Journal of the Mathematical Society of Japan Vol. 3, No. 1, May, 1951.

Sur la Théorie du Corps de Classes

André WEIL

I. Rappel de résultats connus.

Nous allons rappeler d'abord, en la mettant sous la forme qui nous parait la plus appropriée, l'interprétation donnée par Chevalley ([5a], [5b]), au moyen des idèles, des théorèmes fondamentaux de Takagi (complétés par Artin) sur la théorie des corps de classes. Soit k un corps de nombres algébriques, de degré fini sur le corps des rationnels, ou bien un corps de fonctions algébriques de dimension 1 sur un corps de constantes fini. Par une valuation v de k, on entend un homomorphisme du groupe multiplicatif k^* des éléments non nuls de k dans le groupe additif R des réels, tel que $v(k^*) \neq \{0\}$ et qu'en posant $f(x) = e^{-\lambda v(x)}$ pour $x \in k^*$ et $f(0) = 0$, la fonction $f(x)$ satisfasse à $f(x+y) \leq f(x) + f(y)$ pourvu que λ soit un nombre positif suffisamment petit; si alors on complète k par rapport à la "distance" $f(x-y)$, on obtient un corps k_v localement compact; k_v ne change pas si on multiplie v par un facteur constant positif; on convient de ne pas distinguer deux valuations qui ne diffèrent que par un tel facteur. On peut "normer" les valuations de k, c'est-à-dire multiplier chacune par un facteur convenable, de telle sorte que l'on ait $\sum_v v(x) = 0$ quel que soit $x \in k^*$, la somme étant étendue à toutes les valuations essentiellement distinctes de k; c'est la formule dite "du produit" ([2]), récrite en notation additive. On désignera encore par v la valuation v étendue par continuité à k_v. On dit, comme on sait, que v est archimédienne si k_v est isomorphe, soit au corps des réels, soit au corps des complexes; on dira dans le premier cas que v est réelle, dans le second que v est complexe. Dans tout autre cas l'ensemble des valeurs de v, sur k ou sur k_v, est un sous-groupe discret de R, et on dit que v est discrète; k_v est alors isomorphe, soit à un corps $\mathfrak{p}$-adique, soit à un corps de séries formelles à une variable sur un corps de constantes fini, suivant que k est un corps de nombres ou de fonctions. On notera k_v^* le groupe multiplicatif des éléments non nuls de k_v; et, si v est discrète, on désignera par U_v le groupe des unités de k_v, c'est-à-dire le sous-groupe de k_v^* sur lequel v prend la valeur 0; U_v est alors un groupe compact, et k_v^*/U_v est isomorphe au groupe additif

Z des entiers. Si v est archimédienne complexe, on posera $U_v = k_v^*$. Si v est archimédienne réelle, on désignera par U_v le groupe multiplicatif des éléments >0 de k_v^*, k_v étant en ce cas identifié avec le corps des réels. Dans le groupe (non topologique) Πk_v^*, où le produit est étendu à toutes les valuations v de k, considérons le sous-groupe I_k des éléments $a=(a_v)$ tels que $a_v \in U_v$ sauf au plus pour des valuations v en nombre fini ; les éléments de I_k s'appellent, comme on sait, les *idèles* de k. Sur I_k, on définit une topologie comme suit : sur le sous-groupe $U=\Pi U_v$ de I_k, on prend pour topologie la topologie produit de celles des U_v ; et on impose à I_k la condition que I_k/U soit un groupe discret, ou autrement dit on prend la famille de tous les voisinages de l'élément neutre dans U comme système fondamental de voisinages de cet élément dans I_k. Muni de cette topologie, I_k s'appellera *le groupe des idèles de* k ; c'est un groupe abélien séparé, localement compact. Si k est un corps de fonctions, U est compact, et U et I_k sont totalement discontinus. Si k est un corps de nombres, le produit $H_k=\Pi' U_v$, étendu aux seules valuations archimédiennes v de k, est la composante connexe de l'élément neutre dans I_k, et dans U ; en ce cas, U/H_k est compact, et U/H_k et I_k/H_k sont totalement discontinus. Si, pour tout idèle $a=(a_v)$, on pose $d(a)=\sum v(a_v)$, la somme étant étendue à toutes les valuations de k, d est un homomorphisme de I_k sur le groupe additif R des réels si k est un corps de nombres, et (les valuations étant convenablement normées) sur le groupe additif Z des entiers si k est un corps de fonctions. Si, pour chaque v, i_v est l'isomorphisme "naturel" de k dans k_v, on définit un isomorphisme de k^* dans I_k en posant, pour $x \in k^*$, $i(x)=(i_v(x))$; le groupe $P_k=i(k^*)$ s'appelle le groupe des idèles principaux de k ; on l'identifie parfois avec k^* quand il n'y a pas de danger de confusion ; en vertu de la formule du produit, l'homomorphisme d prend la valeur 0 sur P_k.

De plus, P_k est un sous-groupe *discret* de I_k. En effet, si k est un corps de fonctions, $P_k \cap U$ se réduit au groupe multiplicatif des constantes non nulles, donc à un groupe fini ; si k est un corps de nombres, $P_k \cap U$ est l'image $i(E)$ du groupe E des unités totalement positives de k ; et, comme il ne peut y avoir qu'un nombre fini d'entiers de k dont les images dans les corps k_v correspondant à toutes les valuations archimédiennes v de k soient bornées en valeur absolue, il n'y a à plus forte raison qu'un

nombre fini d'éléments de $i(E)$ dans un voisinage compact de l'élément neutre de U. Par conséquent, le groupe $C_k = I_k/P_k$ est un groupe séparé, localement compact, localement isomorphe à I_k; C_k s'appellera *le groupe des classes d'idèles de k.* Si k est un corps de nombres, les caractères de C_k sont les *Grössencharaktere* de Hecke ([8]), au moyen desquels sont formées les séries L de Hecke attachées au corps k.

Comme l'homomorphisme d, défini plus haut sur I_k au moyen de $d(a) = \sum_v v(a_v)$ pour $a = (a_v)$, prend la valeur 0 sur P_k, on en déduit, par passage au quotient, un homomorphisme de C_k, sur R ou sur Z suivant le cas; soit C_k^0 le noyau de celui-ci, c'est-à-dire le sous-groupe de C_k où il prend la valeur 0. *Le groupe C_k^0 est compact*: c'est ce qui résulte, si k est un corps de fonctions, du fait que les classes de diviseurs de degré 0 sont en nombre fini, et, si k est un corps de nombres, du théorème de Dirichlet et du fait que les classes d'idéaux de k sont en nombre fini. Il s'ensuit que C_k est isomorphe au produit direct de C_k^0 et de C_k/C_k^0, ce dernier groupe étant isomorphe à R ou à Z suivant que k est un corps de nombres ou de fonctions.

Soit alors A_k l'extension abélienne maximale de k; elle est bien définie, à un isomorphisme près, comme la réunion, dans une extension algébriquement close de k, de toutes les extensions abéliennes de k de degré fini. Pour énoncer le théorème fondamental de la théorie du corps de classes, supposons d'abord que k soit un corps de fonctions, sur un corps de constantes fini k_0 à q éléments. Alors A_k contient une extension algébriquement close $\bar{k}_0$ de k_0. Soit G_k^0 le sous-groupe du groupe de Galois de A_k sur k formé des automorphismes qui laissent invariants tous les éléments de $\bar{k}_0$; on peut le considérer comme groupe de Galois de A_k sur le composé de k et de $\bar{k}_0$; muni de la topologie habituelle, c'est un groupe compact. Soit G_k le sous-groupe du groupe de Galois de A_k sur k, formé des automorphismes qui induisent sur $\bar{k}_0$ un automorphisme de la forme $\xi \to \xi^{q^d}$, où d est un entier quelconque; on topologisera G_k par la condition que G_k/G_k^0 soit un groupe discret (isomorphe à Z). Cela posé, *la théorie du corps de classes affirme l'existence d'un isomorphisme canonique entre C_k et G_k.* On peut dire qu'elle donne une interprétation de C_k au moyen d'un groupe de Galois.

Si k est un corps de nombres, une telle interprétation n'est plus possible, puisqu'en raison de l'existence de valuations archimédiennes C_k et

C_k^0 ne sont plus totalement discontinus. Mais soient D_k la composante connexe de l'élément neutre dans C_k, et G_k' le groupe de Galois de A_k sur k; G_k' est compact. *La théorie du corps de classes affirme ici l'existence d'un isomorphisme canonique entre* $C_k'=C_k/D_k$ *et* G_k'; elle donne donc une interprétation, sinon de C_k, tout au moins de C_k' au moyen d'un groupe de Galois.

La recherche d'une interprétation pour C_k *si* k *est un corps de nombres*, analogue en quelque manière à l'interprétation par un groupe de Galois quand k est un corps de fonctions, *me semble constituer l'un des problèmes fondamentaux de la théorie des nombres* à l'heure actuelle; il se peut qu'une telle interprétation renferme la clef de l'hypothèse de Riemann; il est plausible qu'il convienne de la chercher du côté de la théorie des espaces fibrés, dont l'importance se fait de plus en plus grande dans tant de branches des mathématiques, topologie bien entendu, mais déjà aussi géométrie algébrique, espaces de Hilbert, et bientôt sans doute arithmétique. Nous n'entendons pas aborder ici ces grands problèmes, mais traiter seulement une question préjudicielle, dont la solution montre en tout cas qu'on a le droit de songer à une interprétation de C_k telle que nous l'envisageons.[1]

II. Position du problème.

Comme ci-dessus, soit k un corps de nombres ou de fonctions; soit K une extension galoisienne de k de degré fini; on désignera par $\mathfrak{g}(K/k)$ le groupe de Galois de K sur k. Si G est un groupe abélien, topologique ou non, attaché à K d'une manière invariante, les éléments de $\mathfrak{g}(K/k)$, c'est-à-dire les automorphismes de K laissant les éléments de k invariants, induiront en général d'une manière " naturelle " (si évidente le plus souvent qu'il sera inutile de la préciser) des automorphismes de G, de sorte que G sera " naturellement " muni d'une structure de groupe à opérateurs sur $\mathfrak{g}(K/k)$; si $x\in G$, et $\alpha\in\mathfrak{g}(K/k)$, on notera x^α le transformé de x par α. On appelle norme de x, et on note $N_{K/k}(x)$ ou plus brièvement $N(x)$, le

(1) Si l'on ne considère que la structure du groupe G_K, $_k$, celle-ci est déterminée par une classe de système de facteurs de $\mathfrak{g}(K/k)$ dans C_K. T. Nakayama a obtenu une autre caractérisation invariante de cette classe de système de facteurs; v. [10a], et aussi [10b], où on trouvera un grand nombre de résultats intéressants sur ce sujet.

produit $N(x)=\prod_{\alpha} x^{\alpha}$, étendu à tous les $\alpha\in\mathfrak{g}(K/k)$. On aura à considérer des systèmes de facteurs, et plus généralement des cocycles de diverses dimensions ([6]) de $\mathfrak{g}(K/k)$ dans G ; un système de facteurs est un cocycle de dimension 2, dont la classe d'homologie détermine, à un isomorphisme près, une extension de G par $\mathfrak{g}(K/k)$.

En particulier, I_K et C_K peuvent ainsi être considérés comme groupes à opérateurs sur $\mathfrak{g}(K/k)$. D'autre part, si w est une valuation de K, w induit une valuation v sur k, et k_v peut être considéré comme canoniquement plongé dans K_w ; alors, si a est un idèle de I_k, on définit un idèle $\bar{a}=(\bar{a}_w)$ de I_K en posant $\bar{a}_w=a_v$ pour toute valuation w de K, v étant la valuation induite par w sur k ; on vérifie immédiatement que l'application $a\to\bar{a}$ est un isomorphisme de I_k dans I_K ; et on identifiera le plus souvent I_k avec son image dans I_K par cet isomorphisme. On vérifie alors aisément que I_k n'est autre que l'ensemble des éléments de I_K qui sont invariants par tous les automorphismes de $\mathfrak{g}(K/k)$, d'où s'ensuit en particulier que l'on a $P_k=P_K\cap I_k$. Par passage au quotient, on voit alors que l'isomorphisme canonique de I_k dans I_K induit une représentation biunivoque de C_k dans C_K. Plus précisément, si W est un voisinage de l'élément neutre 1 dans I_K, tel que $P_K\cap(W^{-1}W)=\{1\}$, on a $P_K\cap I_kW=P_k$, d'où résulte que l'isomorphisme canonique de I_k dans I_K induit un *isomorphisme* de C_k dans C_K, au moyen duquel on identifiera le plus souvent C_k avec le sous-groupe correspondant de C_K. Si a est un représentant dans I_K d'un élément de C_K invariant par tous les automorphismes de $\mathfrak{g}(K/k)$, on aura, quel que soit $\alpha\in\mathfrak{g}(K/k)$, $a^{\alpha-1}=\xi_\alpha\in P_K$, d'où $\xi_{\alpha\beta}=\xi_\alpha{}^{\beta}\xi_\beta$, et par suite, en vertu d'un théorème célèbre de Hilbert (qu'on peut exprimer en disant que le premier groupe de cohomologie de $\mathfrak{g}(K/k)$ dans K^* est trivial), $\xi_\alpha=\eta^{1-\alpha}$ avec $\eta\in P_K$; donc $a'=a\eta$ est invariant par $\mathfrak{g}(K/k)$ et est dans I_k. On voit donc que C_k est l'ensemble des éléments de C_K qui sont invariants par tous les automorphismes de $\mathfrak{g}(K/k)$.

Si de plus k et K sont des corps de nombres, et si comme toujours D_k et D_K sont les composantes connexes de l'élément neutre dans C_k et C_K, il est clair que $D_k\subset D_K$, et par suite l'isomorphisme canonique de C_k dans C_K induit une représentation canonique de $C_k'=C_k/D_k$ dans $C_K'=C_K/D_K$; mais en général, comme on le verra au § III, celle-ci n'est pas biunivoque.

Si H est un groupe topologique non abélien, on notera H^c l'adhérence dans H du groupe engendré par les commutateurs de H, et par H^a le groupe quotient abélien $H^a=H/H^c$. On aura besoin de la notion de *trans-*

fert: si H' est un sous-groupe fermé de H, d'indice fini, le transfert (" *Verlagerung* ") de H dans H' est une certaine représentation de H dans H'^a, qu'on conviendra de noter $t_{H/H'}$; pour sa définition, cf. [14]. Comme H'^a est abélien, le noyau de $t_{H/H'}$ contient H^c, et par suite on déduit de $t_{H/H'}$, par passage au quotient, une représentation $\bar{t}_{H/H'}$ de H^a dans H'^a qu'on appellera le *transfert réduit* de H dans H'. Le transfert réduit est transitif, c'est-à-dire que, si H'' est un sous-groupe de H' d'indice fini, on a $\bar{t}_{H/H''}=\bar{t}_{H'/H''}\circ\bar{t}_{H/H'}$. Dans les cas que nous avons principalement en vue, H' sera un groupe abélien G attaché à K, admettant $\mathfrak{g}(K/k)$ comme groupe d'opérateurs, et H sera une extension de G par $\mathfrak{g}(K/k)$. Dans ce cas, soit (s_α) un système de représentants dans H des éléments α de $\mathfrak{g}(K/k)$; soit $a_{\alpha,\beta}=s_{\alpha\beta}^{-1}s_\alpha s_\beta$; alors $(a_{\alpha,\beta})$ est un système de facteurs de $\mathfrak{g}(K/k)$ dans G; et, pour $x\in G$, on a $s_\alpha^{-1}xs_\alpha=x^\alpha$. Tout élément de H est alors de la forme $s_\alpha x$, avec $x\in G$, et on trouve que son transfert est

$$t_{H/G}(s_\alpha x)=(\prod_\beta a_{\alpha,\beta})\cdot N(x)\ ;$$

on vérifie aisément d'ailleurs que c'est là un élément de G invariant par tous les automorphismes de $\mathfrak{g}(K/k)$, ou autrement dit que c'est un élément du centre de H. En particulier, on a $t_{H/G}(x)=N(x)$, d'où $t_{H/G}(G)=N(G)$. Si $\mathfrak{g}(K/k)$ est un groupe cyclique engendré par un élément σ d'ordre n, on trouve que $t_{H/G}(s_\sigma)=s_\sigma^n$.

Maintenant, soit d'abord k un corps de fonctions, sur le corps de constantes fini k_0 à q éléments; K étant une extension galoisienne de k, de degré fini, l'extension abélienne maximale A_K de K est galoisienne sur k. Soit $G_{K,k}$ le sous-groupe du groupe de Galois de A_K sur k, formé des automorphismes qui induisent sur $\bar{k}_0$ un automorphisme de la forme $\xi\to\xi^{q^d}$; soit $G^0_{K,k}$ le sous-groupe de $G_{K,k}$ formé des automorphismes qui laissent invariants les éléments de $\bar{k}_0$; $G^0_{K,k}$ peut être considéré comme groupe de Galois de A_K sur le composé de k et de $\bar{k}_0$, et topologisé comme tel, ce qui en fait un groupe compact; on topologisera $G_{K,k}$ par la condition que $G_{K,k}/G^0_{K,k}$ soit discret (et par suite isomorphe à Z). Alors le groupe que nous avons noté G_K est le sous-groupe fermé de $G_{K,k}$ qui laisse invariants les éléments de K; et $G_{K,k}/G_K$ peut être identifié avec $\mathfrak{g}(K/k)$. Si en même temps on identifie G_K avec C_K au moyen de la théorie du corps de classes, alors il résulte de celle-ci que les automophismes induits sur $C_K=G_K$ par un système de représentants de $\mathfrak{g}(K/k)$ dans $G_{K,k}$ ne sont autres

que les automorphismes " naturels " déterminés par $\mathfrak{g}(K/k)$ sur C_K. De plus, les groupes $G_{K,k}$ satisfont aux trois conditions suivantes, dont la première est une conséquence de la théorie du corps de classes[2], et les autres sont évidentes :

(A) On peut identifier G_k avec $G^a_{K,k}$, car $G^c_{K,k}$ est le sous-groupe fermé de $G_{K,k}$ formé des automorphismes qui laissent invariants les éléments de l'extension abélienne maximale A_k de k ; le transfert réduit de $G_{K,k}$ dans G_K est donc une représentation de G_k dans le sous-groupe de G_K formé des éléments de G_K invariants par $\mathfrak{g}(K/k)$. Si donc on identifie G_k avec C_k, et G_K avec C_K, le transfert réduit de $G_{K,k}$ dans G_K détermine une représentation de C_k dans le sous-groupe C_k de C_K ; *cette représentation est l'isomorphisme canonique de* C_k *dans* C_K.

(B) Si k' est un corps intermédiaire entre k et K, $G_{K,k'}$ *est le sous-groupe de* $G_{K,k}$ *laissant invariants les éléments de* k' ; *c'est donc l'image réciproque de* $\mathfrak{g}(K/k')$ *dans* $G_{K,k}$ *par l'homomorphisme canonique de* $G_{K,k}$ *sur* $\mathfrak{g}(K/k) = G_{K,k}/G_K$.

(C) Soit K' une extension de K de degré fini, galoisienne sur k ; $G^c_{K',K}$ est le sous-groupe de $G_{K',K}$ qui laisse invariants les éléments de l'extension abélienne maximale A_K de K ; donc *on peut identifier* $G_{K,k}$ *avec* $G_{K',k}/G^c_{K',K}$, le sous-groupe G_K de $G_{K,k}$ s'identifiant alors avec $G^a_{K',K}$ conformément à (A).

De plus, pour les corps de fonctions, ces résultats, joints à ceux qui ont été énoncés précédemment, contiennent toute la théorie du corps de classes. En particulier, le " théorème de translation " pour les extensions galoisiennes est contenu dans (A), et le même théorème pour les extensions finies quelconques résulte aussitôt de (A) et (B).

Passons aux corps de nombres. Soit $G'_{K,k}$ le groupe de Galois de A_K sur k ; c'est un groupe compact ; le groupe de Galois G'_K de A_K sur K est un sous-groupe fermé de $G'_{K,k}$, qu'on peut identifier avec C'_K, et le groupe $G'_k = G'^a_{K,k} = G'_{K,k}/G'^c_{K,k}$ peut de même être identifié avec C'_k. On voit alors, comme tout à l'heure, que les groupes $G'_{K,k}$ satisfont à des conditions exactement analogues à (A), (B), (C), à cela près que l'isomorphisme

(2) Bien que cette propriété (A) (ou " théorème de transfert ") ne semble pas avoir été jamais explicitement formulée, elle est contenue en substance dans les raisonnements d'Artin sur le " Hauptidealsatz " ([1b] ; cf. [7] et [9]). Pour la démonstration du théorème local correspondant, qui, lui, est beaucoup moins facile à vérifier, v. [5c].

canonique de C_k dans C_K doit être remplacé par la représentation canonique de C_k' dans C_K', qui n'est pas biunivoque en général ; pour cette raison, (A) et (B) n'impliquent plus le théorème de translation.

On peut conjecturer que, si l'on savait interpréter convenablement les groupes C_k, on pourrait tirer de là une définition de groupes $G_{K,k}$ jouissant de propriétés analogues à celles qu'on vient d'énumérer. Alors $G_{K,k}$ *aurait un sous-groupe invariant fermé qu'on pourrait identifier canoniquement avec* C_K, *le quotient* $G_{K,k}/C_K$ *s'identifiant canoniquement avec* $\mathfrak{g}(K/k)$, *et* $G_{K,k}/D_K$ *avec* $G'_{K,k}$; *les automorphismes induits sur* C_K *par un système de représentants dans* $G_{K,k}$ *des éléments* α *de* $\mathfrak{g}(K/k)$ *seraient les automorphismes "naturels"* $x \to x^\alpha$ *de* C_K ; *les groupes* $G_{K,k}$ *satisferaient aux conditions* (A), (B), (C) ; *et les diverses représentations de ces groupes les uns dans les autres qui figurent dans l'énoncé de ces conditions induiraient par passage au quotient les représentations correspondantes des groupes* $G'_{K,k}$ *les uns dans les autres.* En revanche, s'il n'existait pas de tels groupes $G_{K,k}$, ce serait signe que l'analogie entre corps de fonctions et corps de nombres ne s'étend pas complètement aux groupes C_k.

Pour que cette analogie soit parfaite, il faut d'ailleurs que les propriétés des groupes $G_{K,k}$ contiennent le théorème de translation. On se convainc aisément qu'il en sera ainsi pourvu qu'ils satisfassent, en plus des conditions ci-dessus, à la suivante :

(D) Soit t le transfert de $G_{K,k}$ dans C_K ; t applique en tout cas $G_{K,k}$ dans C_k (et même sur C_k si (A) est satisfaite). Soient x un élément de $G_{K,k}$, x' son image dans $G'_{K,k}$, et x'' l'image de $t(x)$ dans $C_k' = G_k'$. Alors *l'automorphisme* x'' *de* A_k *doit être celui qui est induit sur* A_k *par l'automorphisme* x' *de* A_K.

Notre but est de construire des groupes $G_{K,k}$ possédant toutes les propriétés qu'on vient d'énoncer. D'une manière plus précise, il s'agit donc d'attacher à chaque couple de corps K, k, où K est galoisien sur k, un groupe topologique $G_{K,k}$, un isomorphisme f de C_K sur un sous-groupe invariant fermé de $G_{K,k}$, et un homomorphisme φ de $G_{K,k}$ sur $G'_{K,k}$, de noyau $f(D_K)$, de manière que $\varphi \circ f$ soit l'homomorphisme canonique de C_K sur le sous-groupe $C_K' = G_K'$ de $G'_{K,k}$ et que les autres conditions ci-dessus soient satisfaites. Nous montrerons que *les conditions* (B) *et* (D) *déterminent la solution du problème d'une manière unique*, et que *cette solution satisfait à* (A) *et* (C).

III. Résultats auxiliaires.

On désignera par Z, Q, R et T les groupes additifs des entiers, des rationnels, des réels, et des réels modulo 1, respectivement.

Nous allons démontrer d'abord quelques résultats relatifs à un seul corps de nombres k. Soient r et s les nombres de valuations archimédiennes réelles et complexes de k, respectivement. Alors la composante connexe H_k de l'élément neutre dans I_k est isomorphe à $R^{r+s} \times T^s$. On désignera par H_k' le sous-groupe compact maximal de H_k; il est formé des idèles $a=(a_v)$ tels que $v(a_v)=0$, c'est-à-dire $|a_v|=1$, pour toute valuation v archimédienne complexe, et $a_v=1$ pour toute autre valuation de k. L'homomorphisme canonique de I_k sur C_k induit sur H_k' une représentation biunivoque, donc, puisque H_k' est compact, un isomorphisme, sur son image dans C_k; cette image sera désignée par D_k'; étant connexe, c'est un sous-groupe de D_k.

On dit, comme on sait, qu'un groupe abélien (noté multiplicativement) possède la propriété d'*unique divisibilité* si l'application $x \to x^n$ de ce groupe dans lui-même est un automorphisme quel que soit l'entier $n \neq 0$. On va montrer que D_k/D_k' *possède la propriété d'unique divisibilité.*

Soit $\mathfrak{m}$ un idéal entier de k, autre que (0); soit $\mathfrak{m}=\prod_i \mathfrak{p}_i^{m_i}$ sa décomposition en puissances d'idéaux premiers distincts; soit v_i la valuation (discrète) de k attachée à $\mathfrak{p}_i$; notons aussi $\mathfrak{p}_i$ l'idéal premier de k_{v_i}. On désignera alors par $I_\mathfrak{m}$ le groupe des idèles $a=(a_v)$ tels que $a_v \in U_v$ quelle que soit v, $a_v=1$ pour toute valuation archimédienne de k, et $a_{v_i} \equiv 1 \bmod. \mathfrak{p}_i^{m_i}$ pour tout i. Les $I_\mathfrak{m}$ sont compacts, et tout voisinage de l'élément neutre dans I_k contient tous les $I_\mathfrak{m}$ sauf un nombre fini d'entre eux. Il est immédiat que $H_k I_\mathfrak{m}$ est un sous-groupe ouvert de I_k, produit direct de H_k et $I_\mathfrak{m}$.

Comme plus haut, soit i l'isomorphisme canonique de k^* sur P_k; et, pour $\xi \in k^*$, soit $j(\xi)$ la projection de $i(\xi)$ sur le produit partiel $\Pi' k_v^*$, où Π' désigne le produit étendu aux seules valuations archimédiennes de k. D'après le théorème de Dirichlet, j induit, sur le groupe E des unités totalement positives de k, un isomorphisme de E sur son image $j(E)$ dans $\Pi' k_v^*$; et on a $j(E) \subset H_k$. Alors $H_k \cap P_k I_\mathfrak{m}$ est l'image $j(E_\mathfrak{m})$ du groupe $E_\mathfrak{m}$ des unités totalement positives de k qui sont $\equiv 1 \bmod. \mathfrak{m}$.

Soit encore f la représentation de H_k dans D_k induite sur H_k par l'ho-

momorphisme canonique de I_k sur C_k ; soient D_k^*, H_k^* les groupes duaux (ou groupes des caractères ; cf. [13], chap. VI) de D_k et H_k, et soit f^* la duale (ou transposée) de f, qui est une représentation de D_k^* dans H_k^*. Pour qu'un caractère χ de H_k soit l'image par f^* d'un caractère de D_k, il faut et il suffit qu'il soit prolongeable à un caractère ψ de I_k qui prenne la valeur 1 sur P_k. Mais, ψ devant être continu, et le groupe $I_\mathfrak{m}$ pouvant être pris aussi petit qu'on veut, il y aura un $\mathfrak{m}$ tel que $\psi=1$ sur $I_\mathfrak{m}$, donc sur $P_kI_\mathfrak{m}$, d'où $\chi=1$ sur $H_k\cap P_kI_\mathfrak{m}=j(E_\mathfrak{m})$. Réciproquement, supposons que χ soit tel. Comme on a $H_kI_\mathfrak{m}=H_k\times I_\mathfrak{m}$, on pourra, d'une manière et d'une seule, prolonger χ à $H_kI_\mathfrak{m}$ par la condition que $\chi=1$ sur $I_\mathfrak{m}$; alors on a $\chi=1$ sur $H_kI_\mathfrak{m}\cap P_kI_\mathfrak{m}$. Comme $H_kI_\mathfrak{m}$ est ouvert dans I_k, donc dans $H_kI_\mathfrak{m}P_k$, on pourra dans ces conditions prolonger χ à $H_kI_\mathfrak{m}P_k$ d'une manière et d'une seule par la condition que $\chi=1$ sur P_k ; puis on pourra prolonger χ à un caractère de I_k. Ce raisonnement montre de plus que, si $\chi=1$ sur H_k, il y a un $\mathfrak{m}$ tel que $\psi=1$ sur $H_kI_\mathfrak{m}P_k$; ce dernier groupe étant ouvert dans I_k, il en est de même de son image dans C_k, image qui contient donc D_k, de sorte que le caractère de C_k qui se déduit de ψ par passage au quotient prend la valeur 1 sur D_k. On a ainsi démontré que f^* est une représentation biunivoque de D_k^* dans H_k^*, et que $f^*(D_k^*)$ est l'ensemble des caractères de H_k qui prennent la valeur 1 sur l'un des groupes $j(E_\mathfrak{m})$.

Mais, en vertu d'un théorème de Chevalley ([5c]), *si m est un entier* >0, *il existe un idéal* $\mathfrak{m}\neq(0)$ *tel que* $E_\mathfrak{m}\subset E^m$; autrement dit, tout sous-groupe de E d'indice fini contient un groupe $E_\mathfrak{m}$. Comme les $E_\mathfrak{m}$ sont d'indice fini dans E, on voit que $f^*(D_k^*)$ est l'ensemble des caractères de H_k qui prennent la valeur 1 sur un sous-groupe d'indice fini de $j(E)$. Au moyen du théorème de Dirichlet sur les unités, on voit alors, élémentairement, que H_k^* peut être identifié avec $R^{r+s}\times Z^s$ de telle sorte que $f^*(D_k^*)$ se trouve identifié avec $R\times Q^{r+s-1}\times Z^s$, où Q est considéré comme sous-groupe de R. D'ailleurs, puisque C_k est isomorphe au produit de R et d'un groupe compact, il en est de même de D_k ; donc D_k^* est isomorphe au produit de R et d'un groupe discret. Il s'ensuit que D_k^* est isomorphe à $R\times Q^{r+s-1}\times Z^s$, R étant muni de la topologie habituelle, et Q et Z étant discrets. De plus, le dual de H_k/H_k' est le sous-groupe R^{r+s} de $H_k^*=R^{r+s}\times Z^s$; D_k' ayant été défini comme l'image de H_k' dans D_k, on conclut alors aisément que le dual de D_k/D_k' est isomorphe à $R\times Q^{r+s-1}$ et a donc la propriété d'unique divisibilité, ce qui entraîne que D_k/D_k' la possède aussi.

Convenons maintenant de désigner par Γ_k le groupe des idèles $a=(a_v)$ tels que $a_v=\pm 1$ pour toute valuation archimédienne réelle de k, et $a_v=1$ pour toute autre valuation ; c'est un groupe à 2^r éléments d'ordre 2, et on a $\prod_v' k_v=\Gamma_k\times H_k$. L'homomorphisme canonique de I_k sur C_k induit sur Γ_k un isomorphisme de Γ_k snr son image dans C_k, image qu'on désignera par γ_k. Alors, pour tout $\mathfrak{m}$, on a $(\Gamma_k H_k)\cap(P_k I_{\mathfrak{m}})=j(E'_{\mathfrak{m}})$, où $E_{\mathfrak{m}}'$ est le groupe des unités $\equiv 1$ mod. $\mathfrak{m}$ dans k. En vertu du théorème de Chevalley, on peut choisir $\mathfrak{m}$ de façon que toute unité de $E_{\mathfrak{m}}'$ soit totalement positive, donc que $E_{\mathfrak{m}}'=E_{\mathfrak{m}}$; on aura alors $(\Gamma_k H_k)\cap(P_k I_{\mathfrak{m}})\subset H_k$, d'où $\Gamma_k\cap H_k I_{\mathfrak{m}} P_k\subset \Gamma_k\cap H_k=\{1\}$. Mais, comme on vient de le voir, l'image de $H_k I_{\mathfrak{m}} P_k$ dans C_k contient D_k ; par suite l'image réciproque de D_k dans I_k est contenue dans $H_k I_{\mathfrak{m}} P_k$; elle est donc sans élément commun autre que 1 avec Γ_k. *On voit donc que l'on a* $\gamma_k\cap D_k=\{1\}$, d'où il s'ensuit que l'homomorphisme canonique de $C_{k_{\mathfrak{m}}}$ sur C_k' induit sur γ_k un isomorphisme de γ_k sur son image γ_k' dans C_k'.

Soit maintenant K une extension galoisienne de k ; soit $\mathfrak{g}=\mathfrak{g}(K/k)$ son groupe de Galois. Comme D_K/D_K' a la propriété d'unique divisibilité, il résulte d'un raisonnement bien connu[3] que les groupes de cohomologie de $\mathfrak{g}$ dans D_K/D_K' sont triviaux, et par suite que ceux de $\mathfrak{g}$ dans D_K sont les mêmes que ceux de $\mathfrak{g}$ dans D_K' ; autrement dit, tout cocycle de $\mathfrak{g}$ dans D_K est homologue à un cocycle de $\mathfrak{g}$ dans D_K', et celui-ci ne peut être trivial dans D_K' que si le premier l'est dans D_K. Pour connaître les groupes de cohomologie de $\mathfrak{g}$ dans D_K, il suffit donc de déterminer ceux de $\mathfrak{g}$ dans D_K', ou, ce qui revient au même, dans H_K'. Mais la théorie de Galois permet de déterminer immédiatement la structure de H_K' en tant que groupe à opérateurs sur $\mathfrak{g}$. Si on groupe ensemble toutes les valuations complexes de K qui induisent une même valuation, réelle ou complexe, sur k, on voit que H_K' est produit direct de tores, dont chacun est invariant par $\mathfrak{g}$ et

---

(3) Avec la notation "homogène" de [6], soit $F(a_0,\cdots\cdots,a_d)$ un cocycle de dimension d d'un groupe fini $\mathfrak{g}$ d'ordre n dans un groupe G écrit additivement, sur lequel $\mathfrak{g}$ opère à gauche. Supposons que $x\to nx$ soit un automorphisme de G. Alors on a $F=\partial F'$, F' étant la cochaîne définie par $nF'(a_1,\cdots\cdots,a_d)=\sum_{\beta\in\mathfrak{g}} F(\beta,a_1,\cdots\cdots,a_d)$. Pour $d=0$, $F(a)$ est un cocycle si $F(a)=x=ax$ quel que soit a ; et le résultat qu'on vient d'énoncer subsiste si on convient de considérer ce cocycle comme trivial chaque fois que $x=\sum_\beta \beta y$, c'est-à-dire chaque fais que x est une trace (ou, en notation multiplicative, une norme) ; cette convention, qui diffère de celle de [6], semble plus indiquée quand $\mathfrak{g}$ est un groupe fini.

correspond, soit à une valuation complexe de k, soit à une valuation réelle de k qui se ramifie dans K; ceux de la première sorte sont de dimension $n=[K:k]$, et ceux de la seconde sorte sont de dimension $n/2$. Les premiers, en tant que groupes à opérateurs, sont tous isomorphes à $\theta=\prod_\lambda T_\lambda$, où le produit $\prod_\lambda$ est étendu à tous les éléments λ de $\mathfrak{g}$, où $T_\lambda=T'$ quel que soit λ, et où le transformé de $x=(x_\lambda)$ par $a\in\mathfrak{g}$ est $x^a=(x_{a\lambda})$. Considérons d'autre part un tore de la seconde sorte, correspondant à une valuation réelle v de k; soit w l'une des valuations complexes de K qui prolongent v. Le sous-groupe H de $\mathfrak{g}$ qui laisse w invariante est d'ordre 2; soit $H=\{\varepsilon,\sigma\}$, où ε est l'élément neutre de $\mathfrak{g}$, et σ est un élément d'ordre 2. Alors le tore de seconde sorte correspondant à v peut être identifié avec le sous-groupe θ_σ de θ formé des éléments $x=(x_\lambda)$ tels que $x_{\lambda\sigma}=-x_\lambda$ pour tout λ.

Les groupes de cohomologie de $\mathfrak{g}$ dans D_K', ou dans H_K', sont alors produits directs des groupes correspondants de $\mathfrak{g}$ dans les tores de première et de seconde sorte. Mais, en vertu d'un théorème général[4], les groupes de $\mathfrak{g}$ dans θ sont triviaux; ceux de $\mathfrak{g}$ dans θ_σ sont respectivement isomorphes à ceux de H dans T si H opère sur T par la loi $x^\sigma=-x$; et ces derniers sont triviaux dans les dimensions impaires, et d'ordre 2 dans les dimensions paires, en vertu des résultats connus sur la cohomologie des groupes cycliques ([6], p. 77). On conclut de là, en premier lieu, que *les groupes de cohomologie de* $\mathfrak{g}$ *dans* H_K', D_K' *et* D_K *sont triviaux dans les dimensions impaires.*

Soient maintenant v_i $(1\leq i\leq r_0)$ toutes les valuations réelles de k qui se ramifient dans K; pour chacune, soit θ_i le sous-groupe de H_K' formé des idèles $a=(a_w)\in H_K'$ tels que $a_w=1$ pour toute valuation w de K qui n'induit pas v_i sur k. D'après ce qui précède, il existe pour chaque dimension paire un cocycle non trivial b_i de $\mathfrak{g}$ dans θ_i et un seul; b_i^2 est

---

(4) Il s'agit du théorème suivant. Soient $\mathfrak{g}$ un groupe fini, $\mathfrak{g}'$ un sous groupe de $\mathfrak{g}$; soit G un groupe abélien, sur lequel $\mathfrak{g}'$ opère à gauche. Soit $A=\prod_{\lambda\in\mathfrak{g}} A_\lambda$, où $A=G$ quel que soit $\lambda\in\mathfrak{g}$; si $x=(x_\lambda)\in A$, soit $x^a=(x_{a\lambda})$; soit A_0 le sous-groupe de A formé des $x=(x_\lambda)$ tels que $x_{\lambda\sigma}=\sigma^{-1}x_\lambda$ quels que soient $\lambda\in\mathfrak{g}$ et $\sigma\in\mathfrak{g}'$. Soit f un cocycle de dimension d de $\mathfrak{g}$ dans A_0, $\mathfrak{g}$ opérant sur A_0 par la loi $(x,a)\to x^a$. Pour $\sigma_i\in\mathfrak{g}'$ $(1\leq i\leq d)$, soit $f'(\sigma_1,\cdots\cdots,\sigma_d)$ la coordonnée de $f(\sigma_1,\cdots\cdots,\sigma_d)$ relative à A_ε, ε étant l'élément neutre de $\mathfrak{g}$. Alors f' est un cocycle de $\mathfrak{g}'$ dans G; et la correspondance $f\to f'$ induit un isomorphisme du groupe de cohomologie de dimension d de $\mathfrak{g}$ dans A_0 sur celui de $\mathfrak{g}'$ dans G. Pour la démonstration, v. [10b].

un cocycle trivial de $\mathfrak{g}$ dans θ_i; tout cocycle de $\mathfrak{g}$ dans H'_K de cette dimension est homologue à un cocycle et un seul de la forme $\Pi b_i^{f_i}$, où $f_i=0$ ou 1 pour $1 \leq i \leq r_0$; et tout cocycle de $\mathfrak{g}$ dans D_K est homologue à l'image d'un tel cocycle et d'un seul par l'isomorphisme canonique de H'_K sur D'_K.

Ce qui précède s'applique en particulier à la dimension 0 (cf.[2]). Tout élément x de D_K, invariant par $\mathfrak{g}$, est donc de la forme $y\Pi a_i^{f_i}$, où y est " trivial " c'est-à-dire de la forme $N(z)=N_{K/k}(z)$ avec $z \in D_K$, et où a_i est l'image dans D'_K d'un élément $\bar{a}_i$ non trivial de θ_i, invariant par $\mathfrak{g}$. Mais les seuls éléments de θ_i invariants par $\mathfrak{g}$ sont les deux idèles (a_v) de I_k tels que $a_{v_i}=\pm 1$, et $a_v=1$ pour $v \neq v_i$; donc $\bar{a}_i$ est celui de ces idèles pour lequel $a_{v_i}=-1$. Soit $\gamma_{k,K}$ le sous-groupe de γ_k d'ordre 2^{r_0} qui est engendré par les a_i. On a donc démontré que le groupe $D_K \cap C_k$ des éléments de D_K invariants par $\mathfrak{g}$ est le groupe $N(D_K)\gamma_{k,K}$. On a vu plus haut que $\gamma_k \cap D_k=\{1\}$, donc a fortiori $\gamma_{k,K} \cap D_k=\{1\}$; d'ailleurs, D_k étant connexe, on a $D_k \subset D_K$, donc $D_k \subset D_K \cap C_k$; et, D_K étant connexe, $N(D_K)$ l'est aussi, d'où $N(D_K) \subset D_k$. *Il s'ensuit*, d'une part, *que* $D_k=N(D_K)$, *et*, d'autre part, *que* $D_K \cap C_k$ *est le produit direct de* D_k *et de* $\gamma_{k,K}$. Donc l'homomorphisme canonique de C_k sur C'_k induit sur $\gamma_{k,K}$ un isomorphisme de $\gamma_{k,K}$ sur son image dans C'_k, et celle-ci est l'image de $D_K \cap C_k$ dans C'_k, c'est-à-dire le noyau de la représentation canonique de C'_k dans C'_K.

IV. Transformation du problème.

Dans tout ce qui suit, chaque fois qu'on a à considérer un couple de corps K, k, où K est galoisien sur k, les groupes attachés à K, et en particulier C_K et $C'_K=G'_K$, doivent être considérés comme munis de leur structure de groupes à opérateurs sur $\mathfrak{g}(K/k)$.

Pour simplifier les notations, on identifiera toujours C_K avec son image $f(C_K)$ dans le groupe $G_{K,k}$ qu'on se propose de définir, au moyen de l'isomorphisme qu'on a noté f. Dans ces conditions, $G_{K,k}$ devient une extension de C_K par $\mathfrak{g}(K/k)$; et on a à définir, en même temps que $G_{K,k}$, un homomorphisme φ de $G_{K,k}$ sur $G'_{K,k}$, de noyau D_K. Le transfert réduit de $G_{K,k}$ dans C_K est alors en tout cas une représentation de $G^a_{K,k}$ dans le groupe C_k des éléments de C_K invariants par $\mathfrak{g}(K/k)$; ce doit être un

isomorphisme de $G^a_{K,k}$ sur C_k (condition (A)). Si $k \subset k' \subset K$, et si $G_{K,k'}$ et φ' sont le groupe et l'homomorphisme attachés à K, k', il doit exister un isomorphisme ω de $G_{K,k'}$ sur l'image réciproque $\varphi^{-1}(G'_{K,k'})$, dans $G_{K,k}$, du sous-groupe $G'_{K,k'}$ de $G'_{K,k}$, induisant sur C_K l'automorphisme identique, et tel que $\varphi' = \varphi \circ \omega$ (condition (B)). Si $k \subset K \subset K'$, K' étant galoisien sur k, soient $G_{K',k}$ et φ'' le groupe et l'homomorphisme attachés à K', k; soit $H = \varphi''^{-1}(G'_{K',K})$; soit λ l'homomorphisme canonique de $G_{K',k}$ sur $G_{K',k}/H^c$; soit λ' l'homomorphisme canonique de $G'_{K',k}/G'^c_{K',K}$. Au moyen de l'isomorphisme qui existe entre H et $G_{K',K}$ en vertu de (B), et par application de (A) à $G_{K',K}$, on voit que le transfert réduit de H dans $C_{K'}$ détermine un isomorphisme τ de $H^a = H/H^c$ sur C_K. Il doit alors exister un isomorphisme η de $G_{K',k}/H^c$ sur $G_{K,k}$, coïncidant avec τ sur H/H^c, et tel que l'on ait $\varphi \circ \eta \circ \lambda = \lambda' \circ \varphi''$ (condition (C)). Enfin, la condition (D) doit être satisfaite.

Pour abréger, écrivons de nouveau $\mathfrak{g}$ au lieu de $\mathfrak{g}(K/k)$. Soit $s' = (s'_\alpha)$ un système de représentants dans $G'_{K,k}$ des éléments α de $\mathfrak{g} = G'_{K,k}/C'_K$; soit $a'_{\alpha,\beta} = s'^{-1}_{\alpha\beta} s'_\alpha s'_\beta$; $a' = (a'_{\alpha,\beta})$ est un système de facteurs, ou en d'autres termes un cocycle de dimension 2, de $\mathfrak{g}$ dans C'_K. Supposons construits $G_{K,k}$ et φ ; pour chaque α, soit s_α un élément de $\varphi^{-1}(s'_\alpha)$; soit $a_{\alpha,\beta} = s^{-1}_{\alpha\beta} s_\alpha s_\beta$; $a = (a_{\alpha,\beta})$ est un système de facteurs de $\mathfrak{g}$ dans C_K, qui se réduit à a' modulo D_K. Les s'_α étant donnés, tout autre choix des s_α revient à remplacer ceux-ci par des éléments $s_\alpha x_\alpha$, avec $x_\alpha \in D_K$; en notant ∂x le " cobord " de la " cochaîne " (de dimension 1) $x = (x_\alpha)$, on voit que a est alors remplacé par $a(\partial x)$. A tout choix des s'_α se trouve ainsi attaché un ensemble $F(s')$ de cocycles a de $\mathfrak{g}$ dans C_K, ne différant les uns des autres que par des cobords de cochaînes de $\mathfrak{g}$ dans D_K. Si on change le choix des s'_α, ceux-ci seront remplacés par des éléments $s'_\alpha u'_\alpha$, où les u'_α sont des éléments quelconques de C'_K, donc des images dans C'_K d'éléments u_α de C_K, et alors $F(s')$ doit être remplacé par $F(s') \cdot (\partial u)$; on a donc $F(s'u') = F(s') \cdot (\partial u)$.

Réciproquement, s' et a' étant comme ci-dessus, soit a un système de facteurs de $\mathfrak{g}$ dans C_K, se réduisant à a' modulo D_K; construisons l'extension G de C_K par $\mathfrak{g}$ déterminée par le système de facteurs a ; ce sera un groupe engendré par C_K et des représentants s_α des éléments de $\mathfrak{g}$, avec la loi de multiplication $(s_\alpha u)(s_\beta v) = s_{\alpha\beta} a_{\alpha,\beta} u^\beta v$ pour $u \in C_K$, $v \in C_K$; il est immédiat qu' alors on définit un homomorphisme φ de G sur $G'_{K,k}$ en posant $\varphi(s_\alpha) = s'_\alpha$ et en convenant que φ induit sur C_K l'homomorphisme canonique de C_K

sur C'_K. Soit $F(s')$ l'ensemble des systèmes de facteurs qui se déduisent de a par multiplication par le cobord d'une cochaîne de $\mathfrak{g}$ dans D_K ; d'après ce qui précède, le fait de remplacer a par un autre système de facteurs appartenant à $F(s')$ équivaut à changer les représentants s_α des s'_α dans G, et fournit essentiellement le même groupe G et le même homomorphisme φ. Si u est une cochaîne de $\mathfrak{g}$ dans C_K, et u' son image dans C'_K, on obtiendra encore le même groupe G et le même homorphisme φ au moyen du système de représentants $(s'u')$ et d'un système de facteurs appartenant à l'ensemble $F(s')\cdot(\partial u)$.

On conviendra de désigner par $F_{K,k}(s')$ l'ensemble $F(s')$ des systèmes de facteurs de $\mathfrak{g}$ dans C_K relatif au système de représentants $s'=(s'_\alpha)$, et au groupe $G_{K,k}$ et à l'homomorphisme φ que l'on se propose de construire. On aura, avec les notations ci-dessus, $F_{K,k}(s'u')=F_{K,k}(s')\cdot(\partial u)$.

Supposons le groupe $G_{K,k}$ ainsi construit au moyen d'un système de facteurs $a\in F_{K,k}(s')$; soient s_α les représentants correspondants des s'_α dans $G_{K,k}$; soit t le transfert de $G_{K,k}$ dans C_K. Pour $u\in C_K$, on aura $t(s_\alpha u)=\prod_\beta a_{\alpha,\beta}\,N(u)$. En vertu de la condition (D), l'image de $t(s_\alpha u)$ dans $G'_k=C'_k$ doit déterminer sur A_k le même automorphisme qui est induit sur A_k par l'automorphisme de A_K déterminé par l'élément $s'_\alpha u'=\varphi(s_\alpha u)$ de $G'_{K,k}$. Comme G'_k est abélien, il suffit d'écrire cette condition, d'une part pour s_α, et d'autre part pour u ; mais pour u elle n'est autre que le " théorème de translation " de la théorie du corps de classes. La condition (D) peut donc être remplacée par la condition suivante :

(D′) Pour $a\in F_{K,k}(s')$, l'automorphisme induit sur A_k par l'automorphisme s'_α de A_K doit être celui qui est déterminé par l'image dans C'_k de l'élément $\prod_{\beta\in\mathfrak{g}} a_{\alpha,\beta}$ de C_k.

Soit maintenant $\mathfrak{g}'$ un sous-groupe de $\mathfrak{g}$; soit k' le corps intermédiaire entre k et K qui correspond à $\mathfrak{g}'$. Si on tient compte de (B), la condition (D′), appliquée à K et k', donne ce qui suit :

(D″) Si $a\in\mathfrak{g}'$, l'automorphisme induit par s'_α sur $A_{k'}$ est celui qui est déterminé par l'image dans $C'_{k'}$ de l'élément $\prod_{\beta\in\mathfrak{g}'} a_{\alpha,\beta}$ de $C_{k'}$.

Soit de plus R un système de représentants dans $\mathfrak{g}$ des classes à droite suivant $\mathfrak{g}'$; tout élément de $\mathfrak{g}$ se met donc, d'une manière et d'une seule, sous la forme $a\rho$, avec $a\in\mathfrak{g}'$, $\rho\in R$. Comme a est un système de facteurs, on a $a_{\alpha,\beta\rho}=a_{\alpha,\beta}^{\rho}a_{\alpha\beta,\rho}a_{\beta,\rho}^{-1}$, donc, pour $a\in\mathfrak{g}'$:

$$\prod_{\lambda\in\mathfrak{g}} a_{\alpha,\lambda} = \prod_{\beta\in\mathfrak{g}'} \prod_{\rho\in K} a_{\alpha,\beta\rho} = N_{k'/k}\left(\prod_{\beta\in\mathfrak{g}'} a_{\alpha,\beta}\right) \qquad \text{(N)}.$$

De là, et du théorème de translation de la théorie du corps de classes, il résulte immédiatement que, si (D″) est satisfaite pour un $\alpha\in\mathfrak{g}'$, (D′) l'est aussi pour ce même élément α. Donc, pour que (D′) soit satisfaite pour un élément α, il suffit que (D″) le soit pour α et pour le groupe cyclique $\mathfrak{g}'$ engendré par α. Autrement dit, pour que (D) soit satisfaite pour K et k, il suffit que la condition suivante le soit :

(E) Quel que soit $\alpha\in\mathfrak{g}$, soient $\mathfrak{g}_\alpha$ le groupe cyclique engendré par α, et k_α le corps correspondant ; alors l'automorphisme induit par s'_α sur A_{k_α} doit être celui qui est déterminé par l'image dans C'_{k_α} de l'élément $\prod_{\beta\in\mathfrak{g}_\alpha} a_{\alpha,\beta}$ de C_{k_α}.

Réciproquement, d'après ce qui précède, si (E) et (B) sont satisfaites, (D) le sera pour tous les couples K, k', où k' est l'un quelconque des corps intermédiaires entre K et k.

On va donc examiner de plus près le cas des extensions cycliques. Supposons $\mathfrak{g}$ engendré par un élément σ d'ordre n. On sait qu'on peut alors " normaliser " tout système de facteurs $x=(x_{\alpha,\beta})$ de $\mathfrak{g}$ dans un groupe G en normalisant le système correspondant $s=(s_\alpha)$ de représentants de $\mathfrak{g}$, dans l'extension de G par $\mathfrak{g}$ déterminée par x, par la condition $s_{\sigma\mu}=s_\sigma{}^\mu$ pour $0\leq\mu\leq n-1$. Alors, si on pose $s_\sigma{}^n=\bar{x}$, $\bar{x}$ est un élément de G invariant par $\mathfrak{g}$; et, pour $0\leq\mu\leq n-1$, $0\leq\nu\leq n-1$, on a $x_{\sigma_\mu,\sigma_\nu}=1$ ou $\bar{x}$ suivant que $\mu+\nu\leq n-1$ ou $\mu+\nu\geq n$. Pour que x soit trivial, il faut et il suffit que $\bar{x}$ soit une norme. On conviendra d'identifier le système de facteurs normalisé x avec l'élément $\bar{x}$.

On a d'ailleurs ici $k\subset K\subset A_k\subset A_K$; et on sait ([5a]) que l'image réciproque dans C_k du sous-groupe de $G'_k=C'_k$ qui correspond à K n'est autre que $N(C_K)$; on peut donc identifier canoniquement $\mathfrak{g}$ avec $C_k/N(C_K)$. Soit a un élément de C_k dont l'image dans $\mathfrak{g}=C_k/N(C_K)$ soit σ ; soit a' son image dans C'_k ; soit s'_σ un élément de $G'_{K,k}$ ayant a' pour image dans $C'_k=G'_k=G'_{K,k}/G'^c_{K,k}$. Soit a^* l'élément représentatif d'un système de facteurs normalisé de $\mathfrak{g}$ dans C_K qui se réduise à a' modulo D_K ; a^* est un élément de C_K invariant par $\mathfrak{g}$, donc est dans C_k ; alors a^*a^{-1} est dans $D_K\cap C_k$; d'après le § III, a^* est donc de la forme $a^*=abz$, avec $b\in\gamma_{k,K}$, $z\in D_k$.

Soit $\mathfrak{g}'$ un sous-groupe de $\mathfrak{g}$, engendré par σ^d, où d est un diviseur

de n; soit k' le corps correspondant. Supposons le système de représentants s' de $\mathfrak{g}$ dans $G'_{K,k}$ normalisé par $s'_{\sigma\mu}=s'^{\mu}_{\sigma}$ pour $0\leq\mu\leq n-1$; et, pour simplifier, notons aussi s' le système de représentants de $\mathfrak{g}'$ dans $G'_{K,k'}$ formé par les $s'^{d\nu}_{\sigma}$ pour $0\leq\nu<n/d$. Alors la condition (B) appliquée à k, k' et K montre que, si a^* est l'élément représentatif d'un système de facteurs normalisé appartenant à l'ensemble $F_{K,k}(s')$, c'est aussi l'élément représentatif d'un système normalisé appartenant à $F_{K,k'}(s')$. D'autre part, le transfert de s'_{σ} dans $G'_{K,k'}$ est l'image de s'^{d}_{σ} dans $G'_{K,k'}/G'^{e}_{K,k'}$; comme nous savons que ces groupes satisfont à (C), il s'ensuit que cette dernière image, c'est-à-dire l'automorphisme de $A_{k'}$ induit par s'^{d}_{σ}, est l'image dans $C'_{k'}$ de l'élément a de $C_k\subset C_{k'}$. Dans ces conditions, on vérifie aussitôt que (D'') sera satisfaite pour K et k' si l'image de a^*a^{-1} dans $C'_{k'}$ est 1, et réciproquement; cela équivaut à dire que $a^*a^{-1}=bz$ doit être dans $D_{k'}\cap C_k=\gamma_{k,k'}D_k$, ou encore que b doit être dans $\gamma_{k,k'}$. Pour $k'=k$, cette condition se réduit à $b=1$.

Soit v une valuation réelle de k qui se ramifie dans K, s'il en existe; soit w l'une des valuations de K qui la prolongent; prenons pour $\mathfrak{g}'$ le sous-groupe de $\mathfrak{g}$ qui laisse w invariante; comme $\mathfrak{g}'$ doit être d'ordre 2, n est alors pair, et on a $\mathfrak{g}'=\{e,\sigma^{n/2}\}$. Puisque w est invariante par $\mathfrak{g}'=\mathfrak{g}(K/k')$, w induit sur k' une valuation réelle; il n'y a donc pas de valuation réelle de k qui se ramifie dans k', et on a $\gamma_{k,k'}=\{1\}$. Si donc (D'') est satisfaite pour K et k', (D') est satisfaite pour K et k, et réciproquement. Si d'autre part il n'y a pas de valuation réelle de k qui se ramifie dans K, et en particulier si n est impair, on a $\gamma_{k,K}=\{1\}$; en ce cas (D') est vérifiée d'elle-même pour K et k, et (D'') l'est pour K et tout corps k' intermédiaire entre K et k.

Revenons au cas d'une extension galoisienne quelconque K de k. Comme on l'a vu, compte tenu de (B), il faut et il suffit, pour que (D) soit satisfaite pour K et tout corps intermédiaire entre K et k, que (D'') le soit pour tout sous-groupe cyclique de $\mathfrak{g}$, ou, ce qui revient au même, que (E) le soit; et de plus notre étude des extensions cycliques nous a montré qu'il en sera ainsi pourvu que (D'') le soit pour les sous-groupes d'ordre 2, c'est-à-dire que (E) le soit pour les éléments d'ordre 2.

Pour appliquer cette condition, nous supposerons désormais tout système de facteurs $x=(x_{\alpha,\beta})$ de $\mathfrak{g}$ dans un groupe G normalisé par la condition que $x_{\varepsilon,\alpha}=x_{\alpha,\varepsilon}=1$ quel que soit α; cela revient, comme on sait, à normaliser le système correspondant $s=(s_\alpha)$ de représentants de $\mathfrak{g}$, dans l'extension de

G par $\mathfrak{g}$ déterminée par x, par la condition que s_ε soit l'élément neutre de cette extension. Sur un groupe à deux éléments, cette normalisation coïncide avec celle qui résulte des conventions faites ci-dessus pour les groupes cycliques. Cela étant entendu une fois pour toutes, on voit qu'au lieu de (E) il suffit de s'imposer la condition suivante :

(F) Quel que soit l'élément σ d'ordre 2 dans $\mathfrak{g}$, soit k_σ le corps correspondant au sous-groupe $\{\varepsilon, \sigma\}$ de $\mathfrak{g}$; alors l'automorphisme induit sur A_{k_σ} par s'_σ doit être celui qui est déterminé par l'image dans C'_{k_σ} de l'élément $a_{\sigma,\sigma}$ de C_{k_σ}.

V. Solution du problème.

Avec les mêmes notations que plus haut, nous allons montrer maintenant, en premier lieu, qu'il existe un système de facteurs $a=(a_{\alpha,\beta})$ de $\mathfrak{g}$ dans C_K qui se réduit à a' modulo D_K et qui satisfait à (F), et que ces conditions déterminent a au cobord près d'une cochaîne de $\mathfrak{g}$ dans D_K. L'ensemble des systèmes de facteurs qui y satisfont étant désigné par $F_{K,k}(s')$, les groupes $G_{K,k}$ et les homomorphismes φ déterminés par les $F_{K,k}(s')$ satisfont trivialement à (B) ; nous ferons voir qu'ils satisfont aussi à (A) et à (C).

Pour cela, soient $a^*_{\alpha,\beta}$ des éléments de C_K se réduisant respectivement aux $a'_{\alpha,\beta}$ modulo D_K ; comme $\partial a'=1$, ∂a^* est une cochaîne de dimension 3 de $\mathfrak{g}$ dans D_K ; c'est évidemment un cocycle ; d'après le § III, celui-ci est trivial dans D_K, c'est-à-dire de la forme ∂z, où z est une cochaîne de $\mathfrak{g}$ dans D_K, et par suite a^*z^{-1} est un cocycle. Autrement dit, en remplaçant a^* par a^*z^{-1}, on a le droit de supposer que a^* lui-même est un cocycle. Supposons le problème résolu ; soit $a\in F_{K,k}(s')$; on a $a=a^*b$, où b est un cocycle de $\mathfrak{g}$ dans D_K qu'il s'agit de déterminer, ou plus exactement dont il s'agit de déterminer la classe d'homologie, puisque a n'est déterminé qu'à un cocycle trivial près de $\mathfrak{g}$ dans D_K. Autrement dit, il s'agit de déterminer un $a\in F_{K,k}(s')$ parmi les cocycles a^*b quand on fait parcourir à b un système complet de représentants des classes de cohomologie de $\mathfrak{g}$ dans D_K. Un tel système a été déterminé au § III ; il se compose des images dans D'_K des cocycles $\prod_i b_i^{f_i}$, où b_i est un cocycle non trivial de $\mathfrak{g}$ dans le " tore de seconde sorte " θ_i, et où $f_i=0$ ou 1, pour $1\leq i\leq r_0$.

Soit maintenant σ un élément d'ordre 2 de $\mathfrak{g}$; soit a'_σ l'automorphisme de A_{k_σ} induit par s'_σ ; soit a_σ un élément de C_{k_σ} ayant a'_σ pour image dans

C'_{k_σ}. Le transfert de s'_σ de G'_{K,k_σ} dans C'_K est $a'_{\sigma,\sigma}$; en vertu de (A) appliquée à G'_{K,k_σ}, $a'_{\sigma,\sigma}$ est donc l'image de a'_σ par la représentation canonique de C'_{k_σ} dans C'_K. Autrement dit, $a^*_{\sigma,\sigma}$ et a_σ ont même image dans C'_K, c'est-à-dire que, si on pose $a_\sigma a^{*-1}_{\sigma,\sigma}=d_\sigma$, on a $d_\sigma \in D_K$. Comme d'ailleurs a^* est un système de facteurs normalisé, on a $a^{*\sigma}_{\sigma,\sigma}=a^*_{\sigma,\sigma}$, donc $a^*_{\sigma,\sigma}\in C_{k_\sigma}$, d'où, puisque $a_\sigma \in C_{k_\sigma}$, $d_\sigma \in D_K \cap C_{k_\sigma}$.

Soient de plus α quelconque dans $\mathfrak{g}$, et $\tau=\alpha^{-1}\sigma\alpha$; τ est aussi d'ordre 2 ; le cas $\tau=\sigma$ n'est pas exclu. On a, dans ces conditions, $\alpha\tau=\sigma\alpha$, $s'_\sigma s'_\alpha = s'_{\sigma\alpha}a'_{\sigma,\alpha}$, $s'_\alpha s'_\tau = s'_{\alpha\tau}a'_{\alpha,\tau}$, d'où :

$$s'_\tau = (s'^{-1}_\alpha s'_\sigma s'_\alpha)\, a'_{\alpha,\tau}\, a'^{-1}_{\sigma,\alpha}.$$

Mais, d'après la théorie du corps de classes, l'automorphisme de A_{k_τ} induit par $s'^{-1}_\alpha s'_\sigma s'_\alpha$ est l'image de a^α_σ dans C'_{k_τ} ; au moyen du théorème de translation, il s'ensuit que a_τ a même image dans C'_{k_τ} que $a_\sigma{}^\alpha N_{K/k_\tau}(a^*_{\alpha,\tau}a^{*-1}_{\sigma,\alpha})$, ou autrement dit n'en diffère que par un facteur $z\in D_{k_\tau}$.

D'autre part, comme a^* est un système de facteurs normalisé, on a $a^{*\alpha}_{\sigma,\sigma}=a^*_{\sigma,\sigma\alpha}a^*_{\sigma,\alpha}$, $a^{*\tau}_{\alpha,\tau}a^*_{\alpha\tau,\tau}=a^*_{\tau,\tau}$, $a^{*\tau}_{\sigma,\alpha}a^*_{\sigma\alpha,\tau}=a^*_{\sigma,\alpha\tau}a^*_{\alpha,\tau}$. En tenant compte de $\alpha\tau=\sigma\alpha$, on en tire $a^*_{\tau,\tau}=a^{*\alpha}_{\sigma,\sigma}N_{K/k_\tau}(a^*_{\alpha,\tau}a^{*-1}_{\sigma,\alpha})$. Par suite, on a $d_\tau=d_\sigma{}^\alpha z$, avec $z\in D_{k_\tau}$. Comme d'ailleurs d_σ est dans C_{k_σ}, c'est-à-dire est invariant par σ, $d_\sigma{}^\alpha$ est invariant par τ, donc est dans C_{k_τ} ; donc d_τ et $d_\sigma{}^\alpha$ sont tous deux dans $D_K\cap C_{k_\tau}$, qui est (§ III) le produit direct de D_{k_τ} et de $\gamma_{k_\tau,K}$; comme ils ne diffèrent que par le facteur z, ils ont donc même composante dans $\gamma_{k_\tau,K}$. Autrement dit, si on pose $d_\sigma=\xi_\sigma u_\sigma$, avec $\xi_\sigma\in\gamma_{k_\sigma,K}$, $u_\sigma\in D_{k_\sigma}$, on a $\xi_\tau=\xi^\alpha_\sigma$.

Cela posé, soit $a=a^*b$. Pour que a satisfasse à (F), il faut et il suffit que, pour tout σ d'ordre 2, $a_{\sigma,\sigma}a_\sigma{}^{-1}$ soit dans D_{k_σ}, ou autrement dit que l'on ait $a^*_{\sigma,\sigma}b_{\sigma,\sigma}a_\sigma{}^{-1}\in D_{k_\sigma}$, ou encore $b_{\sigma,\sigma}\in\xi_\sigma D_{k_\sigma}$.

Posons $b_{i\sigma}=(b_i)_{\sigma,\sigma}$; c'est un idèle de I_K, invariant par σ puisque les systèmes de facteurs b_i sont supposés normalisés. Par suite, $b_{i\sigma}$ est un idèle de I_{k_σ}, dont toutes les composantes relatives aux valuations discrètes de k_σ ont la valeur 1, et qu'on peut donc mettre sous la forme $b'_{i\sigma}b''_{i\sigma}$ avec $b'_{i\sigma}\in\Gamma_{k_\sigma}$, $b''_{i\sigma}\in H'_{k_\sigma}$; posons $b'_\sigma=\prod_i b'^{f_i}_{i\sigma}$, $b''_\sigma=\prod_i b''^{f_i}_{i\sigma}$. Alors $b_{\sigma,\sigma}$ est le produit des images de b'_σ et de b''_σ dans C_{k_σ} ; la première est dans γ_{k_σ}, la seconde

dans D_{k_σ}. Si donc on désigne par Ξ_σ l'élément de I'_{k_σ} qui a pour image ξ_σ dans γ_{k_σ}, on voit que la condition $b_{\sigma,\sigma} \in \xi_\sigma D_{k_\sigma}$ équivaut à $b'_\sigma = \Xi_\sigma$. Donc, pour toute valuation réelle de k_σ, b'_σ et Ξ_σ doivent avoir la même composante, cette composante ne pouvant être que ± 1. D'ailleurs, comme l'image ξ_σ de Ξ_σ dans γ_{k_σ} est dans $\gamma_{k_\sigma,K}$, les composantes de Ξ_σ relatives aux valuations réelles de k_σ non ramifiées dans K ont la valeur 1 ; et il en est de même de $b_{i\sigma}$, qui, considéré comme élément de I_K, est dans θ_i, donc a toutes ses composantes égales à 1 à l'exception de celles relatives aux valuations, toutes complexes, de K qui prolongent la valuation réelle v_i de k. Il s'ensuit que notre problème consiste à déterminer les f_i de telle sorte que, pour chaque σ, les composantes de b'_σ relatives aux valuations réelles de k_σ qui se ramifient dans K soient respectivement égales aux composantes correspondantes de Ξ_σ.

Pour chaque i, choisissons, parmi les valuations de K qui prolongent v_i, une valuation w_i ; les autres sont alors les valuations w_i^α, avec $\alpha \in \mathfrak{g}$. Soit σ_i l'élément d'ordre 2 de $\mathfrak{g}$ qui laisse w_i invariante ; on a $w_i^{\sigma_i \alpha} = w_i^\alpha$, de sorte qu'il n'y a bien que $n/2$ valuations w_i^α distinctes. Toute valuation réelle de k_σ qui se ramifie dans K induit sur k l'une des valuations v_i, et la valuation de K qui la prolonge est alors de la forme w_i^α ; comme celle-ci doit être invariante par σ, on a donc alors $\sigma = \alpha^{-1}\sigma_i\alpha$. Nous avons donc à exprimer que, pour chaque i et chaque $\alpha \in \mathfrak{g}$, les idèles $\prod_j b'^{f_j}_{j\sigma}$ et Ξ_σ, où l'on a pris $\sigma = \alpha^{-1}\sigma_i\alpha$, ont même composante relative à la valuation induite sur k_σ par w_i^α. Mais, pour $j \neq i$, $b_{j\sigma}$, donc aussi $b'_{j\sigma}$, a la composante 1 pour cette valuation ; d'autre part, pour cette valuation, qui est réelle sur k_σ, tout élément de H'_{k_σ}, donc en particulier $b''_{i\sigma}$, a la composante 1 ; enfin, il résulte d'un théorème déjà cité (v.[4]) que, pour cette valuation, $b_{i\sigma}$ a la composante -1, car dans le cas contraire le système de facteurs b_i serait trivial dans θ_i. En définitive, on a donc à déterminer les f_i par la condition que la composante de Ξ_σ relative à la valuation induite par w_i^α sur k_σ soit égale à $(-1)^{f_i}$. Mais, d'après ce qu'on a démontré plus haut, on a $\xi_\sigma = \xi_{\sigma_i}^\alpha$, d'où $\Xi_\sigma = \Xi_{\sigma_i}^\alpha$. Autrement dit, la composante de Ξ_σ relative à w_i^α est égale à la composante de Ξ_{σ_i} relative à w_i ; cette dernière doit donc être égale à $(-1)^{f_i}$, et, si on prend les f_i tels qu'il en soit ainsi, ils fournissent une solution du problème. Cela achève la première partie de notre démonstration.

On désignera donc par $G_{K,k}$ et φ le groupe et l'homomorphisme déterminés par l'ensemble de sytèmes de facteurs $F_{K,k}(s')$ qu'on vient de

construire ; ils satisfont à (D) par construction, et, comme on l'a déjà observé, ils satisfont trivialement à (B) ; pour $k \subset k' \subset K$, on identifiera donc dorénavant $G_{K,k'}$ avec son image dans $G_{K,k}$ par l'isomorphisme ω dont il a été question au début du § IV.

En particulier, s'il s'agit d'une extension cyclique, on a déjà déterminé au § IV un système de facteurs normalisé satisfaisant à la condition (D''), et qui par suite appartient à $F_{K,k}(s')$; c'est donc là un système de facteurs qui permet de définir $G_{K,k}$ dans ce cas.

On va montrer maintenant que $G_{K,k}$ est produit direct d'un groupe isomorphe à R et d'un groupe compact. On a vu en effet qu'il en est ainsi de C_K, et on a défini au § I un homomorphisme d de C_K sur R, ayant pour noyau le sous-groupe compact maximal C_K^0 de C_K ; la définition de d montre que d est invariant par tout automorphisme de K, de sorte que $\mathfrak{g}$ induit sur C_K/C_K^0 l'automorphisme identique. En se servant du fait que le groupe des représentations de R dans C_K^0 (et plus généralement dans tout groupe abélien) a la propriété d'unique divisibilité, on vérifie alors aisément qu'on peut écrire C_K comme produit direct $X \times C_K^0$, où X est isomorphe à R et a tous ses éléments invariants par $\mathfrak{g}$; il est clair que $X \subset D_K$. Soit $a=(a_{\alpha,\beta}) \in F_{K,k}(s')$; alors les $d(a_{\alpha,\beta})$ forment un système de facteurs de $\mathfrak{g}$ dans R, nécessairement trivial, donc de la forme ∂b, où b est une cochaîne de $\mathfrak{g}$ dans C_K/C_K^0 ; en identifiant ce dernier groupe avec X, b devient une cochaîne de $\mathfrak{g}$ dans $X \subset D_K$; on voit donc qu'en remplaçant a par $a(\partial b^{-1})$, on peut supposer que a est un systéme de facteurs de $\mathfrak{g}$ dans C_K^0. Il est immédiat qu'alors $G_{K,k}$ est le produit direct de X et de l'extension de C_K^0 par $\mathfrak{g}$ déterminée par ce systéme. Il s'ensuit en particulier que $G_{K,k}^c$, adhérence du groupe engendré par les commutateurs de $G_{K,k}$ est compact ; et $G_{K,k}^a$ est produit direct d'un groupe isomorphe à R et d'un groupe compact.

Passons à la vérification de (A). Soit t le transfert de $G_{K,k}$ dans C_K ; nous devons faire voir d'abord que t applique $G_{K,k}$ sur C_k. Nous savons déjà que $t(G_{K,k}) \subset C_k$, et que $t(G_{K,k}) \supset t(C_K) = N(C_K)$. Si K' est une extension cyclique, alors, d'après la détermination explicite de $F_{K,k}(s')$ donnée pour ce cas, nous savons qu'il y a dans $G_{K,k}$ un représentant s_σ du générateur σ de $\mathfrak{g}$ tel que $s_\sigma^n = a$, où a est dans C_K et tel que son image dans $\mathfrak{g} = C_k/N(C_K)$ soit σ ; comme on a en ce cas $t(s_\sigma) = s_\sigma^n$, on a donc bien $t(G_{K,k}) = C_k$. Passons au cas général ; posons $T = t(G_{k,k})$, et soit T' l'image de T dans C_k'. Comme $G_{K,k}'$ satisfait à (A), l'image de T' dans C_K' par

la représentation canonique de C'_k dans C'_K n'est autre que celle de C'_k ; il revient au même de dire que $TD_k\gamma_{k,K}=C_k$. Comme $D_k=N(D_K)\subset T$, il nous reste donc seulement à montrer que $T\supset\gamma_{k,K}$. Pour cela, v_i, w_i, σ_i ayant le même sens que précédemment, soit de nouveau $\bar{a}_i=(a_v)$ l'idèle de I_k tel que $a_{v_i}=-1$ et $a_v=1$ pour $v\neq v_i$. Posons $k_i=k_{\sigma_i}$; soit $\bar{c}_i=(c_w)$ l'idèle de I_K tel que $c_{w_i}=-1$ et $c_w=1$ pour $w\neq w_i$; $\bar{c}_i$ est invariant par σ_i, et est donc dans I_{k_i}. Le groupe $\gamma_{k,K}$ est engendré par les images a_i des $\bar{a}_i$ dans C_k. Comme notre résultat est vrai pour les extensions quadratiques, il l'est pour K et k_i, et il y a donc un élément s_i de G_{K,k_i} dont l'image, par le transfert de G_{K,k_i} dans C_K, soit l'image c_i de $\bar{c}_i$ dans C_{k_i}. La formule (N) du § IV donne alors $t(s_i)=N_{k_i/k}(c_i)=a_i$, ce qui achève la démonstration.

Montrons maintenant que le noyau de t est $G^c_{K,k}$. Comme $G'_{K,k}$ satisfait à (A), le transfert réduit de $G'_{K,k}$ dans C'_K n'est autre que la représentation canonique de $C'_k=G'^a_{K,k}$ dans C'_K et a donc pour noyau l'image γ' de $\gamma_{k,K}$ dans C'_k ; le transfert t' de $G'_{K,k}$ dans C'_K a donc pour noyau l'image réciproque N' de γ' dans $G'_{K,k}$; comme t' se déduit de t par passage au quotient, le noyau de t est donc contenu dans l'image réciproque N de N' dans $G_{K,k}$. Le groupe N' admet $G'^c_{K,k}$ comme sous-groupe d'indice égal à l'ordre de γ', c'est-à-dire à 2^{r_0}. D'autre part, comme l'adhérence $G^c_{K,k}$ du groupe des commutateurs de $G_{K,k}$ est compacte, son image dans $G'_{K,k}$ l'set aussi et est donc l'adhérence $G'^c_{K,k}$ du groupe des commutateurs de $G'_{K,k}$; et $G^c_{K,k}D_K$ est un sous-groupe fermé de $G_{K,k}$, image réciproque de $G'^c_{K,k}$ dans $G_{K,k}$. Il s'ensuit que N admet $G^c_{K,k}D_K$ comme sous-groupe d'indice 2^{r_0}. Soient de nouveau les s_i les éléments introduits tout à l'heure, tels que $t(s_i)=a_i$; comme $a_i\in\gamma_{k,K}$, l'image de a_i dans C'_K est 1, donc, si s'_i est l'image de s_i dans $G'_{K,k}$, on a $t'(s'_i)=1$, c'est-à-dire $s'_i\in N'$, d'où $s_i\in N$. Si d'autre part les e_i sont des entiers tels que $\Pi_i s_i^{e_i}\in G^c_{K,k}D_K$, on a $t(\Pi_i s_i^{e_i})\in t(D_K)$ c'est-à-dire $\Pi_i a_i^{e_i}\in N(D_K)=D_k$, donc $\Pi_i a_i^{e_i}=1$ puisque $\gamma_{k,K}\cap D_k=\{1\}$, et par suite $e_i\equiv 0$ mod. 2 quel que soit i. On voit donc que les 2^{r_0} éléments $\Pi_i s_i^{e_i}$ de N qu'on obtient en prenant les e_i égaux à 0 ou 1 sont tous distincts modulo $G^c_{K,k}D_K$, et forment par suite un système complet de représentants des classes suivant ce groupe dans N.

Tout élément z de N est donc de la forme $z=xy\Pi_i s_i^{e_i}$, avec $x\in G^c_{K,k}$, $y\in D_K$, et $e_i=0$ ou 1 pour $1\leq i\leq r_0$; on a alors $t(z)=N(y)\Pi_i a_i^{e_i}$. Sup-

posons qu'on ait $t(z)=1$; alors on a $\prod_i a_i^{e_i} \in N(D_K)$, donc, comme plus haut, $e_i=0$ quel que soit i, et $N(y)=1$. Le noyau de t est donc l'ensemble des $z=xy$, où $x \in G^c_{K,k}$, $y \in D_K$, et $N(y)=1$; et il reste à montrer qu'alors $y \in G^c_{K,k}$. D'ailleurs, si $w \in C_K$, on a $s_\alpha^{-1} w^{-1} s_\alpha w = w^{1-\alpha} \in G^c_{K,k}$, et il suffit de faire voir que y est dans le groupe engendré par les $w^{1-\alpha}$. Comme D_K/D'_K a la propriété d'unique divisibilité, on a $y=w^n u$, avec $w \in D_K$, $u \in D'_K$, et comme toujours $n=[K:k]$. On a alors $N(w)^n = N(u^{-1}) \in D'_K$, donc, d'après la propriété d'unique divisibilité, $N(w) \in D'_K$. En posant $u_1 = N(w)u$, on aura alors $y = (\prod_\alpha w^{1-\alpha}) u_1$, $u_1 \in D'_K$, $N(u_1)=1$. Il suffit donc de montrer que u_1 est alors dans le groupe engendré par les $v^{1-\alpha}$ avec $v \in D'_K$, $\alpha \in \mathfrak{g}$; et, comme D'_K est produit direct des tores de première et seconde sorte définis au § III, tout revient à démontrer que chacun de ces tores possède la propriété en question, ce qui ne fait pas de difficulté[5]. Le noyau de t est donc bien $G^c_{K,k}$, c'est-à-dire que le transfert réduit $\bar{t}$ de $G_{K,k}$ dans C_K est une représentation biunivoque de $G^a_{K,k}$ sur C_k. Comme d'ailleurs chacun de ces derniers groupes est produit direct d'un groupe isomorphe à R et d'un groupe compact, il est facile, soit en examinant plus attentivement la nature de la représentation $\bar{t}$, soit par application de théorèmes généraux sur la représentation des groupes abéliens (cf. [13], chap. VI) de conclure que $\bar{t}$ est un isomorphisme, ce qui complète la vérification de (A).

Passons à (C) ; soit K' une extension de K, galoisienne sur k ; il s'agit de définir un isomorphisme η de $\Gamma = G_{K',k}/G^c_{K',K}$ sur $G_{K,k}$, ayant les propriétés indiquées au début du § IV. Le groupe Γ admet $G^a_{K',K} = G_{K',K}/G^c_{K',K}$ comme sous-groupe invariant fermé, le groupe quotient étant $G_{K',k}/G_{K',K} = \mathfrak{g}(K/k)$; en vertu de (A), le transfert réduit $\bar{t}$ de $G_{K',K}$ dans $C_{K'}$ est un isomorphisme de $G^a_{K',K}$ sur C_K. Soit φ'' l'homomorphisme de $G_{K',K}$ sur $G'_{K',k}$ attaché à K' et k ; on a vu que $\varphi''(G^c_{K',K}) = G'^c_{K',K}$; par passage au quotient, φ'' définit donc un homomorphisme μ de Γ sur $G'_{K',k}/G'^c_{K',K} = G'_{K,k}$. Si on identifie $G^a_{K',K}$ avec C_K au moyen de $\bar{t}$, Γ devient une extension de C_K par $\mathfrak{g}(K/k)$, munie d'un homomorphisme μ sur $G'_{K,k}$; et il résulte de (D) appliquée à K' et K que μ coïncide sur C_K avec l'homomorphisme canonique de C_K sur C'_K. Dans ces conditions, tout revient à vérifier que Γ, muni de cet homomorphisme μ, satisfait à (F). Il revient au même de

(5) On notera l'analogie entre cette démonstration et celle qui a servi à déterminer les groupes de cohomologie de $\mathfrak{g}$ dans D_K ; il serait à souhaiter qu'on pût les réunir toutes deux en une seule.

vérifier (C) pour les systèmes de corps K', K, k', où k' est intermédiaire entre k et K et tel que $[K: k']=2$, ou encore de vérifier (C) pour K', K et k dans le cas où $[K: k]=2$. Supposons même, plus généralement, que K soit cyclique de degré n sur k; soient σ un générateur de $\mathfrak{g}(K/k)$, et ρ un représentant de σ dans $\mathfrak{g}(K'/k)$. Soient (s_α) un système de représentants de $\mathfrak{g}(K'/k)$ dans $G_{K',k}$, et (s'_α) son image dans $G'_{K',k}$; posons $a_{\alpha,\beta}=s_{\alpha\beta}^{-1}s_\alpha s_\beta$. Alors $(a_{\alpha,\beta})$ est un système de facteurs de $\mathfrak{g}(K'/k)$ dans $C_{K'}$ qui satisfait à (D'); en particulier, l'automorphisme de A_k induit par s'_ρ est celui qui est déterminé par l'image de $a=\prod_\alpha a_{\rho,\alpha}$ dans C'_k, le produit $\prod_\alpha$ étant étendu aux éléments α de $\mathfrak{g}(K'/k)$. Mais, comme $G_{K',k}/G_{K',K}$ n'est autre que le groupe cyclique $\mathfrak{g}(K/k)$, le transfert de s_ρ de $G_{K',k}$ dans $G_{K',K}$ est l'image de s_ρ^n dans $G^a_{K',K}$ par l'homomorphisme canonique de $G_{K',K}$ sur $G^a_{K',K}$. Le transfert réduit étant transitif, il s'ensuit que le transfert de s_ρ^n de $G_{K',K}$ dans $C_{K'}$ n'est autre que le transfert de s_ρ de $G_{K',k}$ dans $C_{K'}$, qui est égal à l'élément a de C_k défini plus haut. Autrement dit, quand on identifie $G^a_{K',K}$ avec C_K au moyen de $\bar{t}$, l'image de s_ρ^n dans $G^a_{K',K}$ se trouve identifiée avec a. Cela achève la démonstration.

Nous avons donc bien construit les groupes $G_{K,k}$ possédant les propriétés annoncées, et montré qu'ils sont seuls à les posséder. Il faut avouer que la vérification qui précède a été assez pénible (encore certains points ont-ils été seulement esquissés); peut-être pourra-t-on la simplifier, mais il ne faut sans doute pas s'attendre à obtenir une démonstration vraiment naturelle tant qu'on n'aura pas résolu le problème fondamental de l'interprétation des groupes C_k.

Tout ce qui précède s'applique en particulier si on prend pour k le corps Q des nombres rationnels. Si en même temps on prend une suite K_n de corps galoisiens sur Q, tels que $K_n \subset K_{n+1}$ quel que soit n, dont la réunion soit le corps de tous les nombres algébriques, on pourra construire les groupes $G_n=G_{K_n,Q}$, et, au moyen de (C), définir pour tout n un homomorphisme de G_{n+1} sur G_n, permettant de passer à la "limite projective" (cf. [13]); celle-ci est alors un groupe qui, en un sens qu'il est facile de préciser, est "universel" pour tous les groupes $G_{K,k}$, ceux-ci étant des groupes quotients de sous-groupes du "groupe universel" (de même que le groupe de Galois sur Q du corps de tous les nombres algébriques est "universel" pour les groupes $G'_{K,k}$).

VI. Application aux fonctions L.

Les résultats qui précèdent permettent d'obtenir une décomposition en facteurs des fonctions L de Hecke (" mit Grössencharakteren," c'est-à-dire définies sur un corps K au moyen d'un caractère quelconque de C_K), décomposition qui contient comme cas particulier celle qu'Artin a obtenue pour les fonctions L ordinaires (définies sur un corps K au moyen d'un caractère de C'_K). Pour cela, quelques préliminaires sont nécessaires.

Tout d'abord, soit Ω une extension finie ou infinie d'un corps de nombres k; soit v une valuation de Ω, non archimédienne, c'est-à-dire telle que $v(x+y) \geq \inf [v(x), v(y)]$; soit $\mathfrak{p}$ l'idéal premier de k associé à la valuation discrète induite par v sur k; on posera $q = N_{k/Q}(\mathfrak{p})$. Soit $\bar{\Omega}$ le corps complété de Ω au moyen de la valuation v (c'est-à-dire au moyen de la distance $e^{-v(x-y)}$) ; pour toute extension finie K de k, contenue dans Ω, on désignera par K_v l'adhérence de K dans $\bar{\Omega}$; K_v est isomorphe au complété de K par la valuation induite par v sur K; de plus, le composé $k_v(K)$ de k_v et K dans $\bar{\Omega}$ est un sous-espace vectoriel de K_v sur le corps k_v, donc est fermé dans K_v, et contient K, donc n'est autre que K_v. Si donc on désigne par Ω_v la réunion de tous les corps K_v, on aura $\Omega_v = k_v(\Omega)$, et Ω_v sera une extension algébrique, finie ou infinie, de k_v. On désignera par Ω_v^t la plus grande extension non ramifiée de k_v, contenue dans Ω_v; c'est l'extension de k_v engendrée par toutes les racines de l'unité d'ordre premier à q contenues dans Ω_v. On posera $\Omega_t = \Omega \cap \Omega_v^t$, et $\Omega_z = \Omega \cap k_v$; Ω_t et Ω_z s'appelleront le *corps d'inertie* et *le corps de décomposition* de v dans Ω, relativement à k.

Supposons de plus, à partir de maintenant, que Ω soit galoisien sur k; soit Γ son groupe de Galois, topologisé comme à l'ordinaire; les sous-groupes Γ_t, Γ_z de Γ qui correspondent respectivement à Ω_t et Ω_z s'appelleront les *groupes d'inertie* et *de décomposition* de v dans Γ. Si Ω est de degré fini sur k, ces notions coïncident avec celles qu'on définit ordinairement sous ces mêmes noms. En vertu d'un théorème général de théorie de Galois ([3], chap. V, § 10, $n°4$), Ω et k_v sont linéairement disjoints sur $\Omega_z = \Omega \cap k_v$, et on peut identifier le groupe de Galois Γ_z de Ω sur Ω_z avec celui de $\Omega_v = k_v(\Omega)$ sur k_v, un élément de ce dernier étant identifié avec l'élément de Γ_z, c'est-à-dire avec l'automorphisme de Ω, qu'il induit sur Ω; de plus, dans ces conditions, la relation $\Omega_t = \Omega \cap \Omega_v^t$ implique $\Omega_v^t = k_v(\Omega_t)$, et le groupe de Galois de Ω_v sur Ω_v^t peut être identifié avec Γ_t. Comme

Ω_v^t est abélien sur k_v, il s'ensuit que Γ_t est un sous-groupe invariant de Γ_z, et que Γ_z/Γ_t est abélien. Plus précisément, on définit un automorphisme φ (dit " de Frobenius ") de Ω_v^t sur k_v en posant $\varepsilon^\varphi=\varepsilon^q$ pour toute racine ε de l'unité d'ordre premier à q dans Ω_v^t ; et le groupe engendré par φ est partout dense dans le groupe de Galois de Ω_v^t sur k_v ; ce dernier étant identifié avec Γ_z/Γ_t, on appellera *classe de Frobenius* de v dans Γ l'image réciproque Φ de φ dans Γ_z. Si $\sigma\in\Phi$, on a $\Phi=\sigma\Gamma_t$; et Γ_z est l'adhérence, dans Γ, du groupe Γ_f engendré par Φ, ou, ce qui revient au même, par Γ_t et σ.

Comme d'ailleurs la valuation v de k_v ne peut être prolongée que d'une seule manière à toute extension algébrique de k_v, et par suite à Ω_v, tout automorphisme de Ω_v sur k_v laisse v invariante ; d'autre part, tout automorphisme de Ω sur k qui laisse v invariante peut être prolongé par continuité à un automorphisme de Ω_v qui laisse invariante l'adhérence k_v de k. Il s'ensuit que Γ_z n'est autre que le sous-groupe de Γ qui laisse v invariante. Quant à Γ_t, c'est le sous-groupe de Γ_z qui laisse invariantes toutes les racines de l'unité d'ordre premier à q dans Ω_v. Mais, dans toute extension algébrique de k_v, à tout élément x tel que $v(x)=0$ correspond une racine ε de l'unité d'ordre premier à q, et une seule, telle que $v(x-\varepsilon)>0$; de plus, comme $\Omega_v=k_v(\Omega)$, il correspond à tout $x\in\Omega_v$ un $y\in\Omega$ tel que $v(x-y)>0$. Donc Γ_t peut être défini comme le sous-groupe de Γ_z qui transforme tout $y\in\Omega$ tel que $v(y)\geq 0$ en un y' tel que $v(y-y')>0$; Φ peut être défini comme l'ensemble des éléments de Γ_z qui transforment tout $y\in\Omega$ tel que $v(y)\geq 0$ en un y' tel que $v(y'-y^q)>0$; et le groupe Γ_f engendré par Φ est l'ensemble des éléments σ de Γ_z tels qu'il existe un entier $n\in Z$ pour lequel on ait $v(y^\sigma-y^{q^n})>0$ pour tout $y\in\Omega$ tel que $v(y)\geq 0$. Soit alors K une extension finie de k, contenue dans Ω, et appartenant à un sous-groupe Γ' de Γ ; il résulte de ce qui précède que les groupes de décomposition et d'inertie de v dans Γ' sont $\Gamma'_z=\Gamma_z\cap\Gamma'$ et $\Gamma'_t=\Gamma_t\cap\Gamma'$. Soit de plus $\mathfrak{P}$ l'idéal premier de K associé à la valuation induite sur K par v ; et soit $N_{K/k}(\mathfrak{P})=\mathfrak{p}^f$, d'où $N_{K/Q}(\mathfrak{P})=q^f$; alors la classe de Frobenius de v dans Γ' est $\Phi'=\Phi^f\cap\Gamma'$; et K_v contient une racine primitive d'ordre q^f-1 de l'unité, d'où il suit que $\Phi'^m\cap\Gamma'=\phi$ pour $m\not\equiv 0$ mod. f. Par suite, le groupe Γ'_f engendré par Φ' est donné par $\Gamma'_f=\Gamma_f\cap\Gamma'$.

On notera de plus que toutes les valuations de Ω qui prolongent une valuation donnée de k sont transformées les unes des autres par les automorphismes de Ω sur k, comme il résulte aussitôt du fait qu'il en est ainsi

pour toute extension galoisienne de k de degré fini contenue dans Ω. Par suite, si $\mathfrak{p}$ est donné, les groupes Γ_z, Γ_t, Γ_f, et la classe Φ, sont déterminés à un automorphisme intérieur près de Γ; ils sont complètement déterminés si Γ est abélien.

Appliquons ce qui précède au cas où K est une extension galoisienne finie d'un corps de nombres k, et où on prend $\Omega = A_K$. Avec nos notations ordinaires, le groupe de Galois de Ω sur k sera $\Gamma = G'_{K,k}$, et K appartiendra au sous-groupe $\Gamma' = G'_K = C'_K$ de Γ. La valuation v étant comme ci-dessus, soit U_v, comme au § I, le sous-groupe de I_K formé des idèles dont la coordonnée relative à v (ou plutôt à la valuation induite sur K par v) est une unité de K_v, et dont toute autre coordonnée est 1; soit $\overline{\mathfrak{p}}$ un idèle dont la coordonnée $\mathfrak{p}_v$ relative à v engendre l'idéal premier adhérence de $\mathfrak{P}$ dans K_v (c'est-à-dire est telle que $v(\mathfrak{p}_v)$ soit >0 et engendre le groupe des valeurs prises par v sur K), et dont toute autre coordonnée soit 1; U_v et $\overline{\mathfrak{p}}$ engendrent le groupe des idèles dont toute coordonnée, sauf celle relative à v, est 1, groupe qu'on peut identifier avec K_v^*. Soient V, V_0, $\mathfrak{p}$ les images de K_v^*, U_v et $\overline{\mathfrak{p}}$ dans C_K; il est immédiat que V est un sous-groupe fermé de C_K, engendré par V_0 et $\mathfrak{p}$, et que l'homomorphisme canonique de I_K sur C_K induit sur K_v^* un isomorphisme de K_v^* sur V. Soient V', V'_0, $\mathfrak{p}'$ les images de V, V_0, $\mathfrak{p}$ dans C'_K. Il résulte de la théorie du corps de classes (cf. [5a]) que le groupe d'inertie de v dans $\Gamma' = C'_K$ est $\Gamma'_t = V'_0$, que la classe de Frobenius de v dans Γ' est $\Phi' = \mathfrak{p}' V'_0$, et par suite que le groupe de décomposition Γ'_z de v dans Γ' est l'adhérence du groupe $\Gamma'_f = V'$ engendré par Φ'. De plus, la représentation de K_v^* sur V', induite par l'homomorphisme canonique de I_K sur C'_K, est fournie par le symbole de restes normiques; comme d'ailleurs on sait ([11]) que Ω_v est l'extension abélienne maximale de K_v, on conclut de là, et de la théorie du corps de classes local, que la représentation en question est biunivoque, donc en particulier, puisque U_v est compact, qu'elle induit sur U_v un isomorphisme de U_v sur V'.

Avec les mêmes notations que plus haut, on a donc, dans ces conditions, $\Gamma'_f = V' = \Gamma_f \cap G'_K$; on a aussi $\Omega_z \cap K = K_z$, c'est-à-dire que $\Gamma_z G'_K$ est l'image réciproque, dans $G'_{K,k}$, du groupe de décomposition $\mathfrak{g}_z = \mathfrak{g}(K/K_z)$ de v, ou autrement dit de $\mathfrak{P}$, dans $\mathfrak{g}(K/k) = G'_{K,k}/G'_K$. Comme G'_K est ouvert dans $G'_{K,k}$, et que Γ_f est partout dense dans Γ_z, on a donc $\Gamma_f G'_K = \Gamma_z G'_K = G'_{K,K_z}$, d'où il suit que l'image de Γ_f dans $\mathfrak{g}(K/k)$ est $\mathfrak{g}_z$. Par suite, Γ_f est une extension de $\Gamma'_f = V'$ par $\mathfrak{g}_z$.

Choisissons donc dans Γ_f un système de représentants s'_α des éléments a de $\mathfrak{g}_z$; ce seront en même temps des représentants des a dans G'_{K,K_z}. Si on pose $a'_{\alpha,\beta}=s'^{-1}_{\alpha\beta}s'_\alpha s'_\beta$, $(a'_{\alpha,\beta})$ est un système de facteurs de $\mathfrak{g}_z$ dans $V'\subset C'_K$; soit $a=(a_{\alpha,\beta})$ le système de facteurs de $\mathfrak{g}_z$ dans $V\subset C_K$ dont $(a'_{\alpha,\beta})$ est l'image dans V' ; on va montrer que $a\in F_{K,K_z}(s')$. D'après le § V, il suffira pour cela de faire voir qu'il en est bien ainsi dans le cas où $k=K_z$ et $[K:k]=2$. Supposons même plus généralement que K soit cyclique de degré n sur k, et que $k=K_z$; soit σ un générateur de $\mathfrak{g}(K/k)=\mathfrak{g}_z$; soit s'_σ un représentant de σ dans Γ_f ; soit $a'=s'^n_\sigma$. Alors a' est dans V' et est invariant par σ ; c'est donc l'image dans V' d'un élément a de k_v^*. Il s'agit de prouver que l'automorphisme de A_k induit par s'_σ est celui qui est déterminé par l'image de a dans C'_k. On a vu en effet qu'on peut identifier Γ_z avec le groupe de Galois de $\Omega_v=k_v(\Omega)$ sur k_v, et aussi que le sous-corps $k_v(A_k)$ de Ω_v est l'extension abélienne maximale de k_v. Il résulte alors du théorème de transfert local[6] que l'automorphisme de $k_v(A_k)$ induit par l'automorphisme s'_σ de Ω_v est celui qui correspond à a par le symbole de restes normiques ; l'automorphisme de A_k induit par s'_σ est donc bien celui qui est déterminé par l'image de a.

Par conséquent on a en général $a\in F_{K,K_z}(s')$; on peut donc choisir des représentants s_α des s'_α dans $G_{K,k}$ de telle sorte que $s^{-1}_{\alpha\beta}s_\alpha s_\beta=a_{\alpha,\beta}$ quels que soient α, β dans $\mathfrak{g}_z$. Soit H_z le sous-groupe de $G_{K,k}$ engendré par V et par les éléments s_α ainsi choisis ; c'est un groupe fermé, puisqu'il admet le sous-groupe fermé V de C_K comme sous-groupe d'indice fini. Il est clair que l'homomorphisme canonique de $G_{K,k}$ sur $G'_{K,k}$ induit sur H_z une représentation biunivoque de H_z sur Γ_f ; soient H_t et F les images réciproques de Γ_t et de Φ dans H_z par cette représentation ; F est une classe dans H_z suivant H_t, et H_z est engendré par F. On a d'ailleurs $\Gamma'_t=\Gamma_t\cap G'_K=V'_0$; et on a $\Omega_t\cap K=K_t$, c'est-à-dire que $\Gamma'_tG'_K$ est l'image réciproque G'_{K,K_t} dans $G'_{K,k}$, du groupe d'inertie $\mathfrak{g}_t$ de $\mathfrak{P}$ dans $\mathfrak{g}(K/k)$; on en conclut que Γ'_t est une extension de V'_0 par $\mathfrak{g}_t$, d'où il suit que H_t est une extension de V_0 par $\mathfrak{g}_t$, et est donc compact. Comme Γ'_t est invariant

(6) C'est le théorème local analogue á notre propriété (A) du § II ; pour la démonstration, v. [5c]. On notera que, pour les besoins de notre démonstration, il suffirait de connaître ce théorème pour les extensions quadratiques ; le cas général résulterait alors de ce qui suit.

dans Γ_z, donc dans Γ_f, H_t est invariant dans H_z ; et H_z/H_t est engendré par l'image dans ce groupe d'un élément quelconque de F. D'ailleurs H_z/H_t n'est pas fini, puisque H_t est compact et que H_z, qui contient le groupe non compact V, n'est pas compact. Donc H_z/H_t est isomorphe à Z.

Le groupe H_z dépend d'ailleurs du choix des s_α, choix que les conditions énoncées ci-dessus ne suffisent pas à déterminer. Mais tout autre choix, conforme à ces conditions, ne peut consister qu'à remplacer les s_α par $s_\alpha z_\alpha$, avec $z_\alpha \in D_K$ et $\partial z = 1$; comme le groupe de cohomologie de dimension 1 de $\mathfrak{g}_z$ dans D_K est trivial, on aura donc $z_\alpha = u^{\alpha-1}$, avec $u \in D_K$, d'où $s_\alpha z_\alpha = u s_\alpha u^{-1}$. Autrement dit, tout autre choix des s_α conduit à remplacer H_z par $uH_z u^{-1}$, avec $u \in D_K$; l'un quelconque de ces groupes s'appellera un *groupe de décomposition* de la valuation v dans $G_{K,k}$. Si H_z est fixé, H_t et F sont complètement déterminés et s'appelleront le *groupe d'inertie* et la *classe de Frobenius* de v dans H_z.

Si donc H_1 est un groupe de décomposition de v dans $G_{K,k}$, on a $H_1 \cap C_K = V$, et l'image de H_1 dans $G'_{K,k}$ est Γ'_f. Réciproquement, si un sous-groupe H_1 de $G_{K,k}$ a pour image Γ'_f dans $G'_{K,k}$, et si $H_1 \cap C_K \subset V$, H_1 est un groupe de décomposition de v dans $G_{K,k}$. En effet, soit t_α, pour chaque $\alpha \in \mathfrak{g}_z$, un représentant de s'_α dans H_1 ; comme t_α a même image que s_α dans $G'_{K,k}$, on a $t_\alpha = s_\alpha z_\alpha$, avec $z_\alpha \in D_K$, d'où $t_{\alpha\beta}^{-1} t_\alpha t_\beta = a_{\alpha,\beta} (\partial z)_{\alpha,\beta}$. Comme $H_1 \cap C_K \subset V$, $t_{\alpha\beta}^{-1} t_\alpha t_\beta$ doit être dans V, donc $(\partial z)_{\alpha,\beta}$ dans $D_K \cap V$. Comme l'homomorphisme canonique de C_K sur C'_K induit sur V une représentation biunivoque sur V', on a $V \cap D_K = \{1\}$, d'où $\partial z = 1$, et par suite, comme tout à l'heure, $z = \partial u$, avec $u \in D_K$. De plus, comme Γ_f contient V' qui est image biunivoque de V, on doit avoir $H_1 \cap C_K = V$. On a donc $H_1 = uH_z u^{-1}$.

Si on suppose seulement donné l'idéal premier $\mathfrak{p}$, ou, ce qui revient au même, la valuation induite par v sur k, alors, comme on a vu, Γ_z, Γ_f, Γ_t, Φ sont déterminés seulement à un automorphisme intérieur près de $G'_{K,k}$; il s'ensuit qu'alors H_z, H_t, F sont déterminés seulement à un automorphisme intérieur près de $G_{K,k}$; leurs transformés par un tel automorphisme seront dits un groupe de décomposition, un groupe d'inertie, et une classe de Frobenius de $\mathfrak{p}$ dans $G_{K,k}$. De même, si $\mathfrak{P}$ est donné, c'est-à-dire si v est donnée sur K seulement, H_z, H_t et F sont déterminés à un automorphisme intérieur près de $G_{K,k}$ laissant $\mathfrak{P}$ invariant, c'est-à-dire de

la forme $x \to uxu^{-1}$ avec $u \in G_{K,K_z}$.

Avec les mêmes notations, soit de plus $\mathfrak{g}'$ un sous-groupe de $\mathfrak{g}(K/k)$, et soit k' le sous-corps correspondant de K. Comme, d'après ce qui précède, le groupe $H'_z = H_z \cap G_{K,k'}$ a pour image dans $G'_{K,k'}$ le groupe $\Gamma_f \cap G'_{K,k'}$, qui est le sous-groupe de $G'_{K,k'}$ défini comme Γ_f l'est dans $G'_{K,k}$, et qu'on a $H'_z \cap C_K = V$, H'_z est un groupe de décomposition de v dans $G_{K,k'}$. Soit $\mathfrak{p}'$ l'idéal premier de k' associé à la valuation induite par v sur k' ; et soit $N_{k'/k}(\mathfrak{p}') = \mathfrak{p}^f$. Comme on a vu que la classe de Frobenius de v dans $G'_{K,k'}$ est $\Phi^f \cap G'_{K,k'}$, et qu'on a $\Phi^m \cap G'_{K,k'} = \phi$ pour $m \not\equiv 0 \bmod f$, il s'ensuit, par la correspondance biunivoque entre H'_z et son image dans $G'_{K,k'}$, que la classe de Frobenius de v dans H'_z est donnée par $F' = F^f \cap G_{K,k'}$ et qu'on a $F'^m \cap G_{K,k'} = \phi$ pour $m \not\equiv 0 \bmod f$; il s'ensuit que $F'^n = F^{nf} \cap G_{K,k'}$, et en particulier, pour $n=0$, que $H'_t = H_t \cap G_{K,k'}$ est le groupe d'inertie de v dans H'_z. En particulier, si $k' = K$, on a $H'_z = V$, $H'_t = V_0$, $F' = pV_0$.

Soit maintenant W l'image dans C_k du groupe des idèles de I_k dont toutes les composantes ont la valeur 1 à l'exception au plus de celle relative à la valuation induite par v sur k ; W est le groupe de décomposition, dans C_k, de la valuation w induite par v sur A_k. Soit t le transfert de $G_{K,k}$ dans C_K ; on a $t(V) = N(V) \subset W$; et, pour $\alpha \in \mathfrak{g}_z$, la formule (N) du § IV donne $t(s_\alpha) = N_{K_z/k}(\prod_{\beta \in \mathfrak{g}_z} a_{\alpha,\beta}) \in W$; on a donc $t(H_z) \subset W$. Les résultats qui précèdent, ainsi que l'application de la propriété (A) à $G'_{K,k}$, montrent d'ailleurs que l'image de $t(F)$ dans C'_k est la classe de Frobenius de w dans $C'_k = G'_k$, et que par suite l'image de $t(H_z)$ dans C'_k est le groupe engendré par cette classe, c'est-à-dire l'image de W dans C'_k. On en conclut immédiatement que $t(H_z) = W$, et que $t(H_t)$ et $t(F)$ sont respectivement le groupe d'inertie et la classe de Frobenius de w dans C_k.

Soit de plus K' une extension de K de degré fini, galoisienne sur k ; au moyen de (C), identifions $G_{K,k}$ avec $G_{K',k}/G^c_{K',K}$. Soit $\bar{v}$ une valuation de $A_{K'}$, prolongeant la valuation v de A_K ; soit $\bar{H}_z$ un groupe de décomposition de $\bar{v}$ dans $G_{K',k}$, et soient $\bar{H}_t$ et $\bar{F}$ le groupe d'inertie et la classe de Frobenius de $\bar{v}$ dans $\bar{H}_z$. On va montrer que les images de $\bar{H}_z$, $\bar{H}_t$, $\bar{F}$ dans $G_{K,k}$, par l'homomorphisme canonique de $G_{K',k}$ sur $G_{K,k} = G_{K',k}/G^c_{K',K}$, sont respectivement un groupe de décomposition de v dans $G_{K,k}$, et le groupe d'inertie et la classe de Frobenius correspondants. En effet, d'après ce que nous savons déjà, les images de ces images dans $G'_{K,k}$ sont

les groupes Γ_z, Γ_t et la classe Φ ; d'autre part, d'après ce qu'on a démontré plus haut, $\bar{H}_z \cap G_{K',K}$ est un groupe de décomposition de $\bar{v}$ dans $G_{K',K}$, et par suite son image dans $C_K = G_{K',K}/G^c_{K',K}$, au moyen du transfert de $G_{K',K}$ dans $C_{K'}$, est V. Cela suffit, comme nous savons, pour démontrer notre assertion au sujet de l'image de $\bar{H}_z$ dans $G_{K,k}$; le reste s'ensuit immédiatement.

Par un caractère de $G_{K,k}$, on entendra la trace d'une représentation irréductible de $G_{K,k}$ par des matrices unitaires ; comme $G_{K,k}$ est produit direct d'un gronpe isomorphe à R et du groupe compact $G^0_{K,k}$, l'étude des caractères de $G_{K,k}$ se ramène à celle des caractères de $G^0_{K,k}$. Soit φ une fonction continue sur $G_{K,k}$, à valeurs numériques complexes, invariante par les automorphismes intérieurs de $G_{K,k}$; ce pourra être par exemple un caractère de $G_{K,k}$, ou une combinaison linéaire de tels caractères. Pour chaque idéal premier $\mathfrak{p}$ de k, choisissons une classe de Frobenius $F_\mathfrak{p}$ de $\mathfrak{p}$ dans $G_{K,k}$; si $H_\mathfrak{p}$ est le groupe d'inertie correspondant, $F_\mathfrak{p}$ est une classe suivant $H_\mathfrak{p}$ dans $G_{K,k}$, et il en est de même de $F_\mathfrak{p}^n$ quel que soit l'entier n. Comme $H_\mathfrak{p}$ est un sous-groupe compact de $G_{K,k}$, on peut définir sur $H_\mathfrak{p}$, d'une manière unique, la valeur moyenne des fonctions continues sur $H_\mathfrak{p}$ de façon que cette moyenne soit invariante par translation (ce sera l'intégrale prise au moyen de la mesure de Haar sur $H_\mathfrak{p}$, normée de telle sorte que l'intégrale de la constante 1 soit 1) ; et on peut transporter, par translation, cette notion de moyenne à toute classe suivant $H_\mathfrak{p}$ dans $G_{K,k}$, donc en particulier aux classes $F_\mathfrak{p}^n$. Dans ces conditions, soit $M(\varphi, \mathfrak{p}^n)$ la moyenne de φ sur $F_\mathfrak{p}^n$; tout autre choix de $F_\mathfrak{p}$ reviendrait à transformer $H_\mathfrak{p}$, $F_\mathfrak{p}$, $F_\mathfrak{p}^n$ par un automorphisme intérieur de $G_{K,k}$, donc ne changerait pas $M(\varphi, \mathfrak{p}^n)$ puisque φ est invariante par un tel automorphisme. Nous définirons alors une fonction $L(s, \varphi ; K/k)$ par la formule

$$\log L(s, \varphi ; K/k) = \sum_{\mathfrak{p},n} \frac{M(\varphi, \mathfrak{p}^n)}{n(N\mathfrak{p})^{ns}},$$

où l'on a posé $N\mathfrak{p} = N_{k/\mathbb{Q}}(\mathfrak{p})$, et où la somme est étendue à tous les idéaux premiers $\mathfrak{p}$ de k, et à tous les entiers $n > 0$.

Il est clair que $\log L(s, \varphi ; K/k)$ dépend linéairement de φ. Si K' est une extension de K de degré fini, galoisienne sur k, soit φ' la composée de φ et de l'homomorphisme de $G_{K',k}$ sur $G_{K,k}$, défini en vertu de (C) ;

en particulier, si φ est un caractère de $G_{K,k}$, φ' en sera un de $G_{K',k}$. On a vu que l'image dans $G_{K,k}$ d'une classe de Frobenius de $\mathfrak{p}$ dans $G_{K',k}$ est une classe de Frobenius de $\mathfrak{p}$ dans $G_{K,k}$. On en conclut aussitôt qu'on a, dans ces conditions :

$$L(s, \varphi'; K'/k)=L(s, \varphi; K/k).$$

D'autre part, soit k' un corps intermédiaire entre k et K; soit χ un caractère de $G_{K,k'}$, soit ψ la trace de la représentation imprimitive de $G_{K.k}$ (irréductible ou non) qui est " induite " par la représentation de $G_{K,k'}$ de trace χ. Si on tient compte des résultats démontrés plus haut, on trouve, au moyen d'un calcul tout à fait analogue à celui d'Artin ([1a]), et qui n'offre pas de difficulté :

$$L(s, \psi; K/k)=L(s, \chi; K/k').$$

Bien entendu, si $K=k$, et si χ est un caractère de C_k, $L(s, \chi; k/k)$ n'est autre qu'une fonction L de Hecke (" mit Grössencharakteren ") attachée au corps k; si χ est la constante 1, c'est la fonction zêta de k; sinon, c'est une fonction entière satisfaisant à l'équation fonctionnelle établie par Hecke ([8]). D'autre part, si la représentation de $G_{K,k}$ de caractère χ a un noyau contenant D_K, χ peut être considéré comme un caractère de $G'_{K,k}$, et $L(s, \chi; K/k)$ est l'une des séries L " non abéliennes " introduites et étudiées dar Artin ([1a], [1c]).

Il n'y a alors qu'à suivre Artin pas à pas pour obtenir toute la théorie des fonctions $L(s, \chi; K/k)$ attachées aux caractères de groupes $G_{K,k}$. Le seul raisonnement dont l'extension n'est pas immédiate est la démonstration donnée par Artin du caractère algébroïde de ses fonctions. Mais nous allons même démontrer, au moyen du théorème de Brauer ([4]), que les fonctions $L(s, \chi; K/k)$ sont méromorphes. D'après ce qui précède, il suffit de considérer les fonctions $L(s, \chi; K/k)$ attachées aux caractères des représentations irréductibles primitives de $G_{K,k}$. Soit M une telle représentation, de degré r, de caractère χ; un raisonnement classique (cf. [12], th. 168, p. 192) montre que M doit alors induire sur C_K une représentation de C_K de la forme $\omega(x)\cdot 1_r$, où 1_r désigne la matrice unité à r lignes et r colonnes, et où ω est un caractère de C_K invariant par les automorphismes de $\mathfrak{g}(K/k)$. Soient s_α des représentants dans $G_{K,k}$ des éléments de $\mathfrak{g}(K/k)$, et soit $a_{\alpha,\beta}=s_{\alpha\beta}^{-1}s_\alpha s_\beta$; alors les $\omega(a_{\alpha,\beta})$ forment un

système de facteurs de $\mathfrak{g}(K/k)$ dans le groupe multiplicatif γ des nombres complexes de valeur absolue 1, $\mathfrak{g}(K/k)$ opérant trivialement sur γ (c'est-à-dire que tout élément de $\mathfrak{g}(K/k)$ y induit l'automorphisme identique). Soit γ_0 le sous-groupe de γ formé des racines n-ièmes de l'unité, où $n=[K : k]$; on sait que tout système de facteurs de $\mathfrak{g}(K/k)$ dans γ est équivalent à un système de facteurs de $\mathfrak{g}(K/k)$ dans γ_0, et on peut donc écrire $\omega(a_{\alpha,\beta})=\eta_{\alpha\beta}^{-1}\eta_\alpha\eta_\beta\zeta_{\alpha,\beta}$, où $\eta_\alpha\in\gamma$ et $\zeta_{\alpha,\beta}\in\gamma_0$ quels que soient α, β. Alors le sytème de facteurs $\zeta_{\alpha,\beta}$ définit une extension E de γ_0 par $\mathfrak{g}(K/k)$, qui est un groupe fini d'ordre n^2 dont le centre contient γ_0. Soient t_α des représentants dans E des éléments de $\mathfrak{g}(K/k)$; soit ω_0 l'automorphisme identique de γ_0, qu'on peut considérer comme un caractère de γ_0. Alors il y a une correspondance biunivoque entre les représentations N de degré s de $G_{K,k}$, induisant sur C_K la représentation $\omega(x)\cdot 1_s$, et les représentations N_0 de degré s de E, induisant sur γ_0 la représentation $\omega_0(\xi)\cdot 1_s$, correspondance déterminée par la formule $N(s_\alpha)=\eta_\alpha N_0(t_\alpha)$; si N est irréductible, il en est de même de N_0, et réciproquement. Soit en particulier M_0 la représentation de degré r de E qui correspond ainsi à M, et soit χ_0 son caractère.

D'autre part, si λ est une représentation de degré 1 d'un sous-groupe g de E, il est facile de vérifier que la représentation monomiale de $g\gamma_0$, induite par λ, est réductible et somme directe de représentations de degré 1 de $g\gamma_0$; et par suite la représentation monomiale de E, induite par λ, est somme directe de représentations monomiales induites par des représentations de degré 1 de $g\gamma_0$. D'après le théorème de Brauer, on peut écrire le caractère χ_0 de M_0 comme combinaison linéaire $\sum_i a_i\psi_i$, à coefficients entiers, de caractères ψ_i de représentations monomiales induites par des représentations λ_i de degré 1 de sous-groupes g_i de E ; d'après ce qu'on vient de dire, on a le droit de supposer de plus que chacun des g_i contient γ_0. On a alors, quels que soient $x\in E$ et $\xi\in\gamma_0$, $\chi_0(x\xi)=\chi_0(x)\omega_0(\xi)$ et $\psi_i(x\xi)=\psi_i(x)\lambda_i(\xi)$, d'où $\chi_0(x)=\sum_i a_i\psi_i(x)\lambda_i(\xi)\omega_0(\xi^{-1})$; en vertu de l'indépendance linéaire des caractères de γ_0, cette relation subsiste si on ne conserve au second membre que les termes pour lesquels $\lambda_i(\xi)=\omega_0(\xi)$. Autrement dit, on a le droit de supposer de plus que chacun des λ_i coïncide avec ω_0 sur γ_0. Cela étant, soit $\mathfrak{g}_i$ l'image de g_i dans $\mathfrak{g}(K/k)=E/\gamma_0$; soit k_i le sous-corps de K correspondant à $\mathfrak{g}_i$. A la représentation monomiale de caractère ψ_i, qui induit sur γ_0 la représentation $\omega_0(\xi)\cdot 1_s$ avec $s=[G : g_i]$, correspond, comme il a été expliqué, une représentation de $G_{K,k}$, induisant

$\omega(x)\cdot 1_s$ sur C_K; il est immédiat que cette représentation sera, elle aussi, monomiale, et induite par une representation θ_i de degré 1 de G_{K,k_i}; si φ_i en est le caractère, on aura $\chi=\sum_i a_i\varphi_i$, et par suite :

$$L(s,\ \chi\ ;\ K/k)=\prod_i L(s,\ \varphi_i\ ;\ K/k)^{a_i}=\prod L(s,\ \theta_i\ ;\ K/k_i)^{a_i}.$$

Comme les $L(s, \theta_i\ ;\ K/k_i)$ sont des fonctions de Hecke, cela achève la démonstration.

Bien entendu, il y a lieu de conjecturer, comme le fait Artin au sujet de ses fonctions L non abéliennes, que les fonctions L introduites ici sont des fonctions entières. Mais, comme la démonstration des conjectures analogues dans les corps de fonctions l'a fait apparaître nettement, la conjecture d'Artin est étroitement liée à l'hypothèse de Riemann ; c'est assez dire qu'elle dépasse les moyens de démonstration dont nous disposons à ce jour.

Bibliographie.

1. E. Artin : (a) *Über eine neue Art von* L-*Reihen*, Hamb. Abh. 3 (1923), p. 89 ; (b) *Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz*, ibid. 7 (1930), p. 46 ; (c) *Zur Theorie der* L-*Reihen mit allgemeinen Gruppencharakteren*, ibid. 8 (1931), p. 292.

2. E. Artin and G. Whaples, *Axiomatic characterization of fields by the product formula for valuations*, Bull. Am. Math. Soc. 51 (1945), p. 469.

3. N. Bourbaki, *Algèbre*, Chap. IV-V, Hermann et Cie, Paris 1950.

4. R. Brauer, *On Artin's* L-*series with general group characters*, Ann. of Math. 48 (1947), p. 502.

5. C. Chevalley : (a) *:Généralisation de la théorie du corps de classes pour les extensions infinies*, J. de Liouville (IX) 15 (1936), p. 359 ; (b) *La théorie du corps de classes*, Ann. of Math. 41 (1940), p. 394 ; (c) *Deux théorèmes d'arithmétique*, ce vol. p. 36.

6. S. Eilenberg and S. MacLane, *Cohomology theory in abstract groups* I, Ann. of Math. 48 (1947), p. 51.

7. Ph. Furtwängler, *Beweis des Hauptidealsatzes*, Hamb. Abh. 7 (1930), p. 14.

8. E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen*, Math. Zeitschr. 1 (1918), p. 357 und 6 (1919), p. 11.

9. S. Iyanaga, *Zum Beweis des Hauptidealsatzes*, Hamb. Abh. 10 (1934), p. 349.

10 (a). T. Nakayama, *Idèle-class factor-sets and class-field theory*, paraîtra dans Ann. of Math., (b) G. Hochschild and T. Nakayama, *Cohmology in class-field theory*, *ibid.*

11. F. K. Schmidt, *Zur Klassenkörpertheorie im Kleinen*, Crelles J. 162 (1930), p. 155.

12. A. Speiser, *Die Theorie der Gruppen von endlicher Ordnung*, 2te Aufl., J. Springer, Berlin 1927.

13. A. Weil, *L'intégration dans les groupes topologiques et ses applications*, Hermann et Cie, 2e éd., Paris 1951.

14. H. Zassenhaus, *Lehrbuch der Gruppentheorie* I, Teubner, Leipzig-Berlin 1937.