Séminaires & Congrès
5, 2001, p. 27–41

MÉTHODES TOPOLOGIQUES ET ANALYTIQUES EN THÉORIE INVERSE DE GALOIS : THÉORÈME D'EXISTENCE DE RIEMANN

par

Pierre Dèbes

Résumé. — Cet exposé couvre la partie classique de la théorie des revêtements et du groupe fondamental, avec la théorie de Galois en perspective. On aboutit au théorème d'existence de Riemann, qui fait le lien entre les aspects topologique, analytique et algébrique des revêtements de la droite. Le problème inverse de Galois géométrique sert de fil conducteur. Un exposé détaillé est proposé en annexe du volume.

***Abstract* (Riemann's existence theorem).** — With Galois theory in perspective we cover the classical part of the theory of covers and fundamental groups. We end at Riemann's existence theorem which makes the connection between the topological, the analytic and the algebraic aspects of the covers of the line. The geometric inverse Galois problem is used as a motivation and a guide into the theory. A more detailed treatment is offered in an appendix of the volume.

Cet exposé a été donné lors du colloque « Revêtements » à St-Étienne en mars 2000 et lors du Von Neumann symposium « Arithmetic Fundamental Groups and Noncommutative Algebra » en août 1999 au M.S.R.I. à Berkeley. Dans les deux cas, le but était de couvrir la partie classique de la théorie des revêtements et du groupe fondamental avant d'en aborder la partie arithmétique. Les méthodes employées sont topologiques et analytiques, avec en perspective la théorie de Galois. Nous avons essayé de donner une vue globale de ce premier volet en donnant des énoncés précis et en dégageant les idées directrices. Le lecteur trouvera plus de détails dans l'annexe [De2] de ce volume qui contient quatre chapitres extraits d'un cours de DEA donné à Lille sur le sujet en 1994/95.

***Classification mathématique par sujets* (2000).** — 14H30, 30F10, 55-99, 12F12, 14H05.
Mots clefs. — Revêtements, groupes fondamentaux, monodromie, revêtements galoisiens, surfaces de Riemann, fonctions méromorphes, fonctions algébriques, corps de fonctions, théorème d'existence de Riemann.

1. Résultats principaux

Le théorème d'existence de Riemann (TER) est un résultat central de la théorie des revêtements. On l'invoque généralement pour justifier l'équivalence des aspects algébrique, analytique et topologique de la notion de revêtement d'une surface de Riemann compacte. Nous en donnerons plusieurs formes et essaierons d'en distinguer les diverses composantes. Outre Riemann, il convient de citer Hurwitz à qui revient une part importante des résultats présentés ici.

Le lien avec la théorie de Galois est que le TER permet de résoudre le

Problème inverse de Galois sur $\mathbb{C}(T)$. — *Tout groupe fini G est le groupe de Galois d'une extension $E/\mathbb{C}(T)$ (où $\mathbb{C}(T)$ est le corps des fractions rationnelles en l'indéterminée T et E est un corps).*

Ce résultat constitue le point de départ de l'approche moderne du problème inverse de Galois classique sur $\mathbb{Q}$: il s'agit de « descendre » de $\mathbb{C}(T)$ à $\mathbb{Q}(T)$; le théorème d'irréductibilité de Hilbert permettrait alors d'obtenir le résultat sur $\mathbb{Q}$ lui-même (*Cf.* [De1]).

Le TER est plus précisément un résultat de classification. En termes d'extensions de corps et de réalisation de groupes, on peut en donner la première forme suivante.

***Théorème d'existence de Riemann* (forme pratique)**. — *Supposons donnés*

– *un groupe fini G*
– *un entier $r > 0$*
– *r classes de conjugaison $C_1, \ldots, C_r$ de G.*

Pour tous $t_1, \ldots, t_r \in \mathbb{P}^1(\mathbb{C})$, r points distincts, il existe une correspondance bijective entre

l'ensemble des extensions de corps $E/\mathbb{C}(T)$		*l'ensemble des r-uplets $(g_1, \ldots, g_r) \in G^r$ tels que*
– *galoisiennes de groupe G*		– $\langle g_1, \ldots, g_r \rangle = G$
– *ramifiées en $t_1, \ldots, t_r$*	*et*	– $g_1 \cdots g_r = 1$
– *de générateurs distingués de l'inertie en t_i dans C_i, $i = 1, \ldots, r$*		– $g_i \in C_i$, $i = 1, \ldots, r$
modulo les $\mathbb{C}(T)$-isomorphismes		*modulo la conjugaison (composante par composante) par des éléments de G.*

La notion de « générateurs distingués de l'inertie » est expliquée plus bas. Si on préfère, on peut laisser de côté les points où ces générateurs et les classes $C_1, \ldots, C_r$ interviennent ; l'énoncé obtenu est juste un peu moins précis.

Le problème inverse sur $\mathbb{C}(T)$ découle de cette première forme du TER : tout groupe fini G possède un r-uplet $(g_1, \ldots, g_r)$ comme ci-dessus, pourvu que r soit assez grand (supérieur strictement au rang $\mathrm{rg}(G)$, *i.e.*, au nombre minimal de générateurs de G).

Cette première forme du TER ne s'exprime pas en termes de revêtements. Nous allons expliquer dans la suite comment ils apparaissent, et démontrer le résultat dans ce contexte. Nous travaillerons plus généralement avec des revêtements non nécessairement galoisiens, même si nous garderons le cas galoisien présent à l'esprit, en vue de l'application à la théorie de Galois.

2. Revêtements algébriques et extensions de corps de fonctions

Cette section est pure géométrie algébrique mais n'en utilise que des notions standard ; le chapitre 1 du livre de Hartshorne [Ha] par exemple est suffisant.

Étant donnés

– K un corps de base algébriquement clos (*e.g.* $K = \mathbb{C}$),

– B une K-variété projective régulière géométriquement irréductible (*e.g.* $B = \mathbb{P}^1$), on appelle *revêtement algébrique de B sur K* un morphisme algébrique $\mathrm{f} : X \to B$, fini, génériquement non-ramifié et défini sur K avec X une variété normale et géométriquement irréductible. Dans le cas $B = \mathbb{P}^1$, la donnée d'un revêtement équivaut à celle d'une fonction rationnelle non-constante $\mathrm{f} : X \cdots\to \mathbb{P}^1$ avec X une courbe projective lisse.

Au revêtement $\mathrm{f} : X \to B$ est associée l'*extension de corps de fonctions* $K(X)/K(B)$. C'est une extension finie séparable avec $K(X)/K$ régulière (*i.e.* $K(X) \cap \overline{K} = K$).

Il est classique que le foncteur « corps des fonctions » fournit une *équivalence de catégories* entre la catégorie des K-revêtements algébriques de B et celle des extensions finies séparables et régulières (sur K) de $K(B)$. Le foncteur inverse est donné par le procédé de *normalisation* : étant donné $E/K(B)$ comme ci-dessus, on considère, pour tout ouvert affine $U = \mathrm{Spec}(R)$ de B, la clôture intégrale $\widetilde{R}$ de R in E ; les morphismes associés $\mathrm{Spec}(\widetilde{R}) \to \mathrm{Spec}(R)$ se recollent pour fournir le revêtement f cherché.

Une autre description de la normalisation peut être donnée dans le cas de revêtements de $\mathbb{P}^1$ sur $\mathbb{C}$. Si $E/\mathbb{C}(T)$ est une extension finie, le revêtement f lui correspondant est le suivant : $\mathbb{P}^1_{\mathbb{C}}$ [resp. X] est l'ensemble des *places* (triviales sur $\mathbb{C}$) de $\mathbb{C}(T)$ [resp. de E] et f est l'application de restriction [Ha ; Ch. I p.45].

Dans cette équivalence de catégories, nous avons les *correspondances* suivantes :

• deg (f)	$=$	$[K(X) : K(B)]$
• Aut (f)	$\underset{\text{anti}}{\simeq}$	$\mathrm{Aut}\,(K(X)/K(B))$
• f revêtement galoisien	ssi	$K(X)/K(B)$ extension galoisienne
i.e. $\lvert\mathrm{Aut}\,(\mathrm{f})\rvert = \deg(\mathrm{f})$		*i.e.* $\lvert\mathrm{Aut}\,(K(X)/K(B))\rvert = [K(X) : K(B)]$

Rappelons aussi les *invariants* classiques d'un revêtement $\mathrm{f} : X \to \mathbb{P}^1$ sur $\mathbb{C}$:

– le groupe : $G = \mathrm{Gal}(\widehat{\mathbb{C}(X)}/\mathbb{C}(T))$ plongé dans S_d ($d = \deg(\mathrm{f})$) *via* son action sur les d conjugués d'un élément primitif de $\mathbb{C}(X)/\mathbb{C}(T)$,

– les points de branchement : $t_1, \ldots, t_r \in \mathbb{P}^1(\mathbb{C})$, *i.e.*, les points t tels que la clôture galoisienne $\widehat{\mathbb{C}(X)}$ n'est pas totalement décomposée sur $\mathbb{C}((T-t))$,

– l'invariant canonique de l'inertie : $\mathbf{C}^{\mathrm{alg}} = (C_1^{\mathrm{alg}}, \ldots, C_r^{\mathrm{alg}})$ défini comme suit. Soit $\widehat{\mathbb{C}(X)}/\mathbb{C}(T)$ la clôture galoisienne de l'extension $\mathbb{C}(X)/\mathbb{C}(T)$; son groupe de Galois est le groupe G. Pour $i = 1, \ldots, r$, l'extension d'algèbres

$$\widehat{\mathbb{C}(X)} \otimes_{\mathbb{C}(T)} \mathbb{C}((T-t_i))/\mathbb{C}((T-t_i))$$

s'écrit comme produit d'extensions *locales* de corps $E_{ij}/\mathbb{C}((T-t_i))$. D'après le théorème de Puiseux, ces extensions, qui sont galoisiennes, sont nécessairement de la forme $E_{ij} \simeq \mathbb{C}((\,(T-t_i)^{1/e_i}))$ pour un certain entier e_i (l'indice de ramification). Les groupes de Galois de ces extensions locales sont les *groupes d'inertie* ; ils sont conjugués dans G et cycliques. La classe C_i^{alg} est la classe de conjugaison dans G des *générateurs distingués* des groupes d'inertie I en t_i, *i.e.*, ceux qui correspondent à $e^{2i\pi/e_i}$ dans les isomorphismes

$$\begin{cases} I \longrightarrow \mu_{e_i} = \{\text{racines } e_i\text{-èmes de } 1\} \\ \sigma \longmapsto \qquad \dfrac{\sigma(\,(T-t_i)^{1/e_i})}{(T-t_i)^{1/e_i}} \end{cases}$$

3. Revêtements topologiques

Cette section est pure topologie. Nous rappelons deux points fondamentaux de la théorie du groupe fondamental : la structure du groupe fondamental de la sphère de Riemann privée d'un certain nombre de points et la correspondance entre revêtements topologiques et représentation du groupe fondamental. Nous nous limitons aux énoncés. Le lecteur pourra se reporter à l'annexe [De2] pour plus de détails, précisément au chapitre 1 pour le premier point et au chapitre 2 pour le second.

Groupe fondamental de $\mathbb{P}^1(\mathbb{C})$ privé de r points $t_1, \ldots, t_r$. — On a

$$\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}, t_o) \simeq \begin{array}{l} \text{groupe libre à } r \text{ générateurs} \\ \gamma_1, \ldots, \gamma_r \text{ modulo la} \\ \text{relation } \gamma_1 \cdots \gamma_r = 1 \end{array}$$

On peut préciser comment réaliser cet isomorphisme : on peut prendre pour $\gamma_1, \ldots, \gamma_r$ des lacets « tournant une fois dans le sens direct » autour de $t_1, \ldots, t_r$ respectivement et ne se croisant pas mutuellement.

Revêtements et groupe fondamental

Théorème. — *Soit $\mathcal{B}$ un espace topologique connexe par arcs, localement connexe par arcs et localement simplement connexe (e.g. $\mathcal{B} = \mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$). Soit $t_o \in \mathcal{B}$. Il existe une correspondance bijective entre*

l'ensemble des revêtements connexes de degré d $f : \mathcal{X} \to \mathcal{B}$ *modulo l'équivalence des revêtements*	*et*	*l'ensemble des représentations transitives* $\phi : \pi_1(\mathcal{B}, t_o) \to S_d$ *modulo l'équivalence des représentations.*

On rappelle que deux revêtements $f : \mathcal{X} \to \mathcal{B}$ et $g : \mathcal{Y} \to \mathcal{B}$ sont dits équivalents s'il existe un homéomorphisme $\chi : \mathcal{X} \to \mathcal{Y}$ tel que $g \circ \chi = f$, et que deux représentations $\phi, \psi : \pi_1(\mathcal{B}, t_o) \to S_d$ sont dites équivalentes s'il existe $\omega \in S_d$ tel que $\phi = \omega\psi\omega^{-1}$.

En combinant ce résultat au précédent, on obtient, dans le cas des revêtements de $\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$, une correspondance bijective entre

l'ensemble des revêtements connexes de degré d de $\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$ modulo l'équivalence des revêtements	et	l'ensemble des r-uplets transitifs $(g_1, \ldots, g_r) \in (S_d)^r$ tels que $g_1 \cdots g_r = 1$ modulo conjugaison (composante par composante) par des éléments de S_d.

La correspondance $f \to \phi$ est fournie par la *monodromie* : étant donnée une classe de lacets $[\gamma] \in \pi_1(\mathcal{B}, t_o)$ et un point $x \in f^{-1}(t_o)$, il existe un unique relèvement de γ à un chemin sur $\mathcal{X}$ commençant en x. Ce chemin se termine en un point $y \in f^{-1}(t_o)$. On a construit de cette façon une permutation de la fibre $f^{-1}(t_o)$, qui, après numérotation de cette fibre, donne l'élément $\phi([\gamma]) \in S_d$. Le *groupe de monodromie* est le sous-groupe de S_d de toutes les permutations obtenues de cette façon, *i.e.*, le groupe $\phi(\pi_1(\mathcal{B}, t_o))$.

Correspondances :

•	$\deg(f) \overset{\text{déf}}{=} \operatorname{card}\big(f^{-1}(t_o)\big)$	$=$	d
•	groupe de monodromie $\mathrm{G}(f)$	$\simeq$	$G \overset{\text{déf}}{=} \phi(\pi_1(\mathcal{B}, t_o))$
•	gpe d'automorphismes $\mathrm{Aut}(f)$	$\simeq$	$\mathrm{Cen}_{S_d}(G)$
•	f revêtement galoisien		
	i.e. $\vert\mathrm{Aut}(f)\vert = d$	ssi	$\vert\mathrm{Cen}_{S_d}(G)\vert = d$
	ssi	l'action	de
	$\mathrm{Aut}(f)$ sur $f^{-1}(t_o)$		$\mathrm{Cen}_{S_d}(G)$ sur $\{1, \ldots, d\}$
	est transitive	(et libre)	et alors
	$\mathrm{Aut}(f)$	$\simeq$	$\mathrm{Cen}_{S_d}(G)$
	$\vert \wr$ anti		$\vert \wr$ anti
	$\mathrm{G}(f)$	$\simeq$	G $(= \mathrm{Nor}_G(G(1))/G(1)$)

(où $G(1) \subset G$ est le fixateur de 1 dans la représentation $G \hookrightarrow S_d$).

Cette section fournit en particulier le résultat suivant.

Corollaire. — *Pour tout groupe fini G, si r est un entier $> \mathrm{rg}(G)$ et $t_1, \ldots, t_r$ sont r points distincts dans $\mathbb{P}^1(\mathbb{C})$, alors G est groupe de monodromie et groupe d'automorphismes d'un revêtement topologique galoisien de $\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$.*