THESE présentée

pour l'obtention

du

DIPLOME D' HABILITATION
à diriger des recherches

à

L' UNIVERSITE PIERRE ET MARIE CURIE
- Paris 6 -

Spécialité : MATHEMATIQUES
Mention : THEORIE DES NOMBRES

Par M. Pierre DEBES

Sujet de la thèse:

ETUDE ARITHMETIQUE DES REVETEMENTS DE $\mathbf{P}^1$

soutenue le 5 Décembre 1991 devant la commission composée de:

M. Andrzej SCHINZEL Président
M. Daniel BERTRAND
M. Daniel BARSKY
M. Jean-Claude DOUAI
M. Michael D. FRIED
M. B. Heinrich MATZAT
M. Michel WALDSCHMIDT

J'ai grand plaisir à remercier MM. Barsky, Bertrand, Douai, Fried, Matzat, Schinzel et Waldschmidt, de l'honneur qu'ils me font de participer à mon jury d'habilitation. Je suis fier que M. Schinzel ait accepté de le présider; qu'il soit sûr de ma gratitude.

Je souhaite également remercier tous ceux qui ont contribué à ce que je sois ici aujourd'hui. Michel Waldschmidt, qui, depuis le début, dirige mes recherches avec justesse et enthousiasme. Mike Fried, qui depuis quelques années, a donné un nouvel essor à mon travail. Jean-Claude Douai, Michel Emsalem avec qui il m'est toujours agréable de travailler. Daniel Bertrand, dont les avis et les conseils sont toujours bienvenus, et toute l'équipe "Problèmes diophantiens" dont je partage la vie depuis dix ans. Et aussi toutes les personnes que j'ai pu croiser pendant ces années et qui ont pris le temps de s'intéresser à mon travail.

ETUDE ARITHMETIQUE DES REVETEMENTS DE P_1

Pierre Dèbes

Les revêtements finis de la droite projective P_1 ont de multiples descriptions que nous évoquerons tour à tour. Définissons les pour commencer comme données d'une courbe algébrique projective irréductible et lisse C et d'un morphisme fini $\varphi: C \to P_1$. Nous supposerons ces données définies sur un corps K de caractéristique 0. Dans les diverses situations arithmétiques que nous avons en vue, le corps K sera un corps de nombres ou un corps de fonctions. Les problèmes que nous considérons sont de deux types. Le premier est l'étude arithmétique **des fibres du revêtement**. On peut ainsi regarder les points t de $P_1(K)$ tels que la fibre $\varphi^{-1}(t)$ soit un diviseur premier sur C_K (i.e., sur C vu comme schéma sur K): plus simplement, ce sont les points de $P_1(K)$ qui se relèvent en des points de C définis sur une extension de K de degré égal au degré de φ (i.e., aussi grand que possible). C'est la première partie de mon travail; elle est liée au théorème d'irréductibilité de Hilbert. On peut au contraire regarder les points de $P_1(K)$ qui se relèvent en des points K-rationnels sur C. Avec les théorèmes de Siegel, Mordell-Weil et Faltings, on dispose dans ce contexte de résultats de finitude puissants. Nous donnons à l'inverse un critère d'existence de points rationnels sur C. Un tel résultat peut servir par exemple pour la construction de courbes elliptiques possédant de nombreux points rationnels. Le second problème concerne **les corps de définition des revêtements**. Il s'agit d'un problème de descente: un revêtement défini sur $\bar{Q}$ peut-il être défini sur un sous-corps K si on sait que certains de ses invariants sont définis sur K? Nous développerons l'application fondamentale suivante. Etant donné un groupe fini G quelconque, on sait construire un revêtement galoisien défini sur $\bar{Q}$ de groupe de Galois isomorphe à G. Quand on peut descendre jusqu'au corps Q des rationnels le corps de définition d'un tel revêtement, on résout le "problème inverse de la théorie de Galois" pour le groupe G.

THEOREME D'IRREDUCTIBILITE DE HILBERT.

Soit $\varphi: C \to P_1$ un revêtement défini sur K. Dans cette partie, le corps K est un corps de nombres. Le corps K(C) des fonctions de C est une extension finie du corps $K(\varphi)$. Choisissons un élément primitif θ de cette extension. Il existe alors un polynome P irréductible dans K(T)[Y] tel que $P(\varphi,\theta) = 0$. Pour tout t dans K sauf un nombre fini, la fibre $\varphi^{-1}(t)$ est un diviseur premier sur C_K ssi le polynôme P(t,Y) est irréductible dans K[Y]. Le théorème d'irréductibilité de Hilbert affirme qu'il existe une infinité d'éléments t de K pour lesquels il y a irréductibilité. Plus précisément, étant donnés n polynômes $P_1,...,P_n$ irréductibles dans K(T)[Y], on note $H_{P_1,...,P_n}$ l'ensemble des éléments t de K tels que chacun des polynômes $P_i(t,Y)$ soit irréductible dans K[Y], i = 1,...,n. Le théorème de Hilbert énonce que tout ensemble du type $H_{P_1,...,P_n}$, qu'on appelle partie hilbertienne de K, est infini. Ce résultat s'étend facilement aux dimensions supérieures, i.e., au cas de polynômes $P_1,...,P_n$ dans $K(T_1,...,T_p)[Y_1,...,Y_q]$; la conclusion devient que les parties hilbertiennes $H_{P_1,...,P_n}$ sont Zariski-denses dans l'espace affine $A^p(K)$.

Le théorème d'irréductibilité de Hilbert est un résultat fondamental puisqu'il autorise dans certaines situations à spécialiser des paramètres sans modifier la structure

algébrique. Par exemple, un groupe G qui est le groupe de Galois d'une extension de $\mathbf{Q}(T)$ est aussi le groupe de Galois d'une extension de $\mathbf{Q}$ (Cf. 3ème partie). Le théorème de Hilbert sert également à construire des courbes elliptiques définies sur $\mathbf{Q}$ de rang élevé: on travaille sur le corps $\mathbf{Q}(T_1,...,T_p)$ et on spécialise ensuite rationnellement les indéterminées $T_1,...,T_p$; Néron a montré que l'ensemble des spécialisations $(t_1,...,t_p)$ pour lesquels le rang se conserve est un ouvert d'une partie hilbertienne et donc est non vide.

La première partie de mon travail donne des formes plus précises du théorème de Hilbert. J'ai démontré les résultats suivants.

THEOREME 1 — Soit b un élément de K non nul et non racine de l'unité. Alors toute partie hilbertienne de K contient une progression géométrique de raison b. C'est-à-dire, étant donnés n polynômes $P_1,...,P_n$ irréductibles dans K(T)[Y], il existe un entier a de K tel que pour tout entier m suffisamment grand, le polynôme $P_i(ab^m,Y)$ est irréductible dans K[Y], $i = 1,...,n$.

Ce résultat montre en particulier que le théorème d'irréductibilité de Hilbert peut être combiné aux théorèmes d'approximation usuels pour les nombres algébriques (Artin-Whaples ou autre): il existe des éléments de K qui satisfont simultanément leurs conclusions.

THEOREME 2 — Soient P un polynôme irréductible dans K(T)[Y] et b un élément de K non nul et non racine de l'unité. Les propositions suivantes sont équivalentes.
(i) Le polynôme $P(b^m,Y)$ est réductible dans K[Y] pour une infinité d'entiers m.
(ii) Le polynôme P est un diviseur dans K(T)[Y] d'un polynôme de la forme

$$\begin{cases} A(T,Y)^p - b^{-u}T \\ \text{ou} \\ 4A(T,Y)^4 + b^{-u}T \end{cases}$$

où p est premier, $u \in \mathbf{Z}$ et $A \in K(T)[Y]$.

THEOREME 3 — Soit $P \in K(T)[Y]$ un polynôme irréductible dans $\bar{\mathbf{Q}}(T)[Y]$. Soit b un élément de K qui n'est pas une puissance stricte dans K ni de la forme $-4w^4$ avec $w \in K$. Alors, le polynôme $P(b^m,Y)$ est irréductible dans K[Y] pour une infinité d'entiers m (en fait, pour tout m dans une progression arithmétique $(\alpha n+\beta)_{n\geq 0}$).

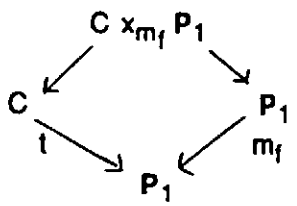
Ces résultats sont démontrés dans [De9], de façon non effective: on utilise le théorème de Siegel sur la finitude des points entiers d'une courbe algébrique. Mais dans le cas $K = \mathbf{Q}$ et $b \in \mathbf{Z}\backslash\{0,1,-1\}$, il y a une autre méthode qui conduit à une version effective du Th.1: on peut préciser le nombre d'entiers m exceptionnels. Ce résultat, antérieur aux précédents, est expliqué dans [De6]. Cette question d'effectivité a de l'importance puisque cette première version du Th.1 m'a permis de construire explicitement une partie hilbertienne universelle, c'est-à-dire une partie de $\mathbf{Q}$ contenue dans toute partie hilbertienne, à un nombre fini de ses éléments près [De7]. Seul un exemple, dû à Sprindzuk, était connu jusque là; d'autres ont été fournis depuis par l'analyse non-standard. Mais décrivons un peu mieux ces deux approches du Th.1. Pour simplifier, traitons le cas d'un seul polynôme P. Rappelons aussi une réduction classique: on peut se contenter d'une conclusion d'irrationalité plutôt que d'irréductibilité; essentiellement,

il s'agit de montrer que, pour a bien choisi, le polynôme $P(ab^m,Y)$ n'a pas de racines dans K pour m assez grand.

Il y a une idée commune aux deux méthodes. Elle consiste à se ramener au cas où la fonction φ, qu'il est agréable de noter t, n'a que des zéros simples sur C, ce qui équivaut à demander que le polynôme P(T,Y) ait toutes ses racines dans $\bar{K}((T))$. D'après le théorème de Puiseux, il suffit donc de remplacer le polynôme P(T,Y) par le polynôme $P(T^f,Y)$ pour f convenablement choisi. Il faut cependant noter que le polynôme $P(T^f,Y)$ peut être réductible dans K(T)[Y]; ce problème est étudié en détails dans [De9;§2.1]. Mais on peut dans tous les cas, en remplaçant préalablement T par aT avec a convenablement choisi dans l'anneau des entiers O_K de K, s'arranger pour que cela ne se produise pas: c'est le sens de la Prop.3 de [De5;§3].

Si on ne soucie pas de l'effectivité, on peut poursuivre comme ceci. Si la fonction t n'a que des zéros simples sur C et si t est de degré ≥ 2 (i.e.,$\deg_Y P \geq 2$), alors l'ensemble Ω des points se projetant soit sur 0 soit sur ∞ par la fonction t, contient nécessairement au moins 3 points. Le théorème de Siegel s'applique donc à la courbe algébrique affine $C\backslash\Omega$; la finitude des points S-entiers sur $C\backslash\Omega$, pour S bien choisi, conduit à la conclusion désirée (Cf.[De9;§3]).

L'idée générale, dans le contexte du théorème de Hilbert, de se ramener à une courbe algébrique où le théorème de Siegel s'applique, revient à Néron. Mais Néron se ramenait à une situation où le genre de C est > 0 en remplaçant la courbe P(t,y) = 0 par une courbe du type P(u(t),y) = 0 avec u polynôme en T. Ici, on a joué sur le nombre de points à l'infini en changeant T en T^f. Géométriquement, cela revient à ceci. Notons m_f le revêtement $m_f: \mathbf{P}_1 \to \mathbf{P}_1$ donné par $m_f(t) = t^f$. On a le diagramme



C'est à la courbe C x_{m_f} $\mathbf{P}_1$, quand elle est irréductible, qu'on applique le théorème de Siegel. On est ainsi ramené à l'étude de la réductibilité du produit C x_{m_f} $\mathbf{P}_1$ de deux revêtements de $\mathbf{P}_1$. Ce dernier point est une question générale importante à laquelle se ramènent de nombreux problèmes arithmétiques ([Fr1],[Fr2],[Fr6]). On la résout ici utilisant le lemme de Capelli (Cf. [De9;§2.1]); cela conduit à la caractérisation donnée par le Th.2. Le Th.3 se démontre à partir du Th.2 [De9;§2.3].

Si $K = \mathbf{Q}$, on peut substituer deux arguments effectifs au théorème de Siegel; c'est la seconde approche du Th.1. Dans un premier temps, on montre qu'on peut conclure si la fonction t a au moins 2 zéros non conjugués sur $\mathbf{Q}$ (dans la méthode précédente, il suffisait que t ait 2 zéros distincts). Cela va résulter d'un énoncé assez général sur les valeurs d'une fonction rationnelle t en des points rationnels d'une courbe algébrique C. Cet énoncé, expliqué ci-dessous, est dû essentiellement à Sprindzuk [Sp2]. Il constitue aussi un thème d'étude majeur de [De3]: j'en ai affiné les hypothèses, amélioré les constantes et donné des formulations plus intrinsèques. Bombieri, par la suite, en a proposé une approche plus géométrique [Bo2].

Rappelons que si ω est un élément d'un corps de nombres K, sa hauteur (logarithmique) de Weil est définie par la formule:

$$h(\omega) = \frac{1}{[K:Q]} \sum_v d_v \mathrm{Log}^+(|\omega|_v)$$

où la somme porte sur toutes les places v du corps K, où d_v désigne le degré local $[K_v:Q_v]$ de la place v, où $\mathrm{Log}^+(u) = \mathrm{Log}(\max(1,u))$ et où les places v de K sont normalisées de telle façon qu'elles prolongent les valeurs absolues usuelles de Q [1]. Soit maintenant M un point K-rationnel sur C non pôle de t. Les termes locaux $|1/t(M)|_v$ prédominants dans la hauteur $h(1/t(M))$ $(= h(t(M))$ proviennent des places v pour lesquelles M est proche d'un zéro de t. Le résultat dont il est question ci-dessus donne une estimation de la contribution d'un zéro donné Q de t, K-rationnel sur C. Précisément, on a:

$$(1) \quad \frac{1}{[K:Q]} \sum_{v \in S(M,Q)} d_v \mathrm{Log}^+(|1/t(M)|_v) \underset{h(t(M))\to\infty}{\sim} \frac{\mathrm{ord}_Q t}{\deg t}\ h(t(M))$$

où $\deg t = [\bar{K}(C) : \bar{K}(t)] = \deg_Y P$ et S(M,Q) est l'ensemble des places pour lesquelles M est "proche" de Q (voir [De5;Th.2 et Th.3] pour un énoncé précis). Bien sûr, une des difficultés est de préciser cette notion de proximité. D'ailleurs l'énoncé de Bombieri, qui utilise la théorie des fonctions de Weil, est incorrect sur ce point. Je l'ai rectifié dans [De4]. Une alternative à l'emploi des fonctions de Weil consiste à montrer une forme effective du théorème des fonctions implicites; c'est ce que j'ai fait (voir [De2;§4] et [De4;§3]).

Un mot sur les méthodes. Celle de Bombieri est algébrique: elle s'appuie sur la théorie des fonctions de Weil sur les courbes algébriques et les propriétés des hauteurs sur les variétés abéliennes. On peut également utiliser des méthodes provenant de la théorie des nombres transcendants. Pour cela, on voit l'élément primitif θ du début du paragraphe comme fonction, algébrique, $\psi(t)$ de t. A cause de notre hypothèse "P est décomposé dans $\bar{Q}((T))$", cette fonction a un développement en série de Laurent au voisinage de 0 (en toute place v). Cette série vérifie des équations différentielles et des théorèmes classiques contrôlent la taille de ses coefficients. De façon précise, la série $\psi(t)$ est une G-fonction; c'est un des cadres habituels des méthodes transcendantes. Les valeurs de G-fonctions ont été étudiées par Bombieri [Bo1], suivant une méthode élaborée par Siegel, le père des E et des G-fonctions. Sprindzuk, pour démontrer son résultat, utilise la même approche, mais dans le cadre plus restreint des fonctions algébriques. Dans [De5], j'ai montré que le résultat de Sprindzuk se déduit du résultat général de Bombieri sur les G-fonctions et donné une démonstration plus rapide du résultat de Bombieri, cela en utilisant une autre méthode issue de la transcendance, la méthode de Gel'fond.

Revenons au Th.1. A partir de l'estimation (1), on conclut en remarquant que s'il existe une infinité de points rationnels où la valeur prise par t est une puissance de b, alors sauf pour un nombre fini de ces points, l'équivalence peut être remplacée par une égalité (Cf.[De5; §3 Prop.1]). Sous l'hypothèse "t a au moins 2 zéros non conjugués sur Q", la formule obtenue conduit à une contradiction.

---

[1] Si K = Q, la hauteur de Weil est la hauteur habituelle: $h(p/q) = \mathrm{Log}(\max(|p|,|q|))$.

Une autre conséquence de l'estimation (1) mérite d'être dégagée.

COROLLAIRE [De5;§2.4] — Sauf pour un nombre fini de points Q-rationnels M sur C, le nombre de places v de K où $|t(M)|_v < 1$ est au moins égal au nombre de zéros de t sur C, comptés à conjugaison sur Q près.

Par exemple, si t a au moins deux zéros non conjugués sur Q, il n'y a qu'un nombre fini de points rationnels M sur C tel que t(M) soit un nombre premier (ou une puissance d'un nombre premier); si t a au moins deux pôles non conjugués sur Q, il n'y a qu'un nombre fini de points rationnels M sur C tels que t(M) soit un entier (appliquer le résultat à 1/t). Enoncé sous des formes diverses, on trouve trace de ce résultat dans de nombreux travaux: [Sp1], [Bo2;Th.p.305], [De5;§2.3 et §2.4], [Fr4;Prop.4.4], [We]. L'énoncé ci-dessus en est la variante la plus générale.

Il reste à expliquer le second argument de la preuve effective du Th.1, c'est-à-dire ce que l'on fait quand les zéros de la fonction t sont tous conjugués sur Q. Cela revient essentiellement à dire que le polynôme P(0,Y) est irréductible dans Q[Y]. On sait alors, par un lemme de Hasse, pour lequel on dispose de versions effectives, qu'il existe une infinité de nombres premiers p tels que modulo p, le polynôme P(0,Y) n'a pas de racines dans F_p. Si on a choisi pour a un multiple de l'un ce ces nombres premiers, les polynômes $P(ab^m,Y)$ ne peuvent pas avoir de racines dans Q, n'en ayant pas modulo p.

Analysons le dernier argument. Le groupe de Galois G du polynôme P(0,Y) agit transitivement sur ses racines $y_1,...,y_d$; cela a pour conséquence qu'il existe un élément σ de G tel $\sigma(y_i) \neq y_i$, $i = 1,...,d$. Le théorème de Cebotarev permet alors de conclure que, pour une infinité de p, les extensions engendrées par chacune des racines de P(0,Y) modulo p sont toutes de degré > 1. Retenons qu'une propriété du groupe de Galois a eu une conséquence arithmétique. Une autre idée majeure de cette première partie est le rôle joué par la ramification dans ce type de problèmes. Ici c'est à travers l'hypothèse "t n'a que des zéros simples" qu'elle apparaît; dans [De7], j'ai noté son importance dans d'autres travaux ([Fr4],[DvZa]). Ces deux observations font le lien avec la suite. En effet, la seconde partie de notre travail s'appuie sur une étude systématique de la ramification des revêtements ainsi que des propriétés de son groupe de Galois.

EXISTENCE DE POINTS RATIONNELS.

Cette partie renvoie à [DeFr1], qui est issu d'un travail commun avec M. Fried. Le résultat principal est le Th.3.14. Ce résultat est un critère d'existence de points rationnels sur une courbe algébrique. Comme dans la première partie, on se donne un revêtement $\varphi: C \to P_1$, mais ici on voit C et P_1 comme surfaces de Riemann.

Le morphisme $\varphi: C \to P_1$ induit un revêtement non ramifié de la sphère de Riemann P_1 privée d'un nombre fini de points, les points de ramification $t_1,...,t_r$ du revêtement. De tels revêtements sont classés par les sous-groupes du groupe fondamental π de $P_1\backslash\{t_1,...,t_r\}$. Se donner un sous-groupe H d'indice fini de π revient à se donner une représentation transitive de π dans S_d

$$\Phi : \pi \to S_d,$$

à savoir l'action de π par translation sur les classes à gauche modulo H ; $d = [\pi:H]$ est le degré du revêtement. Cet homomorphisme décrit en fait l'action de la monodromie. Concrètement, on obtient Φ de la façon suivante. Un point base $t_o \in P_1\setminus\{t_1,...,t_r\}$ étant choisi, le groupe $\pi = \pi_1(P_1\setminus\{t_1,...,t_r\},t_o)$ agit naturellement sur l'ensemble des points de la fibre $\varphi^{-1}(t_o)$: pour $[\gamma]$ la classe d'homotopie d'un chemin fermé basé en t_o, $\Phi([\gamma])$ est la permutation de $\varphi^{-1}(t_o)$ qui envoie $p \in \varphi^{-1}(t_o)$ sur le point final de l'unique relèvement de γ sur C qui commence en p.

On sait que le groupe π est le quotient du groupe libre à r générateurs $x_1,...,x_r$ par l'unique relation $x_1...x_r = 1$. A équivalence près, le revêtement de $P_1\setminus\{t_1,...,t_r\}$ est donc entièrement déterminé par la donnée de ses points de ramification $t_1,...,t_r$ et des r éléments de S_d, $\sigma_i = \Phi(x_i)$, $i = 1,...,r$. D'après le théorème d'existence de Riemann, cette donnée permet également de retrouver le revêtement complet $\varphi: C \to P_1$. Pour $i = 1,...,r$, considérons la décomposition de σ_i en cycles à support disjoints dans S_d:

$$\sigma_i = \beta_{i1}...\beta_{il_i}.$$

On sait également que pour $i = 1,...,r$, les points dans la fibre $\varphi^{-1}(t_i)$ correspondent aux cycles $(\beta_{ij})_{ij}$ de la décomposition de σ_i, la longueur de chaque cycle étant égale à l'indice de ramification de φ au point correspondant.

Considérons l'ensemble $\mathfrak{R}$ réunion de toutes les fibres $\varphi^{-1}(t_i)$ où $i = 1,...,r$. L'objectif de [DeFr1] est une étude arithmétique de l'ensemble $\mathfrak{R}$. Supposons $\varphi: C \to P_1$ défini sur un corps de nombres K. Commençons par décrire notre résultat dans un cas simple, celui où les classes de conjugaison dans S_d des cycles de ramification σ_i, $i = 1,...,r$, sont distinctes; cela impose que les points de ramification $t_1,...,t_r$ sont K-rationnels. Pour $i = 1,...,r$ et λ désignant la longueur d'un des cycles β_{ij} de la décomposition de σ_i, notons $\sigma(i,\lambda)$ l'ensemble des cycles de longueur λ dans σ_i et $P(i,\lambda)$ l'ensemble des points de C correspondant aux cycles de $\sigma(i,\lambda)$. Il est clair que le diviseur "somme (formelle) des points dans $P(i,\lambda)$" est un diviseur K-rationnel sur C. Notre résultat dit que l'on peut faire mieux: notre résultat explique comment l'action du groupe de Galois $G(\overline{K}/K)$ sur $P(i,\lambda)$ est liée à l'action d'un certain "groupe de tresses" sur l'ensemble $\sigma(i,\lambda)$.

Le groupe des tresses d'Hurwitz, noté H(r), peut être défini comme quotient du groupe libre à r-1 générateurs $Q_1,...,Q_{r-1}$ par certaines relations (données par exemple dans [DeFr1]). Il agit sur les r-uples $(s_1,...,s_r)$ de produit $s_1,...,s_r = 1$ de la manière suivante:

$$(s_1,...,s_r)Q_i = (s_1,...,s_{i-1},s_is_{i+1}s_i^{-1},s_i,s_{i+2},...,s_r) \qquad i = 1,...,r-1.$$

Considérons le sous-groupe H_σ de H(r) constitué des éléments Q de H(r) qui fixent le r-uple $\sigma = (\sigma_1,...,\sigma_r)$ à conjugaison près dans S_d. Précisément, on pose

$$H_\sigma = \{Q \in H(r) \mid \exists\, \gamma \in S_d \text{ tq } (\sigma_1,...,\sigma_r)Q = (\gamma\sigma_1\gamma^{-1},...,\gamma\sigma_r\gamma^{-1})\}$$

Notons G le groupe engendré par $\sigma_1,...,\sigma_r$; par définition, G est le groupe de monodromie du revêtement. Et supposons que le centralisateur $Cen_{S_d}G$ de G dans S_d soit trivial. Alors l'élément γ associé dans la définition à tout élément Q de H_σ est unique. L'action de Q combinée à celle de la conjugaison par γ fixe le r-uple σ et donc permute les cycles dans $\sigma(i,\lambda)$; on obtient donc une action de H_σ sur $\sigma(i,\lambda)$. Nous commençons par une forme affaiblie du Th.3.14 de [DeFr1] (Cf. Th.5 plus bas).

THEOREME 4 — Sous les hypothèses décrites ci-dessous, si l'action de H_σ sur $\sigma(i,\lambda)$ a un unique point fixe, alors il y a un point rationnel dans $P(i,\lambda)$.

L'action de H_σ sur $\sigma(i,\lambda)$ dépend a priori du r-uple σ, i.e., essentiellement du choix des générateurs $x_1,\ldots,x_r$ de π. Classiquement, on choisit pour $x_1,\ldots,x_r$ les classes d'homotopie de "boucles convenables" basées en t_0 entourant chacun des points de ramification. Il existe une donnée qui ne dépend pas de ce choix: pour $i = 1,\ldots,r$, c'est la classe de conjugaison dans le groupe de monodromie G de σ_i; cette classe correspond à tous les cycles de ramification $\Phi([\gamma])$ induits par des lacets γ "tournant une fois autour de t_i". Il est alors naturel de définir l'ensemble

$$sni(C_1,\ldots,C_r) = \left\{ (\sigma'_1,\ldots,\sigma'_r) \in G^r \;\middle|\; \begin{cases} \sigma'_1,\ldots,\sigma'_r \text{ engendrent } G \\ \sigma'_1\ldots\sigma'_r = 1 \\ \sigma'_i \in C_i,\ i = 1,\ldots,r \end{cases} \right\}$$

Cet ensemble, appelée classe de Nielsen du r-uple $C = (C_1,\ldots,C_r)$, a été introduit par M. Fried [Fr2]; il est parfois noté $\Sigma(C_1,\ldots,C_r)$ ([Se3],[De8]). On peut maintenant préciser les hypothèses de notre résultat. Il y a un sous-groupe naturel SH(r) de H(r) qui agit sur l'ensemble $sni(C_1,\ldots,C_r)$. En plus de la condition $Cen_{S_d}G = \{1\}$, nous supposons que l'action de SH(r) est transitive sur les éléments de $sni(C_1,\ldots,C_r)$ regardés à conjugaison près dans S_d. Notons que sous cette condition, l'action de H_σ sur $\sigma(i,\lambda)$ ne dépend pas du r-uple choisi dans $sni(C_1,\ldots,C_r)$; on explique en fait dans [DeFr1] comment cette action peut être définie de façon plus intrinsèque (Cf. Remark 3.13).

Nous venons de décrire le Th.3.14 de [DeFr1] dans une situation particulière; en effet, en toute généralité, les classes de conjugaison $C_1,\ldots,C_r$ ne sont pas distinctes; en conséquence, les points de ramification ne sont pas nécessairement rationnels. Cela complique un peu l'énoncé général du Th.3.14 mais l'idée reste essentiellement la même. Au lieu de travailler au dessus d'un point de ramification t_i, on va travailler au dessus d'un diviseur K-rationnel à support dans $\{t_1,\ldots,t_r\}$. Précisons quels vont être ces diviseurs. Un argument de base [Fr2;"branch cycle argument" p.62] montre que l'action de $G(\bar{K}/K)$ sur l'ensemble des points de ramification $t_1,\ldots,t_r$ a la propriété suivante. Pour $\tau \in G(\bar{K}/K)$ et $i = 1,\ldots,r$, si $t_i^\tau = t_j$, alors

(2) il existe $\gamma \in S_d$ et un entier a premier à l'ordre des éléments de C_i tels que $C_j = \gamma C_i^a \gamma^{-1}$.

(voir aussi [DeFr2;§2.4]). La condition (2) définit une relation d'équivalence sur l'ensemble des indices $\{1,\ldots,r\}$. Il résulte de la propriété ci-dessus que les diviseurs

$$\sum_i (t_i),$$

où i parcourt une classe d'équivalence $\mathfrak{l}$, sont des diviseurs K-rationnels. C'est au dessus de ces diviseurs que l'on travaille. C'est-à-dire, on considère l'ensemble $\sigma(\mathfrak{l},\lambda)$ des cycles de longueur λ intervenant dans la décomposition des σ_i, $i \in \mathfrak{l}$; de façon analogue au cas décrit plus haut, on définit une action, dérivée de l'action du groupe de tresses H(r) sur l'ensemble $\sigma(\mathfrak{l},\lambda)$; sous les bonnes hypothèses, on montre que, si cette action a un unique point fixe, alors il y a un point rationnel dans l'ensemble $P(\mathfrak{l},\lambda)$ des points correspondant aux cycles de $\sigma(\mathfrak{l},\lambda)$. D'autres versions du résultat sont données dans [DeFr1], en particulier une où on suppose qu'un des points de ramification du revêtement est égal à un point donné de $P_1(K)$, par exemple le point à l'infini.

La démonstration du Th.3.14 fait intervenir la théorie des familles de Hurwitz. Un sous-groupe transitif G de S_d et r classes de conjugaison $C_1,...,C_r$ de G étant fixés, il s'agit en fait de démontrer un résultat sur tous

(3) les revêtements de P_1 de degré d non ramifiés en dehors de r points $t_1,...,t_r$, de groupe de monodromie égal à G et tels que, pour un certain $\gamma \in S_d$, pour $i = 1,...,r$ et pour un certain $\alpha \in S_r$, $\gamma C_{\alpha_i} \gamma^{-1}$ [1], soit, à l'intérieur du groupe 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 [Fr2], on peut mettre une structure algébrique sur l'ensemble des objets (3). De façon plus précise, si la condition $Cen_{S_d}G = \{1\}$ est remplie, ce qui assure que les objets (3) n'ont pas d'automorphismes, alors il existe une famille algébrique de revêtements de P_1

$$\mathcal{T} \to \mathcal{H} \times P_1$$

avec la propriété suivante:

(4) les membres ou fibres de cette famille $\mathcal{T}_\varkappa \to P_1$, $\varkappa \in \mathcal{H}$, correspondent de façon biunivoque aux classes d'équivalence de revêtements décrits dans (3).

L'espace $\mathcal{H}$ et la famille $\mathcal{F}: \mathcal{T} \to \mathcal{H} \times P_1$ sont respectivement appelés espace et famille de Hurwitz associés à la donnée $C = (C_1,...,C_r)$. Leur construction est analytique mais grâce au dictionnaire GAGA, on obtient que ce sont des objets algébriques; l'espace de Hurwitz, par exemple, peut être vu comme revêtement analytique non ramifié d'une variété algébrique $\mathcal{U}_r$, à savoir la variété qui paramètre les ensembles $\{t_1,...,t_r\}$ des points de ramification des revêtements. L'hypothèse faite plus haut de transitivité de l'action du groupe de tresses H(r), qui est en fait le groupe fondamental de $\mathcal{U}_r$, fournit l'irréductibilité de $\mathcal{H}$.

L'intérêt des familles de Hurwitz est que les propriétés arithmétiques du type de celles que nous étudions, une fois établies sur le revêtement générique de la famille (i.e., correspondant au point générique de $\mathcal{H}$), s'étendent à toutes les fibres et donc à tous les revêtements décrits dans (3) ([DeFr1;Prop.1.8 et Prop.3.4]). Le Th.3.14 est un énoncé sur ce revêtement générique.

THEOREME 5 — Supposons satisfaites les hypothèses du Th.4. Soient $\varphi: C \to P_1$ le revêtement générique de la famille de Hurwitz $\mathcal{F}$ et F son corps de définition. Alors les orbites de H_σ sur $\sigma(\mathfrak{l},\lambda)$ correspondent exactement aux orbites de $G(\bar{F}/F\bar{Q})$ sur $P(\mathfrak{l},\lambda)$. En particulier, les orbites de $G(\bar{F}/F)$ sur $P(\mathfrak{l},\lambda)$ sont réunions disjointes d'orbites de même longueur de l'action de H_σ sur $\sigma(\mathfrak{l},\lambda)$.

Le critère donné par le Th.4 n'est intéressant que s'il y a des points rationnels sur C qui sont des points ramifiés de φ. Pour les genres 0 et 1, le Th.5 fournit des critères d'existence de points rationnels bien meilleurs [DeFr1;Cor3.15 et Cor.3.17]. Pour cela, on le combine à la remarque suivante. Pour trouver un point rationnel sur une courbe de genre 0, il suffit de trouver un diviseur rationnel de degré impair, et sur une courbe de genre 1, il suffit de trouver plusieurs diviseurs rationnels de degrés premiers entre

[1] La conjugaison par $\gamma \in S_d$ provient du fait que l'action de la monodromie $T: \pi \to S_d$ dépend de toute façon de la numérotation des points de la fibre au dessus du point base x_0.

eux. Plus généralement, cela conduit à la notion de points rationnels produits par la ramification [DeFr1;§3.2]: ce sont les points rationnels, qui comme diviseurs, sont dans le groupe engendré par les diviseurs rationnels à support dans l'ensemble des points ramifiés de φ et les diviseurs de fonctions rationnelles. Cette définition pose des problèmes intéressants: ainsi, on peut conjecturer, que, "génériquement", pour les genres 0 et 1, l'existence de points rationnels est équivalente à l'existence de points rationnels produits par la ramification. Si tel est le cas, le Th.5 devient, pour les genres 0 et 1, un critère décisif quant à l'existence de points $F\bar{Q}$-rationnels sur le revêtement générique de la famille de Hurwitz. Nous avons vérifié la conjecture sur un exemple où le genre est 0 et pour lequel la ramification ne produit pas de points rationnels [DeFr1;§3.6]; nous montrons que la famille de Hurwitz associée est une famille de coniques ne possédant pas génériquement de points rationnels [DeFr1;§4].

En résumé, on peut retenir que si on connait la ramification d'un revêtement $\varphi: C \to P_1$, on peut trouver des points rationnels sur C en étudiant les orbites d'une certaine action de groupe associée de façon complètement explicite au revêtement. Notons que l'application du critère ne dépend que des propriétés du groupe G et des classes de conjugaison $C_1,...,C_r$; on peut donc aussi utiliser le résultat pour construire des courbes possédant des points rationnels. On peut ainsi envisager d'aborder par ce procédé le problème de la construction de courbes elliptiques de rang élevé. Il y a plusieurs difficultés. Les courbes construites de cette façon sont a priori définies sur C (elles sont données par le théorème d'existence de Riemann); peut-on descendre leur corps de définition? C'est ce type de problèmes qu'on étudie dans la troisième partie. Ensuite, il faut pouvoir minorer le rang du groupe qu'engendrent les points rationnels trouvés par ce procédé. Signalons enfin une difficulté pratique: les calculs se révèlent assez compliqués. Ils sont d'un ordre de complexité comparable aux calculs qu'a demandés la réalisation comme groupes de Galois sur Q de certains groupes simples sporadiques et pour lesquels Matzat a conçu un programme sur ordinateur. On regardera [DeFr1;§3.6 et §3.7] pour se faire une idée.

Dans un article suivant [DeFr2], nous étudions avec M. Fried des problèmes analogues, c'est-à-dire, l'existence de points rationnels dans les fibres d'un revêtement, mais cette fois en prenant le corps R des réels comme corps de rationalité. On se donne un revêtement $\varphi: C \to P_1$ défini sur R et $t_0 \in P_1(R)$ un point distinct des points de ramification du revêtement. Nous expliquons comment, connaissant l'action de la monodromie sur la fibre $\varphi^{-1}(t_0)$, on peut explicitement calculer l'action de la conjugaison complexe sur cette même fibre $\varphi^{-1}(t_0)$ [DeFr2;§2]. On montre ensuite comment en déduire l'action de la conjugaison complexe sur une fibre $\varphi^{-1}(t_i)$ au dessus d'un point de ramification t_i [DeFr2;§4.1]. De cette étude, on déduit par exemple l'énoncé suivant.

COROLLAIRE — Soit $\varphi: C \to P_1$ un revêtement défini sur R avec exactement 3 points de ramification. S'il existe $t_0 \in P_1$, distinct des points de ramification, tel que la fibre $\varphi^{-1}(t_0)$ ne consiste qu'en des points réels, alors le groupe de monodromie du revêtement est isomorphe à un groupe diédral.

On obtient aussi un critère permettant de décider si un revêtement, a priori défini sur C, peut être défini sur R. Mais nous reportons à la troisième partie la discussion de ce problème, qui porte cette fois sur le corps de définition du revêtement.

CORPS DE DEFINITION ET GROUPES DE GALOIS.

On sait ce que signifie qu'un revêtement est défini sur un corps K mais fréquemment on utilise la même expression pour dire qu'un revêtement est seulement "définissable" sur K, i.e., équivalent (sur $\overline{K}$) à un revêtement défini sur K. Une autre source de confusion est que, dans le cas galoisien, le corps de définition dont on souhaite généralement étudier la descente, c'est le corps de définition du revêtement et de ses automorphismes, et non pas celui du revêtement seul. Il existe une autre présentation du problème qui supprime ces ambiguïtés; elle consiste à utiliser le langage des extensions de corps. Il ne s'agit pas seulement d'une question de forme puisqu'à ces deux langages correspondent deux approches du problème. La première utilise le groupe fondamental topologique et le critère de descente de Weil; la seconde utilise le groupe fondamental algébrique et transforme la question de la descente en un problème de prolongement d'homomorphismes de groupes. Le choix n'est pas évident, car le langage des "revêtements", malgré ses lourdeurs, reste parfois plus intuitif. L'utilisation des familles de Hurwitz rend par exemple ce point de vue plus approprié dans [DeFr2] et [DeFr3]. L'approche algébrique, en revanche, donne plus de clarté et d'unité à la théorie. Nous adopterons ici ce point de vue, à la manière de [De8].

On passe de l'un à l'autre des deux langages grâce au foncteur "corps des fonctions". Un revêtement $\varphi: C \to \mathbf{P}_1$ défini sur un corps K induit une extension $K(C)/K(T)$ du corps des fonctions $K(T)$ de $\mathbf{P}_1$; c'est une extension régulière, i.e., $K(C) \cap \overline{K} = K$. Inversement, on retrouve un revêtement $\varphi: C \to \mathbf{P}_1$ à partir d'une extension régulière $E/K(T)$ en prenant pour C l'ensemble des places de E et pour morphisme φ la restriction naturelle de ces places au corps $K(T)$. La question que l'on pose est la suivante. A quelles conditions une extension donnée $E/\overline{K}(T)$ de $\overline{K}(T)$ provient-elle par extension des scalaires d'une extension régulière de $K(T)$? Si l'extension initiale $E/\overline{K}(T)$ est galoisienne, il y a une seconde question, plus forte: on demande si elle provient d'une extension galoisienne (régulière) de $K(T)$? Cette seconde question, appelée question galoisienne dans la suite, est évidemment importante en raison de son application directe au "problème inverse de la théorie de Galois": tout groupe fini G est-il le groupe de Galois d'une extension de $\mathbf{Q}$? Construire une extension galoisienne $E/\overline{K}(T)$ de groupe de Galois G ne pose pas de problèmes (voir plus bas). Si la descente jusqu'au corps K est possible, le groupe G se trouve réalisé comme groupe de Galois sur $K(T)$. Le théorème d'irréductibilité de Hilbert montre alors que c'est aussi le groupe de Galois d'une extension de K.

On attend des réponses à ces questions s'exprimant en fonction de certains invariants de l'extension $E/\overline{K}(T)$. Ici aussi, la ramification et le groupe de Galois de l'extension vont jouer un rôle-clé. Pour poser le problème, on introduit l'analogue algébrique du groupe fondamental topologique. Soient $t_1,...,t_r$ r points distincts de $\mathbf{P}_1(\overline{K})$ et Ω l'extension algébrique maximale de $\overline{K}(T)$ non ramifiée en dehors de $t_1,...,t_r$. L'extension $\Omega/\overline{K}(T)$ est galoisienne; son groupe de Galois se note Π^{alg}: c'est le groupe fondamental algébrique de $\mathbf{P}_1(\overline{K})\backslash\{t_1,...,t_r\}$. Si le diviseur $(t_1)+...+(t_r)$ de $\mathbf{P}_1$ est K-rationnel[1], l'extension $\Omega/K(T)$ est également galoisienne. On note Π_K son groupe de Galois. La théorie de Galois fournit la suite exacte:

$$(5) \qquad 1 \to \Pi^{alg} \to \Pi_K \to \Lambda_K \to 1 \qquad \text{où } \Lambda_K = G(\overline{K}/K)$$

---

[1] ce qui est nécessaire pour une extension de $K(T)$ non ramifiée en dehors de $t_1,...,t_r$.

Se donner une extension $E/\bar{K}(T)$ de degré d non ramifiée en dehors de $\{t_1,...,t_r\}$, c'est se donner un sous-groupe H d'indice d de Π^{alg}, ou de façon équivalente, une représentation transitive

$$\Phi : \Pi^{alg} \to S_d.$$

L'extension provient d'une extension $E_K/K(T)$ de $K(T)$ ssi l'homomorphisme $\Phi: \Pi^{alg} \to S_d$ se prolonge en un homomorphisme $\Phi: \Pi_K \to S_d$. Si l'extension $E/\bar{K}(T)$ est galoisienne, i.e., si H est distingué dans Π^{alg}, l'extension $E_K/K(T)$ reste galoisienne ssi l'homomorphisme prolongé $\Phi: \Pi_K \to S_d$ a la même image que $\Phi: \Pi^{alg} \to S_d$, à savoir le groupe de Galois $G = \Phi(\Pi^{alg})$ de l'extension $E/\bar{K}(T)$[1]. Les questions que nous avons posées se ramènent donc à celles du prolongement au groupe Π_K d'un homomorphisme défini sur Π^{alg}.

Or, la structure des groupes Π^{alg} et Π_K est bien connue. Notons Π le groupe libre à r générateurs $x_1, ..., x_r$ avec la relation $x_1...x_r = 1$; on reconnait le groupe fondamental topologique de $P_1(C)\backslash\{t_1, ..., t_r\}$. 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. Quant au groupe Π_K, il est isomorphe au produit semi-direct $\Pi^{alg} \times^s \Lambda_K$. En effet, la suite exacte (5) est scindée: à tout point base $t_0 \in P_1(K)\backslash\{t_1,...,t_r\}$ correspond une section $\Lambda_K \to \Pi_K$ de l'homomorphisme $\Pi_K \to \Lambda_K$. En conclusion, un homomorphisme de groupes Φ défini sur Π^{alg} est déterminé par la donnée d'un r-uple $(g_1,...,g_r) \in G^r$ tel que $g_1...g_r = 1$ et $\langle g_1...g_r\rangle = G$ [2]. Il se prolonge au produit semi-direct $\Pi_K = \Pi^{alg} \times^s \Lambda_K$ ssi il existe un morphisme $\tau \to \varphi_\tau$ de Λ_K dans S_d (ou G pour la question galoisienne), qui vérifie la condition de compatibilité suivante:

$$(6) \quad \Phi(x^\tau) = \varphi_\tau \Phi(x)(\varphi_\tau)^{-1} \text{ pour } x \in \Pi^{alg} \text{ et } \tau \in \Lambda_K.$$

où $x \to x^\tau$ est l'action de $\tau \in \Lambda_K$ sur Π^{alg}.

Nous sommes au coeur du problème. Pouvoir étudier la condition (6) demande de connaître l'action de Λ_K sur le groupe Π^{alg}. On sait peu de choses en général sur cette action. Il y a les relations évidentes $\langle x_1^\tau, ..., x_r^\tau\rangle = \Pi^{alg}$ et $x_1^\tau...x_r^\tau = 1$, pour tout $\tau \in \Lambda_K$. Il en existe une troisième qui provient du contrôle que l'on a sur l'action de $\tau \in \Lambda_K$ sur les groupes d'inertie de l'extension $\Omega/\bar{K}(T)$(voir [De8;p.233]). Sous certaines hypothèses sur le groupe G, on peut construire un homomorphisme $\Phi: \Pi^{alg} \to S_d$ tel que ces trois relations seules entraînent la condition (6) de prolongeabilité de Φ à Π_K. C'est ce cas qu'on appelle le cas "rigide"; il a été défini et développé indépendamment par Belyi, Fried, Matztat, Shih et Thompson (voir [De8;Sit.1]). Les hypothèses sont cependant assez contraignantes: en particulier, pratiquement, elles imposent $r \leq 3$. Notons d'autre part que le résultat n'est pas, comme souhaité, un critère de descente pour une extension donnée.

Il existe un cas où le problème général de la descente peut être traité avec précision, celui de la conjugaison complexe $c \in \Lambda_R$: c'est ce que nous expliquons, avec M. Fried, dans [DeFr2]. Il s'agit d'une situation assez particulière puisque l'action de c sur le

---

[1] En général, le groupe $\Phi(\Pi_K)$ contient strictement le groupe G; on l'appelle le groupe de Galois arithmétique de l'extension $E_K/K(T)$.

[2] On voit en particulier que construire une extension de $\bar{K}(T)$ de groupe de Galois G demande seulement de choisir r assez grand.

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 $\pi_1(P_1(C)\backslash\{t_1, ..., t_r\}, t_o) \simeq \Pi$. Or, si on choisit bien les générateurs $x_1,...,x_r$, cette action est donnée par des formules complètement explicites [DeFr2;§2]. En conséquence, on obtient un critère pratique permettant de décider si une extension de C(T) provient d'une extension de R(T), ou si on préfère, si un revêtement peut être défini sur R. Ce critère s'exprime très simplement s'il n'y a aucun point de ramification réel: il permet de montrer notamment que tout groupe est groupe de Galois d'une extension régulière de R(T) [Se3;p.107]. Dans le cas contraire, qui est important puisqu'il englobe le cas où tous les points de ramification sont rationnels sur Q, les formules se compliquent (voir [De8;p.235]. Nous avons cependant montré qu'elles conduisaient aux caractérisations simples suivantes [DeFr3;Th.1.1 et Th.3.1].

THEOREME 6 — (a) Un groupe fini G est le groupe de Galois d'une extension galoisienne régulière de R(T) avec r points de ramification réels ssi il est engendré par r éléments d'ordre ≤ 2.
(b) Un groupe fini G est le groupe de monodromie d'un revêtement défini sur R avec points de ramification réels ssi il existe des générateurs $\alpha_1,...,\alpha_s$ de G et un automorphisme h de G tel que $h(\alpha_i) = \alpha_i^{-1}$, $i = 1,...,s$.

Le Th.6 montre les limites du cas "rigide": les groupes obtenus par la méthode de rigidité sont engendrés par des éléments d'ordre ≤ 2. Il est naturel de demander si ces propriétés particulières de la conjugaison complexe ont des analogues p-adiques, de façon plus précise, s'il existe, dans la situation $K = Q_p$, des formules dans le groupe Π donnant l'action du Frobenius $F_p \in \Lambda_{Q_p}$ sur le groupe Π^{alg}. Nous avons montré qu'il n'en existe pas de "naturelles" [DeFr3;§3.7]. Précisons qu'Harbater a démontré par d'autres arguments que tout groupe G est le groupe de Galois d'une extension régulière de $Q_p(T)$ [Ha].

Les résultats précédents ont mis en évidence deux paramètres importants du problème: la position des points de ramification $t_1,...,t_r$ et le rôle des groupes d'inertie. Précisons ce dernier point. On peut définir, à conjugaison près dans Π^{alg}, un générateur "canonique" des groupes d'inertie de l'extension $\Omega/\bar{K}(T)$ au dessus de t_i, $i = 1,...,r$. Notons c_i, $i = 1,...,r$, la classe de conjugaison de Π^{alg} correspondante. On peut montrer que les générateurs $x_1,...,x_r$ du groupe Π^{alg} peuvent être respectivement choisis dans les classes de conjugaison $c_1,...,c_r$ (Cf. [Se3;§7.3]). Si $\Phi: \Pi^{alg} \to G$ est notre homomorphisme donné, notons C_i la classe de conjugaison dans G de l'élément $\Phi(x_i) = g_i$, $i = 1,...,r$. On retrouve ainsi, par la voie algébrique, les classes de conjugaison $C_1,...,C_r$ de la seconde partie. Et on obtient avec la condition (2) une condition nécessaire pour que la descente sur K soit possible, i.e., pour que l'homomorphisme se prolonge à Π_K[1]. On peut préciser l'exposant a de (2): c'est la valeur en τ du caractère cyclotomique

$$\chi_K: \Lambda_K \to \prod_N G(K(\mu_N)/K)$$

du corps K. Noter que, pour la question galoisienne, la condition (2) se simplifie puisque l'élément γ, qui peut être choisi dans G, disparait. On obtient en particulier que le r-

[1] On peut retrouver ici cette condition comme conséquence de la troisième relation entre les x_i et les x_i^τ évoquée plus haut.

uple $\mathbf{C} = (C_1,...,C_r)$ doit être invariant, à l'ordre près, sous l'élévation à la puissance $\chi_K(\tau)$-ième, pour tout $\tau \in \Lambda_K$. On dit dans ce cas que $\mathbf{C}$ est un r-uple K-rationnel de classes de conjugaisons de G. Si $K = \mathbf{Q}$ et si $t_1,...,t_r$ sont dans $\mathbf{Q}$, chacune des classes C_i doit être rationnelle, i.e., invariante sous l'élévation à toute puissance première à l'ordre de g_i: c'est l'hypothèse classique de rationalité du théorème de rigidité.

Concentrons nous maintenant sur le problème de la recherche d'extensions galoisiennes de K(T) de groupe de Galois donné G. On peut procéder de la façon suivante. On se donne un r-uple $\mathbf{C} = (C_1,...,C_r)$ de classes de conjugaisons de G, qu'on suppose K-rationnel, et on regarde, en faisant varier $\{t_1,...,t_r\}$, l'ensemble de toutes

(7) les extensions galoisiennes de $\mathbf{P}_1(T)$ non ramifiées en dehors de $t_1,...,t_r$, de groupe de Galois G et tels que, pour $i = 1,...,r$, les générateurs canoniques 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

(8) les G-revêtements de $\mathbf{P}_1$ (i.e., revêtements galoisiens de $\mathbf{P}_1$ de groupe G donnés avec l'action de G) non ramifiés en dehors de $t_1,...,t_r$ et tels que, pour $i = 1,...,r$ 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".

Il s'agit de voir, si parmi tous ces objets, il en existe qui soient définis sur K. Si le centre Z(G) du groupe est trivial, il existe un espace de modules qui paramètre les objets (7) (ou (8)): c'est l'espace de Hurwitz $\mathcal{H}(\mathbf{C})$ introduit dans la seconde partie. Cet espace est défini sur K du fait de la K-rationalité de $\mathbf{C}$; on sait qu'il est irréductible ssi une certaine action du groupe de tresses H(r) est transitive. Ce qui est important est que notre problème se trouve ramené à celui de trouver un point K-rationnel sur $\mathcal{H}(\mathbf{C})$. Signalons que le cas "rigide" correspond à une situation où l'espace de Hurwitz $\mathcal{H}(\mathbf{C})$ est une variété K-rationnelle.

Cette approche du problème a donné de nombreux résultats: elle a permis notamment de "réaliser" comme groupes de Galois sur $\mathbf{Q}$ tous les groupes simples sporadiques (sauf le groupe de Mathieu M_{23}) non couverts par le théorème de rigidité. La méthode, due indépendamment à Fried ([Fr2],[Fr5]) et Matzat [Ma], consiste à ramener l'étude de $\mathcal{H}(\mathbf{C})$ à celle d'une courbe. Ils expliquent ensuite comment en calculer le genre g. La méthode permet de conclure que $\mathcal{H}(\mathbf{C})$ est, comme dans le cas rigide, une variété K-rationnelle si $g = 0$ et si on peut trouver un point K-rationnel sur la courbe. Les calculs sont malheureusement compliqués, se faisant même parfois sur ordinateur; pratiquement, la méthode n'est utilisable que pour $r \leq 4$. Cette méthode est également détaillée dans [DeFr3] où nous l'appliquons au groupe $G = S_d$. On y obtient le résultat suivant:

(9) pour $d = 4, 5, 6, 7, 10$, il existe une extension galoisienne régulière $E/\mathbf{Q}(T)$ de groupe S_d ramifiée en $r = 4$ points rationnels et telle que les extensions résiduelles $E_t/\mathbf{Q}$ soient totalement réelles pour tout t dans un ouvert non vide de $\mathbf{P}_1(\mathbf{R})$.

Serre a montré que pour $r = 3$ à la place de $r = 4$, seul le groupe symétrique S_3 a cette propriété [Se2].

En dehors de ces cas de rationalité, la recherche de points rationnels sur les espaces de Hurwitz est un problème difficile. On peut commencer par regarder le problème sur les complétions de $\mathbf{Q}$. Ainsi, nos résultats sur la conjugaison complexe peuvent

s'interpréter comme un critère d'existence de points R-rationnels sur les espaces de Hurwitz [De8;Th.4bis]. Pour les corps p-adiques Q_p, on peut utiliser un travail de Harbater [Ha]. En combinant ces résultats, j'ai pu construire une famille d'exemples où l'espace de Hurwitz $\mathcal{H}$ vérifie $\mathcal{H}(R) \neq \emptyset$ et $\mathcal{H}(Q_p) \neq \emptyset$ pour tout nombre premier [De8]. Montrer que $\mathcal{H}(Q) \neq \emptyset$ serait un pas important: en effet, dans cet exemple, le groupe G peut être n'importe quel groupe engendré par des éléments d'ordre 2. Mais à l'inverse, nous avons donné également un exemple où l'espace de Hurwitz est irréductible, défini sur Q et n'a aucun point Q-rationnel. Ce dernier exemple est intéressant car il montre bien la difficulté du problème, même pour un groupe aussi simple que le groupe diédral D_m d'ordre 2m. Cet exemple s'obtient comme conséquence du résultat plus précis suivant.

THEOREME 7 — Soient m un nombre premier > 7 et K un corps de nombres de degré [K:Q] = n premier à m-1. Alors les propriétés suivantes sont équivalentes.
(i) Le groupe diédral D_m est le groupe de Galois d'une extension galoisienne régulière de K(T) ramifiée en au plus 5 points.
(ii) Il existe un point K-rationnel sur la courbe modulaire $Y_0(m)$ qui ne soit pas une pointe.

Le Th.7 est démontré dans [DeFr3] dans le cas K = Q; la généralisation ci-dessus n'est pas difficile. Le cas essentiel est celui où r = 4 et où les classes de conjugaison $C_1,\ldots,C_4$ sont égales à la classe des éléments d'ordre 2 du groupe (en particulier, elles sont rationnelles). L'espace de Hurwitz peut être comparé dans ce cas à la courbe modulaire $Y_0(m)$. En combinant le Th.7 avec le théorème de Mazur [Se1], on obtient en particulier que si m est un nombre premier > 7, alors le groupe diédral D_m ne peut être réalisé comme groupe de Galois sur Q(T) que si on autorise au moins 6 points de ramification.

REFERENCES

[Bo1] E. Bombieri, On G-functions, Recent progress in analytic number theory, H. Halberstam and C. Hooley ed., Acad. Press, (1981), Vol. 2, 1-67.
[Bo2] E. Bombieri, On Weil's "Théorème de décomposition", Amer. J. Math., 105, (1983), 295-308.
[De1] P. Dèbes, Une version effective du théorème d'irréductibilité de Hilbert, Sém. Anal. Ultram., Amice-Christol-Robba, 10ème année, (1982/83), n°10.
[De2] P. Dèbes, Spécialisations de polynômes, Math. Rep. Acad. Sci., Royal Soc. Canada, Vol. V, n°6, (Déc. 1983).
[De3] P. Dèbes, Valeurs algébriques de fonctions algébriques et théorème d'irréductibilité de Hilbert, Thèse 3ème cycle, Publ. Univ. P. et M. Curie (Paris VI), (1984).
[De4] P. Dèbes, Quelques remarques sur un article de Bombieri concernant la théorème de décomposition de Weil, Amer. J. Math., 107, (1985), 39-44.
[De5] P. Dèbes, G-fonctions et théorème d'irréductibilité de Hilbert, Acta Arithmetica, Vol.47, n° 4, (1986).
[De6] P. Dèbes, Parties hilbertiennes et progressions géométriques, C.R. Acad. Sc. Paris, t.302, Série I, n° 3, (1986).
[De7] P. Dèbes, Résultats récents liés au théorème d'irréductibilité de Hilbert, Sém. Th. Nombres, Paris, 1985-86, Birkhauser, (1987).
[De8] P. Dèbes, Groupes de Galois sur K(T), Sém. Th. Nombres, Bordeaux 2, (1990), 229-243.
[De9] P. Dèbes, On the irreducibility of the polynomials $P(t^m,Y)$, preprint, (1991), envoyé au J.Number Theory.
[DeFr1] P. Dèbes and M. Fried, Arithmetic variation of fibers, J. für die reine und angew. Math., 409,

(1990), 106-137.
[DeFr2] P. Dèbes and M. Fried, Rigidity and real residue class fields, Acta Arithmetica, Vol 56, n° 4, (1990).
[DeFr3] P. Dèbes and M. Fried, Non rigid situations in constructive Galois theory, preprint, (1990), envoyé au J.Number Theory.
[DvZa] R. Dvornicich and U. Zannier, Field containing values of algebraic functions, Publ. Univ. Pisa, (Nov. 1983).
[Fr1] M. Fried, Arithmetical properties of value sets of polynomials, Acta Arithmetica, Vol. 15, (1969).
[Fr2] M. Fried, Fields of definition of function fields and Hurwitz families - Groups as Galois groups, Comm. in Alg., 5(1), (1977), 17-82.
[Fr3] M. Fried, Exposition on an arithmetic-group theoretic connection via Riemann's existence theorem, Proceedings of symposia in pure mathematics, Vol. 37, The Santa Cruz conference on finite groups, (1980).
[Fr4] M. Fried, On the Sprindzuk-Weissauer approach to universal Hilbert subsets, Israel J. Math., Vol. 51, n° 4, (1985).
[Fr5] M. Fried, Arithmetic of 3 and 4 branch point covers, Sém. Th. Nombres, Paris 1987-88, Birkhauser, (1990).
[Fr6] M. Fried, Rigidity and applications of the classification of simple groups to monodromy, Part I-Super rational connectivity; Examples, and Part II-Applications of connectivity; Davenport-Hilbert-Siegel problems, preprint.
[Ha] D. Harbater, Galois covering of the arithmetic line, Proc. of the NY Number Thy. Conf. of 1985, LNM 1240, Springer.
[Ma] B.H. Matzat, Konstruktive Galoistheorie, LNM 1284, Springer-Verlag, (1987).
[Se1] J-P Serre, Points rationnels des courbes modulaires, Séminaire Bourbaki, 30ème année, 1977/78, n° 511.
[Se2] J-P Serre, Groupes de Galois sur Q, Séminaire Bourbaki, Volume 1987/88, n°689.
[Se3] J-P Serre, Topics in Galois theory, Course at Harvard University (Fall 1988), Notes written by Henri Darmon, preprint.
[Sp1] V.G. Sprindzuk, Reducibility of polynomials and rational points on algebraic curves, J. Reine und Angew. Math., Sém. Th. Nombres, Paris 1979-80, Birkhauser, (1981), 287-309.
[Sp2] V.G. Sprindzuk, Arithmetic specialisations in polynomials, J. Reine und Angew. Math., 340, (1983), 26-52.
[We] R. Weissauer, Hilbertsche Körper, Thesis, Heidelberg, (1980).

Pierre Dèbes
"Problèmes diophantiens"
Institut Henri Poincaré
11, rue Pierre et Marie Curie
75231 PARIS CEDEX 05
FRANCE
E-mail: pde@frunip62.bitnet