JEAN-PIERRE SERRE

Sur les corps locaux à corps résiduel algébriquement clos

Bulletin de la S. M. F., tome 89 (1961), p. 105-154

<http://www.numdam.org/item?id=BSMF_1961__89__105_0>

Bull. Soc. math. France,
89, 1961, p. 105 à 154.

SUR LES CORPS LOCAUX
À CORPS RÉSIDUEL ALGÉBRIQUEMENT CLOS ;

PAR

JEAN-PIERRE SERRE

Introduction. — Soit K un *corps local*, c'est-à-dire un corps muni d'une valuation discrète, et complet pour la topologie définie par cette valuation. Soit $\mathfrak{A}_K$ le groupe de Galois de l'extension abélienne maximale de K. Lorsque le corps résiduel k de K est un corps *fini* (ou plus généralement quasi-galoisien au sens de WHAPLES [27]), on peut déterminer explicitement $\mathfrak{A}_K$ au moyen de la théorie du corps de classes local : c'est le complété du groupe multiplicatif K^* pour une certaine topologie (*cf.* WHAPLES [25]). Le but du présent mémoire est d'édifier une théorie analogue lorsque *le corps résiduel k est algébriquement clos.* Il faut d'abord munir le groupe U_K des unités de K d'une structure de *groupe proalgébrique sur k*, au sens de [21]; c'est possible, en vertu des résultats généraux de GREENBERG [7], appliqués au groupe multiplicatif G_m. On peut donc parler du *groupe fondamental $\pi_1(U_K)$ du groupe U_K* (*cf.* [21], n° 6.1), et la détermination de $\mathfrak{A}_K$ se fait en construisant un *isomorphisme*

$$\theta : \quad \pi_1(U_K) \to \mathfrak{A}_K.$$

En termes imagés, on peut dire que les *extensions abéliennes* de K correspondent biunivoquement aux *isogénies* du groupe U_K.

Le contenu des différents paragraphes est le suivant :

Le § 1 rappelle la définition de la structure proalgébrique de U_K, et établit ses principales propriétés. Le § 2 donne deux définitions équivalentes de l'homomorphisme θ; l'une est directe, l'autre est basée sur une *formation de classes*, au sens d'Artin-Tate [celle formée par les $\pi_1(U_L)$, pour L parcourant l'ensemble des extensions finies séparables de K]. Les deux définitions montrent immédiatement que θ est surjectif. Qu'il soit injectif constitue le *théorème d'existence*, démontré au § 4. Comme dans le cas classique, la démonstration consiste à construire « suffisamment » d'extensions abéliennes de K, au moyen d'équations bien choisies; nous utilisons principalement les « équations d'Artin-Schreier » (*cf.* MacKenzie-Whaples [14]). Le § 3 complète l'analogie avec la théorie du corps de classes local en montrant que l'isomorphisme θ transforme la filtration naturelle de $\pi_1(U_K)$ en la filtration de $\mathfrak{A}_K$ définie par les groupes de ramification (numérotés à la Herbrand); on a donc une théorie du conducteur, qui montre en particulier que le conducteur d'Artin est entier; les démonstrations suivent de près celles données par Hasse dans le cas classique (*cf.* [8]). Le § 5 indique comment les résultats locaux des paragraphes 2, 3, 4 se relient à ceux de la théorie des courbes algébriques.

Comme nous l'avons indiqué au début, tout ce qui précède ne concerne que le cas d'un corps résiduel algébriquement clos. On peut, dans une certaine mesure, passer de là au cas général par une méthode analogue à celle utilisée par Lang pour les corps de fonctions (*cf.* [18], chap. VI, ainsi que [19], n° 7). Nous n'exposerons pas ici cette méthode; ce ne serait d'ailleurs possible qu'en changeant assez sensiblement le cadre dans lequel nous nous sommes placés.

§ 1. Structure proalgébrique sur le groupe des unités.

L'existence et les propriétés générales de cette structure sont dues à Greenberg [7]; les numéros 1.1 à 1.6 reproduisent sans grand changement ses démonstrations. Les deux derniers numéros contiennent des théorèmes de structure relatifs au cas des anneaux de valuation.

Dans tout ce paragraphe, la lettre k désigne un corps *algébriquement clos*, de caractéristique quelconque.

1.1. Modules sur les vecteurs de Witt. — Supposons que k soit de caractéristique p, et soit W l'anneau des vecteurs de Witt de longueur infinie à coefficients dans k (pour tout ce qui concerne les vecteurs de Witt, *voir* Witt [28], ou Hasse [9], § 10). On sait que W est un anneau de valuation discrète, complet, de corps résiduel k, et dont l'idéal maximal est engendré par p (ces propriétés le caractérisent d'ailleurs à un isomorphisme unique près). Pour $x \in k$, on pose $r(x) = (x, 0, \ldots, 0, \ldots)$; c'est le *représentant multiplicatif* de x. Si $w = (x_0, x_1, \ldots)$, on a

$$w = \sum_{i=0}^{\infty} r(x_i^{p^{-i}}) p^i.$$

Si n est un entier ≥ 0, nous noterons W_n l'anneau des vecteurs de Witt de longueur n, anneau qui s'identifie à $W/p^n W$; les coordonnées (x_i) font de W_n une variété algébrique sur k. Comme l'addition et la multiplication sont données par des formules polynomiales, W_n est même un *anneau algébrique*. Si $m \geqq n$, la structure algébrique de W_n est *quotient* de celle de W_m.

Si E est un produit fini de W_{n_i}, on munira E de la structure algébrique produit de celles des W_{n_i}. On a :

LEMME 1. — *Soient $E_0, E_1, \ldots, E_k$ des produits finis de W_{n_i}, et soit $f : E_1 \times \ldots \times E_k \to E_0$ une application W-multilinéaire. Si l'on munit $E_0, \ldots, E_k$ des structures algébriques produits de celles des W_{n_i} l'application f est un morphisme.*

La multilinéarité permet de se ramener au cas où chaque E_i est isomorphe à un W_{n_i}, et le lemme est immédiat dans ce cas.

Lorsque $k = 1$, on voit en particulier que toute application linéaire $f : E_1 \to E_0$ est un morphisme; si f est bijective, ce résultat, appliqué à f^{-1}, montre que f est un isomorphisme.

Soit maintenant E un W-module de longueur finie. D'après le théorème de structure des modules sur un anneau principal, il existe un isomorphisme $g : E \to E_0$, où E_0 est un produit de W_{n_i}; nous transporterons à E la structure algébrique de E_0 au moyen de g^{-1}. Comme g est unique à un automorphisme W-linéaire près de E_0, et qu'un tel automorphisme respecte la structure algébrique de E_0, on en conclut que la structure algébrique de E *ne dépend pas du choix de g*. On l'appellera la *structure canonique* de E.

PROPOSITION 1. — *Soient $E_0, E_1, \ldots, E_k$ des W-modules de longueur finie, munis de leurs structures canoniques de variétés algébriques.*

(*a*) *Toute application W-multilinéaire $f : E_1 \times \ldots \times E_k \to E_0$ est un morphisme.*

(*b*) *Si $f : E_1 \to E_0$ est une application W-linéaire surjective, la structure algébrique de E_0 s'identifie à la structure quotient $E_1/\mathrm{Ker}\,(f)$.*

(*c*) *Si $p^n E_0 = 0$, l'application $(w, x) \to w.x$ de $W_n \times E_0$ dans E_0 est un morphisme.*

L'assertion (*a*) résulte du lemme 1, et (*c*) est un cas particulier de (*a*). Dans le cas (*b*), f définit un morphisme bijectif f_0 de $E_1/\mathrm{Ker}\,(f)$ sur E_0, et il nous faut prouver que ce morphisme est un isomorphisme. On peut supposer que $E_0 = \prod_{i=1}^{i=k} W_{n_i}$. Choisissons un entier n tel que $p^n E_1 = 0$; on peut donc considérer E_1 et E_0 comme des W_n-modules, et l'on a, en particulier, $n \geqq n_i$ pour tout i. Soit E' le produit de k facteurs égaux chacun à W_n, et soit g l'application de E' sur E_0 produit des projections canoniques $W_n \to W_{n_i} (1 \leqq i \leqq k)$. Il est clair que la structure algébrique de E_0 s'identifie à celle de $E'/\mathrm{Ker}(g)$. Comme E' est un W_n-module libre, il existe un W-homomorphisme $h : E' \to E_1$ tel que $g = f \circ h$. L'application h est un morphisme, et applique $\mathrm{Ker}(g)$ dans $\mathrm{K}(f)$; elle définit donc par passage au quotient un morphisme h_0 de $E'/\mathrm{Ker}(g) = E_0$ dans $E_1/\mathrm{Ker}(f)$. On vérifie tout de suite que f_0 et h_0 sont des morphismes inverses l'un de l'autre, et ce sont donc des isomorphismes, ce qui achève de prouver (b).

Remarque. — Si E_1 est un sous-module de E_0, il n'est pas vrai en général que la structure algébrique canonique de E_1 soit *induite* par celle de E_0 (sauf, bien sûr, si E_1 est facteur direct dans E_0). Exemple : $E_1 = W_1$, $E_0 = W_2$, le module E_1 étant identifié à un sous-module de E_0 au moyen de l'application W-linéaire $x \to (0, x^p)$, déduite par passage au quotient de la multiplication par p dans W; si l'on note E'_1 la structure algébrique sur E_1 induite par celle de E_0, l'application identique $E_1 \to E'_1$ est une *isogénie radicielle* de degré p.

1.2. **Anneaux locaux artiniens.** — Soit A un anneau local artinien de corps résiduel k; nous notons s l'homomorphisme canonique de A sur k. Nous allons munir A d'une structure de k-variété algébrique qui en fera un *anneau algébrique*. Distinguons deux cas :

(i) *La caractéristique de k est nulle.*

On sait (*cf.* par exemple Cohen [5], § 4) qu'il existe alors un corps de représentants de k, c'est-à-dire un homomorphisme $r : k \to A$ tel que $s \circ r = 1$ Nous *choisirons* une fois pour toutes un tel homomorphisme. L'anneau A devient alors une k-algèbre de dimension finie (égale à la longueur de A), et sa structure de variété algébrique est évidente.

(ii) *La caractéristique de k est* $p \neq 0$.

Il existe alors une application $r : k \to A$, et une seule, qui vérifie les deux conditions suivantes :

(a) $s \circ r = 1$;
(b) $r(x^p) = r(x)^p$ pour tout $x \in k$.

Si $x \in k$, l'élément $r(x)$ de A est appelé le *représentant multiplicatif* de x; cette terminologie est justifiée par la formule :

(c) $r(xy) = r(x).r(y)$ (*cf.* Cohen [5], § 5).

L'application r permet de définir un homomorphisme bien déterminé $\chi : W \to A$ par la formule

$$\chi(x_0, x_1, \ldots) = \sum_{i=0}^{\infty} r(x_i^{p^{-i}}).p^i,$$

cf. Witt [28], où est traité le cas des anneaux de valuation discrète (le cas général se traite de même). Notons que, dans la formule précédente, tous les termes sont nuls à l'exception d'un nombre fini.

L'anneau A se trouve ainsi muni d'une structure de W-algèbre, et en particulier d'une structure de W-module de longueur finie. On le munit de la structure canonique de variété algébrique correspondant à cette structure de module (*cf.* n° 1.1). Comme la multiplication est une application W-bilinéaire de $A \times A$ dans A, la proposition 1 montre que A est un *anneau algébrique*.

Dans les deux cas (i) et (ii), les applications $r : k \to A$ et $s : A \to k$ sont des morphismes; comme $s \circ r = 1$, on en conclut que r est un *isomorphisme* de k sur une sous-variété fermée (pour la topologie de Zariski) de A. Noter également que, si A est de longueur n, il est isomorphe en tant que variété algébrique à l'espace affine de dimension n.

1.3. **Groupe des unités d'un anneau local artinien.** — Nous conservons les notations du numéro précédent. Soit $\mathfrak{m}$ l'idéal maximal de A, et soit $U = A - \mathfrak{m}$ le groupe des unités de A. Soit U^1 le sous-groupe de U formé des $x \in A$ tels que $x \equiv 1 \bmod \mathfrak{m}$, et soit G_m le sous-groupe formé des $r(x)$, $x \in k^*$. Il est clair que U est produit direct des sous-groupes G_m et U^1.

Comme $s : A \to k$ est un morphisme, $\mathfrak{m} = s^{-1}(0)$ et $U^1 = s^{-1}(1)$ sont fermés pour la topologie de Zariski de A, et U est ouvert. Quant à $G_m = U \cap r(k)$, il est fermé dans U. La structure de variété algébrique de A induit donc sur chacun des trois groupes U, G_m et U^1 une structure de variété algébrique.

Proposition 2.

(*a*) *Les structures algébriques définies ci-dessus font de U, U^1 et G_m des groupes algébriques.*

(*b*) *L'application $r : k^* \to G_m$ est un isomorphisme.*

(*c*) *Le groupe U est produit direct* (*en tant que groupe algébrique*) *des groupes G_m et U^1.*

Puisque la multiplication $(x, y) \to x.y$ est un morphisme de $A \times A$ dans A, elle induit sur U un morphisme de $U \times U$ dans U, et de même pour U^1 et G_m. Pour montrer que ces groupes sont des groupes algébriques, il nous reste à prouver que $x \to x^{-1}$ est aussi un morphisme. Cela peut se faire, soit par un raisonnement général utilisant le « main theorem » de Zariski, soit directement de la façon suivante :

Pour G_m, c'est clair, car les applications $r : k^* \to G_m$ et $s : G_m \to k^*$ sont des morphismes inverses l'un de l'autre, donc des isomorphismes, ce qui établit en même temps (*b*).

Pour U^1, on remarque que, si $x = 1 - a$, avec $a \in \mathfrak{m}$, et si $\mathfrak{m}^k = 0$, on a

$$x^{-1} = 1 + a + \ldots + a^{k-1} = 1 + (1 - x) + \ldots + (1 - x)^{k-1},$$

ce qui définit évidemment un morphisme de U^1 dans lui-même.

Reste le cas de U. L'application évidente de $G_m \times U^1$ dans U est un morphisme. On va montrer que c'est un isomorphisme, ce qui établira à la fois (*c*) et le fait que U est un groupe algébrique. Il faut donc voir que l'application inverse est un morphisme. Or cette application s'écrit explicitement $x \to (r(s(x)), x.r(s(x)^{-1}))$, ce qui montre bien que c'est un morphisme.

Proposition 3. — *Le groupe U^1 est un groupe unipotent.*

En caractéristique zéro, l'application $a \to \exp(a)$ est un isomorphisme du k-espace vectoriel $\mathfrak{m}$ sur le groupe U^1, ce qui montre bien que U^1 est unipotent. En caractéristique p, la relation $x \equiv 1 \bmod \mathfrak{m}^i (i \geq 1)$ entraîne $x^p \equiv 1 \bmod \mathfrak{m}^{i+1}$, d'où $x^{p^m} = 1$ pour $x \in U^1$, si m est assez grand, ce qui montre encore que U^1 est unipotent.

Remarque. — La décomposition $U = G_m \times U^1$ est un cas particulier du théorème de décomposition de Borel-Kolchin : tout groupe algébrique commutatif affine connexe est produit direct d'un tore par un groupe unipotent.

1.4. Passage à la limite. — Soit A un anneau local noethérien complet, de corps résiduel k. Lorsque la caractéristique de k est nulle, nous supposons choisi un relèvement $r : k \to A$ (*cf.* Cohen [5], § 4).

Soit $\mathfrak{m}$ l'idéal maximal de A, et soit $\mathfrak{q}$ un *idéal de définition* de A, c'est-à-dire un idéal contenu dans $\mathfrak{m}$ et contenant une puissance de $\mathfrak{m}$. L'anneau $A/\mathfrak{q}$ est alors un anneau local artinien, et l'anneau A s'identifie à la limite projective des $A/\mathfrak{q}$, pour $\mathfrak{q}$ parcourant l'ensemble des idéaux de définition de A. En caractéristique zéro, le relèvement $r : k \to A$ définit un relèvement de k dans $A/\mathfrak{q}$. On peut donc appliquer à $A/\mathfrak{q}$ les constructions du n° 1.2; d'où une structure d'anneau algébrique sur $A/\mathfrak{q}$, et une structure de groupe algébrique sur son groupe des unités, groupe que nous noterons $U(A/\mathfrak{q})$. Si $\mathfrak{q} \subset \mathfrak{q}'$, la structure algébrique de $A/\mathfrak{q}'$ est quotient de celle de $A/\mathfrak{q}$; c'est évident si k est de caractéristique nulle; en caractéristique p, cela résulte de la partie (b) de la proposition 1. Comme $A/\mathfrak{q}$ et $A/\mathfrak{q}'$ sont des groupes algébriques, cela montre que l'application tangente à la projection $A/\mathfrak{q} \to A/\mathfrak{q}'$ est partout surjective. Il en est donc de même de l'application tangente à la projection $U(A/\mathfrak{q}) \to U(A/\mathfrak{q}')$, ce qui montre que *la structure algébrique de $U(A/\mathfrak{q}')$ est quotient de celle de $U(A/\mathfrak{q})$.*

Quand $\mathfrak{q}$ varie, on a donc un *système projectif d'anneaux algébriques*, à savoir les $A/\mathfrak{q}$, dont la limite s'identifie à A, et un *système projectif de groupes algébriques*, à savoir les $U(A/\mathfrak{q})$, dont la limite s'identifie au groupe U des unités de A [on a, en effet, $U(A/\mathfrak{q}) = U/(1+\mathfrak{q})$].

A côté de ces structures de groupes algébriques, on peut considérer les structures de *groupes quasialgébriques* (au sens de [21], n° 1.2) qui leur sont associées. Comme U est limite projective des $U/(1+\mathfrak{q})$, on voit que U se trouve muni d'une structure de *groupe proalgébrique* sur k, admettant les sous-groupes $1+\mathfrak{q}$ comme ensemble de définition (*cf.* [21], n° 2.1, Remarque 2). De même, A, considéré comme groupe additif, est muni d'une structure de groupe proalgébrique admettant les sous-groupes $\mathfrak{q}$ pour ensemble de définition.

1.5. **Anneaux de valuation discrète.** — A partir de maintenant, nous supposons que A est un *anneau de valuation discrète* (complet, bien entendu), c'est-à-dire l'anneau des entiers d'un corps local K. Distinguons deux cas :

(*a*) *Égale caractéristique* (K et k ont même caractéristique).

L'ensemble $r(k)$ est alors un sous-corps de K, et, en le prenant pour corps des constantes, on voit que A s'identifie à *l'anneau des séries formelles* $k[[T]]$, et K au corps $k((T))$. Les idéaux de définition de A sont les idéaux principaux (T^n), $n = 1, 2, \ldots$. Le groupe des unités de $A/(T^n)$ est le groupe multiplicatif des « séries tronquées »

$$a_0 + a_1 T + \ldots + a_{n-1} T^{n-1}, \qquad a_0 \neq 0$$

et sa structure algébrique s'obtient en considérant les a_i comme des coordonnées. On reconnaît là le *groupe local* qui intervient dans la construction des *jacobiennes généralisées* de Rosenlicht (*cf.* [18], chap. V, n° 14). La composante unipotente U^1 de U est donnée par l'équation $a_0 = 1$. On peut facilement déterminer sa structure : en caractéristique zéro, U^1 est isomorphe à un k-espace vectoriel de dimension $n - 1$ (*cf.* la démonstration de la proposition 3, ou bien [18], chap. V, n° 15); en caractéristique p, U^1 est isomorphe à un certain produit de groupes additifs de Witt (*cf.* [18], chap. V, n° 16).

En passant à la limite sur n, on voit que, si la caractéristique est nulle, le groupe proalgébrique U^1 est isomorphe à un produit infini de groupes isomorphes à G_a, et, si la caractéristique est $p \neq 0$, il est isomorphe à un produit de groupes isomorphes à W. Nous retrouverons d'ailleurs ce résultat au n° 1.8.

(*b*) *Inégale caractéristique* (K est de caractéristique zéro, et k de caractéristique p).

L'homomorphisme $\chi : W \to A$ du numéro 1.2 est alors injectif. Si v désigne l'unique valuation *normée* de K (c'est-à-dire appliquant K^* sur $\mathbf{Z}$), on posera $e = v(p)$; c'est « l'indice de ramification absolu » de K. Si π est une uniformisante de K, les éléments

$$1, \quad \pi, \quad \pi^2, \quad \ldots, \quad \pi^{e-1}$$

forment une *base* de A considéré comme W-module [*cf.* par exemple Hasse [9], § 10, *f*)].

Les idéaux $\mathfrak{q}_n = (p^n)$ forment une famile cofinale d'idéaux de définition de A, et tout élément de $A/\mathfrak{q}_n$ s'écrit de façon unique sous la forme

$$a = w_0 + w_1 \pi + \ldots + w_{e-1} \pi^{e-1}, \qquad w_i \in W_n.$$

Les coordonnées des w_i définissent la structure algébrique de $A/\mathfrak{q}_n$. On a $a \in U(A/\mathfrak{q}_n)$ si et seulement si $w_0 \notin p W_n$, c'est-à-dire si la première coordonnée du vecteur de Witt w_0 est non nulle.

Ici, il paraît difficile de préciser exactement la structure du groupe $U(A/\mathfrak{q}_n)$ considéré comme *groupe algébrique;* nous nous bornerons à étudier sa structure de *groupe quasialgébrique* (*cf.* n° 1.8).

1.6. **Filtration du groupe des unités.** — Nous conservons les notations du numéro précédent. Soit $\mathfrak{m}$ l'idéal maximal de A, et soit U^n le sous-groupe de U formé des $x \in A$ tels que $x \equiv 1 \bmod \mathfrak{m}^n$. Le groupe U/U^n est le groupe des unités de l'anneau d'Artin $A/\mathfrak{m}^n$, et les U^n forment une famille de définition du groupe proalgébrique U. On a évidemment

$$U = U^0 \supset U^1 \supset U^2 \supset \ldots,$$

les U^n forment donc une *filtration décroissante* du groupe U.

Déterminons le *groupe gradué* associé à cette filtration, c'est-à-dire l'ensemble des quotients successifs U^n/U^{n+1}. On a tout d'abord :

Proposition 4. — *Le groupe proalgébrique U est produit direct du groupe G_m et du groupe U^1.*

(En particulier, on a $U^0/U^1 = G_m$.)

Cela résulte de la proposition 2.

Supposons donc $n \geq 1$, et soit x_n un élément de valuation n, c'est-à-dire appartenant à $\mathfrak{m}^n$ et n'appartenant pas à $\mathfrak{m}^{n+1}$. Pour tout $t \in A$, on a $1 + t x_n \in U^n$; l'application $t \to 1 + t x_n$ définit par passage au quotient une application

$$\alpha_{x_n} : \quad G_a \to U^n/U^{n+1},$$

où G_a désigne le corps k considéré comme groupe additif. On vérifie immédiatement que α_{x_n} est un isomorphisme pour les structures de groupes de G_a et de U^n/U^{n+1}. Plus précisément :

Proposition 5. — *L'application $\alpha_{x_n} : G_a \to U^n/U^{n+1}$ définie ci-dessus est un isomorphisme pour les structures de groupes quasialgébriques de G_a et de U^n/U^{n+1}.*

Dans l'anneau algébrique $A/\mathfrak{m}^{n+1}$, l'application $t \to 1 + t x_n$ est un morphisme de A dans un sous-groupe de $U(A/\mathfrak{m}^{n+1})$ qui s'identifie à U^n/U^{n+1}; en passant au quotient, on voit donc que α_{x_n} est un morphisme pour les structures de groupes algébriques de G_a et de U^n/U^{n+1}, donc *a fortiori* pour leurs structures de groupes quasialgébriques. Comme α_{x_n} est bijectif, c'est un isomorphisme ([21], § 1, prop. 4).

Remarque. — Dans le cas d'égale caractéristique, la proposition précédente reste valable si l'on remplace « quasialgébrique » par « algébrique » dans son énoncé. Il n'en est plus de même en inégale caractéristique : si e désigne l'indice de ramification absolu de K, on montre par un calcul facile que α_{x_n} est une isogénie radicielle de degré p^{h_n}, où h_n est égal à la partie entière de n/e; ce n'est donc un isomorphisme que si $n < e$.

Donnons ici l'énoncé d'un lemme qui nous servira plus loin :

Lemme 2. — *Soient A et A' deux groupes abéliens munis de filtrations décroissantes $\{A_n\}$ et $\{A'_n\}$, avec $A_0 = A$, $A'_0 = A'$. Supposons que les homomorphismes canoniques $A \to \varprojlim A/A_n$ et $A' \to \varprojlim A'/A'_n$ soient bijectifs. Soit $u : A \to A'$ un homomorphisme appliquant A_n dans A'_n Si les homomorphismes $u_n : A_n/A_{n+1} \to A'_n/A'_{n+1}$ définis par u sont tous injectifs (resp. surjectifs), il en est de même de u.*

Rappelons la démonstration de ce résultat bien connu (*cf.* Bourbaki, *Alg. comm.*, chap. III, § 2).

Si les u_n sont injectifs, on a $\mathrm{Ker}(u) \cap A_n = \mathrm{Ker}(u) \cap A_{n+1}$, d'où par récurrence sur n, $\mathrm{Ker}(u) \subset A_n$ pour tout n, et comme $\bigcap A_n = 0$ par hypothèse, on voit bien que u est injectif.

Supposons les u_n surjectifs, et soit $a' \in A' = A'_0$. Il existe alors $a_0 \in A_0$ et $a'_1 \in A'_1$ tels que $u(a_0) = a' - a'_1$. Utilisant la surjectivité de u_1, on voit qu'il existe $a_1 \in A_1$ et $a'_2 \in A'_2$ tels que $u(a_1) = a'_1 - a'_2$. On construit de même a_2, a_3, ... et a'_3, a'_4, ... Si l'on munit A de la topologie définie par les A_n, on obtient un groupe topologique complet, et la série $a_0 + a_1 + \ldots$ converge donc vers un élément $a \in A$. On a $u(a) - a' \in A'_n$ pour tout n, d'où $u(a) = a'$. C. Q. F. D.

1.7. **Opération de puissance $p^{\text{ième}}$ dans le groupe des unités.** — Dans ce numéro et dans le suivant, nous supposerons que la caractéristique de k est différente de zéro, et nous la noterons p. L'application $x \to x^p$ est un endomorphisme u du groupe U. Nous nous proposons de déterminer son effet sur la filtration des U^n.

Nous poserons comme précédemment $e = v(p)$, v désignant la valuation normée du corps local K. Si K est de caractéristique p, on a $e = +\infty$; si K est de caractéristique zéro, on a $1 \leqq e < +\infty$. Pour tout entier $n \geqq 0$, nous poserons

$$\lambda(n) = \inf(pn, n + e).$$

La fonction λ est une fonction linéaire par morceaux, strictement croissante, et à valeurs entières. Si l'on pose $e_1 = e/(p-1)$, on a

$$\begin{aligned} \lambda(n) &= pn && \text{si } n \leqq e_1, \\ \lambda(n) &= n + e && \text{si } n \geqq e_1. \end{aligned}$$

Proposition 6. — *L'homomorphisme $u : U \to U$ applique U^n dans $U^{\lambda(n)}$, U^{n+1} dans $U^{\lambda(n)+1}$, et définit par passage au quotient un homomorphisme surjectif*

$$u_n : \quad U^n/U^{n+1} \to U^{\lambda(n)}/U^{\lambda(n)+1}.$$

Le noyau de u_n est toujours nul, sauf si $n = e_1$, auquel cas il est cyclique d'ordre p.

La démonstration est standard (*cf.* par exemple HASSE [9], § 15, *c*). Si $n = 0$, la proposition est évidente. Pour $n \geq 1$, choisissons un élément x_n de valuation n, et soit $x = 1 + tx_n$, $t \in A$, un élément de U^n. On a

$$u(x) = (1 + tx_n)^p = 1 + ptx_n + \ldots + t^p x_n^p.$$

La valuation de px_n est égale à $n + e$, celle de x_n^p est égale à pn, et les termes non écrits ont une valuation strictement supérieure à

$$\inf(pn, n + e) = \lambda(n).$$

On voit donc bien que u applique U^n dans $U^{\lambda(n)}$, d'où aussi U^{n+1} dans $U^{\lambda(n)+1}$ puisque $\lambda(n+1) \geq \lambda(n) + 1$. La même formule donne explicitement u_n :

(*a*) Si $n < e_1$, on a $u(x) = 1 + t^p x_n^p \bmod U^{pn+1}$ et, si l'on identifie U^n/U^{n+1} à G_a au moyen de α_{x_n} (*cf.* prop. 5), et U^{pn}/U^{pn+1} à G_a au moyen de $\alpha_{(x_n^p)}$, l'application u_n s'identifie à l'application $t \to t^p$ de G_a dans lui-même.

(*b*) Si $n = e_1$, le même raisonnement montre que u_n s'identifie à une application de G_a dans lui-même de la forme

$$u_n(t) = at^p + bt \qquad (a, b \neq 0),$$

et cette application est bien surjective, et de noyau isomorphe à $\mathbf{Z}/p\mathbf{Z}$ (comparer à [21], n° 8.3, lemme 1).

(*c*) Si $n > e_1$, le même raisonnement montre que u_n s'identifie à l'application identique de G_a dans lui-même.

On a donc bien vérifié la proposition 6 dans tous les cas.

COROLLAIRE 1. — *Si $n > e_1$, l'homomorphisme u applique isomorphiquement U^n sur U^{n+e}.*

On applique le lemme 2 à $u : U^n \to U^{n+e}$, le groupe U^n étant filtré par les $U^{n+m} (m = 0, 1, \ldots)$, le groupe U^{n+e} par les $U^{n+e+m} (m = 0, 1, \ldots)$. L'application correspondante des gradués associés est bijective, et il en est donc de même de u.

COROLLAIRE 2. — *Pour que le corps local K contienne une racine $p^{\text{ième}}$ de l'unité non triviale, il faut et il suffit que $p - 1$ divise e.*)

(Si $e = +\infty$, on convient que $p - 1$ *ne divise pas* e.)

Si $p - 1$ ne divise pas e, l'entier n ne peut pas être égal à e_1, et u définit des morphismes injectifs

$$U^n/U^{n+1} \to U^{\lambda(n)}/U^{\lambda(n+1)}.$$

D'après le lemme 2, u est injectif, ce qui signifie bien que K ne contient pas de racine de l'unité non triviale.

Supposons maintenant que e_1 soit entier. La proposition 6 montre alors qu'il existe un élément x de U^{e_1}, non situé dans U^{e_1+1}, tel que x^p appartienne à U^{e_1+e+1}. D'après le corollaire 1, il existe $y \in U^{e_1+1}$ tel que $y^p = x^p$. En posant $z = x/y$, on a $z^p = 1$, et z n'appartient pas à U^{e_1+1} : c'est bien une racine $p^{\text{ième}}$ de l'unité non triviale.

Remarque. — Le corollaire 1 reste vrai même lorsqu'on ne fait plus d'hypothèses sur le corps résiduel k : la démonstration est la même. Il n'en est évidemment plus de même du corollaire 2 (*cf.* Hasse, *loc. cit.*).

1.8. **Structure du groupe U^1 en caractéristique p.** — Nous allons déterminer cette structure en nous servant uniquement des renseignements fournis par les propositions 5 et 6. De façon plus précise, considérons un groupe proalgébrique H filtré par une famille décroissante de sous-groupes fermés

$$H = H_1 \supset H_2 \supset \ldots$$

vérifiant les conditious suivantes :

(*a*) *On a* $\bigcap H_i = 0$.

(*b*) *Pour tout* $n \geq 1$, *le groupe* H_n/H_{n+1} *est isomorphe au groupe* G_a.

La condition (*a*) entraîne $H = \varprojlim H/H_n$ (*cf.* [21], 2.5, prop. 10, cor. 3). La condition (*b*) entraîne que G/H_n est un groupe unipotent de dimension $n-1$.

Lemme 3. — *Soit i un entier ≥ 1, et soit f un morphisme de G_a dans H_i/H_{i+1}. Il existe alors un morphisme φ de W dans H_i tel que le diagramme*

$$\begin{array}{ccc} W & \xrightarrow{\varphi} & H_i \\ {\scriptstyle\rho}\downarrow & & \downarrow \\ G_a & \xrightarrow{f} & H_i/H_{i+1} \end{array}$$

soit commutatif (ρ *désignant l'application canonique de W sur G_a*).

Il s'agit de remonter à H_i le morphisme $f \circ \rho : W \to H_i/H_{i+1}$. Supposons que $f \circ \rho$ soit déjà remonté en $\varphi_n : W \to H_i/H_{i+n}$. On a une suite exacte :

$$\mathrm{Hom}(W, H_i/H_{i+n+1}) \to \mathrm{Hom}(W, H_i/H_{i+n}) \to \mathrm{Ext}^1(W, H_{i+n}/H_{i+n+1}).$$

Comme $\mathrm{Ext}^1(W, G_a) = 0$ (*cf.* [21], n° 8.5, th. 1), cette suite exacte montre que φ_n se remonte en $\varphi_{n+1} : W \to H_i/H_{i+n+1}$. La collection des φ_n définit un morphisme $\varphi : W \to \varprojlim H_i/H_{i+n}$, et comme $\varprojlim H_i/H_{i+n}$ s'identifie à H_i, le lemme est démontré.

Soit maintenant $\lambda : \mathbf{N}^* \to \mathbf{N}^*$ une application *strictement croissante* de l'ensemble des entiers non nuls dans lui-même. Nous supposerons que la filtration $\{H_n\}$ vérifie l'une des deux conditions suivantes :

(c_λ) *Le morphisme $x \to px$ applique H_n dans $H_{\lambda(n)}$ et définit pour tout n un isomorphisme de H_n/H_{n+1} sur $H_{\lambda(n)}/H_{\lambda(n)+1}$.*

(c'_λ) *Même énoncé que (c_λ), à cela près que pour une valeur particulière n_0 de n le morphisme de H_n/H_{n+1} sur $H_{\lambda(n)}/H_{\lambda(n)+1}$ a un noyau cyclique d'ordre p.*

[Quand on prend $H = U^1$, filtré par les U^n, on se trouve dans le cas (c'_λ), ou le cas (c_λ), suivant que K contient, ou ne contient pas, de racine $p^{\text{ième}}$ de l'unité non triviale.]

Soit $I = \mathbf{N}^\star - \lambda(\mathbf{N}^\star)$ le complémentaire de l'image de λ, et soit $G = W^I$ le produit de I copies du groupe de Witt W; le $i^{\text{ième}}$ facteur de G sera noté $W^{(i)}$. Pour tout $i \in I$, soit $f_i : G_a \to H_i/H_{i+1}$ un isomophisme, et soit $\varphi_i : W^{(i)} \to H_i$ un morphisme qui relève $f_i \circ \rho$ (*cf.* lemme 3). Comme les H_i tendent vers o, la somme des φ_i est bien définie, et c'est un morphisme de $G = W^I$ dans le groupe H. Le théorème de structure que nous avons en vue s'énonce alors ainsi :

Proposition 7. — *Si H vérifie les conditions (a), (b) et (c_λ), le morphisme $\varphi : W^I \to H$ est un isomorphisme. Si H vérifie les conditions (a), (b) et (c'_λ), le morphisme φ est surjectif, et son noyau est isomorphe au groupe $\mathbf{Z}_p$ des entiers p-adiques.*

Nous allons en fait démontrer un résultat plus précis : nous allons munir W d'une filtration, et montrer que φ applique cette filtration *sur* celle de H.

Si m est un entier $\geq$ o, nous noterons λ^m le $m^{\text{ième}}$ itéré de l'application λ. On a :

Lemme 4. — *Le morphisme $\varphi_i : W^{(i)} \to H_i$ applique $p^m W^{(i)}$ dans $H_{\lambda^m(i)}$ et définit par passage au quotient un morphisme surjectif*

$$p^m W^{(i)}/p^{m+1} W^{(i)} \to H_{\lambda^m(i)}/H_{\lambda^m(i)+1}.$$

Le noyau de ce morphisme est réduit à zéro, sauf, dans le cas (c'_λ), lorsqu'il existe un entier $r \leq m - 1$ tel que $\lambda^r(i) = n_0$, auquel cas ce noyau est cyclique d'ordre p.

Pour $m = 0$, c'est évident d'après la construction des morphisme φ_i. A partir de là on raisonne par récurrence sur m, en utilisant le diagramme commutatif

$$\begin{array}{ccc} p^{m-1} W^{(i)}/p^m W^{(i)} & \to & H_{\lambda^{m-1}(i)}/H_{\lambda^{m-1}(i)+1} \\ \downarrow & & \downarrow \\ p^m W^{(i)}/p^{m+1} W^{(i)} & \to & H_{\lambda^m(i)}/H_{\lambda^m(i)+1} \end{array}$$

où les flèches verticales sont induites par la multiplication par p.

Nous définirons maintenant la filtration du groupe $G = W^I$ en posant

$$G_n = \prod_{i \in I} p^{m(n,i)} W^{(i)},$$

où $m(n, i)$ désigne le plus petit entier m tel que $\lambda^m(i) \geqq n$.

L'entier n peut être écrit de façon unique sous la forme $n = \lambda^q(j)$, avec $q \geqq 0$, $j \in I$. Si $i \neq j$, il est clair que la $i^{\text{ième}}$ composante de G_{n+1} coïncide avec celle de G_n; par contre, pour $i = j$, celle de G_n est $p^q W^{(j)}$ et celle de G_{n+1} est $p^{q+1} W^{(j)}$. On a donc $G_{n+1} \subset G_n$, et le quotient G_n/G_{n+1} s'identifie à $p^q W^{(j)}/p^{q+1} W^{(j)}$, lui-même isomorphe à G_a. Les groupes G_n forment une filtration décroissante de G, qui vérifie les conditions (a), (b) et (c_λ).

On vérifie tout de suite que φ applique G_n dans H_n. De plus, le lemme 4 montre que le morphisme

$$G_n/G_{n+1} \to H_n/H_{n+1}$$

défini par φ est bijectif, sauf, dans le cas (c'_λ), lorsque n est de la forme $\lambda^s(n_0)$, $s \geqq 1$, auquel cas il est cyclique d'ordre p. En appliquant le lemme 2 à G_n et H_n, on voit que φ applique G_n *sur* H_n, et que, dans le cas (c_λ), *c'est un isomorphisme*.

Reste à considérer le cas (c'_λ). Soit alors Γ le noyau de φ, et posons $\Gamma_n = \Gamma \cap G_n$. Le quotient Γ_n/Γ_{n+1} s'identifie au noyau du morphisme de G_n/G_{n+1} dans H_n/H_{n+1} défini par φ. On a donc $\Gamma_n = \Gamma_{n+1}$ si n n'est pas de la forme $\lambda^s(n_0)$; s'il l'est, le quotient Γ_n/Γ_{n+1} est isomorphe à $\mathbf{Z}/p\mathbf{Z}$. En particulier, on a $\Gamma = \Gamma_{\lambda(n_0)}$, et $\Gamma_{\lambda(n_0)}/\Gamma_{\lambda(n_0)+1} = \mathbf{Z}/p\mathbf{Z}$. Soit x un élément de $\Gamma_{\lambda(n_0)}$ non contenu dans $\Gamma_{\lambda(n_0)+1}$. On peut évidemment considérer G comme un $\mathbf{Z}_p$-module. Soit Γ' le sous-$\mathbf{Z}_p$-module de G engendré par x; on a $\Gamma' \subset \Gamma$, et Γ' est isomorphe à $\mathbf{Z}_p$. Si l'on pose $\Gamma'_n = \Gamma' \cap G_n$, on vérifie tout de suite que Γ'_n/Γ'_{n+1} est isomorphe à $\mathbf{Z}/p\mathbf{Z}$ lorsque n est de la forme $\lambda^s(n_0)$. Appliquant le lemme 2 à l'injection de Γ' dans Γ, on voit que $\Gamma' = \Gamma$, ce qui achève de démontrer la proposition.

Remarques. — Lorsqu'on applique ce qui précède au groupe $H = U^1$, l'ensemble I est l'ensemble des entiers $< e_1 + e$ et premiers à p; c'est un ensemble à e éléments.

Quant aux homomorphismes $\varphi_i : W \to U_i$, définis ici grâce à l'annulation de $\mathrm{Ext}^1(W, G_a)$, il peuvent s'obtenir aussi, de façon explicite, grâce à *l'exponentielle de Artin-Hasse :*

L'exponentielle de Artin-Hasse est un homomorphisme

$$E : \quad W \to 1 + W[[T]],$$

où $1 + W[[T]]$ désigne le groupe multiplicatif des séries formelles à coefficients dans W, et de terme constant égal à 1. A un vecteur de Witt a, elle fait donc correspondre une série formelle en T, qu'on notera $E(a, T)$, et qui est définie par la formule

$$E(a, T) = \exp.\left(-\sum_{n=0}^{\infty} \frac{T^{p^n}}{p^n} . F^n(a)\right)$$

(*cf.*, par exemple, Whaples [26], n° 9, ou Šafarevič [16], § 1).

Si A est un anneau local complet noethérien, de corps résiduel k, et si t appartient à l'idéal maximal de A, on peut substituer t à T dans la série $E(a, T)$, et l'on obtient ainsi un élément $E(a, t)$ du groupe $U(A)$ des unités de A. Il n'est pas difficile de vérifier que l'application $a \to E(a, t)$ est un *morphisme* du groupe proalgébrique W dans le groupe proalgébrique $U(A)$. Dans le cas considéré ici, on prend pour t un élément de valuation i, et le morphisme $A \to E(a, t)$ correspondant est le morphisme φ_i cherché. C'est la méthode suivie par Šafarevič (*loc. cit.*), à une petite complication près, due au fait qu'il travaille avec un corps résiduel qui n'est pas algébriquement clos; c'est aussi la méthode qui, en égale caractéristique, donne la structure de *groupe algébrique* des quotients U^1/U^n ([18], chap. V, n° 16).

§ 2. L'homomorphisme $\theta : \pi_1(U_K) \to \mathfrak{C}_K$.

2.1. **Préliminaires (proalgébriques).** — Dans tout ce paragraphe, K désigne un corps local, de corps résiduel k algébriquement clos. Lorsque k est de caractéristique nulle, on se donne un relèvement de k dans l'anneau A_K des entiers de K. On munit le groupe U_K des unités de K de la structure de groupe proalgébrique définie au § 1.

Soit L une extension finie de K; on sait que L est un corps local, de corps résiduel K. En caractéristique zéro, le relèvement r de k dans A_K peut être considéré comme un relèvement de k dans A_L, et c'est ce relèvement que nous choisirons. On vérifie alors sans difficultés que l'injection de K dans L définit un *morphisme* du groupe proalgébrique U_K dans le groupe U_L; en sens inverse, l'opération de *norme* est un *morphisme* de U_L dans U_K (cela peut se vérifier, soit en remarquant que la norme est donnée par une formule « polynomiale », soit en se ramenant au cas galoisien, où le résultat est évident).

Si L est galoisien sur K, de groupe de Galois $\mathfrak{g}$, les éléments de $\mathfrak{g}$ définissent des *automorphismes* du groupe proalgébrique U_L : c'est évident par transport de structure.

2.2. **Préliminaires (cohomologiques).** — Si $\mathfrak{g}$ est un groupe fini, et A un $\mathfrak{g}$-module, nous noterons $H^q(\mathfrak{g}, A)$ les groupes de cohomologie de $\mathfrak{g}$ à coefficients dans A, modifiés à la Tate; ce sont les groupes $\hat{H}^q(\mathfrak{g}, A)$ de Cartan-Eilenberg ([4], chap. XII); ils sont définis pour tout $q \in \mathbf{Z}$. On a, en particulier :

$$H^0(\mathfrak{g}, A) = A^{\mathfrak{g}}/NA, \qquad H^{-1}(\mathfrak{g}, A) = A_N/IA,$$

$A^{\mathfrak{g}}$ désignant l'ensemble des éléments invariants de A, NA (resp. A_N) désignant l'image (resp. le noyau) de la norme $N : A \to A$, et I désignant l'idéal de l'algèbre de groupe $\mathbf{Z}[\mathfrak{g}]$ engendré par les $1 - \sigma$, pour $\sigma \in \mathfrak{g}$.

Proposition 1. — *Soit L/K une extension galoisienne finie, de groupe de Galois $\mathfrak{g}$. Le $\mathfrak{g}$-module $L^\star$ est alors cohomologiquement trivial* (*cf.* Rim [15]), *autrement dit on a $H^q(\mathfrak{h}, L^\star) = 0$ pour tout $q \in \mathbf{Z}$ et tout sous-groupe $\mathfrak{h}$ de $\mathfrak{g}$.*

Le théorème de Hilbert-Speiser montre que $H^1(\mathfrak{h}, L^\star) = 0$. En vertu du théorème de Tate (*cf.* Tate [23], ou Rim [15], th. 4.12), il suffit donc de prouver que $H^2(\mathfrak{h}, L^\star) = 0$, ou encore que le groupe de Brauer de toute extension finie de K est nul; c'est là un résultat bien connu (on sait même que K est quasi-algébriquement clos, *cf.* Lang [13]).

Au lieu d'utiliser la nullité de H^2, on pourrait aussi utiliser celle de H^0, c'est-à-dire le fait que tout élément de $K^\star$ est norme d'un élément de $L^\star$; on trouvera une démonstration directe de ce fait dans Whaples [24], lemme 2 (*voir* aussi plus loin, n° 3.4, prop. 6).

Corollaire. — *L'application norme $N : L^\star \to K^\star$ applique $L^\star$ sur $K^\star$ et U_L sur U_K.*

Le fait que $N(L^\star) = K^\star$ a déjà été explicité. D'autre part, si $y \in L^\star$ est tel que $N(y)$ soit une unité dans K, il est clair que y est une unité dans L, d'où la seconde partie du corollaire.

Soit maintenant $w : L^\star \to \mathbf{Z}$ la valuation normée du corps local L. Si l'on fait opérer $\mathfrak{g}$ trivialement sur $\mathbf{Z}$, la suite

$$(1) \qquad 0 \to U_L \to L^\star \xrightarrow{w} \mathbf{Z} \to 0$$

est une suite exacte de $\mathfrak{g}$-modules.

Proposition 2. — *Pour tout sous-groupe $\mathfrak{h}$ de $\mathfrak{g}$ et tout $q \in \mathbf{Z}$, l'opérateur cobord*

$$\delta : \quad H^q(\mathfrak{h}, \mathbf{Z}) \to H^{q+1}(\mathfrak{h}, U_L),$$

défini par la suite exacte (1), *est un isomorphisme.*

Cela résulte de la nullité des $H^q(\mathfrak{h}, L^\star)$.

Corollaire. — *Le groupe $H^{-1}(\mathfrak{h}, U_L)$ est isomorphe au groupe $\mathfrak{h}/\mathfrak{h}'$, quotient de $\mathfrak{h}$ par son groupe des commutateurs.*

C'est le cas particulier $q = -2$ de la proposition 2, compte tenu de l'isomorphisme $H^{-2}(\mathfrak{h}, \mathbf{Z}) = \mathfrak{h}/\mathfrak{h}'$ (*cf.* Cartan-Eilenberg, *loc. cit.*, p. 237).

Remarque. — L'isomorphisme $\mathfrak{h}/\mathfrak{h}' \to H^{-1}(\mathfrak{h}, U_L)$ est facile à expliciter. Bornons-nous, pour simplifier, au cas où $\mathfrak{h} = \mathfrak{g}$. Si V_L désigne le noyau de $N : U_L \to U_K$, on a par définition $H^{-1}(\mathfrak{g}, U_L) = V_L/I.U_L$. Si T est une uniformisante de L, l'élément $\sigma(T)/T$ appartient à V_L pour tout $\sigma \in \mathfrak{g}$, et l'on vérifie tout de suite que $\sigma \to \sigma(T)/T$ définit par passage au quotient l'isomorphisme cherché de $\mathfrak{g}/\mathfrak{g}'$ sur $V_L/I.U_L$.

2.3. **L'isomorphisme** $\theta_{L/K} : \pi_1(U_K)/N\pi_1(U_L) \rightarrow \mathfrak{g}/\mathfrak{g}'$. — Nous allons maintenant faire intervenir les structures proalgébriques des groupes U_L et U_K. La suite exacte

$$(2) \qquad 0 \rightarrow V_L \rightarrow U_L \xrightarrow{N} U_K \rightarrow 0$$

montre tout d'abord que V_L est un sous-groupe proalgébrique de U_L. De plus :

PROPOSITION 3. — *La composante connexe de* V_L (au sens de [21], n° 5.1) *est égal à* $I.U_L$.

Le sous-groupe $I.U_L$ est somme des sous-groupes $(1-\sigma).U_L$, $\sigma\in\mathfrak{g}$; comme U_L est connexe, chacun de ces sous-groupes est un groupe proalgébrique connexe, et il en est de même de $I.U_L$; donc $I.U_L$ est contenu dans la composante connexe V_L^0 de V_L. D'autre part, le corollaire à la proposition 2 montre que $V_L/I.U_L$ est un groupe fini. On en conclut que $I.U_L$ contient V_L^0 (*loc. cit.*, prop. 1), d'où la proposition.

COROLLAIRE. — *Le groupe* $\pi_0(V_L)$ *s'identifie au groupe* $\mathfrak{g}/\mathfrak{g}'$.

Cela résulte de la proposition 3, et du corollaire à la proposition 2.

On peut interpréter les résultats précédents de la façon suivante : si l'on divise U_L par $I.U_L$, on obtient un groupe connexe U_L' et la suite exacte (2), jointe à l'isomorphisme $V_L/I.U_L = \mathfrak{g}/\mathfrak{g}'$, donne *la suite exacte*

$$(3) \qquad 0 \rightarrow \mathfrak{g}/\mathfrak{g}' \rightarrow U_L' \rightarrow U_K \rightarrow 0.$$

On a donc associé à toute extension galoisienne L/K une « isogénie » du groupe U_K, ayant pour groupe de Galois le groupe $\mathfrak{g}/\mathfrak{g}'$. Le théorème d'existence montrera que toute isogénie de U_K est obtenue de cette façon, et même au moyen d'une extension abélienne; on obtiendra ainsi une correspondance bijective entre extensions abéliennes de K et isogénies de U_K.

D'un point de vue pratique, il est plus commode de parler de « groupe fondamental » que d' « isogénies ». Au lieu de considérer la suite exacte (3), on écrit la *suite exacte d'homotopie* ([21], n° 5.3) associée à (2) :

$$(4) \qquad \pi_1(U_L) \xrightarrow{N} \pi_1(U_K) \xrightarrow{\partial} \pi_0(V_L) \rightarrow \pi_0(U_L).$$

Comme U_L est connexe, on a $\pi_0(U_L) = 0$. D'autre part, le corollaire à la proposition 3 permet d'identifier $\pi_0(V_L)$ à $\mathfrak{g}/\mathfrak{g}'$. On en déduit donc un *isomorphisme*

$$(5) \qquad \theta_{L/K} : \pi_1(U_K)/N\pi_1(U_L) \rightarrow \mathfrak{g}/\mathfrak{g}',$$

qui va jouer le même rôle que l'isomorphisme de réciprocité en théorie du corps de classes local. Notons tout d'abord :

PROPOSITION 4. — *L'injection de* U_K *dans* U_L *définit une injection de* $\pi_1(U_K)$ *dans* $\pi_1(U_L)$ *qui applique* $\pi_1(U_K)$ *sur* $\pi_1(U_L)^{\mathfrak{g}}$.

Soit $C^i(\mathfrak{g}, U_L)$ le groupe des i-cochaînes de $\mathfrak{g}$ à valeurs dans U_L; c'est un produit d'un certain nombre de copies de U_L, et c'est donc un groupe proalgébrique; on vérifie immédiatement que le cobord

$$d: \quad C^i(\mathfrak{g}, U_L) \to C^{i+1}(\mathfrak{g}, U_L)$$

est un morphisme.

Par définition, on a une suite exacte

$$0 \to (U_L)^{\mathfrak{g}} \to C^0(\mathfrak{g}, U_L) \to C^1(\mathfrak{g}, U_L).$$

Mais le foncteur π_1 est *exact à gauche* ([21], n° 10.2); on a donc la suite exacte

$$0 \to \pi_1((U_L)^{\mathfrak{g}}) \to \pi_1(C^0(\mathfrak{g}, U_L)) \to \pi_1(C^1(\mathfrak{g}, U_L)),$$

qui peut encore s'écrire

$$0 \to \pi_1(U_K) \to C^0(\mathfrak{g}, \pi_1(U_L)) \to C^1(\mathfrak{g}, \pi_1(U_L)).$$

On en déduit bien que $\pi_1(U_K)$ s'identifie à $\pi_1(U_L)^{\mathfrak{g}}$.

C. Q. F. D.

REMARQUE. — Si l'on effectue l'identification $\pi_1(U_K) = \pi_1(U_L)^{\mathfrak{g}}$, l'homomorphisme $N: \pi_1(U_L) \to \pi_1(U_K)$ devient simplement la *norme* dans le $\mathfrak{g}$-module U_L, et le quotient $\pi_1(U_K)/N\pi_1(U_L)$ n'est autre que $H^0(\mathfrak{g}, \pi_1(U_L))$.

2.4. **L'homomorphisme** θ. — Soit M une extension galoisienne de K, contenant l'extension L; nous noterons $\mathfrak{g}_{M/K}$ (resp. $\mathfrak{g}_{L/K}$) le groupe de Galois de M/K (resp. de L/K); le groupe $\mathfrak{g}_{L/K}$ est *quotient* du groupe $\mathfrak{g}_{M/K}$.

PROPOSITION 5. — *Le diagramme suivant est commutatif*

$$(6) \qquad \begin{array}{ccc} \pi_1(U_K)/N\pi_1(U_M) & \to & \pi_1(U_K)/N\pi_1(U_L) \\ \downarrow{\scriptstyle \theta_{M/K}} & & \downarrow{\scriptstyle \theta_{L/K}} \\ \mathfrak{g}_{M/K}/\mathfrak{g}'_{M/K} & \to & \mathfrak{g}_{L/K}/\mathfrak{g}'_{L/K} \end{array}$$

(Les homomorphismes horizontaux étant définis de façon évidente.)

Le diagramme suivant est évidemment commutatif :

$$(7) \qquad \begin{array}{ccccccccc} 0 & \to & V_M & \to & U_M & \to & U_K & \to & 0 \\ & & \downarrow{\scriptstyle N_{M/L}} & & \downarrow{\scriptstyle N_{M/L}} & & \downarrow{\scriptstyle \mathrm{id.}} & & \\ 0 & \to & V_L & \to & U_L & \to & U_K & \to & 0 \end{array}$$

$N_{M/L}$ désignant la norme dans l'extension M/L. On en déduit la commutativité du diagramme

$$(8) \qquad \begin{array}{ccc} \pi_1(U_K)/N\pi_1(U_M) & \xrightarrow{\partial} & \pi_0(V_M) \\ \downarrow & & \downarrow{\scriptstyle N_{M/L}} \\ \pi_1(U_K)/N\pi_1(U_L) & \xrightarrow{\partial} & \pi_0(V_L) \end{array}$$

Vu les définitions de $\theta_{M/K}$ et $\theta_{L/K}$, il ne nous reste plus qu'à établir la commutativité du diagramme suivant :

$$\begin{array}{ccc} \mathfrak{g}_{M/K}/\mathfrak{g}'_{M/K} & \to & \pi_0(V_M) \\ \downarrow & & \downarrow N_{M/L} \\ \mathfrak{g}_{L/K}/\mathfrak{g}'_{L/K} & \to & \pi_0(V_L) \end{array} \tag{9}$$

Or, soit T une uniformisante de M; l'élément $t = N_{M/L}(T)$ est une uniformisante de L. On a vu au n° 2.2 que l'homomorphisme $\mathfrak{g}_{M/K} \to \pi_0(V_M)$ s'obtient à partir de l'application $\sigma \to \sigma(T)/T$. De même $\mathfrak{g}_{M/K} \to \mathfrak{g}_{L/K} \to \pi_0(V_L)$ s'obtient à partir de $\sigma \to \sigma(t)/t$. Comme $N_{M/L}$ commute à σ, on a

$$N_{M/L}(\sigma(T)/T) = \sigma(t)/t,$$

ce qui prouve bien la commutativité de (9), et achève la démonstration.

Soit maintenant $\mathfrak{A}_K$ le groupe de Galois de l'extension abélienne maximale de K; c'est la limite projective des groupes $\mathfrak{g}_{L/K}/\mathfrak{g}'_{L/K}$, pour L parcourant l'ensemble des extensions galoisiennes finies de K. La proposition 5 montre que les homomorphismes $\pi_1(U_K) \to \mathfrak{g}_{L/K}/\mathfrak{g}'_{L/K}$ définis par les $\theta_{L/K}$ sont compatibles entre eux. *Ils définissent donc un homomorphisme*

$$\theta : \quad \pi_1(U_K) \to \mathfrak{A}_K.$$

Proposition 6. — *L'homomorphisme θ est surjectif. Son noyau est l'intersection des groupes $N\pi_1(U_L)$ pour L parcourant l'ensemble des extensions finies séparables (resp. galoisiennes, resp. abéliennes) de K.*

On sait qu'images et noyaux commutent aux limites projectives (*cf.* [21], n° 2.5); d'où la proposition (noter également que les extensions galoisiennes sont cofinales dans les extensions séparables).

Soit maintenant K' une extension séparable finie de K, et soit L une extension galoisienne finie de K, contenant K'. Le groupe $\mathfrak{g}_{L/K'}$ est un sous-groupe d'indice fini de $\mathfrak{g}_{L/K}$; on a donc deux homomorphismes canoniques

$$i : \quad \mathfrak{g}_{L/K'}/\mathfrak{g}'_{L/K'} \to \mathfrak{g}_{L/K}/\mathfrak{g}'_{L/K},$$
$$t : \quad \mathfrak{g}_{L/K}/\mathfrak{g}'_{L/K} \to \mathfrak{g}_{L/K'}/\mathfrak{g}'_{L/K'},$$

le premier étant défini par l'*injection* de $\mathfrak{g}_{L/K'}$ dans $\mathfrak{g}_{L/K}$, le second étant le *transfert* (*cf.* [4], p. 264, exerc. 10).

Par passage à la limite sur L, on en déduit des homomorphismes

$$i : \quad \mathfrak{A}_{K'} \to \mathfrak{A}_K \qquad \text{et} \qquad t : \quad \mathfrak{A}_K \to \mathfrak{A}_{K'}.$$

Proposition 7. — *Les deux diagrammes suivants sont commutatifs*

$$\begin{array}{ccc} \pi_1(U_K) & \xrightarrow{j} & \pi_1(U_{K'}) \\ \theta \downarrow & & \theta \downarrow \\ \mathfrak{A}_K & \xrightarrow{t} & \mathfrak{A}_{K'} \end{array} \tag{10}$$

$$(11)\qquad \begin{array}{ccc} \pi_1(U_{K'}) & \xrightarrow{N} & \pi_1(U_K) \\ \theta \downarrow & & \theta \downarrow \\ \mathfrak{A}_{K'} & \xrightarrow{i} & \mathfrak{A}_K \end{array}$$

l'homomorphisme j étant induit par l'injection $U_K \to U_{K'}$, et l'homomorphisme N par la norme $N_{K'/K} : U_{K'} \to U_K$.

La démonstration sera donnée au numéro suivant.

REMARQUE. — Les homomorphismes j, t, N, i sont définis même si K' est une extension *inséparable* de K. Le diagramme (11) est encore commutatif; le diagramme (10) l'est aussi à condition d'y remplacer t par son produit avec $[K' : K]_i$. [Ces assertions se démontrent, soit directement, soit par réduction au cas où $K' = k((T))$, $K = k((T^p))$.]

2.5. **Une formation de classes.** — Soit de nouveau L/K une extension galoisienne finie, de groupe de Galois $\mathfrak{g}$. Le groupe $\mathfrak{g}$ est un groupe d'automorphismes du groupe proalgébrique U_L; il opère donc aussi sur le *revêtement universel* $\overline{U_L}$ de U_L (*cf.* [21], n° 6.2).

PROPOSITION 8. — *Le $\mathfrak{g}$-module $\overline{U_L}$ est cohomologiquement trivial.*

(La démonstration qui suit m'a été indiquée par J. TATE.)

Puisque le foncteur « revêtement universel » est *exact* ([21], n° 10.3, th. 3), il commute aux groupes de cohomologie (*cf.* la démonstration de la proposition 4). En d'autres termes, si $\mathfrak{h}$ est un sous-groupe de $\mathfrak{g}$, les groupes $H^q(\mathfrak{h}, \overline{U_L})$ s'identifient aux revêtements universels des groupes $H^q(\mathfrak{h}, U_L)$. Comme ces derniers sont des groupes *finis* (prop. 2), leurs revêtements universels sont nuls, d'où la proposition.

Considérons maintenant la suite exacte

$$(12)\qquad 0 \to \pi_1(U_L) \to \overline{U_L} \to U_L \to 0.$$

En la combinant avec la suite exacte (1), on obtient la nouvelle suite exacte

$$(13)\qquad 0 \to \pi_1(U_L) \to \overline{U_L} \to L^* \to \mathbf{Z} \to 0.$$

C'est une suite exacte de $\mathfrak{g}$-modules. Elle donne naissance à un *cobord itéré*

$$\delta^2 : \quad H^q(\mathfrak{g}, \mathbf{Z}) \to H^{q+2}(\mathfrak{g}, \pi_1(U_L)).$$

PROPOSITION 9. — *L'homomorphisme δ^2 défini ci-dessus est un isomorphisme.*

Cela résulte de ce que $\overline{U_L}$ et L^* sont cohomologiquement triviaux.

Pour $q = -2$, on a $H^{-2}(\mathfrak{g}, \mathbf{Z}) = \mathfrak{g}/\mathfrak{g}'$, et

$$H^0(\mathfrak{g}, \pi_1(U_L)) = \pi_1(U_K)/N\pi_1(U_L),$$

on l'a vu.

PROPOSITION 10. — *L'isomorphisme* $\delta^2 : \mathfrak{g}/\mathfrak{g}' \to \pi_1(U_K)/N\pi_1(U_L)$ *et l'isomorphisme* $\theta_{L/K}$ *du* n° 2.3 *sont inverses l'un de l'autre.*

Remontons aux définitions de δ^2 et de $\theta_{L/K}$. Dans les deux cas, on a identifié $\mathfrak{g}/\mathfrak{g}'$ tout d'abord à $H^{-2}(\mathfrak{g}, \mathbf{Z})$, puis à $H^{-1}(\mathfrak{g}, U_L) = V_L/I.U_L$, au moyen du cobord défini par la suite exacte (1). Ensuite, pour définir $\theta_{L/K}$, on a utilisé l'isomorphisme

$$f: \quad \pi_1(U_K)/N\pi_1(U_L) \to V_L/I.U_L = \pi_0(V_L)$$

défini par l'opérateur bord $\partial : \pi_1(U_K) \to \pi_0(V_L)$; pour définir δ^2 on a utilisé l'isomorphisme

$$g: \quad V_L/I.U_L \to \pi_1(U_K)/N\pi_1(U_L)$$

défini par le cobord associé à la suite exacte (12).

Tout revient donc à prouver que $g \circ f = 1$.

Soit $a \in \pi_1(U_K)/N\pi_1(U_L)$, et calculons $f(a)$. Soit $a' \in \pi_1(U_K)$ un représentant de a; on a $f(a) = \partial(a')$. Mais, d'après [21], n° 10.3, on peut calculer $\partial(a')$ de la manière suivante : on choisit $b \in \overline{U_L}$ dont l'image par $N : \overline{U_L} \to \overline{U_K}$ soit égale à a', et l'on considère l'image c de b dans U_L; c'est un élément de V_L dont la classe dans $\pi_0(V_L)$ est égale à $\partial(a') = f(a)$. Pour calculer maintenant $g \circ f(a)$, on doit d'abord relever $f(a)$ en un élément de V_L : on peut prendre c. Puis on doit relever c en un élément de $\overline{U_L}$, et prendre la norme du résultat : on peut choisir b pour relèvement, et comme $N(b) = a'$, on voit qu'on trouve un représentant de a, ce qui démontre que $g \circ f = 1$, et achève la démonstration.

Il n'y a plus maintenant aucune difficulté à expliciter la « formation de classes » des $\pi_1(U_L)$. Observons tout d'abord que la proposition 9, appliquée pour $q = -1$, montre que $H^1(\mathfrak{g}, \pi_1(U_L)) = 0$; pour $q = 0$, si l'on pose $u_{L/K} = \delta^2(1)$, l'élément $u_{L/K}$ engendre le groupe $H^2(\mathfrak{g}, \pi_1(U_L))$, groupe qui est d'ailleurs isomorphe à $\mathbf{Z}/n\mathbf{Z}$, avec $n = [L:K]$. Si $x \in H^q(\mathfrak{g}, \mathbf{Z})$, on a

$$\delta^2(x) = \delta^2(x.1) = x.\delta^2(1) = x.u_{L/K}, \tag{14}$$

le produit étant le *cup-produit* relatif à l'accouplement naturel de $\mathbf{Z} \times \pi_1(U_L)$ dans $\pi_1(U_L)$ (comparer avec TATE [23]).

PROPOSITION 11. — *La donnée des* $\pi_1(U_L)$ *et des classes* $u_{L/K}$ *constituent une formation de classes au sens d'Artin-Tate* (*cf.* KAWADA [12]).

Il nous faut vérifier que les clasees $u_{L/K}$, ou, ce qui revient au même, les homomorphismes δ^2, vérifient certaines propriétés formelles. De façon précise, il y a deux cas à considérer :

(i) On se donne une extension galoisienne M de K contenant l'extension galoisienne L/K; on note $\delta^2_{L/K}$ et $\delta^2_{M/K}$ les cobords itérés relatifs à L/K et M/K respectivement. On doit alors vérifier la formule

$$\mathrm{Inf} \circ \delta^2_{L/K} = [M:L].\delta^2_{M/K} \circ \mathrm{Inf}, \tag{15}$$

où Inf désigne l'homomorphisme appelé « inflation » par ARTIN-TATE (c'est celui qui provient de l'homomorphisme $\mathfrak{g}_{M/K} \rightarrow \mathfrak{g}_{L/K}$; on notera qu'il n'est défini *qu'en degrés positifs*).

La formule (15) résulte tout de suite de la commutativité du diagramme

$$\begin{array}{ccccccccc} 0 \rightarrow & \pi_1(U_M) & \rightarrow & \overline{U_M} & \rightarrow & M^* & \rightarrow & \mathbf{Z} & \rightarrow 0 \\ & \uparrow & & \uparrow & & \uparrow & & \uparrow & \\ 0 \rightarrow & \pi_1(U_L) & \rightarrow & \overline{U_L} & \rightarrow & L^* & \rightarrow & \mathbf{Z} & \rightarrow 0 \end{array} \tag{16}$$

où les flèches verticales sont induites par les injections évidentes, à l'exception de $\mathbf{Z} \rightarrow \mathbf{Z}$ qui est la multiplication par $[M:L]$.

(ii) On se donne une extension finie K' de K, et une extension galoisienne finie L de K, contenant K'. On doit vérifier les formules

$$\mathrm{Res} \circ \delta^2_{L/K} = \delta^2_{L/K'} \circ \mathrm{Res}, \tag{17}$$

$$\mathrm{Cor} \circ \delta^2_{L/K'} = \delta^2_{L/K} \circ \mathrm{Cor}, \tag{18}$$

où Res (resp. Cor) désigne l'homomorphisme de « restriction » (resp. « corestriction » ; c'est le « transfert » de CARTAN-EILENBERG [4], chap. XII, n° 8), défini par l'injection de $\mathfrak{g}_{L/K'}$ dans $\mathfrak{g}_{L/K}$.

Ces formules sont d'ailleurs évidentes, car $\delta^2_{L/K'}$ et $\delta^2_{L/K}$ sont les cobords itérés définis par *la même* suite exacte (13), et l'on sait que les cobords commutent à Res et Cor.

Ceci achève la démonstration de la proposition **11**.

REMARQUE. — Si l'on applique les formules (17) et (18) aux homomorphismes

$$\delta^2_{L/K} : \quad H^{-2}(\mathfrak{g}_{L/K}, \mathbf{Z}) \rightarrow H^0(\mathfrak{g}_{L/K}, \pi_1(U_L))$$

et

$$\delta^2_{L/K'} : \quad H^{-2}(\mathfrak{g}_{L/K'}, \mathbf{Z}) \rightarrow H^0(\mathfrak{g}_{L/K'}, \pi_1(U_L)),$$

on obtient les diagrammes commutatifs

$$\begin{array}{ccc} \pi_1(U_K) & \xrightarrow{j} & \pi_1(U_{K'}) \\ \downarrow & & \downarrow \\ \mathfrak{g}_{L/K}/\mathfrak{g}'_{L/K} & \xrightarrow{t} & \mathfrak{g}_{L/K'}/\mathfrak{g}'_{L/K'} \end{array} \tag{19}$$

$$\begin{array}{ccc} \pi_1(U_{K'}) & \xrightarrow{N} & \pi_1(U_K) \\ \downarrow & & \downarrow \\ \mathfrak{g}_{L/K'}/\mathfrak{g}'_{L/K'} & \xrightarrow{i} & \mathfrak{g}_{L/K}/\mathfrak{g}'_{L/K} \end{array} \tag{20}$$

les lettres j, N, i, t ayant le même sens qu'au numéro 2.4. En passant à la limite sur L, ces diagrammes deviennent identiques aux diagrammes (10) et (11), ce qui démontre la proposition 7.

§ 3. Ramification et conducteur.

3.1. **Groupes de ramification.** — Nous allons rappeler la définition et les principales propriétés de ces groupes. Pour les démonstrations, le lecteur pourra se reporter à Samuel-Zariski [17], chap. V, § 10, ou à Artin [3], chap. IV-V.

Soit K un corps local, et soit L une extension galoisienne finie de K, de groupe de Galois $\mathfrak{g}$. Dans ce numéro, nous ne supposons plus que le corps résiduel k de K est algébriquement clos, mais nous nous bornons au cas où L/K est *totalement ramifiée* (L et K ont même corps résiduel).

Soient A_K et v_K (resp. A_L et v_L) l'anneau des entiers et la valuation normée de K (resp. de L). Si $g=[L:K]$, on a

$$(1) \qquad v_K(x)=g.v_L(x) \quad \text{pour tout } x\in K.$$

Soit T une uniformisante de L. Si n est un entier $\geqq 0$, on notera $\mathfrak{g}_n$ l'ensemble des $\sigma\in\mathfrak{g}$ tels qu'on ait

$$(2) \qquad v_L(\sigma(T)/T-1)\geqq n.$$

La condition (2) équivaut à

$$(3) \qquad v_L(\sigma(x)-x)\geqq n+1 \quad \text{pour tout } x\in A_L.$$

L'ensemble $\mathfrak{g}_n$ est un sous-groupe invariant de $\mathfrak{g}$, appelé $n^{\text{ième}}$ *groupe de ramification* de L/K. Les $\mathfrak{g}_n$ forment une filtration décroissante de $\mathfrak{g}$, avec $\mathfrak{g}_0=\mathfrak{g}$, et $\mathfrak{g}_n=\{1\}$ pour n assez grand.

Proposition 1. — *L'application $\sigma\to\sigma(T)/T$ définit par passage au quotient un isomorphisme de $\mathfrak{g}_n/\mathfrak{g}_{n+1}$ sur un sous-groupe de U_L^n/U_L^{n+1}.*

La démonstration est immédiate.

Corollaire 1. — *Si k est de caractéristique zéro, on a $\mathfrak{g}_1=\{1\}$, et le groupe $\mathfrak{g}$ est cyclique.*

En effet, pour $n\geqq 1$, le groupe U_L^n/U_L^{n+1} est isomorphe à k, et ne contient aucun sous-groupe fini non nul; d'où $\mathfrak{g}_1=\mathfrak{g}_2=\ldots=\{1\}$. De plus le groupe U_L/U_L^1 est isomorphe à k^*, et l'on sait qu'un sous-groupe fini de k^* est cyclique.

Corollaire 2. — *Si k est de caractéristique p, le groupe $\mathfrak{g}_1$ est un p-groupe, et le groupe $\mathfrak{g}/\mathfrak{g}_1$ est cyclique d'ordre premier à p.*

Même démonstration que pour le corollaire 1.

PROPOSITION 2. — *Si* $\mathfrak{h}$ *est un sous-groupe de* $\mathfrak{g}$, *on a* $\mathfrak{h}_n = \mathfrak{h} \cap \mathfrak{g}_n$ *pour tout* $n \geqq 0$.

C'est évident.

La détermination des groupes de ramification d'un *groupe quotient* est moins simple; avant d'énoncer le résultat (dû à HERBRAND [10]), il est nécessaire de définir *une autre numérotation* des groupes $\mathfrak{g}_n$; cela se fait au moyen des fonctions φ et ψ de HASSE (*cf.* [8], ou TAMAGAWA [22]), dont nous allons rappeler la définition :

Pour tout nombre réel positif x, nous définirons $\mathfrak{g}_x$ comme étant égal à $\mathfrak{g}_i$, où i est le plus petit entier $\geqq x$. Nous poserons

$$\varphi(x) = \int_0^x \frac{dt}{(\mathfrak{g} : \mathfrak{g}_t)}. \tag{4}$$

Si l'on note g_i l'ordre du groupe $\mathfrak{g}_i$, et si l'on suppose x compris entre les entiers q et $q+1$, on a

$$\varphi(x) = \frac{1}{g}\left[g_1 + g_2 + \ldots + g_q + (x-q)\, g_{q+1}\right]. \tag{5}$$

Propriétés de la fonction φ.

a. C'est une fonction continue, linéaire par morceaux, strictement croissante, concave.

b. On a $\varphi(0) = 0$.

c. Si l'on désigne par $\varphi'_d(x)$ et $\varphi'_g(x)$ les dérivées à droite et à gauche de φ, on a

$$\varphi'_g(x) = \varphi'_d(x) = 1/(\mathfrak{g} : \mathfrak{g}_x) \quad \text{si } x \text{ n'est pas un entier}, \tag{6}$$

$$\varphi'_g(x) = 1/(\mathfrak{g} : \mathfrak{g}_x) \quad \text{et} \quad \varphi'_d(x) = 1/(\mathfrak{g} : \mathfrak{g}_{x+1}) \quad \text{si } x \text{ est entier}. \tag{7}$$

L'application $\varphi : \mathbf{R}_+ \to \mathbf{R}_+$ est bijective. On notera ψ l'application réciproque.

Propriétés de la fonction ψ.

a'. C'est une fonction continue, linéaire par morceaux, strictement croissante, convexe.

b'. On a $\psi(0) = 0$.

c'. Si $y = \varphi(x)$, on a $\psi'_d(y) = 1/\varphi'_d(x)$, $\psi'_g(y) = 1/\varphi'_g(x)$. En particulier, ψ'_d et ψ'_g ne prennent que des valeurs entières.

d'. Si y est entier, il en est de même de $\psi(y)$.

[Pour démontrer *d'*, on applique (5) avec $x = \varphi(y)$. On trouve

$$(x-q)\, g_{q+1} = gy - (g_1 + \ldots + g_q).$$

Comme g_{q+1} divise $g, g_1, \ldots, g_q$, on en déduit que $x - q$ est entier, d'où le résultat cherché.]

Nous définirons maintenant la *numérotation supérieure* des groupes de ramification en posant

$$(8) \qquad \mathfrak{g}^y = \mathfrak{g}_{\psi(y)} \qquad \text{ou encore} \qquad \mathfrak{g}^{\varphi(x)} = \mathfrak{g}_x.$$

Le théorème de Herbrand s'énonce alors :

PROPOSITION 3. — *Soit* $\mathfrak{k}$ *un sous-groupe invariant de* $\mathfrak{g}$, *et soit* $\mathfrak{h} = \mathfrak{g}/\mathfrak{k}$. *Pour tout* $s \in \mathbf{R}_+$, *on a*

$$(9) \qquad \mathfrak{h}^s = \mathfrak{g}^s \mathfrak{k}/\mathfrak{k}.$$

[Autrement dit, la filtration des $\mathfrak{h}^s$ est *l'image* de la filtration des $\mathfrak{g}^s$.]

Pour la démonstration, *voir* HERBRAND [10], ou ARTIN [3], p. 99.

La proposition 3 permet de définir, par passage à la limite, les groupes de ramification $\mathfrak{g}^s$ d'une *extension galoisienne infinie* L/K, de groupe de Galois $\mathfrak{g}$.

Nous aurons besoin par la suite d'une propriété de *transitivité* des fonctions φ et ψ. Pour l'énoncer, nous conviendrons de noter $\varphi_{L/K}$ et $\psi_{L/K}$ les fonctions φ et ψ relatives à une extension galoisienne L/K.

PROPOSITION 4. — *Soit* K' *une extension galoisienne de* K *contenue dans* L. *On a*

$$(10) \qquad \psi_{L/K} = \psi_{L/K'} \circ \psi_{K'/K} \qquad \textit{et} \qquad \varphi_{L/K} = \varphi_{K'/K} \circ \varphi_{L/K}.$$

La formule relative à $\psi_{L/K}$ est démontrée dans TAMAGAWA [22] (elle est d'ailleurs essentiellement équivalente au théorème de Herbrand). L'autre formule s'en déduit.

REMARQUE. — Comme l'a observé KAWADA, la proposition 4 permet de définir les fonctions $\varphi_{L/K}$ et $\psi_{L/K}$ pour des extensions finies quelconques (pour une extension radicielle, on pose $\varphi(x) = x$).

3.2. **Énoncé du théorème.** — A partir de maintenant, et *jusqu'à la fin de ce paragraphe*, nous revenons aux hypothèses du § 2 ; en particulier, le corps résiduel k de K est supposé *algébriquement clos*.

Puisque le foncteur π_1 est exact à gauche ([21], n° 10.2), l'injection de U_K^n dans U_K définit une injection de $\pi_1(U_K^n)$ dans $\pi_1(U_K)$. Quand n varie, les $\pi_1(U_K^n)$ forment donc une *filtration décroissante* de $\pi_1(U_K)$; le quotient $\pi_1(U_K)/\pi_1(U_K^n)$ s'identifie à $\pi_1(U_K/U_K^n)$, comme le montre la suite exacte d'homotopie. De plus, la formule

$$\bigcap U_K^n = 0$$

montre que $\varprojlim U_K^n = 0$, d'où ([21], n° 5.3, prop. 4) $\varprojlim \pi_1(U_K^n) = 0$, c'est-à-dire $\bigcap \pi_1(U_K^n) = 0$. La filtration des $\pi_1(U_K^n)$ est donc *séparée*. Il est commode d'étendre cette filtration aux valeurs réelles positives de l'exposant, en posant

$$U_K^s = U_K^n \quad \text{si } n \text{ est le plus petit entier} \geqq s.$$

D'autre part, si $\mathfrak{A}_K$ désigne le groupe de Galois de l'extension abélienne maximale de K, on peut filtrer $\mathfrak{A}_K$ au moyen des groupes de ramification $\mathfrak{A}_K^s$, définis comme il a été dit au numéro précédent.

Théorème 1. — *L'homomorphisme* $\theta : \pi_1(U_K) \to \mathfrak{A}_K$, *défini au* § 2, *applique* $\pi_1(U_K^s)$ *sur* $\mathfrak{A}_K^s$, *pour tout* $s \in \mathbf{R}_+$.

La démonstration sera donnée au n° 3.5. Observons tout de suite que le cas d'un corps résiduel de caractéristique zéro est trivial. En effet, on a alors $\mathfrak{A}_K^s = 0$ pour tout $s > 0$ (cor. 1 à la prop. 1), et $\pi_1(U_K^s) = 0$ pour tout $s > 0$ car U_K^s est unipotent, donc simplement connexe d'après [21], n° 8.2.

3.3. Cas d'une extension cyclique de degré premier. — Dans tout ce numéro, L/K désigne une extension *cyclique de degré premier* l; on note $\mathfrak{g}$ son groupe de Galois. On conserve les notations et hypothèses du n° 3.1 (et l'on suppose, en outre, que k est algébriquement clos).

Il existe évidemment un entier $t \geqq 0$ tel qu'on ait

$$\mathfrak{g} = \mathfrak{g}_0 = \ldots = \mathfrak{g}_t,$$
$$\mathfrak{g}_{t+1} = \mathfrak{g}_{t+2} = \ldots = \{1\}.$$

Le calcul des fonctions φ et ψ est immédiat. On trouve

$$\psi(x) = \begin{cases} x & \text{si } x \leqq t. \\ t + l(x-t) & \text{si } x \geqq t. \end{cases} \tag{11}$$

Nous noterons $\mathfrak{P}$ (resp. $\mathfrak{p}$) l'idéal maximal de A_L (resp. A_K).

Lemme 1. — *La différente* $\mathfrak{D}$ *de l'extension* L/K *est égale à* $\mathfrak{P}^m$, *avec* $m = (t+1)(l-1)$.

Si T est une uniformisante de L, on sait que $\mathfrak{D}$ est engendrée par $\prod_{\sigma \neq 1} (\sigma(T) - T)$; comme chaque terme a une valuation égale à $t+1$, on en déduit bien le lemme.

Lemme 2. — *Soit* $\mathrm{Tr} : L \to K$ *la trace dans l'extension* L/K. *Posons* $m = (t+1)(l-1)$. *Pour tout entier* $s \geqq 0$, *on a*

$$\mathrm{Tr}(\mathfrak{P}^s) = \mathfrak{p}^r, \quad \textit{avec} \quad r = [(m+s)/l]. \tag{12}$$

[Le symbole $[x]$ désigne la *partie entière* du nombre réel x.]

Puisque la trace est une application A_K-linéaire de A_L dans A_K, $\mathrm{Tr}(\mathfrak{P}^s)$ est un idéal de A_K. Si r est un entier $\geqq 0$, on a $\mathrm{Tr}(\mathfrak{P}^s) \subset \mathfrak{p}^r$ si et seulement si $\mathrm{Tr}(\mathfrak{p}^{-r}\mathfrak{P}^s) \subset A_K$, c'est-à-dire si $\mathfrak{p}^{-r}\mathfrak{P}^s \subset \mathfrak{D}^{-1}$, vu la définition de la différente au moyen de la trace; d'après le lemme 1, cette dernière inclusion équivaut à l'inégalité $s - lr \geqq -m$, c'est-à-dire $r \leqq [(m+s)/l]$.

C. Q. F. D.

Lemme 3. — *Si T_s est un élément de L de valuation $\geqq s$, on a*

$$(13) \qquad N(1+T_s) \equiv 1 + \mathrm{Tr}(T_s) + N(T_s) \mod \mathrm{Tr}(\mathfrak{P}^{2s}).$$

On a, par définition,

$$N(1+T_s) = \prod_{\sigma \in \mathfrak{g}} (1 + T_s^{\sigma}),$$

d'où, en développant,

$$N(1+T_s) = \sum_{\lambda} T_s^{\lambda},$$

où λ parcourt l'ensemble des éléments de l'algèbre de groupe $\mathbf{Z}[\mathfrak{g}]$ qui sont de la forme $\lambda = \sigma_1 + \ldots + \sigma_k$, les σ_i étant des éléments de $\mathfrak{g}$ deux à deux distincts. On posera $n(\lambda) = k$: c'est *l'augmentation* de λ. Les λ d'augmentation $0, 1$ et l donnent les termes 1, $\mathrm{Tr}(T_s)$ et $N(T_s)$ de la formule (13). Tout revient donc à prouver que la somme des autres termes appartient à $\mathrm{Tr}(\mathfrak{P}^{2s})$. Or, soit σ un générateur de $\mathfrak{g}$. Si $\sigma = \sigma\lambda$, l'élément λ est nécessairement multiple de la norme. Si $2 \leqq n(\lambda) \leqq l-1$, on a donc $\lambda \neq \sigma\lambda$. Groupant ensemble les $\sigma^i\lambda$, $0 \leqq i \leqq l-1$, on obtient $\mathrm{Tr}(T_s^{\lambda})$; comme $n(\lambda) \geqq 2$, on a $T_s^{\lambda} \in \mathfrak{P}^{2s}$, d'où $\mathrm{Tr}(T_s^{\lambda}) \in \mathrm{Tr}(\mathfrak{P}^{2s})$, ce qui achève la démonstration.

Proposition 5.

(*a*) *Pour tout entier $s \geqq 0$, on a $N(U_L^{\psi(s)}) = U_K^s$ et $N(U_L^{\psi(s)+1}) = U_K^{s+1}$.*

(*b*) *Soit $N_s : U_L^{\psi(s)}/U_L^{\psi(s)+1} \to U_K^s/U_K^{s+1}$ l'application définie par passage au quotient à partir de N. Pour $s \neq t$, N_s est un isomorphisme. Pour $s = t$, on a la suite exacte*

$$(14) \qquad 0 \to \mathfrak{g} \xrightarrow{\gamma} U_L^t/U_L^{t+1} \xrightarrow{N_t} U_K^t/U_K^{t+1} \to 0,$$

où γ est défini par $\sigma \to \sigma(T)/T$ (cf. proposition 1).

Nous démontrerons simultanément (*b*) et un résultat plus faible que (*a*) :

(*a'*) *On a $N(U_L^{\psi(s)}) \subset U_K^s$ et $N(U_L^{\psi(s)+1}) \subset U_K^{s+1}$.*

Une fois (*a'*) et (*b*) démontrés, on peut appliquer le lemme 2 du numéro 1.6 au groupe complet $U_L^{\psi(s)}$, filtré par les $U_L^{\psi(s+n)}$, et au groupe U_K^s, filtré par les U_K^{s+n} : comme $\psi(s)+1 \leqq \psi(s+1)$, (*b*) montre que N applique

$U_L^{\psi(s+n)}/U_L^{\psi(s+n+1)}$ *sur* U_K^{s+n}/U_K^{s+n+1}, donc, d'après le lemme en question, N applique $U_L^{\psi(s)}$ *sur* U_K^s. On en déduit aussi $N(U_L^{\psi(s)+1}) \supset N(U_L^{\psi(s+1)}) = U_K^{s+1}$ et, en tenant compte de (a'), on voit bien que $N(U_L^{\psi(s)+1}) = U_K^{s+1}$.

Tout revient donc à démontrer (a') et (b). Nous distinguerons quatre cas :

(i) *On a* $s = 0$.

Il est clair que $N(U_L^0) \subset U_K^0$ et $N(U_L^1) \subset U_K^1$. Le morphisme

$$N_0 : \quad G_m \to G_m$$

est donné par $\lambda \to \lambda^l$. Si l est égal à la caractéristique de k, N_0 est un isomorphisme; comme on a $t \geqq 1$ dans ce cas (n° 3.1, cor. 2 à la prop. 1), on a bien vérifié (b). Si, d'autre part, l n'est pas égal à la caractéristique de k, on a $t = 0$ (*loc. cit.*), et le noyau de N_0 est le groupe cyclique d'ordre l formé des racines $l^{\text{ièmes}}$ de l'unité; d'après la proposition 1, ce groupe s'identifie à $\mathfrak{g}$ au moyen de γ, d'où encore (b) dans ce cas.

(ii) *On a* $1 \leqq s < t$.

Puisque $t \geqq 1$, le nombre premier l est nécessairement égal à la caractéristique de k, caractéristique que nous noterons p. On a de plus $\psi(s) = s$.

Soit $X_s \in \mathfrak{P}^s$; on a $N(X_s) \in \mathfrak{p}^s$. D'autre part, le lemme 2 montre que la valuation de $\mathrm{Tr}(X_s)$ est supérieure ou égale à l'entier

$$\left[\frac{(t+1)(l-1)+s}{l}\right] \geqq \left[s+2-\frac{2}{l}\right] \geqq s+1.$$

Le même calcul montre que $\mathrm{Tr}(\mathfrak{P}^{2s}) \subset \mathfrak{p}^{s+1}$. D'après le lemme 3, on a donc

$$(15) \qquad N(1+X_s) \equiv 1 + N(X_s) \mod \mathfrak{p}^{s+1}.$$

Comme $N(X_s)$ appartient à $\mathfrak{p}^s$, cette formule montre que N applique U_L^s dans U_K^s; si $X_s \in \mathfrak{P}^{s+1}$, on a $N(X_s) \in \mathfrak{p}^{s+1}$, donc N applique U_L^{s+1} dans U_K^{s+1}, ce qui démontre (a'). Pour déterminer N_s, choisissons un élément T_s de valuation s dans L; tout élément de U_L^s est congru modulo U_L^{s+1} à un élément de la forme $1 + a\mathrm{T}_s$, avec $a \in A_K$. Appliquant (15) à aT_s, on trouve

$$(16) \qquad N(1+aT_s) \equiv 1 + a^p N(T_s) \mod \mathfrak{p}^{s+1}.$$

Si l'on identifie U_L^s/U_L^{s+1} et U_K^s/U_K^{s+1} au groupe additif G_a (*cf.* n° 1.6), la formule (16) montre que N_s est de la forme $\lambda \to \alpha\lambda^p$; comme $N(T_s)$ est un élément de valuation s, on a $\alpha \neq 0$, et N_s est un isomorphisme, ce qui achève de prouver (b) dans ce cas.

(iii) *On a* $1 \leqq s = t$.

Ici encore, $l = p$, et $\psi(t) = t$. Soit $X_t \in \mathfrak{P}^t$; un calcul analogue à celui du cas précédent montre que

$$(17) \qquad N(1+X_t) \equiv 1 + \mathrm{Tr}(X_t) + N(X_t) \mod \mathfrak{p}^{t+1}.$$

Cette formule, jointe au lemme 2, montre que $N(1+X_t) \equiv 1 \mod \mathfrak{p}^{t+1}$ si $X_t \in \mathfrak{P}^{t+1}$, d'où (a'). Pour démontrer (b), on choisit un $X_t \in \mathfrak{P}^t$ tel que $\mathrm{Tr}(X_t)$ soit de valuation t : c'est possible en vertu du lemme 2. Si $a \in A_K$, on a

$$(18) \qquad N(1+aX_t) \equiv 1 + a\,\mathrm{Tr}(X_t) + a^p N(X_t) \mod \mathfrak{p}^{t+1}.$$

Par passage au quotient, cette formule montre que $N_t : G_a \rightarrow G_a$ est de la forme $\lambda \rightarrow \alpha\lambda + \beta\lambda^p$, avec $\alpha\beta \neq 0$. Le morphisme N_t est donc surjectif et son noyau est cyclique d'ordre p. Comme $N(\sigma(T)/T) = 1$, ce noyau contient l'image de $\mathfrak{g}$ par γ, donc est égal à cette image, ce qui démontre bien (b) dans ce cas.

(iv) *On a* $s > t$.

Ici $\psi(s) = t + l(s-t)$. Si $X_s \in \mathfrak{P}^{\psi(s)}$, le lemme 2 montre que $\mathrm{Tr}(X_s) \in \mathfrak{p}^s$, et le lemme 3 donne la formule

$$(19) \qquad N(1+X_s) \equiv 1 + \mathrm{Tr}(X_s) \mod \mathfrak{p}^{s+1}.$$

Le morphisme $N_s : G_a \rightarrow G_a$ est de la forme $\lambda \rightarrow \alpha\lambda$, avec $\alpha \neq 0$; c'est un isomorphisme.

Nous avons donc vérifié (a') et (b) dans tous les cas.

C. Q. F. D.

3.4. Extensions abéliennes.

Proposition 6. — *Soit L/K une extension galoisienne finie, de groupe de Galois $\mathfrak{g}$, et soit ψ la fonction associée* (*cf.* n° 3.1).

(*a*) *Pour tout entier $s \geq 0$, on a $N(U_L^{\psi(s)}) = U_K^s$ et $N(U_L^{\psi(s)+1}) = U_K^{s+1}$.*

(*b*) *Soit $N_s : U_L^{\psi(s)}/U_L^{\psi(s)+1} \rightarrow U_K^s/U_K^{s+1}$ l'application définie par passage au quotient à partir de N, et soit γ_s l'homomorphisme de $\mathfrak{g}_{\psi(s)}/\mathfrak{g}_{\psi(s)+1}$ dans $U_L^{\psi(s)}/U_L^{\psi(s)+1}$ défini par $\sigma \rightarrow \sigma(T)/T$ (cf. prop. 1). La suite*

$$(20) \quad 0 \rightarrow \mathfrak{g}_{\psi(s)}/\mathfrak{g}_{\psi(s)+1} \xrightarrow{\gamma_s} U_L^{\psi(s)}/U_L^{\psi(s)+1} \xrightarrow{N_s} U_K^s/U_K^{s+1} \rightarrow 0$$

est alors exacte.

Nous raisonnerons par récurrence sur l'ordre g de $\mathfrak{g}$, le cas $g=1$ étant trivial. Les corollaires de la proposition 1 montrent que $\mathfrak{g}$ est *résoluble*. Il existe donc une sous-extension K'/K de L/K telle que K'/K soit cyclique d'ordre premier, et que L/K' soit galoisienne. D'après l'hypothèse de récurrence (resp. la proposition 5), la proposition est vraie pour L/K' (resp. pour K'/K). Si l'on pose

$$s' = \psi_{K'/K}(s), \qquad s'' = \psi_{L/K'}(s'),$$

on a donc

$$N_{L/K'}(U_L^{s''}) = U_{K'}^{s'} \quad \text{et} \quad N_{K'/K}(U_{K'}^{s'}) = U_K^s, \qquad \text{d'où} \qquad N_{L/K}(U_L^{s''}) = U_K^s.$$

La proposition 4 montre que $s''=\psi_{L/K}(s)$, ce qui démontre la première formule de (a). La seconde se démontre de même. Pour (b), on remarque que N_s se factorise en

$$U_L^{s''}/U_L^{s''+1} \xrightarrow{N''} U_{K'}^{s'}/U_{K'}^{s'+1} \xrightarrow{N'} U_K^s/U_K^{s+1},$$

où N'' et N' sont respectivements induits par $N_{L/K'}$ et $N_{K'/K}$. On en déduit que N_s est surjectif, et que l'ordre m de son noyau est égal au produit des ordres m' et m'' des noyaux de N' et N''. Si $\mathfrak{h}$ est le groupe de Galois de L/K', la proposition 6 (appliquée à L/K', ce qui est licite), montre que $m''=(\mathfrak{h}_{s''}:\mathfrak{h}_{s''+1})$. Convenons de noter $f'_{d/g}(x)$ le quotient $f'_d(x)/f'_g(x)$ de la dérivée à droite de f en x par la dérivée à gauche en x, Les propriétés de ψ énoncées au nº 3.1 montrent qu'on a

$$m''=(\psi_{L/K'})'_{d/g}(s').$$

De même, $m'=(\psi_{K'/K})'_{d/g}(s)$. Comme $\psi_{L/K}=\psi_{L/K'}\circ\psi_{K'/K}$, la formule donnant la dérivée d'une fonction composée montre qu'on a

$$m=\psi'_{d/g}(s)=(\mathfrak{g}_{\psi(s)}:\mathfrak{g}_{\psi(s)+1}). \tag{21}$$

D'autre part, on sait que γ_s est injectif, et il est clair que $\mathrm{Ker}(N_s)\supset \mathrm{Im}(\gamma_s)$. La formule précédente montre que ces deux groupes ont même nombre d'éléments; ils sont donc égaux, ce qui achève la démonstration.

Corollaire. — *Pour tout $s\in\mathbf{R}_+$, on a $N\big(U_L^{\psi(s)}\big)=U_K^s$.*

Choisissons des entiers r et t tels que

$$r<s\leqq r+1 \qquad \text{et} \qquad t<\psi(s)\leqq t+1.$$

On a alors, par définition (*cf.* nº 3.2), $U_K^s=U_K^{r+1}$ et $U_L^{\psi(s)}=U_L^{t+1}$. Comme les inégalités écrites ci-dessus entraînent

$$\psi(r)+1\leqq t+1\leqq\psi(r+1),$$

la proposition précédente montre que $N(U_L^{t+1})=U_K^{r+1}=U_K^s$.

C. Q. F. D.

Remarques.

1º Le corollaire ci-dessus s'étend immédiatement au cas où l'extension L/K n'est plus supposée galoisienne, ni même séparable.

2º La proposition précédente est essentiellement due à Hasse [8]. On notera que, lorsqu'on ne suppose pas k algébriquement clos, la suite exacte (20) doit être remplacée par une *suite exacte de k-groupes quasi-algébriques*. Le fait qu'un point rationnel d'un quotient ne puisse pas toujours se remonter en un point rationnel explique pourquoi l'application norme n'est plus surjective (Hasse, *loc. cit.*).

Nous allons maintenant étudier d'un peu plus près le noyau V_L de l'homomorphisme $N : U_L \to U_K$. Pour tout entier $n \geqq 0$, nous poserons

$$V_n = V_L \cap U_L^{\psi(n)}. \tag{22}$$

Le groupe V_n est le noyau de $N : U_L^{\psi(n)} \to U_K^n$.

Proposition 7. — *On a une suite exacte :*

$$0 \to U_L^{\psi(n)+1}/U_L^{\psi(n+1)} \to V_n/V_{n+1} \to \mathfrak{g}_{\psi(n)}/\mathfrak{g}_{\psi(n)+1} \to 0. \tag{23}$$

Il est clair que V_n/V_{n+1} s'identifie au noyau de l'homomorphisme $\overline{N}_n : U_L^{\psi(n)}/U_L^{\psi(n+1)} \to U_K^n/U_K^{n+1}$ défini par la norme. De plus, la proposition 6 montre que $\overline{N}_n$ est nul sur le sous-groupe $U_L^{\psi(n)+1}/U_L^{\psi(n+1)}$ de $U_K^{\psi(n)}/U_K^{\psi(n+1)}$; la suite exacte (23) résulte immédiatement de là, et de la suite exacte (20).

Corollaire 1. — *Le groupe $\pi_0(V_n/V_{n+1})$ s'identifie au quotient $\mathfrak{g}_{\psi(n)}/\mathfrak{g}_{\psi(n)+1}$.*

C'est évident.

[Comme d'habitude, l'identification fait correspondre à $\sigma \in \mathfrak{g}_{\psi(n)}$ la classe dans $\pi_0(V_n/V_{n+1})$ de $\sigma(T)/T$.]

Corollaire 2. — *Le groupe $\pi_0(V_n)$ est un groupe fini dont l'ordre divise le produit des indices $(\mathfrak{g}_{\psi(n+k)} : \mathfrak{g}_{\psi(n+k)+1})$, pour k entier $\geqq 0$.*

Supposons d'abord que n soit assez grand pour que $g_{\psi(n)} = \{1\}$. Le corollaire 1 montre que $\pi_0(V_{n+1}) \to \pi_0(V_n)$ est surjectif. En appliquant ce résultat à $n+1$, $n+2$, et en passant à la limite, on voit que $\varprojlim \pi_0(V_{n+k}) \to \pi_0(V_n)$ est surjectif. Mais $\varprojlim V_{n+k} = \bigcap V_{n+k} = 0$, d'où ([21], n° 5.1, prop. 2) $\varprojlim \pi_0(V_{n+k}) = 0$ et $\pi_0(V_n) = 0$. Le corollaire 2 est donc exact pour n assez grand. D'autre part, le corollaire 1 montre que, si le corollaire 2 est exact pour $n+1$, il l'est pour n. D'où le résultat cherché.

Corollaire 3. — *L'application $\sigma \to \sigma(T)/T$ définit par passage au quotient un homomorphisme surjectif*

$$\delta_n : \quad \mathfrak{g}_{\psi(n)} \to \pi_0(V_n).$$

Soient $\sigma, \tau \in \mathfrak{g}_{\psi(n)}$. On a

$$\sigma\tau(T)/T = \sigma(T)/T . \tau(T)/T . \sigma(u)/u, \qquad \text{avec} \quad u = \tau(T)/T.$$

Les éléments de la forme $\sigma(u)/u$, $u \in U_L$ forment un sous-groupe connexe de V_n; leur image dans $\pi_0(V_n)$ est donc nulle, et δ_n est un *homomorphisme*. Un argument analogue montre qu'il ne dépend pas du choix de l'uniformisante T.

Le corollaire 1 montre que, si δ_{n+1} est surjectif, il en est de même de δ_n. Comme $\pi_0(V_n) = 0$ pour n assez grand, ceci démontre le corollaire.

3.5. **Extensions abéliennes.** — Nous conservons toutes les notations du numéro précédent.

PROPOSITION 8. — *Supposons l'extension L/K abélienne. Pour tout entier $n \geq 0$ on a :*

(i) $\mathfrak{g}_{\psi(n)+1} = \mathfrak{g}_{\psi(n+1)}$.

(ii) *L'homomorphisme $\delta_n : \mathfrak{g}_{\psi(n)} \to \pi_0(V_n)$ est bijectif.*

(iii) *L'homomorphisme $\pi_0(V_n) \to \pi_0(V_L)$ défini par l'inclusion de V_n dans V_L est injectif.*

(iv) *Soit $\partial : \pi_1(U_K) \to \pi_0(V_L)$ l'homomorphisme bord dans la suite exacte* (2) *du* n° 2.3. *L'image par ∂ de $\pi_1(U_K^n)$ est égale à $\pi_0(V_n)$.*

[Dans (iv), on convient d'identifier $\pi_0(V_n)$ à un sous-groupe de $\pi_0(V_L)$, ce qui est licite d'après (iii).]

DÉMONSTRATION DE (i). — En appliquant le corollaire 2 de la proposition 3 avec $n = 0$, on voit que l'ordre de $\pi_0(V_L)$ divise le produit des $(\mathfrak{g}_{\psi(n)} : \mathfrak{g}_{\psi(n)+1})$, pour n entier ≥ 0. Si l'on avait $\mathfrak{g}_{\psi(n)+1} \neq \mathfrak{g}_{\psi(n+1)}$ pour un entier n, ce produit serait strictement inférieur à l'ordre de $\mathfrak{g}$; mais c'est impossible, car, puisque $\mathfrak{g}$ est abélien, il est isomorphe à $\pi_0(V_L)$ (*cf.* n° 2.3, cor. à la prop. 3).

DÉMONSTRATION DE (ii). — On raisonne par récurrence sur n, le cas $n = 0$ étant connu. Le diagramme

$$
\begin{tikzcd}
 & \pi_0(V_{n+1}) \arrow[r] & \pi_0(V_n) \arrow[r] & \pi_0(V_n/V_{n+1}) \arrow[r] & 0 \\
0 \arrow[r] & \mathfrak{g}_{\psi(n+1)} \arrow[r] \arrow[u, "\delta_{n+1}"] & \mathfrak{g}_{\psi(n)} \arrow[r] \arrow[u, "\delta_n"] & \mathfrak{g}_{\psi(n)}/\mathfrak{g}_{\psi(n+1)} \arrow[r] \arrow[u] & 0
\end{tikzcd}
\tag{24}
$$

est commutatif. Tenant compte de l'hypothèse de récurrence et du corollaire 1 à la proposition 7, on voit que δ_{n+1} est injectif. Comme on sait qu'il est surjectif, c'est bien un isomorphisme.

DÉMONSTRATION DE (iii). — Le diagramme (24) montre que $\pi_0(V_{n+1}) \to \pi_0(V_n)$ est injectif. En itérant, on obtient le résultat cherché.

DÉMONSTRATION DE (iv). — On a le diagramme commutatif :

$$
\begin{tikzcd}
0 \arrow[r] & V_n \arrow[r] \arrow[d] & U_L^{\psi(n)} \arrow[r, dashed] \arrow[d] & U_K^n \arrow[r] \arrow[d] & 0. \\
0 \arrow[r] & V_L \arrow[r] & U_L \arrow[r] & U_K \arrow[r] & 0
\end{tikzcd}
\tag{25}
$$

On en tire le diagramme commutatif :

$$
\begin{tikzcd}
\pi_1(U_K^n) \arrow[r] \arrow[d] & \pi_0(V_n) \arrow[d] \\
\pi_1(U_K) \arrow[r] & \pi_0(V_L)
\end{tikzcd}
\tag{26}
$$

ce qui exprime exactement (iv).

Corollaire 1. — *Si m est un entier $\geqq 0$ tel que $\mathfrak{g}_m \neq \mathfrak{g}_{m+1}$, le nombre réel $\varphi(m)$ est un entier.*

Si $\varphi(m)$ n'était pas entier, il existerait un entier $n \geqq 0$ tel que

$$\psi(n) < m < \psi(n+1).$$

Comme m est entier, on aurait

$$m \geqq \psi(n) + 1 \qquad \text{et} \qquad m + 1 \leqq \psi(n+1).$$

En appliquant (i) on trouverait

$$\mathfrak{g}_{\psi(n)+1} = \mathfrak{g}_m = \mathfrak{g}_{m+1} = \mathfrak{g}_{\psi(n+1)},$$

contrairement à l'hypothèse.

Corollaire 2. — *Soit $\theta_L : \pi_1(U_K) \to \mathfrak{g}$ l'homomorphisme défini au* § 2. *Pour tout $s \in \mathbf{R}_+$, l'image par θ_L de $\pi_1(U_K^s)$ est égale à $\mathfrak{g}^s = \mathfrak{g}_{\psi(s)}$.*

Supposons d'abord que s soit entier. Par définition, θ_L s'obtient en composant $\partial : \pi_1(U_K) \to \pi_0(V_L)$, avec l'isomorphisme réciproque de $\partial : \mathfrak{g} \to \pi_0(V_L)$. La formule $\theta_L(\pi_1(U_K^s)) = \mathfrak{g}_{\psi(s)}$ résulte immédiatement de là et des assertions (ii) et (iv).

Dans le cas général, soient r et t deux entiers tels que

$$r < s \leqq r + 1 \qquad \text{et} \qquad t < \psi(s) \leqq t + 1.$$

On a

$$\psi(r) + 1 \leqq t + 1 \leqq \psi(r+1), \qquad \text{d'où} \qquad \mathfrak{g}_{t+1} = \mathfrak{g}_{\psi(r+1)},$$

d'après (i). Par définition, on a $U_K^s = U_K^{r+1}$, $\mathfrak{g}_{\psi(s)} = \mathfrak{g}_{t+1}$. En appliquant à $r+1$ le résultat démontré ci-dessus, il vient

$$\theta_L(\pi_1(U_K^s)) = \theta_L(\pi_1(U_K^{r+1})) = \mathfrak{g}_{\psi(r+1)} = \mathfrak{g}_{t+1} = \mathfrak{g}_{\psi(s)}.$$

C. Q. F. D.

Remarques.

1° Par passage à la limite sur L, on voit que le corollaire 2 reste valable même si L est une *extension abélienne infinie* de K.

En prenant pour L l'extension abélienne maximale de K, on a $\mathfrak{g} = \mathfrak{A}_K$, et *l'on a donc démontré le théorème* 1 *du* n° 3.2.

2° Soit n un entier $\geqq 0$. On vient de voir que θ_L applique $\pi_1(U_K^n)$ sur $\mathfrak{g}^n$, et $\pi_1(U_K^{n+1})$ sur $\mathfrak{g}^{n+1}$. Par passage au quotient, il définit donc un homomorphisme $\theta_n : \pi_1(U_K^n/U_K^{n+1}) \to \mathfrak{g}^n/\mathfrak{g}^{n+1}$. *Cet homomorphisme n'est autre que l'homomorphisme bord associé à la suite exacte* (20), *relative à $s = n$.* C'est immédiat, à partir du diagramme commutatif :

$$\begin{array}{ccccccccc} 0 & \to & V_n & \to & U_L^{\psi(n)} & \to & U_K^n & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \mathfrak{g}^n/\mathfrak{g}^{n+1} & \to & U_L^{\psi(n)}/U_L^{\psi(n)+1} & \to & U_K^n/U_K^{n+1} & \to & 0. \end{array} \tag{27}$$

En particulier, dans le cas d'une extension cyclique de degré premier, θ_L est nul sur $\pi_1(U_K^{t+1})$, et l'homomorphisme de $\pi_1(U_K^t)/\pi_1(U_K^{t+1})$ sur $\mathfrak{g}$ qu'il définit n'est autre que l'opérateur bord dans la suite exacte (14).

3° Le corollaire 1 impose des conditions très restrictives à la filtration des groupes de ramification. Considérons, par exemple, le cas d'un groupe $\mathfrak{g}$ cyclique d'ordre p^k. Notons $\mathfrak{g}(i)$ le sous-groupe de $\mathfrak{g}$ d'ordre p^i, et soit n_i le nombre des entiers n tels que $\mathfrak{g}_n = \mathfrak{g}(i)$. Le corollaire 1 équivaut à dire que n_i *est divisible par* p^{k-i}.

3.6. **Conducteur (cas abélien).** — Gardons les notations et hypothèses du numéro précédent. On appelle *conducteur* de l'extension L/K le plus petit entier f tel que l'homomorphisme

$$\theta_L : \quad \pi_1(U_K) \to \mathfrak{g}$$

soit trivial sur $\pi_1(U_K^f)$.

PROPOSITION 9. — *Soit c l'unique entier tel que $\mathfrak{g}_c \neq \{1\}$ et $\mathfrak{g}_{c+1} = \{1\}$* (si $L = K$, on convient de poser $c = -1$). *Le conducteur f de L/K est égal à $\varphi(c)+1$.*

Le cas $L = K$ est trivial : on a $f = 0$. Supposons donc $L \neq K$. D'après le corollaire 2 à la proposition 8, f est le plus petit entier ≥ 0 tel que $\mathfrak{g}_{\psi(f)} = \{1\}$. On a donc $f \geq 1$, et $\mathfrak{g}_{\psi(f-1)} \neq \{1\}$. D'autre part, l'assertion (i) de la proposition 8 montre que

$$\mathfrak{g}_{\psi(f-1)+1} = \mathfrak{g}_{\psi(f)} = \{1\}.$$

On a donc $c = \psi(f-1)$, c'est-à-dire $f = \varphi(c)+1$. C. Q. F. D.

3.7. **Le conducteur d'Artin.** — Rappelons d'abord sa définition (*cf.* ARTIN [2], *voir* aussi [20]). Soit L/K une extension galoisienne finie, de groupe de Galois $\mathfrak{g}$. Si χ est une *fonction centrale* sur $\mathfrak{g}$, à valeurs complexes, on pose

$$\chi(\mathfrak{g}_i) = \frac{1}{g_i} \sum_{\sigma \in \mathfrak{g}_i} \chi(\sigma), \qquad g_i \text{ désignant l'ordre de } \mathfrak{g}_i. \tag{28}$$

Le *conducteur* $f(\chi)$ de χ est le nombre complexe défini par

$$f(\chi) = \frac{1}{g} \sum_{i=0}^{i=\infty} g_i(\chi(1) - \chi(\mathfrak{g}_i)), \tag{29}$$

somme qui a un sens puisque $\chi(1) - \chi(\mathfrak{g}_i) = 0$ pour i assez grand. On a évidemment

$$f(\lambda_1\chi_1 + \lambda_2\chi_2) = \lambda_1 f(\chi_1) + \lambda_2 f(\chi_2). \tag{30}$$

Il suffit donc de connaître $f(\chi)$ lorsque χ est un *caractère* de $\mathfrak{g}$, et même, si l'on veut, un *caractère irréductible*. Dans ce cas, il est immédiat que $f(\chi)$ est un nombre rationnel positif. En fait :

THÉORÈME 2. — *Si χ est un caractère de $\mathfrak{g}$, $f(\chi)$ est un entier positif.*

Ce théorème est dû à ARTIN [2] (dans le cas particulier où le corps résiduel k est un corps fini), et ARF [1] (dans le cas général). Nous allons montrer rapidement comment on peut le déduire des résultats des n^{os} 3.5 et 3.6.

D'après le théorème de Brauer, tout caractère χ de $\mathfrak{g}$ est combinaison linéaire (à coefficients dans $\mathbf{Z}$) de caractères χ_i^* induits par des caractères χ_i de degré 1 de sous-groupes de $\mathfrak{g}$. Or, si $\mathfrak{h}$ est un sous-groupe de $\mathfrak{g}$, correspondant à l'extension K'/K, et si χ est un caractère de $\mathfrak{h}$, on a la formule (ARTIN [2])

$$f(\chi^*) = f(\chi) + \chi(1)\, d(K'/K), \tag{31}$$

où $d(K'/K)$ désigne la valuation dans K du discriminant de K'/K. Cette formule montre que $f(\chi)$ est entier si les $f(\chi_i)$ le sont. On est donc ramené au cas d'un *caractère de degré* 1. Dans ce cas on a même un résultat plus précis (qui justifie le terme de « conducteur ») :

PROPOSITION 10. — *Soit χ un caractère de degré 1 de $\mathfrak{g}$, soit $\mathfrak{h}_\chi$ le noyau de $\chi : \mathfrak{g} \to \mathbf{C}^*$, et soit L_χ la sous-extension de L correspondant à $\mathfrak{h}_\chi$. Le conducteur de l'extension L_χ/K est égal à $f(\chi)$.*

Si χ est trivial sur $\mathfrak{g}$, on a $f(\chi) = 0$, $L_\chi = K$, et la proposition est vérifiée. Supposons donc χ non trivial. Il existe un entier $c \geqq 0$ tel que χ soit non trivial sur $\mathfrak{g}_c$, mais soit trivial sur $\mathfrak{g}_{c+1}$. On a alors $\chi(\mathfrak{g}_i) = 0$ si $i \leqq c$, et $\chi(\mathfrak{g}_i) = 1$ si $i \geqq c+1$. La formule (29) s'écrit donc

$$f(\chi) = \frac{1}{g}\sum_{i=0}^{i=c} g_i \tag{32}$$

ou encore, en comparant avec la formule (5) du n° 3.1,

$$f(\chi) = 1 + \varphi_{L/K}(c). \tag{33}$$

Posons $c_\chi = \varphi_{L/L_\chi}(c)$. Le théorème de Herbrand montre que $(\mathfrak{g}/\mathfrak{h}_\chi)_{c_\chi}$ est l'image dans $\mathfrak{g}/\mathfrak{h}_\chi$ de $\mathfrak{g}_c$, donc est différent de $\{1\}$, par définition même de c. De même, on a $(g/h_\chi)_{c_\chi+1} = \{1\}$. La proposition 9 montre alors que le conducteur de l'extension L_χ/K est égal à $1 + \varphi_{L_\chi/K}(c_\chi) = 1 + \varphi_{L/K}(c)$, d'après la transitivité de la fonction φ. Ceci achève la démonstration de la proposition 10, et, en même temps, du théorème 2.

REMARQUES.

1° La formule (31), appliquée au caractère unité du sous-groupe $\mathfrak{h}$, donne une décomposition de $d(K'/K)$. En particulier, pour $\mathfrak{h} = \{1\}$, on obtient la « Führerdiskriminantenproduktformel » (*cf.* ARTIN [2] et HASSE [8])

$$d(L/K) = \sum_\chi \chi(1) f(\chi), \tag{34}$$

où χ parcourt l'ensemble des caractères irréductibles de $\mathfrak{g}$.

2° *A priori*, la démonstration du théorème 2 donnée ci-dessus suppose le corps résiduel k algébriquement clos; en fait, il est facile de ramener le cas général à celui-là :

Si L_0/K_0 est une extension totalement ramifiée, de corps résiduel k_0, galoisienne et de groupe de Galois $\mathfrak{g}$, on construit une extension L/K, de corps résiduel la clôture algébrique k de k_0, qui a même groupe de Galois et mêmes groupes de ramifications que L_0/K_0; l'extension L/K a donc les mêmes conducteurs d'Artin que L_0/K_0, et, puisque le théorème 2 est vrai pour L/K, il l'est aussi pour L_0/K_0.

[La construction de L/K peut se faire de la manière suivante : on choisit une clôture algébrique $\overline{L}_0$ de L_0, ainsi qu'une extension K' de K_0, contenue dans $\overline{L}_0$, de même groupe des ordres que K_0, et maximale pour ces propriétés; on vérifie tout de suite que le corps résiduel de K' est isomorphe à k, et que L_0 et K' sont linéairement disjoints sur K_0; si l'on pose $L' = L_0K'$, l'extension L'/K' est galoisienne, de groupe de Galois $\mathfrak{g}$, et L' (resp. K') a même groupe des ordres que L_0 (resp. K_0); en complétant L' et K' on trouve l'extension L/K cherchée.]

§ 4. Le théorème d'existence.

Les notations et hypothèses de ce paragraphe sont les mêmes que dans les paragraphes 2 et 3.

4.1. Énoncé du théorème. — C'est le suivant :

THÉORÈME 1. — *Si K est un corps local, à corps résiduel k algébriquement clos, l'homomorphisme*

$$\theta : \quad \pi_1(U_k) \to \mathcal{C}\!\ell_K$$

défini au § 2 *est un isomorphisme.*

On sait déjà que θ est surjectif; il suffira donc de montrer qu'il est injectif.

Les groupes $\pi_1(U_K)$ et $\mathcal{C}\!\ell_K$ sont des groupes proalgébriques de dimension zéro. Ils se décomposent donc en produit de *composantes primaires* (*cf.* [21], n° 4.1)

$$\pi_1(U_K) = \prod_l \pi_1(U_K)_l, \qquad \mathcal{C}\!\ell_K = \prod_l (\mathcal{C}\!\ell_K)_l,$$

l parcourant l'ensemble des nombres premiers. Comme θ est produit des homomorphismes $\theta_l : \pi_1(U_K)_l \to (\mathcal{C}\!\ell_K)_l$, il suffira de prouver que les θ_l sont *injectifs*.

Supposons que l soit distinct de la caractéristique de k. Si l'on décompose U_K en $U_K = G_m \times U_K^1$ (*cf.* n° 1.6, prop. 4), on a

$$\pi_1(U_K) = \pi_1(G_m) \times \pi_1(U_K^1).$$

Comme U_K^1 est unipotent, on a $\pi_1(U_K^1)_l = 0$ (cela résulte, par exemple, du fait que la multiplication par l est un isomorphisme de U_K^1 sur lui-même, donc aussi de $\pi_1(U_K^1)_l$ sur lui-même); on sait que $\pi_1(G_m)_l = \mathbf{Z}_l$, groupe des entiers l-adiques (*cf.* [21], n° 6.5). On a donc

$$\pi_1(U_K)_l = \mathbf{Z}_l. \tag{1}$$

D'autre part, puisque l est distinct de la caractéristique de k, le corps local K contient les racines l^n-ièmes de l'unité, quel que soit l'entier $n \geq 0$. Si T est une uniformisante de K, l'adjonction à K d'une racine de l'équation

$$X^{l^n} = T \tag{2}$$

définit une extension L_n/K qui est cyclique d'ordre l^n. La réunion L des L_n est une extension abélienne de K de groupe de Galois isomorphe à $\mathbf{Z}_l$. Le groupe $(\mathfrak{A}_K)_l$ a donc un quotient isomorphe à $\mathbf{Z}_l$, et puisque $\theta_l : \mathbf{Z}_l \to (\mathfrak{A}_K)_l$ est surjectif, c'est nécessairement un isomorphisme.

Il ne nous reste donc plus qu'à traiter le cas où *le corps résiduel k est de caractéristique $p \neq 0$, et où $l = p$*. C'est ce que nous allons faire dans les prochains numéros.

4.2. **Résultats auxiliaires.** — A partir de maintenant, et jusqu'à la fin de ce paragraphe, on suppose que k est un corps de caractéristique $p \neq 0$.

Si U est un k-groupe proalgébrique, nous noterons $H(U)$ le groupe $\mathrm{Hom}(\pi_1(U), \mathbf{Z}/p\mathbf{Z})$. On sait (*cf.* [21], n° 6.3) que ce groupe s'identifie canoniquement à $\mathrm{Ext}(U, \mathbf{Z}/p\mathbf{Z})$ si U est connexe. Si $f : U \to V$ est un morphisme de groupes proalgébriques, on notera $f^* : H(V) \to H(U)$ l'homomorphisme qu'il définit. De même on note $H(K)$ le groupe $\mathrm{Hom}(\mathfrak{A}_K, \mathbf{Z}/p\mathbf{Z})$, et $\theta^* : H(K) \to H(U_K)$ l'homomorphisme défini par θ.

[On peut interpréter $H(K)$ comme le groupe dual du groupe de Galois de l'extension de K engendrée par les extensions cycliques de degré p.]

Lemme 1. — *Soit $0 \to N \to G' \xrightarrow{f} G \to 0$ une suite exacte de groupes proalgébriques. On suppose que G et G' sont connexes, et que $\pi_0(N)$ est un groupe fini d'ordre h. Le noyau de*

$$f^* : \quad H(G) \to H(G')$$

est alors un groupe fini d'ordre divisant h.

On utilise la suite exacte des Ext

$$\mathrm{Hom}(N, \mathbf{Z}/p\mathbf{Z}) \to \mathrm{Ext}(G, \mathbf{Z}/p\mathbf{Z}) \to \mathrm{Ext}(G', \mathbf{Z}/p\mathbf{Z}).$$

On a $\mathrm{Ext}(G, \mathbf{Z}/p\mathbf{Z}) = H(G)$, et de même pour G'; d'autre part, on a $\mathrm{Hom}(N, \mathbf{Z}/p\mathbf{Z}) = \mathrm{Hom}(\pi_0(N), \mathbf{Z}/p\mathbf{Z})$, et ce dernier groupe est évidemment fini et d'ordre divisant h. D'où le lemme.

Posons, pour simplifier l'écriture, $U = U_K$ et $U^n = U_K^n$. L'injection canonique

$$i_n : \quad U^n/U^{n+1} \to U/U^{n+1}$$

définit par transposition un homomorphisme

$$(3) \qquad i_n^\star : \quad H(U/U^{n+1}) \to H(U^n/U^{n+1}).$$

Si v désigne la valuation normée de K, on posera, comme au n° 1.6,

$$(4) \qquad e = v(p), \qquad e_1 = e/(p-1).$$

Lemme 2.

(*a*) *Si $n < pe_1$ et si p divise n, l'image de $i_n^\star$ est nulle.*

(*b*) *Il en est de même si $n > pe_1$.*

(*c*) *Si $n = pe_1$, l'image de $i_n^\star$ a* 1 *ou p éléments.*

Soit m l'entier défini, dans le cas (*a*), par $m = n/p$, dans les cas (*b*) et (*c*) par $m = n - e$. Soit $u : U \to U$ l'homomorphisme $x \to px$ (le groupe U étant ici noté additivement). On sait (n° 1.7, prop. 6) que u applique U^m dans U^n, U^{m+1} dans U^{n+1}, et définit par passage au quotient un homomorphisme surjectif

$$u_m : \quad U^m/U^{m+1} \to U^n/U^{n+1}$$

dont le noyau est nul dans les cas (*a*) et (*b*), et isomorphe à $\mathbf{Z}/p\mathbf{Z}$ dans le cas (*c*).

Considérons le diagramme commutatif

$$(5) \qquad \begin{tikzcd} & U^m/U^{m+1} \arrow[rr, "u_m"] & & U^n/U^{n+1} \arrow[dr, "i_n"] & \\ U^m/U^{n+1} \arrow[ur, "\alpha"] \arrow[rr, "\beta"] & & U/U^{n+1} \arrow[rr, "p"] & & U/U^{n+1} \end{tikzcd}$$

où α et β désignent les applications canoniques évidentes, et où p désigne la multiplication par p dans U/U^{n+1}. Le foncteur H transforme le diagramme (5) en le diagramme commutatif suivant :

$$\begin{tikzcd} & H(U^m/U^{m+1}) \arrow[dl, "\alpha^\star"'] & & H(U^n/U^{n+1}) \arrow[ll, "u_m^\star"'] & \\ H(U^m/U^{n+1}) & & H(U/U^{n+1}) \arrow[ll, "\beta^\star"'] & & H(U/U^{n+1}). \arrow[ll, "p^\star"'] \arrow[ul, "i_n^\star"'] \end{tikzcd}$$

Comme la multiplication par p est nulle dans $\mathbf{Z}/p\mathbf{Z}$, elle l'est aussi dans $H(V)$ pour tout groupe proalgébrique V; on a donc $p^\star = 0$, d'où $\alpha^\star \circ u_m^\star \circ i_n^\star = 0$. Comme α est surjectif et de noyau connexe, le lemme 1 montre que $\alpha^\star$ est injectif, d'où $u_m^\star \circ i_n^\star = 0$. D'après le lemme 1, appliqué cette fois à u_m, le noyau de u_m^* est nul dans les cas (a) et (b), et d'ordre 1 ou p dans le cas (c). Il en est donc de même de l'image de i_n^*, ce qui démontre le lemme.

La suite exacte des Ext associée à la suite exacte

$$(6) \qquad 0 \to U^n \to U \to U/U^n \to 0$$

s'écrit

$$(7) \qquad 0 \to H(U/U^n) \to H(U) \to H(U^n).$$

Nous pouvons donc *identifier* $H(U/U^n)$ *à un sous-groupe de* $H(U)$, à savoir le sous-groupe des homomorphismes de $\pi_1(U)$ dans $\mathbf{Z}/p\mathbf{Z}$ qui sont nuls sur $\pi_1(U^n)$.

Lemme 3.

(i) *Si* $n = pe_1$, *il existe un élément* $\xi \in H(K)$ *tel que* $\xi' = \theta^*(\xi)$ *appartienne à* $H(U/U^{n+1})$, *et que l'image de* ξ' *dans* $H(U^n/U^{n+1})$ *soit non nulle.*

(ii) *Si* $n < pe_1$ *et* $(n, p) = 1$, *pour tout élément* $\eta \in H(U^n/U^{n+1})$ *il existe* $\xi \in H(K)$ *tel que* $\xi' = \theta^*(\xi)$ *appartienne à* $H(U/U^{n+1})$ *et que l'image de* ξ' *dans* $H(U^n/U^{n+1})$ *soit égale à* η.

La démonstration sera donnée au nº 4.3 pour le cas (i), et au nº 4.4 pour le cas (ii).

Proposition 1. — *L'homomorphisme* $\theta^* : H(K) \to H(U)$ *est bijectif.*

Puisque θ est surjectif, θ^* est injectif. Montrons qu'il est injectif. Le groupe $\pi_1(U)$ est limite projective des $\pi_1(U/U^n)$; donc $H(U)$ est limite inductive (c'est-à-dire réunion) des $H(U/U^n)$. Il nous suffit donc de montrer que $\mathrm{Im}(\theta^*)$ contient $H(U/U^n)$, ce que nous ferons par récurrence sur n, le cas $n = 0$ étant trivial.

Pour passer de n à $n+1$ on utilise la suite exacte

$$(8) \qquad 0 \to H(U/U^n) \to H(U/U^{n+1}) \to H(U^n/U^{n+1}).$$

Il suffit évidemment de montrer que $H(U/U^{n+1})$ et $\mathrm{Im}(\theta^*) \cap H(U/U^{n+1})$ ont même image dans $H(U^n/U^{n+1})$. C'est trivial dans chacun des cas (a) et (b) du lemme 2, puisque cette image est nulle. Dans le cas (c), l'image de $H(U/U^{n+1})$ a au plus p éléments (lemme 2), et celle de $\mathrm{Im}(\theta^*) \cap H(U/U^{n+1})$ a au moins p éléments (lemme 3); ces deux images coïncident donc bien. Enfin, dans le cas restant où $n < pe_1$ et $(n, p) = 1$, l'image de $\mathrm{Im}(\theta^*) \cap H(U/U^{n+1})$ dans $H(U^n/U^{n+1})$ est égale à tout $H(U^n/U^{n+1})$ (lemme 3), d'où encore le résultat dans ce cas.

4.3. **Extensions données par une équation $x^p = \pi$.** — Soit d'abord L/K une extension dont le groupe de Galois $\mathfrak{g}$ est cyclique d'ordre p, et fixons un isomorphisme $\mathfrak{g} = \mathbf{Z}/p\mathbf{Z}$ (autrement dit choisissons un générateur σ de $\mathfrak{g}$).

Comme $\mathfrak{g}$ est quotient de $\mathfrak{A}_K$, la donnée de L/K revient à la donnée d'un homomorphisme non nul

$$\xi : \quad \mathfrak{A}_K \rightarrow \mathbf{Z}/p\mathbf{Z}.$$

On peut donc considérer ξ comme un élément de $H(K)$. La suite exacte (3) du n° 2.3 s'écrit ici

$$(9) \qquad 0 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow U_L/I.U_L \rightarrow U \rightarrow 0$$

et *l'homomorphisme bord* $\partial : \pi_1(U) \rightarrow \mathbf{Z}/p\mathbf{Z}$ *associé à cette suite exacte n'est autre que* $\xi' = \theta^*(\xi)$, par définition même de θ.

Soit de plus t le plus grand entier tel que $\mathfrak{g}_t = \mathfrak{g}$ (*cf.* n° 3.3). L'entier $t+1$ est le *conducteur* de L/K (*cf.* n° 3.6). L'homomorphisme

$$\xi' : \quad \pi_1(U) \rightarrow \mathbf{Z}/p\mathbf{Z}$$

est nul sur $\pi_1(U^{t+1})$ et non nul sur $\pi_1(U^t)$, par définition du conducteur; on peut donc le considérer comme un élément de $H(U/U^{t+1})$. La remarque 2 du n° 3.5 montre, en outre, que *l'image* η' *de* ξ' *dans* $H(U^t/U^{t+1})$ *n'est autre que l'homomorphisme bord*

$$\partial : \quad \pi_1(U^t/U^{t+1}) \rightarrow \mathbf{Z}/p\mathbf{Z}$$

associé à la suite exacte (14) *du* n° 3.3

$$(10) \qquad 0 \rightarrow \mathbf{Z}/p\mathbf{Z} \xrightarrow{\gamma} U_L^t/U_L^{t+1} \xrightarrow{N_t} U^t/U^{t+1} \rightarrow 0.$$

[Rappelons que N_t est défini par passage au quotient à partir de la norme, et que γ applique σ sur la classe de $\sigma(T)/T$, T étant une uniformisante de L.]

Comme U_L^t/U_L^{t+1} est connexe, on a $\eta' \neq 0$ (cela résulte aussi du fait que ξ' n'appartient pas à $H(U/U^t)$). En particulier, pour démontrer la partie (i) du lemme 3, *il suffit de construire une extension* L/K, *cyclique de degré* p, *et telle que* $t = pe_1$.

Or, puisqu'on suppose que pe_1 est entier, $p-1$ divise e, et le corps K contient une racine primitive $p^{\text{ième}}$ de l'unité, soit z (n° 1.7, cor. 2 à la prop. 6). Si π est une uniformisante de K, l'équation $x^p = \pi$ définit une extension galoisienne L de K, cyclique de degré p; on peut supposer que le générateur σ de son groupe de Galois applique x sur zx. On a donc

$$\sigma(x)/x = z.$$

L'élément x est une uniformisante de L. D'autre part, il est bien connu (et on l'a vu au cours de la démonstration du corollaire cité plus haut) que $z \in U^{e_1}$, $z \notin U^{e_1+1}$. On a donc

$$t = v_L(1-z) = pv_K(1-z) = pe_1.$$

C. Q. F. D.

4.4. Extensions d'Artin-Schreier.

Lemme 4. — *Soit n un entier ≥ 1, avec $n < pe_1$ et $(n, p) = 1$. Soit λ un élément de K de valuation $-n$.*

(a) L'équation « d'Artin-Schreier »

$$x^p - x = \lambda \tag{11}$$

est irréductible sur K, et engendre une extension L/K cyclique de degré p.

(b) L'entier t correspondant à cette extension (nº 3.3) *est égal à n.*

(c) Soit η'_λ l'élément de $H(U^n/U^{n+1})$ associé à L/K comme il a été dit au numéro précédent. On a $\eta'_\lambda \neq 0$; pour tout élément non nul η de $H(U^n/U^{n+1})$ il existe un λ tel que $\eta'_\lambda = \eta$.

Il est clair que ce lemme entraîne la partie (ii) du lemme 3.

Démonstration. — Les assertions (a) et (b) sont bien connues (*cf.* Whaples [25], nº 6, ou MacKenzie-Whaples [14]). Rappelons-en les démonstrations :

Soit $L = K(x)$ le corps obtenu en adjoignant à K une racine x de l'équation (11). Comme $v_L(\lambda) < 0$, il en est de même de $v_L(x)$, et l'on a

$$v_L(x) = p^{-1} v_L(\lambda) = -p^{-1}[L:K]n. \tag{12}$$

Comme p ne divise pas n, on a nécessairement $[L:K] = p$, ce qui montre que (11) est irréductible.

De plus, si l'on cherche à quelle condition $x + y$ est racine de (11), on trouve

$$y^p - y + p\,F(x, y) = 0 \tag{13}$$

où $F(x, y) = ((x+y)^p - x^p - y^p)/p$ est un polynôme à coefficients entiers. Comme $v_L(x) = -n$, $v_L(p) = pe$, on a $v_L(p) + (p-1)\,v_L(x) > 0$, ce qui montre que les coefficients de $p\,F(x, y)$, considéré comme polynôme en y, appartiennent à l'idéal maximal $\mathfrak{P}$ de A_L. La réduction modulo $\mathfrak{P}$ de (13) s'écrit donc

$$\bar{y}^p - \bar{y} = 0, \tag{14}$$

équation qui admet les p racines simples $\bar{y}_i = i$, $i \in \mathbf{Z}/p\mathbf{Z}$. D'après le lemme de Hensel, l'équation (13) a p solutions $y_i \in A_L$, avec

$$y_i \equiv i \mod \mathfrak{P}, \qquad i \in \mathbf{Z}/p\mathbf{Z}. \tag{15}$$

Les $x + y_i = x_i$ sont p solutions distinctes de (11), ce qui montre que L/K est galoisienne. Son groupe de Galois $\mathfrak{g}$ est nécessairement cyclique d'ordre p. Nous choisirons comme générateur de ce groupe l'élément σ qui vérifie

$$\sigma(x) = x + y_1, \qquad \text{c'est-à-dire} \quad \sigma(x) - x \equiv 1 \mod \mathfrak{P}. \tag{16}$$

Pour prouver (b), choisissons une uniformisante T de L. On peut écrire $x = u . T^{-n}$, où u est une unité de L. Par définition de t, on a

$$\sigma(T)/T = 1 + z, \qquad \text{avec} \quad v_L(z) = t. \tag{17}$$

On en déduit

$$\sigma(u)/u \equiv 1 \mod \mathfrak{P}^{t+1}$$
$$\sigma(T^{-n})/T^{-n} \equiv 1 - nz \mod \mathfrak{P}^{t+1},$$

d'où

$$\sigma(x)/x \equiv 1 - nz \mod \mathfrak{P}^{t+1}.$$

D'autre part, d'après (16), on a

$$\sigma(x)/x \equiv 1 + x^{-1} \mod \mathfrak{P}^{n+1} \qquad \text{et} \qquad v_L(x^{-1}) = n. \tag{18}$$

Comparant les deux expressions obtenues pour $\sigma(x)/x$, on voit que $t = n$, ce qui démontre (b). On voit également qu'on a

$$-nz \equiv x^{-1} \mod \mathfrak{P}^{n+1}. \tag{19}$$

Reste à démontrer (c), et pour cela il nous faut expliciter l'élément $\eta'_\lambda \in H(U^n/U^{n+1})$. D'après ce que nous avons vu au numéro précédent, η'_λ coïncide avec l'opérateur bord de la suite exacte

$$0 \to \mathbf{Z}/p\mathbf{Z} \xrightarrow{\gamma} U_L^n/U_L^{n+1} \xrightarrow{N_n} U^n/U^{n+1} \to 0, \tag{20}$$

γ et N_n étant des homomorphismes qu'on a déjà explicités plusieurs fois.

Comme $v_L(x^{-1}) = n$, tout élément de U_L^n/U_L^{n+1} peut se représenter par un élément de la forme $1 - sx^{-1}$, avec $s \in A_K$. Si l'on fait correspondre à $1 - sx^{-1}$ l'image $\bar{s}$ de s dans k, on obtient un *isomorphisme de* U_L^n/U_L^{n+1} *sur* G_a, qui nous permet d'identifier ces deux groupes. L'homomorphisme $\gamma : \mathbf{Z}/p\mathbf{Z} \to U_L^n/U_L^{n+1}$ se transforme alors en un homomorphisme

$$f : \quad \mathbf{Z}/p\mathbf{Z} \to G_a.$$

Par définition, γ applique σ sur la classe de $\sigma(T)/T = 1 + z$; en utilisant (19), on voit donc que $\gamma(\sigma)$ est la classe de $1 - n^{-1}x^{-1}$, ce qui montre que *f est la multiplication par n^{-1}*.

Après avoir explicité γ, explicitons N_n. On a

$$N(1 - sx^{-1}) = N(s - x)/N(-x) = (s^p - s - \lambda)/(-\lambda).$$

D'où

$$N(1 - sx^{-1}) = 1 - \lambda^{-1}(s^p - s). \tag{21}$$

Soit π_n un élément de K de valuation n. On peut écrire

$$\lambda^{-1} = \pi_n \mu, \qquad \text{avec} \quad \mu \in U. \tag{22}$$

Identifions U^n/U^{n+1} à G_a en faisant correspondre à $1+s'\pi_n$, $s' \in A_K$, la classe $\bar{s}'$ de s' dans k.

L'homomorphisme $N_n : U_L^n/U_L^{n+1} \to U^n/U^{n+1}$ se transforme par les identifications précédentes en un homomorphisme

$$g : \quad G_a \to G_a.$$

La formule (21) *montre que*

$$(23) \qquad g(\bar{s}) = -\bar{\mu}(\bar{s}^p - \bar{s}),$$

$\bar{\mu}$ désignant l'image de μ dans k^*.

Nous avons donc remplacé la suite exacte (20) par la suite exacte

$$(24) \qquad 0 \to \mathbf{Z}/p\mathbf{Z} \xrightarrow{f} G_a \xrightarrow{g} G_a \to 0,$$

où f et g ont été déterminés explicitement. Il ne nous reste plus qu'à calculer l'élément $\eta'_\lambda \in \mathrm{H}(G_a)$ associé à (24). Or, on sait que $H(G_a)$ *s'identifie à* k ([21], n° 8.3, prop. 3); de plus, on sait calculer l'élément de k correspondant à une suite exacte du type (24) ([21], *loc. cit.*, lemme 1); c'est

$$(25) \qquad -1/\bar{\mu}n^{-1} = -n/\bar{\mu}.$$

Il est clair que $-n/\bar{\mu}$ n'est pas nul, et que tout élément non nul de k est de la forme $-n/\bar{\mu}$, pour une unité μ convenable. Ceci achève la démonstration du lemme 4, donc aussi celle du lemme 3.

4.5. **Fin de la démonstration du théorème 1.** — Pour simplifier les notations, nous poserons $B_K = \pi_1(U_K)$, et nous noterons D_K le noyau de $\theta : B_K \to \mathfrak{A}_K$. Les résultats du n° 4.1 montrent que D_K est un *groupe p-primaire*. On a, de plus,

$$(26) \qquad D_K \subset pB_K.$$

En effet, soit $D'_K = D_K \cap pB_K$. On a la suite exacte

$$(27) \qquad 0 \to D_K/D'_K \to B_K/pB_K \to \mathfrak{A}_K/p\mathfrak{A}_K \to 0.$$

Les groupes qui figurent dans cette suite exacte sont tous annulés par p. Le dual de B_K/pB_K est donc $\mathrm{Hom}(B_K, \mathbf{Z}/p\mathbf{Z}) = H(U)$, et celui de $\mathfrak{A}_K/p\mathfrak{A}_K$ est $H(K)$. D'après la proposition 1, l'homomorphisme $H(K) \to H(U)$ est un isomorphisme. Il en est donc de même de $B_K/pB_K \to \mathfrak{A}_K/p\mathfrak{A}_K$, ce qui montre que $D'_K = D_K$ et établit (26).

On a, d'autre part, $D_K = \bigcap N_{L/K}(B_L)$, pour L parcourant l'ensemble des extensions finies et séparables de K (*cf.* n° 2.4, prop. 6). Si L/K est une telle extension, le fait que le morphisme $N_{L/K} : B_L \to B_K$ commute aux intersections ([21], n° 2.5) permet d'écrire

$$N_{L/K}(D_L) = N_{L/K}\Big(\bigcap N_{M/L}(B_M)\Big) = \bigcap N_{M/K}(B_M) = D_K.$$

En appliquant à L la relation (26), on voit alors qu'on a

$$D_K \subset \bigcap p N_{L/K}(B_L),$$

d'où, pour la raison déjà invoquée ci-dessus,

$$D_K \subset p \bigcap N_{L/K}(B_K) = p D_K.$$

Mais tout groupe p-primaire D qui vérifie $D = pD$ est réduit à zéro (sinon, il admettrait un quotient fini non trivial vérifiant la même identité, ce qui est absurde). Donc $D_K = 0$. C. Q. F. D.

Variante. — Une fois démontré (26) on peut aussi raisonner de la façon suivante : puisque le groupe de Brauer de K et de toutes ses extensions finies est réduit à 0, le groupe de Galois $G(p)$ de la p-extension maximale de K est un *p-groupe libre* au sens de KAWADA et TATE (*cf.* [6], th. 4.2 et prop. 3.4). Comme le plus grand quotient abélien de $G(p)$ n'est autre que $(\mathfrak{A}_K)_p$, ce dernier groupe est produit de groupes isomorphes à $\mathbf{Z}_p$, autrement dit est *projectif* dans la catégorie des groupes proalgébriques (*cf.* [21], n° 4.4). Le groupe D_K est alors facteur direct dans B_K, et la formule (26) signifie que $D_K = pD_K$, d'où $D_K = 0$ comme ci-dessus.

4.6. **Extensions infinies.** — Soit L une extension algébrique infinie de K. Lorsque K' parcourt l'ensemble filtrant des extensions finies de K contenues dans L, les groupes $U_{K'}$ forment de façon naturelle un système projectif (pour les applications de norme). On *définit* alors un groupe proalgébrique U_L en posant

$$U_L = \varprojlim U_{K'}.$$

(On notera que le groupe abélien sous-jacent à U_L *n'est pas* le groupe des unités de L.)

Il résulte immédiatement du théorème d'existence et de la proposition 7 du n° 2.4 que *le groupe $\pi_1(U_L)$ est isomorphe au groupe de Galois de l'extension abélienne maximale de L.* En particulier, si L est la clôture algébrique de K, le groupe U_L est simplement connexe.

§ 5. Application aux courbes algébriques.

5.1. **Structure de groupe proalgébrique sur le groupe des classes d'idèles de degré zéro.** — Nous allons rappeler un certain nombre de définitions et de résultats bien connus (*cf.* par exemple [18]).

Soit k un corps algébriquement clos, et soit X une courbe algébrique irréductible, projective, non singulière, définie sur k. Soit $K = k(X)$ le corps des fonctions rationnelles sur X; la connaissance de l'extension K/k

détermine la courbe X de façon unique. Si $P \in X$, on note K_P le complété de K pour la valuation discrète normée v_P définie par P; c'est un corps local, muni d'une structure de k-algèbre, et isomorphe au corps des séries formelles $k((T))$; on note U_P son groupe des unités.

Un *idèle* x de K (ou de X, c'est la même chose) est, par définition, une famille $(x_P)_{P \in X}$, avec $x_P \in K_P^*$ et même $x_P \in U_P$ pour presque tout P (c'est-à-dire sauf pour un nombre fini de points P). Les idèles forment un groupe multiplicatif $I(K)$, dans lequel se plonge de façon évidente le groupe K^*; les éléments de K^* sont appelés *idèles principaux;* le quotient $C(K) = I(K)/K^*$ est le *groupe des classes d'idèles* de K.

Le *degré* d'un idèle $x = (x_P)_{P \in X}$ est défini par la formule

$$\deg(x) = \sum_{P \in X} v_P(x_P). \tag{1}$$

Si $x \in K^*$, on a $\deg(x) = 0$, ce qui permet de définir le degré d'une classe d'idèles. Les classes d'idèles de degré zéro forment un sous-groupe $C_0(K)$ de $C(K)$; on a la suite exacte

$$0 \to C_0(K) \to C(K) \to \mathbf{Z} \to 0. \tag{2}$$

Soit maintenant $\mathfrak{m} = \sum_{P \in X} n_P P$ un *diviseur positif* sur X, et posons

$$I_{\mathfrak{m}}(K) = \prod_{P \in X} U_P^{n_P}. \tag{3}$$

Le groupe $I_{\mathfrak{m}}(K)$ est un sous-groupe de $I(K)$. On vérifie facilement que $I(K)$ s'identifie à la limite projective des quotients $I(K)/I_{\mathfrak{m}}(K)$, et que $C(K)$ s'identifie à la limite projective des groupes

$$C_{\mathfrak{m}}(K) = I(K)/K^* I_{\mathfrak{m}}(K),$$

pour $\mathfrak{m}$ parcourant l'ensemble ordonné filtrant des diviseurs positifs de X. Le groupe $C_{\mathfrak{m}}(K)$ est canoniquement isomorphe au *groupe des classes de diviseurs de* $X - \mathrm{Supp}(\mathfrak{m})$ *pour la relation d'équivalence définie par* $\mathfrak{m}$ (*cf.* [18], chap. V, n° 2). Comme $\deg(x) = 0$ si $x \in I_{\mathfrak{m}}(K)$, le degré d'un élément de $C_{\mathfrak{m}}(K)$ est défini; les éléments de $C_{\mathfrak{m}}(K)$ de degré zéro forment un sous-groupe $J_{\mathfrak{m}}(K)$. On a la suite exacte

$$0 \to J_{\mathfrak{m}}(K) \to C_{\mathfrak{m}}(K) \to \mathbf{Z} \to 0 \tag{4}$$

et la formule

$$C_0(K) = \varprojlim J_{\mathfrak{m}}(K). \tag{5}$$

D'après Rosenlicht, il existe sur $J_{\mathfrak{m}}(K)$ une structure canonique de variété algébrique, qui en fait un groupe algébrique, appelée *jacobienne géné-*

ralisée de X relativement à $\mathfrak{m}$ (*cf.* [18], chap. V). Si $\mathfrak{m}' \geq \mathfrak{m}$, l'application $J_{\mathfrak{m}'}(K) \to J_{\mathfrak{m}}(K)$ est un morphisme, ce qui permet, grâce à la formule (5), de définir sur $C_0(K)$ une structure de *groupe proalgébrique*. On observera que, pour tout $P \in X$, l'application canonique de U_P dans $C_0(K)$ est un *morphisme de groupes proalgébriques* (cela résulte de la structure des jacobiennes généralisées, *cf.* [18], chap. V, § 3); comme cette application est évidemment injective, elle identifie U_P à un sous-groupe fermé de $C_0(K)$; nous reviendrons là-dessus au n° 5.3.

Si n est un entier, nous noterons $J_{\mathfrak{m}}^{(n)}(K)$ l'ensemble des éléments de degré n de $C_{\mathfrak{m}}(K)$; c'est un espace principal homogène sur $J_{\mathfrak{m}}(K)$. On désignera par

$$\varphi_{\mathfrak{m}}: \quad X - \mathrm{Supp}(\mathfrak{m}) \to J_{\mathfrak{m}}^{(1)}(K)$$

l'application qui fait correspondre à un point P la classe du diviseur réduit à P; on sait ([18], *loc. cit.*) que $\varphi_{\mathfrak{m}}$ est un morphisme de variétés algébriques.

5.2. **Le groupe de Galois de l'extension abélienne maximale de K.** — Soit $\mathfrak{m}$ un diviseur positif sur X, et considérons une *isogénie séparable au-dessus de* $J_{\mathfrak{m}}(K)$, autrement dit une suite strictement exacte

$$0 \to \mathfrak{g} \to H \to J_{\mathfrak{m}}(K) \to 0, \tag{6}$$

où $\mathfrak{g}$ est un groupe abélien fini, et H un groupe algébrique commutatif connexe (*cf.* [21], n° 6.4). En choisissant un point dans $J_{\mathfrak{m}}^{(1)}(K)$, on peut identifier $J_{\mathfrak{m}}^{(1)}(K)$ et $J_{\mathfrak{m}}(K)$, donc définir à partir de (6) un revêtement abélien $H^{(1)}$ de $J_{\mathfrak{m}}^{(1)}(K)$, de groupe de Galois $\mathfrak{g}$; du fait que k est algébriquement clos, ce revêtement ne dépend pas du point choisi dans $J_{\mathfrak{m}}^{(1)}(K)$. L'image réciproque de $H^{(1)}$ par le morphisme

$$\varphi_{\mathfrak{m}}: \quad X - \mathrm{Supp}(\mathfrak{m}) \to J_{\mathfrak{m}}^{(1)}(K)$$

est un revêtement abélien de $X - \mathrm{Supp}(\mathfrak{m})$. On sait ([18], chap. VI, n° 11) que ce revêtement est irréductible. Son corps des fonctions L est donc une extension abélienne de K, de groupe de Galois $\mathfrak{g}$. Si $\mathfrak{A}_K$ désigne le groupe de Galois de l'extension abélienne maximale de K, on obtient donc un homomorphisme surjectif $\mathfrak{A}_K \to \mathfrak{g}$. Les isogénies (6) forment un système filtrant croissant, et la limite projective des groupes $\mathfrak{g}$ correspondants n'est autre que $\pi_1(J_{\mathfrak{m}}(K))$ (*cf.* [21], n° 6.4, prop. 7). On a donc construit un homomorphisme surjectif

$$\psi_{\mathfrak{m}}: \quad \mathfrak{A}_K \to \pi_1(J_{\mathfrak{m}}(K)). \tag{7}$$

En passant à la limite sur $\mathfrak{m}$, on en déduit un homomorphisme surjectif

$$\psi: \quad \mathfrak{A}_K \to \pi_1(C_0(K)). \tag{8}$$

PROPOSITION 1. — *L'homomorphisme ψ défini ci-dessus est un isomorphisme.*

Cela revient à dire que toute extension abélienne L/K peut être obtenue par le procédé ci-dessus, ce qui est un résultat connu ([18], chap. VI, prop. 9).

On peut aussi, comme au § 2, définir directement un homomorphisme en sens inverse

$$\theta : \quad \pi_1(C_0(K)) \to \mathfrak{A}_K.$$

Pour cela, soit L/K une extension galoisienne finie de groupe de Galois $\mathfrak{g}$; le groupe $\mathfrak{g}$ opère sur L^*, $I(L)$, $C(L)$, $C_0(L)$, et l'on a le résultat suivant (*cf.* HOCHSCHILD-NAKAYAMA [11], th. 4.3) :

LEMME 1. — *Les $\mathfrak{g}$-modules L^*, $I(L)$ et $C(L)$ sont cohomologiquement triviaux.*

On en déduit, en particulier, que $C(L)^{\mathfrak{g}} = C(K)$, et que la norme $N : C(L) \to C(K)$ est surjective; les mêmes résultats valent pour $C_0(L)$ et $C_0(K)$. De plus, la suite exacte

$$(9) \qquad 0 \to C_0(L) \to C(L) \to \mathbf{Z} \to 0$$

montre que $\mathfrak{g}/\mathfrak{g}'$ s'identifie à $H^{-1}(\mathfrak{g}, C_0(L))$. Si l'on note W_L le noyau de $N : C_0(L) \to C_0(K)$, on en déduit, comme au n° 2.3, que la composante connexe de W_L est égale à $I.C_0(L)$, et qu'on a

$$(10) \qquad \mathfrak{g}/\mathfrak{g}' = \pi_0(W_L).$$

L'isomorphisme en question fait correspondre à $\sigma \in \mathfrak{g}$ la classe dans $\pi_0(W_L)$ de $\sigma(D)/D$, où D est un élément de degré 1 de $C(L)$. La suite exacte

$$(11) \qquad 0 \to W_L \to C_0(L) \xrightarrow{N} C_0(K) \to 0$$

donne naissance à un homomorphisme bord

$$(12) \qquad \pi_1(C_0(K)) \to \pi_0(W_L) = \mathfrak{g}/\mathfrak{g}'.$$

Passant à la limite sur L, on obtient l'homomorphisme cherché

$$\theta : \quad \pi_1(C_0(K)) \to \mathfrak{A}_K.$$

PROPOSITION 2. — *Les homomorphismes ψ et θ sont inverses l'un de l'autre.*

Soit L/K une extension abélienne finie, de groupe de Galois $\mathfrak{g}$, provenant de l'isogénie (6). Considérons le diagramme

$$(13) \qquad \begin{array}{ccc} \pi_1(C_0(K)) & \to & \mathfrak{g} \\ \downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ \pi_1(J_{\mathfrak{m}}(K)) & \to & \mathfrak{g} \end{array}$$

Si l'on démontre que (13) est commutatif, par passage à la limite on en déduira que $\psi \circ \theta = 1$, d'ou la proposition.

Soit Y la courbe normalisée de X dans L/K; l'application rationnelle de Y dans $H^{(1)}$ se prolonge en un homomorphisme $C_0(L) \to H$ de groupes proalgébriques (c'est une conséquence d'un théorème de ROSENLICHT, *cf.* [18], chap. III). D'après un résultat connu ([18], chap. III, prop. 4), le diagramme

$$\begin{array}{ccc} C_0(L) & \xrightarrow{N} & C_0(K) \\ \downarrow & & \downarrow \\ H & \rightarrow & J_{\mathfrak{m}}(K) \end{array}$$

est commutatif. Il peut donc se plonger dans le diagramme commutatif suivant :

$$(14) \qquad \begin{array}{ccccccccc} 0 & \rightarrow & W_L & \rightarrow & C_0(L) & \xrightarrow{N} & C_0(K) & \rightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \rightarrow & \mathfrak{g} & \rightarrow & H & \rightarrow & J_{\mathfrak{m}}(K) & \rightarrow & 0 \end{array}$$

L'homomorphisme $W_L \to \mathfrak{g}$ ainsi obtenu définit par passage au quotient un homomorphisme de $\pi_0(W_L)$ dans $\mathfrak{g}$ *qui n'est autre que l'isomorphisme* (10) : cela se vérifie sans difficultés. La commutativité de (13) résulte alors de celle de (14). C. Q. F. D.

REMARQUE. — Ici encore, on peut définir une *formation de classes* en utilisant la suite exacte

$$(15) \qquad 0 \to \pi_1(C_0(L)) \to \overline{C_0(L)} \to C(L) \to \mathbf{Z} \to 0.$$

On sait, en effet, que $C(L)$ est cohomologiquement trivial, et le raisonnement de la proposition 8 du n° 2.5 montre qu'il en est de même de $\overline{C_0(L)}$. On en déduit un isomorphisme

$$(16) \qquad \delta^2 : \quad H^q(\mathfrak{g}, \mathbf{Z}) \to H^{q+2}(\mathfrak{g}, \pi_1(C_0(L))).$$

Pour $q = -2$, l'isomorphisme $\delta^2 : \mathfrak{g}/\mathfrak{g}' \to \pi_1(C_0(L))/N\pi_1(C_0(K))$ est inverse de l'isomorphisme défini au moyen de (12) : la démonstration est identique à celle de la proposition 10 du n° 2.5.

3.3. **Groupes de décomposition.** — Soit L/K une extension abélienne finie, de groupe de Galois $\mathfrak{g}$, et soit Y la courbe normalisée de X dans L/K. Soit $P \in X$, et choisissons un point $Q \in Y$ se projetant en P. Le sous-groupe de $\mathfrak{g}$ formé des éléments σ tels que $\sigma(Q) = Q$ ne dépend pas du choix de Q (du fait que $\mathfrak{g}$ est abélien); nous l'appellerons le *groupe de décomposition de* P, et nous le noterons $\mathfrak{g}_P$. C'est le groupe de Galois de l'extension de corps locaux L_Q/K_P. D'après la théorie locale du § 2, on a un homomorphisme surjectif : $\pi_1(U_P) \to \mathfrak{g}_P$ et, d'après ce qu'on vient de voir au numéro précédent, on a un homomorphisme surjectif : $\pi_1(C_0(K)) \to \mathfrak{g}$.

LEMME 2. — *Le diagramme*

$$(17) \qquad \begin{array}{ccc} \pi_1(U_P) & \rightarrow & \mathfrak{g}_P \\ \downarrow & & \downarrow \\ \pi_1(C_0(K)) & \rightarrow & \mathfrak{g} \end{array}$$

est commutatif.

Cela résulte immédiatement de la commutativité du diagramme

$$(18) \qquad \begin{array}{ccccccccc} 0 \rightarrow & \pi_1(U_Q) & \rightarrow & \overline{U_Q} & \rightarrow & L_Q^\star & \rightarrow & \mathbf{Z} & \rightarrow 0 \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow \scriptstyle{\mathrm{id}} & \\ 0 \rightarrow & \pi_1(C_0(L)) & \rightarrow & \overline{C_0(L)} & \rightarrow & C(L) & \rightarrow & \mathbf{Z} & \rightarrow 0. \end{array}$$

Passons à la limite sur L. On a $\mathfrak{A}_K = \varprojlim \mathfrak{g}$, et la limite des groupes $\mathfrak{g}_P$ est un sous-groupe fermé $(\mathfrak{A}_K)_P$ de $\mathfrak{A}_K$, que nous appellerons encore le *groupe de décomposition* de P. Si K_a désigne l'extension abélienne maximale de K, $\mathfrak{A}_K$ est le groupe de Galois de K_a/K, et $(\mathfrak{A}_K)_P$ est le groupe de Galois d'une extension composée K_aK_P/K_P; en particulier, $(\mathfrak{A}_K)_P$ s'identifie à un groupe quotient de $\mathfrak{A}_{K_P}$ (le groupe de Galois de l'extension abélienne maximale de K_P).

PROPOSITION 3.

(*a*) *Le groupe* $(\mathfrak{A}_K)_P$ *s'identifie à* $\mathfrak{A}_{K_P}$.

(*b*) *L'image de* $\pi_1(U_P)$ *par l'isomorphisme* $\theta : \pi_1(C_0(L)) \rightarrow \mathfrak{A}_K$ *est égale au groupe de décomposition* $(\mathfrak{A}_K)_P$, *et la restriction de* θ *à* $\pi_1(U_P)$ *coïncide avec l'isomorphisme* θ *du* § 2.

Par passage à la limite, le diagramme (17) donne

$$(19) \qquad \begin{array}{ccc} \pi_1(U_P) & \rightarrow & (\mathfrak{A}_K)_P \\ \downarrow & & \downarrow \\ \pi_1(C_0(K)) & \xrightarrow{\theta} & \mathfrak{A}_K \end{array}$$

et l'homomorphisme $\pi_1(U_P) \rightarrow (\mathfrak{A}_K)_P$ se factorise en

$$(20) \qquad \pi_1(U_P) \xrightarrow{\theta} \mathfrak{A}_{K_P} \rightarrow (\mathfrak{A}_K)_P.$$

Comme $U_P \rightarrow C_0(K)$ est injectif, il en est de même de $\pi_1(U_P) \rightarrow \pi_1(C_0(K))$. On en conclut que l'homomorphisme (20) est injectif, d'où à la fois le fait que θ est injectif (ce qu'on avait déjà démontré au § 4), et l'assertion (*a*). L'assertion (*b*) ne fait que traduire la commutativité de (19).

REMARQUES.

1° La nouvelle démonstration du *théorème d'existence* que nous venons d'obtenir est nettement plus satisfaisante que celle du § 4 (qui reposait sur un « dévissage » plutôt pénible); malheureusement, elle ne s'applique qu'*au cas d'égale caractéristique.*

2° L'assertion (a) signifie que l'extension composée $K_a K_P/K_P$ est *l'extension abélienne maximale* de K_P; on sait qu'un résultat analogue est valable dans la théorie du corps de classes usuelle.

3° Revenons à une extension abélienne finie L/K, de groupe de Galois $\mathfrak{g}$. Le *conducteur* de L/K a été défini dans [18], chap. VI, § 2, comme le plus petit diviseur positif $\mathfrak{m}$ tel que l'homomorphisme

$$\pi_1(C_0(K)) \to \mathfrak{g}$$

puisse se factoriser en $\pi_1(C_0(K)) \to \pi_1(J_{\mathfrak{m}}(K)) \to \mathfrak{g}$. La proposition précédente montre que *le coefficient d'un point P dans* $\mathfrak{m}$ *est égal au conducteur* (au sens du n° 3.6) *de l'extension locale* L_Q/K_P *correspondante.*

BIBLIOGRAPHIE.

[1] ARF (Cahit). — Untersuchungen über reinverzweigte Erweiterungen diskret bewerteter perfekter Körper, *J. reine ang. Math.*, t. 181, 1940, p. 1-44.

[2] ARTIN (Emil). — Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper, *J. reine ang. Math.*, t. 164, 1931, p. 1-11.

[3] ARTIN (Emil). — *Algebraic numbers and algebraic functions.* — Princeton University, 1950-1951 (polycopié).

[4] CARTAN (Henri) and EILENBERG (Samuel). — *Homological algebra.* — Princeton, University Press, 1956. (Princeton math. Series, 19).

[5] COHEN (Irvin). — On the structure and ideal theory of complete local rings, *Trans. Amer. math. Soc.*, t. 59, 1946, p. 54-106.

[6] DOUADY (Adrien). — Cohomologie des groupes compacts totalement discontinus, *Séminaire Bourbaki*, t. 12, 1959-1960, exposé 189.

[7] GREENBERG (Marvin). — Schemata over local rings, *Annals of Math.*, t. 73, 1961, p. 624-648.

[8] HASSE (Helmut). — Normenresttheorie galoisscher Zahlkörper mit Anwendungen auf Führer und Diskriminante abelscher Zahlkörper, *J. Fac. Sc. Tokyo*, t. 2, 1934, p. 477-498.

[9] HASSE (Helmut). — *Zahlentheorie.* — Berlin, Akademie-Verlag, 1949.

[10] HERBRAND (Jacques). — Sur la théorie des groupes de décomposition, d'inertie et de ramification, *J. Math. pures et appl.*, Série 9, t. 10, 1931, p. 481-498.

[11] HOCHSCHILD (Gerhard) and NAKAYAMA (Tadasi). — Cohomology in class field theory, *Annals of Math.*, t. 55, 1952, p. 348-366.

[12] KAWADA (Yukiyosi). — Class formations, *Duke math. J.*, t. 22, 1955, p. 165-178.

[13] LANG (Serge). — On quasi algebraic closure, *Annals of Math.*, t. 55, 1952, p. 373-390.

[14] MACKENZIE (Robert) and WHAPLES (George). — Artin-Schreier equations in characteristic zero, *Amer. J. of Math.*, t. 78, 1956, p. 473-485.

[15] RIM (Dock Sang). — Modules over finite groups, *Annals of Math.*, t. 69, 1959, p. 700-712.

[16] ŠAFAREVIČ. (Igor). — A general reciprocity law, *Mat. Sbornik*, t. 26, 1950, p. 113-146 (*Amer. math. Soc. Transl.*, Series 2, vol. 4, p. 73-106).

[17] SAMUEL (Pierre) and ZARISKI (Oscar). — *Commutative algebra*, I. — Princeton, Van Nostrand, 1958.

[18] SERRE (Jean-Pierre). — *Groupes algébriques et corps de classes.* — Paris, Hermann, 1959 (*Act. scient. et ind.*, 1264; *Publ. Inst. Math. Univ. Nancago*, 7).

[19] SERRE (Jean-Pierre). — Corps locaux et isogénies, *Séminaire Bourbaki*, t. 11, 1958-1959, exposé 185.

[20] SERRE (Jean-Pierre). — Sur la rationalité des représentations d'Artin, *Annals of Math.*, t. 72, 1960, p. 406-420.

[21] SERRE (Jean-Pierre). — Groupes proalgébriques, *Inst. H. Ét. scient.*, *Publ. math.*, n° 7, 1960, p. 1-67.

[22] TAMAGAWA (Tsuneo). — On the theory of ramification groups and conductors, *Jap. J. of Math.*, t. 21, 1951, p. 197-215.

[23] TATE (John). — The higher dimensional groups of class field theory, *Annals of Math.*, t. 56, 1952, p. 294-297.

[24] WHAPLES (George). — Generalized local class field theory, I : reciprocity law, *Duke math. J.*, t. 19, 1952, p. 505-517.

[25] WHAPLES (George). — Generalized local class field theory, II : existence theorem, *Duke math. J.*, t. 21, 1954, p. 247-256.

[26] WHAPLES (George). — Generalized local class field theory, III : second form of the existence theorem; structure of analytic groups, *Duke math. J.*, t. 21, 1954, p. 583-586.

[27] WHAPLES (George). — The generality of local class field theory (Generalized local class field theory, V), *Proc. Amer. math. Soc.*, t. 8, 1957, p. 137-140.

[28] WITT (Ernst). — Zyklische Körper und Algebren der Charakteristik p vom Grade p^m, *J. reine ang. Math.*, t. 176, 1936, p. 126-140.

(Manuscrit reçu le 30 octobre 1960)

Jean-Pierre SERRE,
6, avenue de Montespan,
Paris, 16e.