

KLAUS POTTHOFF

Ultraproduits des groupes finis et applications à la théorie de Galois

Publications du Département de Mathématiques de Lyon, 1979, tome 16, fascicule 3-4
, p. 39-45

http://www.numdam.org/item?id=PDML_1979__16_3-4_39_0

© Université de Lyon, 1979, tous droits réservés.

L'accès aux archives de la série « Publications du Département de mathématiques de Lyon » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

ULTRAPRODUITS DES GROUPE FINIS ET APPLICATIONS A LA THEORIE DE GALOIS

par Klaus POTTHOFF

A. Robinson a démontré qu'on peut obtenir des compactifications de groupes par des ultrapuissances de groupes. M. Richter a trouvé des relations entre les limites inverses et des ultraproducts. Nous voulons prouver quelques faits sur des groupes pro-finis en les considérant comme des images homomorphes des ultraproducts des groupes finis.

Puis nous donnerons une preuve directe et canonique d'un théorème de J. Ax.

I - GROUPE PRO-FINIS

1.1. Définition. On dit qu'un groupe topologique est pro-fini si ce groupe est compact et totalement discontinu.

Les groupes pro-finis sont exactement les limites inverses des groupes finis. Par exemple, $\mathbb{Z}_p$, le groupe additif des entiers p-adiques et $\hat{\mathbb{Z}} = \prod_{p \in P} \mathbb{Z}_p$ sont des groupes pro-finis.

Soit $\mathcal{P} = (I, \leq, (G_i)_{i \in I}, \phi_{i,j})_{i \geq j}$, un système inverse des groupes finis, $\phi_{i,j}$ les épimorphismes de G_i sur G_j . Soit D un ultra-filtre sur I contenant les ensembles $\{j \mid i \leq j\}$ pour chaque $i \in I$.

Définissons

$$M_i(j) = \begin{cases} \ker \phi_{j,i}, & \text{si } j \geq i \\ \{1\}, & \text{sinon} \end{cases}$$

et

$$M_i^* = \{f/D \in \prod_{i \in I} G_i/D \mid \{j \mid f(j) \in M_i(j)\} \in D\}.$$

(On peut considérer M_i^* comme $\prod_{j \in I} M_i(j)/D$).

Soit $G_{\mathcal{P}}^* = \prod_{i \in I} G_i / D$ et $\Gamma_{\mathcal{P}} = \bigcap_{i \in I} M_i^*$.

Lorsque l'indice de $M_i(j)$ dans G_i est fini et constant, M_i^* a un indice fini dans G^* . En outre M_i^* est un sous-groupe normal de $G_{\mathcal{P}}^*$.

Les ensembles M_i^* , $i \in I$, forment un système de voisinage de l'élément neutre.

Si on considère $G_{\mathcal{P}}^*$ comme groupe topologique muni de cette topologie, on obtient le théorème suivant :

1.2. Théorème. $G_{\mathcal{P}}^*$ est quasi-compact et de dimension zéro.

Comme corollaire direct on obtient :

1.3. Corollaire. $\hat{G}_{\mathcal{P}} = \hat{G}_{\mathcal{P}} / \Gamma_{\mathcal{P}}$ est un groupe pro-fini.

On peut obtenir ce corollaire directement en prouvant le théorème suivant :

1.4. Théorème. $\hat{G}_{\mathcal{P}}$ est isomorphe (algébriquement et topologiquement) à la limite inverse $\lim_{\leftarrow} \mathcal{P}$ de $\mathcal{P}$.

On définit l'homomorphisme ϕ de $G_{\mathcal{P}}^*$ par :

$$\phi(f/D)(i) = \text{l'unique } g \in G_i \text{ avec } \{j \mid \phi_{j,i}(f(j)) = g\} \in D$$

($\lim_{\leftarrow} \mathcal{P}$ est un sous-ensemble de $\prod_{i \in I} G_i$ tel que pour chaque élément $f \in \lim_{\leftarrow} \mathcal{P}$ $\phi_{j,i}(f(j)) = f(i)$ pour $j \geq i$). Il est simple de prouver que

$$\ker \phi = \bigcap_{i \in I} M_i^* = \Gamma_{\mathcal{P}}.$$

Etant donné que chaque groupe pro-fini est une limite inverse des groupes finis, on déduit du théorème 1.4. le métacorollaire suivant :

1.5. Métacorollaire. La théorie des formules liées positives des groupes pro-finis est égale à la théorie des formules liées positives des groupes finis.

Par dualité, on peut représenter les limites directes comme sous-

structure d'un ultraproduit. Dans la deuxième partie nous voulons utiliser cette donnée et appliquer les résultats de la première partie.

II - ULTRAPRODUITS DANS LA THEORIE DES CORPS

Nous voulons donner une preuve d'un théorème de J. Ax, qui explique le fait surprenant que les corps $Q(\sigma)$ des nombres algébriques, restant invariants sous l'automorphisme σ , sont isomorphes aux nombres absolument algébriques d'un ultraproduit des corps premiers et finis.

Soit L une extension galoisienne du corps K et V_L l'ensemble des corps M tel que $K \subseteq M \subseteq L$ et que M est une extension galoisienne et finie de K .

Soit D un ultrafiltre sur V_L contenant tous les ensembles $\{M \mid M_0 \subseteq M \in V_L\}$ pour chaque $M_0 \in V_L$. Alors on peut considérer L comme sous-corps de $L^* = \prod_{M \in V_L} M/D$ par l'identification de $a \in L$ avec l'élément f/D de L^* définit par

$$f(M) = \begin{cases} a, & \text{si } a \in M \\ 0, & \text{sinon.} \end{cases}$$

Par cette identification, K devient aussi un sous-corps de L^* et on prouve directement que les éléments de L sont exactement les éléments de L^* qui sont algébriquement sur K .

Il est bien connu que le groupe galoisien $G(L/K)$ de L sur K est la limite inverse des groupes $G(M/K)$ avec $M \in V_L$. Donc $G(L/K)$ est isomorphe à une image homomorphe d'un ultraproduit $G^* = \prod_{M \in V_L} G(M/K)/D$.

On peut considérer chaque élément g/D de G^* comme un automorphisme de L^* défini par :

$$g/D (f/D) = h/D \quad \text{et} \quad h(M) = g(M) (f(M)).$$

$(g(M))$ est un automorphisme de M sur K et $f(M) \in M$.

Bien que L^* ne soit pas une extension algébrique de L , le groupe de Galois de L sur K est égal au groupe G^*/Γ , Γ étant le groupe des automorphismes qui laissent invariants les éléments de L .

On s'aperçoit que les extensions algébriques des corps sont des sous-corps des ultraproducts et que leurs groupes de Galois sont des images homomorphes des ultraproducts des groupes de Galois des extensions finies.

Soit $\hat{\mathbb{Q}}$ la fermeture algébrique de $\mathbb{Q}$, $G(\hat{\mathbb{Q}}, \mathbb{Q})$ son groupe de Galois.

En utilisant les méthodes mentionnées ci-dessus nous prouvons le théorème suivant :

2.1. Théorème (Ax [1]). Soit $\sigma \in G(\hat{\mathbb{Q}}, \mathbb{Q})$ et

$Q(\sigma) = \{a \in \hat{\mathbb{Q}} \mid \sigma(a) = a\}$. Il existe donc une suite $(p_n)_{n \in \mathbb{N}}$ des nombres premiers, telle que pour chaque ultrafiltre D non-principal les corps $\text{Abs}(\prod_{p \in D} F_{p_n/D})$, celui-ci étant le corps des nombres absolument algébriques de l'ultraproduit $\prod_{n \in \mathbb{N}} F_{p_n/D}$ des corps premiers, est isomorphe à $Q(\sigma)$.

Comme M. Ax nous supposons le résultat suivant :

(*) Soit L une extension cyclique et finie du corps K , K étant une extension finie de $\mathbb{Q}$. Il existe donc un ensemble infini des nombres premiers p et des idéaux γ et $\mathfrak{p}$ de K resp. L tels que

- i) $\mathfrak{p} \mid \gamma(p)$,
- ii) γ est de degré 1 ($\bar{K} = F_p$),
- iii) $\mathfrak{p}$ est de degré $(L : K)$.

Soit $(a_n)_{n \in \mathbb{N}}$ une suite de nombres algébriques telle que

$Q(a_n) \subseteq Q(a_{n+1})$, $Q(a_n)$ est une extension galoisienne de $\mathbb{Q}$ et $\hat{\mathbb{Q}} = \bigcup_{n \in \mathbb{N}} Q(a_n)$.

Soit

$$L_n = Q(a_n) \text{ et } K_n = \text{Fix}_{L_n}(\sigma \mid L_n) = \{a \in L_n \mid \sigma(a) = a\}.$$

L_n est une extension cyclique et finie de K_n .

Soit p_n le plus petit nombre premier plus grand que p_{n-1}

(p_{-1} soit égal à 0) tel qu'il existe deux idéaux $\mathfrak{P}_n$ et $\mathfrak{P}'_n$ ayant la propriété (*) i) - iii).

Donc on obtient $\sigma(\mathfrak{P}) = \mathfrak{P}$ et σ définit un automorphisme $\bar{\sigma}_n$ du corps résiduel $\bar{L}_n$ de L_n sur $\bar{K}_n$ et le diagramme

$$(1) \quad \begin{array}{ccc} I(L_n) & \xrightarrow{\sigma|_{I(L_n)}} & I(L_n) \\ \downarrow \Pi & & \downarrow \Pi \\ \bar{L}_n & \xrightarrow{\bar{\sigma}_n} & \bar{L}_n \end{array}$$

est commutatif ($I(L_n)$ étant l'ensemble de nombres entiers de L_n).

Soit D un ultrafiltre non-principal sur $\mathbb{N}$ et $\tilde{\phi}$ l'injection suivante de $\tilde{\mathbb{Q}}$ dans $F = \prod_{n \in \mathbb{N}} \bar{L}_n / D$:

$$\text{Pour } a \in I(\tilde{\mathbb{Q}}) \text{ soit } \tilde{\phi}(a) = f/D \text{ avec } f(n) = \begin{cases} 0, & \text{si } a \notin L_n \\ \Pi(a), & \text{si } a \in L_n. \end{cases}$$

Soit $\bar{\sigma}^* = \prod_{n \in D} \bar{\sigma}_n / D$, c'est à dire :

$$\bar{\sigma}^*(f/D) = h/D \text{ avec } h(n) = \bar{\sigma}_n(f(n)).$$

En raison de (1), le diagramme

$$(2) \quad \begin{array}{ccc} \tilde{\mathbb{Q}} & \xrightarrow{\sigma} & \tilde{\mathbb{Q}} \\ \downarrow \tilde{\phi} & & \downarrow \tilde{\phi} \\ F & \xrightarrow{\bar{\sigma}^*} & F \end{array}$$

est commutatif.

$$\text{Alors } \text{Fix}_F(\bar{\sigma}^*) = \prod_{n \in \mathbb{N}} K_n / D = \prod_{n \in \mathbb{N}} F_{P_n} / D \text{ et par (2)}$$

$$\mathcal{Q}(\sigma) \text{ est isomorphe à } \tilde{\phi}(\tilde{\mathbb{Q}}) \cap \text{Fix}_F(\bar{\sigma}^*) = \text{Abs} \left(\prod_{n \in \mathbb{N}} F_{P_n} / D \right).$$

Remarquons que $\text{Abs} \left(\prod_{n \in \mathbb{N}} F_{p_n/D} \right)$ ne dépend pas de l'ultrafiltre D , nous supposons seulement que D est non-principal.

M. Jarden a prouvé [2] que presque pour tout σ (dans le sens de la mesure de Haar) $\mathbb{Q}(\sigma)$ est quasi-fini. De ce résultat et ceux de M. Ax on déduit le théorème suivant sur $\prod K_{n/D}$, $\prod F_{p_n/D}$ et $\mathbb{Q}(\sigma)^{\mathbb{N}/D}$:

2.2. Théorème (CH). Soit K_n , F_{p_n} , $\mathbb{Q}(\sigma)$, D comme ci-dessus. Puis pour presque tout σ $\prod_{n \in \mathbb{N}} F_{p_n/D}$, $\mathbb{Q}(\sigma)^{\mathbb{N}/D}$ et $\prod K_{n/D}$ sont isomorphes.

REFERENCES

- [1] Ax, J. The elementary theory of finite fields.
Ann. of Math. (2) 85 (1967), 161-183.
- [2] Jarden, M. Elementary statements over large algebraic fields.
TAMS 164 (1972), 67-91.
- [3] Ribes, L. Introduction to pro-finite groups and Galois cohomology.
Queens papers in pure and applied mathematics N° 24.
- [4] Richter, M. "Limites in Kategorien von Relationalsystemen".
Zeitschrift f. math. Logik und Grundle. d. Math., Bd. 17
(1971), S. 75-90.
- [5] Robinson, A. "Compactifications of groups and rings and Non-Standard-
Analysis". Note 1968.