# RÉDACTION N° 171

COTE : NBR 072

TITRE : RAPPORT D'ALGÈBRE UNIDIMENSIONNELLE
CHAPITRE II : ARITHMÉTIQUE DES CORPS
DE NOMBRES ALGÉBRIQUES

ASSOCIATION DES COLLABORATEURS DE NICOLAS BOURBAKI

NOMBRE DE PAGES : 73

NOMBRE DE FEUILLES : 73

(171)

RAPPORT D'ALGÈBRE UNIDIMENSIONNELLE

# CHAPITRE II

# ARITHMÉTIQUE DES CORPS DE NOMBRES ALGÉBRIQUES

## Sommaire



## Commentaires (par un des rédacteurs).

Le rédacteur susdit s'excuse humblement de ne présenter à son illustre Maître qu'une moitié de chapitre . Le plan prévu pour la fin du chapitre comprendra , s'il plaît à Bourbaki , les §§ suivants :

§ 4 : La théorie du corps de classes global : III . Théorèmes de transfert .

§ 5 : Théorie et applications des séries L .

§ 6 : Algèbres simples sur un corps de nombres algébriques .

§ 7 : Formes quadratiques sur un corps de nombres algébriques .

Le rédacteur , n'ayant pu prendre connaissance de la littérature ultérieure , s'excuse du caractère déjà désuet de la partie cohomologique de la démonstration

# CHAPITRE II

## ARITHMÉTIQUE DES CORPS DE NOMBRES ALGÉBRIQUES

### § 1 . Divisibilité dans un corps de nombres algébriques .

1 . Valeurs absolues et idèles .

Un corps de nombres algébriques K est une extension algébrique de degré fini n du corps Q des nombres rationnels . On sait que l'ensemble $\Phi_0$ de toutes les valeurs absolues de Q , formé de la valeur absolue ordinaire $|x| = |x|_\infty$ , et des valeurs absolues p-adiques $|x|_p = p^{-v_p(x)}$ ($v_p(x)$ exposant de p dans x) vérifie la condition (P) du chap.I, § 4 , et la formule du produit

$$(1) \qquad \prod_{p \in \Phi_0} |x|_p = 1 \ .$$

($\Phi_0$ étant identifié à un ensemble somme de l'ensemble des nombres premiers et du symbole $\infty$ ) . Il en résulte (chap.I, § 4, n°2) que , si $\Phi$ est l'ensemble de toutes les valeurs absolues $|x|_P$ sur K (normées par la condition de prolonger les valeurs absolues de $\Phi_0$) , on a la formule du produit

$$(2) \qquad \prod_{P \in \Phi} |x|_P^{n(P)} = 1$$

où n(P) est le degré local de K sur Q , correspondant à P (degré du complété $K_P$ de K pour P , sur le complété $Q_p$ de Q pour la valeur absolue p que prolonge P). Si $P_i$ ($1 \leq i \leq s$) sont les valeurs absolues qui prolongent une même valeur absolue $p \in \Phi_0$ , on sait (chap.I, § 2, n°2, formule (10)) qu'on a la relation des degrés

$$(3) \qquad \sum_{i=1}^{s} n(P_i) = n \ .$$

Les valeurs absolues de K qui prolongent la valeur absolue $\infty$ sont encore dites (par abus de langage) places à l'infini ; elles forment une partie finie $\Phi_\infty$ de $\Phi$ . Pour une telle place P , le corps $K_P$ est égal à R ou à C ; nous désignerons par $r_1$ (resp. $r_2$) le nombre de places à l'infini P telles que $K_P = R$ (resp. $K_P = C$); on a donc $r_1 + 2r_2 = n$ d'après (3) . Si K est supposé plongé dans C , l'une des valeurs absolues $|x|_P$ pour un $P \in \Phi_\infty$ est égale à la valeur absolue ordinaire $|x|$ ;

les autres sont de la forme $|s_i(x)|$ , où $s_i$ $(1\leq i\leq n)$ sont les Q-isomorphismes de K dans C ; $r_1$ est le nombre des isomorphismes $s_i$ tels que $s_i(K)\subset R$ .

Pour tout nombre premier p , soit $\Phi_p$ l'ensemble des valeurs absolues $P_j$ $(1\leq j\leq g)$ qui prolongent $|x|_p$ ; la réunion des $\Phi_p$ est le complémentaire de $\Phi_\infty$ , que nous noterons $\Phi_{fin}$ et dont nous appellerons les éléments les places finies de K ; rappelons qu'on note P|p la relation "P prolonge p" . Pour tout $x\in K$ , on a (chap.I, § 2, formule (19))

$$|N_{K/Q}(x)| = \prod_{j=1}^{g} |x|_{P_j}^{n(P_j)} \quad . \tag{4}$$

Si P prolonge p , le corps $K_P$ est localement compact ; le corps résiduel correspondant $k_P$ est un corps fini , extension de degré f(P) de $F_p$ , qui a donc $p^{f(P)}$ éléments ; rappelons que f(P) est appelé le degré résiduel (ou simplement degré) de P sur p ; le nombre $p^{f(P)}$ est appelé norme absolue (ou norme) de la place P , et noté N(P) . Si e(P) est l'indice de ramification de P sur p , rappelons (chap.I, § 2, cor. à la prop.2) que e(P)f(P)=n(P) . Soit $v_P$ la valuation normée correspondant à P ; pour tout $x\in Q$ , on a $|x|_P=|x|_p=p^{-v_p(x)}=p^{-v_P(x)/e(P)}$ , et par suite $|x|_P^{n(P)}=p^{-f(P)v_P(x)}=(N(P))^{-v_P(x)}$ ; cette formule étant vraie dans Q , et définissant d'autre part sur K une valeur absolue qui prolonge $|x|_p^{n(P)}$ et est nécessairement une puissance de $|x|_P$ , on a , pour tout $x\in K$

$$|x|_P^{n(P)}=(N(P))^{-v_P(x)} \quad . \tag{5}$$

Les éléments de K qui sont entiers sur l'anneau Z sont appelés entiers algébriques de K . On sait que pour que $x\in K$ soit entier algébrique , il faut et il suffit que $|x|_P\leq 1$ pour toute place finie P ; l'anneau A des entiers algébriques est l'intersection des anneaux des valuations $v_P$ $(P\in\Phi_{fin})$ . Lorsqu'on parle de divisibilité dans K , il est sous-entendu (sauf mention expresse du contraire) qu'il s'agit de divisibilité par rapport à A ; pour que x|y , il faut et il suf-

fit donc que $|x|_P \geqslant |y|_P$ pour toute place finie P . Les unités de A (éléments inversibles de A) aussi appelées , par abus de langage , les unités du corps K , sont les $x \in K$ tels que $|x|_P = 1$ pour toute place finie P ; les unités telles que $|x|_P = 1$ pour toute place P (finie ou non) sont les unités absolues de K (ce sont les racines de l'unité dans K ; cf. chap. I, § 4, n°1) .

Rappelons que les idèles sont les éléments $z = (z_P)_{P \in \Phi}$ de l'anneau produit $\prod_{P \in \Phi} K_P$ tels que $z_P \neq 0$ pour toute place P , et $|z_P|_P = 1$ pour presque toute place P; on pose $|z|_P = |z_P|_P$ ; nous désignerons par $J_K$ (ou simplement J) le groupe multiplicatif des idèles . Tout élément $x \in K^*$ est identifié à l'idèle $z = (z_P)$ tel que $z_P = x$ pour toute place P (idèle principal associé à x) . On identifiera $K^*$ avec le groupe des idèles principaux , de sorte que $K^*$ est un sous-groupe de J .

Le groupe J peut être considéré comme sous-groupe du produit $\prod_{P \in \Phi} K_P^*$ ; rappelons que sur J on définit la topologie de produit direct local en prenant pour sous-groupe ouvert de $K_P^*$ le groupe $K_P^*$ lui-même si P est une place infinie , et le groupe compact $U_P$ des unités de $K_P$ si P est une place finie . Pour cette topologie , J est localement compact et $K^*$ un sous-groupe discret et fermé de J . On a un système fondamental de voisinages (compacts) de 1 dans J en prenant un nombre fini de places $P_i$ (comprenant toutes les places à l'infini) , des nombres réels $\varepsilon_i > 0$ , et en considérant les idèles $z = (z_P)$ tels que $|z_{P_i} - 1|_{P_i} \leqslant \varepsilon_i$ pour tout i , et $|z|_P = 1$ pour les autres places P .

Pour tout ensemble fini $S \subset \Phi$ contenant $\Phi_\infty$ , le sous-groupe $J_S = (\prod_{P \in S} K_P^*) \times (\prod_{P \notin S} U_P)$ est un sous-groupe ouvert de J (groupe des S-idèles) , sur lequel la topologie induite par celle de J est la topologie produit . On écrira $J_\infty$ au lieu de $J_{\Phi_\infty}$ ; le groupe des unités U de K est identifié à $K^* \cap J_\infty$ .

PROPOSITION 1 .- Si $0 < \alpha < 1 < \beta$ , l'ensemble V des idèles z tels que $\alpha \leqslant |z|_P \leqslant \beta$

pour toute place P est une partie compacte de J .

En effet , pour toute place finie P , la relation $\alpha \leq |z|_P \leq \beta$ pour un élément $z \in K_P$ s'écrit

$$-e(P).\log\beta/\log p \leq v_P(z) \leq -e(P).\log\alpha/\log p$$

et entraîne donc

$$-n.\log\beta/\log p \leq v_P(z) \leq -n.\log\alpha/\log p \ .$$

Comme $v_P$ ne prend que des valeurs entières , on voit donc que ces relations entraînent $v_P(z)=0$ sauf pour un ensemble fini S' de places finies P . Si $S=S' \cup \Phi_\infty$ on voit donc que $V \subset J_S$ ; en outre les projections de V sur les facteurs de $J_S$ sont évidemment compactes et V est le produit de ses projections .

COROLLAIRE .- Le groupe $U_o$ des unités absolues de K est identique au groupe des racines de l'unité de K et est fini .

La première assertion a déjà été démontrée (chap.I, § 4, n°1) . D'autre part , $U_o$ est l'intersection de $K^*$ et de l'ensemble compact (prop.1) des idèles tels que $|z|_P=1$ pour toute place P ; c'est donc un groupe compact et discret , donc fini .

2 . Diviseurs et idéaux .

Quand on parle de diviseurs de K , il est toujours sous-entendu qu'il s'agit des diviseurs relatifs à l'ensemble $\Phi_{fin}$ des places finies . Il est d'usage de noter ce groupe multiplicativement ; il est isomorphe à $Z^{(N)}$ et a pour base canonique l'ensemble des places finies $P \in \Phi_{fin}$ ; tout diviseur s'écrit donc d'une manière et d'une seule

$$a = \prod_{P \in \Phi_{fin}} P^{m_P(a)} \qquad (6)$$

où les $m_P(a)$ sont des entiers rationnels presque tous nuls ; si $m_P(a) \geqslant 0$ pour toute place finie P , on dit que a est un diviseur entier ; les diviseurs $P \in \Phi_{fin}$

sont appelés <u>divisaurs premiers</u> . La relation d'ordre dans le groupe D des diviseurs se note $a|b$ (et s'énonce "a divise b" ou "b est multiple de a") ; elle signifie donc que $m_P(a) \leq m_P(b)$ pour toute place finie P .

On sait qu'à tout idèle $z=(z_P)$ correspond un diviseur $a_z$ défini par les conditions $m_P(a_z)=v_P(z)$ pour toute place finie P ; l'application $z \to a_z$ est une représentation du groupe (non topologique) J <u>sur</u> le groupe D , dont le noyau est le groupe $J_\infty$ ; D est donc idomorphe à $J/J_\infty$ (algébriquement) . D'ailleurs comme $J_\infty$ est ouvert dans J , il est naturel de considérer D comme discret ; $z \to a_z$ est alors un homomorphisme (topologique) de J sur D .

On sait d'autre part que l'anneau A est un <u>anneau de Dedekind</u> (chap. des valuations) et que les <u>idéaux fractionnaires</u> $\neq 0$ de K (par rapport à A) forment un groupe multiplicatif I canoniquement isomorphe à D ; de façon précise , à tout diviseur a on fait correspondre l'idéal fractionnaire formé des $x \in K$ tels que $v_P(x) \geq m_P(a)$ pour toute place finie . Nous <u>identifierons</u> dans ce qui suit (sauf mention expresse du contraire) les groupes D et I au moyen de cet isomorphisme . Les places finies P sont identifiées aux <u>idéaux maximaux</u> de A (qui sont d'ailleurs les seuls idéaux premiers de A) ; en d'autres termes , P désigne aussi l'idéal de valuation (dans K) de la valuation $v_P$ . Les diviseurs entiers sont identifiés aux <u>idéaux de</u> A (idéaux entiers de K).L'idéal principal (x) (pour tout $x \in K^*$) est ainsi identifié au diviseur $a_x$,et appelé aussi <u>diviseur principal</u>;la relation de divisibilité $x|y$ dans K , équivalente à $(x) \supset (y)$,signifie aussi que $a_x|a_y$ ;par extension,lorsque $a_x$ divise un diviseur b (resp.que b divise $a_x$),on écrira $x|b$ (resp. $b|x$).Le groupe des idéaux principaux,isomorphe à $K^*/U=K^*/(K^* \cap J_\infty)$ est ainsi identifié au groupe $J_\infty K^*/J_\infty$ , image de $K^*$ dans $J/J_\infty = D$ .

A tout idéal principal Zx dans Q (identifié au diviseur correspondant dans Q) correspond par <u>extension</u> (chap.I,§ 3,n°5) l'idéal principal Ax de K ; cette identification est un isomorphisme du groupe multiplicatif des idéaux principaux

de Q (qu'on peut d'ailleurs identifier à $Q_+^*$) dans le groupe D ; on identifie généralement ce groupe à un sous-groupe de D, ce qui justifie la notation $P|p$ .

La norme d'un diviseur a de K par rapport à Q (dite aussi norme absolue) se note multiplicativement, et est identifiée au nombre rationnel

$$N(a)=\prod_{P\in\Phi_{fin}} (N(P))^{m_P(a)} \qquad (7)$$

(cf. chap. I, § 3, n°5) .

L'application $a\to N(a)$ est un homomorphisme de D dans $Q_+^*$ ; pour tout $x\in K^*$, on a

$$N((x))=N(a_x)=\left|N_{K/Q}(x)\right|=\prod_{P\in\Phi_\infty} |x|_P^{n(P)} \qquad (8)$$

comme il résulte aussitôt de la formule (4) et de l'hypothèse $N((x))>0$ .

Si on identifie un diviseur entier a avec l'idéal qui lui correspond , N(a) est aussi égale au nombre d'éléments de l'anneau quotient A/a (Alg., chap. VII, § 1, prop. 4). Si on considère A comme Z-module , on sait que A admet une base sur Z (Alg., chap. VII, § 3) ; le sous-module a de A admet donc aussi une base (loc. cit. et N(a) est égal au produit des facteurs invariants de a par rapport à A (Alg., chap. VII, § 4). Il en résulte (loc. cit.) que le déterminant $\Delta$ d'une base de a par rapport à la base canonique de $C^n$ (quand on considère K comme plongé dans le produit de ses conjugués) est égal au déterminant d'une base de A (par rapport à la base canonique de $C^n$) multiplié par N(a) . Or , le discriminant d de K est égal au carré du déterminant d'une base de A , d'où la formule $\Delta^2=d.(N(a))^2$ . Cette formule est d'ailleurs exacte pour un diviseur quelconque a de K , puisque un tel diviseur est de la forme yb, où b est un diviseur entier et $y\in Q^*$.

3 . Enoncé des théorèmes fondamentaux .

Les résultats les plus importants de la théorie des nombres algébriques sont :

THÉORÈME 1 .- Si K est un corps de nombres algébriques de degré n (sur Q) , le groupe localement compact $J/K^*$ (localement isomorphe à J) est isomorphe à un groupe de la forme $R\times G$ , où G est un groupe compact dont la composante connexe $G_0$ de 1 est isomorphe à $T^{n-1}$ .

THÉORÈME 2 .- Le groupe (abélien) compact totalement discontinu $G/G_0$ est isomorphe au groupe de Galois (topologique) d'une clôture abélienne de K .

Le th.2 est le résultat essentiel de la théorie du corps de classes (global) qui sera développée aux §° 2,3 et 4 . Dans ce §, nous allons démontrer le th.1 et en indiquer quelques conséquences .

Soit $P_0$ une place à l'infini de K . Dans le corps $K_{P_0}$ (isomorphe à R ou C) désignons par L le sous-groupe multiplicatif formé des multiples réels $>0$ de l'unité ; nous identifierons ce groupe à $R_+^*$ , et nous le considérerons comme sous-groupe fermé de J (le nombre réel $\lambda$ étant identifié à l'idèle z tel que $z_P = \lambda$ et $z_P=1$ pour $P\neq P_0$). Si à tout idèle z on fait correspondre le nombre $\lambda(z) = \prod_{P\in\Phi_0} |z|_P^{n(P)}$ si $n(P_0)=1$ et $(\lambda(z))^{\frac{1}{2}}$ si $n(P_0)=2$ , on définit un projecteur continu de J sur L , et par suite J est isomorphe au produit (topologique) $L\times H$ , où H est le noyau de ce projecteur , c'est-à-dire le sous-groupe fermé de J formé des idèles z tels que $\prod_P |z|_P^{n(P)}=1$. On a $K^*\subset H$ en vertu de la formule du produit ; par suite $J/K^*$ est isomorphe à $L\times(H/K^*)$, et $H/K^*$ est isomorphe à $J/LK^*$ . Notre but est de prouver que $J/LK^*$ est compact . Ce résultat est conséquence de la proposition suivante :

PROPOSITION 2 .- Il existe une constante $c>1$ telle que , pour tout idèle $z\in J$, il existe $x\in K^*$ tel que , pour toute place $P\neq P_0$ , on ait

$$(9) \qquad 1\leq |xz|_P \leq c \ .$$

Supposons en effet la prop.2 démontrée , et soit V l'ensemble des idèles satisfaisant à $1\leq|z|_P\leq c$ pour toutes les places P . Pour tout idèle $z\in J$ , soit $x\in K^*$ satisfaisant à (9) pour $P\neq P_0$ . Si on pose $\lambda=|xz|_{P_0}^{-1}$ , on a $\lambda x\in LK^*$ et $1\leq|\lambda xz|_P\leq c$ pour toute place P . Autrement dit , toute classe mod.$LK^*$ rencontre V , et par suite $J/LK^*$ est l'image canonique de V ; mais V est compact (prop.1), donc aussi $J/LK^*$ .

Cela fait , la fin de la démonstration du th.1 est immédiate . En effet , la

composante connexe de J est isomorphe à $(\mathbf{R}_+^*)^{r_1} \times (\mathbf{C}^*)^{r_2}$ , c'est-à-dire à $\mathbf{R}^{r_1+r_2}\mathbf{T}^{r_2}$ ; elle est donc localement isomorphe à $\mathbf{R}^n$ . Comme $J/K^*$ est localement isomorphe à J , la composante connexe de $J/K^*$ est localement isomorphe à $\mathbf{R}^n$ ; elle est donc isomorphe à un groupe de la forme $\mathbf{R}^p \times \mathbf{T}^{n-p}$ , et comme elle est de la forme $\mathbf{R} \times G_0$ , où $G_0$ est compact , on a nécessairement p=1 , et $G_0$ est donc isomorphe à $\mathbf{T}^{n-1}$ .

Remarque .- On peut en fait montrer que $G_0$ est facteur direct dans G . Par dualité , cela se transforme en la proposition suivante : si , dans un groupe abélien localement compact $\hat{G}$ , un sous-groupe M est tel que $\hat{G}/M$ soit isomorphe à $\mathbf{Z}^m$ , M est facteur direct . Il suffit de récurer sur m , et d'appliquer l'exerc.9 d'Alg., chap.I, § 6 . Le rédacteur a la flemme de chercher une démonstration directe ; la proposition mérite-t-elle d'ailleurs plus qu'un exercice ?

4 . Le théorème de Minkowski .

La prop.2 est à son tour conséquence du théorème suivant :

THÉORÈME 3 (Minkowski) .- Soit d le discriminant du corps K . Pour tout idèle z tel que $\prod_{P \in \Phi} |z|_P^{n(P)} \geqslant \sqrt{|d|}$ , il existe au moins un élément $x \in K^*$ tel que l'on ait

(10) $$|x|_P \leqslant |z|_P$$

pour toute place P .

Montrons alors qu'on peut réaliser les inégalités (9) pour $P \neq P_0$ , avec le nombre $x = \sqrt{|d|}$ . En effet , pour tout idèle $z \in J$ , on peut multiplier z par un idèle $\lambda \in L$ sans changer les valeurs de $|z|_P$ pour $P \neq P_0$ , et de façon que $\prod_{P \in \Phi} |z|_P^{n(P)} = c$ . D'après (10) , il existe alors $y \in K^*$ tel que $|y|_P \leqslant |z|_P$ pour toute place P . Si on pose $x = y^{-1}$ , on en déduit d'abord $|xz|_P \geqslant 1$ pour toute place P . D'autre part , on a $\prod_P |xz|_P^{n(P)} = \prod_P |z|_P^{n(P)} = c$ , donc $|xz|_P^{n(P)} = c\left(\prod_{P' \neq P} |xz|_{P'}^{n(P')}\right)^{-1} \leqslant c$ pour tout $P \neq P_0$ , ce qui prouve (9) , puisque $n(P) \geqslant 1$ .

Pour démontrer le th.3 , remarquons que les inégalités (9) relatives aux places finies signifient que $x \in a_z$ . D'autre part , on a , d'après (5) , $\prod_{P \in \Phi_{fin}} |z|_P^{n(P)} = (N(a_z))^{-1}$ . Le th.3 signifie donc qu'étant donné un idéal $a \in I$ , et $r_1+r_2$ nombres $\rho_P > 0$ ($P \in \Phi_\infty$) , il existe $x \neq 0$ dans K tel que $x \in a$ et que l'on ait les inégalités $|x|_P \leq \rho_P$ pour $P \in \Phi_\infty$ , pourvu que $\prod_{P \in \Phi_\infty} \rho_P^{n(P)} \geq \sqrt{|d|} . N(a)$ . Soit $(u_i)_{1 \leq i \leq n}$ une base de l'idéal a , considéré comme Z-module . Si on considère K comme plongé canoniquement dans le produit $\prod_{P \in \Phi_\infty} K_P$ , identifié à $R^n$ , le déterminant d'une base de A (comme Z-module) par rapport à la base canonique de $R^n$ est $2^{-r_2}\sqrt{|d|}$ , comme on le vérifie aisément , donc le déterminant des n vecteurs $u_i$ par rapport à la base canonique de $R^n$ est $2^{-r_2}\sqrt{|d|} . N(a)$ . L'ensemble des vecteurs $v=(v_P)$ de $\prod_{P \in \Phi_\infty} K_P$ tels que $|v_P| \leq \rho_P$ pour toute place $P \in \Phi_\infty$ est évidemment un corps convexe symétrique , dont la mesure de Lebesgue dans $R^n$ est $2^{r_1} \pi^{r_2} \prod_{P \in \Phi_\infty} \rho_P^{n(P)}$ , comme on le voit aussitôt . On applique alors le Lemme de Minkowski .- Soient $(a_k)_{1 \leq k \leq n}$ n vecteurs de $R^n$ , et soit $\Delta$ le déterminant de ces vecteurs par rapport à la base canonique . Si W est un corps convexe symétrique de mesure $\mu(W) \geq 2^n |\Delta|$ , il existe dans W un point $\neq 0$ du Z-module M engendré par les $a_k$ .

(Démonstration standard : on remarque que si $\overset{\circ}{W}$ ne contient aucun point $\neq 0$ de M , $\frac{1}{2}W$ ne contient aucun couple de points congrus mod.M ; autrement dit , l'image de $\frac{1}{2}W$ par l'homomorphisme canonique $\varphi$ de $R^n$ sur $R^n/M$ est biunivoque , et on écrit que la mesure de $\varphi(\frac{1}{2}W)$ est au plus égale à celle de $R^n/M$).

La fin de la démonstration du th. de Minkowski résulte alors de ce que $\pi > 2$ . Le th.1 est ainsi complètement démontré .

5 . Classes d'idéaux et unités d'un corps de nombres algébriques .

Le th.1 entraîne immédiatement le

THÉORÈME 4 .- Le groupe quotient D/P du groupe des diviseurs par le sous-groupe P des diviseurs principaux est fini .

En effet , comme D est isomorphe à $J/J_\infty$ et P à $K^*J_\infty/J_\infty$ , D/P est isomorphe à $J/K^*J_\infty$ ; c'est donc le groupe quotient de $J/K^*$ par le sous-groupe $K^*J_\infty/K^*$ , qui est ouvert , comme image du sous-groupe ouvert $J_\infty$ de J . Comme par ailleur $L \subset J_\infty$ , $J/K^*J_\infty$ est isomorphe au quotient du groupe compact G par un sous-groupe ouvert de G , donc il est compact et discret , et par suite fini .

Les éléments de D/P sont appelées les classes de diviseurs (ou classes d'idéaux) absolues . Le th.4 prouve que , si h est le nombre d'éléments de D/P , la puissance h-ème de tout diviseur est un diviseur principal .

Soit S un ensemble fini de places contenant $\Phi_\infty$ . On appelle S-unités de K les $x \in K^*$ tels que $|x|_P = 1$ pour $P \notin S$ ; ces éléments forment un groupe qui n'est autre que $K^* \cap J_S$ , et qui contient évidemment le groupe U des unités de K .

THÉORÈME 5 (Dirichlet-Chevallev) .- Si S est un ensemble de s places (contenant $\Phi_\infty$ ) le groupe $U_S = K^* \cap J_S$ des S-unités est isomorphe à $U_0 \times Z^{s-1}$ .

En effet , comme $L \subset J_S$ , le groupe $K^*J_S/K^*$ , isomorphe à l'image canonique de $J_S$ dans $J/K^*$ , est isomorphe au produit de R par un sous-groupe ouvert $G_1$ de G, qui est compact . D'autre part , comma $J_S$ est ouvert dans J , $K^*J_S/K^*$ est isomorphe au groupe topologique $J_S/(K^* \cap J_S) = J_S/U_S$ (Top.Gén., chap.I, 2e éd?§ 9, prop.6) . Or , il est clair que $J_S$ est isomorphe à $R^r \times Z^{s-r} \times V$ , où r=r1+r2 et où V est le groupe compact des idèles z tels que $|z|_P = 1$ pour toute place P . Soit $\varphi$ la projection de $J_S$ sur $R^r \times Z^{s-r}$ , et soit $W = \varphi(U_S)$ ; en vertu du th. X

d'isomorphie , $(R^r \times Z^{s-r})/W$ est isomorphe à $J_S/VU_S$ , puisque $VU_S=\varphi^{-1}(W)$ . Or , $J_S/VU_S$ est isomorphe au quotient de $J_S/U_S=R\times G_1$ par $H=VU_S/U_S$ ; H , image canonique du groupe compact V , est compact dans $J_S/U_S$ , donc contenu dans le plus grand groupe compact $G_1$ de $J_S/U_S$ ; on en conclut que $J_S/VU_S$ est isomorphe au produit $R\times(G_1/H)$ , et il en est donc de même de $(R^r\times Z^{s-r})/W$ . Mais $W=\varphi(U_S)$ est isomorphe à $VU_S/V$ , donc aussi à $U_S/(U_S\cap V)=U_S/U_o$ , puisque V est compact (cf... La théorie des sous-groupes fermés de $R^s$ (Top.gén.,chap.VII,§ 1) montre que $(R^r\times Z^{s-r})/W$ ne peut être produit de R par un groupe compact que si W est un Z-module de rang s-1 ; d'ailleurs $U_S$ étant discret , il en est de même de $U_S/U_o$, donc de W , et par suite W est isomorphe à $Z^{s-1}$ . Comme $U_o$ est fini , $U_S$ est un groupe abélien de type fini , donc isomorphe au produit de son groupe de torsion $U_o$ par $Z^{s-1}$ (Alg.,chap.VII).

En particulier , le groupe U des unités de K est isomorphe au produit $U_o\times Z^{r-1}$; il existe donc dans U des supplémentaires de $U_o$ qui sont des groupes libres (multiplicatifs) ; si $(\varepsilon_j)_{1\leqslant j\leqslant r-1}$ est une base d'un tel supplémentaire , toute unité $\eta\in U$ peut se mettre d'une manière et d'une seule sous la forme

$$\eta=\rho\,\varepsilon_1^{\nu_1}\varepsilon_2^{\nu_2}\cdots\varepsilon_{r-1}^{\nu_{r-1}} \tag{11}$$

où $\rho$ est une racine de l'unité dans K , les $\nu_k$ des entiers rationnels quelconques; on dit que $(\varepsilon_k)$ est un système fondamental d'unités de K . A une telle base , on associe dans $R^r$ les r-1 vecteurs $\ell(\varepsilon_j)=(\log|\varepsilon_j|_P^{n(P)})_{P|\infty}$ . En vertu de la formule du produit et du fait que $|\varepsilon|_P=1$ pour toute unité $\varepsilon$ et toute place finie P , les r-1 vecteurs $\ell(\varepsilon_j)$ sont tous dans l'hyperplan N d'équation $\sum_{P|\infty} u_P=0$ dans $R^r$, et forment une base de cet hyperplan . Lorsqu'on passe de la base $(\varepsilon_j)$ à une autre $(\varepsilon'_j)$ , il est clair que ce passage définit une transformation linéaire inversible dans N , dont la matrice , rapportée à la base des $\ell(\varepsilon_j)$ est à coefficients

entiers ainsi que son inverse , ce qui entraîne que son déterminant est $\pm 1$ . On peut prolonger cette transformation à tout l'espace $R^r$ en lui imposant par exemple de laisser invariant le vecteur dont toutes les composantes sont 1 , qui n'appartient pas à N ; la transformation ainsi définie a encore son déterminant égal à $\pm 1$ . De ces remarques , il suit que le nombre

$$(12) \qquad R = \begin{vmatrix} \log|\varepsilon_1|_{P_1}^{n(P_1)} & \cdots & \log|\varepsilon_{r-1}|_{P_1}^{n(P_1)} & \frac{1}{n} \\ \log|\varepsilon_1|_{P_2}^{n(P_2)} & \cdots & \log|\varepsilon_{r-1}|_{P_2}^{n(P_2)} & \frac{1}{n} \\ \cdots & \cdots & \cdots & \cdots \\ \log|\varepsilon_1|_{P_r}^{n(P_r)} & \cdots & \log|\varepsilon_{r-1}|_{P_r}^{n(P_r)} & \frac{1}{n} \end{vmatrix} \qquad (P_k \text{ places à l'infini})$$

est tel que $|R|$ ne dépend pas du système fondamental d'unités $(\varepsilon_j)$ considéré ; on dit que $|R|$ est le régulateur du corps K .

6 . Compléments .

La méthode de Minkowski conduit aussi au résultat suivant :

PROPOSITION 3 .- Pour tout idéal a de K , il existe un élément $x \in K^*$ appartenant à a et tel que

$$(13) \qquad N(x) \leqslant \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d|}\, N(a) \quad .$$

On utilise l'inégalité de la moyenne géométrique

$$\Big(\prod_{P|\infty} |x|_P^{n(P)}\Big)^{1/n} \leqslant \sum_{P|\infty} n(P)|x|_P$$

et on raisonne comme dans le th.3 , en appliquant le lemme de Minkowski à l'ensemble convexe défini par $\sum_{P|\infty} n(P)|u_P| \leqslant 1$ .

De la prop.3 , on déduit comme corollaire l'inégalité

$$(14) \qquad |d| \geqslant \left(\frac{\pi}{4}\right)^{2r_2} \left(\frac{n^n}{n!}\right)^2$$

(en l'appliquant à un idéal principal a=(x)). En particulier , on a $|d| > 1$ pour tout entier n , autrement dit , pour tout corps de nombres algébriques , il y a

des places finies ramifiées sur Q . En outre , on déduit facilement de (14) qu'il n'y a qu'un nombre fini de corps dont le discriminant soit tel que d donné .

On pourrait aussi donner les inégalités d'Artin , qui montrent que le nombre m des éléments de K qui satisfont à (10) est tel que

$$C \prod_{P\in\Phi} |z|_P^{n(P)} \leq m \leq \mathrm{Max}(1, C' \prod_{P\in\Phi} |z|_P^{n(P)}) \quad .$$

Ces formules , importantes pour le cas des courbes algébriques , ne semblent pas avoir d'applications pour les nombres algébriques ; les mettre dans le texte ne se justifierait donc que par des raisons esthétiques ; l'avis du rédacteur est qu'elles doivent rester en exercices jusqu'à nouvel ordre .

7 . Exemples : I . Corps quadratiques .

Soit m un entier rationnel sans facteur carré . Dans $K=Q(\sqrt{m})$ , si $x=\alpha+\beta\sqrt{m}$ est entier algébrique , sa trace $2\alpha$ et sa norme $\alpha^2-\beta^2 m$ sont entiers rationnels . Il en est par suite de même de $4\beta^2 m$ , donc aussi de $2\beta$ . Si $\alpha=k+\frac{1}{2}$ , k entier , on a $(2\beta)^2 m \equiv 1 \pmod 4$ , donc $m\equiv 1 \pmod 4$ ; lorsqu'il en est ainsi , on vérifie inversement que $\frac{1}{2}(1+\sqrt{m})$ est entier dans K , et forme donc avec 1 une base de l'anneau A des entiers de K (comme Z-module) . Lorsque $m \not\equiv 1 \pmod 4$ , $\alpha$ doit être entier , et si on avait $\beta=k+\frac{1}{2}$ , on en conclurait $m\equiv 0 \pmod 4$ , ce qui est impossible ; dans ce cas , 1 et $\sqrt{m}$ forment une base de A sur Z . On en déduit que le discriminant $d=m$ si $m\equiv 1 \pmod 4$ , et $d=4m$ dans le cas contraire .

Le nombre de places à l'infini de K est 1 si $d<0$ , 2 si $d>0$ .

Pour un nombre premier rationnel $p>0$ , on a $2=efg$ , g étant le nombre de diviseurs premiers distincts dans K divisant p , f le degré résiduel (degré résiduel d'un tel diviseur) sur p , e l'indice de ramification de chacun d'eux ; deux des trois nombres e,f,g sont donc 1 . le dernier étant 2 . On sait que le cas $e=2$ , $f=g=1$ , donc $p=P^2$ , se

produit si et seulement si $p|d$ . Si p ne divise pas d , on aura $f=1, g=2$ , donc $p=P_1P_2$ si $Q_p(\sqrt{m})=Q_p$ , et $f=2, g=1$, p premier dans K , si $[Q_p(\sqrt{m}):Q_p]=2$ .

Supposons d'abord $p\neq 2$ . Alors p ne divise pas m , et sur le corps fini $F_p$ , le polynôme $X^2-m$ ne peut avoir que des racines simples ; en vertu de Hensel , $X^2-m$ a donc des racines dans $Q_p$ si et seulement si $X^2-m$ a des racines dans $F_p$, c'est-à-dire si m est un carré mod.p .

Si $p=2$ , p est ramifié dans K lorsque $m\not\equiv 1 \pmod 4$ , puisqu'il divise alors $d=4m$ . Supposons donc $m\equiv 1 \pmod 4$ ; alors l'entier $\frac{1}{2}(1+\sqrt{m})$ de K vérifie l'équation $x^2-x-\frac{m-1}{4}=0$ ; sur le corps $F_2$ , le polynôme $X^2-X-\frac{m-1}{4}$ ne peut avoir que des racines simples . Pour que ce polynôme ait des racines dans $Q_2$ , il faut et il suffit , d'après Hensel , qu'il ait des racines dans $F_2$ ; mais cela signifie évidemment que $(m-1)/4\equiv 0 \pmod 2$ , autrement dit que $m\equiv 1 \pmod 8$ . On notera que cette condition équivaut au fait que m est un carré mod.8 .

Pour $p\neq 2$ , le groupe multiplicatif $F_p^*=G(p)$ est un groupe cyclique d'ordre pair $p-1$ ; le sous-groupe $G^2(p)$ des carrés des éléments de G(p) est donc un sous-groupe cyclique d'ordre $(p-1)/2$ et d'indice 2 dans G(p) . Considérons l'homomorphisme $\varphi$ de G(p) sur le groupe multiplicatif $\{+1,-1\}$ , qui a pour noyau $G^2(p)$ ("caractère quadratique" de G(p)) ; pour tout nombre rationnel s non divisible par p , on désigne par $\left(\frac{s}{p}\right)$ (symbole de Legendre) la valeur de $\varphi$ pour la classe de s mod.p . On a évidemment , en raison de cette définition

$$\left(\frac{s}{p}\right)\left(\frac{t}{p}\right)=\left(\frac{st}{p}\right) \tag{15}$$

pour s et t non divisibles par p . En outre , comme $s^{p-1}\equiv 1 \pmod p$ pour tout entier $s\not\equiv 0 \pmod p$ , la relation $\left(\frac{s}{p}\right)\equiv \pm 1 \pmod p$ équivaut à $s^{(p-1)/2}\equiv \pm 1 \pmod p$

Avec la notation précédente , on a donc la

PROPOSITION 4 . - Pour que le nombre premier impair p tel que $m\not\equiv 0 \pmod p$ soit décomposé en deux diviseurs premiers distincts (resp. soit premier) dans $K=Q(\sqrt{m})$

il faut et il suffit que $\left(\frac{m}{p}\right)=1$ (resp. $\left(\frac{m}{p}\right)=-1$). Pour que 2 soit décomposé en deux diviseurs premiers distincts dans K, il faut et il suffit que $m\equiv 1 \pmod 8$.

On pose encore $\left(\frac{m}{2}\right)=1$ si $m\equiv 1 \pmod 8$, $\left(\frac{m}{2}\right)=-1$ si m est impair et $m\not\equiv 1 \pmod 8$; on peut aussi écrire $\left(\frac{m}{2}\right)=(-1)^{(m^2-1)/8}$.

8. Exemples : II. Corps des racines n-ièmes de l'unité.

Soit p un nombre premier, et considérons le corps $K=R_{p^k}(Q)$ des racines $p^k$-èmes de l'unité sur Q. On sait que $K=Q(\zeta)$, où $\zeta$ est une racine primitive $p^k$-ème de l'unité, racine du polynôme cyclotomique

$$\Phi_{p^k}(X)=X^{p^{k-1}(p-1)}+X^{p^{k-1}(p-2)}+\ldots+1 .$$

Le degré de K sur Q est donc $\leq \varphi(p^k)=p^{k-1}(p-1)$. On sait qu'on peut écrire $\Phi_{p^k}(X)=\prod_r (X-\zeta^r)$, où r parcourt l'ensemble des nombres $<p^k$ non divisibles par p. Il est clair que $\zeta$ est entier algébrique ; il en est donc de même de $\varepsilon_r=(1-\zeta^r)/(1-\zeta)=1+\zeta+\ldots+\zeta^{r-1}$. En outre, si r n'est pas divisible par p, il existe s tel que $rs\equiv 1 \pmod{p^k}$, donc $\zeta^{rs}=\zeta$, et par suite $\varepsilon_r^{-1}=(1-\zeta^{rs})/(1-\zeta^r)=1+\zeta^r+\ldots+\zeta^{r(s-1)}$ est aussi entier algébrique, donc $\varepsilon_r$ est une unité de K. Si on pose $\pi=1-\zeta$, on a donc dans K

$$p=\Phi_{p^k}(1)=\pi^{p^{k-1}(p-1)}\varepsilon \tag{16}$$

où $\varepsilon=\prod_r \varepsilon_r$ (r parcourant l'ensemble des nombres $<p^k$ et non divisibles par p); $\varepsilon$ est donc une unité de K. De la formule (16) il suit que tout diviseur premier de p dans K a un indice de ramification $\geq p^{k-1}(p-1)$. Mais comme cet indice est au plus égal à $[K:Q]$, on voit en premier lieu que $[K:Q]=\varphi(p^k)=p^{k-1}(p-1)$; en outre, l'idéal principal $(\pi)$ est premier, de degré résiduel f=1 et d'indice de ramification $e=\varphi(p^k)$.

La différente $\delta$ de $\zeta$ est $\Phi'_{p^k}(\zeta)$. Comme on a $(X^{p^{k-1}}-1)\Phi_{p^k}(X)=X^{p^k}-1$, on voit aussitôt que

$$\Phi'_{p^k}(\zeta)=-p^k/\zeta(1-\zeta^{p^{k-1}}) . \tag{17}$$

On a évidemment $N_{K/Q}(\zeta)=(-1)^{\varphi(p^k)}$ , ce qui donne +1 dans tous les cas ; d'autre part , $1-\zeta^{p^{k-1}}$ est racine de l'équation irréductible $\Phi_p(1-X)=0$ , dont le terme constant est p et le coefficient de $X^{p-1}$ est $(-1)^{p-1}$ ; d'où $N_{K/Q}(1-\zeta^{p^{k-1}})=p^{p^{k-1}}$

Le discriminant $d(\zeta)$ de $\zeta$ étant égal à

$$(-1)^{\frac{1}{2}\varphi(p^k)(\varphi(p^k)-1)}N_{K/Q}(\zeta)$$

est finalement donné par la formule

$$d(\zeta)=\rho p^{p^{k-1}(kp-k-1)} \tag{18}$$

où $\rho=-1$ si $p^k=4$ ou si $p\equiv 3 \pmod 4$ , $\rho=1$ dans les autres cas . Comme le discriminant de K divise $d(\zeta)$ , la formule (18) montre que p est le seul nombre premier ramifié dans K . Pour tout diviseur premier $P\neq(\pi)$ de K , P ne divise pas $d(\zeta)$ donc (chap.I, § 5, prop.4) , les éléments $\zeta^j$ $(0\leq j\leq\varphi(p^k)-1)$ forment une base de l'anneau $A_P$ des entiers P-adiques sur $Z_q$ (q désignant le nombre premier qui divise P) . D'autre part , comme $K_{(\pi)}$ est complètement ramifié sur $Q_p$ et que $\pi$ est une uniformisante de $K_{(\pi)}$ , les $\pi^j$ $(1\leq j\leq\varphi(p^k)-1)$ forment une base de $A_{(\pi)}$ sur $Z_p$ , et comme $d(\pi)=d(-\zeta)$ , il en est de même des $\zeta^j$ ; il résulte aussitôt de la définition des entiers de $\mathbb{Q}$ comme entiers pour toutes les valuations , que les $\zeta^j$ forment une base de A sur Z , d'où en particulier $d=d(\zeta)$.

Ces propriétés permettent de démontrer la proposition suivante :

PROPOSITION 5 .- *Pour tout entier $n>1$ , le corps $R_n(Q)$ des racines n-èmes de l'unité sur Q est une extension abélienne de Q , de degré $\varphi(n)$ , dont le groupe de Galois est isomorphe au groupe G(n) des éléments inversibles de l'anneau Z/(n) . Si $n=\prod_h p_h^{\nu_h}$ est la décomposition de n en facteurs premiers , $R_n(Q)$ est isomorphe au produit tensoriel (sur Q) des corps $R_{p_h^{\nu_h}}(Q)$ ; en outre , si $A_h$ désigne l'anneau des entiers du corps $R_{p_h^{\nu_h}}(Q)$ , l'anneau A des entiers de $R_n(Q)$ est produit tensoriel (sur Z) des anneaux $A_h$ . Enfin , si $\zeta$ est une racine primitive n-ème de l'unité , les entiers $\zeta^j$ $(0\leq j\leq\varphi(n)-1)$ forment une base de A sur*

Z .

En effet , les discriminants des corps $K_h = R_{p_h^{\nu_h}}(Q)$ étant deux à deux étrangers, chacun des sous-corps $K_h$ de $K=R_n(Q)$ est linéairement disjoint du composé $K'_h$ des sous-corps $K_{h'}$ d'indice $h' \neq h$ (chap.I,§ 2,n°5) . Comme K est composé des corps $K_h$ , il est isomorphe à leur produit tensoriel , et son degré sur Q est donc égal à $\prod_h \varphi(p_h^{\nu_h}) = \varphi(n)$ (en d'autres termes , le polynôme cyclotomique $\Phi_n$ est irréductible sur Q) . Le fait que les discriminants des $K_h$ soient deux à deux étrangers entraîne que A soit isomorphe au produit tensoriel des $A_h$ sur Z (chap.I,§ 4,prop.5) . Enfin , comme $\zeta = \prod_h \zeta_h$ , où $\zeta_h$ est une racine primitive $p_h^{\nu_h}$-ème de l'unité , la formule de transitivité des discriminants (chap.I,§ 4, n°5) montre que $d(\zeta)$ est égal au discriminant de K sur Q , ce qui achève la démonstration .

PROPOSITION 6 .- Soit p un nombre premier ne divisant pas n . Si f est le plus petit entier $>0$ tel que $p^f \equiv 1 \pmod{n}$ , et $g=\varphi(n)/f$ , p n'est pas ramifié dans $R_n(Q)$ et se décompose en g diviseurs premiers de degré résiduel f . Si $m=p^k n$ , p se décompose dans $R_m(Q)$ en g diviseurs premiers , dont chacun est de degré résiduel f et a un indice de ramification $e=p^{k-1}(p-1)$ .

Nous savons déjà que p n'est pas ramifié dans $K=R_n(Q)$ , puisqu'il ne divise pas le discriminant de K . Le degré résiduel f est le degré de $R_n(F_p)$ sur $F_p$ ; or , si $\xi$ est une racine primitive n-ème de l'unité sur $F_p$ , elle appartient au corps $F_{p^f}$ , donc $\xi^{p^f-1}=1$ , ce qui entraîne $p^f \equiv 1 \pmod{n}$ ; si on avait $p^{f'} \equiv 1 \pmod{n}$ pour $f' < f$ , on aurait inversement $\xi^{p^{f'}-1}=1$ , donc $\xi$ appartiendrait au corps $F_{p^{f'}}$ , et $R_n(F_p)=F_p(\xi)$ aurait un degré $<f$ sur $F_p$ . D'autre part , on a $R_m(Q_p)=R_{p^k}(R_n(Q_p))$ , et le degré de $R_m(Q_p)$ sur $R_n(Q_p)$ est donc au plus $\varphi(p^k)$ . Mais l'extension $R_n(Q_p)$ de $Q_p$ n'est pas ramifiée , et d'après (16) l'indice de ramification de $R_{p^k}(Q_p)$ sur $Q_p$ est $\varphi(p^k)$ ; par suite $R_m(Q_p)$ est complètement ramifiée sur $R_n(Q_p)$ et est de degré (égal à son indice de ramification) $\varphi(p^k)$

sur $R_n(Q_p)$ , ce qui achève de démontrer la prop.6 .

9 . Applications : I . Nombre de racines de l'unité d'un corps .

PROPOSITION 7 .- Dans un corps de nombres algébriques K , de discriminant d , le nombre w des racines de l'unité divise 2d .

En effet , pour tout nombre premier p , soit $p^k$ la plus haute puissance de p divisant w ; le corps K contient donc le corps $R_{p^k}(Q)$, et par suite d est divisible par le discriminant de $R_{p^k}(Q)$ (transitivité des discriminants) . Ce dernier étant donné par la formule (18) , on voit que d est divisible par $p^{p^{k-1}(kp-k-1)}$ Or , si $p\neq 2$ , on a $p^{k-1}(k(p-1)-1) \geqslant k(p-1)-1 \geqslant k$ , et par suite d est divisible par $p^k$ ; il en est de même si p=2 et $k \geqslant 2$ ; d'où la proposition .

10 . Applications : II . Loi de réciprocité des restes quadratiques .

Soit p un nombre premier impair . Le groupe de Galois G(p) de $L=R_p(Q)$ est cyclique d'ordre p-1 , donc L contient un seul corps quadratique K sur Q , correspondant au sous-groupe d'ordre $\frac{1}{2}(p-1)$ de G(p) . Le discriminant d de K divise celui de L , donc il ne peut contenir que le facteur premier p d'après la formule (18) ; des résultats du n°7 , on déduit aussitôt que $K=Q(\sqrt{p})$ si $p \equiv 1 \pmod 4$ , et $K=Q(\sqrt{-p})$ si $p \equiv -1 \pmod 4$ ; on a donc dans tous les cas $K=Q(\sqrt{(-1)^{(p-1)/2}p})$ .

Soit maintenant q un nombre premier quelconque $\neq p$ . En vertu de la prop.6 , q n'est pas ramifié dans L , et si f est le plus petit entier tel que $q^f-1 \equiv 0 \pmod p$ , q se décompose en $g=(p-1)/f$ diviseurs premiers distincts dans L . Le groupe de décomposition de q dans L est d'ordre f , le corps de décomposition $M=L\cap Q_q$ de q est de degré g sur Q . Pour tout corps E intermédiaire entre Q et L , on a $E\cap Q_q=E\cap M$ , et pour que q ne soit pas premier dans E , il faut et il suffit que $M\cap E\neq Q$ . Pour E=K , on en conclut (puisque M est un corps cyclique de degré g sur Q) que la relation $M\cap K=Q$ équivaut à dire que g est impair . On voit donc que , pour que q soit décomposé (resp. premier) dans K , il faut et

il suffit que $g$ soit pair (resp. impair) .

Ce résultat peut s'exprimer d'une autre manière en considérant le symbole de Legendre $\left(\frac{q}{p}\right)$. En effet , si $g$ est pair , la relation $p-1=fg$ s'écrit aussi $\frac{1}{2}(p-1)=f.(\frac{1}{2}g)$ , donc $q^{(p-1)/2}=(q^f)^{g/2}\equiv 1 \pmod{p}$ , et par suite $\left(\frac{q}{p}\right)=+1$ . Si au contraire $g$ est impair , $f$ est pair , donc $\frac{1}{2}(p-1)=(\frac{1}{2}f)g$ , et par suite $q^{(p-1)/2}=(q^{f/2})^g$ ; mais $(q^{f/2})^2\equiv 1 \pmod{p}$ , et on ne peut avoir $q^{f/2}\equiv 1 \pmod{p}$ par définition de $f$ , donc $q^{f/2}\equiv -1 \pmod{p}$ , c'est-à-dire $\left(\frac{q}{p}\right)=-1$ . Si maintenant on compare ces résultats à ceux de la prop.4 , on voit qu'on a la proposition suivante :

PROPOSITION 8 .- Si $p$ est un nombre premier impair , on a , pour tout nombre premier $q\neq p$

$$\left(\frac{q}{p}\right)=\left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) \tag{19}$$

(loi de réciprocité des réstes quadratiques) .

On peut expliciter la formule (19) . Tout d'abord , si $q$ est impair , on déduit de (19) , en permutant les rôles de $p$ et $q$ , que l'on a $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)=\left(\frac{(-1)^{\frac{q-1}{2}}}{p}\right)$ ; prenant $p=3$ , il vient $\left(\frac{-1}{q}\right)=\left(\frac{(-1)^{\frac{q-1}{2}}}{3}\right)=(-1)^{(q-1)/2}$ . Donc , si $p$ et $q$ sont premiers impairs , on a

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \tag{20}$$

Si au contraire $q=2$ , comme $(-1)^{(p-1)/2}p\equiv 1 \pmod{4}$ , on a , pour tout nombre premier impair $p$

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}} \tag{21}$$

## § 2 . La théorie du corps de classes global :

### I . La loi de réciprocité .

#### 1 . Position du problème .

Soit $K$ un corps de nombres algébriques de degré $n$ , $J\supset K^*$ le groupe localement compact des idèles de $K$ : on a vu (§ 1, th.1) que $J/K^*$ est isomorphe à un groupe de la forme $R\times G$ , où $G$ est compact et a une composante connexe $G_0$ de

isomorphe à $T^{m-1}$ . Le but de ce § et du suivant est de démontrer le th.2 du § 1 établissant l'isomorphie du groupe compcat $G/G_0$ et du groupe de Galois topologique $\mathcal{A}$ d'une clôture abélienne $\Omega$ de K . Nous démontrerons en fait davantage en définissant un <u>isomorphisme canonique</u> de $G/G_0$ sur $\mathcal{A}$. Il nous suffira pour cela de définir un homomorphisme canonique de $J/K^*$ sur $\mathcal{A}$ , dont le noyau soit la composante connexe de 1 dans $J/K^*$ ; il revient au même de définir un homomorphisme canonique $\psi$ de J sur $\mathcal{A}$ , dont le noyau soit le produit de $K^*$ et de la composante connexe de 1 dans J . Or, on sait (chap. ,§ ) que ce produit est l'intersection des sous-groupes ouverts $H_\alpha$ de J contenant $K^*$ ; en outre, $J/H_\alpha$ est un groupe abélien compact et discret , donc fini ; l'image $\mathcal{H}_\alpha$ de $H_\alpha$ par $\psi$ doit donc être un sous-groupe ouvert de $\mathcal{A}$, donc le groupe de Galois de $\Omega$ par rapport à une extension abélienne de degré fini $L_\alpha$ de K ; par passage aux quotients , $\psi$ donnera un homomorphisme $\psi_\alpha$ de J sur le groupe de Galois $\mathcal{L}_\alpha = \mathcal{A}/\mathcal{H}_\alpha$ de $L_\alpha$ sur K . En outre , si $H_\beta$ est un second sous-groupe ouvert de J contenant $K^*$ et tel que $H_\beta \subset H_\alpha$ , on a $L_\alpha \subset L_\beta$ , et $\mathcal{L}_\alpha$ peut être canoniquement considéré comme groupe quotient de $\mathcal{L}_\beta$ ; si $\theta_{\alpha\beta}$ est l'homomorphisme canonique de $\mathcal{L}_\beta$ sur $\mathcal{L}_\alpha$ , on doit avoir

(1) $$\theta_{\alpha\beta} \circ \psi_\beta = \psi_\alpha \ .$$

Inversement , supposons donné , pour chaque extension abélienne $L_\alpha \subset \Omega$ de degré fini de K , un homomorphisme $\psi_\alpha$ de J sur le groupe discret $\mathcal{L}_\alpha$ , dont le noyau (ouvert) $H_\alpha$ contienne $K^*$ , et tel que la relation (1) soit satisfaite lorsque $L_\alpha \subset L_\beta$ . Soit $H_0$ l'intersection des sous-groupes $H_\alpha$ ; remarquons d'autre part que le groupe compact $\mathcal{A}$ peut être identifié au sous-groupe du produit $\prod_\alpha \mathcal{L}_\alpha$ , formé des $s=(s_\alpha)$ tels que $s_\alpha = \theta_{\alpha\beta} \circ s_\beta$ pour $L_\alpha \subset L_\beta$ . On définit alors une représentation $\psi$ de J sur $\mathcal{A}$ , de noyau $H_0$ , en faisant correspondre à tout idèle $z \in J$ l'élément $(\psi_\alpha(z))$ de $\prod_\alpha \mathcal{L}_\alpha$ , qui appartient bien à $\mathcal{A}$

d'après (1) . Chacune des représentations $\psi_\alpha$ étant continue , il en est de même de $\psi$, qui est par suite un homomorphisme de J sur $\mathcal{G}$ . Reste à prouver que $H_0$ est identique au produit de $K^*$ par la composante connexe de 1 dans J ; cela revient à établir que tout sous-groupe ouvert H de J contenant $K^*$ est identique à un des sous-groupes $H_\alpha$ .

En résumé , nous sommes ramenés à résoudre les deux problèmes suivants :

1° Etant donnée une extension abélienne L de K , de degré fini , définir un homomorphisme $\psi_{L/K}$ de J sur le groupe de Galois $\mathcal{G}$ de L (par rapport à K) , dont le noyau $\psi^{-1}_{L/K}(1)$ contienne $K^*$ , les homomorphismes ainsi définis vérifiant la propriété de compatibilité (1) . Ce problème est résolu par la loi de réciprocité d'Artin (n$^{os}$ 2 et 9) .

2° Etant donné un sous-groupe ouvert H de J , contenant $K^*$ , montrer qu'il existe une extension abélienne L de K telle que $\psi^{-1}_{L/K}(1)=H$ . Ce problème est résolu par le théorème d'existence (§ 3,n°1) .

2 . Enoncé de la loi de réciprocité .

Soit L une extension abélienne de K , de degré n . Dans tout ce qui suit , nous désignerons par $J_K$ (resp. $J_L$) le groupe des idèles de K (resp. L) . Nous supposerons tous les corps locaux $K_p$, de K plongés dans une même extension algébriquement close $\Omega_0$ de K , dans laquelle nous supposerons aussi plongées toutes les extensions algébriques de K que nous envisagerons . Soit P' une place de K , et soient $P_j$ $(1\leqslant i\leqslant g)$ les places de L prolongeant P' ; comme L est abélien , les corps de décomposition de toutes les $P_j$ sont confondus avec $L\cap K_{p'}$ , et pour chacun des corps locaux $L_{P_j}$ , il existe un $K_{p'}$-isomorphisme de ce corps sur $K_{p'}(L)$ , tous ces $K_{p'}$-isomorphismes s'obtenant en composant avec l'un d'eux les éléments du groupe de décomposition $\mathcal{L}_{p'}$ (groupe de $K_{p'}(L)$ sur $K_{p'}$ , identifié à celui de L sur $L\cap K_{p'}$) . Chacun des groupes de normes

$N_{L_{P_j}/K_{P'}}(L^*_{P_j})$ est donc identique au groupe $N_{K_{P'}(L)/K_{P'}}(K_{P'}(L)^*)$ ; ce dernier n'est autre que l'intersection $K^*_{P'} \cap N_{L/K}(J_L)$ . En effet , par définition ,cette intersection est formée des éléments de $K^*_{P'}$ de la forme $z=z_1z_2..z_g$ , où $z_j$ est norme d'un élément de $L^*_{P_j}$ ; z est donc norme d'un élément de $K_{P'}(L)^*$ , et réciproquement , toute norme y d'un élément de $K_{P'}(L)^*$ peut être mise sous la forme $z_1z_2..z_g$ , en prenant $z_1=y$ et $z_j=1$ pour $j>1$ .

Cela étant , la théorie du corps de classes local (chap.I, § 6) permet , pour chaque place P' de K , de définir un isomorphisme canonique $\psi_{K_{P'}(L)/K_{P'}}$ du groupe $\mathcal{L}_{P'}$ sur le groupe quotient $K^*_{P'}/(K^*_{P'} \cap N_{L/K}(J_L))$ (appelé isomorphisme principal au chap.I, § 6) . En composant l'isomorphisme réciproque avec l'homomorphisme canonique de $K^*_{P'}$ sur $v^*_{P'}/(K^*_{P'} \cap N_{L/K}(J_L))$ , on obtient donc un homomorphisme canonique de $K^*_{P'}$ sur $\mathcal{L}_{P'}$ , que nous noterons $\psi_{L/K,P'}$ ou simplement $\psi_{P'}$ .

Soit alors $z=(z_{P'})$ un idèle quelconque de $J_K$ . On sait que pour toute place finie P' de K non ramifiée dans L , toute unité P'-adique est norme d'un élément de $K_{P'}(L)$ (chap.I, § 6,prop.1) ; d'autre part , presque tous les $z_{P'}$ sont des unités P'-adiques . Donc on a $\psi_{P'}(z_{P'})=1$ pour presque toute place P' , ce qui montre que le produit

$$\psi_{L/K}(z)=\prod_{P' \in \Phi} \psi_{L/K,P'}(z_{P'}) \tag{2}$$

est un élément bien défini du groupe de Galois $\mathcal{L}$ de L sur K (les groupes $\mathcal{L}_{P'}$ étant tous des sous-groupes de $\mathcal{L}$ ) .

Nous pouvons maintenant énoncer la loi de réciprocité :

THÉORÈME 1 (loi de réciprocité d'Artin) .- *L'homomorphisme $\psi_{L/K}$ de $J_K$ dans le groupe de Galois $\mathcal{L}$ de L sur K applique $J_K$ sur $\mathcal{L}$ , et a pour noyau le sous-groupe $K^*N_{L/K}(J_L)$ .*

Remarquons tout de suite que les homomorphismes canoniques $\psi_{L/K}$ ainsi définis pour toute extension abélienne L de K satisfont à la condition de compatibilité

(1) ; en effet , cela résulte de la définition (2) et de la prop.8 du chap.I, § 6 , appliquée , pour chaque place P' de K , aux extensions $K_{P'}(L_\alpha)$ et $K_{P'}(L_\beta)$ de $K_{P'}$ .

La démonstration du th.1 peut se diviser en 3 étapes . Dans les deux premières, on prouve que pour une extension cyclique L de K , l'ordre $n=[L:K]$ du groupe de Galois $\mathcal{L}$ est égal à l'ordre de $J_K/(K^*N_{L/K}(J_L))$ , en montrant successivement que :

1° $[L:K]$ divise $(J_K:(K^*N_{L/K}(J_L)))$ (première inégalité fondamentale) ;

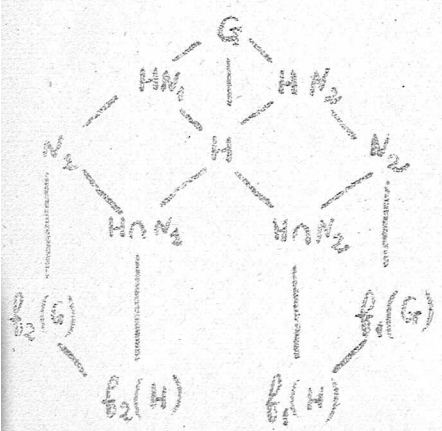
2° $(J_K:(K^*N_{L/K}(J_L)))$ divise $[L:K]$ (seconde inégalité fondamentale) .

Les résultats obtenus dans la démonstration de ces deux inégalités permettent enfin de démontrer le th.1 , en passant au préalable par le cas particulier où L est une extension cyclique de K contenue dans un corps de racines de l'unité sur K .

3 . Deux lemmes préliminaires à la première inégalité fondamentale .

Lemme 1 (lemme de Herbrand) .- Soient G un groupe abélien multiplicatif , H un sous-groupe d'indice fini de G , $f_1$ et $f_2$ deux endomorphismes de G tels que $f_1(G)\subset f_2^{-1}(1)=N_2$ , $f_2(G)\subset f_1^{-1}(1)=N_1$ , et que $f_1(H)\subset H$ , $f_2(H)\subset H$ . Alors , si les indices $((H\cap N_1):f_2(H))$ et $((H\cap N_2):f_1(H))$ sont finis , il en est de même de $(N_1:f_2(G))$ et $(N_2:f_1(G))$ , et l'on a

(3) $$\frac{(N_1:f_2(G))}{(N_2:f_1(G))}=\frac{((H\cap N_1):f_2(H))}{((H\cap N_2):f_1(H))}$$




En effet , on peut écrire $(G:H)=(G:HN_1)(HN_1:H)$ . Le groupe $G/HN_1$ est isomorphe à $f_1(G)/f_1(H)$ , et le groupe $HN_1/H$ est isomorphe à $N_1/(H\cap N_1)$ ; on a donc

$$(G:H)=(f_1(G):f_1(H))(N_1:(H\cap N_1)) .$$

De même , en vertu de l'hypothèse , $(N_1:f_2(H))$ est fini et donné par

$$(N_1:f_2(H))=(N_1:(H\cap N_1))((H\cap N_1):f_2(H)) .$$

Il en résulte que $(N_1:f_2(G))$ est fini et qu'on a

$$(N_1:f_2(H))=(N_1:f_2(G))(f_2(G):f_2(H))$$

d'où on déduit que

$$(G:H)=(f_1(G):f_1(H))(f_2(G):f_2(H)).(N_1:f_2(G))/((H\ N_1):f_2(H)) .$$

En permutant les indices 1 et 2 dans cette formule , il vient la relation (3)

Lemme 2 .- Dans l'espace $R^m$ , soit H un hyperplan d'équation $\sum_{i=1}^{m}\lambda_i x_i=0$ , où $\lambda_i>0$ pour $1\leqslant i\leqslant m$ . Si G est un sous-groupe fermé de rang m-1 contenu dans H, il existe dans G m vecteurs $a_i=(a_{ij})_{1\leqslant j\leqslant m}$ $(1\leqslant i\leqslant m)$ tels que $a_{ii}>0$ et $a_{ij}<0$ pour $j\neq i$ . Inversement , m vecteurs de H ayant ces propriétés sont tels que m-1 quelconques d'entre eux sont linéairement indépendants .

On peut se limiter au cas où G=H : en effet , G contient un sous-groupe discret de rang m-1 , engendré par m-1 vecteurs $b_k$ linéairement indépendants $(1\leqslant k\leqslant m-1)$ ; tout point de H est donc à une distance euclidienne $<\sum_{k=1}^{m-1}\|b_k\|=r$ d'un point de G . Si $c=(c_j)$ est un point de H dont toutes les coordonnées sont $\neq 0$ , en prenant $\mu>0$ assez grand , les valeurs absolues des coordonnées de $\mu c$ sont toutes $>r$ , donc il existe dans G un point dont les coordonnées ont mêmes signes que les coordonnées de même indice de c . Or , pour G=H , la première partie du lemme est évidente , car si on prend arbitrairement les m-1 nombre $a_{ij}<0$ $(j\neq i)$ , la relation $\lambda_i a_{ii}=-\sum_{j\neq i}\lambda_j a_{ij}$ montre que $a_{ii}>0$ .

Montrons inversement , par exemple , que les m-1 vecteurs $a_i$ $(1\leqslant i\leqslant m-1)$ sont linéairement indépendants . Il suffit de prouver que la matrice $(a_{ij})$ $(1\leqslant i\leqslant m-1,\ 1\leqslant i\leqslant m-1)$ est inversible . Dans le cas contraire , il existerait m-1 nombres $t_i$ non tous nuls $(1\leqslant i\leqslant m-1)$ tels que $\sum_{j=1}^{m-1}\lambda_j t_j a_{ij}=0$ pour $1\leqslant i\leqslant m-1$ ; soit $t_k$ un des $t_j$ dont la valeur absolue est la plus grande ; on peut évidemment supposer $t_k>0$. On a alors $\lambda_j t_j a_{kj}\geqslant\lambda_j t_k a_{kj}$ pour $1\leqslant j\leqslant m-1$ , d'où

$$0=\sum_{j=1}^{m-1}\lambda_j t_j a_{kj}\geqslant t_k\sum_{j=1}^{m-1}\lambda_j a_{kj}=-\lambda_m t_k a_{km}>0 \text{ (puisque } k\neq m)$$

ce qui est absurde .

## 4 . La première inégalité fondamentale .

Soit L une extension cyclique de K , de degré n . Il existe un ensemble fini S' de places de K telles que :

1° S'contient les places à l'infini et les places de K qui se ramifient dans L.

2° Si $S$ est l'ensemble des places de L prolongeant les places $P' \in S'$; et si $J_K^{S'}$ (resp. $J_L^S$) désigne le groupe des S'-idèles de K (resp. des S-idèles de L) , on a $J_K = K^* J_K^{S'}$ et $J_L = L^* J_L^S$ (cf.§ 1, th.4) . De cette dernière relation , on déduit que $K^* N_{L/K}(J_L) = K^* N_{L/K}(J_L^S)$ . Par suite (puisque $N_{L/K}(J_L^S) \subset J_K^{S'}$)

$$(4)\quad (J_K : K^* N_{L/K}(J_L)) = (K^* J_K^{S'} : K^* N_{L/K}(J_L^S)) = (J_K^{S'} : (J_K^{S'} \cap K^* N_{L/K}(J_L^S))) =$$
$$= (J_K^{S'} : N_{L/K}(J_L^S)) / ((J_K^{S'} \cap K^* N_{L/K}(J_L^S)) : N_{L/K}(J_L^S)) .$$

Calculons le numérateur $(J_K^{S'} : N_{L/K}(J_L^S))$ de cette dernière expression . Le groupe $N_{L/K}(J_L^S)$ est le produit des groupes $K_{P'}^* \cap N_{L/K}(J_L) = N_{K_{P'}(L)/K_{P'}}(K_{P'}(L)^*)$ pour $P' \in S'$ et des groupes $U_{P'} \cap N_{L/K}(J_L)$ pour $P' \notin S'$ . Mais toute place $P' \notin S'$ est non ramifiée dans L , donc tout élément de $U_{P'}$ est norme d'un élément de $K_{P'}(L)^*$ (chap.I, § 6, prop.1) , et par suite $U_{P'} \cap N_{L/K}(J_L) = U_{P'}$ pour $P' \notin S'$ . Le th. d'isomorphie du corps de classes local (chap.I, § 6, th.3) montre d'autre part que $N_{K_{P'}(L)/K_{P'}}(K_{P'}(L)^*)$ est d'indice $n(P')$ dans $K_{P'}^*$ , $n(P')$ désignant le degré local de L sur K pour la place P' . On a donc

$$(5)\quad (J_K^{S'} : N_{L/K}(J_L^S)) = \prod_{P' \in S'} n(P') .$$

D'autre part , comme $N_{L/K}(J_L^S) \subset J_K^{S'}$ , on a $J_K^{S'} \cap K^* N_{L/K}(J_L^S) = K(K^* \cap J_K^{S'}) N_{L/K}(J_L^S) = U_K^{S'} N_{L/K}(J_L^S)$ , où $U_K^{S'}$ désigne le groupe des S'-unités de K . On peut donc écrire

$$(6)\quad ((J_K^{S'} \cap K^* N_{L/K}(J_L^S)) : N_{L/K}(J_L^S)) = (U_K^{S'} N_{L/K}(J_L^S) : N_{L/K}(J_L^S)) = (U_K^{S'} : (U_K^{S'} \cap N_{L/K}(J_L^S))) =$$
$$= (U_K^{S'} : N_{L/K}(U_L^S)) / ((U_K^{S'} \cap N_{L/K}(J_L^S)) : N_{L/K}(U_L^S))$$

en désignant par $U_L^S$ le groupe des S-unités de L .

Nous calculerons seulement le numérateur $(U_K^{S'} : N_{L/K}(U_L^S))$ de cette dernière expression . Soit $\sigma$ un générateur du groupe de Galois de L sur K , et considérons

dans le groupe $U_L^S$ les endomorphismes $f_1$ et $f_2$ définis par $f_1(y)=N_{L/K}(y)$ , $f_2(y)=y^{1-\sigma}$ . Par définition de S , on a $U_L^S \cap K^* = U_K^{S'}$ , donc $U_K^{S'} = \bar{f}_2^1(1)$ ; l'indice $(U_K^{S'} : N_{L/K}(U_L^S))$ s'écrit donc $(\bar{f}_2^1(1) : f_1(U_L^S))$ . Comme on a $f_1(U_L^S) \subset \bar{f}_2^1(1)$ , et $f_2(U_L^S) \subset \bar{f}_1^1(1)$ , nous allons appliquer le lemme de Herbrand pour évaluer l'indice cherché .

Il nous faut pour cela définir un sous-groupe H d'indice fini du groupe $U_L^S$ , tel que les indices du second membre de la formule (3) se calculent commodément Soient $P_i'$ $(0 \leqslant i \leqslant s')$ les places de S' . Pour chaque indice i , soit $P_i$ l'une des places de S qui prolongent $P_i'$ . En vertu du th. de Dirichlet-Chevalley (§ 1, th.5) appliqué aux S-unités de L , de la formule du produit (§ 1, formule (2)) et du lemme 2 , il existe pour chaque indice i $(0 \leqslant i \leqslant s')$ un élément $a_i \in U_L^S$ tel que $\log |a_i|_{P_i} < 0$ , et $\log |a_i|_P > 0$ pour toute autre place $P \in S$ . Soit $M_i$ le corps de décomposition de $P_i'$ dans L , et posons $b_i = N_{L/M_i}(a_i)$ ; les conjugués de $a_i$ (par rapport à K) étant des S-unités , il en est de même de $b_i$ ; en outre tout élément $\rho$ du groupe de décomposition de $P_i'$ transforme $P_i$ en elle-même , et transforme toute place $P \in S$ ne prolongeant pas $P_i'$ en une place $\neq P_i$ . On a donc $|\rho(a_i)|_{P_i} < 1$ et $|\rho(a_i)|_P > 1$ pour toute autre place $P \in S$ ; d'où $|b_i|_{P_i} < 1$ et $|b_i|_P > 1$ pour toute autre place de S . Pour tout élément $\tau$ du groupe de Galois de L sur K , on a donc $|\tau(b_i)|_{\tau(P_i)} < 1$ et $|\tau(b_i)|_{\tau(P)} > 1$ pour toute place $P \neq P_i$ . Mais toute place de S peut se mettre sous la forme $\tau(P_i)$ pour un $\tau$ et un i convenables ; lorsque i parcourt les s'+1 indices de $[0, s']$ , et $\tau$ le groupe de Galois de L sur K , on obtient donc s+1 éléments $\tau(b_i)$ distincts en nombre égal au nombre d'éléments de S . En outre , la formule du produit et le lemme 2 ci-dessus prouvent que s quelconques des éléments $\tau(b_i)$ sont logarithmiquement indépendants , et engendrent donc un sous-groupe de rang s de $U_L^S$ ; en vertu du th. de Dirichlet-Chevalley , le sous-groupe $H_1$ de $U_L^S$ engendré par les s+1 éléments $\tau(b_i)$ distincts est donc d'indice fini . Posons

$m_i=[M_i:K]=n/n(P_i')$ , $e_i=N_{M_i/K}(b_i)$ , et $c_i=b_i^{m_i}/e_i$ $(0\leqslant i\leqslant s')$ , et considérons le sous-groupe $H_2$ de $H_1$ engendré par les $e_i$ , les $c_i$ et les conjugués $\tau(c_i)$ des $c_i$ ; $H_2$ contient les éléments $b_i^n=(b_i^{m_i})^{n(P_i')}$ et les éléments $(\tau(b_i))^n$ pour $0\leqslant i\leqslant s'$ , donc est d'indice fini dans $H_1$ , et par suite dans $U_L^S$ . D'autre part on a par définition $N_{M_i/K}(c_i)=1$ ; comme L est cyclique , le groupe de $M_i$ sur K est formé des $m_i$ éléments $\sigma^k$ $(0\leqslant k\leqslant m_i-1)$ ; on voit donc que le groupe $H_2$ est engendré par les $e_i$ $(0\leqslant i\leqslant s')$ et les $c_i^{\sigma^k}$ $(0\leqslant i\leqslant s', 0\leqslant k\leqslant m_i-2)$ . Par définition, les $s'+1$ éléments $e_i$ sont des S'-unités de K ; en vertu du th. de Dirichlet-Chevallev appliqué à K , il existe donc une puissance d'exposant $>0$ de $\mathfrak{N}$ l'une d'elles , par exemple de $e_0$ , qui est égale à un produit de puissances des $e_i$ $(1\leqslant i\leqslant s')$ ; le sous-groupe H de $H_2$ engendré par les $e_i$ $(1\leqslant i\leqslant s')$ et les $c_i^{\sigma^k}$ $(0\leqslant i\leqslant s', 0\leqslant k\leqslant m_i-2)$ est donc d'indice fini dans $H_2$ , et a fortiori dans $U_L^S$ . En outre , le nombre des générateurs de H que nous venons d'indiquer est $s'+\sum_{i=0}^{s'}(m_i-1)=(\sum_{i=0}^{s'}m_i)-1$ ; mais ce nombre est égal à s , puisque $\sum_{i=0}^{s'}m_i$ est le nombre total de places de S (définition des corps de décomposition) ; en vertu du th. de Dirichlet-Chevalley appliqué à $\mathfrak{M}$ L , ces générateurs sont logarithmiquement indépendants (sans quoi $U_L^S/H$ ne serait pas fini) , donc forment une base (multiplicative) du groupe H . En d'autres termes , tout élément de H peut s'écrire sous la forme $\prod_{i=1}^{s'}e_i^{u_i}\prod_{i=0}^{s'}c_i^{h_i(\sigma)}$ , où les $u_i$ sont des entiers rationnels bien déterminés , et où $h_i(\sigma)$ est un polynôme en $\sigma$ , à coefficients entiers rationnels , bien déterminé modulo $(1+\sigma+\sigma^2+\ldots+\sigma^{m_i-1})$ (en raison des relations $N_{M_i/K}(c_i)=1$) .

Nous pouvons maintenant appliquer le lemme de Herbrand au sous-groupe H et aux endomorphismes $f_1$ et $f_2$ (car par construction il est clair que $f_1(H)\subset H$ et $f_2(H)\subset H$) , ce qui donne

$$(7)\qquad \frac{(U_K^{S'}:N_{L/K}(U_L^S))}{(\mathfrak{f}_1(\mathfrak{A}):f_2(U_L^S))}=\frac{((H\cap U_K^{S'}):f_1(H))}{((H\cap\mathfrak{f}_1(\mathfrak{A})):f_2(H))}$$

(compte tenu de $f_2(U_L^S)=U_K^{S'}$) , pourvu que les indices du second membre de cette formule soient finis .

Montrons d'abord que $f_1^{-1}(1)=f_2(U_L^S)$ ; en effet , si pour un élément $z\in U_L^S$ , on a $f_1(z)=N_{L/K}(z)=1$ , il résulte du th. normique de Hilbert (Alg., chap.V, § 11 th.3) qu'il existe $y\in L^*$ tel que $z=y^{1-\sigma}$ . Or , pour toute place $P\in S$ , P prolonge une place non ramifiée P' de K , donc tout élément de $L_P^*$ est produit d'un élément de $K_{P'}^*$ et d'une unité P-adique ; autrement dit , on a $J_L=J_K J_L^S$ (en identifiant $J_K$ à son extension dans $J_L$) ; comme $J_K=K^* J_K^{S'}$ , on a $J_L=K^* J_K^{S'} J_L^S=K^* J_L^S$ puisque $J_K^{S'}\subset J_L^S$ ; il en résulte que $L^*=K^*(L^*\cap J_L^S)=K^* U_L^S$ ; on peut donc écrire $y=xt$ , où $x\in K^*$ et $t\in U_L^S$ ; la relation $z=y^{1-\sigma}$ donne $z=t^{1-\sigma}$ ce qui démontre notre assertion .

Déterminons en second lieu le groupe $H\cap U_K^{S'}$ . Soit $z=\prod_{i=1}^{s'} e_i^{u_i}\prod_{i=0}^{s'} c_i^{h_i(\sigma)}$ un élément de ce groupe ; on doit donc avoir $z^{1-\sigma}=1$ , ce qui donne $h_i(\sigma)(1-\sigma)\equiv 0$ $(\mathrm{mod}.(1+\sigma+\ldots+\sigma^{m_i-1}))$ , et par suite $h_i(\sigma)\equiv 0$ $(\mathrm{mod}.(1+\sigma+\ldots+\sigma^{m_i-1}))$ , d'où $z=\prod_{i=1}^{s'} e_i^{u_i}$ . D'autre part , comme $N_{L/K}(c_i)=(N_{M_i/K}(c_i))^{n(P_i')}=1$ , $f_1(H)$ est le groupe des $z^n$ lorsque z parcourt $H\cap U_K^{S'}$ . On en conclut que $((H\cap U_K^{S'}):f_1(H))=n^{s'}$

Déterminons enfin les groupes $H\cap f_1^{-1}(1)$ et $f_2(H)$ . Si $z=\prod_{i=1}^{s'} e_i^{u_i}\prod_{i=0}^{s'} c_i^{h_i(\sigma)}$ est tel que $N_{L/K}(z)=1$ , il vient $(\prod_{i=1}^{s'} e_i^{u_i})^n=1$ , d'où $u_i=0$ pour $1\leqslant i\leqslant s'$ ; la réciproque est évidente . Supposons maintenant que $z\in f_2(H)$ ; on a alors $z=\prod_{i=0}^{s'} c_i^{(1-\sigma)g_i(\sigma)}$ , donc $h_i(\sigma)\equiv(1-\sigma)g_i(\sigma)$ $(\mathrm{mod}.(1+\sigma+\ldots+\sigma^{m_i-1}))$ . Montrons que cette dernière relation est équivalente à $h_i(1)\equiv 0$ $(\mathrm{mod}.m_i)$ ; elle l'entraîne évidemment ; d'autre part , si inversement on a $h_i(1)=k_i m_i$ , $k_i$ étant entier rationnel , on peut écrire $h_i(\sigma)-k_i m_i=(1-\sigma)p(\sigma)$ , où p est un polynôme à coefficients entiers rationnels (Alg., chap.IV, § 1, prop.4) ; on a de même $k_i(1+\sigma+\ldots+\sigma^{m_i-1})-k_i m_i=(1-\sigma)q(\sigma)$, où q est un polynôme à coefficients entiers rationnels ; d'où $h_i(\sigma)=(1-\sigma)(p(\sigma)-q(\sigma))+k_i(1+\sigma+\ldots+\sigma^{m_i-1})$ , ce qui prouve notre assertion . On en conclut que l'on a $((H\cap f_1^{-1}(1)):f_2(H))=\prod_{i=0}^{s'} m_i=n^{s'+1}/\prod_{P'\in S'} n(P')$ .

Ces résultats donnent , en vertu de la formule (7) , l'expression

$$(U_K^{S'} : N_{L/K}(U_L^S)) = \Big( \prod_{P' \in S'} n(P') \Big) / n$$

et finalement , en vertu des formules (4),(5) et (6) , la <u>première inégalité fondamentale</u> sous la forme plus précise

(8) $$(J_K : K^* N_{L/K}(J_L)) = [L:K] \cdot ((U_K^{S'} \cap N_{L/K}(J_L^S)) : N_{L/K}(U_L^S)) \quad .$$

<u>5 . Application à la décomposition des diviseurs premiers dans une extension cyclique</u> .

PROPOSITION 1 .- <u>Soit</u> L <u>une extension cyclique de</u> K , <u>dont le degré sur</u> K <u>est une puissance</u> $q^k$ <u>d'un nombre premier . Il existe alors dans</u> K <u>une infinité de diviseurs premiers qui ne se décomposent pas dans</u> L (autrement dit , qui sont encore des diviseurs premiers dans L).

Supposons d'abord que $[L:K]=q$ soit premier . Si les diviseurs premiers de K étaient tous décomposés dans L , à l'exception d'un ensemble fini S' d'entre eux, on aurait $L \cap K_{P'} \neq K$ pour tout $P' \notin S'$, et comme $[L:K]$ est premier , cela n'est possible que si $L \subset K_{P'}$ , donc $K_{P'}(L) = K_{P'}$ , et par suite $K_{P'}^* \subset N_{L/K}(J_L)$ pour tout $P' \notin S'$ . Mais en vertu du th. d'approximation , pour tout idèle $z \in J_K$ , il existe un $x \in K^*$ tel que $xz_{P'} \in (K_{P'}^*)^q \subset N_{L/K}(J_L)$ pour toutes les places $P' \in S'$ ,d'où $xz \in N_{L/K}(J_L)$ . On aurait donc $J_K = K^* N_{L/K}(J_L)$ , ce qui contredit la première inégalité fondamentale .

Passons au cas où $[L:K]=q^k$ , $k>1$ . Soit M le sous-corps de L tel que $[M:K]=q$ . D'après ce qui précède , il existe une infinité de diviseurs premiers de K qui ne se décomposent pas dans M . Soit P' l'un d'eux , et soit $E = L \cap K_{P'}$ son corps de décomposition dans L . Comme $[E:K]$ est une puissance de q , on ne peut avoir que E=K ou $E \supset M$ ; mais dans le second cas , P' se décomposerait dans M , contrairement à l'hypothèse . On a donc E=K , ce qui signifie que P' ne se décompose pas dans L .

Bien entendu , si L est une extension abélienne <u>non cyclique</u> de K , toute

place non ramifiée de K se décompose dans L , puisque le groupe de décomposition d'une place est nécessairement cyclique , donc ne peut coïncider avec le groupe de Galois de L sur K .

6 . La seconde inégalité fondamentale .

Nous nous proposons de montrer que , pour toute extension abélienne L de K , l'indice $(J_K : K^* N_{L/K}(J_L))$ divise $[L:K]=n$ . Remarquons en premier lieu que chacun des degrés locaux de L sur K étant un diviseur de n , pour tout idèle $z \in J_K$ $z^n$ appartient à $N_{L/K}(J_L)$ ; donc l'ordre d'un élément quelconque du groupe quotient $J_K/(K^* N_{L/K}(J_L))$ divise en tout cas n . Pour prouver que l'ordre de ce groupe lui-même divise n , nous allons d'abord montrer qu'on peut se borner au cas où n est premier , et où K contient les racines n-èmes de l'unité .

En effet , soit M une sous-extension (abélienne) de L . On peut écrire

$$(J_K : K^* N_{L/K}(J_L)) = (J_K : K^* N_{M/K}(J_M))(K^* N_{M/K}(J_M) : K^* N_{L/K}(J_L))$$

Comme $N_{L/K}(J_L) = N_{M/K}(N_{L/M}(J_L)) \subset N_{M/K}(J_M)$ , le second indice du produit précédent est égal à

$$(N_{M/K}(J_M) : (N_{M/K}(J_M) \cap (K^* N_{M/K}(N_{L/M}(J_L))))$$

qui divise $(N_{M/K}(J_M) : N_{M/K}(M^* N_{L/M}(J_L)))$ . Mais l'application $z \to N_{M/K}(z)$ de $J_M$ dans $J_K$ étant un homomorphisme , $(N_{M/K}(J_M) : N_{M/K}(M^* N_{L/M}(J_L)))$ divise $(J_M : M^* N_{L/M}(J_L))$ ; donc $(J_K : K^* N_{L/K}(J_L))$ divise le produit

$$(J_K : K^* N_{M/K}(J_M))(J_M : M^* N_{L/M}(J_L)) \quad .$$

Comme L est une extension abélienne de M , on voit que si la seconde inégalité fondamentale est vraie pour tous les diviseurs de n , elle l'est pour n , ce qui permet donc de se borner au cas où n est premier . Soit alors K' l'extension abélienne de K obtenue par adjonction à K de toutes les racines n-èmes de l'unité ; d'après ce qui précède , $(J_K : K^* N_{K'(L)/K}(J_{K'(L)}))$ divise le produit $(J_{K'} : K'^* N_{K'(L)/K'}(J_{K'(L)})) \cdot (J_K : K^* N_{K'/K}(J_{K'}))$ . Mais l'ordre de tout élément de $J_K/(K^* N_{K'/K}(J_{K'}))$ divise le degré $[K':K]$ , qui est lui-même un diviseur de n-1 (§ 1, prop. 5) , donc est étranger à n ; on en conclut que $(J_K : K^* N_{K'/K}(J_K))$

est étranger à n . D'autre part , comme l'ordre de tout élément $\neq 1$ de $J_K/(K^*N_{L/K}(J_L))$ divise n (donc est égal à n) , $(J_K:K^*N_{L/K}(J_L))$ est une puissance de n ; comme elle divise $(J_K:K^*N_{K'(L)/K}(J_{K'(L)}))$ , elle divise aussi $(J_{K'}:K'^*N_{K'(L)/K'}(J_{K'(L)}))$ : la seconde inégalité fondamentale sera démontrée si on prouve que ce dernier indice divise $[K'(L):K'] = n$ . Nous pourrons donc supposer dans ce qui suit que n est premier et que K contient toutes les racines n-èmes de l'unité . On sait alors (Alg., chap.V, § 11, prop.6) que L est le corps des racines d'un polynôme $X^n - \beta_0$ , où $\beta_0 \in K$ n'est pas puissance n-ème d'un élément de K .

Soit S un ensemble fini de places de K , satisfaisant aux conditions suivantes : S contient les places à l'infini , les places de K ramifiées dans L , celles qui divisent n ; en outre , $\beta_0$ est une S-unité , et on a $J_K = K^* J_K^S$ (cf. § 1, th.4) . Désignons par $J_K^{S,n}$ le sous-groupe ouvert $(\prod_{P \in S} K_P^{*n}) \times (\prod_{P \notin S} U_P)$ , et par H le groupe $K^* J_K^{S,n}$ ; nous allons étudier la structure du groupe quotient $J_K/H$ . Nous désignerons par s+1 le nombre d'éléments de S .

Démontrons d'abord le lemme suivant :

Lemme 3 .- Il existe s S-unités $\beta_1, \beta_2, \ldots, \beta_s$ , ainsi que s+1 places $P_i$ $(0 \leq i \leq s)$ dans $\beta^S$ , telles que :

1° $\beta_i \notin (K_{P_j}^*)^n$ pour $0 \leq i \leq s$ , $0 \leq j \leq s$ , $i \neq j$ ;

2° $\beta_i \notin (K_{P_i}^*)^n$ pour $0 \leq i \leq s$ .

Le groupe $U_0$ des racines de l'unité dans K est cyclique et a un ordre multiple de n par hypothèse ; il résulte alors du th. de Dirichlet-Chevalley (§ 1, th.5) que le groupe quotient $U_K^S/(U_K^S)^n$ est produit direct de s+1 groupes cycliques d'ordre n . Comme $\beta_0$ n'est pas une puissance n-ème dans K , il existe s éléments $\beta_i$ $(1 \leq i \leq s)$ de $U_K^S$ dont les classes mod. $(U_K^S)^n$ forment , avec celle de $\beta_0$ , une base (sur $F_p$) du groupe quotient $U_K^S/(U_K^S)^n$ . Montrons que , si $E_i$ $(0 \leq i \leq s)$ désigne le corps des racines de $X^n - \beta_i$ sur K , les s+1 corps $E_i$ sont linéairement disjoints

sur K . Il nous suffira de prouver par récurrence sur j ($1 \leqslant j \leqslant s+1$) que j quelconques des s+1 corps $E_i$ sont linéairement disjoints . Considérons par exemple les j+1 corps $E_i$ tels que $0 \leqslant i \leqslant j$ , et soit M le corps composé des $E_i$ d'indice $\leqslant j-2$. Si $\gamma_i$ est une racine de $X^n-\beta_i$ , il suffit de prouver que $\gamma_j$ n'est pas contenu dans $M(\gamma_{j-1})$ ; dans le cas contraire , on aurait $\beta_j=\lambda^n\beta_{j-1}^k$ , où $\lambda \in M$ et k est étranger à n (Alg., chap.V, § 11, prop.6) . Mais comme les $\beta_i$ appartiennent à K , on aurait $\lambda^n \in K$ ; montrons que cela entraîne $\lambda=\mu\prod_{i=0}^{j-2}\gamma_i^{h_i}$ avec $\mu \in K$ . En effet , soit $\sigma_i$ un générateur du groupe de $E_i$ sur K , prolongé à M par la condition de laisser invariants les éléments des $E_h$ d'indice $\neq i$ ($0 \leqslant i \leqslant j-2$) ; on a $\sigma_i(\gamma_i)=\zeta_i\gamma_i$ , où $\zeta_i$ est une racine primitive n-ème de l'unité . Comme $\lambda^n \in K$ , on a $\sigma_i(\lambda)=\zeta_i^{h_i}\lambda$ , donc $\lambda\gamma_i^{-h_i}$ est invariant par $\sigma_i$ . On en déduit aussitôt que $\lambda\prod_{i=0}^{j-2}\gamma_i^{-h_i}$ est invariant par tous les $\sigma_i$, donc dans K . Mais on aurait alors $\beta_j=\mu^n\beta_{j-1}^k\prod_{i=0}^{j-2}\beta_i^{h_i}$ , contrairement à la définition des $\beta_i$ .

Soit T le corps composé des s+1 corps $E_i$ , et pour chaque i , soit $T_i$ le corps composé des $E_j$ d'indice $j \neq i$ . On a $[T:T_i]=n$ ; il existe donc (prop.1) une infinité de places de $T_i$ qui ne se décomposent pas dans T ; en particulier il existe une telle place $P_i'$ prolongeant une place $P_i \in S$ de K , non ramifiée dans T . D'autre part , le groupe de décomposition $\Delta_i$ de $P_i$ dans T est cyclique et non réduit à l'élément neutre par hypothèse ; comme le groupe de Galois de T sur K est produit direct de s+1 groupes cycliques d'ordre premier n , $\Delta_i$ est nécessairement d'ordre n . Si $T_i'$ est le corps de décomposition de $P_i$ dans T , on a donc $[T:T_i']=n$ . Par ailleurs $T_i'=T \cap K_{P_i} \subset T \cap (T_i)_{P_i'}=T_i$ puisque $P_i'$ n'est pas décomposé dans T ; on en conclut que $T_i'=T_i$ . Cela prouve que , si $j \neq i$ , on a $\gamma_j \in K_{P_i}^*$ , c'est-à-dire $\beta_j \in (K_{P_i}^*)^n$ , et $\gamma_i \notin K_{P_i}$ , donc $\beta_i \notin (K_{P_i}^*)^n$ .

Ce lemme étant démontré , pour tout indice i tel que $0 \leqslant i \leqslant n$ , soit $z_i$ un idèle dont toutes les composantes sont 1 , sauf celle d'indice $P_i$, égale à une uniformisante de $K_{P_i}$ . Comme $z_i \in K^* J_K^S = J_K$ , on a $z_i^n \in K^* J_K^{S,n} = H$ . Soit $H_1$ le sous-groupe

de $J_K$ engendré par H et les $z_i$ $(0\leqslant i\leqslant s)$ ; nous allons prouver que $H_1=J_K$ et que le groupe quotient $H_1/H$ est produit direct des s+1 groupes cycliques d'ordre n engendrés par les classes des $z_i$ (mod.H) .

Etablissons d'abord ce second point ; il suffit pour cela de montrer que si on a une relation de la forme $\prod_{i=0}^{s} z_i^{t_i}=\theta u$ , où $\theta\in K^*$ et $u\in J_K^{S,n}$ , $\theta$ est nécessairement une puissance n-ème dans $K^*$ ; en considérant les $P_i$-composantes des deux membres de cette relation , il en résultera en effet que les $t_i$ sont des multiples de n , ce qui prouvera notre assertion .

Soit V l'extension de K obtenue en adjoignant à K une racine $\gamma$ du polynôme $f(X)=X^n-\theta$ ; il faut montrer que $[V:K]=1$ . Dans le cas contraire , V serait une extension cyclique de K , de degré n ; mais nous allons voir qu'on aurait alors $J_K=K^*N_{V/K}(J_V)$ , contrairement à la première inégalité fondamentale . En effet, soit d'abord P une place de S ; comme on a $u\in J_K^{S,n}$ , $\theta$ est puissance n-ème d'un élément de $K_P$ , d'où $K_P(V)=K_P$ et $K_P^*\subset N_{V/K}(J_V)$ . Si $P\notin S$ , mais est distinct des $P_i$ , P n'est pas ramifié dans V ; en effet , la différente de $\gamma$ est $f'(\gamma)=n\gamma^{n-1}$, donc les diviseurs premiers du discriminant de $\gamma$ divisent n ou $\theta$ , et $\theta$ est par définition une unité dans $K_P$ . On a donc $U_P\subset N_{V/K}(J_V)$ (chap.I, § 6, prop.1) . Enfin , on a $\beta_i\in(K_{P_j}^*)^n$ pour $j\neq i$ (lemme 3) ; d'autre part , pour $P\in S$ , la composante de $\beta_i$ dans $K_P$ appartient à $N_{V/K}(J_V)$ d'après ce qui précède , et enfin si $P\notin S$ et est distinct des $P_j$ , la composante de $\beta_i$ dans $K_P^*$ est une unité , donc appartient encore à $N_{V/K}(J_V)$ . On voit ainsi que toutes les composantes de $\beta_i$, à l'exception de celle dans $K_{P_i}$ , appartiennent à $N_{V/K}(J_V)$ ; l'idèle $a_i$ dont toutes les composantes sont 1 , sauf celle dans $K_{P_i}^*$ égale à $\beta_i$ , appartient donc à $K^*N_{V/K}(J_V)$ . Mais on sait que $(U_{P_i}:(U_{P_i})^n)=n$ , puisque $K_{P_i}$ contient les racines n-èmes de l'unité , et que $P_i$ ne divise pas n (chap.I, § 1, n°7) . En vertu du lemme 3 , le groupe $U_{P_i}$ est engendré par $(U_{P_i})^n$ et par $a_i$ , d'où $U_{P_i}\subset K^*N_{V/K}(J_V)$ . On a ainsi démontré que $J_K^S\subset K^*N_{V/K}(J_V)$ , et comme $J_K=K^*J_K^S$ , on aurait

bien $J_K=K^*N_{V/K}(J_V)$ .

Ce résultat prouve entre autres que $(H_1:H)=n^{s+1}$ . Pour montrer que $H_1=J_K$ , il nous suffit d'établir que $(J_K:H)=n^{s+1}$ . On peut écrire $(J_K:H)=(K^*J_K^S:K^*J_K^{S,n})=$ $=(J_K^S:(J_K^S\cap(K^*J_K^{S,n})))$ . Or , on a $J_K^S\cap(K^*J_K^{S,n})=U_K^SJ_K^{S,n}$ , donc

$$(9)\qquad (J_K:H)=(J_K^S:U_K^SJ_K^{S,n})=(J_K^S:J_K^{S,n})/(U_K^SJ_K^{S,n}:J_K^{S,n}) .$$

L'étude de la structure de $H_1/H$ nous a montré entre autres que $U_K^S\cap J_K^{S,n}=(U_K^S)^n$ (il suffit de prendre $t_i=0$ pour tout i dans la démonstration) ; on a donc $(U_K^SJ_K^{S,n}:J_K^{S,n})=(U_K^S:(U_K^S)^n)=n^{s+1}$ , comme on l'a vu dans la démonstration du lemme 3 . D'autre part , on a $(J_K^S:J_K^{S,n})=\prod_{P\in S}(K_P^*:(K_P^*)^n)$ par définition . Si P est une place à l'infini , et $K_p=C$ , on a $(K_p^*:(K_p^*)^n)=1$ . Si P est une place à l'infini et $K_p=R$ , le nombre premier n ne peut être que 2 , puisque $K_p$ contient les racines n-èmes de l'unité ; on a alors $(K_p^*:(K_p^*)^n)=n$ . Enfin , si $P\notin S$ est une place finie , on a $(K_p^*:(K_p^*)^n)=n^2N(P^{v_P(n)})$ (chap.I,§ 1,n°7) . Si t est le nombre de places finies dans S , on a donc $(J_K^S:J_K^{S,n})=n^{2t+r_1}N(n)=n^{2t+r_1+n}$ (puisque S contient tous les diviseurs premiers de n). Mais on a $n=r_1+2r_2$ et $s+1=t+r_1+r_2$ donc $2t+r_1+n=2(s+1)$ , et $(J_K^S:J_K^{S,n})=n^{2(s+1)}$ . Portant ces résultats dans (9) , il vient $(J_K:H)=n^{s+1}$ , d'où $J_K=H_1$ .

Considérons maintenant dans $J_K$ le sous-groupe H' engendré par H et les $z_i$ d'indice $i\geqslant 1$ ; on a $(J_K:H')=n$ d'après ce qui précède . D'autre part , on a évidemment $J_K^{S,n}\subset N_{L/K}(J_L)$ , puisque $U_P\subset N_{L/K}(J_L)$ pour toute place $P\notin S$ (non ramifiée par hypothèse dans L) ; donc $H\subset K^*N_{L/K}(J_L)$ . Mais pour $i\geqslant 1$ , on a $\pi_0\in(K_{P_i}^*)^n$ d'après le lemme 3 , donc $K_{P_i}^*\subset N_{L/K}(J_L)$ . On a donc $H'\subset K^*N_{L/K}(J_L)$ , ce qui achève la démonstration de la seconde inégalité fondamentale .

Remarque .- Avec les notations précédentes , nous allons voir que les raisonnements précédents permettent de démontrer le lemme suivant :

Lemme 4 .- Le sous-groupe H de $J_K$ est identique au sous-groupe $K^*N_{T/K}(J_T)$ .

En effet , si $H_i$ est le sous-groupe de $J_K$ engendré par H et les $z_j$ d'indice $j\neq i$ , nous venons de voir que $\bigcap_i H_i \subset K^* N_{K(\gamma_i)/K}(J_{K(\gamma_i)})$ ; en vertu de la première inégalité fondamentale , on a nécessairement $H_i = K^* N_{K(\gamma_i)/K}(J_{K(\gamma_i)})$ ; le groupe $K^* N_{T/K}(J_T)$ étant évidemment contenu dans tous les groupes $H_i$ est contenu dans leur intersection , qui n'est autre que H . Mais la seconde inégalité fondamentale montre que $(J_K : K^* N_{T/K}(J_T)) \leqslant [T:K] = n^{s+1} = (J_K : H)$ ; on a donc bien $H = K^* N_{T/K}(J_T)$ .

COROLLAIRE .- Toute extension cyclique Z de K de degré n , telle que les diviseurs premiers $P \notin S$ ne soient pas ramifiés dans Z , est contenue dans T .

En effet , Z est obtenu en adjoignant à K les racines d'un polynôme $X^n - \alpha$ , où $\alpha \in K^*$ n'est pas puissance n-ème . Si un diviseur premier $P \notin S$ divise $\alpha$ , $v_p(\alpha)$ est nécessairement un multiple de n , sinon , pour une racine y de $X^n - \alpha$ et un diviseur premier P' de P dans Z , $v_{P'}(y)$ ne serait pas entier , contrairement à l'hypothèse que P est non ramifié dans Z . Si $\varpi$ est une uniformisante de $K_p$, la relation $J_K = K^* J_K^S$ montre que $\varpi^n = \lambda^n u$ , où $\lambda \in K^*$ et $u \in J_K^{S,n}$ ; en multipliant $\alpha$ par une puissance n-ème , on peut donc supposer que $\alpha \in J_K^S$ , donc $\alpha \in U_K^S$ ; $\alpha$ est par suite produit d'une puissance n-ème et d'un produit de puissances des $\beta_i$ $(0 \leqslant i \leqslant s)$ , et par suite toute racine y de $X^n - \alpha$ appartient à T .

7 . Le théorème de Hasse .

Soit L une extension abélienne de K . L'application canonique $\psi_{L/K,P'}$ de $K_p^*$, sur le groupe de décomposition $\mathcal{L}_{p'}$ de la place P' (dans L) est encore appelée le symbole de restes normiques relatif à P' ; on dit qu'un élément $x \in K^*$ est reste normique pour P' s'il est dans le noyau de $\psi_{L/K,P'}$ , c'est-à-dire si , dans le corps $K_p$, , x appartient à $K_{p'}^* \cap N_{L/K}(J_L) = N_{K_{p'}(L)/K_p}(K_{p'}(L^*))$

THÉORÈME 2 (Hasse) .- Soit L une extension cyclique de K . Pour qu'un élément $x \in K^*$ soit norme d'un élément de $L^*$ , il faut et il suffit que , pour toute place P de K , x soit reste normique (autrement dit que , dans tout corps local

$K_{p'}$ , x soit norme d'un élément de $K_{p'}(L)$).

En effet , les deux ~~XXXX~~ inégalités fondamentales prouvent alors que $(J_K : K^* N_{L/K}(J_L)) = [L:K]$ . On déduit donc de la formule (8à que l'on a $N_{L/K}(U_L^S) = U_K^{S'} \cap N_{L/K}(J_L^S)$ . Nous allons en déduire que $K^* \cap N_{L/K}(J_L) = N_{L/K}(L^*)$ , ce qui prouvera le th.2 . Soit en effet x un élément quelconque de $K^* \cap N_{L/K}(J_L)$ ; on peut supposer S' pris assez grand pour que x soit une S'-unité ; en outre , on a $N_{L/K}(J_L^S) = J_K^{S'} \cap N_{L/K}(J_L)$ , car une unité dans $K_{p'}$ ne peut être norme que d'une unité dans $K_{p'}(L)$ . On a donc $x \in N_{L/K}(U_L^S) \subset N_{L/K}(L^*)$ . Ceci montre que $K^* \cap N_{L/K}(J_L) \subset N_{L/K}(L^*)$ ; l'inclusion opposée est évidente .

La conclusion du th.2 n'est plus valable lorsque L est une <u>extension abélienne non cyclique</u> quelconque de K .

<u>8 . Lemmes auxiliaires sur les extensions cycliques circulaires</u> .

Nous dirons qu'une extension L de K est <u>circulaire</u> si elle est contenue dans un corps de racines de l'unité $R_m(K)$ sur le corps K . Nous allons d'abord établir une forme affaiblie de la loi de réciprocité pour certaines extensions cycliques circulaires :

<u>Lemme 5 .- Soit L une extension cyclique de K , contenue dans $R_m(K)$ , et dont les corps locaux correspondant aux places à l'infini ~~XXXX~~ de L sont identiques à C . Soit x un élément de K tel que x soit reste normique pour toute place finie de K divisant m . Alors on a $\psi_{L/K}(x) = 1$ .</u>

On a évidemment $\psi_{L/K}(y) = 1$ pour tout élément de K qui est norme d'un élément de L , en particulier pour toute puissance n-ème d'un élément de K (si $n = [L:K]$). Soient $P_i'$ ($1 \leqslant i \leqslant h$) les places finies de K divisant m , et pour chaque indice i, soit $P_i$ une place de L prolongeant $P_i'$ . Par hypothèse , pour chaque indice i , il existe un élément $u_i \in L_{P_i}$ tel que $x = N_{L_{P_i}/K_{P_i'}}(u_i)$ . En vertu du th. d'approximation , il existe $y \in L$ tel que

$$v_{P_i}(y-u_i) > v_{P_i'}(m) + v_{P_i'}(x) - (n-1)\inf(0, v_{P_i}(u_i))$$

pour $1 \leqslant i \leqslant h$ ; d'où aussitôt

$$v_{P'_i}(x \cdot N_{L/K}(y)) > v_{P'_i}(m) + v_{P'_i}(x)$$

ce qui montre que $x_1 = N_{L/K}(y)/x$ est une unité $P'_i$-adique pour $1 \leqslant i \leqslant h$ et que $x_1 \equiv 1 \pmod{m}$. En outre, si $(x_1) = ab^{-1}$, où a et b sont des diviseurs entiers étrangers de K, a et b sont étrangers aux $P'_i$, donc il en est de même de $\beta = N(b)$, qui est par suite un entier rationnel étranger à m ; il existe donc un entier rationnel $\gamma$ étranger à m tel que $\beta\gamma \equiv 1 \pmod{m}$ ; on en conclut que $(\beta\gamma)^n x_1 = x_2$ est entier dans K, est reste normique pour tous les $P'_i$ $(1 \leqslant i \leqslant h)$ et tel que $x_2 \equiv 1 \pmod{m}$. Remplaçant x par $x_2$, nous pouvons désormais supposer que x possède les trois propriétés précédentes.

Toute place finie P' distincte des $P'_i$ dans K est non ramifiée dans $R_m(K)$, car le nombre premier $p_i$ multiple de $P'_i$ n'est pas ramifié dans $R_m(Q)$ (§ 1, prop.6 et chap.I, § 1, n°3). Soit $\sigma_{P'}$ l'automorphisme de Frobenius de $R_m(K)$ pour la place P' ; il induit sur L l'automorphisme de Frobenius pour P' ; par suite, $\psi_{L/K,P'}(x)$ est le K-automorphisme de L restriction de $\sigma_{P'}^{v_{P'}(x)}$ ; $\prod_{P' \in \Phi_{fin}} \psi_{L/K,P'}(x)$ est donc la restriction à L de $\tau = \prod_{P' \notin S'} \sigma_{P'}^{v_{P'}(x)}$ (S' ensemble des $P'_i$ et des places à l'infini de K). Soit $\zeta$ une racine m-ème primitive de l'unité ; nous allons calculer $\tau(\zeta)$. On a par définition $\sigma_{P'}(\zeta) \equiv \zeta^{N(P')} \pmod{P}$, où P est un diviseur premier de P' dans $R_m(K)$ ; mais $\sigma_{P'}(\zeta)$ est nécessairement de la forme $\zeta^k$ (k entier), et on ne peut avoir $\zeta^j - \zeta^k \equiv 0 \pmod{P}$ que si $\zeta^j = \zeta^k$ : en effet, $\zeta$ est une unité, et on a $m = \prod_{k=1}^{m-1}(1 - \zeta^k)$, donc P, qui ne divise pas m, ne peut diviser aucun des éléments $1 - \zeta^k \neq 0$. On a donc $\sigma_{P'}(\zeta) = \zeta^{N(P')}$, d'où $\tau(\zeta) = \zeta^t$, où $t = \prod_{P' \notin S'} N(P')^{v_{P'}(x)}$. Comme $v_{P'_i}(x) = 0$ pour $1 \leqslant i \leqslant h$, on a aussi $t = \prod_{P' \in \Phi_{fin}} N(P')^{v_{P'}(x)} = |N_{K/Q}(x)|$. D'autre part, pour toute place à l'infini P' de K, on ne peut avoir par hypothèse $\psi_{L/K,P'}(x) \neq 1$ que si $K_{P'}$ est égal à R et si x est négatif dans $K_{P'}$ ; si s est le nombre des places P' qui satisfont à ces conditions,

$\prod_{p \in \Phi_\infty} \psi_{L/K,p}(x)$ est la restriction à L de l'automorphisme $\tau'$ tel que $\tau'(\zeta) = \zeta^{(-1)^s}$. Finalement, on voit que $\psi_{L/K}(x)$ est la restriction à L de l'automorphisme $\sigma$ de $R_m(K)$ tel que $\sigma(\zeta) = \zeta^{(-1)^s |N_{K/Q}(x)|}$. Mais par définition de s, $N_{K/Q}(x)$ a le signe de $(-1)^s$ ; d'autre part, $N_{K/Q}(x)$ est un entier rationnel qui est $\equiv 1 \pmod{m}$ en vertu du choix de x ; on a donc $\sigma(\zeta) = \zeta$, ce qui achève de démontrer le lemme.

Lemme 6.- Etant donnés deux entiers rationnels m,n et des nombres premiers rationnels $p_1, \ldots, p_s$, il existe un entier rationnel $r > 2$ étranger à m, et un caractère $\chi$ du groupe multiplicatif G(r) des éléments inversibles de Z/(r) tels que $\chi(-1)$ soit d'ordre 2 et que $\chi(p_i)$ ait un ordre multiple de n pour $1 \leqslant i \leqslant s$.

Commençons par considérer le cas où $n = \ell^{\nu+1}$, où $\ell$ est un nombre premier et $\nu \geqslant 1$. Montrons que pour tout nombre premier p, il existe un nombre premier q étranger à m, tel que le plus petit des entiers k tels que $p^k \equiv 1 \pmod{q}$ soit de la forme $\ell^h$, avec $h \geqslant \nu+1$. Pour tout entier $h \geqslant 0$, posons $U_h = p^{\ell^h} - 1$ ; on a $U_{h+1}/U_h = V_h = 1 + p^{\ell^h} + p^{2\ell^h} + \ldots + p^{(\ell-1)\ell^h} \equiv \ell \pmod{U_h}$, et $V_h > \ell$. Ceci nous montre d'abord que le pgcd de $U_h$ et $V_h$ divise $\ell$. Distinguons deux cas :

1° $p \not\equiv 1 \pmod{\ell}$. Alors $p^{\ell^h} \equiv p \not\equiv 1 \pmod{\ell}$, donc $U_h \not\equiv 0 \pmod{\ell}$ pour tout h, d'où $V_h \not\equiv 0 \pmod{\ell}$, $U_h$ et $V_h$ sont étrangers.

2° $p \equiv 1 \pmod{\ell}$. Par récurrence sur h, on voit alors que $U_h \equiv 0 \pmod{\ell^2}$ pour $h \geqslant 1$, et $V_0 \equiv 0 \pmod{\ell}$, donc $\ell$ est le pgcd de $U_h$ et $V_h$ pour $h \geqslant 1$, et $V_1$ n'est pas divisible par $\ell^2$.

De ces résultats et du fait que $V_h > \ell$, il résulte que pour tout entier $h \geqslant 1$, il existe un nombre premier $q_h \neq \ell$, divisant $V_h$ et ne divisant pas $U_h$ ; tous ces nombres premiers sont évidemment distincts, puisque $V_h$ divise tous les $U_k$ d'indice $k > h$. On peut donc prendre h assez grand pour que $h \geqslant \nu$ et que $q_h$ soit é-

tranger à m ; alors $\ell^{h+1}$ est le plus petit entier k tel que $p^k \equiv 1 \pmod{q_h}$, ce qui prouve notre assertion .

Soit $\omega$ un entier rationnel $\geqslant 1$ tel que $\ell^{\nu+\omega} > s$ . Du raisonnement précédent résulte qu'il existe s nombres premiers distincts $q_i$ $(1 \leqslant i \leqslant s)$ étrangers à m ,et tels que l'ordre de $p_i$ modulo $q_i$ soit une puissance de $\ell$ multiple de $\ell^{\nu+\omega}$ .Soit $\ell^{\mu_i}$ la plus grande puissance de $\ell$ divisant $q_i - 1$ , et soit $\chi_i$ un caractère de $G(q_i)$ d'ordre $\ell^{\mu_i}$ ; alors $\chi_i(p_i)$ a pour ordre une puissance $\ell^{\nu+\alpha_i}$ , où $\alpha_i \geqslant \omega$ et $\nu+\alpha_i \leqslant \mu_i$ . Pour tout svstème d'entiers $c_i$ tels que $0 \leqslant c_i \leqslant \ell^{\mu_i} - 1$ $(1 \leqslant i \leqslant s)$ , le caractère $\chi_0(x) = \prod_{i=1}^{s} (\chi_i(x))^{c_i}$ est un caractère de $G(r_0)$ , où $r_0 = q_1 q_2 \cdots q_s$ .Nous allons voir qu'on peut choisir les $c_i$ de sorte que l'ordre de chacun des $\chi_0(p_i)$ soit multiple de $\ell^{\nu+1}$ , c'est-à-dire que chacune des s inégalités $(\chi_0(p_i))^{\ell^\nu} \neq 1$ $(1 \leqslant i \leqslant s)$ soit vérifiée . Or , la relation $(\chi_0(p_1))^{\ell^\nu} = 1$ s'écrit

$$(10) \qquad (\chi_1(p_1))^{c_1 \ell^\nu} = \prod_{j=2}^{s} (\chi_j(p_1))^{-c_j \ell^\nu} \quad ;$$

comme l'ordre de $(\chi_1(p_1))^{\ell^\nu}$ est $\ell^{\alpha_1}$ , lorsque les $c_i$ d'indice $> 1$ sont donnés il y a au plus $\ell^{\mu_1 - \alpha_1}$ nombres $c_1$ vérifiant (10) ; le nombre des systèmes $(c_1, \ldots, c_s)$ vérifiant (10) est donc au plus

$$\ell^{\left(\sum_{i=1}^{s} \mu_i\right) - \alpha_1} \leqslant \ell^{\left(\sum_{i=1}^{s} \mu_i\right) - \omega}$$

Par suite , le nombre des systèmes $(c_1, \ldots, c_s)$ vérifiant l'une des relations $(\chi_0(p_i))^{\ell^\nu} = 1$ au moins , est au plus

$$s \cdot \ell^{\left(\sum_i \mu_i\right) - \omega} < \ell^{\sum_i \mu_i}$$

Mais comme le nombre total des $(c_1, \ldots c_s)$ est $\ell^{\sum_i \mu_i}$ , il y au moins un de ces systèmes répondant à la question .

Si $\ell \neq 2$ , $\chi_0$ est d'ordre impair , donc $\chi_0(-1) = 1$ . Si $\ell = 2$ et $\chi_0(-1) = 1$ , soit p un nombre premier de la forme $4k-1$ divisant $4a-1$ , où $a = r_0 m p_1 p_2 \cdots p_s$ (il en existe) ; p est étranger à m , distinct des $p_i$ et des $q_i$ ; si on pose $\chi(x) = \chi_0(x)\left(\frac{x}{p}\right)$ , $\chi$ est un caractère du groupe $G(r_0 p)$ , et on a $\chi(-1) = \left(\frac{-1}{p}\right) = -1$

(§ 1, prop.10) . D'autre part , on a $(\chi(p_i))^{2^\nu}=(\chi_0(p_i))^{2^\nu}\neq 1$ puisque $\nu\geqslant 1$ . Cela étant , pour démontrer le lemme , on peut supposer que n est pair ; soit $n=\prod_j \ell_j^{\nu_j}$ la décomposition de n en facteurs premiers . On peut , d'après ce qui précède , trouver pour chaque j un nombre $r_j>2$ étranger à m et un caractère $\chi_j$ de $G(r_j)$ de sorte que $\chi_j$ soit d'ordre impair pour $\ell_j\neq 2$ , que $\chi_j(p_i)$ ait un ordre multiple de $\ell_j^{\nu_j}$ pour $1\leqslant i\leqslant s$ et pour tout j , et que $\chi_j(-1)=-1$ pour $\ell_j=2$ ; on peut en outre supposer que les $r_j$ sont étrangers deux à deux . Le nombre $r=r_1r_2\cdots r_j$ , et le caractère $\chi=\prod_j\chi_j$ de $G(r)$ répondent alors aux conditions du lemme .

Lemme 7 .- Soient $P_1',P_2',\ldots,P_s'$ des places finies de K , n un entier rationnel . Il existe alors un entier rationnel r non divisible par les $P_i'$ , et une extension cyclique Z de K contenue dans $R_r(K)$ et satisfaisant aux conditions suivantes : 1° chacun des $P_i'$ est non ramifié dans Z , et chacun des degrés locaux $[K_{P_i'}(Z):K_{P_i'}]$ est multiple de n ; 2° tous les corps locaux correspondant aux places à l'infini de Z sont identiques à C .

Soit $p_i$ le nombre premier rationnel multiple de $P_i'$ ($1\leqslant i\leqslant s$) . En vertu du lemme 6 , il existe un entier r étranger aux $p_i$ et au discriminant de K (par rapport à Q) , et un caractère $\chi$ de $G(r)$ , tels que $\chi(-1)=-1$ et que $\chi(p_i)$ ait un ordre multiple de $nf_i$ , où $f_i$ désigne le degré résiduel de $P_i'$ sur $p_i$ ($1\leqslant i\leqslant s$) . Comme le discriminant de $R_r(Q)$ sur Q ne contient que des facteurs premiers de r, et est donc premier au discriminant de K , K et $R_r(Q)$ sont linéairement disjoints sur Q (chap.I, § 5, n°5) et $R_r(K)$ est leur composé ; le groupe de Galois $\Gamma$ de $R_r(K)$ par rapport à K peut donc être identifié à $G(r)$ (§ 1, prop.5) par l'isomorphisme qui , à tout $\sigma\in\Gamma$ , fait correspondre la classe (mod.r) de l'entier $a(\sigma)$ tel que $\sigma(\zeta)=\zeta^{a(\sigma)}$ , où $\zeta$ est une racine r-ème primitive de l'unité . Soit $\Delta$ le sous-groupe de $\Gamma$ , noyau du caractère $\chi$ ; comme $\Gamma/\Delta$ est isomorphe

à $\chi(\Gamma)$ , donc cyclique , le sous-corps Z de $R_r(K)$ , correspondant au sous-groupe $\Delta$ , est une extension cyclique de K ; nous allons voir qu'elle satisfait aux conditions du lemme .

Soit $\sigma_i$ l'automorphisme de Frobenius de $R_r(K)$ pour la place $P_i'$ (qui n'est pas ramifiée dans $R_r(K)$ , puisque $p_i$ est étranger à r , donc non ramifié dans $R_r(Q)$ (§ 1,prop.6 et chap.I,§ 1,n°3)) . On voit comme dans le lemme 5 qu'on a nécessairement $\sigma_i(\zeta)=\zeta^{N(P_i')}$ , avec $N(P_i')=p_i^{f_i}$ ; mais $\sigma_i$ induit sur Z l'automorphisme de Frobenius pour la place $P_i'$ , et le degré local $n(P_i')$ de Z sur K relatif à $P_i'$ est le plus petit exposant t tel que $\sigma_i^t$ , restreint à Z , soit l'automorphisme identique . Comme le groupe de Galois de Z sur K est isomorphe à $\chi(\Gamma)$ , t est l'ordre de $\chi(p_i^{f_i})$ , donc $tf_i$ , ordre de $\chi(p_i)$ , est multiple de $nf_i$ , ce qui prouve que t est multiple de n . Enfin , comme $\chi(-1)=-1$ , l'automorphisme $\zeta\to\zeta^{-1}$ de $R_r(K)$ ne laisse pas fixes tous les éléments de Z . Il est clair que pour toute place à l'infini ~~XXXXX~~ P de $R_r(K)$ , le corps local correspondant est égal à C . Soit P' une place à l'infini de K ; si $K_{P'}=C$ , on a $Z_{P''}=C$ pour toute place à l'infini P'' de Z prolongeant P' . Si au contraire $K_{P'}=R$ , le sous-corps $Z_{P''}$ de C contient des éléments non invariants par l'automorphisme $z\to\bar{z}$ de C , donc il est égal à C , ce qui achève la démonstration .

9 . Démonstration de la loi de réciprocité .

Pour démontre la loi de réciprocité (n°2,th.1) , nous prouverons successivement les trois points suivants :

A) pour tout $x\in K^*$ , $\psi_{L/K}(x)=1$ ;

B) $\psi_{L/K}$ est un homomorphisme de $J_K$ sur $\mathcal{L}$ ;

C) le noyau de $\psi_{L/K}$ est identique à $K^*N_{L/K}(J_L)$ .

A) L'extension abélienne L de K est composée d'extensions cycliques $L_i$ de K , puisque le groupe de Galois de L sur K est produit direct de groupes cycliques.

Or , pour chaque indice i , $\psi_{L_i/K}(x)$ (pour $x \in K^*$) est la restriction à $L_i$ de l'automorphisme $\psi_{L/K}(x)$ de L ; par suite , pour démontrer que $\psi_{L/K}(x)=1$ , il suffit de prouver que $\psi_{L_i/K}(x)=1$ pour tout indice i ; en d'autres termes , on peut se borner au cas où L est une extension cyclique de K . Nous poserons $[L:K]=n$ .

Désignons par $\lambda$ un générateur du groupe de Galois $\mathcal{L}$ de L sur K . On sait qu'à $x \in K^*$ on associe un cocycle $f \in Z^2(\mathcal{L}, L^*)$ en posant $f(\lambda^i, \lambda^j)=1$ si $i+j<n$ , $f(\lambda^i, \lambda^j)=x$ si $i+j \geqslant n$ (chap.I, § 6, lemme à la prop.5) ; nous désignerons par u la classe de f dans le groupe de cohomologie $H^2(\mathcal{L}, L^*)$ .

On sait (n°2) que $\psi_{P'}(x)=1$ pour presque toute place P' de K , c'est-à-dire que x est reste normique pour P' sauf pour un nombre fini de places ; soient $P'_i$ ($1 \leqslant i \leqslant s$) les places finies de K pour lesquelles $x \notin N_{K_{P'_i}(L)/K_{P'_i}}(K_{P'_i}(L)^*)$ . Soit Z une extension cyclique de K contenue dans $R_r(K)$ , satisfaisant aux conditions du lemme 7 , et considérons l'extension cyclique Z(L) de Z ; nous désignerons par $\mathcal{J}$ le groupe de Galois de Z sur K . Nous nous proposons de montrer que : A 1) x est norme d'un élément de Z(L) par rapport à Z .

En vertu du th. de Hasse (th.2) , il suffit de montrer que pour toute place $\overline{P}'$ de Z , x est reste normique (relativement à l'extension Z(L) de Z). C'est immédiat si $\overline{P}'$ est une place à l'infini de Z , car $Z_{\overline{P}'}$ est alors égal à C en vertu des conditions du lemme 7 , donc $Z(L)_{\overline{P}}=C$ pour toute place $\overline{P}$ de Z(L) prolongeant $\overline{P}'$ .

Supposons en second lieu que $\overline{P}'$ soit une place finie de Z ne prolongeant aucune des $P'_i$ , et soit $\overline{P}$ une place de Z(L) prolongeant $\overline{P}'$ ; soient P et P' les restrictions de $\overline{P}$ à L et à K ; on a $Z(L)_{\overline{P}}=Z_{\overline{P}'}(L_P)$ . Par hypothèse , il existe $y \in L_P$ tel que $x=N_{L_P/K_{P'}}(y)$ . Comme le groupe de Galois de $Z_{\overline{P}'}(L_P)$ sur $Z_{\overline{P}'}$ peut être identifié au groupe de $L_P$ sur $L_P \cap Z_{\overline{P}'}$ , on peut écrire $x=N_{(L_P \cap Z_{\overline{P}'})/K_{P'}}(z$

où $z=N_{Z_{\overline{P}_i}(L_P)/Z_{\overline{P}_i}}(y)$ ; or, si $\sigma_j$ $(1\leqslant j\leqslant q)$ sont les $Z_{\overline{P}_i}$-automorphismes de $Z_{\overline{P}_i}(L_P)$, on tire de la relation $z=\prod_j \sigma_j(y)$ que, pour tout $K_{P_i}$-automorphisme $\tau$ de $Z_{\overline{P}_i}(L_P)$, on a $\tau(z)=\prod_j \tau(\sigma_j(y))=\prod_j \sigma_j(\tau(y))$, puisque $Z_{\overline{P}_i}(L_P)$ est une extension abélienne de $K_{P_i}$ ; tous les conjugués de z par rapport à $K_{P_i}$ sont donc des normes (dans $Z_{\overline{P}_i}$) d'éléments de $Z_{\overline{P}_i}(L_P)$, et par suite il en est de même de leur produit x .

Considérons enfin le cas où $P'=P'_i$ (avec les notations précédentes) . La restriction du cocycle f au groupe de décomposition $\mathcal{L}_{P'_i}$ de $P'_i$ dans L, est un cocycle de $Z^2(\mathcal{L}_{P'_i},L_P^*)$ ; soit $u_{P'_i}$ la classe de ce cocycle dans $H^2(\mathcal{L}_{P'_i},L_P^*)$ ; comme $\mathcal{L}_{P'_i}$ est le groupe de Galois de $L_P$ sur $\mathfrak{E}_{P'_i}$, $H^2(\mathcal{L}_{P'_i},L_P^*)$ s'identifie canoniquement à un sous-groupe de $H^2(\mathcal{M},Z_{\overline{P}_i}(L_P)^*)$, en désignant par $\mathcal{M}$ le groupe de Galois de $Z_{\overline{P}_i}(L_P)$ sur $K_{P_i}$ (chap.I, § 6, n°4) . Mais $Z_{\overline{P}_i}$ est, en vertu du lemme 7, une extension non ramifiée de $K_{P'_i}$, dont le degré est multiple de $[L_P:K_{P'_i}]$ ; $Z_{\overline{P}_i}$ contient donc l'extension non ramifiée de $K_{P'_i}$ de degré $[L_P:K_{P'_i}]$. Alors, le groupe $H^2(\mathcal{J}_{P'_i},Z_{\overline{P}_i}^*)$ ($\mathcal{J}_{P'_i}$ groupe de Galois de $Z_{\overline{P}_i}$ sur $K_{P'_i}$) étant canoniquement identifié à un sous-groupe de $H^2(\mathcal{M},Z_{\overline{P}_i}(L_P)^*)$, on sait que $H^2(\mathcal{J}_{P'_i},Z_{\overline{P}_i}^*)$ contient $H^2(\mathcal{L}_{P'_i},L_P^*)$, ce dernier étant identifié au groupe de cohomologie de l'unique extension non ramifiée de $K_{P'_i}$ ayant même degré que $L_P$ (chap.I, § 6, th.2 et cor.2) . Mais $H^2(\mathcal{J}_{P'_i},Z_{\overline{P}_i}^*)$ est le noyau de l'homomorphisme canonique de $H^2(\mathcal{M},Z_{\overline{P}_i}(L_P)^*)$ dans $H^2(\mathcal{N},Z_{\overline{P}_i}(L_P)^*)$, en désignant par $\mathcal{N}$ le groupe de Galois de $Z_{\overline{P}_i}(L_P)$ sur $Z_{\overline{P}_i}$ (chap.I, § 6, prop.6) . Cela entraîne que la restriction de $u_{P'_i}$ à $\mathcal{N}$ est la classe unité du groupe de cohomologie $H^2(\mathcal{N},Z_{\overline{P}_i}(L_P)^*)$, ou encore que tout cocycle de cette classe est un cobord . Or, $\mathcal{N}$ peut être identifié au groupe de Galois de $L_P$ sur $L_P\cap Z_{\overline{P}_i}$, c'est-à-dire à un sous-groupe de $\mathcal{L}_{P'_i}$, engendré par une puissance $\lambda^\alpha$ de $\lambda$, et d'ordre $n/\alpha$ ; le cocycle f' de $H^2(\mathcal{N},Z_{\overline{P}_i}(L_P)^*)$ défini par $f'(\lambda^{\alpha j},\lambda^{\alpha k})=1$ pour $j+k<n/\alpha$, $f'(\lambda^{\alpha j},\lambda^{\alpha k})=x$ pour

$j+k \geqslant n/\alpha$ appartient évidemment à la restriction de $u_{P'_i}$ ; dire que c'est un cobord entraîne que x est une norme d'un élément de $Z_{\overline{P}'}(L_P)$ par rapport à $Z_{\overline{P}'}$ (chap.I, § 6, cor.2 du th.2).

A 2) Nous allons maintenant utiliser le fait que x est norme d'un élément de Z(L) par rapport à Z pour transférer le calcul de $\psi_{L/K}(x)$ au calcul de $\psi_{Z/K}(y)$, où y est un élément de K que nous allons définir . Le groupe $H^2(\mathcal{L}, L^*)$ étant identifié canoniquement à un sous-groupe de $H^2(\mathcal{G}, Z(I)^*)$ ($\mathcal{G}$ groupe de Galois de Z(L) sur K) , le fait que x soit norme (par rapport à Z) d'un élément de Z(L) entraîne que la classe de cohomologie u appartient au noyau del'homomorphisme canonique de $H^2(\mathcal{G}, Z(L)^*)$ dans $H^2(\mathcal{H}, Z(L)^*)$ , où $\mathcal{H}$ est le groupe de Z(L) par rapport à Z (chap.I, § 6, prop.5 (homomorphisme japonois)) ; donc u appartient au groupe $H^2(\mathcal{Z}, Z^*)$ quand on identifie ce dernier à un sous-groupe de $H^2(\mathcal{G}, Z(L)^*)$ (chap.I, § 6, prop.6) ; en d'autres termes , u est transportable à $H^2(\mathcal{Z}, Z^*)$ ; nous poserons $v=\tau_{L,Z}(u)$ . Comme Z est cyclique sur K , il existe un élément $y \in K$ et un générateur $\rho$ de $\mathcal{Z}$ tels que v contienne le cocycle g défini par $g(\rho^i, \rho^j)=1$ pour $i+j<m$ , $g(\rho^i, \rho^j)=y$ pour $i+j \geqslant m$ , en posant $m=[Z:K]$ (chap.I, § 6, lemme à la prop.5). Pour toute place P' de K , les éléments du groupe de décomposition de P' dans Z(L) induisent sur L (resp. Z) les éléments du groupe de décomposition de P' dans L (resp. Z) ; on en déduit que les classes de cohomologie $u_{P'}, v_{P'}$ déterminées par les restrictions des cocycles f,g aux groupes de décomposition respectifs $\mathcal{L}_{P'}, \mathcal{Z}_{P'}$ , sont encore transportables l'une sur l'autre .

Nous allons déduire de ce résultat des relations entre les valeurs de $\psi_{L/K,P'}(x)$ et $\psi_{Z/K,P'}(y)$ pour toute place P' de K .

En premier lieu , si $\psi_{L/K,P'}(x)=1$ , la classe de cohomologie $u_{P'}$ est l'identité, donc il en est de même de $v_{P'}$ , ce qui signifie que $\psi_{Z/K,P'}(y)=1$ (chap.I, § 6, th.2 et cor.2) Soit ensuite P' une place à l'infini de K pour laquelle $\psi_{L/K,P'}(x) \neq 1$ ; cela signifie que $K_{P'}=R$ , $L_P=C$ et que , dans $K_{P'}$ , on a $x<0$ ;

$\psi_{L/K,P'}(x)$ est alors l'unique automorphisme d'ordre 2 de $\mathcal{L}$, l'élément $\lambda^{n/2}$. Ces places sont aussi celles pour lesquelles $Z_{P'}=C$ et $y<0$ dans $K_{P'}$ ; d'où $\psi_{Z/K,P'}(y)=\rho^{m/2}$.

Supposons enfin que P' soit l'une des places $P'_i$, et posons $\psi_{L/K,P'_i}(x)=\lambda^{e_i}$ ; soit $n_i$ le degré local de L pour la place $P'_i$ (degré de $K_{P'_i}(L)$ sur $K_{P'_i}$). Comme le groupe de décomposition $\mathcal{L}_{P'_i}$ est engendré par $\lambda^{n/n_i}$, $e_i$ est multiple de $n/n_i$ ; en outre, si $c_i$ est la classe principale de cohomologie de $K_{P'_i}(L)$ sur $K_{P'_i}$ (chap. I, § 6, n°5), il résulte de la définition de l'homomorphisme principal (loc.cit.) qu'on a $u_{P'_i}=c_i^{e_i n_i/n}$.

D'autre part (lemme 7), $P'_i$ n'est pas ramifiée dans Z, et le degré $m_i$ de $K_{P'_i}(Z)$ sur $K_{P'_i}$ est multiple de n, donc de $n_i$ ; autrement dit, $K_{P'_i}(Z)$ contient l'extension non ramifiée $T_i$ de $K_{P'_i}$, de degré $n_i$ ; en outre, la classe principale de cohomologie de $T_i$ est la puissance $d_i^{m_i/n_i}$ de la classe principale de cohomologie $d_i$ de $K_{P'_i}(Z)$ (parce que l'automorphisme de Frobenius relatif à $T_i$ est la restriction de l'automorphisme de Frobenius relatif à $K_{P'_i}(Z)$ ; cf. chap. I, § 6, n°5). Comme par définition, $c_i$ se transporte sur $d_i$ (loc.cit.), on a $v_{P'_i}=d_i^{e_i m_i/n}$. Le groupe de décomposition de $P'_i$ dans Z étant engendré par $\rho^{m/m_i}$, on voit comme ci-dessus que $\psi_{Z/K,P'_i}(y)=\rho^{e_i m/n}$ (on notera que m, multiple de $m_i$, est a fortiori multiple de n).

Appliquons maintenant le lemme 5 ; on a la relation $\prod_{P'}\psi_{Z/K,P'}(y)=1$, puisque les $P'_i$ ne divisent pas r, et que les corps locaux correspondant aux places à l'infini de Z sont égaux à C. Cette relation s'écrit d'après ce qui précède

$$tm/2+\sum_{i=1}^{s} e_i m/n \equiv 0 \pmod{m}$$

en désignant par t le nombre des places à l'infini où $\psi_{L/K,P'}(x)\neq 1$. On en tire $tn/2+\sum_{i=1}^{s} e_i \equiv 0 \pmod{n}$, ce qui, en vertu de ce qui précède, signifie que $\psi_{L/K}(x)=\prod_{P'}\psi_{L/K,P'}(y)=1$. Le point A) est donc complètement démontré.

B) L'extension L est composée d'extensions cycliques $L_i$ dont les degrés sont

des puissances de nombres premiers , le groupe de Galois de L sur K étant isomèr phe au produit des groupes de Galois des $L_i$ sur K . Soit $M_i$ le corps composé des $L_j$ d'indice $j \neq i$ ; $\mathcal{L}$ est produit direct des groupes $\mathcal{L}_i$ , où $\mathcal{L}_i$ est le groupe de L sur $M_i$ , isomorphe au groupe de $L_i$ sur K . Comme L est une extension cyclique de $M_i$ dont le degré est une puissance d'un nombre premier , il existe une place finie $P_i$ de $M_i$ non ramifiée et non décomposée dans L (n°5,prop.1) . Le groupe de décomposition de $P_i$ dans L est donc égal à $\mathcal{L}_i$ ; soit alors z un idèle de $M_i$ dont la $P_i$-composante est une uniformisante de $(M_i)_{P_i}$ , les autres étant égales à 1 ; par définition , $\psi_{L/M_i}(z)$ est l'automorphisme de Frobenius relatif à $P_i$ , donc engendre $\mathcal{L}_i$ . Mais on a $\psi_{L/M_i}(z)=\psi_{L/K}(N_{M_i/K}(z))$ (chap.I,§ 6,prop.8) donc $\psi_{L/K}(J_K)$ contient tous les groupes $\mathcal{L}_i$ , et par suite $\mathcal{L}$ , ce qui prouve B)

C) Il résulte de A) et de la définition des $\psi_{L/K,P'}$ que le noyau de $\psi_{L/K}$ contient le groupe $K^* N_{L/K}(J_L)$ ; en outre, comme $\psi_{L/K}$ applique $J_K$ sur $\mathcal{L}$ , on a $(J_K : K^* N_{L/K}(J_L)) \geq [L:K]$ . Mais la seconde inégalité fondamentale (n°6) montre alors qu'on a nécessairement $(J_K : K^* N_{L/K}(J_L)) = [L:K]$ , et par suite $K^* N_{L/K}(J_L)$ est le noyau de $\psi_{L/K}$ . La loi de réciprocité est ainsi complètement démontrée .

Remarque .- La relation $\prod_{P'} \psi_{L/K,P'}(x)=1$ pour tout $x \in K^*$ montre que si $\psi_{L/K,P'}(x)=1$ sauf pour une place $P' \in \Phi$ , on a nécessairement $\psi_{L/K,P'}(x)=1$ pour toute place P' ; autrement dit , x est reste normique pour toutes les places (si en outre L est cyclique , x est alors une norme en vertu du th. de Hasse) .

10 . Le théorème de translation .

PROPOSITION 2 ("théorème de translation") .- Soient K un corps de nombres algébriques , L une extension abélienne de K , E une extension algébrique quelconque de K . On a alors , pour tout idèle $z \in J_E$

(11) $$\psi_{E(L)/E}(z)=\psi_{L/K}(N_{E/K}(z)) .$$

(en identifiant le groupe de E(L) sur E canoniquement avec le groupe de L sur

$L \cap E$) .

En effet , soit P' une place quelconque de K , P une place de E prolongeant P' . Tout revient à démontrer que l'on a

$$\psi_{E(L)/E,P}(z)=\psi_{L/K,P'}(N_{E/K}(z))$$

et comme $E_p$ est une extension algébrique de $K_{P'}$ , cela résulte du th.6 du chap I, § 6 .

COROLLAIRE .- Si L est une extension abélienne de K , E une extension algébrique quelconque de K telle que $K^*N_{E/K}(J_E) \subset K^*N_{L/K}(J_L)$ , on a $L \subset E$ .

En effet , il résulte alors de la formule (11) que l'on a $\psi_{E(L)/E}(z)=1$ pour tout idèle $z \in J_E$ . En vertu de la loi de réciprocité , cela signifie que l'extension abélienne E(L) de E est de degré 1 , donc égale à E , d'où le corollaire .

## § 3 . La théorie du corps de classes global :

## II . Théorèmes d'existence . Applications .

### 1 . Le théorème d'existence des corps de classes .

Nous conservons les notations du § 2 , K désignant donc un corps de nombres algébriques de degré fini sur Q , $J_K$ le groupe des idèles de K . Toutes les extensions algébriques de K que nous considérons sont supposées plongées dans une extension algébriquement close $\Omega_0$ de K , contenant tous les corps locaux de K .

Nous établirons deux lemmes préliminaires en vue de la démonstration du théorème d'existence :

Lemme 1 .- Soit L une extension abélienne de K , et soit H un sous-groupe de $J_K$ contenant le groupe $K^*N_{L/K}(J_L)$ ; il existe alors un corps intermédiaire M et un seul entre K et L tel que $H=K^*N_{M/K}(J_M)$ .

Soit $\Delta = \psi_{L/K}(H)$ , et soit M le corps des invariants de $\Delta$ dans L . Pour tout

idèle $z \in J_K$ , l'automorphisme $\psi_{M/K}(z)$ est la restriction à M de $\psi_{L/K}(z)$ ; la relation $\psi_{M/K}(z)=1$ équivaut donc à $\psi_{L/K}(z) \in A$ , et comme H contient le noyau de $\psi_{L/K}$ , cette dernière relation équivaut à $z \in H$ . Il résulte donc de la loi de réciprocité que $H=K^* N_{M/K}(J_M)$ ; l'unicité du corps M est une conséquence immédiate du corollaire du th. de translation (§ 2, no.2).

Lemme 2 .- Soit H un sous-groupe ouvert de $J_K$ contenant K , et soit Z une extension cyclique de K . Supposons que l'image réciproque $H_1$ de H par l'homomorphisme $z \to N_{Z/K}(z)$ de $J_Z$ dans $J_K$ soit de la forme $Z^* N_{L/Z}(J_L)$ , où L est une extension abélienne de Z . Alors L est une extension abélienne de K , et $K^* N_{L/K}(J_L)$ est contenu dans H .

La seconde assertion du lemme est une conséquence évidente de la première . Il qu'il suffit donc de démontrer . Soit $\theta$ un K-isomorphisme de L dans $\Omega_0$ ; comme Z est extension galoisienne de K , on a $\theta(Z)=Z$ ; d'autre part , si $z \in H_1$ , comme la restriction de $\theta$ à Z est un K-automorphisme de Z , on a $N_{Z/K}(\theta(z))=N_{Z/K}(z) \in H$ , et par suite $\theta(H_1)=H_1$ ; d'où $\theta(L)=L$ (cor. du th. de translation) ; cela montre que L est une extension galoisienne de K . Soit $\sigma$ un K-automorphisme de L dont la restriction à Z est un générateur du groupe de Galois de Z sur K . Soit z un idèle quelconque de $J_Z$ , et posons $\psi_{L/Z}(z)=\tau$ ; on a alors $\psi_{L/Z}(\sigma(z))=\sigma\tau\sigma^{-1}$ (transport de structure) ; mais on a évidemment $N_{Z/K}(\sigma(z))=N_{Z/K}(z)$ , donc $(\sigma(z))z^{-1} \in H_1$ par définition de $H_1$ , ce qui entraîne $\psi_{L/Z}(\sigma(z))=\psi_{L/Z}(z)=\tau$ , d'où $\sigma\tau=\tau\sigma$ . Or , tout K-automorphisme de L est de la forme $\sigma^h\tau$ où $\tau$ est un Z-automorphisme de L ; en vertu de la loi de réciprocité , $\tau$ est de la forme $\psi_{L/Z}(x)$ , donc il résulte de ce qui précède que deux K-automorphismes quelconques de L sont permutables , c'est-à-dire que L est une extension abélienne de K .

THÉORÈME 1 (théorème d'existence des corps de classes) .- Pour tout sous-groupe ouvert H de $J_K$ contenant $K^*$ , il existe une (et une seule) extension abélienne

L de K telle que $\mathfrak{H}=K^*N_{L/K}(J_L)$ .

L'unicité résulte du lemme 1 ; pour démontrer l'existence de L , il suffit , en vertu du lemme 1 , d'établir l'existence d'une extension abélienne E de K telle que $K^*N_{E/K}(J_E)\subset\mathfrak{H}$ . Nous distinguerons plusieurs cas .

1° $J_K/H$ est d'ordre premier n et K contient toutes les racines n-èmes de l'unité . Soit S un ensemble fini de places de K , satisfaisant aux conditions suivantes : S contient les places à l'infini , les diviseurs premiers de n , les places finies P pour lesquelles $U_P\not\subset H$ (qui sont en nombre fini , puisque H est un sous-groupe ouvert de $J_K$) , et enfin on a $J_K=K^*J_K^S$ (§ 1,th.4) . Il résulte aussitôt de ces conditions que l'on a (avec les notations du § 2,n°6) , $J_K^{S,n}\subset H$ ; comme on a aussi par hypothèse $K^*\subset H$ , on a $H_0=K^*J_K^{S,n}\subset H$ . Or , le lemme 4 du § 2,n°6 montre que $H_0=K^*N_{T/K}(J_T)$ , où T est l'extension abélienne de K obtenue par adjonction des racines n-èmes des éléments de $U_K^S$ ; en vertu de la remarque faite au début de la démonstration , le théorème est démontré dans ce cas .

2° $J_K/H$ est d'ordre premier n , mais K ne contient pas nécessairement le corps des racines n-èmes de l'unité . Soit K' le corps obtenu par adjonction à K de toutes les racines n-èmes de l'unité . On sait que $R_n(K)$ est une extension cyclique de K dont le degré sur K divise n-1 ; il en est donc de même de K' . Soit H' l'image réciproque de H dans $J_{K'}$ par l'homomorphisme $s\to N_{K'/K}(s)$ ; comme $J_{K'}/H'$ est isomorphe à $N_{K'/K}(J_{K'})/H$ , c'est un groupe dont l'ordre divise n, et qui par suite ne peut être que d'ordre 1 ou n . En vertu de 1° , il existe donc une extension abélienne E de K' telle que $H'=K'^*N_{E/K'}(J_E)$ ; mais le lemme 2 prouve alors que E est une extension abélienne de K et que l'on a $K^*N_{E/K}(J_E)\subset H$ ; le théorème est donc encore démontré dans ce cas .

3° $J_K/H$ est un groupe cyclique d'ordre $n^k$ , où n est premier . Il suffit alors de raisonner par récurrence sur k , le théorème étant vrai pour k=1 d'après le

2° . Soit $H_1$ le sous-groupe de $J_K$ tel que $H \subset H_1 \subset J_K$ et que $H_1/H$ soit d'ordre n. Comme $J_K/H_1$ est cyclique d'ordre $n^{k-1}$ , il existe une extension cyclique Z de K telle que $H_1 = K^* N_{Z/K}(J_Z)$ ; en outre , si H' est l'image réciproque de H dans $J_Z$ par l'homomorphisme $z \to N_{Z/K}(z)$ , $J_Z/H'$ est isomorphe à $HN_{Z/K}(J_Z)/H$ , qui est contenu dans $H_1/H$ , donc est d'ordre 1 ou n . Il existe donc une extension abélienne E de Z telle que $H' = Z^* N_{E/Z}(J_E)$ ; le lemme 2 montre alors que E est une extension abélienne de K et que l'on a $K^* N_{E/K}(J_E) \subseteq H$ .

4° $J_K/H$ est un groupe abélien fini quelconque . Ce groupe est somme directe de groupes cycliques $H_i/H$ ($1 \leqslant i \leqslant m$) dont chacun a pour ordre une puissance d'un nombre premier ; pour chaque i , soit $H_i'$ le composé des groupes $H_j$ d'indice $j \neq i$ $J_K/H_i'$ est isomorphe à $H_i/H$ , et par suite cyclique et d'ordre une puissance d'un nombre premier . Il existe donc (d'après 3°) pour chaque indice i une extension cyclique $Z_i$ de K telle que $H_i' = K^* N_{Z_i/K}(J_{Z_i})$ . Or , on a $H = \bigcap_i H_i'$ ; d'autre part, si L est le composé des extensions cycliques $Z_i$ , L est une extension abélienne de K et on a $K^* N_{L/K}(J_L) \subset H_i'$ pour tout indice i , d'où $K^* N_{L/K}(J_L) \subset H$ , ce qui achève la démonstration .

On dit que l'extension abélienne L de K telle que $H = K^* N_{L/K}(J_L)$ est le <u>corps de classes</u> correspondant au sous-groupe ouvert H de $J_K$ .

THÉORÈME 2 .- <u>Soit</u> $\Omega$ <u>la clôture abélienne de</u> K <u>dans</u> $\Omega_0$ . <u>L'application qui , à toute extension abélienne</u> $L \subset \Omega$ <u>de degré fini de</u> K , <u>fait correspondre le sous-groupe ouvert</u> $K^* N_{L/K}(J_L)$ <u>de</u> $J_K$ , <u>est une application biunivoque et décroissante de l'ensemble des corps intermédiaires entre</u> K <u>et</u> $\Omega$ , <u>de degré fini sur</u> K , <u>sur l'ensemble des sous-groupes ouverts de</u> $J_K$ , <u>contenant</u> $K^*$ , <u>telle que</u> $[L:K] = (J_K : K^* N_{L/K}(J_L))$ .

Cet énoncé est une conséquence immédiate de la loi de réciprocité , du th. d'existence et du cor. du th. de translation (§ 2, cor. de la prop.2).

COROLLAIRE 1 .- <u>Soient</u> $H_1, H_2$ <u>deux sous-groupes ouverts de</u> $J_K$ <u>contenant</u> $K^*$ , $L_1$ ,

$L_2$ les corps de classes de $H_1, H_2$ respectivement . Alors $L_1 \cap L_2$ est corps de classes de $H_1 H_2$ et $K(L_1 \cup L_2)$ corps de classes de $H_1 \cap H_2$ .

COROLLAIRE 2 .- Soit E une extension algébrique quelconque (de degré fini) de K . Le sous-groupe $H = K^* N_{E/K}(J_E)$ de $J_K$ est ouvert , et le corps de classes L de H est la plus grande extension abélienne de K contenue dans E .

En effet , il n'y a qu'un nombre fini de places de K ramifiées dans E . pour toute place P de K non ramifiée dans E , $K_p(E)$ est une extension non ramifiée de $K_p$ , donc cyclique , et tout élément de $U_p$ est donc norme d'un élément de $K_p(E)^*$ (chap.I,§ 6,prop.1) . Comme d'ailleurs , pour toute place P de K , l'homomorphisme $z \to N_{K_p(E)/K_p}(z)$ est un homomorphisme de $(K_p(E))^*$ sur un sous-groupe ouvert de $K_p^*$ , on voit que $N_{E/K}(J_E)$ est un sous-groupe ouvert de $J_K$ , et il en est de même a fortiori de H . On a alors $L \subset E$ d'après le cor. du th. de translation (§ 2,prop.2) ; en outre , s'il existait une extension abélienne $L' \neq L$ de K , intermédiaire entre L et E , on aurait $H = K^* N_{E/K}(J_E) \subset K^* N_{L'/K}(J_{L'})$ et $K^* N_{L'/K}(J_{L'}) \neq K^* N_{L/K}(J_L)$ en vertu du th.2 , ce qui est absurde .

Avec les notations de ce corollaire , on a donc l'inégalité

$$(1) \qquad (J_K : K^* N_{E/K}(J_E)) \leqslant [E:K]$$

l'égalité n'avant lieu que lorsque E est une extension abélienne de K . En outre lorsque E est une extension galoisienne de K , le cor.2 montre que le groupe $J_K / K^* N_{E/K}(J_E)$ est isomorphe au quotient du groupe de Galois de E sur K par son groupe des commutateurs .

COROLLAIRE 3 .- Soit E une extension algébrique quelconque (de degré fini) de K. Soient H un sous-groupe ouvert de $J_K$ contenant $K^*$ et $H_1$ l'image réciproque de H par l'application $z \to N_{E/K}(z)$ de $J_E$ dans $J_K$ . Si L est le corps de classes du groupe H , le corps de classes du groupe $H_1$ est E(L) .

C'est une conséquence immédiate du th.1 et du th. de translation (§ 2,prop.2).

2 . Décomposition et ramification des idéaux premiers dans un corps de classes .

PROPOSITION 1 .- Soient H un sous-groupe ouvert de $J_K$ contenant $K^*$ , et L le corps de classes de H . Pour toute place P de K , soient $H_1=HU_P$ (si P est finie) $H_2=HK_P^*$ ; le corps de classes correspondant à $H_1$ (resp. $H_2$) est le corps d'inertie (resp. le corps de décomposition) de P dans L . En outre , si $\varpi$ est une uniformisante de $K_P$ , le degré résiduel de toute place de L prolongeant P est égal au plus petit entier f tel que $\varpi^f \in H_1$ .

Comme le noyau de $\psi_{L/K}$ est H , on a $H\cap K_P^*=N_{K_P(L)/K_P}(K_P(L)^*)$ ; par suite , si e est l'indice de ramification de P dans L , on a $(U_P:(U_P\cap H))=e$ (chap.I, § 6, prop.non explicitée) ; pour que P soit non ramifiée dans L , il faut et il suffit donc que $U_P\subset H$ . On en déduit que le corps de classes $L_1$ correspondant à $H_1=HU_P$ est le plus grand sous-corps de L tel que P soit non ramifiée dans $L_1$ , c'est-à-dire le corps d'inertie de P (dans L). On a évidemment $H_1\cap K_P^*=N_{K_P(L_1)/K_P}(K_P(L_1)^*)$ le degré f de $K_P(L_1)$ sur $K_P$ est donc égal à $(K_P^*:(H_1\cap K_P^*))$ (chap.I, § 6, th.3) , et comme $H_1$ contient $U_P$ et que $K_P^*/U_P$ est un groupe cyclique engendré par la classe de $\varpi$ (mod.$U_P$) , on voit que f est le plus petit exposant tel que $\varpi^f\in H_1$ . En particulier , pour que e=f=1 , c'est-à-dire que P soit non ramifié et complètement décomposé dans L , il faut et il suffit que $H=H_1=K_P^*$ . On en déduit que le corps de classes $L_2$ correspondant à $H_2=HK_P^*$ est le plus grand sous-corps de L tel que P soit complètement décomposé dans $L_2$ , c'est-à-dire le corps de décomposition de P dans L , ce qui achève la démonstration .

COROLLAIRE .- Pour toute place finie P de K , $\psi_{L/K,P}(U_P)$ est le groupe d'inertie de P dans L .

3 . Détermination des corps de classes . Rayons .

Soit H un sous-groupe ouvert de $J_K$ contenant $K^*$ , et soit L le corps de classes de H ; on a donc $H=K^*N_{L/K}(J_L)$ , et pour toute place P de K , on a $H\cap K_P^*=$

$=K_P^{*}\cap N_{L/K}(J_L)=N_{K_p(L)/K_p}(K_{\mathfrak{P}}(L)^{*})$ . On a en outre la propriété d'unicité suivante

PROPOSITION 2 .- *Soient $H_1$ et $H_2$ deux sous-groupes ouverts de $J_K$ contenant K ; si on a $H_1\cap K_P^{*}=H_2\cap K_P^{*}$ pour toutes les places de K à l'exception d'un nombre fini d'entre elles , on a $H_1=H_2$ .*

Soit S un ensemble fini de places de K tel que , pour $P\notin S$ , on ait $H_1\cap K_P^{*}=$ $=H_2\cap K_P^{*}$ et $U_p\subset H_1\cap H_2$ . Pour tout $P\in S$ , il existe un sous-groupe ouvert $M_P$ de $K_P^{*}$ tel que $M_p\subset H_1\cap H_2$ ; pour tout idèle z , il existe , en vertu du th. d'approximation , un $x\in K^{*}$ tel que $x_P^{-1}z_P\in M_P$ pour tout $P\in S$ ; soit $T\subset \complement S$ l'ensemble fini des places pour lesquelles $x_P^{-1}z_P\notin U_P$ ; l'idèle $x^{-1}z$ appartient donc au produit $\prod_{P\in S} M_P\times \prod_{P\notin S\cup T} U_P\times \prod_{P\in T} K_P^{*}$ . Soient $L_1,L_2$ les corps de classes de $H_1$ et $H_2$ ; on a , en vertu de l'hypothèse , $K_p(L_1)=K_p(L_2)=K_p(L_1\cup L_2)$ pour toute place $P\notin S$ ; on peut donc , en remplaçant au besoin $L_2$ par $K(L_1\cup L_2)$ , supposer que $L_1\subset L_2$ , donc que $H_2\subset H_1$ . Mais si $z\in H_1$ , on a $\psi_{L_1/K}(z)=\psi_{L_1/K}(x^{-1}z)=$ $=\prod_{P\in T}\psi_{L_1/K,P}(z)^{-1}z)=1$ , et la dernière formule montre qu'on a aussi $\prod_{P\in T}\psi_{L_2/K,P}(x^{-1}z)=1$ , d'où $\psi_{L_2/K}(z)=1$ , $z\in H_2$ ; on a donc bien $H_1=H_2$ .

COROLLAIRE .- *Soient $L_1,L_2$ deux extensions abéliennes de K telles que , pour toutes les places de K à l'exception d'un nombre fini d'entre elles , les degrés locaux de $L_1$ et $L_2$ soient égaux ; alors $L_1=L_2$ .*

En effet , pour toute place $P$, non ramifiée dans $L_1$ ni dans $L_2$ , et où les degrés locaux sont égaux , on a $H_1\cap K_P^{*}=H_2\cap K_P^{*}$ .

Soit H un sous-groupe ouvert de $J_K$ contenant K , et soit S l'ensemble des places infinies et des places finies telles que $U_P\not\subset H$ (ces dernières sont , comme il résulte de la prop.1 , celles qui sont ramifiées dans le corps de classes de H) . Pour tout $P\in S$ , soit $M_p$ un sous-groupe ouvert de $K_P^{*}$ contenu dans $H\cap K_P^{*}$ ; si P est une place à l'infini complexe , on a nécessairement $M_P=K_P^{*}=C^{*}$ ; si P est une place à l'infini réelle , on peut avoir , soit $M_P=R^{*}$, soit $M_P=R_+^{*}$ ; en-

fin , si P est une place finie telle que $U_p \not\subset H$ , on prendra d'ordinaire $M_p \subset U_p \cap H$ . Posons $W = \prod_{P\in S} M_p \times \prod_{P\notin S} K_P^*$ , et $V = \prod_{P\in S} M_p \times \prod_{P\notin S} U_P$ ; on a donc $V \subset H$ . Pour tout idèle $z \in H$ , il existe , en vertu du th. d'approximation , un $x \in K^*$ tel que $x_p^{-1} z_p \in M_p$ pour toute $P \in S$ , autrement dit $x^{-1}z \in W$ , et comme $K^* \subset H$ , $x^{-1}z \in H \cap W$ , ce qui signifie qu'on a $H = K^*(W \cap H)$ ; la donnée du groupe $W \cap H$ détermine donc complètement H .

Le plus souvent , pour les places finies $P \in S$ , on prend pour $M_p$ le plus grand sous-groupe de $U_p$ de la forme $1+P^k$ qui est contenu dans $H \cap U_p$ ; si $1+P^{c(P)}$ est ce sous-groupe (avec $c(P) \geqslant 1$) , le diviseur entier $P^{c(P)}$ est appelé le P-conducteur du groupe H , et leur produit $f_H$ est appelé le conducteur de H (ou du corps de classes L de H , auquel cas on le note $f_{L/K}$). On notera que la donnée du conducteur de H ne détermine pas complètement ce groupe en général , car $H \cap U_p$ n'est pas nécessairement de la forme $1+P^k$ . Avec les notations précédentes , on a évidemment $W \cap H \supset V$ et $W \cap H \supset K^* \cap W$ , donc $W \cap H \supset (K^* \cap W)V$ ; si on a pris $M_p = R_+^*$ pour les places réelles à l'infini , $K^* \cap W$ est formé des éléments $x \in K^*$ tels que $x \equiv 1 \pmod{f_H}$ et tels que x soit $> 0$ dans tous les corps $K_P$ égaux à R (ce qu'on exprime en disant que x est totalement positif) ; le groupe multiplicatif formé par ces éléments est appelé le rayon modulo $f_H$ , et on a évidemment $H \supset K^*V = K^*(K^* \cap W)V$ ; on dit que le corps de classes du groupe $K^*V$ correspond au rayon $K^* \cap W$ . Inversement , pour tout diviseur entier $m = \prod_P P^{m(P)}$ , le rayon modulo m peut se mettre sous la forme $W \cap K^*$ , avec $M_p = R_+^*$ pour les places réelles à l'infini , et $M_p = 1+P^{m(P)}$ pour les places finies divisant m ; le corps de classes correspondant est associé au groupe d'idèles $K^*V$ . On voit ainsi que tout corps de classes est contenu dans le corps de classes d'un rayon .

On notera que le conducteur du groupe d'idèles $K^*V$ correspondant à m est un diviseur de m , mais ne lui est pas nécessairement égal , car il peut se faire que $M_p$ soit égal à $U_p$ même pour $m(P) > 0$ : c'est ce qui se passe

Samuel

(171)





par exemple pour $K=Q$ , $m=(2)=P$ et $m(P)=1$ .

Le groupe de Galois du corps de classes du rayon $K^*\cap W$ est isomorphe à $J_K/K^*V$ ; en vertu du th. d'approximation , on a $J_K=K^*W$ , donc $J_K/K^*V=K^*W/K^*V$ ; comme V est un sous-groupe ouvert de W , le dernier groupe quotient est aussi isomorphe à $W/(W\cap K^*V)=W/(K^*\cap W)V$ , et finalement à $(W/V)/((K^*\cap W)V/V)$ . Or , le groupe W/V est isomorphe au groupe $A_m$ des diviseurs étrangers au module m du rayon $K^*\cap W$ : en effet , pour tout idèle $z=(z_p)\in W$ , on a $v_p(z_p)=0$ pour tout diviseur premier P|m ; inversement , si z est tel que $v_p(z_p)=0$ pour P|m , il existe un idèle u dont toutes les composantes (pour les places finies) sont des unités p-adiques, tel que $uz\in W$ , d'où $a_z=a_{zu}$ ; cela prouve l'isomorphie de W/V et de $A_m$ , puisque le quotient de deux idèles de W appartenant à la même classe mod.V est un idèle dont toutes les composantes (pour les places finies) sont des unités p-adiques, et réciproquement . On voit de même que $(K^*\cap W)V/V$ est isomorphe au sous-groupe $H_m$ de $A_m$ formé des idéaux principaux (x) engendrés par les éléments x du rayon modulo m . Finalement , nous avons montré que le groupe $J_K/K^*V$ est isomorphe au groupe quotient $A_m/H_m$ .

PROPOSITION 3 .- Pour tout diviseur premier P de K ne divisant pas m , le degré résiduel de tout diviseur premier de P dans le corps de classes du rayon mod.m est le plus petit entier f tel que $P^f$ appartienne à $H_m$ .

Cela résulte aussitôt de la prop.1 , si on remarque que dans l'isomorphie entre W/V et $A_m$ , la classe mod.V d'une uniformisante $\varpi$ de $K_p$ correspond au diviseur premier P .

Un cas particulier important est celui où on prend $m=(1)$ , ce qui signifie que S est réduit aux places à l'infini . Il est clair alors que $A_m$ est identique au groupe D de tous les diviseurs . D'autre part , le groupe $H_m=H_1$ est alors le sous-groupe du groupe $D_0$ de tous les diviseurs principaux , formé des idéaux principaux engendrés par les éléments totalement positifs de $K^*$ . Le corps de

classes correspondant au ravon modulo 1 est appelé le corps de classes absolu M de K : c'est la plus grande extension abélienne dans laquelle tout diviseur premier de K est non ramifié (ou encore la plus grande extension abélienne de discriminant (1) par rapport à K) ; son degré est égal à l'ordre $h_1$ du groupe $D/H_1$. On peut encore dire que c'est le corps de classes correspondant au groupe d'idèles $K^*J'_\infty$ , où $J'_\infty$ est le sous-groupe de $J_\infty$ formé des idèles dont la composante d'indice P est dans $U_p$ pour toute place finie P , et $>0$ pour toute place à l'infini réelle . Le corps de classes correspondant au groupe d'idèles $K^*J_\infty$ est un sous-corps $M_0$ de M , dont le groupe sur K est isomorphe au groupe $D/D_0$ des classes d'idéaux de K , et dont le degré sur K est en particulier égal au nombre h de ces classes ; on l'appelle le corps de classes absolu restreint .

A tout élément $x \in K^*$ , faisons correspondre l'élément $\eta(x)$ du groupe multiplicatif $\Sigma = (\{-1,+1\})^{r_1}$ formé de la suite des signes de x dans les corps locaux $K_p$ égaux à R , rangés dans un certain ordre (signature de x) ; en vertu du th. d'approximation , $\eta$ est un homomorphisme de K sur $\Sigma$ . L'image par cet homomorphisme du groupe U des unités de K est un sous-groupe $\Sigma_0$ de $\Sigma$ ; il est clair que le groupe $D/D_0$ est isomorphe à $\Sigma/\Sigma_0$ . On en conclut que le groupe de M par rapport à $M_0$ est isomorphe à $\Sigma/\Sigma_0$ : c'est donc un groupe dont l'ordre est de la forme $2^\nu$ , et qui est produit direct de groupes cycliques d'ordre 2 .

4 . Applications : I . Extensions abéliennes de Q .

THÉORÈME 3 (Kronecker-Weber) .- Toute extension abélienne de Q de degré fini est un corps circulaire .

(En d'autres termes , l'extension abélienne maximale de Q est le corps engendré par toutes les racines de l'unité sur Q).

D'après les résultats du n°3 , il suffit deprouver que , pour tout entier m , le corps de classes $K_m$ du rayon modulo m est un corps circulaire . Nous allons montrer qu'en fait $K_m = R_m(Q)$ ; d'après le cor. de la prop.2 , il suffit pour cela

de prouver que pour tout nombre premier p non diviseur de m (et par suite non ramifié dans $K_m$ ni dans $R_m(K)$) , les degrés locaux de $K_m$ et de $R_m(Q)$ pour la place p sont égaux . Or , pour $R_m(Q)$ , ce degré local est le plus petit nombre f tel que $p^f \equiv 1 \pmod{m}$ (§ 1,prop.6) ; il résulte aussitôt de la prop.3 que f est aussi le degré local de $K_m$ en p , ce qui démontre le théorème .

On se gardera de croire que le théorème s'étende à un corps de nombres algébriques quelconque (cf. "rêve de jeunesse de Kronecker" pour les corps quadratiques imaginaires , avec la théorie de la multiplication complexe (chap.III).

Remarque .- La structure du groupe de Galois G de l'extension abélienne maximale $\Omega_0$ de Q se détermine aisément par la théorie du corps de classes et les résultats du § 1 : en effet , $R \times G$ est isomorphe à $J_Q/Q^*$ , et comme on a $J_Q = Q^* J_\infty$ , $J_Q/Q^*$ est isomorphe à $J_\infty/U$ , où U est le groupe des unités de Q , réduit ici à $\{-1,+1\}$ ; comme d'autre part , $J_\infty = R^* \times \prod_p U_p$ $J_\infty$ est produit direct de U et du groupe $R_+^* \times \prod_p U_p$ ; on en conclut que G est isomorphe au produit $\prod_p U_p$ des groupes des unités p-adiques , p parcourant l'ensemble des nombres premiers .

5 . Applications : II . Lois de réciprocité des restes de puissances .

Soient m un entier $> 0$ , K un corps de nombres algébriques contenant toutes les racines m-èmes de l'unité ; pour tout élément $\alpha \in K$ , considérons le corps L des racines du polynôme $X^m - \alpha$ ; on sait (Alg.,chap.V,§ 11,prop.7) que L est une extension cyclique de K , dont le degré d est le plus petit entier tel que $\alpha^d$ soit puissance m-ème dans K (d est évidemment un diviseur de m) ; on sait en outre que L est engendré par une quelconque des racines de $X^m - \alpha$ ; dans ce qui suit nous désignerons par $\sqrt[m]{\alpha}$ l'une de ces racines , prise arbitrairement ; on a donc $L = K(\sqrt[m]{\alpha})$ ; un tel corps est dit corps kummerien sur K . La différente de $\theta = \sqrt[m]{\alpha}$ étant $m\theta^{m-1}$ , tout diviseur premier de K qui se ramifie dans $K(\sqrt[m]{\alpha})$ est diviseur de m ou de $\alpha$ . En d'autres termes , le discriminant

$d_\alpha$ de L sur K ne contient que des diviseurs premiers facteurs de m ou de $\alpha$, et il en est de même du conducteur $f_\alpha$ (n°3) de L sur K .

On sait que pour tout K-automorphisme $\sigma$ de L , on a $\sigma(\sqrt[m]{\alpha})=\zeta_\sigma \cdot \sqrt[m]{\alpha}$ , où $\zeta_\sigma$ est une racine m-ème de l'unité , et l'application $\sigma \to \zeta_\sigma$ est un isomorphisme du groupe de Galois $\mathcal{L}$ de L sur un groupe de racines m-èmes de l'unité . Pour tout idèle $z \in J_K$ , on pose

(2) $$\psi_{L/K}(z)\sqrt[m]{\alpha}=\left(\frac{\alpha}{z}\right)\sqrt[m]{\alpha} \quad .$$

Soit P un diviseur premier de K non ramifié dans L ; si on identifie une uniformisante $\varpi$ pour P à l'idèle dont la P-composante est $\varpi$ et les autres 1 , l'élément $\left(\frac{\alpha}{\varpi}\right)$ ne dépend que de P , et non de l'uniformisante $\varpi$ considérée ; on note cette racine de l'unité $\left(\frac{\alpha}{P}\right)$ , et on l'appelle le symbole de restes de puissances m-èmes modulo P . Cette terminologie est justifiée par la proposition suivante :

PROPOSITION 4 .- Soit P un diviseur premier de K ne divisant pas m ; l'application $\alpha \to \left(\frac{\alpha}{P}\right)$ , restreinte à l'ensemble des $\alpha \in K^*$ qui sont étrangers à P (c'est-à-dire des unités P-adiques) est un homomorphisme de $K^* \cap U_P$ sur le groupe des racines m-èmes de l'unité , dont le noyau est $K^* \cap (U_p)^m$ .(En d'autres termes , pour que $\left(\frac{\alpha}{P}\right)=1$ lorsque P ne divise pas $\alpha$ , il faut et il suffit que $\alpha$ soit puissance m-ème dans $K_P^*$).

En effet, pour que l'on ait $\left(\frac{\alpha}{P}\right)=1$ , il faut et il suffit que $\psi_{L/K}(\varpi)$ soit l'identité , c'est-à-dire que $K_P(\sqrt[m]{\alpha})=K_P$ , puisque K ⊂ P n'est pas ramifié dans L ; cela signifie évidemment que $\alpha$ est puissance m-ème dans $K_P$ . Pour prouver que $\alpha \to \left(\frac{\alpha}{P}\right)$ est un homomorphisme , c'est-à-dire que

(3) $$\left(\frac{\alpha_1\alpha_2}{P}\right)=\left(\frac{\alpha_1}{P}\right)\left(\frac{\alpha_2}{P}\right) \qquad (\alpha_1 \text{ et } \alpha_2 \text{ dans } K^* \cap U_P)$$

considérons le corps $M=K(\sqrt[m]{\alpha_1},\sqrt[m]{\alpha_2})$ qui est une extension abélienne de K ; $\sigma=\psi_{M/K}(\varpi)$ est l'automorphisme de Frobenius (relatif à P) de ce corps , et induit sur $K(\sqrt[m]{\alpha_1})$ , $K(\sqrt[m]{\alpha_2})$ et $K(\sqrt[m]{\alpha_1\alpha_2})$ les automorphismes de Frobenius correspondan

la formule (3) résulte alors de ce que $\sigma(\sqrt[m]{\alpha_1\alpha_2})=\sigma(\sqrt[m]{\alpha_1})\sigma(\sqrt[m]{\alpha_2})$ . Enfin , comme P ne divise pas m , on sait (chap.I,§ 1,n°7) que $(U_P:(U_P)^n)=m$ ; en vertu du th. d'approximation , pour tout $x\in U_P$ , il existe $\alpha\in K^*$ tel que $\alpha x^{-1}\in (U_P)^m$ , et par suite $(K^*\cap U_P)/(K^*\cap(U_P)^m)$ est aussi d'ordre m , ce qui achève la démonstration .

Comme $K_P$ contient les racines m-èmes de l'unité , il en est de même de son corps résiduel $F_q$ , où $q=N(P)$ ; par suite q-1 est multiple de m , et le groupe $F_q^*/(F_q^*)^m$ est d'ordre m ; on en conclut aussitôt que l'ordre d'un élément $\alpha\in U_P$, modulo $(U_P)^m$ , est égal à l'ordre de son image $\tilde{\alpha}$ dans $F_q^*$ modulo $(F_q^*)^m$ . Soit $\zeta$ une racine primitive (q-1)-ème de l'unité dans K (existence par Hensel); $\zeta^{(q-1)/m}=\zeta_0$ est donc une racine primitive m-ème de l'unité ; pour tout $\alpha\in K^*\cap U_P$ , soit $\tilde{\alpha}=\tilde{\zeta}^a$ $(0\leq a\leq q-1)$ ; l'ordre de $\alpha$ modulo $(U_P)^m$ est le plus petit nombre h tel que $ah\equiv 0 \pmod m$ , autrement dit c'est l'ordre de la racine m-ème de l'unité $\zeta_0^a$ , ce qui prouve que $\left(\frac{\alpha}{P}\right)=\zeta_0^a$ . Comme $\zeta_0^a=\tilde{\alpha}^{(q-1)/m}$ , on peut aussi exprimer ce résultat par la congruence

$$\left(\frac{\alpha}{P}\right)\cdot\alpha^{-(q-1)/m}\equiv 1 \pmod P \tag{4}$$

Pour K=Q et m=2 , le symbole $\left(\frac{\alpha}{P}\right)$ coïncide avec le symbole de Legendre (pour $p\neq 2$) , et les propriétés précédentes généralisent les propriétés du symbole de Legendre vues au § 1,n°7 .

La définition de $\left(\frac{\alpha}{P}\right)$ s'applique aussi au cas où $\alpha$ est divisible par P , mais où $v_P(\alpha)\equiv 0 \pmod m$ ; en effet , dans ce cas , en désignant par $\beta$ un élément de K tel que $v_P(\beta)=v_P(\alpha)/m$ (élément qui existe en vertu du th. d'approximation) , $\alpha\beta^{-m}$ n'est plus divisible par P , donc P n'est pas ramifié dans $K(\sqrt[m]{\alpha\beta^{-m}})=K(\sqrt[m]{\alpha})$ Il est d'ailleurs évident réciproquement que si P n'est pas ramifié dans $K(\sqrt[m]{\alpha})$ on doit avoir $v_P(\alpha)\equiv 0 \pmod m$ , puisque $\alpha$ est une puissance m-ème dans $K(\sqrt[m]{\alpha})$ ; les éléments $\alpha$ ayant cette propriété sont appelés P-primaires . Il est immédiat que la formule (3) est encore valable pour ces éléments P-primaires (P non di-

viseur de m).

Soit A le groupe des diviseurs $b=\prod_P P^{h_P(b)}$ tels que pour tous les diviseurs premiers P d'exposant $h_P(b)\neq 0$, $\alpha$ soit P-primaire ; si on pose $\left(\frac{\alpha}{b}\right)=\prod_P\left(\frac{\alpha}{P}\right)^{h_P(b)}$, il est clair que l'application $b\to\left(\frac{\alpha}{b}\right)$ est un homomorphisme de A dans le groupe des racines m-èmes de l'unité . Si $\varpi_P$ est une uniformisante pour P (identifiée comme ci-dessus à l'idèle de P-composante $\varpi_P$ et dont les autres composantes sont 1) , et si on pose $\overline{b}=\prod_P \varpi_P^{h_P(b)}$ (idèle dont b est le diviseur associé) , il résulte de (2) que l'on a

$$(5)\qquad \psi_{L/K}(\overline{b})(\sqrt[m]{\alpha})=\left(\frac{\alpha}{b}\right)\sqrt[m]{\alpha}$$

et la loi de réciprocité d'Artin entraîne donc la proposition suivante :

PROPOSITION 5 (première forme de la loi de réciprocité des restes de puissances m-èmes) .- Le noyau de l'homomorphisme $b\to\left(\frac{\alpha}{b}\right)$ est formé des diviseurs b tels que l'idèle $\overline{b}$ appartienne au groupe $K^*N_{L/K}(J_L)$ .

COROLLAIRE .- Pour tout élément $\beta$ appartenant au rayon modulo $f_\alpha$ , on a $\left(\frac{\alpha}{\beta}\right)=1$ (on écrit $\left(\frac{\alpha}{\beta}\right)$ au lieu de $\left(\frac{\alpha}{(\beta)}\right)$ ).

En effet , on sait que le diviseur principal $(\beta)$ est alors dans le groupe A et que l'idèle $\overline{b}$ correspondant est dans $K^*N_{L/K}(J_L)$ (n°3).

Pour tout élément $\beta\in K^*$ , et toute place (finie ou infinie) P de K , on pose

$$(6)\qquad \psi_{L/K,P}(\beta)\left(\sqrt[m]{\alpha}\right)=\left(\frac{\beta,\alpha}{P}\right)\sqrt[m]{\alpha}$$

et la racine m-ème de l'unité $\left(\frac{\beta,\alpha}{P}\right)$ est appelée le symbole normique de Hilbert

On sait que la loi de réciprocité (pour l'extension $L=K(\sqrt[m]{\alpha})$) est équivalente à la formule du produit

$$(7)\qquad \prod_{P\in\phi}\left(\frac{\beta,\alpha}{P}\right)=1 .$$

La relation $\left(\frac{\beta,\alpha}{P}\right)=1$ signifie donc que $\beta$ , considéré comme élément de $K_P$ , est norme d'un élément de $K_P(\sqrt[m]{\alpha})$.

Lorsque P est un diviseur premier ne divisant pas $f_\alpha$ , il résulte des formules

(2) et (6) que l'on a

(8) $$\left(\frac{\beta,\alpha}{P}\right)=\left(\frac{\alpha}{P}\right)^{v_P(\beta)}$$

Par définition de $\psi_{L/K,P}$, on a

(9) $$\left(\frac{\beta_1\beta_2,\alpha}{P}\right)=\left(\frac{\beta_1,\alpha}{P}\right)\left(\frac{\beta_2,\alpha}{P}\right)$$

quels que soient $\beta_1,\beta_2$ dans $K^*$ ; on a en outre la formule

(10) $$\left(\frac{\beta,\alpha_1\alpha_2}{P}\right)=\left(\frac{\beta,\alpha_1}{P}\right)\left(\frac{\beta,\alpha_2}{P}\right)$$

quels que soient $\alpha_1$ et $\alpha_2$ dans $K^*$ ; la démonstration est analogue à celle de la formule (3), en utilisant la prop.8 du chap.I, § 6 ("transitivité des homomorphismes principaux"). Nous allons en déduire la propriété suivante :

PROPOSITION 6 .- Quels que soient $\alpha$ et $\beta$ dans $K^*$, on a, pour toute place P de K

(11) $$\left(\frac{\beta,\alpha}{P}\right)=\left(\frac{\alpha,\beta}{P}\right)^{-1}$$

(formule d'échange).

Remarquons pour cela que, pour tout $\mu\in K^*$, on a

(12) $$\left(\frac{-\mu,\mu}{P}\right)=1 .$$

En effet, il suffit deprouver que $-\mu$ est norme d'un élément de $K(\sqrt[m]{\mu})$ ; si r est le plus petit entier tel que $\mu^r$ soit puissance m-ème dans K, et si m=dr, on a $\mu=\mu_0^d$ (Alg., chap.V, § 11, prop.7) et $K(\sqrt[m]{\mu})=K(\sqrt[r]{\mu_0})$. Or, si $\omega$ est une racine primitive r-ème de l'unité, la norme de $-\sqrt[r]{\mu_0}$ est $(-1)^r\omega^{r(r-1)/2}\mu_0$ ; pour r impair, ce nombre est égal à $-\mu_0$, et il en est de même pour r pair, car si $r=2r'$, $\omega^{r(r-1)/2}=\omega^{r'}=-1$ ; si alors d est impair, la norme de $(-\sqrt[r]{\mu_0})^d$ est $(-\mu_0)^d=-\mu$ ; si au contraire d est pair, -1 est puissance r-ème dans K, car d(m-1)/2 est entier, et en désignant par $\zeta$ une racine primitive m-ème de l'unité, on a $(\zeta^{d(m-1)/2})^r=\zeta^{m(m-1)/2}=-1$ puisque m est pair. On a donc dans tous les cas la formule (12). On peut alors écrire, d'après (9), (10) et (12)

$$\left(\frac{\beta,\alpha}{P}\right)=\left(\frac{\beta,\alpha}{P}\right)\left(\frac{\beta,-\beta}{P}\right)^{-1}=\left(\frac{\beta,\alpha}{P}\right)\left(\frac{\beta,-\beta^{-1}}{P}\right)=\left(\frac{\beta,-\alpha\beta^{-1}}{P}\right)=\left(\frac{\alpha\beta^{-1},-\alpha\beta^{-1}}{P}\right)\left(\frac{\beta,-\alpha\beta^{-1}}{P}\right)=\left(\frac{\alpha,-\alpha\beta^{-1}}{P}\right)=$$
$$=\left(\frac{\alpha,-\alpha}{P}\right)\left(\frac{\alpha,\beta^{-1}}{P}\right)=\left(\frac{\alpha,\beta}{P}\right)^{-1} .$$

PROPOSITION 7 (seconde forme de la loi de réciprocité des restes de puissances m-èmes) .- Soient $\alpha$ et $\beta$ deux éléments de $K^*$, $f_\alpha$ et $f_\beta$ les conducteurs de $K(\sqrt[m]{\alpha})$ et $K(\sqrt[m]{\beta})$ . On pose $(\alpha)=aa_\beta$ (resp. $(\beta)=bb_\alpha$) , où $a_\beta$ (resp. $b_\alpha$) ne contient que des diviseurs premiers de $f_\beta$ (resp. $f_\alpha$) , et où tout diviseur premier de $f_\beta$ (resp. $f_\alpha$) figure dans a (resp. b) avec un exposant multiple de m . Dans ces conditions , on a

$$\left(\frac{\beta}{a}\right)\left(\frac{\alpha}{b}\right)^{-1} = \prod_{\mathfrak{P}\in\Phi_{\alpha\beta}} \left(\frac{\beta,\alpha}{\mathfrak{P}}\right) \tag{13}$$

en désignant par $\Phi_{\alpha\beta}$ l'ensemble des places à l'infini et des places finies divisant le pgcd de $f_\alpha$ et $f_\beta$ .

En effet , d'après la formule du produit (7) , la relation (13) est équivalente à

$$\left(\frac{\alpha}{b}\right)\left(\frac{\beta}{a}\right)^{-1} = \prod_{\mathfrak{P}\notin\Phi_{\alpha\beta}} \left(\frac{\beta,\alpha}{\mathfrak{P}}\right) \tag{14}$$

Or , par définition , $\beta$ est P-primaire pour tout diviseur premier P de a , et si $a=\prod_P P^{h_P(a)}$ , on a $\left(\frac{\beta}{a}\right)=\prod_P \left(\frac{\beta}{P}\right)^{h_P(a)}$ ; de même , $\alpha$ est P-primaire pour tout diviseur premier P de b , et si $b=\prod_P P^{h_P(b)}$ , $\left(\frac{\alpha}{b}\right)=\prod_P \left(\frac{\alpha}{P}\right)^{h_P(b)}$ . Cela étant , si P divise le pgcd de $f_\alpha$ et $f_\beta$ , on a $h_P(a)\equiv 0 \pmod m$ et $h_P(b)\equiv 0 \pmod m$ ; dans le cas contraire , ou bien P ne divise pas $f_\alpha$ , et alors $\alpha$ est P-primaire , donc (tenant compte de la définition de a) , $h_P(a)\equiv 0 \pmod m$ ; d'autre part , $h_P(b)=$ $=v_P(\beta)$ , donc , en vertu de la formule (8)

$$\left(\frac{\alpha}{\mathfrak{P}}\right)^{h_\mathfrak{P}(b)}\left(\frac{\beta}{\mathfrak{P}}\right)^{-h_\mathfrak{P}(a)} = \left(\frac{\beta,\alpha}{\mathfrak{P}}\right)$$

On vérifie de même cette formule lorsque P ne divise par $f_\beta$ , en tenant compte de la formule d'échange (11) ; d'où la formule (14) .

COROLLAIRE .- Lorsque $\alpha$ , $\beta$ et m sont deux à deux étrangers , on a

$$\left(\frac{\beta}{\alpha}\right)\left(\frac{\alpha}{\beta}\right)^{-1} = \prod_{\mathfrak{P}\in\Phi_m} \left(\frac{\beta,\alpha}{\mathfrak{P}}\right) \tag{15}$$

où $\Phi_m$ est l'ensemble des places à l'infini et des diviseurs premiers de m .

En effet , $f_\alpha$ et $f_\beta$ ont alors uniquement comme diviseurs premiers communs des

diviseurs de m ; avec les notations de la prop.7 , on a donc a=($\alpha$) et b=($\beta$) . Reste à montrer que , dans le second membre de (13) , on peut remplacer $\Phi_{\alpha\beta}$ par $\Phi_m$ , c'est-à-dire que si un diviseur premier P de m ne divise pas le pgcd de $f_\alpha$ et $f_\beta$ , on a $\left(\frac{\beta,\alpha}{P}\right)=1$ . En effet , supposons par exemple que P ne divise pas $f_\alpha$ ; comme P ne divise pas $\beta$ , on a $v_P(\beta)=0$ , et la formule (8), qui est applicable , donne bien $\left(\frac{\beta,\alpha}{P}\right)=1$ . On raisonne de même lorsque P ne divise pas $f_\beta$ , en utilisant la formule d'échange (11) .

Lorsque K=Q et m=2 , et que $\alpha$ et $\beta$ sont deux nombres premiers distincts de 2 , la formule (15) se réduit à

$$\left(\frac{\beta}{\alpha}\right)\left(\frac{\alpha}{\beta}\right)^{-1}=\left(\frac{\beta,\alpha}{2}\right)$$

et on a $\left(\frac{\beta,\alpha}{2}\right)=\pm 1$ suivant que l'équation $\beta=x^2-\alpha y^2$ a ou non des solutions dans $Q_2$ ; il est facile de retrouver ainsi la loi de réciprocité quadratique (pour deux nombres premiers impairs) .

Le calcul explicite du second membre de (15) n'a été fait que pour des corps particuliers (Artin , Hasse , Shafarevitch) ; faut-il en donner des exemples en dehors de la loi de réciprocité quadratique ?

6 . Le théorème de Grünwald-Wang .

Soit K un corps de nombres algébriques , P un diviseur premier de K . Pour tout entier n , on sait qu'il existe des extensions cycliques de $K_P$ , de degré n (entre autres une extension cyclique non ramifiée , d'ailleurs unique en son genre; cf. chap.I, § 1,n°3) . Proposons-nous de chercher s'il existe de même des extensions cycliques de K de degré donné , que nous chercherons en outre à assujettir à un nombre fini de conditions supplémentaires relatives à certains diviseurs premiers de K .

Nous démontrerons plusieurs lemmes préliminaires . Le premier généralise le résultat de la prop.1 du § 2 :

Lemme 3 .- Soient $E_i$ ($1\leq i\leq r$) des extensions cycliques de K , dont les degrés sont des puissances d'un même nombre premier $\ell$ , et telles que pour tout i , $E_i$ soit

linéairement disjoint du corps engendré par les $E_j$ d'indice $\neq i$ . Alors , pour tout $k \leq r$ , il existe une infinité de diviseurs premiers de K qui restent premiers dans $E_1, E_2, \ldots, E_k$ et sont complètement décomposés dans $E_{k+1}, \ldots, E_r$ .

Montrons d'abord que , si L est le corps composé des $E_i$ , il existe une extension cyclique Z de K , de degré $\ell$ , linéairement disjointe de L . En effet ,il existe une infinité de nombres premiers distincts $q_n$ tels que $q_n$ divise $2^{\ell^n}-1$ (démonstration du lemme 6 du § 2) ; comme la période de 2 mod. $q_n$ divise $q_n-1$ , $\ell$ divise $q_n-1$ , et par suite le corps $R_{q_n}(Q)$ contient une extension cyclique de degré $\ell$ de Q ; cela prouve qu'il existe une infinité d'extensions cycliques de Q de degré $\ell$ (les corps $R_{q_n}(Q)$ étant linéairement disjoints) , donc il y en a une $Z_0$ non contenue dans L , telle par suite que $Z_0 \cap L = Q$ ; le corps $Z = K(Z_0)$ répond à la question . Soit $M = L(Z)$ , extension abélienne de K , dont le degré est une puissance de $\ell$ .

Soit $\sigma$ un K-automorphisme de L ; nous allons voir qu'il existe un entier m premier à $\ell$ pour lequel il y a une infinité de diviseurs premiers P de K non ramifiés dans L et tels que l'automorphisme de Frobenius $\sigma_P$ correspondant soit égal à $\sigma^m$ . Pour démontrer le lemme , il suffira de prendre $\sigma = \sigma_1 \sigma_2 \ldots \sigma_k$ , en désignant par $\sigma_i$ un automorphisme engendrant le groupe de Galois de $E_i$ sur K (prolongé canoniquement à L) .

Soit $\tau$ un automorphisme engendrant le groupe de Galois de Z sur K , et considérons le sous-corps F de M invariant par l'automorphisme $\sigma\tau$ ($\sigma$ et $\tau$ étant prolongés canoniquement à M) ; M est cyclique sur F , et son degré sur F est une puissance de $\ell$ ; il existe donc une infinité de diviseurs premiers de F qui restent premiers dans M (§ 2.prop.1). Par suite , il y a un entier c premier à $\ell$ tel que pour une infinité de diviseurs premiers $\mathfrak{P}$ de F , l'automorphisme de Frobenius $\rho_{\mathfrak{P}}$ de M correspondant à $\mathfrak{P}$ soit $(\sigma\tau)^c = \sigma^c \tau^c$ . Pour chacun de ces divi-

seurs $\overline{P}$ , soit P le diviseur premier de K multiple de $\overline{P}$ . Parmi les diviseurs premiers $\overline{P}$ précédents , il en existe une infinité pour lesquels P est non ramifié dans M , et pour lesquels le degré résiduel f de $\overline{P}$ sur P a une même valeur. Pour un tel diviseur $\overline{P}$ , l'automorphisme de Frobenius $\rho_P$ de M correspondant à P est tel que $\rho_{\overline{P}}=\rho_P^f$ . Comme $\tau^c\neq 1$ , il résulte d'abord de là que f est premier à $\ell$ ; comme $[M:K]$ est une puissance de $\ell$ , il existe un entier d tel que $df\equiv 1 \pmod{[M:K]}$ ; d'où $\rho_P^{df}=\rho_P=\sigma^{cd}\tau^{cd}$ et comme l'automorphisme de Frobenius $\sigma_P$ de L correspondant à P est la restriction de $\rho_P$ à L , on a $\sigma_P=\sigma^{cd}$ , avec cd=m premier à $\ell$, ce qui démontre le lemme.

Dans ce qui suit , $\ell$ désignera un nombre premier <u>impair</u> , r un entier $\geqslant 0$ , s un entier $\geqslant 1$, $\zeta_s$ une racine primitive $\ell^s$-ème de l'unité ; comme $Q(\zeta_s)$ est une extension <u>cyclique</u> de Q , de degré $\varphi(\ell^s)=\ell^{s-1}(\ell-1)$ (§ 1,prop.5 et Alg.,chap.VII § 2,n°4) , $K(\zeta_s)$ est une extension cyclique de K . Soient E une extension cyclique de K , de degré une puissance de $\ell$ , linéairement disjointe de $K(\zeta_s)$ par rapport à K ; soit Z une extension cyclique de K quelconque , de degré $\ell^r$ . Soit $H=K^*N_{Z/K}(J_Z)$ le groupe d'idèles de K dont Z est corps de classes , et soit $H_P=N_{N_P(Z)/K_P}(K_P(Z)^*)$ l'intersection de H et de $K_P^*$ pour toute place P de K . Nous allons démontrer le lemme suivant :

<u>Lemme 4 .- Soient</u> S <u>un ensemble fini de places de</u> K , <u>contenant toutes les places à l'infini et toutes les places finies ramifiées dans</u> Z . <u>Il existe alors un ensemble fini</u> T <u>de diviseurs premiers de</u> K <u>n'appartenant pas à</u> S , <u>restant premiers dans</u> E , <u>et ayant la propriété suivante : si</u> $V^{S\cup T}$ <u>désigne le groupe des idèles</u> $z\in J_K$ <u>dont la</u> P-<u>composante est égale à 1 pour</u> $P\in S\cup T$ , <u>et une unité</u> P-<u>adique pour</u> $P\notin S\cup T$ , <u>alors , pour tout entier</u> $\nu$ <u>tel que</u> $1\leqslant\nu\leqslant s$ , <u>l'intersection de</u> $\prod_{P\in S} H_P$ <u>et de</u> $K^*H^{\ell^\nu}V^{S\cup T}$ <u>soit égale à</u> $\prod_{P\in S} H_P^{\ell^\nu}$ .

Soit $F=K(\zeta_s)$ , et soit S' un ensemble fini de places de F , contenant toutes les places prolongeant les places de S , ainsi que les diviseurs premiers de

$\ell$ dans F ; soit L l'extension abélienne de F engendrée par les racines $\ell$-èmes de toutes les S'-unités de F ; on sait que toute extension cyclique de F , de degré $\ell$ , dans laquelle les places $\overline{P} \notin S'$ ne sont pas ramifiées , est contenue dans L (§ 2,cor. du lemme 4) ; nous désignerons par $L_k$ ($1 \leqslant k \leqslant m$) les extensions cycliques de degré $\ell$ de F contenues dans L (et qui sont en nombre fini) . Pour chacun des corps $L_k$ , ou bien $L_k \subset E(\zeta_s)$ , ou bien $L_k$ et $E(\zeta_s)$ sont linéairement disjoints . Dans les deux cas , il résulte du lemme 3 qu'il existe un diviseur premier $\overline{P}_k$ de F , non contenu dans S' , et qui reste premier dans $L_k$ et dans $E(\zeta_s)$ ; nous désignerons par $P_k$ le diviseur premier de K multiple de $\overline{P}_k$ ; puisque $\overline{P}_k$ reste premier dans $E(\zeta_s)$ , $P_k$ reste premier dans E (l'intersection de $E(\zeta_s)$ et de $E_{\overline{P}_k}$ étant réduite à F , l'intersection de E et de $K_{P_k}$ est contenue dans $E \cap F = K$ , donc identique à K).

Soit alors z un idèle de $\prod_{P \in S} H_P$ appartenant à $K^* H^{\ell^\nu} V^{S \cup T}$ , en désignant par T un ensemble fini quelconque de places contenant les $P_k$ . On a donc $z = \alpha u^{\ell^\nu} v$ , où $\alpha \in K^*$, $u \in H$ et $v \in V^{S \cup T}$ ; nous allons montrer que $\alpha$ est une puissance $\ell^\nu$-ème dans $F = K(\zeta_s)$ . Dans le cas contraire , $F(\sqrt[\ell^\nu]{\alpha})$ serait une extension cyclique de F , de degré une puissance de $\ell$ , et distincte de F . Or , par définition de $\alpha$ , pour tout $P \notin S$ , $v_P(\alpha)$ est un multiple de $\ell^\nu$, et comme P ne divise pas $\ell$ , P n'est pas ramifié dans $F(\sqrt[\ell^\nu]{\alpha})$ . D'après la définition de L , il existe donc un des corps $L_k$ contenu dans $F(\sqrt[\ell^\nu]{\alpha})$ ; mais par définition de $\alpha$ , $\alpha$ est une puissance $\ell^\nu$-ème dans $K_{P_k}$ , donc a fortiori dans $F_{\overline{P}_k}$ ; cela signifie que $\overline{P}_k$ est complètement décomposé dans $F(\sqrt[\ell^\nu]{\alpha})$ , et a fortiori dans $L_k$ , contrairement au choix de $\overline{P}_k$ .

Remarquons maintenant que $F = K(\zeta_s)$ est une extension cyclique de K , dont le degré divise $\varphi(\ell^s) = \ell^{s-1}(\ell-1)$ ; F est donc composé de deux extensions cycliques linéairement disjointes $W_1, W_2$ de K , telles que $[W_1 : K]$ divise $\ell-1$ , et que $[W_2 : K]$ soit une puissance de $\ell$ (éventuellement réduite à l'unité) . En vertu du lemme 3

il existe un diviseur premier $P_o$ de K , distinct des $P_k$ et n'appartenant pas à S , qui reste premier dans $W_2$ et dans E . Nous allons voir que si T contient $P_o$ $\alpha$ est une puissance $\ell^\nu$-ème dans K . En effet , $\alpha$ est par définition une puissance $\ell^\nu$-ème dans $K_{P_o}$ ; soit $\theta \in K_{P_o}$ tel que $\theta^{\ell^\nu}=\alpha$ , et soit $f(X)=X^n+\ldots+a_n$ le polynôme minimal de $\theta$ sur K ; on a évidemment $K(\theta) \subset K(\zeta_s)$ d'après ce qui a été vu plus haut . Montrons en outre que $n<\ell$ . Ceci est évident si $W_2=K$ . Dans le cas contraire , la relation $n \geqslant \ell$ entraîne que $[K(\theta):K]$ , qui divise $[P:K]$ , est divisible par $\ell$ , donc que $K(\theta) \cap W_2$ n'est pas réduit à K . Mais par définition de $P_o$, $P_o$ se décompose complètement dans $K(\theta)$ , et a fortiori dans $K(\theta) \cap W_2$ , ce qui contredit l'hypothèse que $P_o$ reste premier dans $W_2$ . On a donc bien $n<\ell$ . Nous allons en déduire que K contient une racine $\ell^\nu$-ème de $\alpha$ . En effet , on a $a_n=\eta\theta^n$ , $\eta$ étant une racine $\ell^\nu$-ème de l'unité . Comme $n<\ell$ , n et $\ell$ sont étrangers , donc il existe deux entiers u,v tels que $un+v\ell^\nu=1$ , et K contient le nombre $a_n^u \alpha^v=\eta^u\theta^{un+v\ell^\nu}=\eta^u\theta$ , ce qui démontre notre assertion .

La relation $z=\alpha u^{\ell^\nu} v$ montre alors que les P-composantes de z sont des puissances $\ell^\nu$-èmes pour tout $P \in S \cup T$ ; on peut donc écrire $z=u'^{\ell^\nu} v'$ , où $v' \in V^{S \cup T}$ ; mais pour $P \notin S$ , cette relation implique que la P-composante de u' est une unité , donc dans $H_p$ , puisque P n'est pas ramifié dans Z ; on a donc $u' \in H$ , ce qui montre bien que , pour $P \in S$ , la P-composante de z appartient à $H_P^{\ell^\nu}$ .

Nous utiliserons encore le résultat suivant de théorie des groupes abéliens : ~~XXXXXXX~~ (cf. Alg., chap. VII, § 2, exerc. 7c)) :

Lemme 5 .- Soit G un groupe abélien fini dont tout élément est d'ordre $\ell^s$ . Soit H un sous-groupe de G tel que pour $1 \leqslant \nu \leqslant s$ , on ait $H \cap G^{\ell^\nu}=H^{\ell^\nu}$ ; alors il existe un sous-groupe $H_1$ de G tel que G soit produit direct de H et $H_1$ .

En effet , G/H est produit direct de groupes cycliques $G_i$ $(1 \leqslant i \leqslant m)$ d'ordre une puissance de $\ell$ ; soit $\bar{a}_i$ un élément engendrant $G_i$ , et $a_i$ un élément de la classe $\bar{a}_i$ mod. H . Si $\ell^h$ est l'ordre de $\bar{a}_i$ , on a $a_i^{\ell^h} \in H$ , donc il existe par hypo-

thèse $b_i \in H$ tel que $a_i^{\ell^h} = b_i^{\ell^h}$ , autrement dit $a_i' = a_i b_i^{-1}$ est d'ordre $\ell^h$ . On en déduit aussitôt que le sous-groupe $H_1$ engendré par les $a_i'$ est supplémentaire de H.

Avec les notations précédentes , proposons-nous de chercher à quelle condition il existe une extension cyclique L de K , de degré $\ell^{r+s}$ , et contenant l'extension donnée Z de degré $\ell^r$ . Pour toute place P de K , l'homomorphisme canonique $\psi_{Z/K,P}$ de $K_P$ dans le groupe de Galois de Z par rapport à K , doit être composé de l'homomorphisme canonique du groupe de Galois de L sur celui de Z , et de l'homomorphisme canonique $\psi_{L/K,P}$ . Soient $\ell^{r(P)}$ et $\ell^{r(P)+s(P)}$ les degrés locaux de Z et L en P ; la relation $r(P) > 0$ signifie que le corps de décomposition $Z \cap K_P$ de P dans Z est distinct de Z ; comme L est cyclique sur K , $L \cap K_P$ contient Z ou est contenu dans Z , et l'hypothèse que $Z \cap K_P$ est distinct de Z entraîne que $L \cap K_P$ est contenu dans Z et identique à $Z \cap K_P$ ; par suite , le degré de L sur $L \cap K_P$ est égal à $\ell^{r(P)+s}$ , autrement dit $s(P)=s$ . Si au contraire $r(P)=0$, on a seulement l'inégalité $s(P) \leqq s$ .

Nous allons nous donner un groupe cyclique $\Gamma$ d'ordre $\ell^{r+s}$ , $\sigma$ étant un générateur de ce groupe . Soit $L_P$ une extension cyclique de $K_P$ , contenant $K_P(Z)$ , et de degré $\ell^{r(P)+s(P)}$ sur $K_P$ . Soit $\Delta$ le sous-groupe de $\Gamma$ , d'ordre $\ell^s$ , engendré par $\sigma^{\ell^r}$ , et soit $\omega$ un isomorphisme du groupe de Galois G de Z sur K , sur le groupe ~~XXXXXXXX~~ quotient $\Gamma/\Delta$ . Soit $G_P$ le groupe de $L_P$ sur $K_P$ , cyclique d'ordre $\ell^{r(P)+s(P)}$ , et soit $\rho_P$ l'homomorphisme canonique de $G_P$ sur le groupe $H_P$ de $K_P(Z)$ sur ~~XX~~ $K_P$ , d'ordre $\ell^{r(P)}$ ; $H_P$ est canoniquement identifié à un sous-groupe de G , donc il lui correspond par $\omega$ un sous-groupe $\Gamma_P/\Delta$ de $\Gamma/\Delta$ , où $\Gamma_P$ est le sous-groupe de $\Gamma$ d'ordre $\ell^{r(P)+s}$ . Supposons d'abord $r(P) > 0$ et $s(P)=s$ ; alors il est immédiat qu'il existe un isomorphisme $\omega_P$ de $G_P$ sur $\Gamma_P$ tel que $\omega \circ \rho_P = \rho_P' \circ \omega_P$ , où $\rho_P'$ est l'homomorphisme canonique de $\Gamma_P$ sur $\Gamma_P/\Delta$ . Lorsque $r(P)=0$ , $s(P) \leqq s$ , $\Gamma_P/\Delta$ et $H_P$ sont réduits à l'élément neutre , et il existe encore un isomorphisme $\omega_P$ de $G_P$ sur un sous-groupe de $\Gamma_P = \Delta$ tel que $\omega \circ \rho_P =$

$=\rho'_P \circ \omega_P$ . Cela étant , l'homomorphisme canonique $\psi_{Z/K,P}$ est composé de $\rho_P$ et de l'homomorphisme canonique $\psi_{L_P/K_P}$ (chap.I,§ 6) ; on a donc $\omega \circ \psi_{Z/K,P} = \rho'_P \circ \omega_P \circ \psi_{L_P/K_P}$ . Sous les conditions précédentes , on peut donc identifier G à $\Gamma/\Delta$ par l'isomorphisme $\omega$, et $G_P$ à $\Gamma_P$ (ou à un de ses sous-groupes) par l'isomorphisme $\omega_P$ ; nous supposerons dans tout ce qui suit qu'on a fait ces identifications ; pour toute place P de K , on a alors pour tout $z_P \in K_P^*$

(16) $$\psi_{Z/K,P}(z_P) \equiv \psi_{L_P/K_P}(z_P) \pmod{\Delta} .$$

Nous pouvons alors énoncer le théorème d'existence suivant :

THÉORÈME 4 (Grünwald-Wang) .- *Soient K un corps de nombres algébriques , $\ell$ un nombre premier impair , E une extension cyclique de K , de degré une puissance de $\ell$ , et linéairement disjointe de $K(\zeta_s)$ . Soit Z une extension cyclique de K , de degré $\ell^r$ . Soit S un ensemble fini de places de K , contenant toutes les places à l'infini et toutes les places ramifiées dans Z ; pour tout $P \in S$ , soit $\ell^{r(P)}$ le degré local de Z sur K , et soit $L_P$ une extension cyclique de $K_P$ , contenant $K_P(Z)$ , et de degré $\ell^{r(P)+s(P)}$ ; on suppose que $s \geqslant \max_{P \in S} s(P)$ et que , lorsque $r(P) > 0$ , on a $s(P) = s$ . Dans ces conditions, il existe une extension cyclique L de K , de degré $\ell^{r+s}$ , contenant Z , telle que $K_P(L) = L_P$ pour tout $P \in S$ , que $\psi_{L/K,P} = \psi_{L_P/K_P}$ pour tout $P \in S$ , et que tout diviseur premier n'appartenant pas à S et ramifié dans L reste premier dans E .*

Nous supposerons que S contient un diviseur premier $P_o$ ne divisant pas $\ell$ , restant premier dans Z , et pour lequel $L_{P_o}$ est l'extension (cyclique) non ramifiée de $K_{P_o}$ de degré $\ell^{r+s}$ : si S ne contenait pas un tel diviseur , on lui adjoindrait un diviseur $P_o$ ne divisant pas $\ell$ et restant premier dans Z , et on choisirait $L_{P_o}$ comme il vient d'être dit (les conditions de l'énoncé étant évidemment vérifiées alors pour $P_o$) .

Posons $H = K^* N_{Z/K}(J_Z)$ , $H_P = N_{K_P(Z)/K_P}(K_P(Z)^*)$ , et considérons l'homomorphisme $\varphi$

de $\prod_{P\in S} K_P^*$ dans $\Gamma$ , défini par la formule

(17) $$\varphi(z)=\prod_{P\in S}\psi_{L_P/K_P}(z_P)\ ;$$

en raison de l'hypothèse sur $L_{P_o}$ , $\varphi$ est un homomorphisme de $\prod_{P\in S} K_P^*$ sur $\Gamma$, et il existe $\beta_o\in K_{P_o}$ tel que $\psi_{L_{P_o}/K_{P_o}}(\beta_o)=\sigma$ . Soit $N_S$ le noyau de $\varphi$ ; les formules (16) montrent que $N_S\subset H_S=\prod_{P\in S} H_P$ ; en outre , $\prod_{P\in S} K_P^*$ est engendré par $\beta_o$ et $N_S$.

Soit T un ensemble fini de diviseurs premiers de K satisfaisant aux conditions du lemme 4 ; avec les notations de ce lemme , posons $H_o=K^*N_S H^{\ell^s} V^{S\cup T}$ . On a , en vertu des hypothèses , $H_o\subset H$ ; soit $G=H/H_o$ , et $G_1=H_S H_o/H_o$ . Comme $K^*H^{\ell^s}V^{S\cup T}$ est d'indice fini dans H (étant ouvert et contenant $K^*$ , il est déjà d'indice fini dans $J_K$) , il en est de même de $H_o$ ; en outre , tout élément de G a un ordre diviseur de $\ell^s$ . Nous allons appliquer le lemme 5 au groupe G et à son sous-groupe $G_1$ ; considérons le groupe $G_1\cap G^{\ell^\nu}$ (pour $1\leqslant\nu\leqslant s$) ; un élément de ce groupe est la classe mod.$H_o$ d'un idèle $z\in H_S$ et d'un idèle $u^{\ell^\nu}$ , où $u\in H$ ; on a donc une relation de la forme

(18) $$z=u^{\ell^\nu}.\alpha y v^{\ell^s} w$$

où $\alpha\in K^*$ , $y\in N_S$ , $v\in H$ et $w\in V^{S\cup T}$ ; cette relation s'écrit

$$zy^{-1}=\alpha u^{\ell^\nu}.\ell^s w$$

et comme $\nu\leqslant s$ , il résulte du lemme 4 qu'il existe un idèle $x\in H_S$ tel que $zy^{-1}=x^{\ell^\nu}$ ; en d'autres termes , z et $x^{\ell^\nu}$ sont dans la même classe mod.$H_o$ ; cela montre que $G_1\cap G^{\ell^\nu}=G_1^{\ell^\nu}$ , et en vertu du lemme 5 , il existe donc un groupe $G_2$ supplémentaire de $G_1$ dans G . Cela signifie qu'il existe un groupe $H_2$ tel que $H_o\subset H_2\subset H$ , $H_S H_2=H$ et $H_S\cap H_2=H_S\cap H_o$ . Nous allons voir que le corps de classes L correspondant au groupe d'idèles $H_2$ répond aux conditions de l'énoncé .

Comme $H_2\subset H$ , on a $Z\subset L$ ; comme $H_2\supset V^{S\cup T}$ , toute place de K n'appartenant pas à $S\cup T$ est non ramifiée dans L ; toute place de K ramifiée dans L et n'appartenant pas à S appartient donc à T et par suite reste un diviseur premier dans E

171



(lemme 4) . Pour montrer que $K_p(L)=L_p$ lorsque $p\in S$ , considérons le groupe $H_2\cap \prod_{p\in S}K_p^*$ . Comme $H_2\subset H$ , on a $(\prod_{p\in S}K_p^*)\cap H_2=H_S\cap H_2=H_S\cap H_o$ en vertu du choix de $H_2$ ; mais si $z\in H_S\cap H_o$ , on a $z=\alpha yv^{\ell^s}w$ , où $\alpha\in K^*$, $y\in N_S$, $v\in H$ et $w\in V^{S\cup T}$ ; en vertu du lemme 4 , il existe $x\in H_S$ tel que $zy^{-1}=x^{\ell^s}$ ; d'autre part , en raison du choix de $P_o$ , $K_{P_o}(Z)=K_{P_o}$ , donc $H_{P_o}$ est engendré par $U_{P_o}$ et $\beta_o^{\ell^r}$ , et par suite $H_S$ est engendré par $N_S$ et $\beta_o^{\ell^r}$ ; on a donc $x=\beta_o^{\ell^r}t$ , où $t\in N_S$, et comme $\beta_o^{\ell^{r+s}}\in N_S$ , on voit finalement que $z\in N_S$ , autrement dit $(\prod_{p\in S}K_p^*)\cap H_2=N_S$ . En particulier , si $p\in S$ , la relation $z_p\in H_2$ (pour un élément $z_p\in K_p$) est équivalente à $\psi_{L_p/K_p}(z_p)=1$ , ce qui prouve que $K_p(L)=L_p$ . D'autre part , le groupe engendré par $\beta_o$ et $H_2$ contient le groupe engendré par $\beta_o$ et $N_S$ , c'est-à-dire $\prod_{p\in S}K_p^*$ , et a fortiori le groupe $H_S$ . Mais comme $H_2H_S=H$ , ce groupe contient $\beta_o$ et $H$ , et en raison du choix de $P_o$ et des relations (16) , $\beta_o$ et $H$ engendrent $J_K$ tout entier , donc il en est de même de $\beta_o$ et $H_2$ . Comme $\beta_o^{\ell^{r+s}}\in H_2$ , on a $(J_K:H_2)\leqslant \ell^{r+s}$ ; par ailleurs $[L_{P_o}:K_{P_o}]=\ell^{r+s}$ , et par suite $[L:K]=\ell^{r+s}$ , et $L$ est cyclique sur $K$ . Il est clair en outre que le groupe de Galois de $L$ sur $K$ est engendré par $\psi_{L/K}(\beta_o)$ ; en identifiant $\psi_{L/K}(\beta_o)$ avec $\sigma$ , on identifie le groupe de Galois de $L$ sur $K$ avec $\Gamma$ ; comme $H_2\cap(\prod_{p\in S}K_p^*)=N_S$ , et que $\prod_{p\in S}K_p^*$ est engendré par $\beta_o$ et $N_S$ , on voit après cette identification que $\varphi$ coïncide avec la restriction à $\prod_{p\in S}K_p^*$ de $\psi_{L/K}$ , et en particulier qu'on a $\psi_{L/K,p}=\psi_{L_p/K_p}$ pour toute place $p\in S$ , ce qui achève la démonstration .

Pour $\ell=2$ le théorème n'est plus exact sans condition supplémentaire dans l'énoncé . Le rédacteur a la flemme de rédiger la démonstration dans ce cas , et préfère attendre que Bourbaki ait pris une décision sur le maintien ou le rejet du th. de Grünwald-Wang .

---