RÉDACTION N° 171BIS

COTE : NBR 073

TITRE : RAPPORT D'ALGÈBRE UNIDIMENSIONNELLE
CHAPITRE I : ARITHMÉTIQUE DES CORPS VALUÉS

ASSOCIATION DES COLLABORATEURS DE NICOLAS BOURBAKI

NOMBRE DE PAGES : 75

NOMBRE DE FEUILLES : 75

NBR 073
171 bis
2

RAPPORT SUR L'ALGEBRE DITE UNIDIMENSIONNELLE .

CHAPITRE I

ARITHMETIQUE DES CORPS VALUES .

Sommaire.

Commentaires d'un des rédacteurs .

L'essentiel de ce chapitre est formé par des résultats locaux . Le rédacteur s'excuse donc d'y avoir inséré un § global (§ 4). Ce § est ici afin de permettre de faire d'un seul coup toute la théorie de la différente (qui "passe" trivialement du local au global , une fois la machinerie mise en place). Certains pourraient préférer voir ce § au début du second chapitre du rapport c'est là une question de lignes et colonnes , dont on ne pourra décider qu'en liaison avec l'étude des chapitres "Valuations et spécialisations" , "anneaux noetheriens" et "algèbre locale" . Le rédacteur se demande d'ailleurssi l'on pourra établir un plan valable sans avoir sous les yeux le chap.III du rapport

(corps de fonctions algébriques) et un rapport sur la Géométrie algébrique .

A ce propos le rédacteur signale que , s'il n'a pas eu lui-même de trop grandes difficultés à donner un traitement presque "gleichberechtigt" des p-adiques et séries formelles , son collègue global a dû séparer nombres et fonctions , et ceci pour des raisons qui semblent sérieuses . Ceci ne peut qu'apporter de l'eau au moulin de ceux qui veulent traiter les corps de fonctions au moyen de courbes , produits de courbes et jacobiennes . Cependant le rédacteur demande qu'on ne s'engage pas à la légère à renoncer à l'analogie entre fonctions et nombres .

Le rédacteur signale les détails suivants :

a) La prop.3 du § 1 pourrait être améliorée par prolongement de la valeur absolue d'une algèbre normée réelle à sa complexifiée .

b) Les résultats sur les extensions non ramifiées (§ 2,fin du n°3) méritent des énoncés en forme .

c) Le n° des représentants multiplicatifs (§ 2,n°5) est inutile pour la suite Celui de l'exponentielle (§ 2,n°6) l'est presque , n'étaient l'utilisation de la finitude de $(K : K^n)$ dans le th. d'existence du corps de classes local (§ 6,n°7) , et le besoin de la valeur de cet indice qu'a eu le collègue global. Par contre l'exponentielle est inutile pour l'inégalité $(K : N(L))$ $L:K$ (K localement compact , L galoisienne) , qui est fondamentale pour le corps de classes : on peut démontrer celle-ci , soit par une astuce krasnérienne (cf.§ 6 n°1) , soit comme conséquence de la Führerdiskriminantenformel (§ 6,n°8) ; ce n'est pas nettement plus compliqué que la méthode Chevalley .

d) Le n° du groupe de décomposition est mal fichu (§ 3,n°1) . Il faudrait des énoncés en forme au § 3,n°3 .

e) Le rédacteur est affolé par les amas de cocycles du corps de classes local , et ne comprend rien à tous ces calculs . Il a l'impression que la méthode des algèbres simples rend les choses plus claires . Mais il sera ravi si le Haut Commissariat à la Topologie algébrique prend les n^{os} 2,3 et 4 du § 6 à son compte et y met de l'ordre .

RAPPORT D'ALGÈBRE UNIDIMENSIONNALLE .

CHAPITRE I
ARITHMÉTIQUE DES CORPS VALUÉS .

§ 1 . Valeurs absolues et valuations .

Rappelons qu'étant donné un corps K , on appelle valeur absolue sur K une application f de K dans R_+ telle que $f(xy)=f(x)f(y)$, $f(x+y)\leqslant f(x)+f(y)$,et que $f(x)=0$ entraîne $x=0$; la distance $f(x-y)$ définit alors sur K une topologi compatible avec sa structure de corps .

Soit maintenant v une valuation de K dont le groupe des ordres est archimédien , c'est-à-dire isomorphe à un sous-groupe additif de R . La fonction numérique $e^{-v(x)}$ est une valeur absolue sur K ; on dit qu'une telle valeur absolue est valuative .

PROPOSITION 1 .- Pour qu'une valeur absolue f d'un corps K soit valuative , il faut et il suffit que l'une ou l'autre des conditions suivantes soit vérifiée :

a) $f(x+y)\leqslant \mathrm{Max}(f(x),f(y))$;

b) $f(n.1)\leqslant 1$ pour tout entier naturel n .

C'est évident pour a) . a) entraîne b) car $f(1)=1$. Réciproquement la formul du binôme montre que $f((a+b)^n)\leqslant (n+1)\mathrm{Max}(f(a)^n,f(b)^n)$, d'où a) en faisant te dre n vers l'infini .

COROLLAIRE .- Toute valeur absolue d'un corps de caractéristique $p\neq 0$ est valuative .

En effet , tout élément n.1 est une racine de l'unité .

On dit (Top.gén.,chap.IX,§ 3,n°2) que deux valeurs absolues f,g de K sont équivalentes s'il existe un nombre réel s tel que $f(x)=g(x)^s$.

PROPOSITION 2 .- Toute valeur absolue f de Q est équivalente à une valeur absolue p-adique , ou à la valeur absolue ordinaire .

Ceci a déjà été vu dans le cas où f est valuative (chap. des valuations) . Sinon , soit n un entier tel que $f(n)>1$. Soient a et b des entiers >1 ; écrivons $a^h=a_0+a_1b+\ldots+a_qb^q$, où $0\leqslant a_i\leqslant b-1$. On en déduit

NSR 073

$f(a^h) \leq b(q+1).\mathrm{Max}(1, f(b)^q)$. Or on a $q \sim h.\log a/\log b$. On en déduit , en faisant tendre h vers l'infini , $f(a) \leq \mathrm{Max}(1, f(b)^{\log a/\log b})$. En prenant $a=n$, on en déduit $f(b) > 1$ pour tout entier $b > 1$. L'inégalité précédente s'écrit alors $f(a) \leq f(b)^{\log a/\log b}$, ou encore $\log(f(a))/\log a \leq \log(f(b))/\log b$. En échangeant les rôles de a et b , on en déduit que $\log(f(a))/\log a$ est une constante s indépendante de l'entier $a > 1$. Autrement dit $f(a)=a^s$ (on a $0 \leq s \leq 1$ car $f(a) \leq a$). D'où $f(a)=x^s$ pour tout nombre rationnel $x > 0$,et $f(x)=|x|^s$ pour tout $x \in Q$.

PROPOSITION 3 .- Un corps K muni d'une valeur absolue non valuative f est isomorphe à un sous-corps de C (muni d'une valeur absolue équivalente à la valeur absolue usuelle).

En effet K est de caractéristique 0 (cor. de la prop.1) . Donc il contient Q et la restriction de f à Q est de la forme $|x|^s$ (prop.2) . Donc le complété $\hat{K}$ de K contient R . Alors $\hat{K}(i)$, muni de la valeur absolue $g(a+bi)=(f(a^2+b^2))^{\frac{1}{2}}$ si $i \notin \hat{K}$ (il faut ici vérifier que $f(1+x^2) < 1$ est impossible , ce qui se fait au moyen du développement en série de $(1-(1+x^2))^{\frac{1}{2}}$) contient C , et on applique Gelfand-Mazur .

PROPOSITION 4 .- Soient K un corps , et f une valeur absolue de K faisant de K un corps localement compact non discret . Alors , ou bien K est isomorphe à R ou à C , ou bien f se déduit d'une valuation v dont le corps des valeurs est fini .

Comme K est complet , il suffit d'examiner le cas d'une valuation (prop.3). Alors il existe un nombre réel strictement positif r tel que l'ensemble des x tels que $f(x) \leq r$ soit compact . On peut supposer qu'il existe $a \in K$ tel que $f(a)=r$. Soit A l'anneau de v ; comme Aa est compact , il en est de même de A par homothétie . Comme tout idéal I de A est ouvert , A/I est compact et discret , donc fini . Par conséquent v est discrète et son corps des valeurs est fini .

PROPOSITION 5 .- Deux valeurs absolues f et g définissant la même topologie sur un corps K sont équivalentes (Top.gén., chap.IX, § 3, prop.5) .

PROPOSITION 6 (théorème d'approximation) .- Soient K un corps , (f_i) n valaurs absolues non deux à deux équivalentes de K , (a_i) n éléments de K , et ε un nombre réel >0 . Il existe $x \in K$ tel que $f_i(x-a_i) \leq \varepsilon$ pour tout i .

Notons K_i le corps K muni de la topologie définie par f_i ; le résultat à démontrer équivaut au suivant : dans le produit $\prod_i K_i$ la diagonale D est partout dense . Nous procéderons par récurrence sur n , le cas n=1 étant trivial . Comme f_i et f_j ne sont pas équivalentes , il existe x_{ij} tel que $f_i(x_{ij})<1$ et $f_j(x_{ij})\geq 1$. Montrons par récurrence sur h l'existence de x_h tel que $f_1(x_h)<1$ $f_2(x_h)\geq 1$, $f_i(x_h)\neq 1$ pour $i\leq h$; pour h=2 il suffit de prendre $x_2=x_{12}$; si $f_{h+1}(x_h)\neq 1$ on prend $x_{h+1}=x_h$; si $f_{h+1}(x_h)=1$, on choisit z tel que $f_{h+1}(z)\neq 1$, et $x_{h+1}=(x_h)^s z$ répond à la question pour s assez grand . Posons $y=x_n(x_{n+1})^{-1}$, et considérons la suite des puissances $(y^k)_{k\geq 1}$; elle tend vers 0 dans K_1 , vers 1 dans K_2 , vers 0 ou 1 dans les autres K_i . D'où un point $\neq 0$ adhérent à la diagonale D et contenu dans la diagonale d'un sous-espace E de coordonnées. On conclut en remarquant que $\overline{D}$ est un sous-espace vectoriel , et en appliquant l'hypothèse de récurrence au supplémentaire de E et à E .

§ 2 . Extensions algébriques finies de corps valués .

1 . Formules utiles sur les normes , traces , polynômes caractéristiques .

Soient A un anneau commutatif , F une algèbre commutative sur A telle que le A-module F admette une base finie . Pour tout $z \in F$ la multiplication par z dans F est un endomorphisme M_z du A-module F . Le polynôme caractéristique $\det(X.1-M_z)$ est appelé le polynôme caractéristique de z sur A ; c'es aussi le déterminant de l'endomorphisme $X.1-M_z$ du A[X]-module F[X] (Alg., chap. VII) , c'est-à-dire de l'endomorphisme M_{X-z} , multiplication par X-z . Ce polynôme s'écrit $\det(X.1-M_z)=X^n-a_1X^{n-1}+\ldots+(-1)^n a_n$ $(a_i \in A)$;
les coefficients a_1 et a_n sont appelés la trace et la norme de z sur A et se notent $\mathrm{Tr}_{F/A}(z)$ et $N_{F/A}(z)$; on a évidemment les formules :

(1) $\mathrm{Tr}_{F/A}(z)=\mathrm{Tr}(M_z)$, $N_{F/A}(z)=\det(M_z)$

(2) $N_{F[X]/A[X]}(X-z)$ est le polynôme caractéristique de z sur A .

(3) $\mathrm{Tr}_{F/A}(z_1+z_2)=\mathrm{Tr}_{F/A}(z_1)+\mathrm{Tr}_{F/A}(z_2)$, $\mathrm{Tr}_{F/A}(a)=na$ pour $a \in A$.

(4) $N_{F/A}(z_1z_2)=N_{F/A}(z_1)N_{F/A}(z_2)$, $N_{F/A}(a)=a^n$ pour $a\in A$.

Dans le cas où A est un corps , et F un surcorps de ~~M~~ A séparable sur A , les notions de norme et trace ici définies coïncident avec celles définies comme somme et produit de conjugués en Alg.,chap.V . Il résulte en effet d'Alg.,chap. VII que le polynôme caractéristique de l'endomorphisme M_z est une puissance du polynôme minimal (irréductible) de z , l'exposant étant évidemment $[F:A]/[A(z):A]$

Lorsque F est composée directe de sous-algèbres F_i sur A , on voit aussitôt que le polynôme caractéristique de l'élément $z=(z_1,..,z_k)$ de F est le produit des polynômes caractéristiques des éléments z_i de F_i . Il en résulte les formules

(5) $Tr_{F/A}((z_1,...,z_k))=Tr_{F_1/A}(z_1)+...+Tr_{F_k/A}(z_k)$

(6) $N_{F/A}((z_1,..,z_k))=N_{F_1/A}(z_1)...N_{F_k/A}(z_k)$.

Cherchons maintenant des formules de transitivité . Considérons un F-module E admettant une base finie , et soit u un endomorphisme de E ; notons u_A l'endomorphisme u de E considéré comme A-module . En prenant (oh! horreur) une base (f_i) de F sur A , une base (e_j) de E sur F , et (f_ie_j) pour base (dite "télescopique" par H.Weyl) de E sur A , et en considérant la décomposition en blocs de la matrice de u_A par rapport à cette base , la formule de calcul d'un déterminant par blocs montre que

(7) $$\det(u_A)=\det(M_{\det(u)})=N_{F/A}(\det(u))$$

(Au concours : remplacer ces quelques lignes par trois pages sur les relations entre les algèbres extérieures de E sur F et sur A).

En appliquant ceci à $E[X]$, on obtient la formule suivante ~~EXEMPLE~~ reliant les polynômes caractéristiques

(8) $$\det(X.1-u_A)=\det(M_{\det(X.1-u)})=N_{F[X]/A[X]}(\det(X.1-u)) .$$

Supposons maintenant que E soit une algèbre commutative sur F , et prenons $u=M_z$ où $z\in E$. Il résulte aussitôt de (7) que l'on a

(9) $$N_{E/A}(z)=N_{F/A}(N_{E/F}(z)) .$$

Pour les traces , on regarde encore la décomposition par blocs : si $u(e_j)=\sum_k u_{jk}e_k$ $(u_{jk}\in F)$, la matrice de u_A est celle des $M_{u_{jk}}$; d'où

(7') $$Tr(u_A)=\sum_j Tr(M_{u_{jj}})=Tr(M_{Tr(u)})$$

(9') $Tr_{E/A}(z)=Tr_{F/A}(Tr_{E/F}(z))$.

2 . Prolongement d'une valeur absolue à une extension algébrique .

Soient K' un corps , f' une valeur absolue sur K' , K une extension algébrique finie de degré n de K' . Il existe une valeur absolue f de K prolongeant f' : si f' est valuative , on l'a démontré au chap. des valuations ; sinon $K' \subset C$ et l'on peut plonger K dans C qui est algébriquement clos . Lorsque K' est complet , ce prolongement f est unique et K est complet pour la topologie définie par f : en effet cette topologie est nécessairement celle de K'^n (Esp. vect.top.,chap.I,§ 2) , et l'on applique la prop.5 du § 1 . En prolongeant f à l'extension normale de K' engendrée par K , on voit que , pour tout $a \in K$, on a $f(a)=f'(N_{K/K'}(a))^{1/n}$ (la vérification directe du fait que cette formule définit bien une valeur absolue n'est pas difficile) . Lorsque K' est quelconque , nous allons compléter (c'est le cas de le dire!) ce qui a été dit au chapitre des valuations .

Soit $\hat{K}'$ le complété de K' pour f' . Formons l'algèbre étendue $K_{(\hat{K}')}=T$. Soit f_i un prolongement de f' à K ; notons $\hat{K}_i$ le complété de K pour f_i ; $\hat{K}_i$ est une extension algébrique finie de $\hat{K}'$ engendrée par K , car $\hat{K}'(K)$ est complet (Esp. vect.top.,chap.I,§ 2) et contient K . Ainsi $\hat{K}_i=\hat{K}'(K)=\hat{K}'[K]$ (Alg.,chap.V) est un corps quotient de l'algèbre étendue T , soit T/M_i ; et l'idéal maximal M_i est déterminé de façon unique par f_i . Réciproquement , pour tout idéal maximal M de T , le corps quotient T/M contient des sous-corps U' et V canoniquement isomorphes à $\hat{K}'$ et K , et est engendré par ceux-ci ; c'est donc une extension algébrique finie du corps complet U' , et partant peut être muni d'une valeur absolue (unique) prolongeant celle de U' ; en transportant à K la restriction de cette valeur absolue à V , on en conclut que T/M est obtenu par la méthode indiquée . Donc :

PROPOSITION 1 .- Soient K' un corps , f' une valeur absolue sur K' , $\hat{K}'$ son-

complété , et K une extension algébrique finie de K' . Les prolongements distincts f_i de f' à K sont en correspondance biunivoque avec les corps quotients T/M_i de l'algèbre étendue $T=K_{(\hat{K}')}$, le complété $\hat{K}_i$ de K pour f_i étant isomorphe à T/M_i .

Lorsque K (ou $\hat{K}'$) est une extension séparable de K' (ce qui sera désormais supposé sauf mention expresse du contraire) , l'algèbre T est somposée directe de sous-corps (chap. des anneaux primitifs) , qui sont respectivement isomorphes aux $\hat{K}_i$ (auxquels nous les identifierons désormais) . D'où

(10) $$[K:K']=\sum_i [\hat{K}_i:\hat{K}'] .$$

D'autre part , pour $z \in K$, il résulte des formules du n°1 que l'on a (en posant $z=(z_i)$, $z_i \in \hat{K}_i$) :

(11) Le polynôme caractéristique de z sur K' est égal au produit des polynômes caractéristiques des z_i sur $\hat{K}'$.

(11') Idem pour les polynômes minimaux (prendre $K=K'(z)$)

(12) $$Tr_{K/K'}(z)=Tr_{T/\hat{K}'}(z)=\sum_i Tr_{\hat{K}_i/\hat{K}'}(z_i)$$

(13) $$N_{K/K'}(z)=N_{T/\hat{K}'}(z)=\prod_i N_{\hat{K}_i/\hat{K}'}(z_i) .$$

Remarque .- Lorsque $K=K'(z)$ est une extension monogène , on a $K=K'[X]/(g(X))$ (g : polynôme minimal de z sur K') , et $T=\hat{K}'[X]/(g(X))$. Alors la décomposition de T en composé direct de sous-corps $\hat{K}_i$ correspond à la décomposition de $g(X)$ en facteurs irréductibles sur $\hat{K}'$. On en déduit aussitôt (11) , (12) et (13) dans ce cas .

3 . Cas d'une valuation discrète .

Nous supposerons ici que K' est muni d'une valuation discrète v' (alors $f'(x)=e^{-sv(x)}$) , et que Z est le groupe des ordres de v' . Nous noterons A' et P' l'anneau et l'idéal de v' , U' le groupe multiplicatif des éléments inversibles (ou unités) de A' , $k'=A'/P'$ le corps des valeurs de v' . Soient K une extension algébrique finie de K' , (v_i) les prolongements de v' à K , A_i, P_i, U_i l'anneau , l'idéal , le groupe des unités de v_i , $k_i=A_i/P_i$ son corps des valeurs ; on pose $f_i=[k_i:k']$ (degré résiduel) ; le groupe des ordres de v_i est de la forme $(1/e_i)Z$ (e_i : indice de ramification de v_i sur K') . Posons enfin $n=[K:K']$, $n_i=[\hat{K}_i:K']$. Rappelons (chap. des valuations) que $\bigcap_i A_i$ est la fermeture inté-

grale de A' dans K (= anneau des éléments de K qui sont entiers sur A').

Lorsque K est complet, le prolongement v de v' à K est unique ; nous supprimons alors les indices i.

PROPOSITION 2.- Soient K' un corps complet pour la valuation discrète v', K une extension algébrique finie de K', v l'unique prolongement de v' à K, p une uniformisante pour v (=générateur de l'idéal P de v =élément d'ordre 1/e pour v), (a_j) des représentants dans A des éléments d'une base de k sur k'. Alors les $(a_j p^k)$ $(0 \leqslant k \leqslant e-1)$ forment une base de A sur A' (donc de K sur K').

Indépendance linéaire : si $\sum_{jk} b'_{jk} a_j p^k = 0$ $(b'_{jk} \in A')$, il y a au moins deux termes de cette somme dont l'ordre pour v est minimum (chap. des valuations) ; alors l'ordre des b'_{jk} correspondants est minimum puisque $0 \leqslant k \leqslant e-1$, et l'exposant k y est minimum ; on met alors ce p^k en facteur ; par une mise en facteur dans les $\sum_i b'_{ij}$ on peut supposer que l'ordre minimum des b'_{ij} est 0 ; et il suffit de réduire modulo P.

Les $(a_j p^k)$ engendrent A : comme la topologie de A est engendrée par les (AP'^s) il suffit de montrer que les classes des $a_j p^k$ mod.AP' $(=P^e)$ engendrent A/P^e sur A'/P' (en vertu de la prop.6, § 3 du chap. d'Algèbre locale) ; or, k étant fixé, il est clair par homothétie que les classes des $a_j p^k$ mod.P^{k+1} engendrent P^k/P^{k+1} sur A'/P'. D'où la conclusion.

COROLLAIRE.- Si K' est complet, on a n=ef.

Rappelons l'important résultat suivant (Alg.locale, § 2, th.2) :

THEOREME 1 ("lemme de Hensel").- Soient K un corps complet pour une valuation discrète v, A et P l'anneau et l'idéal de v ; f(X) un polynôme de degré n sur A, γ et γ' des polynômes sur A/P tels que $\gamma\gamma'$ soit le polynôme $\bar{f}(X)$ obtenu à partir de f(X) par réduction mod.P des coefficients, et que γ et γ' soient étrangers. Il existe alors des polynomes g et g' sur A, tels que f=gg', et que γ et γ' soient obtenus à partir de g et g' par réduction mod.P de leurs coefficients.

COROLLAIRE 1.- Si f est un polynôme irréductible sur A, $\bar{f}$ est puissance d'un polynôme irréductible sur A/P.

NSR073

COROLLAIRE 2 .- Si f est un polynôme sur A tel que $\bar{f}$ ait une racine simple α dans A/P , il existe dans A une racine simple a de f telle que α soit la classe de a mod.P .

Remarque : forme Krasner du lemme de Hensel .
Soient K un corps complet pour une valuation v , K' un sous-corps de K fini sous K , a un élément de K séparable sur K' et tel que les conjugués a_i de a sur K' appartiennent à K . Si b est un élément de K tel que $v(b-a) > v(b-a_i)$ pour tout $a_i \neq a$, alors $K'(a) \subset K'(b)$.
Démonstration (indépendante de Hensel) : les conjugués de b-a sur K'(b) sont parmi les $b-a_i$; comme ils doivent tous avoir le même ordre pour v (en vertu de l'unicité de v) , ils se réduisent à b-a ; donc $b-a \in K'(b)$ en vertu de la séparabilité .
On déduit de ceci le cor.2 de Hensel (en se plaçant dans le corps des racines de f(X) et en prenant pour b un représentant dans K de α) puis Hensel lui-même par un raisonnement simple de théorie de Galois .

Etant donné un élément z d'un surcorps K de K' , nous noterons $m_{z,K'}(X)$ et $c_{z,K/K'}(X)$ le polynôme minimal de z sur K' et le polynôme caractéristique sur K' de z considéré comme élément de K . Notons enfin h l'homomorphisme canonique de A sur A/P . On a , si $z \in A$

(14) $h(c_{z,K/K'}(X)) = (c_{h(z);k/k'}(X))^e$

(15) $h(\mathrm{Tr}_{K/K'}(z)) = e.\mathrm{Tr}_{k/k'}(h(z))$, $h(N_{K/K'}(z)) = (N_{k/k'}(h(z))^e$.

En effet (15) se déduit aussitôt de (14) . D'après le lemme de Hensel (cor.1) $h(m_{z,K'}(X))$ est une puissance de $m_{h(z),k'}(X)$, l'exposant étant égal à l'indice de ramification de K'(z) sur K' en vertu du cor. à la prop.2 . On en déduit (15) en remarquant que $c_{z,K/K'}(X) = (m_{z,K'}(X))^{n/[K'(z):K']}$ et $c_{h(z),k/k'} = (m_{h(z),k'}(X))^{f/[k'(z):k']}$.

Etudions maintenant les extensions non ramifiées de K' , c'est-à-dire celles telles que e=1 (ou f=n) . Etant donnée une sous-extension séparable k" du corps des valeurs k , il existe une sous-extension non ramifiée K" de K ayant k" pour corps des valeurs : en effet , en posant $k" = k'(\bar{z})$, on relève $m_{\bar{z},k'}(X)$ en un polynôme unitaire g(X) de degré $[k":k']$ sur A ; celui-ci est irréductible et admet une racine $z \in K$ (cor.2 du lemme de Hensel) ; on prend $K" = K'(z)$. Dans ces conditions la sous-extension non ramifiée K" est unique : en effet le polynôme

$g(X)$ a une racine z_1 telle que $h(z_1)=\bar{z}$ dans toute sous-extension de ~~M~~ K dont le corps des valeurs contient $\bar{z}$; d'où $z=z_1$ car $\bar{z}$ est racine simple de $h(g(X))$. Le même raisonnement montre l'existence et l'unicité (à un isomorphisme près) d'une extension non ramifiée de K' ayant pour corps des valeurs une extension séparable donnée de k' (non nécessairement plongée dans un corps des valeurs k).

Contre-exemples variés lorsque k" n'est pas séparable .

On en déduit que , si K" et K_1'' sont des sous-extensions non ramifiées de K dont les corps des valeurs k" et k_1'' sont séparables sur k' , leur extension composée $K''(K_1'')$ est non ramifiée : en effet la sous-extension non ramifiée de K ayant $k''(k_1'')$ pour corps des valeurs contient K" et K_1'' en vertu de l'unicité.

Enfin , si K est une extension non ramifiée de K' telle que k soit séparable sur k' , et si F est une extension quelconque de K' , le corps composé K(F) est extension non ramifiée de F : soit en effet f le corps des valeurs de F ; comme k(f) est extension séparable de f , il existe une extension non ramifiée L de F contenue dans K(F) et ayant k(f) comme corps des valeurs ; comme k est une sous-extension séparable de k(f) , L contient K d'après l'unicité , et par suite L est identique à K(F) .

4 . Cas d'une valuation discrète (K' non complet) .

Nous reprenons les notations du début du n°3 , et nous supposons que K (ou $\hat{K}'$) est séparable sur K' ; alors l'algèbre étendue $T=K_{(\hat{K}')}$ est composée directe des complétés $\hat{K}_i$ de K . Comme un corps et son complété ont même groupe des ordres et même corps des valeurs , il résulte du cor. à la prop.2 que l'on a la relation des degrés

(16) $$n=\sum_i e_i f_i \quad .$$

D'autre part , pour $z \in K$, il résulte des formules (5) et (6) du n°1 que l'on a

(17) $$c_{z,K/K'}(X)=\prod_i (c_{z,\hat{K}_i/\hat{K}'}(X))$$

(18) $$Tr_{K/K'}(z)=\sum_i Tr_{\hat{K}_i/\hat{K}'}(z) \quad , \quad N_{K/K'}(z)=\prod_i N_{\hat{K}_i/\hat{K}'}(z) \quad .$$

On déduit de la seconde formule (18) et du fait que $v(N_{\hat{K}_i/\hat{K}'}(z))=n_i v_i(z)$ (démontré au début du n°2) que l'on a

(19) $$v(N_{K/K'}(z))=\sum_i n_i v_i(z) \quad .$$

Enfin les formules (14),(15),(17) et (18) donnent (en appelant h et h_i les homomorphismes canoniques de $\hat{A}'$ sur k' et de $\hat{A}_i$ sur k_i , et en notant z un élément de K entier sur A')

(20) $h(c_{z,K/K'}(X))=\prod_i (c_{h_i(z),k_i/k'}(X))^{e_i}$

(21) $h(\mathrm{Tr}_{K/K'}(z))=\sum_i e_i . \mathrm{Tr}_{k_i/k'}(h_i(z))$, $h(N_{K/K'}(z))=\prod_i (N_{k_i/k'}(h_i(z))^{e_i}$.

5 . Complément : les représentants multiplicatifs .

Soient K un corps complet pour une valuation discrète v , A et P l'anneau et l'idéal de v , k=A/P le corps des valeurs et h l'homomorphisme canonique de A sur k . Nous supposerons que k est un corps de caractéristique $p\neq 0$.

Lemme .- Si x et y sont des éléments de A tels que $x-y\in P^n$ $(n\geqslant 1)$, alors $x^{p^s}-y^{p^s}\in P^{n+s}$ pour tout entier $s>0$.

Par récurrence on se borne au cas s=1 ; alors x^p-y^p est le produit de x-y par une somme z de p termes dont chacun est congru à x^{p-1} mod.P^n ; alors $z\in P$ puisque p.1 est élément de P .

Etant donné un élément $\bar{a}$ de k , on appelle représentant multiplicatif de $\bar{a}$ un élément $a\in A$ tel que $h(a)=\bar{a}$ et que a admette quel que soit s une racine p^s-ème dans A . Pour que $\bar{a}$ ait un représentant multiplicatif dans A , il faut donc que, pour tout s , $\bar{a}$ admette une racine p^s-ème dans k . Cette condition est aussi suffisante : soit $\bar{a}_n$ la racine p^n-ème de $\bar{a}$ dans k , et soit $c_n\in A$ tel que $h(c_n)=\bar{a}_n$; fixons un entier q et considérons la suite $(c_{q+n}^{p^n})$; c'est une suite de Cauchy d'après le lemme ; notons a_q sa limite ; on vérifie aussitôt que pour $q'\geqslant q$, on a $a_{q'}^{p^{q'-q}}=a_q$; ainsi $a=a_0$ est un représentant multiplicatif de $\bar{a}$. D'autre part , lorsque $\bar{a}$ admet un représentant multiplicatif , celui-ci est unique : si a et b sont représentants multiplicatifs de $\bar{a}$, soient a_n et b_n des racines p^n-èmes de a et b dans A ; on a $b_n-a_n\in P$ puisque la racine p^n-ème de $\bar{a}$ est unique ; d'où $b-a\in P^n$ en vertu du lemme , et b=a puisque ceci a lieu pour tout n .

Toute cette théorie marche dans le cas où A est un anneau local complet , et où P est son idéal maximal .

Par conséquent , si $\bar{a}$ et $\bar{b}$ dans k ont a et b pour représentants multiplicatifs,

ab est le représentant multiplicatif de $\overline{ab}$, et , lorsque K est lui aussi de caractéristique p , a+b celui de $\overline{a}+\overline{b}$.

Lorsque k est parfait , tout élément de k admet un représentant multiplicatif Lorsque k est un corps fini avant q éléments , les représentants multiplicatifs ne sont autres que les racines (dans K) du polynôme X^q-X ; dans ce cas l'existence de ces q racines est aussi une conséquence immédiate du lemme de Hensel .

Lorsque K est de caractéristique p et que k est parfait , il résulte de ce qui précède que les représentants multiplicatifs constituent un sous-corps K_0 de K , isomorphe à k au moyen de h ($h(K_0)=k$) . D'ailleurs un tel "corps de représentants des classes mod.P" est , dans ce cas , nécessairement égal à K_0 en vertu de l'unicité des représentants multiplicatifs . K est alors isomorphe au corps des séries formelles à une indéterminée sur K_0 .

Remarque .- Lorsque K et k sont de caractéristique 0 , l'existence d'un "corps de représentants" se démontre facilement par zornification sur les sous-corps de A et utilisation de Hensel (cf.chapitre d'Algèbre locale) . Lorsque K et k sont de caractéristique $p\neq 0$ et k imparfait , on peut encore fabriquer un tel "corps de représentants" , mais c'est horriblement compliqué (et d'ailleurs sans grand intérêt). On peut aussi dire quelque chose dans le cas d'inégales caractéristiques (0 pour K ,p pour k) . Ceux que ça intéresse liront la thèse de I.S.Cohen (Trans.A.M.S.,1946) , ou le fascicule d'Algèbre locale du rédacteur (Mémorial).

6 . Complément : exponentielle et logarithme dans les corps complets .

Soit K un corps valué complet . On se propose de trouver des séries entières exp(X) et log(1+X) , convergentes dans un voisinage de 0 de K , et telles que exp(x+v)=exp(x)exp(y) et log(ab)=log a+log b . Un calcul formel élémentaire montre que , si on norme convenablement ces séries (c.a.d. à une multiplication près de X par une constante) , elles sont nécessairement de la forme :

(22) $\exp(X)=1+X+X^2/2!+\ldots+X^n/n!+\ldots$

(23) $\log(1+X)=X-X^2/2+X^3/3+\ldots+(-1)^{n-1}X^n/n+\ldots$

Ces formules montrent (hélas!) que de telles séries ne peuvent exister que si K est de caractéristique 0 , ce que nous supposerons dans ce n° .

Nous laisserons de côté le cas non valuatif , qui est relativement classique. Dans le cas valuatif , rappelons d'abord que , pour qu'une série soit commutativement convergente , il suffit que son terme général tende vers 0 .

Lorsque le corps des valeurs ~~K~~ k est de caractéristique 0 , on a $v(n!)=v(n)=0$; donc , pour que les séries (22) et (23) convergent , il faut et il suffit que $v(x)>0$; ainsi $\exp(x)$ et $\log(1+x)$ sont définies sur l'idéal P de la valuation v .

Examinons maintenant le cas où k est de caractéristique $p\neq 0$. On a alors $v(p)=e$ ("indice de ramification absolu") ($e\geqslant 1$) et $v(q)=0$ pour tout nombre premier $q\neq p$. Le nombre de facteurs premiers p figurant dans n est $\leqslant \log_p n$, donc $\underline{o}(n)$ Ainsi $nv(x)-\underline{o}(n)\leqslant v(x^n/n)\leqslant nv(x)$.

D'autre part , le nombre des facteurs premiers p figurant dans n! est $[n/p]+[n/p^2]+\ldots+[n/p^s]+\ldots \sim n/(p-1)$. Ainsi $v(x^n/n!)\sim nv(x)-e/(p-1)$.

Par conséquent le domaine de convergence de $\log(1+x)$ est P , et celui de $\exp(x)$ est P^m , où m est le plus petit entier $>e/(p-1)$ (on prend m=1 lorsque k est de caractéristique 0) .

Remarquons que $v(\exp(x)-1)=v(x)$ et que $v(\log(1+x))=v(x)$. Donc , pour tout x de P^m on peut former $\log(\exp(x))=\log(1+\exp(x)-1)$, et pour tout y de $1+P^m$ on peut former $\exp(\log(y))$. Un calcul formel facile (ou le principe de prolongement des identités) montre alors , en tenant compte de la convergence absolue des séries en cause , que

(24) $\log(\exp(x))=x$ pour $x\in P^m$

(25) $\exp(\log(y))=y$ pour $y\in 1+P^m$.

Ainsi les applications exp et log sont des isomorphismes , réciproques l'un de l'autre , entre le groupe additif P^m et le groupe multiplicatif $1+P^m$ (topologiques , et même métriques) .

Remarques .- 1) Pour $a\in 1+P$ et $x\in P^{m-1}$, on peut définir a^x par la formule $a^x=\exp(x.\log(a))$; identités habituelles .

2) Comme tout élément de $P^{m+v(n)}$ est de la forme nx avec $x\in P^m$, tout élément de $1+P^{m+v(n)}$ est une puissance n-ème dans K . En particulier , lorsque K est un corps P-adique (c.a.d. quand k est fini) $(K^*:K^{*n})$ est fini .

3) Si un élément ~~XE~~ y de $1+P$ est tel que $\log(y)=0$, on a $y^{p^{m-k}} \in 1+P^m$ en vertu du lemme du n°5 ; alors , comme la fonction log est biunivoque dans $1+P^m$, on a $y^{p^{m-1}}=1$. Réciproquement , un élément ~~XE~~ $y \in K$ tel que $y^{p^s}=1$ est bécessairement dans $1+P$ puisque k est de caractéristique p ; alors $p^s\log(v)=0$ et $\log(y)=0$; en ce cas , on a déjà $y^{p^{m-1}}=1$. Ceci montre auasi que les seules racines de l'unité qui sont dans $1+P$ sont les racines p^{n-1}-èmes de l'unité .

Supposons maintenant que K soit une extension galoisienne de K' , et soit s un K'-automorphisme de K . En vertu de l'unicité de la valuation de K prolongeant celle de K' , l'automorphisme s conserve les ordres , et est donc un automorphisme métrique de K . Donc , si $z \in K$

(26) $\exp(s(z))=s(\exp(z))$, $\log(s(z))=s(\log(z))$

(27) $\exp(\mathrm{Tr}(z))=N(\exp(z))$, $\log(N(z))=\mathrm{Tr}(\log(z))$.

7 . Calcul de $(K^*:K^{*n})$.

Examinons d'abord le cas où K est un corps P-adique . Remarquons que les racines de l'unité de K sont en nombre fini ; cela résulte de la remarque 3) du n°6 pour celles d'ordre puissance de p , du lemme de Hensel et du fait que le corps des valeurs de K est fini pour celles d'ordre étranger à p ; elles forment donc un groupe cyclique V d'ordre N . Choisissons un entier s multiple de n , de N , et d'une puissance suffisamment grande de p pour que , avec les notations du n°6 , on ait $U^s \subset 1+P^m$; alors la fonction logarithmique est définie et biunivoque sur U^s , et on a $(U^s:U^{sn})=(\log(U^s):n.\log(U^s))$. Comme le groupe $\log(U^s)$ est compact , c'est un module sur l'anneau A' des entiers p-adiques ; comme il contient une puissance de l'idéal P , $\log(U^s)$ et A sont des modules libres de même rang sur A' (cf.prop.2) : ce sont donc des A'-modules isomorphes , et on a $(\log(U^s):n.\log(U^s))=(A:nA)=q^{v(n)}$, où q désigne le nombre d'éléments du corps des valeurs de K . D'autre part , comme V est le groupe des racines s-èmes de l'unité de K , on a ~~XXXXXXXXXXXXXXXXXX~~ $(U:U^n)=(U:VU^n)(VU^n:U^n)=$ $=(U^s:U^{sn})(V:(V\cap U^n))$; mais comme V est le groupe de toutes les racines de l'unité de K , on a $V\cap U^n=V^n$; et , comme il est cyclique d'ordre N , le second indice est pgcd(n,N) ; d'où $(U:U^n)=q^{v(n)}\,\mathrm{pgcd}(n,N)$. Enfin , comme tout élément de K^{*n} a un ordre multiple de n , on a $(K^*:K^{*n})=n(U:U^n)$. En résumé :

(27 bis) $(K^*:K^{*n})=q^{v(n)}n.\mathrm{pgcd}(n,N)$.

Lorsque K contient les racines n-èmes de l'unité , on a donc

(27 ter) $(K^*:K^{*n})=n^2q^{v(n)}$.

Passons maintenant au second cas de locale compacité , c'est-à-dire celui où K est un corps de séries formelles $k((T))$ sur un corps fini k (n°5). Soit $q=p^r$ le nombre d'éléments de k . Lorsque n est multiple de p , $K^{*n}\cup(0)$ est contenu dans le sous-corps $K^p=k((T^p))$ de K , et K^{*n} ne peut être d'indice fini dans K^* . Nous supposerons donc n étranger à p . Or , pour qu'une série formelle soit une puissance n-ème , il faut que son terme de plus bas degré en soit une , et ceci suffit d'après Hensel puisque n n'est pas multiple de p . Ceci équivaut à : a) ordre multiple de n , b) premier coefficient puissance n-ème dans k ; comme k^* est cyclique d'ordre q-1 , on en déduit aussitôt

(27 quater) $(K^*:K^{*n})=n.\mathrm{pgcd}(n,q-1)$.

Si K contient les racines n-èmes de l'unité , q-1 est multiple de n et on a

(27 quinquiès) $(K^*:K^{*n})=n^2$.

On remarquera que (27 bis) et (27 ter) donnent (27 quater) et (27 quinquiès dans le cas où $\mathrm{pgcd}(n,p)=1$ (car $v(n)=0$).

§ 3 . Extensions galoisiennes des corps valués .

1 . Valuations conjuguées . Groupe de décomposition .

Soient K' un corps valué par une valuation v' , K une extension galoisienne finie de K' , G son groupe de Galois . Si v est une extension à K de la valuation v' , et si $s\in G$, $v\circ s$ est une valuation de K prolongeant v' ; on dit que v et $v\circ s$ sont des valuations conjuguées de K .

PROPOSITION 1 .- Toutes les valuations de K prolongeant v' sont conjuguées de l'une d'entre elles .

Soient v une valuation de K prolongeant v' , $v\circ s$ $(s\in G)$ ses conjuguées et w_i les valuations de K prolongeant v' et non équivalentes aux $v\circ s$. Il existe alor (§ 1,prop.6) $a\in K$ tel que $v(s(a))=0$ pour tout s et que $w_i(a)>0$ pour tout i . On a alors $v'(N(a))=v(\prod_{s\in G} s(a))=0$, et $v'(N(a))>0$ d'après la formule (19) (§ 2 n°4) ; contradiction .

Par conséquent et transport de structure , les degrés locaux f_i et les indices

NBR073

de ramification e_i sont tous égaux , pour tous les prolongements distincts v_i de v' . En appelant e et f leurs valeurs communes , et g le nombre des prolongements distincts de v' à K , on a

(28) $\quad n=efg$

car $n=\sum_i e_i f_i$ puisque K est séparable .

Soit v un prolongement de v' à K . Les éléments s de G tels que $v=v\circ s$ forment un sous-groupe G_v de G (vérification immédiate) , qui se nomme le groupe de décomposition de v . Le corps des invariants K_v de G_v a nom le corps de décomposition de v . Comme les divers prolongements de v' à K sont des valuations conjuguées , les divers groupes de décomposition sont conjugués , et les divers corps de décomposition itou . Le groupe G_v est d'ordre $n/g=ef$, et le corps K_v de degré g sur K' . La restriction de v à K_v n'admet pas d'autre prolongement à K que v . Lorsque K est une extension abélienne , les divers groupes (et corps) de décomposition sont égaux . On pourra donc parler du groupe et du corps de décomposition de la valuation v' .

PROPOSITION 2 .- Pour qu'un automorphisme $s\in G$ appartienne au groupe de décomposition G_v de v , il faut et il suffit qu'il soit continu pour la topologie définie par v ; c'est alors un automorphisme métrique de K .

Nécessité : évident . Suffisance : si s est continu , $\lim_{n\to\infty} x^n=0$ implique $\lim_{n\to\infty} s(x^n)=0$, donc $v'x)>0$ entraîne $v(s(x))>0$; le th. d'approximation montre alors que v et $v\circ s$ sont équivalentes (§ 1,prop.6) ; comme leurs restrictions à K' sont égales , elles sont égales . (On peut aussi prolonger s au complété , ce qui est plus simple) .

Par conséquent les automorphismes s G_v ne sont autres que ceux qui se prolongent au complété $\hat{K}_v$ de K pour v : en effet les automorphismes de $\hat{K}_v$ sont tous continus en vertu de l'unicité du prolongement des valuations d'un corps complet à une extension algébrique finie (§ 2,n°2) . En particulier , lorsque K' est complet , les groupes de décomposition sont tous égaux au groupe de Galois G de K .

N.B.: tout ceci s'applique aux valeurs absolues quelconques , sans y changer

grand chose .

Dans le cas général , le complété $\hat{K}'$, considéré comme plongé dans le complété $\hat{K}$ de K pour v , contient le corps de décomposition K_v , donc K_v a même corps des valeurs k' (pour v) que K' . D'autre part , le corps $\hat{K}$ est extension galoisienne (de degré n/g) de $\hat{K}'$, et son groupe de Galois est canoniquement isomorphe au groupe de décomposition G_v .

2 . Groupe d'inertie et groupes de ramification .

Soient K un corps , extension galoisienne de K' , v une valuation discrète de K , A,P et k son anneau , son idéal et son corps des valeurs , A',P' et k' ceux de la restriction v' de v à K' , et G le groupe de Galois de K . Les automorphismes $s \in G$ tels que $s(a)-a \in P$ (resp. $s(a)-a \in P^{n+1}$ pour $n \geqslant 1$) pour tout $a \in A$ appartiennent tous au groupe de décomposition G_v , puisque $s(A) \subset A$ pour un tel automorphisme . Ils forment , comme on le voit asinitrottant , un sous-groupe T (resp. V_n) de G_v , qui est invariant dans G_v puisque tout élément de G_v conserve les ordres ; le sous-groupe T (resp. V_n) est appelé le groupe d'inertie (resp. n-ème groupe de ramification) de v ; on a

$$G \supset G_v \supset T \supset V_1 \supset V_2 \supset \ldots \supset V_n \supset \ldots$$

L'intersection des V_n se réduit à (1) ; comme G est fini , on en déduit que $V_n=(1)$ pour n assez grand . Le corps des invariants de T (resp. V_n) s'appelle le corps d'inertie (resp. n-ème corps de ramification) de v et se note K_T (resp. K_{V_n}) : ce sont des extensions galoisiennes du corps de décomposition K_v ; on a

$$K' \subset K_v \subset K_T \subset K_{V_1} \subset K_{V_2} \subset \ldots \subset K_{V_n} \subset \ldots$$

et K_{V_n} est égal à K pour n assez grand .

Nous allons maintenant étudier la structure des groupes quotients $G_v/T, T/V_1, \ldots, V_i/V_{i+1}, \ldots$ qui sont les groupes de Galois de K_T sur K_v , de K_{V_1} sur K_T , .. de $K_{V_{i+1}}$ sur K_{V_i} , ...

PROPOSITION 3 .- L'extension k du corps des valeurs k' , quand elle est séparable , est galoisienne , et son groupe de Galois est canoniquement isomorphe à G_v/T .

En effet , un automorphisme $s \in G_v$ laisse A et P globalement invariants , et définit donc un automorphisme $\bar{s}$ de $k=A/P$. Le noyau de $s \to \bar{s}$ est évidemment le groupe d'inertie T . Le corps des invariants du groupe des automorphismes $\bar{s}$ contient évidemment k' . Réciproquement , si $\bar{x}$ est un élément de k invariant par les $\bar{s}$, et si $x \in A$ est un représentant de $\bar{x}$, on a $s(x)-x \in P$ pour tout $s \in G_v$. Alors le polynôme minimal F(X) de x sur le corps de décomposition K_v donne , par réduction mod.P , un polynôme de la forme $(X-\bar{x})^r$ à coefficients dans le corps des valeurs k' de K_v . Comme $\bar{x}$ est séparable sur k' , il en résulte que $\bar{x} \in k'$.

Remarque .- L'extension k de k' peut fort bien n'être pas séparable (exemple : $k'=F_2(X)$, $K'=k'((T))$, K= extension quadratique de K' définie par l'équation séparable $Y^2+TY+X=0$; alors k est l'extension radicielle de k' définie par l'équation $Y^2+X=0$). Le raisonnement ci-dessus montre cependant qu'elle est en tout cas normale et admet G_v/T pour groupe de Galois .

Toujours dans le cas où k est séparable sur k' , la prop.3 appliquée à K considéré comme extension galoisienne de K_T montre que k est le corps des valeurs de K_T .

En général le corps k est radiciel sur le corps des valeurs de K_T . L'exemple précédent montre qu'il peut en être distinct (le groupe d'inertie y est égal au groupe de Galois , mais e=1 , f=n=2 ; je me détourne avec horreur et dégoût...!)

Comme $[K_v:K_T]=f$ d'après la prop.3 , K_T est extension non ramifiée de K_v (c'est d'ailleurs la plus grande) , et K est extension complètement ramifiée de degré e de K_T (utiliser la formule n=ef). Résumons les résultats obtenus dans le tableau suivant (k étant supposé séparable sur k') :

Corps :	K'	K_v	K_T	K
Degré sur K' :	1	g	fg	efg
Corps des valeurs :	k'	k'	k	k
Groupe des ordres :	eZ	eZ	eZ	Z

Passons maintenant aux groupes de ramification , en supposant toujours que k

soit séparable sur k' .

Lemme .- Soit s un élément ($\neq 1$) du groupe d'inertie T ; lorsque a parcourt l'anneau A de v , le minimum de $v(s(a)-a)$ est atteint lorsque a est une uniformisante u pour v .

Soit $a \in A$ (on suppose v normée) . Comme K_T a même corps des valeurs k que K , il existe des b_i entiers dans K_T tels que

$$a \equiv b_0 + b_1 u + \ldots + b_n u^n \pmod{P^{n+1}}$$

Ceci montre aussitôt que a-s(a) est congru mod.P^{n+1} à un multiple de u-s(u) , donc que $v(a-s(a)) \geqslant \mathrm{Min}(n+1, v(u-s(u))$. Ceci montre que si $s \neq 1$, on a $s(u) \neq u$ (sinon $s(a)=a$ pour tout $a \in A$) , et d'autre part , en prenant $n=v(u-s(u))$, que $v(a-s(a)) \geqslant v(u-s(u))$ (on a l'égalité si et seulement si b_1 est une unité).

Par conséquent , avec les notations du lemme , $v(u-s(u))$ est , pour tout $s \neq 1$ de T , un entier $r(s) \geqslant 1$ tel que $v(a-s(a)) \geqslant r(s)$ pour tout $a \in A$. On pose $r(1) = +\infty$. Le n-ème groupe de ramification V_n n'est autre que l'ensemble des $s \in T$ tels que $r(s) \geqslant n+1$. Les entiers distincts $r_1 < r_2 < \ldots < r_m$ parmi les r(s) ($s \neq 1$) sont appelés les nombres de ramification de K pour v . Les seuls groupes de ramification deux à deux distincts sont donc

$$V_{r_1-1} \ (=T) \ , \ V_{r_2-1} \ , \ \ldots \ , \ V_{r_m-1} \ \text{ et } (1) \ ;$$

pour $r_i \leqslant n \leqslant r_{i+1}-1$, on a $V_n = V_{r_{i+1}-1}$.

PROPOSITION 4 .- Le groupe quotient T/V_1 est isomorphe à un sous-groupe multiplicatif du corps des valeurs k .

Soit u une uniformisante pour v . Notons h l'homomorphisme canonique de A sur $A/P=k$. Pour tout $s \in T$, considérons $h(s(u)/u)$. L'application $s \to h(s(u)/u)$ est un homomorphisme de T dans k (multiplicatif) : en effet $h(st(u)/u) = h(st(u)/s(u)) . h(s(u)/u)$ (puisque s et t conservent les ordres) $= h(s(t(u)/u)) . h(s(u)/u) = h(t(u)/u) . h(s(u)/u)$ puisque $t(u)/u \equiv s(t(u)/u) \pmod{P}$ étant donné que $s \in T$. Le noyau de cet homomorphisme est l'ensemble des s tels que $s(u)/u - 1 \in P$, c'est-à-dire tels que $s(u)-u \in P^2$; autrement dit c'est V_1 (lemme)

PROPOSITION 5 .- Pour tout $n \geqslant 1$, le groupe quotient V_n/V_{n+1} est isomorphe à un sous-groupe additif du corps des valeurs k .

Gardons les notations de la prop.4 . Pour tout $s \in V_n$, on a $s(u)-u \in P^{n+1}$. Considérons l'application $s \to h((s(u)-u)/u^{n+1})$. C'est un homomorphisme de V_n dans le groupe additif de k ; posons en effet $s(u)=u+a_s u^{n+1}$ ($a_s \in A$) ; alors $st(u)-u=s(t(u)-u)+s(u)-u=s(a_t)s(u^{n+1})+a_s u^{n+1} \equiv (a_s+a_t)u^{n+1}$ (mod. P^{n+2}) puisque $a_t-s(a_t) \equiv P^{n+1}$ et que $s(u^{n+1})-u^{n+1} \in P^{2n+1} \subset P^{n+2}$ (en tant que produit de $s(u)-u$ par un élément d'ordre n au moins). Le noyau de cet homomorphisme est l'ensemble des $s \in V_n$ tels que $s(u)-u \in P^{n+2}$, c'est-à-dire V_{n+1} en vertu du lemme .

3 . Conséquences .

a) Le groupe quotient T/V_1 est cyclique , puisqu'il est isomorphe à un groupe fini de racines de l'unité (prop.4) .

b) Lorsque k est de caractéristique 0 , les groupes V_n/V_{n+1} ($n \geqslant 1$) sont tous réduits à l'élément unité puisqu'ils sont finis (prop.5) ; alors T est un groupe cyclique . Lorsque k est de caractéristique p , les groupes V_n/V_{n+1} sont tous du type (p,p,...,p).

c) En général le groupe T est résoluble . Le groupe de Galois G lui-même est résoluble , lorsque $G=G_v$ et que G/T est résoluble , en particulier (prop.3) lorsque K' est un corps complet dont le corps des valeurs k' n'a que des extensions résolubles , par exemple si k' est un corps fini , ou algébriquement clos , ou ordonné maximal , ou encore un corps complet dont le corps des valeurs n'a que des extensions résolubles , par exemple un corps fini , ou un corps algébriquement clos , ou ordonné maximal , ou encore.... (Au concours : mettre cette phrase en musique afin qu'on puisse chanter la rengaine au prochain Congrès).

d) Ainsi toute extension galoisienne d'un corps valué localement compact est résoluble .

e) Une extension séparable non ramifiée K d'un corps valué localement compact K' est cyclique .

En effet le corps des valeurs k est extension cyclique de k' puisque k' est fini (Alg.,chap.V) . D'autre part relevons le polynôme minimal sur k' d'un élément primitif de k en un polynôme unitaire F de même degré n sur K' . D'a-

près Hensel ce polynôme F a ses n racines dans K , et celles-ci engendrent K puisque K est de degré n sur K' , et sont simples . Donc K est galoisienne ,et il suffit d'appliquer la prop.3 .

§ 4 . Grand fourbi global : diviseurs , répartitions , idèles .

1. Les axiomes .

Nous considérerons ici un corps K et une famille Φ de valeurs absolues de K qui soient , ou bien non valuatives , ou bien valuatives discrètes . Nous supposerons que l'axiome de finitude suivant est vérifié :

(F) Pour tout $x\neq 0$ de K , les $f\in\Phi$ telles que $f(x)\neq 1$ sont en nombre fini .

Nous dirons aussi que $f(x)=1$ pour presque toute f . Il résulte de (F) que, dans Φ , les valeurs absolues non valuatives sont en nombre fini (considérer $f(2)$).

Nous dirons que la famille Φ est complète si elle satisfait à l'axiome suivant

(C) Pour tout $x\neq 0$ de K et toute $f\in\Phi$ telle que $f(x)<1$, il existe $g\in\Phi$ telle que $g(x)>1$.

Lorsque la famille Φ est complète l'intersection des ensembles A_f (A_f : ensemble des $x\in K$ tels que $f(x)\leqslant 1$) où f parcourt Φ est égale à l'ensemble des $y\in K$ tels que $f(y)=1$ pour toute $f\in\Phi$. En particulier , lorsque toutes les valeurs absolues $f\in\Phi$ sont valuatives , les A_f sont des anneaux , et leur intersection est donc un sous-corps K_0 de K , appelé le corps des constantes de K relatif à la famille Φ . Lorsque Φ contient des valeurs absolues non valuatives les éléments $x\in K$ tels que $f(x)=1$ pour toute $f\in\Phi$ ne sont autres que les racines de l'unité contenues dans K .

Démonstration : on peut se borner au cas où les complétés de K par rapport aux f_i non valuatives sont tous isomorphes à C . Si x tel que $f(x)=1$ pour toute f n'est pas racine de l'unité , alors , pour tout i , x (considéré comme élément du complété C de K pour f_i) se met sous la forme $x=e(a_i)$,où a_i est irrationnel . D'après le th. de Kronecker (Top.gén.,chap.VII, § 1, prop.2) il existe des entiers q et p_i tels que $|qa_i-p_i|<1/8$ pour tout i . Alors on a $f_i(x^q-1)<1$ pour tout i . D'autre part $f(x^q-1)\leqslant 1$ pour toute f valuative , puisque $f(x)=1$. Ceci est contraire à l'axiome (C) .

Parmi les familles complètes , nous étudierons en particulier celles (dites fa-

milles d'Artin) qui satisfont à l'axiome suivant :

(A) Il existe des nombres réels $r(f)$ strictement positifs tels que, pour tout $x \neq 0$ de K, on ait la relation (dite "formule du produit")

$$\prod_{f \in \Phi} f(x)^{r(f)} = 1 \quad .$$

Cette relation a un sens d'après l'axiome (F). Il est clair que l'axiome (A) entraîne l'axiome (C). Dans le cas où toutes les f sont valuatives, et proviennent de valuations v, on utilise surtout la notation additive (le rédacteur, dont les préférences sont bien connues, se demande d'ailleurs pourquoi on ne l'utilise pas dans tous les cas !) ; la formule du produit s'écrit alors

$$\sum_{v} r(v)v(x) = 0$$

les $r(v)$ étant des nombres réels > 0 ; comme les v sont discrètes, on peut les supposer normées, et prendre alors les $r(v)$ rationnels.

Remarque.- Une famille complète de valeurs absolues non triviales est nécessairement infinie en vertu du th. d'approximation (§ 1, prop. 6).

2. Exemples.

a) Corps des nombres rationnels. On prend pour Φ la famille de toutes ses valeurs absolues (p-adiques $f_p(x) = p^{-(\text{exposant de } p \text{ dans } x)}$ et ordinaire). Alors les axiomes (F) et (A) sont vérifiés (avec des exposants $r(f)$ tous égaux à 1 : décomposition de x en facteurs premiers).

b) Corps de fractions rationnelles à une indéterminée $k(X)$. On prend pour Φ la famille de toutes les valuations (normées) de $k(X)$ qui sont triviales sur k : celles v_p correspondant aux polynômes unitaires irréductibles p de $k[X]$, et celle v_∞ définie par "degré du dénominateur - degré du numérateur". Les axiomes (F) et (A) sont vérifiés, avec, dans la "formule de la somme", les coefficients $r(v_p) = \deg p$ et $r(v_\infty) = 1$. Le corps des constantes est k. Lorsque k est algébriquement clos la formule de la somme s'énonce ainsi : le nombre de zéros d'une fraction rationnelle est égal au nombre de pôles.

c) Corps de fractions rationnelles à plusieurs indéterminées. On prend pour famille Φ de valuations de $K = k(X_1, \ldots, X_n)$ les valuations v_p correspondant aux polynômes unitaires irréductibles p de $k[X_1, \ldots, X_n]$ et la valuation v_∞ définie

NBR 073

par "deg.dénom.-deg.num." . Axiomes (F) et (A) vérifiés dans les mêmes conditions que dans b) . Mais il y a bien d'autres valuations de K triviales sur k que celles de Φ .

d) On prend pour K le corps des fractions d'un <u>anneau normal</u> [A], et pour Φ une famille de définition de A (par exemple la famille des valuations essentielles de A). L'axiome (F) est vérifié . Mais Φ n'est pas complète .

e)* On prend pour K le corps des fractions rationnelles (à corps de définition quelconque dans Ω) sur une <u>Variété Abstraite normale</u> [V] à la Weil , et pour Φ la famille des valuations v_A correspondant aux sous-variétés A de dimension dim(V)-1 de V . L'axiome (F) est vérifié . La famille Φ est complète lorsque V est complète (réciproque fausse : enlever d'une Variété complète V une sous-variété de dimension $\leqslant$dim(V)-2) . Il y a une formule de la somme pour les Variétés projectives (Bezout) , pour les Courbes complètes , pour les Variétés abéliennes , et probablement aussi dans le cas général (intersecter par les courbes d'un système algébrique pas trop mal fichu).*

f) (Analogue algébrique du précédent) On prend pour K une extension de type fini d'un corps k , pour Φ une famille de valuations discrètes de K , triviales sur k , et satisfaisant aux conditions suivantes : 1) Il existe un recouvrement fini (Φ_i) de Φ tel que les Φ_i soient des complémentaires de parties finies de Φ ; 2) pour tout i , il existe un anneau normal A_i engendré par un nombre fini d'éléments sur k , et tel que les $v \in \Phi_i$ soient presque toutes les valuations essentielles de A_i ; 3) si P_i (resp. P_j) est un idéal premier de A_i (resp. A_j) tel que tous les idéaux premiers minimaux de A_i (resp. A_j) contenus dans P_i (resp. P_j) soient des centres de valuations $v \in \Phi_i$ (resp. Φ_j) , et s'il existe un idéal premier M de $A_i[A_j]$ tel que $M \cap A_i = P_i$ et $M \cap A_j = P_j$, alors les idéaux premiers minimaux de A_i (resp. A_j) contenus dans P_i (resp. P_j) sont les centres sur A_i (resp. A_j) des valuations d'une même partie de $\Phi_i \cap \Phi_j$.(Au concours : essayer de simplifier ces conditions ; 3) peut sembler baroque , mais est là pour assurer la birégularité des correspondances birationnelles aux en-

droits où Weil l'exige). L'axiome (F) est vérifié .

g) Passage à un sous-corps . Soient K un corps , Φ une famille de valaurs absolues de K , et K' un sous-corps de K . La famille Φ' des restrictions à K' des $f \in \Phi$ satisfait à (F) (resp. C),(A)) avec Φ .

h) Passage à une extension de degré fini . Soient K un corps , Φ une famille de valeurs absolues de K , et E une extension de degré fini n de K . On prend pour famille Ψ de valeurs absolues de E celles de tous les prolongements de toutes les $f \in \Phi$ à E . Alors lorsque Φ satisfait à (F) (resp. (C),(A)) , il en est de même de Ψ : la formule $f(N(x)) = \prod_{f_i \text{ prol.} f} (f_i(x))^{n_i}$ (§ 2)/ démontre aussitôt les assertions relatives à (C) et (A) ; pour (F) on peut se borner aux valeurs absolues valuatives de E , les autres étant en nombre fini ; pour $x \in E$, les coefficients du polynôme minimal de x sur K sont entiers pour presque tous les f valuatives de Φ ; donc x est entier pour presque tous les prolongements de celles-ci , c'est-à-dire pour presque toutes les g de Ψ ; comme il en est de même de $1/x$, (F) est vérifiée par Ψ .

3 . Diviseurs .

Soient K un corps , Φ une famille de valeurs absolues de K . On appelle diviseur de K (relatif à Φ) une application $f \to m(f)$ qui , à toute $f \in \Phi$, fait correspondre un nombre réel m(f) du sous-groupe additif $\overline{\log(f(K^*))}$, de telle sorte que presque tous les m(f) soient nuls . L'ensemble des diviseurs de K est évidemment muni d'une structure de groupe additif . En identifiant f avec le diviseur qui fait correspondre 1 à f et 0 à toute $g \neq f$, on peut donc écrire tout diviseur sous la forme $D = \sum_{f \in \Phi} m(f).f$. D'ordinaire on se borne au cas où Φ ne contient que des valeurs absolues valuatives discrètes , qu'on suppose normées ; alors les m(f) sont des entiers presque tous nuls . Nous ferons d'ailleurs cette convention pour toutes les valeurs absolues valuatives de Φ , même si Φ en contient d'autres .

Exemple : Diviseur d'un élément de K . Soit x un élément de K ; à toute $f \in \Phi$ faisons correspondre le nombre réel $-\log(f(x))$. En vertu de (F) , ceci définit un diviseur , appelé diviseur de x , et noté D(x) . On a $D(xy) = D(x) + D(y)$.

On dit qu'un diviseur $D=\sum m(f).f$ est positif (ou effectif) si tous les $m(f)$ sont positifs . D'où une relation d'ordre sur le groupe des diviseurs . L'axiome (C) exprime que le seul diviseur positif qui soit de la forme $D(x)$ ($x\in K^*$) est le diviseur 0 (correspondant à x constante ou racine de l'unité (n°1)).

Lorsque satisfait à une formule du produit $\prod_{f\in\Phi} f(x)^{r(f)}=1$, on appelle degré du diviseur $D=\sum m(f).f$ (relativement à cette formule du produit) le nombre réel $d(D)=\sum r(f)m(f)$. L'application $D\to d(D)$ est un homomorphisme croissant du groupe des diviseurs dans R . La formule du produit exprime que , pour tout $x\neq 0$ de K , D(x) est un diviseur de degré 0 .

4 . Répartitions . Idèles .

Soient K un corps , Φ une famille de valeurs absolues de K ; notons $\hat{K}_f$ le corps complété de K pour la topologie définie par $f\in\Phi$, et A l'anneau produit $A=\prod_{f\in\Phi}\hat{K}_f$. On appelle répartition sur K (relativement à Φ) un élément $X=(x_f)$ de A tel que $f(x_f)\leqslant 1$ pour presque toute f . Lorsque les f non valuatives de Φ sont en nombre fini (ce qui a lieu lorsque l'axiome (F) est vérifié) , les répartitions X forment un sous-anneau de A .

On appelle idèle sur K (relativement à Φ) un élément $I=(a_f)$ de A tel que $a_f\neq 0$ pour toute f et que $f(a_f)=1$ pour presque toute f . Les idèles I forment un sous-groupe multiplicatif J_K de A .

Exemple : répartitions principales et idèles principaux . Soit x un élément de K . L'élément (x_f) de A défini par $x_f=x$ pour toute f est (lorsque (F) est vérifié) une répartition , appelée répartition principale attachée à x , et notée X_x . Lorsque $x\neq 0$, X_x est un idèle , appelé idèle principal attaché à x . On a $X_{x+y}=X_x+X_y$ et $X_{xy}=X_xX_y$. On identifiera souvent K (resp. K^*) à un sous-corps (resp. un sous-groupe) de l'anneau des répartitions (resp. du groupe J_K des idèles) au moyen de l'application $x\to X_x$.

Etant donnée une répartition $X=(x_f)$ et un diviseur $D=\sum m(f).f$, on dit que X est un multiple de D si l'on a $-\log(f(x_f))\geqslant m(f)$ pour toute f . Lorsque $I=(a_f)$ est un idèle , l'application $f\to -\log(f(a_f))$ est un diviseur , appelé diviseur de l'idèle I , et noté D(I) . Les relations "I est un multiple de D" et

"$D(I)\geqslant D$" sont équivalentes . On a , pour tout $x\neq 0$ de K , $D(X_x)=D(x)$. On dit qu'un élément x de K est multiple d'un diviseur D , lorsque la répartition X_x est multiple de D , c'est-à-dire quand $D(x)\geqslant D$.

Lorsque toutes les $f\in\Phi$ sont valuatives , les répartitions qui sont multiples d'un diviseur donné D forment un module sur l'anneau intersection des anneaux de valuations correspondant aux $f\in\Phi$. Lorsque Φ vérifie l'axiome (C) (c'est-à-dire est complète) , les répartitions multiples de D forment donc un espace vectoriel V(D) sur le corps des constantes K_0 .

5 . Passage à une extension séparable de degré fini .

Soient K' un corps , $(f_{p'})=\Phi'$ une famille de valeurs absolues de K' qui soient ou bien non valuatives , ou bien valuatives discrètes . Nous les supposerons normées de la façon suivante : si $f_{p'}$ est non valuative , $f_{p'}$ est la restriction à K' de la valeur absolue usuelle de son complété R ou C ; si $f_{p'}$ est valuative on a $f_{p'}(x)=e^{-v_{p'}(x)}$, la valuation discrète $v_{p'}$ étant normée .

Soit maintenant K une extension algébrique finie de K' . Nous considérerons sur K la famille $\Phi=(f_p)$ des valeurs absolues obtenues en normant comme ci-dessus tous les prolongements à K des $f_{p'}$. Nous noterons $P\mid P'$ la relation "f_p est équivalente à un prolongement de $f_{p'}$". Nous noterons n le degré de K sur K' , $\hat{K}_p$ (resp. $\hat{K}'_{p'}$) le complété de K (resp. K') par rapport à f_p (resp. $f_{p'}$) , et n(P) le degré de $\hat{K}_p$ sur $\hat{K}'_{p'}$ (pour $P\mid P'$) . Nous noterons e(P) l'indice $(f_p(\hat{K}_p):f_p(\hat{K}'_{p'}))$, et f(P) le quotient n(P)/e(P) . Lorsque f_p est non valuative on a e(P)=1 et f(P)=n(P) . Lorsque f_p est valuative , e(P) est l'indice de ramification de f_p par rapport à K' , et f(P) en est le degré résiduel (§ 2,n°3). On a les relations

(29) $f_{p'}(x')=(f_p(x'))^{1/e(P)}$ pour $x'\in K'$ et $P\mid P'$.

(30) $f_{p'}(N_{K/K'}(x))=\prod_{P\mid P'}(f_p(x))^{f(P)}$ pour $x\in K$, et lorsque la relation des degrés $n=\sum_{P\mid P'} e(P)f(P)$ est vraie ; ceci a lieu pour tout P' lorsque K est séparable sur K' (§ 2).

Au lieu de $\sum_P m(f_p).f_p$ et $\sum_{P'} m(f_{p'}).f_{p'}$, nous écrirons $\sum_P m(P).P$ et $\sum_{P'} m(P').P'$ les diviseurs de K et K' .

Etant donné un diviseur $D'=\sum_{P'} m(P').P'$ de K' , nous appellerons extension de D' à K et noterons $\mathrm{Ext}_{K',K}(D')$ le diviseur de K défini par

(31) $\mathrm{Ext}_{K',K}(\sum_{P'} m(P').P')=\sum_{P'} m(P').(\sum_{P|P'} e(P).P)$.

Il est clair que $\mathrm{Ext}_{K',K}$ est un isomorphisme croissant du groupe ordonné des diviseurs de K' dans celui des diviseurs de K . En vertu de (29) on a

(32) $\mathrm{Ext}_{K',K}(D'(x'))=D(x')$ pour $x'\in K'$.

Si $K''\subset K'\subset K$, et pour tout diviseur D'' de K'', on a

(33) $\mathrm{Ext}_{K',K}(\mathrm{Ext}_{K'',K'}(D''))=\mathrm{Ext}_{K'',K}(D'')$.

Etant donné un diviseur $D=\sum_{P} m(P).P$ de K , nous appellerons norme de K à K' de D , et noterons $N_{K/K'}(D)$ le diviseur de K' défini par

(34) $N_{K/K'}(D)=\sum_{P'} (\sum_{P|P'} m(P)f(P)).P'$.

Il est clair que $N_{K/K'}$ est un homomorphisme croissant du groupe ordonné des diviseurs de K dans celui des diviseurs de K' . Comme $\sum_{P|P'} e(P)f(P)=n$, on voit que

(35) $N_{K/K'}(\mathrm{Ext}_{K',K}(D'))=n.D'$.

D'autre part (30) montre que l'on a

(36) $D'(N_{K/K'}(x))=N_{K/K'}(D(x))$ pour tout $x\in K$.

Enfin , si $K''\subset K'\in K$, et si D est un diviseur de K , on a

(37) $N_{K'/K''}(N_{K/K'}(D))=N_{K/K''}(D)$.

Supposons maintenant que Φ' satisfasse à une formule du produit $\prod_{P'} (f_{P'}(x'))^{r(P')}=1$. Alors , en vertu de (30) , Φ satisfait à la formule du produit $\prod_{P}(f_P(x))^{r(P)}=1$, où $r(P)=f(P)r(P')$ pour $P|P'$. D'après la définition des degrés des diviseurs , et comme $\sum_{P|P} e(P)f(P)=n$, on a , pour tout couple de diviseurs D' de K' et D de K :

(38) $d(\mathrm{Ext}_{K',K}(D'))=n.d(D')$ et $d(N_{K/K'}(D))=d(D)$.

Etant donnée une répartition $X'=(x'_{P'})$ $(x'_{P'}\in \hat{K}'_{P'})$, nous appellerons extension de X' à K et noterons $\mathrm{Ext}_{K',K}(X')$ la répartition sur K définie par $X=(x_P)$, où , pour $P|P'$, l'élément x_P de $\hat{K}_P$ est $x'_{P'}$. Il est clair que l'application $\mathrm{Ext}_{K',K}$ est un isomorphisme de l'anneau des répartitions sur K' dans ce-

lui des répartitions sur K . Pour un idèle I' de K' , $\mathrm{Ext}_{K',K}(I')$ est un idèle de K . En ce qui concerne les répartitions principales , l'extension à K de celle attachée à $x' \in K'$ est la répartition principale de K attachée à x' considéré comme élément de K . Pour un idèle I' de K' on a

(39) $\mathrm{Ext}_{K',K}(D'(I'))=D(\mathrm{Ext}_{K',K}(I'))$ ("extension du diviseur"="diviseur de l'extension") .

Enfin une formule évidente de transitivité .

Etant dnnnée une répartition $X=(x_p)$ sur K , on appelle trace et norme de K à K' de X , et on note $\mathrm{Tr}_{K/K'}(X)$ et $\mathrm{N}_{K/K'}(X)$ les répartitions $(a_{p'})$ et $(b_{p'})$ de K' définies par

(40) $a_{p'}=\sum_{p|p'} \mathrm{Tr}_{\hat{K}_p/\hat{K}'_{p'}}(x_p)$ et $b_{p'}=\prod_{p|p'} \mathrm{N}_{\hat{K}_p/\hat{K}'_{p'}}(x_p)$.

D'après les formules (12) et (13) (§ 2,n°2) les restrictions de $\mathrm{Tr}_{K/K'}$ et $\mathrm{N}_{K/K'}$ aux répartitions principales (identifiées aux éléments de K) coïncident avec les applications $\mathrm{Tr}_{K/K'}$ et $\mathrm{N}_{K/K'}$ définies pour les éléments de K . Il est clair que l'application $\mathrm{Tr}_{K/K'}$ est une application K'-linéaire de l'ensemble des répartitions de K dans celui de K' , pour leurs structures d'espaces vectoriels sur K' . La norme d'un idèle de K est un idèle de K' , et l'application $\mathrm{N}_{K/K'}$ est un homomorphisme du groupe multiplicatif J_K dans le groupe multiplicatif $J_{K'}$. On a enfin les formules suivantes (que l'on vérifie comme l'âne qui trotte) :

(41) $\mathrm{Tr}_{K/K'}(z.\mathrm{Ext}_{K',K}(X'))=(\mathrm{Tr}_{K/K'}(z)).X'$ pour $z \in K$.

(42) $\mathrm{Tr}_{K/K'}(\mathrm{Ext}_{K',K}(X'))=n.X'$.

(43) $\mathrm{N}_{K/K'}(\mathrm{Ext}_{K',K}(X'))=(X')^n$.

(44) $D'(\mathrm{N}_{K/K'}(I))=\mathrm{N}_{K/K'}(D(I))$ pour tout idèle I de K .

(45) formules de transitivité .

6 . Topologies sur l'espace des répartitions et sur le groupe des idèles .

Soit (G_α) une famille de groupes topologiques , (H_α) une famille se sous-groupes ouverts distingués de G_α. Sur le groupe produit $G=\prod_\alpha G_\alpha$ on met la topologie pour laquelle un système fondamental de voisinages de l'élément neutre est for-

NBK073

mé par les voisinages de l'élément neutre dans le groupe topologique produit $H=\prod_\alpha H_\alpha$. Ceci définit sur G une structure de groupe topologique appelé produit local des G_α (relativement aux H_α) . Cette topologie sur G est plus fine que la topologie produit ; donc les projections y sont continues . Lorsque les G_α sont tous localement compacts et les H_α presque tous compacts , le produit local G est un groupe localement compact .

Soit $\Phi=(f_p)$ une famille de valeurs absolues sur un corps K (l'axiome (F) étant vérifié) . Notons $\hat{K}_p$ le complété de K pour f_p . Pour chaque P nous noterons $\hat{A}_p$ le sous-anneau ouvert de $\hat{K}_p$ qui est $\hat{K}_p$ lui-même si f_p est non valuative , et l'anneau de valuation de $\hat{K}_p$ correspondant à f_p lorsque celle-ci est valuative .Considérons sur le groupe additif $A=\prod_p \hat{K}_p$ la structure de produit local des $\hat{K}_p$ (relativement aux $\hat{A}_p$) ; les sous-groupes additifs R_K des répartitions , et $\prod_p \hat{A}_p$ en sont des sous-groupes ouverts . La topologie du produit local A n'est pas en général compatible avec sa structure d'anneau ; mais comme pour toute répartition $X\in R_K$, il existe un voisinage V de 0 dans $\prod_p \hat{A}_p$ tel que $XV\subset\prod_p \hat{A}_p$, la topologie induite sur R_K par celle du produit local A est compatible avec la structure d'anneau de R_K . Un système fondamental de voisinages de 0 dans R_K est formé par les ensembles V(D) (V(D) : ensemble des répartitions multiples du diviseur D de K). Le corps K , considéré comme sous-corps de R_K , est muni de la topologie discrète lorsque Φ est complète (considérer V(D) lorsque D est un diviseur strictement positif) ; c'est donc un sous-corps fermé (Top.gén.,chap.III) de R_K . En particulier R_K est alors un espace vectoriel topologique sur K muni de la topologie discrète (et aussi sur tout sous-corps de K , par exemple le corps K_0 des constantes lorsqie toutes les f_p sont valuatives).

Lorsque K est un corps de nombres algébriques , ou un corps de fonctions algébriques d'une variable sur un corps fini , l'anneau R_K des répartitions de K est localement compact (et donc aussi l'espace quotient R_K/K) . Lorsque K est un corps de fonctions algébriques d'une variable sur un corps quelconque k (muni de la famille des valuations qui sont triviales sur k) , alors R_K (et R_K/K) sont des espaces vectoriels "localement linéairement compacts" sur k .

Considérons maintenant les groupes multiplicatifs topologiques $\hat{K}_P^*$, et dans chacun le sous-groupe ouvert $\hat{U}_P$, qui est $\hat{K}_P^*$ lui-même lorsque f_P est non valuative, et le groupe des unités de $\hat{A}_P$ lorsque f_P est valuative. Sur le produit $G=\prod_P \hat{K}_P^*$ considérons la structure de <u>produit local</u> relative aux $\hat{U}_P$. Le groupe J_K des idèles de K en est un sous-groupe ouvert. La topologie de G n'est <u>pas</u> la topologie induite par celle de l'anneau A, mais celle de J_K est la topologie induite par celle de l'anneau R_K des répartitions. Par conséquent un système fondamental de voisinages de 1 dans J_K est formé par les ensembles $J_{K,D}$ suivants : D étant un diviseur de K, $J_{K,D}$ est l'ensemble des idèles I tels que la répartition I-1 soit multiple de D. D'autre part, lorsque Φ est complète, on déduit de ce qui a été vu ci-dessus que K^* est un <u>sous-groupe discret et fermé</u> de J_K.

Remarques analogues sur la locale compacité de J_K.

C'est ici qu'on pourrait introduire les <u>différentielles</u>. Pour les corps de fonctions algébriques d'une variable, ce sont les <u>applications linéaires continues</u> de l'espace quotient R_K/K dans le corps des constantes K_0. Le rédacteur se demande ce que sont, en général, ces applications linéaires continues lorsque les f_P sont toutes valuatives, et tâchera d'y réfléchir. Dans la théorie du corps de classes (où J_K est localement compact), on appelle <u>différentielles</u> les caractères de J_K/K^*. Y a-t-il un moyen de court-circuiter les deux notions ?

Enfin il faut dérouler le <u>sorite</u> lorsqu'on a un corps K' et une extension algébrique finie K (séparable ?). Le rédacteur, qui en a marre d'avoir déroulé celui du n°4, se contente de mentionner les résultats :

a) $\mathrm{Ext}_{K',K}$ est un <u>isomorphisme</u> de l'anneau topologique $R_{K'}$ (resp. du groupe topologique J_K) <u>dans</u> l'anneau topologique R_K (resp. dans le groupe topologique J_K).

b) Les applications $\mathrm{Tr}_{K/K'}$ et $N_{K/K'}$ sont des applications <u>continues et ouvertes</u> de R_K dans $R_{K'}$ (et de J_K dans $J_{K'}$ pour $N_{K/K'}$) ; donc $\mathrm{Tr}_{K/K'}$ (resp. $N_{K/K'}$) est un <u>homomorphisme</u> additif (resp. multiplicatif) de R_K (resp. J_K) dans $R_{K'}$

(resp. $J_{K'}$) .

c) Par transposition de $Ext_{K',K}$ et $Tr_{K/K'}$ (pour les répartitions) , on obtient les opérations $Tr_{K/K'}$ et $Ext_{K',K}$ sur les différentielles additives de K et K' (avec en plus de la transposition , le passage d'un corps des constantes à l'autre). Pour les différentielles multiplicatives (= caractères de J_K/K^* et de $J_{K'}/K'^*$) on transpose les homomorphismes $Ext_{K',K}$ et $N_{K/K'}$ (pour les idèles). Il y a des tas de formules plaisantes et délectables , transposées de celles du n°4 , et dont on trouvera les paradigmes entre les pages 103 et 107 du bouquin de Chevallev sur les fonctions algébriques .

§ 5 . Différente et discriminant .

NB. Le rédacteur s'aperçoit que le rédacteur du § précédent a soigneusement caché à ses malheureux lecteurs que , lorsqu'on prend pour Φ la famille des valuations essentielles d'un anneau normal A (ayant K comme corps des fractions) , il correspond à tout diviseur D de K un idéal fractionnaire de K : l'idéal des x qui sont multiples de D , autrement dit , si $D=\sum_P m(P).P$, l'idéal des x tels que $v_p(x) \geqslant m(P)$ pour tout P . Lorsque A est un anneau de Dedekind, on obtient ainsi tous les idéaux fractionnaires de K , et de façon plus précise , on a un isomorphisme entre le groupe des diviseurs et celui des idéaux . Avec un anneau de Dedekind A' , et l'anneau A des entiers d'une extension séparable K du corps des fractions K' de A' , les opérations $Ext_{K',K}$ et $N_{K/K'}$ pour les diviseurs correspondent , pour les idéaux , aux opérations "idéal de A engendré par l'idéal $\mathfrak{a}'$ de A' " , et "idéal de A' engendré par les normes des éléments de l'idéal $\mathfrak{a}$ de A " .

1 . Introduction heuristique .

Soit K' un corps , Φ' une famille de valuations (discrètes) de K' satisfaisant à l'axiome de finitude (F) . Considérons une extension séparable K de K' et la famille Φ de tous les prolongements à K des $v \in \Phi'$. Nous nous proposons de chercher les valuations $w \in \Phi$ qui sont ramifiées par rapport à K' , c'est-à-dire dont l'indice de ramification par rapport à K' est >1 ; lorsque w est ramifiée , on dira que sa restriction à K' se ramifie dans K .

Regardonc d'abord le cas où $K=K'(z)$; soit $F(X)$ le polynôme minimal de z sur K . Considérons une valuation v' de K' , et ses prolongements v_i à K ; supposons z entier sur l'anneau de v' . La formule (20) (§ 2,n°4) donnant le polynôme obtenu à partir de $F(X)$ par réduction de ses coefficients modulo l'idéal de v' montre que , pour que v' se ramifie , il faut que ce polynôme $h(F(X))$ ait au moins une racine multiple (c'est-à-dire que , les (z_j) désignant les conjugués de z sur K' , l'élément $\prod_{j\neq k}(z_j-z_k)$ de K' appartienne à l'idéal de v'). D'autre part , la formule correspondante (14) , appliquée aux complétés de K' et de K pour v_i montre que , pour que v_i soit ramifiée , il faut que le polynôme déduit du polynôme minimal de z ($z\in\hat{K}_i$) sur $\hat{K}'$ ait une racine multiple , et , a fortiori , que $F'(z)$ appartienne à l'idéal de v_i . Ainsi s'introduisent les éléments $F'(z)$ de K et $N_{K/K'}(F'(z))$ de K' . On voit aussi que , lorsque Φ' vérifie l'axiome (F) de finitude , les valuations de K' qui se ramifient , et celles de K qui sont ramifiées , sont en nombre fini : en effet, les coefficients du polynôme minimal de z sont entiers pour presque toutes les v' , et on applique le raisonnement ci-dessus à ces valuations .

Considérons d'autre part la formule (21) :

$$h(Tr_{K/K'}(z))=\sum_i e_i\cdot Tr_{k_i/k'}(h_i(z))$$

Lorsque $v_i(z)>0$ pour tout i , on en déduit que $v'(Tr(z))>0$. En supposant les v' et v_i toutes normées , et en considérant $a'z$ où a' est un élément de K' tel que $v'(a')=-1$, on voit que , si y est un élément de K tel que $v_i(y)>-e_i$ pour tout i , on a $v'(Tr(y))\geqslant 0$. Donc , si l'une au moins des v_i est ramifiée , il y a des éléments y de K non entiers pour v_i dont la trace est un élément de K' entier pour v' . Nous sommes ainsi amenés à étudier les éléments de K dont la trace est entière .

2 . La différente comme idéal .

Soient A' un anneau normal $(v'_{p'})$ ses valuations essentielles , A l'anneau des entiers d'une extension séparable finie K du corps des fractions K' de A' , (v_p) les valuations essentielles de A . On appelle différente de A sur A' l'ensemble des x de K tels que $zx\in A$ pour tout z de K tel que $Tr_{K/K'}(zA)\subset A'$.

C'est évidemment un idéal entier de A .

Considérons en particulier les complétés $\hat{K}_P$ et $\hat{K}'_{P'}$ de K et K' pour v_P et pour $v'_{P'}$, équivalente à la restriction de v_P ; notons Tr_P la trace $Tr_{\hat{K}_P/\hat{K}'_{P'}}$, et $\hat{A}_P$ et $\hat{A}'_{P'}$, les anneaux d'entiers de ces complétés . La différente de $\hat{A}_P$ sur $\hat{A}'_{P'}$, est l'ensemble des x de $\hat{A}_P$ tels que $v_P(x)$ soit plus grand qu'un certain entier m(P) , appelé l'exposant différentiel de v_P . Cet entier est fini , car en vertu de la séparabilité , il existe un élément y de $\hat{K}_P$ de trace non nulle ; il suffit alors de multiplier y par un élément de $\hat{K}'_{P'}$, d'ordre suffisamment grand négatif pour obtenir un élément de trace non entière .

PROPOSITION 1 .- La différente de A est l'ensemble des $x \in K$ tels que $v_P(x) \geq m(P)$ pour tout P .

Il suffit de montrer que "$v_P(z) \geqslant -m(P)$ pour tout P" équivaut à "$Tr(zA) \subset A'$ ". Passons d'abord au "semi-local" ; notons $A_{P'}$ l'anneau $\bigcap_{P|P'} A_P$ des éléments entiers sur l'anneau $A'_{P'}$ de la valuation $v'_{P'}$; il est clair que "$Tr(zA_{P'}) \subset A'_{P'}$ pour tout P' " entraîne "$Tr(zA) \subset A'$ " (puisque A' est l'intersection des $A'_{P'}$). Réciproquement , supposons que $Tr(zA) \subset A'$ et qu'il existe P' et $a \in A_{P'}$ tel que $Tr(za) \notin A'_{P'}$; alors le th. d'approximation des anneaux normaux ~~KRHAPXI~~ (chap. des valuations) montre qu'il existe $b' \in A'$ tel que $v_{P'}(b')=0$ et que , pour $Q' \neq P'$, $v_{Q'}(b')$ soit assez grand pour que ab' appartienne à A ; alors , comme $Tr(zA) \subset A'$, on a $b'Tr(za)=Tr(zab') \in A'$ contrairement à l'hypothèse .

Pour passer de là au cas local , il faut montrer que "$Tr(zA_{P'}) \subset A'_{P'}$" équivaut à "$Tr(z\hat{A}_P) \subset \hat{A}'_{P'}$, quel que soit $P|P'$ " . La formule $Tr(y)=\sum_{P|P'} Tr_P(y)$ (§ 2,n°2, formule (12)) montre que la seconde assertion implique la première . Réciproquement , supposons que $Tr(zA_{P'}) \subset A'_{P'}$, et qu'il existe $P|P'$ et y dans $\hat{A}_P$ tels que $Tr_P(zy) \notin \hat{A}'_{P'}$. En approchant suffisamment y par $b \in A_P$ (pour v_P) , puis b par un élément de $A_{P'}$ tel que za soit entier pour ~~QX~~ $Q \neq P$ (ce qui est possible par le th. d'approximation) , on a $Tr_P(za) \notin \hat{A}'_{P'}$, $Tr_Q(za) \in \hat{A}'_{P'}$ pour $Q \neq P$, et $Tr(za) \in A'_{P'}$, contrairement à la formule rappelée .

PROPOSITION 2 .- On a $m(P) \geqslant e(P)-1$. Pour qu'il y ait égalité , il faut et il suffit que e(P) ne soit pas multiple de la caractéristique p du corps des va-

leurs k_P de v_P et que celui-ci soit séparable sur le corps des valeurs $k'_{P'}$ de $v'_{P'}$.

Supprimons les indices P et P' pour la démonstration . Notons h l'homomorphisme canonique de A sur k . Nous allons utiliser la formule $h(Tr(y))=e.Tr(h(y))$ $(y\in A)$. Soit u' une uniformisante pour v' ; on a v(u')=e . Pour z tel que $v(z)\geqslant -e+1$, on a $v(zu')\geqslant 1$, donc $h(Tr(zu'))=0$, donc $v(Tr(zu'))=v(u'Tr(z))=$ $=e+v(Tr(z))\geqslant e$; cela montre que $Tr(z)\in A'$, d'où l'inégalité . Lorsque k est séparable sur k' , il existe $\bar{y}$ dans k de trace non nulle dans k' ; prenons y tel que $h(y)=\bar{y}$; c'est une unité ; si e n'est pas multiple de p , la formule $h(Tr(y))=e.Tr(h(y))\neq 0$ montre aussitôt que l'élément y/u' (d'ordre -e) est de trace non entière ; d'où l'égalité e=m-1 dans ce cas . Réciproquement , l'existence d'un élément z d'ordre -e et de trace non entière implique , en posant y=zu' , l'existence d'une unité y telle que $h(Tr(y))\neq 0$, c'est-à-dire de $\bar{y}$ dans k tel que $e.Tr(\bar{y})\neq 0$; ceci implique $Tr(\bar{y})\neq 0$, d'où la séparabilité , - et aussi que e n'est pas multiple de p .

COROLLAIRE .- Lorsque le corps des valeurs $k'_{P'}$ de $v'_{P'}$ est parfait , les relations $e(P)>1$ et $m(P)>0$ sont équivalentes .

3 . Propriétés de finitude . Différente et discriminant comme diviseurs .

PROPOSITION 3 .- Soient K' un corps valué complet , K une extension séparable finie de K' , A' et A les anneaux de valuations de K' et K , y un élément de A tel que K'(y)=K , et F(X) le polynôme minimal de y sur K' . On a alors $v(F'(y))\geqslant m(P)$. Pour qu'il y ait égalité , il faut et il suffit que $1,y,\ldots,y^{n-1}$ $(n=[K:K'])$ forment une base de A sur A' .

Soit z un élément de K . Ecrivons z=g(y) , où g est un polynôme de degré $\leqslant n-1$ sur K' . Si les y_i $(1\leqslant i\leqslant n)$ sont les conjugués de y sur K' , on a , en vertu de la formule d'interpolation de Lagrange

$$g(X)=\sum_i g(y_i)F(X)/(F'(y_i)(X-y_i))=Tr(zF(X)/(F'(y)(X-y)))$$

(la trace d'un polynôme étant définie par coefficients) . Or , F(X)/(X-y) a ses coefficients entiers . Si $v(z/F'(y))\geqslant -m(P)$, les coefficients de g(X) sont entiers d'après la définition de m(P) ; donc z=g(y) est entier ; et l'on en

NBR 073

déduit que $v(F'(v)) \geqslant m(P)$. La relation $v(F'(y))=m(P)$ entraîne que , pour tout z entier , on a $z=g(v)$ où g est un polynôme à coefficients dans A' , c'est-à-dire que $1,v,\ldots,v^{n-1}$ forment une base de A sur A' . Réciproquement , si $1,y,\ldots y^{n-1}$ forment une base de A sur A' , on a $Tr(z/F'(y)) \in A'$ pour tout $z \in A$ (regarder le coefficient de X^{n-1} dans l'identité ci-dessus) ; donc $v(F'(y)) \leqslant m(P)$, et $v(F'(v))=m(P)$.

Conséquences et compléments .

a) Soient K' un corps , $(v'_{p'})$ une famille de valuations de K' satisfaisant à l'axiome de finitude (F) , K une extension séparable finie de K' , (v_p) la famille des valuations de K prolongeant les $v'_{p'}$. Notons y un élément primitif de K sur K' , et F(X) son polynôme minimal . Pour presque toute v_p , y est entier et F'(v) est une unité (en vertu de (F)) . Donc les exposants différentiels m(P) sont presque tous nuls . En particulier il n'y a qu'un nombre fini de v_p qui sont ramifiées par rapport à K' . D'autre part , les entiers m(P) définissent un diviseur $\sum_P m(P).P$ de K , appelé le diviseur différente de K sur K' (par rapport aux valuations données) ; on le note $\mathfrak{D}_{K/K'}$.

b) Lorsque $(v'_{p'})$ est la famille des valuations essentielles d'un anneau normal A' , et (v_p) la famille des valuations essentielles de l'anneau A des éléments de K qui sont entiers sur A' , l'ensemble des éléments de K qui sont multiples du diviseur différente n'est autre que l'idéal différente défini au n°1 (prop.1) .

c) Dans ce dernier cas , on a $D(F'(y)) \geqslant \mathfrak{D}_{K/K'}$ pour tout $y \in A$. Montrons que l'on a même (lorsque les corps des valeurs sont séparables)

(46) $$\mathfrak{D}_{K/K'} = \inf_{y \in A} D(F'(y)) .$$

Démonstration .- 1) Il s'agit d'abord de montrer que , dans les hypothèses de la prop.3 , il existe un élément y de A tel que $1,y,\ldots,y^{n-1}$ soit une base de A sur A' . Comme le corps des valeurs k est supposé séparable sur le corps des valeurs k' , il existe dans K une plus grande sous-extension non ramifiée T de K' (§ 2,n°3) . On a $[K:T]=e$, $[T:K']=f$, et le corps des valeurs de T est k . Soit a un élément de T obtenu en relevant un élément primitif de k sur k' , et soit u une uniformisante pour K . Les éléments $(a^i u^j)$ $(0 \leqslant i \leqslant f-1 , 0 \leqslant j \leqslant e-1)$ forment une base de A sur A'

(§ 2,n°3,prop.2). Lorsque e=1 , il suffira de prendre y=a . Sinon , on prendra y=a+u ; en effet , si G est le polynôme minimal (de degré f) de a sur K' , $G(y)=G(a+u)\equiv G'(a)u \pmod{P^2}$ est une uniformisante de K puisque G'(a) est une unité ; donc les $y^i(G(y))^j$ forment une base de A sur A' , donc aussi les y^s $(0\leqslant s\leqslant n-1)$, puisque y est entier sur A'.

2) Passons maintenant au global . Pour chaque v_P nous avons un élément $y_P\in A_{P'}$ tel que $v_P(H'_P(y_P))=m(P)$ (H_P désignant le polynôme minimal de y_P sur $K'_{P'}$). Il s'agit alors de trouver un élément y de A ,tel que $v_P(y-y_P)\geqslant 2$ (alors $v_P(F'_P(y)=m(P)$ d'après le 1° , F_P désignant le polynôme minimal de y sur $K'_{P'}$) , et que $v_P(F'(y))=v_P(F'_P(y))$, F désignant le polynôme minimal de y sur K' . Or (§ 2,n°2,formule (11')) , on a $F(X)=\prod_{Q|P'} F_Q(X)$; d'où $F'(y)=F'_P(y)\prod_{Q\neq P} F_Q(y)$. En prenant y tel que $v_Q(y)\geqslant 1$ pour $Q\neq P$ et $Q|P'$, on aura $v_P(F_Q(y))=v_P(y^{n(Q)})=0$ et notre condition sera réalisée . Or , le th. d'approximation et celui des anneaux normaux permettent de trouver un tel y .

Soient maintenant K' un corps , K une extension séparable de degré n de K' , et $(u_1,..,u_n)$ une base de K sur K' . On appelle discriminant de la base (u_i) l'élément $d(u_1,..,u_n)=d(u)=\det(\mathrm{Tr}_{K/K'}(u_iu_j))$. En appelant s_j les K'-isomorphismes de K dans une clôture algébrique de K , on a

(47) $d(u)=(\det(s_j(u_i))^2$.

Donc (Alg.,chap.V) $d(u)\neq 0$ puisque K est séparable . Lorsque y est élément primitif de K , on a (déterminant de Vandermonde)

(48) $d(1,y,..,y^{n-1})=\prod_{j\neq k}(s_j(y)-s_k(y))=N_{K/K'}(F'(y))$.

Formule de changement de base $(a'_{ij}\in K')$:

(49) $d(\sum_j a'_{ij}u_j)=(\det(a'_{ij}))^2.d(u)$.

En particulier , d'après la définition "hypercomplexe" de la norme :

(50) $d(yu_1,..,yu_n)=(N_{K/K'}(y))^2.d(u_1,..,u_n)$. $(y\in K)$.

PROPOSITION 4 .- Soient $v'_{P'}$ une valuation de K' , (v_P) les valuations de K la prolongeant , A' l'anneau de $v'_{P'}$, A la clôture intégrale de A' dans K (= intersection des anneaux des v_P) , et $u=(u_i)$ une base de K sur K' composée d'éléments de A . On a alors $v'(d(u))\geqslant \sum_{P|P'} m(P)f(P)$. Une condition nécessaire et suffisante d'égalité est que (u_i) soit une base de A sur A' .

Soit y un élément de K tel que $v_P(y)=-m(P)$ pour tout P (il en existe , dit le th. d'approximation) . Alors (prop.1) les éléments z tels que $\mathrm{Tr}(zA)\subset A'$

ne sont autres que ceux de Ay . Considérons le système linéaire en (v_j) : $Tr(u_i v_j)=\delta_{ij}$; en posant $v_j=\sum_s a'_{js}u_s$ $(a'_{js}\in K')$, il s'écrit $\sum_s a'_{js}Tr(u_i u_s)=\delta_{ij}$, et a donc une solution unique dans K puisque $d(u)\neq 0$. Pour $z=\sum_i b'_i u_i$ $(b'_i\in K')$ et $a'_j\in K'$, on a $Tr(z(\sum a'_j v_j))=\sum a'_j b'_j$. Supposons que (u_i) soit une base de A . Alors , pour que $\sum_j a'_j v_j$ appartienne à Ay , il faut et il suffit que $\sum_j a'_j b'_j$ appartienne à A' pour tout système d'entiers $b'_j\in A'$, c'est-à-dire que les a'_j soient entiers . Par conséquent , (v_j) est une base de Ay . Comme $u_i=\sum_j Tr(u_i u_j)v_j$ (calcul facile) , on a $d(u)d(v)=1$ (formule (49)) . Comme les v_j/y forment une base de A , les discriminants $d(u)$ et $d(v/y)$ sont associés (formule (49)) . Or $d(v/y)=d(v)/(N(y))^2$ (formule (50)) . Donc $(d(u)/N(y))^2$ et $d(u)/N(y)$ sont des unités , ce qui démontre que $v_{P'}(d(u))=\sum_{P|P'} m(P)f(P)$ lorsque (u_i) est une base de A .

Lorsque (u_i) est une base composée d'éléments de A , l'inégalité s'en déduit en vertu de (49) . Et , s'il y a égalité , il suffit de comparer avec une base de A et d'appliquer encore (49) pour résoudre le système linéaire . Notons que dans tout ceci , nous avons tacitement utilisé l'existence d'une base de A sur A' , ce qui résulte de la séparabilité (cf.chap. des valuations) .

Conséquences et compléments .

a) Existence (dans le cas global) du diviseur de K' $\sum_{P'}(\sum_{P|P'} m(P)f(P)).P'$. C'est la norme du diviseur différente $\mathfrak{D}_{K/K'}=\sum_P m(P).P$ (§ 4,n°5) . On l'appelle le diviseur discriminant et on le note $\mathfrak{d}_{K/K'}$.

b) Avec un anneau normal A' et sa clôture intégrale A dans une extension séparable , on a $D(d(u))\geqslant \mathfrak{d}_{K/K'}$ pour toute base $u=(u_i)$ de K sur K' composée d'éléments de A . On a même l'égalité

(52) $$\mathfrak{d}_{K/K'}=\inf(D(d(u)))\ ,$$

u parcourant les bases de K sur K' composées d'éléments de A . Il suffit en effet , pour chaque P' , de former une base $u=(u_i)$ de $A_{P'}$ sur $A'_{P'}$ composée d'éléments de A , ce qui est possible par multiplication des éléments d'une base (v_i) de $A_{P'}$ sur $A'_{P'}$ par un même élément $a'\in A'$ qui soit une unité en P' .

Remarquons aussi que , si (u_i) est une base de l'anneau normal A sur A' (il en existe lorsque A' est principal) , c'est aussi une base de $A_{P'}$ sur $A'_{P'}$ (vérification facile par multiplication par un élément de A' d'ordre assez grand pour les $Q' \neq P'$) . On a alors $D(d(u)) = \mathfrak{d}_{K/K'}$.

Enfin voici les formules de transitivité , où $K'' \subset K' \subset K$, K étant séparable de degré fini sur K" (donc aussi K sur K' et K' sur K") :

$$(53) \quad \mathfrak{D}_{K/K''} = \mathfrak{D}_{K/K'} \cdot \mathrm{Ext}_{K',K}(\mathfrak{D}_{K'/K''})$$

$$(54) \quad \mathfrak{d}_{K/K''} = N_{K'/K''}(\mathfrak{d}_{K/K'}) \cdot [K:K']\, \mathfrak{d}_{K'/K''} \quad .$$

En effet la formule des discriminants se déduit de celle des différentes par prise des $N_{K/K''}$ des deux membres et utilisation des formules (35) et (37) du § 4, n°5 . La formule des différentes se déduit aussitôt de la formule locale correspondante . Pour démontrer celle-ci , supposons K complet , appelons A, A', A" les anneaux de valuation de K, K', K" , $m(K,K')$, $m(K',K'')$ et $m(K,K'')$ les exposants différentiels des trois extensions , et $e(K,K')$ l'indice de ramification relatif à l'extension K de K' . Soient z un élément de K , et u' une uniformisante de K' . Les relations suivantes sont équivalentes :

$$v_P(z) \geqslant -m(K,K'') \qquad \mathrm{Tr}_{K/K''}(zA) \subset A'' \quad , \quad \mathrm{Tr}_{K'/K''}(\mathrm{Tr}_{K/K'}(zA)) \subset A''$$

$$\mathrm{Tr}_{K'/K''}(\mathrm{Tr}_{K/K'}(zA) \cdot A') \subset A'' \quad , \quad v_{P'}(\mathrm{Tr}_{K/K'}(zA)) \geqslant -m(K',K'')$$

$$\mathrm{Tr}_{K/K'}(zu'^{m(K',K'')}A) \subset A' \quad , \quad v_P(zu'^{m(K',K'')}) \geqslant -m(K,K')$$

$$v_P(z) \geqslant -m(K,K') - e(K,K')m(K',K'') \quad .$$

En comparant les relations extrêmes , on en déduit que l'on a $m(K,K'') = m(K,K') + e(K,K')m(K',K'')$. Ceci démontre (53) dans le cas local d'après la définition de Ext .

4 . Cas d'une extension galoisienne . Formule de Hilbert .

Soit K une extension galoisienne de K' , et soit v $(= v_P)$ une valuation de K. Notons K_Z, K_T, K_{V_j} les corps de décomposition , d'inertie , de j-ème ramification de v . Avec les notations du § 3 , on a $[K_Z:K'] = g$, $[K_T:K_Z] = f$, $[K:K_T] = e$; , otons n_j le degré $[K:K_{V_j}]$; alors $n_0 = e$. Soit y une uniformisante de K . Comme K est extension complètement ramifiée de K_{V_j} , la prop.3 montre que l'exposant différentiel $m(K,K_{V_j})$ est $\sum_s v(s(y)-y)$, où s parcourt l'ensemble des éléments

$\neq 1$ du j-ème groupe de ramification V_j . De même $m(K,K_{V_{j-1}})=\sum_{t\in V_{j-1},\, t\neq 1} v(t(y)-y)$. Par conséquent

$$m(K,K_{V_{j-1}})-m(K,K_{V_j})=\sum_{t\in V_{j-1},\, t\notin V_j} v(t(y)-y) \ .$$

Or , d'après la définition même de V_{j-1} et de V_j , et d'après le lemme du § 2, n°2 , on a , pour $t\in V_{j-1}$ et $t\notin V_j$, $v(t(y)-y)=j$. Par conséquent , on a $m(K,K_{V_{j-1}})-m(K,K_{V_j})=j(n_{j-1}-n_j)$. Comme $K=K_{V_m}$ pour m assez grand , on en déduit par addition que l'on a

$$m(K,K_T)=(n_0-n_1)+2(n_1-n_2)+\ldots+j(n_{j-1}-n_j)+\ldots$$

D'autre part , comme K_T est extension non ramifiée de K' , et si l'on suppose que le corps des valeurs k est séparable sur le corps des valeurs k' , la prop. 2 montre que l'exposant différentiel $m(K_T,K')$ est nul . Alors la formule de transitivité (53) donne

$$(55)\quad m(K,K')=n_0-n_1+2(n_1-n_2)+\ldots+j(n_{j-1}-n_j)+\ldots$$

Pour calculer à partir de là le coefficient de P' ($v_{P'}$ désignant la restriction de v_P à K') dans le diviseur discriminant $\mathfrak{d}_{K/K'}$, il suffit de remarquer que , pour les $g=n/ef$ valuations v_Q prolongeant $v_{P'}$, les exposants différentiels $m(Q)$ sont tous égaux , et les degrés résiduels $f(Q)$ tous égaux à f (par transport de structure!) . Donc , d'après la définition de $\mathfrak{d}_{K/K'}$, le coefficient de P' dans $\mathfrak{d}_{K/K'}$ est

$$(56)\quad ne^{-1}((n_0-n_1)+2(n_1-n_2)+\ldots+j(n_{j-1}-n_j)+\ldots) \ .$$

5 . Quelques propriétés des extensions composées .

Soient K' un corps , K_1 et K_2 deux extensions séparables de degré fini de K', et K leur corps composé . Considérons un sous-anneau normal A' de K' , ayant K' pour corps des fractions , et soient A_1, A_2 et A les fermetures intégrales de A' dans K_1, K_2 et K . L'anneau $A_1[A_2]=B$ est entier sur A' et admet K pour corps des fractions ; nous allons étudier si B est égal à A ; il revient au même d'étudier si B est intégralement clos . Nous supposerons que , pour toute valuation essentielle $v_{P'}$ de A' , les extensions de son corps des valeurs k'_P, sont séparables .

NBK073

Lorsque v_p, se ramifie dans K_1 et K_2, on peut avoir $B \neq A$. Exemple des extensions $K'(\sqrt{X})$ et $K'(\sqrt{2X})$ (ou $K'(\sqrt{X})$ et $K'(\sqrt[3]{X})$) du corps des séries formelles $K'=F_5((X))$: comme $\sqrt{2} \notin F_5$, on ne peut avoir $\sqrt{2}=\sum_i f_i(\sqrt{X})g_i(\sqrt{2X})$ où f_i et g_i sont des séries formelles à coefficients entiers ; idem avec $\sqrt[6]{X}$ dans l'autre exemple. Remarquons que, dans ces deux exemples, les extensions étudiées sont linéairement disjointes, et K' est complet.

Nous établirons d'abord quelques inégalités, valables dans le cas général. Soit v un élément primitif sur K' de A_2, F son polynôme minimal sur K', H son polynôme minimal sur K_1 ; on a $F(y)=G(y)H(y)$ (sur K_1) avec $G(y) \neq 0$; ainsi, dans le corps K, on a l'inégalité $D(F'(y)) \geqslant D(H'(y))$ entre diviseurs ; d'après la conséquence c) de la prop.3 (n°3) on en déduit

(a) $\mathfrak{D}_{K/K_1} \leqslant \mathrm{Ext}_{K_2,K}(\mathfrak{D}_{K_2/K'})$

D'où en prenant les normes

(b) $\mathfrak{d}_{K/K_1} \leqslant \mathrm{Ext}_{K',K_1}(\mathfrak{d}_{K_2/K'})$.

Appliquons la formule (53) de transitivité des différentes aux extensions (K,K_1,K') et (K,K_2,K') ; il vient, en tenant compte de (a)

(c) $\sup(\mathrm{Ext}_{K_1,K}(\mathfrak{D}_{K_1,K'}),\mathrm{Ext}_{K_2,K}(\mathfrak{D}_{K_2,K'})) \leqslant \mathfrak{D}_{K/K'} \leqslant$

$$\leqslant \mathrm{Ext}_{K_1,K}(\mathfrak{D}_{K_1,K'})+\mathrm{Ext}_{K_2,K}(\mathfrak{D}_{K_2,K'}) .$$

De même pour les discriminants (en tenant compte de quelques trivialités)

(d) $\sup([K:K_1]\mathfrak{d}_{K_1/K'},[K:K_2]\mathfrak{d}_{K_2/K'}) \leqslant \mathfrak{d}_{K/K'} \leqslant [K:K_1]\mathfrak{d}_{K_1/K'}+[K:K_2]\mathfrak{d}_{K_2/K'}$.

Lorsque K_1 est non ramifiée sur K', on a $\mathfrak{D}_{K_1/K'}=0$ et $\mathfrak{d}_{K_1/K'}=0$ puisque les extensions des corps des valeurs ont été supposées séparables ; alors (c) et (d) s'écrivent

(c') $\mathfrak{D}_{K/K'}=\mathrm{Ext}_{K_2,K}(\mathfrak{D}_{K_2/K'})$

(d') $\mathfrak{d}_{K/K'}=[K:K_2]\mathfrak{d}_{K_2/K'}$.

Plus généralement, lorsque les discriminants $\mathfrak{d}_{K_1/K'}$ et $\mathfrak{d}_{K_2/K'}$ sont <u>étrangers</u>, la théorie des groupes réticulés (<u>Alg.</u>, chap.VI) montre que (c) et (d) s'écrivent

(c") $\mathfrak{D}_{K/K'}=\mathrm{Ext}_{K_2,K}(\mathfrak{D}_{K_2/K'})+\mathrm{Ext}_{K_1,K}(\mathfrak{D}_{K_1/K'})$

(d") $\mathfrak{d}_{K/K'}=[K:K_2]\mathfrak{d}_{K_2/K'}+[K:K_1]\mathfrak{d}_{K_1/K'}$.

Supposons les discriminants <u>étrangers</u>, et les extensions K_1 et K_2 <u>linéaire-</u>

ment disjointes . Si (a_i) est une base de K_1 et (b_j) une base de K_2 composées d'entiers , les discriminant de la base "télescopique" $(a_i b_j)$ est $d(a)^{[K_2:K']} . d(b)^{[K_1:K']}$, comme on le voit en regardant des déterminants . Les formules (d") et (52) montrent alors que l'on a $\mathfrak{d}_{K/K'}=\inf(D(d(u)))$, u parcourant l'ensemble des bases télescopiques de K de la forme $(a_i b_j)$ $(a_i \in A_1 , b_j \in A_2)$ Ceci entraîne que l'on a $A=A_1[A_2]$ dans le cas "semi-local" (cf.prop.4) . Dans le cas général , on en déduit , en posant $B=A_1[A_2]$, que l'anneau $B_{p'}$ (ou plutôt $B_{A'-p'}$ avec la notation Weil) est intégralement clos ; donc B est intégralement clos (cf.chap. des valuations , § des entiers) . Par conséquent , on a $A=A_1[A_2] \simeq A_1 \otimes A_2$:

PROPOSITION 5 .- Lorsque K_1 et K_2 sont des extensions séparables linéairement disjointes , de discriminants étrangers , l'anneau des entiers de leur extension composée est isomorphe au produit tensoriel des anneaux des entiers de K_1 et K_2 .

Remarque .- Lorsque K' n'admet aucune extension non ramifiée (p.ex. K'=Q , K'=k(X)) , l'hypothèse que K_1 et K_2 aient leurs discriminants étrangers entraîne qu'elles sont linéairement disjointes . Soit en effet x un élément primitif de K_1 sur K' , et soit P(X) le polynôme minimal de x sur K_2 ; notons F le corps engendré sur K' par les coefficients de P(X) . Le corps F est contenu dans K_2 , et aussi dans l'extension galoisienne L de K' engendrée par K_1 . Le discriminant $\mathfrak{d}_{L/K'}$ est , d'après (d) , majoré par un multiple de $\mathfrak{d}_{K_1/K'}$; il est donc étranger à $\mathfrak{d}_{K_2/K'}$. La formule (54) de transitivité des discriminants montre alors que $\mathfrak{d}_{F/K'}$ est nul , donc que F=K' . Par conséquent K_1 et K_2 sont linéairement disjointes .

§ 6 . Corps de classes local .

La théorie du corps de classes local a pour objet d'étudier les extensions abéliennes des corps valués localement compacts .

Rappelons qu'un tel corps K est , soit R ou C , soit un corps valué complet pour une valeur absolue valuative ; en ce cas son corps des valeurs est fini , et son groupe des ordres est Z (§ 1,prop.4) . Si K est un corps de caractéris-

tique $p \neq 0$, les représentants multiplicatifs des éléments du corps des valeurs k forment un corps K_0 canoniquement isomorphe à k (§ 2,n°5) ; en notant u une uniformisante de K , K est isomorphe au corps des séries formelles $K_0((u))$. Lorsque K est de caractéristique 0 et k de caractéristique p , K contient le corps Q_p des nombres p-adiques (=complété de Q pour la valeur absolue p-adique; alors l'anneau de valuation A de K a pour corps des valeurs une extension finie de celui de l'anneau Z_p des entiers p-adiques ; comme Z_p est complet , il résulte de (Alg.locale, § 3,n°4,prop.6) que A est un Z_p-module de type fini ; en particulier K est extension finie de Q_p .

1 . Une inégalité fondamentale .

THÉORÈME 1 .- Soient K' un corps valué localement compact et K une extension galoisienne de degré fini n de K' ; on a alors

$$(K'^* : N_{K/K'}(K^*)) \leqslant n .$$

Le cas K'=R , K=C étant immédiat , nous supposerons que la valeur absolue de K est valuative . Alors K est une extension résoluble de K' (§ 3,n°3). Soit alors L une sous-extension galoisienne de K . En vertu de la transitivité des normes , on a

$$(K'^* : N_{K/K'}(K^*)) \leqslant (K'^* : N_{L/K'}(L^*)) . (L^* : N_{K/L}(K^*)) .$$

Il nous suffira donc de démontrer le th.1 dans les deux cas suivants :

a) K est extension non ramifiée de K' .

b) K est extension complètement ramifiée cyclique de degré premier de K' .

C'est ce qui résultera des deux propositions suivantes :

PROPOSITION 1 .- Soient K' un corps localement compact valué pour une valeur absolue valuative , et K une extension non ramifiée de degré n de K' ; alors en notant v la valuation normée de K , toute unité de K' est norme d'un élément de K , et $N_{K/K'}(K^*)$ est l'ensemble des éléments de K' dont l'ordre pour v est multiple de n ; en particulier le groupe quotient $K'^*/N_{K/K'}(K^*)$ est cyclique d'ordre n , et engendré par la classe des uniformisantes de K' . D'autre part, K est une extension cyclique de K' , dont le groupe de Galois est engendré par l'automorphisme (dit "de Frobenius") qui , par passage aux quotients (§ 3,prop.

3) donne le k'-automorphisme $x \to x^q$ du corps des valeurs k de K (k' corps des valeurs de K') (q désignant le nombre d'éléments du corps fini k') .

Le second groupe d'assertions a été démontré au § 3,n°3 . La formule $v(N(x)) = nv(x)$ montre que les normes ont des ordres multiples de n . Comme il existe des normes de tous les ordres multiples de n (des puissances n-èmes dans K' par exemple) , il ne reste plus qu'à montrer que toute unité a' de K' est une norme . Or , la classe $\bar{a}'$ de a' dans k' est norme d'un élément primitif $\bar{a}$ de k (Alg.,chap.V,§ 11,cor. du th.3) . Relevons le polynôme minimal $\bar{P}(X)$ de $\bar{a}$ sur k' en un polynôme unitaire P(X) sur K' dont le terme constant soit $(-1)^n a'$ Alors , d'après Hensel , P(X) a une racine a dans K , et l'on a N(a)=a' .

PROPOSITION 2 .- Soient K' un corps valué pour une valeur absolue valuative et localement compact , et K une extension cyclique complétement ramifiée de degré premier e de K' ; on a alors

$$(K'^{*} : N_{K/K'}(K^{*})) = e \ .$$

Soit v la valuation normée de K ; on a $v(K'^{*}) = e\mathbb{Z}$ par hypothèse . Comme il y a des éléments de $N(K^{*})$ de tous ordres (pour v) multiples de e , il nous suffira , en notant U et U' les groupes des unités de K et K' , de montrer que l'on a $(U' : N(U)) = e$.

Soit G le groupe de Galois de K . Pour tout $s \neq 1$ de G , le minimum d_s de $v(s(a)-a)$ (a parcourant l'anneau A de v) est atteint lorsqu'il existe un élément a' de K' tel que a-a' soit une uniformisante pour v (§ 3,n°2,lemme). Comme $d_{s^i} \geqslant d_s$ (puisque $s^2(a)-a = (s^2(a)-s(a))+(s(a)-a)$) et que tous les éléments $s \neq 1$ de G engendrent G (puisque K est cyclique de degré premier) , tous les d_s sont égaux à un même entier d . En prenant pour a une uniformisante y de K , le fait que $(1, y, \ldots, y^{e-1})$ est une base de A sur A' (§ 2,n°3,prop.2) et la théorie de la différente (§ 5,n°3,prop.3) montrent que (e-1)d est l'exposant différentiel de K sur K' .

Désignons par m un entier suffisamment grand de la forme je+d=(j+d)e-(e-1)d . Soit a une unité de K telle que $v(s(a)-a) = d$ pour tout $s \neq 1$ de G . Si b est un élément de K tel que $v(b-a) \geqslant m$, c'est une unité (si $m \geqslant 1$) , et comme

$N(a)-N(b) \equiv N(a).\sum_{s\in G}(s(a)-s(b))/s(a) = N(a).Tr((a-b)/a) \pmod{P^{2m}}$

on a $N(b) \in N(a)+P'^{j+d}$, puisque $m=(j+d)e-(e-1)d$, et que $v(Tr((a-b)/a)) \geq (j+d)e$ en vertu de la théorie de la différente (§ 5, n°3) .

Soit , réciproquement , b' un élément de la classe $N(a)+P'^{j+d}$, j étant suffisamment grand . Soit $F(X)=X^n+\ldots+(-1)^n N(a)$ le polynôme minimal de a sur K' ; posons $F_1(X)=F(X)+(-1)^n(b'-N(a))$, et considérons , dans la clôture algébrique de K' valuée par un prolongement (noté encore v) de v , une racine b de $F_1(X)$. Comme $F(b)=(-1)^n(N(a)-b')$, on a $v(F(b))=\sum_{s\in G} v(b-s(a)) \geq e(j+d)$. Or , les b-s(a) sont tous entiers sur A' . Donc il existe au moins un $s \in G$ tel que $v(b-s(a)) \geq j+d$. En prenant $j \geq 1$, on voit donc que b est plus proche de s(a) que tous les conjugués de s(a) . Ainsi la forme Krasner du lemme de Hensel montre (puisque a , et donc aussi b , est séparable sur K') que l'on a $K'(s(a))=K \subset K'(b)$, c'est-à-dire $K=K'(b)$ puisque b est de degré e sur K' . Par un changement de notation on peut supposer que l'on a $v(b-a) > d$; alors $v(b-s(a))=d$ pour tout $s \neq 1$ puisque $v(a-s(a))=d$; et l'on a $v(b-a) \geq e(j+d)-(e-1)d=ej+d=m$.

En résumé , <u>la classe de</u> a $\bmod.P^m$ ($m=ej+d$ assez grand) <u>a pour image par l'application</u> $N_{K/K'}$ <u>la classe de</u> N(a) $\bmod.P'^{j+d}$ <u>tout entière</u> . Par homothétie on en déduit que toute classe de U $\bmod.P^{ej+d}$ est appliquée par $N_{K/K'}$ <u>sur</u> une classe de U' $\bmod.P'^{j+d}$.

Or , q désignant le nombre d'éléments du corps des valeurs k de K' et K , il y a $(q-1)q^{ej+d-1}$ classes $\bmod.P^{ej+d}$ dans U , et $(q-1)q^{j+d-1}$ classes $\bmod.P'^{j+d}$ dans U' . Il ne nous reste plus qu'à <u>compter</u> combien de classes $\bmod.P^m$ ($m=ej+d$) ont la même image , c'est-à-dire , par homothétie , combien contiennent <u>des éléments de norme</u> 1 .

Or , comme K est <u>cyclique</u> , les éléments de norme 1 sont ceux de la forme s(z)/z d'après le th. normique de Hilbert (<u>Alg.</u>, chap.V, § 11, th.3). On a $(K^{*1-s}:U^{1-s})=e$ puisque le noyau de $K^* \to K^{*1-s}$ est K' , et que K^{*1-s}/U^{1-s} est donc isomorphe à K^*/UK'^* qui a e éléments (K étant complètement ramifiée) . Ainsi K^{*1-s} se compose de e classes compactes $\bmod.U^{1-s}$; alors les distances mutuelles de celles-ci sont non nulles et , pour m assez grand , deux classes dis-

tinctes mod.U^{1-s} ne peuvent rencontrer la même classe mod.P^m . Nous sommes donc ramenés à compter les classes mod.P^m qui rencontrent U^{1-s} .

Remarquons pour cela que si $s(x)/x$ et $s(y)/y$ appartiennent à la même classe mod.P^m , on a $s(x)/z \in 1+P^m$ avec $z=x/y$, c'est-à-dire $z-s(z) \in P^m$ puisqu'il s'agit d'unités . Prenons une uniformisante u de K , et posons $u_1=u$, $u_2=u.s(u)$, $u_3=u.s(u).s^2(u)$, ..., $u_n=u.s(u)...s^{n-1}(u)$; on a $u_n \in K'$ pour n multiple de e ; et $v(u_n)=n$. Ecrivons

$$z=a'_0+a'_1u+\ldots+a'_nu_n+\ldots \text{ , où } a'_n \in K' \text{ et } a'_n=0 \text{ si } a'_n \in P' \text{ ,}$$

et exprimons que $v(z-s(z)) \geqslant m$. Comme $u_n-s(u_n))=s(u)s^2(u)..s^{n-1}(u)(u-s^n(u))$ est d'ordre n+d-1 pour n non multiple de e , la relation $v(z-s(z)) \geqslant m$ entraîne que le plus petit indice n non multiple de e tel que $a'_n \neq 0$ est $\geqslant m-d+1$. Autrement dit , on a $z \in K'+P^{m-d+1}$. La réciproque étant évidente , les relations "$s(z)-z \in P^m$ " et "$z \in K'+P^{m-d+1}$ " sont équivalentes .

Or , dans U , il y a $(q-1)q^{m-d}$ classes mod.P^{m-d+1} , et , pour $m=je+d$, $(q-1)q^j$ sont représentées par des éléments de K' . Donc U^{1-s} rencontre $q^{m-d-j}=q^{(e-1)j}$ classes mod.P^m . Ainsi , des $(q-1)q^{ej+d-1}$ classes de U mod.P^{ej+d} , il y en a $q^{(e-1)j}.e$ qui ont pour image par $N_{K/K'}$ la même classe mod.P'^{j+d} . Par conséquent il y a , dans U' , $(q-1)q^{ej+d-1}/e.q^{(e-1)j}=(q-1)q^{j+d-1}/e$ classes mod.P'^{j+d} qui sont composées de normes d'éléments de U. Comme il y a en tout $(q-1)q^{j+d-1}$ classes mod.P'^{j+d} dans U' , on a $(U':N(U))=e$, et la prop.2 est démontrée . OUF!

2 . Cohomologie des groupes de Galois .

Soient L une extension galoisienne finie d'un corps quelconque K , $\mathcal{L}$ son groupe de Galois . Le groupe abélien $C^n(\mathcal{L},L^*)$ des applications de $\mathcal{L}^n$ dans le groupe multiplicatif L^* est appelé le groupe des cochaînes de dimension n de $\mathcal{L}$ à valeurs dans L^* ; on pose $C^0(\mathcal{L},L^*)=L^*$. Définissons un homomorphisme d de $C^n(\mathcal{L},L^*)$ dans $C^{n+1}(\mathcal{L},L^*)$ par la formule :

$$(56)\quad (df)(s_1,..,s_{n+1})=f(s_2,..,s_{n+1})^{s_1}\Big(\prod_{i=1}^{n} f(s_1,..,s_is_{i+1},..,s_{n+1})^{(-1)^i}\Big).f(s_1,..,s_n)^{(-1)^{n+1}},$$

où $f \in C^n$, $s_j \in \mathcal{L}$, et où a^s ($a \in L, s \in \mathcal{L}$) désigne le transformé de a par l'au

tomorphisme s . On a l'important résultat suivant :

(57) $d(df)=1$ pour tout $f\in C^n$.

En effet , d'après (56) , $(ddf)(s_1,\dots,s_{n+2})$ est le produit de

a) $(df)(s_2,\dots,s_{n+2})^{s_1}$, c'est-à-dire

$$f(s_3,\dots,s_{n+2})^{s_1s_2}\Big(\prod_{i=2}^{n+1}f(s_2,\dots,s_is_{i+1},\dots,s_{n+2})^{(-1)^{i-1}s_1}\cdot f(s_2,\dots,s_{n+1})^{(-1)^{n+1}s_1}$$

b) $(df)(s_1,\dots,s_is_{j+1},\dots,s_{n+2})^{(-1)^i}$, lui-même produit de

$$f(s_3,\dots,s_{n+2})^{-s_1s_2}f(s_1s_2s_3,s_4,\dots,s_{n+2})\Big(\prod_{j=3}^{n+1}f(s_1s_2,s_3,\dots,s_js_{j+1},\dots,s_{n+2})^{(-1)^j}\Big)\cdot$$
$$\cdot f(s_1s_2,s_3,\dots,s_{n+1})^{(-1)^n},$$

du produit pour $2\leqslant i\leqslant n$ de

$$f(s_2,\dots,s_is_{i+1},\dots,s_{n+2})^{(-1)^is_1}\prod_{j=2}^{i-2}f(s_1,\dots,s_js_{j+1},\dots,s_is_{i+1},\dots,s_{n+2})^{(-1)^{i+j}}\cdot$$
$$\cdot f(s_1,\dots,s_{i-1}s_is_{i+1},\dots,s_{n+2})^{-1}f(s_1,\dots,s_is_{i+1}s_{i+2},\dots,s_{n+2})\cdot$$
$$\cdot\prod_{j=i+2}^{n+1}f(s_1,\dots,s_is_{i+1},\dots,s_js_{j+1},\dots,s_{n+2})^{(-1)^{i+j-1}}\cdot f(s_1,\dots,s_is_j,\dots,s_{n+1})^{(-1)^{i+n+1}}$$

et de

$$f(s_2,\dots,s_{n+1}s_{n+2})^{(-1)^{n+1}s_1}\cdot\prod_{i=2}^{n-1}f(s_1,\dots,s_is_{i+1},\dots,s_{n+1}s_{n+2})^{(-1)^{n+1+i}}\cdot$$
$$\cdot f(s_1,\dots,s_ns_{n+1}s_{n+2})^{-1}f(s_1,\dots,s_n)$$

c) $(df)(s_1,\dots,s_{n+1})^{(-1)^{n+2}}$, c'est-à-dire

$$f(s_2,\dots,s_{n+1})^{(-1)^ns_1}\cdot\prod_{i=2}^{n}f(s_1,\dots,s_is_{i+1},\dots,s_{n+1})^{(-1)^{n+1}}\cdot f(s_1,\dots,s_n)^{-1}\ .$$

On constate , en mettant ses meilleures lunettes et en bandant au maximum ses facultés d'attention , que tous les facteurs se simplifient , et qu'il reste =1 (Le savant Cosinus a beaucoup travaillé pour pas grand chose).

Ecrivons la formule (56) pour n=0,1,2 :

(56 bis) $(df)(s)=f^{s-1}$ pour $f\in L^*$.

$(df)(s,t)=f(t)^sf(st)^{-1}f(s)$.

$(df)(s,t,u)=f(t,u)^sf(st,u)^{-1}f(s,tu)f(s,t)^{-1}$.

Et , étant donné que nous n'aurons besoin de (57) que pour des cochaînes f de dimensions 0 et 1 , vérifions encore cette formule dans ces cas particuliers :

a) n=0 , $f\in L^*$: $(ddf)(s,t)=df(t)^s.df(st)^{-1}.df(s)=f^{s(t-1)}f^{-st+1}f^{s-1}=1$.

NBL073

b) $n=1$: $(ddf)(s,t,u)=df(t,u)^s.df(st,u)^{-1}.df(s,tu).df(s,t)^{-1}=$
$=f(u)^{st}f(tu)^{-s}f(t)^s.f(u)^{-st}f(stu)f(st)^{-1}.f(tu)^sf(stu)^{-1}f(s).f(t)^{-s}f(st)f(s)^{-1}$
$=1$.

Une cochaîne $f\in C^n$ telle que $df=1$ est appelée un cocycle de dimension n ; les cocycles de dimension n forment un sous-groupe , noté $Z^n(\mathcal{L},L^*)$ de $C^n(\mathcal{L},L^*)$. Une cochaîne $f\in C^n$ qui est de la forme $f=dg$ $(g\in C^{n-1})$ est appelée un cobord ; comme $ddg=1$, tout cobord est un cocycle ; ainsi les cobords forment un sous-groupe , noté $B^n(\mathcal{L},L^*)$ de $Z^n(\mathcal{L},L^*)$. Le groupe quotient Z^n/B^n est appelé le n-ème groupe de cohomologie de $\mathcal{L}$ à valeurs dans L^* , et se note $H^n(\mathcal{L},L^*)$.

PROPOSITION 3 .- Pour toute extension galoisienne finie L d'un corps K , on a $H^1(\mathcal{L},L^*)=(1)$.

Soit f un cocycle de dimension 1 , c'est-à-dire une application de $\mathcal{L}$ dans L^* telle que $f(st)=f(t)^sf(s)$. En vertu du th. d'indépendance linéaire des automorphismes (Alg., chap.V) il existe $b\in L^*$ tel que $\sum_t f(t)b^t\neq 0$; soit a^{-1} cet élément de L^* . On a $a^{-s}=\sum_t f(t)^sb^{st}=\sum_t f(st)b^{st}f(s)^{-1}=a^{-1}f(s)^{-1}$. D'où $f(s)=a^{s-1}$, ce qui montre que f est un cobord .

Remarque .- Supposons L cyclique , et soient u un générateur de $\mathcal{L}$ et x un élément de L tel que $N_{L/K}(s)=1$. Posons , pour q entier positif , $f(u^q)=x^{(1+u+\ldots+u^{q-1})}$; ceci est cohérent puisque $N(x)=1$. Comme $1+u+\ldots+u^{p+q-1}=1+u+\ldots+u^{q-1}+u^q(1+u+\ldots+u^{p-1})$, on a $f(u^pu^q)=f(u^q)^{u^p}f(u^p)$ et f est un cocycle . La prop.3 montre alors qu'il existe $a\in L$ tel que $f(u^q)=a^{u^q-1}$; en particulier $x=f(u)=a^{u-1}$, et on retrouve le théorème normique de Hilbert (Alg., chap.V) .

PROPOSITION 4 .- Soit a un automorphisme de l'extension galoisienne L de K . Alors l'automorphisme de $H^n(\mathcal{L},L^*)$ extension canonique de a est l'automorphisme identique .

Pour éviter des débauches d'indices , dans lesquelles le rédacteur ne voit rien , on va faire la démonstration dans le cas $n=3$, qui permet de bien saisir le mécanisme du calcul du cas général . Le transformé du cocycle f est le cocycle f^a défini par $f^a(s,t,u)=f(a^{-1}sa,a^{-1}ta,a^{-1}ua)^a$. Nous allons montrer que $f^{-1}f^a$ est un cobord . Considérons pour cela la cochaîne g de dimension 2 défi-

nie par $g=g_0g_1^{-1}g_2$, où $g_0(s,t)=f(s,t,a)$, $g_1(s,t)=f(s,a,a^{-1}ta)$ et $g_2(s,t)=$
$=f(a,a^{-1}sa,a^{-1}ta)$. Formons $(dg)(s,t,u)$ en disposant comme suite/ le calcul :

$1=(df)(s,t,u,a)^{-1}=f(t,u,a)^{-s}f(st,u,a)f(s,tu,a)^{-1}f(s,t,ua)f(s,t,u)^{-1}$

$(dg_0)(s,t,u)=f(t,u,a)^{s}f(st,u,a)^{-1}f(st,u,a)f(s,t,a)^{-1}$

$1=(df)(s,t,a,a^{-1}ua)=f(t,a,a^{-1}ua)^{s}f(st,a,a^{-1}ua)^{-1}f(s,ta,a^{-1}ua)f(s,t,ua)^{-1}f(s,t,a)$

$(dg_1)(s,t,u)^{-1}=f(t,a,a^{-1}ua)^{-s}f(st,a,a^{-1}ua)f(s,a,a^{-1}tua)^{-1}f(s,a,a^{-1}ta)$

$1=(df)(s,a,a^{-1}ta,a^{-1}ua)^{-1}=f(a,a^{-1}ta,a^{-1}ua)^{-s}f(sa,a^{-1}ta,a^{-1}ua)f(s,ta,a^{-1}ua)^{-1}\cdot$
$\cdot f(s,a,a^{-1}tua)f(s,a,a^{-1}ua)^{-1}$

$(dg_2)(s,t,u)=f(a,a^{-1}ta,a^{-1}ua)^{s}f(a,a^{-1}sta,a^{-1}ua)^{-1}f(a,a^{-1}sa,a^{-1}tua)\cdot$
$\cdot f(a,a^{-1}sa,a^{-1}ta)^{-1}$

$1=(df)(a,a^{-1}sa,a^{-1}ta,a^{-1}ua)=f(a^{-1}sa,a^{-1}ta,a^{-1}ua)^{a}f(sa,a^{-1}ta,a^{-1}ua)^{-1}\cdot$
$\cdot f(a,a^{-1}sta,a^{-1}ua)f(a,a^{-1}sa,a^{-1}tua)^{-1}f(a,a^{-1}sa,a^{-1}ta)$

Lorsqu'on fait le produit , les facteurs se simplifient à un maximum de deux lignes d'intervalle , et il reste $(dg)(s,t,u)=(f^{-1}f^{a})(s,t,u)$, ce qui montre que $f^{-1}f^{a}$ est un cobord .

3 . L'homomorphisme japonois .

Soit c un élément de $H^2(\mathcal{L},L^*)$. Pour tout représentant f de c dans $Z^2(\mathcal{L},L^*)$ on pose $\overline{f}(s)=\prod_{t\in\mathcal{L}} f(t,s)$. Faisons le produit des formules (56 bis) du cobord, d'abord pour u et s fixes et t parcourant $\mathcal{L}$, puis pour u et t fixes et s parcourant $\mathcal{L}$; il vient

$$1=\overline{f}(u)^{s}\overline{f}(u)^{-1}$$

$$1=N(f(t,u))\cdot\overline{f}(u)^{-1}\overline{f}(tu)\overline{f}(t)^{-1} .$$

Donc $\overline{f}(u)\in K^*$ quel que soit $u\in\mathcal{L}$, et $\overline{f}$ définit , par passage au quotient , un homomorphisme $\overline{f}'$ de $\mathcal{L}$ dans $K^*/N(L^*)$. L'application $f\to\overline{f}'$ est évidemment un homomorphisme de $Z^2(\mathcal{L},L^*)$ dans le groupe $\mathrm{Hom}(\mathcal{L},K^*/N(L^*))$ des homomorphismes de $\mathcal{L}$ dans $K^*/N(L^*)$. Lorsque f est un cobord , on a $f(t,s)=dg(t,s)=$
$=g(s)^{t}g(ts)^{-1}g(t)$; d'où $\overline{f}(s)=N(g(s))$ en faisant le produit par rapport à t ; ainsi l'homomorphisme $\overline{f}'$ applique $\mathcal{L}$ sur l'élément unité de $K^*/N(L^*)$. Par conséquent , pour un cocycle quelconque f de $Z^2(\mathcal{L},L^*)$, l'homomorphisme $\overline{f}'$ ne dépend que de la classe de cohomologie c de f ; on le notera c' ; ainsi $c\to c'$

est un homomorphisme de $H^2(\mathcal{L},L^*)$ dans $\mathrm{Hom}(\mathcal{L},K^*/N(L^*))$ qu'on appelle l'homomorphisme japonois .

PROPOSITION 5 .- Lorsque L est une extension cyclique de K , l'homomorphisme japonois est un isomorphisme de $H^2(\mathcal{L},L^*)$ sur $\mathrm{Hom}(\mathcal{L},K^*/N(L^*))$.

Remarquons d'abord le résultat suivant :

(58) Pour une extension galoisienne quelconque tout cocycle f de dimension 2 est cohomologue à un cocycle f_1 tel que $f_1(1,s)=f_1(s,1)=1$ pour tout $s\in\mathcal{L}$.

En effet , soit g la cochaîne constante définie par $g(t)=f(1,1)$ pour tout t ; alors $(dg)(s,t)=f(11)^s=f(s,1)$ puisque f est un cocycle (56 bis) ; d'où , en posant $f_1=f.(dg)^{-1}$, $f_1(s,1)=1$. Quant à la relation $f_1(1,s)=1$, elle se déduit de la relation $f_1(1,t)=f_1(1,tu)$ qui est vraie pour tout cocycle et qui s'obtient en exprimant que $(df_1)(1,t,u)=1$.

Démontrons maintenant le lemme suivant :

Lemme .- Soient L une extension cyclique de degré n de K et s un générateur de son groupe de Galois $\mathcal{L}$. Alors tout élément e de $Z^2(\mathcal{L},L^*)$ est cohomologue à un cocycle f de la forme $f(s^i,s^j)=1$ pour $i+j<n$, $f(s^i,s^j)=a\in K^*$ pour $i+j\geqslant n$ $(0\leqslant i,j\leqslant n-1)$. Réciproquement toute cochaîne de la forme précédente est un cocycle .

D'après (58) on peut supposer que $e(s^i,1)=e(1,s^i)=1$. Soit g la cochaîne de dimension 1 définie par $g(s^q)=\prod_{i=0}^{q-1} e(s^i,s)$. Pour $p+q<n$, on a $(dg)(s^p,s^q)=$ $=\prod_{i=0}^{q-1} e(s^i,s)^{s^p}\prod_{i=0}^{p+q-1} e(s^i,s)^{-1}\prod_{i=0}^{p-1} e(s^i,s)=\prod_{i=0}^{q-1} e(s^i,s)^{s^p}e(s^ps^i,s)^{-1}$. Pour $p+q\geqslant n$, on a $(dg)(s^p,s^q)=\prod_{i=0}^{q-1}e(s^i,s)^{s^p}\prod_{i=0}^{p+q-1} e(s^i,s)^{-1}\prod_{i=0}^{p-1} e(s^i,s)=\bar{e}(s)\prod_{i=q}^{p+q-1} e(s^i,s)^{s^p}e(s^ps^i,s)^{-1}$ Or , en exprimant que $(de)(s^p,s^1,s)=1$, on voit que $e(s^i,s)^{s^p}e(s^ps^i,s)^{-1}=$ $=e(s^p,s^{i+1})^{-1}e(s^p,s^i)$; d'où $\prod_{i=0}^{q-1} e(s^i,s)^{s^p}e(s^ps^i,s)^{-1}=e(s^p,s^q)^{-1}e(s^p,1)=$ $=e(s^p,s^q)^{-1}$ puisque e est normalisé . Donc le cobord $(dg)(s^p,s^q)$ vaut $e(s^p,s^q)^{-1}$ pour $p+q<n$ et $e(s^p,s^q)^{-1}.\bar{e}(s)$ pour $p+q\geqslant n$. Par conséquent le cocycle $f=e.dg$ est de la forme indiquée , avec $a=\bar{e}(s)\in K^*$.

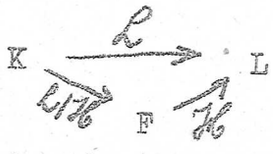
Réciproquement , si f est une cochaîne de la forme indiquée , on a , puisque $a\in K^*$, $(df)(s^p,s^q,s^r)=f(s^q,s^r)f(s^{p+q},s^r)^{-1}f(s^p,s^{q+r})f(s^p,s^q)^{-1}$. Prenons $0\leqslant p,q,r\leqslant n-1$. Pour $p+q+r<n$, les 4 facteurs valent 1 . Pour $p+q<n$, $q+r<n$,

$p+q+r \geqslant n$, on trouve $1.a^{-1}.a.1^{-1}=1$. Pour $p+q \geqslant n$, $q+r \geqslant n$, on trouve $a.1^{-1}.1.a^{-1}=1$ si $p+q+r<2n$ et $a.a^{-1}.a.a^{-1}=1$ si $p+q+r \geqslant 2n$. Pour $p+q<n$, $q+r \geqslant n$, on a $p+q+r<2n$, et on trouve $a.a^{-1}.1.1^{-1}=1$. Le cas $p+q \geqslant n$, $q+r<n$ se ramène au précédent . Donc f est bien un cocycle .

Démontrons maintenant la prop.5 . Pour un cocycle f de la forme indiquée dans le lemme , on a $\bar{f}(s)=f(s^{n-1},s)=a$; comme on peut choisir arbitrairement a dans K , l'homomorphisme japonois applique $H^2(\mathcal{L},L^*)$ sur $\mathrm{Hom}(\mathcal{L},K^*/N(L^*))$. D'autre part , toute classe de son noyau contient un cocycle f du lemme pour lequel $\bar{f}(s)=a$ est une norme ; soit $a=N(b)$ $(b \in L^*)$. Considérons la cochaîne g définie par $g(s^q)=b^{1+s+\ldots+s^{q-1}}$ pour $0 \leqslant q \leqslant n-1$. Le cobord $(dg)(s^p,s^q)=g(s^q)s^p g(s^{p+q})^{-1}.g(s^p)$ vaut $b^{(1+s+\ldots+s^{q-1})s^p-(1+s+\ldots+s^{p+q-1})+(1+s+\ldots+s^{p-1})}=1$ pour $p+q<n$, et $b^{(1+s+\ldots+s^{q-1})s^p-(1+s+\ldots+s^{p+q-n-1})+(1+s+\ldots+s^{p-1})}=b^{1+s+\ldots+s^{n-1}}=N(b)=a$ pour $p+q \geqslant n$. On a donc $f=dg$ et l'homomorphisme japonois est biunivoque .

4 . Transport des classes de cohomologie de dimension 2 .

Soient L une extension galoisienne finie de K , $\mathcal{L}$ son groupe de Galois , F une sous-extension galoisienne de L , $\mathcal{H}$ le sous-groupe invariant des éléments de $\mathcal{L}$ laissant F invariant (c/à.d. le groupe de Galois de L sur F). Alors le groupe de Galois de F sur K s'identifie canoniquement à $\mathcal{L}/\mathcal{H}$ (Alg., chap.V, § 10) :



Soit f une cochaîne de dimension n de $\mathcal{L}$; c'est une application de $\mathcal{L}^n$ dans L^* . Sa restriction à $\mathcal{H}^n$ est une cochaîne de $\mathcal{H}$. On obtient ainsi un homomorphisme canonique de $C^n(\mathcal{L},L^*)$ sur $C^n(\mathcal{H},L^*)$. L'image d'un cocycle (resp. cobord) par cet homomorphisme est évidemment un cocycle (resp. cobord) . On obtient donc , par passage aux quotients , un homomorphisme canonique de $H^n(\mathcal{L},L^*)$ dans $H^n(\mathcal{H},L^*)$.

Considérons maintenant une cochaîne f de dimension n de $\mathcal{L}/\mathcal{H}$; c'est une application de $(\mathcal{L}/\mathcal{H})^n$ dans F^* . Pour $(s_1,\ldots,s_n) \in \mathcal{L}^n$, posons $\tilde{f}(s_1,\ldots,s_n)=f(\bar{s}_1,\ldots,\bar{s}_n)$, $\bar{s}_i$ désignant la classe de s_i mod. $\mathcal{H}$; comme $F^* \subset L^*$, $\tilde{f}$ est un

élément de $C^n(\mathcal{L},L^*)$. L'image par l'homomorphisme $f\to\tilde{f}$ d'un cocycle (resp. cobord) est évidemment un cocycle (resp. cobord) . On obtient donc , par passage aux quotients , un homomorphisme canonique de $H^n(\mathcal{L}/\mathcal{H},F^*)$ dans $H^n(\mathcal{L},L^*)$.

Dans le cas n=2 , on a les résultats suivants :

PROPOSITION 6 .- Soient L une extension galoisienne finie de K , $\mathcal{L}$ son groupe de Galois , F une sous-extension galoisienne de L , et $\mathcal{H}$ le sous-groupe invariant des éléments de $\mathcal{L}$ laissant F invariant . Alors l'homomorphisme canonique de $H^2(\mathcal{L}/\mathcal{H},F^*)$ dans $H^2(\mathcal{L},L^*)$ est biunivoque , et l'image de $H^2(\mathcal{L}/\mathcal{H},F^*)$ par cet isomorphisme est égale au noyau de l'homomorphisme canonique de $H^2(\mathcal{L},L^*)$ dans $H^2(\mathcal{H},L^*)$. Autrement dit , on a la suite exacte :

$(1)\to H^2(\mathcal{L}/\mathcal{H},F^*)\to H^2(\mathcal{L},L^*)\to H^2(\mathcal{H},L^*)$.

Soit f un cocycle de $\mathcal{L}/\mathcal{H}$ dont l'image canonique $\tilde{f}\in Z^2(\mathcal{L},L^*)$ soit un cobord dg ($g\in C^1(\mathcal{L},L^*)$) . On peut supposer (58) que l'on a $\tilde{f}(s,1)=\tilde{f}(1,s)=1$; comme $\tilde{f}(s,t)=g(t)^s g(st)^{-1}g(s)$, on en déduit g(1)=1 . Pour h et h' dans $\mathcal{H}$, on a $(dg)(h,h')=\tilde{f}(h,h')=f(\bar{1},\bar{1})=1$. Donc la restriction de g à $\mathcal{H}$ est un cocycle , et , d'après la prop.3 , il existe $a\in L^*$ tel que $g(h)=a^{h-1}$ pour $h\in\mathcal{H}$. Posons, pour $s\in\mathcal{L}$, $g(s)=a^{s-1}g'(s)$; comme a^{s-1} est un cobord , on a $dg'=dg=\tilde{f}$. D'autre part g'(h)=1 pour $h\in\mathcal{H}$. De $1=\tilde{f}(s,1)=\tilde{f}(1,s)$ on déduit alors g'(sh)=g'(s) ; autrement dit la cochaîne g' est constante sur les classes mod. $\mathcal{H}$. De $1=\tilde{f}(1,t)=\tilde{f}(h,t)$ on déduit de même $g'(t)^h g'(ht)^{-1}g'(h)=1$, c'est-à-dire , puisque g' est constante sur les classes mod. $\mathcal{H}$, et que g'(h)=1 , $g'(t)^h=g'(t)$; autrement dit , les valeurs prises par g' sont invariantes par $\mathcal{H}$, c'est-à-dire dans F^*. Par conséquent g' provient d'une cochaîne de $C^1(\mathcal{L}/\mathcal{H},F^*)$, et le cocycle f dont nous sommes partis est un cobord . Ceci démontre l'assertion de biunivocité .

Soit $f\in Z^2(\mathcal{L}/\mathcal{H},F^*)$, et soit $\tilde{f}$ son image dans $Z^2(\mathcal{L},L^*)$. La restriction de $\tilde{f}$ à $\mathcal{H}$ est alors un cocycle constant dont la valeur b appartient à F^* . Posons g(h)=b : alors , pour $h,h'\in\mathcal{H}$, on a $(dg)(h,h')=b^{h'}b^{-1}b=b$, puisque $b\in F^*$. Donc la restriction de $\tilde{f}$ à $\mathcal{H}$ est un cobord , et l'image canonique de $H^2(\mathcal{L}/\mathcal{H},F^*)$ dans $H^2(\mathcal{L},L^*)$ est contenue dans le noyau de $H^2(\mathcal{L},L^*)\to H^2(\mathcal{H},L^*)$.

Reste à démontrer , réciproquement , que tout cocycle $f \in Z^2(\mathscr{L}, L^*)$ dont la restriction à $\mathscr{H}$ est un cobord est cohomologue à un cocycle provenant d'un cocycle de $Z^2(\mathscr{L}/\mathscr{H}, F^*)$, c'est-à-dire est cohomologue à un cocycle constant sur les classes mod. $\mathscr{H}$ et prenant ses valeurs dans F^* . Soit $g \in C^1(\mathscr{H}, L^*)$ tel que, pour $h,h' \in \mathscr{H}$, on ait $f(h,h')=g(h')^h g(hh')^{-1} g(h)$. Nous pouvons supposer (58) que $f(1,s)=f(s,1)=1$; alors $g(1)=1$. Notons (t_i) un système de représentants (contenant 1) des classes de $\mathscr{L}$ mod. $\mathscr{H}$. Nous prolongerons g à $\mathscr{L}$ en posant $g(t_i h)=g(h)^{t_i} f(t_i,h)^{-1}$ (puisque $f(1,h)=1$) . Posons $f'=f(dg)^{-1}$. Quels que soient $s \in \mathscr{L}$ et $h \in \mathscr{H}$, on a $f'(s,h)=1$; en effet , si t est le représentant de la classe de s et si $s=th'$, on a $f'(s,h)=f(th',h)g(h)^{-th'} g(th'h)g(th')^{-1}=$ $=g(h)^{-th'} g(h'h)^t g(h')^{-t} f(th',h)f(t,h'h)^{-1}f(t,h')=f(h',h)^{-t}f(th',h)f(t,h'h)^{-1}$. $f(t,h')=1$ puisque $df=1$. Notre assertion résulte alors du lemme suivant :

Lemme .- Les notations étant celles de la prop.6 , soit $e \in Z^2(\mathscr{L}, L^*)$ un cocycle tel que $e(s,h)=1$ pour $s \in \mathscr{L}$ et $h \in \mathscr{H}$. Alors $e(s,t)$ ne dépend que de s et de la classe de t mod. $\mathscr{H}$. Pour tout $s \in \mathscr{L}$, il existe $a_s \in L^*$ ne dépendant que de la classe de s mod. $\mathscr{H}$, tel que $a_1=1$ et que $e(h,s)=(a_s)^{h-1}$. La cochaîne e' définie par $e'(s,t)=e(s,t)(a_t)^{-s} a_{st} (a_s)^{-1}$ est un cocycle cohomologue à e , dont la valeur $e'(s,t)$ ne dépend que des classes de s et t mod. $\mathscr{H}$, et est élément de F^* .

La relation $(de)(s,t,h)=1$ s'écrit $e(t,h)^s e(st,h)^{-1} e(s,th) e(s,t)^{-1}=1$ et entraîne $e(s,th)=e(s,t)$ puisque $e(t,h)=e(st,h)=1$; d'où le fait que $e(s,t)$ ne dépend que de s et de la classe de t . Posons $g_s(h)=e(h,s)$; on a $(dg_s)(h,h')=$ $=g_s(h')^h g_s(hh')^{-1} g_s(h)=e(h',s)^h e(hh',s)^{-1} e(h,s)$ qui , en vertu de $(de)(h,h',s)$ $=1$ vaut $e(h,h's)^{-1} e(h,h')e(h,s)=e(h,h')$ (d'après ce qui vient d'être vu)$=1$ (par hypothèse). Donc g_s est un cocycle de dimension 1 ; il ne dépend que de la classe de s , et $g_1=1$ d'après l'hypothèse ; l'existence de a_s résulte alors de la prop.3 . Le fait que e' est cohomologue à e est clair , et aussi le fait que $e'(s,t)$ ne dépend que de s et de la classe de t . Pour montrer qu'il ne dépend aussi que de la classe de s , formons $e'(sh,t)$; on a $e'(sh,t)=$ $=e(sh,t)(a_t)^{-sh} a_{sht} (a_{sh})^{-1}$; or $a_{sht}=a_{st}$, $a_{sh}=a_s$ et $(a_t)^h=e(h,t)a_t$; donc

$e'(sh,t)=e(sh,t)e(h,t)^{-s}(a_t)^{-s}a_{st}(a_s)^{-1}=e'(s,t)e(s,t)^{-1}e(sh,t)e(h,t)^{-s}$; en écrivant que $(de)(s,h,t)=1$, il vient $e'(sh,t)=e'(s,t)e(s,t)^{-1}e(s,ht)e(s,h)^{-1}=$ $=e'(s,t)$ puisque $e(s,t)=e(s,ht)$ (première assertion) et que $e(s,h)=1$ (hypothèse) ; ceci montre bien que $e'(s,t)$ ne dépend que des classes de s et t . Enfin la formule $(de')(h,s,t)=1$ s'écrit $e'(s,t)^h=e'(hs,t)e'(h,st)^{-1}e'(h,s)$; comme $e'(h,s)=e'(h,st)=1$ par construction , on en déduit que $e'(s,t)^h=e'(s,t)$, c'est-à-dire que $e'(s,t)\in F^*$. CQFD . OUF!

COROLLAIRE .- Si $\mathscr{H}$ est d'ordre n , et si c est un élément de $H^2(\mathscr{L},L^*)$, alors c^n est dans l'image canonique de $H^2(\mathscr{L}/\mathscr{H},F^*)$.

Pour tout $f\in Z^2(\mathscr{L},L^*)$, posons $f'(s)=\prod_{h\in\mathscr{H}} f(s,h)$. Alors $(df')(s,t)=$ $=f'(t)^s f'(st)^{-1}f'(s)=\prod_h f(t,h)^s \prod_h f(st,h)^{-1}\prod_h f(s,h)$; or , comme $(df)(s,t,h)=$ $=1$, on a $f(t,h)^s f(st,h)^{-1}=f(s,th)^{-1}f(s,t)$; d'où $(df')(s,t)=f(s,t)^n\prod_h f(s,th)^{-1}$. $\prod_h f(s,h)$; si l'on prend $t=h'$, on a donc $(df')(s,h')=f(s,h')^n$. Prenons pour f un représentant de c ; la formule précédente montre que la restriction de f^n à $\mathscr{H}$ est un cobord , donc que f^n est dans le noyau de $H^2(\mathscr{L},L^*)\to H^2(\mathscr{H},L^*)$. Le corollaire résulte donc de la seconde assertion de la prop.6 .

Nous supposerons désormais toutes les extensions du corps K plongées dans une même clôture algébrique Ω de K . La manière dont ce plongement est effectué n'a pas d'influence sur les groupes de cohomologie en vertu de la prop.4. Soient E et F deux extensions galoisiennes de K , C leur extension composée , $\mathscr{E}$, $\mathscr{F}$ et $\mathscr{C}$ leurs groupes de Galois . Les isomorphismes canoniques $H^2(\mathscr{E},E^*)\to H^2(\mathscr{C},C^*)$ et $H^2(\mathscr{F},F^*)\to H^2(\mathscr{C},C^*)$ (prop.5) identifient $H^2(\mathscr{E},E^*)$ et $H^2(\mathscr{F},F^*)$ à des sous-groupes de $H^2(\mathscr{C},C^*)$; à l'intersection de ces sous-groupes correspondent des sous-groupes $H^2(\mathscr{E},E^*)_F$ de $H^2(\mathscr{E},E^*)$ et $H^2(\mathscr{F},F^*)_E$ de $H^2(\mathscr{F},F^*)$ canoniquement isomorphes par des isomorphismes réciproques $\tau_{E,F}$ et $\tau_{F,E}$. Une classe de cohomologie $c\in H^2(\mathscr{E},E^*)$ pour laquelle $\tau_{E,F}(c)$ est définie (c.à.d. un élément de $H^2(\mathscr{E},E^*)_F$) est dite transportable à F . On vérifie , comme l'âne qui trotte , la propriété de transitivité

(59) $$\tau_{F,G}\,\tau_{E,F}=\tau_{E,G}$$

NBR 073

(dans le sens : "si le premier membre est défini , le se ond l'est aussi , et il y a égalité").

Etudions enfin les propriétés "fonctorielles" de l'homomorphisme japonois(n°3)

PROPOSITION 7 .- Soient F une sous-extension galoisienne de l'extension galoisienne L de K , $\mathcal{L}$, $\mathcal{H}$ et $\mathcal{L}/\mathcal{H}$ les groupes de Galois de L sur K , de L sur F et de F sur K ; soit $c \in H^2(\mathcal{L}, L^*)$, et soit m le degré de L sur F . Notons $e = \mu_{L,F}(c)$ l'unique élément de $H^2(\mathcal{L}/\mathcal{H}, F^*)$ tel que $c^m = \mu_{F,L}(e)$ (prop.6 et cor.). Notons $\rho(c)$ l'image canonique de c dans $H^2(\mathcal{H}, L^*)$. On a alors le diagramme de commutation suivant :

$$\begin{array}{ccccc} \mathcal{H} & & \mathcal{L} & & \mathcal{L}/\mathcal{H} = \mathcal{F} \\ \rho(c)' \downarrow & & c' \downarrow & & (\mu_{L,F}(c))' \downarrow \\ F^*/N_{L/F}(L^*) & \xrightarrow{N_{F/K}} & K^*/N_{L/K}(L^*) & \longrightarrow & K^*/N_{F/K}(F^*) \end{array}$$

Examinons d'abord le carré de gauche . Soit $f \in Z^2(\mathcal{L}, L^*)$ un représentant de c ; alors $\rho(c)$ est la classe de la restriction g de f à $\mathcal{H}$. Soient (t_i) des représentants des classes de $\mathcal{L}$ mod. $\mathcal{H}$. Comme $(h \in \mathcal{H})$, $\bar{g}(h) = \prod_{h'} f(h', h) \in F^*$, on a $N_{F/K}(\bar{g}(h)) = \prod_{h', t_i} f(h', h)^{t_i}$. Or , comme $(df)(t_i, h', h) = 1$, on a $f(h', h)^{t_i} = f(t_i h', h) \cdot f(t_i, h'h)^{-1} f(t_i, h')$. Puisque h'h parcourt $\mathcal{H}$ en même temps que h', on a $\prod_{h' \in \mathcal{H}} f(t_i, h'h)^{-1} f(t_i, h') = 1$. D'où $N_{F/K}(\bar{g}(h)) = \prod_{h', t_i} f(t_i h', h) = \bar{f}(h)$. Ceci démontre l'assertion relative au carré de gauche .

Passons au carré de droite . Soit toujours f un représentant de c . Comme dans le cor.à la prop.6 , considérons $f_1(s) = \prod_h f(s, h)$; posons $g(s,t) = (f^m (df_1)^{-1})(s,t)$; la démonstration dudit corollaire montre que $g(s,t) = \prod_h f(s, th) f(s,h)^{-1}$. Donc $g(s,h') = 1$ $(h' \in \mathcal{H})$ et $g(s,th') = g(s,t)$. On peut donc appliquer à g le lemme à la prop.6 : il existe des $a_s \in L^*$ ne dépendant que de la classe de s tels que $g(h,s) = (a_s)^{h-1}$ et que $g'(s,t) = g(s,t)(a_t)^{-s} a_{st} (a_s)^{-1}$ soit un élément de F ne dépendant que des classes de s et t ; ainsi l'on peut prendre g' (préalablement passé au quotient et à l'autoclave) comme représentant de la classe $\mu_{L,F}(c)$. Soit (t_i) un système de représentants des classes de $\mathcal{L}$ mod. $\mathcal{H}$; notons $\bar{s}$ la classe de s . On a $\bar{g}'(\bar{s}) = \prod_{t_i} g'(t_i, s) = \prod_{t_i} (g(t_i, s)(a_s)^{-t_i} a_{t_i s} (a_{t_i})^{-1}$. Comme a_v ne dépend que de la clas-

se de u , et que $t_i s$ parcourt un système de représentants des classes en même temps que s , l'expression précédente se réduit à $\bar{g}'(\bar{s}) = \prod_{t_i} g(t_i,s)(a_s)^{-t_i}$. Or nous avons vu que $g(t_i,s)=\prod_h f(t_i,sh)f(t_i,h)^{-1}$; comme $\mathcal{H}$ est invariant , ceci s'écrit , en regroupant les termes , $g(t_i,s)=\prod_h f(t_i,hs)f(t_i,h)^{-1}$; en se servant du fait que $(df)(t_i,h,s)=1$, ceci s'écrit aussi $\prod_h f(t_ih,s)f(h,s)^{-t_i}$. On a par conséquent $\bar{g}'(\bar{s})=\prod_{t_i,h} f(t_ih,s)\cdot\prod_{t_i}(a_s\prod_h f(h,s))^{-t_i}$. Comme t_ih parcourt $\mathcal{L}$, le premier facteur n'est autre que $\bar{f}(s)$. D'autre part , on a $b_s=a_s\prod_h f(h,s)\in F^*$; en effet , d'après la définition de a_s , on a $(a_s)^{h'}=a_s g(h',s)=a_s\prod_k f(h',sh)f(h',h)^{-1}$; d'où $(b_s)^{h'}=a_s\prod_k f(h,s)^{h'}f(h',sh)f(h',h)^{-1}$; par regroupement de termes , on peut écrire $f(h',hs)$ au lieu de $f(h',sh)$; d'où , en vertu de $(df)(h',h,s)=1$, $(b_s)^{h'}=a_s\prod_k f(h'h,s)=b_s$ puisque $h'h$ parcourt $\mathcal{H}$ en même temps que h ; ainsi b_s est invariant par $\mathcal{H}$. Par conséquent $\bar{g}'(\bar{s})=\bar{f}(s)\prod_{t_i}(b_s)^{-t_i}=\bar{f}(s).N_{F/K}(b_s)$. On en conclut que les classes de $\bar{g}'(\bar{s})$ et de $\bar{f}(s)$ sont égales mod.$N_{F/K}(F^*)$, ce qui n'est autre que la commutativité exprimée par le carré de droite .CUF!

5 . L'homomorphisme principal dans le cas des corps localement compacts .

Le cas de R et C étant facile , nous considérerons ici un corps valué complet K pour une valuation discrète telle que le corps des valeurs k de K soit fini. Considérons l'unique extension non ramifiée Z de degré n de K . En vertu de la prop.1 elle est cyclique , et son groupe de Galois $\mathcal{G}$ est engendré par l'automorphisme de Frobenius s ; le groupe quotient $K^*/N(Z^*)$ est aussi un groupe cyclique d'ordre n , engendré par la classe des uniformisantes (prop.1) ; soit $\varphi_{Z/K}$ l'isomorphisme de $\mathcal{G}$ sur $K^*/N(Z^*)$ qui applique l'automorphisme de Frobenius sur la classe des uniformisantes . D'après la prop.5 il existe un élément $c_{Z/K}$ et un seul de $H^2(\mathcal{G},Z^*)$ tel que $\varphi_{Z/K}=(c_{Z/K})'$; comme $\mathrm{Hom}(\mathcal{G},K^*/N(Z^*))$ est un groupe cyclique d'ordre n engendré par $\varphi_{Z/K}$, la prop.5 montre aussi que $H^2(\mathcal{G},Z^*)$ est un groupe cyclique d'ordre n engendré par la classe de cohomologie $c_{Z/K}$. Le lemme à la prop.5 montre que la classe $c_{Z/K}$ admet pour représentant le cocycle f défini par $f(s^i,s^j)=1$ pour $i+j<n$ et $f(s^i,s^j)=$uniformisante pour $i+j\geqslant n$ $(0\leqslant i,j\leqslant n-1)$.

THEOREME 2 .- Soient K un corps localement compact , L une extension galoisienne de degré n de K , et Z l'extension non ramifiée de degré n de K . Alors tout élément de $H^2(\mathcal{Z},Z^*)$ est transportable à L .

Comme $c_{Z/K}$ (défini ci-dessus) est un générateur de $H^2(\mathcal{Z},Z^*)$ il nous suffit de montrer que $c_{Z/K}$ est transportable à L . Soit T le corps d'inertie de L ;posons $[T:K]=f$, $[L:T]=e$ (§ 3) ; alors $n=ef$. Considérons l'extension composée U de L et Z ; c'est une extension complètement ramifiée de degré e de Z , et une extension non ramifiée de degré e de L . On a le diagramme de Hasse :

$$\begin{array}{ccccc} K & \rightarrow & T & \hookrightarrow & Z \\ & & & \searrow & \downarrow \\ & & & & L \\ & & & \searrow & \downarrow \\ & & & & U \end{array}$$

Soit $\mathcal{U}$ le groupe de Galois de U sur K , et soit $\mathcal{U}_L$ le sous-groupe des élément de $\mathcal{U}$ laissant L invariant , c'est-à-dire le groupe de Galois de U sur L . Pour montrer que $c_{Z/K}$ est transportable à L il suffit de montrer que $\tau_{Z,U}(c_{Z/K})$ est dans l'image de l'isomorphisme canonique $H^2(\mathcal{U}/\mathcal{U}_L,L^*) \rightarrow H^2(\mathcal{U},U^*)$, c'est-à-dire (prop.6) dans le noyau de l'homomorphisme canonique $H^2(\mathcal{U},U^*) \rightarrow H^2(\mathcal{U}_L,U^*)$ Soit c_1 l'image canonique de $c_{Z/K}$ par l'homomorphisme composé $H^2(\mathcal{Z},Z^*) \rightarrow$ $\rightarrow H^2(\mathcal{U},U^*) \rightarrow H^2(\mathcal{U}_L,U^*)$. Comme U est extension non ramifiée , et donc cyclique , de L , il va nous suffire de montrer que l'homomorphisme $(c_1)'$ (de $\mathcal{U}_L$ dans $L^*/N_{U/L}(L^*)$ (n°3)) est égal à 1 (prop.5) .

Or l'automorphisme de Frobenius t de l'extension non ramifiée U de L induit sur Z la puissance s^f de l'automorphisme de Frobenius de Z sur K . Si a désigne une uniformisante de Z et g le représentant de $c_{Z/K}$ défini par $g(s^i,s^j)=1$ pour $i+j<n$, et a pour $i+j \geq n$, on en déduit que $(c_1)'(t)$ est la classe modulo $N_{U/L}(U^*)$ de l'élément $\prod_{i=0}^{e-1} g(s^{if},s^f)$, lequel vaut a . Comme a est d'ordre e pour la valuation normée de U , c'est un élément de $N_{U/L}(U^*)$ (prop.1) , et l'on a $(c_1)'(t)=1$, et donc $(c_1)'=1$ puisque t engendre $\mathcal{U}_L$. CQFD

COROLLAIRE 1 .- Pour toute extension galoisienne L de K , le nombre d'éléments du groupe $H^2(\mathcal{L},L^*)$ est multiple de $[L:K]$.

En effet $H^2(\mathcal{L},L^*)$ contient comme sous-groupe l'image de $H^2(\mathcal{Z},Z^*)$ par l'isomorphisme canonique $\tau_{Z,L}$.

COROLLAIRE 2 .- Pour toute extension cyclique L de K , les groupes $H^2(\mathcal{L},L^*)$ $\mathrm{Hom}(\mathcal{L},K^*/N_{L/K}(L^*))$ et $K^*/N_{L/K}(L^*)$ ont tous $[L:K]$ éléments et sont cycliques . En effet les deux premiers sont isomorphes (prop.5) et leur nombre d'éléments est multiple de $[L:K]$. D'autre part le nombre d'éléments de $K^*/N(L^*)$ est $\leq [L:K]$ (th.1) . Comme $\mathcal{L}$ est cyclique on en déduit que $\mathrm{Hom}(\mathcal{L},K^*/N(L^*))$ a au plus $[L:K]$ éléments . Donc $H^2(\mathcal{L},L^*)$ a $[L:K]$ éléments , et est par conséquent isomorphe par $\tau_{Z,L}$ à $H^2(\mathcal{Z},Z^*)$ qui , en tant qu'isomorphe à $\mathrm{Hom}(\mathcal{Z},K^*/N_{Z/K}(Z^*))$ est cyclique . D'où la conclusion .

Dans le cas général d'une extension galoisienne L de K , la classe de cohomologie $\tau_{Z,L}(c_{Z/K}) \in H^2(\mathcal{L},L^*)$, obtenue par transport à L de la classe de cohomologie $c_{Z/K}$ de $H^2(\mathcal{Z},Z^*)$ est appelée la classe principale de cohomologie de L, et se note $c_{L/K}$. L'homomorphisme correspondant $(c_{L/K})'$ de $\mathcal{L}$ dans $K^*/N_{L/K}(L^*)$ s'appelle l'homomorphisme principal de L , et se note $\varphi_{L/K}$. On déduit aussitôt du cor.2 au th.2 que , si L est cyclique , alors $\varphi_{L/K}$ est un isomorphisme de $\mathcal{L}$ sur $K^*/N_{L/K}(L^*)$. Les homomorphismes principaux ont la propriété suivante de "naturalité" :

PROPOSITION 8 .- Soient K un corps localement compact , L une extension galoisienne de K , F une sous-extension galoisienne de L , $\mathcal{L}$ le groupe de Galois de L sur K , $\mathcal{L}_F \subset \mathcal{L}$ celui de L sur F . On a le diagramme de commutation :

$$\begin{array}{ccccc} \mathcal{L}_F & \longrightarrow & \mathcal{L} & \longrightarrow & \mathcal{L}/\mathcal{L}_F \\ \varphi_{L/F}\downarrow & & \varphi_{L/K}\downarrow & & \varphi_{F/K}\downarrow \\ F^*/N_{L/F}(L^*) & \xrightarrow[N_{F/K}]{} & K^*/N_{L/K}(L^*) & \longrightarrow & K^*/N_{F/K}(F^*) \end{array}$$

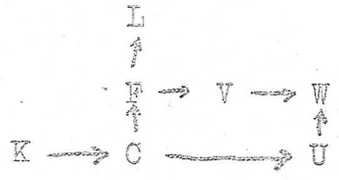
Soit $c=c_{L/K}$ la classe principale de cohomologie de L (sur K) , $c_{L/F}$ et $c_{F/K}$ celles de L sur F et de F sur K . D'après la prop.7 , et avec les notations de celle-ci , il suffit de montrer que $c_{L/F}=f(c)$ et que $c_{F/K}=f_{L;F}(c)$.

Démontrons d'abord la formule $c_{F/K}=f_{L/F}(c_{L/K})$. Les notations $f_{L,F}$ et $\tau_{L,F}$ d'Hochschild étant à l'envers , nous écrirons $M_{F,L}$ et $T_{F,L}$ à la place (il serait bon que le prochain rédacteur le fît dès le début) . Il s'agit ainsi de montrer que $c_{F/K}=M_{F,L}(c_{L/K})$, c'est-à-dire $c_{F/K}=T_{F,L}(c_{L/K}^{[L:F]})$.

Faisons-le d'abord lorsque L est non ramifiée sur K ; soit $[L:K]=n$, $[L:F]=d$; soit s l'automorphisme de Frobenius de L sur K . L'automorphisme de Frobenius de F sur K est la classe de s mod. $\mathcal{L}_F$. Comme dans le cas d'extensions non ramifiées , on a $\varphi_{L/K}$(Frobenius)=classe des uniformisantes mod.normes , la commutativité exprimée par le carré de droite est vraie dans ce cas , et la prop.7 montre que l'on a bien $\varphi_{F/K}=(M_{F,L}(c_{L/K}))'$, c'est-à-dire $c_{F/K}=M_{F,L}(c_{L/K})$ en vertu de la prop.5 .

Passons maintenant au cas général . Posons $[L:K]=n$ et $[L:F]=d$. Soient T et U les extensions non ramifiées de K , de degrés n/d et n . On a $c_{F/K}=T_{F,T}(c_{T/K})=$ $=T_{T,T}(M_{T,U}(c_{U/K}))$ (d'après ce qui vient d'être vu) $=T_{F,T}(T_{T,U}(c^d_{U/K}))=T_{F,U}(c^d_{U/K})$ (transitivité des transports) . D'autre part $M_{F,L}(c_{L/K})=M_{F,L}(T_{L,U}(c_{U/K}))=$ $=T_{F,L}(T_{L,U}(c^d_{U/K}))=T_{F,U}(c^d_{U/K})$. Notre assertion est démontrée .

Montrons maintenant que $c_{L/F}$ s'obtient à partir de $c_{L/K}$ par restriction à $\mathcal{L}_F$. Soient U l'extension non ramifiée de degré n de K , V l'extension non ramifiée de degré d de F , W l'extension composée de V et U ; si e est l'indice de ramification de F sur K , W est extension de degré e de U et de V . Diagramme de Hasse :



(C désignant le corps d'inertie de F sur K ; soit $f=[C:K]$; on a $n=ef$). Soit s l'automorphisme de Frobenius de W sur F . La restriction de s à U est évidemment l'automorphisme de Frobenius de U sur C , c'est-à-dire t^f , t désignant l'automorphisme de Frobenius de U sur K . Au moyen de la commutativité de droite appliquée aux corps K,U,W , on en déduit aisément que la commutativité de gauche est vraie pour les corps K,F,W . Comme W est extension cyclique de F, la prop.5 montre alors (compte tenu de la prop.7 de commutativité des japonois) que l'on a $c_{W/F}=(c_{W/K})^{R_{K,F}}$, $R_{K,F}$ désignant l'opération de restriction au sous-groupe des automorphismes de W laissant F invariant .

Or $c_{L/F}=T_{L,V}(c_{V,F})=T_{L,V}(M_{V,W}(c_{W/F}))$ (d'après la première partie)

$=T_{L,V}(T_{V,W}(c^e_{W/F}))=T_{L,W}(c^e_{W/F})=T_{L,W}((c^e_{W/K})R_{K,F})$ (d'après ce qui vient d'être vu). D'autre part $c_{L/K}=T_{L,U}(c_{U/K})=T_{L,U}(M_{U,W}(c_{W/K}))$ (première partie) $=T_{L,U}(T_{U,W}(c^e_{W/K}))=T_{L,W}(c^e_{W/K})$. Par conséquent $(c_{L/K})R_{K,F}=T_{L,W}(c^e_{W/K}))R_{K,F}$. En comparant cette dernière relation avec $c_{L/F}=T_{L,W}((c^e_{W/K})R_{K,F})$, on en déduit que $c_{L/F}=(c_{L/K})R_{K,F}$ puisque les opérations de restriction et de transport sont permutables. CQFD

6. Théorèmes d'isomorphie et d'unicité.

Soient K un corps localement compact, L une extension galoisienne de K. Nous étendrons ainsi la définition de l'homomorphisme principal au cas K=R, L=C : $\varphi_{C/R}$(conjugaison)=classe de -1 mod.R^*_+ ; alors $\varphi_{C/R}$ est bien un isomorphisme du groupe de Galois de C sur R (composé de l'identité et de la conjugaison) sur $R^*/R^*_+=R^*/N_{C/R}(C^*)$. Les théorèmes qui vont suivre sont triviaux dans ce cas.

THÉORÈME 3 (théorème d'isomorphisme).- Soient L une extension abélienne d'un corps localement compact K, et $\mathcal{L}$ son groupe de Galois. Alors l'homomorphisme principal $\varphi_{L/K}$ est un isomorphisme de $\mathcal{L}$ sur $K^*/N_{L/K}(L^*)$.

Ceci a déjà été démontré dans le cas d'une extension cyclique (cor.2 du th.2). Comme le groupe de Galois $\mathcal{L}$ de L est produit direct de groupes cycliques (Alg. chap.VII), L est extension composée d'un certain nombre fini n d'extensions cycliques de K. Nous raisonnerons par récurrence sur n. Si L est extension composée de n extensions cycliques, elle est aussi extension composée d'une extension cyclique Z et d'une extension abélienne F composée de n-1 extensions cycliques. Soient $\mathcal{L}_F$ et $\mathcal{L}_Z$ les groupes de Galois de L sur F et sur Z.

Considérons un élément $s\in\mathcal{L}$ tel que $\varphi_{L/K}(s)=N_{L/K}(L^*)$. D'après la prop.8 on a en désignant par s_F et s_Z les classes de s mod. $\mathcal{L}_F$ et $\mathcal{L}_Z$, $\varphi_{F/K}(s_F)=N_{F/K}(F^*)=1$ et $\varphi_{Z/K}(s_Z)=N_{Z/K}(Z^*)=1$. D'après l'hypothèse de récurrence appliquée à F et Z, on en déduit que $s_Z=1$ et $s_F=1$. Par conséquent les restrictions de s à Z et F sont les automorphismes identiques ; ainsi s=1, et $\varphi_{L/K}$ est biunivoque. Alors l'inégalité fondamentale $(K^*:N_{L/K}(L^*))\leqslant[L:K]$ (n°1, th.1) et le fait que $\mathcal{L}$ a $[L:K]$ éléments montrent que $\varphi_{L/K}(\mathcal{L})=K^*/N_{L/K}(L^*)$. CQFD

THÉOREME 4 (ordination et unicité).- Soit K un corps localement compact. A

N8R073

toute extension galoisienne L de K associons le sous-groupe $N_{L/K}(L^*)$ de K^*. L'application $L \to N_{L/K}(L^*)$ est décroissante (pour les relations d'inclusion), et sa restriction à l'ensemble des extensions abéliennes est biunivoque : plus précisément, si L' et L" sont des extensions abéliennes de K telles que $N_{L'/K}(L'^*) \subset N_{L''/K}(L''^*)$, on a $L' \supset L''$. Enfin, si L est une extension galoisienne de K, et si A est la plus grande extension abélienne de K contenus dans L (c'est-à-dire le corps des invariants du groupe des commutateurs du groupe de Galois $\mathcal{L}$ de L), on a $N_{L/K}(L^*)=N_{A/K}(A^*)$.

La décroissance de l'application $L \to N_{L/K}(L^*)$ est conséquence immédiate de la transitivité des normes. Soient L' et L" deux extensions galoisiennes de K telles que $N_{L'/K}(L'^*) \subset N_{L''/K}(L''^*)$, et que L' soit abélienne ; soit L leur extension composée, soit s un automorphisme de L sur K, et soient s' et s" les restrictions de s à L' et L" ; alors (prop.8) $\varphi_{L''/K}(s'')$ est la classe mod.$N(L''^*)$ de $\varphi_{L/K}(s)$, donc aussi la classe de $\varphi_{L'/K}(s')$ mod.$N(L''^*)$ (puisque $N(L''^*) \supset N(L'^*) \supset N(L^*)$) ; comme $\varphi_{L'/K}$ est un isomorphisme, ceci montre que s'=1 implique s"=1 ; d'où $L' \supset L''$ puisque L' et L" sont des corps d'invariants. La biunivocité se déduit aussitôt de ceci et du fait que $(K^* : N_{L/K}(L^*)) = [L:K]$ lorsque L est abélienne (th.3).

Soit maintenant $\mathcal{L}'$ le groupe des commutateurs du groupe de Galois $\mathcal{L}$ de L. Considérons le diagramme de commutativité (prop.8)

$$\begin{array}{ccc} \mathcal{L} & \longrightarrow & \mathcal{L}/\mathcal{L}' \\ \varphi_{L/K} \downarrow & & \varphi_{A/K} \downarrow \\ K^*/N(L^*) & \longrightarrow & K^*/N(A^*) \end{array}$$

Comme $K^*/N(L^*)$ est commutatif, le noyau de $\varphi_{L/K}$ contient $\mathcal{L}'$; donc $\varphi_{L/K}$ définit par passage aux quotients un homomorphisme h de $\mathcal{L}/\mathcal{L}'$ dans $K^*/N(L^*)$; le composé de h et de l'homomorphisme canonique de $K^*/N(L^*)$ sur $K^*/N(A^*)$ est $\varphi_{A/K}$. Puisque $\varphi_{A/K}$ est un isomorphisme (th.3), h est un isomorphisme de $\mathcal{L}/\mathcal{L}'$ dans $K^*/N(L^*)$. Ainsi l'assertion $N_{L/K}(L^*)=N_{A/K}(A^*)$ équivaut à "h est sur", c.à.d. à "$\varphi_{L/K}$ est un homomorphisme de $\mathcal{L}$ sur $K^*/N_{L/K}(L^*)$". Comme l'assertion à démontrer est vraie pour les extensions de degré premier (qui sont cycliques), nous allons la démontrer par récurrence sur $[L:K]$. Comme L est

extension résoluble de K (§ 3, n°3), on a $A \neq K$ (si $L \neq K$). Alors, d'après l'hypothèse de récurrence, $\varphi_{L/A}$ est un homomorphisme de $\mathcal{L}'$ sur $A^*/N_{L/A}(L^*)$. Considérons un élément $b \in K^*$ de la forme $b = N_{A/K}(a)$ $(a \in A^*)$; il existe $s \in \mathcal{L}'$ tel que a soit dans la classe $\varphi_{L/A}(s)$ mod. $N_{L/A}(L^*)$; donc b est dans la classe image de $\varphi_{L/A}(s)$ par l'application $A^*/N_{L/A}(L^*) \to K^*/N_{L/K}(L^*)$ déduite de $N_{A/K}$ par passage aux quotients ; autrement dit (prop.8) b est dans la classe $\varphi_{L/K}(s)$ mod. $N_{L/K}(L^*)$; mais comme s appartient au groupe des commutateurs de $\mathcal{L}$, cette classe n'est autre que $N_{L/K}(L^*)$. Par conséquent $N_{A/K}(A^*) \subset N_{L/K}(L^*)$, et $N_{A/K}(A^*) = N_{L/K}(L^*)$ puisque l'inclusion inverse est évidente.

COROLLAIRE 1 .- *L'homomorphisme principal $\varphi_{L/K}$ est un homomorphisme de $\mathcal{L}$ sur $K^*/N_{L/K}(L^*)$.*

Vu en cours de démonstration.

COROLLAIRE 2 .- *Pour toute extension galoisienne L de K, on a $(K^* : N_{L/K}(L^*)) \leqslant [L:K]$; l'égalité $(K^* : N_{L/K}(L^*)) = [L:K]$ caractérise les extensions abéliennes.*

Remarque .- En se servant du fait (évident) que le diagramme de gauche de la prop.8 est valable pour une extension quelconque F, on montre facilement que l'égalité $N(L^*) = N(A^*)$ est vraie pour une extension séparable quelconque L.

THÉORÈME 5 (théorème de translation) .- *Soient K un corps localement compact, L une extension abélienne de K, F une extension algébrique finie de K, U l'extension composée de L et F. Alors $N_{U/F}(U^*)$ est égal au sous-groupe H des éléments a de F tels que $N_{F/K}(a) \in N_{L/K}(L^*)$.*

L'inclusion $N_{U/F}(U^*) \subset H$ est conséquence immédiate de la transitivité des normes. Pour démontrer l'inclusion inverse, nous aurons besoin du diagramme suivant, où l'on note $\mathcal{L}$ le groupe de Galois de L sur K et $\mathcal{U}_F$ celui de U sur F (qui s'identifie à un sous-groupe de $\mathcal{L}$), et $\bar{N}$ l'application déduite de $N_{F/K}$ par passage aux quotients

$$\begin{array}{ccc} \mathcal{U}_F & \longrightarrow & \mathcal{L} \\ \downarrow \varphi_{U/F} & & \downarrow \varphi_{L/K} \\ F^*/N(U^*) & \xrightarrow{\bar{N}} & K^*/N(L^*) \end{array}$$

(Celui-ci se démontre asinitrottant à partir de la prop.8, par passage à

l'extension galoisienne V de K engendrée par U , et en remarquant que le carré de gauche du diagramme de la prop.8 est valable pour une extension (quelconque) Ceci étant , soit a un élément de H , $\bar{a}$ sa classe mod.$N_{U/F}(U^*)$, et s l'élément de $\mathcal{U}_F$ tel que $\bar{a}=\varphi_{U/F}(s)$; comme $N(\bar{a})=1$ par hypothèse , on a $\varphi_{L/K}(s)=1$, donc s=1 , et $a\in N_{U/F}(U^*)$. CQFD .

COROLLAIRE .- Avec les mêmes notations , on a $N_{U/K}(U^*)=N_{L/K}(L^*)\cap N_{F/K}(F^*)$.

En effet , le th.6 s'écrit $N_{U/F}(U^*)=N_{F/K}^{-1}(N_{L/K}(L^*)\cap N_{F/K}(F^*))$; il suffit alors de prendre le $N_{F/K}$ des deux membres .

7 . Le théorème d'existence (non "gleichberechtigt"!)

Nous nous proposons de montrer que tout sous-groupe d'indice fini (ou presque de K^* est un groupe de normes d'une extension abélienne de K . Nous aurons besoin des lemmes suivants :

Lemme 1 .- Soient K localement compact , L une extension abélienne de K , H' un sous-groupe de K^* contenant $N_{L/K}(L^*)$; il existe une extension abélienne L' de K contenue dans L , telle que $H'=N_{L'/K}(L'^*)$.

Soit $\mathcal{L}$ le groupe de Galois de L , et soit $\mathcal{L}'$ le sous-groupe de $\mathcal{L}$ image réciproque par $\varphi_{L/K}$ de $H'/N_{L/K}(L^*)$; notons L' le corps des invariants de $\mathcal{L}'$; c'est une extension abélienne de K . Le diagramme de la prop.8

$$\begin{array}{ccc} \mathcal{L} & \longrightarrow & \mathcal{L}/\mathcal{L}' \\ {\scriptstyle \varphi_{L/K}}\downarrow & & \downarrow{\scriptstyle \varphi_{L'/K}} \\ K^*/N(L^*) & \longrightarrow & K^*/N(L'^*) \end{array}$$

et le fait que $\varphi_{L/K}$ et $\varphi_{L'/K}$ sont des isomorphismes sur (th.3) montrent aussitôt que $H'=N_{L'/K}(L'^*)$.

Lemme 2 .- Soient C une extension abélienne de K localement compact , et L une extension abélienne de C ; il existe une extension abélienne F de K (contenant C) telle que $N_{F/K}(F^*)=N_{L/K}(L^*)$.

Soit H le sous-groupe des éléments $x\in C$ tels que $N_{C/K}(x)\in N_{L/K}(L^*)$; il contient $N_{L/C}(L^*)$ d'après la transitivité des normes ; il existe donc (lemme 1) une extension abélienne U de C telle que $N_{U/C}(U^*)=H$. Montrons que U est extension galoisienne de K ; soit en effet s un K-automorphisme de la clôture algé-

brique de K ; on a $s(C)=C$ et $s(H)=H$; d'où $N_{s(U)/C}(s(U)^*)=N_{s(U)/s(C)}(s(U)^*)=$ $=s(N_{U/C}(U^*))=s(H)=H=N_{U/C}(U^*)$; ceci implique $s(U)=U$ d'après le théorème d'unicité (th.4) , et U est galoisienne sur K . Il est clair que $N_{U/K}(U^*)=N_{L/K}(L^*)$. Il suffit alors de prendre pour F la plus grande extension abélienne de K contenue dans U (th.4).

THÉORÈME 5 (théorème d'existence) .- *Soient K un corps localement compact , H un sous-groupe d'indice fini de K^* ; il existe une extension abélienne F de K telle que $N_{F/K}(F^*)=H$ lorsque l'une des deux conditions suivantes est satisfaite*

a) *K est un corps P-adique .*

b) *K est un corps de séries formelles sur un corps fini de caractéristique étrangère à n .*

Soit R le corps obtenu en adjoignant à K les racines n-èmes de l'unité ; c'est une extension abélienne de K (Alg.,chap.V,§ 11) et , dans les hypothèses faites l'indice $(R^*:R^{*n})$ est fini (§ 2,n°7) . Soit U l'extension obtenue en adjoignant à R toutes les racines n-èmes d'éléments de R^*. Décomposons le groupe R^*/R^{*n} en produit direct de groupes cycliques G_i ; ceux-ci sont d'ordre $n(i)$ diviseurs de n ; soit x_i un représentant dans R^* d'un générateur de G_i . En adjoignant à R les racines n-èmes de x_i , on obtient une extension cyclique Z_i de degré $n(i)$ (Alg.,chap.V,§ 11) ; et U est extension composée des Z_i ; elle est donc abélienne finie , et de degré $\leqslant \prod n(i)=(R^*:R^{*n})$. Montrons que l'on a l'égalité $[U:R]=(R^*:R^{*n})$; ceci vient d'être vu lorsque R^*/R^{*n} est cyclique; procédons par récurrence sur le nombre de facteurs cycliques G_i de R^*/R^{*n} ; tout revient à montrer que , dans Z_1^* , les seules relations de la forme $\prod_{i\neq 1} x_i^{s(i)} \in Z_1^{*n}$ sont celles où $s(i)$ est multiple de $n(i)$; or ceci résulte du fait que $(Z_1^{*n})\cap R^*$ est le sous-groupe engendré par R^{*n} et x_1 (Alg.,chap.V,§ 11, prop.6) . Comme $N_{Z_i/R}(Z_i^*)$ contient R^{*n} , il en est de même de $N_{U/R}(U^*)$ (cor. du th.5) ; donc $R^{*n}=N_{U/R}(U^*)$ d'après le th. d'isomorphisme .

Passons maintenant à la démonstration proprement dite du th.6 . Désignons par H_1 le sous-groupe des éléments x de R^* tels que $N_{R/K}(x)\in H$. Comme H contient

NBR 073

K^{*n} , H_1 contient R^{*n} . D'après le lemme 1 et ce qui vient d'être vu , H_1 est donc de la forme $N_{L/R}(L^*)$, L étant une extension abélienne de R . Alors $N_{L/K}(L^*)=N_{R/K}(H_1)$ est un sous-groupe H' de K^* contenu dans H . Or (lemme 2) H' est de la forme $N_{F'/K}(F'^*)$, où F' est une extension abélienne de K . Comme $H \supset H'$, H est donc aussi le groupe des normes d'une extension abélienne de K (lemme 1) . CQFD

8 . La Führerdiskriminantenformel .

Commentaire . Le rédacteur s'excuse de présenter à son Illustre Maître un exposé aussi peu bourbachique . Il a eu un mal de chien à comprendre les astuces de Hasse , mais a été incapable d'en extirper le caractère d'astuces . Il fait remarquer que le cas "cyclique de degré premier" se rédige de façon moins lourde (mais les astuces essentielles y restent) ; on pourrait peut-être se contenter de ce cas qui est suffisant pour le théorème d'existence pour les séries formelles (cf.ci-dessous) , - et qui peut remplacer la démonstration de l'inégalité fondamentale (c.à.d. la prop.2 du n°1 , elle-même assez pénible) ; il est vrai qu'on perd ainsi divers jolis résultats du cas général ; les simplifications d'exposé seront notées au passage . Au début on ne suppose rien du corps de classes .

A) Le point sur lequel porte la démonstration .

Soit K une extension galoisienne finie d'un corps localement compact K' ; notations usuelles A,P,A',P',k et k' . On se propose d'étudier le groupe quotient $K'^*/(1+P'^h)N(K^*)$: pour cela on le dévisse en $K'^*/U'N(K^*)$, en $U'N(K^*)/(1+P')N(K^*)$ et en les $(1+P'^u)N(K^*)/(1+P'^{u+1})N(K^*)$ $(1 \leqslant u \leqslant h-1)$. Ces groupes sont finis : c'est clair pour le premier (il y a des normes de tous les ordres multiples de f) ; les autres sont isomorphes à $U'/(U' \cap (1+P')N(K^*))$ et $(1+P'^u)/((1+P'^u) \cap (1+P'^{u+1})N(K^*))$ qui sont des quotients de $U'/(1+P')$ (isomorphe à k'^*) et de $(1+P'^u)/(1+P'^{u+1})$ (isomorphe à k' additif) . Notons B_u le sous-groupe multiplicatif $\bar{N}^{-1}(1+P'^u)$; les groupes en question sont $U'/(1+P')N(U'$ et $(1+P'^u)/(1+P'^{u+1})N(B_u)$.

Pour tout u il existe évidemment un entier v tel que $N(1+P^v) \subset 1+P'^u$ (nous en déterminerons un avec précision tout à l'heure) , donc tel que $1+P^v \subset B_u$; ainsi $N(B_u)(1+P'^{u+1}) \supset N(1+P^v)(1+P'^{u+1})$, et l'indice $((1+P'^u)N(K^*):(1+P'^{u+1})N(K^*)) = ((1+P'^u):(1+P'^{u+1})N(B_u))$ est inférieur à $((1+P'^u):N(1+P^v)(1+P'^{u+1}))$. Pour la fonction v de u qui sera définie plus loin, nous montrerons que ce dernier indice est "presque toujours égal à 1" , et nous en trouverons une borne supérieure dans les autres cas . Ceci montrera que , pour h assez grand , l'indice $(K'^*:(1+P'^h)N(K^*))$ reste constant, donc (puisque $N(K^*)$ est un sous-groupe fermé de K'^* , et par suite intersection de ses voisinages $(1+P'^h)N(K^*)$) , que $N(K^*)$ contient un $1+P'^h$ pour h assez grand ; nous déterminerons aussi , dans le cas abélien , le plus petit h avant cette propriété : l'idéal P^h est alors appelé le Führer de l'extension .

B) Une mirificque formule normo-tracique .

Soit x un élément de K . On a

(a) $N(1+x) = 1+G_1(x)+\ldots+G_n(x)$ $\quad (n=[K:K'])$

où $G_j(x)$ est la somme , étendue aux combinaisons j à j des éléments du groupe de Galois $\mathcal{G}$ de K , des $x^{s_1+s_2+\ldots+s_j}$ ($s_i \in \mathcal{G}$; notation d'Alg., chap. V, § 6, n°10) Faisons opérer $\mathcal{G}$ sur ces combinaisons (ou éléments de l'algèbre de $\mathcal{G}$ sur Z) : $(s_1+\ldots+s_n)s = s_1s+\ldots+s_js$. Soit C une classe d'intransitivité de cet ensemble de combinaisons , et soit $\mathcal{J}(C)$ le sous-groupe de $\mathcal{G}$ laissant chaque élément de C invariant . Deux cas peuvent se produire :

a) La combinaison $S(\mathcal{J}(C)) = \sum_{s \in \mathcal{J}(C)} s$ figure dans la classe C . Les éléments de C sont alors les combinaisons $S(\mathcal{J}(C).s)$ des classes à droite de $\mathcal{G}$ mod. $\mathcal{J}(C)$. Notons que deux sous-groupes distincts $\mathcal{J}$, $\mathcal{J}'$ de $\mathcal{G}$ donnent des classes C distinctes . Soit $\bar{K}$ le corps des invariants du sous-groupe $\mathcal{J}$; la contribution à la somme $G_j(x)$ de la classe d'intransitivité C correspondante est alors évidemment $Tr_{\bar{K}/K'}(N_{K/\bar{K}}(x))$.

b) Dans le cas contraire les éléments de la classe C sont des sommes de plusieurs termes , de la forme $S(\mathcal{J}(C).s_1)+\ldots+S(\mathcal{J}(C).s_q)$. En notant encore $\bar{K}$

le corps des invariants de $\mathcal{J}(C)$, la contribution à $G_j(x)$ de la classe d'intransitivité C est de la forme $\mathrm{Tr}_{\overline{K}/K'}(N_{K/\overline{K}}(x^{s_1}x^{s_2}..x^{s_q}))$ avec $q \geqslant 2$.

En résumé on a la formule suivante :

(b) $N_{K/K'}(1+x)=1+\sum_{\overline{K}}{}' \mathrm{Tr}_{\overline{K}/K'}(N_{K/\overline{K}}(x))+$

$$+\sum_{\overline{K}}{}' \Big(\sum_{s_1,..,s_q}{}' \mathrm{Tr}_{\overline{K}/K'}(N_{K/\overline{K}}(x^{s_1}..x^{s_q}))\Big) .$$

les sommes $\sum_{\overline{K}}{}'$ étant étendues à tous les corps intermédiaires $\overline{K}$ entre K et K', et la somme $\sum_{s_1..s_q}{}'$ étant étendue à certaines combinaisons de q éléments du groupe de Galois $\mathcal{G}$ $(q \geqslant 2)$.

L'intérêt de ceci est le suivant : prenons pour x un élément de l'idéal P^v $(v \geqslant 1)$: alors le produit $x^{s_1}..x^{s_q}$ appartient au moins à P^{2v} , et en tout cas à P^{v+1} . On a donc

(c) $N_{K/K'}(1+x)=1+\sum_{\overline{K}}{}' \mathrm{Tr}_{\overline{K}/K'}(N_{K/\overline{K}}(x))+\sum_{\overline{K}}{}' \Big(\sum_{\alpha}{}' \mathrm{Tr}_{\overline{K}/K'}(N_{K/\overline{K}}(y_\alpha))\Big)$

où les y_α appartiennent à P^{v+1} si $x \in P^v$ $(v \geqslant 1)$.

Et les termes de la sommation double sont dans des puissances suffisamment hautes de P' pour ne pas gêner .

Cas cyclique de degré premier .- On voit aussitôt que , si $x \in P^v$, on a aussi $N(1+x)=1+\mathrm{Tr}(x)+N(x)+\mathrm{Tr}(y)$, où $y \in P^{2v}$ (ça résulte aussi de (c) , car ici $\overline{K}$ est , soit K , soit K').

C) Une miraculeuse fonction , qui se trouve être linéaire par morceaux .

Nous supposerons d'abord que K est complètement ramifiée sur K' ; posons $n=[K:K']$. Notons K_j le j-ème corps de ramification de K sur K' , et $n(j)=[K:K_j]$ Rappelons que n(j) est l'ordre du j-ème groupe de ramification de K sur K' , c'est-à-dire de l'ensemble des $s \in \mathcal{G}$ tels que $s(a)-a \in P^{j+1}$ pour tout $a \in A$ (§ 3, n°2) ; comme K est complètement ramifiée , on a $K_0=K'$ et $n(0)=n$. Pour tout nombre réel $t \geqslant -1$, nous poserons $n(t)=n(j)$, j désignant le plus petit entier $\geqslant t$. Et nous considérerons la fonction

(d) $u(v)=n^{-1}\int_0^v n(t)dt$.

Comme $n(t) \geqslant 1$, la fonction u(v) est strictement croissante (et linéaire par morceaux , puisque n(t) est constante par morceaux) .

Considérons maintenant un corps intermédiaire $\overline{K}$. La théorie de Galois montre aussitôt que son j-ème corps de ramification est $\overline{K}(K_j)$; posons $\overline{n}(j)=[K:\overline{K}(K_j)]$ (c'est un diviseur de $n(j)$) . On a encore $\overline{n}(0)=\overline{n}=[K:\overline{K}]$; d'où $[\overline{K}:K']=n/\overline{n}$.

La formule de Hilbert donnant l'exposant différentiel $m(K,K')$ de K sur K' (§ 5, n°4) peut s'écrire (puisque $n(t)=1$ pour t assez grand) :

(e) $\quad m(K,K')=\int_{-1}^{+\infty}(n(t)-1)dt$.

De même $m(K,\overline{K})=\int_{-1}^{+\infty}(\overline{n}(t)-1)dt$. Et la formule de transitivité des différentes $m(K,K')=m(K,\overline{K})+e(K,\overline{K})m(\overline{K},K')$ (§ 5,n°3) donne :

(f) $\quad m(\overline{K},K')=\overline{n}^{-1}\int_{-1}^{+\infty}(n(t)-\overline{n}(t))dt$.

Considérons $N_{K/K'}(1+P^v)$ et $N_{K/K'}(1+P^{v+1})$, et appliquons-leur la formule (c) de B) . On a $N_{K/\overline{K}}(P^v)\subset\overline{P}^v$ et $N_{K/\overline{K}}(P^{v+1})\subset\overline{P}^{v+1}$. D'après la théorie de la différente (§ 5,n°3) , pour que l'on ait $\mathrm{Tr}(\overline{P}^v)\subset P'^u$ (resp. $\mathrm{Tr}(\overline{P}^{v+1})\subset P'^{u+1}$, il faut et il suffit que l'on ait $(n/\overline{n})u-v\leqslant m(\overline{K},K')$ (resp. $(n/\overline{n})(u+1)-(v+1)\leqslant m(\overline{K},K')$) . La seconde inégalité entraîne d'ailleurs la première ; et , sauf s'il y a égalité dans cette seconde inégalité , on a $\mathrm{Tr}(\overline{P}^v)\subset P'^{u+1}$. Nous allons étudier ceci lorsque u est lié à v par la formule (d) . Un facile calcul donne alors

(g) $\quad (n/\overline{n})(u+1)-(v+1)=(1/\overline{n})\int_{-1}^{v}(n(t)-\overline{n})dt$

En comparant avec (f) on en déduit que la quantité à étudier , $\overline{n}(m(\overline{K},K')-(n/\overline{n})(u+1)+(v+1))$ vaut $\int_{-1}^{+\infty}(n(t)-\overline{n}(t))dt-\int_{-1}^{v}(n(t)-\overline{n})dt$, c'est-à-dire:

(h) $\quad \int_{-1}^{v}(\overline{n}-\overline{n}(t))dt+\int_{v}^{+\infty}(n(t)-\overline{n}(t))dt$.

Cette quantité est positive , puisque $\overline{n}(t)\leqslant\overline{n}$ et que $\overline{n}(t)$ divise $n(t)$; d'où l'inégalité cherchée , et les inclusions

(i) $\quad \mathrm{Tr}(\overline{P}^v)\subset P'^u$, $\mathrm{Tr}(\overline{P}^{v+1})\subset P'^{u+1}$.

Pour qu'il y ait égalité , il faut et il suffit que l'on ait $\overline{n}(t)=\overline{n}$ pour $-1\leqslant t\leqslant v$, et $\overline{n}(t)=n(t)$ pour $t>v$. En d'autres termes la condition d'égalité est $\overline{n}(v')=\overline{n}(0)$ pour tout entier $v'\leqslant v$, et $\overline{n}(v'')=n(v'')$ pour tout entier $v''\geqslant v+1$; ceci se traduit par $\overline{K}(K_{v'})=\overline{K}$ et $\overline{K}(K_{v''})=K_{v''}$, ou encore $K_{v'}\subset\overline{K}\subset K_{v''}$, qui est équivalent à

(j) $\quad K_v\subset\overline{K}\subset K_{v+1}$.

Or , la fonction $n(t)$ est constante par morceaux , avec des sauts en un nombre

fini de points entiers $v_1,\dots,v_r$ (qui sont les nombres de ramification définis au § 3,n°2) ; on pose $v_0=-1$, $v_{r+1}=+\infty$; la fonction $n(t)$ est constante pour $v_{j-1}<t\leqslant v_j$. Donc , pour qu'il y ait égalité :

1) Ou bien l'entier v est distinct des v_j $(1\leqslant j\leqslant r)$ et alors $\overline{K}=K_v$.

2) Ou bien v est l'un des v_j $(1\leqslant j\leqslant r)$, et alors $K_v\subset\overline{K}\subset K_{v+1}$.

D) Application à l'étude de $(1+P'^u)/(1+P'^{u+1})N(1+P^v)$.

Nous continuons à supposer K complètement ramifiée sur K' , et u et v liés par la formule $u(v)=(1/n)\int_0^v n(t)dt$. Remarquons qu'à une valeur entière de v peut correspondre une valeur fractionnaire de u ; par contre , si u est entier , la valeur correspondante de v est entière , puisque n(t) divise n .Posons $u_j=u(v_j)$ $(1\leqslant j\leqslant r)$; ces nombres ne sont peut-être pas entiers .

Remarquons d'abord le cas où u et v sont $\geqslant 0$ (et entiers) . Il résulte de ce qui vient d'être vu , et de son application à la formule normotracique (e) , que l'on a (avec $x\in P^v$)

(k) $N(1+P^v)\subset 1+P'^u$, $N(1+P^{v+1})\subset 1+P'^{u+1}$

(k') $N(1+x)\equiv 1+Tr_{K_v/K'}(N_{K/K_v}(x))$ $(\mathrm{mod}.P^{u+1})$ lorsque u est distinct des u_j .

(k") $N(1+x)\equiv 1+\sum_{K_{v_j}\subset\overline{K}\subset K_{v_{j+1}}} Tr_{\overline{K}/K'}(N_{K/\overline{K}}(x))$ $(\mathrm{mod}.P'^{u+1})$ lorsque u est l'un des u_j qui sont entiers .

(en effet , les termes non écrits de (c) sont dans P'^{u+1} d'après la discussion faite en C)) . Il résulte aussi de cette discussion que chaque trace figurant au second membre de (k') ou (k") est exactement d'ordre u (pour P') pour un x convenable de P^v .

Etudions ce que donne (k') . Soit a un élément de A' . La classe de $N(1+ax)$ mod.$(1+P'^{u+1})$ ne dépend que de celle de a mod.P' . On a $N(1+ax)\equiv 1+a^{n(v)}\cdot Tr_v(N_v(x))$ $(\mathrm{mod}.P'^{u+1})$ (Tr_v et N_v désignant ce qui est dans (k')) . Or on peut supposer $Tr_v(N_v(x))$ d'ordre u . Comme $v\geqslant 0$, l'entier n(v) est une puissance de la caractéristique p du corps des valeurs k (§ 3,n°3,b)) , la classe de $a^{n(v)}$ mod.P' parcourt k' tout entier en même temps que la classe de a mod.

NBL073

P' . Donc la classe de $N(1+ax)$ parcourt $(1+P'^{u})/(1+P'^{u+1})$ tout entier , et l'indice $((1+P'^{u}):N(1+P^{v})(1+P'^{u+1}))$ est égal à 1 .

Voyons maintenant ce que donne (k") . Avec a comme ci-dessus on a $N(1+ax)\equiv$ $\equiv 1+\sum_{\bar{K}} a^{\bar{n}}Tr_{\bar{K}}(N_{\bar{K}}(x))$ (mod.P'^{u+1}) pour $u=u_j$ et pour $K_{v_j}\subset\bar{K}\subset K_{v_{j+1}}$. On a alors $n(v_j+1)\mid\bar{n}\mid n(v_j)$. Comme $u=u_j>0$, $n(v_j)$ est une puissance de p , et donc aussi $\bar{n}$ et $\bar{n}/n(v_{j+1})$ (§ 3,n°3,b)) . Or , en prenant pour y un élément d'ordre u de P'^{u} , les applications $a\to 1+ax$ ($a\in A'$) et $b\to 1+by$ ($b\in A$) donnent , par passage aux quotients des isomorphismes de k (=k') additif sur $(1+P^{v})/(1+P^{v+1})$ et sur $(1+P'^{u})/(1+P'^{u+1})$. Au moyen de ces isomorphismes , l'homomorphisme $\bar{N}$ de $(1+P^{v})/(1+P^{v+1})$ sur $N(1+P^{v})/(1+P'^{u+1})$ (déduit de $N_{K/K'}$ par passage aux quotients se transforme en l'endomorphisme (additif) de k défini par $z\to\sum_{\bar{K}}\lambda_{\bar{K}}z^{\bar{n}}$, où $\lambda_{\bar{K}}$ désigne la classe mod.P' de $y^{-1}.Tr_{\bar{K}}(N_{\bar{K}}(x))$. Le noyau de cet endomorphisme g est formé par les racines de l'équation $\sum_{\bar{K}}\lambda_{\bar{K}}z^{\bar{n}}=0$; celle-ci n'est pas identiquement vérifiée d'après ce qu'on a vu plus haut ; son degré est au plus $n(v_j)$ et tous les exposants $\bar{n}$ sont des puissances de p multiples de $n(v_j+1)$; donc l'ordre du noyau de g est $\leqslant n(v_j)/n(v_j+1)$. Par conséquent l'indice dans k de l'image g(k) est $\leqslant n(v_j)/n(v_j+1)$. Autrement dit , l'indice $((1+P'^{u}):N(1+P^{v})(1+P'^{u+1}))$ est $\leqslant n(v_j)/n(v_j+1)$ pour $u=u_j$, $v=v_j$ (si u_j est entier) .

E) Etude des cas laissés de côté , et conclusions dans le cas galoisien .

Examinons $U'/(1+P')N(U)$ (par abus de langage , on peut appelre ça le cas $u=v=0$) . Il est clair que $N(1+P)\subset 1+P'$. Supposons encore K complètement ramifiée. Si $v_1>0$ (et alors $u_1>0$) , le groupe d'inertie est un groupe de ramification supérieure , et son ordre n est une puissance de p . La classe de $N(x)$ ($x\in U$) mod.P est celle de x^{n} puisque k=k' ; donc elle parcourt k^{*} en même temps que celle de x ; donc $U'=(1+P')N(U)$. Lorsque $v_1=u_1=0$, $n(1)$ est distinct de $n(0)$, et $n(0)/n(1)$ est le produit des facteurs étrangers à p de $n(0)$ (§ 3,n°2,prop.4) soit q le nombre d'éléments de k ; comme $N(x)\equiv x^{n}$ (mod.P') ($x\in U$) , le sous-groupe $(1+P')N(U)/(1+P')$ de $U'/(1+P')$ correspond à celui des puissances n-èmes

de k^* au moyen de l'isomorphisme $U'/(1+P') \to k^*$; son indice est donc $(n, q-1) = (n(0)/n(1), q-1)$ (car $q-1$ est étranger à p) , et est inférieur à $n(0)/n(1)$. Donc les conclusions de D) restent valables pour $u=v=0$.

Débarrassons-nous enfin de l'hypothèse que K est complètement ramifiée . Notons K" le corps d'inertie de K sur K' (notations standard P",A",U",k"). Il va nous suffira , en vertu de la transitivité des normes , que l'application $\bar{N}$ de $(1+P''^u)/(1+P''^{u+1})$ dans $(1+P'^u)/(1+P'^{u+1})$ déduite de $N_{K''/K'}$ par passage aux quotients soit une application sur . Pour $u>0$ prenons x d'ordre u pour P' et $y \in A''$; alors $N_{K''/K'}(1+xy) \equiv 1+xTr(y) \pmod{P'^{u+1}}$; on conclut en se souvenant que tout élément de k' est trace d'un élément de k" (Alg., chap.V, § 11, cor. du th.3) . Pour $u=0$ on voit que $\bar{N}(U''/(1+P'')) \subset U'/(1+P')$ en se souvenant que tout élément de k' est norme d'un élément de k" .

On a donc le résultat suivant :

THÉORÈME 7 .- Soient K' un corps localement compact , K une extension galoisienne finie de K' . Notons $n(j)$ l'ordre du j-ème groupe de ramification de K , et pour $t > -1$, posons $n(t)=n(j)$, j étant le plus petit entier $\geqslant t$. Soit $u(v)$ la fonction $(1/n(0))\int_0^v n(t)dt$. Soient $v_1, \ldots, v_r$ les nombres de ramification de K (c.à.d. les points de discontinuité de la fonction $n(t)$) . On pose $1+P^0=U$, $1+P'^0=U'$, $u_i=u(v_i)$. Alors :

a) $N(1+P^v) \subset 1+P'^u$, $N(1+P^{v+1}) \subset 1+P'^{u+1}$.

b) $((1+P'^u)N(K^*):(1+P'^{u+1})N(K^*)) \leqslant ((1+P'^u):N(1+P^v)(1+P'^{u+1}))$.

c) L'indice $((1+P'^u):N(1+P^v)(1+P'^{u+1}))$ est inférieur à $n(v)/n(v+1)$. Il ne peut donc être distinct de 1 que si u est l'un des u_i qui sont entiers .

d) Pour $u \geqslant u_r+1$, l'indice $(K'^*:(1+P'^u)N(K^*))$ garde une valeur constante inférieure à $[K:K']$.

e) Le sous-groupe $N(K^*)$ contient $1+P'^{u_r+1}$ et est d'indice fini $\leqslant [K:K']$ dans K'^*.

Remarque .- Dans le cas cyclique de degré premier n (complètement ramifié) , notons d le minimum de l'ordre de $s(a)-a$ ($s \neq 1$, $a \in A$). L'exposant différentiel est alors $n(d-1)$. Les $d-1$ premiers groupes de ramification sont égaux au groupe de Galois , et les autres réduits à (1) .

Les nombres de ramification sont $v_0=-1$ et $v_1=d-1$. On a $u(v)=v$ pour $-1 \leqslant v \leqslant d-1$, et $u(v)=(v+(d-1)(e-1))/n$ pour $v \geqslant d-1$. Le sous-groupe $N(K^*)$ contient $1+P'^d$. Peu de simplifications essentielles dans les démonstrations .

F) Le cas abélien .

On applique alors le résultat suivant du corps de classes : $(K'^*:N(K^*))=[K:K']$ Les résultats d) et e) du th.7 montrent que les inégalités données en b) et c) doivent être toutes des égalités . Donc :

THÉORÈME 8 .- Les notations étant celles du th.7 , supposons de plus que K soit extension abélienne de K' . Alors :

a) Les nombres u_i sont tous entiers ; autrement dit $v_{i+1}-v_i$ est multiple de $n(0)/n(v_{i+1})$.

b) Pour tout $u \geqslant 0$, on a $((1+P'^u)N(K^*):(1+P'^{u+1})N(K^*))=((1+P'^u):(1+P'^{u+1}).N(1+P^v))=n(v)/n(v+1)$.

c) Le plus grand idéal P'^s tel que $N(K^*) \supset 1+P'^s$ est P'^{u_r+1} . C'est là le Führer ; Sieg! Heil!!

9 . Le théorème d'existence ; cas des séries formelles .

THÉORÈME 9 .- Soit K un corps de séries formelles sur un corps fini k à $q=p^f$ éléments . Pour tout sous-groupe H d'indice fini de K^* , qui contienne un sous-groupe $1+P^u$ (c.à.d. un sous-groupe ouvert de K^*) , il existe une extension abélienne finie E de K telle que $N_{E/K}(E^*)=H$.

Le rédacteur ne sait pas s'il peut exister des sous-groupes d'indice fini de K^* qui ne soient pas ouverts . Le th.6 montre qu'il n'y en a pas qui soient d'indice étranger à p (car un groupe de normes est ouvert , puisqu'il y a un Führer).

En considérant la composante p-primaire H'/H de K^*/H et un supplémentaire H"/H de celle-ci , le fait que H" est groupe de normes (th.6) et le cor. au th.5 montrent qu'il suffit de prouver que H' est un groupe de normes , c.à.d. de démontrer le th.9 dans le cas où l'indice de H est une puissance p^j de p . Par récurrence sur j on se ramène au cas où $(K^*:H)=p$. En effet si H est d'indice p^j , il existe un groupe H' contenant H et d'indice p . Donc il existe

une extension abélienne L' telle que $N_{L'/K}(L'^*)=H'$. Le sous-groupe $N^{-1}_{L'/K}(H)$ est d'indice p^{j-1} dans L'^* ; donc , d'après l'hypothèse de récurrence , il existe une extension abélienne L'' de L' telle que $N_{L''/L'}(L''^*)=N^{-1}_{L'/K}(H)$, donc telle que $N_{L''/K}(L''^*)\subset H$. Le lemme 2 au th.6 (n°7) montre alors qu'il existe une extension abélienne E de K telle que $N_{E/K}(E^*)\subset H$, et le lemme 1 au th. 6 qu'il existe une sous-extension abélienne F de E telle que $N_{F/K}(F^*)=H$.

Nous sommes ainsi ramenés au cas où H est d'indice p et contient un $1+P^u$. Alors f, s étant un entier assez grand , H contient $K^{*p}(1+P^{sp})$. D'après le lemme 1 au th.6 , il va nous suffire de montrer que $K^{*p}(1+P^{sp})$ est un groupe de normes . Son indice $(K^*:K^{*p}(1+P^{sp}))$ vaut $p.(U:U^p(1+P^{sp}))=pq^{s(p-1)}$ puisque U se compose de toutes les séries formelles inversibles n'ayant que des termes de degrés multiples de p .

Considérons un élément $a\in P^{-sp}$ et l'équation $X^p-X=a$; si x est une de ses racines , les autres sont évidemment $x+1,..,x+p-1$; donc l'extension K(x) est cyclique de degré p (lorsque $x\notin K$) . Il est clair que $N(K(x))\supset K^{*p}$. Pour montrer que $N(K(x))\supset 1+P^{sp}$ considérons un élément c d'ordre s de K ; en posant $x=y/c$, le polynôme minimal F de y sur K est $y^p-c^{p-1}y-ac^p$, et y est entier sur A ; on a $v(F'(y))=v(c^{p-1})=(p-1)s$ (si la valuation v est normée sur K) ; donc l'exposant différentiel m de K(x) sur K est $\leq p(p-1)s$ (§ 5,n°3,prop.3) ; il en résulte (remarque suivant le th.7) que le conducteur de $\varphi(x)$ contient P^{sp} . Ainsi $N(K(x))\supset K^{*p}(1+P^{sp})$. Nous allons alors considérer l'extension E composée de toutes les K(x) où $x^p-x\in P^{-sp}$; ce qui précède et le th. d'ordination (th.4) montrent que c'est une extension abélienne finie de K . Pour montrer que $N(E)=K^{*p}(1+P^{sp})$ il suffira , d'après le th. d'unicité (th.4) , de faire voir que $[E:K]=(K^*:K^{*p}(1+P^{sp}))=pq^{s(p-1)}$.

Or , en notant W l'endomorphisme (additif) $x\to x^p-x$ de E , on a $(P^{-sp}+W(K):W(K))=(P^{-sp}:(W(K)\cap P^{-sp}))=(P^{-sp}:W(P^{-s}))=(P^{-sp}:P)/(W(P^{-s}):W(P))$ (car $W(P)=P$ d'après Hensel)$=q^{sp+1}/p^{-1}.q^{s+1}$ (car le noyau de W est le corps premier) $=pq^{s(p-1)}$. Il nous suffira donc de démontrer le lemme suivant :

NBR073

Lemme .- Soit C un sous-groupe additif de K tel que $(C+W(K))/W(K)$ soit fini ; alors $[K(\tilde{W}^{-1}(C)):K]=(C+W(K):W(K))$.

Soient $c_1,\dots,c_n$ des éléments de C dont les classes forment une base de $(C+W(K))/W(K)$ sur le corps premier F_p , et soit x_i un élément de $E=K(\tilde{W}^{-1}(C))$ tel que $x_i^p-x_i=c_i$. Comme $\tilde{W}^{-1}(C)$ est contenu dans le groupe additif engendré par K et les x_i , on a $E=K(x_1,\dots,x_n)$. Il va nous suffira , par récurrence sur n , de montrer que $x_n\notin K(x_1,\dots,x_{n-1})$ (car alors $[E:K(x_1,\dots,x_{n-1})]=p$, et $[E:K]=p^n$) , c'est-à-dire que $c_n\notin W(K(x_1,\dots,x_n))$. Or , si K est un corps de caractéristique p , c un élément de K , et x une racine de $X^p-X-c=0$, on a $K\cap W(K(x))=W(K)+cF_p$: en effet , si $y^p-y=b\in K$ $(y\in K(x))$, on a , en notant s un générateur du groupe de Galois de K(x) sur K , $s(y^p-y)=y^p-y$, c'est-à-dire $(y-s(y))^p=y-s(y)$, ou $s(y)=y+j$ $(j\in F_p)$; or $s(x)=x+1$; donc $s(jx)=jx+j$ et $s(y-jx)=y-jx$; autrement dit $y\in xF_p+K$, ou $b\in cF_p+W(K)$. Donc , si c_n appartenait à $W(K(x_1,\dots,x_{n-1}))$, il appartiendrait à $(c_{n-1}F_p+W(K(x_1,\dots,x_{n-2}))\cap K=c_{n-1}F_p+(W(K(x_1,\dots,x_{n-2}))\cap K)=$ $=c_{n-1}F_p+c_{n-2}F_p+\dots+c_1F_p+W(K)$ par applications successives ; ceci est contraire à l'hypothèse faite sur les c_i . CQFD

OUF§§§§
