \to A \to B \to C \to 0$ *une suite exacte de G-modules et supposons que deux des trois quotients de Herbrand* $h(A)$, $h(B)$, $h(C)$ *sont définis. Le troisième l'est alors aussi, et l'on a* :

$$h(B) = h(A).h(C).$$

Cela résulte immédiatement de l'hexagone exact écrit ci-dessus. (De façon générale, lorsque des groupes finis $A_1, \ldots, A_{2n}$ forment un $2n$-gone exact, le produit alterné de leurs ordres est égal à 1.)

[On pourrait aussi invoquer « l'additivité » des caractéristiques d'Euler-Poincaré.]

PROPOSITION 8. *Si* A *est un* G*-module fini, on a* $h(A) = 1$.

La suite exacte :

$$0 \longrightarrow A^G \longrightarrow A \xrightarrow{D} A \longrightarrow A_G \longrightarrow 0$$

montre tout d'abord que A^G et A_G ont même nombre d'éléments. La suite exacte :

$$0 \longrightarrow H^1(A) \longrightarrow A_G \xrightarrow{N} A^G \longrightarrow H^0(A) \longrightarrow 0$$

montre ensuite que $H^1(A)$ et $H^0(A)$ ont même nombre d'éléments, c.q.f.d.

[On peut aussi dire que la caractéristique d'Euler-Poincaré de K(A) est définie, et évidemment égale à 1; comme la caractéristique d'Euler-Poincaré est invariante par passage à la cohomologie, on en déduit bien $h(A) = 1$.]

COROLLAIRE. *Soient* A *et* B *deux* G*-modules, et soit* $f : A \to B$ *un* G*-homomorphisme dont le noyau et le conoyau sont finis. Alors* A *et* B *ont même quotient de Herbrand* (de façon plus correcte, si $h(A)$ est défini, $h(B)$ l'est aussi et est égal à $h(A)$, et de même si $h(B)$ est défini).

Cela résulte des propositions 7 et 8.

Exercice. Étendre la définition du quotient de Herbrand et les propositions 7 et 8 aux groupes finis à cohomologie périodique (cf. Cartan-Eilenberg [13], Chap. XII, § 11).

§ 5. *Quotient de Herbrand dans le cas cyclique d'ordre premier*

Soit G un groupe cyclique d'ordre premier p, et soit A un groupe abélien; si l'on fait opérer trivialement G sur A, on a :

$$\begin{cases} H^1(G, A) = {}_pA \text{ (sous-groupe de A formé des éléments } a \text{ tels que } pa = 0) \\ H^2(G, A) = A_p = A/pA. \end{cases}$$

Si les groupes ${}_pA$ et A_p sont finis, on peut définir le « quotient de Herbrand trivial » de A, noté $\varphi(A)$, qui est le quotient de l'ordre de A_p par celui de ${}_pA$. La proposition suivante, due à Tate, généralise un théorème de Chevalley ([17], th. 10. 3) :

PROPOSITION 9. *Soit* A *un* G*-module tel que* $\varphi(A)$ *soit défini (autrement dit, le noyau et le conoyau de* $p : A \to A$ *sont finis). Alors* $\varphi(A^G)$, $\varphi(A_G)$ *et* $h(A)$ *sont définis, et l'on a :*

$$h(A)^{p-1} = \varphi(A^G)^p/\varphi(A) = \varphi(A_G)^p/\varphi(A).$$

La démonstration de Tate repose sur le fait que $\mathbf{Z}[G]/(N)$ est isomorphe à l'anneau des entiers du corps des racines p-ièmes de l'unité, et que, dans cet anneau, l'idéal engendré par p est la puissance $(p-1)$-ième de l'idéal engendré par D. Cette démonstration est reproduite dans Artin-Tate [8]. Nous allons donner ci-dessous une autre démonstration, nettement plus longue, mais qui a l'avantage d'élucider en même temps la structure des G-modules A tels que $\varphi(A)$ soit défini.

LEMME 1. *Soit* $0 \to A' \to A \to A'' \to 0$ *une suite exacte de* G*-modules tels que* $\varphi(A')$ *et* $\varphi(A'')$ *soient définis. Si la prop.* 9 *est vraie pour* A' *et* A'', *elle l'est pour* A.

Il est clair que $\varphi(A)$ et $h(A)$ sont définis, et que l'on a $\varphi(A) = \varphi(A').\varphi(A'')$ et $h(A) = h(A').h(A'')$. On a en outre la suite exacte :

$$0 \to A'^G \to A^G \to A''^G \to H^1(G, A') \to \cdots,$$

et comme $H^1(A')$ est fini (puisque $h(A')$ est défini), ceci donne :

$$0 \to A'^G \to A^G \to A''^G \to N \to 0,$$

où N est un groupe fini.

On en conclut que $\varphi(A^G) = \varphi(A'^G).\varphi(A''^G)$, d'où aussitôt le lemme, par multiplication. (On raisonne de même pour A_G.)

LEMME 2. *Soit* A *un* G*-module tel que* $\varphi(A)$ *soit défini. Il existe alors une suite exacte*

$$0 \to A' \to A \to A'' \to 0$$

de G*-modules, où* A' *est un groupe abélien de type fini, et* A'' *vérifie* $A'' = pA''$; *de plus* $\varphi(A')$ *et* $\varphi(A'')$ *sont définis.*

Par hypothèse, A/pA est fini. Il existe donc un sous-groupe de type fini de A qui s'applique sur A/pA; quitte à remplacer ce sous-groupe par la somme de ses

transformés par les éléments de G, on peut le supposer stable par G. Désignons-le alors par A', et posons $A'' = A/A'$. On a la suite exacte :

$$0 \to {}_pA' \to {}_pA \to {}_pA'' \to A'_p \to A_p \to A''_p \to 0.$$

Par construction, $A'_p \to A_p$ est surjectif; donc $A''_p = 0$, i.e. $A'' = pA''$; de plus, puisque A' est de type fini sur **Z**, ${}_pA'$ et A'_p sont finis, i.e. $\varphi(A')$ est défini; il est évident que $\varphi(A'')$ est défini.

Les lemmes 1 et 2 permettent de se borner au cas où A est, ou bien de type fini, ou bien divisible par p.

a) Cas où A est un groupe abélien de type fini,

Remarquons d'abord que, si A et A' sont deux G-modules de type fini, tels que $A \otimes_{\mathbf{Z}} \mathbf{Q}$ et $A' \otimes_{\mathbf{Z}} \mathbf{Q}$ soient G-isomorphes, on a $h(A) = h(A')$, $\varphi(A) = \varphi(A')$, $\varphi(A^G) = \varphi(A'^G)$ et $\varphi(A_G) = \varphi(A'_G)$: cela résulte en effet du corollaire à la prop. 8. Cela permet de se ramener au cas où $A_{\mathbf{Q}} = A \otimes_{\mathbf{Z}} \mathbf{Q}$ est une représentation linéaire *simple* de $\mathbf{Q}[G]$. Mais l'algèbre $\mathbf{Q}[G]$ est produit de $\mathbf{Q}$ par le corps K des racines p-ièmes de l'unité (on définit immédiatement un homomorphisme $\mathbf{Q}[G] \to \mathbf{Q} \times K$, et un raisonnement de dimension montre que c'est un isomorphisme — bien entendu, il faut utiliser le fait que $[K : \mathbf{Q}] = p - 1$, cf. Chap. IV, § 4). Il y a donc *deux* représentations simples de $\mathbf{Q}[G]$ à considérer :

a1) La représentation triviale de degré 1.

Dans ce cas, on peut prendre pour A' le groupe **Z** sur lequel G opère trivialement. On a $h(A) = \varphi(A) = \varphi(A^G)$, et la formule de la prop. 9 est bien vérifiée.

a2) La représentation de degré $p - 1$ donnée par K.

On peut prendre pour A' le quotient de $\mathbf{Z}[G]$ par **Z**. Comme $h(\mathbf{Z}[G]) = 1$, on a $h(A) = p^{-1}$; on voit tout de suite que $\varphi(A) = p$, $\varphi(A^G) = \varphi(A_G) = 1$, d'où la formule cherchée.

b) Cas où A est divisible par p.

Soit A' le sous-groupe de A formé des $a \in A$ tels qu'il existe n avec $p^n a = 0$. Dans $A'' = A/A'$ la multiplication par p est bijective, et il s'ensuit que

$$H^q(G, A'') = 0$$

pour tout $q \geqslant 1$; en particulier, on a $h(A'') = 1$, $\varphi(A''^G) = 1$, et $\varphi(A'') = 1$. On est ainsi ramené à A', c'est-à-dire au cas où tout élément de A est annulé par une puissance convenable de p (A étant toujours divisible par p, et ${}_pA$ fini).

On pourrait alors déterminer la structure de A, par un raisonnement semblable à celui de *a*). On peut aussi, et c'est plus rapide, utiliser *la dualité de Pontrjagin* : elle transforme A en un groupe compact $\hat{A}$, qui est un module libre de type fini sur l'anneau $\mathbf{Z}_p$ des entiers p-adiques, et sur lequel opère G. On vérifie tout de suite que $h(A) = h(\hat{A})^{-1}$, $\varphi(A) = \varphi(\hat{A})^{-1}$, $\varphi(A^G) = \varphi(\hat{A}_G)^{-1}$. On est donc ramené à

démontrer la formule pour $\hat{A}$, ce qui se fait comme dans le cas *a*), l'anneau $\mathbf{Z}_p$ remplaçant l'anneau $\mathbf{Z}$ [on sait en effet (cf. Chap. IV, § 4) que le corps obtenu en adjoignant à $\mathbf{Q}_p$ une racine primitive p-ième de l'unité est de degré $p-1$, et la classification des représentations simples de G sur $\mathbf{Q}_p$ est donc la même que sur $\mathbf{Q}$.]

Remarques. 1) La suite exacte $0 \longrightarrow A^G \longrightarrow A \xrightarrow{D} A \longrightarrow A_G \longrightarrow 0$ montre directement que $\varphi(A^G) = \varphi(A_G)$.

2) Le raisonnement fait plus haut montre que tout G-module A tel que $\varphi(A)$ soit défini admet une suite de composition dont les facteurs sont de l'un des six types suivants :

i) un groupe fini,

ii) un groupe où la multiplication par p est bijective,

iii) le groupe $\mathbf{Z}$ sur lequel G opère trivialement,

iv) le groupe $\Lambda = \mathbf{Z}[G]/\mathbf{Z}$,

v) le groupe $T = \mathbf{Q}_p/\mathbf{Z}_p$ sur lequel G opère trivialement,

vi) le groupe $T \otimes_{\mathbf{Z}} \Lambda$ sur lequel G opère comme sur Λ.

Exercices. 1. Comment faut-il modifier la prop. 9 lorsque G est un groupe cyclique d'ordre une puissance de p?

2. Soient G_1 et G_2 deux groupes cycliques d'ordre premier p, et soit $G = G_1 \times G_2$. Soit A un G-module tel que ${}_pA$ et A_p soient finis. On note $h^1(A)$ le quotient de Herbrand de A par rapport à G_1, et de même pour $h^2(A)$. En utilisant la proposition 9, démontrer la formule suivante (qui se réduit à la prop. 9 lorsque l'un des deux groupes opère trivialement) :

$$h^1(A^{G_2})_p . h^2(A) = h^2(A^{G_1}) . h^1(A).$$

CHAPITRE IX

LES THÉORÈMES DE TATE ET DE NAKAYAMA

§ 1. *p*-groupes

Soit p un nombre premier. On sait qu'un groupe fini G est appelé un *p-groupe* si son ordre Card (G) est une puissance de p.

LEMME 1. *Soit* G *un p-groupe opérant sur un ensemble fini* E, *et soit* E^G *l'ensemble des éléments de* E *invariants par* G. *On a alors* :

$$\text{Card}\,(E^G) \equiv \text{Card}\,(E) \mod p.$$

En effet, $E - E^G$ est réunion d'orbites disjointes Gx non réduites à un point, et on a évidemment $\text{Card}\,(Gx) \equiv 0 \mod p$.

LEMME 2. *Si un p-groupe opère sur un p-groupe non réduit à l'élément neutre, alors les points fixes forment un sous-groupe non réduit à l'élément neutre.*

En effet, le nombre de ces points fixes est divisible par p, d'après le lemme 1.

THÉORÈME 1. *Le centre d'un p-groupe non réduit à l'élément neutre n'est pas réduit à l'élément neutre.*

Cela résulte du lemme précédent, en faisant opérer le groupe sur lui-même par automorphismes intérieurs.

COROLLAIRE. *Un groupe* G *d'ordre* p^n *admet une suite de composition*

$$\{1\} = G_n \subset G_{n-1} \subset \cdots \subset G_0 = G$$

où les G_i *sont invariants dans* G, *et où les* G_i/G_{i+1} *sont cycliques d'ordre* p.

Cela résulte du th. 1, par récurrence sur n.

THÉORÈME 2. *Soit* G *un p-groupe. Toute représentation linéaire non nulle de* G *sur un corps de caractéristique* p *contient la représentation unité.*

Soit E l'espace de la représentation. Soit x un élément non nul de E, et soit H le sous-groupe de E engendré par les $s.x$, $s \in G$; c'est un espace vectoriel de dimen-

sion finie sur le corps premier $\mathbf{F}_p$. En appliquant à H le lemme 2, on voit qu'il existe $y \in H$, $y \neq 0$, tel que $s.y = y$, c.q.f.d.

COROLLAIRE. *Soit* G *un p-groupe, et soit k un corps de caractéristique p. Le noyau* I_G *de l'homomorphisme d'augmentation* $k[G] \to k$ *est le radical de* $k[G]$, *et c'est un idéal nilpotent.*

En effet, le radical r de $k[G]$ est l'intersection des noyaux des représentations irréductibles de $k[G]$ (ou de G, c'est la même chose), et le théorème 2 montre que G n'a qu'une seule représentation irréductible, la représentation unité; on a donc $r = I_G$. Comme $k[G]$ est une k-algèbre de dimension finie, on sait que son radical est nilpotent (cf. Bourbaki, *Alg.*, Chap. VIII, § 6, th. 3); donc I_G est nilpotent.

§ 2. *Groupes de Sylow*

THÉORÈME 3 (Sylow). *Soit* G *un groupe fini d'ordre* $n = p^m q$, *avec p premier et* $(p, q) = 1$. *Alors* G *contient des sous-groupes d'ordre* p^m (appelés sous-groupes de Sylow de G), *ces sous-groupes sont conjugués, et tout p-groupe contenu dans* G *est contenu dans l'un d'eux.*

Démonstration (d'après Miller et Wielandt). Soit E l'ensemble des parties X de G ayant p^m éléments. Le groupe G opère sur E par translations. On a

$$\text{Card (E)} = \binom{n}{p^m}.$$

LEMME 3. *Si* $n = p^m q$, *avec* $(p, q) = 1$, *on a* $\binom{n}{p^m} \equiv q \mod p$.

En effet, soient X et Y deux indéterminées sur un corps de caractéristique p. On a :

$$(X + Y)^n = (X + Y)^{p^m q} = (X^{p^m} + Y^{p^m})^q = X^{p^m q} + q\, X^{p^m(q-1)} Y^{p^m} + \cdots + Y^{p^m q},$$

et en comparant avec le développement de $(X + Y)^n$, on obtient bien la congruence cherchée.

Revenons à la démonstration du théorème de Sylow. Le lemme 3 montre que Card (E) $\not\equiv 0 \mod p$. Il s'ensuit que, pour au moins un $X \in E$, l'orbite G.X de X est telle que (Card G.X) $\not\equiv 0 \mod p$. Si H désigne l'ensemble des $s \in G$ tels que $s.X = X$, G.X est équipotent à G/H, d'où Card (G/H) $\not\equiv 0 \mod p$, ce qui signifie que p^m divise l'ordre de H. Mais d'autre part, si $x \in X$, on a $H \subset X.x^{-1}$, d'où

$$\text{Card (H)} \leqslant \text{Card (X)} = p^m.$$

On a donc Card (H) $= p^m$, ce qui démontre *l'existence* des sous-groupes de Sylow.

Soit maintenant H' un p-groupe contenu dans G, et faisons opérer H' sur l'espace homogène G/H, où H est un p-groupe de Sylow de G. On a Card (G/H) $= q \not\equiv 0 \mod p$. Le lemme 1, appliqué à G/H, montre alors que l'ensemble des points de G/H invariants par H' est non vide, ce qui signifie que H' est contenu dans un conjugué de H. Si en outre Card (H') $= p^m$, H' est donc égal à un conjugué de H, ce qui achève la démonstration.

Les propriétés « fonctorielles » suivantes des groupes de Sylow résultent immédiatement du théorème 3 :

a) Si G′ est un sous-groupe de G, tout p-groupe de Sylow de G′ est l'intersection avec G′ d'un p-groupe de Sylow de G.

b) Si G′ est un quotient de G, les p-groupes de Sylow de G′ sont les images des p-groupes de Sylow de G.

Les groupes de Sylow interviennent en cohomologie à cause du théorème suivant :

THÉORÈME 4. *Soit* G *un groupe fini, soit* p *un nombre premier, et soit* G_p *un* p*-groupe de Sylow de* G. *Pour tout* G*-module* A, *et pour tout* $n \in \mathbf{Z}$, *l'homomorphisme*

$$\mathrm{Res} : \hat{H}^n(G, A) \to \hat{H}^n(G_p, A)$$

est injectif sur la composante p*-primaire de* $\hat{H}^n(G, A)$.

Soit $x \in \hat{H}^n(G, A)$ tel que $\mathrm{Res}(x) = 0$. Si $q = \mathrm{Card}(G/G_p)$, on a

$$q.x = \mathrm{Cor} \circ \mathrm{Res}\,(x) = 0 \qquad \text{(Chap. VIII, prop. 4)}.$$

D'autre part, si x appartient à la composante p-primaire de $\hat{H}^n(G, A)$, il existe un entier a tel que $p^a.x = 0$. Comme $(q, p^a) = 1$, on en déduit bien $x = 0$.

COROLLAIRE. *Soient* G *un groupe fini,* A *un* G*-module,* n *un entier. Supposons que, pour tout nombre premier* p, *on ait* $\hat{H}^n(G_p, A) = 0$, G_p *désignant un* p*-groupe de Sylow de* G. *Alors* $\hat{H}^n(G, A) = 0$.

En effet, toutes les composantes primaires du groupe de torsion $\hat{H}^n(G, A)$ sont nulles.

Remarque. On trouvera dans Cartan-Eilenberg ([13], Chap. XII, th. 10. 1) une caractérisation de *l'image* de $\mathrm{Res} : \hat{H}^n(G, A) \to \hat{H}^n(G_p, A)$.

Exercice. Les notations étant celles de la démonstration du th. 3, soit d le nombre des p-groupes de Sylow de G. Montrer que le nombre des translatés de ces sous-groupes est égal à dq. En comparant avec le nombre d'éléments de E montrer que $d \equiv 1 \bmod p$.

§ 3. *Modules induits et modules cohomologiquement triviaux*

Soit G un groupe fini, et soit A un G-module. On dit que A est *cohomologiquement trivial* si, pour tout sous-groupe H de G, et pour tout $n \in \mathbf{Z}$, on a $\hat{H}^n(H, A) = 0$.

Exemples. Tout module *induit* est cohomologiquement trivial; en effet un tel module est induit pour tout sous-groupe H de G, et l'on sait (Chap. VIII, § 1) que cela entraîne la nullité de sa cohomologie. Il en est de même des modules *relativement projectifs*, puisqu'ils sont facteurs directs de modules induits.

A partir d'un module induit A, on peut en fabriquer d'autres par le procédé général suivant :

Soit $\mathcal{C}$ la catégorie des groupes abéliens, et soit $T : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ un bifoncteur additif, que nous supposerons bicovariant pour fixer les idées. Si A et B sont deux G-modules, on définit une structure de G-module sur T(A, B) de la manière suivante : tout $s \in G$ définit un élément $s_A \in \mathrm{Hom}(A, A)$, et un élément $s_B \in \mathrm{Hom}(B, B)$, donc un élément $T(s_A, s_B) \in \mathrm{Hom}(T(A, B), T(A, B))$: c'est l'automorphisme de T(A, B) associé à s.

PROPOSITION 1. *Si* A *est induit (resp. relativement projectif), alors* T(A, B) *est induit (resp. relativement projectif), donc cohomologiquement trivial.*

Quitte à passer à un facteur direct, on peut se borner au cas où A est induit, c'est-à-dire somme directe des $s.A'$, où A' est un sous-groupe. Le groupe T(A, B) est alors somme directe des $T(s.A', B)$; mais $T(s.A', B) = T(s.A', s.B) = s.T(A', B)$. Donc T(A, B) est induit, c.q.f.d.

COROLLAIRE. *Soient* A *et* B *deux* G*-modules, l'un d'eux étant relativement projectif. Les* G*-modules ci-dessous sont relativement projectifs (donc cohomologiquement triviaux)* :

$A \otimes B$, Hom (A, B), Tor (A, B), Ext (A, B).

[Bien entendu, les foncteurs $\otimes$, Hom, ..., sont relatifs à l'anneau Z des entiers.]

§ 4. *Cohomologie d'un p-groupe*

LEMME 4. *Soit* G *un p-groupe et soit* A *un* G*-module tel que* $pA = 0$. *Les trois conditions ci-dessous sont équivalentes* :

(i) $A = 0$.

(ii) $H^0(G, A) = 0$.

(iii) $H_0(G, A) = 0$.

Les implications (i) $\Longrightarrow$ (ii) et (i) $\Longrightarrow$ (iii) sont triviales. L'implication (ii) $\Longrightarrow$ (i) a déjà été démontrée (théorème 2). Montrons que (iii) $\Longrightarrow$ (i). Soit $A' = \mathrm{Hom}(A, \mathbf{F}_p)$ le dual de A, considéré comme $\mathbf{F}_p$-espace vectoriel. On voit tout de suite que $H^0(G, A')$ est dual de $H_0(G, A)$. On a donc $H^0(G, A') = 0$, d'où $A' = 0$ et $A = 0$.

[Autre démonstration de (iii) $\Longrightarrow$ (i) : Soit r l'idéal d'augmentation de $\mathbf{F}_p[G]$. La nullité de $H_0(G, A)$ signifie que $A = rA$. Mais r est nilpotent (cor. au th. 2). Donc $A = 0$.]

LEMME 5. *Les hypothèses étant celles du lemme* 4, *supposons que* $H_1(G, A) = 0$. *Alors* A *est un module libre sur l'algèbre* $\Lambda = \mathbf{F}_p[G]$.

Soit encore r l'idéal d'augmentation de Λ. On a $A/rA = H_0(G, A)$, c'est un espace vectoriel sur $\mathbf{F}_p$. Soit h_λ une base de cet espace et relevons-la en une famille $a_\lambda \in A$. Puisque les h_λ engendrent A/rA, les a_λ engendrent A (appliquer le lemme 4 au quotient de A par le sous-Λ-module engendré par les a_λ). On a ainsi défini un G-homomorphisme surjectif $L \to A$, où L est un Λ-module libre; par construction, cet homomorphisme induit un isomorphisme de L/rL sur A/rA. Soit R son noyau.

On a une suite exacte :

$$H_1(G, A) \to H_0(G, R) \to H_0(G, L) \to H_0(G, A).$$

Comme $H_1(G, A) = 0$ et que $H_0(G, L) \to H_0(G, A)$ est bijectif, on en déduit que $H_0(G, R) = 0$, d'où $R = 0$ (lemme 4), c.q.f.d.

Remarque. Les deux lemmes ci-dessus sont des cas particuliers de théorèmes généraux sur les « anneaux locaux non commutatifs », cf. Bourbaki, *Alg. comm.*, Chap. II, § 3.

THÉORÈME 5. *Soit* G *un p-groupe et soit* A *un* G*-module annulé par p. Les conditions suivantes sont équivalentes* :

(i) *Il existe un entier q tel que* $\hat{H}^q(G, A) = 0$,

(ii) A *est cohomologiquement trivial,*

(iii) A *est un* G*-module induit,*

(iv) A *est un* $F_p[G]$*-module libre.*

Il suffit évidemment de démontrer (i) $\Rightarrow$ (iv). Un procédé de « décalage » déjà utilisé plusieurs fois permet de construire un G-module B, annulé par p, avec $\hat{H}^n(G, A) = \hat{H}^{n-q-2}(G, B)$. Si $\hat{H}^q(G, A) = 0$, $H_1(G, B) = 0$, donc, par le lemme 5, B est Λ-libre. Ses groupes de cohomologie sont alors nuls, en particulier

$$H_1(G, A) = \hat{H}^{-2}(G, A) = \hat{H}^{-q-4}(G, B) = 0,$$

et le lemme 5 permet de conclure.

THÉORÈME 6. *Soit* G *un p-groupe et soit* A *un* G*-module sans p-torsion. Il y a équivalence entre les conditions* :

(i) $\hat{H}^q(G, A) = 0$ *pour deux dimensions consécutives,*

(ii) A *est cohomologiquement trivial,*

(iii) *Le* $F_p[G]$*-module* A/pA *est libre.*

Le G-module A n'ayant pas de p-torsion, on a la suite exacte :

$$0 \to A \xrightarrow{p} A \to A/pA \to 0.$$

Passant à la cohomologie, on obtient la suite exacte :

$$\hat{H}^q(G, A) \xrightarrow{p} \hat{H}^q(G, A) \to \hat{H}^q(G, A/pA) \to \hat{H}^{q+1}(G, A) \xrightarrow{p} \hat{H}^{q+1}(G, A).$$

Si $\hat{H}^q(G, A) = \hat{H}^{q+1}(G, A) = 0$, cette suite montre que $\hat{H}^q(G, A/pA) = 0$, et A/pA est libre d'après le théorème 5. Donc (i) $\Rightarrow$ (iii). Si (iii) est vérifiée, la même suite exacte montre que l'homothétie de rapport p est bijective dans tous les $\hat{H}^q(G, A)$; comme cette homothétie est nilpotente, on a $\hat{H}^q(G, A) = 0$. Le même raisonnement s'applique à tout sous-groupe H de G, car A/pA est $F_p[H]$-libre. Donc (iii) $\Rightarrow$ (ii). Enfin l'implication (ii) $\Rightarrow$ (i) est triviale.

COROLLAIRE. *Soit* A *un* G*-module* **Z***-libre vérifiant les conditions équivalentes du théorème* 6. *Pour tout* G*-module sans torsion* B, *le* G*-module* $N = \mathrm{Hom}_{\mathbf{Z}}(A, B)$ *est cohomologiquement trivial.*

Le module N est sans torsion. On va vérifier que N/pN est cohomologiquement trivial, ce qui entraînera le résultat cherché en vertu des théorèmes précédents. La suite exacte :

$$0 \to B \xrightarrow{p} B \to B/pB \to 0$$

donne la suite exacte :

$$0 \to N \xrightarrow{p} N \to \mathrm{Hom}\,(A, B/pB) \to 0$$

d'où un isomorphisme $N/pN = \mathrm{Hom}\,(A/pA, B/pB)$. Or A/pA est libre sur $\mathbf{F}_p[G]$, donc induit, et N/pN est cohomologiquement trivial d'après le corollaire à la proposition 1.

Remarque. En fait, ce corollaire n'est qu'un lemme pour le théorème 7. Une fois ce théorème démontré, on saura en effet que A est projectif, donc que N est relativement projectif.

§ 5. *Cohomologie d'un groupe fini*

THÉORÈME 7. *Soient* G *un groupe fini,* A *un* G*-module* **Z***-libre, et* G_p *les groupes de Sylow de* G. *Il y a équivalence entre* :

(i) *Pour tout nombre premier* p *le* G_p*-module* A *vérifie les conditions équivalentes du théorème* 6,

(ii) A *est* $\mathbf{Z}[G]$*-projectif.*

Il faut montrer que (i) entraîne (ii). Écrivons A comme quotient d'un $\mathbf{Z}[G]$-module libre L :

$$0 \to N \to L \to A \to 0.$$

Le $\mathbf{Z}$-module A étant libre, on en déduit la suite exacte :

$$(*) \qquad 0 \to \mathrm{Hom}_{\mathbf{Z}}(A, N) \to \mathrm{Hom}_{\mathbf{Z}}(A, L) \to \mathrm{Hom}_{\mathbf{Z}}(A, A) \to 0.$$

D'après le corollaire au théorème 6, (i) entraîne que le G_p-module $\mathrm{Hom}_{\mathbf{Z}}(A, N)$ a une cohomologie nulle en toute dimension, donc que $H^1(G, \mathrm{Hom}_{\mathbf{Z}}(A, N)) = 0$ par le corollaire au théorème 4.

La suite exacte de cohomologie de (*) montre alors que

$$\mathrm{Hom}_G(A, L) \to \mathrm{Hom}_G(A, A)$$

est surjectif, donc que l'application identique de A se prolonge en un G-homomorphisme de A dans L, c'est-à-dire que A est facteur direct de L comme G-module, donc projectif.

Remarque. Soient P et P′ deux modules projectifs de type fini sur $\mathbf{Z}[G]$; on dit qu'ils sont équivalents s'il existe deux modules libres de type fini L et L′ tels que

$P \oplus L$ soit isomorphe à $P' \oplus L'$. Soit $P(G)$ l'ensemble des classes d'équivalence de $\mathbf{Z}[G]$-modules projectifs de type fini (pour la relation d'équivalence ci-dessus). La loi de composition $(P, P') \to P \oplus P'$ fait de $P(G)$ un groupe abélien, appelé *groupe des classes de G-modules projectifs*. Lorsque G est cyclique d'ordre premier p, Dock Sang Rim [51] a montré que $P(G)$ est isomorphe au groupe des classes d'idéaux du corps des racines p-ièmes de l'unité; en particulier, on peut avoir $P(G) \neq 0$, ce qui montre l'existence de G-modules projectifs qui ne sont pas libres. L'étude de $P(G)$ a été approfondie par Swan [62], qui a notamment montré que c'est un groupe *fini*.

LEMME 6. *Soit* $0 \to X_1 \to X_2 \to \cdots \to X_n \to 0$ *une suite exacte de G-modules. Si tous les* X_i, *sauf éventuellement l'un d'entre eux, sont cohomologiquement triviaux, alors ce dernier l'est aussi.*

Posons $N_i = \operatorname{Ker}(X_i \to X_{i+1})$, $N_0 = N_{n+1} = 0$. On a les $n+1$ suites exactes :

$$(E_i) \qquad 0 \to N_i \to X_i \to N_{i+1} \to 0, \qquad 0 \leqslant i \leqslant n.$$

Si X_i est cohomologiquement trivial pour $i \neq p$, on montre par la considération des suites $E_0, \ldots, E_{p-1}$ que $N_1, \ldots, N_p$ sont cohomologiquement triviaux, puis, par celle des suites $E_n, \ldots, E_{p+1}$ que $N_n, \ldots, N_{p+1}$ le sont aussi, et on conclut en utilisant la suite E_p.

THÉORÈME 8. *Soit* A *un G-module quelconque. Il y a équivalence entre* :

(i) *Pour tout nombre premier p,* $\hat{H}^q(G_p, A) = 0$ *pour deux valeurs consécutives de q (pouvant dépendre de p),*

(ii) A *est cohomologiquement trivial,*

(iii) *Il existe une suite exacte* $0 \to P_k \to P_{k-1} \to \cdots \to P_0 \to A \to 0$ *où les* P_i *sont des* $\mathbf{Z}[G]$*-modules projectifs,*

(iv) *Il existe une suite exacte* $0 \to P_1 \to P_0 \to A \to 0$ *où les* P_i *sont* $\mathbf{Z}[G]$*-projectifs.*

(Dans la terminologie de Cartan-Eilenberg, la condition (iii) signifie que la *dimension projective* de A est finie, et la condition (iv) qu'elle est $\leqslant 1$.)

On a (iv) $\Longrightarrow$ (iii) trivialement, (iii) $\Longrightarrow$ (ii) d'après le lemme 6, et (ii) $\Longrightarrow$ (i) trivialement. Montrons que (i) $\Longrightarrow$ (iv) : Soit $0 \to R \to L \to A \to 0$ une suite exacte de G-modules, avec L libre sur $\mathbf{Z}[G]$. *A fortiori*, L est libre sur $\mathbf{Z}$, donc aussi R. Comme d'autre part R vérifie l'hypothèse (i) du théorème 7, on en conclut que R est $\mathbf{Z}[G]$-projectif, c.q.f.d.

THÉORÈME 9. *Soient* A *et* B *deux G-modules, avec* A *cohomologiquement trivial. Pour que* $A \otimes B$ (resp. $\operatorname{Hom}(A, B)$, resp. $\operatorname{Hom}(B, A)$) *soit cohomologiquement trivial, il faut et il suffit que* $\operatorname{Tor}(A, B)$ (resp. $\operatorname{Ext}(A, B)$, resp. $\operatorname{Ext}(B, A)$) *le soit.*

(Ici encore, les foncteurs $\otimes$, Tor, etc., sont pris sur l'anneau $\mathbf{Z}$.)

D'après le théorème 8, (iv), il existe une résolution de A par des modules projectifs :

$$0 \to P_1 \to P_0 \to A \to 0.$$

On a donc une suite exacte :

$$0 \to \mathrm{Tor}\,(A, B) \to P_1 \otimes B \to P_0 \otimes B \to A \otimes B \to 0.$$

Le corollaire à la proposition 1 montre que $P_1 \otimes B$ et $P_0 \otimes B$ sont cohomologiquement triviaux; en appliquant le lemme 6, on voit bien alors que $A \otimes B$ est cohomologiquement trivial si et seulement si $\mathrm{Tor}\,(A, B)$ l'est. Même raisonnement pour $\mathrm{Hom}\,(A, B)$ et $\mathrm{Ext}\,(A, B)$. Pour $\mathrm{Hom}\,(B, A)$ on utilise la suite exacte à six termes :

$$0 \to \mathrm{Hom}\,(B, P_1) \to \mathrm{Hom}\,(B, P_0) \to \mathrm{Hom}\,(B, A) \to \mathrm{Ext}\,(B, P_1) \to \mathrm{Ext}\,(B, P_0) \to \mathrm{Ext}\,(B, A) \to 0.$$

Le corollaire à la proposition 1 montre que les quatre modules

$$\mathrm{Hom}\,(B, P_1), \qquad \mathrm{Hom}\,(B, P_0), \qquad \mathrm{Ext}\,(B, P_1), \qquad \mathrm{Ext}\,(B, P_0)$$

sont cohomologiquement triviaux, et on conclut de la même manière, en appliquant le lemme 6.

COROLLAIRE. *Si* A *est cohomologiquement trivial, et si* A *ou* B *est sans torsion, alors* $A \otimes B$ *est cohomologiquement trivial.*

En effet, $\mathrm{Tor}\,(A, B)$ est nul, donc cohomologiquement trivial.

Exercices. 1) Montrer que, si A est cohomologiquement trivial, et si, pour tout p divisant l'ordre de G, l'un des groupes A et B est sans p-torsion, alors $A \otimes B$ est cohomologiquement trivial. (Montrer que $\mathrm{Tor}(A, B)$ est cohomologiquement trivial et appliquer ensuite le théorème 9.)

2) Soit G le groupe cyclique d'ordre 6. Montrer qu'il existe un G-module A tel que $\hat{H}^n(G, A) = 0$ pour tout $n \in \mathbf{Z}$, qui n'est pas cohomologiquement trivial. (Prendre $A = \mathbf{Z}/3\mathbf{Z}$ sur lequel G opère par $x \to -x$, et remarquer que $\hat{H}^0(g, A) \neq 0$ si g désigne le sous-groupe d'ordre 3 de G.)

3) Soit G le groupe cyclique d'ordre 2, et soit $A = \mathbf{Z}/8\mathbf{Z}$; on fait opérer G sur A par $x \to 3x$. Soit $B = \mathbf{Z}/2\mathbf{Z}$ sur lequel G opère trivialement. Montrer que A est cohomologiquement trivial, mais que $A \otimes B$ ne l'est pas. En déduire que A n'est pas relativement projectif, cf. [13], p. 263, exer. 3.

(Noter que A est isomorphe au groupe multiplicatif $\mathbf{F}_9^*$ du corps à 9 éléments, sur lequel opère le groupe de Galois de l'extension $\mathbf{F}_9/\mathbf{F}_3$.)

§ 6. *Résultats duaux*

LEMME 7. *Soit* G *un groupe fini, et soit* A *un* G*-module qui soit* $\mathbf{Z}[G]$*-injectif. Alors* A *est* $\mathbf{Z}$*-injectif (c'est-à-dire divisible).*

Soit C un groupe abélien. On doit montrer que le foncteur $\mathrm{Hom}_{\mathbf{Z}}(C, A)$ est exact. Or on sait que, si l'on note Λ l'anneau $\mathbf{Z}[G]$, on a un isomorphisme fonctoriel :

$$\mathrm{Hom}_{\mathbf{Z}}(C, A) = \mathrm{Hom}_{\Lambda}(C \otimes_{\mathbf{Z}} \Lambda, A).$$

Comme Λ est $\mathbf{Z}$-libre, le foncteur $C \otimes_{\mathbf{Z}} A$ est exact, et comme A est Λ-injectif, il en est de même du foncteur $\mathrm{Hom}_{\Lambda}(\ ,\ A)$, d'où le résultat cherché.

THÉORÈME 10 (dual du théorème 7). *Soit* G *un groupe fini, et soit* A *un* G*-module* $\mathbf{Z}$*-injectif. Pour que* A *soit cohomologiquement trivial, il faut et il suffit qu'il soit* $\mathbf{Z}[G]$*-injectif.*

La suffisance est triviale. Pour voir la nécessité, plongeons A dans un module I qui soit $\mathbf{Z}[G]$-injectif. On a une suite exacte :

$$0 \to A \to I \to R \to 0.$$

Puisque A est $\mathbf{Z}$-injectif, on a une suite exacte :

$$0 \to \mathrm{Hom}_{\mathbf{Z}}(R, A) \to \mathrm{Hom}_{\mathbf{Z}}(I, A) \to \mathrm{Hom}_{\mathbf{Z}}(A, A) \to 0.$$

Si A est cohomologiquement trivial, $\mathrm{Hom}_{\mathbf{Z}}(R, A)$ l'est aussi (théorème 9). La suite exacte de cohomologie montre alors que l'application

$$\mathrm{Hom}_{G}(I, A) \to \mathrm{Hom}_{G}(A, A)$$

est surjective, donc que A est facteur direct de I, et A est bien $\mathbf{Z}[G]$-injectif.

THÉORÈME 11 (dual du théorème 8). *Pour que* A *soit cohomologiquement trivial, il faut et il suffit qu'il existe une suite exacte* $0 \to A \to I_0 \to I_1 \to 0$ *où les* I_i *sont des* $\mathbf{Z}[G]$*-modules injectifs.*

Formons comme précédemment une suite exacte :

$$0 \to A \to I_0 \to R \to 0$$

où I_0 est $\mathbf{Z}[G]$-injectif. Puisque A est cohomologiquement trivial, il en est de même de R; d'autre part, puisque I_0 est $\mathbf{Z}[G]$-injectif, I_0 est $\mathbf{Z}$-injectif (lemme 7), et R l'est aussi. En appliquant à R le théorème 10, on en déduit bien que R est injectif, c.q.f.d.

Note. Les résultats des trois paragraphes précédents sont essentiellement dus à Nakayama ([47], [48]). Pour la présentation, j'ai suivi un mémoire de Dock Sang Rim [51], qui a grandement simplifié les démonstrations de Nakayama, et généralisé certains de ses résultats.

7. *Un théorème de comparaison*

THÉORÈME 12. *Soit* G *un groupe fini, soient* A *et* A′ *deux* G*-modules, et soit* $f : A' \to A$ *un* G*-homomorphisme. Pour tout nombre premier* p*, soit* G_p *un* p*-groupe de Sylow de* G*, et supposons qu'il existe un entier* n_p *tel que l'homomorphisme*

$$f_i^* : \hat{H}^i(G_p, A') \to \hat{H}^i(G_p, A)$$

soit surjectif pour $i = n_p$*, bijectif pour* $i = n_p + 1$*, injectif pour* $i = n_p + 2$.

Alors, si B *est un* G*-module tel que* Tor (A, B) = Tor (A′, B) = 0, *l'homomorphisme* :

$$\hat{H}^i(g, A' \otimes B) \to \hat{H}^i(g, A \otimes B)$$

est bijectif pour tout sous-groupe g *de* G, *et tout* $i \in \mathbf{Z}$. *En particulier,* $\hat{H}^i(g, A') \to \hat{H}^i(g, A)$ *est bijectif pour tout* i.

On va employer une construction analogue à celle du « mapping-cylinder » en topologie. Soit $\overline{A'}$ le module induit défini canoniquement par A′, et soit $i : A' \to \overline{A'}$ l'injection canonique de A′ dans $\overline{A'}$ (rappelons, cf. Chap. VII, § 6, qu'un élément de $\overline{A'}$ est une application $\varphi : G \to A'$, que l'on a $(s.\varphi)(t) = \varphi(ts)$, et $i(a)(t) = t.a$, si $a \in A'$). Posons $A^* = A \oplus \overline{A'}$. Le couple (f, i) définit une injection $\theta : A' \to A^*$; si A″ désigne le conoyau de θ, on a donc la suite exacte :

$$0 \to A' \to A^* \to A'' \to 0.$$

Comme $\overline{A'}$ est cohomologiquement trivial, la cohomologie de A* s'identifie à celle de A. La suite exacte de cohomologie, jointe à l'hypothèse faite sur les f_i^*, montre alors que l'on a :

$$\hat{H}^q(G_p, A'') = 0 \qquad \text{pour } q = n_p,\ n_p + 1.$$

D'après le théorème 8, il s'ensuit que A″ *est cohomologiquement trivial.* D'autre part, A′ est facteur direct dans $\overline{A'}$ (comme **Z**-module, bien entendu), donc aussi dans A*; comme A* est somme directe de A et d'un certain nombre de copies de A′, l'hypothèse faite sur B entraîne Tor (A*, B) = 0, d'où Tor (A″, B) = 0, et le théorème 9 montre que A″ ⊗ B est cohomologiquement trivial. La suite exacte :

$$0 \to A' \otimes B \to A^* \otimes B \to A'' \otimes B \to 0$$

permet d'en déduire que $\hat{H}^q(g, A' \otimes B) \to \hat{H}^q(g, A^* \otimes B)$ est bijectif. Comme il en est de même de $\hat{H}^q(g, A^* \otimes B) \to \hat{H}^q(g, A \otimes B)$, cela achève la démonstration.

Remarque. Supposons que A et A′ soient **Z**-libres. Les G-modules $\overline{A'}$ et A″ sont alors projectifs (le premier est même libre). En d'autres termes, on a factorisé f en :

$$A' \xrightarrow{i} A' \oplus P' \xrightarrow{F} A \oplus P \xrightarrow{\pi} A$$

avec P et P′ projectifs, F étant un isomorphisme, et i (resp. π) désignant l'injection (resp. la projection) évidente. Lorsque A et A′ sont de type fini, P et P′ peuvent être pris de type fini; dans la terminologie d'Eckmann-Hilton ([23], voir aussi l'exposé [58]), f est une *équivalence d'homotopie.*

Exercice. Avec les notations et hypothèses de la remarque ci-dessus, montrer que l'élément $(f) = P' - P$ du groupe P(G) ne dépend que de f, et pas du choix de P et P′. Montrer que $(fg) = (f) + (g)$. Montrer que $(f) = 0$ si et seulement si P et P′ peuvent être choisis libres de type fini sur **Z**[G].

§ 8. *Le théorème de Tate et Nakayama*

THÉORÈME 13. *Soient* G *un groupe fini*, A, B, C *trois* G*-modules, et* $\varphi : A \times B \to C$ *une application bilinéaire invariante par* G. *Soit* $q \in \mathbf{Z}$, *et soit* $a \in \hat{H}^q(G, A)$. *Pour tout sous-groupe* g *de* G, *et tout* G*-module* D, *notons*

$$f(n, g, D) : \hat{H}^n(g, B \otimes D) \to \hat{H}^{n+q}(g, C \otimes D)$$

l'homomorphisme défini par le cup produit avec la classe $a_g = \mathrm{Res}_{G/g}(a)$ (relativement à l'application bilinéaire évidente de $A \times (B \otimes D)$ dans $C \otimes D$).

Supposons que, pour tout nombre premier p, *et tout* p*-groupe de Sylow* G_p *de* G, *il existe un entier* n_p *tel que* $f(n, G_p, \mathbf{Z})$ *soit surjectif pour* $n = n_p$, *bijectif pour* $n = n_p + 1$, *et injectif pour* $n = n_p + 2$.

Alors $f(n, g, D)$ *est bijectif pour tout* n, *tout* g, *et tout* G*-module* D *tel que*

$$\mathrm{Tor}(B, D) = \mathrm{Tor}(C, D) = 0.$$

Traitons d'abord le cas $q = 0$. La classe $a \in \hat{H}^0(G, A)$ peut être représentée par un élément $a \in A^G$. En posant $f(b) = \varphi(a, b)$, on obtient un G-homomorphisme

$$f : B \to C.$$

Il est facile de vérifier que l'homomorphisme

$$f(n, g, D) : \hat{H}^n(g, B \otimes D) \to \hat{H}^n(g, C \otimes D)$$

est simplement l'homomorphisme induit par $f \otimes 1 : B \otimes D \to C \otimes D$, et l'on est ramené au théorème 12.

Le cas général se traite par décalage. Indiquons par exemple comment on passe de $q - 1$ à q. On plonge A dans le module induit canonique $\overline{A}$ qu'il définit, et l'on pose $A_1 = \overline{A}/A$; on définit de même $C_1 = \overline{C}/C$ et $\varphi_1 : A_1 \times B \to C_1$. La classe $a \in \hat{H}^q(G, A)$ s'écrit $a = \delta(a_1)$, $a_1 \in \hat{H}^{q-1}(G, A_1)$. Cette classe a_1 définit par cup-produit des homomorphismes

$$f_1(n, g, D) : \hat{H}^n(g, B \otimes D) \to \hat{H}^{n+q-1}(g, C_1 \otimes D).$$

En combinant f_1 avec l'isomorphisme

$$\delta : \hat{H}^{n+q-1}(g, C_1 \otimes D) \to \hat{H}^{n+q}(g, C \otimes D),$$

on obtient $f(n, g, D)$ (utiliser le fait que les cup-produits commutent aux cobords, cf. Chap. VIII, § 3). Si le théorème est vrai pour la classe a_1, il l'est donc aussi pour a.

Le cas particulier le plus important est le suivant :

THÉORÈME 14. *Soient* G *un groupe fini*, A *un* G*-module, et* a *un élément de* $H^2(G, A)$. *Pour tout nombre premier* p, *soit* G_p *un* p*-groupe de Sylow de* G, *et supposons que* :

(1) *On a* $H^1(G_p, A) = 0$.

(2) $H^2(G_p, A)$ *est engendré par* $\mathrm{Res}_{G/G_p}(a)$, *et d'ordre égal à celui de* G_p.

Alors, si D *est un* G*-module tel que* Tor (A, D) = 0, *le cup-produit par* $a_g = \mathrm{Res}_{G/g}(a)$ *induit des isomorphismes*

$$\hat{H}^n(g, D) \to \hat{H}^{n+2}(g, A \otimes D)$$

pour tout $n \in \mathbf{Z}$ *et pour tout sous-groupe* g *de* G.

On applique le théorème 13 avec $B = \mathbf{Z}$, $C = A$, $q = 2$, $\varphi : A \times \mathbf{Z} \to A$ étant l'application évidente. On prend $n_p = -1$. Pour $n = -1$, l'hypothèse (1) montre que le cup-produit est surjectif; pour $n = 1$, l'hypothèse (2) montre qu'il est bijectif; pour $n = 1$, il est injectif puisque $H^1(G_p, \mathbf{Z}) = 0$. Toutes les hypothèses sont donc vérifiées.

Corollaire (Tate [63]). *Pour tout* $n \in \mathbf{Z}$, *et pour tout sous-groupe* g *de* G, *le cup-produit par* a_g *définit un isomorphisme*

$$\hat{H}^n(g, \mathbf{Z}) \to \hat{H}^{n+2}(g, A).$$

C'est le cas particulier $D = \mathbf{Z}$.

On verra au Chapitre XI comment ce résultat s'applique aux formations de classes.

CHAPITRE X

COHOMOLOGIE GALOISIENNE

§ 1. Premiers exemples

Soit K/k une extension galoisienne finie, de groupe de Galois G. Le groupe G opère de façon naturelle sur le groupe additif de K ainsi que sur son groupe multiplicatif K^*; on peut donc parler des groupes de cohomologie correspondants.

PROPOSITION 1. *On a* $\hat{H}^n(G, K) = 0$ *pour tout* $n \in \mathbf{Z}$.

En effet, le théorème de la *base normale* (Bourbaki, *Alg.*, Chap. V, § 10) montre que K est un module *induit*, et l'on sait que la cohomologie d'un tel module est triviale.

[Si l'on veut éviter le théorème de la base normale, on peut simplement remarquer que K contient un élément de trace 1, ce qui entraîne que K est relativement projectif (Cartan-Eilenberg [13], p. 233, prop. 1. 1), donc cohomologiquement trivial.]

Passons maintenant au groupe multiplicatif :

PROPOSITION 2. *On a* $H^1(G, K^*) = 0$.

Soit $s \to a_s$ un 1-cocycle. Si $c \in K$, formons la « série de Poincaré »

$$b = \sum_{s \in G} a_s . s(c).$$

Il résulte du théorème d'indépendance linéaire des automorphismes (Bourbaki, *loc. cit.*, § 7, n° 5) que l'on peut choisir c de telle sorte que $b \neq 0$. D'autre part, on a :

$$\begin{aligned} s(b) &= \sum s(a_t) . st(c) \\ &= \sum a_s^{-1} a_{st} . st(c) = a_s^{-1} . b \end{aligned}$$

ce qui montre que a_s est un cobord, c.q.f.d.

COROLLAIRE. *Si* G *est engendré par un élément* s, *et si* $x \in K^*$ *est tel que* $N_{K/k}(x) = 1$, *il existe* $y \in K^*$ *tel que* $x = y/s(y)$.

Cela résulte de la détermination de $H^1(G, \ )$ lorsque G est cyclique.

Remarques. 1) Le corollaire ci-dessus n'est autre que le célèbre « théorème 90 » de Hilbert. Dans la littérature, c'est souvent la prop. 2 que l'on appelle le « théorème 90 ».

2) Les groupes de cohomologie supérieurs $H^q(G, K^*)$ ne sont pas nuls en général. Nous reviendrons plus loin sur le cas $q = 2$ (groupe de Brauer).

La proposition 2 se généralise de la manière suivante (cf. Speiser [60]) : soit $\mathbf{GL}(n, K)$ le groupe des matrices inversibles de degré n à coefficients dans K; le groupe G opère de façon évidente sur $\mathbf{GL}(n, K)$, ce qui permet de définir l'ensemble de cohomologie $H^1(G, \mathbf{GL}(n, K))$, cf. Chap. VII, annexe.

PROPOSITION 3. *On a* $H^1(G, \mathbf{GL}(n, K)) = \{1\}$.

La démonstration est analogue à celle de la proposition 2. Soit a_s un 1-cocycle, et soit $c \in \mathbf{M}_n(K)$ une matrice quelconque. On construit encore la série de Poincaré

$$b = \sum_{s \in G} a_s . s(c)$$

et l'on démontre que $s(b) = a_s^{-1} . b$. Cette formule montre que a_s est un cobord, pourvu qu'on puisse choisir c de telle sorte que la matrice b soit *inversible*. Lorsque K est infini, l'existence de c résulte simplement du théorème *d'indépendance algébrique des automorphismes* (Bourbaki, *Alg.*, Chap. V, § 10, th. 4). Malheureusement, cet argument ne s'applique plus lorsque K est fini. C'est pourquoi nous allons utiliser un autre procédé, dû à Cartier :

Soit x un vecteur de K^n, et formons $b(x) = \sum_{s \in G} a_s(s(x))$. Les $b(x)$, $x \in K^n$, *engendrent* K^n comme K-espace vectoriel. En effet, si u est une forme linéaire nulle sur tous les $b(x)$, on a, pour tout $h \in K$,

$$0 = u(b(hx)) = \sum a_s . u(s(h)s(x)) = \sum s(h) u(a_s(s(x))).$$

Faisant varier h, on obtient une relation linéaire entre les $s(h)$. D'après le théorème de Dedekind déjà cité, cela entraîne que chacun des $u(a_s(s(x)))$ est nul, et puisque les a_s sont inversibles, cela entraîne $u = 0$.

Ce point étant acquis, soient $x_1, \ldots, x_n$ des vecteurs de K^n tels que les $y_i = b(x_i)$ soient linéairement indépendants sur K. Soit c la matrice de l'application qui envoie la base canonique e_i de K^n sur les x_i. Si l'on calcule la matrice b correspondante, on voit que $b(e_i) = y_i$, d'où le fait que b est inversible, ce qui achève la démonstration.

COROLLAIRE. *On a* $H^1(G, \mathbf{SL}(n, K)) = \{1\}$.

La suite exacte :

$$\{1\} \longrightarrow \mathbf{SL}(n, K) \longrightarrow \mathbf{GL}(n, K) \xrightarrow{\det} K^* \longrightarrow \{1\}$$

donne naissance (cf. Chap. VII, annexe) à la suite exacte :

$$H^0(G, \mathbf{GL}(n, K)) \to H^0(G, K^*) \to H^1(G, \mathbf{SL}(n, K)) \to \{1\},$$

ou encore :

$$\mathbf{GL}(n, k) \to k^* \to \mathrm{H}^1(\mathrm{G}, \mathbf{SL}(n, \mathrm{K})) \to \{1\}.$$

Comme det : $\mathbf{GL}(n, k) \to k^*$ est surjectif, il en résulte bien que $\mathrm{H}^1(\mathrm{G}, \mathbf{SL}(n, \mathrm{K})) = \{1\}$.

Remarque. Soit A un *schéma en groupes sur k* (ou encore, dans la terminologie de Weil, une « variété de groupe définie sur k »). Si K est une k-algèbre commutative quelconque, l'ensemble A_K des points de A à valeurs dans K est un *groupe*, dépendant fonctoriellement de K. En particulier, si K/k est une extension galoisienne finie de groupe de Galois G, le groupe G opère sur le groupe A_K, et les groupes de cohomologie $\mathrm{H}^q(\mathrm{G}, \mathrm{A}_\mathrm{K})$ sont définis (si A n'est pas abélien, seuls H^0 et H^1 sont définis, et H^1 n'est qu'un « ensemble pointé »). L'ensemble $\mathrm{H}^1(\mathrm{G}, \mathrm{A}_\mathrm{K})$ a une interprétation géométrique simple : c'est l'ensemble des classes d'espaces principaux homogènes pour A, définis sur k, et qui ont un point rationnel dans K (cf. Lang-Tate [41]). Les cas traités ci-dessus correspondent à $\mathrm{A} = \mathrm{G}_a$, G_m, $\mathbf{GL}(n)$, $\mathbf{SL}(n)$; nous verrons au § 2 ce que donnent le groupe orthogonal et le groupe symplectique.

Bien entendu, il n'y a aucune raison de se borner au cas des groupes linéaires. Les variétés abéliennes posent des problèmes extrêmement intéressants, pour lesquels nous ne pouvons que renvoyer le lecteur à l'exposé de Tate [64], et aux mémoires de Cassels [14].

Exercices. 1. Étendre la proposition 3 au groupe des automorphismes d'un espace vectoriel de dimension infinie.

2. Soit K/k une extension galoisienne finie, de groupe de Galois G, et soit M une k-algèbre à élément unité, de dimension finie sur k. Soit $\mathrm{M}_\mathrm{K} = \mathrm{M} \otimes_k \mathrm{K}$, et soit M_K^* le groupe multiplicatif des éléments inversibles de M_K; c'est un G-module. Montrer que $\mathrm{H}^1(\mathrm{G}, \mathrm{M}_\mathrm{K}^*) = \{1\}$.

[Lorsque k est infini, on peut utiliser les « séries de Poincaré ». Lorsque k est fini, on se ramènera au cas où M est semi-simple, et l'on appliquera la prop. 3 (on pourrait également utiliser un résultat général de Lang [39]).]

§ 2. *Quelques exemples de « descente »*

Soit V un k-espace vectoriel, muni d'un tenseur x d'espèce fixée (p, q) (autrement dit, on a $x \in \bigotimes^p \mathrm{V} \otimes \bigotimes^q \mathrm{V}^*$, où V^* désigne le dual de V). Deux couples (V, x) et (V', x') sont dits *k-isomorphes* s'il existe un isomorphisme k-linéaire

$$f : \mathrm{V} \to \mathrm{V}'$$

tel que $f(x) = x'$.

Soit maintenant K/k une extension galoisienne finie, de groupe de Galois G. Soit $\mathrm{V}_\mathrm{K} = \mathrm{V} \otimes_k \mathrm{K}$ l'espace vectoriel obtenu en étendant les scalaires de k à K; le tenseur x définit de façon évidente un tenseur x_K sur V_K, tenseur que nous noterons le plus souvent x. Nous dirons que (V, x) et (V', x') sont *K-isomorphes* (ou « deviennent isomorphes sur K ») si $(\mathrm{V}_\mathrm{K}, x_\mathrm{K})$ et $(\mathrm{V}'_\mathrm{K}, x'_\mathrm{K})$ sont isomorphes. Nous noterons $\mathrm{E}_{\mathrm{V}, x}(\mathrm{K}/k)$ *l'ensemble des classes à k-isomorphisme près de couples* (V', x') *qui sont* K*-isomorphes à* (V, x). Nous nous proposons d'interpréter $\mathrm{E}_{\mathrm{V}, x}(\mathrm{K}/k)$ comme un H^1.

Pour cela, soit A_K le groupe des K-*automorphismes de* (V_K, x_K). Le groupe G opère sur A_K de la façon suivante : tout d'abord, il opère sur V_K par $s(x \otimes \lambda) = x \otimes s(\lambda)$; ensuite, si $f : V_K \to V_K$ est une application K-linéaire, on pose

$$s(f)(x) = s.f(s^{-1}(x)), \qquad \text{i.e.} \quad s(f) = s \circ f \circ s^{-1}.$$

Nous nous proposons de *comparer* $E_{V,x}(K/k)$ *et* $H^1(G, A_K)$. Pour simplifier, nous écrirons $E(K/k)$ au lieu de $E_{V,x}(K/k)$.

Soit donc $(V', x') \in E(K/k)$, et soit $f : V_K \to V'_K$ un K-isomorphisme. Posons :

$$p_s = f^{-1} \circ s(f) = f^{-1} \circ s \circ f \circ s^{-1}, \qquad s \in G.$$

On a évidemment $p_s \in A_K$; de plus, un calcul immédiat montre que $s \to p_s$ est un 1-cocycle, et que changer f revient à remplacer p_s par un cocycle équivalent. La classe de p_s dans $H^1(G, A_K)$ est donc bien déterminée, et nous avons ainsi défini une application

$$\theta : E(K/k) \to H^1(G, A_K).$$

PROPOSITION 4. *L'application* θ *définie ci-dessus est bijective.*

Montrons que θ est *injective*. Soient (V'_1, x'_1) et (V'_2, x'_2) deux couples correspondant au même cocycle p_s, et soient f_1 et f_2 les K-isomorphismes correspondants. On a $f_1^{-1} \circ s(f_1) = f_2^{-1} \circ s(f_2)$ d'où $s(f_2 f_1^{-1}) = f_2 f_1^{-1}$. L'application $f = f_2 f_1^{-1}$ est un k-isomorphisme de (V'_1, x'_1), sur (V'_2, x'_2), ce qui montre bien que θ est injective.

Montrons que θ est *surjective*. Soit p_s un 1-cocycle de G à valeurs dans A_K; on a $A_K \subset \mathbf{GL}(V_K)$, et, en appliquant la prop. 3, on voit qu'il existe un K-automorphisme f de V_K tel que

$$p_s = f^{-1} \circ s(f) \qquad \text{pour tout } s \in G.$$

Étendons f à l'algèbre tensorielle de V_K, et posons $x' = f(x)$. L'élément x' est « rationnel sur k » (i.e. appartient à l'algèbre tensorielle de V sur k); en effet, on a :

$$s(x') = s(f)(s(x)) = s(f)(x) = f \circ p_s(x) = f(x) = x'.$$

Il en résulte que (V, x') appartient à $E(K/k)$, et il est clair que l'image de cet élément par θ est égale à la classe du cocycle p_s, c.q.f.d.

Remarque. On aurait pu définir θ en remarquant que l'ensemble des « isomorphismes » de (V, x) sur (V', x') est un espace principal homogène pour le groupe algébrique A.

Exemples. Prenons pour tenseur x une forme quadratique non dégénérée Φ. L'ensemble $E(K/k)$ est alors l'ensemble des classes de formes quadratiques qui sont K-isomorphes à Φ. Le groupe A_K est le groupe orthogonal $\mathbf{O}_K(\Phi)$ de la forme Φ sur K. On a donc :

COROLLAIRE 1. *L'ensemble* $H^1(G, \mathbf{O}_K(\Phi))$ *est en correspondance bijective avec l'ensemble des classes de k-formes quadratiques qui sont* K*-isomorphes à* Φ.

Cette interprétation de $H^1(G, \mathbf{O}_K(\Phi))$ permet évidemment de donner des exemples où cet ensemble est non trivial ($k = \mathbf{R}$, $K = \mathbf{C}$).

Au lieu de prendre une forme quadratique, on peut prendre une forme alternée non dégénérée; le groupe A_K est alors le groupe symplectique $\mathbf{Sp}(n, K)$. Comme deux formes alternées non dégénérées de même rang sont équivalentes (Bourbaki, *Alg.*, Chap. IX, § 5), on en tire :

COROLLAIRE 2. *On a* $H^1(G, \mathbf{Sp}(n, K)) = \{1\}$.

Remarque. Ce qui précède est un cas particulier de la méthode de « descente galoisienne » en géométrie algébrique (cf. par exemple [56], Chap. V; § 4), elle-même englobée dans la « théorie de la descente » de Grothendieck (cf. [28], [29], [80]).

§ 3. *Extensions galoisiennes infinies*

Il est souvent commode de « passer à la limite » en prenant des extensions galoisiennes de plus en plus grandes. Nous allons indiquer rapidement comment la question se présente du point de vue cohomologique.

Soit K/k une extension galoisienne (non nécessairement finie). Son groupe de Galois G est un groupe topologique compact, totalement discontinu, limite projective des groupes de Galois $G(K'/k)$, où K' parcourt l'ensemble des sous-extensions galoisiennes finies de K.

Soit A un G-module. On dit que c'est un G-module *topologique* si, pour tout $a \in A$, l'ensemble des $s \in G$ tels que $s(a) = a$ est un sous-groupe ouvert de G. Il revient au même de dire que

$$A = \bigcup A^H$$

lorsque H parcourt l'ensemble des sous-groupes invariants ouverts de G. Cette condition est réalisée lorsque A est le groupe des points rationnels sur K d'un schéma en groupes de type fini sur k; on pourra prendre, par exemple, $A = K$ ou $A = K^*$.

Si A est un G-module topologique, on définit $H^q(G, A)$ par la formule :

$$H^q(G, A) = \varinjlim H^q(G/H, A^H)$$

pour H parcourant l'ensemble des sous-groupes invariants ouverts de G (la limite inductive est prise relativement aux homomorphismes d'*inflation*, cf. Chap. VII, § 5). Ces groupes de cohomologie jouissent de propriétés tout analogues à celles des groupes de cohomologie usuels; ils forment un foncteur cohomologique (le cobord se définissant lui aussi par passage à la limite); ils peuvent être définis par des *cochaînes continues* à valeurs dans A. Leurs propriétés ont été étudiées systématique-

ment par Tate (cf. [20], [113]). Nous allons en donner deux applications élémentaires :

a) *Théorie d'Artin-Schreier.*

Soit k un corps de caractéristique $p \neq 0$, soit K sa clôture séparable, et soit G le groupe de Galois de K/k. L'application

$$\wp : K \to K$$

définie par $\wp(x) = x^p - x$, est un homomorphisme de G-modules. Elle est surjective, car l'équation $\wp(x) = a$ est séparable; son noyau est $\mathbf{Z}/p\mathbf{Z}$ (sur lequel G opère trivialement). On a donc la suite exacte :

$$0 \to \mathbf{Z}/p\mathbf{Z} \to K \to K \to 0.$$

En écrivant la suite exacte de cohomologie, et en tenant compte de ce que

$$H^1(G, K) = 0$$

d'après la prop. 1, on obtient :

$$k \to k \to H^1(G, \mathbf{Z}/p\mathbf{Z}) \to 0.$$

En d'autres termes, le groupe Hom(G, $\mathbf{Z}/p\mathbf{Z}$) des homomorphismes continus de G dans $\mathbf{Z}/p\mathbf{Z}$ *est isomorphe à* $k/\wp(k)$. L'isomorphisme en question fait correspondre à $a \in k$ l'homomorphisme $\varphi_a : G \to \mathbf{Z}/p\mathbf{Z}$ défini de la manière suivante : on résout l'équation $x^p - x = a$, et l'on pose $s(x) = x + \varphi_a(s)$.

Si l'on note k_p la composée de toutes les extensions abéliennes de type $(p, \ldots, p)$ de k, on voit que *le groupe* $G(k_p/k)$ *est isomorphe au groupe dual* $(k/\wp(k))^\wedge$ *du groupe discret* $k/\wp(k)$.

Si l'on veut remplacer $\mathbf{Z}/p\mathbf{Z}$ par $\mathbf{Z}/p^n\mathbf{Z}$, il faut utiliser la suite exacte :

$$0 \longrightarrow \mathbf{Z}/p^n\mathbf{Z} \longrightarrow W_n(K) \xrightarrow{F-1} W_n(K) \longrightarrow 0$$

où W_n désigne le groupe additif des vecteurs de Witt de longueur n.

b) *Théorie de Kummer.*

Soit n un entier premier à la caractéristique de k, et supposons que k^* contienne le groupe E_n des racines n-ièmes de l'unité. Si K désigne encore la clôture séparable de k, on a la suite exacte de G-modules :

$$0 \to E_n \to K^* \xrightarrow{u} K^* \to 0$$

avec $u(x) = x^n$. On en déduit, en appliquant la proposition 2, un *isomorphisme* $k^*/k^{*n} \to \mathrm{Hom}(G, E_n)$. Cet isomorphisme fait correspondre à un élément $a \in k^*$ l'homomorphisme $\varphi_a : G \to E_n$ défini de la manière suivante : on résout l'équation

$x^n = a$, et l'on pose $s(x) = \varphi_a(s).x$, avec $\varphi_a(s) \in E_n$. Si k_n désigne la composée de toutes les extensions abéliennes de k dont le groupe de Galois est annulé par n, on voit que $G(k_n/k)$ est isomorphe au groupe $E_n \otimes (k^*/k^{*n})\hat{}$, lui-même isomorphe (non canoniquement) à $(k^*/k^{*n})\hat{}$.

§ 4. *Le groupe de Brauer*

On va maintenant s'occuper exclusivement du *groupe multiplicatif*. Si K/k est une extension galoisienne, finie ou infinie, de groupe de Galois G, on écrira $H^q(K/k)$ au lieu de $H^q(G, K^*)$. Ces groupes dépendent fonctoriellement du couple (K, k). De façon précise, soit K'/k' une extension galoisienne, de groupe de Galois G', le corps k' étant une extension du corps k. Supposons qu'il existe un k-isomorphisme f de K dans K'. Une telle application définit un homomorphisme $\bar{f}: G' \to G$ de la manière suivante : si $s' \in G'$, $\bar{f}(s')$ est l'unique élément $s \in G$ tel que $f \circ s = s' \circ f$. L'homomorphisme $\bar{f}$ est *compatible* avec $f: K^* \to K'^*$, au sens du Chap. VII, § 5. Il définit donc des homomorphismes :

$$f_q : H^q(K/k) \to H^q(K'/k').$$

Proposition 5. *Les homomorphismes f_q sont indépendants du choix de $f: K \to K'$.*

En effet, deux tels choix f et f' diffèrent par un élément de G, et l'on applique à cet élément la prop. 3 du Chap. VII.

(Bien entendu, la proposition précédente s'applique à tout schéma en groupes sur k.)

En particulier, si $k' = k$, et si K et K' sont isomorphes, il existe un *isomorphisme canonique* de $H^q(K/k)$ sur $H^q(K'/k)$; ceci s'applique notamment en prenant pour K la *clôture séparable* k_s de k; les groupes $H^q(k_s/k)$ ainsi définis seront aussi notés $H^q(\ /k)$. Il est clair qu'ils dépendent fonctoriellement de k.

Le groupe $H^1(\ /k)$ est nul (prop. 2). Le groupe $H^2(\ /k)$ s'appelle le *groupe de Brauer* du corps k; nous le noterons B_k. Par définition, c'est la limite inductive des $H^2(K/k)$, pour K parcourant l'ensemble des extensions galoisiennes finies de k. Cette limite inductive est en fait une réunion. En effet :

Proposition 6. *Soit L/k une extension galoisienne contenant l'extension galoisienne K/k. On a la suite exacte :*

$$0 \to H^2(K/k) \to H^2(L/k) \to H^2(L/K).$$

Soit $G = G(L/k)$, et soit $H = G(L/K)$. On a $H^1(H, L^*) = 0$, ce qui permet d'appliquer la prop. 5 du Chap. VII avec $q = 2$. On obtient la suite exacte :

$$0 \longrightarrow H^2(G/H, K^*) \xrightarrow{\text{Inf}} H^2(G, L^*) \xrightarrow{\text{Res}} H^2(H, L^*),$$

qui n'est autre que la suite exacte cherchée.

Corollaire. *On a la suite exacte :*

$$0 \to H^2(K/k) \to B_k \to B_K.$$

Cela résulte de la suite exacte de la proposition 6, en passant à la limite sur L.

Remarques. 1. La proposition 6 et son corollaire sont encore valables lorsque K/k et L/k sont des extensions galoisiennes infinies; cela se voit par passage à la limite.

2. On dit qu'un élément $a \in B_k$ *est décomposé par* K s'il est dans le noyau de $B_k \to B_K$; lorsque K/k est une extension galoisienne, il revient au même (d'après le corollaire ci-dessus), de dire que a appartient à $H^2(K/k)$, considéré comme sous-groupe de B_k.

Exercices. 1. Soit k un corps de caractéristique p, et soit $K = k^{p^{-1}}$. Montrer qu'un élément $a \in B_k$ est décomposé par K si et seulement si $pa = 0$. En déduire que la composante p-primaire de B_k est nulle si k est parfait.
2. Soit K/k une extension de degré fini n, et soit $a \in B_k$ un élément décomposé par K. Montrer que $na = 0$. (Traiter séparément le cas radiciel et le cas séparable; utiliser l'exer. 1 pour le premier, et la prop. 6 du Chap. VII pour le second.)

§ 5. *Comparaison avec la définition classique du groupe de Brauer*

Rappelons d'abord cette définition :

PROPOSITION 7. *Soit k un corps et soit* A *une k-algèbre de dimension finie. Les conditions suivantes sont équivalentes* :

a) A *n'a pas d'idéal bilatère non trivial, et son centre est k.*

b) *Si* K *désigne la clôture algébrique de k, l'algèbre étendue* $A_K = A \otimes_k K$ *est isomorphe à une algèbre de matrices sur* K.

b') *Il existe une extension galoisienne finie K/k telle que* A_K *soit isomorphe à une algèbre de matrices sur* K.

c) A *est k-isomorphe à une algèbre de matrices sur un corps gauche de centre k.*

Pour la démonstration, voir Bourbaki, *Alg.*, Chap. VIII, §§ 5, 10. Une telle algèbre est appelée une *algèbre simple centrale* sur k. Deux telles algèbres sont dites *équivalentes* si les corps gauches qui leur sont associés par c) sont k-isomorphes; si ces algèbres ont même dimension, cela revient à dire qu'elles sont k-isomorphes.

Soit A_k l'ensemble des classes d'algèbres simples centrales (pour la relation d'équivalence définie ci-dessus); le produit tensoriel définit par passage au quotient une structure de groupe abélien sur A_k. C'est ce groupe que l'on appelle classiquement le « groupe de Brauer » (cf. Bourbaki, *loc. cit.*, § 10). C'est un foncteur covariant de k : si K est une extension de k, l'extension des scalaires de k à K définit un homomorphisme

$$A_k \to A_K.$$

Nous noterons $A(K/k)$ le noyau de cet homomorphisme. Il résulte de la proposition 7 que A_k *est réunion des* $A(K/k)$, *pour* K *parcourant l'ensemble des extensions galoisiennes finies de k.* Pour montrer que A_k est isomorphe à B_k, il suffira donc de construire *des isomorphismes* $A(K/k) \to H^2(K/k)$ compatibles avec les injections :

$$A(K/k) \to A(K'/k) \qquad \text{et} \qquad H^2(K/k) \to H^2(K'/k), \qquad \text{pour } K' \supset K$$

On va procéder par « descente ». Soit $A(n, K/k)$ l'ensemble des classes de k-algèbres A telles que $A \otimes_k K$ soit isomorphe à l'algèbre de matrices $\mathbf{M}_n(K)$. Le groupe $A(K/k)$ est réunion des sous-ensembles $A(n, K/k)$ pour $n = 1, 2, \ldots$ Le procédé du § 2 s'applique à $A(n, K/k)$: un élément de $A(n, K/k)$ peut être considéré comme un couple (V, x), où V est un espace vectoriel de dimension n^2 et où x est un tenseur de type (1, 2) (la loi de composition), ce couple étant K-isomorphe au couple standard défini par l'algèbre de matrices $\mathbf{M}_n$. On en conclut que, si G désigne le groupe de Galois de K/k, et si C_K désigne le groupe des K-automorphismes de $\mathbf{M}_n(K)$, l'application

$$\theta : A(n, K/k) \to H^1(G, C_K)$$

définie au § 2 est une bijection.

Mais on sait que tout automorphisme de $\mathbf{M}_n(K)$ est intérieur. On a donc la suite exacte :

$$\{1\} \to K^* \to \mathbf{GL}(n, K) \to C_K \to \{1\}. \tag{1}$$

Cette suite permet *d'identifier* C_K *au groupe projectif* $\mathbf{PGL}(n, K)$. En résumé :

PROPOSITION 8. *On a une bijection canonique*

$$\theta : A(n, K/k) \to H^1(G, \mathbf{PGL}(n, K)).$$

D'autre part, la suite exacte (1) définit (cf. Chap. VII, annexe) un opérateur « cobord »

$$\Delta_n : H^1(G, \mathbf{PGL}(n, K)) \to H^2(G, K^*).$$

En composant θ et Δ_n, on obtient une application

$$\delta_n : A(n, K/k) \to H^2(G, K^*) = H^2(K/k).$$

Un calcul sans difficultés montre que, si $C \in A(n, K/k)$ et $C' \in A(n', K/k)$, on a

$$\delta_{nn'}(C \otimes C') = \delta_n(C) + \delta_{n'}(C').$$

D'autre part, on a $\delta_n(C) = 0$ si et seulement si C est une algèbre de matrices (cela résulte de la proposition 2 de l'annexe du Chap. VII). On en conclut que les applications δ_n sont compatibles entre elles, et définissent un homomorphisme

$$\delta : A(K/k) \to H^2(K/k).$$

PROPOSITION 9. *L'homomorphisme* $\delta : A(K/k) \to H^2(K/k)$ *est bijectif.*

On a déjà vu qu'il est injectif. Le lemme suivant montre qu'il est surjectif :

LEMME 1. *Soit* $n = [K : k]$. *L'application* $\delta_n : A(n, K/k) \to H^2(K/k)$ *est surjective.*

(Comparer avec Bourbaki, *Alg.*, Chap. VIII, § 10, prop. 7.)

Vu ce qui précède, il suffit de montrer que Δ_n est surjectif, c'est-à-dire que tout 2-cocycle $a_{s,t}$ à valeurs dans K^* peut s'écrire :

$$a_{s,t} = p_s\, s(p_t) p_{st}^{-1}, \qquad \text{avec } p_s \in \mathbf{GL}(n, K).$$

Soit V un espace vectoriel sur K ayant pour base une famille de vecteurs e_s, $s \in G$. Soit $p_s \in \mathrm{Hom}_K(V, V)$ l'automorphisme de V qui applique e_t sur $a_{s,t} e_{st}$. Montrons que les p_s vérifient l'équation ci-dessus. On a :

$$\begin{aligned} p_s\, s(p_t)(e_u) &= a_{s,tu}\, s(a_{t,u}) e_{stu} \\ a_{s,t}\, p_{st}(e_u) &= a_{s,t} a_{st,u} e_{stu} \end{aligned}$$

et l'on trouve bien le même résultat, puisque $a_{s,t}$ est un cocycle.

On a donc obtenu l'isomorphisme $A(K/k) \to H^2(K/k)$ cherché. Lorsque K'/k est une extension galoisienne contenant K/k, on vérifie trivialement la commutativité du diagramme :

$$\begin{array}{ccc} A(K/k) & \to & H^2(K/k) \\ \downarrow & & \downarrow \\ A(K'/k) & \to & H^2(K'/k). \end{array}$$

On peut donc passer à la limite sur K, et l'on obtient ainsi *un isomorphisme* $\delta : A_k \to B_k$, ce qui achève de montrer l'équivalence des deux définitions du groupe de Brauer.

Remarque. On trouvera dans la littérature (cf. par exemple Deuring [19] ou Artin-Nesbitt-Thrall [7]) une autre façon d'identifier $A(K/k)$ et $H^2(K/k)$, reposant sur la construction de « produits croisés ». On peut montrer (cf. exer. 2) que c'est *l'opposée* de l'identification que nous avons utilisée.

Exercices. 1. Soit K/k une extension galoisienne finie, de groupe de Galois G, et soit A une k-algèbre de dimension finie. Soit u_s un cocycle de G à valeurs dans $\mathrm{Aut}_K(A \otimes_k K)$. Soit B l'ensemble des $x \in A \otimes_k K$ tels que $x = u_s(s(x))$ pour tout $s \in G$. Montrer que B est une sous-k-algèbre de $A \otimes_k K$, que l'injection $i : B \to A \otimes_k K$ se prolonge en un K-isomorphisme j: $B \otimes_k K \to A \otimes_k K$, et que $u_s = j \circ s(j)^{-1}$. En déduire que la classe de cohomologie associée à B par le procédé de la prop. 4 est celle de u_s.

2. Appliquer ce qui précède au cas $A = \mathbf{M}_n(k)$, u_s étant l'automorphisme intérieur défini par un élément $p_s \in \mathbf{GL}(n, K)$. En déduire que B est la sous-algèbre de $\mathbf{M}_n(K)$ formée des éléments x tels que $x \circ p_s = p_s \circ s(x)$. Déterminer explicitement B lorsque les p_s sont ceux définis dans la démonstration du lemme 1 (on trouve que B est le « produit croisé » défini par le système de facteurs $st(a_{t^{-1}, s^{-1}})$, lequel est cohomologue à $-a$).

3. Soit D un corps gauche de centre k et de rang n^2 sur k. Soit x l'élément du groupe de Brauer B_k correspondant à D, et soit d l'ordre de x dans B_k.

a) Montrer que d divise n. (Appliquer l'exer. 2 du § 4 à un sous-corps commutatif maximal de D.)

b) Montrer que tout facteur premier de n divise d. (Soit p un nombre premier ne divisant pas d; soit K/k une extension galoisienne, de groupe de Galois G, décomposant x, et soit G_p un p-groupe de Sylow de G. Montrer que l'image de x dans $H^2(G_p, K^*)$ par restriction est nulle; si K' désigne le sous-corps de K correspondant à G_p, en déduire que K' décompose x, et comme $[K' : k]$ est premier à p, en conclure que p ne divise pas n.)

§ 6. *Une interprétation géométrique du groupe de Brauer : les variétés de Severi-Brauer*

Soit k un corps de base, et soit $\mathbf{P}_{n-1}$ l'espace projectif de dimension $n-1$, considéré comme un *schéma sur* k. Soit V un schéma sur k. On dit que V est une *variété de Severi-Brauer* s'il existe une extension algébrique séparable K/k telle que V et $\mathbf{P}_{n-1}$ soient K-isomorphes (autrement dit, $V\otimes_k K$ et $\mathbf{P}_{n-1}\otimes_k K$ sont des K-schémas isomorphes). Cette notion est due à F. Châtelet [15], [16].

Exemples. 1. Dans le plan projectif une conique non singulière est une variété de Severi-Brauer de dimension 1 : elle est K-isomorphe à $\mathbf{P}_1$ si et seulement si elle a au moins un point à valeurs dans K.

2. Les diviseurs positifs appartenant à une classe de diviseurs rationnelle sur k forment une variété de Severi-Brauer. [Nous laissons au lecteur le soin de préciser le sens de cet énoncé !]

Soit V une variété de Severi-Brauer de dimension $n-1$, et soit K/k une extension galoisienne finie, de groupe de Galois G, telle que V « se décompose dans K » ; il existe donc un isomorphisme

$$f : \mathbf{P}_{n-1}\otimes_k K \to V\otimes_k K.$$

Pour tout $s\in G$, $p_s = f^{-1}\circ s(f)$ est un automorphisme de $\mathbf{P}_{n-1}\otimes_k K$, c'est-à-dire un élément de $\mathbf{PGL}(n, K)$. Appliquant la théorie de la descente, on en conclut que *les variétés de Severi-Brauer de dimension* $n-1$ *sur* k *décomposées par* K *correspondent bijectivement* (à isomorphisme près) *aux éléments de* $H^1(G, \mathbf{PGL}(n, K))$, donc aussi *aux éléments de* $A(n, K/k)$. Cette correspondance entre algèbres simples et variétés de Severi-Brauer peut aussi s'expliciter de la manière suivante :

Soit A une algèbre simple, de centre k, et de degré n^2 sur k. Soit Gr (A) la grassmannienne des sous-variétés linéaires de dimension n de A, considérée comme un schéma sur k. Soit V le sous-schéma fermé de Gr (A) défini par la condition que, si $v\in V$, la variété linéaire associée à v est stable par la multiplication à droite par A (V est la variété des « idéaux à droite de rang n sur k de A »). On démontre que V est une variété de Severi-Brauer, et qu'elle correspond (par la correspondance ci-dessus) à l'algèbre simple centrale A.

Pour plus de détails sur les variétés de Severi-Brauer, voir Châtelet (*loc. cit.*), Amitsur [1], Grothendieck [83], Azumaya [10], Auslander-Goldman [9], ainsi que les exercices de Bourbaki, *Alg. comm.*, Chap. II, § 5.

Exercices. 1. (Châtelet). Montrer qu'une variété de Severi-Brauer V est triviale (i.e. isomorphe à $\mathbf{P}_{n-1}$) si et seulement si elle possède un point rationnel.

2. (Amitsur). Soient V et V′ deux variétés de Severi-Brauer, de même dimension, et soient a, a' les éléments correspondants du groupe de Brauer. Montrer que, si V et V′ sont birationnellement isomorphes, a et a' engendrent le même sous-groupe. [On ignore si la réciproque est vraie.]

§ 7. *Exemples de groupes de Brauer*

Le groupe de Brauer est l'un des principaux invariants dont on dispose pour mesurer le « degré de complication » d'un corps k. Commençons par donner des exemples de corps pour lesquels il est *nul* :

Soit k un corps. On dit que k est quasi-algébriquement clos (ou C_1) s'il vérifie la condition suivante :

Si $f(x_1, \ldots, x_n)$ est un polynôme homogène, de degré $d \neq 0$, à coefficients dans k, et qui ne s'annule que pour $(0, \ldots, 0)$, on a $d \geqslant n$.

PROPOSITION 10. *Si un corps k vérifie la propriété C_1, le groupe de Brauer de toute extension finie K de k est nul.*

En effet, soit D un corps gauche, de centre K, et de degré r^2 sur K. Soit $s = [K : k]$. Si $x \in D$, soit $\mathrm{Nrd}(x) \in K$ sa *norme réduite* (Bourbaki, *Alg.*, Chap. VIII, § 12, n° 3), et posons :

$$f(x) = N_{K/k}(\mathrm{Nrd}(x)).$$

La fonction f ne s'annule que pour $x = 0$. D'autre part, si l'on prend une base $\{e_i\}$ de D sur k, et si l'on écrit $x = \sum x_i e_i$, la fonction f devient une fonction $f(x_1, \ldots, x_n)$, avec $n = s.r^2$, qui est un polynôme homogène de degré sr (*loc. cit.*, prop. 11). Puisque k est C_1, on a donc $sr^2 \leqslant sr$, i.e. $r = 1$ et $D = K$, ce qui montre bien que le groupe de Brauer de K est nul.

La nullité du groupe de Brauer a des conséquences intéressantes :

PROPOSITION 11. *Soit k un corps. Les trois conditions suivantes sont équivalentes :*

(1). *Le groupe de Brauer de toute extension séparable finie de k est nul.*

(2). *Si L/K est une extension galoisienne finie, avec K fini et séparable sur k, le $G(L/K)$-module L^* est cohomologiquement trivial.*

(3). *Les hypothèses sur L/K étant les mêmes que dans (2), l'homomorphisme $N_{L/K} : L^* \to K^*$ est surjectif.*

Supposons (2) vérifié. On a alors $\hat{H}^0(G(L/K), L^*) = 0$, d'où (3), et

$$H^2(G(L/K), L^*) = 0$$

d'où (1) en passant à la limite sur L. Réciproquement, supposons (1) (resp. (3)) vérifié. Si H est un sous-groupe quelconque de $G(L/K)$ on a donc

$$\hat{H}^2(H, L^*) = 0 \quad (\text{resp. } \hat{H}^0(H, L^*) = 0);$$

comme d'autre part $H^1(H, L^*) = 0$, on peut appliquer le théorème 8 du chapitre IX, et l'on en déduit bien que L^* est cohomologiquement trivial.

Remarque. Il suffit de vérifier (3) lorsque L/K est *cyclique de degré premier*. En effet, on passe de là au cas d'une extension résoluble par dévissage, puis au cas général en utilisant les groupes de Sylow.

COROLLAIRE. *Soit* L/K *une extension vérifiant les conditions* (2). *Si* E *est un* G(L/K)-*module sans torsion, le* G(L/K)-*module* $L^* \otimes E$ *est cohomologiquement trivial.*

Cela résulte du corollaire au théorème 9 du Chapitre IX.

Application. Soit A un « tore » sur k, de groupe des caractères X. Soit K/k une extension galoisienne, de groupe de Galois G, assez grande pour que tout élément $\chi \in X$ soit rationnel sur K. Le groupe A_K des points de A rationnels sur K est alors isomorphe à $K^* \otimes X'$, où X′ désigne le dual de X. Si k vérifie les conditions de la proposition 11, on a donc $\hat{H}^n(G, A_K) = 0$ pour tout $n \in \mathbf{Z}$. En particulier, tout espace principal homogène sur A est trivial.

Exemples de corps à groupe de Brauer nul.

a) Un corps *fini*. En effet, dans ce cas $H^1(G, K^*)$ et $H^2(G, K^*)$ ont même ordre (cf. Chap. VIII, prop. 8), et comme le premier groupe est nul (prop. 2), il en est de même du second.

[On peut également obtenir ce résultat en montrant qu'un corps fini est C_1, cf. Bourbaki, *Alg.*, Chap. IV, § 2, exer. 8.]

b) *L'extension maximale non ramifiée* K_{nr} d'un corps K complet pour une valuation discrète à corps résiduel *parfait*. En effet, la condition (3) de la proposition 11 est vérifiée (cf. Chap. V, § 4, prop. 7).

Ceci s'applique en particulier à un corps complet pour une valuation discrète à corps résiduel algébriquement clos.

[Les corps K_{nr} sont C_1; la démonstration (qui est loin d'être triviale) se trouve dans la thèse de Lang [38].]

c) Une extension *de degré de transcendance* 1 d'un corps algébriquement clos. On montre en effet qu'un tel corps est C_1 (« théorème de Tsen », cf. Lang, *loc. cit.*).

d) Une extension algébrique de $\mathbf{Q}$ contenant toutes les racines de l'unité. Cela résulte, par passage à la limite, de la détermination du groupe de Brauer d'un corps de nombres.

[On ignore si un tel corps est C_1; cela a été conjecturé par Artin.]

Exemples de corps à groupe de Brauer non nul.

e) Le corps $\mathbf{R}$. Le groupe de Brauer est égal à $H^2(G, \mathbf{C}^*)$, où $G = G(\mathbf{C}/\mathbf{R})$ est cyclique d'ordre 2. On a donc :

$$B_R = \mathbf{C}^{*G}/N\mathbf{C}^* = \mathbf{R}^*/\mathbf{R}_+^* = \mathbf{Z}/2\mathbf{Z}.$$

L'élément non nul de B_R correspond au *corps des quaternions* $\mathbf{H}$. La variété de Severi-Brauer correspondante est la conique :

$$x^2 + y^2 + z^2 = 0.$$

f) Un corps *complet* pour une valuation discrète *à corps résiduel fini*. Le groupe de Brauer est isomorphe à $\mathbf{Q}/\mathbf{Z}$, cf. Chap. XIII.

g) *Un corps de nombres algébriques.* Soit k un tel corps, et soient k_t les complétés de k pour les diverses topologies définies par des valeurs absolues de k. D'après ce qui précède, B_{k_t} est égal à $\mathbf{Q}/\mathbf{Z}$ si la valeur absolue correspondante est valuative, il est égal au sous-groupe $\left\{0, \frac{1}{2}\right\}$ de $\mathbf{Q}/\mathbf{Z}$ si $k_t = \mathbf{R}$, et il est nul si $k_t = \mathbf{C}$. Comme k s'envoie dans chaque k_t, B_k s'envoie dans le produit des B_{k_t}. On montre qu'il s'envoie en fait dans la *somme directe* $\oplus B_{k_t}$, et que la suite ci-dessous est exacte :

$$0 \to B_k \to \oplus B_{k_t} \xrightarrow{\sigma} \mathbf{Q}/\mathbf{Z} \to 0$$

σ étant l'application définie par $\sigma((x_t)) = \sum x_t$.

Ce résultat se démontre en même temps que les théorèmes du corps de classes (cf. Artin-Tate [8], Chap. VII, ou Deuring [19], Chap. VII).

h) Les corps de fonctions algébriques *d'une variable* sur un *corps de base fini*. Le résultat est le même que pour les corps de nombres.

CHAPITRE XI

FORMATIONS DE CLASSES

La notion de formation de classes a été introduite par Artin-Tate [8] à la suite des travaux de Weil [67] et de Hochschild-Nakayama [36]. Cette notion clarifie l'aspect cohomologique de la théorie du corps de classes, à la fois dans le cas local et dans le cas global. Le présent chapitre se borne aux propriétés principales des formations de classes; le lecteur trouvera dans Artin-Tate [8] divers compléments (théorème de Šafarevič, groupes de Weil).

§ 1. *La notion de formation*

On se donne tout d'abord un groupe G et un ensemble de sous-groupes $\{G_E\}_{E \in X}$ de G, *d'indice fini* dans G; on suppose que $G_E = G_{E'}$ entraîne $E = E'$ (de sorte que l'on pourrait identifier X à une partie de l'ensemble des sous-groupes de G — mais ce ne serait pas commode dans les applications). On suppose que les $\{G_E\}_{E \in X}$ vérifient les propriétés suivantes :

a) *Pour toute famille finie* F_i *d'éléments de* X, *il existe* $F \in X$ *tel que* $G_F = \bigcap G_{F_i}$.

b) *Tout sous-groupe* G' *de* G *contenant un sous-groupe* G_F, $F \in X$, *est de la forme* $G_{F'}$, *avec* $F' \in X$.

c) *Si* $s \in G$ *et* $F \in X$, *le sous-groupe* $s.G_F.s^{-1}$ *est de la forme* $G_{F''}$, *avec* $F'' \in X$.

Exemples. 1. Soit E un corps, soit Ω une extension galoisienne de E, et soit X l'ensemble des sous-corps de Ω contenant E et finis sur E. On prend pour G le *groupe de Galois topologique* $G(\Omega/E)$, et pour G_F le sous-groupe $G(\Omega/F)$ de G. Les conditions (*a*), (*b*), (*c*) résultent de la théorie de Galois.

[Dans la pratique, on prendra souvent pour Ω la *clôture séparable* de E.]

2. Plus généralement, on peut prendre pour G un groupe topologique quelconque, et pour $\{G_E\}$ l'ensemble de ses sous-groupes fermés d'indice fini.

Remarque. Dans toute la suite, le groupe G n'interviendra que par l'intermédiaire de ses *quotients finis* G/G_E, avec G_E invariant dans G, et $E \in X$. On pourrait donc le

remplacer par le groupe G *limite projective* des G/G_E, qui est un groupe *profini*, cf. [113].

Si G et les $\{G_E\}_{E\in X}$ vérifient les conditions ci-dessus, on transporte à X la terminologie de la théorie de Galois. Les éléments de X sont appelés les « corps ». On dit que $E \subset F$ si $G_E \supset G_F$, on dit que F/E est une extension galoisienne si G_F est un sous-groupe invariant de G_E, et l'on définit alors le « groupe de Galois » G(F/E) (noté aussi $G_{F/E}$) comme le quotient G_E/G_F. Dans la situation de (*a*), on dit que F est le « composé » des F_i, et on écrit $F = \prod F_i$; dans la situation de (*c*), on écrit $F' = s(F)$ ou sF. On peut parler d'extension abélienne, résoluble, etc. Noter que toute extension F/E est contenue dans une extension galoisienne; en effet, comme G_F est un sous-groupe d'indice fini de G_E, ses conjugués $s.G_F.s^{-1}$ sont en nombre fini, et leur intersection est de la forme $G_{F'}$, avec $F' \in X$. L'extension F'/E est galoisienne et contient F.

On va maintenant se donner un G-module A vérifiant la condition suivante :

(*) *Pour tout* $a \in A$, *l'ensemble des* $s \in G$ *tels que* $s.a = a$ *est l'un des sous-groupes* G_E, *avec* $E \in X$.

[Cette condition signifie que A peut être considéré comme un $\hat{G}$-*module topologique*, au sens du Chap. X, § 3 ($\hat{G}$ désignant la limite projective des G/G_E).]

La donnée de G, des $\{G_E\}_{E\in X}$, et de A, vérifiant les conditions ci-dessus, s'appelle une *formation*.

Soit $\{G, \{G_E\}_{E\in X}, A\}$ une formation. Si $E \in X$, on note A_E le sous-groupe de A formé des $a \in A$ tels que $s.a = a$ pour tout $s \in G_E$; on a donc $A_E = H^0(G_E, A)$, et l'axiome (*) signifie que A est réunion des A_E, quand E parcourt X. Si F/E est une extension galoisienne, le groupe G(F/E) opère sur A_F, et l'on a :

$$H^0(G(F/E), A_F) = A_E.$$

Cohomologie dans une formation.

Revenons au cas d'une extension *galoisienne* F/E. Comme le groupe G(F/E) opère sur A_F, les groupes de *cohomologie* $H^q(G(F/E), A_F)$ sont définis; nous les noterons $H^q(F/E)$. Notation analogue pour les groupes *d'homologie* $H_q(F/E)$, et pour les groupes de cohomologie *modifiés* (au sens de Tate) $\hat{H}^n(F/E)$, $n \in \mathbf{Z}$. Ces groupes sont reliés entre eux par les opérations suivantes :

(i) Supposons que F/E et F'/E' soient galoisiens, avec $E' \supset E$ et $F' \supset F$. On a alors un homomorphisme canonique $G_{F'/E'} \to G_{F/E}$ qui est compatible avec l'injection $A_F \to A_{F'}$ (cf. Chap. VII, § 5). On en déduit des homomorphismes

$$H^q(F/E) \to H^q(F'/E'), \qquad q \geqslant 0, \quad \text{dits canoniques.}$$

(ii) Supposons que $F' \supset F \supset E$, avec F'/E galoisien ainsi que F/E (c'est le cas particulier E = E' de (i)). L'homomorphisme canonique de (i) prend alors le nom d'*inflation*, et se note

$$\mathrm{Inf} : H^q(F/E) \to H^q(F'/E), \qquad q \geqslant 0.$$

(iii) Supposons que $F \supset E' \supset E$, avec F/E galoisien, donc aussi F/E'; c'est le cas particulier $F = F'$ de (i). Le groupe $G_{F/E'}$ est un sous-groupe du groupe $G_{F/E}$, et l'on a $A_F = A_{F'}$. Les homomorphismes canoniques $H^q(F/E) \to H^q(F/E')$ s'étendent alors aux groupes de cohomologie modifiés, et prennent le nom de *restriction* (cf. Chap. VIII, § 2). On les note :

$$\mathrm{Res} : \hat{H}^n(F/E) \to \hat{H}^n(F/E'), \qquad n \in \mathbf{Z}.$$

A côté de ces homomorphismes, on a des homomorphismes en sens inverse, qui prennent le nom de *corestriction* (*loc. cit*). On les note :

$$\mathrm{Cor} : \hat{H}^n(F/E') \to \hat{H}^n(F/E), \qquad n \in \mathbf{Z}.$$

(iv) Soit F/E une extension galoisienne, et soit $s \in G$. L'application $t \to s^{-1}ts$ est un isomorphisme : $G(sF/sE) \to G(F/E)$. L'application $a \to s.a$ est un isomorphisme de A_F sur A_{sF}. On vérifie tout de suite que ces deux applications sont compatibles, et elles définissent donc (par transport de structure) un isomorphisme

$$s^* : \hat{H}^n(F/E) \to \hat{H}^n(sF/sE), \qquad n \in \mathbf{Z}.$$

Lorsque s « est l'identité sur E », i.e. $s \in G_E$, on a $sE = E$, $sF = F$, et s^* est *l'application identique* de $\hat{H}^n(F/E)$ sur $\hat{H}^n(F/E)$; cela se voit en appliquant la proposition 3 du Chap. VII.

§ 2. *Formations de classes*

Une formation de classes consiste en la donnée d'une *formation* $\{G, \{G_E\}_{E \in \mathfrak{E}}, A\}$, et, pour chaque extension galoisienne F/E, d'un homomorphisme

$$\mathrm{inv}_E : H^2(F/E) \to \mathbf{Q}/\mathbf{Z}$$

ces données vérifiant les axiomes I et II ci-dessous :

Axiome I. *Pour toute extension galoisienne* F/E, *on a* $H^1(F/E) = 0$.

Cet axiome est équivalent à l'axiome en apparence plus faible suivant :

Axiome I'. *On a* $H^1(F/E) = 0$ *pour toute extension cyclique de degré premier.*

Supposons l'axiome I' vérifié, et soit F/E une extension galoisienne de degré p^n, avec p premier. Vu les propriétés élémentaires des p-groupes (Chap. IX, § 1), il existe E', avec $F \supset E' \supset E$, et E'/E cyclique de degré p. En appliquant la suite exacte des H^1 (Chap. VII, prop. 4), on obtient la suite exacte :

$$0 \longrightarrow H^1(E'/E) \xrightarrow{\mathrm{Inf}} H^1(F/E) \xrightarrow{\mathrm{Res}} H^1(F/E').$$

En raisonnant par récurrence sur n, on peut supposer que $H^1(F/E') = 0$. Vu l'axiome I', on a $H^1(E'/E) = 0$. On en déduit donc que $H^1(F/E) = 0$.

Si maintenant F/E est une extension galoisienne quelconque, et si les G_p sont les sous-groupes de Sylow de $G_{F/E}$, ce qui précède montre que $H^1(G_p, A_F) = 0$ pour tout p, d'où $H^1(F/E) = 0$ d'après le corollaire au théorème 4 du Chap. IX.

Avant d'énoncer l'axiome II, nous introduirons la notation $H^q(\ /E)$ pour désigner la limite inductive des $H^q(F/E)$ pour F parcourant l'ensemble des extensions galoisiennes de E; si $F' \supset F \supset E$, on prend pour homomorphisme

$$H^q(F/E) \to H^q(F'/E)$$

l'homomorphisme *d'inflation* (cf. § 1). Pour $q = 2$ ces homomorphismes sont *injectifs* : cela résulte de l'axiome I et de la proposition 5 du Chapitre VII. Le groupe $H^2(\ /E)$ est donc *réunion* des $H^2(F/E)$: la situation est tout à fait analogue à celle du groupe de Brauer.

La dernière donnée d'une formation de classes peut alors s'exprimer par un homomorphisme $\mathrm{inv}_E : H^2(\ /E) \to \mathbf{Q}/\mathbf{Z}$ vérifiant l'axiome :

Axiome II. *a) L'homomorphisme* inv_E *est injectif, et applique* $H^2(F/E)$ *sur l'unique sous-groupe de* $\mathbf{Q}/\mathbf{Z}$ *d'ordre égal à* $[F : E]$.

(Ceci doit avoir lieu pour toute extension galoisienne F/E.)

b) Si $E' \supset E$ *est une extension quelconque, on a* :

$$(**) \qquad \mathrm{inv}_{E'} \circ \mathrm{Res}_{E/E'} = [E' : E].\ \mathrm{inv}_E.$$

Proposition 1. (i) *Pour toute extension* E'/E, *l'homomorphisme*

$$\mathrm{Res}_{E/E'} : H^2(\ /E) \to H^2(\ /E')$$

est surjectif.

(ii) *Pour toute extension* E'/E, *l'homomorphisme*

$$\mathrm{Cor}_{E'/E} : H^2(\ /E') \to H^2(\ /E)$$

est injectif, et l'on a $\mathrm{inv}_E \circ \mathrm{Cor}_{E'/E} = \mathrm{inv}_{E'}$.

(iii) *Pour tout* $s \in G$, *notons* s^* *l'isomorphisme* $H^2(\ /E) \to H^2(\ /sE)$ *défini par passage à la limite à partir des homomorphismes du* § 1. *On a alors*

$$\mathrm{inv}_{sE} \circ s^* = \mathrm{inv}_E.$$

Pour prouver (i) il suffit de montrer que, si F est une extension galoisienne de E contenant E', l'homomorphisme de restriction applique $H^2(F/E)$ sur $H^2(F/E')$; or, soit $n = [F : E]$ et soit $n' = [F : E']$; si $x' \in H^2(F/E')$, l'élément $y' = \mathrm{inv}_{E'}(x')$ de $\mathbf{Q}/\mathbf{Z}$ vérifie $n'.y' = 0$; comme $\mathbf{Q}/\mathbf{Z}$ est divisible, il existe $y \in \mathbf{Q}/\mathbf{Z}$ tel que

$$[E' : E].y = y'$$

et l'on a $n.y = 0$; il existe donc $x \in H^2(F/E)$ tel que $\mathrm{inv}_E(x) = y$, et la formule (**) montre que $\mathrm{Res}(x)$ et x' ont même invariant. Comme $\mathrm{inv}_{E'}$ est injectif, on a donc bien $x' = \mathrm{Res}(x)$, ce qui démontre (i).

Puisque $\mathrm{Res}_{E/E'}$ est surjectif, la formule $\mathrm{inv}_E \circ \mathrm{Cor}_{E'/E} = \mathrm{inv}_{E'}$ équivaut à la formule :

$$\mathrm{inv}_E \circ \mathrm{Cor}_{E'/E} \circ \mathrm{Res}_{E/E'} = \mathrm{inv}_{E'} \circ \mathrm{Res}_{E/E'}.$$

Or cette dernière formule est bien exacte; en effet le membre de gauche est égal à $[E' : E].\mathrm{inv}_E$ (Chap. VII, proposition 6), et il en est de même du membre de droite d'après (**). Comme $\mathrm{inv}_{E'}$ est injectif, on voit en même temps que $\mathrm{Cor}_{E'/E}$ est injectif, ce qui achève de démontrer (ii).

Pour démontrer (iii), notons E_0 le « corps » correspondant au sous-groupe de G réduit à G lui-même (E_0 joue le rôle d'un corps de base). Comme $s \in G_{E_0}$, l'homomorphisme

$$s^* : H^2(\ /E_0) \to H^2(\ /sE_0) = H^2(\ /E_0)$$

est l'identité (§ 1), et l'on a bien $\mathrm{inv}_{sE_0} \circ s^* = \mathrm{inv}_{E_0}$. Si maintenant E est un corps quelconque, il résulte de (i) que tout $x \in H^2(\ /E)$ est de la forme $\mathrm{Res}_{E_0/E}(x_0)$, avec $x_0 \in H^2(\ /E_0)$. Comme Res et s^* commutent (transport de structure !), on en déduit :

$$\begin{aligned}\mathrm{inv}_{sE}(s^*x) &= \mathrm{inv}_{sE} \circ \mathrm{Res}_{sE_0/sE}(s^*x_0) = [sE : sE_0].\mathrm{inv}_{sE_0}(s^*x_0)\\ &= [E : E_0].\mathrm{inv}_{E_0}(x_0) = \mathrm{inv}_E(x), \text{ c.q.f.d.}\end{aligned}$$

§ 3. *Les classes fondamentales et l'application de réciprocité*

Jusqu'à la fin de ce chapitre nous notons $\{G, \{G_E\}_{E \in \mathbf{X}}, A, \mathrm{inv}_E\}$ une formation de classes.

Pour toute extension galoisienne F/E, de degré $n = [F : E]$, il existe un élément $u_{F/E} \in H^2(F/E)$ et un seul tel que $\mathrm{inv}_E(u_{F/E}) = 1/n$. De plus, d'après l'axiome II, cet élément *engendre* le groupe $H^2(F/E)$, qui est un groupe cyclique d'ordre n. Les propriétés des opérations Inf, Res, Cor, s^* vis-à-vis des invariants se traduisent sur les $u_{F/E}$ par les formules :

$$\begin{aligned}\mathrm{Inf}(u_{F/E}) &= [F' : F].u_{F'/E} && \text{si } F' \supset F \supset E, \text{ avec } F'/E \text{ et } F/E \text{ galoisiens.}\\ \mathrm{Res}(u_{F/E}) &= u_{F/E'} && \text{si } F \supset E' \supset E, \text{ avec } F/E \text{ galoisien.}\\ \mathrm{Cor}(u_{F/E'}) &= [E' : E].u_{F/E} && \text{—} \quad \text{—} \quad \text{—}\\ u_{sF/sE} &= s^*(u_{F/E}) && \text{si } F/E \text{ est galoisien et } s \in G.\end{aligned}$$

[En fait, on pourrait se donner les $u_{F/E}$ à la place de inv_E. Il faudrait supposer que $H^2(F/E)$ est cyclique d'ordre $[F : E]$, de générateur $u_{F/E}$, et que les $u_{F/E}$ vérifient les deux premières formules écrites ci-dessus.]

Les classes $u_{F/E}$ vérifient les hypothèses du théorème de Tate-Nakayama (Chap. IX, théorème 14). Nous nous bornerons à énoncer à nouveau le théorème de Tate :

THÉORÈME 1. *Pour toute extension galoisienne* F/E *et tout* $n \in \mathbf{Z}$, *l'homomorphisme*

$$\theta^n(F/E) : \hat{H}^n(G_{F/E}, \mathbf{Z}) \to \hat{H}^{n+2}(G_{F/E}, A_F) = \hat{H}^{n+2}(F/E)$$

défini par $x \to u_{F/E}.x$ (*cup-produit*), *est bijectif.*

Si $F \supset E' \supset E$, avec F/E galoisien, les homomorphismes θ^n *commutent avec la restriction et la corestriction.* Cela résulte des formules écrites ci-dessus pour les $u_{F/E}$ et

de formules relatives au cup-produit. Faisons la vérification, par exemple, pour la restriction. On doit montrer que :

$$\mathrm{Res}_{E/E'}(u_{F/E} \cdot x) = u_{F/E'} \cdot \mathrm{Res}_{E/E'}(x)$$

pour tout $x \in \hat{H}^n(G_{F/E}, \mathbf{Z})$.

Or le premier membre est égal à $\mathrm{Res}_{E/E'}(u_{F/E}) \cdot \mathrm{Res}_{E/E'}(x)$, d'après Cartan-Eilenberg [13], Chap. XII, p. 256. On en déduit bien le résultat cherché.

Si $F' \supset F \supset E$, avec F'/E et F/E galoisiens, les homomorphismes θ^n ne commutent pas avec l'*inflation* $\mathrm{Inf} : H^n(F'/E) \to H^n(F/E)$, $n \geqslant 0$, mais on a :

$$\mathrm{Inf} \circ \theta^n(F/E) = [F' : F] \cdot \theta^n(F'/E) \circ \mathrm{Inf}$$

cela se voit comme ci-dessus.

Cas particuliers. On a $H^1(G_{F/E}, \mathbf{Z}) = \mathrm{Hom}\,(G_{F/E}, \mathbf{Z}) = 0$, d'où $H^2(F/E) = 0$. D'autre part, la suite exacte :

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0$$

montre que $H^2(G_{F/E}, \mathbf{Z})$ s'identifie au groupe $\mathrm{Hom}\,(G_{F/E}, \mathbf{Q}/\mathbf{Z})$, c'est-à-dire au groupe des *caractères de degré* 1 de $G_{F/E}$; on a donc $H^1(F/E) = \mathrm{Hom}\,(G_{F/E}, \mathbf{Q}/\mathbf{Z})$.

Mais, bien entendu, le cas particulier le plus important est $n = -2$. On sait en effet que $\hat{H}^{-2}(G_{F/E}, \mathbf{Z})$ s'identifie au groupe $G_{F/E}$ rendu abélien, groupe que nous noterons $G^a_{F/E}$ ou $G_{F/E}/G'_{F/E}$ (un isomorphisme explicite a été donné au Chap. VII, § 4). D'autre part, on a :

$$\hat{H}^0(F/E) = A_E/N_{F/E}A_F$$

en notant $N_{F/E}$ l'opération de norme dans le $G_{F/E}$-module A_F. On voit donc que θ^{-2} définit un isomorphisme

$$\theta : G^a_{F/E} \to A_E/N_{F/E}A_F.$$

Si u est un 2-cocycle de la classe $u_{F/E}$, un calcul de cup-produit (annexe, lemme 4) montre que l'on a :

$$\theta(s) \equiv \sum_{t \in G} u(t, s) \bmod. N_{F/E}A_F, \qquad s \in G.$$

L'isomorphisme réciproque de θ est appelé *l'isomorphisme de réciprocité*, et noté :

$$a \to (a, F/E), \qquad a \in A_E, (a, F/E) \in G^a_{F/E}.$$

La proposition suivante donne une caractérisation commode de l'élément $(a, F/E)$:

PROPOSITION 2. *Soit* $\chi \in \mathrm{Hom}\,(G_{F/E}, \mathbf{Q}/\mathbf{Z})$ *un caractère de degré* 1 *du groupe* $G_{F/E}$ *(ou du groupe* $G^a_{F/E}$, *cela revient au même). Pour tout* $s \in G^a_{F/E}$ *posons*

$$\langle \chi, s \rangle = \chi(s) \in \mathbf{Q}/\mathbf{Z}.$$

Soit d'autre part $d\chi \in H^2(G_{F/E}, \mathbf{Z})$ *l'image de* χ *par le cobord associé à la suite exacte*

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0.$$

Enfin, si $a \in A_E$, *notons* $\bar{a}$ *l'image de* a *dans* $\hat{H}^0(F/E)$. *Avec ces notations, on a la formule*

$$(***) \qquad \langle \chi,\ (a,\ F/E)\rangle = \mathrm{inv}_E\,(\bar{a}.d\chi)$$

où $\bar{a}.d\chi \in H^2(F/E)$ *désigne le cup-produit des classes de cohomologie* $\bar{a}$ *et* $d\chi$.

[La formule (***) caractérise bien $(a, F/E)$ dans le groupe abélien $G_{F/E}$, puisqu'elle donne son produit scalaire avec tout élément du groupe dual.]

Pour simplifier l'écriture, nous poserons $s_a = (a, F/E)$; si $s \in G_{F/E}$ nous noterons $\bar{s}$ l'image canonique de s dans $\hat{H}^{-2}(G_{F/E}, \mathbf{Z}) = G^a_{F/E}$. Par définition même de θ, on a :

$$u_{F/E}.\bar{s}_a = \bar{a} \qquad \text{dans } \hat{H}^0(G_{F/E}, A_F).$$

En utilisant l'associativité du cup-produit, ceci donne :

$$\bar{a}.d\chi = u_{F/E}.(\bar{s}_a.d\chi), \qquad \text{avec } \bar{s}_a.d\chi \in \hat{H}^0(G_{F/E}, \mathbf{Z}).$$

Vu la commutation du cup-produit avec d, on a :

$$\bar{s}_a.d\chi = d(\bar{s}_a.\chi), \qquad \text{avec } \bar{s}_a.\chi \in \hat{H}^{-1}(G_{F/E}, \mathbf{Q}/\mathbf{Z}).$$

Si $n = [F : E]$, on peut identifier $\hat{H}^{-1}(G_{F/E}, \mathbf{Q}/\mathbf{Z})$ avec le sous groupe $\frac{1}{n}\mathbf{Z}/\mathbf{Z}$ de ses éléments d'ordre divisant n, et le cup-produit $\bar{s}_a.\chi$ s'identifie alors à $\langle \chi, s_a\rangle$, cf. annexe, lemme 3. Si l'on écrit $\langle \chi, s_a\rangle = r/n$, avec $r \in \mathbf{Z}$, on doit calculer

$$d(r/n) \in \hat{H}^0(G_{F/E}, \mathbf{Z})$$

et un calcul immédiat montre que $d(r/n) = r$. On en déduit que $u_{F/E}.(\bar{s}_a.d\chi) = r.u_{F/E}$, et l'invariant de cette classe de cohomologie est donc r/n, c'est-à-dire justement $\langle \chi, s_a\rangle$, c.q.f.d.

Propriétés fonctorielles de l'application de réciprocité.

Elles sont résumées par les quatre diagrammes commutatifs ci-dessous.

$$(1)\quad \begin{array}{ccc} A_{E'} & \xrightarrow{\text{norme}} & A_E \\ \downarrow & & \downarrow \\ G_{F/E'} & \xrightarrow{\text{can.}} & G^a_{F/E} \end{array} \qquad (2)\quad \begin{array}{ccc} A_E & \xrightarrow{\text{incl.}} & A_{E'} \\ \downarrow & & \downarrow \\ G^a_{F/E} & \xrightarrow{\text{Ver}} & G^a_{F/E'} \end{array}$$

$$(3)\quad \begin{array}{ccc} A_E & \xrightarrow{s^*} & A_{sE} \\ \downarrow & & \downarrow \\ G^a_{F/E} & \xrightarrow{s^*} & G^a_{sF/sE} \end{array} \qquad (4)\quad \begin{array}{ccc} A_E & = & A_E \\ \downarrow & & \downarrow \\ G^a_{F/E} & \xrightarrow{\text{proj.}} & G^a_{F/E}. \end{array}$$

Dans le diagramme (1), on a $F \supset E' \supset E$, avec F/E galoisien, et $G_{F/E'}$ est sous-groupe

de $G_{F/E}$; ceci définit un homomorphisme de $G^q_{F/E'}$ dans $G^q_{F/E}$, appelé canonique. Le diagramme est commutatif, car les deux flèches horizontales ne sont autres que des homomorphismes Cor, pour $n = 0$ et $n = -2$.

La situation est la même dans le diagramme (2) que dans (1). On note Ver le *transfert* (Chap. VII, § 7). Le diagramme est commutatif car les deux flèches horizontales ne sont autres que des homomorphismes Res, pour $n = 0$ et $n = -2$.

Dans le diagramme (3), on a $s \in G$; l'homomorphisme $s^* : A_E \to A_{sE}$ applique a sur $s.a$; l'homomorphisme analogue sur $G^q_{F/E}$ applique t sur sts^{-1}. La commutativité résulte d'un simple transport de structure, compte tenu de ce que

$$s^*(u_{F/E}) = u_{sF/sE}.$$

Dans le diagramme (4), on a $F' \supset F \supset E$, avec F/E et F'/E galoisiens. La commutativité ne résulte pas ici de celle de l'inflation mais elle se voit directement sur la caractérisation de $(a, F/E)$ donnée dans la proposition 2.

Le symbole $(a, */E)$.

La commutativité du diagramme (4) ci-dessus permet de passer à la limite sur des extensions croissantes F/E, E restant fixe. De façon précise, définissons $\mathfrak{A}(E)$ comme la *limite projective* des $G^q_{F/E}$ lorsque F parcourt l'ensemble ordonné filtrant des extensions galoisiennes de E. Dans le cas de la théorie de Galois, $\mathfrak{A}(E)$ est le groupe de Galois (topologique) de l'extension abélienne maximale du corps E. Si $a \in A_E$, la commutativité du diagramme (4) montre que les $(a, F/E)$ sont cohérents, et définissent donc un élément de $\mathfrak{A}(E)$, élément que l'on notera $(a, */E)$. On obtient ainsi un homomorphisme canonique :

$$A_E \to \mathfrak{A}(E).$$

Si E'/E est une extension quelconque, en passant à la limite sur les diagrammes (1) et (2) on obtient des diagrammes commutatifs

$$(1)_* \quad \begin{array}{ccc} A_{E'} & \xrightarrow{\text{norme}} & A_E \\ \downarrow & & \downarrow \\ \mathfrak{A}(E') & \xrightarrow{\text{can.}} & \mathfrak{A}(E) \end{array} \qquad (2)_* \quad \begin{array}{ccc} A_E & \xrightarrow{\text{incl.}} & A_{E'} \\ \downarrow & & \downarrow \\ \mathfrak{A}(E) & \xrightarrow{\text{Ver}} & \mathfrak{A}(E') \end{array}$$

Le diagramme (3) donne la formule :

$$(s.a, */sE) = s.(a, */E).s^{-1}.$$

Exercice. Montrer que $H^q(\ /E) = 0$ pour $q \geqslant 3$, pourvu que, pour tout entier n, il existe une extension F/E de degré multiple de n.

§ 4. *Extensions abéliennes et groupes de normes*

Soit E'/E une extension (galoisienne ou non), et soient s_i des représentants des classes à gauche de G_E mod.$G_{E'}$. Pour tout élément $a' \in A_{E'}$, on posera

$$N_{E'/E}(a') = \sum s_i.a'.$$

On vérifie tout de suite que $N_{E'/E}(a')$ ne dépend pas du choix des s_i et que c'est un élément de A_E. L'homomorphisme

$$N_{E'/E} : A_{E'} \to A_E$$

s'appelle la *norme*. Dans le cas galoisien, on retrouve la définition habituelle.

DÉFINITION. *Un sous-groupe* I *de* A_E *est appelé un groupe de normes s'il existe une extension* E'/E *telle que* $N_{E'/E}(A_{E'}) = I$.

Lorsque E'/E est une extension *abélienne*, l'isomorphisme de réciprocité

$$A_E/N_{E'/E}A_{E'} \to G_{E'/E}$$

montre que $N_{E'/E}A_{E'}$ est un sous-groupe *d'indice fini* de A_E, cet indice étant égal au degré [E' : E]. La proposition suivante ramène le cas général au cas abélien :

PROPOSITION 3. *Soit* E'/E *une extension, et soit* E'' *la plus grande extension abélienne de* E *contenue dans* E'. *On a alors*

$$N_{E'/E}(A_{E'}) = N_{E''/E}(A_{E''}).$$

Soit F une extension galoisienne de E contenant E', et soit $G = G_{F/E}$ son groupe de Galois. Soit $H = G_{F/E'}$. Le groupe de Galois de F/E'' est alors G'.H.

Soit $a \in N_{E''/E}(A_{E''})$. On a $(a, E''/E) = 1$ dans G/G'.H, ce qui signifie que l'élément $(a, F/E)$ de G/G' est dans l'image de l'homomorphisme H/H' → G/G'. La commutativité du diagramme (1) du § 3 et le fait que $A_{E'} \to H/H'$ est surjectif montrent qu'il existe $a' \in A_{E'}$ tel que

$$(N_{E'/E}a', F/E) = (a, F/E).$$

On en déduit qu'il existe $a'' \in A_F$ avec $N_{F/E}a'' = N_{E'/E}a' - a$, d'où :

$$a = N_{E'/E}(a' - N_{F/E'}a'')$$

ce qui montre que $N_{E''/E}(A_{E''}) \subset N_{E'/E}(A_{E'})$. L'inclusion opposée résulte de la transitivité des normes.

COROLLAIRE. *Le groupe de normes* $N_{E'/E}A_{E'}$ *est d'indice fini dans* A_E; *cet indice divise* [E' : E], *et lui est égal si et seulement si* E' *est une extension abélienne de* E.

En effet, on a $(A_E : N_{E''/E}A_{E''}) = [E'' : E]$, qui divise [E' : E], et l'égalité a lieu si et seulement si E' = E''.

Soit F/E une extension abélienne; pour simplifier l'écriture, on posera

$$I_F = N_{F/E}A_F.$$

PROPOSITION 4. *L'application* $F \to I_F$ *est une bijection de l'ensemble des extensions abéliennes de* E *sur l'ensemble des groupes de normes de* A_E; *cette correspondance renverse l'inclusion, et l'on a* :

$$I_{F.F'} = I_F \cap I_{F'}, \qquad I_{F \cap F'} = I_F + I_{F'}.$$

De plus, tout sous-groupe de A_E *qui contient un groupe de normes est un groupe de normes.*

Si F et F′ sont deux extensions abéliennes, F.F′ est une extension abélienne, et $I_{F.F'} \subset I_F \cap I_{F'}$; inversement, si $a \in I_F \cap I_{F'}$, l'élément $(a, F.F'/E)$ de $G_{F.F'/E}$ a une image triviale dans $G_{F/E}$ et $G_{F'/E}$, donc est trivial, ce qui montre que $a \in I_{F.F'}$. En particulier, si $I_F \supset I_{F'}$, on voit que $I_{F.F'} = I_{F'}$, d'où $[F.F' : E] = [F : E]$ et $F' \subset F$. On en déduit que la correspondance $F \to I_F$ est bijective et renverse l'inclusion. Les autres assertions de la proposition sont immédiates.

Il résulte de la proposition précédente que les groupes de normes définissent sur A_E une *topologie*. Si l'on note $\hat{A}_E$ le complété-séparé de A_E pour cette topologie, on a (par définition) :

$$\hat{A}_E = \varprojlim A_E/I \qquad (I \text{ parcourant les groupes de normes})$$

et le symbole $(a, */E)$ définit un *isomorphisme de* $\hat{A}_E$ *sur le groupe topologique* $\mathfrak{A}(E)$ du § 3.

La topologie que nous venons de définir sur A_E est appelée parfois la topologie « normique », pour la distinguer de celle qui intervient dans le théorème d'existence.

§ 5. *Le théorème d'existence*

Il s'agit de caractériser les groupes de normes de A_E. Pour cela, on supposera que l'on s'est donné sur chacun des A_E une topologie, compatible avec la structure de groupe de A_E, et telle que si $E \subset F$, la topologie de A_E soit *induite* par celle de A_F, et que, pour tout $s \in G$, l'application $a \to s.a$ soit une application *continue* de A_E dans A_{sE}. Ces conditions entraînent que l'application $N_{F/E} : A_F \to A_E$ est *continue*.

Nous allons imposer à ces topologies les axiomes III-1, III-2 et III-3 ci-dessous, et nous verrons que l'on peut alors caractériser les groupes de normes comme les sous-groupes fermés d'indice fini de A_E (théorème 2).

Axiome III-1. *Pour toute extension* F/E, *l'application*

$$N_{F/E} : A_F \to A_E$$

a une image fermée et un noyau compact.

[Lorsque A_E et A_F sont localement compacts dénombrables à l'infini — ce qui est le cas dans toutes les applications — l'axiome III-1 signifie que $N_{F/E}$ est une application *propre*.]

Comme $N_{F/E}A_F$ est *fermé*, et *d'indice fini* dans A_E, c'est un sous-groupe *ouvert* de A_E (son complémentaire est fermé, car c'est une réunion finie d'ensembles fermés). En particulier la topologie donnée sur A_E est *plus fine* que la topologie normique.

Définition. *On appelle groupe des normes universelles de* E, *et on note* D_E, *l'intersection de tous les groupes de normes de* E.

Si $a \in A_E$, on a $a \in D_E$ si et seulement si $(a, F/E) = 1$ pour toute extension abélienne F/E; le groupe D_E est donc le noyau de l'application de réciprocité $A_E \to \mathfrak{A}(E)$.

PROPOSITION 5. *Pour toute extension* F/E, *on a* $N_{F/E}D_F = D_E$.

L'inclusion $N_{F/E}D_F \subset D_E$ résulte de la transitivité des normes. Inversement, soit $a \in D_E$, et soit F′ une extension de F; notons K(F′) l'ensemble des $b \in A_F$ dont la norme dans E est égale à a, et qui sont normes d'éléments de F′. On a :

$$K(F') = N_{F'/F}A_{F'} \cap N_{F/E}^{-1}(a)$$

ce qui montre que K(F′) est compact; de plus, puisque $a \in D_E$, on a $a = Nb'$, avec $b' \in A_{F'}$, et l'image de b' dans A_F appartient à K(F′), qui est donc non vide. Lorsque F′ varie, les K(F′) forment une famille filtrante décroissante de sous-espaces compacts non vides de A_F; leur intersection est donc non vide, et si $b \in \bigcap K(F')$, il est clair que $b \in D_F$ et que $N_{F/E}(b) = a$, c.q.f.d.

AXIOME III-2. *Pour tout nombre premier p il existe un corps* E_p *tel que, pour* $E \supset E_p$, *l'application* $\varphi_p : x \to px$ *de* A_E *dans lui-même vérifie la condition suivante* :

(i) *Le noyau de* φ_p *est compact, et son image contient* D_E.

[C'est le seul axiome dont la vérification soit difficile dans les applications.]

PROPOSITION 6. *Pour tout corps* E, *le groupe* D_E *est divisible, et égal à* $\bigcap n.A_E$.

Nous allons d'abord montrer que, pour tout corps E, et tout nombre premier p, on a $D_E = p.D_E$. Soit $a \in D_E$ et soit F une extension de E contenant E_p (i.e. « suffisamment grande »); soit L(F) l'ensemble des $b \in A_E$ tels que $pb = a$ et $b \in N_{F/E}A_F$; c'est un sous-ensemble compact de A_E. On a $L(F) \neq \emptyset$; en effet, d'après la proposition 5, on a $a = N_{F/K}x$, avec $x \in D_F$, d'où $x = py$, avec $y \in A_F$, et on peut prendre $b = N_{F/E}y$. On en conclut comme ci-dessus que l'intersection des L(F) est non vide. Si b appartient à cette intersection, on a $pb = a$ et $b \in D_E$, ce qui démontre notre assertion.

On tire de là le fait que D_E est un groupe divisible. On a donc en tout cas

$$D_E \subset \bigcap n.A_E.$$

Inversement, si $a \in \bigcap n.A_E$, et si F/E est de degré n, on a $a = n.b$, $b \in A_E$, d'où $a = N_{F/E}b$, ce qui montre que $a \in D_E$, c.q.f.d.

AXIOME III-3. *Il existe un sous-groupe compact* U_E *de* A_E *tel que tout sous-groupe fermé d'indice fini de* A_E *qui contient* U_E *soit un groupe de normes.*

THÉORÈME 2. *Supposons les axiomes* III-1, III-2, III-3 *vérifiés. Pour qu'un sous-groupe de* A_E *soit un groupe de normes, il faut et il suffit qu'il soit fermé et d'indice fini dans* A_E.

On sait que ces conditions sont nécessaires. Soit I un sous-groupe de A_E les vérifiant; si $(A_E : I) = n$, on a $n.A_E \subset I$, d'où $D_E \subset I$ d'après la proposition 6. Si N parcourt l'ensemble des groupes de normes, on a donc

$$\bigcap (N \cap U_E) = D_E \cap U_E \subset I.$$

Comme les $N \cap U_E$ sont compacts, et que I est ouvert, il existe un N tel que $N \cap U_E \subset I$. On a alors l'inclusion :

$$N \cap (U_E + (N \cap I)) \subset I.$$

En effet, si a appartient à cette intersection, on peut écrire $a = a' + a''$, avec $a' \in U_E$ et $a'' \in N \cap I$; on a $a' = a - a'' \in N$, d'où $a' \in U_E \cap N$ et $a' \in I$, ce qui montre bien que $a \in I$.

Le groupe $N \cap I$ est fermé et d'indice fini (l'intersection de deux sous-groupes d'indice fini étant d'indice fini); donc $U_E + (N \cap I)$, qui le contient, est fermé, d'indice fini, et contient U_E; d'après III-3, c'est un groupe de normes. Il en est alors de même de $N \cap (U_E + (N \cap I))$ (proposition 4), donc de I (proposition 4), c.q.f.d.

Exemple. Dans le cas du corps de classes local, on prend $A_E = E^*$, et l'on munit E^* de la topologie induite par celle de E, qui en fait un groupe localement compact. L'axiome III-1 est trivial. Dans l'axiome III-3, on prend pour U_E le groupe des *unités*; la suite exacte

$$0 \to U_E \to E^* \to \mathbf{Z} \to 0$$

montre que les sous-groupes d'indice fini de E^* contenant U_E sont les images réciproques des sous-groupes $n.\mathbf{Z}$ de $\mathbf{Z}$; ils sont groupes de normes pour les extensions *non ramifiées* de E. On montre de plus que $D_E = 0$. On en déduit la structure du groupe topologique $\mathfrak{A}(E) = \hat{A}_E$: on a une suite exacte :

$$0 \to U_E \to \mathfrak{A}(E) \to \hat{\mathbf{Z}} \to 0$$

où $\hat{\mathbf{Z}}$ désigne le complété de $\mathbf{Z}$ pour la topologie définie par les $n.\mathbf{Z}$ (c'est le produit des groupes additifs $\mathbf{Z}_p$, p premier). Nous reviendrons là-dessus au Chap. XIV, § 6.

Quelques calculs de cup-produits

Notations. On désigne par G un groupe fini, et par A, B, ..., des G-modules. Si a est un élément de A invariant par G (resp. tel que $Na = 0$), on note $\bar{a}^0$ (resp. $\bar{a}_0$) son image canonique dans le groupe $\hat{H}^0(G, A)$ (resp. $\hat{H}^{-1}(G, A)$).

LEMME 1. *Soient* A *et* B *deux* G*-modules, et soit* $a \in A^G$; *soit* $f_a : \mathbf{Z} \to A$ *le* G*-homomorphisme qui applique* $1 \in \mathbf{Z}$ *sur* $a \in A$. *Soit* $x \in \hat{H}^n(G, B)$. *Le cup-produit*

$$\bar{a}^0 . x \in \hat{H}^n(G, A \otimes B)$$

est égal à l'image de x *par l'homomorphisme* $f_a \otimes 1 : B \to A \otimes B$.

Faisons la démonstration pour $n \geqslant 0$, par exemple. Pour $n = 0$, on a effectivement $\bar{a}^0 . x = (f_a \otimes 1)(x)$, par définition même du cup-produit. Raisonnons par récurrence sur n. On sait qu'il existe une suite exacte de G-modules

$$0 \to B \to B' \to B'' \to 0$$

où B' est un G-module *induit*, et où B est facteur direct dans B' pour sa structure de groupe abélien. On peut alors écrire $x = dy$, avec $y \in \hat{H}^{n-1}(G, B)$, d'où

$$\bar{a}^0 . x = \bar{a}^0 . dy = d(\bar{a}^0 . y)$$

et l'hypothèse de récurrence, appliquée au produit $\bar{a}^0 . y$, donne le résultat cherché.

LEMME 2. *Soit* $a \in A$ *un élément tel que* $Na = 0$, *et soit* f *un* 1*-cocycle de* G *à valeurs dans* B; *soit* $\bar{f} \in H^1(G, B)$ *la classe de cohomologie de* f. *On a alors* :

$$\bar{a}_0 . \bar{f} = \bar{c}^0 \qquad \text{dans } \hat{H}^0(G, A \otimes B), \qquad \text{avec } c = -\sum_{t \in G} ta \otimes f(t).$$

On choisit une suite exacte

$$0 \to B \to B' \to B'' \to 0$$

vérifiant les mêmes propriétés que ci-dessus. Comme $H^1(G, B') = 0$, il existe $b' \in B'$ tel que $f(t) = t.b' - b'$. Soit $b'' \in (B'')^G$ l'image de b' dans B''. On a :

$$\bar{f} = d(\bar{b}''^0) \qquad \text{dans } H^1(G, B).$$

d'où $\bar{a}_0.\bar{f} = -d(\bar{a}_0.\bar{b}'^0)$, puisque $\bar{a}_0$ est une classe de cohomologie de degré *impair*.

D'après le lemme 1, on a $\bar{a}_0.\bar{b}'^0 = \overline{a\otimes b'^0}$. On en déduit (compte tenu de ce que l'opérateur $d : \hat{H}^{-1}(G, A\otimes B') \to H^0(G, A\otimes B)$ est défini par la norme) :

$$\bar{a}_0.\bar{f} = -\bar{c}^0, \qquad \text{avec } c = N(a\otimes b') = \sum_{t\in G} ta\otimes tb'$$

Or ceci peut s'écrire :

$$c = \sum_{t\in G} ta\otimes(f(t) + b') = \sum_{t\in G} ta\otimes f(t)$$

puisque $Na = 0$, c.q.f.d.

Considérons maintenant la suite exacte :

$$0 \to I \to \mathbf{Z}[G] \to \mathbf{Z} \to 0$$

et, pour tout $s\in G$, notons i_s l'élément $s - 1$ de I. On a donc $(\overline{i_s})_0 \in \hat{H}^{-1}(G, I)$. Soit $\bar{s}\in\hat{H}^{-2}(G, \mathbf{Z})$ tel que $d\bar{s} = (\overline{i_s})_0$. L'application $s \to \bar{s}$ définit par passage au quotient *l'isomorphisme canonique* de G/G' sur $\hat{H}^{-2}(G, \mathbf{Z})$, cf. Chap. VII, § 4.

LEMME 3. *Soit* B *un* G*-module et soit* $f : G \to B$ *un* 1*-cocycle de* G *à valeurs dans* B. *Soit* $\bar{f}\in H^1(G, B)$ *la classe de cohomologie de* f. *Pour tout* $s\in G$, *on a :*

$$\bar{s}.\bar{f} = \overline{f(s)}_0 \qquad \textit{dans } \hat{H}^{-1}(G, B).$$

[On a identifié les G-modules $\mathbf{Z}\otimes B$ et B.]

L'homomorphisme $d : \hat{H}^{-1}(G, B) \to \hat{H}^0(G, I\otimes B)$ est un isomorphisme. Il suffira donc de montrer que les images par d des éléments $\bar{s}.\bar{f}$ et $\overline{f(s)}_0$ coïncident. Vu la définition de d, on a :

$$d(\overline{f(s)}_0) = \bar{x}^0, \qquad \text{avec } x = \sum_{t\in G} t\otimes t.f(s).$$

D'autre part, on a :

$$d(\bar{s}.\bar{f}) = (\overline{i_s})_0.\bar{f} = \bar{y}^0, \qquad \text{avec } y = -\sum_{t\in G} t.i_s\otimes f(t)$$

en vertu du lemme 2.

Ceci s'écrit :

$$y = \sum_{t\in G}(t - ts)\otimes f(t)$$
$$= \sum_{t\in G} t\otimes f(t) - \sum_{t\in G} ts\otimes f(t)$$

Mais $f(ts) = f(t) + t.f(s)$, et la somme $\sum ts \otimes f(t)$ peut être écrite sous la forme $\sum ts \otimes f(ts) - \sum ts \otimes t.f(s)$. Le premier terme se détruit avec $\sum t \otimes f(t)$, et il reste :

$$y = \sum_{t \in G} ts \otimes t.f(s).$$

On a donc $x - y = \sum_{t \in G} t(1 - s) \otimes t.f(s) = N((1 - s) \otimes f(s))$, ce qui montre bien que $\bar{x}^0 = \bar{y}^0$, c.q.f.d.

LEMME 4. *Soit* B *un* G*-module, et soit* $u : G \times G \to B$ *un 2-cocycle de* G *à valeurs dans* B. *Soit* $\bar{u} \in H^2(G, B)$ *la classe de cohomologie de* u. *Pour tout* $s \in G$, *on a* :

$$\bar{s}.\bar{u} = a^0, \qquad \text{avec } a = \sum_{t \in G} u(t, s).$$

Soit $0 \to B \to B' \to B'' \to 0$ une suite exacte de G-modules, où B′ est un G-module *induit*. Puisque $H^2(G, B') = 0$, il existe une 1-cochaîne $f' : G \to B'$ telle que :

$$u(x, y) = x.f'(y) - f'(xy) + f'(x), \qquad x, y \in G.$$

En composant avec $B' \to B''$, on obtient un 1-cocycle $f'' : G \to B$ dont la classe de cohomologie $\overline{f''}$ vérifie $d(\overline{f''}) = \bar{u}$. On en déduit :

$$\begin{aligned} \bar{s}.\bar{u} = \bar{s}.d(\overline{f''}) = d(\bar{s}.\overline{f''}) &= d(\overline{f''(s)}_0) \quad \text{(lemme 3)} \\ &= \overline{N(f''(s))}^0. \end{aligned}$$

On est donc ramené à calculer $a = N(f''(s)) = \sum_{t \in G} t.f''(s)$. L'identité :

$$u(t, s) = t.f''(s) - f''(ts) + f''(t)$$

donne par sommation :

$$\sum_{t \in G} u(t, s) = a - \sum_{t \in G} f''(ts) + \sum_{t \in G} f''(t) = a, \quad \text{c.q.f.d.}$$

QUATRIÈME PARTIE

CORPS DE CLASSES LOCAL

CHAPITRE XII

GROUPE DE BRAUER D'UN CORPS LOCAL

Dans tout ce chapitre, la lettre K désigne un corps complet pour une valuation discrète v. On note A l'anneau de v, et $\mathbf{K}$ son corps résiduel.

§ 1. *Existence d'un corps neutralisant non ramifié*

THÉORÈME 1. *Supposons que le corps résiduel* $\mathbf{K}$ *soit parfait. Tout élément du groupe de Brauer* B_K *de* K *est alors décomposé par une extension finie non ramifiée de* K.

Soit K_{nr} l'extension maximale non ramifiée de K. On sait (Chap. X, § 7, exemple (*b*)) que son groupe de Brauer est nul. Si $a \in B_K$, l'image de a dans $B_{K_{nr}}$ est donc nulle, et comme K_{nr} est réunion filtrante croissante de sous-extensions finies non ramifiées K′ de K, il s'ensuit que l'image de a dans l'un des $B_{K'}$ est nulle.

[Nous avons utilisé le fait suivant, dont la vérification est triviale : si un corps E est réunion d'une famille filtrante croissante de sous-corps E_i, l'homomorphisme canonique $\varinjlim B_{E_i} \to B_E$ est un isomorphisme.]

COROLLAIRE. *Le groupe de Brauer de* K *s'identifie à* $H^2(K_{nr}/K)$.

C'est une traduction du th. 1.

Remarques. 1) L'hypothèse suivant laquelle $\mathbf{K}$ est parfait ne peut pas être supprimée, cf. Chap. XIV, § 5, exer. 2.

2) La démonstration du théorème 1 donnée ci-dessus repose en définitive sur les calculs de norme du Chap. V. Le lecteur trouvera au paragraphe suivant une autre démonstration, basée sur l'interprétation du groupe de Brauer au moyen des classes d'algèbres centrales simples.

Exercices. 1. Montrer que $H^q(\ /K) = H^q(K_{nr}/K)$ pour tout $q \geqslant 0$ (utiliser la suite spectrale des extensions de groupes, obtenue par passage à la limite à partir de celle des groupes finis, cf. [37]).

2. Soit K un corps complet pour une valuation discrète, et soit L/K une extension galoisienne finie, totalement ramifiée, de groupe de Galois G. Soit $w : L^* \to \mathbf{Z}$ la valuation de L.

a) Montrer que l'homomorphisme $\hat{H}^q(G, L^*) \to \hat{H}^q(G, \mathbf{Z})$ défini par w est nul pour tout $q \in \mathbf{Z}$. (Construire une extension L_0/K_0 par le procédé de l'exer. 4 du Chap. II, § 2; factoriser w en $L^* \to \hat{L}_0^* \to \mathbf{Z}$, et remarquer que $\hat{L}_0^*$ est cohomologiquement trivial.)

b) En déduire une suite exacte :

$$0 \to \hat{H}^{q-1}(G, \mathbf{Z}) \xrightarrow{\delta} \hat{H}^q(G, U_L) \to \hat{H}^q(G, L^*) \to 0.$$

Expliciter les cas particuliers $q = 1$ et $q = 2$.

c) Soit π une uniformisante de L, et soit $a \in H^1(G, U_L)$ la classe de l'homomorphisme croisé $s \to \pi^{s-1}$ (en notation exponentielle). Montrer que $\delta(x) = a.x$ pour tout $x \in \hat{H}^{q-1}(G, \mathbf{Z})$.

d) Soit V (resp. W) le sous-groupe de L^* formé des éléments $\prod_{s \in G} x_s^{s-1}$, où x_s parcourt L^* (resp. U_L). Soit G^a le quotient de G par son groupe des commutateurs. Montrer que l'application $s \to \pi^{s-1}$ définit par passage au quotient un isomorphisme de G^a sur V/W. (Appliquer (*a*) avec $q = -1$.)

§ 2. *Existence d'un corps neutralisant non ramifié (démonstration directe)*

Soit D un *corps gauche* de centre K et de rang n^2 sur K. Nous allons commencer par définir sur D une « valuation discrète » prolongeant celle de K. On procède exactement comme dans le cas commutatif (cf. Chap. II, § 2) :

Soit Nrd : $D^* \to K^*$ la *norme réduite* (cf. Bourbaki, *Alg.*, Chap. VIII, § 12). Si $x \in D^*$, posons :

$$v'(x) = v(\mathrm{Nrd}(x)), \qquad v'(0) = +\infty.$$

L'application $v' : D^* \to \mathbf{Z}$ est un homomorphisme; on a $v'(x) = nv(x)$ si $x \in K^*$ (car $\mathrm{Nrd}(x) = x^n$ dans ce cas); soit d le générateur positif du sous-groupe $v'(D^*)$ de $\mathbf{Z}$; posons :

$$w = \frac{1}{d} v'.$$

L'application $w : D^* \to \mathbf{Z}$ est un homomorphisme surjectif.

PROPOSITION 1. a) *On a* $w(x) = \frac{n}{d} v(x)$ *si* $x \in K^*$.

b) *On a* $w(x + y) \geqslant \mathrm{Inf}(w(x), w(y))$ *et* $w(xy) = w(x) + w(y)$.

c) *Soit a un nombre réel strictement compris entre* 0 *et* 1. *Si l'on pose* $\|x\|_D = a^{w(x)}$ *on obtient une norme sur* D; *la topologie définie par cette norme est la topologie produit de* D (*identifié à* K^n).

d) *Pour qu'un élément* $x \in D$ *soit entier sur* A, *il faut et il suffit que* $w(x)$ *soit* $\geqslant 0$. *L'ensemble* B *de ces éléments est un sous-anneau de* D.

Si L est un sous-corps commutatif de D contenant K, et si $x \in L$, Nrd (x) est une puissance de $N_{L/K}(x)$; cela se voit, par exemple, en se ramenant au cas où L

est maximal, auquel cas cela résulte de la définition de la norme réduite (Bourbaki, *loc. cit.*). Il s'ensuit que la restriction de w à L est un *multiple* de la valuation discrète v_L de L prolongeant v; cette remarque, appliquée au corps $L = K(x^{-1}y)$, montre que $w(1 + x^{-1}y) \geqslant \mathrm{Inf}(w(1), w(x^{-1}y))$, d'où en ajoutant $w(x)$ aux deux membres : $w(x + y) \geqslant \mathrm{Inf}(w(x), w(y))$, ce qui démontre b). L'assertion a) est triviale. On en déduit que $\|x\|_D$ est une norme sur D, et fait de D un espace vectoriel normé sur K; comme K est complet, on en déduit c) (cf. Bourbaki, *Esp. Vect. Top.*, Chap. I, § 2, th. 2). Enfin, pour que $x \in D$ soit entier sur A, il faut et il suffit (cf. Chap. II, § 2) que la valuation de x dans $K(x)$ soit $\geqslant 0$, ce qui équivaut bien à dire que $w(x) \geqslant 0$. Les formules b) montrent que B est un anneau.

LEMME 1. *Supposons* K *parfait, et* $n \geqslant 2$. *Il existe alors un sous-corps commutatif* L *de* D, *contenant* K, *non ramifié sur* K, *et distinct de* K.

Supposons qu'un tel corps n'existe pas. Alors, pour toute sous-extension commutative L de K contenue dans D, le corps résiduel $\bar{L}$ de L est égal à $\bar{K}$ (sinon, en effet, le cor. 3 au th. 3 du Chap. III, § 5 montrerait que L contient une sous-extension non ramifiée distincte de K). Soit π un élément de D tel que $w(\pi) = 1$ (π est une « uniformisante » de D), et soit $b \in B$. Appliquant ce qui précède au corps $L = K(b)$, on voit qu'il existe $a \in A$ tel que $w(b - a) \geqslant 1$, i.e. :

$$b = a + \pi b_1, \qquad \text{avec } b_1 \in B.$$

En appliquant ceci à b_1, et en itérant, on conclut que pour tout entier N, on a :

$$b = a + \pi a_1 + \cdots + \pi^{N-1} a_{N-1} + \pi^N b_N, \qquad \text{avec } a_i \in A,\ b_N \in B$$

ce qui montre que b est adhérent à $K(\pi)$. Comme $K(\pi)$ est un sous-espace vectoriel de D, il est fermé (cf. Bourbaki, *loc. cit.*, cor. 1 au th. 2), et l'on a $b \in K(\pi)$, d'où $B \subset K(\pi)$. Mais, pour tout $x \in D$, on a $\pi^m x \in B$ pour m assez grand. On a donc $D = K(\pi)$, et D est commutatif, contrairement à l'hypothèse $n \geqslant 2$.

PROPOSITION 2. *Supposons* K *parfait. Il existe alors un sous-corps commutatif maximal de* D *qui est non ramifié sur* K.

Procédons par récurrence sur n. Le cas $n = 1$ étant trivial, on peut supposer $n \geqslant 2$. D'après le lemme 1, il existe une sous-extension non ramifiée K'/K, contenue dans D, avec $K' \neq K$. Soit D' le commutant de K' dans D. Le corps gauche D' a pour centre K' (théorème de bicommutation, cf. Bourbaki, *Alg.*, Chap. VIII, § 10, th. 2) et son degré est $< n^2$. D'après l'hypothèse de récurrence, il existe un sous-corps commutatif maximal L de D', contenant K', et non ramifié sur K'. Le corps L est non ramifié sur K. De plus, on a :

$$[L : K]^2 = [L : K']^2 [K' : K]^2 = [D' : K'][K' : K]^2 = [D' : K][K' : K]$$
$$= [D : K] \qquad \text{(cf. Bourbaki, } \textit{loc. cit.}\text{)}$$

ce qui montre que L est un sous-corps commutatif maximal de D, et achève de démontrer la proposition.

Le théorème 1 résulte directement de la proposition précédente, puisqu'un sous-corps commutatif maximal d'un corps gauche est corps neutralisant pour ce corps gauche.

Exercices. 1) *a*) Montrer que B est un A-module libre de rang n^2. (Utiliser la trace réduite, ou bien raisonner comme au Chap. II, § 2.)

b) Montrer que tout idéal de B est bilatère, et égal, soit à 0, soit à l'ensemble des $x \in D$ tels que $w(x) \geqslant n$ $(n = 0, 1, \ldots)$.

c) Déduire de *b*) que tout B-module de type fini sans torsion est libre.

2) Soit $\overline{B} = B/\pi B$. Montrer que $\overline{B}$ est un corps gauche. Si l'on pose $\varphi = [\overline{B} : \overline{K}]$, et si e est l'indice de ramification de w par rapport à v (i.e. l'entier $\frac{n}{d}$ de la prop. 1) montrer que $e\varphi = n^2$.

3) On suppose que $\overline{K}$ est parfait. On note $\overline{E}$ le centre de $\overline{B}$, et l'on pose

$$[\overline{E} : \overline{K}] = e', \qquad [\overline{B} : \overline{E}] = f^2.$$

On a $ee'f^2 = n^2$. Montrer que tout sous-corps commutatif de $\overline{B}$ est de degré $\leqslant n$ sur $\overline{K}$ (relever dans B un élément primitif d'un tel corps); en déduire que $ef \leqslant n$. En utilisant la prop. 2, montrer qu'il existe un sous-corps de $\overline{B}$ de degré n sur $\overline{K}$, et en déduire que $ef = n$, d'où $e = e'$.

4) Les hypothèses et notations étant celles de l'exercice précédent, définir la *différente* de B par rapport à A au moyen de la trace réduite. Montrer qu'elle est égale à B si et seulement si $e = 1$.

[Pour plus de détails sur la structure de B, voir Deuring [19], Chap. VI, ou Schilling [54], Chap. V.]

§ 3. *Détermination du groupe de Brauer*

On suppose à partir de maintenant que K est parfait.

PROPOSITION 3. *Le groupe* B_K *est réunion des sous-groupes* $H^2(L/K)$, *où* L *parcourt l'ensemble des extensions galoisiennes finies non ramifiées de* K.

En effet, ces extensions correspondent aux sous-extensions L de K_{nr} qui sont finies et galoisiennes sur K, et la réunion de ces L est K_{nr}; la réunion des L est donc K_{nr}.

Nous sommes ainsi ramenés à déterminer $H^2(L/K)$. Posons :

$$\mathfrak{g} = G(L/K) = G(\overline{L}/\overline{K}).$$

Considérons la suite exacte :

$$0 \to U_L \to L^* \xrightarrow{v} \mathbf{Z} \to 0$$

où v désigne la valuation de L (qui prolonge celle de K avec indice de ramification 1).

C'est là une suite exacte de $\mathfrak{g}$-modules; de plus, cette suite « se décompose » : le choix d'une uniformisante π de K permet en effet d'identifier L^* à $U_L \times \mathbf{Z}$ de façon compatible avec les opérations de $\mathfrak{g}$ (bien entendu, il n'en irait plus de même si L/K était ramifiée).

On en déduit donc la suite exacte décomposée de groupes abéliens :

$$0 \to H^q(\mathfrak{g}, U_L) \to H^q(L/K) \to H^q(\mathfrak{g}, \mathbf{Z}) \to 0, \qquad q \geqslant 0.$$

Comme au Chap. IV, notons U_L^n le sous-groupe de U_L formé des $a \in U_L$ tels que $v(1-a) \geqslant n$.

LEMME 2. *On a* $H^q(\mathfrak{g}, U_L^n) = 0$ *pour tout* $q \geqslant 1$.

Filtrons U_L^1 par les U_L^n; les quotients U_L^n/U_L^{n+1} sont isomorphes comme $\mathfrak{g}$-modules au groupe additif $\bar{L}$; ils ont donc une cohomologie triviale (Chap. X, § 1, prop. 1), et le lemme 2 est un cas particulier du suivant :

LEMME 3. *Soit* $\mathfrak{g}$ *un groupe fini, et soit* M *un* $\mathfrak{g}$*-module filtré par une suite décroissante* M_n, $n \geqslant 1$, *de sous-*$\mathfrak{g}$*-modules, avec* $M_1 = M$. *On suppose que* M *est séparé et complet pour la topologie définie par les* M_n. *Soit q un entier* $\geqslant 0$. *Si* $H^q(\mathfrak{g}, M_n/M_{n+1}) = 0$ *pour tout* $n \geqslant 1$, *on a* $H^q(\mathfrak{g}, M) = 0$.

Soit $\varphi(g_1, \ldots, g_q)$ un q-cocycle de $\mathfrak{g}$ à valeurs dans M. Puisque $H^q(\mathfrak{g}, M_1/M_2) = 0$, il existe une $(q-1)$-cochaîne ψ_1 de $\mathfrak{g}$ à valeurs dans M_1, telle que l'on ait :

$$\varphi = \delta\psi_1 + \varphi_1, \qquad \varphi_1 \text{ étant un } q\text{-cocycle à valeurs dans } M_2.$$

On construit ainsi de proche en proche une suite (ψ_n, φ_n) où ψ_n est une $(q-1)$-cochaîne à valeurs dans M_n, et φ_n un q-cocycle à valeurs dans M_{n+1}, avec :

$$\begin{aligned} \varphi &= \delta\psi_1 + \varphi_1 \\ &\vdots \\ \varphi_n &= \delta\psi_{n+1} + \varphi_{n+1} \\ &\vdots \end{aligned}$$

Posons $\psi = \psi_1 + \cdots + \psi_n + \cdots$. Vu les hypothèses faites sur M, cette série converge et définit une $(q-1)$-cochaîne de $\mathfrak{g}$ à valeurs dans M. En sommant les égalités précédentes, on voit que $\varphi = \delta\psi$, ce qui démontre le lemme.

Revenons à la cohomologie du groupe U_L. On a une suite exacte de $\mathfrak{g}$-modules :

$$0 \to U_L^1 \to U_L \to \bar{L}^* \to 0.$$

Compte tenu du lemme 2, on en tire :

$$H^q(\mathfrak{g}, U_L) = H^q(\mathfrak{g}, \bar{L}^*) = H^q(\bar{L}/\bar{K}), \qquad q \geqslant 1.$$

En résumé :

PROPOSITION 4. *Soit* L/K *une extension galoisienne finie non ramifiée, de groupe de Galois* $\mathfrak{g}$. *On a la suite exacte décomposée suivante* :

$$0 \to H^q(L/K) \to H^q(L/K) \to H^q(\mathfrak{g}, \mathbf{Z}) \to 0, \qquad q \geqslant 1.$$

En passant à la limite sur L, on obtient :

COROLLAIRE. *Soit* $\mathfrak{g}$ *le groupe de Galois de* K_{nr}/K. *On a la suite exacte décomposée* :

$$0 \to H^q(\ /K) \to H^q(K_{nr}/K) \to H^q(\mathfrak{g}, \mathbf{Z}) \to 0, \quad q \geqslant 1.$$

(Noter que $\mathfrak{g}$ est aussi le groupe de Galois de $K_{nr}/\bar{K}$, où K_{nr} est la clôture algébrique de K.)

Faisons maintenant $q = 2$. Le groupe $H^2(\ /K)$ n'est autre que le *groupe de Brauer* $B_{\bar{K}}$ de $\bar{K}$; de même, $H^2(K_{nr}/K)$ s'identifie à B_K (cor. au th. 1). Il reste à expliciter $H^2(\mathfrak{g}, \mathbf{Z})$. Or on a la suite exacte :

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0.$$

Comme $\mathbf{Q}$ a une cohomologie triviale, on en déduit un isomorphisme

$$\mathrm{Hom}\,(\mathfrak{g}, \mathbf{Q}/\mathbf{Z}) \to H^2(\mathfrak{g}, \mathbf{Z})$$

d'ailleurs déjà utilisé au Chapitre précédent. Le groupe Hom $(\mathfrak{g}, \mathbf{Q}/\mathbf{Z})$ est bien entendu le groupe des homomorphismes *continus* de $\mathfrak{g}$ (c'est-à-dire ceux dont le noyau est ouvert); nous le noterons $X(\mathfrak{g})$, et nous l'appellerons le *groupe des caractères* de $\mathfrak{g}$ (c'est le dual, au sens de Pontrjagin, du groupe $\mathfrak{g}$ rendu abélien). On obtient donc finalement le résultat suivant, dû à Witt [72] :

THÉORÈME 2. *Soit* K *un corps complet pour une valuation discrète de corps résiduel parfait* $\bar{K}$. *Soit* $\mathfrak{g}$ *le groupe de Galois de la clôture algébrique de* $\bar{K}$ *sur* $\bar{K}$, *et soit* $X(\mathfrak{g})$ *son groupe des caractères. On a la suite exacte décomposée* :

$$0 \to B_{\bar{K}} \to B_K \to X(\mathfrak{g}) \to 0.$$

(La décomposition de cette suite résulte du choix d'une uniformisante π de K, on l'a vu.)

Remarque. L'homomorphisme $B_{\bar{K}} \to B_K$ s'interprète particulièrement bien dans la théorie d'Azumaya-Auslander-Goldman : dans cette théorie, le *groupe de Brauer* B_A *de* A est défini, et le caractère fonctoriel du groupe de Brauer montre que B_A s'envoie à la fois dans $B_{\bar{K}}$ et dans B_K. Comme le premier homomorphisme $B_A \to B_{\bar{K}}$ est un isomorphisme ([10], th. 31, ou [9], th. 6. 5), on en déduit bien un homomorphisme $B_{\bar{K}} \to B_K$ et l'on vérifie qu'il coïncide avec celui du th. 2.

Exercices. 1. Les hypothèses sur K étant celles du th. 2, on suppose en outre que le groupe de Brauer de $\bar{K}$ est nul. Montrer que tout élément de B_K d'ordre n est décomposé par une extension cyclique non ramifiée de K de degré n, et par une seule.

2. Les hypothèses sur K étant celles du th. 2, soit L/K une extension finie, d'indice de ramification égal à e. Démontrer la commutativité du diagramme suivant :

$$\begin{array}{ccccccc} 0 & \longrightarrow & B_{\overline{K}} & \longrightarrow & B_K & \longrightarrow & X(\vartheta_K) \longrightarrow 0 \\ & & \mathrm{Res}\downarrow & & \mathrm{Res}\downarrow & & e.\mathrm{Res}\downarrow \\ 0 & \longrightarrow & B_{\overline{L}} & \longrightarrow & B_L & \longrightarrow & X(\vartheta_L) \longrightarrow 0. \end{array}$$

3. Soit K un corps complet pour une valuation discrète de corps résiduel $\overline{K}$; on ne suppose pas que $\overline{K}$ soit parfait. Soit B'_K le sous-groupe de B_K formé des éléments décomposés par K_{nr}.

a) Montrer que la suite exacte du th. 2 s'applique à B'_K.

b) Soit p la caractéristique de $\overline{K}$. Montrer que tout élément de B_K d'ordre premier à p appartient à B'_K. (Représenter un tel élément par un corps gauche D de centre K, et de rang n^2 sur K; noter que $(n, p) = 1$ d'après l'exer. 3 du Chap. X, § 5; reprendre les raisonnements du § 2, et en déduire que D contient un sous-corps commutatif maximal qui est non ramifié sur K.)

CHAPITRE XIII

CORPS DE CLASSES LOCAL

La théorie usuelle du corps de classes local s'occupe de corps complets K dont le corps résiduel $\mathbf{K}$ est fini. Comme l'a montré Moriya (voir aussi Schilling [54] et Whaples [71]), l'hypothèse de finitude faite sur $\mathbf{K}$ peut être remplacée par une hypothèse plus faible (celle que $\mathbf{K}$ est « quasi-fini », au sens du § 2); c'est dans ce cadre que nous nous plaçons.

Le dernier paragraphe contient un résultat de Dwork [21], utile à la fois pour des calculs explicites de symboles locaux et pour faire le pont avec le point de vue « proalgébrique » de [59].

§ 1. *Le groupe $\hat{\mathbf{Z}}$ et sa cohomologie*

Nous noterons $\hat{\mathbf{Z}}$ le complété du groupe $\mathbf{Z}$ pour la topologie des sous-groupes d'indice fini; c'est un groupe compact totalement discontinu, qui s'identifie à la *limite projective des groupes* $\mathbf{Z}/n\mathbf{Z}$. En décomposant ces groupes en leur composantes p-primaires, on voit que $\hat{\mathbf{Z}}$ est canoniquement isomorphe au produit $\prod \mathbf{Z}_p$ (p par courant l'ensemble des nombres premiers).

Posons $\mathfrak{g} = \hat{\mathbf{Z}}$, et $\mathfrak{g}_n = n\hat{\mathbf{Z}}$; on a $\mathfrak{g} = \varprojlim \mathfrak{g}/\mathfrak{g}_n$, et tout sous-groupe ouvert de $\mathfrak{g}$ coïncide avec l'un des $\mathfrak{g}_n$. Soit A un $\mathfrak{g}$-module topologique au sens du Chap. X, § 3. Le générateur canonique $1 \in \hat{\mathbf{Z}}$ définit un automorphisme F de A; dire que A est un $\mathfrak{g}$-module *topologique* signifie que pour tout $a \in A$, il existe un entier n tel que $F^n a = a$. Le groupe A est donc réunion des sous-groupes $A^{\mathfrak{g}_n}$, et ceux-ci sont des $\mathfrak{g}/\mathfrak{g}_n$-modules. Les groupes de cohomologie de $\mathfrak{g}$ à valeurs dans A sont définis par la formule :

$$(*) \qquad H^q(\mathfrak{g}, A) = \varinjlim H^q(\mathfrak{g}/\mathfrak{g}_n, A^{\mathfrak{g}_n}).$$

On a évidemment $H^0(\mathfrak{g}, A) = A^{\mathfrak{g}}$. Pour H^1, on trouve

PROPOSITION 1. *Soit* A′ *le sous-groupe de* A *formé des* $a \in A$ *tels qu'il existe un entier* n *avec* $(1 + F + \cdots + F^{n-1})a = 0$. *On a* :

$$H^1(g, A) = A'/(F - 1)A.$$

(L'isomorphisme s'obtient en attachant à tout 1-cocycle $\varphi : g \to A$ la classe de $\varphi(1)$ dans $A'/(F - 1)A$.)

Cela résulte, par passage à la limite, de la formule (*) et de la détermination du H^1 d'un groupe cyclique.

COROLLAIRE. *Le groupe dual* $X(g)$ *de* g *s'identifie à* $\mathbf{Q}/\mathbf{Z}$.

En effet, ce groupe n'est autre que $H^1(g, \mathbf{Q}/\mathbf{Z})$, g opérant trivialement sur $\mathbf{Q}/\mathbf{Z}$.

Remarque. Le groupe A′ de la prop. 1 *contient le sous-groupe de torsion* A_f de A. En effet, si $a \in A_f$, on a d'une part $F^m a = a$ pour m assez grand, et $na = 0$ pour n assez grand. On en conclut que

$$(1 + F + \cdots + F^{mn-1})a = nF^m a = 0$$

ce qui montre bien que $a \in A'$.

PROPOSITION 2. *Si* A *est soit un groupe divisible, soit un groupe de torsion, on a* $H^2(g, A) = 0$.

Supposons d'abord A fini. On a $H^2(g/g_n, A^{g_n}) = A^g/N_n A^{g_n}$, avec

$$N_n = 1 + F + \cdots + F^{n-1}.$$

Soit m un entier $\geqslant 1$. On vérifie sans difficultés que l'homomorphisme

$$A^g/N_n A^{g_n} \to A^g/N_{nm} A^{g_{nm}}$$

qui intervient dans le système inductif (*) est induit par la multiplication par m. Si m est multiple de l'ordre de A, cet homomorphisme est donc nul, ce qui prouve bien que $\varinjlim H^2(g/g_n, A^{g_n})$ est nul.

[Variante : soit E un groupe compact totalement discontinu, extension de g par A. En relevant dans E le générateur canonique de g, on définit un homomorphisme section $g \to E$, ce qui montre que l'extension E est triviale. D'où $H^2(g, A) = 0$.]

Si A est de torsion, on a $A = \varinjlim A_\alpha$, où les A_α sont finis et stables par g, d'où $H^2(g, A) = \varinjlim H^2(g, A_\alpha) = 0$.

Supposons enfin A divisible. Si n est un entier $\geqslant 1$, soit ${}_nA$ le noyau de l'homothétie de rapport n dans A. La suite exacte :

$$0 \to {}_nA \to A \xrightarrow{n} A \to 0$$

donne la suite exacte de cohomologie :

$$H^2(g, {}_nA) \to H^2(g, A) \xrightarrow{n} H^2(g, A).$$

D'après ce qui précède, on a $H^2(\mathfrak{g}, {}_nA) = 0$. La multiplication par n est donc injective dans $H^2(\mathfrak{g}, A)$. Comme ce groupe est un groupe de torsion (cf. la formule (*) par exemple), il est donc nul, c.q.f.d.

Exercices. 1. En utilisant le calcul de la cohomologie d'un groupe cyclique (cf. Chap. VIII, § 4), expliciter les homomorphismes :

$$H^q(\mathfrak{g}/\mathfrak{g}_n, A^{\mathfrak{g}_n}) \to H^q(\mathfrak{g}/\mathfrak{g}_{nm}, A^{\mathfrak{g}_{nm}}).$$

Montrer que, si $q = 2h$ ou $q = 2h + 1$, ils sont induits par la multiplication par m^h.

En déduire que $H^q(\mathfrak{g}, A) = 0$ pour $q \geqslant 3$ et pour tout $\mathfrak{g}$-module topologique A.

2. Soit L un groupe libre (non abélien), et soit $\mathfrak{g}$ son complété pour la topologie des sous-groupes d'indice fini.

a) Montrer que, si $\mathfrak{h}$ est un groupe compact totalement discontinu et si $f : \mathfrak{h} \to \mathfrak{g}$ est un homomorphisme continu surjectif, il existe un homomorphisme continu $s : \mathfrak{g} \to \mathfrak{h}$ tel que $f \circ s = 1$.

b) En déduire que $H^2(\mathfrak{g}, A) = 0$ pour tout $\mathfrak{g}$-module topologique A qui est soit de torsion, soit divisible.

[Pour plus de détails sur ces questions, voir [20] et [113].]

§ 2. *Corps quasi-finis*

Soit tout d'abord $\mathfrak{g}$ un groupe compact totalement discontinu quelconque, et soit $s \in \mathfrak{g}$. Il existe alors un homomorphisme continu

$$f_s : \hat{\mathbf{Z}} \to \mathfrak{g}$$

et un seul tel que $f_s(1) = s$. Si l'on note multiplicativement le groupe $\mathfrak{g}$, on écrira s^ν à la place de $f_s(\nu)$, $\nu \in \hat{\mathbf{Z}}$.

Soit k un corps, soit k_s une clôture algébrique de k, et soit $F \in G(k_s/k)$. Nous dirons que F munit k d'une *structure de corps quasi-fini* si les deux conditions suivantes sont vérifiées :

1) *k est parfait.*

2) *L'application $\nu \to F^\nu$ est un isomorphisme de $\hat{\mathbf{Z}}$ sur le groupe $G(k_s/k)$.*

(On exprimera aussi la condition (2) en disant que F est un *générateur libre* de $G(k_s/k)$.)

En d'autres termes, un corps quasi-fini est un corps parfait k tel que $G(k_s/k)$ soit isomorphe à $\hat{\mathbf{Z}}$, l'isomorphisme étant *donné* dans la structure.

Remarque. La définition précédente semble dépendre du choix de la clôture algébrique k_s. En fait, si k'_s est une autre clôture algébrique de k, le groupe $G(k'_s/k)$ est *canoniquement isomorphe* à $G(k_s/k)$, du fait qu'il est abélien; le choix d'un générateur libre F de $G(k_s/k)$ détermine donc automatiquement un générateur libre F' de $G(k'_s/k)$.

La théorie de Galois montre que les seules extensions finies de k contenues dans k_s sont les extensions cycliques k_n formées des éléments invariants par F^n. Inversement, si k est un corps parfait, si pour chaque entier n il existe une sous-extension k_n/k de k_s/k qui est cyclique de degré n, si ces extensions sont emboîtées et ont pour réunion k_s, et si l'on s'est donné pour tout n un générateur F_n de $G(k_n/k)$ de telle sorte que l'image de $F_{nm} \in G(k_{nm}/k)$ dans $G(k_n/k)$ soit F_n, alors k est un corps quasi-fini.

Exemples de corps quasi-finis. a) *Corps finis.* Soit k un corps à q éléments, et soit k_s une clôture algébrique de k. On prend pour F la « substitution de Frobenius » $x \to x^q$; il est bien connu que c'est un générateur libre de $G(k_s/k)$, cf. par exemple Bourbaki, *Alg.*, Chap. V, § 11.

b) Soit C un corps algébriquement clos de caractéristique zéro, et soit $k = C((T))$. Pour tout entier $n \geqslant 1$, $k_n = C((T^{1/n}))$ est une extension cyclique de degré n de k, et la réunion k_s des k_n est une clôture algébrique de k (cf. Chap. IV, prop. 8). Un générateur F_n de $G(k_n/k)$ est défini par $T^{1/n} \to a_n T^{1/n}$, où a_n est une racine primitive n-ième de l'unité. Pour que les F_n définissent un même élément F, il faut choisir les a_n de telle sorte que $(a_{mn})^m = a_n$, ce qui est possible (cf. Bourbaki, *loc. cit*); lorsque $C = \mathbf{C}$, on peut prendre $a_n = \exp(2\pi i/n)$. On voit donc que k est quasi-fini.

Il existe bien d'autres exemples de corps quasi-finis (cf. exer. 3) mais les deux qui précèdent semblent être les seuls « non pathologiques ».

PROPOSITION 3. *Soit k un corps quasi-fini, et soit* F *le générateur libre de son groupe de Galois. Soit k'/k une extension de degré fini n, et soit $F' = F^n$. On a alors $F' \in G(k_s/k')$, et F' munit k' d'une structure de corps quasi-fini.*

C'est clair.

Chaque fois que l'on aura une extension finie d'un corps quasi-fini, on la munira de la structure de corps quasi-fini définie dans la proposition précédente.

PROPOSITION 4. *Soit k un corps quasi-fini, et soit* F *le générateur libre du groupe de Galois* $\mathfrak{g} = G(k_s/k)$.

a) *Si $w \in k_s^*$ est une racine de l'unité, il existe $y \in k_s^*$ tel que $w = y^{F-1}$ (i.e. $w = F(y)/y$).*

b) *Si k est de caractéristique $\neq 0$, l'homomorphisme $F - 1 : k \to k$ est surjectif.*

On a $H^1(\mathfrak{g}, k_s^*) = 0$ (Chap. X, prop. 2); si l'on pose $A = k_s^*$, on a donc $A' = (F - 1)A$, cf. prop. 1; comme w appartient au groupe de torsion de A, on a bien $w \in A'$, d'où a).

On raisonne de même pour b), en tenant compte de ce que $H^1(\mathfrak{g}, k_s)$ est nul (Chap. X, prop. 1).

PROPOSITION 5. *Le groupe de Brauer d'un corps quasi-fini est nul.*

Posons encore $\mathfrak{g} = G(k_s/k)$. Le $\mathfrak{g}$-module k_s^* est divisible (puisque k_s est algébriquement clos). D'après la prop. 2, on a donc $H^2(\mathfrak{g}, k_s^*) = 0$, c.q.f.d.

COROLLAIRE. *Si k' est une extension finie d'un corps quasi-fini k, on a $N(k'^*) = k^*$.*

En effet, puisque cette extension est cyclique, $H^2(k'/k)$ est isomorphe à $k^*/N(k'^*)$, et l'on applique la proposition précédente.

Exercices. 1. Soit k un corps parfait, et soit k_s une clôture algébrique de k. On suppose que, pour chaque entier $n \geqslant 1$, il existe une et une seule sous-extension de k_s qui est de degré n sur k. Montrer que k peut être muni d'une structure de corps quasi-fini.

2. Soit k un corps quasi-fini, et soit F le générateur libre de $G(k_s/k)$ qui soit donné. Pour quelles valeurs de $v \in \hat{\mathbf{Z}}$ l'élément F^v est-il un générateur libre de $G(k_s/k)$?

3. *a*) Soit L/K une extension galoisienne de groupe de Galois isomorphe à $\hat{\mathbf{Z}}$, et soit Ω la clôture algébrique de L. Montrer qu'il existe une extension E de K, contenue dans Ω, et qui est un corps quasi-fini. (Relever dans $G(\Omega/K)$ le générateur canonique de $G(L/K)$.)

b) Montrer que, si K est un corps premier, il existe une extension L/K ayant les propriétés de *a*) (pour $K = \mathbf{Q}$, considérer le corps L' engendré par toutes les racines de l'unité, et montrer que $G(L'/K)$ admet $\hat{\mathbf{Z}}$ comme facteur direct; en déduire la construction du corps L cherché.)

c) Soient L et K comme dans *b*), et soit $\{T_\alpha\}$ une famille d'indéterminées. On pose $L' = L(T_\alpha)$, $K' = K(T_\alpha)$. Montrer que L'/K' est galoisienne et de groupe de Galois $\hat{\mathbf{Z}}$.

d) Déduire de ce qui précède que, pour tout corps algébriquement clos Ω, il existe un sous-corps quasi-fini E de Ω qui admet Ω pour clôture algébrique.

§ 3. *Le groupe de Brauer*

A partir de maintenant, et jusqu'à la fin de ce chapitre, K désigne *un corps complet pour une valuation discrète v dont le corps résiduel* $\mathbf{K}$ *est quasi-fini.* Si K_{nr} désigne l'extension maximale non ramifiée de K, on pose :

$$\mathfrak{g} = G(K_{nr}/K) = G(\mathbf{K}_{nr}/\mathbf{K})$$

et l'on note F le générateur libre de $\mathfrak{g}$ qui définit la structure de corps quasi-fini de $\mathbf{K}$.

D'après le théorème 2 du Chap. XII, on a une suite exacte :

$$0 \to B_{\mathbf{K}} \to B_K \to X(\mathfrak{g}) \to 0$$

$X(\mathfrak{g})$ désignant le groupe des caractères de $\mathfrak{g}$. D'après le corollaire à la prop. 1, $X(\mathfrak{g})$ s'identifie à $\mathbf{Q}/\mathbf{Z}$. On obtient donc ainsi un homomorphisme $B_K \to \mathbf{Q}/\mathbf{Z}$ que nous noterons inv_K.

PROPOSITION 6. *L'homomorphisme* $\mathrm{inv}_K : B_K \to \mathbf{Q}/\mathbf{Z}$ *est un isomorphisme.*

Cela résulte de la suite exacte écrite ci-dessus et du fait que $B_{\mathbf{K}} = 0$ (prop. 5).

Il est nécessaire pour la suite de bien préciser la définition de inv_K. Considérons les isomorphismes suivants :

$$B_K \xleftarrow{\alpha} H^2(\mathfrak{g}, K_{nr}^*) \xrightarrow{\beta} H^2(\mathfrak{g}, \mathbf{Z}) \xleftarrow{\delta} H^1(\mathfrak{g}, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\gamma} \mathbf{Q}/\mathbf{Z},$$

où α est l'injection canonique de $H^2(K_{nr}/K)$ dans B_K, où β est induit par $v : K_{nr}^* \to \mathbf{Z}$, où δ est le cobord dans la suite exacte $0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0$, et où enfin γ fait correspondre à tout caractère χ de $\mathfrak{g}$ l'élément $\chi(F) \in \mathbf{Q}/\mathbf{Z}$. Par construction même, on a :

$$\mathrm{inv}_K = \gamma \circ \delta^{-1} \circ \beta \circ \alpha^{-1}.$$

PROPOSITION 7. *Soit* L *une extension de* K, *de degré fini* n, *et soit* $\mathrm{Res}_{K/L} : B_K \to B_L$ *l'homomorphisme canonique de* B_K *dans* B_L (cf. Chap. X, § 4, ainsi que Chap. XI, §§ 1, 2). *On a* :

$$\mathrm{inv}_L \circ \mathrm{Res}_{K/L} = n.\mathrm{inv}_K.$$

En d'autres termes, le diagramme :

$$\begin{array}{ccc} B_K & \longrightarrow & \mathbf{Q}/\mathbf{Z} \\ \downarrow & & \downarrow n \\ B_L & \longrightarrow & \mathbf{Q}/\mathbf{Z} \end{array}$$

est commutatif.

Démonstration. Commençons par deux cas particuliers :

a) L/K *est non ramifiée.*

On peut supposer que L est contenue dans K_{nr}; on a alors $K_{nr} = L_{nr}$; posons $\mathfrak{g}_n = G(K_{nr}/L) = G(K_{nr}/\overline{L})$: c'est l'unique sous-groupe de $\mathfrak{g}$ d'indice n.

Considérons le diagramme :

$$\begin{array}{ccccccccc} B_K & \xleftarrow{\alpha} & H^2(\mathfrak{g}, K_{nr}^*) & \xrightarrow{\beta} & H^2(\mathfrak{g}, \mathbf{Z}) & \xleftarrow{\delta} & H^1(\mathfrak{g}, \mathbf{Q}/\mathbf{Z}) & \xrightarrow{\gamma} & \mathbf{Q}/\mathbf{Z} \\ \mathrm{Res}\downarrow & & \mathrm{Res}\downarrow & & \mathrm{Res}\downarrow & & \mathrm{Res}\downarrow & & n\downarrow \\ B_L & \xleftarrow{\alpha'} & H^2(\mathfrak{g}_n, K_{nr}^*) & \xrightarrow{\beta'} & H^2(\mathfrak{g}_n, \mathbf{Z}) & \xleftarrow{\delta'} & H^1(\mathfrak{g}_n, \mathbf{Q}/\mathbf{Z}) & \xrightarrow{\gamma'} & \mathbf{Q}/\mathbf{Z} \end{array}$$

où tous les homomorphismes verticaux sont des homomorphismes de restriction, à l'exception de celui situé à l'extrême droite qui est la multiplication par n. Tout revient à montrer que ce diagramme est commutatif. La commutativité des carrés ne faisant intervenir que des « Res » est évidente; reste le dernier carré :

$$\begin{array}{ccc} H^1(\mathfrak{g}, \mathbf{Q}/\mathbf{Z}) & \xrightarrow{\gamma} & \mathbf{Q}/\mathbf{Z} \\ \mathrm{Res}\downarrow & & n\downarrow \\ H^1(\mathfrak{g}_n, \mathbf{Q}/\mathbf{Z}) & \xrightarrow{\gamma'} & \mathbf{Q}/\mathbf{Z}. \end{array}$$

Si $\chi \in H^1(\mathfrak{g}, \mathbf{Q}/\mathbf{Z})$, on a $\gamma(\chi) = \chi(F)$. D'autre part Res (χ) est simplement la restriction de χ au sous-groupe $\mathfrak{g}_n$ de $\mathfrak{g}$, et le générateur canonique de $\mathfrak{g}_n$ est F^n (cf. § 2). On a donc

$$\gamma'(\mathrm{Res}\ (\chi)) = \chi(F^n) = n\chi(F)$$

d'où la commutativité cherchée.

b) L/K *est totalement ramifiée* (*i.e.* $\mathbf{L} = \mathbf{K}$).

L'extension K_{nr}/K est alors linéairement disjointe de L/K, et $L_{nr} = K_{nr}L$. Le groupe $\mathfrak{g}$ est le même pour K et pour L. Considérons le diagramme :

$$\begin{array}{ccccccccc} B_K & \xleftarrow{\alpha} & H^2(\mathfrak{g}, K_{nr}^*) & \xrightarrow{\beta} & H^2(\mathfrak{g}, Z) & \xleftarrow{\delta} & H^1(\mathfrak{g}, \mathbf{Q}/Z) & \xrightarrow{\gamma} & \mathbf{Q}/Z \\ \mathrm{Res}\downarrow & & i\downarrow & & n\downarrow & & n\downarrow & & n\downarrow \\ B_L & \xleftarrow{\alpha'} & H^2(\mathfrak{g}, L_{nr}^*) & \xrightarrow{\beta'} & H^2(\mathfrak{g}, Z) & \xleftarrow{\delta'} & H^1(\mathfrak{g}, \mathbf{Q}/Z) & \xrightarrow{\gamma'} & \mathbf{Q}/Z, \end{array}$$

où i est induit par l'injection de K_{nr}^* dans L_{nr}^*. La commutativité du premier carré est évidente; celle du second résulte de ce que la valuation w de L_{nr} prolonge la valuation v de K_{nr} avec l'indice de ramification $e = n$; celle des autres carrés est triviale. La proposition en résulte dans ce cas.

Dans le cas général, L est extension totalement ramifiée d'un corps intermédiaire K′ qui est non ramifié sur K (cf. Chap. III, § 5, cor. 3 au th. 3), et l'on est ainsi ramené aux deux cas précédents, c.q.f.d.

COROLLAIRE 1. *Les hypothèses et notations étant celles de la proposition* 7, *pour qu'un élément* $a \in B_K$ *soit décomposé par* L, *il faut et il suffit que l'on ait* $na = 0$.

En effet, dire que a est décomposé par L signifie que $\mathrm{Res}_{K/L}(a) = 0$, c'est-à-dire que $\mathrm{inv}_L \circ \mathrm{Res}_{K/L}(a) = 0$, ou encore $\mathrm{inv}_K(na) = 0$, autrement dit $na = 0$.

COROLLAIRE 2. *Supposons* L/K *galoisienne. L'homomorphisme* $\mathrm{inv}_K : B_K \to \mathbf{Q}/Z$ *applique le sous-groupe* $H^2(L/K)$ *de* B_K *isomorphiquement sur le sous-groupe* $\frac{1}{n}Z/Z$ *de* $\mathbf{Q}/Z$. C'est clair.

COROLLAIRE 3. *Soit* D *un corps gauche de centre* K *et de rang* n^2 *sur* K. *Soit* $a \in B_K$ *l'élément correspondant du groupe de Brauer de* K. *Alors* a *est d'ordre* n *dans* B_K, *et toute extension de degré* n *de* K *peut être plongée dans* D.

Tout sous-corps commutatif maximal de D décompose D; d'après le cor. 1, on a donc $na = 0$ (c'est d'ailleurs là un fait général, cf. Chap. X, § 5, exer. 3). Si d est l'ordre de a, on a $d|n$. Le cor. 1 montre que D est décomposé par une extension L/K de degré d (par exemple, une extension non ramifiée), et la classe de D contient une algèbre centrale simple de rang d^2 (cf. Bourbaki, *Alg.*, Chap. VIII, § 10, prop. 7). Comme D est un corps, ceci entraîne $n|d$, d'où $n = d$. Enfin, si K′/K est une extension de degré n, le cor. 1 montre que K′ est corps neutralisant de D, donc est isomorphe à un sous-corps commutatif maximal de D, cf. Bourbaki, *loc. cit.*

Remarque. Le corollaire précédent montre que $\mathrm{inv}_K(a) = m/n$, avec $(m, n) = 1$. On en conclut qu'il existe $\varphi(n)$ corps gauches de centre K et de rang n^2 sur K (à isomorphisme près, bien entendu).

Exercices. 1. Soit K un corps vérifiant les hypothèses du §, soit D un corps gauche de centre K et de rang n^2 sur K, et soit Nrd : $D^* \to K^*$ la norme réduite.

a) Les notations étant celles de l'exer. 3 du Chap. XII, § 2, montrer que l'on a $e = n, f = 1$.

b) En déduire que si π est une uniformisante de D, $\mathrm{Nrd}(\pi)$ est une uniformisante de K.

c) Montrer que toute unité de K est norme réduite d'une unité de D. (Utiliser le fait que D contient une extension non ramifiée de degré n, et appliquer le cor. à la prop. 3 du Chap. V.)

d) Montrer que $\mathrm{Nrd}(D^*) = K^*$.

2. Soit K un corps complet pour une valuation discrète à corps résiduel $\overline{K}$ parfait. On suppose que, pour toute extension séparable finie E de K, on s'est donné un isomorphisme

$$i_E : B_E \to \mathbf{Q}/\mathbf{Z}$$

tel que $i_{E'} \circ \mathrm{Res}_{E/E'} = [E' : E] i_E$ si $E' \supset E$. Montrer qu'il existe sur $\overline{K}$ une structure de corps quasi-fini et une seule telle que l'isomorphisme $\mathrm{inv}_E : B_E \to \mathbf{Q}/\mathbf{Z}$ correspondant soit l'isomorphisme donné i_E. (Utiliser le th. 2 et l'exer. 2 du Chap. XII, § 3; montrer que $B_{\overline{E}} = 0$, puis que $\mathfrak{g}_E$ est abélien.)

[En d'autres termes, l'hypothèse que le corps résiduel $\overline{K}$ est quasi-fini est *nécessaire et suffisante* pour la validité de la théorie du corps de classes local.]

§ 4. *La formation de classes*

Nous conservons les hypothèses du § 3 : K désigne un corps complet pour une valuation discrète v, et de corps résiduel $\overline{K}$ quasi-fini. Nous allons associer à K une *formation de classes*, au sens d'Artin-Tate (cf. Chap. XI).

Choisissons d'abord une clôture séparable K_s de K, et soit X l'ensemble des sous-extensions de K_s qui sont finies sur K. Soit $G = G(K_s/K)$, et, pour tout $E \in X$, soit $G_E = G(K_s/E)$ le sous-groupe de G correspondant à E. Le groupe G opère sur K_s^*, et l'on obtient ainsi une *formation* au sens du Chap. XI, § 1. De plus, si E appartient à X, le corps résiduel $\overline{E}$ de E est une extension finie de $\overline{K}$ et se trouve canoniquement muni d'une structure de corps quasi-fini, cf. § 2. On en déduit, comme on l'a vu au § 3, un isomorphisme

$$\mathrm{inv}_E : H^2(\ \ /E) \to \mathbf{Q}/\mathbf{Z}$$

puisque $H^2(\ \ /E) = B_E$, groupe de Brauer de E.

Théorème 1. *La formation précédente, et la donnée des* inv_E, *constituent une formation de classes* (cf. Chap. XI, § 2).

On doit vérifier les axiomes suivants :

I. *Pour toute extension galoisienne* F/E, *on a* $H^1(F/E) = 0$.

C'est la prop. 2 du Chap. X (« théorème 90 »).

II a) *L'homomorphisme* inv_E *est injectif. Si* F/E *est galoisienne,* inv_E *applique* $H^2(F/E)$ *sur l'unique sous-groupe de* $\mathbf{Q}/\mathbf{Z}$ *d'ordre égal à* $[F : E]$.

C'est le cor. 2 à la prop. 7.

II b) *Si* E'/E *est une extension quelconque, on a*

$$\mathrm{inv}_{E'} \circ \mathrm{Res}_{E/E'} = [E' : E].\mathrm{inv}_E.$$

C'est la proposition 7.

Puisque l'on a une formation de classes, on peut lui appliquer les résultats du Chap. XI. Nous allons reproduire les plus importants.

Soit d'abord F/E une extension galoisienne (avec $E, F \in X$, comme toujours); nous noterons $G_{F/E}$ son groupe de Galois. D'après II a), il existe un élément

$$u_{F/E} \in H^2(F/E)$$

et un seul tel que $\mathrm{inv}_E(u_{F/E}) = 1/n$, avec $n = [F : E]$. On l'appelle *la classe fondamentale* de l'extension F/E.

PROPOSITION 8. *Pour tout* $n \in \mathbf{Z}$, *le cup-produit par* $u_{F/E}$ *définit un isomorphisme* :

$$\hat{H}^n(G_{F/E}, \mathbf{Z}) \to \hat{H}^{n+2}(G_{F/E}, F^*).$$

C'est le théorème de Tate (th. 1 du Chap. XI).

Pour $n = -2$, on a $\hat{H}^{-2}(G_{F/E}, \mathbf{Z}) = G^a_{F/E}$ (i.e. le groupe $G_{F/E}$ rendu abélien). Donc :

COROLLAIRE. *Le cup-produit par* $u_{F/E}$ *définit un isomorphisme*

$$\theta_{F/E} : G^a_{F/E} \to E^*/NF^* \quad (N \textit{ désignant la norme dans } F/E).$$

En particulier, on a $(E^* : NF^*) = [F : E]$ *si* F/E *est une extension abélienne.*

Réciproquement (cf. Chap. XI, cor. à la prop. 3) :

PROPOSITION 9. *Si* F/E *est une extension finie séparable,* NF^* *est d'indice fini dans* E^*; *cet indice divise* $[F : E]$ *et lui est égal si et seulement si* F/E *est abélienne.*

Revenons maintenant à l'isomorphisme

$$\theta_{F/E} : G^a_{F/E} \to E^*/NF^*$$

du corollaire à la prop. 8. L'isomorphisme réciproque $\omega = \theta^{-1}_{F/E}$ s'appelle *l'isomorphisme de réciprocité.* Si $x \in E^*$ a pour image $\bar{x}$ dans E^*/NF^*, on pose :

$$(x, F/E) = \omega(\bar{x}), \qquad \text{c'est un élément de } G^a_{F/E}.$$

En particulier, si F/E est abélienne (cas auquel on peut toujours se ramener), $(x, F/E)$ est un élément de $G_{F/E}$. On a :

$$(xx', F/E) = (x, F/E).(x', F/E)$$
$$(x, F/E) = 1 \qquad \text{si et seulement si } x \in NF^*.$$

Tout $s \in G^a_{F/E}$ est de la forme $(x, F/E)$, avec $x \in E^*$.

[On dit parfois, à cause de la deuxième propriété, que $(x, F/E)$ est le *symbole de reste normique* de x dans F/E.]

Les propriétés fonctorielles de l'isomorphisme de réciprocité sont données par les trois propositions suivantes, démontrées au Chap. XI, § 3 :

PROPOSITION 10. *Considérons une extension* $F \supset E' \supset E$, *avec* F/E *galoisienne. Le groupe* $G_{F/E'}$ *est un sous-groupe de* $G_{F/E}$.

a) *Si* $x \in E'^*$, *et si* $y = N_{E'/E}(x)$, *l'image de* $(x, F/E') \in G^a_{F/E'}$ *dans* $G^a_{F/E}$ *est égale à* $(y, F/E)$.

b) *Si* $x \in E^*$, *l'image de* $(x, F/E) \in G^a_{F/E}$ *dans* $G^a_{F/E'}$ *par le transfert est égale à* $(x, F/E')$.

PROPOSITION 11. *Si* F/E *est une extension galoisienne, et si* $s \in G$, *on a*

$$(sx, sF/sE) = s \circ (x, F/E) \circ s^{-1} \qquad \textit{pour tout } x \in E^*.$$

PROPOSITION 12. *Considérons une extension* $F' \supset F \supset E$, *avec* F/E *et* F'/E *galoisiennes. Si* $x \in E^*$, *l'image de* $(x, F'/E)$ *dans* $G^a_{F/E}$ *est égale à* $(x, F/E)$.

Cette dernière proposition permet de définir $(x, F/E)$ lorsque F/E est une extension galoisienne quelconque (non nécessairement finie); elle montre aussi qu'on peut se borner aux extensions *abéliennes*. Lorsque F est *l'extension abélienne maximale* E^a de E, on écrit $(x, */E)$ au lieu de $(x, E^a/E)$. C'est un élément du groupe de Galois $\mathfrak{A}_E = G(E^a/E)$. L'application de réciprocité permet *d'identifier* $\mathfrak{A}_E$ *au complété-séparé de* E^* *pour la topologie définie par les groupes de normes*, cf. Chap. XI, § 4. Nous déterminerons cette topologie au Chapitre suivant, dans le cas particulier où K est fini.

Le calcul explicite de $(x, F/E)$ est facile dans le cas non ramifié :

PROPOSITION 13. *Soit* L/K *une extension non ramifiée. Si l'on identifie les groupes* $G_{L/K}$ *et* $G_{L/\bar{K}}$, *on a* :

$$(x, L/K) = F_K^{v(x)},$$

où F_K *désigne le générateur canonique de* $G_{L/\bar{K}}$, *et où* v *est la valuation de* K.

Posons, pour simplifier, $\mathfrak{g} = G_{L/K}$ et $F = F_K$. Soit χ un caractère de $\mathfrak{g}$. On doit vérifier que :

$$\chi((x, L/K)) = \chi(F^{v(x)}).$$

D'après la proposition 2 du Chap. XI, le membre de gauche est égal à $\mathrm{inv}_K(x . \delta\chi)$. Quant à l'homomorphisme inv_K, il a été défini au § 3 comme le composé :

$$H^2(\mathfrak{g}, L^*) \xrightarrow{\beta} H^2(\mathfrak{g}, Z) \xrightarrow{\delta^{-1}} H^1(\mathfrak{g}, Q/Z) \xrightarrow{\gamma} Q/Z.$$

Il est clair que l'image de $x . \delta\chi$ dans $H^2(\mathfrak{g}, Z)$ est égale à $v(x) . \delta\chi$: son image dans $H^1(\mathfrak{g}, Q/Z)$ est donc $v(x) . \chi$, et son image dans Q/Z est $v(x)\chi(F) = \chi(F^{v(x)})$, c.q.f.d.

COROLLAIRE. *Soit* F/E *une extension abélienne, de groupe de Galois* G. *Soit* $U_E \subset E^*$ *le groupe des unités de* E. *L'application de réciprocité* $E^* \to G$ *applique* U_E *sur le sous-groupe d'inertie de* G.

Soit T le sous-groupe d'inertie de G, et soit E′ la sous-extension de F correspondant à T. L'extension E′/E est non ramifiée; en lui appliquant la proposition précédente, on en déduit que U_E s'applique trivialement dans G/T, donc l'image de U_E est contenue dans T. Inversement, soit $t \in T$, et soit $a \in E^*$ tel que $(a, F/E) = t$. Posons $f = [E' : E]$. Comme $(a, F/E)$ est trivial sur E′, la proposition précédente montre que f divise $v(a)$. Il existe donc $b \in F^*$ tel que $N(b)$ et a aient même valuation. Si l'on pose $u = a.N(b)^{-1}$, on a $u \in U_E$, et $(u, F/E) = (a, F/E) = t$, ce qui montre bien que U_E s'applique sur T, c.q.f.d.

Remarque. On a un résultat analogue pour la ramification supérieure : l'application de réciprocité $E^* \to G$ applique les U_E^n sur les groupes de ramification G^n (en numérotation supérieure); cf. Chap. XV, § 2.

La proposition 13 s'énonce de façon plus agréable en « passant à la limite ». Soit $\mathfrak{A}_K$ le groupe de Galois de l'extension abélienne maximale K^a de K; si K_{nr} est l'extension maximale non ramifiée de K, on a $K_{nr} \subset K^a$, d'où la suite exacte :

$$0 \to \mathfrak{T}_K \to \mathfrak{A}_K \to \hat{\mathbf{Z}} \to 0$$

où $\mathfrak{T}_K$ est le *groupe d'inertie de* K^a/K (défini par passage à la limite à partir du cas fini).

On a d'autre part la suite exacte

$$0 \to U_K \to K^* \to \mathbf{Z} \to 0.$$

La proposition 13 s'exprime alors sous forme de diagramme commutatif :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_K & \longrightarrow & K^* & \longrightarrow & \mathbf{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \omega_T} & & \downarrow{\scriptstyle \omega} & & \downarrow{\scriptstyle i} & & \\ 0 & \longrightarrow & \mathfrak{T}_K & \longrightarrow & \mathfrak{A}_K & \longrightarrow & \hat{\mathbf{Z}} & \longrightarrow & 0 \end{array}$$

où ω est l'application de réciprocité $x \to (x, */K)$, et où i est l'injection canonique de $\mathbf{Z}$ dans $\hat{\mathbf{Z}}$. Quant à ω_T, elle permet d'identifier $\mathfrak{T}_K$ au complété de U_K pour la topologie induite par les groupes de normes; nous verrons au Chap. XIV que c'est un isomorphisme dans le cas classique (c'est-à-dire quand $\mathbf{K}$ est fini).

Exercice. Soit E′/E une extension finie (non nécessairement séparable), soit F/E une extension galoisienne, et soit F′ = E′F. On identifie le groupe de Galois $G_{F'/E'}$ à un sous-groupe du groupe $G_{F/E}$.

a) Soit $y \in E'^*$ et soit $x = N_{E'/F}(y)$. Montrer que $(x, F/E) \in G^a_{F/E}$ est l'image canonique de $(y, F'/E') \in G^a_{F'/E'}$.

b) Posons $d = [F' : F] = [E' : F \cap E']$. Soit $x \in E^*$. Montrer que $(x, F'/E')$ est la puissance d-ième du transfert de $(x, F/E)$ dans $G^a_{F'/E'}$.

(Traiter séparément le cas où E′/E est radiciel, et celui où il est séparable; raisonner directement dans le premier cas; dans le deuxième, appliquer les prop. 10 et 12 à une extension galoisienne de E contenant F′.)

c) On suppose que F/E est abélienne. Montrer que, pour qu'un élément $y \in E'^*$ appartienne à $N_{F'/E'}(F'^*)$, il faut et il suffit que $N_{F'/E}(y)$ appartienne à $N_{F/E}(F^*)$.

§ 5. *Le théorème de Dwork*

Dans tout ce §, L/K désigne une extension totalement ramifiée, galoisienne de groupe de Galois G. Si K_{nr} est l'extension maximale non ramifiée de K, et si l'on pose $L_{nr} = LK_{nr}$, on sait que L_{nr}/K_{nr} est galoisienne de groupe de Galois G; il en est de même de l'extension des complétés $\hat{L}_{nr}/\hat{K}_{nr}$. On notera v (resp. w) la valuation discrète de $\hat{K}_{nr}$ (resp. $\hat{L}_{nr}$). On utilisera la notation exponentielle x^s pour désigner $s(x)$, $s \in G$, $x \in \hat{L}_{nr}^*$.

Commençons par un résultat général (qui vaut sans supposer que K soit quasi-fini) :

PROPOSITION 14. *On a* $\hat{H}^q(G, \hat{L}_{nr}^*) = 0$ *pour tout* $q \in \mathbf{Z}$.

Cela résulte de la prop. 11 du Chap. X combinée avec la prop. 7 du Chap. V.

COROLLAIRE 1. *La suite exacte* $0 \to \hat{U}_{nr} \to \hat{L}_{nr}^* \to \mathbf{Z} \to 0$ *définit un isomorphisme de* $G^a = \hat{H}^{-2}(G, \mathbf{Z})$ *sur* $\hat{H}^{-1}(G, \hat{U}_{nr})$.

C'est évident.

(On notera que cet isomorphisme fait correspondre à un élément $s \in G$ la classe de π^{s-1} dans $\hat{H}^{-1}(G, \hat{U}_{nr})$, π étant une uniformisante de $\hat{L}_{nr}$.)

COROLLAIRE 2. *Soient* $s_i \in G$ *et* $z_i \in \hat{L}_{nr}^*$ *des éléments tels que* :

$$\prod z_i^{s_i - 1} = 1.$$

On a alors $\prod s_i^{w(z_i)} = 1$ *dans* G^a.

Soit π une uniformisante de $\hat{L}_{nr}$. On a $z_i = u_i \pi^{n_i}$, avec $n_i = w(z_i)$. On en déduit :

$$\pi^{\sum n_i (s_i - 1)} \prod z_i^{s_i - 1} = 1.$$

Soit I l'idéal d'augmentation de $\mathbf{Z}[G]$. Si l'on pose $s = \prod s_i^{n_i}$, on a

$$s - 1 \equiv \sum n_i (s_i - 1) \bmod \mathrm{I}^2, \qquad \text{et} \qquad \pi^{s-1} \in \hat{U}_{nr}^{\mathrm{I}}.$$

La formule ci-dessus signifie donc que l'image de π^{s-1} dans $\hat{H}^{-1}(G, \hat{U}_{nr})$ est nulle, et d'après le corollaire précédent, cela entraîne que l'image de s dans G^a est triviale.

Revenons maintenant au cas où K est quasi-fini. Posons

$$\mathfrak{g} = G(K_{nr}/K) = G(L_{nr}/L)$$

et soit F le générateur canonique de $\mathfrak{g}$. Les éléments de $\mathfrak{g}$, et en particulier F, se prolongent par continuité en des automorphismes de $\hat{L}_{nr}$ et $\hat{K}_{nr}$ qui commutent aux éléments de G. [Noter toutefois que les $\mathfrak{g}$-modules $\hat{L}_{nr}^*$ et $\hat{K}_{nr}^*$ *ne sont pas des* $\mathfrak{g}$*-modules topologiques*.]

LEMME 1. *Pour qu'un élément x de $\hat{L}_{nr}$ (resp. de $\hat{K}_{nr}$) appartienne à L (resp. à K), il faut et il suffit que $Fx = x$.*

La nécessité est évidente. Démontrons la suffisance dans le cas de L (celui de K se traite de même). Soit $x \in \hat{L}_{nr}$ tel que $Fx = x$, et soit π une uniformisante de L. On peut écrire $x = \pi^n u$, avec $w(u) = 0$, et l'on a $Fu = u$; on est ainsi ramené au cas où x est une unité. Si $\bar{x} \in \bar{L}_{nr}$ désigne l'image de x dans le corps résiduel de $\hat{L}_{nr}$, on a $F\bar{x} = \bar{x}$, d'où $\bar{x} \in \bar{L}$, et il existe $a_0 \in U_L$ tel que $\bar{a}_0 = \bar{x}$. On peut donc écrire $x = a_0 + \pi x_1$, avec $w(x_1) \geqslant 0$, et $Fx_1 = x_1$. En appliquant à x_1 le raisonnement précédent, et en itérant, on en déduit un développement en série pour x

$$x = a_0 + \pi a_1 + \cdots + \pi^n a_n + \cdots, \qquad a_i \in L, \quad w(a_i) \geqslant 0,$$

et comme L est complet, ceci montre bien que x appartient à L.

Dans l'énoncé ci-dessous, on note N la norme dans l'extension $\hat{L}_{nr}/\hat{K}_{nr}$; elle prolonge évidemment $N_{L/K}$.

THÉORÈME 2 (Dwork). *Soit L/K une extension totalement ramifiée, de groupe de Galois abélien G. On suppose que le corps résiduel $\mathbf{K} = \bar{L}$ est quasi-fini. Soit $x \in K^*$; soit $y \in \hat{L}_{nr}^*$ tel que $Ny = x$; soient $z_i \in \hat{L}_{nr}^*$, $s_i \in G$ tels que*

$$y^{F-1} = \prod z_i^{s_i} t^{-1}.$$

Posons $s = \prod s_i^{w(z_i)}$. On a alors $(x, L/K) = s^{-1}$.

[Si x est donné, on peut toujours choisir y tel que $Ny = x$, puisque $N(\hat{L}_{nr}^*) = \hat{K}_{nr}^*$ (on pourrait même prendre y dans L_{nr}^*, si l'on y tenait). On a alors $N(y^{F-1}) = x^{F-1}$; d'après la prop. 14, il existe donc des z_i et des s_i tels que $y^{F-1} = \prod z_i^{s_i} t^{-1}$, et d'après le cor. 2 à la prop. 14, l'élément $s = \prod s_i^{w(z_i)}$ ne dépend pas du choix des z_i et des s_i. Le théorème 2 fournit donc *un procédé de calcul* pour $(x, L/K)$.]

Posons $y = y_0 y'$, avec $y_0 \in L^*$, et y' unité de $\hat{L}_{nr}$. On a $x = x_0 x'$, avec $x_0 = Ny_0$, $x' = Ny'$, d'où

$$(x, L/K) = (x', L/K).$$

D'autre part, on a $y'^{F-1} = y^{F-1} = \prod z_i^{s_i} t^{-1}$. Il suffit donc de démontrer le théorème pour x' et y'; en d'autres termes, *on peut supposer que x et y sont des unités.*

Le groupe de Galois de $L_{nr} = L \otimes_K K_{nr}$ sur K s'identifie au produit direct $G \times \mathfrak{g}$; les éléments de ce groupe opèrent sur $\hat{L}_{nr}$ (prolongement par continuité). Posons

$$t = (x, L/K)$$

et considérons le sous-corps L' de L_{nr} invariant par $t.F = t \otimes F$. Comme le sous-groupe fermé $\mathfrak{g}'$ de $G \times \mathfrak{g}$ engendré par $t.F$ est un supplémentaire de G, la théorie de Galois montre que l'extension L'/K est linéairement disjointe de K_{nr}/K, et que $L'K_{nr} = L_{nr}$. En particulier $N_{L'/K}$ n'est autre que la restriction de N à L'.

Soit π une uniformisante de L, et soit $\pi_K = N\pi$; c'est une uniformisante de K. On a :

$$t.F = (x\pi_K, L_{nr}/K).$$

En effet, $(x, L_{nr}/K)$ est égal à t sur L/K, et à l'identité sur K_{nr}/K puisque x est une unité; d'autre part, $(\pi_K, L_{nr}/K)$ est l'identité sur L/K puisque π_K est une norme, et c'est F sur K_{nr}/K d'après la prop. 13.

Comme $t.F$ est trivial sur L', il existe $z \in L'^*$ tel que $Nz = x\pi_K$. On a donc

$$Nz = N(y\pi), \text{ i.e. } N(z^{-1}y\pi) = 1.$$

Appliquant la prop. 14 avec $q = -1$, on voit qu'il existe des $b_j \in \hat{L}_{nr}^*$ et des $s_j \in G$ tels que

$$z^{-1}y\pi = \prod b_j^{s_j - 1}.$$

Écrivons maintenant que $z^{F-1} = 1$. On a $\pi^{F-1} = \pi^{f-1}$, et

$$y^{F-1} = y^{-1}(y.\prod z_i^{s_i-1})^f = y^{f-1}\prod z_i^{(s_i-1)}.$$

On en déduit

$$y^{f-1}\pi^{f-1}\prod z_i^{(s_i-1)} = \prod b_j^{((F-1)(s_j-1)}.$$

En appliquant le cor. 2 à la prop. 14 à cette identité, et en tenant compte de ce que $w(y) = 0$, $w(\pi) = 1$, $w(z_i') = w(z_i)$, $w(b_j^{F-1}) = 0$, on trouve $t.s. = 1$, c.q.f.d.

COROLLAIRE. *Soient* $x \in K^*$, $y \in \hat{L}_{nr}^*$, $s \in G$ *tels que*

$$x = Ny, \qquad y^{F-1} = \pi^{s-1}, \qquad \pi \textit{ étant une uniformisante de } \hat{L}_{nr}.$$

Alors $(x, L/K) = s^{-1}$.

C'est évident.

Lorsque K est de caractéristique $p > 0$, ce qui est de beaucoup le cas le plus intéressant, le corollaire ci-dessus suffit à déterminer l'isomorphisme de réciprocité. En effet, on a tout d'abord :

PROPOSITION 15. *Supposons que* K *soit de caractéristique non nulle, et soit* V *le groupe des unités de* $\hat{L}_{nr}$. *Pour tout entier* $m \geqslant 1$, *l'homomorphisme* $x \to x^{F-1}$ *applique* $V^{(m)}$ *sur* $V^{(m)}$. *Si* x *est un élément de* V *tel que* $\bar{x} \in K_{nr}^*$ *soit une racine de l'unité, il existe* $y \in V$ *tel que* $x = y^{F-1}$.

(On a noté $V^{(m)}$ l'ensemble des $x \in V$ tels que $w(x - 1) \geqslant m$.)

Le groupe $V^{(m)}$ est séparé et complet pour la filtration des $V^{(m+k)}$ et les quotients $V^{(m+k)}/V^{(m+k+1)}$ s'identifient au groupe additif K_{nr}. Comme $F - 1 : K_{nr} \to K_{nr}$ est surjectif (prop. 4), le lemme 2 du Chap. V montre que $F - 1 : V^{(m)} \to V^{(m)}$ l'est aussi. Si en outre $x \in V$ est tel que $\bar{x}$ soit une racine de l'unité, la prop. 4, *a*) montre l'existence d'un $z \in V$ tel que $\bar{z}^{F-1} = \bar{x}$, d'où $x = z^{F-1}x'$, avec $x' \in V^{(1)}$; d'après ce qui précède on a $x' = y'^{F-1}$, c.q.f.d.

COROLLAIRE. *Si* K *est un corps fini, on a* $V = V^{F-1}$.

(Si l'on utilisait la structure proalgébrique de V, cela résulterait aussi d'un théorème général de Lang [39] sur les groupes algébriques.)

Revenons maintenant à la situation du théorème 1, en supposant toujours que $\mathbf{K}$ est de caractéristique non nulle. Soit $s \in G$ et soit π une uniformisante de $\hat{L}_{nr}$. Formons π^{s-1}; c'est un élément de V, et son image dans K_{nr}^* est une racine de l'unité (cf. Chap. IV, § 2). D'après la proposition 15, il existe donc $y \in V$ tel que $y^{F-1} = \pi^{s-1}$. Prenons la norme des deux membres, et posons $x = Ny$; on trouve $x^{F-1} = 1$, d'où $x \in K^*$ (lemme 1). On est donc dans les conditions d'application du corollaire, et l'on voit que $(x, L/K) = s^{-1}$. Ainsi, *le corollaire suffit bien à déterminer l'application de réciprocité.*

Exercices. 1. Soit V le groupe des unités de $\hat{L}_{nr}$; montrer que V/V^{F-1} est un groupe divisible sans torsion; en déduire que c'est un G-module cohomologiquement trivial.

2. Soit L/K une extension galoisienne finie, de groupe de Galois G, non nécessairement totalement ramifiée. On définit L_{nr} comme le produit tensoriel $K_{nr} \otimes_K L$, et de même pour $\hat{L}_{nr}$. Ce sont des produits de corps. On fait opérer G et F de façon évidente sur L_{nr} et $\hat{L}_{nr}$.

a) Soit $\hat{L}_{nr}^*$ le groupe multiplicatif des éléments inversibles de $\hat{L}_{nr}$, soit $w : \hat{L}_{nr}^* \to \mathbf{Z}$ la somme des valuations discrètes des différents composants de $\hat{L}_{nr}$, et soit $V = \mathrm{Ker}(w)$. Soit V' l'ensemble des y^{F-1}, $y \in \hat{L}_{nr}^*$. On a $V' \subset V$, et l'on pose $H = V/V'$. Montrer que H et L_{nr}^* sont des G-modules cohomologiquement triviaux. (Utiliser l'exercice du Chap. VII, § 5 pour se ramener au cas totalement ramifié.)

b) En utilisant les cobords des suites exactes :

$$0 \longrightarrow L^* \longrightarrow \hat{L}_{nr}^* \xrightarrow{F-1} V' \longrightarrow 0$$

$$0 \longrightarrow V \longrightarrow \hat{L}_{nr}^* \xrightarrow{w} \mathbf{Z} \longrightarrow 0$$

ainsi que l'isomorphisme $\hat{H}^q(G, V') \to \hat{H}^q(G, V)$, définir des isomorphismes :

$$\gamma : \hat{H}^q(G, \mathbf{Z}) \to \hat{H}^{q+2}(G, L^*), \qquad q \in \mathbf{Z}.$$

Montrer que γ est donné par le cup-produit par la classe $v_{L/K} = \gamma(1)$ de $H^2(G, L^*)$.

c) Montrer que les $v_{L/K}$ sont les classes fondamentales d'une formation de classes (cf. Chap. XI, § 3).

d) Soit $u_{L/K}$ la classe fondamentale définie au § 4. Montrer que $v_{L/K} = -u_{L/K}$. (Se ramener au cas non ramifié grâce à *c*), et faire un calcul direct dans ce cas.)

e) Expliciter γ pour $q = -2$, et en déduire une autre démonstration du théorème de Dwork grâce à *d*).

CHAPITRE XIV

SYMBOLES LOCAUX ET THÉORÈME D'EXISTENCE

§ 1. Définition générale des symboles locaux

Soit K un corps, soit K_s une clôture séparable de K, et soit $G = G(K_s/K)$. Si χ est un *caractère* de G, autrement dit un élément de $H^1(G, \mathbf{Q}/\mathbf{Z})$, on sait que $\delta\chi$ est un élément de $H^2(G, \mathbf{Z})$. Si $b \in K^*$, le cup-produit $b.\delta\chi$ est un élément du groupe de Brauer $H^2(G, K_s^*) = B_K$. Nous désignerons cet élément par le symbole (χ, b).

PROPOSITION 1. (i) $(\chi + \chi', b) = (\chi, b) + (\chi', b)$.
(ii) $(\chi, bb') = (\chi, b) + (\chi, b')$.
C'est clair.

Donnons-nous un caractère χ de G, et soit H_χ son noyau. Soit L_χ l'extension de K correspondant à H_χ. C'est une extension cyclique. De façon plus précise, si n est égal à l'ordre de χ, L_χ/K est cyclique de degré n, et l'on choisit pour générateur de son groupe de Galois un élément s tel que $\chi(s) = \frac{1}{n}$. Ce choix de s permet d'identifier K^*/NL_χ^* au sous-groupe $H^2(L_\chi/K)$ de B_K.

PROPOSITION 2. *Soit $b \in K^*$. L'élément de $H^2(L_\chi/K)$ qui correspond à b n'est autre que (χ, b).*
Cela résulte de ce qui a été dit au Chap. VIII, § 4.

COROLLAIRE 1. *Pour que (χ, b) soit nul, il faut et il suffit que b soit une norme dans l'extension L_χ/K.*

COROLLAIRE 2. *Pour qu'un élément de B_K soit de la forme (χ, b), il faut et il suffit qu'il soit décomposé par L_χ.*

Passons maintenant au cas du corps de classes local, autrement dit supposons que K est *complet* pour une valuation discrète v à corps résiduel $\bar{K}$ *quasi-fini*. On a vu au Chapitre précédent que l'on a alors un isomorphisme

$$\mathrm{inv}_K : B_K \to \mathbf{Q}/\mathbf{Z}.$$

Nous poserons

$$(\chi, b)_v = \mathrm{inv}_K(\chi, b)$$

c'est un élément de $\mathbf{Q}/\mathbf{Z}$. La proposition suivante en donne une définition plus directe :

PROPOSITION 3. *Soit* $s_b = (b, */K)$ *l'élément de* G^a *défini par l'application de réciprocité. On a :*

$$(\chi, b)_v = \chi(s_b).$$

Cela résulte de la prop. 2 du Chap. XI, § 3.

COROLLAIRE. *Si* χ *est un caractère tel que* $(\chi, b)_v = 0$ *pour tout* $b \in K^*$, *on a* $\chi = 0$.

En effet on a alors $\chi(s_b) = 0$ pour tout b, et comme les éléments de G^a de la forme s_b sont denses dans G^a, on en déduit bien que χ est trivial.

Remarque. La proposition 3 montre que *la connaissance des* $(\chi, b)_v$ *pour tout* χ *équivaut à celle de* $(b, */K)$. C'est ce qui fait l'intérêt de ces symboles.

Pour rendre ce qui précède plus explicite, il reste à exhiber des caractères χ. On a essentiellement deux méthodes pour cela :

i) la théorie de Kummer (cf. Chap. X, § 3), qui conduit aux symboles (a, b),

ii) la théorie d'Artin-Schreier (*loc. cit.*), qui conduit aux symboles $[a, b)$.

C'est là le sujet des prochains paragraphes. Nous verrons ensuite comment les résultats obtenus entraînent le théorème d'existence pour les corps locaux à corps résiduel fini.

Exercice. Soit L une extension finie séparable de K, et soit $H = G(K_s/L)$. On considère les homomorphismes

$$\begin{array}{ll} \mathrm{Res} : B_K \to B_L, & \mathrm{Res} : X(G) \to X(H) \\ \mathrm{Cor} : B_L \to B_K, & \mathrm{Cor} : X(H) \to X(G). \end{array}$$

Montrer que l'on a

$$\begin{array}{ll} \mathrm{Res}\,(\chi, b) = (\mathrm{Res}\,\chi, b) & \text{si } \chi \in X(G),\ b \in K^*, \\ \mathrm{Cor}\,(\psi, b) = (\mathrm{Cor}\,\psi, b) & \text{si } \psi \in X(H),\ b \in K^*, \\ \mathrm{Cor}\,(\chi, c) = (\chi, Nc) & \text{si } \chi \in X(G),\ c \in L^*. \end{array}$$

Comment faut-il modifier ces formules lorsqu'on ne suppose plus que l'extension L/K est séparable?

§ 2. *Le symbole (a, b)*

Soit n un entier $\geqslant 1$. Nous supposons dans tout ce § que *n est premier à la caractéristique de* K, et que K *contient le groupe* E_n *des racines n-ièmes de l'unité.*

On a vu au Chap. X, § 3 que tout élément $a \in K^*$ définit un homomorphisme $\varphi_a : G \to \mathbf{Z}/n\mathbf{Z}$ de la manière suivante : on choisit dans K, une racine α de l'équation

$\alpha^n = a$, et l'on pose $\varphi_a(s) = s(\alpha)/\alpha$. Faisons choix d'une *racine primitive n-ième de l'unité*, soit w; cela a pour effet d'identifier E_n au groupe $\mathbf{Z}/n\mathbf{Z}$; si l'on pose alors

$$\chi_a(s) = \frac{1}{n}\varphi_a(s)$$

on obtient un homomorphisme de G dans le sous-groupe $\frac{1}{n}\mathbf{Z}/\mathbf{Z}$ de $\mathbf{Q}/\mathbf{Z}$, autrement dit un *caractère* de G, On sait (*loc. cit.*) que l'application $a \to \chi_a$ définit un isomorphisme de K^*/K^{*n} sur le groupe des caractères de G d'ordre divisant n.

Soit maintenant $b \in K^*$. Nous poserons :

$$(a, b) = (\chi_a, b).$$

C'est un élément de B_K d'ordre divisant n.

PROPOSITION 4. (i) $(aa', b) = (a, b) + (a', b)$.

(ii) $(a, bb') = (a, b) + (a, b')$.

(iii) *Pour que* $(a, b) = 0$, *il faut et il suffit que* b *soit une norme dans l'extension* $K(a^{1/n})/K$.

(iv) *Si* $a \in K^*$ *et* $x \in K$ *sont tels que* $x^n - a \neq 0$, *on a* $(a, x^n - a) = 0$. *En particulier* $(a, -a) = 0$ *et* $(a, 1 - a) = 0$.

(v) $(a, b) + (b, a) = 0$.

Les propriétés (i) et (ii) résultent de la prop. 1; (iii) résulte du cor. 1 à la prop. 2. Pour (iv), on s'appuie sur l'identité :

$$x^n - a = \prod_{i=0}^{n-1}(x - w^i\alpha), \qquad \alpha^n = a.$$

Soit d le plus grand diviseur de n tel que l'équation $a = y^d$ soit résoluble dans K, et posons $n = dm$. L'extension $K(\alpha)/K$ est cyclique de degré m, et les conjugués de $x - w^i\alpha$ ne sont autres que les éléments $x - w^j\alpha$, avec $j \equiv i \bmod d$. On a donc

$$x^n - a = \prod_{i=0}^{d-1} N(x - w^i\alpha)$$

ce qui montre bien que $x^n - a$ est une norme dans l'extension $K(\alpha)/K$. En faisant $x = 0$ on trouve $(a, -a) = 0$ et en faisant $x = 1$, on trouve $(a, 1 - a) = 0$. Enfin, on a :

$$\begin{aligned} 0 = (ab, -ab) &= (a, -ab) + (b, -ab) \\ &= (a, -a) + (a, b) + (b, a) + (b, -b) \\ &= (a, b) + (b, a) \end{aligned}$$

ce qui démontre (v).

Remarques. 1) Le symbole (a, b) *dépend du choix de* w; si l'on voulait éviter ce choix, il faudrait le définir comme un élément de $E_n \otimes B_{K,n}$, où $B_{K,n}$ désigne le groupe des éléments ξ de B_K tels que $n\xi = 0$.

2) Les propriétés (i) et (ii) montrent que (a, b) ne dépend que des classes de a et de b mod. K^{*n}.

3) Pour $n = 2$, on a $E_n = \{\pm 1\}$ et le symbole (a, b) est défini sous la seule condition que la caractéristique de K soit différente de 2. La variété de Severi-Brauer correspondante est la conique d'équation homogène $x^2 - ay^2 - bz^2 = 0$. En particulier on a $(a, b) = 0$ si et seulement si cette conique a un point rationnel sur K.

Le symbole (a, b) peut être interprété comme le cup-produit de deux classes de cohomologie de degré 1. De façon plus précise, considérons la suite exacte :

$$0 \to \mathbf{Z}/n\mathbf{Z} \to K_s^* \xrightarrow{v} K_s^* \to 0$$

où $\mathbf{Z}/n\mathbf{Z}$ a été identifié à E_n, et où $v(x) = x^n$. Comme $H^1(G, K_s^*) = 0$, on en déduit la suite exacte :

$$0 \to H^2(G, \mathbf{Z}/n\mathbf{Z}) \to B_K \xrightarrow{n} B_K.$$

Nous noterons i l'injection ainsi définie de $H^2(G, \mathbf{Z}/n\mathbf{Z})$ dans le groupe de Brauer B_K.

Soient maintenant a et b deux éléments de K^*. D'après ce qui a été dit au début du §, on peut leur associer des éléments φ_a, φ_b du groupe $H^1(G, \mathbf{Z}/n\mathbf{Z})$. Par cup-produit, on en déduit un élément $\varphi_a . \varphi_b$ de $H^2(G, \mathbf{Z}/n\mathbf{Z})$.

PROPOSITION 5. *On a* $(a, b) = i(\varphi_a . \varphi_b)$.

Pour faciliter le calcul, on écrira additivement tous les G-modules considérés, et en particulier K_s^*. De plus, si φ désigne une fonction sur G à valeurs dans $\mathbf{Z}/n\mathbf{Z}$, on notera $\bar{\varphi}$ un relèvement de cette fonction à $\mathbf{Z}$.

Soit $\beta \in K_s^*$ tel que $n\beta = b$. Par définition, (a, b) est égal à $b . \delta\chi_a$, et peut donc être représenté par le cocycle :

$$(s, t) \to b . \left[\frac{1}{n} (\bar{\varphi}_a(s) + \bar{\varphi}_a(t) - \bar{\varphi}_a(st))\right] = \beta . (\bar{\varphi}_a(s) + \bar{\varphi}_a(t) - \bar{\varphi}_a(st)).$$

D'autre part, l'anticommutativité du cup-produit montre que $\varphi_a . \varphi_b = -\varphi_b . \varphi_a$. Vu la formule donnant le cup-produit de deux cocycles (cf. Cartan-Eilenberg [13], p. 221), la classe $-i(\varphi_b . \varphi_a)$ peut être représentée par le cocycle :

$$(s, t) \to -i(\varphi_b(s) . \bar{\varphi}_a(t)) = -(s\beta - \beta)\bar{\varphi}_a(t).$$

La différence de ces deux cocycles est :

$$(s, t) \to s\beta . \bar{\varphi}_a(t) - \beta . \bar{\varphi}_a(st) + \beta . \bar{\varphi}_a(s)$$

et c'est le cobord de la cochaîne $s \to \beta . \bar{\varphi}_a(s)$, c.q.f.d.

Remarque. La proposition précédente montre que *l'anticommutativité du symbole* (a, b) *provient de celle du cup-produit.* On peut de même donner une démonstration cohomologique de la trivialité du symbole $(a, -a)$, cf. exer. 1.

Revenons maintenant au corps de classes local, autrement dit supposons que K soit un corps complet pour une valuation discrète v à corps résiduel $\mathbb{K}$ quasi-fini. Si $a, b \in K^*$, on peut appliquer inv_K à (a, b), et l'on obtient un élément $\mathrm{inv}(a, b)$ du sous-groupe $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ de $\mathbb{Q}/\mathbb{Z}$. On pourrait prendre cet élément comme « symbole local »; en fait, il est plus commode (et plus traditionnel) de le remplacer par le suivant :

$$(a, b)_v = w^{n \cdot \mathrm{inv}(a, b)},$$

définition qui a un sens, puisque $n.\mathrm{inv}(a, b)$ est un élément de $\mathbb{Z}/n\mathbb{Z}$. Ainsi, $(a, b)_v$ *est une racine n-ième de l'unité.*

Proposition 6. *Si* $\alpha \in K_v^*$ *est une racine n-ième de* a, *et si* $s_b = (b, */K)$, *on a* :

$$(a, b)_v = s_b(\alpha)/\alpha.$$

En effet
$$\begin{aligned}(a, b)_v &= w^{n \cdot \mathrm{inv}(a, b)} = w^{n \cdot \mathrm{inv}(\chi_a, b)} \\ &= w^{n\chi_a(b)}, \quad \text{d'après la prop. 3,} \\ &= w^{\varphi_a(b)} = s_b(\alpha)/\alpha, \quad \text{vu la définition de } \varphi_a.\end{aligned}$$

Corollaire. *Le symbole* $(a, b)_v$ *ne dépend pas du choix de la racine de l'unité* w.

En effet, la formule de la prop. 6 suffit à caractériser $(a, b)_v$, et cette formule ne fait pas intervenir w.

Proposition 7. (i) $(aa', b)_v = (a, b)_v.(a', b)_v$.

(ii) $(a, bb')_v = (a, b)_v.(a, b')_v$.

(iii) *Pour que* $(a, b)_v = 1$, *il faut et il suffit que* b *soit une norme dans l'extension* $K(a^{1/n})/K$.

(iv) $(a, -a)_v = 1$ *et* $(a, 1-a)_v = 1$.

(v) $(a, b)_v.(b, a)_v = 1$.

(vi) *Si* $(a, b)_v = 1$ *pour tout* $b \in K^*$, *on a* $a \in K^{*n}$.

Les propriétés (i) à (v) résultent des propriétés correspondantes du symbole (a, b), cf. prop. 4. Sous les hypothèses de (vi), on a $(\chi_a, b)_v = 0$ pour tout $b \in K^*$, d'où $\chi_a = 0$ (cor. à la prop. 3), i. e. $a \in K^{*n}$.

Corollaire. *Si un élément* $b \in K^*$ *est une norme dans toute extension cyclique de* K *de degré divisant* n, *on a* $b \in K^{*n}$.

D'après (iii), on a alors $(a, b)_v = 1$ pour tout a, d'où d'après (v) $(b, a)_v = 1$, et d'après (vi) $b \in K^{*n}$.

Remarque. Le symbole $(a, b)_v$ défini ici est *l'inverse* de celui d'Artin-Tate ([8], Chap. XII), mais est le même que celui du Bericht de Hasse ([31], Teil II, § 11), grâce à deux changements de signe qui se compensent.

Exercices. 1. On suppose que n est pair, et l'on pose $m = n/2$.

a) Soit G un groupe et soit $\varphi \in H^1(G, \mathbf{Z}/n\mathbf{Z})$. Montrer que le carré $\varphi.\varphi \in H^2(G, \mathbf{Z}/n\mathbf{Z})$ est égal à $m.\pi(\delta\varphi)$, où δ est le cobord dans la suite exacte $0 \to \mathbf{Z} \xrightarrow{n} \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z} \to 0$, et où π est l'homomorphisme canonique de $H^2(G, \mathbf{Z})$ dans $H^2(G, \mathbf{Z}/n\mathbf{Z})$. (Se ramener à un groupe cyclique d'ordre n, et faire un calcul explicite de cocycles.)

b) Soit $a \in K^*$. En appliquant *a*) à $\varphi = \varphi_a$, retrouver la formule $(a, a) = (a, -1)$.

2. Soient $a, b \in K^*$, avec $a + b \neq 0$. Montrer que :

$$(a, b) = (a, a + b) + (a + b, b) + (-1, a + b).$$

3. On suppose que n est impair. Soient $a, b, c \in K^*$ trois éléments tels que $a + b + c = 0$. Démontrer la formule :

$$(a, b) + (b, c) + (c, a) = 0.$$

4. Soit L/K une extension finie séparable. On note $(a, b)_K$ le symbole (a, b) calculé dans K, et $(a, b)_L$ celui calculé dans L. Montrer que l'on a :

$$\begin{aligned} \mathrm{Res}(a, b)_K &= (a, b)_L \qquad \text{si } a \in K^*,\ b \in K^*, \\ \mathrm{Cor}(a, c)_L &= (a, \mathrm{N}c)_K \qquad \text{si } a \in K^*,\ c \in L^*. \end{aligned}$$

En déduire des formules analogues pour les symboles $(a, b)_v$.

5. Les hypothèses étant celles de la théorie du corps de classes local, soit $a \in K^*$. Pour que $(a, b)_v = 1$ pour toute unité b de K^*, il faut et il suffit que l'extension $K(a^{1/n})/K$ soit non ramifiée.

§ 3. *Calcul du symbole (a, b), dans le cas « modéré »*

Nous continuons à nous placer dans la situation du corps de classes local, autrement dit nous supposons que K est un corps complet pour une valuation discrète v à corps résiduel $\mathbf{K}$ quasi-fini. Nous supposons en outre que *n est un entier premier à la caractéristique de* K; les extensions $K(a^{1/n})/K$ ne font donc pas intervenir la ramification supérieure : elles sont « modérément ramifiées » (« tamely ramified » dans la terminologie anglaise).

LEMME 1. *Pour que* K *contienne le groupe des racines n-ièmes de l'unité, il faut et il suffit qu'il en soit de même de* $\mathbf{K}$, *et l'homomorphisme canonique* $U_K \to K^*$ *induit un isomorphisme du groupe* E_n *des racines n-ièmes de l'unité de* K *sur le groupe* $\mathbf{E}_n$ *des racines n-ièmes de l'unité de* $\mathbf{K}$.

Si $\mathbf{K}$ est un corps de caractéristique zéro, K est isomorphe à $\mathbf{K}((T))$ et le lemme est évident. Supposons donc $\mathbf{K}$ de caractéristique $p \neq 0$. Si $\mathbf{K}$ contient le groupe $\mathbf{E}_n$ des racines n-ièmes de l'unité, les représentants multiplicatifs (au sens du Chap. II, § 4) des $\mathbf{E}_n$ forment un sous-groupe E_n de U_K, appliqué isomorphiquement sur $\mathbf{E}_n$; le corps K contient donc les racines n-ièmes de l'unité. Inversement, si K contient E_n, les éléments de E_n sont nécessairement des représentants multiplicatifs (cela résulte de l'assertion (ii) de la prop. 8 du Chap. II), et l'image $\mathbf{E}_n$ de E_n dans $\mathbf{K}^*$ est isomorphe à E_n, ce qui montre bien que $\mathbf{K}$ contient les racines n-ièmes de l'unité.

Nous supposerons pour le reste de ce paragraphe que *n vérifie les conditions du lemme* 1, et nous conviendrons d'identifier les groupes E_n et $\bar{E}_n$. On peut aussi considérer que le symbole $(a, b)_n$ prend ses valeurs dans $\bar{E}_n$; nous nous proposons de le calculer explicitement.

Nous aurons besoin du résultat auxiliaire suivant :

LEMME 2. *Soit k un corps quasi-fini contenant le groupe E_n des racines n-ièmes de l'unité (n étant premier à la caractéristique de k). Si $x \in k^*$, soit $y \in k^*_s$ tel que $y^n = x$, et soit $z = Fy/y$. On a $z \in E_n$, l'élément z ne dépend pas de y, et, si on le note $P_n(x)$, l'application P_n définit par passage au quotient un isomorphisme de k^*/k^{*n} sur E_n.*

Cela résulte, *via* la théorie de Kummer, du fait que k possède une extension cyclique de degré n et une seule.

Exemple. Si k est un *corps fini* à q éléments, l'hypothèse suivant laquelle k contient E_n équivaut à dire que n *divise* $q - 1$. L'application P_n est donnée par la formule suivante :

$$P_n(x) = x^{\frac{q-1}{n}}.$$

En effet, si $y^n = x$, on a $P_n(x) = Fy/y = y^{q-1} = x^{(q-1)/n}$.

Pour $n = 2$, on retrouve le *symbole de Legendre.*

Revenons maintenant au calcul de $(a, b)_n$:

PROPOSITION 8. *Soient a et b deux éléments de K^*, et soient α et β leurs valuations. Posons :*

$$c = (-1)^{\alpha\beta} \frac{a^\beta}{b^\alpha}.$$

Alors c est une unité de K, et si l'on note $\bar{c}$ son image dans K^*, on a :

$$(a, b)_n = P_n(\bar{c}).$$

COROLLAIRE. *Si K est un corps fini à q éléments, on a :* $(a, b)_n = \bar{c}^{\frac{q-1}{n}}$.

Démonstration de la proposition 8. Il est clair que c est une unité, et que $P_n(\bar{c})$ dépend bilinéairement (au sens multiplicatif) de a et de b; comme il en est de même du symbole $(a, b)_n$ on est ramené à démontrer la formule lorsque a et b sont des uniformisantes. Posons alors $a = \pi$, $b = -\pi u$, où u est une unité. Les deux membres sont égaux à 1 pour $a = \pi$, $b = -\pi$; on est donc ramené au cas $a = \pi$, $b = u$, puis, par symétrie, au cas $a = u$, $b = \pi$. Posons $x = \bar{u}$, et soit K' une extension finie de K contenant une racine n-ième y de x; soit K' l'extension non ramifiée de K correspondant à K'. Comme l'équation $T^n = x$ admet la racine simple $T = y$ dans K', l'équation $T^n = u$ admet une racine v se projetant sur y, cf. Chap. II, § 4, prop. 7.

D'après la prop. 13 du Chap. XIII, on a $(\pi, K'/K) = F$, générateur canonique du groupe de Galois $G(K'/K)$. Si $w = (u, \pi)_n$, la prop. 6 montre que $w = Fv/v$, d'où $\overline{w} = Fy/y = P_n(x) = P_n(\overline{u})$, c.q.f.d.

Exercice. Soit K un corps complet pour une valuation discrète à corps résiduel $\overline{K}$ parfait. On suppose que K contient les racines n-ièmes de l'unité, n étant premier à la caractéristique de $\overline{K}$. Déterminer explicitement le symbole $(a, b) \in B_K$ en utilisant la décomposition de B_K comme $B_{\overline{K}} \times X(\mathfrak{g})$ obtenue à partir du choix d'une uniformisante de K (cf. Chap. XII, § 3, th. 2).

§ 4. *Calcul du symbole (a, b), pour le corps* $\mathbf{Q}_p$ *(n = 2)*

(Nous nous bornons à cet exemple particulièrement simple. Le lecteur en trouvera d'autres, moins triviaux, dans Artin-Tate [8], Chap. XII, ou dans Hasse [31], Teil II, §§ 15-21; voir aussi Chap. XV, § 3.)

On prend $n = 2$, et $K = \mathbf{Q}_p$, corps p-adique usuel. On écrit $(a, b)_p$ au lieu de $(a, b)_n$. Il y a deux cas à distinguer :

(i) $p \neq 2$.

On se trouve dans le cas modéré, et l'on peut appliquer la prop. 8. Si $x \in \mathbf{F}_p^*$, on a $P_2(x) = x^{(p-1)/2} = \left(\frac{x}{p}\right)$, symbole de Legendre. Si l'on écrit alors a et b sous la forme :

$$a = p^{\alpha}a', \qquad b = p^{\beta}b',$$

a' et b' étant des unités, on a

$$c = (-1)^{\alpha\beta\frac{p-1}{2}} \frac{a'^{\beta}}{b'^{\alpha}}$$

d'où :

$$(a, b)_p = (-1)^{\alpha\beta\frac{p-1}{2}} \left(\frac{b'}{p}\right)^{\alpha} \left(\frac{a'}{p}\right)^{\beta}.$$

En particulier, on a $(p, p)_p = (-1)^{(p-1)/2}$, et $(p, b)_p = \left(\frac{b}{p}\right)$ si b est une unité.

(ii) $p = 2$.

On ne se trouve plus dans le cas modéré, on doit raisonner directement. Comme $(a, b)_2$ est une forme bilinéaire sur K^*/K^{*2}, la première chose à faire est de déterminer ce groupe. Or, on a le lemme suivant :

LEMME 3. *Tout élément x de $\mathbf{Z}_2$ qui est congru à* 1 mod. 8 *est un carré.*

Admettons pour un instant ce lemme. Soit U le groupe des unités de $\mathbf{Q}_2$, et soit U' le sous-groupe de U formé des x congrus à 1 mod. 8. Un système de représentants de U/U' est $\{1, -1, 5, -5\}$; le carré de chacun de ces éléments appartient à U'.

On a donc $U' = U^2$, et le groupe Q_2^*/Q_2^{*2} est un groupe de type (2, 2, 2) engendré par $\{2, 5, -1\}$. Il suffit donc de déterminer $(a, b)_2$ pour ces valeurs particulières.

On a $(-1, x)_2 = 1$ si et seulement si x est une norme de l'extension $Q_2(\sqrt{-1})/Q_2$ c'est-à-dire si x s'écrit sous la forme $y^2 + z^2$, avec $y, z \in Q_2$. Comme $5 = 4 + 1$ et $2 = 1 + 1$, on a $(-1, 2)_2 = (-1, 5)_2 = 1$. Si l'on avait $(-1, -1)_2 = 1$, on aurait alors $(-1, x)_2 = 1$ pour tout x, et -1 serait un carré dans Q_2^*, ce qui n'est pas le cas. Donc $(-1, -1)_2 = -1$.

On a $(2, 2)_2 = (2, -1)_2 = 1$ et de même $(5, 5)_2 = (5, -1)_2 = 1$. Reste à déterminer $(2, 5)_2$. S'il était égal à 1, on aurait $(2, x)_2 = 1$ pour tout x, et 2 serait un carré, ce qui n'est pas. Donc $(2, 5)_2 = -1$, ce qui achève le calcul de $(a, b)_2$ dans Q_2. Le résultat peut s'énoncer de la façon suivante :

Si u est une unité de Q_2, soit $\omega(u)$ la classe mod. 2 de $\dfrac{u^2 - 1}{8}$, et soit $\varepsilon(u)$ la classe mod. 2 de $(u-1)/2$. On vérifie facilement que ω et ε sont des homomorphismes de U dans $\mathbf{Z}/2\mathbf{Z}$. Avec ces notations, on a :

$$(2, u)_2 = (-1)^{\omega(u)} \qquad \text{si } u \text{ est une unité,}$$
$$(u, v)_2 = (-1)^{\varepsilon(u)\varepsilon(v)} \qquad \text{si } u \text{ et } v \text{ sont des unités.}$$

Reste à démontrer le lemme 3. Plus généralement :

PROPOSITION 9. *Soit* K *un corps complet pour une valuation discrète* v; *on suppose que* K *est de caractéristique zéro, et que son corps résiduel* $\mathbf{K}$ *est de caractéristique* $p \neq 0$. *Soit* $e = v(p)$ *l'indice de ramification absolu de* K (*cf.* Chap. II, § 5). *Pour tout entier* $m \geqslant 1$, *notons* $U^{(m)}$ *le groupe multiplicatif des éléments* x *de* K *tels que* $v(x-1) \geqslant m$, *cf.* Chap. IV, § 2. *Alors, si* $m > e/(p-1)$, *l'application* $x \to x^p$ *est un isomorphisme de* $U^{(m)}$ *sur* $U^{(m+e)}$.

(Lorsque $K = Q_2$, on a $p = 2$, $e = 1$, et en prenant $m = 2$, on voit que $x \to x^2$ est un isomorphisme de $U^{(2)}$ sur $U^{(3)}$, ce qui démontre le lemme 3.)

Soit π une uniformisante de K. Soit $y \in U^{(m+1)}$. On peut écrire y sous la forme :

$$y = 1 + a\pi^{m+1}, \qquad \text{avec } v(a) \geqslant 0.$$

Posons $p = b\pi^e$, avec $v(b) = 0$. Cherchons une racine $x \in U^{(m)}$ de l'équation $x^p = y$. Si l'on pose $x = 1 + z\pi^m$, avec $v(z) \geqslant 0$, on est conduit à l'équation :

$$1 + a\pi^{m+e} = 1 + pz\pi^m + \cdots + z^p\pi^{mp}.$$

Vu l'inégalité $m > e/(p-1)$, tous les termes du membre de droite, sauf les deux premiers, ont une valuation $> m + e$. On peut donc écrire l'équation précédente sous la forme :

$$a = bz + g(z)$$

où $g(z)$ est un polynôme à coefficients tous divisibles par π. En réduisant mod. π, on trouve l'équation $\bar{a} = \bar{b}.\bar{z}$, et comme $\bar{b} \neq 0$, cette équation a une racine et une seule. D'après la prop. 7 du Chap. II, il en est donc de même de l'équation $x^p = y$. c.q.f.d.

La proposition précédente est le point de départ de l'étude de la structure du groupe U, cf. Hasse [34], § 15 ou bien [59], § 1.8. Nous nous bornerons à en donner une application simple :

Le groupe $U^{(1)}$ est limite projective des groupes $U^{(1)}/U^{(m)}$, chacun annulé par une puissance de p; en passant à la limite on en conclut que $U^{(1)}$ est un *module sur l'anneau $\mathbf{Z}_p$ des entiers p-adiques.*

PROPOSITION 10. *Les hypothèses et notations étant celles de la proposition 9, supposons en outre que* K *soit une extension finie de degré n du corps $\mathbf{Q}_p$. Alors, si $m > e/(p-1)$, le groupe $U^{(m)}$ est un $\mathbf{Z}_p$-module libre de rang n, et le groupe $U^{(1)}$ est produit d'un $\mathbf{Z}_p$-module libre de rang n, et d'un groupe cyclique d'ordre une puissance de p.*

Soit $q = p^f$ le nombre d'éléments de $\mathbf{K}$; on a $ef = n$. Le groupe $U^{(m)}/U^{(m+e)}$ est un groupe abélien de type $(p, \ldots, p)$ et d'ordre $q^e = p^n$. Soient $x_1, \ldots, x_n$ des éléments de $U^{(m)}$ engendrant $U^{(m)}$ mod. $U^{(m+e)}$. Ils définissent un homomorphisme

$$\theta : \mathbf{Z}_p^n \to U^{(m)}.$$

Supposons $m > e/(p-1)$. Filtrons $\mathbf{Z}_p^n$ par les $(p^k\mathbf{Z}_p)^n$ et $U^{(m)}$ par les $U^{(m+ke)}$. La prop. 9 montre que θ est compatible avec ces filtrations et définit un isomorphisme des gradués associés. D'après le lemme 2 du Chap. V, c'est donc un isomorphisme, ce qui démontre la première partie de la proposition. [On pourrait aussi remplacer θ par une exponentielle.] La seconde en résulte en remarquant que $U^{(1)}/U^{(m)}$ est un groupe fini, donc que $U^{(1)}$ et $U^{(m)}$ ont même rang, et que le sous-module de torsion de $U^{(m)}$ est nécessairement cyclique.

Exemples. (i) Si $\mathbf{K} = \mathbf{Q}_p$, avec $p \neq 2$, on peut prendre $m = 1$, et l'on voit que $U^{(1)}$ est isomorphe à $\mathbf{Z}_p$; un élément x de $U^{(1)}$ est un générateur si et seulement s'il n'appartient pas à $U^{(2)}$; $x = 1 + p$ en est un exemple.

(ii) Si $\mathbf{K} = \mathbf{Q}_2$, on peut prendre $m = 2$. Le groupe $U = U^{(1)}$ s'identifie au produit direct $\{\pm 1\} \times U^{(2)}$. Le groupe $U^{(2)}$ est isomorphe à $\mathbf{Z}_2$; un élément x de $U^{(2)}$ est un générateur si et seulement s'il n'appartient pas à $U^{(3)}$; $x = 1 + 2^2 = 5$ en est un exemple.

(On retrouve ainsi des résultats bien connus, cf. Bourbaki, *Alg.*, Chap. VII, § 2, n° 4.)

Exercices. 1. Interpréter les homomorphismes ω et ε du groupe U des unités de $\mathbf{Q}_2$ dans $\mathbf{Z}/2\mathbf{Z}$ au moyen de la décomposition en produit $U = \{\pm 1\} \times U^{(2)}$.

2. Soit K un corps complet pour une valuation discrète à corps résiduel fini. Si la caractéristique de K est nulle, montrer que tout sous-groupe d'indice fini de K^* est fermé. Si K est de caractéristique $p \neq 0$, montrer qu'il existe des sous-groupes d'indice p de K^* qui ne sont pas fermés; quel est le cardinal de l'ensemble de ces sous-groupes?

3. Les hypothèses étant celles de l'exer. 2, soit m un entier premier à la caractéristique de K. Soit E_m le groupe des racines m-ièmes de l'unité contenues dans K^*, et soit

$$\varphi(K^*) = (K^* : K^{*m})/\mathrm{Card}\,(E_m);$$

c'est le quotient de Herbrand de K^* pour le groupe $\mathbf{Z}/m\mathbf{Z}$ opérant trivialement. Montrer que l'on a :

$$\varphi(K^*) = m/\|m\|_K,$$

où $\|x\|_K$ désigne la valeur absolue normalisée de K (cf. Chap. II, § 1). (Utiliser la prop. 10 pour montrer que $\varphi(U^{1)}) = 1/\|m\|_K$.)

§ 5. *Le symbole* $[a, b)$

Dans tout ce paragraphe, K désigne un corps *de caractéristique* $p \neq 0$. On pose $\wp(x) = x^p - x$; c'est un endomorphisme du groupe additif de K.

Soit K_s une clôture séparable de K, et soit $G = G(K_s/K)$. On a vu au Chap. X, § 3 que tout élément $a \in K$ définit un homomorphisme $\varphi_a : G \to \mathbf{Z}/p\mathbf{Z}$ de la manière suivante : on choisit dans K_s une racine α de l'équation $\wp(\alpha) = a$, et l'on pose $\varphi_a(s) = s\alpha - \alpha$. Si $\psi_a(s) = \frac{1}{p}\varphi_a(s)$, l'application ψ_a est un homomorphisme de G dans le sous-groupe $\frac{1}{p}\mathbf{Z}/\mathbf{Z}$ de $\mathbf{Q}/\mathbf{Z}$, autrement dit un *caractère de* G. On sait (*loc. cit.*) que l'application $a \to \psi_a$ définit un isomorphisme de $K/\wp(K)$ sur le groupe des caractères ψ de G tels que $p\psi = 0$.

Soit maintenant $b \in K^*$. Conformément aux définitions générales du § 1, nous poserons :

$$[a, b) = (\psi_a, b).$$

C'est un élément de B_K; on a $p[a, b) = 0$.

PROPOSITION 11. (i) $[a + a', b) = [a, b) + [a', b)$.

(ii) $[a, bb') = [a, b) + [a, b')$.

(iii) *Pour que* $[a, b) = 0$, *il faut et il suffit que b soit une norme dans l'extension* $K(\alpha)/K$, *avec* $\wp(\alpha) = a$.

(iv) $[a, a) = 0$ *pour tout* $a \in K^*$.

Les propriétés (i) et (ii) résultent de la prop. 1; (iii) résulte du cor. 1 à la prop. 2. L'assertion (iv) est évidente si a est de la forme $\wp(\alpha)$, avec $\alpha \in K$. Sinon, l'extension $K(\alpha)/K$ est de degré p, et les conjugués de α sont les éléments $\alpha + i$, $i \in \mathbf{Z}/p\mathbf{Z}$. Comme on a :

$$\alpha(\alpha - 1) \dots (\alpha - p + 1) = \alpha^p - \alpha = a$$

on voit que a est égal à la norme de α dans $K(\alpha)/K$, d'où $[a, a) = 0$ d'après (iii).

Exemple. Pour $p = 2$, la variété de Severi-Brauer correspondant à $[a, b)$ est la conique d'équation homogène $x^2 + xy + ay^2 + bz^2 = 0$. En particulier on a $[a, b) = 0$ si et seulement si cette conique a un point rationnel sur K.

Passons maintenant au cas où K est le corps des séries formelles $k((t))$ sur un corps k de caractéristique p. Si $\omega = f\,dt$ est une forme différentielle de K, le coefficient de t^{-1} dans f est appelé le *résidu* de ω, et noté $\mathrm{Res}(\omega)$. On démontre (*cf.* par exemple [56], Chap. II, prop. 5') qu'il ne dépend pas du choix de l'uniformisante t.

PROPOSITION 12. *Soit* $K = k((t))$, *où* k *est un corps parfait de caractéristique* $p \neq 0$. *Si* $a \in K$ *et* $b \in K^*$, *soit* $c = \mathrm{Res}\,(a\frac{db}{b}) \in k$. *On a alors* :

$$[a, b) = [c, t) \qquad \textit{dans } B_K.$$

Comme les 2 membres sont bilinéaires, on peut se borner à considérer le cas où b est une uniformisante, c'est-à-dire (quitte à changer de variable), le cas $b = t$. Si $a = \sum a_n t^n$, on décompose a en a_0, $\sum_{n<0} a_n t^n$, $\sum_{n>0} a_n t^n$, et on considère séparément chacun de ces cas :

(i) *a est une constante.* On a $\mathrm{Res}\,(a\frac{dt}{t}) = a$, et la formule à démontrer s'écrit $[a, t) = [a, t)$.

(ii) $a = ut^{-n}$, *avec* $u \in k$ *et* $n > 0$. On a $\mathrm{Res}\,(a\frac{dt}{t}) = 0$, et l'on doit vérifier que $[a, t) = 0$. On raisonne par récurrence sur n :

Si n est premier à p, on a la relation :

$$-n[ut^{-n}, t) = [ut^{-n}, t^{-n}) = [ut^{-n}, ut^{-n}) - [ut^{-n}, u).$$

Or $[ut^{-n}, ut^{-n}) = 0$ d'après la prop. 11, et $[ut^{-n}, u) = 0$ puisque u est une puissance p-ième. Comme n est premier à p, on en déduit bien $[ut^{-n}, t) = 0$.

Si $n = mp$, on pose $u = v^p$, d'où

$$ut^{-n} = \wp(vt^{-m}) + vt^{-m}, \qquad \text{et} \qquad [ut^{-n}, t) = [vt^{-m}, t) = 0$$

d'après l'hypothèse de récurrence.

(iii) $a = \sum_{n>0} a_n t^n$. On a $\mathrm{Res}\,(a\frac{dt}{t}) = 0$, et l'on voit vérifier que $[a, t) = 0$. Cela résulte de la formule $a = -\wp(a')$, avec

$$a' = a + a^p + a^{p^2} + \cdots$$

Remarque. La proposition précédente ramène le calcul de $[a, b)$ à celui de $[c, t)$, où c est une constante. Ce dernier calcul peut s'effectuer dans le cas général (cf. exer. 1) ; nous nous bornerons toutefois au cas du corps de classes local.

Supposons donc que k soit un corps *quasi-fini*. On peut alors transformer l'élément $[a, b)$ au moyen de l'isomorphisme $\mathrm{inv}_K : B_K \to \mathbf{Q}/\mathbf{Z}$. On trouve un élément $\mathrm{inv}\,[a, b)$ de $\frac{1}{p}\mathbf{Z}/\mathbf{Z}$. Nous poserons :

$$[a, b)_* = p.\mathrm{inv}\,[a, b).$$

C'est un élément de $\mathbf{Z}/p\mathbf{Z}$.

PROPOSITION 13. *Si* $\alpha \in K$, *est une racine de l'équation* $\wp(\alpha) = a$, *et si* $s_b = (b, {}^*/K)$, *on a* :

$$[a, b)_* = s_b(\alpha) - \alpha.$$

Cela résulte de la proposition 3.

PROPOSITION 14. (i) $[a + a', b)_v = [a, b)_v + [a', b)_v$.

(ii) $[a, bb')_v = [a, b)_v + [a, b')_v$.

(iii) *Pour que* $[a, b)_v = 0$, *il faut et il suffit que* b *soit une norme dans l'extension* $K(\alpha)/K$, *avec* $\wp(\alpha) = a$.

(iv) $[a, a)_v = 0$ *pour tout* $a \in K^*$.

(v) *Si* $[a, b)_v = 0$ *pour tout* $b \in K^*$, *on a* $a \in \wp(K)$.

Les propriétés (i) à (iv) résultent des propriétés correspondantes du symbole $[a, b)$, cf. prop. 11. La propriété (v) résulte du corollaire à la prop. 3.

Nous nous proposons maintenant de calculer explicitement $[a, b)_v$. Nous aurons besoin du résultat suivant, tout à fait analogue au lemme 2 :

LEMME 4. *Soit* k *un corps quasi-fini de caractéristique* $p \neq 0$. *Si* $x \in k$, *soit* $y \in k_s$ *tel que* $\wp(y) = x$, *et soit* $z = y^{p^f} - y$. *On a* $z \in \mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, *l'élément* z *ne dépend pas de* y, *et, si on le note* $S(x)$, *l'application* S *définit par passage au quotient un isomorphisme de* $k/\wp(k)$ *sur* $\mathbf{Z}/p\mathbf{Z}$.

Cela résulte de la théorie d'Artin-Schreier et du fait que k possède une extension cyclique de degré p et une seule.

Exemple. Si k est un *corps fini* à $q = p^f$ éléments, l'application S est donnée par la formule :

$$S(x) = x^{p^{f-1}} + x^{p^{f-2}} + \cdots + x^p + x = \mathrm{Tr}_{k/\mathbf{F}_p}(x).$$

On a en effet :

$$\begin{aligned} S(x) &= Fy - y = y^{p^f} - y \\ &= (y^{p^f} - y^{p^{f-1}}) + \cdots + (y^p - y) \\ &= x^{p^{f-1}} + \cdots + x^p + x = \mathrm{Tr}_{k/\mathbf{F}_p}(x). \end{aligned}$$

Revenons maintenant au calcul de $[a, b)_v$:

PROPOSITION 15. *Soit* $K = k((t))$, *où* k *est un corps quasi-fini de caractéristique* p. *Si* $a \in K$ *et* $b \in K^*$, *on a* :

$$[a, b)_v = S\left(\mathrm{Res}\left(a\frac{db}{b}\right)\right).$$

COROLLAIRE. *Si* k *est un corps fini, on a* $[a, b)_v = \mathrm{Tr}_{k/\mathbf{F}_p}\left(\mathrm{Res}\left(a\frac{db}{b}\right)\right)$.

Vu la proposition 12, on peut se borner au cas où a est une constante (i. e. un élément de k), et où $b = t$. On doit montrer que l'on a $[a, t)_v = S(a)$.

Soit k' une extension finie de k contenant une racine α de l'équation $\wp(\alpha) = a$, et soit $K' = k'((t))$. L'extension K'/K est non ramifiée, et la prop. 13 du Chap. XIII montre que $(t, K'/K) = F$, générateur canonique du groupe de Galois

$$G(K'/K) = G(k'/k).$$

D'après la prop. 13, on a :

$$[a, t)_v = F\alpha - \alpha = S(a), \qquad \text{c.q.f.d.}$$

PROPOSITION 16. *Soit* $K = k((t))$ *où* k *est un corps quasi-fini de caractéristique* p. *Si un élément* $b \in K^*$ *est une norme dans toute extension cyclique de* K *de degré* p, *on a* $b \in K^{*p}$.

L'hypothèse revient à dire que $[a, b)_v = 0$ pour tout $a \in K$. Si b n'était pas une puissance p-ième, la forme différentielle db/b ne serait pas identiquement nulle; pour toute constante c, on pourrait alors choisir a de telle sorte que $a\frac{db}{b} = c\frac{dt}{t}$; d'après la prop. 15, on aurait $S(c) = 0$, ce qui est absurde puisque $S : k/\wp(k) \to \mathbf{Z}/p\mathbf{Z}$ est surjectif.

Remarques. 1) La prop. 15 est due à H. Schmid [55]; on en trouvera une démonstration par voie « globale » dans [56], Chap. VI, n° 30.

2) Tous les résultats de ce paragraphe s'étendent aux caractères d'ordre une puissance de p donnés par les vecteurs de Witt; on est ainsi conduit à des symboles $[a, b)$ avec $a \in W_n(K)$, $b \in K^*$, cf. Witt [73].

Exercices. 1. Soit k un corps parfait de caractéristique p, soit $\mathfrak{g} = G(k_s/k)$, et soit $X(\mathfrak{g})$ le groupe des caractères de $\mathfrak{g}$. Soit $K = k((t))$. La composante p-primaire du groupe de Brauer de k est nulle (cf. Chap. X, § 4, exer. 1). Le th. 2 du Chap. XII montre alors que la composante p-primaire de B_K s'identifie à celle de $X(\mathfrak{i})$. Soit $c \in k$. Montrer que l'image de $[c, t)$ par cet isomorphisme est l'élément ψ_c de $X(\mathfrak{g})$ défini comme on l'a dit au début du §.

2. Soit k un corps de caractéristique p, soit $K = k((t))$, et soit $c \in k$, $c \notin k^p$. Montrer que $[t^{-1}, c)$ est un élément de B_K d'ordre p qui n'est décomposé par aucune extension non ramifiée de K.

§ 6. *Le théorème d'existence*

Nous nous plaçons maintenant dans le cadre *usuel* de la théorie du corps de classes local : K désigne un corps complet pour une valuation discrète v à corps résiduel *fini* (c'est donc un corps *localement compact*, cf. Chap. II, § 1).

THÉORÈME 1. *Tout sous-groupe fermé d'indice fini du groupe* K^* *est un groupe de normes* (au sens du Chap. XI, § 4).

(En d'autres termes, si H est un tel sous-groupe, il existe une extension abélienne finie L/K telle que $N_{L/K}(L^*) = H$; on sait d'ailleurs que, si une telle extension existe, elle est unique.)

Considérons la formation de classes du Chap. XIII, § 4. Nous allons montrer qu'elle vérifie les conditions du th. 2 du Chap. XI, § 5. Il y a trois axiomes à considérer.

III. 1. *Pour toute extension finie* F/E (E étant une extension finie de K), *l'application* $N_{F/E} : F^* \to E^*$ *est propre.*

En effet, tout compact de E est contenu dans un nombre fini de translatés du groupe des unités U_E, et $N_{F/E}^{-1}(U_E) = U_F$, qui est compact.

III. 2. *Pour tout nombre premier p, il existe un corps E_p tel que, si E contient E_p, l'application $x \to x^p$ de E^* dans lui-même a un noyau compact et une image qui contient les normes universelles.*

Si p est distinct de la caractéristique de K, on prend pour E_p le corps obtenu en adjoignant à K les racines p-ièmes de l'unité. Si E contient E_p, le noyau de $x \to x^p$ est cyclique d'ordre p, donc compact. Si $x \in E^*$ est une norme universelle, le corollaire à la prop. 7 montre que $x \in E^{*p}$.

Si p est égal à la caractéristique de K, on prend $E_p = K$. Le noyau de $x \to x^p$ est réduit à $\{1\}$. Si $x \in E^*$ est une norme universelle, la prop. 16 montre que $x \in E^{*p}$ et l'axiome III. 2 est bien vérifié.

III. 3. *Il existe un sous-groupe compact U_E de E^* tel que tout sous-groupe fermé d'indice fini de E^* contenant U_E soit un groupe de normes.*

On prend pour U_E le *groupe des unités* de E. Les sous-groupes d'indice fini de E^* contenant U_E sont les images réciproques par la valuation discrète v_E des sous-groupes $n\mathbf{Z}$ de $\mathbf{Z}$. La prop. 13 du Chap. XIII (ou bien la prop. 3 du Chap. V, au choix) montre que ces groupes sont groupes de normes pour les extensions non ramifiées de K, c.q.f.d.

COROLLAIRE 1. *Pour qu'un sous-groupe d'indice fini de K^* soit groupe de normes, il faut et il suffit qu'il contienne $U_K^{(n)}$, pour n assez grand.*

En effet, dire qu'un sous-groupe H de K^* contient un $U_K^{(n)}$ équivaut à dire que H est *ouvert*; si H est d'indice fini dans K^*, les conditions « H est ouvert » et « H est fermé » sont trivialement équivalentes.

Remarque. Pour un groupe de normes H donné, il existe évidemment un *plus petit entier* n tel que H contienne $U_K^{(n)}$; nous verrons au chapitre suivant comment cet entier se détermine à partir des groupes de ramification de l'extension correspondant à H.

COROLLAIRE 2. (i) *L'intersection des groupes de normes de K^* est réduite à $\{1\}$.*

(ii) *Si $\mathfrak{T}_K$ désigne le groupe d'inertie de l'extension K^a/K (cf.* Chap. XIII, § 3), *l'application de réciprocité $U_K \to \mathfrak{T}_K$ est un isomorphisme de groupes topologiques.*

(iii) *Le groupe $\mathfrak{A}_K = G(K^a/K)$ est extension de $\hat{\mathbf{Z}}$ par U_K.*

Soit π une uniformisante de K; si m et n sont deux entiers $\geqslant 1$, soit $V_{m,n}$ le sous-groupe de K^* engendré par π^m et $U_K^{(n)}$. Ces sous-groupes sont fermés, d'indice fini, et leur intersection est réduite à $\{1\}$; comme, d'après le théorème 1, ce sont des groupes de normes, on en déduit (i). Pour (ii), il suffit de remarquer que la topologie de U_K est définie par ses sous-groupes fermés d'indice fini, et que U_K est *compact* pour cette topologie. Enfin (iii) résulte de (ii), puisque $\mathfrak{A}_K/\mathfrak{T}_K = \hat{\mathbf{Z}}$.

(On peut dire, de façon quelque peu imprécise, que $\mathfrak{A}_K$ s'obtient à partir de K^* en remplaçant le facteur direct $\mathbf{Z}$ par son complété $\hat{\mathbf{Z}}$.)

Remarques. 1) Lorsque K est de caractéristique zéro, tout sous-groupe d'indice fini de K^* est fermé (cf. § 4, exer. 2); il n'en est plus de même lorsque K est de caractéristique $p \neq 0$ (*idem*).

2) On peut présenter le th. 1 de façon plus frappante en procédant comme le le fait Weil [67] pour les corps de fonctions :

Soit K^a l'extension abélienne maximale de K, qui contient K_{nr}. Soit $\mathfrak{A}_K^0$ le sous-groupe de $\mathfrak{A}_K = G(K^a/K)$ formé des éléments de $\mathfrak{A}_K$ qui induisent sur K_{nr} une puissance *entière* de la substitution de Frobenius F. On a $\mathfrak{T}_K \subset \mathfrak{A}_K^0$ et $\mathfrak{A}_K^0/\mathfrak{T}_K = \mathbf{Z}$; on topologise $\mathfrak{A}_K^0$ en considérant $\mathfrak{T}_K$ comme un sous-groupe *ouvert* de $\mathfrak{A}_K^0$. Ceci étant, *l'application de réciprocité* $x \to (x, */K)$ *définit un isomorphisme du groupe topologique* K^* *sur le « groupe de Galois modifié »* $\mathfrak{A}_K^0$.

3) Soit K un corps complet pour une valuation discrète à corps résiduel *quasi-fini* $\overline{K}$. Le th. 1 est encore valable pour les sous-groupes de K^* d'indice fini premier à la caractéristique de $\overline{K}$, cf. exer. 2, mais il ne l'est plus pour ceux dont l'indice est une puissance de cette caractéristique ; cf. Whaples [71], où l'on trouvera diverses caractérisations des groupes de normes, reposant essentiellement sur la structure de « groupe proalgébrique » du groupe des unités de K; voir aussi Chap. XV, § 1, exer. 2.

Exercices. 1. Soit K' une extension finie de K; montrer que l'application naturelle $\mathfrak{A}_{K'} \to \mathfrak{A}_K$ et le transfert $\mathfrak{A}_K \to \mathfrak{A}_{K'}$ appliquent l'un dans l'autre les sous-groupes $\mathfrak{A}_K^0$ et $\mathfrak{A}_{K'}^0$. Expliciter les props. 10, 11, 12, 13 du Chap. XIII au moyen de l'isomorphisme $K^* \to \mathfrak{A}_K^0$.

2. Soit K un corps complet pour une valuation discrète à corps résiduel $\overline{K}$ quasi-fini. Soit H un sous-groupe d'indice fini de K^*, et soit $n = (U_K : H \cap U_K)$. On suppose que n est premier à la caractéristique de $\overline{K}$.

a) Montrer que H contient $U_K^{(1)}$. Le groupe $H \cap U_K$ est donc image réciproque d'un sous-groupe $\overline{H}$ d'indice n de K^*.

b) En utilisant l'exer 1. du § 1 du Chap. XV, montrer que $\overline{H} = \overline{K}^{*n}$, que K et $\overline{K}$ contiennent les racines n-ièmes de l'unité, et que H est groupe de normes d'une extension abélienne de K.

§ 7. *Exemple : extension abélienne maximale de* $\mathbf{Q}_p$.

THÉORÈME 2. *Soit p un nombre premier, et soit* E *le corps obtenu en adjoignant toutes les racines de l'unité à* $\mathbf{Q}_p$. *Le corps* E *est l'extension abélienne maximale de* $\mathbf{Q}_p$.

Posons $K = \mathbf{Q}_p$, et soit K^a l'extension abélienne maximale de K. On a évidemment $E \subset K^a$. Nous avons vu au Chap. IV, § 4 que E est composée des extensions linéairement disjointes K_{nr} et K_{p^∞}, dont nous avons déterminé les groupes de Galois sur K. On a :

$$K^a \supset E \supset K_{nr}$$

d'où un homomorphisme surjectif $\pi : G(K^a/K_{nr}) \to G(E/K_{nr})$. D'après le corollaire 2 au théorème 1, $G(K^a/K_{nr})$ est isomorphe au groupe U_p des unités de $\mathbf{Q}_p$; il en est

de même de $G(E/K_{nr}) = G(K_{p^\infty}/K)$ d'après la remarque 1) du Chap. IV, § 4. L'homomorphisme π peut donc être considéré comme un *endomorphisme surjectif* de U_p. Mais U_p est un $\hat{\mathbf{Z}}$-module isomorphe au produit d'un groupe fini par $\mathbf{Z}_p$, cf. § 4; en particulier, c'est un $\hat{\mathbf{Z}}$-module noethérien. Or tout endomorphisme surjectif d'un module noethérien est bijectif (Bourbaki, *Alg.*, Chap. VIII, § 2, lemme 3). Donc π est bijectif, ce qui entraîne $E = K^a$, c.q.f.d.

Remarques. 1) On a en fait $\pi(x) = x^{-1}$. C'est immédiat par voie globale en utilisant la loi de réciprocité d'Artin (cf. Annexe) et Dwork [21] en a donné une démonstration « locale ».

2) Le th. 2, ainsi que la formule $\pi(x) = x^{-1}$, est un cas particulier d'un théorème général de Lubin-Tate [98] donnant une description explicite de K^a pour toute extension finie K de $\mathbf{Q}_p$; les racines de l'unité d'ordre une puissance de p sont alors remplacées par les « points d'ordre fini » d'un certain groupe formel associé à K (cf. [98], ainsi que [75], p. 146-155).

Exercice. Montrer que p est une norme dans chacune des extensions K_{p^n}/K. En déduire que $(p, K_{p^\infty}/K) = 1$.

ANNEXE

Cas global (énoncé de résultats)

Soit K un *corps de nombres algébriques*, c'est-à-dire une extension finie de $\mathbf{Q}$. A toute valeur absolue v de K on associe le complété K_v de K pour la topologie définie par v. Ces corps sont de deux sortes : pour v ultramétrique, K_v est un corps du type considéré au paragraphe précédent, pour v non ultramétrique K_v est isomorphe à $\mathbf{R}$ ou $\mathbf{C}$. On notera que la théorie du corps de classes local s'applique (trivialement !) à $\mathbf{R}$ et $\mathbf{C}$; en particulier, on a un « isomorphisme de réciprocité »

$$f : \mathbf{R}^*/N(\mathbf{C}^*) \to G(\mathbf{C}/\mathbf{R})$$

qui se définit de façon évidente.

Un *idèle* de K est, par définition, une famille $\{x_v\}$, avec $x_v \in K_v^*$ pour tout v, et x_v étant une unité pour presque tout v. Les idèles forment un groupe I_K pour la multiplication; le groupe multiplicatif K^* se plonge de façon naturelle dans I_K.

Soit maintenant L/K une extension abélienne finie, de groupe de Galois G. Pour toute valeur absolue v de K, choisissons une valeur absolue w de L prolongeant v. Le groupe de décomposition D_v de w ne dépend pas du choix de w; c'est le groupe de Galois de l'extension locale L_w/K_v. On a donc pour tout v (y compris les valeurs absolues non ultramétriques) un isomorphisme de réciprocité :

$$f_v : K_v^*/NL_w^* \to D_v.$$

Si $x = \{x_v\}$ est un idèle de K, les $f_v(x_v)$ sont presque tous égaux à 1. En effet, presque toutes les extensions locales L_w/K_v sont non ramifiées, et presque tous les x_v sont des unités : notre assertion résulte de la prop. 13 du chap. 13. On peut donc multiplier les $f_v(x_v)$, et définir une « application de réciprocité » globale

$$f : I_K \to G.$$

La loi de réciprocité d'Artin s'exprime ainsi :

THÉORÈME. *L'application f est surjective, et son noyau est engendré par* K^* *et* $N_{L/K}(I_L)$.

Pour la démonstration, voir Artin-Tate [8], Chap. VII, § 3. L'un des points essentiels est le fait que K^* est contenu dans le noyau de f; ce ne serait plus vrai si l'on changeait le choix des substitutions de Frobenius dans les corps locaux K_v.

Le théorème ci-dessus contient comme cas particulier celui que nous avions appelé « loi de réciprocité » au Chap. I, § 8. De façon plus précise, soient v_i les valuations discrètes de K qui sont ramifiées dans L. Dans l'extension locale L_{w_i}/K_{v_i}, le groupe de normes N_i est un sous-groupe ouvert de $K_{v_i}^*$, et il existe donc un entier n_i tel que $v_i(x-1) \geqslant n_i$ entraîne $x \in N_i$, cf. cor. 1 au th. 1. Considérons alors un élément $x \in K^*$ vérifiant les deux conditions suivantes :

(i) $v_i(x-1) \geqslant n_i$ *pour tout* i.

(ii) x *est* > 0 *dans tout plongement réel de* K *qui n'est pas induit par un plongement réel de* L.

Soit $\mathfrak{a} = (x)$ l'idéal principal engendré par x. Alors *le symbole d'Artin* $(\mathfrak{a}, L/K)$ *est égal à* 1, ce qui précise l'énoncé du Chap. I (en indiquant comment on doit choisir les n_i).

La démonstration est immédiate : on écrit que $f(x) = \prod_v f_v(x)$ est égal à 1. Les termes correspondant aux v_i et aux valuations non ultramétriques sont triviaux, à cause des conditions (i) et (ii). Les autres se calculent au moyen de la prop. 13 du Chap. XIII, et donnent comme produit $(\mathfrak{a}, L/K)$, d'où le résultat.

Autre application : Supposons que K contienne les racines n-ièmes de l'unité, et soient $a, b \in K^*$. Soit $L = K(a^{1/n})$. En appliquant à $b \in K^*$ la formule $f(b) = 1$, on trouve la relation :

$$(*) \qquad \prod_v (a, b)_v = 1.$$

[Lorsque $K_v = \mathbf{R}$, ce qui ne peut se produire que si $n = 2$, le symbole $(a, b)_v$ correspondant est égal à -1 si a et b sont négatifs, à $+1$ sinon.]

Exemple : Prenons $K = \mathbf{Q}$, $n = 2$, et choisissons pour a et b des nombres premiers $\neq 2$ distincts. D'après le § 5, on a :

$$(a, b)_a = \left(\frac{b}{a}\right), \qquad (a, b)_b = \left(\frac{a}{b}\right), \qquad (a, b)_2 = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}},$$

et les autres $(a, b)_v$ sont égaux à 1. La formule $(*)$ redonne la *loi de réciprocité quadratique* :

$$\left(\frac{a}{b}\right)\cdot\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}.$$

Pour d'autres exemples, voir Artin-Tate [8], Chap. XII, § 4, Cassels-Fröhlich [75] ainsi que Hasse [31].

CHAPITRE XV

RAMIFICATION

Soit K un corps complet pour une valuation discrète de corps résiduel K quasi-fini. Soit L/K une extension abélienne finie, de groupe de Galois G. On a défini au Chap. XIII, § 4 l'isomorphisme de réciprocité

$$\omega : K^*/NL^* \to G.$$

Le but du présent chapitre est de déterminer les relations existant entre ω et la filtration de G donnée par les groupes de ramification; nous verrons en particulier que l'image de U_K^n par ω est égale à G^n (cf. § 2).

§ 1. *Noyau et conoyau d'un polynôme additif (resp. multiplicatif)*

Dans tout ce paragraphe, k désigne un corps *quasi-fini*.

Soit P un *polynôme additif* non constant, à coefficients dans k (cf. Chap. V, § 5). Si k_s désigne la clôture algébrique de k, l'homomorphisme $P : k_s \to k_s$ est surjectif.

PROPOSITION 1. *Soit* N *le noyau de* P *dans* k_s. *Si* $x \in k$, *choisissons* $y \in k_s$ *tel que* $P(y) = x$, *et soit* $z = Fy - y$. *On a* $z \in N$, *et l'image* $\bar{z}$ *de* z *dans* $N/(F-1)N$ *ne dépend pas du choix de* y. *Si on la note* $\delta_p(x)$, *l'application* δ_p *définit par passage au quotient un isomorphisme de* $k/P(k)$ *sur* $N/(F-1)N$.

Changer y revient à le remplacer par $y + t$, avec $t \in N$, et z est alors remplacé par $z + (Ft - t)$; cela montre bien que $\bar{z}$ ne dépend pas du choix de y. On voit tout de suite que $\delta_p(x) = 0$ si et seulement si $x = P(y)$, avec $y \in k$. Reste à voir que

$$\delta_p : k/P(k) \to N/(F-1)N$$

est surjectif. Si k est de caractéristique zéro, c'est trivial : P est de la forme aX, $a \in k^*$, et $N = 0$. Si k est de caractéristique p, soit $z \in N$; d'après la prop. 4 du Chap. XIII, il existe $y \in k_s$ tel que $Fy - y = z$. Si l'on pose $x = P(y)$, on a

$$Fx - x = P(Fy - y) = P(z) = 0$$

d'où $x \in k$, et il est clair que $\delta_p(x) = \bar{z}$, e.q.f.d.

[*Variante.* Soit $\mathfrak{g} = G(k_s/k)$. On applique la suite exacte de cohomologie à la suite exacte de $\mathfrak{g}$-modules

$$0 \to N \to k_s \xrightarrow{P} k_s \to 0.$$

On obtient la suite exacte :

$$k \xrightarrow{P} k \to H^1(\mathfrak{g}, N) \to 0$$

et comme $H^1(\mathfrak{g}, N) = N/(F - 1)N$, on obtient bien la prop. 1.]

COROLLAIRE 1. *Si tout élément de* N *appartient à* k, *l'application* δ_p *est un isomorphisme de* $k/P(k)$ *sur* N.

En effet, on a alors $Fz = z$ pour tout $z \in N$.

COROLLAIRE 2. *L'ordre de* $k/P(k)$ *est fini, c'est un diviseur du degré séparable* $d_s(P)$ *de* P, *et il lui est égal si et seulement si* N *est contenu dans* k.

En effet, on sait que l'ordre de N est égal à $d_s(P)$, cf. Chap. V, § 5.

COROLLAIRE 3. *Le noyau et le conoyau de* $P : k \to k$ *sont des groupes finis équipotents.*

Soit N_k le noyau de $P : k \to k$, c'est-à-dire l'intersection de N avec k. On a la suite exacte :

$$0 \to N_k \to N \xrightarrow{F-1} N \to N/(F - 1)N \to 0.$$

Comme N est fini, il en résulte que N_k et $N/(F - 1)N$ sont équipotents, d'où le résultat.

Exemples. 1) Plaçons-nous en caractéristique $p \neq 0$, et prenons pour P le polynôme $\wp(X) = X^p - X$. On a $N = \mathbf{Z}/p\mathbf{Z}$, et l'isomorphisme $\delta_\wp : k/\wp(k) \to \mathbf{Z}/p\mathbf{Z}$ n'est autre que l'isomorphisme S du Chap. XIV, § 5.

2) Prenons plus généralement $P = aX^p + bX$, $a, b \in k^*$. Si P n'a pas de zéro non trivial dans k, on a $N/(F - 1)N = 0$, d'où $k = P(k)$. Si P a un zéro non trivial, soit c, l'équation $P(y) = x$ s'écrit :

$$ac^p(y^p/c^p) + bc(y/c) = x,$$

ou encore :

$$(y/c)^p - y/c = a^{-1}c^{-p}x.$$

On a donc :

$$P(x) = Fy - y = c.(F(y/c) - y/c) = c.S(a^{-1}c^{-p}x) = -c.S(b^{-1}c^{-1}x)$$

ce qui ramène le calcul de δ_p à celui de S.

Passons maintenant au cas multiplicatif :

PROPOSITION 2. *Soit* $P = X^n$, *avec* $n \geqslant 1$, *et soit* N *le noyau de* $P : k_s^* \to k_s^*$. *Si* $x \in k$, *choisissons* $y \in k_s^*$ *tel que* $P(y) = x$, *et soit* $z = y^{F-1}$. *On a* $z \in N$, *et l'image* $\bar{z}$ *de* z *dans* N/N^{F-1} *ne dépend pas du choix de* y. *Si on la note* $\delta_p(x)$, *l'application* δ_p *définit par passage au quotient un isomorphisme de* $k^*/P(k^*)$ *sur* N/N^{F-1}.

(Pour respecter l'analogie avec le cas additif, on a utilisé la notation exponentielle : $y^F = F(y)$.)

La démonstration est la même que celle de la prop. 1.

COROLLAIRE 1. *Si tout élément de* N *appartient à* k^*, *l'application* δ_p *est un isomorphisme de* $k^*/P(k^*)$ *sur* N.

COROLLAIRE 2. *L'ordre de* $k^*/P(k^*)$ *est fini, c'est un diviseur du degré séparable* $d_s(P)$ *de* P, *et il lui est égal si et seulement si* N *est contenu dans* k^*.

COROLLAIRE 3. *Le noyau et le conoyau de* $P : k^* \to k^*$ *sont des groupes finis équipotents.*

Les démonstrations sont les mêmes que pour les corollaires correspondants du cas additif.

Exemple. Supposons que n soit premier à la caractéristique de k, et que k^* contienne le groupe E_n des racines n-ièmes de l'unité. On a $N = E_n$, et l'isomorphisme $\delta_p : k^*/k^{*n} \to E_n$ n'est autre que l'isomorphisme P_n du Chap. XIV, § 3.

Exercices. 1. Soit k un corps quasi-fini.

a) Soit m un entier $\geqslant 1$, et premier à la caractéristique de k. Soit E_m le groupe des racines m-ièmes de l'unité dans k_s^*. Montrer qu'il existe un diviseur n de m et un seul tel que $E_m \cap k^* = E_n$. Montrer que $k^{*m} = k^{*n}$, et en déduire que k^*/k^{*m} est cyclique d'ordre n.

b) Soit H un sous-groupe de k^* d'indice fini m. Montrer que m est premier à p. Si n est l'entier défini dans (*a*), montrer que $m = n$ et $H = k^{*n}$ (noter que H contient k^{*m}).

c) Déduire de (*b*) que les sous-groupes d'indice fini de k^* sont les sous-groupes k^{*n}, où n parcourt l'ensemble des entiers premiers à la caractéristique de k, et tels que $E_n \subset k^*$.

2. Soit k un corps quasi-fini, et soit A un k-groupe algébrique commutatif (sans éléments nilpotents), linéaire, et absolument irréductible (c'est donc le produit d'un groupe de type multiplicatif par un groupe unipotent). On note A_k (resp. A_{k_s}) le groupe des points de A rationnels sur k (resp. sur k_s).

a) Soit $\mathfrak{g} = G(k_s/k)$. Montrer que $H^q(\mathfrak{g}, A_{k_s}) = 0$ pour tout $q \geqslant 1$.

b) Soit A′ un k-groupe algébrique vérifiant les mêmes hypothèses que A, et de même dimension. Soit $P : A' \to A$ un homomorphisme de noyau fini N. Définir un isomorphisme

$$\delta_P : A_k/P(A'_k) \to N/(F - 1)N$$

par le procédé des propositions 1 et 2. Généraliser les corollaires 1, 2, 3.

c) Un sous-groupe de A_k est dit *normique* s'il est de la forme $P(A'_k)$, pour un homomorphisme $P : A' \to A$ convenable. Montrer que l'intersection de deux sous-groupes normiques est normique, et que tout sous-groupe contenant un sous-groupe normique est normique.

d) Lorsque k est un corps *fini*, montrer que l'hypothèse « A est linéaire » est superflue, et que tout sous-groupe de A_k est normique (cf. Lang [39]). Donner un exemple montrant qu'il n'en est plus ainsi dans le cas général.

[Les sous-groupes normiques interviennent dans le *théorème d'existence* de Whaples [71] : si K est complet pour une valuation discrète à corps résiduel $\overline{K}$ quasi-fini, un sous-groupe H d'indice fini de K* est groupe de normes si et seulement si il contient U_K^n pour n assez grand, et si l'image de $H \cap U_K$ dans U_K/U_K^n est un sous-groupe normique de U_K/U_K^n (ce dernier étant considéré comme l'ensemble des points rationnels sur $\overline{K}$ du groupe algébrique $U_{K_n}/U_{K_n}^n$, cf. Greenberg [25]).]

§ 2. *Les groupes de normes*

Nous supposons à partir de maintenant que K est un corps complet pour une valuation discrète de corps résiduel $\overline{K}$ quasi-fini.

Soit L/K une extension galoisienne *totalement ramifiée*, de groupe de Galois G. On voit tout de suite que U_K/NU_L s'identifie à K^*/NL^*. Nous allons étudier la filtration de U_K/NU_L définie par les images des U_K^n.

D'après la prop. 9 du Chap. VI, on a une suite exacte :

$$0 \to G_{\psi(n)}/G_{\psi(n)+1} \to U_L^{\psi(n)}/U_L^{\psi(n)+1} \xrightarrow{N_n} U_K^n/U_K^{n+1}$$

où N_n est défini par un polynôme additif (resp. multiplicatif) si $n \geqslant 1$ (resp. si $n = 0$). Le degré séparable de ce polynôme est égal à $(G_{\psi(n)} : G_{\psi(n)+1})$, ce qui permet de lui appliquer le cor. 1 à la prop. 1 (resp. à la prop. 2). On obtient ainsi :

PROPOSITION 3. *Le groupe* $U_K^n/U_K^{n+1}NU_L^{\psi(n)}$ *est isomorphe au groupe* $G_{\psi(n)}/G_{\psi(n)+1}$.

Posons $h_n = (G_{\psi(n)} : G_{\psi(n)+1})$.

COROLLAIRE 1. *On a* $(U_K^n : U_K^{n+1}NU_L^{\psi(n)}) = h_n$.

C'est clair.

COROLLAIRE 2. *Le groupe* $NU_L^{\psi(n)}$ *est un sous-groupe d'indice fini de* U_K^n. *Si* v_n *désigne cet indice, on a* $v_n = 1$ *pour n assez grand; de plus,* v_n *divise* $v_{n+1}h_n$, *l'égalité ayant lieu si et seulement si l'homomorphisme canonique* :

$$(*_n) \qquad U_K^{n+1}/NU_L^{\psi(n+1)} \to U_K^n/NU_L^{\psi(n)}$$

est injectif.

On sait que $U_K^n = NU_L^{\psi(n)}$ si n est assez grand (cf. Chap. V, § 6, cor. 3 à la prop. 9). D'autre part, on a la suite exacte :

$$U_K^{n+1}/NU_L^{\psi(n+1)} \to U_K^n/NU_L^{\psi(n)} \to U_K^n/U_K^{n+1}NU_L^{\psi(n)} \to 0$$

Cette suite exacte montre que, si v_{n+1} est fini, il en est de même de v_n, et que v_n divise $v_{n+1}h_n$; le quotient $v_{n+1}h_n/v_n$ est égal à l'ordre du noyau de l'homomorphisme $(*_n)$, d'où le corollaire.

COROLLAIRE 3. *L'entier* $v_0 = (U_K : NU_L) = (K^* : NL^*)$ *est un diviseur du produit des* h_n.

En effet, v_0 divise $v_1 h_0$, qui divise $v_2 h_1 h_0$, ..., qui divise $v_n h_{n-1} \dots h_0$. En prenant n assez grand pour que $v_n = 1$, on obtient le résultat eherché.

Remarque. Comme le produit des h_n divise $[L : K]$, on retrouve le fait que $(K^* : NL^*)$ divise $[L : K]$, cf. Chap. XIII, prop. 9.

THÉORÈME 1. *Supposons* G *abélien. Alors :*

a) On a $G_m = G_{m+1}$ *si* $\varphi(m)$ *n'est pas entier.*

b) On a $v_n = v_{n+1} h_n$ *pour tout* n.

c) L'application canonique de $U_K^n/NU_L^{\psi(n)}$ *dans* K^*/NL^* *est injective.*

D'après la prop. 9 du Chap. XIII, on a $v_0 = [L : K]$, ou, ce qui revient au même :

$$v_0 = \prod_{m=0}^{\infty} (G_m : G_{m+1}).$$

Mais d'autre part, le eor. 3 à la prop. 3 montre que v_0 divise le produit $\prod (G_{\psi(n)} : G_{\psi(n)+1})$. Il s'ensuit que $(G_m : G_{m+1}) = 1$ si m est pas de la forme $\psi(n)$, c'est-à-dire si $\varphi(m)$ n'est pas entier, d'où (a). De même, si v_n divisait strictement $v_{n+1} h_n$ pour un entier n, v_0 diviserait strictement le produit des h_n, ee qui est impossible; d'où (b). D'après le cor. 2 à la prop. 3, les homomorphismes

$$(*_n) : U_K^{n+1}/U_L^{\psi(n+1)} \to U_K^n/NU_L^{\psi(n)}$$

sont tous injectifs. En les composant, on voit que

$$U_K^{n+1}/NU_L^{\psi(n+1)} \to U_K/NU_L$$

est injectif, d'où (c) puisque $U_K/NU_L = K^*/NL^*$.

Remarque. L'assertion (a) n'est autre que le théorème de Hasse-Arf, dont on obtient ainsi une seconde démonstration (valable seulement lorsque le eorps résiduel est quasi-fini).

COROLLAIRE 1. *Les groupes* $U_K^n/NU_L^{\psi(n)}$ *forment une filtration décroissante de* K^*/NL^*. *On a* $U_K^n/NU_L^{\psi(n)} = 0$ *si et seulement si* $G^n = \{1\}$.

La première assertion ne fait que reformuler (c). Pour la seconde, on remarque que $v_n = 1$ équivaut à $h_n = h_{n+1} = \dots = 1$, c'est-à-dire $G^n = G^{n+1} = \dots = \{1\}$.

COROLLAIRE 2. *Soit* c *le plus grand entier tel que* $G_c \neq \{1\}$, *et soit* $f = \varphi(c) + 1$. *On a alors* $U_K^f \subset NL^*$, *et* f *est le plus petit entier jouissant de cette propriété.*

[L'idéal $\mathfrak{p}_K^f$ s'appelle le *conducteur* de l'extension L/K; lorsque L/K est l'extension cyclique définie par un caractère χ de degré 1 de $G(K_s/K)$, le eor. à la prop. 6 du Chap. VI montre que $\mathfrak{p}_K^f$ coïncide avec le *conducteur d'Artin* $\mathfrak{f}(\chi)$ de χ.]

On sait que U_K^f est eontenu dans NL^*, cf. Chap. V, § 6, cor. 3 à la prop. 9.

D'autre part, le corollaire 1 montre que U_K^{f-1} n'est pas contenu dans NL^*, puisque $G^{f-1} = G_0$ est non trivial.

COROLLAIRE 3. *L'application de réciprocité* $\omega : K^*/NL^* \to G$ *transforme la filtration des* $U_K^n/NU_L^{\psi(n)}$ *en la filtration des* G^n.

Il suffit de montrer que, pour tout sous-groupe H de G, les relations :

$$\omega(U_K^n) \subset H \qquad \text{et} \qquad G^n \subset H$$

sont équivalentes. Passant au quotient par H, cela revient à dire que $\omega(U_K^n) = \{1\}$ équivaut à $G^n = \{1\}$. Or, d'après le cor. 2, la première relation équivaut à $n \geqslant f$; la seconde relation signifie que $G_{\psi(n)} = \{1\}$, c'est-à-dire $\psi(n) > c$, ou encore

$$n \geqslant \varphi(c) + 1 = f, \qquad \text{c.q.f.d.}$$

THÉORÈME 2. *Soit* L/K *une extension abélienne, de groupe de Galois* G. *L'image de* U_K^n *par l'application de réciprocité* $\omega : K^* \to G$ *est dense dans* G^n.

Vu la définition de G^n, cela revient à dire que $\omega(U_K^n) = G^n$ lorsque L/K est finie. Soit alors T le groupe d'inertie de G, et K'/K l'extension abélienne correspondante. Notons ω' l'application de réciprocité dans l'extension L/K'. D'après le cor. 3 au th. 1, on a

$$\omega'(U_{K'}^n) = T^n = G^n.$$

D'autre part, on a $\omega \circ N_{K'/K} = \omega'$ (Chap. XIII, prop. 10), et $N_{K'/K}(U_{K'}^n) = U_K^n$ (Chap. V, prop. 3). On en déduit bien $\omega(U_K^n) = G^n$, c.q.f.d.

Remarque. Dans le cas « usuel » où K est *fini*, on a $\omega(U_K^n) = G^n$ puisque U_K^n est compact.

§ 3. *Calculs explicites*

Revenons à la situation du théorème 1. Soit donc L/K une extension abélienne finie, totalement ramifiée, de groupe de Galois G. On a vu (cor. 3 au th. 1) que l'isomorphisme de réciprocité

$$\omega : K^*/NL^* \to G$$

transforme les sous-groupes $U_K^n/NU_L^{\psi(n)}$ de K^*/NL^* en les groupes de ramification G^n de G. Par passage au quotient, on en déduit des isomorphismes

$$\omega_n : U_K^n/U_K^{n+1}NU_L^{\psi(n)} \to G^n/G^{n+1}.$$

D'autre part, on a vu que l'homomorphisme

$$N_n : U_L^{\psi(n)}/U_L^{\psi(n)+1} \to U_K^n/U_K^{n+1}$$

est induit par un polynôme additif (resp. multiplicatif si $n \geqslant 1$ (resp. si $n = 0$), polynôme que l'on peut en outre déterminer canoniquement (c'est-à-dire de telle

sorte qu'il soit invariant par extension résiduelle, cf. Chap. V, § 6, remarque 2). A ce polynôme est associé par le procédé du § 1 un isomorphisme

$$\delta_n : U_K^n/U_K^{n+1}NU_L^{\psi(n)} \to G_{\psi(n)}/G_{\psi(n)+1}$$

cf. prop. 3. On a $G_{\psi(n)} = G^n$, et le théorème de Hasse-Arf montre que $G_{\psi(n)+1} = G^{n+1}$. Ainsi, ψ_n *et* δ_n *appliquent tous deux* $U_K^n/U_K^{n+1}NU_L^{\psi(n)}$ *dans* G^n/G^{n+1}. Il s'impose de les comparer :

PROPOSITION 4. *On a* $\omega_n(\alpha) = \delta_n(\alpha^{-1})$ *pour tout* $\alpha \in U_K^n/U_K^{n+1}NU_L^{\psi(n)}$.

Posons $L_0 = \hat{L}_{nr}$, $K_0 = \hat{K}_{nr}$, cf. Chap. XIII, § 5, Commençons par expliciter le calcul de $\delta_n(\alpha)$. Vu les définitions du § 1, on doit choisir un élément $\beta \in U_{L_0}^{\psi(n)}/U_{L_0}^{\psi(n)+1}$ tel que $N_n(\beta) = \alpha$, former $\zeta = \beta^{F-1}$, qui est un élément du noyau de N_n, et est donc de la forme π^{s-1} mod. $U_{L_0}^{\psi(n)+1}$, avec $s \in G^n$, π étant une uniformisante de L; on a alors $\delta_n(\alpha) \equiv s$ mod. G^{n+1}. De façon encore plus explicite, choisissons un représentant $x \in U_K^n$ de α, et un $y \in U_{L_0}^{\psi(n)}$ tel que $Ny = x$ (c'est possible, cf. Chap. V, § 6, cor. 3 à la prop. 9). Posons $z = y^{F-1}$; on a $z = \pi^{s-1}z'$, avec $s \in G^n$ et $z' \in U_{L_0}^{\psi(n)+1}$ et

$$\delta_n(\alpha) \equiv s \text{ mod. } G^{n+1}.$$

Distinguons maintenant deux cas :

a) *La caractéristique de* K *est différente de zéro.*

D'après la prop. 15 du Chap. XIII, il existe $y' \in U_{L_0}^{\psi(n)+1}$ tel que $z' = y'^{F-1}$. On en déduit $(yy'^{-1})^{F-1} = \pi^{s-1}$. Si $x' = Ny'$, on a $(xx'^{-1})^{F-1} = 1$, d'où $xx'^{-1} \in K^*$ et $x' \in K^*$. En outre, le théorème de Dwork (Chap. XIII, § 5, cor. au th. 2) montre que $\omega(xx'^{-1}) = s^{-1}$. Comme x' appartient à $U_K^{n+1} \cap K^* = U_K^{n+1}$, on a $\omega(x') \in G^{n+1}$, et $\omega(x) \equiv s^{-1}$ mod. G^{n+1}, ce qui démontre la proposition dans ee cas.

b) *La caractéristique de* K *est égale à zéro.*

On a $G^n = \{1\}$ si $n \geqslant 1$, et l'on peut donc supposer que $n = 0$. De plus, le groupe G est cyclique, et si r est son ordre, le corps K contient le groupe des racines r-ièmes de l'unité, cf. Chap. IV, § 2. On peut choisir pour x et y des *représentants multiplicatifs* (cf. Chap. II, § 4); l'élément $z = y^{F-1}$ est alors une racine r-ième de l'unité, et l'on montre facilement qu'elle peut se mettre sous la forme π^{s-1}, où π est une uniformisante de L et s un élément de G eonvenablement choisis. On applique ensuite le théorème de Dwork comme dans le cas *a*).

La proposition précédente ramène le calcul de ω_n à eelui de δ_n, c'est-à-dire en définitive à celui de N_n. Donnons-en un exemple :

PROPOSITION 5. *Soit* L/K *une extension cyclique, totalement ramifiée, de degré premier p égal à la caractéristique de* K; *soit* G *son groupe de Galois, et soit s un générateur de* G; *soit t le plus grand entier tel que* $G_t \neq \{1\}$. *Soit* π *une uniformisante de* L, *et posons* $M = s(\pi)/\pi - 1$. *Soit* $x \in U_K^t$, *et soit* $c(x) = \dfrac{x-1}{\mathrm{Tr}(M)}$. *Alors* $c(x)$ *appartient à l'anneau de valuation de* K, *et, si* $\bar{c}(x)$ *désigne son image dans* K, *on a* :

$$(x, L/K) = s^{\mathrm{s}(\bar{c}(x))}.$$

[Pour la définition de $S : K \to \mathbf{Z}/p\mathbf{Z}$, voir Chap. XIV, § 4.]

Soit π' un élément de K tel que $v_K(\pi') = t$. On a alors $\mathrm{Tr}(M) = b\pi'$, $N(M) = a\pi'$ avec $a, b \in U_K$, cf. Chap. V, § 3. Si l'on pose $y = 1 + \eta M$, avec $\eta \in A_L$, on a :

$$N(y) \equiv 1 + (a\eta^p + b\eta)\pi' \mod U_K^{t+1}, \qquad \text{cf. Chap. V, § 3.}$$

L'application N_t se représente donc par le polynôme additif $P_t(\eta) = \bar{a}\eta^p + \bar{b}\eta$, et puisque $N(\pi^{t-1}) = 1$, $\eta = 1$ est un élément du noyau de P_t. D'après l'exemple 2 du § 1, $\delta_{P_t}(\bar{\xi})$ est égal à $-S(\bar{b}^{-1}\bar{\xi})$. Si $x = 1 + \xi\pi'$, $\delta_t(x)$ est donc égal à s^{-m}, avec $m = -S(\bar{b}^{-1}\bar{\xi}) = -\bar{c}(x)$, d'où le résultat, compte tenu de la proposition 4.

La proposition 5 peut elle-même servir à calculer certains symboles locaux $(a, b)_v$. Nous nous bornerons à en donner un exemple :

PROPOSITION 6. *Supposons que* K (*resp.* K) *soit de caractéristique zéro* (*resp.* p), *et que* K *contienne le groupe* E_p *des racines* p*-ièmes de l'unité. Soit* w *un générateur de ce groupe. Soit* $e = v_K(p)$ *l'indice de ramification absolu de* K, *et soit* $t = ep/(p-1)$; *c'est un entier. Si* $a \in K^*$ *et* $b \in U_K^t$, *on a :*

$$(a, b)_v = w^{v_K(a)\cdot m(b)}, \qquad \text{avec} \qquad m(b) = S\left(\frac{b-1}{p(w-1)}\right).$$

[On convient d'écrire $S(c)$ au lieu de $S(\bar{c})$ si c est un élément de A_K.]

On sait (cf. Chap. IV, prop. 17) que $v_K(w-1) = e/(p-1)$, ce qui montre bien que t est un entier. D'autre part, la linéarité du symbole $(a, b)_v$ permet de se borner au cas où a est une uniformisante de K. Soit π une racine p-ième de a, et soit $L = K(\pi)$; on peut appliquer la prop. 5 à l'extension L/K. Choisissons le générateur s de G(L/K) de telle sorte que $\pi^{s-1} = w$; on voit alors que

$$t = ep/(p-1), \qquad M = w - 1, \qquad \mathrm{Tr}(M) = p(w-1).$$

D'où :

$$(b, L/K) = s^{m(b)}, \qquad \text{avec} \qquad m(b) = S\left(\frac{b-1}{p(w-1)}\right).$$

On a donc $(a, b)_v = \pi^{(b, L/K)-1} = w^{m(b)}$, c.q.f.d.

Exercices. 1. Les notations étant celles de la prop. 5, montrer que l'on a :

$$c(x) \equiv -\frac{x-1}{N(M)} \equiv -\frac{x-1}{M^p} \qquad \text{mod. } \mathfrak{p}_L.$$

2. Les notations étant celles de la prop. 6, montrer que l'extension $K(b^{1/p})/K$ est non ramifiée, et en déduire une autre démonstration de la proposition en question.

3. Les notations étant celles de la prop. 6, soient i et j deux entiers $\geqslant 0$ tels que $i + j = t$. Soit $a \in U_K^i$ et soit $b \in U_K^j$. Démontrer la formule :

$$(a, b)_v = w^{t.S\left(\frac{(a-1)(b-1)}{p(w-1)}\right)}.$$

BIBLIOGRAPHIE

[1] S. Amitsur. *Generic splitting fields of central simple algebras.* Ann. of. Maths., **62**, 1955, p. 8-43.

[2] C. Arf. *Untersuchungen über reinverzweigte Erweiterungen diskret bewerteter perfekter Körper.* J. reine ang. Math., **181**, 1940, p. 1-44.

[3] E. Artin. *Beweis des allgemeinen Reziprozitätsgesetzes.* Hamb. Abh., **5**, 1927, p. 353-363.

[4] E. Artin. *Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz.* Hamb. Abh., **7**, 1929, p. 46-51.

[5] E. Artin. *Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren.* Hamb. Abh., 8, 1930, p. 292-306.

[6] E. Artin. *Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper.* J. reine ang. Math., **164**, 1931, p. 1-11.

[7] E. Artin, C. Nesbitt et R. Thrall. *Rings with minimum condition.* University of Michigan Press, Ann Arbor, 1948.

[8] E. Artin et J. Tate. *Class field theory.* Benjamin, New York, 1967.

[9] M. Auslander et O. Goldman. *The Brauer group of a commutative ring.* Trans. Amer. Math. Soc., **97**, 1960, p. 367-409.

[10] G. Azumaya. *On maximally central algebras.* Nagoya Math. J., 2, 1951, p. 119-150.

[11] R. Brauer et J. Tate. *On the characters of finite groups.* Ann. of Maths., **62**, 1955, p. 1-7.

[12] H. Cartan et C. Chevalley. *Géométrie algébrique.* Séminaire E.N.S., 1955-1956.

[13] H. Cartan et S. Eilenberg. *Homological algebra.* Princeton Math. Ser., n° **19**, Princeton, 1956.

[14] J. Cassels. *Arithmetic on curves of genus* 1. *I. On a conjecture of Selmer.* J. reine ang. Math., **202**, 1959, p. 52-99. *II. A general result. Ibid.*, **203**, 1960, p. 174-208. *III, IV, V, ..., VIII.*

[15] F. Chatelet. *Variations sur un thème de H. Poincaré.* Annales E.N.S., **61**, 1944, p. 249-300.

[16] F. Chatelet. *Géométrie diophantienne et théorie des algèbres.* Séminaire Dubreil, 1954-1955, exp. 17.

[17] C. Chevalley. *Class field theory.* Nagoya, 1954.

[18] I. Cohen. *On the structure and ideal theory of complete local rings.* Trans. Amer. Math. Soc., **59**, 1946, p. 54-106.

[19] M. Deuring. *Algebren.* Ergebn. der Math., IV-1, 1935.

[20] A. Douady. *Cohomologie des groupes compacts totalement discontinus.* Séminaire Bourbaki, 1959-1960, exp. 189.

[21] B. Dwork. *Norm residue symbol in local number fields.* Hamb. Abh., **22**, 1958, p. 180-190.

[22] B. Eckmann. *Cohomology of groups and transfer.* Ann. of Maths., **58**, 1953, p. 481-493.

[23] B. Eckmann. *Homotopie et dualité.* Colloque de Topologie algébrique, Louvain, 1956, p. 41-53.

[24] J. FRENKEL. *Cohomologie non abélienne et espaces fibrés*. Bull. Soc. Math. France, 85, 1957, p. 135-220.
[25] M. GREENBERG. *Schemata over local rings*. Ann. of Maths., 73, 1961, p. 624-648.
[26] A. GROTHENDIECK. *Sur quelques points d'algèbre homologique*. Tôhoku Math. J., 9, 1957, p. 119-221.
[27] A. GROTHENDIECK. *A general theory of fibre spaces with structure sheaf*. Univ. of Kansas, Report n° 4, 1955.
[28] A. GROTHENDIECK. *Technique de descente et théorèmes d'existence en géométrie algébrique. I. Généralités. Descente par morphismes fidèlement plats*. Séminaire BOURBAKI, 1959-1960, exp. 190.
[29] A. GROTHENDIECK. *Séminaire de géométrie algébrique*. Inst. Htes. Et. Scient., 1960-1961-...
[30] M. HALL. *The theory of groups*. The Macmillan Cy., New York, 1959.
[31] H. HASSE. *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*. Jahr. der D. Math. Ver., 35, 1926, p. 1-55; *ibid.*, 36, 1927, p. 255-311; *ibid.*, 89, 1930, p. 1-204.
[32] H. HASSE. *Führer, Diskriminante und Verzweigungskörper relativ Abelscher Zahlkörper*. J. reine ang. Math., 162, 1930, p. 169-184.
[33] H. HASSE. *Normenresttheorie galoisscher Zahlkörper mit Anwendungen auf Führer und Diskriminante abelscher Zahlkörper*. J. Fac. Sci. Tokyo, 2, 1934, p. 477-498.
[34] H. HASSE. *Zahlentheorie*. Berlin, Akademie-Verlag, 1949.
[35] G. HOCHSCHILD. *Relative homological algebra*. Trans. Amer. Math. Soc., 82, 1956, p. 246-269.
[36] G. HOCHSCHILD et T. NAKAYAMA. *Cohomology in class field theory*. Ann. of. Maths., 55, 1952, p. 348-366.
[37] G. HOCHSCHILD et J.-P. SERRE. *Cohomology of group extensions*. Trans. Amer. Math. Soc., 74, 1953, p. 110-134.
[38] S. LANG. *On quasi-algebraic closure*. Ann. of Maths., 55, 1952, p. 373-390.
[39] S. LANG. *Algebraic groups over finite fields*. Amer. J. of Maths., 78, 1956, p. 555-563.
[40] S. LANG. *Abelian varieties*. Interscience Tracts n° 7, New York, 1959.
[41] S. LANG et J. TATE. *Principal homogeneous spaces over abelian varieties*. Amer. J. of. Maths., 80, 1958, p. 659-684.
[42] M. LAZARD. *Détermination des anneaux p-adiques et π-adiques dont les anneaux de restes sont parfaits*. Séminaire KRASNER, 1953-1954, exp. 9.
[43] M. LAZARD. *Bemerkungen zur Theorie der bewerteten Körper und Ringe*. Math. Nach., 12, 1954, p. 67-73.
[44] M. LAZARD. *Sur les groupes nilpotents et les anneaux de Lie*. Annales E.N.S., 71, 1954, p. 101-190.
[45] R. MACKENZIE et G. WHAPLES. *Artin-Schreier equations in characteristic zero*. Amer. J. of Maths., 78, 1956, p. 473-485.
[46] Y. NAKAI. *On the theory of differentials in commutative rings*. J. Math. Soc. Jap., 13, 1961, p. 63-84.
[47] T. NAKAYAMA. *Cohomology of class field theory and tensor product modules. I*. Ann. of Maths., 65, 1957, p. 255-267.
[48] T. NAKAYAMA. *On modules of trivial cohomology over a finite group. I*. Illinois J. Math., 1, 1957, p. 36-43; *II*, Nagoya Math. J., 12, 1957, p. 171-176.
[49] O. ORE. *Abriss einer arithmetischen Theorie der Galoisschen Körper. I*. Math. Ann., 100, 1928, p. 650-673; *II*, *ibid.*, 102, 1930, p. 283-304.
[50] O. ORE. *On a special class of polynomials*. Trans. Amer. Math. Soc., 35, 1933, p. 559-584 (*Errata*, *ibid.*, 36, 1934, p. 275).
[51] D. RIM. *Modules over finite groups*. Ann. of Maths., 69, 1959, p. 700-712.
[52] P. ROQUETTE. *Abspaltung des Radikals in vollständigen lokalen Ringen*. Hamb. Abh., 23, 1959, p. 75-113.
[53] P. SAMUEL et O. ZARISKI. *Commutative Algebra*. Van Nostrand.
[54] O. SCHILLING. *The theory of valuations*. Math. Surveys IV, New-York, 1950.

[55] H. SCHMID. *Ueber das Reziprozitätsgesetz in relativ-zyklischen algebraischen Funktionenkörpern mit endlichem Konstantenkörper.* Math. Zeit., **40**, 1936, p. 94-109.
[56] J.-P. SERRE. *Groupes algébriques et corps de classes.* Paris, Hermann, 1959.
[57] J.-P. SERRE. *Sur la rationalité des représentations d'Artin.* Ann. of Maths., **72**, 1960, p. 406-420.
[58] J.-P. SERRE. *Groupes finis à cohomologie périodique (d'après* R. SWAN). Séminaire BOURBAKI, 1960-1961, exp. 209.
[59] J.-P. SERRE. *Sur les corps locaux à corps résiduel algébriquement clos.* Bull. Soc. Math. France, **89**, 1961, p. 105-154.
[60] A. SPEISER. *Zahlentheoretische Sätze aus der Gruppentheorie.* Math. Zeit., **5**, 1919, p. 1-6.
[61] A. SPEISER. *Die Zerlegungsgruppe.* J. reine ang. Math., **149**, 1920, p. 174-188.
[62] R. SWAN. *Induced representations and projective modules.* Ann. of Maths., **71**, 1960, p. 552-578.
[63] J. TATE. *The higher dimensional cohomology groups of class field theory.* Ann. of Maths., **56**, 1952, p. 294-297.
[64] J. TATE. *WC-groups over p-adic fields.* Séminaire BOURBAKI, 1957-1958, exp. 156.
[65] B. VAN DER WAERDEN. *Moderne Algebra.* I. 5^te Auflage, Springer, 1960.
[66] A. WEIL. *Sur les courbes algébriques et les variétés qui s'en déduisent.* Hermann, Paris, 1948.
[67] A. WEIL. *Sur la théorie du corps de classes.* J. Math. Soc. Jap., **3**, 1951, p. 1-35.
[68] H. WEYL. *Algebraic theory of numbers.* Ann. of Math. St., n° 1, Princeton, 1940.
[69] G. WHAPLES. *Additive polynomials.* Duke Math. J., **21**, 1954, p. 55-66.
[70] G. WHAPLES. *Galois cohomology of additive polynomial and* n*-th power mappings of fields.* Duke Math. J., **24**, 1957, p. 143-150.
[71] G. WHAPLES. *Generalized local class field theory. I.* Duke Math. J., **19**, 1952, p. 505-517; *II, ibid.*, 21, 1954, p. 247-256; *III, ibid.*, p. 575-581; *IV, ibid.*, p. 583-586.
[72] E. WITT. *Schiefkörper über diskret bewerteten Körpern.* J. reine ang. Math., **176**, 1936, p. 153-156.
[73] E. WITT. *Zyklische Körper und Algebren der Charakteristik p vom Grade* p^n. J. reine ang. Math., **176**, 1936, p. 126-140.

BIBLIOGRAPHIE SUPPLÉMENTAIRE
(Troisième édition)

Ouvrages généraux : Cassels-Fröhlich [75]; Lang [94]; Serre [114]; Weil [123].
Cohomologie des groupes : Koch [88]; Lang [93]; Poitou [102]; Serre [110]; Tate [117], [118], [121].
Groupe de Brauer : Grothendieck [83]; Serre [110]; Weil [123].
Cohomologie non abélienne : Giraud [80]; Serre [113].
Groupes de Galois des corps locaux : Demuškin [77]; Iwasawa [84]; Koch [88]; Labute [91]; Šafarevič [104], [105]; Weil [123].
Nombre des extensions de degré donné d'un corps local : Krasner [89]; Serre [115].
Groupes de ramification : Fontaine [78]; Maus [99]; Sen [106], [107]; Sen-Tate [109]; Wiman [125].
Conducteurs d'Artin et applications : Fontaine [78]; Martinet [79]; Ogg [101]; Raynaud [103]; Serre [112].
Symboles locaux, lois de réciprocité : Coates-Wiles [76]; Iwasawa [85]; Lubin-Tate [98]; Tate [120]; Wiles [125].
Groupes formels, groupes p-divisibles et modules de Hodge-Tate : Cassels-Fröhlich [75]; Lubin [97]; Lubin-Tate [98]; Sen [108]; Serre [111], [116]; Tate [119]; Wiles [124].
Équations à coefficients dans un corps local : Ax-Kochen [74]; Greenberg [81], [82]; Terjanian [122].
Groupes de Lie p-adiques : Lazard [95]; Moore [100].
Fonctions zêta p-adiques : Coates [79]; Iwasawa [86]; Koblitz [87]; Kubota-Leopoldt [90].
Math. Reviews : Leveque [96].

[74] J. Ax and S. Kochen, *Diophantine problems over local fields, I.* Amer J. of Math. **87** (1965), p. 605-630; *II, ibid.* p. 631-648; *III,* Ann. of Math. **83** (1966), p. 437-456.
[75] J. Cassels and A. Fröhlich, *Algebraic Number Theory*, Acad. Press, New York, 1967.
[76] J. Coates and A. Wiles, *Explicit reciprocity laws*, Astérisque 41-42 (1977), p. 7-17.
[77] S. Demuškin, *The group of a maximal p-extension of a number field* (in Russian), Izv. Akad. Nauk SSR Ser. Mat. **25** (1961), p. 329-346.
[78] J.-M. Fontaine, *Groupes de ramification et représentations d'Artin*, Ann. Sci. E.N.S. (4), **4** (1971), p. 337-392.
[79] A. Fröhlich (édit.), *Algebraic Number Fields (L-functions and Galois properties)*, Acad. Press, London, 1977.
[80] J. Giraud, *Cohomologie non abélienne*, Grund. math. Wiss. 179, Springer-Verlag, 1971.
[81] M. Greenberg, *Rational points in Henselian discrete valuation rings*, Publ. Math. I.H.E.S. **31** (1966), p. 59-64.
[82] M. Greenberg, *Lectures on Forms in Many Variables*, Benjamin, New York, 1969.
[83] A. Grothendieck, *Le groupe de Brauer I, II, III*, Dix exposés sur la cohomologie des schémas (J. Giraud *et al.*), p. 46-188, Masson, North-Holland, 1968.
[84] K. Iwasawa, *On Galois groups of local fields*, Trans. A.M.S. **80** (1955), p. 448-449.
[85] K. Iwasawa, *On explicit formulas for the norm residue symbol*, J. Math. Soc. Japan **20** (1968), p. 151-165.
[86] K. Iwasawa, *Lectures on p-adic L-Functions*, Ann. Math. Studies **74**, Princeton Univ. Press, Princeton, 1972.
[87] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, G.T.M. **58**, Springer-Verlag, 1977.
[88] H. Koch, *Galeissche Theorie der p-Erweiterungen*, Math. Mon. **10**, V.E.B. Deutscher Verlag der Wiss., Berlin, 1970.
[89] M. Krasner, *Nombre des extensions d'un degré donné d'un corps p-adique*, Colloque C.N.R.S. **143**, Clermont-Ferrand (1966), p. 143-169.

[90] T. KUBOTA and H. LEOPOLDT, *Eine p-adische Theorie der Zetawerte I.* Crelle J. **214/215** (1964), p. 328-339.
[91] J. LABUTE, *Classification of Demuškin groups*, Canad. J. of Math. **19** (1967), p. 106-132.
[92] J. LABUTE, *Demuškin groups of rank* $\aleph_0$, Bull. Soc. Math. France **94** (1966), p. 211-244.
[93] S. LANG, *Rapport sur la cohomologie des groupes*, Benjamin, New York, 1966.
[94] S. LANG, *Algebraic Number Theory*, Addison-Wesley, 1970.
[95] M. LAZARD, *Groupes analytiques p-adiques*, Publ. Math. I.H.E.S. **26** (1965), p. 1-219.
[96] W. J. LEVEQUE (édit.), *Reviews in Number Theory*, vol. 5, chap. S, 304-354, Amer. M.S., 1974.
[97] J. LUBIN, *One-parameter formal Lie groups over p-adic integer rings*, Ann. of Math. **80** (1964), p. 464-484 (Correction : *ibid.* **84** (1966), p. 372).
[98] J. LUBIN and J. TATE, *Formal complex multiplication in local fields*, Ann. of Math. **81** (1965), p. 380-387.
[99] E. MAUS, *Die gruppentheoretische Struktur der Verzweigungsgruppenreihen*, Crelle J. **230** (1968), p. 1-28.
[100] C. C. MOORE, *Group extensions of p-adic and adelic linear groups*, Publ. Math. I.H.E.S. **35** (1968), p. 157-221.
[101] A. OOO, *Elliptic curves and wild ramification*, Amer. J. of Math. **89** (1967), p. 1-21.
[102] G. POITOU, *Cohomologie galoisienne des modules finis*, Dunod, Paris, 1967.
[103] M. RAYNAUD, *Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes*, Sém. Bourbaki, 1964-65, exp. 286.
[104] I. ŠAVAREVIČ, *On Galois groups of p-adic fields* (in Russian), Dokl. Akad. Nauk SSR **53** (1946), p. 15-16.
[105] I. ŠAVAREVIČ, *On p-extensions* (in Russian), Math. Sbornik **20** (1947), p. 351-363.
[106] S. SEN, *On automorphisms of local fields*, Ann. of Math. **90** (1969), p. 33-46.
[107] S. SEN, *Ramification in p-adic Lie extensions*, Inv. Math. **17** (1972), p. 44-50.
[108] S. SEN, *Lie algebras of Galois groups arising from Hodge-Tate modules*, Ann. of Math. **97** (1973), p. 160-170.
[109] S. SEN and J. TATE, *Ramification groups of local fields*, J. Ind. Math. Soc. **27** (1963), p. 197-202.
[110] J.-P. SERRE, *Applications algébriques de la cohomologie des groupes*, Sém. H. Cartan, E.N.S. 1950/51, exp. 5, 6, 7, Benjamin, New York, 1967.
[111] J.-P. SERRE, *Sur les groupes de Galois attachés aux groupes p-divisibles*, Proc. Conf. Local Fields, p. 118-131, Springer-Verlag, 1967.
[112] J.-P. SERRE, *Conducteurs d'Artin des caractères réels*, Inv. Math. **14** (1971), p. 173-183.
[113] J.-P. SERRE, *Cohomologie Galoisienne*, Lect. Notes in Math, **5**, 4th edit., Springer-Verlag, 1973.
[114] J.-P. SERRE, *Cours d'arithmétique*, 2e édit., Presses Univ. de France, Paris, 1977.
[115] J.-P. SERRE, *Une « formule de masse » pour les extensions totalement ramifiées de degré donné d'un corps local*, C.R. Acad. Sci. Paris, série A, **286** (1978), p. 1031-1036.
[116] J.-P. SERRE, *Groupes algébriques associés aux modules de Hodge-Tate*, Astérisque vol. **65**, Soc. Math. France (1979), p. 155-188.
[117] J. TATE, *Duality theorems in Galois cohomology over number fields*, Proc. Int. Congress, Stockholm 1962, p. 288-295.
[118] J. TATE, *Cohomology groups of tori in finite Galois extensions of Algebraic Number Fields*, Nagoya Math. J. **27** (1966), p. 709-719.
[119] J. TATE, *p-divisible groups*, Proc. Conf. Local Fields, 158-183, Springer-Verlag, 1967.
[120] J. TATE, *Symbols in arithmetic*, Actes Congrès Int. Nice 1970, t. I, p. 201-211.
[121] J. TATE, *Relations between* K_2 *and Galois cohomology*, Inv. Math. **36** (1976), p. 257-274.
[122] G. TERJANIAN, *Un contre-exemple à une conjecture d'Artin*, C.R. Acad. Sci. Paris **262** (1966), p. 612.
[123] A. WEIL, *Basic Number Theory*, Grund. math. Wiss., 3rd edit., Springer-Verlag, 1974.
[124] A. WILES, *Higher explicit reciprocity laws*, Ann. of Math. **107** (1978), p. 235-254.
[125] B. WYMAN, *Wildly ramified gamma extensions*, Amer. J. of Math. **91** (1969), p. 135-152.

INDEX

Les chiffres de référence indiquent successivement le chapitre et le paragraphe.