A propos d'une version faible du problème inverse de Galois

Bruno Deschamps et François Legrand

Résumé

L'objectif de cet article est de construire des corps k qui satisfont au Problème Inverse de Galois Faible (qui énonce que, pour tout groupe fini G, il existe une extension finie séparable L/k telle que $\mathrm{Aut}(L/k) = G$), mais qui ne satisfont pas au traditionnel Problème Inverse de Galois (qui énonce lui que, pour tout groupe fini G, il existe une extension finie galoisienne L/k telle que $\mathrm{Gal}(L/k) = G$). Cette construction est obtenue, *in fine*, en montrant que la forme régulière du Problème Inverse de Galois Faible est vraie sur n'importe quel corps.

Abstract

The aim of this paper is to construct fields k which fulfill the Weak Inverse Galois Problem (stating that, for every finite group G, there exists a finite separable extension L/k such that $\mathrm{Aut}(L/k) = G$), but which do not fulfill the usual Inverse Galois Problem (stating that, for every finite group G, there exists a finite Galois extension L/k such that $\mathrm{Gal}(L/k) = G$). As a main step in our construction, we show that every field fulfills the regular version of the Weak Inverse Galois Problem.

1.— Introduction.

Le problème inverse de la théorie de Galois sur un corps k ($\mathrm{PIG}_{/k}$ en abrégé) consiste à savoir si tous les groupes finis apparaissent comme groupes de Galois sur le corps k ou non. Le problème originel de Hilbert-Noether est le cas $k = \mathbb{Q}$ et reste à ce jour une question toujours ouverte. L'approche moderne pour tenter de résoudre le $\mathrm{PIG}_{/k}$ consiste à introduire une indéterminée T et, pour un groupe fini G donné, à regarder si l'on peut construire ou non une extension finie galoisienne $E/k(T)$ de groupe de Galois G telle que E/k soit régulière (c'est-à-dire telle que k soit algébriquement clos dans E). Il s'agit du Problème Inverse de Galois Régulier sur k ($\mathrm{PIGR}_{/k}$ en abrégé), forme géométrique du Problème Inverse de Galois sur k. Nous renvoyons notamment aux livres classiques [Völ96] et [MM99] pour un vaste aperçu de ce problème, ainsi qu'à [Zyw14] pour des résultats plus récents. Il est conjecturé (voir par exemple [DD97, §2.1.1]) que le $\mathrm{PIGR}_{/k}$ est vrai pour tout corps k (ce qui équivaut en fait à dire qu'il est vrai sur tout corps premier). Si k est un corps hilbertien[1], on voit par spécialisation que l'on a $\mathrm{PIGR}_{/k} \Longrightarrow \mathrm{PIG}_{/k}$. Il est donc assez raisonnable de conjecturer que le $\mathrm{PIG}_{/k}$ soit vrai pour tout corps hilbertien k, et donc, en particulier, pour $k = \mathbb{Q}$.

En 1978, dans [FK78], E. Fried et J. Kollár ont annoncé avoir montré que tout groupe fini apparaissait comme groupe d'automorphismes d'une extension finie (non nécessairement galoisienne) de $\mathbb{Q}$. Leur preuve comportait cependant une erreur que M. Fried corrigea deux ans plus tard dans [Fri80]. Ce résultat invite naturellement à considérer la forme faible du $\mathrm{PIG}_{/k}$ suivante : pour tout groupe fini G, existe-t-il une extension finie séparable L/k telle que $\mathrm{Aut}(L/k) = G$? Dans la suite, nous appellerons cette variante le Problème Inverse de Galois Faible sur k, que nous abrègerons en $\mathrm{PIGF}_{/k}$. Depuis l'article de M. Fried évoqué ci-dessus, plusieurs avancées significatives sur ce problème ont été effectuées. La plus générale est aussi la plus récente et est due à Paran et au second auteur du présent article qui montrent dans [LP17] que le $\mathrm{PIGF}_{/k}$ admet une réponse positive dès que k est un corps hilbertien. Ce résultat généralise donc le cas $k = \mathbb{Q}$ mentionné précédemment ainsi que des travaux de Takahashi et Geyer sur ce problème[2], et vient conforter la conjecture que le $\mathrm{PIG}_{/k}$ est vrai pour tout corps hilbertien k. Il ne permet toutefois pas de mesurer l'éventuelle distance qui pourrait exister entre le PIG et son petit frère le PIGF. L'objet central de cet article est de montrer comment construire des exemples explicites de corps k (non hilbertiens) pour lesquels le $\mathrm{PIGF}_{/k}$ est vrai, mais le $\mathrm{PIG}_{/k}$ est faux.

Étant donné un corps k, on peut aussi affaiblir l'énoncé $\mathrm{PIGR}_{/k}$, en demandant seulement de réaliser tout groupe fini G comme le groupe d'automorphismes d'une extension finie séparable

[1] C'est le cas par exemple si k est un corps de nombres ou le corps des fractions rationnelles en une variable à coefficients dans un corps quelconque. Nous renvoyons à [FJ08] pour un vaste aperçu de ces corps.

[2] Nous renvoyons à [LP17, §1] pour plus de détails et des références.

$E/k(T)$ telle que E/k soit régulière. Dans la suite, nous appellerons cette variante le Problème Inverse de Galois Régulier Faible (sur k), que nous abrègerons en PIGRF$_{/k}$. A notre connaissance, le résultat connu le plus général sur ce sujet affirme que cet énoncé possède une réponse positive pour tout corps k de caractéristique nulle, cf. [Fri80].

Le premier élément important que nous présentons dans cet article est que ce résultat est en fait valable pour tout corps. Nous établissons ce fait en nous appuyant sur la preuve originelle de M. Fried et en montrant :

Théorème 1.— *Pour tout groupe fini G et tout corps k, il existe une extension finie séparable $E/k(T)$ de groupe d'automorphismes G telle que E/k soit régulière.*

En fait, nous pouvons faire en sorte que $\widetilde{E}/k$ soit régulière, où $\widetilde{E}$ désigne la clôture galoisienne de E sur $k(T)$, et nous explicitons le groupe de Galois de cette extension. Nous renvoyons au théorème 6 pour plus de détails.

Lorsque le corps de base k est hilbertien, le théorème 1 fournit par spécialisation une réponse positive au PIGF$_{/k}$, ce qui permet de retrouver le résultat principal de [LP17][3].

Pour aborder le PIGF sur d'autres corps, potentiellement non hilbertiens, nous nous intéressons ensuite à la notion de clôture d'un corps k relativement à une classe $\mathscr{C}$ de groupes finis : il s'agit du corps $k^{\mathscr{C}}$ qui est, par définition, le compositum de toutes les extensions finies galoisiennes de k dont le groupe de Galois soit un élément de $\mathscr{C}$. Le caractère potentiellement non hilbertien du corps $k^{\mathscr{C}}$ résulte du fait que, sous certaines hypothèses sur la classe $\mathscr{C}$ (cf. théorème 19), le corps $k^{\mathscr{C}}$ est $\mathscr{C}$*-clos*, c'est-à-dire qu'aucun élément non trivial de $\mathscr{C}$ ne se réalise comme groupe de Galois sur $k^{\mathscr{C}}$. Nous consacrons les sections 3 et 4 de cet article à l'étude de certaines propriétés relatives aux classes de groupes finis et à celle de l'arithmétique des clôtures associées d'un corps. Cette double étude, combinée avec le théorème 1, nous permet alors de montrer le résultat central de cet article :

Théorème 2.— *Considérons une classe $\mathscr{C}$ de groupes finis stable par passage au quotient et un corps hilbertien k de caractéristique différente de 2. S'il existe une infinité de groupes alternés n'appartenant pas à $\mathscr{C}$, alors le* PIGF$_{/L}$ *admet une réponse positive pour tout corps intermédiaire $k \subseteq L \subseteq k^{\mathscr{C}}$.*

Nous renvoyons au théorème 23 pour une version plus générale de ce théorème également valable en caractéristique 2.

Nous appliquons enfin le théorème 2 à plusieurs classes de groupes finis explicites, comme par exemple celle des groupes résolubles (cf. corollaire 24). Une conséquence notable de notre étude permet alors de montrer l'écart important qui existe entre le Problème Inverse de Galois et sa version Faible sur les corps non hilbertiens :

Théorème 3.— *Pour tout groupe fini non trivial G, il existe un corps non hilbertien k tel que le* PIGF$_{/k}$ *admette une réponse positive, mais tel que G ne se réalise pas comme groupe de Galois sur k.*

On peut en fait obtenir ce même résultat en prenant à la place de G une famille finie (et même infinie sous certaines conditions) de groupes finis non triviaux (voir corollaire 26).

Remerciements. Le second auteur de cet article bénéficie de bourses de l'Israel Science Foundation (bourses No. 693/13 et 577/15).

2.— Résolution du Problème Inverse de Galois Régulier Faible.

L'objectif de cette section est de démontrer le théorème 1 qui affirme que le PIGRF$_{/k}$ admet une réponse positive pour tout corps k. Le résultat principal de cette partie est le théorème 6 à venir.

Précisons tout d'abord quelques points de terminologie. Étant donnés un corps k de clôture algébrique $\overline{k}$ et des indéterminées $T_1, \dots, T_n$, on dira, pour une extension finie galoisienne $E/k(T_1, \dots, T_n)$ donnée, que E/k est *régulière* si $E \cap \overline{k} = k$. Dans le cas $n = 1$ (on pose alors $T_1 = T$ pour simplifier), si $E \cdot \overline{k}$ désigne le compositum de E et $\overline{k}(T)$ (dans une clôture algébrique de $k(T)$ fixée au préalable), un élément t_0 de $\mathbb{P}^1(\overline{k})$ est un *point de branchement* de $E/k(T)$ si l'idéal premier de $\overline{k}[T - t_0]$ engendré

[3] Pour tout corps hilbertien k et tout groupe fini G, la méthode utilisée dans [LP17] fournit une extension finie séparable $E/k(T)$ de groupe d'automorphismes G telle que $E \not\subseteq \overline{k}(T)$. Il s'agit certes d'une conclusion plus faible que celle du théorème 1, mais qui reste bien entendu suffisante pour donner une réponse positive au PIGF$_{/k}$ pour tout corps hilbertien k.

par $T - t_0$ est ramifié dans l'extension $E \cdot \overline{k}/\overline{k}(T)$ [4]. Dans la suite, r désignera le nombre de points de branchement de $E/k(T)$. Rappelons que r est nécessairement fini et que l'on a $r = 0$ si et seulement si $E \cdot \overline{k} = \overline{k}(T)$ (ce qui est équivalent à $E = k(T)$ si E/k est régulière). Enfin, on dira qu'un groupe fini G est *groupe de Galois régulier sur k* s'il existe une extension finie galoisienne $E/k(T)$ de groupe de Galois G telle que E/k soit régulière, et qu'une telle extension $E/k(T)$ est une *réalisation régulière de G sur k*. Le lemme classique ci-dessous, qui montre que la restriction au cas $n = 1$ dans la définition précédente n'est en fait pas nécessaire, sera utilisé à maintes reprises dans cet article.

Lemme 4.— *S'il existe un entier strictement positif n, des indéterminées $T_1, \dots, T_n$ et une extension finie galoisienne $E/k(T_1, \dots, T_n)$ de groupe de Galois G donné telle que E/k soit régulière, alors G est groupe de Galois régulier sur k.*

Preuve : La conclusion résulte essentiellement du caractère hilbertien du corps $\overline{k}(T)$, mais on a besoin ici d'une propriété un peu plus fine qui assure l'existence de bonnes spécialisations dans $k(T)$ (et non pas dans $\overline{k}(T)$). Cette propriété est classique quand k est infini, cf. par exemple [FJ08, §16.2]. Dans le cas où k est fini, nous renvoyons à la démonstration de [DL13, Lemma 4.2] pour plus de détails.

□

En toute généralité, étant donnée une extension finie galoisienne M/k de groupe de Galois G, la théorie de Galois assure que le groupe d'automorphismes $\mathrm{Aut}(L/k)$ d'une sous-extension L/k de M/k donnée s'identifie au groupe quotient $N_G(H)/H$, où $H = \mathrm{Gal}(M/L)$ et $N_G(H)$ désigne le normalisateur de H dans G. Cette propriété donne bien sûr un fil conducteur pour aborder le $\mathrm{PIGF}_{/k}$, ce qui nous mène dans la situation régulière à considérer, pour deux groupes finis G et Γ donnés, l'énoncé suivant :

$(*/G/\Gamma/k)$ *Γ est groupe de Galois régulier sur k et il existe un sous-groupe H de Γ tel que $G \cong N_\Gamma(H)/H$.*

On voit alors que :

Lemme 5.— *Pour qu'il existe une extension finie séparable $E/k(T)$ de groupe d'automorphismes G donné telle que E/k soit régulière*[5]*, il suffit que l'énoncé $(*/G/\Gamma/k)$ soit vrai pour au moins un groupe fini Γ.*

2.1.— Réalisation de $(*/G/\Gamma/k)$.

Étant donné un groupe fini G, le théorème suivant fournit plusieurs situations de groupes finis Γ pour lesquelles l'énoncé $(*/G/\Gamma/k)$ est vrai.

Théorème 6.— *Fixons un groupe fini G et un corps k de caractéristique $p \geq 0$.*

1) *Étant donnés*

- *un groupe de Galois régulier sur k, G_1, dans lequel se plonge G,*
- *un groupe fini simple non abélien, G_2, possédant une réalisation régulière sur k ayant $r \leq 2$ points de branchement, tous k-rationnels,*

il existe un entier $N \in \{1, \dots, |G_1|\}$ et un groupe Γ, extension[6] *de G_2^N par G_1, tel que $(*/G/\Gamma/k)$ soit vrai.*

2) *Étant donnés*

- *un groupe de Galois régulier sur k, G_1, dans lequel se plonge G et tel que $p \nmid 2|G_1|$,*
- *un groupe fini simple non abélien, G_2, possédant une réalisation régulière sur k ayant $r = 3$ points de branchement, tous k-rationnels,*

il existe un entier $N \in \{1, \dots, |G_1|\}$ et un groupe Γ, extension de G_2^N par G_1, tel que $(*/G/\Gamma/k)$ soit vrai.

3) *Si $p \neq 2$, étant donnés*

- *un entier strictement positif n tel que $n \notin \{1, 2, 3, 4, 6\}$ et $n \geq |G| + 2$,*
- *un entier strictement positif m tel que $m \notin \{1, 2, 3, 4, 6\}$,*

il existe un entier $N \in \{1, \dots, n!/2\}$ et un groupe Γ, extension de A_m^N par A_n, tel que $(*/G/\Gamma/k)$ soit vrai.

Remarque : Bien qu'il n'y ait aucune hypothèse explicite sur p dans le 1), il convient de remarquer que, d'après le théorème d'existence de Riemann, cette situation ne peut s'appliquer si $p = 0$.

[4] Si $t_0 = \infty$, $T - t_0$ doit être remplacé par $1/T$.

[5] Comme précédemment, $\widetilde{E}$ désigne la clôture galoisienne de E sur $k(T)$.

[6] Dans cet article, nous dirons qu'un groupe G est extension d'un groupe N par un groupe H si l'on a une suite exacte $1 \to N \to G \to H \to 1$.

Avant de détailler la preuve du théorème 6, nous indiquons comment obtenir le théorème 1 énoncé dans l'introduction.

Preuve du théorème 1 : Étant donnés un groupe fini G et un corps k, pour montrer qu'il existe une extension finie séparable $E/k(T)$ de groupe d'automorphismes G telle que E/k soit régulière, il suffit, en vertu du lemme 5, de trouver un groupe fini Γ tel que l'énoncé $(*/G/\Gamma/k)$ soit vrai.

Supposons tout d'abord que k ne soit pas de caractéristique 2. Dans ce cas, le 3) du théorème 6 montre que l'on peut prendre pour Γ une certaine extension de A_m^N par A_n, pour des entiers strictement positifs m, N et n bien choisis. Supposons maintenant que k soit de caractéristique 2. Dans ce cas, nous utilisons le 1) du théorème 6. Tout d'abord, en vertu de [Bri04, Theorem 11] et du lemme 4, on peut prendre pour G_1 le groupe A_n pour un certain entier n impair. Ensuite, grâce à [AY94b], on peut par exemple prendre pour G_2 le groupe de Mathieu M_{23}.

□

2.2.— Démonstration des 1) et 2) du théorème 6.

A partir de maintenant, on se donne deux indéterminées T et U, et $\overline{k}$ la clôture algébrique du corps k. Étant donné un groupe de Galois régulier sur k, G_1, contenant G, on se donne une réalisation régulière $L/k(T)$ de G_1 sur k. Considérons un élément $y(T)$ du sous-corps L^G de L tel que $L^G = k(T)(y(T))$.

Si G_2 désigne un groupe fini simple non abélien comme dans les 1) et 2) du théorème 6, on se donne une extension finie galoisienne $M/k(U)$ de groupe de Galois G_2, telle que M/k soit régulière et telle que $M/k(U)$ possède

- $r \leq 2$ points de branchement, tous k-rationnels (si l'on est dans le cas 1)),
- $r = 3$ points de branchement, tous k-rationnels (si l'on est dans le cas 2)).

Quitte à faire un changement de variable, on peut supposer que l'ensemble des points de branchement de l'extension $M/k(U)$ est

- $\{0\}$ si l'on est dans le cas 1) et $r = 1$,
- $\{0, \infty\}$ si l'on est dans le cas 1) et $r = 2$,
- $\{0, 1, \infty\}$ si l'on est dans le cas 2).

Considérons alors un sous-groupe maximal G_3 de G_2 et le sous-corps M^{G_3} de M. On se donne un élément primitif $x_0(U)$ de $M^{G_3}/k(U)$, que l'on peut supposer entier sur $k[U]$, et l'on note $P(U, X) \in k[U][X]$ le polynôme minimal de $x_0(U)$ sur $k(U)$. Comme l'extension M/k est régulière, le polynôme $P(U, X)$ reste irréductible sur $L^G(U)$. En particulier, le polynôme tordu $P(U - y(T), X)$ est irréductible sur $L^G(U)$. Fixons une racine $x_{y(T)}(U)$ de $P(U - y(T), X)$ et notons E le compositum de $L(U)$ et $L^G(U, x_{y(T)}(U))$. Clairement, on a $E = L(U, x_{y(T)}(U))$.

Nous déterminons maintenant le groupe d'automorphismes de l'extension $E/k(T, U)$:

Lemme 7.— *On a* $\mathrm{Aut}(E/k(T, U)) = G$.

Preuve : • Commençons par montrer que

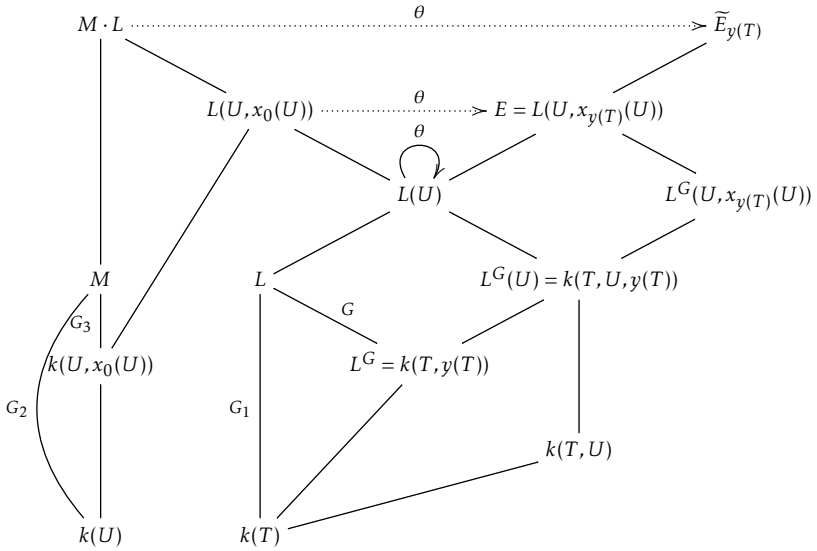
$$\mathrm{Aut}(E/L^G(U)) = G. \tag{1}$$

Par un argument de régularité déjà utilisé, le polynôme tordu $P(U - y(T), X)$ est irréductible sur $L(U)$, c'est-à-dire les corps $L(U)$ et $L^G(U, x_{y(T)}(U))$ sont linéairement disjoints sur $L^G(U)$. Comme $L(U)/L^G(U)$ est finie galoisienne de groupe de Galois G, il en est de même de $E/L^G(U, x_{y(T)}(U))$. Ainsi, pour établir (1), il suffit de montrer que tout automorphisme σ de $E/L^G(U)$ fixe $x_{y(T)}(U)$. Supposons que ce ne soit pas le cas pour un certain σ. Alors $\sigma(x_{y(T)}(U))$ est une autre racine du polynôme $P(U - y(T), X)$ contenue dans E. En particulier, $\mathrm{Aut}(E/L(U))$ n'est pas trivial.

Considérons maintenant le compositum $M \cdot L$ de M et $L(U)$. Comme l'extension M/k est régulière, la restriction res : $\mathrm{Gal}(M \cdot L/L(U)) \to \mathrm{Gal}(M/k(U))(= G_2)$ est un isomorphisme de groupes. Notons que le corps $M \cdot L$ est en fait la clôture galoisienne de $L(U, x_0(U))$ sur $L(U)$. Considérons également la clôture galoisienne $\widetilde{E}_{y(T)}$ de E sur $L(U)$ et l'automorphisme de corps $\theta \in \mathrm{Aut}(L(U)/L)$ défini par $\theta(U) = U - y(T)$. Puisque le polynôme minimal de $x_{y(T)}(U)$ sur $L(U)$ est le tordu par θ du polynôme minimal de $x_0(U)$ sur $L(U)$, on voit que θ se relève en un isomorphisme de corps $\theta : L(U, x_0(U)) \to$

$L(U, x_{y(T)}(U))$ vérifiant $\theta(x_0(U)) = x_{y(T)}(U)$. Un argument classique montre alors que θ se relève aux clôtures galoisiennes sur $L(U)$ de ces deux corps. Ainsi θ définit un isomorphisme $\theta : M \cdot L \to \widetilde{E}_{y(T)}$ qui fixe les éléments de L.

Le diagramme suivant récapitule la situation :



L'isomorphisme de corps θ permet alors de définir un isomorphisme de groupes

$$\psi_{y(T)} : \mathrm{Gal}(\widetilde{E}_{y(T)}/L(U)) \to G_2$$

en envoyant $\tau \in \mathrm{Gal}(\widetilde{E}_{y(T)}/L(U))$ sur $\mathrm{res}(\theta^{-1}\tau\theta) \in G_2$. De plus, le sous-corps $\widetilde{E}_{y(T)}^{\psi_{y(T)}^{-1}(G_3)}$ de $\widetilde{E}_{y(T)}$ fixé par $\psi_{y(T)}^{-1}(G_3)$ est égal à E. Comme G_2 est simple et G_3 est un sous-groupe maximal de G_2, on a $N_{G_2}(G_3) = G_3$. Ainsi, via $\psi_{y(T)}$, on obtient l'égalité $N_{\mathrm{Gal}(\widetilde{E}_{y(T)}/L(U))}(\mathrm{Gal}(\widetilde{E}_{y(T)}/E)) = \mathrm{Gal}(\widetilde{E}_{y(T)}/E)$. Par conséquent, $\mathrm{Aut}(E/L(U))$ est trivial, ce qui est impossible en vertu de ce qui précède.

• Pour établir le lemme, il suffit donc de montrer que

$$\mathrm{Aut}(E/L^G(U)) = \mathrm{Aut}(E/k(T, U)).$$

Il est clair que le groupe de gauche est un sous-groupe de celui de droite. Pour la réciproque, on se donne $\sigma \in \mathrm{Aut}(E/k(T, U))$ et l'on suppose que $\sigma \notin \mathrm{Aut}(E/L^G(U))$. Alors $\sigma(y(T)) \neq y(T)$ et $\sigma(x_{y(T)}(U))$ est une racine du polynôme $P(U - \sigma(y(T)), X)$. Comme précédemment, notons $\widetilde{E}_{y(T)}$ (resp. $\widetilde{E}_{\sigma(y(T))}$) le corps de décomposition sur $L(U)$ du polynôme $P(U - y(T), X)$ (resp. du polynôme $P(U - \sigma(y(T)), X)$). Par construction, l'ensemble des points de branchement de $\widetilde{E}_{y(T)}/L(U)$ (resp. de $\widetilde{E}_{\sigma(y(T))}/L(U)$) est

- $\{y(T)\}$ (resp. $\{\sigma(y(T))\}$) si l'on est dans le cas 1) et $r = 1$,
- $\{y(T), \infty\}$ (resp. $\{\sigma(y(T)), \infty\}$) si l'on est dans le cas 1) et $r = 2$,
- $\{y(T), 1 + y(T), \infty\}$ (resp. $\{\sigma(y(T)), 1 + \sigma(y(T)), \infty\}$) si l'on est dans le cas 2).

Dans chaque cas, on vérifie aisément que les extensions $\widetilde{E}_{y(T)}/L(U)$ et $\widetilde{E}_{\sigma(y(T))}/L(U)$ ont des ensembles de points de branchement différents. En particulier, les corps $\widetilde{E}_{y(T)}$ et $\widetilde{E}_{\sigma(y(T))}$ sont distincts, ce qui entraîne $L(U, \sigma(x_{y(T)}(U))) \neq L(U, x_{y(T)}(U))(= E)$. Comme σ est dans $\mathrm{Aut}(E/k(T, U))$, on obtient que le corps $L(U, \sigma(x_{y(T)}(U)))$ est strictement contenu dans E, ce qui est impossible car ces deux corps sont de degré $|G_2|/|G_3|$ sur $L(U)$.

□

Pour tout $\sigma \in \mathrm{Gal}(L(U)/k(T, U))$, notons à nouveau $\widetilde{E}_{\sigma(y(T))}$ le corps de décomposition sur $L(U)$ du polynôme $P(U - \sigma(y(T)), X)$. Comme déjà vu, l'extension $\widetilde{E}_{\sigma(y(T))}/L(U)$ est finie galoisienne de groupe de Galois G_2. Notons $\widetilde{E}$ le compositum

$$\bullet_\sigma \widetilde{E}_{\sigma(y(T))}$$

où σ parcourt le groupe $\mathrm{Gal}(L(U)/k(T,U))$. L'extension finie $\widetilde{E}/L(U)$ est galoisienne et, comme G_2 est simple, son groupe de Galois est égal à G_2^N pour un certain entier $N \in \{1,\dots,|G_1|\}$. Remarquons que le corps E construit précédemmment est contenu dans $\widetilde{E}$ puisque E est contenu dans $\widetilde{E}_{y(T)}$. Par construction, l'extension $\widetilde{E}/k(T,U)$ est galoisienne et son groupe de Galois est une certaine extension de G_2^N par G_1.

Nous démontrons maintenant que l'extension $\widetilde{E}/k$ est régulière. Par construction, il suffit de démontrer le lemme suivant :

Lemme 8.— *Étant donnés $s \geq 2$ et un s-uplet $(\sigma_1,\dots,\sigma_s)$ d'éléments de $\mathrm{Gal}(L(U)/k(T,U))$, supposons que les corps $\widetilde{E}_{\sigma_1(y(T))},\dots,\widetilde{E}_{\sigma_s(y(T))}$ soient linéairement disjoints sur $L(U)$* [7]*. Alors les compositums respectifs*

$$\widetilde{E}_{\sigma_1(y(T))}\cdot\overline{k},\dots,\widetilde{E}_{\sigma_s(y(T))}\cdot\overline{k}$$

de $\widetilde{E}_{\sigma_1(y(T))},\dots,\widetilde{E}_{\sigma_s(y(T))}$ et $\overline{k}$ sont linéairement disjoints sur le compositum $L\cdot\overline{k}(U)$ de $L(U)$ et $\overline{k}$.

Preuve : Par l'absurde, supposons qu'il existe $q \in \{2,\dots,s\}$ tels que les corps $\widetilde{E}_{\sigma_1(y(T))}\cdot\dots\cdot\widetilde{E}_{\sigma_{q-1}(y(T))}\cdot\overline{k}$ et $\widetilde{E}_{\sigma_q(y(T))}\cdot\overline{k}$ ne soient pas linéairement disjoints sur $L\cdot\overline{k}(U)$. Comme l'extension $\widetilde{E}_{\sigma_q(y(T))}\cdot\overline{k}/L\cdot\overline{k}(U)$ est de groupe de Galois G_2, qui est simple, le corps $\widetilde{E}_{\sigma_q(y(T))}\cdot\overline{k}$ est contenu dans le compositum $\widetilde{E}_{\sigma_1(y(T))}\cdot\dots\cdot\widetilde{E}_{\sigma_{q-1}(y(T))}\cdot\overline{k}$ de $\widetilde{E}_{\sigma_1(y(T))}\cdot\overline{k},\dots,\widetilde{E}_{\sigma_s(y(T))}\cdot\overline{k}$. En particulier, tout point de branchement de $\widetilde{E}_{\sigma_q(y(T))}/L(U)$ est un point de branchement de $\widetilde{E}_{\sigma_1(y(T))}\cdot\dots\cdot\widetilde{E}_{\sigma_{q-1}(y(T))}/L(U)$. Si l'on est dans le cas 1), cela entraîne que $\sigma_q(y(T)) = \sigma_i(y(T))$ pour un certain entier $i \in \{1,\dots,q-1\}$, ce qui implique l'égalité $\widetilde{E}_{\sigma_i(y(T))} = \widetilde{E}_{\sigma_q(y(T))}$. En particulier, les corps $\widetilde{E}_{\sigma_1(y(T))}\cdot\dots\cdot\widetilde{E}_{\sigma_{q-1}(y(T))}$ et $\widetilde{E}_{\sigma_q(y(T))}$ ne sont pas linéairement disjoints sur $L(U)$, ce qui est absurde. Si l'on est dans le cas 2), on obtient l'inclusion

$$\{\sigma_q(y(T)), 1+\sigma_q(y(T))\} \subseteq \bigcup_{i=1}^{q-1}\{\sigma_i(y(T)), 1+\sigma_i(y(T))\}.$$

Si $\sigma_q(y(T)) = \sigma_i(y(T))$ pour un certain entier $i \in \{1,\dots,q-1\}$, on aboutit comme précédemment à une contradiction. On a donc

$$\sigma_q(y(T)) = 1+\sigma_i(y(T))$$

pour un certain entier $i \in \{1,\dots,q-1\}$. De manière similaire, on a

$$1+\sigma_q(y(T)) = \sigma_j(y(T))$$

pour un certain entier $j \in \{1,\dots,q-1\}$. Les deux égalités précédentes entraînent alors

$$\sigma_j(y(T)) = 2+\sigma_i(y(T)),$$

c'est-à-dire

$$\sigma_j\sigma_i^{-1}(\sigma_i(y(T))) = 2+\sigma_i(y(T)).$$

Par conséquent, pour tout entier strictement positif l, on a

$$(\sigma_j\sigma_i^{-1})^l(\sigma_i(y(T))) = 2l+\sigma_i(y(T)).$$

Pour $l = |\mathrm{Gal}(L(U)/k(T,U))| = |G_1|$, on obtient

$$\sigma_i(y(T)) = 2|G_1|+\sigma_i(y(T)).$$

Ainsi, p divise $2|G_1|$, ce qui est impossible.

□

On a donc construit une extension finie galoisienne $\widetilde{E}/k(T,U)$ vérifiant les propriétés suivantes :
a) le groupe de Galois $\mathrm{Gal}(\widetilde{E}/k(T,U))$ est une certaine extension Γ de G_2^N par G_1,
b) l'extension $\widetilde{E}/k$ est régulière,
c) l'extension $\widetilde{E}/k(T,U)$ possède une sous-extension $E/k(T,U)$ telle que $\mathrm{Aut}(E/k(T,U)) = G$.

[7] au sens de la définition donnée à la page 35 de [FJo08].

D'après a), b) et le lemme 4, le groupe Γ est groupe de Galois régulier sur k. De plus, par c), Γ possède un sous-groupe H tel que $N_\Gamma(H)/H \cong G$. Par conséquent, l'énoncé $(*/G/\Gamma/k)$ est vrai.

2.3.— Démonstration du 3) du théorème 6.

Ici, on suppose $p \neq 2$ et on se donne deux entiers strictement positifs n et m tels que $n \notin \{1,2,3,4,6\}$, $m \notin \{1,2,3,4,6\}$ et $n \geq |G|+2$.

Tout d'abord, notons que, puisque $n \geq |G|+2$, le groupe fini G se plonge dans A_n. De plus, en vertu du théorème d'existence de Riemann, le groupe A_n est groupe de Galois régulier sur $\mathbb{C}$. La même conclusion est bien entendu vraie pour le groupe A_m et l'on peut faire en sorte que ce groupe possède une réalisation régulière $M/\mathbb{C}(U)$ ayant $r = 3$ points de branchement, tous étant bien sûr $\mathbb{C}$-rationnels. Quitte à faire un changement de variable, on peut supposer qu'il s'agit de 0, 1 et ∞. La même construction que précédemment fournit alors une extension finie galoisienne $\widetilde{E}/\mathbb{C}(T,U)$ vérifiant les deux propriétés suivantes :

a) le groupe de Galois $\mathrm{Gal}(\widetilde{E}/\mathbb{C}(T,U))$ est une certaine extension Γ de A_m^N par A_n (pour un certain entier $N \in \{1,\ldots,n!/2\}$),

b) l'extension $\widetilde{E}/\mathbb{C}(T,U)$ possède une sous-extension $E/\mathbb{C}(T,U)$ telle que $\mathrm{Aut}(E/\mathbb{C}(T,U)) = G$.

Par b), Γ possède un sous-groupe H tel que $N_\Gamma(H)/H \cong G$. Ainsi, pour démontrer que l'énoncé $(*/G/\Gamma/k)$ est vrai, il suffit de voir que Γ est groupe de Galois régulier sur k. Clairement, d'après a), tout facteur de composition[8] de Γ est un groupe alterné A_l avec $l \notin \{1,2,3,4,6\}$. Comme $p \neq 2$, on peut alors appliquer [Bri04, Theorem 15] pour affirmer que tout facteur de composition de Γ possède une réalisation GAR sur k. Il ne reste alors plus qu'à utiliser [FJ08, §16.9] et le lemme 4 pour conclure que Γ est groupe de Galois régulier sur k.

2.4.— Un analogue non régulier.

Nous donnons maintenant un analogue non régulier de notre construction qui, bien que n'étant pas utile pour démontrer les résultats principaux de cet article, présente un intérêt en soi.

Etant donnés un corps k et deux groupes finis G et Γ, considérons l'énoncé suivant :

$(**/G/\Gamma/k)$ *Il existe une extension finie séparable $E/k(T)$ et une extension finie galoisienne $\widetilde{E}/k(T)$ vérifiant les trois conditions suivantes :*

- $E \subseteq \widetilde{E}$ *et* $E \cdot \overline{k} \neq \overline{k}(T)$,
- $\mathrm{Gal}(\widetilde{E}/k(T)) = \Gamma$,
- $\mathrm{Aut}(E/k(T)) = G$.

Clairement, l'énoncé $(**/G/\Gamma/k)$ est vrai dans chacun des trois cas 1), 2) et 3) du théorème 6 puisque l'énoncé plus fort $(*/G/\Gamma/k)$ est alors vrai (sauf peut-être si G est trivial). Nous donnons ci-dessous davantage de conditions suffisantes sur le groupe fini Γ pour que l'énoncé $(**/G/\Gamma/k)$ soit vrai.

Théorème 9.— *Fixons un groupe fini G et un corps k de caractéristique $p \geq 0$.*

1) *Étant donnés*

- *un groupe de Galois sur k, G_1* [9]*, dans lequel se plonge G,*
- *un groupe fini simple non abélien, G_2, possédant une réalisation régulière sur k ayant $r \leq 2$ points de branchement, tous k-rationnels,*

il existe un entier $N \in \{1,\ldots,|G_1|\}$ et un groupe Γ, extension de G_2^N par G_1, tel que $(**/G/\Gamma/k)$ soit vrai.

2) *Étant donnés*

- *un groupe de Galois sur k, G_1, dans lequel se plonge G et tel que $p \nmid 2|G_1|$,*
- *un groupe fini simple non abélien, G_2, possédant une réalisation régulière sur k ayant $r = 3$ points de branchement, dont au moins un k-rationnel,*

il existe un entier $N \in \{1,\ldots,|G_1|\}$ et un groupe Γ, extension de G_2^N par G_1, tel que $(**/G/\Gamma/k)$ soit vrai.

Preuve : La démonstration est entièrement identique à celle du théorème 6, à la seule différence près suivante : au lieu de considérer une réalisation régulière $L/k(T)$ de G_1 sur k, on travaille avec

[8] On renvoie par exemple à [FJ08, §16.9] pour plus de détails sur la terminologie employée ici.

[9] c'est-à-dire G_1 est le groupe de Galois d'au moins une extension finie galoisienne de k.

une extension finie galoisienne L/k de groupe de Galois G_1. Dans chacun des deux cas 1) et 2), la construction fournit alors une extension finie séparable $E/k(U)$ et une extension finie galoisienne $\widetilde{E}/k(U)$ vérifiant les trois propriétés suivantes :

- $E \subseteq \widetilde{E}$ et $[E \cdot \overline{k} : \overline{k}(U)] = |G_2|/|G_3|$, où G_3 désigne un sous-groupe maximal de G_2 fixé au préalable,
- $\mathrm{Gal}(\widetilde{E}/k(U))$ est une certaine extension Γ de G_2^N par G_1 (pour un certain entier $N \in \{1, \ldots, |G_1|\}$),
- $\mathrm{Aut}(E/k(U)) = G$.

En particulier, l'énoncé $(**/G/\Gamma/k)$ est vrai.

□

3.— Quelques propriétés des classes de groupes finis.

Dans cette section, nous étudions quelques propriétés des classes de groupes finis, en relation avec la théorie des corps.

3.1.— Terminologie.

Rappelons tout d'abord (cf. [RZ10, §2.1]) qu'une collection non vide $\mathscr{C}$ de groupes est une *classe* si $\mathscr{C}$ est stable par isomorphismes, c'est-à-dire, si pour tout groupe $G \in \mathscr{C}$ et tout groupe G' isomorphe à G, on a $G' \in \mathscr{C}$.

Dans toute la suite de cet article, on ne considèrera que des classes de groupes finis. Pour une telle classe $\mathscr{C}$ donnée, on s'intéressera aux quatre propriétés suivantes :

(C_0) $\mathscr{C}$ est stable par sous-groupes, c'est-à-dire, pour tout groupe $G \in \mathscr{C}$ et tout sous-groupe H de G, on a $H \in \mathscr{C}$,

(C_1) $\mathscr{C}$ est stable par quotients, c'est-à-dire, pour tout groupe $G \in \mathscr{C}$ et tout sous-groupe normal H de G, on a $G/H \in \mathscr{C}$,

(C_2) $\mathscr{C}$ est stable par extensions, c'est-à-dire, pour tout groupe fini G et tout sous-groupe normal H de G tels que H et G/H soient dans $\mathscr{C}$, on a $G \in \mathscr{C}$,

(C_3) $\mathscr{C}$ est stable par produits fibrés surjectifs, c'est-à-dire, pour tout produit fibré

$$\begin{array}{ccc} & & G_1 \\ & \nearrow & \searrow^{s_1} \\ G_1 \underset{G_0}{\times} G_2 & & \longrightarrow G_0 \\ & \searrow & \nearrow_{s_2} \\ & & G_2 \end{array}$$

avec s_1 et s_2 surjectives et tel que G_1 et G_2 soient dans $\mathscr{C}$, on a $G_1 \underset{G_0}{\times} G_2 \in \mathscr{C}$.

Remarques : 1) La propriété (C_3) est équivalente au fait que, pour tout groupe fini G et tout couple (H_1, H_2) de sous-groupes normaux de G tels que G/H_1 et G/H_2 soient dans $\mathscr{C}$, on ait $G/(H_1 \cap H_2) \in \mathscr{C}$. En effet, on voit facilement que le groupe quotient $G/(H_1 \cap H_2)$ s'identifie au produit fibré surjectif $G/H_1 \underset{G/(H_1H_2)}{\times} G/H_2$.

2) La propriété (C_3) est vérifiée dès que les propriétés ($\mathrm{C}_{0,2}$) le sont.

3) Les propriétés (C_1) et (C_3) trouvent chacune une interprétation galoisienne très claire : les quotients d'un groupe de Galois correspondent aux groupes de Galois des extensions intermédiaires et le produit fibré de deux groupes de Galois sur leur intersection correspond au groupe de Galois du compositum des deux extensions associées.

Dans la continuité de la terminologie introduite dans [RZ10, §2.1] sur le sujet, nous posons :

Définition 10.— *Nous dirons de la classe $\mathscr{C}$ que c'est*

- *une "pré-formation" si elle vérifie la propriété* (C_1),
- *une "formation" si elle vérifie les propriétés* ($\mathrm{C}_{1,3}$),
- *une "formation extensive" si elle vérifie les propriétés* ($\mathrm{C}_{1,2,3}$),
- *une "pré-variété" si elle vérifie les propriétés* ($\mathrm{C}_{0,1}$),

• *une "variété extensive" si elle vérifie les propriétés* $(C_{0,1,2,3})$.

Exemples : • Les classes $\mathscr{C}(p)$ des p-groupes (p premier), $\mathscr{C}(\text{rés})$ des groupes finis résolubles, $\mathscr{C}(\text{gr})$ de tous les groupes finis et $\mathscr{C}(1)$ composée uniquement du groupe trivial sont des variétés extensives.

• Les classes $\mathscr{C}(\text{ab})$ des groupes finis abéliens et $\mathscr{C}(\text{nil})$ des groupes finis nilpotents sont à la fois des pré-variétés et des formations, mais ne sont pas des variétés extensives.

• La classe $\mathscr{C}(\text{cycl})$ des groupes cycliques est une pré-variété qui n'est pas une formation.

3.2.— Classe associée.

Nous généralisons maintenant le passage de la classe des groupes abéliens à celle des groupes résolubles.

Définition 11.— *On appelle "classe associée" à $\mathscr{C}$ la classe, notée $\widehat{\mathscr{C}}$, des groupes finis G possédant une suite de composition*

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

telle que les quotients successifs $G_1/G_0, \ldots, G_n/G_{n-1}$ soient dans $\mathscr{C}$.

Exemples : • On a $\mathscr{C}(\text{rés}) = \widehat{\mathscr{C}(\text{rés})} = \widehat{\mathscr{C}(\text{nil})} = \widehat{\mathscr{C}(\text{ab})}$.

• On a $\widehat{\mathscr{C}(\text{p})} = \mathscr{C}(\text{p})$ pour tout nombre premier p.

• Puisque tout groupe fini possède une suite de Jordan-Hölder, on voit que $\widehat{\mathscr{C}(\text{cycl})} = \mathscr{C}(\text{rés})$ et que, si $\mathscr{C}$ contient la classe $\mathscr{C}(\text{simp})$ des groupes finis simples, alors $\widehat{\mathscr{C}} = \mathscr{C}(\text{gr})$.

Nous montrons ci-dessous que certaines des propriétés précédemment évoquées se transmettent par passage à la classe associée.

Proposition 12.— 1) *Si $\mathscr{C}$ vérifie* (C_0), *alors $\widehat{\mathscr{C}}$ vérifie* (C_0).

2) *Si $\mathscr{C}$ vérifie* (C_1), *alors $\widehat{\mathscr{C}}$ vérifie* (C_1).

3) *La classe $\widehat{\mathscr{C}}$ est la plus petite classe contenant la classe $\mathscr{C}$ et vérifiant* (C_2).

4) *Si $\mathscr{C}$ vérifie* (C_0), *alors $\widehat{\mathscr{C}}$ vérifie* (C_3).

Preuve : 1) On se donne $G \in \widehat{\mathscr{C}}$ et un sous-groupe H de G. Il existe alors une suite de composition

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

de G telle que les quotients successifs $G_1/G_0, \ldots, G_n/G_{n-1}$ soient dans $\mathscr{C}$. Considérons la suite de composition

$$\{1\} = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \cdots \trianglelefteq G_{n-1} \cap H \trianglelefteq G_n \cap H = H$$

de H. Pour tout $i \in \{0, \ldots, n-1\}$, le quotient $(G_{i+1} \cap H)/(G_i \cap H)$ est isomorphe à un sous-groupe de G_{i+1}/G_i et, puisque $G_{i+1}/G_i \in \mathscr{C}$ et $\mathscr{C}$ vérifie (C_0), ce sous-groupe est un élément de $\mathscr{C}$. Ainsi $H \in \widehat{\mathscr{C}}$.

2) On se donne $G \in \widehat{\mathscr{C}}$ et un sous-groupe normal H de G. Il existe alors une suite de composition

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

de G telle que les quotients successifs $G_1/G_0, \ldots, G_n/G_{n-1}$ soient dans $\mathscr{C}$. Notons $\pi : G \to G/H$ la surjection canonique et considérons la suite de composition

$$\{\overline{1}\} = \pi(G_0) \trianglelefteq \pi(G_1) \trianglelefteq \cdots \trianglelefteq \pi(G_{n-1}) \trianglelefteq \pi(G_n) = G/H$$

de G/H. Pour tout $i \in \{0, \ldots, n-1\}$, le quotient $\pi(G_{i+1})/\pi(G_i)$ est isomorphe à un quotient de G_{i+1}/G_i et, puisque $G_{i+1}/G_i \in \mathscr{C}$ et $\mathscr{C}$ vérifie (C_1), ce quotient est un élément de $\mathscr{C}$. Ainsi $G/H \in \widehat{\mathscr{C}}$.

3) Commençons par montrer que $\widehat{\mathscr{C}}$ vérifie (C_2). Pour cela, on se donne un groupe fini G et un sous-groupe normal H de G tels que H et G/H soient dans $\widehat{\mathscr{C}}$. Il existe alors une suite de composition

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = H$$

de H telle que H_{i+1}/H_i soit dans $\mathscr{C}$ pour tout $i \in \{0, \ldots, m-1\}$, et une suite

$$H = H_m \trianglelefteq H_{m+1} \trianglelefteq \cdots \trianglelefteq H_n = G$$

telle que $H \leq H_i$ pour tout $i \in \{m,\dots,n\}$ et telle que

$$\{\overline{1}\} = H_m/H \trianglelefteq H_{m+1}/H \trianglelefteq \cdots \trianglelefteq H_n/H = G/H$$

soit une suite de composition de G/H vérifiant $(H_{i+1}/H)/(H_i/H) \in \mathscr{C}$ pour tout $i \in \{m,\dots,n-1\}$. Puisque $(H_{i+1}/H)/(H_i/H) \simeq H_{i+1}/H_i$ pour tout $i \in \{m,\dots,n-1\}$, on en déduit que

$$\{1\} = H_0 \trianglelefteq \cdots \trianglelefteq H_m = H \trianglelefteq H_{m+1} \trianglelefteq \cdots \trianglelefteq H_n = G$$

est une suite de composition de G telle que $H_{i+1}/H_i \in \mathscr{C}$ pour tout $i \in \{0,\dots,n-1\}$. Ainsi $G \in \widehat{\mathscr{C}}$. Par ailleurs, il est clair que $\mathscr{C} \subseteq \widehat{\mathscr{C}}$.

On se donne maintenant une classe $\mathscr{C}_0$ de groupes finis contenant $\mathscr{C}$ et vérifiant (C_2). Fixons un groupe fini $G \in \widehat{\mathscr{C}}$, muni d'une suite de composition

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

telle que les quotients successifs $G_1/G_0,\dots,G_n/G_{n-1}$ soient dans $\mathscr{C}$. Comme G_0 est trivial et $G_1/G_0 \in \mathscr{C}$, on voit que $G_1 \in \mathscr{C} \subseteq \mathscr{C}_0$. De plus, $G_2/G_1 \in \mathscr{C} \subseteq \mathscr{C}_0$ et $\mathscr{C}_0$ vérifie (C_2). Ainsi G_2 est un élément de $\mathscr{C}_0$. Par récurrence, on voit alors que $G_n = G$ est un élément de $\mathscr{C}_0$. Ainsi $\widehat{\mathscr{C}} \subseteq \mathscr{C}_0$.

4) Il s'agit d'une conséquence immédiate du 1) et du 3) ci-dessus, et du 2) des remarques du §3.1.

□

Corollaire 13.— *Si $\mathscr{C}$ est une pré-variété, alors $\widehat{\mathscr{C}}$ est une variété extensive.*

3.3.— Classe duale.

Nous étudions maintenant une notion capitale pour notre étude : celle de classe duale.

Définition 14.— *On appelle "classe duale" de $\mathscr{C}$ la classe, notée $\mathscr{C}^*$, des groupes finis G tels que, pour tout sous-groupe normal H de G tel que G/H soit dans $\mathscr{C}$, on ait $H = G$.*

Cette notion est intimement liée à la théorie inverse de Galois : si $\mathscr{C}$ désigne la classe des groupes finis qui n'apparaissent pas comme groupes de Galois sur un corps k fixé, on voit que, pour qu'un groupe fini G donné soit groupe de Galois sur k, il faut nécessairement que G soit élément de $\mathscr{C}^*$. L'étude de la classe duale va jouer un rôle important dans cet article, en particulier l'étude des propriétés de $\mathscr{C}^*$ qui découlent de celles de $\mathscr{C}$. Il est déjà facile de voir que le passage à la classe duale dualise certaines des opérations ensemblistes usuelles : si $\mathscr{C}_1$ et $\mathscr{C}_2$ désignent deux classes quelconques de groupes finis, alors

a) $(\mathscr{C}_1 \cup \mathscr{C}_2)^* = \mathscr{C}_1^* \cap \mathscr{C}_2^*$,

b) $\mathscr{C}_1 \subseteq \mathscr{C}_2 \Rightarrow \mathscr{C}_2^* \subseteq \mathscr{C}_1^*$,

c) $\mathscr{C}_1^* \cup \mathscr{C}_2^* \subseteq (\mathscr{C}_1 \cap \mathscr{C}_2)^*$ [10].

De manière un peu moins triviale, on a :

Proposition 15.— 1) *La classe $\mathscr{C}^*$ vérifie (C_1).*

2) *Si $\mathscr{C}$ vérifie (C_1), alors $\mathscr{C}^*$ vérifie (C_2).*

3) *On a $\mathscr{C}^* = \left(\widehat{\mathscr{C}}\right)^*$.*

Preuve : 1) On se donne un groupe fini $G \in \mathscr{C}^*$, un sous-groupe normal H de G et un sous-groupe normal V de G/H tel que $(G/H)/V \in \mathscr{C}$. Clairement, on a $V = H'/H$ pour un certain sous-groupe normal H' de G contenant H. Comme $(G/H)/V \in \mathscr{C}$ et $(G/H)/V = (G/H)/(H'/H) \simeq G/H'$, on a $G/H' \in \mathscr{C}$. Le groupe G étant dans $\mathscr{C}^*$, on obtient $G = H'$, c'est-à-dire $V = G/H$. Ainsi $G/H \in \mathscr{C}^*$.

2) On se donne un groupe fini G et un sous-groupe normal H de G tels que H et G/H soient dans $\mathscr{C}^*$. Par l'absurde, supposons que G ne soit pas dans $\mathscr{C}^*$. Il existe alors un sous-groupe normal H' de G tel que $H' \neq G$ et $G/H' \in \mathscr{C}$. S'il existe un sous-groupe normal H'' de G tel que $H' \leq H'' \neq G$, on a $G/H'' \simeq (G/H')/(H''/H')$. Comme $\mathscr{C}$ vérifie (C_1) et G/H' est dans $\mathscr{C}$, on voit que G/H'' est lui

[10] L'inclusion réciproque est fausse en général. En effet, considérons par exemple les classes $\mathscr{C}_1 = \{\{1\}, \mathbb{Z}/2\mathbb{Z}\}$ et $\mathscr{C}_2 = \{\{1\}, \mathbb{Z}/3\mathbb{Z}\}$. On a alors $\mathscr{C}_1 \cap \mathscr{C}_2 = \mathscr{C}(1)$ et donc $(\mathscr{C}_1 \cap \mathscr{C}_2)^* = \mathscr{C}(\mathrm{gr})$, alors que $\mathbb{Z}/6\mathbb{Z} \notin \mathscr{C}_1^* \cup \mathscr{C}_2^*$.

aussi dans $\mathscr{C}$. On peut donc supposer que G/H' est simple. Si H est contenu dans H', alors H'/H est un sous-groupe normal de G/H et $(G/H)/(H'/H) \cong G/H' \in \mathscr{C}$. Or G/H est un élément de $\mathscr{C}^*$ par hypothèse. On a donc $H'/H = G/H$, c'est-à-dire $H' = G$, ce qui est absurde. Si H n'est pas contenu dans H', alors HH' est un sous-groupe normal de G contenant strictement H'. Comme G/H' est simple, on a $HH' = G$. Ainsi $H/H \cap H' \simeq HH'/H' = G/H' \in \mathscr{C}$. Or H est un élément de $\mathscr{C}^*$ par hypothèse. On a donc $H \cap H' = H$, ce qui est absurde. On en déduit ainsi que G est élément de $\mathscr{C}^*$.

3) Puisque $\mathscr{C} \subseteq \widehat{\mathscr{C}}$ (cf. 3) de la proposition 12), on a $\left(\widehat{\mathscr{C}}\right)^* \subseteq \mathscr{C}^*$ d'après la propriété de dualité ensembliste b) ci-dessus. Réciproquement, on se donne un groupe fini G n'appartenant pas à $\left(\widehat{\mathscr{C}}\right)^*$. Il existe alors un sous-groupe normal H de G tel que $H \neq G$ et $G/H \in \widehat{\mathscr{C}}$. Par définition de $\widehat{\mathscr{C}}$, il existe un sous-groupe normal H' de G/H tel que $(G/H)/H' \in \mathscr{C}$, et que l'on peut de plus supposer différent de G/H puisque $G/H \neq \{1\}$. Clairement, on a $H' = H''/H$ pour un certain sous-groupe normal H'' de G contenant H. Ainsi $G/H'' \in \mathscr{C}$ et on a $H'' \neq G$. Par conséquent, $G \notin \mathscr{C}^*$.

□

3.4.— Multidualité.

Nous finissons cette section en nous intéressant aux classes duales successives de la classe $\mathscr{C}$. Commençons par l'étude de la *classe biduale* $\mathscr{C}^{**} = (\mathscr{C}^*)^*$ de $\mathscr{C}$. Dans ce qui suit, on notera $H \lhd G$ pour dire que H est un sous-groupe normal strict de G et $H \underset{\max}{\lhd} G$ pour dire que H est maximal dans l'ensemble des sous-groupes normaux stricts de G (c'est-à-dire G/H est simple).

Pour un groupe fini G donné, on a :

$$\begin{aligned} G \in \mathscr{C}^{**} &\iff \forall H \lhd G,\ G/H \notin \mathscr{C}^* \\ &\iff \forall H \lhd G,\ \exists \overline{N} \lhd G/H,\ (G/H)/\overline{N} \in \mathscr{C} \\ &\iff \forall H \lhd G,\ \exists N \lhd G \text{ tel que } H \leq N \text{ et } G/N \in \mathscr{C} \\ &\iff \forall H \underset{\max}{\lhd} G,\ G/H \in \mathscr{C}. \end{aligned}$$

De cette caractérisation découlent les deux remarques suivantes :

a) Si $\mathscr{C}$ vérifie (C_1), alors $\mathscr{C}$ est contenue dans $\mathscr{C}^{**}$. En général, l'inclusion $\mathscr{C} \subseteq \mathscr{C}^{**}$ n'est pas vraie, comme le montre l'exemple $\mathscr{C} = \{\mathbb{Z}/4\mathbb{Z}\}$.

b) Si $\mathscr{C}(\text{simp}) \subseteq \mathscr{C}$, alors $\mathscr{C}^{**} = \mathscr{C}(\text{gr})$. Cette remarque prouve en particulier que l'inclusion réciproque $\mathscr{C}^{**} \subseteq \mathscr{C}$ n'est pas vraie non plus en général.

Pour un groupe fini non trivial G donné, rappelons que le *radical de Baer* de G (cf. [Bae64]), que nous noterons $\mathrm{Rad}(G)$, est l'intersection de tous les sous-groupes normaux maximaux de G :

$$\mathrm{Rad}(G) = \bigcap_{H \underset{\max}{\lhd} G} H.$$

Nous pouvons maintenant caractériser les éléments non triviaux de $\mathscr{C}^{**}$ de la manière suivante :

Proposition 16.— *Étant donné un groupe fini non trivial G, les deux assertions*

i) $G \in \mathscr{C}^{**}$,

ii) $G/\mathrm{Rad}(G)$ *est isomorphe à un produit direct non vide de groupes finis simples appartenant à* $\mathscr{C}$,

sont équivalentes.

Preuve : Parmi les sous-groupes normaux H de G tels que $H \underset{\max}{\lhd} G$, l'on considère une famille finie $H_1, \ldots, H_n$ telle que $\mathrm{Rad}(G) = H_1 \cap \cdots \cap H_n$ et telle que $H_{i+1} \cap \cdots \cap H_n \not\subseteq H_i$ pour tout $i \in \{1, \ldots, n-1\}$.

Comme G/H_1 est simple et $K = H_2 \cap \cdots \cap H_n$ est un sous-groupe normal de G non contenu dans H_1, on a $H_1 K = G$. Ainsi, en appliquant le deuxième théorème d'isomorphisme, on a

$$|G/(H_1 \cap K)| = \frac{|H_1 K|}{|H_1 \cap K|} = \frac{|H_1||K|}{|H_1 \cap K|^2} = \frac{|H_1 K|}{|H_1|}\frac{|H_1 K|}{|K|}$$

et donc $|G/(H_1 \cap K)| = |G/H_1 \times G/K|$. Par ailleurs, le morphisme canonique $G \to G/H_1 \times G/K$ est de noyau $H_1 \cap K$, ce qui montre finalement que

$$G/\mathrm{Rad}(G) = G/(H_1 \cap K) \simeq G/H_1 \times G/K = G/H_1 \times G/(H_2 \cap \cdots \cap H_n).$$

Une récurrence immédiate montre alors que $G/\mathrm{Rad}(G) \simeq G/H_1 \times \cdots \times G/H_n$.

Venons-en maintenant à la démonstration de l'équivalence annoncée. Supposons tout d'abord que G soit dans $\mathscr{C}^{**}$. D'après ce qui précède, on a $G/\mathrm{Rad}(G) \simeq G/H_1 \times \cdots \times G/H_n$, et chaque quotient G/H_i est un groupe simple appartenant à $\mathscr{C}$, en vertu de la caractérisation des éléments de la classe biduale vue précédemment. Réciproquement, supposons que $G/\mathrm{Rad}(G)$ soit isomorphe à un produit direct $G_1 \times \cdots \times G_r$ de groupes simples appartenant à $\mathscr{C}$. Pour tout $H \overset{\max}{\lhd} G$, on a alors un épimorphisme $G_1 \times \cdots \times G_r \to G/H$. Comme les groupes $G/H, G_1, \ldots, G_r$ sont simples, cet épimorphisme fournit un isomorphisme $G_j \cong G/H$ pour un certain $j \in \{1, \ldots, r\}$. Ainsi $G/H \in \mathscr{C}$ et G est donc dans $\mathscr{C}^{**}$.

□

Définissons maintenant la *n-ième classe duale* $\mathscr{C}^{*[n]}$ de $\mathscr{C}$ par récurrence sur l'entier n, en posant $\mathscr{C}^{*[0]} = \mathscr{C}$ et, pour tout $n \geq 0$, $\mathscr{C}^{*[n+1]} = \left(\mathscr{C}^{*[n]}\right)^*$.

Nous avons alors le résultat de cyclicité des classes multiduales suivant :

Proposition 17.— 1) *On a $\mathscr{C}^* \subseteq \mathscr{C}^{***}$ et, si $\mathscr{C}$ vérifie* (C_1), *alors $\mathscr{C}^* = \mathscr{C}^{***}$.*

2) *Pour tout entier $n \geq 1$, on a $\mathscr{C}^{*[2n]} = \mathscr{C}^{**}$ et $\mathscr{C}^{*[2n+1]} = \mathscr{C}^{***}$.*

Preuve : 1) D'après le 1) de la proposition 15, la classe $\mathscr{C}^*$ vérifie (C_1) et on a donc $\mathscr{C}^* \subseteq \mathscr{C}^{***}$ en vertu de la remarque a) ci-dessus. Si $\mathscr{C}$ vérifie (C_1), alors on a $\mathscr{C} \subseteq \mathscr{C}^{**}$, et donc $\mathscr{C}^{***} \subseteq \mathscr{C}^*$ d'après la propriété de dualité ensembliste b) du §3.3.

2) Il suffit d'effectuer une récurrence sur l'entier n en appliquant le 1) et en remarquant que, d'après le 1) de la proposition 15, la classe $\mathscr{C}^{*[n]}$ vérifie (C_1) pour tout $n \geq 1$.

□

L'étude de la multidualité de la classe $\mathscr{C}$ se résume donc à la donnée de $\mathscr{C}^*$, $\mathscr{C}^{**}$ et $\mathscr{C}^{***}$ (et, si $\mathscr{C}$ vérifie (C_1), seulement à la donnée des classes duale et biduale de $\mathscr{C}$). L'exemple de la classe $\mathscr{C} = \{\{1\}, \mathbb{Z}/4\mathbb{Z}\}$ montre que $\mathscr{C}, \mathscr{C}^* \notin \{\mathscr{C}, \mathscr{C}(1), \mathscr{C}(\mathrm{gr})\}$, $\mathscr{C}^{**} = \mathscr{C}(1)$ et $\mathscr{C}^{***} = \mathscr{C}(\mathrm{gr})$ peuvent être des classes deux à deux distinctes.

4.— Arithmétique des $\mathscr{C}$-clôtures d'un corps.

On s'intéresse maintenant aux extensions galoisiennes finies à groupe de Galois dans une classe donnée. Dans toute cette section, k désigne un corps de clôture séparable $k^{\mathrm{sép}}$ et $\mathscr{C}$ une classe de groupes finis.

Définition 18.— *On appelle "$\mathscr{C}$-clôture" de k le corps, noté $k^{\mathscr{C}}$, égal au compositum (dans $k^{\mathrm{sép}}$) de toutes les extensions galoisiennes finies de k ayant un groupe de Galois élément de $\mathscr{C}$. Le corps k est dit "$\mathscr{C}$-clos" si $k = k^{\mathscr{C}}$, c'est-à-dire si k ne possède aucune extension galoisienne finie non triviale à groupe de Galois dans $\mathscr{C}$.*

4.1.— Groupes de Galois et $\mathscr{C}$-clôtures.

Si l'on prend pour $\mathscr{C}$ la classe $\mathscr{C}(\mathrm{cycl})$ ou la classe $\mathscr{C}(\mathrm{ab})$, le corps $\mathbb{Q}^{\mathscr{C}}$ est alors la traditionnelle clôture cyclotomique de $\mathbb{Q}$, souvent notée $\mathbb{Q}^{\mathrm{ab}}$. Tous les groupes abéliens finis se réalisant comme groupes de Galois sur $\mathbb{Q}$, l'on voit que, bien que $\mathbb{Q}^{\mathrm{ab}}$ soit la $\mathscr{C}(\mathrm{cycl})$-clôture de $\mathbb{Q}$, l'extension $\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}$ possède des sous-extensions finies galoisiennes sur $\mathbb{Q}$ à groupes de Galois non cycliques. Cette pathologie disparaît si l'on regarde le corps $\mathbb{Q}^{\mathrm{ab}}$ comme la $\mathscr{C}(\mathrm{ab})$-clôture de $\mathbb{Q}$. Pour autant, on peut facilement construire des extensions finies abéliennes non triviales de $\mathbb{Q}^{\mathrm{ab}}$, et $\mathbb{Q}^{\mathrm{ab}}$ n'est donc pas $\mathscr{C}(\mathrm{ab})$-clos. La $\mathscr{C}(\mathrm{rés})$-clôture de $\mathbb{Q}$, notée $\mathbb{Q}^{\mathrm{rés}}$, ne présente elle aucune de ces pathologies : les sous-extensions galoisiennes finies sur $\mathbb{Q}$ de $\mathbb{Q}^{\mathrm{rés}}$ ont toutes un groupe de Galois résoluble et aucune extension galoisienne finie non triviale de $\mathbb{Q}^{\mathrm{rés}}$ ne possède un groupe de Galois résoluble. Le théorème qui suit vise à déterminer quelles propriétés il faut demander à la classe $\mathscr{C}$ pour que la $\mathscr{C}$-clôture associée ait ces "bonnes" propriétés.

Théorème 19.— 1) *Si $\mathscr{C}$ est une formation, alors :*

• *L'extension $k^{\mathscr{C}}/k$ est l'unique extension galoisienne M/k vérifiant la propriété suivante : pour toute extension galoisienne finie L/k, on a l'équivalence* $\mathrm{Gal}(L/k) \in \mathscr{C} \Leftrightarrow L \subseteq M$.

• *L'extension $k^{\mathscr{C}}/k$ est la plus grande extension galoisienne de k ayant pour groupe de Galois un pro-$\mathscr{C}$-groupe.*

• *Si $G \in \mathscr{C}^*$ est le groupe de Galois d'une extension galoisienne finie E/k, alors, pour tout corps intermédiaire $k \subseteq L \subseteq k^{\mathscr{C}}$, le groupe G est aussi le groupe de Galois de l'extension $E \cdot L/L$.*

2) *Si $\mathscr{C}$ est une formation extensive, alors le corps $k^{\mathscr{C}}$ est $\mathscr{C}$-clos. En particulier, si un groupe fini G donné est groupe de Galois sur $k^{\mathscr{C}}$, alors $G \in \mathscr{C}^*$. On a donc $(k^{\mathscr{C}})^{\mathscr{C}^*} = k^{\mathrm{sép}}$.*

3) *Si $\mathscr{C}$ est une variété extensive, alors le corps $k^{\mathscr{C}}$ est le plus petit corps contenant k qui soit $\mathscr{C}$-clos. Dans ce cas, si $k_1 \subseteq k_2$ désignent deux corps quelconques, alors $k_1^{\mathscr{C}} \subseteq k_2^{\mathscr{C}}$ (en particulier, si $k_1 \subseteq k_2 \subseteq k_1^{\mathscr{C}}$, alors $k_1^{\mathscr{C}} = k_2^{\mathscr{C}}$).*

Preuve : 1) • Considérons une extension galoisienne finie L/k quelconque. Si $\mathrm{Gal}(L/k) \in \mathscr{C}$, alors on a $L \subseteq k^{\mathscr{C}}$ par définition de $k^{\mathscr{C}}$. Réciproquement, si $L \subseteq k^{\mathscr{C}}$, alors, comme $[L : k]$ est fini, il existe une famille finie $E_1/k, \ldots, E_n/k$ d'extensions galoisiennes finies à groupes de Galois éléments de $\mathscr{C}$ telle que L soit inclus dans le compositum $E = E_1 \cdot \cdots \cdot E_n$. L'extension finie E/k étant galoisienne et son groupe de Galois étant un produit fibré d'un nombre fini d'éléments de $\mathscr{C}$, on a $\mathrm{Gal}(E/k) \in \mathscr{C}$ par (C_3). Le groupe $\mathrm{Gal}(L/k)$ étant un quotient de $\mathrm{Gal}(E/k)$, il est élément de $\mathscr{C}$ par (C_1).

L'unicité du corps $k^{\mathscr{C}}$, pour cette propriété, est alors évidente puisque toute extension galoisienne est la réunion de ses sous-extensions galoisiennes finies.

• Les groupes de Galois des extensions galoisiennes finies de k incluses dans $k^{\mathscr{C}}$ sont dans $\mathscr{C}$ par ce qui précède. Par conséquent, $\mathrm{Gal}(k^{\mathscr{C}}/k)$ est un pro-$\mathscr{C}$-groupe. On se donne maintenant une extension galoisienne M/k à groupe de Galois pro-$\mathscr{C}$. Par définition, il existe un système projectif filtrant à droite $(G_i)_i$ d'éléments de $\mathscr{C}$ tels que $G = \mathrm{Gal}(M/k) = \varprojlim_i G_i$. La famille des sous-groupes ouverts normaux $(U_i)_i$ associés aux G_i (pour tout i, $G/U_i \cong G_i$ pour les projections canoniques) constitue alors un système fondamental de voisinages du neutre de G. Étant donné $\alpha \in M$, notons $\widetilde{k(\alpha)}$ la clôture galoisienne de $k(\alpha)$ sur k. Puisque $\widetilde{k(\alpha)} \subseteq M$, le sous-groupe $\mathrm{Gal}(M/\widetilde{k(\alpha)})$ de G est un sous-groupe ouvert. Il contient donc un U_i pour un certain i, et il s'ensuit que $\mathrm{Gal}(\widetilde{k(\alpha)}/k)$ est un quotient du groupe G_i. Comme $G_i \in \mathscr{C}$ et $\mathscr{C}$ vérifie (C_1), l'on voit que $\mathrm{Gal}(\widetilde{k(\alpha)}/k)$ est élément de $\mathscr{C}$. Ainsi $\alpha \in \widetilde{k(\alpha)} \subseteq k^{\mathscr{C}}$.

• Le groupe de Galois de l'extension galoisienne finie $E \cap k^{\mathscr{C}}/k$ est, d'une part, un quotient de G, donc dans $\mathscr{C}^*$ (en vertu du 1) de la proposition 15), et, d'autre part, un élément de $\mathscr{C}$ d'après le premier point du 1) ci-dessus. Il est donc trivial. Ainsi on a $E \cap k^{\mathscr{C}} = k$, ce qui équivaut à dire que les corps E et $k^{\mathscr{C}}$ sont linéairement disjoints sur k. On en déduit que, pour tout corps intermédiaire $k \subseteq L \subseteq k^{\mathscr{C}}$, les corps E et L sont également linéairement disjoints sur k. Par conséquent, on a $\mathrm{Gal}(E \cdot L/L) = G$.

2) Considérons une extension galoisienne finie $L/k^{\mathscr{C}}$ telle que $G = \mathrm{Gal}(L/k^{\mathscr{C}})$ soit élément de $\mathscr{C}$ et un élément α de L tel que $L = k^{\mathscr{C}}(\alpha)$.

Démontrons tout d'abord que $L = k^{\mathscr{C}}$ sous l'hypothèse supplémentaire que L/k soit galoisienne à groupe de Galois dans $\mathscr{C}$. Pour cela, notons $P(X) \in k^{\mathscr{C}}[X]$ le polynôme minimal de α sur $k^{\mathscr{C}}$. Comme L/k est galoisienne, pour tout $\sigma \in \mathrm{Gal}(k^{\mathrm{sép}}/k)$, il existe $P_\sigma(X) \in k^{\mathscr{C}}[X]$ tel que $\sigma(\alpha) = P_\sigma(\alpha)$. Puisque α est algébrique sur k, l'on peut choisir $\sigma_1, \ldots, \sigma_n \in \mathrm{Gal}(k^{\mathrm{sép}}/k)$ tels que $P_\sigma(X) \in \{P_{\sigma_1}(X), \ldots, P_{\sigma_n}(X)\}$ pour tout $\sigma \in \mathrm{Gal}(k^{\mathrm{sép}}/k)$. Considérons alors le corps Ω, clôture galoisienne sur k du corps obtenu en adjoignant à k les coefficients des polynômes $P_{\sigma_1}(X), \ldots, P_{\sigma_n}(X)$. Par construction, l'extension $\Omega(\alpha)/k$ est galoisienne, et l'on a $\mathrm{Gal}(\Omega(\alpha)/\Omega) = G$. Puisque Ω/k est une extension galoisienne finie incluse dans $k^{\mathscr{C}}$, on a $\mathrm{Gal}(\Omega/k) \in \mathscr{C}$ d'après le premier point du 1) ci-dessus. La classe $\mathscr{C}$ vérifiant (C_2), l'on voit alors que le groupe $\mathrm{Gal}(\Omega(\alpha)/k)$, en tant qu'extension de $\mathrm{Gal}(\Omega(\alpha)/\Omega) = G \in \mathscr{C}$ par $\mathrm{Gal}(\Omega/k) \in \mathscr{C}$, est aussi un élément de $\mathscr{C}$. En particulier, on a $\alpha \in \Omega(\alpha) \subseteq k^{\mathscr{C}}$ et donc $L = k^{\mathscr{C}}$.

Nous expliquons maintenant comment traiter le cas général. Pour tout $\sigma \in \mathrm{Gal}(k^{\mathrm{sép}}/k)$, l'extension finie $k^{\mathscr{C}}(\sigma(\alpha))/k^{\mathscr{C}}$ est galoisienne de groupe de Galois G. En effet, dans $\mathrm{Gal}(k^{\mathrm{sép}}/k)$, le sous-groupe $\mathrm{Gal}(k^{\mathrm{sép}}/k^{\mathscr{C}}(\sigma(\alpha)))$ est le conjugué par σ du sous-groupe $\mathrm{Gal}(k^{\mathrm{sép}}/k^{\mathscr{C}}(\alpha))$. Puisque la conjugaison par

σ induit un automorphisme de $\mathrm{Gal}(k^{\text{sép}}/k^{\mathscr{C}})$, on a alors $\mathrm{Gal}(k^{\text{sép}}/k^{\mathscr{C}}(\sigma(\alpha))) \trianglelefteq \mathrm{Gal}(k^{\text{sép}}/k^{\mathscr{C}})$ et

$$\begin{aligned}\mathrm{Gal}(k^{\mathscr{C}}(\sigma(\alpha))/k^{\mathscr{C}}) &\simeq \mathrm{Gal}(k^{\text{sép}}/k^{\mathscr{C}})/\mathrm{Gal}(k^{\text{sép}}/k^{\mathscr{C}}(\sigma(\alpha)))\\ &= \mathrm{Gal}(k^{\text{sép}}/k^{\mathscr{C}})/\sigma\mathrm{Gal}(k^{\text{sép}}/k^{\mathscr{C}}(\alpha))\sigma^{-1}\\ &\simeq \mathrm{Gal}(k^{\text{sép}}/k^{\mathscr{C}})/\mathrm{Gal}(k^{\text{sép}}/k^{\mathscr{C}}(\alpha))\\ &\cong \mathrm{Gal}(k^{\mathscr{C}}(\alpha)/k^{\mathscr{C}})\\ &= G.\end{aligned}$$

Le compositum $M = \bullet_\sigma k^{\mathscr{C}}(\sigma(\alpha))$ définit donc une extension galoisienne de k (c'est en fait la clôture galoisienne de $k^{\mathscr{C}}(\alpha)$ sur k) et le groupe de Galois $\mathrm{Gal}(M/k^{\mathscr{C}})$ est alors le produit fibré d'un nombre fini de copies du groupe G. Puisque $\mathscr{C}$ vérifie (C_3), ce groupe est dans $\mathscr{C}$. Par ce qui précède, on a alors $M = k^{\mathscr{C}}$ et donc $L = k^{\mathscr{C}}$.

On se donne enfin une extension galoisienne finie $L/k^{\mathscr{C}}$ de groupe de Galois G et un sous-groupe normal H de G. Alors la sous-extension $L^H/k^{\mathscr{C}}$ de $L/k^{\mathscr{C}}$ est galoisienne finie de groupe de Galois G/H. Si $G/H \in \mathscr{C}$, alors $L^H = k^{\mathscr{C}}$ d'après ce qui précède, et donc $H = G$. Ainsi $G \in \mathscr{C}^*$.

3) On sait déjà, d'après 2), que le corps $k^{\mathscr{C}}$ est $\mathscr{C}$-clos. On se donne maintenant un corps L contenant k qui soit $\mathscr{C}$-clos et une extension galoisienne finie M/k à groupe de Galois dans $\mathscr{C}$. Comme le groupe de Galois de l'extension galoisienne finie $M \cdot L/L$ s'identifie à un sous-groupe de $\mathrm{Gal}(M/k) \in \mathscr{C}$, le groupe $\mathrm{Gal}(M \cdot L/L)$ est lui aussi élément de $\mathscr{C}$ (par (C_0)). Le corps L étant $\mathscr{C}$-clos, on a alors $M \cdot L = L$, c'est-à-dire $M \subseteq L$. En particulier, on a $k^{\mathscr{C}} \subseteq L$.

Si $k_1 \subseteq k_2$ désignent deux corps quelconques, alors $k_1 \subseteq k_2 \subseteq k_2^{\mathscr{C}}$. Puisque $k_2^{\mathscr{C}}$ est $\mathscr{C}$-clos par ce qui précède, on a $k_1^{\mathscr{C}} \subseteq k_2^{\mathscr{C}}$ par minimalité de $k_1^{\mathscr{C}}$.

□

Remarque : Si $\mathscr{C}$ est une formation extensive, on voit que, d'après le 2) du théorème 19, aucun élément non trivial de $\mathscr{C}$ ne se réalise comme groupe de Galois sur $k^{\mathscr{C}}$. Si $\mathscr{C}$ contient de plus un groupe de Galois régulier sur k (par exemple, un groupe abélien fini ou un groupe symétrique[11]), l'on voit que le corps $k^{\mathscr{C}}$ n'est pas hilbertien. Il est évident que

$$\mathscr{C} = \mathscr{C}(1) \text{ et } k \text{ hilbertien} \Longrightarrow k^{\mathscr{C}} \text{ hilbertien.}$$

La réciproque de cette implication est vraie si le $\mathrm{PIGR}_{/k}$ admet une réponse positive, en vertu de ce qui précède. Elle est aussi vraie si $\mathscr{C}$ vérifie (C_0). En effet, si $k^{\mathscr{C}}$ est hilbertien, le raisonnement ci-dessus montre alors que $\mathscr{C}$ ne contient aucun groupe abélien fini non trivial. Puisque $\mathscr{C}$ vérifie (C_0), le théorème de Cauchy assure alors que $\mathscr{C} = \mathscr{C}(1)$. Ainsi $k^{\mathscr{C}} = k$ et k est hilbertien.

Nous donnons ci-dessous une variante du troisième point du 1) du théorème 19 valable sous la seule hypothèse que $\mathscr{C}$ vérifie (C_1).

Proposition 20.— *Si $\mathscr{C}$ est une pré-formation et si un groupe fini $G \in \mathscr{C}^*$ ne possédant que des quotients simples non abéliens est le groupe de Galois d'une extension galoisienne finie E/k, alors, pour tout corps intermédiaire $k \subseteq L \subseteq k^{\mathscr{C}}$, le groupe G est aussi le groupe de Galois de l'extension $E \cdot L/L$.*

Preuve : Démontrons tout d'abord un résultat préliminaire sur les quotients simples d'un produit fibré de deux groupes quelconques :

Étant donnés un groupe simple non abélien S, un groupe G et deux sous-groupes normaux H_1 et H_2 de G, si S n'est quotient ni de G/H_1, ni de G/H_2, alors S n'est quotient de $G/(H_1 \cap H_2)$.

En effet, quitte à quotienter G, H_1 et H_2 par $H_1 \cap H_2$, on peut supposer que H_1 et H_2 sont d'intersection triviale. S'il existe un sous-groupe normal N de G tel que $G/N = S$, alors on a nécessairement $H_1N = H_2N = G$ puisque le groupe simple S n'est quotient ni de G/H_1, ni de G/H_2. L'observation suivante, qui nous a été communiquée par A. Fehm et due à M. Shusterman, permet alors de conclure :

Si H désigne un groupe et U, V deux sous-groupes normaux de H d'intersection triviale, alors, pour tout sous-groupe normal K de H tel que $KU = KV = H$, le groupe H/K est abélien[12].

[11] Voir par exemple [FJo8, Corollaries 16.2.7 & 16.3.6].

[12] En effet, si x et y sont deux éléments quelconques de H, on a $x = k_1u$ et $u = k_2v$ avec $u \in U$, $v \in V$ et $(k_1, k_2)^2 \in K$. On a donc $[x,y] = k_1uk_2vu^{-1}k_1^{-1}v^{-1}k_2^{-1} = k_1(uk_2u^{-1})uvu^{-1}v^{-1}(vk_1^{-1}v^{-1})k_2^{-1}$. Il ne reste plus qu'à remarquer que $[U,V] = \{1\}$ (puisque U et V sont normaux et d'intersection triviale) pour conclure que $[x,y]$ est élément de K.

Venons-en maintenant à la démonstration de la proposition. Clairement, il suffit de démontrer que $E \cap k^{\mathscr{C}} = k$. Si le groupe $\mathrm{Gal}((E \cap k^{\mathscr{C}})/k)$ n'est pas trivial, alors ce groupe possède un quotient simple S qui, en tant que quotient de G, est non abélien et élément de $\mathscr{C}^*$ (d'après le 1) de la proposition 15), et n'est donc pas élément de $\mathscr{C}$. Si L_0 désigne le sous-corps de $E \cap k^{\mathscr{C}}$ tel que $\mathrm{Gal}(L_0/k) = S$, alors on a $L_0 \subseteq k^{\mathscr{C}}$. Puisque $[L_0 : k]$ est fini, il existe une famille finie $M_1/k, \ldots, M_n/k$ d'extensions galoisiennes finies à groupes de Galois éléments de $\mathscr{C}$ telle que L_0 soit inclus dans le compositum $M = M_1 \cdot \cdots \cdot M_n$. La classe $\mathscr{C}$ vérifiant (C_1), le groupe S n'est quotient de $\mathrm{Gal}(M_i/k)$ pour aucun $i \in \{1, \ldots, n\}$. En vertu du résultat préliminaire ci-dessus et d'une récurrence immédiate, le groupe $\mathrm{Gal}(M/k)$, qui s'identifie à un produit fibré successif des groupes $\mathrm{Gal}(M_1/k), \ldots, \mathrm{Gal}(M_n/k)$, n'admet alors pas S comme quotient, ce qui est manifestement impossible puisque L_0 est un sous-corps de M. Par conséquent, $\mathrm{Gal}((E \cap k^{\mathscr{C}})/k)$ est trivial, c'est-à-dire $E \cap k^{\mathscr{C}} = k$.

□

Remarque : Si $\mathscr{C}$ contient tous les groupes finis d'ordre premier, la condition que G ne possède que des quotients simples non abéliens dans la proposition 20 est automatique (par le 1) de la proposition 15).

On définit maintenant la suite $(k^{\mathscr{C}[n]})_{n \geq 0}$ des *$\mathscr{C}$-clôtures successives* du corps k, en posant $k^{\mathscr{C}[0]} = k$ et $k^{\mathscr{C}[n+1]} = (k^{\mathscr{C}[n]})^{\mathscr{C}}$ pour tout $n \geq 0$.

La réunion des $\mathscr{C}$-clôtures successives de k est alors reliée à la $\widehat{\mathscr{C}}$-clôture de k, de la manière suivante :

Théorème 21.— 1) *Pour tout $n \geq 0$, l'extension $k^{\mathscr{C}[n]}/k$ est galoisienne.*

2) *Si $\mathscr{C}$ est une pré-variété, alors $k^{\widehat{\mathscr{C}}} \subseteq \bigcup_{n \geq 0} k^{\mathscr{C}[n]}$.*

3) *Si $\mathscr{C}$ est une pré-variété qui vérifie en plus la condition (C_3), alors $k^{\widehat{\mathscr{C}}} = \bigcup_{n \geq 0} k^{\mathscr{C}[n]}$.*

Preuve : 1) Pour $n \in \{0, 1\}$, l'extension $k^{\mathscr{C}[n]}/k$ est galoisienne. On se donne maintenant $n \geq 1$ et l'on suppose que $k^{\mathscr{C}[n]}/k$ est galoisienne. Étant donné $\alpha \in k^{\mathscr{C}[n+1]}$, il existe une famille finie $M_1/k^{\mathscr{C}[n]}, \ldots, M_m/k^{\mathscr{C}[n]}$ d'extensions galoisiennes finies à groupes de Galois dans $\mathscr{C}$ telle que α appartienne au compositum $M = M_1 \cdot \cdots \cdot M_m$. Fixons alors $i \in \{1, \ldots, m\}$, un élément primitif β_i de $M_i/k^{\mathscr{C}[n]}$ et $\sigma \in \mathrm{Gal}(k^{\mathrm{sép}}/k)$. En utilisant uniquement l'hypothèse $k^{\mathscr{C}[n]}/k$ galoisienne, l'on montre comme dans la preuve du 2) du théorème 19 que l'extension finie $k^{\mathscr{C}[n]}(\sigma(\beta_i))/k^{\mathscr{C}[n]}$ est galoisienne de groupe de Galois $G_i = \mathrm{Gal}(M_i/k^{\mathscr{C}[n]})$. Comme $G_i \in \mathscr{C}$, l'on voit que $\sigma(\beta_i) \in k^{\mathscr{C}[n]}(\sigma(\beta_i)) \subseteq k^{\mathscr{C}[n+1]}$, ce qui montre que $\sigma(M_i) \subseteq k^{\mathscr{C}[n+1]}$. En particulier, on a $\sigma(\alpha) \in \sigma(M) \subseteq k^{\mathscr{C}[n+1]}$.

2) Étant donné $\alpha \in k^{\widehat{\mathscr{C}}}$, considérons la clôture galoisienne M de $k(\alpha)$ sur k; celle-ci est contenue dans $k^{\widehat{\mathscr{C}}}$ puisque $k^{\widehat{\mathscr{C}}}/k$ est galoisienne. Or $\widehat{\mathscr{C}}$ est une formation puisque $\mathscr{C}$ est une pré-variété (cf. corollaire 13). Par le premier point du 1) du théorème 19, on a donc $G = \mathrm{Gal}(M/k) \in \widehat{\mathscr{C}}$. Par définition de $\widehat{\mathscr{C}}$, il existe alors une tour d'extensions finies

$$k = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{n-1} \subseteq M_n = M$$

telle que, pour tout $i \in \{0, \ldots, n-1\}$, l'extension M_{i+1}/M_i soit galoisienne de groupe de Galois $G_i \in \mathscr{C}$. Pour tout $i \in \{0, \ldots, n-1\}$, le groupe de Galois de l'extension galoisienne finie $M_{i+1} \cdot k^{\mathscr{C}[i]}/M_i \cdot k^{\mathscr{C}[i]}$ s'identifie à un sous-groupe de G_i. Or G_i est dans $\mathscr{C}$ et $\mathscr{C}$ vérifie (C_0). On a donc $\mathrm{Gal}(M_{i+1} \cdot k^{\mathscr{C}[i]}/M_i \cdot k^{\mathscr{C}[i]}) \in \mathscr{C}$, et une récurrence immédiate montre alors que $M = M_n \subseteq k^{\mathscr{C}[n]}$. On a donc $\alpha \in M \subseteq k^{\mathscr{C}[n]}$.

3) Réciproquement, on a $k^{\mathscr{C}[0]} = k \subseteq k^{\widehat{\mathscr{C}}}$. On se donne maintenant un entier $n \geq 0$ et l'on suppose que $k^{\mathscr{C}[n]} \subseteq k^{\widehat{\mathscr{C}}}$. Étant donné $\alpha \in k^{\mathscr{C}[n+1]}$, considérons la clôture galoisienne M de $k^{\mathscr{C}[n]}(\alpha)$ sur $k^{\mathscr{C}[n]}$. Comme $M \subseteq k^{\mathscr{C}[n+1]}$ et $\mathscr{C}$ est une formation, on peut à nouveau utiliser le premier point du 1) du théorème 19 : on a $\mathrm{Gal}(M/k^{\mathscr{C}[n]}) \in \mathscr{C}$. Or, par hypothèse, on a $k^{\mathscr{C}[n]} \subseteq k^{\widehat{\mathscr{C}}}$. Par conséquent, $\mathrm{Gal}(M \cdot k^{\widehat{\mathscr{C}}}/k^{\widehat{\mathscr{C}}})$ s'identifie à un sous-groupe de $\mathrm{Gal}(M/k^{\mathscr{C}[n]}) \in \mathscr{C}$. Puisque $\mathscr{C}$ vérifie (C_0) et $\mathscr{C} \subseteq \widehat{\mathscr{C}}$ (cf. 3) de la proposition 12), l'on voit que $\mathrm{Gal}(M \cdot k^{\widehat{\mathscr{C}}}/k^{\widehat{\mathscr{C}}}) \in \widehat{\mathscr{C}}$. La classe $\mathscr{C}$ étant une pré-variété, la classe $\widehat{\mathscr{C}}$ est une formation extensive (cf. corollaire 13). En vertu du 2) du théorème 19, on a alors $M \cdot k^{\widehat{\mathscr{C}}} = k^{\widehat{\mathscr{C}}}$, c'est-à-dire $M \subseteq k^{\widehat{\mathscr{C}}}$. En particulier, on a $\alpha \in M \subseteq k^{\widehat{\mathscr{C}}}$.

□

4.2.— Groupes de Galois sur une $\mathscr{C}$-clôture.

Le 2) du théorème 19 assure que, si $\mathscr{C}$ est une formation extensive, alors les groupes finis qui apparaissent comme groupes de Galois sur le corps $k^{\mathscr{C}}$ sont nécessairement éléments de $\mathscr{C}^*$. La réciproque de cette propriété est fausse en général puisque, par exemple, la clôture résoluble de $\mathbb{F}_p$ est égale à $\overline{\mathbb{F}}_p$ pour tout nombre premier p. Par application du troisième point du 1) du théorème 19, on peut toutefois remarquer que, si le $\mathrm{PIG}_{/k}$ admet une réponse positive, alors tous les groupes finis appartenant à $\mathscr{C}^*$ sont bien groupes de Galois sur $k^{\mathscr{C}}$. Il est donc assez raisonnable de conjecturer que, si k est un corps hilbertien, alors les groupes finis apparaissant comme groupes de Galois sur $k^{\mathscr{C}}$ sont exactement les éléments de $\mathscr{C}^*$.

Nous allons maintenant décrire une autre situation dans laquelle les groupes finis apparaissant comme groupes de Galois sur $k^{\mathscr{C}}$ sont exactement les éléments de $\mathscr{C}^*$, et faire ensuite le lien avec une conjecture très célèbre de théorie inverse de Galois[13].

Proposition 22.— *On suppose que $\mathscr{C}$ est une variété extensive. S'il existe un corps intermédiaire $k \subseteq L \subseteq k^{\mathscr{C}}$ à groupe de Galois absolu prolibre de rang α infini, alors les groupes profinis qui apparaissent comme groupes de Galois sur $k^{\mathscr{C}}$ sont exactement les pro-$\mathscr{C}^*$-groupes de rang $\leq \alpha$.*

En particulier, dans cette situation, les groupes finis qui apparaissent comme groupes de Galois sur $k^{\mathscr{C}}$ sont exactement les éléments de $\mathscr{C}^*$.

Preuve : Étant donné un corps intermédiaire L comme ci-dessus, commençons par remarquer que, d'après le 3) du théorème 19, on a $L^{\mathscr{C}} = k^{\mathscr{C}}$. Ainsi, si l'on identifie le groupe de Galois absolu de L, $\mathrm{Gal}(k^{\mathrm{sép}}/L)$, au groupe prolibre $\widehat{F}_\alpha$, on voit que le groupe $N = \mathrm{Gal}(k^{\mathrm{sép}}/k^{\mathscr{C}})$ (qui, d'après le premier point du 1) du théorème 19, est égal à l'intersection des sous-groupes ouverts normaux Γ de $\widehat{F}_\alpha$ tels que $\widehat{F}_\alpha/\Gamma$ soit élément de $\mathscr{C}$) vérifie les deux propriétés suivantes :

• N est de rang $\leq \alpha$ (en tant que sous-groupe fermé d'un groupe profini de rang infini α),

• N est un pro-$\mathscr{C}^*$-groupe (car les quotients finis de N correspondent aux groupes de Galois des extensions galoisiennes finies de $k^{\mathscr{C}}$ qui, d'après le 2) du théorème 19, sont tous éléments de $\mathscr{C}^*$).

Les groupes profinis qui sont groupes de Galois sur $k^{\mathscr{C}}$ sont exactement les quotients de N. Ils ont donc tous un rang $\leq \alpha$ et sont des pro-$\mathscr{C}^*$-groupes car $\mathscr{C}^*$ vérifie (C_1) (par le 1) de la proposition 15).

Réciproquement, l'on se donne un pro-$\mathscr{C}^*$-groupe G de rang $\leq \alpha$. Par propriété universelle de $\widehat{F}_\alpha$, il existe un épimorphisme $\varphi : \widehat{F}_\alpha \longrightarrow G$ qui induit alors, par passage au quotient, un épimorphisme $\widetilde{\varphi} : \widehat{F}_\alpha/N \longrightarrow G/\varphi(N)$. Par construction, le groupe quotient $\widehat{F}_\alpha/N$ est le groupe de Galois de l'extension galoisienne $L^{\mathscr{C}}/L$; c'est donc un pro-$\mathscr{C}$-groupe en vertu du deuxième point du 1) du théorème 19. Puisque $\mathscr{C}$ vérifie (C_1), l'on voit que, via l'épimorphisme $\widetilde{\varphi}$, le groupe quotient $G/\varphi(N)$ est lui aussi un pro-$\mathscr{C}$-groupe. Tout quotient fini non trivial de $G/\varphi(N)$ est alors un élément de $\mathscr{C}$, mais aussi un élément de $\mathscr{C}^*$ en tant que quotient du pro-$\mathscr{C}^*$-groupe G. On en déduit que $G/\varphi(N)$ n'a pas de quotient non trivial et donc que $G = \varphi(N)$. Ainsi G est un quotient de N et est donc groupe de Galois d'une extension galoisienne de $k^{\mathscr{C}}$.

□

Pour illustrer l'intérêt de la proposition 22, nous considérons la classe $\mathscr{C}(\mathrm{rés})$ des groupes finis résolubles. Comme c'est une variété extensive, les théorèmes 19 et 21 et la proposition 22 peuvent alors être entièrement appliqués. En particulier, la clôture résoluble de k, notée $k^{\mathrm{rés}}$ pour plus de commodité, est l'unique corps M contenant k vérifiant les conditions (équivalentes) suivantes :

i) l'extension M/k est galoisienne et, pour toute extension galoisienne finie L/k, le groupe $\mathrm{Gal}(L/k)$ est résoluble si et seulement si $L \subseteq M$,

ii) l'extension M/k est la plus grande extension galoisienne de k ayant pour groupe de Galois un groupe pro-résoluble,

iii) le corps M est le plus petit corps contenant k qui soit $\mathscr{C}$-clos,

iv) le corps M est égal à la réunion des abélianisés successifs de k.

Puisque l'on a les inclusions $\mathscr{C}(\mathrm{cycl}) \subseteq \mathscr{C}(\mathrm{ab}) \subseteq \mathscr{C}(\mathrm{nil}) \subseteq \mathscr{C}(\mathrm{rés})$, on en déduit que $\mathscr{C}(\mathrm{cycl})^* \supseteq \mathscr{C}(\mathrm{ab})^* \supseteq \mathscr{C}(\mathrm{nil})^* \supseteq \mathscr{C}(\mathrm{rés})^*$ par la propriété de dualité b) du §3.3. Le 3) de la proposition 12 montre que ces inclusions sont en fait des égalités.

[13] La proposition 22 est librement inspirée d'une idée de D. Haran et M. Jarden communiquée au premier auteur de cet article dans une correspondance au sujet de la clôture résoluble de $\mathbb{Q}$.

Par définition, la classe des groupes finis fortement non résolubles, notée $\mathscr{C}(\mathrm{FnR})$, est la classe duale $\mathscr{C}(\mathrm{cycl})^* = \mathscr{C}(\mathrm{ab})^* = \mathscr{C}(\mathrm{nil})^* = \mathscr{C}(\mathrm{rés})^*$. On a alors les propriétés suivantes :

a) Un groupe fini est dans $\mathscr{C}(\mathrm{FnR})$ si et seulement si aucun de ses quotients n'est d'ordre premier.

b) On a $\mathscr{C}(\mathrm{FnR}) = \bigcap_{p\in\mathscr{P}} \mathscr{C}(\mathrm{p})^*$ où $\mathscr{P}$ désigne l'ensemble des nombres premiers.

c) La classe $\mathscr{C}(\mathrm{FnR})$ est la plus grande classe de groupes finis vérifiant (C_1) et ne contenant aucun groupe fini d'ordre premier.

d) La classe $\mathscr{C}(\mathrm{FnR})$ vérifie (C_2). En particulier, toute extension et tout produit fibré de groupes finis simples non abéliens sont des groupes fortement non résolubles.

e) La classe $\mathscr{C}(\mathrm{FnR})$ ne satisfait visiblement pas la condition (C_0). En fait, elle n'est même pas stable par sous-groupes normaux. En effet, considérons par exemple le groupe alterné A_5, qui est simple non abélien et donc fortement non résoluble. Puisqu'il se réalise comme groupe de Galois sur $\mathbb{Q}$, il se réalise aussi sur $\mathbb{Q}^{\mathrm{rés}}$ (en vertu du troisième point du 1) du théorème 19) et l'on peut donc considérer une extension galoisienne finie $L/\mathbb{Q}^{\mathrm{rés}}$ de groupe de Galois A_5. L'extension $\mathbb{Q}^{\mathrm{rés}}/\mathbb{Q}$ étant galoisienne, un célèbre théorème de Weissauer[14] assure alors que L est hilbertien, et donc que $\mathbb{Z}/2\mathbb{Z}$ se réalise comme groupe de Galois sur L. Étant donnés une extension quadratique M/L et $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{rés}})$, l'extension $\sigma(M)/L$ est clairement quadratique. Par conséquent, si l'on note $\widetilde{M}$ le compositum des corps $\sigma(M)$ lorsque σ parcourt le groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{rés}})$ ($\widetilde{M}$ est en fait la clôture galoisienne de M sur $\mathbb{Q}^{\mathrm{rés}}$), l'on voit qu'il existe un entier $N \geq 1$ tel que $\mathrm{Gal}(\widetilde{M}/L) = (\mathbb{Z}/2\mathbb{Z})^N$. Il s'ensuit que $\mathrm{Gal}(\widetilde{M}/\mathbb{Q}^{\mathrm{rés}})$, qui est dans $\mathscr{C}(\mathrm{FnR})$ (puisque se réalisant comme groupe de Galois sur $\mathbb{Q}^{\mathrm{rés}}$), possède un sous-groupe normal, $(\mathbb{Z}/2\mathbb{Z})^N$, qui, étant abélien, ne peut être dans $\mathscr{C}(\mathrm{FnR})$.

f) La classe duale de $\mathscr{C}(\mathrm{FnR})$ (c'est-à-dire la classe biduale de $\mathscr{C}(\mathrm{rés})$) est la classe constituée des groupes finis qui n'admettent pour quotients simples que des groupes d'ordre premier.

Regardons maintenant deux applications de la proposition 22 à la classe $\mathscr{C}(\mathrm{rés})$:

a) $k = \mathbb{Q}$. Comme nous l'avons déjà remarqué, une réponse positive au $\mathrm{PIG}_{/\mathbb{Q}}$ entraînerait que les groupes finis apparaissant comme groupes de Galois sur $\mathbb{Q}^{\mathrm{rés}}$ seraient exactement les groupes finis fortement non résolubles. Il est intéressant de remarquer que, sous la célèbre conjecture de Shafarevich[15], on obtient ce même résultat en appliquant la proposition 22 au corps $L = \mathbb{Q}^{\mathrm{ab}}$. L'intérêt de cette remarque est qu'il n'existe *a priori* aucun lien logique entre le $\mathrm{PIG}_{/\mathbb{Q}}$ et la conjecture de Shafarevich (voir [DD97, Remark 2.2]).

b) $k = \mathbb{F}_q(T)$. On applique la proposition 22 au corps $L = \overline{\mathbb{F}_q}(T)$: le corps L est la clôture cyclotomique du corps k et est donc inclus dans la clôture résoluble de k. Un célèbre théorème dû à Riemann, Harbater et Pop[16] assure alors que le corps L a un groupe de Galois absolu prolibre de rang $\aleph_0$. On peut donc en déduire que les groupes profinis qui apparaissent comme groupes de Galois sur $\mathbb{F}_q(T)^{\mathrm{rés}}$ sont exactement les pro-FnR-groupes de rang $\leq \aleph_0$.

Ce résultat est particulièrement intéressant quand on le compare au précédent. En effet, il s'agit de l'analogue classique entre $\mathbb{Q}$ et $\mathbb{F}_q(T)$: la clôture cyclotomique de $\mathbb{Q}$ est $\mathbb{Q}^{\mathrm{ab}}$ et celle de $\mathbb{F}_q(T)$ est $\overline{\mathbb{F}_q}(T)$. Le théorème de Riemann, Harbater et Pop dit alors que l'analogue de la conjecture de Shafarevich est vraie pour $\mathbb{F}_q(T)$ de la même manière que le b) dit que l'analogue du a) est vrai pour $\mathbb{F}_q(T)$.

5.— Application au Problème Inverse de Galois Faible.

Dans cette dernière section, nous donnons tout d'abord des conditions suffisantes sur une classe $\mathscr{C}$ de groupes finis et un corps k pour que le PIGF possède une réponse positive sur les sous-corps de $k^{\mathscr{C}}$ contenant k. En particulier, dans le théorème 23 à venir, nous généralisons le théorème 2 de l'introduction. Nous appliquons ensuite notre étude à plusieurs classes de groupes finis explicites.

[14] qui assure que toute extension finie stricte et séparable d'une extension galoisienne d'un corps hilbertien est hilbertienne (voir par exemple [FJ08, Theorem 13.9.1]).

[15] Cette conjecture affirme que le groupe de Galois absolu de $\mathbb{Q}^{\mathrm{ab}}$ est isomorphe au groupe prolibre de rang $\aleph_0$, $\widehat{F_\omega}$.

[16] Ce théorème affirme que, pour tout corps séparablement clos K, le groupe de Galois absolu de $K(T)$ est prolibre de rang égal au cardinal de K.

Le corollaire 26 qui suit précise l'écart existant entre le PIG et sa version Faible annoncé dans le théorème 3 de l'introduction.

Dans toute la suite, k désigne un corps hilbertien de caractéristique $p \geq 0$.

5.1.— Résolution du Problème Inverse de Galois Faible sur certaines clôtures d'un corps hilbertien.

Théorème 23.— *On se donne une pré-formation $\mathscr{C}$.*

1) *Si les conditions*

- *$p \neq 2$ ou $\overline{\mathbb{F}_2} \subseteq k$,*
- *il existe une infinité d'entiers $n \geq 1$ tels que le groupe alterné A_n n'appartienne pas à $\mathscr{C}$,*

sont satisfaites, alors le $\mathrm{PIGF}_{/L}$ *admet une réponse positive pour tout corps intermédiaire $k \subseteq L \subseteq k^{\mathscr{C}}$.*

2) *Si les conditions*

- *$p = 2$,*
- *il existe une infinité d'entiers impairs $n \geq 1$ tels que A_n n'appartienne pas à $\mathscr{C}$,*
- *il existe un groupe fini simple non abélien G_0 n'appartenant pas à $\mathscr{C}$ et admettant une réalisation régulière sur k ne possédant qu'un seul point de branchement,*

sont satisfaites, alors le $\mathrm{PIGF}_{/L}$ *admet une réponse positive pour tout corps intermédiaire $k \subseteq L \subseteq k^{\mathscr{C}}$.*

Plus généralement, dans chacun des cas 1) et 2), pour tout groupe fini G et tout corps intermédiaire $k \subseteq L \subseteq k^{\mathscr{C}}$, il existe une suite $(F_n/L)_{n\geq 1}$ d'extensions finies séparables telle que $\mathrm{Aut}(F_n/L) = G$ *pour tout $n \geq 1$ et telle que les corps $F_1, \ldots, F_n$ soient linéairement disjoints sur L pour tout $n \geq 2$.*

Preuve : On se donne un groupe fini G.

Étant donné un corps intermédiaire $k \subseteq L \subseteq k^{\mathscr{C}}$, notons tout d'abord que, pour qu'il existe une suite $(F_n/L)_{n\geq 1}$ d'extensions finies séparables telle que $\mathrm{Aut}(F_n/L) = G$ pour tout $n \geq 1$ et telle que les corps $F_1, \ldots, F_n$ soient linéairement disjoints sur L pour tout $n \geq 2$, il suffit de trouver un groupe fini non trivial Γ vérifiant les trois conditions suivantes :

- $\Gamma \in \mathscr{C}^*$,
- l'énoncé $(*/G/\Gamma/k)$ est vrai,
- aucun quotient simple de Γ n'est abélien.

En effet, par définition de l'énoncé $(*/G/\Gamma/k)$, il existe un sous-groupe H de Γ tel que $N_\Gamma(H)/H \cong G$ et une extension finie galoisienne $E/k(T)$ telle que E/k soit régulière et vérifiant $\mathrm{Gal}(E/k(T)) = \Gamma$. Comme k est hilbertien, Γ est non trivial et E/k est régulière, il existe une suite $(t_n)_{n\geq 1}$ d'éléments de $\mathbb{P}^1(k)$ telle que $\mathrm{Gal}(E_{t_n}/k) = \Gamma$ pour tout $n \geq 1$ et telle que les corps $E_{t_1}, \ldots, E_{t_n}$ soient linéairement disjoints sur k pour tout $n \geq 2$. Étant donné $n \geq 1$, le groupe de Galois de l'extension $E_{t_1} \cdot \cdots \cdot E_{t_{n+1}}/k$ s'identifie au produit direct de $n+1$ copies du groupe Γ. Or Γ est dans $\mathscr{C}^*$ et $\mathscr{C}^*$ vérifie (C_2) en vertu du 2) de la proposition 15. Par conséquent, $\mathrm{Gal}(E_{t_1} \cdot \cdots \cdot E_{t_{n+1}}/k) = \Gamma^{n+1}$ est dans $\mathscr{C}^*$. De plus, puisqu'aucun quotient simple de Γ n'est abélien, il en est de même du groupe Γ^{n+1}. Par la proposition 20, on a donc

$$[E_{t_1} \cdot \cdots \cdot E_{t_{n+1}} \cdot L : L] = [E_{t_1} \cdot \cdots \cdot E_{t_{n+1}} : k]. \tag{2}$$

De même, on a

$$[E_{t_1} \cdot \cdots \cdot E_{t_n} \cdot L : L] = [E_{t_1} \cdot \cdots \cdot E_{t_n} : k] \text{ et } [E_{t_{n+1}} \cdot L : L] = [E_{t_{n+1}} : k]. \tag{3}$$

Comme les corps $E_{t_1}, \ldots, E_{t_{n+1}}$ sont linéairement disjoints sur k, on a

$$[E_{t_1} \cdot \cdots \cdot E_{t_{n+1}} : k] = [E_{t_1} \cdot \cdots \cdot E_{t_n} : k][E_{t_{n+1}} : k]. \tag{4}$$

En combinant (2), (3) et (4), on obtient $[E_{t_1} \cdot \cdots \cdot E_{t_{n+1}} \cdot L : L] = [E_{t_1} \cdot \cdots \cdot E_{t_n} \cdot L : L][E_{t_{n+1}} \cdot L : L]$, ce qui montre bien que les corps $E_{t_1} \cdot L, \ldots, E_{t_{n+1}} \cdot L$ sont linéairement disjoints sur L. Enfin, comme déjà noté dans (3), on a $\mathrm{Gal}(E_{t_n} \cdot L/L) = \Gamma$ et l'on a donc $\mathrm{Aut}((E_{t_n} \cdot L)^H/L) = G$ pour tout $n \geq 1$.

Nous démontrons maintenant que, dans chacun des cas 1) et 2), l'on peut toujours trouver un groupe fini non trivial Γ vérifiant les trois conditions ci-dessus. Pour ce faire, nous utiliserons le résultat préliminaire de théorie des groupes suivant :

Si un groupe Γ est extension d'un groupe G_2 par un groupe G_1, alors tout quotient simple de Γ est un quotient de G_2 ou de G_1. En particulier, si un groupe Γ est extension d'une puissance d'un groupe simple G_2 par un groupe simple G_1, alors G_1 et G_2 sont les seuls quotients simples possibles de Γ [17].

Supposons tout d'abord que l'on soit dans le cas 1) et que $p \neq 2$. Pour au moins un entier n tel que $A_n \notin \mathscr{C}$, disons n_0, on a $n_0 \geq |G| + 2$ et $n_0 \notin \{1, 2, 3, 4, 6\}$. Ainsi, par le 3) du théorème 6, il existe un entier $N \geq 1$ et un groupe fini Γ, extension de $A_{n_0}^N$ par A_{n_0}, tel que l'énoncé $(*/G/\Gamma/k)$ soit vrai. Comme A_{n_0} est simple et n'appartient pas à $\mathscr{C}$, on voit que A_{n_0} est élément de $\mathscr{C}^*$ et, puisque $\mathscr{C}^*$ vérifie (C_2) (en vertu du 2) de la proposition 15), on a $\Gamma \in \mathscr{C}^*$. Le résultat préliminaire ci-dessus assure alors que le seul quotient simple de Γ est A_{n_0}, qui n'est visiblement pas abélien.

Supposons maintenant que l'on soit dans le cas 2). Pour au moins un entier impair n tel que $A_n \notin \mathscr{C}$, disons n_0, que l'on peut supposer être hors de $\{1, 2, 3, 4, 6\}$, le groupe G se plonge dans le groupe simple A_{n_0} qui est un élément de $\mathscr{C}^*$. De plus, A_{n_0} est groupe de Galois régulier sur k en vertu de [Brio4, Theorem 11] et du lemme 4. Donc, d'après le 1) du théorème 6, il existe un entier $N \geq 1$ et un groupe fini Γ, extension de G_0^N par A_{n_0}, tel que $(*/G/\Gamma/k)$ soit vrai. On montre alors comme dans le cas précédent que Γ est dans $\mathscr{C}^*$ et qu'aucun de ses quotients simples n'est abélien.

Supposons enfin que l'on soit dans le cas 1) et que $\overline{\mathbb{F}_2} \subseteq k$. Alors, d'après [AOS94, AY94a], pour tout $n \geq 5$, le groupe A_n possède une réalisation régulière sur k n'ayant qu'un seul point de branchement, et l'on peut donc appliquer le même raisonnement que celui adopté dans le cas 2).

□

Remarques : 1) Plusieurs groupes finis simples non abéliens possèdent une réalisation régulière sur tout corps de caractéristique 2 n'admettant qu'un seul point de branchement. Par exemple, comme déjà utilisé dans la démonstration du théorème 1, le groupe de Mathieu M_{23} vérifie cette condition (cf. [AY94b]). D'autres exemples explicites sont le groupe projectif spécial linéaire $PSL_3(\mathbb{F}_2)$ [AY94a, Theorem 5.3] ou le groupe de Mathieu M_{24} [AY94b]. Par contre, il n'est pas clair que, pour tout $n \geq 5$, le groupe alterné A_n vérifie cette condition[18], ceci expliquant l'hypothèse plus restrictive en caractéristique 2 dans le théorème 23 si k ne contient pas $\overline{\mathbb{F}_2}$.

2) Rappelons qu'un corps K est *RG-hilbertien* (une terminologie introduite par M. Fried et H. Völklein dans [FV92]) si toute extension finie galoisienne $E/K(T)$ telle que E/K soit régulière possède au moins une spécialisation E_{t_0}/K (avec t_0 dans $\mathbb{P}^1(K)$) telle que $\mathrm{Gal}(E_{t_0}/K) = \mathrm{Gal}(E/K(T))$. S'il est clair que tout corps hilbertien est nécessairement RG-hilbertien, la réciproque n'est pas vraie en général, cf. [FV92, DH99]. Cependant, nos arguments montrent que le théorème 23 reste vrai si k est seulement RG-hilbertien.

3) En vertu du 2) de la proposition 12 (et puisque $\mathscr{C}$ et $\widehat{\mathscr{C}}$ contiennent les mêmes groupes simples), la conclusion du théorème 23 est même vraie pour tout corps intermédiaire $k \subseteq L \subseteq k^{\widehat{\mathscr{C}}}$ [19].

4) En utilisant le troisième point du 1) du théorème 19 à la place de la proposition 20, l'on voit que, dans la preuve du théorème 23, il n'est pas nécessaire de supposer qu'aucun quotient simple de Γ ne soit abélien si $\mathscr{C}$ est une pré-variété ou une formation. Comme déjà mentionné dans la remarque qui précède le théorème 21, il en est de même si $\mathscr{C}$ contient tous les groupes finis d'ordre premier.

Comme première application de notre construction, on peut considérer la classe $\mathscr{C}(\text{rés})$ des groupes finis résolubles. C'est une variété extensive qui ne contient aucun groupe fini simple non abélien. Les 1) et 2) du théorème 23 fournissent alors l'énoncé suivant :

Corollaire 24.— *Le* $\mathrm{PIGF}_{/L}$ *admet une réponse positive pour tout corps intermédiaire* $k \subseteq L \subseteq k^{\text{rés}}$.

Remarques : 1) Ce résultat est novateur dans la mesure où de nombreux corps intermédiaires $k \subseteq L \subseteq k^{\text{rés}}$ sont non hilbertiens et dépassent donc le cadre d'application de [LP17]. Par exemple, pour tout nombre premier q, dans l'ensemble de ces corps intermédiaires non hilbertiens figure la pro-q-extension maximale de k, ce corps étant la $\mathscr{C}(q)$-clôture de k [20]. Comme autres corps intermédiaires, l'on trouve également les clôtures abélienne k^{ab} et nilpotente k^{nil} du corps k. Ces cas peuvent être

[17] En effet, fixons un groupe simple S et un épimorphisme $\pi : \Gamma \to S$. Puisque $G_2 \trianglelefteq \Gamma$, on a $\pi(G_2) \trianglelefteq S$. Ainsi, soit $\pi(G_2) = S$ et S est alors un quotient de G_2, soit $\pi(G_2) = \{1\}$ et, dans ces conditions, on a alors $G_2 \leq \ker(\pi)$, ce qui fournit un épimorphisme $G_1 = \Gamma/G_2 \to \Gamma/\ker(\pi) \cong S$.

[18] Il n'est même pas clair *a priori* que tout groupe alterné soit groupe de Galois régulier sur tout corps de caractéristique 2.

[19] Rappelons que, comme remarqué dans le 3) de la proposition 12, on a bien $\mathscr{C} \subseteq \widehat{\mathscr{C}}$.

[20] Ce corps est bien non hilbertien en vertu de la remarque qui précède la proposition 20.

obtenus directement par application du théorème 23 aux classes $\mathscr{C}(\mathrm{ab})$ et $\mathscr{C}(\mathrm{nil})$[21].

2) On voit facilement que la pro-2-extension maximale de $\mathbb{Q}$ est égale au corps $\mathbf{C}(i)$, où $\mathbf{C}$ désigne le corps des nombres réels constructibles à la règle et au compas. Si L désigne un sous-corps de $\mathbf{C}$ distinct de $\mathbb{Q}$, alors le corps L n'est la $\mathscr{C}_0$-clôture de $\mathbb{Q}$ pour aucune pré-formation $\mathscr{C}_0$. En effet, si c'était le cas, alors, par le premier point du 1) du théorème 19, on aurait $\mathbb{Z}/2\mathbb{Z} \in \mathscr{C}_0$. Mais, comme $\mathbb{Q}(i)/\mathbb{Q}$ est quadratique, on aurait $i \in L$, ce qui est impossible. Ceci permet en particulier d'exhiber un exemple d'extension galoisienne $M/\mathbb{Q}$ telle que M ne soit pas hilbertien, telle que le $\mathrm{PIGF}_{/M}$ admettte une réponse positive et telle que M ne soit la $\mathscr{C}_0$-clôture de $\mathbb{Q}$ pour aucune pré-formation $\mathscr{C}_0$: la clôture pythagoricienne de $\mathbb{Q}$, qui est par définition le plus petit corps L contenant $\mathbb{Q}$ tel que $L^2 = L^2 + L^2$. On renvoie par exemple à [Deso1] pour un aperçu des propriétés de la clôture pythagoricienne d'un corps donné.

Un autre exemple d'application peut être obtenu en considérant, pour un entier $n \geq 1$ donné, la classe $\mathscr{C}(\leq \mathrm{n})$ des groupes finis d'ordre au plus n. Il s'agit visiblement d'une pré-variété qui ne contient qu'un nombre fini de groupes alternés. De plus, pour $n \leq 244\,823\,039$ $(= |\mathrm{M}_{24}| - 1)$, elle ne contient pas le groupe de Mathieu M_{24} qui, comme déjà rappelé, possède une réalisation régulière sur tout corps de caractéristique 2 n'admettant qu'un seul point de branchement[22]. Par les 1) et 2) du théorème 23, on a donc :

Corollaire 25.— *Étant donné un entier naturel non nul n, si $p \neq 2$ ou $\overline{\mathbb{F}_2} \subseteq k$ ou $n \leq 244\,823\,039$, alors le $\mathrm{PIGF}_{/L}$ admet une réponse positive pour tout corps intermédiaire $k \subseteq L \subseteq k^{\mathscr{C}(\leq \mathrm{n})}$.*

5.2.— Sur l'écart entre le Problème Inverse de Galois et sa version Faible.

Comme déjà vu dans le §4.2, tout groupe fini se réalisant comme groupe de Galois sur la clôture résoluble d'un corps quelconque est nécessairement un groupe fortement non résoluble. Ainsi le corollaire 24 fournit un premier exemple de corps sur lequel le PIGF admet une réponse positive, mais pas le PIG.

Un exemple similaire peut être obtenu en considérant, pour un sous-ensemble non vide $\mathscr{P}_0$ donné de l'ensemble $\mathscr{P}$ des nombres premiers, la classe $\mathscr{C}(\mathscr{P}_0)$ des groupes finis G tels que tout diviseur premier de $|G|$ soit dans $\mathscr{P}_0$. Visiblement, $\mathscr{C}(\mathscr{P}_0)$ est une variété extensive non triviale et l'on voit que, si $\mathscr{P}_0 \neq \mathscr{P}$, alors $\mathscr{C}(\mathscr{P}_0)$ ne contient qu'un nombre fini de groupes alternés. Par conséquent, d'après le 1) du théorème 23 et le 2) du théorème 19, si $p \neq 2$ ou $\overline{\mathbb{F}_2} \subseteq k$, alors le $\mathrm{PIGF}_{/k^{\mathscr{C}(\mathscr{P}_0)}}$ admet une réponse positive, mais aucun élément non trivial de $\mathscr{C}(\mathscr{P}_0)$ ne se réalise comme groupe de Galois sur $k^{\mathscr{C}(\mathscr{P}_0)}$.

Puisque tout groupe fini non trivial G appartient à $\mathscr{C}(\mathscr{P}_0)$ pour au moins un $\mathscr{P}_0$ (dépendant de G), on obtient le résultat ci-dessous qui généralise le théorème 3 énoncé dans l'introduction :

Corollaire 26.— *On se donne une famille non vide $(G_i)_{i\in I}$ de groupes finis non triviaux telle qu'il existe au moins un nombre premier ne divisant aucun des ordres des groupes G_i $(i \in I)$, ainsi qu'un sous-ensemble non vide strict $\mathscr{P}_0$ de $\mathscr{P}$ contenant tous les diviseurs premiers des ordres des groupes G_i $(i \in I)$. Supposons que $p \neq 2$ ou bien que $\overline{\mathbb{F}_2} \subseteq k$. Alors le $\mathrm{PIGF}_{/k^{\mathscr{C}(\mathscr{P}_0)}}$ admet une réponse positive mais, pour tout $i \in I$, le groupe G_i ne se réalise pas comme groupe de Galois sur $k^{\mathscr{C}(\mathscr{P}_0)}$.*

Remarques : 1) Comme I est non vide, la remarque qui précède la proposition 20 permet d'affirmer qu'aucun corps $k^{\mathscr{C}(\mathscr{P}_0)}$ comme dans le corollaire 26 n'est hilbertien.

2) Comme autre exemple de classes permettant de démontrer le théorème 3, on peut citer la famille $\{\mathscr{C}(\mathrm{A}_{\geq n})^*\}_{n\geq 5}$, où $\mathscr{C}(\mathrm{A}_{\geq n})$ désigne la classe constituée des groupes alternés A_m pour $m \geq n$ et du groupe trivial. En effet, puisque $\mathscr{C}(\mathrm{A}_{\geq n})$ est visiblement une pré-formation, on déduit des 1) et 2) de la proposition 15 que la classe $\mathscr{C}(\mathrm{A}_{\geq n})^*$ vérifie les conditions $(\mathrm{C}_{1,2})$. D'après le résultat préliminaire de théorie des groupes du début de la preuve de la proposition 20, cette classe est en fait une formation extensive. Si G désigne un groupe fini d'ordre au plus n, alors $G \in \mathscr{C}(\mathrm{A}_{\geq n})^*$ et donc, en appliquant le 1) du théorème 23, le 2) du théorème 19 et la remarque qui précède la proposition 20, l'on voit que, si $p \neq 2$ ou $\overline{\mathbb{F}_2} \subseteq k$, alors le corps $k^{\mathscr{C}(\mathrm{A}_{\geq n})^*}$ est un corps non hilbertien pour lequel le PIGF admet une réponse positive, mais sur lequel G ne se réalise pas groupe de Galois.

[21] Par des résultats classiques de Kuyk, cf. [Kuy70, Corollaires 1 & 2], les corps k^{ab} et k^{nil} sont hilbertiens (puisque k l'est). Par conséquent, le fait que le PIGF possède une réponse positive sur ces deux corps, qui est alors une conséquence de [LP17], est réobtenu ici sans utiliser leur caractère hilbertien.

[22] Ce groupe est le plus grand groupe fini simple non abélien vérifiant cette propriété que nous connaissons.

Cette famille de classes contient les deux familles $\{\mathscr{C}(\leq \mathrm{n})\}_{n\geq 1}$ et $\{\mathscr{C}(\mathscr{P}_0)\}_{\emptyset\neq\mathscr{P}_0\subsetneq\mathscr{P}}$ présentées précédemment, ainsi que la classe $\mathscr{C}$(rés) [23]. Elle est intéressante car, en vertu de la propriété de dualité ensembliste b) du §3.3, la suite de classes $(\mathscr{C}(\mathrm{A}_{\geq n})^*)_{n\geq 5}$ est croissante pour l'inclusion et, par le raisonnement ci-dessus, l'on a $\bigcup_{n\geq 5}\mathscr{C}(\mathrm{A}_{\geq n})^* = \mathscr{C}(\mathrm{gr})$. Ainsi, en posant $k_n = k^{\mathscr{C}(\mathrm{A}_{\geq n})^*}$ pour tout $n \geq 5$, on obtient une suite croissante de corps $k \subseteq k_5 \subseteq k_6 \subseteq \cdots \subseteq k_n \subseteq \cdots$ telle que $\bigcup_{n\geq 5} k_n = k^{\mathrm{sép}}$ et telle que, pour tout $n \geq 5$, le PIGF admet une réponse positive sur k_n, mais pas le PIG (si $p \neq 2$ ou $\overline{\mathbb{F}_2} \subseteq k$).

Pour conclure cet article, nous attirons l'attention sur le fait que nous pouvons en fait construire une infinité de réalisations linéairement disjointes d'un groupe fini donné comme groupe d'automorphismes sur la $\mathscr{C}$-clôture considérée du corps hilbertien k dans les corollaires 24 à 26, et l'on peut aussi supposer que k est seulement RG-hilbertien.

Bibliographie

[AOS94] Shreeram S. Abhyankar, Jun Ou, and Avinash Sathaye. Alternating group coverings of the affine line for characteristic two. *Discrete Math.*, 133(1-3):25–46, 1994.

[AY94a] Shreeram S. Abhyankar and Ikkwon Yie. Small degree coverings of the affine line in characteristic two. *Discrete Math.*, 133(1-3):1–23, 1994.

[AY94b] Shreeram S. Abhyankar and Ikkwon Yie. Some more Mathieu group coverings in characteristic two. *Proc. Amer. Math. Soc.*, 122(4):1007–1014, 1994.

[Bae64] Reinhold Baer. Der reduzierte Rang einer Gruppe. (German). *J. Reine Angew. Math.*, 214/215:146–173, 1964.

[Bri04] David Brink. On alternating and symmetric groups as Galois groups. *Israel J. Math.*, 142:47–60, 2004.

[DD97] Pierre Dèbes and Bruno Deschamps. The regular inverse Galois problem over large fields. In *Geometric Galois actions 2*, volume 243 of *London Math. Soc. Lecture Note Ser.*, pages 119–138. Cambridge Univ. Press, Cambridge, 1997.

[Des01] Bruno Deschamps. Corps pythagoriciens, fermatiens et P-réduisants. (French). *J. Number Theory*, 88(1):114–128, 2001.

[DH99] Pierre Dèbes and Dan Haran. Almost Hilbertian fields. *Acta Arith.*, 88(3):269–287, 1999.

[DL13] Pierre Dèbes and François Legrand. Specialization results in Galois theory. *Trans. Amer. Math. Soc.*, 365(10):5259–5275, 2013.

[FJ08] Michael D. Fried and Moshe Jarden. *Field arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics],11. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden. xxiv + 792 pp.

[FK78] Ervin Fried and János Kollár. Automorphism groups of algebraic number fields. *Math. Z.*, 163(2):121–123, 1978.

[Fri80] Michael D. Fried. A note on automorphism groups of algebraic number fields. *Proc. Amer. Math. Soc.*, 80(3):386–388, 1980.

[FV92] Michael D. Fried and Helmut Völklein. The embedding problem over a Hilbertian PAC-field. *Ann. of Math. (2)*, 135(3):469–481, 1992.

[Kuy70] Willem Kuyk. Extensions de corps hilbertiens. *J. Algebra*, 14:112–124, 1970.

[LP17] François Legrand and Elad Paran. Automorphism groups over Hilbertian fields. 2017. To appear in Journal of Algebra. arXiv 1705.02606.

[MM99] Gunter Malle and B. Heinrich Matzat. *Inverse Galois Theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.

[23] au sens où chacune de ces classes est contenue dans $\mathscr{C}(\mathrm{A}_{\geq n})^*$ pour au moins un entier $n \geq 5$.

[RZ10] Luis Ribes and Pavel Zalesskii. *Profinite groups*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 40. Springer-Verlag, Berlin, second edition, 2010. xvi + 464 pp.

[Völ96] Helmut Völklein. *Groups as Galois groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996. xviii+248 pp.

[Zyw14] David Zywina. The inverse Galois problem for orthogonal groups. *Manuscript*, 2014. arXiv 1409.1151.

Bruno Deschamps

Laboratoire de Mathématiques Nicolas Oresme, CNRS UMR 6139
Université de Caen - Normandie
BP 5186, 14032 Caen Cedex - France

———————

Département de Mathématiques — Le Mans Université
Avenue Olivier Messiaen, 72085 Le Mans cedex 9 - France
E-mail : Bruno.Deschamps@univ-lemans.fr

François Legrand

Institut für Algebra, Fachrichtung Mathematik
TU Dresden, 01062 Dresden, Germany
E-mail : francois.legrand@tu-dresden.de