SÉMINAIRE N. BOURBAKI

MARC KRASNER

Généralisations non-abéliennes de la théorie locale des corps de classes

Séminaire N. Bourbaki, 1952, exp. n° 47, p. 383-406

<http://www.numdam.org/item?id=SB_1948-1951__1__383_0>

Séminaire BOURBAKI
(Mai 1951)

GÉNÉRALISATIONS NON-ABÉLIENNES DE LA THÉORIE LOCALE DES CORPS DE CLASSES

par Marc KRASNER.

1. Théorie locale des corps de classes.

Avant d'exposer les généralisations partielles de la théorie locale des corps de classes, construites dans ces dernières années, je dois rappeler brièvement cette théorie (pour plus de détails, se reporter à la conférence de SAMUEL [12].

Soient k un corps de nombres $\mathfrak{P}$-adiques, K une extension finie de k, k^* et K^* leurs groupes multiplicatifs. On appelle groupe de Takagi de K/k le groupe $H_{K/k}$ des normes $N_{K/k}(\alpha)$ de K à k des $\alpha \in K^*$.

On démontre les résultats suivants :

a. Loi d'unicité. - Si K/k est une extension abélienne, elle est complètement déterminée par la donnée de $H_{K/k}$.

b. Loi d'ordination. - K/k et K'/k étant des extensions abéliennes, on a $K' \supseteq K$ si, et seulement si $H_{K'/k} \subseteq H_{K/k}$.

c. Loi d'existence. - Tout sous-groupe d'indice fini H de k^* est le groupe de Takagi d'une extension abélienne convenable K/k.

d. Seconde inégalité fondamentale. Loi de limitation. - K/k étant une extension finie quelconque, $H_{K/k}$ est un sous-groupe d'indice fini de k^* et $(k^* : H_{K/k}) \leqslant (K : k)$. On a $(k^* : H_{K/k}) = (K : k)$ si, et seulement si K/k est une extension abélienne. Plus généralement, K_a/k étant la plus grande sous-extension abélienne de K/k, on a $H_{K/k} = H_{K_a/k}$:

e. Loi d'isomorphisme. - K/k étant abélienne, le groupe de Galois $G_{K/k}$ de K/k est isomorphe à $k^*/H_{K/k}$.

f. Symbole de restes normiques de Hasse. - Il existe une manière canonique d'établir l'isomorphisme précédent, en définissant un symbole (symbole de Hasse) $(\alpha , K/k)$ tel que $\alpha \longrightarrow (\alpha , K/k)$ soit un certain homomorphisme canonique de noyau $H_{K/k}$ de k^* sur $G_{K/k}$.

Si $K' \supset K$, $(\alpha , K'/k)$ induit $(\alpha , K/k)$ dans K.

g. Lois de conducteur. - Il existe des idéaux $\mathfrak{f}$ de k tels que, si $\alpha \equiv I \pmod{\mathfrak{f}}$, on a $\alpha \in H_{K/k}$ (si l'on considère $H_{K/k}$ comme un sous-groupe de k^*

organisé en groupe métrique par la multiplication et la distance

$$d^*(\alpha, \beta) = |\alpha - \beta| : \mathrm{Max}(|\alpha|, |\beta|),$$

ceci signifie que $H_{K/k}$ est un sous-groupe ouvert de k^*). Le p.g.c.d. $f_{K/k}$ de ces f est dit le conducteur de K/k (ou, également, de $H_{K/k}$) ; ainsi, la valuation $|f_{K/k}|$ du conducteur de K/k est le rayon du plus grand cercle de centre I dans k que $H_{K/k}$ contient). La valuation $|f_{K/k}|$ du conducteur de K/k et, aussi, celles des conducteurs des surgroupes de $H_{K/k}$ sont déterminées par certains invariants arithmétiques de K/k, liés à son groupe de Galois, qui sont donnés par la théorie de la ramification de Hilbert (nombres de ramification et ordres des groupes de ramification) : inversement, la structure "métrique" de $H_{K/k}$ détermine ces invariants. Ces déterminations se font explicitement par une formule (Führer-Diskriminantenformel), due à Hasse.

En particulier, $f_{K/k} = (I)$ si, et seulement si K/k n'est pas ramifiée.

2. Théorème des unités de Hensel. Groupe de Galois de l'extension abélienne maximale de k.

Les résultats précédents permettent, grâce à un théorème de Hensel, de déterminer le groupe de Galois $G_{\Omega/k}$ de l'extension abélienne maximale Ω de k, organisé en groupe topologique par sa topologie de Krull. On sait que ce groupe est la limite projective des groupes de Galois $G_{K/k}$ des extensions abéliennes finies K/k, où, si $K' \supset K$, le correspondant dans $G_{K/k}$ d'un $\sigma' \in G_{K'/k}$ est $\sigma \in G_{K/k}$ qu'il induit dans K (conformément aux conventions habituelles, la topologie de la limite projective de groupes discrets est définie par la famille des images réciproques des unités de ces groupes dans l'application canonique de la limite projective sur chacun d'eux). En vertu des e et f, il existe des isomorphismes $(\alpha, K/k) \longrightarrow \alpha H_{K/k}$ des $G_{K/k}$ sur les $k^*/H_{K/k}$ correspondants, qui transforment les homomorphismes $\sigma' \longrightarrow \sigma$ précédents en applications canoniques de $k^*/H_{K'/k}$ sur $k^*/H_{K/k}$. Donc, $G_{\Omega/k}$ est isomorphe, en tant que groupe topologique, au complété de k^* par rapport à la topologie, qui y est définie par la famille $\{H_{K/k}\}$ de ses sous-groupes, K parcourant les extensions abéliennes finies de k. Mais, en vertu des c et d, cette famille est celle des sous-groupes de k^* d'indice fini. On appellera topologie finie d'un groupe sa topologie, définie par la famille de ses sous-groupes d'indice fini, et on appellera sa p-topologie celle définie par la famille de ses sous-groupes d'indice puissance de p, où p est un nombre premier. Ainsi, $G_{\Omega/k}$ est le complété de k^* par rapport à sa topologie finie.

LEMME. - La topologie finie resp. la p-topologie du produit direct d'un nombre fini de groupes est la topologie produit des topologies finies resp. des p-topologies des facteurs.

En effet, si $G = g_1 \times g_2 \times \dots \times g_s$, et si $\overline{g}_i$ est un sous-groupe de g_i d'indice fini, on a $(g_1 \times g_2 \times \dots \times g_s : \overline{g}_1 \times \overline{g}_2 \times \dots \times \overline{g}_s) = (g_1 : \overline{g}_1)$ $(g_2 : \overline{g}_2) \dots (g_s : \overline{g}_s)$. Et si G est un sous-groupe d'indice fini de G $(g_i : \overline{G} \cap g_i)$ divise $(G : \overline{G})$, et on a $\overline{G} \supseteq (g_1 \cap \overline{G}) \times (g_2 \cap \overline{G}) \times \dots \times (g_s \cap \overline{G})$

Ceci posé, soient r le corps résiduel de k, p sa caractéristique, $P = p^{f_o}$ le nombre des éléments (donc, f_o est le degré résiduel de k), $\mathfrak{P}$ l'idéal premier de k, e_o l'ordre de ramification absolu de k (donc $(p) = \mathfrak{P}^e$), $n_o = f_o e_o$ le degré absolu de k, π un nombre de k d'ordre I en $\mathfrak{P}$, Π le groupe des puissances entières de π, U le groupe des $\alpha \equiv I \pmod{\mathfrak{P}}$ de k, $\mathfrak{K}$ la fermeture algébrique valuée de k, $\mathcal{E}_s$ le groupe des racines s-ièmes de l'unité dans $\mathfrak{K}$. On a $\mathcal{E}_{P-1} \subset k$, car, dans tout $\rho \in r$, il existe un élément de $\mathcal{E}_{P-1}$ (à savoir, si α est un élément arbitraire de ρ, c'est la limite des α^{P^q} quand $q \to +\infty$), et on a $k^* = \Pi \mathcal{E}_{P-1} U$, ce produit étant direct en tant que produit de groupes abstraits. Mais, en vertu du lemme précédent, la topologie finie de k^* est produit de celles des Π, $\mathcal{E}_{P-1}$ et U. Donc, $G_{\Omega/k}$ est le produit direct des complétés des Π, $\mathcal{E}_{P-1}$ et U par rapport à leurs topologies finies. Déterminons ces complétés.

A. - Soit Z le groupe additif des entiers rationnels (c'est-à-dire, à isomorphie près, le groupe cyclique infini), et soit, ℓ étant un nombre premier, Λ_ℓ le groupe additif des entiers ℓ-adiques rationnels, organisé par sa topologie valuative (c'est-à-dire définie par la métrique $d(\lambda, \mu) = |\lambda - \mu|$; les idéaux (ℓ^s), $s = 0, 1, 2, \dots$, forment, dans cette topologie, une base des voisinages de l'élément neutre 0). $\pi^m \to m$ est un isomorphisme de Π sur Z. Considérons le produit direct $\Lambda = \prod_\ell \Lambda_\ell$ des groupes Λ_ℓ, étendu à tous les nombres premiers ℓ, et notons λ_ℓ la composante dans Λ_ℓ d'un $\lambda \in \Lambda$. $\ell_1, \ell_2, \dots, \ell_t$ étant un ensemble fini quelconque de nombres premiers, soit

$$V_{\ell_1^{s_1} \ell_2^{s_2} \dots \ell_t^{s_t}}$$

l'ensemble des $\lambda \in \Lambda$ tels que $\lambda_{\ell_i} \equiv 0 \pmod{\ell_i^{s_i}}$. Les V_m forment une base des voisinages de l'élément neutre $0 = (0, 0, \dots, 0, \dots)$ de Λ. Z est

un sous-groupe de tout Λ_ℓ . Appliquons tout $z \in \mathbb{Z}$ sur $\lambda(Z)$ tel que, pour tout ℓ , on ait $\lambda(z)_\ell = z$. L'image $\tilde{Z}$ de Z est dense sur Λ , car, pour tous ℓ_1 , ℓ_2 , ... , ℓ_t , s_1 , s_2 , ... , s_t et pour tout $\lambda \in \Lambda$, on peut trouver un entier z , tel que, pour tout $i = 1, 2, \dots, t$, on ait $z \equiv \lambda_{\ell_i}$ (mod $\ell_i^{s_i}$) . D'autre part, si $m = \ell_1^{s_1} \ell_2^{s_2} \dots \ell_t^{s_t}$, $V_m \cap \tilde{Z}$ est l'ensemble des $\lambda(z)$ tels que, pour tout $i = 1, 2, \dots, t$, $z \equiv 0 \pmod{\ell_i^{s_i}}$. C'est, donc, l'image de l'ensemble des multiples de m dans Z , et la topologie induite par celle de Λ dans Z est sa topologie finie. Par suite, <u>le complété de Π par rapport à sa topologie finie est isomorphe à l'adhérence dans Λ de son sous-groupe Z , c'est-à-dire à Λ</u> .

Un raisonnement analogue montre que le complété de Π par rapport à sa ℓ-topologie est isomorphe à Λ_ℓ .

B. - Soit Z_s le groupe cyclique d'ordre s , considéré à l'isomorphie près. $\mathcal{E}_{P-1}$ étant un groupe d'ordre fini, sa topologie finie est discrète, <u>et son complété est $\mathcal{E}_{P-1} \simeq Z_{P-1}$</u> .

C. - U est complet par rapport à sa topologie valuative. Montrons que la topologie finie de U coïncide avec sa topologie valuative, d'où résultera que le complété de U par rapport à sa topologie finie coïncide avec U .

U_i étant le groupe des éléments $\alpha \equiv I \pmod{\mathfrak{P}^i}$ de k , les U_i constituent une base des voisinages de l'unité dans la topologie valuative de U . Or, $(U : U_i) = P^{i-1} = p^{f_o(i-1)}$ est fini, et, même, est une puissance de p .

Ainsi, la topologie valuative de U est moins fine ou équivalente à sa topologie finie et, même, à sa p-topologie.

Pour démontrer la réciproque, le plus commode est de se servir du principe suivant (KRASNER).

PRINCIPE. - <u>Soient k un corps valué complet, $\mathfrak{K}$ sa fermeture algébrique, α un élément de $\mathfrak{K}$ séparable par rapport à k . Alors, si $\beta \in \mathfrak{K}$ est plus proche de α que de tous ses autres conjugués par rapport à k , on a $k(\beta) \supseteq k(\alpha)$</u> .

DEMONSTRATION. - Les conjugués de $\beta - \alpha$ par rapport à $k(\beta)$ sont tous de la forme $\beta - \alpha'$, où α' est un des conjugués de α par rapport à k . $k(\beta)$ étant aussi complet, on doit avoir, pour un tel $\beta - \alpha'$, $|\beta - \alpha'| = |\beta - \alpha|$. Mais, si $\alpha' \neq \alpha$, ceci est contraire à l'hypothèse. Donc, $\beta - \alpha$ et, par suite,

α n'ont d'autres conjugués par rapport à $k(\beta)$ qu'eux-mêmes. Vu la séparabilité de α, on a $\alpha \in k(\beta)$.

C.Q.F.D.

Remarquons encore que, si $f(x)$ est un polynôme normé irréductible dans k, et si α est un des zéros de $f(x)$ le plus proche d'un $\beta \in \mathfrak{K}$, $|f(\beta)|$ ne dépend, en tant que fonction de β, que de $d = |\beta - \alpha|$, et, en particulier, on a $d \leq |f(\beta)| : |f'(\alpha)|$ (où $f'(x)$ est la dérivée de $f(x)$), le signe étant $=$ si d ne dépasse pas le minimum de distance des zéros de $f(x)$.

En effet, on a, pour tout conjugué α' de α,

$$|\beta - \alpha'| \leqslant \text{Max}\,(|\alpha - \alpha'|, |\beta - \alpha|) = \text{Max}\,(|\alpha - \alpha'|, d)$$

et

$$|\alpha - \alpha'| \leqslant \text{Max}\,(|\beta - \alpha'|, |\beta - \alpha|) = \text{Max}\,(|\beta - \alpha'|, d).$$

Si $|\alpha - \alpha'| > d$, on a donc $|\beta - \alpha'| = |\alpha - \alpha'|$; et, si $|\alpha - \alpha'| \leqslant d$, on a $|\beta - \alpha'| \leqslant d$, d'où $|\beta - \alpha'| = d \geqslant |\alpha - \alpha'|$. Ainsi, on a

$$|f(\beta)| = \prod_{\alpha'} |\beta - \alpha'| \geqslant d \prod_{\alpha' \neq \alpha} |\alpha - \alpha'| = d|f'(\alpha)|;$$

et, si $D_f(d)$ désigne le produit de tous les $|\alpha - \alpha'|$ qui sont $> d$, et ν_d désigne le nombre des $|\alpha - \alpha'|$ qui sont $\leqslant d$, on a $|f(\beta)| = D_f(d)\, d^{\nu_d}$. Or, le groupe de Galois de $k(\alpha)/k$ induit un groupe transitif de permutations de l'ensemble des conjugués de α, et tout élément de ce groupe de Galois préserve la métrique du corps de Galois de $k(\alpha)/k$ (car k est complet). Donc, $D_f(d)$ et ν_d ne dépendent que des d et $f(x)$, et non du choix de α.

Appliquons ces résultats au polynôme $f(x) = x^j - u$, où $u \in U$. Comme $|u| = I$, tous les zéros α de $f(x)$ ont la valuation I. Donc, $f'(\alpha) = |j\alpha^{j-1}| = |j|$. Posons $\beta = I$, et soit α un des zéros de $f(x)$ le plus proche de I. Alors, $|f(\beta)| = |u - I|$ et $|I - \alpha| \leqslant |u - I||j|^{-1}$. Mais deux zéros de $f(x)$ ne diffèrent que par un facteur racine de l'unité, et la distance minimale de deux racines de l'unité est $|p|^{1:(p-1)}$. Ainsi, si $|u - I| < |j||p|^{1:(p-1)}$, I est plus près de α que de ses autres conjugués, et on a $\alpha \in k(1) = k$. Donc, pour un tel u, l'équation $x^j = u$ a dans U un zéro α tel que $|\alpha - I| = |j|^{-1}|u - 1|$.

Soit $G^{(j)}$ le groupe de puissance j-ièmes des éléments d'un groupe abélien G. En vertu de ce qu'on vient de prouver, $U^{(j)}$ contient le cercle de centre I et de tout rayon $\rho < |j||p|^{1:(p-1)}$ dans k, c'est-à-dire tout U_q tel que

$|\pi|^q < |j||p|^{i:(p-1)}$. (En particulier, $U^{(p)} \supseteq U_{[e_o p\ :\ (p-1)]+1}$ et est, donc, un sous-groupe d'indice fini de U).

$\overline{U}$ étant un sous-groupe de U d'un indice fini $j = (U : \overline{U})$, on a $\overline{U} \supseteq U^{(j)}$, et $\overline{U}$ contient quelque U_q . Donc, la topologie valuative de U est plus fine ou équivalente à sa topologie finie. D'où résulte l'équivalence des topologies valuatives, finie et p-topologie de U .

Ainsi, $G_{\alpha/k}$ est isomorphe au produit direct

$$\left(\prod_{\ell} \Lambda_{\ell} \right) \times Z_{p-1} \times U$$

des groupes topologiques Λ_{ℓ} ($\ell = 2$, 3 , 5 , ...) , Z_{p-1} et U . Pour achever sa détermination, il faut déterminer la structure de U . Nous venons de voir que les $U^{(p^i)}$ constituent une base des voisinages de I dans U . Les seuls éléments d'ordre fini de U sont des racines de l'unité (forcément d'exposant-puissance de p) , qui y sont contenues. Elles forment un groupe $\mathfrak{E}_{p^\sigma}$ d'ordre fini, donc discret. Nous avons vu que $U/U^{(p)}$ et, a fortiori, $U/U^{(p)}\,\mathfrak{E}_{p^\sigma}$ sont des groupes d'exposant p (qu'on peut, par suite, considérer comme espaces vectoriels sur le champ de Galois de p éléments) et de rang fini. On notera μ celui de $U/U^{(p)}\,\mathfrak{E}_{p^\sigma}$.

G et $g \subset G$ étant des groupes tels que G/g soit un groupe d'exposant p , un système Γ d'éléments γ_i de G sera dit une base minimale de G (mod g) si les $\gamma_i\, g/g$ forment une base minimale de G/g (considéré comme un espace vectoriel). Soit $T = (\tau_1 , \tau_2 , \ldots , \tau_\mu)$ une base minimale de U (mod $U^{(p)}\,\mathfrak{E}_{p^\sigma}$) , et soit U^* le groupe engendré par T . $U^*\,\mathfrak{E}_{p^\sigma}$ est dense dans U . En effet, on a $U = U^*\,\mathfrak{E}_{p^\sigma}\,U^{(p)}$. L'homomorphisme $\eta_i = \{u \to u^{p^i}\}$ transforme cette égalité en $U^{(p^i)} = U^{*(p^i)}\,\mathfrak{E}_{p^\sigma}^{(p^i)}\,U^{(p^{i+1})}$. Si l'on a déjà prouvé $U = U^*\,\mathfrak{E}_{p^\sigma}\,U^{(p^i)}$, il en résulte $U = U^*\,\mathfrak{E}_{p^\sigma}\,U^{(p^{i+1})}$, et $U^*\,\mathfrak{E}_{p^\sigma}$ est bien dense dans U .

Nous allons prouver que U induit dans $U^*\,\mathfrak{E}_{p^\sigma}$ sa p-topologie et que U^* , en tant qu'un groupe abstrait, est le groupe abélien libre engendré par T . Par définition, on a $(U^*\,\mathfrak{E}_{p^\sigma})^{(p)} = U^*\,\mathfrak{E}_{p^\sigma} \cap U^{(p)}$. Comme $\eta_i \cdot u = I$ entraîne $u \in \mathfrak{E}_{p^\sigma}$, η_i , appliqué aux surgroupes de $\mathfrak{E}_{p^\sigma}$, conserve leur intersection. Ainsi, on a :

$$U^*(p^i)\,\mathcal{E}_{p\sigma}(p^i) = U^*(p^{i-1})\,\mathcal{E}_{p\sigma}(p^{i-1}) \cap U(p^i) \quad ;$$

si l'on a déjà prouvé que $U^*(p^{i-1})\,\mathcal{E}_{p\sigma}(p^{i-1}) = U^*\,\mathcal{E}_{p\sigma} \cap U(p^{i-1})$, on a aussi

$$U^*(p^i)\,\mathcal{E}_{p\sigma}(p^i) = U^*\,\mathcal{E}_{p\sigma} \cap U(p^i) \quad ,$$

d'où résulte, vu que $U^*\,\mathcal{E}_{p\sigma} \supseteq \mathcal{E}_{p\sigma}$, que $U^*(p^i)\,\mathcal{E}_{p\sigma} = (U^*\,\mathcal{E}_{p\sigma} \cap U(p^i))\,\mathcal{E}_{p\sigma} = U^*\,\mathcal{E}_{p\sigma} \cap U(p^i)\,\mathcal{E}_{p\sigma}$. $U^*\,\mathcal{E}_{p\sigma}$ étant dense dans U on a

$$(U : U(p^i)) = (U^*\,\mathcal{E}_{p\sigma} : (U^*\,\mathcal{E}_{p\sigma})(p^i)) \geq (U^*\,\mathcal{E}_{p\sigma} : U^*(p^i)\,\mathcal{E}_{p\sigma}) \,.$$

Donc, la topologie de $U^*\,\mathcal{E}_{p\sigma}/\mathcal{E}_{p\sigma}$, induite par celle de $U/\mathcal{E}_{p\sigma}$ est sa p-topologie. $\mathcal{E}_{p\sigma}$ étant discret, les groupes topologiques $U^*\,\mathcal{E}_{p\sigma}/\mathcal{E}_{p\sigma}$ et U^* sont isomorphes, et la topologie, induite dans U^* par celle de U est aussi sa p-topologie. Si $\tau = \tau_1^{s_1}\tau_2^{s_2}\ldots\tau_\mu^{s_\mu}$ est égal à I, sans que tous les s_μ soient nuls, et si p^i est la contribution de p dans le p.g.c.d. des e_q

$$\tau' = \tau_1^{s_1 p^{-i}}\tau_2^{s_2 p^{-i}}\ldots\tau_\mu^{s_\mu p^{-i}}$$

est un élément de U^* n'appartenant pas à $U^{*(p)}\,\mathcal{E}_{p\sigma}$. Donc,

$$\tau = \tau'^{p^i} \notin U^*(p^{i+1})\,\mathcal{E}_{p\sigma}$$

contre l'hypothèse, et U^* est bien un groupe abélien libre engendré par T. Il ne possède, donc, aucun élément non-neutre d'ordre fini, et le produit $U^*\,\mathcal{E}_{p\sigma}$ est direct.

Le groupe T_i engendré par τ_i est $\simeq Z$. U^* est donc isomorphe, en tant que groupe topologique, au produit direct de μ groupes Z, organisés par leur p-topologie ; et le complété U de $U^*\,\mathcal{E}_{p\sigma}$ l'est au produit direct du complété de $\mathcal{E}_{p\sigma}$ et des μ complétés de Z. Ainsi, on a $U \simeq \mathcal{E}_{p\sigma} \times \Lambda_p^\mu$. Pour achever la détermination de U, il suffit de calculer μ.

Puisque $(U : U^{(p)}) = (U^*\,\mathcal{E}_{p\sigma} : (U^*\,\mathcal{E}_{p\sigma})^{(p)}) = (U^* : U^{*(p)})(\mathcal{E}_{p\sigma} : \mathcal{E}_{p\sigma}^{(p)})$, le rang de $U/U^{(p)}$ est μ ou $\mu+1$ suivant que $\sigma = 0$ ou $\neq 0$. Mais ce rang est égal à la somme des rangs μ_i $(i = 1, 2, \ldots, [e_o\,p : (p-1)])$ des groupes $U_iU^{(p)}/U_{i+1}U^{(p)} \simeq U_i/(U_i \cap U^{(p)})U_{i+1}$, car $U_1U^{(p)} = UU^{(p)} = U$ et

$U_{[e_o p:(p-1)]}U^{(p)} \subseteq U^{(p)}\,U^{(p)} = U^{(p)}$ (où $[a]$ désigne la partie entière du nombre réel a). Soit $\alpha \in U_i$, et soit $\rho_i(\alpha)$ le reste (mod $\mathfrak{P}$) de $\pi^{-i}(\alpha - 1)$. Si $\alpha, \beta \in U_i$ (donc $\beta \equiv 1 \pmod{\mathfrak{P}}$), on a

$$\pi^{-i}(\alpha\beta - 1) = \beta\pi^{-i}(\alpha - 1) + \pi^{-i}(\beta - 1) \equiv \pi^{-i}(\alpha - 1) + \pi^{-i}(\beta - 1) \pmod{\mathfrak{P}}$$

Donc, on a $\rho_i(\alpha\beta) = \rho_i(\alpha) + \rho_i(\beta)$, et $\alpha \to \rho_i(\alpha)$ est un homomorphisme de U_i sur le groupe additif du corps résiduel r de k, dont le noyau est U_{i+1}.

Si $i \leqslant e : (p-1)$, et si $\alpha \in U_i$, on a $\alpha^p = 1 + p(\alpha - 1) + (\alpha - 1)^p + p(\alpha-1)^2 \varphi(\alpha)$, où $\varphi(x)$ est un polynôme à coefficients entiers. On a $|p(\alpha - 1)^2 \varphi(\alpha)| \leqslant |\mathfrak{P}|^{e_o+2i} < |\mathfrak{P}|^{pi}$, $|(\alpha - 1)^p| \leqslant |\mathfrak{P}|^{pi}$ et $|p(\alpha - 1)| \leqslant |\mathfrak{P}|^{e_o+1} \leqslant |\mathfrak{P}|^{pi}$, le dernier signe d'identité ayant lieu si, et seulement si $i = e : (p-1)$. Ainsi, $\alpha^p \in U_{ip}$, et on a $\rho_{ip}(\alpha^p)$ = reste de $\pi^{-ip}(\alpha - 1)^p = \rho_i(\alpha)^p$ ou $\rho_{ip}(\alpha^p)$ = reste de $\pi^{-e_o p}\,\pi^{-i}(\alpha - 1)$ + reste de $\pi^{-ip}(\alpha - 1)^p = \omega\rho_i(\alpha) + \rho_i(\alpha)^p$, où ω est le reste (mod $\mathfrak{P}$) de $\pi^{-e_o p}$, suivant que $i <$ ou $= e_o : (p-1)$.

Soit m_i l'image, par l'homomorphisme $\alpha \to \rho_i(\alpha)$, de $(U_i \cap U^{(p)})U_{i+1}$, qui est également celui de $U_i \cap U^{(p)}$. Comme l'image de U_i est r, on a $U_i/(U_i \cap U^{(p)})U_{i+1} \simeq r/m_i$, et μ_i est égal à la différence du rang f_o de r et du rang de m_i. Si $i \leqslant e_o p : (p-1)$, et si j est le plus petit entier tel que $jp \geqslant i$, on a $U_i \cap U^{(p)} = U_i \cap U_j^{(p)}$. En effet, si $q < j$, on a $qp < i \leqslant e_o p : (p-1)$; donc, si $\alpha \in U_q$, mais $\notin U_{q+1}$, on a $\rho_q(\alpha) \neq 0$, d'où $\rho_{qp}(\alpha^p) = \rho_q(\alpha)^p \neq 0$, et $\alpha^p \notin U_i$. Si $i \not\equiv 0 \pmod p$, on a $jp > i$, d'où $U_i \cap U^{(p)} \subseteq U_{jp} \subseteq U_{i+1}$, et $m_i = 0$; donc, dans ce cas, on a $\mu_i = f_o$. Si $i \not\equiv 0 \pmod p$, $\rho_j(\alpha) \to \rho_i(\alpha^p)$ est un homomorphisme (additif) de r sur m_i. Si $i < e_o p : (p-1)$, cet homomorphisme est l'automorphisme $\rho \to \rho^p$ de r ; donc, dans ce cas, on a $m_i = r$ et $\mu_i = 0$. Enfin, si $i = e_o p : (p-1)$, donc $j = e : (p-1)$, soit m^* le noyau de l'homomorphisme $\rho \to \omega\rho + \rho^p$, et soit μ^* le rang de m^*. Comme $m_i \simeq r/m^*$, on a $\mu_i = f_o - (f_o - \mu^*) = \mu^*$. Or, m^* est l'ensemble des zéros dans r du polynôme $x^p + \omega x$ de degré p. Comme c'est un module, et comme r est un corps de caractéristique p, μ^* est 0 ou 1 suivant que $x^p + \omega x$ n'a pas ou a dans r

des zéros non nuls. Montrons que $x^p + \omega x$ a de tels zéros si et seulement si $\sigma \neq 0$. En effet, si $\sigma \neq 0$, k contient une racine p-ième primitive de l'unité. θ étant cette racine, on a $|\theta - I| = |p|^{1:(p-1)} = |\mathfrak{P}|^{e_o:(p-1)}$, donc $\theta \in U_j$ et $\rho_j(\theta) \neq 0$; mais on a $\rho_i(\theta^p) = \rho_i(1) = 0$. Réciproquement, si ρ est un zéro non nul de $x^p + \omega x$ dans r, soit un $\alpha \in U_j$ $(j = e_o : (p - I))$ tel que $\rho_j(\alpha) = \rho$; alors $|\alpha^p - I| < |\mathfrak{P}|^{e_o p:(p-1)}$; il en résulte que le polynôme $x^p - \alpha^p$ a un zéro β dans k tel que

$$|\beta - I| < |p|^{-1} |\mathfrak{P}|^{e_o p:(p-1)} = |\mathfrak{P}|^{e_o:(p-1)} = |\mathfrak{P}|^j .$$

Donc, on a $\alpha\beta^{-1} \neq 1$ et $(\alpha\beta^{-1})^p = I$.

Ainsi, μ, est, finalement, le produit de f_o par le nombre des entiers $i \not\equiv 0 \pmod p$ de l'intervalle $(0, e_o p : (p - I))$. Ce dernier nombre est $[e_o p : (p - I)] - [e_o : (p - I)] = e_o + [e_o : (p - I)] - [e_o : (p - I)] = e_o$. Donc, on a $\mu = f_o e_o = n_o$.

Ainsi, finalement, on trouve que $G_{\alpha/k}$ est isomorphe au produit

$$\prod_{\ell \neq p} \Lambda_\ell \times \mathcal{E}_{(p-1)p^\sigma} \times \Lambda_p^{n_o+1} .$$

On appelle p-extension de k tout composé (de degré fini ou infini) d'extensions galoisiennes de degré puissance de p. Si α^p est la p-extension abélienne maximale de k, on voit que $G_{\alpha^p/k}$ (c'est le complété, par rapport à sa p-topologie, du quotient de k^* par l'intersection des $k^{*(p^i)}$, c'est-à-dire de $k^*/\mathcal{E}_{p-1} \simeq \Pi \times U$) est isomorphe à

$$\mathcal{E}_{p^\sigma} \times \Lambda_p^{n_o+1} .$$

En particulier, quand $\sigma = 0$, on a $G_{\alpha^p/k} \simeq \Lambda_p^{n_o+1}$. Autrement dit, $G_{\alpha^p/k}$ est isomorphe, dans ce cas, au complété, par rapport à sa p-topologie, du groupe abélien libre à $n_o + 1$ générateurs.

3. Généralisations non-abéliennes de la théorie locale des corps de classes.

A l'heure actuelle, il existe deux généralisations partielles de la théorie locale des corps de classes aux extensions non-abéliennes.

I. Théorie de Schafarevitch. - Cette théorie généralise le dernier résultat indiqué ; à savoir, elle détermine à l'isomorphie près, sous l'hypothèse $\sigma = 0$, le groupe de Galois $G_{\mathfrak{K}^p/k}$ de la p-extension maximale $\mathfrak{K}^p$ de k. Cette théorie permet la détermination du nombre des extensions galoisiennes de k, ayant, comme groupe de Galois, un p-groupe donné. La théorie de Schafarevitch est fondée sur ce qui précède et sur un théorème de Schreier à propos de sous-groupes des groupes libres. Il est à espérer que l'application plus poussée de la théorie des groupes libres permettra de déterminer $G_{\mathfrak{K}^p/k}$ quand $\sigma > 0$ et, peut être, déterminer même $G_{\mathfrak{K}/k}$.

II. Théorie de Krasner. - Cette théorie généralise les "lois de conducteur". Elle s'applique, d'ailleurs, en grande partie, aux extensions séparables des corps valués complets quelconques, et non seulement $\mathfrak{P}$-adiques. Dans cette théorie, une extension est caractérisée par un ensemble convenable de polynômes (généralisant $H_{K/k}$), considéré comme un sous-espace de l'ensemble des polynômes normés irréductibles de k, organisé en un espace métrique par une distance convenable. Il se trouve que cet ensemble caractérisant est une réunion de cercles d'un rayon fixe de l'espace considéré, et que, dans le cas $\mathfrak{P}$-adique, le nombre de ces cercles est fini. La valuation de conducteur d'une extension K/k peut être définie, à peu de chose près, comme le rayon maximal de cercles de cet espace, en lesquels l'ensemble caractérisant se décompose ; et la structure métrique de l'ensemble caractérisant fournit des renseignements étendus sur le groupe de Galois de K/k (sans, toutefois, en déterminer complètement le type), sur ses invariants arithmétiques, liés à ce groupe (objets de la théorie de la ramification et certains autres) et un critère pour décider si K/k est galoisienne (si k est discrètement valué, ce critère permet de déterminer, plus généralement, le nombre des corps conjugués distincts de K/k dans $\mathfrak{K}$). Cette théorie permet, dans le cas des corps k localement compacts, de déterminer le nombre des surcorps $K \subset \mathfrak{K}$ de k, ayant le degré et la différente donnés par le rapport à k (et, même, ayant, en plus, certains invariants arithmétiques donnés), et, dans le cas $\mathfrak{P}$-adique, le nombre des surcorps $K \subset \mathfrak{K}$ de k de degré donné par rapport à k.

Je vais exposer en détail la théorie de Schafarevitch. Je ne donnerai qu'une idée de celle de Krasner, surtout en vue de comparaison.

Pour plus de détails, voir [10].

4. Théorie de Schafarevitch.

G étant un groupe, notons $G^{(1)}$ le groupe engendré par les puissances p-ièmes et par les commutateurs des éléments de G, et soit $G^{(i)} = (G^{(i-1)})^{(1)}$. $G^{(1)}$ est, évidemment, le plus petit sous-groupe de G tel que $G/G^{(1)}$ soit un groupe abélien d'exposant p. Si g est un sous-groupe invariant de G, il est visible que $(G/g)^{(1)} = G^{(1)}g/g$ et, plus généralement, $(G/g)^{(i)} = G^{(i)}g/g$. Si tous les $G^{(i)}$ sont d'indice fini dans G, la topologie de G, définie par les $G^{(i)}$, coïncide avec sa p-topologie : en effet, si g est un sous-groupe de G d'indice puissance de p, $\Gamma = G/g$ est un p-groupe. Or, si $\Gamma \neq I$ est un p-groupe, $\Gamma^{(1)}$ en est un sous-groupe propre (car il est contenu dans tout sous-groupe de Γ d'indice p, et de tels sous-groupes existent).

Il existe, donc, un i tel que $\Gamma^{(i)} = 1$. Mais alors on a $G^{(i)}g \subseteq g$ et $G^{(i)} \subseteq g$. Inversement, si $(G : G^{(i)})$ est fini, il est une puissance de p, car tous les $G^{(i-1)}/G^{(i)}$ sont des groupes d'exposant p.

Supposons que G soit séparé par rapport à sa p-topologie. Soit T un ensemble générateur de G (mod $G^{(1)}$) (puisque $G/G^{(1)}$ est un groupe d'exposant p, on peut prendre comme T une base minimale de G (mod $G^{(1)}$) ; alors, le nombre d'éléments de T est égal au rang de $G/G^{(1)}$). Alors, si tous les $(G : G^{(i)})$ sont finis, le groupe G(T), engendré par T, est dense dans G, organisé par sa p-topologie. En effet, $\Gamma_i = G/G^{(i)}$ est un p-groupe, et on a

$$\Gamma_i^{(1)} = G^{(1)}G^{(i)}/G^{(i)} = G^{(1)}/G^{(i)} .$$

Ainsi, $T_i = TG^{(i)}/G^{(i)}$ engendre aussi $\Gamma_i/\Gamma_i^{(1)}$. Mais on sait que, dans ce cas, T_i engendre Γ_i, donc T engendre G (mod $G^{(i)}$). Les $G^{(i)}$ formant une base des voisinages de l'unité dans la p-topologie de G, G(T) est bien dense dans G par rapport à cette topologie.

Si G est, en plus, complet, il est, donc, le complété de G(T) par rapport à la topologie, qui y est induite par celle de G.

Ceci posé, supposons que $\sigma = 0$, et soient k' le composé de toutes les extensions de degré p de k, et, pour tout i, $k^{(i)} = (k^{(i-1)})^1$. Si le degré absolu n_i de $k^{(i)}$ est fini et $k^{(i)}$ ne contient pas de racines p-ièmes primitives de l'unité, n_{i+1} est aussi fini et $k^{(i+1)}$ ne contient pas de racines p-ièmes primitives de l'unité, car, autrement, on aurait $n_{i+1}n_i^{-1} \equiv 0 \pmod{p-1}$. On a, en vertu de la théorie locale des corps de classes,

$$G_{k^{(i+1)}/k^{(i)}} = G_{\alpha^p/k^{(i)}/G^{(p)}\alpha^p/k^{(i)}} \simeq \Lambda_p^{n_i+1}/(\Lambda_p^{n_i+1})^{(p)}$$

$$= (\Lambda_p/\Lambda_p^{(p)})^{n_i+1} \simeq (Z/Z^{(p)})^{n_i+1} = Z_p^{n_{i+1}}$$

Ainsi, $(k^{(i+1)} : k^{(i)})$ est fini (et, par suite, n_{i+1} est fini) et égal à p^{n_i+1}. Donc, puisque n_o est fini, tout n_i l'est. On a $n_i = n_o\,(k^{(i)} : k)$.

On a $\mathfrak{K}^p = \bigcup_i k^{(i)}$. Ainsi la topologie de $G = G_{\mathfrak{K}^p/k}$ est définie par les $G_{\mathfrak{K}^p/k^{(i)}} = G^{(i)}$ et est séparée ; et, puisque tous les

$$(G : G^{(i)}) = (k^{(i)} : k) = n_i : n_o$$

sont finis, elle coïncide avec sa p-topologie. G est complet par rapport à cette topologie.

Soit T une base minimale de G (mod $G^{(1)}$). G est donc le complété de G(T) par rapport à sa topologie définie par les $G(T) \cap G^{(i)} \supseteq G(T)^{(i)}$. G(T) étant dense sur G, on a $(G : G^{(i)}) = (G(T) : G(T) \cap G^{(i)})$. Le nombre d'éléments de T est égal au rang de $G/G^{(1)} = G_{k'/k} \sim Z_p^{n_o+1}$, donc est $n_o + 1$. Ainsi, G(T) est un groupe à $n_o + 1$ générateurs. C'est donc, à l'isomorphie près, le quotient du groupe libre L_{n_o+1} à $n_o + 1$ générateurs par un sous-groupe convenable g. Donc on a $G(T)^{(i)} = L^{(i)}_{n_o+1}\, g/g$.

On a

$$(k^{(i)} : k) = (G : G^{(i)}) = (G(T) : G(T) \cap G^{(i)}) \leqslant (G(T) : G(T)^{(i)})$$

$$= (L_{n_o+1} : L^{(i)}_{n_o+1}\, g) \leqslant (L_{n_o+1} : L^{(i)}_{n_o+1}) .$$

On ne peut avoir partout les signes d'égalité, c'est-à-dire avoir

$$(k^{(i)} : k) = (L_{n_o+1} : L^{(i)}_{n_o+1}),$$

que si, à la fois on a

$$G(T) \cap G^{(i)} = G(T)^{(i)} \quad \text{et} \quad g \subsetneq L^{(i)}_{n_o+1} .$$

Or, on va prouver cette égalité par induction, en se servant, en particulier, du théorème suivant de Schreier sur les groupes libres :

THÉORÈME de Schreier. - Tout sous-groupe L du groupe libre L_s à s générateurs est libre, et si son indice $j = (L_s : L)$ est fini, le nombre des générateurs de L est $1 + (s - 1)j$.

Soit s_i le nombre de générateurs du groupe libre (en vertu du théorème de Schreier) $L_{n_o+1}^{(i)}$. Alors, $L_{n_o+1}^{(i)}/L_{n_o+1}^{(i+1)}$ est un groupe abélien d'exposant p et de rang s_i. Donc, on a $(L_{n_o+1}^{(i)} : L_{n_o+1}^{(i+1)}) = p^{s_i}$.

On a $s_o = n_o + 1$. Supposons qu'on ait prouvé $(L_{n_o+1} : L_{n_o+1}^{(i)}) = (k^{(i)} : k)$. Alors, on a, en vertu du théorème de Schreier,

$$s_i = 1 + (s_o - 1)(L_{n_o+1} : L_{n_o+1}^{(i)}) = 1 + n_o(k^{(i)} : k) = \quad + n_i \quad .$$

Mais, dès lors, on a $(L_{n_o+1}^{(i)} : L_{n_o+1}^{(i+1)}) = p^{s_i} = p^{n_i+1} = (k^{(i+1)} : k^{(i)})$, d'où résulte $(L_{n_o+1} : L_{n_o+1}^{(i+1)}) = (k^{(i+1)} : k)$. L'égalité est, ainsi, prouvée pour tout i.

Par suite, pour tout i, on a $g \subseteq L_{n_o+1}^{(i)}$ et $G(T) \cap G^{(i)} = G(T)^{(i)}$. Soit L^* l'intersection $\cap L_{n_o+1}^{(i)}$ de tous les $L_{n_o+1}^{(i)}$. La première relation montre que $g \subseteq L^*$. Comme la p-topologie de $G(T) = L_{n_o+1}/g$ est séparée, on a, également, $g \supseteq L^*$, d'où $g = L^*$. La seconde relation montre que la topologie, induite sur $G(T)$ par celle de G est sa p-topologie. Ainsi, finalement, on arrive au

THÉORÈME fondamental de Schafarévitch. - Si $\sigma = 0$, $G_{\mathfrak{K}^p/k}$ est isomorphe au complété, par rapport à sa p-topologie, du groupe topologique séparé associé (au sens de Bourbaki) au groupe libre L_{n_o+1} à n_o+1 générateurs, organisé par sa p-topologie.

COROLLAIRE. - Un p-groupe Γ est isomorphe au groupe de Galois de quelque extension de k, si, et seulement si le nombre minimal de ses générateurs est $\leq n_o + 1$.

En effet, si F est un sous-groupe fermé de $G = G_{\mathfrak{K}^p/k}$ tel que $\Gamma \simeq G/F$, on a aussi $\Gamma \simeq G(T)/F \cap G(T)$. Mais le nombre minimum des générateurs de ce groupe

ne dépasse pas celui $n_o + 1$ des éléments de T. Inversement si le nombre des générateurs de Γ est $\leq n_o + 1$, il existe un sous-groupe F de $G(T)$ tel que $\Gamma \sim G(T)/F$. Mais, puisque la topologie induite de $G(T)$ est sa p-topologie, et puisque Γ est un p-grpupe, F est fermé dans $G(T)$. Dès lors, l'adhérence F^* de F dans G est un sous-groupe fermé de G, et on a $G/F^* \simeq G(T)/F \simeq \Gamma$.

La démonstration du théorème fondamental qu'on vient de faire, montre que, pour toute base minimale T de G (mod $G^{(1)}$), $G(T)$ est dense sur G, et est, en tant que sous-groupe de ce groupe topologique, isomorphe au groupe séparé, associé au groupe libre L_{n_o+1}, organisé par sa p-topologie. Il en résulte le

THÉORÈME. - T étant une base minimale de G (mod $G^{(1)}$), tout automorphisme continu η de G applique biunivoquement T sur une autre base minimale $T' = \eta.T$ de G (mod $G^{(1)}$) et est complètement déterminé par sa restriction à T. Inversement, T' étant une base minimale arbitraire de G (mod $G^{(1)}$), pour toute application biunivoque de T sur T', il existe un automorphisme bicontinu de G, qui la prolonge.

En effet, $G^{(1)}$ étant un sous-groupe caractéristique de G, un automorphisme η le conserve. Donc, η est continu et $\eta.T$ est une base minimale de G (mod $G^{(1)}$). Visiblement, la restriction de η à T détermine η sur $G(T)$. Comme η est continu, il est déterminé aussi sur l'adhérence G de $G(T)$. Inversement, T' étant une base minimale de G (mod $G^{(1)}$), une application biunivoque de T sur T' se prolonge en un isomorphisme du groupe libre engendré par T sur celui engendré par T'. Cet isomorphisme préserve, évidemment, la p-topologie de ces groupes, et induit, par suite, un isomorphisme entre leurs groupes séparés associés $G(T)$ et $G(T')$, qui est aussi un homéomorphisme de ces groupes par rapport à leurs p-topologies. Il est donc uniformément continu, et est prolongeable, par continuité, à l'adhérence G de $G(T)$, qu'il applique sur celle G de $G(T')$. Ce prolongement est, donc, un automorphisme bicontinu de G.

THÉORÈME. - Si deux sous-groupes fermés et invariants F_1 et F_2 de $G = G_{\mathfrak{k}^p/k}$ sont tels que $\Gamma_1 = G/F_1 \simeq \Gamma_2 = G/F_2$, tout isomorphisme η de Γ_1 sur Γ_2 est induit par quelque automorphisme bicontinu de G (une autre manière de formuler ce théorème : si K_1/k et K_2/k sont deux p-extensions, dont les groupes de Galois sont isomorphes, tout isomorphisme continu entre leurs groupes de Galois se prolonge en un automorphisme bicontinu de celui de la p-extension maximale $\mathfrak{k}^p$ de k).

Démontrons, d'abord, ce théorème dans le cas, où $(G : F_1) = (G : F_2)$ est fini. On a $\Gamma_1 / \Gamma_1^{(1)} \simeq G/F_1 G^{(1)}$. Comme $G/G^{(1)}$ est un groupe d'exposant p , la juxtaposition T d'une base minimale $T_1 = \{t_1 , t_2 , \dots , t_s\}$ de $G \pmod{F_1 G^{(1)}}$ et d'une base minimale $T_2 = \{t_{s+1} , \dots , t_{n_o+1}\}$ de $F_1 \pmod{F_1 \cap G^{(1)}}$ est une base minimale de $G \pmod{G^{(1)}}$. Si $t_i^* = t_i F_1$, $(i = 1 , 2 , \dots , s)$, $T_1^* = \{t_1^* , t_2^* , \dots , t_s^*\}$ est une base minimale de $\Gamma_1 / \Gamma_1^{(1)}$ donc un ensemble générateur de Γ_1 . Soit S $(x_1 , x_2 , \dots , x_s)$ l'ensemble des relations définissantes de Γ_1 pour cet ensemble générateur, autrement dit l'ensemble des monômes non-commutatifs $\sigma(x_1 , x_2 , \dots , x_s)$ en $x_1, x_2, \dots, x_s, x_1^{-1}, x_2^{-2}, \dots, x_s^{-1}$, tels que $\sigma(t_1^* , t_2^* , \dots , t_s^*) = 1$. Alors, un groupe dense dans F_1 est engendré par les $\sigma(t_1 , t_2 , \dots , t_s) \in S(t_1 , t_2 , \dots , t_s)$ et par les conjugués dans G des $t_i \in T_2$. D'autre part, puisque η est un isomorphisme de Γ_1 sur Γ_2 , $S(x_1 , x_2 , \dots , x_s)$ est aussi l'ensemble des relations définissantes de Γ_2 pour son ensemble générateur (écrit dans cet ordre) $\eta . T_1^* = \{\eta . t_1^* , \eta . t_2^* , \dots , \eta . t_s^*\}$; ainsi, si t_i' est un élément de G , appartenant à $\eta . t_i^*$ (qui est une classe dans $G \pmod{F_2}$), et si $T_2' = \{t_{s+1}' , t_{s+2}' , \dots , t_{n_o+1}'\}$ est une base minimale de $F_2 G^{(1)} / G^{(1)}$, un sous-groupe dense de F_2 , est engendré par les $\sigma(t_1', t_2', \dots, t_s') \in S(t_1', t_2', \dots, t_s')$ et par les conjugués dans G des $t_i' \in T_2'$. $T' = \{t_1' , t_2' , \dots , t_s'\}$ est visiblement une base minimale de $G \pmod{F_2 G^{(1)}}$. Par suite, la juxtaposition $T' = \{t_1' , t_2' , \dots , t_{n_o+1}'\}$ de T_1' et de T_2' en est une de $G \pmod{G^{(1)}}$.

Il existe, donc, un automorphisme bicontinu η^* de G , qui applique T sur T' . Il applique le groupe, engendré par S $(t_1 , t_2 , \dots , t_s)$ et les conjugués des $t_i \in T_2$, qui est dense dans F_1 , sur un groupe dense dans F_2 . Etant continu, il applique aussi F_1 sur F_2 . η^* induit, visiblement, η sur T_1^* , et, par suite, sur le groupe Γ_1 , qu'il engendre.

Dans le cas général, on construit η^* de la même manière. $\eta . T_1^*$ est, en effet, encore une base minimale de $\Gamma_2 / \Gamma_2^{(1)}$, car les $\Gamma^{(1)}$ sont intrinsèquement définis par la seule loi de composition de groupe Γ , et l'automorphisme de Γ_1 sur Γ_2 applique $\Gamma_1^{(1)}$ sur $\Gamma_2^{(1)}$. Pour la même raison, η induit un isomorphisme de $\Gamma_1 / \Gamma_1^{(1)}$ sur $\Gamma_2 / \Gamma_2^{(1)}$. En appliquant à ces groupes d'ordre fini le raisonnement précédent, on voit que cet automorphisme coïncide avec celui induit par η^* . Donc, pour tout $\sigma \in \Gamma_1$, ses images par η et par η^* ne diffèrent que par un élément appartenant à tout voisinage $\Gamma_2^{(1)}$ de l'unité dans Γ_2 . Γ_2 étant

séparé, ils coïncident, et η^* induit η dans Γ_1.

COROLLAIRE. - Si F et $\overline{F} \subset F$ sont deux sous-groupes fermés invariants de G, tout isomorphisme de G/F sur un groupe quotient de G par un de ses sous-groupes formés se prolonge en un isomorphisme de $G/\overline{F}$ de même forme (autre formulation : si K et $\overline{K} \subset K$ sont deux p-extensions de k, tout isomorphisme de $G_{\overline{K}/k}$ sur le groupe de Galois d'une autre p-extension $\overline{K}'/k$ se prolonge en celui de $G_{K/k}$ sur le groupe de Galois d'une surextension convenable K'/k de $\overline{K}'/k$).

En effet, un isomorphisme de $G_{\overline{K}/k}$ est induit par un automorphisme bicontinu de G, lequel induit dans $G_{K/k}$ l'automorphisme cherché.

COROLLAIRE. - Soient Γ un groupe, dont le nombre des générateurs soit $\leq n_0 + 1$ et γ un sous-groupe invariant de Γ. Alors, tout isomorphisme de Γ/γ sur le groupe de Galois $G_{\overline{K}/k}$ d'une p-extension $\overline{K}/k$ se prolonge en un isomorphisme de Γ sur le groupe de Galois $G_{K/k}$ d'une surextension convenable K/k de $\overline{K}/k$.

En effet, puisque le nombre des générateurs de Γ est $\leq n_0 + 1$, il existe une p-extension K'/k telle que $G_{K'/k} \simeq \Gamma$. Soit η' un isomorphisme de Γ sur $G_{K'/k}$. Soit $\overline{K}'$ le corps, qui appartient à l'image $\eta'.\gamma$ de γ par cet isomorphisme. η' induit un isomorphisme $\overline{\eta}'$ de Γ/γ sur $G_{\overline{K}'/k}$. Ainsi, $\overline{\eta}\,\overline{\eta}'^{-1}$ est un isomorphisme de $G_{\overline{K}'/k}$ sur $G_{\overline{K}/k}$. En vertu du corollaire précédent, il se prolonge par un isomorphisme η^* de $G_{K'/k}$ sur le groupe de Galois d'une extension convenable $K/k \supseteq \overline{K}/k$; et, alors, $\eta^* \eta'$ est un isomorphisme de Γ sur $G_{K/k}$ prolongeant $(\overline{\eta}\,\overline{\eta}'^{-1})\,\overline{\eta}' = \overline{\eta}$.

THÉORÈME. - Γ étant un p-groupe, soient p^m son ordre, ν le nombre minimum de ses générateurs, α le nombre de ses automorphismes. Alors, le nombre des p-extensions K/k telles que $G_{K/k} \simeq \Gamma$ est

$$\frac{1}{\alpha} p^{(m-\nu)(n_0+1)} (p^{n_0+1} - 1)(p^{n_0+1} - p) \cdots (p^{n_0+1} - p^{\nu+1}).$$

DÉMONSTRATION. - Si $G/F \simeq \Gamma$, tout autre groupe $F' \subset G$ tel que $G/F' \simeq \Gamma$ s'obtient, en vertu du théorème précédent, en appliquant à F un automorphisme bicontinu η^* de G. Cet automorphisme conserve $G^{(1)}$. Par suite, si $F \supseteq G^{(1)}$, on a $F' \supseteq G^{(1)}$, et $F'/G^{(1)}$ s'obtient, à partir de $F/G^{(1)}$, par l'automorphisme η de $G/G^{(1)}$, induit par η^*. Si T est une base de $G/G^{(1)}$ (mod $G^{(1)}/G^{(1)}$), qui est la juxtaposition d'une base $T_1 = \{t_1, t_2, \ldots, t_\nu\}$ de $G/G^{(1)}$ (mod $F\,G^{(1)}/G^{(1)}$) et d'une base $T_2 = \{t_{\nu+1}, \ldots, t_{n_0+1}\}$ de $F/G^{(1)}$

(mod $F \cap G^{(1)}/G^{(i)}$), η applique T sur une base T' de $G/G^{(i)}$ (mod $G^{(1)}/G^{(i)}$), qui est située de la même manière par rapport à F'. η est complètement déterminé par cette application. Il est visible que, quel que soit F', un même nombre de ces applications transforment $F/G^{(i)}$ en $F'/G^{(i)}$. Ainsi, le nombre des F' différents est égal au quotient du nombre total de ces applications par celui de ces applications, qui conservent F.

Soit C' un sous-groupe d'un groupe C tel que C/C' soit un groupe abélien d'exposant p. Alors, une application d'une base minimale $\{t_1, t_2, \ldots, t_\theta\}$ de C (mod C') sur une autre base minimale $\{t_1', t_2', \ldots, t_\theta'\}$ de C (mod C') peut se faire comme suit : on applique d'abord la base minimale $\{t_1C', t_2C', \ldots, t_\theta C'\}$ de C/C' sur une autre base minimale $\{t_1^{*\prime}, t_2^{*\prime}, \ldots, t_\theta^{*\prime}\}$ de C/C', et, ensuite, dans tout $t_i^{*\prime}$ qui est classe (mod C'), on choisit un élément t_i'. Le rang de C/C' est θ. Le nombre des applications $t_i C' \to t_i^{*\prime}$ est, en vertu d'un calcul bien connu,

$$(p^\theta - I)(p^\theta - p) \ldots (p^\theta - p^{\theta-1})$$

et t_i' peut être choisi dans $t_i^{*\prime}$ de nombre de manières égal à l'ordre de C'. Ainsi, le nombre d'applications $t_i \to t_i'$ est

$$(\text{ordre de } C')^\theta (p^\theta - I)(p^\theta - p) \ldots (p^\theta - p^{\theta-1}).$$

En particulier, si $(G : G^{(i)}) = p^t$, le nombre d'applications d'une base minimale de $G/G^{(i)}$ (mod $G^{(1)}/G^{(i)}$) sur d'autres bases de cette forme est (puisque $(G : G^{(1)}) = p^{n_o+1}$)

$$p^{(t-n_o-1)(n_o+1)}(p^{n_o+1} - 1)(p^{n_o+1} - p) \ldots (p^{n_o+1} - p^{n_o}).$$

Une telle application conserve F si, et seulement si, à la fois :

a. T_2 est appliqué sur une autre base de $F/G^{(i)}$, (mod $F \cap G^{(1)}/G^{(i)}$) ;

b. $t_i F \to t_i' F$ $(i = I, 2, \ldots, \nu)$ engendre un automorphisme de G/F.

Puisque le rang de $F/F \cap G^{(1)}$ est $n_o + 1 - \nu$, et puisque

$$(F \cap G^{(1)} : G^{(i)}) = p^{t-m-n_o-1+\nu},$$

le nombre d'applications de T_2, satisfaisant à la condition a., est

$$p^{(t-m-n_o-1+\nu)(n_o+1-\nu)}(p^{n_o+1-\nu} - 1)(p^{n_o+1-\nu} - p) \ldots (p^{n_o+1-\nu} - p^{n_o-\nu})$$
$$= p^{(t-m-n_o-1)(n_o+1-\nu)}(p^{n_o+1} - p^\nu)(p^{n_o+1} - p^{\nu-1}) \ldots (p^{n_o+1} - p^{n_o}).$$

Si l'application $t_i F \to t_i^F$ $(i = 1, 2, \dots, \nu)$ est fixée, chaque t_i' peut encore prendre $(F : G^{(1)}) = p^{t-m}$ valeurs, et l'application $t_i \to t_i'$ peut prendre $p^{(t-m)\nu}$ valeurs. Ainsi, en tout, il y a $\alpha p^{(t-m)\nu}$ applications de T_1, satisfaisant à la condition b.

Finalement, il y a

$$\alpha p^{(t-m-n_o-1+\nu)(n_o+1)} (p^{n_o+1} - p^{\nu})(p^{n_o+1} - p^{\nu+1}) \dots (p^{n_o+1} - p^{n_o})$$

applications $t_i \to t_i'$ conservant F. Donc, le nombre des groupes F' distincts, égal au quotient par le nombre précédent de

$$p^{(t-n_o-1)(n_o+1)} (p^{n_o+1} - 1)(p^{n_o+1} - p) \dots (p^{n_o+1} - p^{n_o}),$$

est bien égal à l'expression de l'énoncé.

C.Q.F.D.

Le travail de Schafarevitch contient encore une deuxième partie, où il construit une théorie analogue pour les p-extensions non-ramifiées des corps de fonctions algébriques sur un champ de Galois. En effet, dans ce cas, $G_{k'/k}$ est un groupe abélien d'exposant p et d'un certain rang fini ν (WITT, HASSE). SCHAFAREVITCH démontre que, si K/k est une extension d'un degré fini $n = (K : k)$, le rang ν de $G_{K'/K}$ est $1 + (\nu - 1)n$, ce qui suffit évidemment, pour construire une théorie, semblable à la précédente, pour ce cas. Un exposé détaillé de cette théorie sortirait des cadres de cette conférence.

5. Théorie de Krasner.

Dans cette théorie, k étant un corps valué complet, une extension séparable K/k de degré fini $n = (K : k)$ est caractérisée par l'ensemble $\Sigma_{K/k}$ des polynômes normés définissant des surextensions K'/k de K/k, ou par des parties caractéristiques de cet ensemble, telles l'ensemble $S_{K/k}$ des polynômes normés définissant K/k, celui $S_{K/k}^{(\varepsilon)}$ des polynômes $f \in S_{K/k}$ à coefficients entiers et tels que la valuation $|\delta_f|$ de leur différente δ_f soit $\geq |\delta_{K/k}|(1 - \varepsilon)$, où $\delta_{K/k}$ est la différente arithémtique de K/k (Je rappelle que la différente d'un polynôme normé irréductible dans un corps valué complet (et, également, celle δ_α de son zéro α) est l'idéal, défini par $f'(\alpha)$ (cet idéal ne dépend pas du choix de α) ; et que la différente arithmétique de K/k est le p.g.c.d. des δ_α, α parcourant les entiers de K), et, dans le cas où k est discrètement valué, l'ensemble $S_{K/k}^{(d)}$ des $f \in S_{K/k}$ à coefficients entiers et tels que

$\delta_f = \delta_{K/k}$.

En vertu du principe indiqué dans l'alinéa 2, si $k(\alpha) = K$ et si d_α est le minimum de la distance de α à ses conjugués (par rapport à k) , l'ensemble $\mathfrak{K}(K)$ des $\beta \in \mathfrak{K}$ tels que $k(\beta) \supseteq K$ contient le cercle (non-circonférencié) de centre α et de rayon d_α . Sauf si le corps résiduel r de k est, en un certain sens, "trop proche" de sa fermeture algébrique (et il ne l'est pas quand k est localement compact), la réciproque de ce principe, qui dit que, sur la circonférence $|\beta - \alpha| = d_\alpha$ de $\mathfrak{K}$, il existe des β tels que $k(\beta)$ ne contienne aucune extension conjuguée de K/k , a lieu aussi.

$R(f , g)$ étant le résultant de deux polynômes $f(x)$ et $g(x)$, et s , t étant leurs degrés, organisons l'ensemble S_k des polynômes normés irréductibles de k en un espace ultramétrique (c'est-à-dire en un espace métrique, où a lieu l'inégalité triangulaire renforcée : $d(a , c) \leq \mathrm{Max}(d(a , b) , d(b , c))$.), en posant, pour les f , $g \in S_k$,

$$d(f , g) = |R(f , g)^{n:st}| = |f(\beta)^{n:s}| = |g(\alpha)^{n:t}| ,$$

où α , β sont des zéros quelconques des f , g . Il est clair, en vertu de l'alinéa 2, que pour un f fixé, $d(f , g)$ ne dépend que du minimum de la distance entre les zéros de f et ceux de g , et en est une fonction croissante. Ainsi, l'application

$$(T) \qquad \beta \longrightarrow f_{\beta/k}(x)$$

(où $f_{\beta/k}(x)$ est le polynôme minimal de β par rapport à k) applique, d'une manière monotone, les cercles de $\mathfrak{K}$ de centre α sur les cercles de S_k de centre $f = f_{\alpha/k}(x)$. Et deux cercles de $\mathfrak{K}$ d'un même rayon sont appliqués sur un même cercle de S_k si, et seulement si un d'eux contient un conjugué (par rapport à k) du centre de l'autre. Si $k(\alpha) = K$ (donc $s = n$ et $d(f, g) = |f(\beta)|$) , et si le rayon ρ d'un cercle C de centre α dans $\mathfrak{K}$ est $\leq d_\alpha$, le rayon de son image par T est visiblement (voir l'alinéa 2) $\rho' = |\delta_\alpha| \rho$. Ainsi, le cercle (non-circonférencié) de centre $f = f_{\alpha/k}$ et de rayon $\rho_{\alpha/k} = |\delta_\alpha| d_\alpha$ est le plus grand cercle de ce centre dans S_k contenu dans $\Sigma_{K/k}$, quand la réciproque du principe de l'alinéa 2 a lieu (et, en particulier, quand k est localement compact). Si $d_{K/k} = \mathrm{Sup}\, d_\alpha$, α parcourant les entiers de K , on montre facilement que, quand $|\delta_\alpha| \longrightarrow |\delta_{K/k}|$, on a aussi $d_\alpha \longrightarrow d_{K/k}$. Par suite, f parcourant les polynômes à coefficients entiers de $S_{K/k}$, la borne supérieure $\rho_{K/k}$ du rayon ρ_f du plus grand cercle de centre f dans S_k

contenu dans $\Sigma_{K/k}$ est $|\delta_{K/k}|d_{K/k}$. C'est cette borne supérieure qui généralise la valuation du conducteur $|f_{K/k}|$, et coïncide avec elle dans le cas des extensions abéliennes des corps $\mathfrak{P}$-adiques. Soit $S_k^{(n)}$ le sous-espace de S_k, formé des $f \in S_k$ de degré n. Puisque, pour tout $\eta > 0$, il existe un $\varepsilon > 0$ tel que, si $|\delta_\alpha| \geq |\delta_{K/k}|(1-\varepsilon)$ on a $d_\alpha \geq d_{K/k}(1-\eta)$. On voit facilement que, pour un tel ε, $S_{K/k}^{(\varepsilon)}$ est une réunion de cercles du sous-espace $S_k^{(n)}$ de S_k de rayon fixe $\rho_{K/k}(1-\eta)$. En particulier, si k est discrètement valué, $S_{K/k}^{(d)}$ est une réunion de cercles non-circonférenciés de $S_k^{(n)}$ de rayon $\rho_{K/k}$, ou de cercles circonférenciés de tout rayon $\rho' < \rho_{K/k}$. Quand k est localement compact, c'est une réunion d'un nombre fini de ces cercles, et l'extension K/k est, ainsi, caractérisé d'une manière finie.

La structure métrique de $S_{K/k}$ (à savoir, les intersections de $S_{K/k}$ avec les circonférences de différents rayons et de centres $f \in S_{K/k}$) permet, dans le cas galoisien, de déterminer les nombres de ramification de K/k en α (ou, ce qui revient au même, les distances possibles entre α et ses conjugués) et la structure des quotients des groupes de ramification successifs de K/k en α.

Par un passage à la limite, elle donne donc, pour K/k, les objets analogues de la théorie de la ramification intrinsèque. Ainsi, la structure métrique de $S_{K/k}$ fournit des renseignements assez précis sur le groupe de Galois $G_{K/k}$ de K/k (sans, toutefois, en permettre la détermination complète) et sur les invariants arithmétiques de K/k, qui lui sont liés. Dans le cas non-galoisien, les renseignements analogues (et quelques autres, qui sont triviaux dans le cas galoisien) sont fournis, d'une manière moins directe, par la structure métrique de $\Sigma_{K/k}$.

Soit $\rho < d_{K/k}$. k étant localement compact, l'ensemble $K^{(d)}$ des $\alpha \in K$ tels que $\delta_\alpha = \delta_{K/k}$ est une réunion finie de cercles de rayon ρ (c'est-à-dire de classes modulo une certaine puissance de l'idéal premier $\mathfrak{P}$ de K), dont le nombre, facilement calculable, $\nu_\rho(k, f, e)$ ne dépend quand ρ est fixé que du corps de base k et des degré résiduel f et ordre de ramification e de K/k. Le rayon ρ de chacun de ces cercles C étant inférieur au minimum de la distance entre son centre et ses conjugués, le nombre des cercles considérés, conjugués de C, est égal au nombre des automorphismes de K/k ; ce nombre est $n : \ell_{K/k}$, où $\ell_{K/k}$ est le nombre des corps conjugués distincts de K/k. Par suite, l'image $S_{K/k}^{(d)}$ de $K^{(d)}$ par T est une réunion de $\ell_{K/k}\,\nu_\rho(k, f, e)n^{-1}$ cercles de $S_k^{(n)}$ de rayon $\rho' = |\delta_{K/k}|\rho$. Ce fait a des multiples conséquences.

a. - Le quotient par le nombre des cercles de rayon ρ', composant $S^{(d)}_{K/k}$, du $\nu_\rho(k, f, e)$ est un indice, fourni par la structure métrique de $S^{(d)}_{K/k}$, égal à $n : \ell_{K/k}$. Il est donc égal à n si, et seulement si K/k est galoisienne. Un indice analogue $\leq n$ (quoique non toujours $= n : \ell_{K/k}$) peut être formé, à partir de la structure métrique de $S_{K/k}$, même si k n'est pas localement compact, et il est aussi égal à n si, et seulement si K/k est galoisienne. Ceci constitue une loi de limitation pour les extensions galoisiennes.

b. - Soit $U_{K/k}$ l'intersection de $H_{K/k}$ avec le groupe $\tilde{U}$ des unités de k : Si l'on applique tout $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ sur son dernier coefficient a_n, un cercle de rayon ρ' dans $S^{(n)}_k$ s'applique sur un cercle de même rayon dans k, et $S^{(d)}_{K/k}$ s'applique sur $U_{K/k}$. Vu la structure de $S^{(d)}_{K/k}$, il est facile de prouver que $(\tilde{U} : U_{K/k})$ ne dépasse pas l'indice précédemment introduit, et, en particulier, si K/k est complètement ramifiée, ne dépasse pas $n = e$. La 1ère inégalité fondamentale de la théorie locale des corps de classes en est une conséquence immédiate. Par suite (voir l'exposé de SAMUEL [12]) la théorie locale abélienne s'obtient à partir de la présente théorie, en la combinant avec la théorie hochschildienne de cohomologie de $G_{K/k}$ dans K, qui s'applique aux extensions de tout corps de base k.

c. - Considérons les extensions K/k de degré n et de différence δ fixes. Le nombre des cercles de rayon $\rho' = |\delta| \rho$ de $S^{(d)}_{K/k}$, égal à $\ell_{K/k}\, \nu_\rho(k, f, e) n^{-1}$, est proportionnel au nombre des corps conjugués distincts de K/K. Ainsi, il y a une "densité" fixe $\nu_\rho(k, f, e) n^{-1}$ de ces cercles par chaque corps de degré n et de différente δ sur k (Ceci constitue un analogue local des "lois de densités" de Kronecker et de Frobenius). Il est facile de calculer le nombre des cercles de rayon ρ', qui composent l'ensemble des polynômes à coefficients entiers $f \in S_k$ de degré n et de différente δ, définissant les extensions de même différente, ou qui composent des ensembles plus fins, où l'extension, définie par f, a, en plus, certains autres invariants arithmétiques fixés. En divisant ces nombres par $\nu_\rho(k, f, e) n^{-1}$, on obtient le nombre des surcorps $K \subset \mathfrak{K}$ de k tels que K/k ait le degré n et la différente δ, et ait, éventuellement, d'autres invariants arithmétiques fixés. Comme certains types d'extensions des corps valués complets : extensions primitives, extensions métagaloisiennes (c'est-à-dire obtenues par une suite d'extensions galoisiennes successives), peuvent se caractériser par de tels invariants arithmétiques, leur nombre se calcule également. Enfin, si k est un corps de nombres $\mathfrak{P}$-adiques, le nombre (qui

est fini) de ses surcorps $K \subset \mathfrak{K}$ de degré n sur k se calcule par la sommation sur les valeurs possibles de δ .

Voici le nombre des surcorps, complètement ramifiés par rapport à k , $K \subset \mathfrak{K}$ de k de degré n et de différente δ : soient $n = hp^m$, $h \not\equiv 0 \pmod{p}$, P le nombre d'éléments du corps résiduel r de k , E l'ordre de ramification absolu de K , $\mathfrak{p}$ l'idéal premier de k , $\mathfrak{P}$ celui de K . Alors (résultat dû à ORE), δ peut se représenter et d'une seule manière, sous la forme $\mathfrak{p}^s \mathfrak{P}^{j-1}$, où s et j satisfont aux conditions : $s \leq m$; si $s \neq m$, on a $j \equiv 0 \pmod{p^s}$, mais $j \not\equiv 0 \pmod{p^{s+1}}$; $0 \leq j \leq (m-s)E$. Ceci posé, si ξ est la partie entière $[j : E]$ de $j : E$, le nombre en question est :

$$n \lambda_s P^{\frac{E}{P} + \frac{E}{P^2} + \ldots + \frac{E}{P^{s+\xi}} + \left[\frac{j - \xi E}{P^{s+\xi+1}}\right]} ,$$

où $\lambda_s = P - 1$ ou 1 , selon que $s < m$ ou $s = m$.

6. Comparaison de deux théories. Perpectives d'avenir. Conclusion.

La théorie de Schafarevitch fournit, dans le cas $\sigma = 0$, une description complète du groupe de Galois de la p-extension maximale d'un corps $\mathfrak{P}$-adique k , donc une description algébrique complète de l'ensemble des p-extensions de k (et de leurs sous-extensions non-galoisiennes). Il est à présumer que cette théorie pourra se généraliser au cas $\sigma \neq 0$ et, peut-être, jusqu'à fournir la description du groupe de la fermeture algébrique de k .

Mais cette théorie ignore complètement le propriétés arithmétiques des extensions, dont elle décrit l'ensemble. Pour cette raison, elle ne caractérise pas ces extensions séparément. En effet, on a vu que deux sous-groupes fermés F et F' de $G = G_{\mathfrak{K}^p/k}$ tels que $G/F \simeq G/F'$ (autrement dit, tels que les extensions K/k et K'/k , qui leur appartiennent, ont leurs groupes de Galois isomorphes) peuvent s'appliquer l'une sur l'autre par un automorphisme bicontinu de G ; ainsi, les extensions correspondantes sont indistinguables dans la théorie de Schafarevitch, tandis qu'elles peuvent avoir d'autres propriétés (en particulier, propriétés arithmétiques) très différentes.

Cette théorie permet de calculer le nombre des p-extensions d'un groupe de Galois donné ; par sommation sur les p-groupes possibles d'un ordre donné, elle permettrait de calculer le nombre de sous-extensions de $\mathfrak{K}^p/k$ d'un degré donné p^t . Or, ces extensions ne sont pas autre chose que les extensions métagaloisiennes de

k de degré p^t.

Il semble difficile de généraliser cette théorie de manière à inclure les propriétés arithmétiques des extensions, et fournir non seulement une description de leur ensemble, mais la caractérisation de chacune en particulier. Toutefois, étant donné que $G^{(i)} / G^{(i+1)}$ est isomorphe au groupe $K^{(i)*}/(K^{(i)*})^{(p)}$, avec $G/G^{(1)}$ comme groupe d'opérateurs, il y a un faible espoir qu'en reliant ces deux groupes, on puisse y parvenir par une étude arithmétique du second groupe.

La théorie de Krasner fournit, par contre, caractérisation des extensions de k (quoique sans une loi d'existence suffisamment explicite) et généralise pratiquement toute la partie de la théorie locale des corps de classes, qui a trait aux propriétés arithmétiques des extensions. Dans sa partie essentielle, elle reste encore valable quand le corps de base k est un corps valué complet quelconque ; probablement, elle généralise toute la partie de la théorie classique, qui reste valable pour de tels corps de base, sans s'appliquer aux corps de base absolument quelconque (comme la théorie cohomologique de Hochschild). Par contre, elle ne fournit qu'indirectement les renseignements sur la nature algébrique et les relations algébriques des extensions caractérisés, qui ne suffisent pas à les décrire complètement. Cette théorie permet de calculer le nombre des extensions $K \subset \Omega$ de k d'un degré n, qui ont certaines propriétés arithmétiques fixés. Indirectement, elle permet de calculer le nombre de telles extensions, ayant certaines propriétés algébriques.

Il semble difficile de généraliser cette théorie, dans le cas localement compact (le seul cas où un tel espoir existe), de manière à fournir une description de $G_{K/k}$ à partir de $\Sigma_{K/k}$. Ceci reviendrait, en fait, à construire une bonne généralisation non-abélienne du symbole de Hasse, mais on ne voit guère comment y parvenir.

En conclusion, les deux théories semblent complémentaires, malgré l'existence d'un (mais d'un seul !) résultat, qui semble pouvoir s'obtenir (du moins, en principe) par chacune d'elles (détermination du nombre des extensions métagaloisiennes d'un degré n). Il semble impossible de jamais les réunir en une théorie unique, car la théorie de Schafarevitch est essentiellement à corps de base localement compact, et celle de Krasner ne l'est pas. Mais, pour pouvoir, dans le cas localement compact, couvrir le champ de l'autre, à chacune de ces théories manque une seule et même chose : une bonne généralisation non-abélienne du symbole de Hasse. En trouver une me semble être le problème actuellement le plus essentiel dans la théorie locale non-abélienne des corps de classes.

BIBLIOGRAPHIE

[1] BOURBAKI (Nicolas). - Topologie générale, Chapitres 1 et 2, 2e éd. - Paris, Hermann, 1951 (Act. scient. et ind., 1142 ; Eléments de Mathématique, 2).

[2] BOURBAKI (Nicolas). - Topologie générale, Chapitres 3 et 4, 2e éd. - Paris, Hermann, 1951 (Act. scient. et ind., 916-1143 ; Eléments de Mathématique, 3).

[3] CHEVALLEY (Claude). - Sur la théorie du corps de classes dans les corps finis et les corps locaux, J. Fac. Sc. imp. Univ. Tokyo, t. 2, 1929-1934, p. 365-474.

[4] HASSE (Helmut). - Normenresttheorie Galoisscher Zahlkörper mit Anwendungen auf Führer und Diskriminante Abelscher Zahlkörper, J. Fac. Sc. imp. Univ. Tokyo, t. 2, 1929-1934, p. 477-498.

[5] HASSE (Helmut). - Führer, Diskriminante und Verzweigungskörper relativ-Abelscher Zahlkörper, J. reine und ang. Math., t. 162, 1930, p. 169-184.

[6] HASSE (Helmut). - Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlköper, Teil II : Reziprozitätsgesetz, Jahr. Deutsch. Math. Ver., tome supplémentaire, 1930.

[7] HENSEL (Kurt). - Die multiplikative Darstellung der algebraischen Zahlen für den Bereich eines beliebigen Primteilers, J. reine und ang. Math., t. 146, 1916, p. 189-215.

[8] HOCHSCHILD (G.). - Local class field theory, Annals of Math., Series 2, t. 51, 1950, p. 331-347.

[9] KRASNER (Marc). - Sur la primitivité des corps $\mathfrak{P}$-adiques, Mathematica Cluj, t. 13, 1937, p. 72-191.

[10] KRASNER (Marc). - Quelques méthodes nouvelles dans la théorie des corps valués complets, Algèbre et Théorie des nombres [1949. Paris]. - Paris, Centre national de la Recherche scientifique, 1950 (Coll. intern. C. N. R. S., 14) ; p. 29-39.

[11] ORE (Oystein). - Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern, I., Math. Annalen, t. 96, 1927, p. 313-352 ; II., t. 97, 1927, p. 569-598.

[12] SAMUEL (Pierre). - Théorie du corps de classes local selon G. P. Hochschild, Séminaire Bourbaki, t. 3, 1950/51, n° 42.

[13] ŠAFAREVIČ (SHAFAREVITCH) (I.R.). - O p-rassjrenjjakh (On p-extensions), Recueil math. Soc. math. Moscou (Mat. Sbornik), N. S., t. 20 (62), 1947, p. 351-363.

ADDITIF

[14] KAWADA (Yukiyosi). - On the structure of the Galois group of some infinite extensions, I., J. Fac. Sc. Univ. Tokyo, t. 7, 1954-1958, p. 1-18.

[15] KRASNER (Marc). - Approximation des corps valués complets de caractéristique $p \neq 0$ par ceux de caractéristique 0 , Colloque d'algèbre supérieure [1956. Bruxelles]. - Louvain, Ceuterick, 1957 (Centre belge de Recherches mathématiques); p. 129-206 ; paragraphes 10 et 11.

[16] SKOPIN (A. I.). - p-rassirenija lokal'nogo polja, soderžaščego $\sqrt[p^M]{1}$, Doklady Akad. Nauk SSSR, t. 95, 1954, p. 29-32.

[17] SKOPIN (A. I.). - p-rassirenija local'nogo polja, soderžaščego korni stepeni p^M iz edinicy, Izv. Akad. Nauk SSSR, Série math., t. 19, 1955, p. 445-470.

[Novembre 1958]