SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

J. R. JOLY

Exemples classiques d'extensions normales de Q à groupe de Galois non résoluble

Séminaire de théorie des nombres de Grenoble, tome 2 (1972-1973), exp. n° 5, p. 1-15

<http://www.numdam.org/item?id=STNG_1972-1973__2__A5_0>

J. R. JOLY

19,26 oct. 72 et 22 fév. 73

EXEMPLES CLASSIQUES D'EXTENSIONS NORMALES DE $\mathbb{Q}$ A GROUPE DE GALOIS NON RESOLUBLE

(Cette rédaction résume trois exposés de séminaire faits les 19 et 26 octobre 1972, et le 22 février 1973).

1. INTRODUCTION.

Soit k un corps parfait de clôture algébrique $\bar{k}$. Etant donné un groupe fini G, on peut se poser la question suivante :

(Q) G est-il "réalisable galoisiennement sur k" ? autrement dit, existe-t-il une extension normale K de k telle que $G \simeq \mathrm{Gal}(K/k)$? ou encore, existe-t-il, dans le groupe de Galois "absolu" $\mathfrak{G}_k = \mathrm{Gal}(\bar{k}/k)$, un sous-groupe ouvert distingué U tel que $G \simeq \mathfrak{G}_k/U$?

Lorsque le groupe $\mathfrak{G}_k$ est entièrement connu, la réponse à (Q) est immédiate ; c'est ce qui se produit notamment dans les exemples suivants :

Exemple 1 : $k = \mathbb{F}_q$, corps fini. On a alors $\mathfrak{G}_k \simeq \hat{\mathbb{Z}}$, complété profini de $\mathbb{Z}$, et G est donc réalisable galoisiennement sur k si, et seulement si, il est cyclique.

Exemple 2 : $k = \mathbb{C}\{t\}$, corps des séries formelles restreintes ([1]) en t, à coefficients dans $\mathbb{C}$; ou bien $k = \mathbb{C}((t))$, corps de toutes les séries formelles en t, à coefficients dans $\mathbb{C}$. Dans ce double exemple, on a encore $\mathfrak{G}_k \simeq \hat{\mathbb{Z}}$ (par le théorème de Puiseux, pour $\mathbb{C}\{t\}$; par le théorème de Puiseux "formel" - voir par exemple [9], p. 76, th. 8 - pour $\mathbb{C}((t))$) et la réponse à (Q) est donc la même que dans l'exemple 1.

Exemple 3 : $k = \mathbb{C}(t)$, corps des fractions rationnelles en t, à coefficients dans $\mathbb{C}$. On sait que $\mathfrak{G}_k$ est alors un progroupe libre de

probase équipotente à l'ensemble des éléments de $\mathbb{C}$ (voir [1] ; voir également le § 3 ci-dessous, remarque 2) ; la réponse à (Q) est donc immédiate : tout groupe fini est réalisable galoisiennement sur k .

Exemple 4 : $k = \mathbb{R}(t)$, corps des fractions rationnelles en t , à coefficients dans $\mathbb{R}$. Une description complète de g_k est donnée dans [4] ; la réponse à (Q) est la même que dans l'exemple 3 .

*

Venons-en au cas fondamental, celui de $k = \mathbb{Q}$, corps des nombres rationnels. On voit sans peine, en utilisant les propriétés des corps cyclotomiques, que tout groupe fini commutatif est réalisable galoisiennement sur $\mathbb{Q}$. Plus généralement, Shafarevich a démontré (voir [12] : c'est loin d'être trivial !) que tout groupe fini résoluble est réalisable galoisiennement sur $\mathbb{Q}$. Au contraire, pour un groupe fini G non résoluble, mais par ailleurs quelconque, on ne sait pas, à l'heure actuelle, répondre à la question (Q) (encore qu'il soit assez raisonnable - et en tout cas sans grand risque - de conjecturer , vu l'énormité du groupe $g_{\mathbb{Q}}$, que tout groupe fini est réalisable galoisiennement sur $\mathbb{Q}$) .

Dans ces conditions, le but de cette rédaction est de montrer comment on peut, pour des groupes finis non résolubles G particuliers, prouver l'existence de réalisations galoisiennes de G sur $\mathbb{Q}$; en fait, on traite le cas de $G = GL(2,\mathbb{Z}/n\mathbb{Z})$ (§ 2, th. 1), celui de G = le groupe symétrique $\mathfrak{S}_n$ (§ 3) . La méthode utilisée comporte une application du théorème d'irréductibilité de Hilbert (voir la fin de ce § 1) et ne donne pas de résultats explicites ; on montre donc, au § 4 , comment il est possible, dans certains cas, de tourner cette difficulté, et on donne, à titre d'exemple, une équation explicite à groupe de Galois $PGL(2,\mathbb{Z}/7\mathbb{Z})$ et une équation explicite à groupe de Galois $\mathfrak{S}_{17}$. (Bien entendu, les groupes envisagés ci-dessus sont en général non résolubles ; $\mathfrak{S}_n$ l'est pour $n \geq 5$, du fait que $\mathfrak{A}_n$ est alors simple d'ordre non premier ; $GL(2,\mathbb{Z}/n\mathbb{Z})$ et $PGL(2,\mathbb{Z}/n\mathbb{Z})$ le sont dès que n contient un facteur pre-

mier ≥ 5 , du fait que $PSL(2,\mathbb{F}_q)$ n'est résoluble que pour $q = 2$ ou 3 . Par ailleurs, les seuls "isomorphismes exceptionnels" entre ces divers groupes sont

$$\mathfrak{S}_3 \simeq GL(2,\mathbb{F}_2) \simeq PGL(2,\mathbb{F}_2)$$

$$\mathfrak{S}_4 \simeq PGL(2,\mathbb{F}_3)$$

$$\mathfrak{S}_5 \simeq PGL(2,\mathbb{F}_5) \ . \quad)$$

Les résultats des §§2-3 remontent essentiellement à Weber et Hilbert, en ce qui concerne les groupes $PGL(2,\mathbb{Z}/n\mathbb{Z})$ et $\mathfrak{S}_n$. Quant aux groupes $GL(2,\mathbb{Z}/n\mathbb{Z})$, Serre vient de montrer (comme on le conjecturait depuis longtemps) qu'on en obtient presque systématiquement en adjoignant à $\mathbb{Q}$ les coordonnées des points de division par n de courbes elliptiques définies sur $\mathbb{Q}$; voir [10] (et aussi [9]) ainsi que le §4.2.

*

Le théorème d'irréductibilité de Hilbert, mentionné plus haut, est le résultat suivant : soient $t_1,\ldots,t_m$, x , $m+1$ indéterminées, et soit

$$f(t_1,\ldots,t_m\ ;\ x) = f(t;x)$$

un polynôme à coefficients dans $\mathbb{Z}$ par rapport à ces indéterminées ; alors, si f est irréductible et de degré n par rapport à la seule indéterminée x , il existe une infinité de points $a = (a_1,\ldots,a_m)$ dans $\mathbb{Q}^m$ (et même dans $\mathbb{Z}^m$) tels que le polynôme $f(a_1,\ldots,a_m,x) = f(a,x)$ soit encore irréductible et de degré n ; autrement dit, il existe une infinité de spécialisations $t \to a$, $(a \in \mathbb{Z}^m)$ n'affectant ni le degré, ni le caractère irréductible du polynôme $f(t,x)$ (par rapport à x). Pour une démonstration de ce théorème, voir [3] ou [6] . Une conséquence presque immédiate est la suivante (voir par exemple [6] , p. 141) : avec les mêmes hypothèses et notations, il existe une infinité de $a \in \mathbb{Z}^m$ tels que le groupe de Galois de $f(a,x)$ sur $\mathbb{Q}$ soit le même que le groupe de Galois de $f(t,x)$ sur $\mathbb{Q}(t)$; autrement dit, il existe une infinité de spécialisations $t \to a$ $(a \in \mathbb{Z}^m)$ n'affectant ni le degré, ni l'irréductibi-

lité, ni même le groupe de Galois de $f(t,x)$.

C'est cette forme "forte" du théorème d'irréductibilité qui sera utilisée plus loin, pour $m = 1$. Compte tenu de l'application qu'on veut en faire, il y a d'ailleurs avantage à la réénoncer de la manière suivante (visiblement équivalente à la précédente, compte tenu du théorème de l'élément primitif) :

Théorème 0.

Si un groupe fini G est réalisable galoisiennement sur $\mathbb{Q}(t)$, il est aussi réalisable galoisiennement sur $\mathbb{Q}$.

2. REALISATION GALOISIENNE SUR $\mathbb{Q}$ DES GROUPES $GL(2,\mathbb{Z}/n\mathbb{Z})$ et $PGL(2,\mathbb{Z}/n\mathbb{Z})$.

Théorème 1.

Quel que soit $n \geq 1$, le groupe $GL(2,\mathbb{Z}/n\mathbb{Z})$ est réalisable galoisiennement sur $\mathbb{Q}$.

Démonstration : Soit t un élément transcendant sur $\mathbb{Q}$, et soit E une courbe elliptique, définie sur $\mathbb{Q}(t)$ et ayant t pour invariant modulaire (^{2}) (par exemple, la courbe $y^2 = 4x^3 - gx - g$, avec $g = 27t/(t-1728)$) . Soit E_n le groupe de tous les points de division par n sur E , et soit D le corps obtenu par adjonction à $\mathbb{Q}(t)$ des abscisses et des ordonnées des points de E_n . Comme l'ensemble E_n est algébrique et de dimension 0 sur $\mathbb{Q}(t)$, l'extension $D/\mathbb{Q}(t)$ est galoisienne et de degré fini. Soit G son groupe de Galois. Comme le groupe E_n est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^2$ (on est en caractéristique 0), l'action naturelle de G sur E_n définit un homomorphisme injectif de G dans $GL(2,\mathbb{Z}/n\mathbb{Z})$. Mais :

Lemme 1.

Cet homomorphisme $G \to GL(2,\mathbb{Z}/n\mathbb{Z})$ est un isomorphisme.

[Démonstration du lemme : analogue à celle du th.6.6, (2), de [15], pp. 137-138].

Ce lemme 1 montre donc que $GL(2,\mathbb{Z}/n\mathbb{Z})$ est réalisable galoisiennement sur $\mathbb{Q}(t)$ (par $D/\mathbb{Q}(t)$). Il suffit alors d'appliquer le théorème 0 pour obtenir le théorème 2.

Corollaire.

Tout groupe quotient de $GL(2,\mathbb{Z}/n\mathbb{Z})$ est réalisable galoisiennement sur $\mathbb{Q}$.

Ce corollaire (simple application de la théorie de Galois !) montre en particulier que tout groupe $PGL(2,\mathbb{Z}/n\mathbb{Z})$ est réalisable galoisiennement sur $\mathbb{Q}$. On donne ci-dessous une autre démonstration de ce résultat (^{3}).

*

Théorème 2.

Quel que soit $n \geq 1$, le groupe $PGL(2,\mathbb{Z}/n\mathbb{Z})$ est réalisable galoisiennement sur $\mathbb{Q}$.

Démonstration : Soit j la fonction "invariant modulaire", et soit j_n la fonction définie par $j_n(\tau) = j(n\tau)$ (τ étant une variable décrivant le demi-plan de Poincaré). On sait (voir par exemple [2], ou encore [13]) que j_n est une fonction algébrique de j, et plus précisément qu'il existe un polynôme $F_n(t,x)$, irréductible, à coefficients entiers rationnels, tel que $F_n(j,j_n) = 0$. On sait également (voir [13], prop.6.8, p. 139 ; ou bien [7]) que le groupe de Galois sur $\mathbb{Q}(t)$ de $F_n(t,x)$ est égal à $PGL(2,\mathbb{Z}/n\mathbb{Z})$. Ainsi, $PGL(2,\mathbb{Z}/n\mathbb{Z})$ est réalisable galoisiennement sur $\mathbb{Q}(t)$, donc sur $\mathbb{Q}$ (th.0), et le théorème 2 est (re)démontré.

*

Remarque 1 : Avec les notations du théorème 1, soit η un élément primitif de D sur $\mathbb{Q}(t)$ et soit $f(t,y)$ le polynôme minimal de η sur $\mathbb{Q}(t)$; soit enfin $a \in \mathbb{Z}$ un entier rationnel tel que le groupe de Galois de $f(a,y)$ sur $\mathbb{Q}$ soit isomorphe à $GL(2,\mathbb{Z}/n\mathbb{Z}) = G$ (lemme 1). Alors évidemment :

1) le groupe de Galois de $F_n(a,x)$ sur $\mathbb{Q}$ est isomorphe à $PGL(2,\mathbb{Z}/n\mathbb{Z})$;

2) le groupe de Galois de l'extension de $\mathbb{Q}$ obtenue en adjoignant à $\mathbb{Q}$ les coordonnées des points de division par n sur la courbe elliptique $y^2 = 4x^3 - cx - c$, avec $c = 27a/(a-1728)$, est isomorphe à $GL(2,\mathbb{Z}/n\mathbb{Z})$.

Ce genre de remarque sera utilisé à nouveau au § 4 .

3. REALISATION GALOISIENNE SUR $\mathbb{Q}$ DU GROUPE SYMETRIQUE $\mathbb{S}_n$.

Théorème 3.

Quel que soit $n \geq 1$, le groupe symétrique $\mathbb{S}_n$ est réalisable galoisiennement sur $\mathbb{Q}$. Plus précisément, il existe une infinité d'entiers rationnels a tels que le groupe de Galois sur $\mathbb{Q}$ du polynôme

$$x^n - x + a \tag{3.1}$$

soit isomorphe à $\mathbb{S}_n$.

Démonstration : elle repose essentiellement sur le théorème 0, et sur le lemme suivant :

Lemme 2.

Soient t une variable complexe, et x la fonction algébrique de t définie par l'équation irréductible

$$x^n - x + t = 0 . \tag{3.2}$$

Soit T le plan complexe privé des $n-1$ points de ramification de (3.2),

notés t_j $(1 \leq j \leq n-1)$, et soit X la surface de Riemann de x, privée de ses points "au-dessus des t_j et de ∞", et par conséquent étalée sur T. Alors le groupe de monodromie (voir par exemple [15] - ou patienter un peu) du revêtement (non ramifié) $p : X \to T$ est isomorphe à $\mathfrak{S}_n$.

Admettons provisoirement ce lemme 2, et prouvons le théorème 3. D'après la théorie classique des fonctions algébriques d'une variable complexe, le groupe de Galois du polynôme $x^n - x + t$ sur $\mathbb{C}(t)$ est isomorphe au groupe de monodromie du revêtement $p : X \to T$, donc précisément à $\mathfrak{S}_n$, d'après le lemme 2. Il en résulte que le groupe de Galois (disons, G) de $x^n - x + t$ sur $\mathbb{Q}(t)$ est encore isomorphe à $\mathfrak{S}_n$: si en effet on interprète G comme sous-groupe du groupe des permutations des racines de $x^n - x + t$, on a d'une part $\mathfrak{S}_n \subset G$ (d'après ce qu'on vient de voir : la "restriction" du corps de base de $\mathbb{C}(t)$ à $\mathbb{Q}(t)$ ne peut que "faire grossir" le groupe de Galois) et d'autre part $G \subset \mathfrak{S}_n$ (puisque le polynôme est de degré n). Ainsi, S_n est réalisable galoisiennement sur $\mathbb{Q}(t)$ - donc aussi sur $\mathbb{Q}$ (th.0), et le théorème 3 est prouvé, à condition de démontrer le lemme 2, ce qui va être fait maintenant.

Soit $t_o \in T$ un point de base (choisi une fois pour toutes) et posons $E = \pi_1(T,t_o)$. Soient $x_{o_1},\ldots,x_{o_n}$ les points de X au-dessus de t_o, donc les points de la fibre $p^{-1}(t_o)$, et posons également $F_j = \pi_1(X,x_{o_j})$ pour $j = 1,\ldots,n$. Par la projection p, chaque F_j s'applique injectivement sur un sous-groupe F_{j*} de E, et $(F_{j*})_{1\leq j\leq n}$ est une famille complète de conjugués dans E. Si on pose $F = \bigcap_{1\leq j\leq n} F_{j*}$, F est donc un sous-groupe distingué de E, et le groupe-quotient $\Gamma = E/F$ est par définition le groupe de monodromie du revêtement $p : X \to T$. L'interprétation de Γ est la suivante : pour tout $\tilde{\lambda} \in \pi_1(T,t_o)$, soit λ un lacet de la classe d'homotopie $\tilde{\lambda}$, et soit λ_j le relèvement de λ en un arc tracé sur X et ayant pour "point de départ" x_{oj} ; le "point d'arrivée" de λ_j ne dépend que de $\tilde{\lambda}$ et de x_{oj}, et appartient à la fibre $p^{-1}(t_o)$: c'est donc un x_{ok}, pour un k bien déterminé $(1 \leq k \leq n)$; posons donc $\tilde{\lambda}.x_{oj} = x_{ok}$. L'application $(\tilde{\lambda},x_{oj}) \to \tilde{\lambda}.x_{oj}$ de

$\pi_1(T,t_o) \times p^{-1}(t_o)$ dans $p^{-1}(t_o)$ est alors une action (à droite ou à gauche, selon la façon de noter la composition des lacets !) de $E = \pi_1(T,t_o)$ sur $p^{-1}(t_o)$, et définit donc un homomorphisme de E dans $\mathfrak{S}(p^{-1}(t_o))$, groupe des permutations des n points $x_{o_1},\ldots,x_{o_n}$ de $p^{-1}(t_o)$. Le noyau de cet homomorphisme est évidemment F, et voici donc l'interprétation promise : <u>le groupe de monodromie</u> $\Gamma = E/F$ <u>est isomorphe au groupe des permutations de</u> $p^{-1}(t_o) = \{x_{o_1},\ldots,x_{o_n}\}$ <u>résultant de l'action naturelle de</u> $E = \pi_1(T,t_o)$ <u>sur</u> $p^{-1}(t_o)$.

Examinons maintenant le revêtement particulier du lemme 2. Les $n-1$ points de ramification sont donnés (en posant $f(t,x) = x^n - x + t$) par $t = t_i = -x_i^n + x_i$, où x_i $(1 \le i \le n-1)$ parcourt l'ensemble des $n-1$ racines de l'équation $f'_x(t,x) = nx^{n-1} - 1 = 0$. Ces racines sont distinctes, et le type de ramification est décrit par la figure 1 (on a pris $n = 4$, pour fixer les idées ; Y désigne la surface de Riemann de x au-dessus de $\mathbb{C}$, donc <u>avec</u> points de ramification).

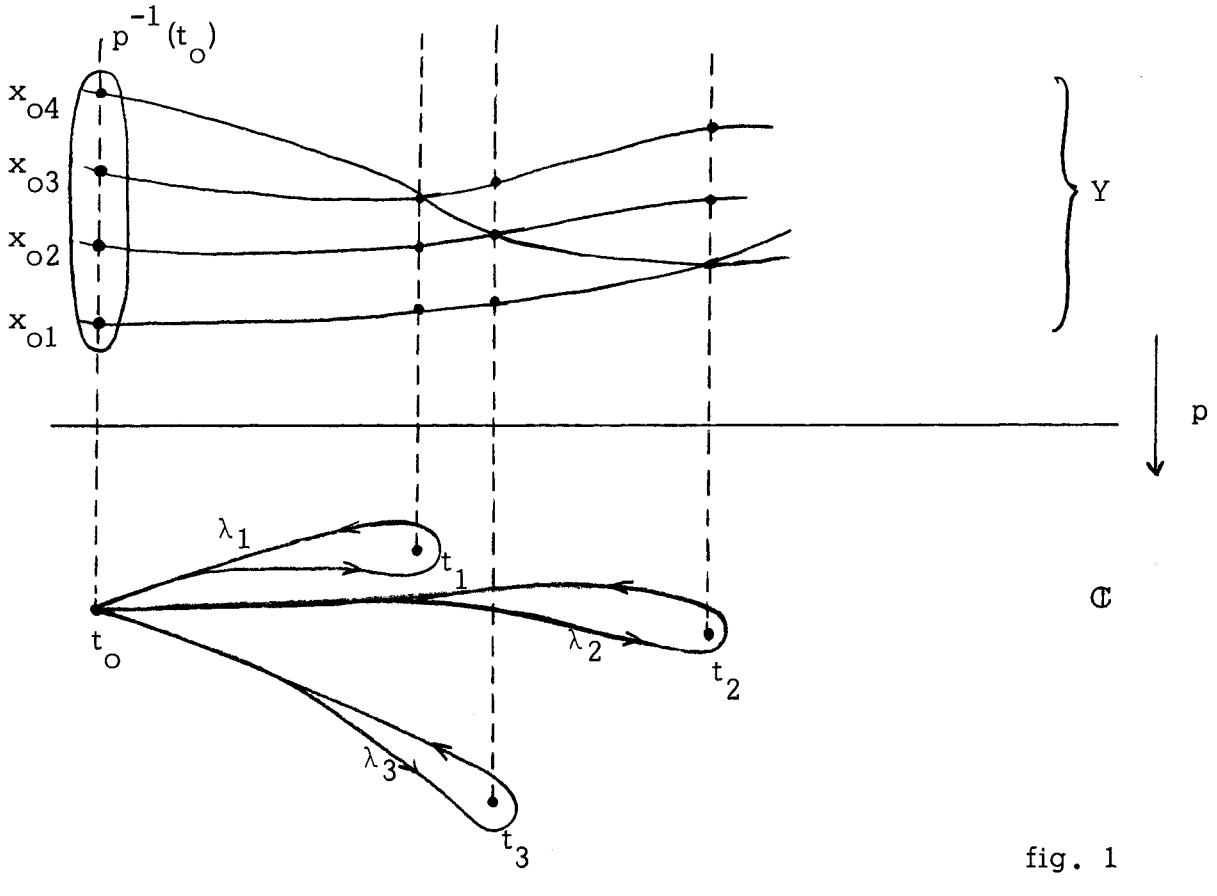

fig. 1

Soient $\tilde{\lambda}_i$ les classes dans $E = \pi_1(T,t_o)$ des lacets λ_i de la fig.1, et σ_i les images des λ_i dans le groupe $\mathfrak{S}(p^{-1}(t_o))$ des permutations de $p^{-1}(t_o)$. Les σ_i ont les propriétés suivantes :

a) $(\sigma_1,\ldots,\sigma_{n-1})$ est un système générateur de $\Gamma = E/F$ en tant que sous-groupe de $\mathfrak{S}(p^{-1}(t_o))$ (avec les identifications évidentes). En effet, $(\tilde{\lambda}_1,\ldots,\tilde{\lambda}_{n-1})$ est un système générateur de $\pi_1(T,t_o) = E$ (c'est bien connu...) .

b) Chaque σ_i est une <u>transposition</u> dans $p^{-1}(t_o)$. Cela résulte du type de ramification : regarder la figure et se prendre la tête entre les mains...

D'autre part :

c) Le groupe Γ opère <u>transitivement</u> sur $p^{-1}(t_o)$. Car, X étant connexe, E opère lui-même transitivement.

Ces propriétés a), b), c) montrent que Γ s'identifie à un sous-groupe <u>transitif</u> de $\mathfrak{S}_n$ ($\simeq \mathfrak{S}(p^{-1}(t_o))$ engendré par $n-1$ transpositions ; un tel sous-groupe est nécessairement égal à $\mathfrak{S}_n$ tout entier, d'où $\Gamma \simeq \mathfrak{S}_n$, et le lemme 2.

<u>Remarque 1</u> : Ce théorème 3 est dû à Hilbert [3] . Dans le même article, Hilbert prouve également -et de manière analogue- que le groupe alterné $\mathfrak{A}_n$ est réalisable galoisiennement sur $\mathbb{Q}$ pour tout n .

<u>Remarque 2</u> : Dans la démonstration du lemme 2, on a utilisé ce résultat de topologie algébrique :

> si S est un ensemble de n points distincts de $\mathbb{C}$, et si on pose $T_S = \mathbb{C}\backslash S$, alors le groupe foncdamental $\pi_1(T_S)$ est un groupe -non nécessairement- commutatif libre à n générateurs (démonstration par récurrence sur $n \geq 1$: pour $n = 1$, on sait que $\pi_1(\mathbb{C}^*) \simeq \mathbb{Z}$; pour la transition $n-1 \to n$, utiliser le théorème de Van Kampen).

Par ailleurs, les résultats généraux sur les revêtements, et le théorème d'uniformisation de Riemann-Poincaré, montrent qu'il revient au même de se donner

- une extension $K/\mathbb{C}(t)$ galoisienne, de degré fini et non ramifiée hors de $S \cup \{\infty\}$;
- un revêtement galoisien $X \to T_S$ de degré fini et non ramifié ;
- un sous-groupe ouvert distingué d'indice fini de $\pi_1(T_S)$;

et par conséquent que le groupe de Galois G_S de l'extension maximale de $\mathbb{C}(t)$ non ramifiée hors de $S\backslash\{\infty\}$ est isomorphe au complété profini $\pi_1(T_S)$. Au total, G_S est donc un progroupe libre à n générateurs, et il suffit de "passer à la limite sur S" (ce qui pose quand même quelques problèmes techniques : mais voir [1]) pour obtenir le théorème de structure de $\mathcal{G}_{\mathbb{C}(t)}$ cité au §1, exemple 3.

Exercice : Soit $\Gamma_o(n)$ le sous-groupe du groupe modulaire $SL(2,\mathbb{Z})$ formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $c \equiv 0 \pmod{n}$. Soient $\mathcal{H}$ le demi-plan de Poincaré, τ une variable complexe décrivant $\mathcal{H}$, $X_o(n)$ la surface de Riemann $\mathcal{H}/\Gamma_o(n)$, et p la projection $X_o(n) \to X_o(1)$ ($X_o(1)$, quotient compactifié de $\mathcal{H}$ par $\Gamma_o(1) = SL(2,\mathbb{Z})$, n'est autre que la sphère de Riemann "lieu de $j(\tau)$") . Montrer que ce revêtement $p : X_o(n) \to X_o(1)$ s'identifie à la surface de Riemann de j_n (voir § 2, th.2) en tant que fonction de j . Calculer le groupe de monodromie correspondant. En déduire le résultat suivant :

> le groupe de Galois sur $\mathbb{C}(t)$ de l'équation $F_n(t,x) = 0$ est isomorphe à $PSL(2,\mathbb{Z}/n\mathbb{Z})$.

Comparer avec ce qui se passe sur le corps de base $\mathbb{Q}(t)$.

4. EXEMPLES NUMERIQUES.

Comme on l'avait annoncé au §1, les résultats des §§2-3 sont des théorèmes d'existence, mais ne donnent pas directement d'exemples

numériques explicites d'équations sur $\mathbb{Q}$ à groupe de Galois non résoluble. Le but de ce §4 est de montrer comment on peut, "à coups de Frobenius" (au sens de la théorie des corps de nombres algébriques, ou de la théorie des courbes elliptiques, selon le cas : mais le raisonnement est essentiellement le même), arriver néanmoins à des exemples explicites (on se limite à deux exemples, mais la généralité de la méthode est évidente ; voir d'ailleurs les remarques).

4.1. Une équation à groupe de Galois $\mathfrak{S}_{17}$.

Il suffit de trouver une "bonne" valeur pour a dans l'équation générale $x^{17} - x + a = 0$ (voir th.3). En fait, on peut prendre $a = 1$. En effet :

- modulo 17 , le polynôme $x^{17} - x + 1$ est irréductible (il l'est donc déjà sur $\mathbb{Q}$) et son groupe de Galois est cyclique d'ordre 17 (engendré par $\alpha \to \alpha+1$) ; le groupe de Galois G de $x^{17} - x + 1$ sur $\mathbb{Q}$ contient donc une "permutation circulaire" d'ordre 17 ;

- modulo 2 , ce même polynôme admet le facteur du second degré $x^2 - x + 1$ (noter que si β est primitif pour $\mathbb{F}_4/\mathbb{F}_2$, on a $\beta^2 - \beta + 1 = 0$ et $\beta^4 = \beta$, donc $\beta^{17} - \beta + 1 = 0$) , facteur évidemment irréductible et de groupe de Galois cyclique d'ordre 2 ; le groupe de Galois G de $x^{17} - x + 1$ sur $\mathbb{Q}$ contient donc une "transposition".

Au total, on a $G \subset \mathfrak{S}_{17}$, et G contient une transposition et une permutation circulaire d'ordre 17 . Donc $G = \mathfrak{S}_{17}$.

Conclusion : le groupe de $x^{17} - x + 1$ sur $\mathbb{Q}$ est $\mathfrak{S}_{17}$.

Remarque 1 : Au sujet de la construction d'équations sur $\mathbb{Q}$ à groupe $\mathfrak{S}_n$, voir l'exposé d'A. Philippe à ce même séminaire [8]. On y trouve par exemple une équation à groupe de Galois $\mathfrak{S}_6$,

$$x^6 + 12x^5 - 2x^4 + 22x^3 + 19x - 31 = 0 \quad .$$

Notons également que la classique équation $x^5-x+1 = 0$ (à groupe $\mathfrak{S}_5$; c'est l'équation "pour laquelle Artin avait un faible" , d'après Lang) rentre dans le paradigme du th.3.

Remarque 2 : Les Frobenius annoncés en début de paragraphe sont la permutation circulaire et la transposition vues ci-dessus (engendrant les groupes de décomposition évidents) et qui "obligent $G \subset \mathfrak{S}_{17}$ à être égal à $\mathfrak{S}_{17}$ tout entier".

4.2. Une équation à groupe de Galois $PGL(2,\mathbb{Z}/7\mathbb{Z})$.

Considérons d'abord de façon générale $n \geq 1$, et utilisons la remarque 1 complétant le th. 2, et les résultats classiques de Fricke sur l'équation $F_n(t,x)$ lorsque cette équation est de genre 0 [2] . Il est clair que si a est l'invariant modulaire j_E d'une courbe elliptique E défini sur $\mathbb{Q}$, sans multiplication complexe, et telle que le groupe de Galois de l'extension $\mathbb{Q}(E_n)/\mathbb{Q}$ (voir §2, remarque 2, 2)) soit isomorphe à $GL(2,\mathbb{Z}/n\mathbb{Z})$, alors le groupe de Galois de $F_n(a,x)$ sur $\mathbb{Q}$ est isomorphe à $PGL(2,\mathbb{Z}/n\mathbb{Z})$. Une telle valeur a peut se trouver en utilisant les résultats de Serre déjà mentionnés ([11], notamment pp.309-316, et pp. 318-320) ; ainsi, on peut prendre, pour $n = 7$,

$$a = -2^{12}.11^{-1} \quad ; \quad a = -2^{12}.11^{-5}.31^3 \quad ;$$

$$a = -2^{-2}.5^6.7^{-1} \quad ; \quad \text{etc...} \qquad \text{(pp. 309-316).}$$

Si on veut des valeurs entières, on peut prendre

$$a = 2^5.7^3 \quad ; \quad a = 2^9.3 \quad ;$$

$$a = -11^2 \quad ; \quad \text{etc... (pp. 118-120) .}$$

(L'article de Shimura [13] déjà cité fournit, de façon relativement élémentaire, la valeur $a = -2^{12}.11^{-5}.31^3$, qui figure d'ailleurs dans la liste ci-dessus, et correspond à la courbe $X_o(11)$, qui est de genre 1). D'autre part, si $F_n(t,x) = 0$ est de genre 0 (et c'est le cas pour $n = 7$) , on peut, en utilisant la fonction "τ" de Fricke (loc. cit.) (fonction telle que $\mathbb{Q}(t,x) = \mathbb{Q}(\tau)$) écrire

$$t = A(\tau) \quad , \quad x = B(\tau) \quad ,$$

A et B étant des éléments èxplicites de $\mathbb{Q}(\tau)$. Faire une spécialisation $t \to a$ revient évidemment à éliminer τ entre les deux équations

$$A(\tau) = a \quad , \quad B(\tau) = x \ ,$$

et on constate alors que le groupe de Galois de $A(\tau) - a = 0$ (équation en τ) sur $\mathbb{Q}$ est le même que celui de $F_n(a,x) = 0$.

Cela étant, faisons donc $n = 7$ et prenons (pour simplifier) $a = -11^2 = -121$. D'après Fricke, $A(\tau) = (\tau^2+13\tau+49)(\tau^2+5\tau+1)^3/\tau$. Ecrivons $A(\tau) - a = 0$, remplaçons $A(\tau)$ et a pour leurs valeurs, multiplions par τ et remplaçons τ par x ("pour que ça ressemble vraiment à une équation"). Nous arrivons à ceci :

CONCLUSION : l'équation

$$(x^2+13x+49)(x^2+5x+1)^3 + 121x = 0$$

a un groupe de Galois sur $\mathbb{Q}$ isomorphe à $PGL(2,\mathbb{Z}/7\mathbb{Z})$.

Remarque 1 : Bien entendu, les valeurs $n = 7$ et $a = -11^2$ n'ont rien de spécial. En fait, la méthode marche pour tout n tel que $F_n(t,x) = 0$ (ou $X_o(n)$) soit de genre 0, ou de genre 1, ou de genre ≥ 2 et hyperelliptique, ce qui permet, "à la Fricke", de "court-circuiter" le polynôme F_n . Noter que ceci n'autorise qu'un nombre fini de n (conjecture de Lehner-Newman, partiellement vérifiée par Larcher).

Remarque 2 : On peut de la même manière, mais en se fatiguant beaucoup plus, fabriquer des équations explicites à groupe de Galois $GL(2,\mathbb{Z}/n\mathbb{Z})$ pour n pas trop grand. On laisse cette tâche au lecteur, à titre d'exercice.

Remarque 3 : Pour l'intervention des Frobenius (annoncés en début de §4, mais complètement invisibles dans ce deuxième exemple), voir notamment l'article de Shimma [13], pp. 213 et 216-218, et bien entendu [11].

*

Notes

(1) c'est-à-dire méromorphes au voisinage de $t = 0$.

(2) ceci, en vue de la remarque 1 ci-dessous.

(3) ceci, en vue de la remarque 1 ci-dessous, et surtout du §4, exemple 2.

*

Bibliographie

[1] DOUADY A., Détermination d'un groupe de Galois, C.R. Acad. Sci. Paris, 258 (1964), 5305-5308.

[2] FRICKE R., Elliptische Funktionen, Leipzig (1922).

[3] HILBERT D., Ueber die Irreducibilität ganzer rationaler Functionen unit ganzzahligen Coefficienten, J. reine angew. Math., 110 (1892), 104-129.

[4] KRULL W. & NEUKIRCH J., Die Struktur der absoluten Galoisgruppe über dem Körper $\mathbb{R}(t)$, Math. Annalen, 193 (1971), 197-209.

[5] LANG S., Algebraic Number Theory, New-York (1970).

[6] LANG S., Diophantine Geometry. New-York (1962).

[7] MACBEATH A.M., Extensions of the rationals with Galois group $PGL(2,\mathbb{Z}_n)$, Bull. London Math. Soc., 1 (1969), 332-338.

[8] PHILIPPE A., Extensions minimales de corps, Mémoire de D.E.A. (1969) = exposé au séminaire de Théorie des Nombres Grenoble (1972).

[9] SERRE J.P., Corps locaux, Paris (1962).

[10] SERRE J.P., Abelian ℓ-adic representations and elliptic curves, New-York (1968).

[11] SERRE J.P., Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inventiones math., 15 (1972), 259-331.

[12] SHAFAREVICH I.R., Construction of fields of algebraic numbers with given Galois group, Izvestiia Akad. Nauk SSSR, 18 (1954), 525-578.

[13] SHIMURA G., A reciprocity law in non-solvable extensions, J. reine angew. Math., 221 (1966), 209-220.

[14] SHIMURA G., Introduction to the arithmetic theory of automorphic functions, Princeton (1971).

[15] SPRINGER G., Introduction to Riemann surfaces, Reading (1957).

[16] WEBER H., Lehrbuch der Algebra, vol.3, Strassburg (1908).

-:-:-:-