DOMINIQUE RUYER

Extensions résolubles des corps de nombres algébriques

Séminaire N. Bourbaki, 1956, exp. nº 128, p. 305-314
<http://www.numdam.org/item?id=SB_1954-1956__3__305_0>

EXTENSIONS RÉSOLUBLES DES CORPS DE NOMBRES ALGÉBRIQUES

par Dominique RUYER

(d'après K. IWASAWA [1])

Première partie : les problèmes de plongement

1. Soit K/k une extension galoisienne finie, G un groupe fini, N un sous-groupe normal de G, φ un isomorphisme de $\Gamma = G/N$ sur le groupe de Galois $G(K/k)$. On cherche une extension galoisienne finie L/k contenant K/k, et un isomorphisme $\psi : G \to G(L/k)$, tels que le diagramme

$$\begin{array}{ccccccccc} 1 & \to & N & \longrightarrow & G & \longrightarrow & \Gamma & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\varphi} & & \\ 1 & \to & G(L/K) & \to & G(L/k) & \to & G(K/k) & \to & 1 \end{array}$$

soit commutatif. On notera par $P(K/k\ ,\ G/N\ ,\ \varphi)$ le problème, par $(L\ ,\ \psi)$ sa solution.

On utilisera dans la suite les procédés de réduction suivants

1° Si $G \to \Gamma$ se décompose en $G \to \Gamma' \to \Gamma$, il suffit de savoir résoudre les problèmes correspondant à $G \to \Gamma'$ et $\Gamma' \to \Gamma$.

2° Si on a le diagramme commutatif (φ_1 sur)

$$\begin{array}{ccc} G' & \xrightarrow{\varphi_1} & G \\ \downarrow{\scriptstyle\varphi'} & & \downarrow{\scriptstyle\varphi} \\ G(K'/k) & \longrightarrow & G(K/k) \end{array}$$

avec $K \subset K'$, on peut déduire de toute solution de $P(K'/k\ ,\ G'/N'\ ,\ \varphi')$ un solution de $P(K/k\ ,\ G/N\ ,\ \varphi)$. On peut choisir un K' contenant une extension finie séparable donnée E/k, et prendre $N' \approx N$.

Soit G un groupe fini, et soit N un sous-groupe normal de N, abélien élémentaire (c'est-à-dire d'exposant p). $\Gamma = G/N$ opère dans N par les automorphismes intérieurs. Si on choisit une base de N, on en déduit une représentation $\sigma \to \bar{A}(\sigma)$ de Γ par des matrices sur le corps Z_p. On a alors le

LEMME 1. – *Soit* $\sigma \to \bar{c}(\sigma)$ *une représentation de degré* 1 *de* Γ *dans* Z_p . *Il existe* G' *et* N' *finis tels que*

α . N' *est normal abélien élémentaire dans* G'

β. *Il existe un homomorphisme de* G' *sur* G *induisant un isomorphisme de* G'/N' *sur* G/N (on identifie alors G'/N' et G/N).

γ. *Il existe une base de* N' , *telle que la représentation* $\sigma \to \bar{B}(\sigma) = \bar{c}(\sigma)^{-1}\bar{A}(\sigma)$ *provienne d'une représentation* $B(\sigma)$ *à coefficients entiers, réduite* mod p .

Nous ne donnerons pas ici la démonstration. Voir [1].

Soit R l'algèbre de Γ sur Z_p , Γ opérant sur R par multiplication à gauche. Soit N_n le Γ-groupe, somme directe de n copies du Γ-groupe (additif) R . Si G_n est une extension de N_n par Γ, G_n est décomposé.

LEMME 2. – *Si l'extension* G *de* N *par* Γ *est décomposée, il existe, pour un entier* n *convenable, un homomorphisme* φ_1 *de* G_n *sur* G , *induisant un isomorphisme de* G_n/N_n *sur* G/N .

La démonstration est facile (voir [1]).

2. On fixe le corps de base k et un nombre premier p différent de la caractéristique de k , et on considère des problèmes $P(K/k , G/N , \varphi)$, pour lesquels N est un p-groupe.

On peut alors supposer que N est abélien élémentaire (car il existe une suite $N = M_1 \supset \dots \supset M_n = e$, M_i normal dans G , M_{i-1}/M_i abélien élémentaire) et que K contient ζ , racine primitive p-ième de l'unité.

Si on pose $\zeta^\sigma = \zeta^{\bar{c}(\sigma)}$ $(\sigma \in G(K/k)$, $\bar{c}(\sigma) \in Z_p)$, on se ramène à un problème $P(K/k , G/N , \varphi)$ tel que

α . N est abélien élémentaire d'ordre p^r

β . K contient ζ

γ. La représentation $\sigma \to \bar{c}(\sigma^{-1})\, \bar{A}(\sigma)$ de $G(K/k) = \Gamma$ provient d'une représentation $B(\sigma) = (b_{ij}(\sigma))$ à coefficients entiers, réduite mod p (Pour une base $(u_1 \dots u_2)$ de N) (on identifiera souvent $\Gamma = G/N$ et $G(K/k)$) . Soit V_K le produit direct de r copies du groupe multiplicatif K_m de K . On fait opérer Γ dans V_K par

$$\xi = (\xi_1 \dots \xi_i \dots \xi_r) \to \xi^\sigma = (\dots \prod_{j=1}^{r} \xi_j^{b_{ij}(\sigma).\sigma} \dots)$$

Si $\chi_1 \dots \chi_r$ sont les caractères de N dans K_m définis par $\chi_i(u_i) = \zeta$, $\chi_i(u_j) = 1$ $(i \neq j)$, et si on pose, pour $u \in N$, $\chi(u) = (\chi_1(u) , \dots , \chi_r(u))$ alors $u \to \chi(u)$ est un Γ-homomorphisme de N dans V_K .

Soit alors $\sigma \to x_\sigma \in G$ un système de représentants de Γ dans G , et soit $u_{\sigma,\tau}$ le système de facteurs correspondant. Alors, $\chi_{\sigma,\tau} = \chi(u_{\sigma,\tau})$ est un 2-cocycle de Γ dans V_K .

Si L est une solution de $P(K/k , G/N , \varphi)$, on définit de même un G-groupe V_L , produit de r copies de L_m. V_K considéré comme G-groupe est sous G-groupe de V_L , c'est le groupe des éléments de V_L fixes par N .

Comme K contient ζ et que L/K est abélienne d'exposant p , la théorie de Kummer montre qu'il existe des éléments $\beta_1 \dots \beta_r$ de L , tels que $\beta_i^{u-1} = \chi_i(u)$ $(u \in N)$ et que $L = K(\beta_1 \dots \beta_r)$. Si on pose $\beta = (\beta_1 \dots \beta_r) \in V_L$, on a $\beta^{u-1} = \chi(u)$ $(u \in N)$. Si $s \in G$, $\beta^{s-1} \in V_K$. En particulier, si on pose $\gamma_\sigma = \beta^{x_\sigma - 1}$, $\gamma_\sigma \in V_K$, on a alors $\gamma_\sigma \gamma_\tau^\sigma \gamma_{\sigma\tau}^{-1} = \chi_{\sigma,\tau}$, c'est-à-dire $\chi = d\gamma$. On a $\chi^p = 1$, donc si on pose $\delta = \gamma^p$, on a $d\delta = 1$. Si on pose $\alpha = \beta^p = (\alpha_1 \dots \alpha_r)$, $\alpha_i = \beta_i^p$, on a $\alpha^{u-1} = 1$ pour tout $u \in N$, donc $\alpha \in V_K$. Enfin, on a $\delta_\sigma = \alpha^{\sigma - 1}$, donc $\delta = d\alpha$.

Comme $\beta_1 \dots \beta_2$ engendrent L sur K , $\alpha_1 \dots \alpha_r$ sont p-indépendants dans K_m mod K_m^p .

Inversement, si $\chi , \gamma , \delta , \alpha = (\alpha_1 \dots \alpha_r)$ ont les propriétés précédentes, le corps $L = K(\beta_1 \dots \beta_r)$ $(\beta_i = \sqrt[p]{\alpha_i})$ et un isomorphisme convenable ψ de G sur $G(L/k)$ donnent une solution de $P(K/k , G/N , \varphi)$ on a donc

LEMME 3. - <u>Pour que</u> $P(K/k , G/N , \varphi)$ <u>vérifient</u> α , β , γ <u>ait une solution, il faut et il suffit qu'on ait les relations</u>

$$\chi = d\gamma \quad , \quad \gamma^p = \delta = d\alpha \quad , \quad \alpha = (\alpha_1 \dots \alpha_r)$$

<u>les</u> α_i <u>étant</u> p-<u>indépendants dans</u> K_m mod K_m^p .

Soit maintenant un problème $P(K/k , G_n/N_n , \varphi)$, G_n et N_n étant définis comme dans le lemme 2, K contenant ζ . On voit facilement que $P(K/k , G_n/N_n , \varphi)$ vérifie les conditions α , β , γ . De plus, l'extension G_n de N_n étant décomposée, on peut prendre $\chi_{\sigma,\tau} \doteq 1$. On obtient alors

LEMME 4. - Pour que $P(K/k\ ,\ G_n/N_n\ ,\ \varphi)$ ait une solution $(\zeta \in K)$, il faut et il suffit qu'il existe dans K_m n éléments $\alpha_1 \dots \alpha_n$ tels que les $\alpha_i^\sigma (1 \leq i \leq n\ ,\ \sigma \in G(K/k))$ soient p-indépendants dans K_m mod K_m^p .

Soit alors $P(K/k\ ,\ G/N\ ,\ \varphi)$ un problème dans lequel l'extension G de N est décomposée, N abélien élémentaire d'odre p^r . On peut se ramener à un problème $P(K'/k\ ,\ G'/N\ ,\ \varphi')$, $K' = K(\zeta)$, l'extension G' de N étant encore décomposée. Le lemme 2 réduit finalement le dernier problème au type $P(K/k\ ,\ G_n/N_n\ ,\ \varphi'')$. La démonstration du lemme 2 montre qu'on peut prendre $n = r$. On obtient

LEMME 5. - Soit $P(K/k\ ,\ G/N\ ,\ \varphi)$, N abélien élémentaire d'ordre p^r , l'extension G de N étant décomposée. Pour que P ait une solution, il faut et il suffit qu'il existe dans K'_m $(K' = K(\zeta))$ r éléments $\alpha_1 \dots \alpha_r$ tels que les $\alpha_i^\sigma (1 \leq i \leq r\ ,\ \sigma \in G(K'/k))$ soient p-indépendants dans K'_m mod K'^p_m .

3. On considère maintenant des problèmes $P(K/k\ ,\ G/N\ ,\ \varphi)$ tels que $\zeta \in k$, et que G soit un p-groupe ($p \neq$ caractéristique k).

Il existe alors une suite de sous-groupes normaux de G

$$N = M_0 \supset \dots \supset M_n = e\ ,$$

telle que M_{i-1}/M_i soit cyclique d'ordre p . On peut donc supposer que N est cyclique d'ordre p . Les représentations $\overline{A}(\sigma)$, $\overline{c}(\sigma)$ et $\overline{B}(\sigma)$ sont alors triviales, et V_K s'identifie au Γ-groupe K_m . Le problème vérifie donc les conditions α , β , γ du paragraphe 2.

Si $\lambda = d\chi$, $\lambda^p = 1$ entraîne que $\delta = \chi^p$ est un 1-cocycle, donc $\delta = d\alpha$ puisque le premier groupe de cohomologie de Galois est nul. Si $\alpha \notin K_m^p$, le problème a une solution. Si $\alpha \in K_m^p$, l'extension G de N est décomposée, et G est produit direct. Le problème revient à trouver Z/k cyclique de degré p , telle que $K \cap Z = k$.

On dira que k est p-trivial, si $H^2(G\ ,\ K_m) = 0$ pour toute extension galoisienne K/k telle que $G = G(K/k)$ soit un p-groupe.

THÉORÈME 1. - Soit p premier et soit k tel que $\zeta \in k$. Pour que tout $P(K/k\ ,\ G/N\ ,\ \varphi)$ ait une solution, G étant un p-groupe, il faut et il suffit que

i. k soit p-trivial.

ii. k_m/k_m^p soit un groupe infini.

Suffisance. - On peut supposer N cyclique d'ordre p. Si l'extension G n'est pas décomposée, l'existence d'une solution est assurée par i., puisque χ est un cobord. Si G est produit direct, on a à construire Z/k cyclique d'ordre p, $Z \cap K = k$, ce qui est possible grâce à la théorie des Kummer, en vertu de ii.

Nécessité. - ii. résulte de la théorie de Kummer, en prenant G abélien élémentaire d'ordre p^n, n arbitrairement grand.

Soit K/k une p-extension, et soit ξ un 2-cocycle de Galois de K/k. On démontre qu'on peut supposer $\xi^p = 1$. Si on prend pour N le groupe W des racines p-ièmes de 1 dans k, et pour G l'extension de N par $G(K/k)$ définie par le système de facteurs $\xi_{\sigma,\tau}$, on peut choisir le générateur de N de sorte que χ attaché à $P(K/k, G/N, \varphi)$ coïncide avec ξ. P ayant une solution, i. est démontré.

4. On considère encore p et k comme précédemment. On démontre alors que :

THÉORÈME 2. - Tout problème $P(K/k', G/N, \varphi)$, où N est un p-groupe, a une solution pour toute extension finie séparable k' de k, si k a les propriétés :

I_p Pour toute extension K/k galoisienne finie et tout $n \geqslant 1$, il existe $\alpha_1 \dots \alpha_n$ dans K_m tels que les α_i^σ $(1 \leq i \leq n,\ \sigma \in G(K/k))$ soient p-indépendants dans K_m mod K_m^p.

II_p Toute extension finie séparable de k est p-triviale.

Supposons d'abord que k ait les propriétés I_p et II_p. Il en est de même de toute extension finie séparable k' de k. Soit $P(K/k', G/N, \varphi)$ un problème du type du paragraphe 2. On montre que les restrictions de χ à tous les q-groupes de Sylow Γ_q de $\Gamma = G/N$ sont triviales (pour $q = p$, cela résulte du fait que le problème, restreint à Γ_p, a une solution d'après le théorème 1). Il en résulte que χ est un cobord, et par transfert de Γ_q à Γ, on obtient $\chi = d\gamma$, $\gamma^p = \delta = d\alpha$.

On peut modifier α de manière que ses composantes deviennent p-indépendantes dans K_m mod K_m^p. Le lemme 3 montre alors que $P(K/k', G/N, \varphi)$ a une solution. Pour la réciproque, supposons que tout problème du type précédent ait une solution. On prend d'abord un problème du type $P(K/k, G_n/N_n, \varphi)$. Le lemme 4 montre alors que k a la propriété I_p.

Soit k'/k finie séparable, et soit ζ un 2-cocycle d'une p-extension K'/k. Si ξ' est le 2-cocycle de $K'(\zeta)/k$, image de ξ par l'homomorphisme canonique $H(G(K'/k), K) \to H(G(K'(\zeta)/k), K'(\zeta))$, ξ' est de même ordre que ξ, donc d'ordre p^k. Mais la restriction ξ'' de ξ' au p-groupe de Sylow $G(K'(\zeta)/k'(\zeta))$ de $G(K'(\zeta)/k')$ est triviale par le théorème 1. ξ est donc trivial, et k a bien la propriété II_p.

5. On considère des problèmes $P(K/k, G/N, \varphi)$, où N est un p-groupe, k étant de caractérisatique p.

On a une théorie analogue à la précédente, avec les simplifications suivantes (on utilise les groupes additifs des corps).

a. la représentation $\overline{B}(\sigma)$ définie au paragraphe 2 peut être considérée comme représentation dans k, ce qui rend inutile la réduction du lemme 1.

b. La cohomologie de Galois dans K_a (groupe additif) est triviale.

On pose $\wp(x) = x^p - x$, $\wp(K_a) = \{\lambda^p - \lambda, \lambda \in K_a\}$

On a alors :

THÉORÈME 1'. - Soit k de caractéristique $p > 0$. Pour que tout $P(K/k, G/N, \varphi)$ ait une solution, G étant un p-groupe, il faut et il suffit que $K_a/\wp(K_a)$ soit infini.

THÉORÈME 2'. - Pour que tout $P(K/k', G/N, \varphi)$ ait une solution, N étant un p-groupe et k' une extension finie séparable de k, il faut et il suffit que k ait la propriété

I'_p Pour toute extension galoisienne finie K/k et tout $n \geq 1$, il existe n éléments $\alpha_1 \dots \alpha_n$ dans K_a, tels que les éléments α_i^σ $(1 \leq i \leq n, \sigma \in G(K/k))$ soient p-indépendants dans K_a mod $\wp(K_a)$.

Soit alors $P(K/k, G/N, \varphi)$ tel que N soit résoluble. Il existe une suite $N = M_0 \supset \dots \supset M_n = e$, M_i invariant dans G, M_{i-1}/M_i étant un p-groupe. On a alors :

THÉORÈME 3. - Pour que tout $P(K/k', G/N, \varphi)$ ait une solution pour tout k' extension séparable de k, et tout N résoluble, il faut et il suffit que k ait les propriétés I_p et II_p pour tout nombre premier différent de la caractéristique de k, et aussi la propriété I'_q si k est de caractéristique $q > 0$.

Deuxième partie : Les groupes de Galois

1. On considère des classes S de groupes finis (qu'on appellera S-groupes) telles que

α. Tout sous-groupe d'un S-groupe est un S-groupe ;

β. Tout quotient d'un S-groupe est un S-groupe ;

γ. Le produit direct de deux S-groupes est un S-groupe. On peut prendre pour S la classe des groupes finis résolubles, ou nilpotents.

On étend ensuite la notion de S-groupe, en appelant S-groupe compact tout groupe compact limite projective de S-groupes finis. Si S est la classe des groupes finis résolubles (resp. nilpotent) un S-groupe compact n'est autre qu'un groupe résoluble (resp. nilpotent) au sens de la théorie des groupes topologiques.

Soit F le groupe libre engendré par un ensemble dénombrable de générateurs $\{x_1 \dots x_n \dots\}$. Soit $\{M\}$ l'ensemble des sous-groupes normaux M de F , tels que M contienne tous les générateurs sauf un nombre fini, et que F/M soit un S-groupe fini. Soit $M_o = \bigcap_{M \in \{M\}} M$. Si on prend $\{M/M_o\}$ comme système fondamental de voisinages de l'unité dans F/M_o , le complété F(S) est un S-groupe compact, séparable et totalement discontinu, appelé la S-complétion de F .

On considère maintenant des problèmes analogues aux problèmes de plongement considérés dans la première partie.

Soit U un groupe compact totalement discontinu, et soit U un sous-groupe ouvert normal de U . Soit G un groupe fini, et soit N un sous-groupe normal de G . Soit enfin Φ un isomorphisme de G/N sur U/V .

On cherche un sous-groupe ouvert normal $W(\subset V)$ et un isomorphisme Ψ de G sur U/W , tels que le diagramme.

$$\begin{array}{ccccccccc}
1 & \to & N & \to & G & \to & G/N & \to & 1 \\
 & & \downarrow & & \downarrow \Psi & & \downarrow \Phi & & \\
1 & \to & V/W & \to & U/W & \to & U/V & \to & 1
\end{array}$$

soit commutatif. Le problème précédent est le problème de relèvement $P(U/V , G/N , \Phi)$ et le couple (W , Ψ) en est la solution.

On démontre alors (assez facilement) le :

THÉORÈME 4. - Soit S une famille de groupes finis (vérifiant $\alpha\beta\gamma$) et soit $F(S)$ la S-complétion de F. $F(S)$ est un S-groupe séparable et compact, et tout problème $P(F(S)/V, G/N, \Phi)$ a une solution pour tout S-groupe fini G. De plus, $F(S)$ est déterminé, à un isomorphisme près, par ces propriétés.

On a également le résultat suivant (qui ne caractérise pas $F(S)$).

LEMME 6. - Tout S-groupe séparable compact est un quotient de $F(S)$.

2. Un extension galoisienne K/k finie ou infinie est appelée S-extension, si $G(K/k)$ est un S-groupe (fini ou compact). L'extension composée de toutes les S-extensions finies de k dans sa fermeture algébrique Ω est la S-extension maximale Σ de k. Toute S-extension de k dans Ω est sous-extension de Σ.

Considérons alors le problème de plongement $P(K/k, G/N, \varphi)$ où G est un S-groupe fini (donc $K \subset \Sigma$) et le problème de relèvement $P(U/V, G/N, \Phi)$ où $U = G(\Sigma/k)$, tels que $V = G(\Sigma/K)$ et que le diagramme ci-contre soit commutatif.

$$\begin{tikzcd}
 & G(K/k) \arrow[d, shift right] \\
G/N \arrow[ur, "\varphi"] \arrow[dr, "\Phi"'] & U/V \arrow[u, shift right]
\end{tikzcd}$$

Il est facile de voir que toute solution de l'un donne une solution de l'autre. On en déduit :

THÉORÈME 5. - Soit k un corps, et soit S une famille de groupes vérifiant α, β, γ. Alors le groupe de Galois $G(\Sigma/k)$ de la S-extension maximale Σ de k est isomorphe à $F(S)$, si et seulement si $G(\Sigma/k)$ est séparable, et si tout problème $P(K/k, G/N, \varphi)$ a une solution pour tout S-groupe fini G.

COROLLAIRE. - Soit k un corps vérifiant les conditions du théorème 3, et tel que le groupe de Galois $G(\Sigma/k)$ de l'extension résoluble maximale de k soit séparable. Alors $G(\Sigma/k)$ est isomorphe à la complétion résoluble de F.

3. Un corps de nombres algébriques sera dit essentiellement abélien, s'il est extension abélienne d'un corps de nombres algébriques fini. Toute extension finie d'un corps essentiellement abélien est encore essentiellement abélienne.

LEMME 7. - Un corps de nombres algébriques essentiellement abélien k a la propriété I_p du théorème 2 pour tout nombre premier p : pour toute extension galoisienne finie K de k et tout $n \geq 1$, il existe n éléments $\alpha_1 \dots \alpha_n$ tels que les α_i^{σ} $(1 \leq i \leq n,\ \sigma \in G(K/k))$ soient p-indépendants dans K_m mod K_m^p.

On voit facilement qu'on peut supposer que K/k_o est l'extension composée de deux extensions disjointes k/k_o abélienne, et K_o/k_o finie, (k_o corps algébrique fini) et que $\zeta \in K$.

De plus, il suffit de démontrer que si H/K_m^p est un sous-groupe fini de K_m/K_m^p , il existe $\alpha \in K_m$ tel que les α^σ, $\sigma \in G(K/k)$, soient p-indépendants mod H .

Soient $\xi_1 \dots \xi_s$ des éléments de K_m engendrant H sur K_m^p . On peut supposer que K_o contient $\xi_1 \dots \xi_s$ et ζ .

Soit P une place finie de K_o telle que les P^σ ($\sigma \in G(K/k)$) soient distinctes P étant première avec p et les ξ_i^σ (P existe, car il existe une infinité de places de k_o complètement décomposées dans K_o). Soit E une extension finie de K_o contenue dans K , telle que $(E : K_o)$ soit une puissance de p et que P soit complètement ramifiée dans E . Si N(P) est la norme absolue de P , on sait que $(E : K_o)$ divise $N(P) - 1$. $(E : K_\sigma)$ étant borné, on le supposera maximum.

Soit Q la place (unique) de E au-dessus de P . Les Q^σ ($\sigma \in G(K/k)$) sont distinctes. Si v_σ est la valuation exponentielle normalisée correspondant à Q^σ , il existe $\alpha \neq 0$ dans E tel que $v_\sigma(\alpha^\sigma) = 1$, $v_\sigma(\alpha^\tau) = 0$ ($\sigma \neq \tau$) .

Si $\alpha^z \in H$ ($z = \sum m_\sigma \sigma$, m_σ entier), on a $\alpha^z = \xi_1^{e_1} \dots \xi_s^{e_s} \beta^p$, $\beta \in K_m$, e_i entier, et $\beta^p \in E$. Comme $\zeta \in E$, $E(\beta)/E$ est triviale ou cyclique de degré p . Dans le dernier cas, Q^σ n'est pas ramifiée dans $E(\beta)$, et v_σ se prolonge à $E(\beta)$ en gardant des valeurs entières.

Alors $v_\sigma(\alpha^z) = \sum e_i v_\sigma(\xi_i) + pv_\sigma(\beta)$. Comme $v_\sigma(\alpha^z) = m_\sigma$, et $v_\sigma(\xi_i) = 0$, on a bien $m_\sigma \equiv 0 \pmod p$.

Soit k un corps de nombres algébriques, contenant toutes les racines de l'unité. Il résulte de la théorie du corps de classes que le deuxième groupe de cohomologie de Galois de toute extension galoisienne de k est trivial. En particulier, k a la propriété II_p , du théorème 2 pour tout p .

On obtient alors

THÉORÈME 6. - Soit k_o un corps de nombres algébriques fini, k l'extension abélienne maximale de k_o , et Σ l'extension résoluble maximale de k_o . Le groupe de Galois $G(\Sigma/k)$ est isomorphe à la complétion résoluble de F .

(La théorie du corps de classes donne $G(k/k_o)$, mais on ne connait pas la structure de l'extension $G(\Sigma/k_o)$ de $G(\Sigma/k)$)

Dans le cas fonctionnel, on obtient d'une manière analogue :

THÉORÈME 7. - Soit k un corps de fonctions algébriques d'une variable sur un corps des constantes k_0 dénombrable et algébriquement fermé, et soit Σ l'extension résoluble maximale de k. Le groupe $G(\Sigma/k)$ est isomorphe à la complétion résoluble de F.

BIBLIOGRAPHIE

[1] IWASAWA (Kenkichi). - On solvable extensions of algebraic number fields, Annals of Math., Series 2, t. 58, 1953, p. 548-572.