Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Geneviève Cazes

Résultats sur la théorie des corps de classe

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 10, n° 2 (1968-1969), exp. n° G1, p. G1-G6

<http://www.numdam.org/item?id=SDPP_1968-1969__10_2_A8_0>

Groupe d'Études de
THÉORIE DES NOMBRES
Année 1968/69, n° 1, 6 p.

9 décembre 1968

RÉSULTATS SUR LA THÉORIE DES CORPS DE CLASSE

par Geneviève CAZES

Historiquement, cette théorie a d'abord essayé de résoudre, dans certains cas particuliers, le problème suivant, dit "problème du type de corps de classe" :

Etant donné un corps de base k, trouver un isomorphisme entre des "objets" définis uniquement à partir de k, et des objets définis à partir de certaines extensions K de k.

Ces théories seront différentes suivant les propriétés du corps k (local ou global par exemple), et les "objets" utilisés (théorie algébrique classique d'HILBERT, développée par TAKAGI, où les "objets" sont des idéaux ; théorie algébrique de CHEVALLEY, où ce sont des idèles ; théorie cohomologique, et des L-séries, faisant intervenir la cohomologie de groupes liés à k).

Exemples de solutions (voir plus loin les définitions) :

- Théorie locale. - k est local, et K parcourt les extensions abéliennes de k. Il y a isomorphisme entre $k^*/(N_{K/k}\, k^*)$ et $G(K/k)$.

[$N_{K/k}$ est la fonction norme de K dans k, et $G(K/k)$ le groupe de Galois de K/k.]

- Théorie globale. - k est global, et K parcourt les extensions abéliennes de k.

(a) Théorie avec idéaux : Il y a isomorphisme entre $I_k^{\mathfrak{f}}/(P_k^{\mathfrak{f}}\, NI_K^{\mathfrak{f}})$ et $G(K/k)$.

[$I_k^{\mathfrak{f}}$ désigne le groupe des idéaux de k premiers à un idéal $\mathfrak{f}$, dit le conducteur de l'extension K/k,

$P_k^{\mathfrak{f}}$ désigne le groupe des idéaux principaux (α) de k, où $\alpha \equiv 1(\mathfrak{f})$,

$NI_K^{\mathfrak{f}}$ le groupe des normes d'idéaux de K, premiers à $\mathfrak{f}$.]

De là vient le nom de "corps de classe" : à certaines classes d'idéaux de k sont associés des corps K, extensions abéliennes de k.

(b) Théorie avec idèles : Il y a isomorphisme entre $J_k/(k^*\, NJ_K)$ et $G(K/k)$.

[J_k désigne le groupe multiplicatif des idèles de k.]

(c) Théorie cohomologique : Si $G = G(K/k)$, il y a isomorphisme entre $H^q(G, \underset{\sim}{Z})$ et $H^{q+2}(G, K^*)$ si k est local, ou entre $H^q(G, \underset{\sim}{Z})$ et $H^{q+2}(G, C_K)$; si k

est global, K étant toujours une extension abélienne de k, $H^q(G, A)$ désigne le q-ième groupe de Tate, défini pour un groupe fini, G opérant sur l'anneau A, et C_K désignant le groupe de classes d'idèles de K.

1. Définitions.

(α) Corps global. - Un corps global k est, soit une extension finie de $\mathbb{Q}$, soit une extension finie de $F(t)$, où F est un corps fini et t transcendant sur F.

Nous ne nous occupons ici que du premier cas.

(β) Valuations. - Un corps global k a une infinité de valuations (i. e. un homomorphisme v du groupe multiplicatif k^* dans le groupe additif des réels, tel que $v(k^*) \neq 0$, et que la fonction $f(x) = e^{-\lambda v(x)}$, avec λ positif petit, vérifie l'inégalité triangulaire, et $v(0) = 0$).

Chaque valuation induit une topologie sur k (par la métrique $f(x - y)$) ; on considère les classes de valuations pour la relation " $v_1 \simeq v_2$ si v_1 et v_2 induisent la même topologie sur k ", qu'on notera toujours valuations pour simplifier. Ces valuations sont de divers types :

1° Les valuations non archimédiennes [telles que la métrique associée est ultramétrique. Dans chaque classe, il existe une valuation canonique dont le "groupe des valeurs", sous-groupe discret de $\mathbb{R}$, est $\mathbb{Z}$].

2° Les valuations archimédiennes, en nombre fini.

Les premières sont en correspondance biunivoque avec les idéaux premiers entiers de A, anneau des entiers de k sur $\mathbb{Z}$ (A est la fermeture intégrale de $\mathbb{Z}$ dans k, c'est un anneau de Dedekind, de corps des fractions k. Les idéaux fractionnaires de A, qui forment donc un groupe multiplicatif avec décomposition unique en facteurs premiers, sont dits idéaux du corps k). D'où un premier de k désignera indifféremment un idéal premier de A, ou la valuation canonique de la classe correspondante.

(γ) Corps local. - Pour chaque valuation v de k, k a un complété k_v local, dans lequel v se prolonge de manière unique. Un corps local est un corps, muni d'une valuation unique, complet pour la topologie associée, tel que son corps de restes, que l'on va définir, soit fini : le corps des restes est $\frac{A_v}{\mathfrak{M}_v}$, où A_v désigne l'anneau de la valuation (i. e. l'ensemble des x de k tels que $v(x) \geqslant 0$), c'est un anneau local dont l'idéal maximal $\mathfrak{M}_v$ est formé des x de k tels que

$v(x) > 0$. Les éléments inversibles de A_v sont ceux non contenus dans l'idéal maximal, c'est-à-dire ceux de valuation nulle, ils forment le groupe U_v des unités de k_v .

Un corps local est, soit $\underset{\sim}{R}$ ou $\underset{\sim}{C}$ (pour v archimédienne réelle, ou complexe), soit une extension finie de $\underset{\sim}{Q}_p$ (pour v non archimédienne). Il est localement compact.

(δ) Idèles. - Notations :

k_v^* : groupe multiplicatif des éléments non nuls de k_v ;

U_v : si v est non archimédienne, U_v est le groupe des unités de k_v , U_v est compact,

si v est archimédienne complexe, $U_v = k_v^*$,

si v est archimédienne réelle, $U_v = k_v^{*+}$.

Dans le groupe $\prod_v k_v^*$, soit le sous-groupe

$$J_k = (a) = (\ldots , a_v , \ldots) , \qquad a_v \in U_v \text{ sauf pour un nombre fini de } v ,$$

muni de la topologie suivante : Un ouvert $\mathcal{O}$ de J_k s'écrit $\prod_v \mathcal{O}_v$, avec $\mathcal{O}_v = U_v$ sauf pour un nombre fini de v , auquel cas $\mathcal{O}_v$ est un ouvert de k_v^* .

J_k est séparé, localement compact : c'est le groupe des idèles de k .

2. Théorie globale.

Le but de ce paragraphe est d'établir un isomorphisme entre un groupe quotient du groupe des idèles de k , et le groupe de Galois $G(K/k)$ de chaque extension abélienne K de k [pour la définition des extensions abéliennes, extensions galoisiennes de groupe de Galois abélien, et la décomposition des premiers, voir [2], chap. V et VI].

Idée générale. - Voici un aperçu de la démonstration donnée en [1], nous y reviendrons ultérieurement. Soient $\mathfrak{M}_k$ l'ensemble des valuations de k , et S un ensemble fini de valuations contenant les valuations archimédiennes. On définit d'abord une fonction de $\mathfrak{M}_k - S$ dans $G(K/k)$, puis on la prolonge par linéarité à l'ensemble I^S des idéaux de k premiers à l'idéal $\mathfrak{f}$ engendré par les valuations non archimédiennes de S (i. e. le groupe des idéaux engendré par les premiers de $\mathfrak{M}_k - S$). Si J_k^S désigne le sous-groupe de J_k formé des éléments dont les v-composantes, pour $v \in S$, sont des unités, on va pouvoir en déduire un homomorphisme de J_k^S dans $G(K/k)$. En effet, on a l'application ω : $J_k^S \to I^S$,

$$x = (\dots , x_v , \dots , \underbrace{u_v , \dots}_{\text{sur } S}) \longmapsto \prod_{v \notin S} v^{v(x_v)}$$

(où v désigne l'idéal premier de k associé à la valuation v), composée avec l'homomorphisme de I^S dans $G(K/k)$, elle définit un homomorphisme de J_k^S dans $G(K/k) = G$. Or on voit aisément que $J_k = \prod_{v \in S} k_v^* \times J_k^S$, et que l'image de k^* dans $\prod_{v \in S} k_v^*$ (définie par $x \longmapsto (x , x , x , \dots)$) est dense (théorème de faible approximation, [1], chap. II, § 6, lemme). Si on munit G de la topologie discrète, pour définir un homomorphisme continu de J_k dans G, qui prolonge celui de J_k^S dans G, il suffit donc de le définir sur l'image de k^*. On démontre en effet ([1], chap. VII, § 4, proposition 4.1) qu'il existe un tel homomorphisme, prenant la valeur 1 sur l'image de k^* dans J_k, donc pouvant être défini de $C_k = J_k/i(k^*)$ dans $G(K/k)$. C'est l'homomorphisme ψ d'Artin, C_k est le groupe de classes d'idèles de k.

Fonction de $\mathfrak{M}_k - S$ dans $G(K/k)$. - Nous revenons sur la construction de cette application (voir [2], chap. 6, § 3). Soient K une extension galoisienne de k, et S l'ensemble des valuations archimédiennes et des valuations ramifiées dans K. S est fini.

Soient $v \in \mathfrak{M}_k - S$, ω un premier de K au-dessus de v, et D_ω le groupe de décomposition de ω (i. e. le sous-groupe de $G(K/k)$ formé des $\sigma \in G(K/k)$, avec $\sigma\omega = \omega$).

On sait que tous les premiers au-dessus de v sont de la forme $\sigma\omega$, avec $\sigma \in G(K/k)$. Si v (qui est non ramifiée, rappelons-le) se décompose en $\omega_1 \omega_2 \cdots \omega_g$ dans K, on sait que $fg = [G(K/k)]$, où f désigne le degré de ramification de ω. On montre facilement que $D_\omega = G(K_\omega/k_v)$ avec des notations évidentes. Comme v est non ramifiée, $G(K_\omega/k_v) \simeq G(K(\omega)/k(v))$, où $k(v)$ et $K(\omega)$ sont les corps de restes de v et ω respectivement, qui sont finis. Donc (voir [2], chap. VI, § 1, ex. 3), $G(K(\omega)/k(v))$ est cyclique, avec un générateur canonique $\sigma_\omega \in G(K/k)$, appelé substitution de Frobenius. Ces éléments ne sont pas les mêmes pour les différents ω au-dessus de v ; plus précisément, on a $\sigma_{\sigma'\omega} = \sigma'^{-1} \sigma_\omega \sigma'$. Mais si l'extension est abélienne, alors $\sigma_{\sigma'\omega} = \sigma_\omega$, et on aura défini une application $F_{K/k}$ de $\mathfrak{M}_k - S$ dans $G(K/k)$.

On montre que cette application est surjective. De plus, si $\sigma = F_{K/k}(v)$ est d'ordre f dans G, alors D_ω est d'ordre f ; or f est le degré de ramification de v, et le nombre de premiers g, intervenant dans la décomposition de v,

est égal à $\frac{[G]}{f}$. Si N désigne le noyau de $F_{K/k}$ (i. e. les idéaux v pour lesquels $f = 1$, $g = [G]$, donc qui sont totalement décomposés), les idéaux qui appartiennent à la même classe suivant N se décomposent dans K de la même manière, car la valeur de $F_{K/k}(v)$ est la même. Ceci est un résultat important de la théorie. Si K est une extension galoisienne non abélienne, on n'a pas pu trouver un sous-groupe N , tel que les premiers appartenant à la même classe suivant N se décomposent de la même manière dans K .

Enoncé des résultats (voir [1], chap. VII, § 5).

(a) Pour chaque extension abélienne K de k , il y a un isomorphisme entre $J_k/(k^* N_{K/k} J_K)$ et $G(K/k)$ [ou entre $C_k/(N_{K/k} C_K)$ et $G(K/k)$, si C_k désigne le groupe des classes d'idèles de k], $N_{K/k} J_K$ désigne l'idèle de k .

(b) Pour chaque sous-groupe N ouvert d'indice fini de C_k , il existe une extension abélienne unique K/k telle que $G(K/k)$ soit isomorphe à C_k/N , avec $N = N_{K/k} C_k$ (N est le "groupe des normes" attaché au "corps de classe" K).

(c) Il y a un diagramme commutatif, si k , K , K' sont des extensions abéliennes :

$$\begin{array}{ccc} C_k/(N_{K'/k} C_{K'}) & \longrightarrow & G(K'/k) \\ \downarrow & & \downarrow \\ C_k/(N_{K/k} C_K) & \longrightarrow & G(K/k) \end{array} ,$$

qui permet de passer à la limite inverse quand K parcourt les extensions abéliennes finies de k : $\varprojlim C_k/N \simeq G(K^{ab}/k)$, où N parcourt les sous-groupes ouverts d'indice fini de C_k , et où K^{ab} désigne l'extension abélienne maximale de k . On trouve en fait $G(K^{ab}/k) \simeq C_k/D_k$, où D_k est la composante connexe de l'élément neutre dans C_k .

3. Théorie locale. Lien avec la théorie globale.

Si k est un corps local, on a des résultats analogues à (a), (b), (c), avec $k^*/(N_{K/k} K^*)$ au lieu de $C_k/(N_{K/k} C_K)$. Si k est global, pour chaque v de k , on définit, de manière évidente, des homomorphismes i_v de k_v dans J_k , et j_v de J_k dans k_v , par

$i_v(x) = (1 , \dots , 1 , x , 1 , \dots , 1 , \dots)$ et $j_v(\dots , x_v , \dots) = x_v$.

On a donc

$$k_v \underset{j_v}{\overset{i_v}{\rightleftarrows}} J_k \longrightarrow G ,$$

où ψ est l'homomorphisme d'Artin. Alors $\psi_v = \psi_0 \, i_v$ est un homomorphisme de k_v dans G, en réalité de k_v dans $G(K^v/k_v)$, où K^v est l'une des complétions K_ω de K pour ω au-dessus de v (elles sont toutes isomorphes). Ce ψ_v est l'homomorphisme local d'Artin de k_v dans $G(K^v/k_v)$.

Résultat particulier intéressant (voir [1], exercice 3). - L'extension abélienne maximale $\bar{K}$ de k, non ramifiée aux premiers non archimédiens de k, s'appelle le corps de classe de Hilbert de k. Son degré sur k est fini, et est égal au nombre de classes d'idéaux de k (i. e. les idéaux de k modulo les idéaux principaux, qui forment un groupe fini).

BIBLIOGRAPHIE

[1] Algebraic number theory. Edited by CASSELS (J. W. S.) and FRÖHLICH (A.). - London, Academic Press ; Washington, Thompson Book Company, 1967.

[2] SAMUEL (Pierre). - Théorie algébrique des nombres. - Paris, Hermann, 1967 (Collection "Méthodes". Mathématiques).

(Texte remis le 22 juillet 1969)

Mlle Geneviève CAZES
Ass. Fac. Sc. Paris
12 rue du Commandeur
75 - PARIS 14