

PIERRE DÈBES

Groupes de Galois sur $K(T)$

Journal de Théorie des Nombres de Bordeaux 2^e série, tome 2, n° 2 (1990),
p. 229-243

http://www.numdam.org/item?id=JTNB_1990__2_2_229_0

© Université Bordeaux 1, 1990, tous droits réservés.

L'accès aux archives de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

Groupes de Galois sur $K(T)$

par PIERRE DÈBES

Soit K un corps de caractéristique 0. On dit qu'un groupe fini G a la propriété Gal_K , ce qu'on notera en abrégé $\text{Gal}_K(G)$ s'il existe une extension galoisienne E/K de K de groupe de Galois $G(E/K) = G$. Le "problème inverse de la théorie de Galois" est l'étude de la conjecture suivante.

CONJECTURE 1. Tout groupe fini G a la propriété $\text{Gal}_{\mathbb{Q}}$.

Le cas des groupes abéliens est facile : on utilise des extensions cyclotomiques. Le cas résoluble, beaucoup plus difficile, a été traité par Shafarevitch [Sha]. Le groupe symétrique S_n et le groupe alterné A_n sont d'autres exemples classiques, dus à Hilbert [Hi].

[Le groupe symétrique S_n a une action naturelle sur le corps $\mathbb{Q}(Y_1, \dots, Y_n)$. Le sous-corps fixé par cette action est le corps $\mathbb{Q}(T_1, \dots, T_n)$ engendré par les fonctions symétriques élémentaires de Y_1, \dots, Y_n . C'est une extension transcendante pure de \mathbb{Q} . On peut donc spécialiser rationnellement les indéterminées T_1, \dots, T_n de telle façon que l'extension résiduelle (de \mathbb{Q}) correspondante soit de même groupe de Galois que l'extension $\mathbb{Q}(Y_1, \dots, Y_n)/\mathbb{Q}(T_1, \dots, T_n)$, i.e., S_n .]

L'argument final de la construction s'appuie sur le théorème d'irréductibilité de Hilbert, qui, sous sa forme la plus simple énonce que, si $P(T, Y)$ est un polynôme irréductible dans $\mathbb{Q}(T)[Y]$, alors, pour une infinité de nombres rationnels t , le polynôme $P(t, Y)$ est irréductible dans $\mathbb{Q}[Y]$.

En particulier, pour tout groupe G , on a :

$$(1) \quad \text{Gal}_{\mathbb{Q}(T)}(G) \Rightarrow \text{Gal}_{\mathbb{Q}}(G).$$

C'est par ce biais qu'on aborde le cas non résoluble. On transpose ainsi le problème sur le corps $\mathbb{Q}(T)$ où on trouve un angle d'attaque géométrique. On sait en effet qu'une extension de $\mathbb{Q}(T)$, si elle est régulière sur \mathbb{Q} , correspond à un revêtement, défini sur \mathbb{Q} , de la droite projective \mathbb{P}_1 . Rappelons qu'une extension $E/K(T)$ est dite régulière sur K si le corps K est algébriquement fermé dans E , i.e., $E \cap \bar{K} = K$. On dira qu'un groupe fini G a la propriété RGal_K s'il existe une extension galoisienne de $K(T)$, régulière sur K et de groupe de Galois G .

CONJECTURE 2. Tout groupe fini G a la propriété $\text{RGal}_{\mathbb{Q}}$.

Note. Le Conj.2 s'énonce de façon équivalente : tout groupe fini G a la propriété RGal_K pour tout corps K de caractéristique 0.

La Conj.2 entraîne la Conj.1. D'après [Hi], elle est vraie pour le groupe symétrique S_n et le groupe alterné A_n . Elle l'est également pour les groupes abéliens [Se3;Ch5]. Citons aussi le résultat de Shih ([Shi1],[Shi2]) : le groupe $PSL_2(\mathbb{F}_p)$ a la propriété $\text{RGal}_{\mathbb{Q}}$ si p est un nombre premier vérifiant l'une des conditions suivantes :

$$(2) \quad \left(\frac{2}{p}\right) = -1; \left(\frac{3}{p}\right) = -1; \left(\frac{7}{p}\right) = -1$$

[Shih utilise l'action de Galois sur les points de p -torsion d'une courbe elliptique. Si E désigne une courbe elliptique définie sur un corps K , considérons $E[p]$ le \mathbb{F}_p -espace vectoriel des points de p -torsion de E . L'action de $G(\overline{K}/K)$ sur $E[p]$ induit un homomorphisme

$$G(\overline{K}/K) \rightarrow PGL_2(\mathbb{F}_p)$$

Sous une certaine condition sur E et p , on peut "tordre" cette représentation de $G(\overline{K}/K)$ de façon à ce qu'elle prenne ses valeurs dans $PSL_2(\mathbb{F}_p)$. La donnée "courbe elliptique + p -torsion" est paramétrée par la courbe modulaire $X_0(p)$. A l'aide de cette description, on arrive à montrer que dans la précédente construction, on peut prendre $K = \mathbb{Q}(T)$ (voir [Se3;Ch6] pour des détails.)

Les travaux de Shih datent du milieu des années 70. C'est quelques années plus tard qu'apparaît la méthode dite "de rigidité". Cette méthode a permis une avancée importante du problème dans le cas des groupes simples non abéliens. Les résultats sont de deux types : une version forte où on montre qu'un groupe G a la propriété $\text{RGal}_{\mathbb{Q}}$ et une seconde version plus faible où on démontre seulement la propriété RGal_K pour $K = \mathbb{Q}^{ab}$, la clôture abélienne de \mathbb{Q} . Pour cette seconde version, les résultats sont presque complets : il ne manque essentiellement que les deux familles de groupes simples 2B_2 et 2F_4 . En revanche, ils sont beaucoup plus partiels pour la première : la propriété $\text{RGal}_{\mathbb{Q}}$ a été démontrée pour

- Le groupe alterné A_n
- 23 des 24 groupes sporadiques (manque le groupe de Mathieu M_{24})
- Quelques unes des familles classiques de groupes simples comme $PSL_2, PSL_3, PSU_3, PSp_4$, quand le corps de base est \mathbb{F}_p où p est un nombre premier devant vérifier de surcroît certaines conditions (du type (2))
- Quelques autres groupes épars : $PSL_2(\mathbb{F}_{25}), PSL_2(\mathbb{F}_{p^2})$ si $p \equiv \pm 2 \pmod{5}, \dots$

On consultera [Ma1], [Ma2] et [Ma3] pour un point précis des résultats.

La rigidité impose diverses contraintes à la ramification des extensions cherchées. On commence par fixer les points de ramification de ces extensions. Soient t_1, \dots, t_r r points distincts dans $\mathbf{P}_1(\overline{K})$ et Ω l'extension algébrique maximale de $\overline{K}(T)$ non ramifiée en dehors de t_1, \dots, t_r . L'extension $\Omega/K(T)$ est galoisienne ; son groupe de Galois se note Π^{alg} : c'est le groupe fondamental algébrique de $\mathbf{P}_1(\overline{K}) \setminus \{t_1, \dots, t_r\}$.

Si le diviseur $(t_1) + \dots + (t_r)$ de \mathbf{P}^1 est K -rationnel, l'extension $\Omega/K(T)$ est également galoisienne. On note Π_K son groupe de Galois. La théorie de Galois fournit la suite exacte :

$$(3) \quad 1 \longrightarrow \Pi^{alg} \longrightarrow \Pi_K \longrightarrow \Lambda_K \longrightarrow 1$$

où $\Lambda_K = G(\overline{K}/K)$

Étant donné un groupe G , la propriété $\text{Gal}_{K(T)}(G)$ équivaut à l'existence d'un homomorphisme $\Phi : \Pi_K \rightarrow G$ surjectif ; la propriété RGal_K est satisfaite si de plus la restriction de Φ à Π^{alg} reste surjective.

On fait ensuite les deux observations suivantes.

1- La construction d'un homomorphisme surjectif $\varphi : \Pi^{alg} \rightarrow G$ ne pose pas de problèmes. En effet, la structure du groupe Π^{alg} est bien connue. Notons Π le groupe libre à r générateurs x_1, \dots, x_r avec la relation $x_1 \dots x_r = 1$; on reconnaît le groupe fondamental topologique de $\mathbf{P}_1(\mathbf{C}) \setminus \{t_1, \dots, t_r\}$. Le groupe Π^{alg} est isomorphe au complété profini $\hat{\Pi}$ du groupe Π , i.e., la limite projective des quotients de Π par des sous-groupes normaux d'indice fini. Plus précisément, il existe un isomorphisme entre ces deux groupes qui envoie chacun des x_i sur un générateur d'un groupe d'inertie au dessus de t_i de l'extension $\Omega/\overline{K}(T)$ ([Se3; Th.7.5 p. 69]).

On définit φ en posant $\varphi(x_i) = g_i, i = 1, \dots, r$ où g_1, \dots, g_r sont des générateurs de G vérifiant $g_1 \dots g_r = 1$. Il suffit donc de choisir r suffisamment grand.

[Structure des groupes d'inertie. Considérons une extension galoisienne finie $Y/\overline{K}(T)$ de groupe de Galois G , non ramifiée en dehors de t_1, \dots, t_r . Les groupes d'inertie au dessus d'un point de ramification t_i sont cycliques et deux à deux conjugués dans G . Notons, pour $i = 1, \dots, r$, e_i leur ordre. La théorie des corps locaux ou plus simplement l'utilisation de séries de Puiseux montre que, pour $i = 1, \dots, r$ et pour chaque groupe d'inertie I au dessus de t_i , il y a un isomorphisme compatible avec l'action de Λ_K , entre I et le groupe μ_{e_i} des racines de l'unité d'ordre e_i . Choisissons un système $(z_n)_n$ cohérent de racines de l'unité (i.e., $(z_{nm})^m = z_n$ pour tous n, m) ; cela permet de munir chacun des groupes d'inertie d'un générateur "canonique". Alors on

peut demander à l'isomorphisme $\hat{\Pi} \rightarrow \Pi^{alg}$ d'envoyer x_i sur le générateur "canonique" d'un des groupes d'inertie au dessus de t_i .]

Il s'agit de voir maintenant à quelle condition l'homomorphisme φ se prolonge à Π_K .

2 - La suite exacte (3) est scindée,

[pour tout $t_0 \in \mathbf{P}_1(K)\{t_1, \dots, t_r\}$, Ω se plonge dans $\overline{K}((T-t_0))$ où Λ_K opère naturellement. L'action induite sur Ω définit une section $\Lambda_K \rightarrow \Pi_K$ de l'homomorphisme $\Pi_K \rightarrow \Lambda_K$.]

de sorte que le groupe Π_K est isomorphe au produit semi-direct $\Pi^{alg} \times^s \Lambda_K$; l'action de $\tau \in \Lambda_K$ sur Π^{alg} sera notée $x \rightarrow x^\tau$. On vérifie sans peine qu'un homomorphisme de groupes $\varphi : \Pi^{alg} \rightarrow G$ se prolonge au produit semi-direct $\Pi^{alg} \times^s \Lambda_K$ si et seulement si il existe un morphisme $\tau \rightarrow \varphi_\tau$ de Λ_K dans G qui vérifie la condition de compatibilité suivante :

$$(4) \quad \varphi(x^\tau) = \varphi_\tau \varphi(x) (\varphi_\tau)^{-1} \text{ pour tout } x \in \Pi^{alg} \text{ et tout } \tau \in \Lambda_K.$$

On obtient en définitive le critère suivant.

THÉORÈME 1. *Un groupe fini G a la propriété RGal_K ssi il existe*

- un entier $r > 0$, un diviseur K -rationnel de $\mathbf{P}_1(\overline{K})$, $t_0 \in \mathbf{P}_1(K) \setminus \{t_1, \dots, t_r\}$
- des éléments g_1, \dots, g_r de G engendrant G et de produit $g_1 \dots g_r = 1$
- un morphisme de groupes $\begin{cases} \Lambda_K \rightarrow G \\ \tau \rightarrow \varphi_\tau \end{cases}$

tels que le morphisme $\varphi : \Pi^{alg} \rightarrow G$ défini par $\varphi(x_i) = g_i, i = 1, \dots, r$ vérifie :

$$(5) \quad \varphi(x_i^\tau) = \varphi_\tau g_i (\varphi_\tau)^{-1} \text{ pour tout } i = 1, \dots, r \text{ et tout } \tau \in \Lambda_K.$$

Note. Si $(\varphi_\tau)_\tau$ est une famille d'éléments de G vérifiant (5), la famille $((\varphi_{\tau\tau'}^{-1}(\varphi_\tau)(\varphi_{\tau'}))_{\tau, \tau'}$ définit un cocycle de Λ_K à valeurs dans le centre $Z(G)$ du groupe G . Donc, si le groupe $H^2(K, Z(G))$ est trivial (e.g., $Z(G) = 1$ ou $K = \mathbb{Q}^{ab}$), il n'est pas nécessaire de demander dans le Th.1 que l'application $\tau \rightarrow \varphi_\tau$ soit un morphisme du groupe.

Toute la question est de connaître les x_i^τ , i.e., l'action de Λ_K sur Π^{alg} . Voici ce qu'on peut dire sur les x_i^τ .

- (i) $x_1^\tau, \dots, x_r^\tau$ engendrent le groupe Π^{alg}
- (ii) $x_1^\tau \dots x_r^\tau = 1$

- (iii) Pour $i = 1, \dots, r$, x_i^τ est conjugué dans Π^{alg} à $(x_j)^{X_K(\tau)}$, où $t_j = t_i^\tau$ et X_K désigne le caractère cyclotomique $X_K : \Lambda_K \rightarrow \prod_N G(K(\mu_N)/K)$ du corps K .

[Seul (iii) demande quelques explications. Considérons une extension galoisienne finie $Y/\overline{K}(T)$ de groupe de Galois G , non ramifiée en dehors de t_1, \dots, t_r . Sous l'action de $\tau \in \Lambda_K$, x_i est envoyé sur un générateur d'un des groupes d'inertie au dessus de $t_j = t_i^\tau$. Ces groupes sont cycliques et conjugués dans G ; leurs générateurs sont donc des conjugués d'une puissance a -ième de x_j , où a est premier avec e_j . Pour voir qu'on peut prendre $a = X_K(\tau)$, il faut utiliser que les x_i sont des générateurs "canoniques" et que les isomorphismes $I \rightarrow \mu_{e_i}$ sont compatibles avec l'action de Λ_K (voir "Structure des groupes d'inertie" plus haut).]

Nous montrons maintenant dans diverses situations comment utiliser le Théorème 1.

Situation 1 : Rigidité avec $K = \mathbb{Q}$ ou $K = \mathbb{Q}^{ab}$.

Le Th.2 ci-dessous est le résultat principal de la méthode. Il est dû indépendamment à Belyi, Fried, Matzat, Shih et Thompson. On se donne un groupe G et des éléments g_1, \dots, g_r de G engendrant G et de produit $g_1 \dots g_r = 1$. Pour $i = 1, \dots, r$, on note C_i la classe de conjugaison de g_i dans G . On rappelle que C_i est dite rationnelle si $g_i^a \in C_i$ pour tout entier a premier à l'ordre de g_i .

Considérons l'ensemble

$$(6) \quad \sum(C_1, \dots, C_r) = \left\{ (g'_1, \dots, g'_r) \in G^r \mid \left\{ \begin{array}{l} g'_1, \dots, g'_r \text{ engendrent } G \\ g'_1 \dots g'_r = 1 \\ g'_i \in C_i \text{ pour } i = 1, \dots, r \end{array} \right. \right\}$$

Il y a une action naturelle du groupe G sur l'ensemble $\sum(C_1, \dots, C_r)$: on fait opérer chaque élément g de G par conjugaison sur chacune des composantes d'un élément de $\sum(C_1, \dots, C_r)$.

THÉORÈME 2. *Si les trois hypothèses suivantes sont satisfaites,*

(H₁) $Z(G) = \{1\}$

(H₂) C_1, \dots, C_r sont rationnelles

(H₃) L'action de G sur $\sum(C_1, \dots, C_r)$ est transitive,

alors le groupe G a la propriété $\text{RGal}_{\mathbb{Q}}$ avec t_1, \dots, t_r quelconques dans $\mathbb{P}_1(\mathbb{Q})$.

Preuve. On choisit de façon quelconque $r + 1$ points t_1, \dots, t_r, t_0 dans $\mathbb{P}_1(\mathbb{Q})$. Soit $\tau \in \Lambda_{\mathbb{Q}}$. Il résulte des propriétés (i), (ii), (iii) des x_i^τ et de l'hypothèse (H₂) que

le r-uple $(\varphi(x_1^\tau), \dots, \varphi(x_r^\tau))$ est un élément de $\sum(C_1, \dots, C_r)$. D'après (H₃), il existe $\varphi_\tau \in G$ tel que

$$(\varphi(x_1^\tau), \dots, \varphi(x_r^\tau)) = \varphi_\tau(g_1, \dots, g_r)(\varphi_\tau)^{-1}.$$

Note. L'hypothèse (H₂) est nécessaire si on précise dans la conclusion du Th.2 que pour $i = 1, \dots, r$, C_i est la classe de conjugaison des générateurs "canoniques" des groupes d'inertie au dessus de t_i : en effet, la rationalité de C_i résulte alors de celle de t_i (utiliser (iii)).

Si $K = \mathbb{Q}^{ab}$, on a besoin ni de l'hypothèse (H₁) (voir note plus haut), ni de l'hypothèse (H₂).

THÉORÈME 3. *Si l'hypothèse (H₃) est satisfaite, alors le groupe G a la propriété $\text{RGal}_{\mathbb{Q}^{ab}}$ avec t_1, \dots, t_r quelconques dans $\mathbb{P}_1(\mathbb{Q}^{ab})$.*

[La démonstration est identique à celle du Th.1. Il faut juste remarquer que le caractère cyclotomique $X_{\mathbb{Q}^{ab}}$ est trivial. Par conséquent, si t_1, \dots, t_r sont choisis dans $\mathbb{P}_1(\mathbb{Q}^{ab})$, pour tout $\tau \in \Lambda_K$ et $i = 1, \dots, r$, x_i^τ est conjugué dans Π^{alg} à x_i . On obtient donc que $\varphi(x_i^\tau)$ est automatiquement conjugué à g_i dans G , sans qu'il soit besoin de faire appel à l'hypothèse (H₂).]

C'est l'hypothèse (H₃) qu'on appelle plus spécifiquement hypothèse de rigidité. Il s'agit d'une hypothèse assez contraignante ; en particulier, pratiquement, elle impose $r \leq 3$. Elle est cependant satisfaite par de nombreux groupes simples : la plupart des résultats cités en introduction se déduisent en effet des Th.2 et Th.3 ou de variantes approchantes. On trouvera plus de détails sur ces applications précises dans [Se3] et [Ma2].

Situation 2 : $K = \mathbb{R}$.

On a $\Lambda_K = \{1, c\}$ où c désigne la conjugaison complexe. Il s'agit d'une situation assez particulière puisque l'action de c sur le groupe $\Pi^{alg} \simeq \hat{\Pi}$ provient d'une action sur le groupe Π , à savoir l'action naturelle de la conjugaison complexe sur le groupe fondamental topologique $\pi_1(\mathbb{P}_1(\mathbb{C}) \setminus \{t_1, \dots, t_r, t_0\}) \simeq \Pi$.

$$(7) \quad \begin{array}{ccc} \Lambda_K = \{1, c\} & \longrightarrow & \text{Aut}(\Pi^{alg}) \\ & \searrow & \uparrow \\ & & \text{Aut}(\Pi) \end{array}$$

De plus, l'action de c sur le groupe Π peut être explicitée. Si t_1, \dots, t_r, t_0 sont dans $\mathbf{P}_1(\mathbf{R})$ et apparaissent dans cet ordre sur la droite projective réelle, on peut choisir les classes d'homotopie x_1, \dots, x_r dans $\pi_1(\mathbf{P}_1(\mathbf{C}) \setminus \{t_1, \dots, t_r\}, t_0)$ de telle façon qu'on ait les formules suivantes.

$$(8) \quad \left\{ \begin{array}{l} x_1^c = (x_2 \dots x_r)^{-1} x_1^{-1} (x_2 \dots x_r) \\ x_2^c = (x_3 \dots x_r)^{-1} x_2^{-1} (x_3 \dots x_r) \\ \cdot \\ \cdot \\ \cdot \\ x_r^c = x_r^{-1} \end{array} \right.$$

Ces formules étaient connues d'Hurwitz [Hu ; p. 357] ; on les trouve aussi dans [KN]. Combinées au Th.1, elles conduisent au résultat suivant [DFr2].

THÉORÈME 4. *Un groupe G a la propriété $\text{RGal}_{\mathbf{R}}$ avec points de ramification t_1, \dots, t_r dans $\mathbf{P}_1(\mathbf{R})$ si et seulement si le groupe G est engendré par r éléments d'ordre ≤ 2 .*

PREUVE: La condition (5) du Th.1 s'écrit

$$(9) \quad \left\{ \begin{array}{ll} (g_2 \dots g_r)^{-1} g_1^{-1} (g_2 \dots g_r) & = \varphi_c g_1 \varphi_c \\ \cdot & \\ \cdot & \\ \cdot & \\ g_r^{-1} g_{r-1}^{-1} g_r & = \varphi_c g_{r-1} \varphi_c \\ g_r^{-1} & = \varphi_c g_r \varphi_c \end{array} \right.$$

De la dernière ligne, on déduit que $\varphi_c g_r$ est d'ordre au plus 2, des deux dernières lignes que $\varphi_c g_{r-1} g_r$ est d'ordre au plus 2, etc...

Le Th.4 appelle deux commentaires. Rappelons en premier lieu qu'on sait montrer que tout groupe G a la propriété $\text{RGal}_{\mathbf{R}}$. La méthode est analogue mais on choisit pour points de ramification $r/2$ paires de nombres complexes conjugués (voir [Se3; Ex. p. 107] et aussi [DFr2; Th.3.1]). Remarquons en second lieu que le Th.4 fournit une condition nécessaire pour qu'un groupe ait la propriété $\text{RGal}_{\mathbf{Q}}$ avec points de ramification t_1, \dots, t_r dans $\mathbf{P}_1(\mathbf{R})$. En particulier, le Th.4 montre les limites du cas "rigide" : les groupes obtenus par le Th.1, par exemple le Monstre, sont engendrés par 3 éléments d'ordre ≤ 2 .

[En fait, on peut vérifier directement que tout groupe G qui satisfait l'hypothèse (H_3) avec de plus $C_i = C_i^{-1}$ pour $i = 1, \dots, r$, peut être engendré par r éléments d'ordre ≤ 2].

On peut se demander si inversement tout groupe engendré par 3 éléments d'ordre ≤ 2 , de centre trivial a la propriété $\text{RGal}_{\mathbb{Q}}$ avec $r = 3$. La réponse est non : pour le groupe diédral D_p d'ordre $2p$, qui est engendré par 2 éléments d'ordre 2, il en faut (beaucoup) plus que 3. Précisément, on a :

THÉORÈME 5. *Supposons p premier > 7 . Si le groupe D_p a la propriété $\text{RGal}_{\mathbb{Q}}$ avec r points de ramification, alors $r \geq 6$.*

On trouvera une démonstration complète dans [DFr2]. Le cas essentiel est celui où $r = 4$ et où tous les groupes d'inertie sont d'ordre 2. On montre dans ce cas que la propriété $\text{RGal}_{\mathbb{Q}}$ est l'équivalente à l'existence d'un point de p -torsion \mathbb{Q} -rationnel sur une courbe elliptique définie sur \mathbb{Q} . Il faut donc recourir au Théorème de Mazur [Se1] pour conclure. Anticipons sur la suite de l'exposé pour dire que cet exemple est d'autant plus intéressant que l'espace de Hurwitz associé à cette situation est irréductible, défini sur \mathbb{Q} et possède des points réels (et même ℓ -adiques pour tout nombre premier ℓ) (cf. Situation 4.(6)).

Situation 3 : $K = \mathbb{Q}_p$.

Il est naturel de demander s'il existe des formules analogues à (8) dans la situation $K = \mathbb{Q}_p, t_1, \dots, t_r$ choisis dans \mathbb{Q}_p et avec c remplacé par le Frobenius $F_p \in \Lambda_{\mathbb{Q}_p}$. La réponse est non. De façon précise, l'action de F_p sur Π^{alg} ne provient pas d'une action sur Π telle que

$$(10) \quad x_i^{F_p} \text{ est conjugué dans } \Pi \text{ à } x_i^p, \text{ pour } i = 1, \dots, r.$$

[La raison est simple : si (10) était vrai, le groupe Π serait engendré par des conjugués de x_i^p , $i = 1, \dots, r$; mais alors tout groupe engendré par des éléments d'ordre p serait trivial ! On peut donner une autre explication. Dans (10), l'exposant p remplace dans le contexte p -adique l'exposant $-1 = X_{\mathbb{R}}(c)$ de la situation 2. Or, p n'est pas la valeur du caractère cyclotomique $X_{\mathbb{Q}_p}$ en F_p : en effet, l'action de F_p sur μ_N n'est l'élévation à la puissance p -ième que si p ne divise pas N .]

Ce paragraphe est aussi l'occasion de rappeler ce résultat de Harbater [Ha].

THÉORÈME 6. *Tout groupe G a la propriété $\text{RGal}_{\mathbb{Q}_p}$, pour tout nombre premier p .*

La méthode qu'il emploie est très différente de la nôtre. Il commence

par établir la propriété $\text{RGal}_{\mathbb{Q}_p}$ pour les groupes cycliques. Il montre ensuite comment “coller ensemble” plusieurs revêtements cycliques, ou si l’on préfère, comment à partir de plusieurs extensions régulières $E_i/\mathbb{Q}_p(T)$ de groupes de Galois des sous-groupes cycliques $G_i, i = 1, \dots, s$ d’un groupe G , on peut, sous certaines conditions, construire une extension régulière $E/\mathbb{Q}_p(T)$ de groupe de Galois $G_1 \dots G_r$. Le résultat clé de cette seconde étape est le Théorème d’existence de Grothendieck, un analogue non archimédien des théorèmes GAGA de Serre.

Situation 4 : Espaces de Hurwitz.

Dans cette section, on fait varier les points de ramification t_1, \dots, t_r . La donnée (t_1, \dots, t_r) décrit la variété algébrique notée \mathcal{U}^r , obtenue en enlevant à $(\mathbb{P}_1)^r$ l’ensemble de tous les r -uplets (t_1, \dots, t_r) dont deux au moins des composantes sont égales. Nous noterons \mathcal{U}_r la variété \mathcal{U}^r/S_r quotient de \mathcal{U}^r par l’action du groupe symétrique S_r ; la variété \mathcal{U}_r paramètre les ensembles de r points distincts de \mathbb{P}_1 .

Fixons un entier r , un groupe G et r classes de conjugaison C_1, \dots, C_r du groupe G . Et pour $\{t_1, \dots, t_r\}$ variant dans \mathcal{U}_r , regardons l’ensemble de toutes

(11) les extensions galoisiennes de $\overline{K}(T)$ non ramifiées en dehors de t_1, \dots, t_r , de groupe de Galois G et telles que, pour $i = 1, \dots, r$, les générateurs canoniques (cf. “Structure des groupes d’inertie” plus haut) des groupes d’inertie au dessus de t_i soient dans C_{σ_i} , pour un certain $\sigma \in S_r$ ou, de façon équivalente, l’ensemble de tous

(12) les G -revêtements de \mathbb{P}_1 (i.e., revêtements galoisiens de \mathbb{P}_1 de groupe G donnés avec l’action de G) non ramifiés en dehors de t_1, \dots, t_r et tels que, pour $i = 1, \dots, r$ et pour un certain $\sigma \in S_r$, C_{σ_i} soit, à l’intérieur du groupe de monodromie G , la classe de conjugaison des cycles de ramification correspondant à des lacets “tournant une fois autour de t_i ”.

D’après un résultat fondamental de M. Fried (e.g. [Fr1],[DFr1],[FrV]), sous certaines conditions, on peut mettre une structure algébrique sur l’ensemble des objets (11) (ou (12)). De façon plus précise, si G est un groupe de centre trivial, alors il existe une famille algébrique de revêtements de \mathbb{P}_1

$$\mathcal{T} \rightarrow \mathcal{H} \times \mathbb{P}_1$$

avec la propriété suivante :

(13) les membres ou fibres de cette famille $\mathcal{T}_{\mathbf{x}} \rightarrow \mathbb{P}_1, \mathbf{x} \in \mathcal{H}$, correspondent de façon biunivoque aux classes d’équivalence des revêtements décrits

en (12).

L'espace \mathcal{H} est appelé espace de Hurwitz associé à la donnée $\mathbf{C} = (C_1, \dots, C_r)$; on le note $\mathcal{H}(\mathbf{C})$ quand on veut indiquer cette dépendance. L'espace de Hurwitz est défini sur K si \mathbf{C} est un r -uple K -rationnel de classes de conjugaisons de G , i.e., s'il est invariant, à l'ordre près, sous l'élévation à la puissance $X_K(\tau)$ -ième, pour tout $\tau \in \Lambda_K$. Et dans ce cas on a

THÉORÈME 7. *Les propositions suivantes sont équivalentes*

- (a) $\mathcal{H}(K) \neq \emptyset$
- (b) Il existe un G -revêtement comme en (12) qui est défini sur K .
- (c) Il existe une extension de $\overline{K}(T)$ comme en (11) qui provient, par extension des scalaires, d'une extension galoisienne et régulière de $K(T)$.

En particulier $\mathcal{H}(K) \neq \emptyset \Rightarrow \text{RGal}_K(G)$

Voici quelques points concernant les espaces de Hurwitz :

[1] Les revêtements $\mathcal{H} \rightarrow \mathcal{U}_r$ et $\mathcal{H}' \rightarrow \mathcal{U}^r$. Il existe une flèche naturelle $\mathcal{H} \rightarrow \mathcal{U}_r$ qui envoie $\mathbf{x} \in \mathcal{H}$ sur l'ensemble des points de ramification du revêtement fibre $\mathcal{T}_{\mathbf{x}} \rightarrow \mathbb{P}_1$; c'est un morphisme [DFr1;Lemma1.5]. Notons \mathcal{H}' le pull-back de \mathcal{H} au-dessus de l'application naturelle $\mathcal{U}^r \rightarrow \mathcal{U}_r$. On a donc le diagramme commutatif suivant :

$$(14) \quad \begin{array}{ccc} & & \mathcal{H}' \\ & \swarrow & \downarrow \\ \mathcal{H} & & \mathcal{U}^r \\ \downarrow & \swarrow & \\ \mathcal{U}_r & & \end{array}$$

Les deux flèches verticales sont des revêtements finis non ramifiés. On peut décrire de façon explicite les actions de groupes associées à ces revêtements. Sans rentrer dans les détails, disons que les groupes fondamentaux des espaces \mathcal{U}^r et \mathcal{U}_r sont bien connus : ce sont les "groupes de tresses" d'Hurwitz, des quotients des groupes des tresses d'Artin. Qu'il existe une action naturelle de ces groupes de tresses sur les ensembles

$$(15) \quad \bigcup_{\sigma \in S_r} \Sigma(C_{\sigma_1}, \dots, C_{\sigma_r}) \quad \text{et} \quad \Sigma(C_1, \dots, C_r)$$

(L'ensemble $\Sigma(C_1, \dots, C_r)$ est défini en (6))

Et qu'alors les deux revêtements verticaux de (14) sont les revêtements non ramifiés de \mathcal{U}^r et \mathcal{U}_r associés à l'action des groupes de tresses sur les ensembles quotients de (15) par l'action du groupe G . En particulier, les espaces \mathcal{H} et \mathcal{H}' sont irréductibles si et seulement si ces actions sont transitives. On trouvera plus de détails dans [BFr],[Fr2] ou [FrV].

[2] *Cas particulier: rigidité.* Le revêtement vertical de droite en (14) est un revêtement de degré $|\sum(C_1, \dots, C_r)/G|$. Sous l'hypothèse (H_3) de rigidité, c'est donc un isomorphisme. D'autre part, sous l'hypothèse (H_2) , il est défini sur \mathbb{Q} . L'espace \mathcal{H}' est donc dans ce cas un ouvert de $(\mathbb{P}_1)^r$: on retrouve le Th.2.

[3] *Un autre cas de rationalité.* Supposons \mathcal{H}' irréductible. On peut en privilégiant une des variables t_1, \dots, t_r , par exemple t_1 , voir la flèche $\mathcal{H}' \rightarrow \mathcal{U}^r$ comme une famille de revêtements de \mathbb{P}_1 paramétrée par les $r - 1$ autres variables. La ramification de ces revêtements est parfaitement connue : ils sont ramifiés aux points t_2, \dots, t_r et les cycles de ramification associés sont donnés par des formules explicites dans un groupe de tresses approprié [BFr]. On peut donc calculer le genre $g(\mathcal{C})$ de ces revêtements grâce à la formule de Riemann-Hurwitz. Dans certaines situations, l'examen de la ramification permet également de conclure à l'existence générique d'un point rationnel au-dessus d'un des points de ramification t_2, \dots, t_r . Si c'est le cas et si le genre est nul, la variété \mathcal{H}' est une variété K -rationnelle ; en particulier $\mathcal{H}'(K) \neq \emptyset$.

Cette méthode a été utilisée pour démontrer la propriété $\text{RGal}_{\mathbb{Q}}$ pour plusieurs groupes simples, en particulier parmi les groupes simples sporadiques [Ma2]. Les calculs sont malheureusement très compliqués et nécessitent même parfois l'usage d'un ordinateur. Un programme adapté à ce genre de calculs a été conçu par Matzat.

La même méthode est utilisée dans [DFr2] pour étudier l'exemple suivant.

Exemple. Le groupe G est le groupe symétrique S_n et $r = 4$. On se donne 3 générateurs $\alpha_1, \alpha_2, \alpha_3$ d'ordre 2 de S_n et on définit C_1, \dots, C_4 comme les classes de conjugaison dans S_n des éléments $\alpha_1, \alpha_1\alpha_2, \alpha_2\alpha_3, \alpha_3$. Noter que le 4-uplet $(\alpha_1, \alpha_1\alpha_2, \alpha_2\alpha_3, \alpha_3)$ est dans l'ensemble $\sum(C_1, \dots, C_4)$ et qu'il vérifie les formules (9) avec $\varphi_c = 1$. Dans le cas où \mathcal{H}' est une variété \mathbb{Q} -rationnelle, cela permet de conclure à l'existence d'une extension galoisienne régulière $E/\mathbb{Q}(T)$ de groupe S_n ramifiée en $r = 4$ points rationnels et telle que les extensions résiduelles E_t/\mathbb{Q} soient totalement réelles pour tout t dans un ouvert non vide de $\mathbb{P}_1(\mathbb{R})$. Serre a montré dans [Se2] que pour $r = 3$ à la place de $r = 4$, seul le groupe S_3 a cette propriété. Nous avons calculé le genre $g(\mathcal{C})$ pour divers choix des générateurs $\alpha_1, \alpha_2, \alpha_3$ et obtenu la \mathbb{Q} -rationalité de \mathcal{H}' dans les cas suivants : $n=4,5,6,7,10$.

[4] *Points réels sur \mathcal{H}' .* Les formules de type (8) fournissent des critères d'existence de points réels sur les espaces \mathcal{H} et \mathcal{H}' . On a ainsi

THÉORÈME 4 BIS. $\mathcal{H}'(\mathbb{R}) \neq \emptyset$ si et seulement s'il existe un r -uplet (g_1, \dots, g_r) et un élément κ dans G vérifiant

- (a) $(g_1, \dots, g_r) \in \sum(C_{\sigma_1}, \dots, C_{\sigma_r})$ pour un certain $\sigma \in S_r$
- (b) Les éléments $\kappa, \kappa g_1, \kappa g_1 g_2, \dots, \kappa g_1 g_2 \dots g_{r-1}$ sont d'ordre ≤ 2 .

[5] On connaît de nombreux exemples où $\mathcal{H}(\mathbb{R}) \neq \emptyset$ et $\mathcal{H}(\mathbb{Q}_p) \neq \emptyset$ pour tout nombre premier p .

[La construction suivante a été inspirée par [Ha]. Soit G un groupe engendré par ρ éléments h_1, \dots, h_ρ d'ordre 2 (par exemple un groupe simple non abélien). Pour tout nombre premier p et pour $i = 1, \dots, \rho$, choisissons un polynôme irréductible f_i dans $\mathbb{F}_p[T]$ de degré $d_i = i$. Fixons également un relèvement F_i de f_i dans $\mathbb{Z}[T]$ de même degré que f_i .

Pour tout p , l'équation $Y^2 = F_i(T)(F_i(T) - p)$ définit un revêtement $\Phi_i : Y_i \rightarrow \mathbb{P}_1$ cyclique de degré 2, défini sur \mathbb{Q}_p . Pour $i = 1, \dots, \rho$, l'ensemble $R_{p,i}$ des points de ramification de Φ_i comporte $2i$ points, à savoir les zéros de $F_i(T) = 0$ et ceux de $F_i(T) = p$. Par construction, les ensembles $R_{p,i}, i = 1, \dots, \rho$ sont deux à deux disjoints modulo p . D'autre part, modulo p, Y_i éclate en deux composantes qui s'envoient isomorphiquement sur \mathbb{P}_1 (avec la terminologie de [Ha], la réduction modulo p du revêtement Φ_i est un "mock cover"). D'après [Ha; Prop.2.2], on peut "coller ensemble" les revêtements $\Phi_i, i = 1, \dots, \rho$. De façon précise, il existe un G -revêtement de \mathbb{P}_1 , défini sur \mathbb{Q}_p , ramifié en chacun des points de $\bigcup_{1 \leq i \leq \rho} R_{p,i}$ et tel que

(16) Pour tout $i = 1, \dots, \rho$, et tout $t \in R_{p,i}, h_i$ est un générateur "canonique" d'un groupe d'inertie au-dessus de t .

Notons pour tout $i = 1, \dots, \rho, C_i$ la classe de conjugaison dans G de h_i, r l'entier $r = \rho(\rho + 1)$ et \mathbf{C} le r -uplet de classes de conjugaison de G :

$$(17) \quad \mathbf{C} = (C_1, C_1, C_2, C_2, C_2, C_2, \dots, \overbrace{C_\rho, C_\rho, \dots, C_\rho, C_\rho}^{2\rho})$$

Les classes $C_i, i = 1, \dots, \rho$ étant rationnelles, l'espace $\mathcal{H} = \mathcal{H}(\mathbf{C})$ est défini sur \mathbb{Q} . La construction précédente montre que $\mathcal{H}(\mathbb{Q}_p) \neq \emptyset$ pour tout p . Quant à l'existence de points \mathbb{R} -rationnels sur \mathcal{H} , elle résulte du Th.4 bis.

Note. On a choisi $d_i = i$ pour $i = 1, \dots, \rho$, par souci de simplicité. En fait, la construction marche de la même façon si les polynômes $f_i, i = 1, \dots, \rho$ sont choisis irréductibles et distincts dans $\mathbb{F}_p[T]$. On peut alors, à $\rho \geq 2$ fixé, essayer de minimiser le nombre final $r = 2(d_1 + \dots + d_\rho)$ de classes de conjugaison dans \mathbf{C} .

Notons $n_p(d)$ le nombre de polynômes irréductibles de degré d dans $\mathbb{F}_p[T]$. On montre sans trop de difficultés que, à d fixé, $n_p(d)$ croît avec p . On procède alors de la façon suivante. On choisit les $2 = n_2(1)$ premiers polynômes f_i de degré 1. On peut choisir les suivants de degré 2 si $n_2(1) + n_2(2) = 4 \geq \rho$; sinon on prend les 2 suivants de degré 2, puis les suivants jusqu'à concurrence de $n_2(3) = 7$, de degré 3 etc...]

6 Il y a des exemples où $\mathcal{H}(\mathbb{Q}) = \emptyset$.

[Reprenons l'exemple du Th.5: G est le groupe diédral $G = D_p$ d'ordre $2p$, $r = 4$ et les quatre classes C_1, \dots, C_4 sont égales à la classe de conjugaison C de tous les éléments d'ordre 2 du groupe, i.e., $C = \{(a, 1) | a \in \mathbb{Z}/p\}$. D'après le Th.5, on a $\mathcal{H}(\mathbb{Q}) = \emptyset$. On notera pourtant que $\mathcal{H}(\mathbb{R}) \neq \emptyset$ et $\mathcal{H}(\mathbb{Q}_\ell) \neq \emptyset$ pour tout ℓ (cet exemple correspond au cas $\rho = 2$ de la construction donnée en 5) pour lequel, si on procède comme dans la note, on a $r = 4$). La démonstration du Th.5 éclaire cet exemple : on montre en fait qu'il existe un morphisme $\mathcal{H} \rightarrow X_0(p)$ de l'espace de Hurwitz sur la courbe modulaire (privée des pointes) ainsi qu'une section $X_0(p) \rightarrow \mathcal{H}$, tous deux définis sur \mathbb{Q} . En particulier, l'espace de Hurwitz \mathcal{H} est irréductible et pour tout corps K , $\mathcal{H}(K) \neq \emptyset$ si et seulement si $X_0(p)(K) \neq \emptyset$.]

Situation 5 : r grand.

Le paramètre r doit être choisi supérieur au rang $\text{rg}(G)$ du groupe G . Mais il paraît raisonnable, au vu du Th.5 par exemple, de penser que, pour être sûr de trouver des points \mathbb{Q} -rationnels sur un espace de Hurwitz \mathcal{H} , il faille prendre r beaucoup plus grand que $\text{rg}(G)$. Dans un article récent [FrV], M. Fried et H. Voelklein ont obtenu des résultats dans ce sens. Ils s'appuient sur le théorème suivant, dû à J.H. Conway et R.A. Parker [CP].

THÉORÈME 8. Soit G un sous-groupe de S_n vérifiant les deux conditions

- (1) Le centralisateur $\text{Cens}_n(G)$ est trivial (en particulier $Z(G) = \{1\}$).
- (2) Le groupe des multiplicateurs de Schur de G est "engendré par les commutateurs".

Il existe un entier b avec la propriété suivante : si C est un r -uplet de classes de conjugaisons de G tel que

- (3) chaque classe de conjugaison de G apparaît au moins b fois dans C .

Alors l'espace de Hurwitz $\mathcal{H}(C)$ est irréductible.

De plus, si toutes les classes de conjugaison de G apparaissent le même nombre de fois, alors l'espace de Hurwitz $\mathcal{H}(C)$ est défini sur \mathbb{Q} .

On trouvera dans [FrV] le sens précis de la condition (2). Les conditions (1) et (2) ne sont pas très restrictives : d'après [FrV; Lemma 2.2], tout

groupe fini est quotient d'un groupe qui les satisfait. En conséquence, à tout groupe fini G , on peut associer une famille infinie \mathcal{F} de variétés \mathcal{H} , irréductibles et définies sur \mathbb{Q} , telles que

(18) Le groupe G a la propriété RGal_K s'il existe un point K -rationnel sur l'une des variétés $\mathcal{H} \in \mathcal{F}$.

Un corps K est dit *Pseudo Algébriquement Clos* si toute variété algébrique définie sur K a des points K -rationnels. On a donc [FrV; Th.2].

COROLLAIRE 1. *Tout groupe fini G a la propriété RGal_K sur tout corps PAC K . Si de plus K est hilbertien, alors G a la propriété Gal_K .*

Les corps PAC sont étudiés par exemple dans [FrJ]. Sont PAC les corps algébriquement clos, les extensions algébriques de corps PAC, les extensions algébriques infinies de \mathbb{F}_p . De (18) ou même du corollaire 1 se déduit également le résultat suivant [FrV;§ 2.2].

COROLLAIRE 2. *Tout groupe fini G a la propriété $\text{RGal}_{\mathbb{F}_p}$ pour tout p sauf un nombre fini.*

RÉFÉRENCES

- [BFr] R. Biggers and M. Fried, *Moduli spaces of covers and the Hurwitz monodromy group*, J. für die reine und angew. Math. **335** (1982), 87–121.
- [CP] J.H. Conway and R.A. Parker, *On the Hurwitz number of arrays of group elements*. Preprint
- [DFr1] P. Dèbes and M. Fried, *Arithmetic variation of fibers*, J. für die reine und angew. Math **400** (1990), 106–137.
- [DFr2] P. Dèbes and M. Fried, *Non rigid situations in constructive Galois theory*. Preprint
- [Fr1] M. Fried, *Fields of definition of function fields and Hurwitz families*, Groups as Galois groups, Comm. in Alg.,5 **1** (1977), 17–82.
- [Fr2] M. Fried, *Arithmetic of 3 and 4 branch point covers*, Séminaire de Théorie des Nombres Delange-Pisot-Poitou (1987–1988), Birkhauser.
- [FrD] M. Fried and P. Dèbes, *Rigidity and real residue class fields*, Acta Arithmetica, **56** (1990).
- [FrJ] M. Fried and M. Jarden, *Field Arithmetic*, Springer, Ergebnisse **11** (1986).
- [FrV] M. Fried and H. Volklein, *The inverse Galois problem and rational points on moduli spaces*,. Preprint.
- [Ha] D. Harbater, *Galois covering of the arithmetic line*, Proc. of the NY Number Thy. Conf. of 1985, LNM 1240, Springer.

- [Hi] D. Hilbert, *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, J. für die reine und angew. Math. 110 (1892), 104–129; (=Gesammelte Abhandlungen, Springer-Verlag (1983) [réimpression Chelsea, 1965], 2 n° 18, 264–286.
- [Hur] A. Hurwitz, *Riemann'sche Flächen mit gegebenen Verzweigungspunkten*, Mathematische Werke, Band I, 321–383.
- [KN] A. Krull and J. Neukirch, *Die Struktur der absoluten Galois gruppe über dem Körper $\mathbb{R}(T)$* , Mathematische Annalen, 193 (1971), 197–209.
- [Ma1] B.H. Matzat, *Konstruktive Galoistheorie*, LNM 1284, Springer-Verlag.
- [Ma2] B.H. Matzat, *Über das Umkehrproblem der Galoisschen Theorie*, Jber.d.Dt. Math.-Verein, 90 (1988), 155–183.
- [Ma3] B.H. Matzat, *Zöpfe und Galoissche Gruppen*,. Preprint.
- [Se1] J.P. Serre, *Points rationnels des courbes modulaires*, Séminaire Bourbaki, 30ème année, 1977/78 n° 511.
- [Se2] J.P. Serre, *Groupe de Galois sur \mathbb{Q}* , Séminaire Bourbaki, 1987/88 n° 689.
- [Se3] J.P. Serre, *Topics in Galois theory*, Course at Harvard University (Fall 1988), Notes written by Henri Darmon, preprint.
- [Sha] I.R. Shafarevich, *Constructions of fields of algebraic numbers with given solvable Galois group*. Izv. Akad. Nauk SSSR 18 (1954), 525-578(=Amer. Math. Transl.4(1956),185-237;=C.P. 139-191)
- [Sh1] K.y. Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. 207 (1974), 99–120.
- [Sh1] K.y. Shih, *p -division points on certain elliptic curves*, Comp. Math. 36 (1978), 113–129.

“Problèmes diophantiens”
 Institut Henri Poincaré
 75231 PARIS cedex 05