Le groupe de Galois absolu de $\mathbb{C}(t)$

Mémoire de M1 à l'Université Paris-Sud
Mémoire de fin de degré à l'Universidad de Zaragoza

Andrés Ibáñez Núñez

encadré par

Olivier Wittenberg
Université Paris-Sud

1 juillet 2019

Table des matières

Introduction **5**

Remerciements **6**

Conventions et langage **7**

1 Revêtements **9**

1.1 Définition et classification 9

1.2 Catégorie des actions d'un groupe 12

1.3 Revêtements galoisiens 14

2 Surfaces de Riemann **19**

2.1 Propriétés élémentaires des surfaces de Riemann 19

2.2 Surfaces de Riemann et revêtements 21

2.3 Surfaces de Riemann et corps 29

2.4 Résumé des équivalences 37

2.5 Application au problème de Galois inverse sur $\mathbb{C}(t)$ 38

3 Extensions infinies de corps **41**

4 Le groupe de Galois absolu de $\mathbb{C}(t)$ **47**

4.1 Extension maximale non ramifiée au-dessus de $X \setminus S$ 47

4.2 Un système cohérent de points de base 49

4.3 Le groupe de Galois absolu de $\mathcal{M}(X)$ 50

4.4 Le groupe de Galois absolu de $\mathbb{C}(t)$ 55

Références **57**

Introduction

La théorie de Galois des corps a des relations étroites avec celle des revêtements topologiques. Les actions d'un groupe et les revêtements ramifiés des surfaces de Riemann ont aussi des caractéristiques similaires. Ces connexions s'expriment de façon très précise comme des équivalences de catégories.

Dans ce travail, on présente et démontre ces équivalences. Elles fournissent un dictionnaire qui permet de regarder le même problème avec des points de vue très différents. Ce changement de cadre peut être une méthode puissante. On s'en sert pour montrer que tout groupe fini se réalise comme le groupe de Galois d'une extension galoisienne du corps $\mathbb{C}(t)$ des fractions rationnelles complexes. Finalement, on calcule son groupe de Galois absolu, toujours à l'aide des équivalences de catégories entre extensions des corps de fonctions méromorphes, revêtements ramifiés des surfaces de Riemann, revêtements topologiques et actions des groupes.

Remerciements

Je tiens d'abord à remercier sincèrement mon encadrant du mémoire, Olivier Wittenberg. J'ai appris énormément de ses conseils et suggestions, et ça a été un grand honneur de pouvoir travailler avec lui.

Je dois aussi remercier chaleureusement Thea pour les conversations si riches sur ce sujet, et pour ses idées, parfois cruciales. Je remercie Gerard pour les intenses discussions sur la somme amalgamée des surfaces de Riemann et sa propositions de contre-exemple. Je remercie Camille pour son aide inestimable avec la langue française.

Ce travail représente le dernier pas d'un séjour mathématique de quatre années. Merci aux professeurs de l'Université de Zaragoza, spécialement à Enrique Artal, pour ses conseils et aide constante ; à Vicente Varea et Pilar Gallego, qui nous ont laissé récemment, mais qui resteront toujours dans notre mémoire ; et à Alberto Elduque, grâce à qui j'ai rencontré les mathématiques. Je remercie tous mes amis de l'université avec qui j'ai partagé ces années : Javier, Juan, Mario, María et bien d'autres. Je remercie Eduardo, pour douze années d'amitié et de mathématiques.

Conventions et langage

Dans une catégorie $\mathcal{C}$, on convient qu'un morphisme f détermine sa source et son but, et on les désigne par dom f et codom f respectivement. On note Aut f le groupe d'automorphismes de f, ou $\mathrm{Aut}_{\mathcal{C}}\, f$ si on veut spécifier la catégorie.

On appelle *fonction continue* un morphisme dans la catégorie **Top** des espaces topologiques, et on comprend que dans un énoncé comme *soit* $p : A \to B$ *une fonction continue*, les symboles A et B désignent des espaces topologiques.

On note $\#S$ le cardinal d'un ensemble S, qui est un nombre naturel si S est fini.

On note $\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}$ et $\mathbb{D}^{\times} = \mathbb{D} \setminus \{0\}$. On notera souvent abusivement z la fonction identité dans $\mathbb{C}$ ou une restriction.

Au sens strict, une extension de corps est un morphisme $\tau\colon K \to L$. Cependant, on se permettra parfois de sous-entendre le morphisme τ et d'écrire seulement $L|K$ ou la phrase L *est une extension de* K.

On ne considérera que des actions de groupes à gauche.

Pour G un groupe et H un sous-groupe, G/H désigne l'ensemble de classes à gauche.

1 Revêtements

1.1 Définition et classification

Dans cette première section, on présente sans preuve des résultats connus de la théorie des revêtements topologiques. On renvoie aux notes en ligne de Geoffroy Horel (`geoffroy.horel.org`) pour les preuves. En particulier, le théorème 14 ci-dessous correspond au théorème 3.41 dans ces notes.

Définition 1 (Revêtement trivial)**.** *Un* ***revêtement trivial*** *est une application continue $p : E \to B$ telle qu'il existe un espace topologique discret S et un homéomorphisme $i : B \times S \to E$ tels que $p \circ i$ est la projection sur la première coordonnée.*

Définition 2 (Revêtement)**.** *Soit B un espace topologique.*

Un ***revêtement*** *de B est une application continue $p : E \to B$ telle que tout point de B admet un voisinage ouvert U dans B tel que la restriction $p \mid p^{-1}(U) \to U$ est un revêtement trivial de U.*

L'espace B est appelé ***base*** *du revêtement.*

On dit que le revêtement p est ***connexe*** *si E est connexe et non vide.*

On dit que p est ***fini*** *si pour tout $b \in B$, la* ***fibre*** *$p^{-1}(b)$ est finie.*

Proposition 3 (Critère pour être un revêtement)**.** *Une application continue $p : E \to B$ est un revêtement si et seulement si pour tout point $b \in B$ il existe un voisinage ouvert U de b et une famille $(U_s)_{s\in S}$ d'ouverts disjoints de E tels que $p^{-1}(U) = \bigcup_{s\in S} U_s$ et pour tout $s \in S$ la restriction $p \mid U_s \to U$ est un homéomorphisme.*

On appelle une telle famille $(U_s)_{s\in S}$ une ***décomposition de U en feuillets****.*

Proposition 4. *Tout revêtement $p : E \to B$ est un homéomorphisme local, c'est-à-dire que tout point de E admet un voisinage ouvert U tel que $p(U)$ est ouvert dans B et la restriction $p \mid U \to p(U)$ est un homéomorphisme. En particulier, tout revêtement est une application ouverte.*

On utilisera souvent implicitement le fait suivant :

Proposition 5 (Surjectivité des revêtements)**.** *Soit $p\colon E \to B$ un revêtement. Si B est connexe et E est non vide, alors p est surjective.*

Pour les revêtements finis, on introduit la notion de degré.

Proposition et définition 6 (Degré d'un revêtement fini)**.** *Soit $p\colon E \to B$ un revêtement avec B connexe et non vide. Le cardinal de la fibre $p^{-1}(b)$ ne dépend pas du point $b \in B$ choisi.*

Si p est fini, on appelle ***degré*** *du revêtement p le cardinal des fibres de p. C'est un nombre naturel.*

Définition 7 (Morphisme de revêtement)**.** *Soient $p : E \to B$ et $q : F \to B$ deux revêtements de B. Un* ***morphisme de revêtement*** *entre p et q est une application continue $f : E \to F$ telle que $q \circ f = p$.*

On vérifie sans peine que l'on a une catégorie $\mathbf{Rev}B$ *où les objets sont les revêtements de B et les morphismes sont les morphismes de revêtement.*

Définition 8 (Relèvement)**.** *Soit $p : E \to B$ un revêtement, et $f : A \to B$ une application continue. Un* ***relèvement*** *de f par rapport à p est une application continue $h : A \to E$ telle que $p \circ h = f$.*

Lemme 9 (Unicité des relèvements)**.** *Soit $p : E \to B$ un revêtement, et $f : A \to B$ une application continue. Si A est connexe, deux relèvements de f qui coïncident en un point sont égaux.*

Pour comprendre ce que sont les revêtements et finalement parvenir à les classifier, il est nécessaire de pouvoir relever des chemins et des homotopies entre chemins.

Théorème 10 (Relèvement des chemins et des homotopies)**.** *Soit $p : E \to B$ un revêtement et $f : [0,1] \times [0,1] \to B$ (resp. $f : [0,1] \to B$) continue. Pour tout $x \in E_{f(0,0)}$ (resp. $x \in E_{f(0)}$) il existe un unique relèvement h de f par rapport à p tel que $h(0,0) = x$ (resp. $h(0) = x$).*

Comme conséquence on peut définir, pour tout point b de B, une action du groupe fondamental $\pi_1(B, b)$ de la base d'un revêtement $p : E \to B$ sur la fibre E_b. Cette action, qu'on appelle action de monodromie, joue un rôle crucial dans la classification des revêtements. On fixe d'abord une notation. Pour tout lacet γ dans B centré en b et tout $x \in E_b$ on note γ_x le seul chemin dans E tel que $\gamma_x(0) = x$ et $p \circ \gamma_x = \gamma$, ce qui a un sens d'après le théorème précédent. Comme on peut relever des homotopies, $\gamma_x(1)$ ne dépend que de la classe d'homotopie de γ. On a :

Proposition et définition 11 (Action de monodromie)**.** *Soit $p : E \to B$ un revêtement et $b \in B$.*

Il existe une action de $\pi_1(B, b)$ sur E_b caractérisée par la formule $[\gamma] \cdot x = \gamma_x(1)$, où γ est un lacet quelconque dans B basé en b, et $[\gamma]$ est sa classe dans $\pi_1(B, b)$. On l'appelle ***action de monodromie*** *de p basé en b.*

Pour que la formule ci-dessus définisse bien une action à gauche, on convient, pour deux chemins α et β avec $\alpha(1) = \beta(0)$, de désigner $\beta \cdot \alpha$ le chemin produit, qui parcourt d'abord α, puis β.

La proposition suivante identifie le stabilisateur de cette action.

Proposition 12. *Soit $p : E \to B$ un revêtement, $x \in E$ et $b = p(x)$. L'application $p_* : \pi_1(E, x) \to \pi_1(B, b) : [\gamma] \mapsto [p \circ \gamma]$ est injective et a pour image le stabilisateur de x pour l'action de monodromie.*

On peut aller plus loin et définir un foncteur de la catégorie des revêtements d'un espace topologique B vers la catégorie des ensembles munis d'une action de $G = \pi_1(B, b)$. Cette dernière, notée G-**Ens**, est définie comme la catégorie des foncteurs $\mathbf{Fonc}(G, \mathbf{Ens})$, où G est vu comme une catégorie à un seul objet. Un objet de G-**Ens** s'appelle G-ensemble.

Proposition et définition 13. *Soient B un espace topologique et $b \in B$ un point. Il existe un foncteur*

$$M_b : \mathbf{Rev}B \to G\text{-}\mathbf{Ens}$$

*qui, à chaque revêtement $p : E \to B$ de B, associe la fibre E_b munie de l'action de monodromie de p basé en b et qui, à chaque morphisme $f : E \to E'$ entre p et $p' : E' \to B$, associe la transformation $f \mid E_b \to E'_b$ entre les actions de monodromie correspondantes. On l'appelle **foncteur fibre** de B basé en b, et on le désigne par $M_{B,b}$ quand on veut préciser l'espace de base.*

On introduit des notations pour les catégories auxquelles on s'intéresse. On note $\mathbf{Revc}B$ la catégorie des revêtements connexes de B (en particulier de source non vide, par définition), qui est une sous-catégorie pleine de $\mathbf{Rev}B$. De même, on note G-**Enst** la catégorie des actions transitives de G, dont les objets s'appellent G-ensembles transitifs. Par convention, l'action vide n'est pas transitive. On note $\mathbf{Revfc}B$ la catégorie des revêtements finis connexes de B. Finalement, on note G-**Ensft** la catégorie des G-ensembles transitifs finis. On définit le **degré** d'un élément de G-**Ensft** comme le cardinal de l'ensemble sous-jacent, qui est un entier positif.

Pour des espaces B non pathologiques, l'action de monodromie caractérise le revêtement à isomorphisme près et réciproquement, toute action du $\pi_1(B, b)$ est isomorphe à l'action de monodromie d'un revêtement. On rappelle qu'un espace topologique non vide X est simplement connexe s'il est connexe par arcs et si pour un point $x \in X$, le groupe fondamental $\pi_1(X, x)$ est trivial. L'espace X est dit localement simplement connexe si sa topologie admet une base d'ouverts simplement connexes.

Maintenant on peut exprimer précisément le théorème de classification :

Théorème 14 (Classification des revêtements)**.** *Soit B un espace topologique connexe et localement simplement connexe. Soit $b \in B$ et $G = \pi_1(B, b)$. Alors le foncteur fibre en b*

$$M_b : \mathbf{Rev}B \to G\text{-}\mathbf{Ens}$$

est une équivalence de catégories.

Un revêtement p de B est connexe si et seulement si l'action $M_b(p)$ est transitive. La restriction du foncteur fibre

$$M_b \mid \mathbf{Revc}B \to G\text{-}\mathbf{Enst}$$

est encore une équivalence de catégories.

Un revêtement p de B est fini si et seulement si le G-ensemble $M_b(p)$ est fini, et la restriction

$$M_b \mid \mathbf{Revfc}B \to G\text{-}\mathbf{Ensft}$$

est une équivalence de catégories qui préserve le degré. On notera cette dernière restriction $\mathbf{\Omega}_{B,b} \colon \mathbf{Revfc}B \to G\text{-}\mathbf{Ensft}$

Il reste encore à comprendre la relation entre les foncteurs M_{b_1} et M_{b_2} pour deux points b_1 et b_2 de B. On l'esquissera rapidement ci-après. Remarquons qu'un morphisme de groupes induit un morphisme entre les catégories des actions dans l'autre sens :

Proposition et définition 15. *Soit $A \colon G_1 \to G_2$ un morphisme de groupes. Alors il existe un foncteur $A^* \colon G_2\text{-}\mathbf{Ens} \to G_1\text{-}\mathbf{Ens}$ qui, à un ensemble S muni d'une G_2-action, associe le même ensemble S muni de la G_1-action définie par la formule $g \cdot x = A(g) \cdot x$, pour $g \in G_1$ et $x \in S$; et qui, à un morphisme de G_2-ensembles $f \colon S \to S'$, associe le morphisme de G_1-ensembles induit par la même application ensembliste. Si A est un isomorphisme, alors A^* est un isomorphisme de catégories.*

D'abord, on note $G_i = \pi_1(B, b_i)$ pour $i = 1, 2$. Comme B est connexe par arcs (étant connexe et localement connexe par arcs), il existe un chemin α reliant b_1 et b_2. Cela induit un isomorphisme $A \colon G_1 \to G_2 \colon \gamma \mapsto \alpha \cdot \gamma \cdot \alpha^{-1}$. On a alors un isomorphisme de catégories $A^* \colon G_2\text{-}\mathbf{Ens} \to G_1\text{-}\mathbf{Ens}$. Alors les foncteurs M_{b_1} et $A^* \circ M_{b_2}$ sont naturellement isomorphes. En effet, pour p un revêtement de B, la bijection $p^{-1}(b_1) \to p^{-1}(b_2) \colon x \mapsto \alpha_x(1)$ convient, où α_x est le seul relèvement de α par rapport à p tel que $\alpha(0) = x$. Les conséquences plus importantes de cet isomorphisme sont :

Proposition 16. *Soit B un espace topologique connexe et localement simplement connexe, et soit b un point de B. Soit un revêtement p de B. Le fait que le stabilisateur de l'action de monodromie $M_b(p)$ soit distingué ou trivial ne dépend pas du point de base b choisi.*

1.2 Catégorie des actions d'un groupe

D'après les résultats précédents, pour étudier les revêtements d'un espace on se ramène à étudier des actions de son groupe fondamental. Il sera utile d'évoquer quelques propriétés de la catégorie des G-ensembles, où G est un groupe quelconque.

Proposition 17. *Soit U un objet de G-$\mathbf{Enst}$ et $a \in U$. Soit H le stabilisateur de a. Alors l'application $G/H \to U \colon gH \mapsto g \cdot a$ est bien définie et est un isomorphisme entre G/H (l'ensemble des classes à gauche) muni de l'action par translation à gauche et U.*

Démonstration. Immédiat. □

Proposition 18. *Soit U un objet de G-**Enst** et $a \in U$. Soit H le stabilisateur de a et soit J le normalisateur de H dans G. Le groupe d'automorphismes de U est isomorphe à J/H.*

On rappelle que le normalisateur J est le sous-groupe des $g \in G$ tels que $gHg^{-1} = H$. C'est le plus grand sous-groupe de G contenant H dans lequel H est distingué.

Démonstration. Par la proposition précédente, il suffit de montrer le résultat dans le cas où U est G/H muni de l'action par translation à gauche. Soit A le groupe d'automorphismes de G/H comme G-ensemble. On a un morphisme

$$\alpha\colon J/H \to A\colon gH \mapsto (uH \mapsto ug^{-1}H)$$

Montrons que $\alpha(gH)$ est bien un morphisme d'actions. Il faut juste vérifier que $ug^{-1}H$ ne dépend pas du représentant u choisi. Or $ug^{-1}H = u'g^{-1}H$ si et seulement si $u^{-1}u' \in g^{-1}Hg$, ce qui est vrai parce que $g \in J$. Alors il est clair que $\alpha(gH)$ ne dépend pas du choix de g et que α est bien un homomorphisme de groupes. Il est clairement injectif. Pour la surjectivité, soit $f \in A$. Alors $f(H) = g^{-1}H$ pour un $g \in G$. Pour tout $h \in H$, on a $g^{-1}H = f(H) = f(hH) = hf(H) = hg^{-1}H$, donc $h \in g^{-1}Hg$ et $H \subset g^{-1}Hg$. Comme f est un automorphisme, son inverse vérifie $f^{-1}(H) = gH$ et on a $H \subset gHg^{-1}$, d'où $H = gHg^{-1}$ et $g \in J$. On a alors $f = \alpha(gH)$. □

Pour la catégorie des G-ensembles transitifs on introduit la notion d'objet galoisien. Plus tard on verra que cela correspond en quelque sorte à la notion d'extension galoisienne de corps.

Définition 19. *On dit qu'un G-ensemble transitif $U \in G$-**Enst** est **galoisien** si le stabilisateur d'un de ses points (et alors de tous) est distingué dans G.*

Proposition 20. *Si U est un G-ensemble transitif galoisien de stabilisateur N (cela ne dépend pas du point choisi), alors son groupe d'automorphismes est isomorphe à G/N.*

Pour des G-ensembles finis, on peut mettre en relation le fait d'être galoisien et le degré.

Proposition 21. *Soit U un G-ensemble transitif fini de degré d. Alors le cardinal du groupe d'automorphismes $\#(\mathrm{Aut}\, U) \leq d$ et on a égalité si et seulement si U est galoisien.*

Démonstration. Soit H le stabilisateur d'un des points de U et soit J le normalisateur de H dans G. Par la proposition 17, $d = (G : H)$, et par la proposition 18, $\#(\mathrm{Aut}\, U) = (J : H)$. Le résultat découle du fait que $(G : H) = (G : J)(J : H)$ et de la finitude des indices . □

1.3 Revêtements galoisiens

Dans cette section, B est un espace topologique connexe localement simplement connexe. On fixe un point $b \in B$ et le foncteur fibre associé, que l'on note simplement M. Le terme *action de monodromie de* p fait référence à $M(p)$. Par la proposition 16, les définitions qui suivent ne dépendent pas du point de base b choisi.

Définition 22 (Revêtement universel)**.** *On appelle **revêtement universel** de B un revêtement connexe de B dont le stabilisateur de son action de monodromie est trivial.*

Par le théorème 14 de classification, deux actions de ce type sont isomorphes, donc deux revêtements universels sont isomorphes.

Proposition 23. *Un revêtement connexe $p : E \to B$ est universel si et seulement si E est simplement connexe.*

Démonstration. L'espace B étant localement connexe par arcs et p un homéomorphisme local, E est localement connexe par arcs. Comme E est connexe, il est aussi connexe par arcs. Rappelons que par définition, E est non vide. Par la proposition 12 le stabilisateur de l'action de monodromie associée à p est isomorphe à $\pi_1(E, x)$, pour $x \in E_b$, donc il est trivial si et seulement si E est simplement connexe. □

Définition 24 (Revêtement galoisien)**.** *Un revêtement connexe $p : E \to B$ est dit **galoisien** si le stabilisateur de son action de monodromie est distingué dans $\pi_1(B, b)$ (c'est-à-dire, si $M(p)$ est un $\pi_1(B, b)$-ensemble galoisien).*

Proposition 25. *Le groupe d'automorphismes $Aut(p)$ d'un revêtement galoisien $p : E \to B$ est isomorphe au quotient $\pi_1(B, b)/N$, où N est le stabilisateur de l'action de monodromie.*

Démonstration. On note $G = \pi_1(B, b)$. Par le théorème 14 de classification il suffit de montrer que le groupe d'automorphismes du G-ensemble E_b est isomorphe à G/N, et c'est ce que montre la proposition 18. □

Proposition 26. *Soit p un revêtement connexe fini de degré d. Alors le cardinal du groupe d'automorphismes $\#(Aut(p)) \leq d$ et on a égalité si et seulement si p est galoisien.*

Démonstration. Tout découle de la proposition 21 et du fait que l'équivalence de catégories du théorème 14 préserve le degré. □

Corollaire 27. *Pour tout sous-groupe distingué N de $\pi_1(B, b)$ il existe un revêtement galoisien $p : E \to B$ dont le groupe d'automorphismes $Aut(p)$ est isomorphe au quotient $\pi_1(B, b)/N$.*

Démonstration. On note $G = \pi_1(B, b)$. Par le théorème de classification, il existe un revêtement $p : E \to B$ tel que $M(p)$ est isomorphe à l'action de G sur G/N par translation à gauche. Le stabilisateur de cette action est N, qui est distingué dans G, donc p est galoisien. En outre, par la proposition précédente, le groupe d'automorphismes de p est isomorphe à G/N. $\square$

Le but de la fin de cette section est de montrer que tout groupe fini est isomorphe au groupe d'automorphismes d'un revêtement galoisien de $\mathbb{P}^1$ (voir la section 2.1 pour la définition) privé d'un nombre fini de points. On commence par calculer le groupe fondamental du plan privé d'un nombre fini de points.

Proposition 28. *Soit S un sous-ensemble fini non vide de $\mathbb{C}$, de cardinal n et $b \in \mathbb{C} \setminus S$ un point qui n'est pas colinéaire avec deux points distincts de S. Alors $\pi_1(\mathbb{C} \setminus S, b)$ est isomorphe au groupe libre F_n engendré par n éléments.*

En plus, soit $\varepsilon < \min\{|x - y| : x, y \in S \cup \{b\}, x \neq y\}$ et pour $a \in S$, soit $\gamma_{a,\varepsilon}$ le lacet basé en b qui va de b vers a en droite ligne, s'arrête à distance ε de a, décrit un cercle de rayon ε autour de a dans le sens trigonométrique et revient à b en parcourant en sens inverse sa trace. Alors les classes des γ_a sont des générateurs de $\pi_1(\mathbb{C} \setminus S, b)$.

Remarquons que alors $\pi_1(\mathbb{C} \setminus S, c)$ est isomorphe à F_n pour tout $c \in \mathbb{C} \setminus S$, puisque $\mathbb{C} \setminus S$ est connexe par arcs. L'avantage d'un point b avec la propriété ci-dessus est qu'on peut décrire facilement les générateurs de $\pi_1(\mathbb{C} \setminus S, b)$.

Démonstration. On rappelle d'abord le théorème de van Kampen :

Théorème 29 (van Kampen)**.** *Soit X un espace topologique connexe et localement simplement connexe. Soient U et V deux ouverts de X qui le recouvrent tels que U, V et $U \cap V$ sont connexes, et soit $x \in U \cap V$. Alors le diagramme*

$$\begin{tikzcd} \pi_1(U \cap V, x) \arrow[r] \arrow[d] & \pi_1(U, x) \arrow[d] \\ \pi_1(V, x) \arrow[r] & \pi_1(X, x) \end{tikzcd}$$

induit par les inclusions est un carré cocartésien dans la catégorie des groupes (c'est-à-dire que le groupe en bas à droite est la somme amalgamée du reste du diagramme).

On peut supposer $b = 0$.

Pour $u < v$ dans $\mathbb{R}$ et $\varepsilon > 0$, soit

$$W_{u,\varepsilon}^{v} = \{re^{i2\pi t} : (r, t) \in (\mathbb{R}_{\geq 0} \times]u, v[) \cup ([0, \varepsilon[\times \mathbb{R})\}$$

Les intersections finies d'ouverts de la forme $W_{u,\varepsilon}^{v}$ sont étoilées, donc en particulier simplement connexes.

On montre par récurrence le résultat plus fort :

$(*)$ *Soit $r > 0$ et soit W un ensemble de la forme $W^v_{u,r}$. Soit S un sous-ensemble fini non vide de $W \setminus \{0\}$ de cardinal n et soit $\varepsilon > 0$ tels que*

1. *0 n'est pas colinéaire avec deux points distincts de S,*
2. $\forall s \in S, |s| > r$,
3. $\varepsilon < \min\{|x - y| : x, y \in S, x \neq y\}$,
4. *Pour tout $a \in S$, la boule fermée $\overline{B}(a, \varepsilon) \subset W$.*

Dans ce cas on dira que le triplet (W, S, ε) est ***intéressant****.*

Alors $\pi_1(W \setminus S, 0)$ est isomorphe au groupe libre F_n engendré par n éléments.

En plus, pour $a \in S$, soit $\gamma_{a,\varepsilon}$ le lacet basé en 0 qui va de 0 vers a en droite ligne, s'arrête à distance ε de a, décrit un cercle de rayon ε autour de a dans le sens trigonométrique et revient à 0 en parcourant en sens inverse sa trace. Alors les classes des γ_a sont des générateurs de $\pi_1(W \setminus S, 0)$.

Pour $n = 1$, $S = \{a\}$, l'espace $W \setminus S$ est homotopiquement équivalent au cercle, dont le groupe fondamental est F_1. L'équivalence d'homotopie

$$W \setminus S \to \mathbb{S}^1 : z \mapsto -\frac{\overline{a}}{|a|} \frac{z - a}{|z - a|}$$

envoie γ_a sur la classe du chemin $t \mapsto e^{i2\pi t}$.

Maintenant soit $n \geq 2$. On peut trouver un élément $a \in S$, un ε' avec $0 < \varepsilon' < \varepsilon$ et deux ouverts U et V de la forme $W^v_{u,r}$ (avec le même r que W) tels que $U \cup V = W$, les triplets $(U, \{a\}, \varepsilon')$ et $(V, S \setminus \{a\}, \varepsilon')$ sont intéressants et $U \cap V \cap S = \varnothing$. Soient $U' = U \setminus \{a\}$, $V' = V \setminus (S \setminus \{a\})$ et $W' = W \setminus S$. On a un diagramme

$$\begin{tikzcd} \pi_1(U' \cap V', 0) \arrow[r] \arrow[d] & \pi_1(U', 0) \\ \pi_1(V', 0) & \end{tikzcd}$$

dont, par le théorème de van Kampen, la somme amalgamée est isomorphe à $\pi_1(W', 0)$. Remarquons que $U' \cap V' = V \cap U$ est simplement connexe. On connaît tous les groupes et morphismes du diagramme précédent, qui peut s'écrire

$$\begin{tikzcd} 1 \arrow[r] \arrow[d] & F_1 \\ F_{n-1} & \end{tikzcd}$$

Sa somme amalgamée est le produit libre de F_1 et F_{n-1}, qui est bien isomorphe à F_n. En plus, les images dans $\pi_1(W', 0)$ des générateurs de $\pi_1(U', 0)$, $\pi_1(V', 0)$ engendrent $\pi_1(W', 0)$. C'est-à-dire, les classes des chemins $\gamma_{c,\varepsilon'}$ pour

$c \in S$ sont des générateurs de $\pi_1(W', 0)$. Pour la condition 3 de $(*)$, les lacets $\gamma_{c,\varepsilon'}$ et $\gamma_{c,\varepsilon}$ sont homotopes dans $(W', 0)$, ce qui conclut. $\square$

Corollaire 30. *Tout groupe fini isomorphe au groupe d'automorphismes d'un revêtement galoisien de* $\mathbb{P}^1 \setminus S$*, pour* S *un certain ensemble fini de* $\mathbb{P}^1$.

Démonstration. Tout groupe fini est isomorphe à un quotient F_n/N, pour n un entier positif assez grand, où N est un sous-groupe distingué de F_n. On prend $S' \subset \mathbb{C}$ de cardinal n, $S = S' \cup \{\infty\}$ et $b \in \mathbb{P}^1 \setminus S$. Comme le groupe fondamental $\pi_1(\mathbb{P}^1 \setminus S, b)$ est bien isomorphe à F_n, on a le résultat par le corollaire 27. $\square$

2 Surfaces de Riemann

2.1 Propriétés élémentaires des surfaces de Riemann

Dans cette section, on donne les définitions et les résultats élémentaires à propos des surfaces de Riemann. L'analyse complexe d'une variable est supposée connue, et on renverra à [Rudin, 1987] quand on en aura besoin.

Définition 31. *Soit X un espace topologique. Un* ***atlas holomorphe*** *sur X est un ensemble $\mathcal{A}$ d'homéomorphismes tel que,*

(i) les sources des éléments de $\mathcal{A}$ sont des ouverts de X qui recouvrent X et les buts sont des ouverts de $\mathbb{C}$.

(ii) pour toute paire d'applications $\varphi_1 : U_1 \to U_1'$, $\varphi_2 : U_2 \to U_2'$ de $\mathcal{A}$, la fonction $\varphi_1\varphi_2^{-1} : \varphi_2(U_1 \cap U_2) \to \varphi_1(U_1 \cap U_2)$ est holomorphe.

L'ensemble des atlas holomorphes sur X est ordonné par inclusion. On vérifie sans peine que tout atlas holomorphe sur X est inclus dans un unique atlas maximal.

Définition 32. *Une* ***surface de Riemann*** *est un espace topologique X séparé et à base dénombrable d'ouverts muni d'un atlas holomorphe maximal. On appelle* ***carte*** *un élément de l'atlas de X.*

Une application $f : Y \to X$ entre surfaces de Riemann est dite ***holomorphe*** *si elle est continue et si pour toutes cartes φ de Y et ψ de X vérifiant $f(dom\ \varphi) \subset dom\ \psi$, l'application $\psi f \varphi^{-1}$ est holomorphe au sens usuel.*

Un ***biholomorphisme*** *est une application holomorphe et bijective entre deux surfaces de Riemann d'inverse holomorphe.*

On a donc une catégorie où les objets sont les surfaces de Riemann et les morphismes sont les applications holomorphes. On l'appelle la catégorie des surfaces de Riemann.

Le premier exemple de surface de Riemann est $\mathbb{C}$ lui-même, avec l'atlas maximal induit par la carte $id_{\mathbb{C}}$. D'autre part, une partie ouverte U d'une surface de Riemann X admet naturellement une structure de surface de Riemann : les cartes de U sont les cartes φ de X dont la source dom $\varphi \subset U$.

Les puissances $\mathbb{D} \to \mathbb{D}$: $z \mapsto z^n$, pour $n \in \mathbb{N}$, sont des fonctions holomorphes simples. C'est un fait fondamental que tout autre application holomorphe est localement comme celles-ci.

Proposition et définition 33 (Forme locale des applications holomorphes)**.** *Soit $f : Y \to X$ une application holomorphe entre surfaces de Riemann et $a \in Y$. Supposons que f n'est pas constante sur la composante connexe de Y contenant a. Alors il existe un unique $n \in \mathbb{N} \setminus \{0\}$ tel qu'il existe des cartes $\varphi : U \to \mathbb{D}$ de Y autour de a et $\psi : V \to \mathbb{D}$ de X autour de $f(a)$ satisfaisant* *(i)* $f(U) \subset V$

(ii) $\varphi(a) = 0$ *et* $\psi(f(a)) = 0$

(iii) $\forall z \in \mathbb{D}, \quad \psi f \varphi^{-1}(z) = z^n$

*L'entier n est appelé **indice de ramification** de f en a. Si n est différent de 1, on dit que a est un **point de ramification** et $f(a)$ est un **point de branchement** de f.*

Démonstration. C'est un résultat local et invariant par composition au but et à la source de f par biholomorphismes, donc on peut supposer que X et Y sont des ouverts de $\mathbb{C}$. Le résultat découle alors du théorème 10.32 de [Rudin, 1987]. □

Le théorème de forme locale a des nombreuses conséquences qui seront utiles.

Corollaire 34 (Application ouverte)**.** *Toute application holomorphe $f : Y \to X$ entre surfaces de Riemann qui n'est constante sur aucune composante connexe de Y est ouverte.*

Démonstration. Cela vient du fait que les puissances $z \mapsto z^n$, avec $n \in \mathbb{N} \setminus \{0\}$, sont des applications ouvertes, et du théorème de forme locale. □

Corollaire 35 (Application inverse)**.** *L'inverse d'une application holomorphe bijective est encore holomorphe.*

Démonstration. Si une application holomorphe $f \colon Y \to X$ est bijective, la seule possibilité est que l'indice de ramification de f en chaque point de Y soit 1. Par la forme locale, l'inverse de f est donc localement holomorphe, c'est-à-dire, holomorphe. □

Corollaire 36 (Principe d'identité)**.** *Soient $f, g : Y \to X$ deux applications holomorphes entre des surfaces de Riemann, avec Y connexe. Si f et g coïncident sur un ensemble $S \subset Y$ qui a un point d'accumulation dans Y, alors $f = g$.*

Démonstration. L'ensemble

$$A = \{z \in Y : f|_U = g|_U \text{ pour un voisinage } U \text{ de z}\}$$

est clairement ouvert. Soit $y \in Y$ un point d'accumulation de S dans Y. Par continuité, $f(y) = g(y) = x$. Soient U et V des voisinages ouverts de y et x dans Y et X, respectivement, tels que $f(U) \subset V$, $g(U) \subset V$ et tels qu'on ait une carte φ de X de source V. Soit $h = \varphi \circ f|_U - \varphi \circ g|_U \colon U \to \mathbb{C}$. Si h n'est pas constante au voisinage de y, quitte à échanger U avec un ouvert plus petit et composer h au but et à la source par des biholomorphismes, on peut supposer que $U = \mathbb{D}$, $y = 0$ et $h \colon z \mapsto z^n$. Or, d'après les hypothèses sur S, l'ensemble $h|_U^{-1}(0)$ est infini. Ceci preuve par contradiction que h est constante (égale à 0, puisque $h(y) = 0$) au voisinage de y. L'ensemble A est donc non vide, parce que $y \in A$. Comme A n'a pas de point isolé, si l'on reprend cet argument en remplaçant S par A, on montre que A est fermé. Par connexité de Y, $A = Y$, et donc $f = g$. □

Le critère suivant est parfois utile pour montrer que certaines applications se prolongent holomorphiquement.

Proposition 37 (Élimination de singularités)**.** *Soient U un ouvert d'une surface de Riemann X, $a \in U$, et $f : U \setminus \{a\} \to \mathbb{C}$ une fonction holomorphe bornée. Alors f admet un unique prolongement à une fonction holomorphe $U \to \mathbb{C}$.*

Démonstration. Il s'agit d'un résultat local, donc on peut supposer que $X = \mathbb{C}$. Le résultat est alors fourni par le théorème 10.20 de [Rudin, 1987]. □

On remarque que les ensembles $S \subset X$ qui n'ont pas de point d'accumulation dans X sont exactement les ensembles fermés et discrets (c'est-à-dire que la topologie induite sur S comme sous-espace de X est discrète) de X. On utilisera plus tard que

Lemme 38. *L'ensemble $S \subset Y$ des points de branchement d'une application holomorphe $f : Y \to X$ entre surfaces de Riemann est fermé et discret dans Y.*

Démonstration. C'est une conséquence directe du théorème 33 de forme locale. □

L'un des exemples plus importants des surfaces de Riemann est la sphère de Riemann. C'est l'espace topologique $\mathbb{P}^1$ défini comme la compactification d'Alexandroff $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$ de $\mathbb{C}$, munie de l'atlas holomorphe induit par les deux applications

$$\mathbb{C} \subset \mathbb{P}^1 \to \mathbb{C} \colon z \mapsto z$$

$$\mathbb{C}^\times \cup \{\infty\} \subset \mathbb{P}^1 \to \mathbb{C} \colon z \mapsto \begin{cases} 1/z & \text{si } z \neq \infty, \\ 0 & \text{si } z = \infty. \end{cases}$$

C'est bien sûr une surface de Riemann compacte. À l'aide de la projection stéréographique, on montre que la sphère de Riemann est homéomorphe à la sphère de dimension 2.

2.2 Surfaces de Riemann et revêtements

Définition 39. *Soit $\alpha : Y \to X$ une application holomorphe entre surfaces de Riemann telle que*

1. *X et Y sont connexes et non vides,*

2. α n'est pas constant,

3. α est propre (la pré-image de tout compact est compact).

On appelle une telle α un ***revêtement ramifié****.*

Proposition 40. *Soit $\alpha : Y \to X$ un revêtement ramifié. Alors α est surjective avec des fibres finies.*

Soit $S \subset Y$ un ensemble fermé discret contenant tous les points de ramification de α et soit $S' = \alpha(S) \subset X$. Alors S et S' sont des sous-ensembles fermés discrets de Y et X, et la restriction $\alpha \mid Y \setminus S \to X \setminus S'$ est un revêtement topologique fini connexe et non vide.

Démonstration. Par la forme locale (33), les fibres de α sont fermées et discrètes. Par propreté de α, elles sont finies. L'image de α est ouverte (voir 34), non vide et fermée (rappelons que les applications propres entre espaces localement compacts sont fermées), donc c'est la totalité de X, par connexité.

On sait déjà que S est fermé discret. Soit $x \in S'$, et soient $y_1, \ldots, y_n$ les différents points de la fibre de α au-dessus de x ($n \in \mathbb{N} \setminus \{0\}$). Prenons des voisinages disjoints $U_1, \ldots, U_n$ de $y_1, \ldots, y_n$ tels que chaque $U_i \setminus \{y_i\}$ ne contient pas des points de S. Alors x est le seule point S' dans $\cap_i \alpha(U_i)$, qui est un voisinage ouvert de x. Le point x est isolé dans S'. De plus, S' est fermé parce que S est fermé et l'application α est fermée.

La dernière partie découle du théorème de forme locale aussi, quitte à montrer que $Y \setminus S$ est connexe et non vide. Il est clairement non vide parce que Y n'est pas discret. Soit $f \colon Y \setminus S \to \mathbb{R}$ localement constant. Soit $s \in S$ et soit U un voisinage de s dans Y homéomorphe au disque tel que $U \cap S = \{s\}$. Alors $f|_{U \setminus \{s\}}$ est constante à valeur c_s, parce que $U \setminus \{s\}$ est connexe. En définissant $f(s) = c_s$ pour chaque $s \in S$, on obtient une fonction continue de Y vers $\mathbb{R}$ localement constant, donc constant, parce que Y est connexe. L'application f originale est donc constant aussi. Ceci montre que $Y \setminus S$ est connexe. □

Lemme 41. *Soient X une surface de Riemann et $\alpha : Y \to X$ un revêtement topologique tel que le cardinal des fibres est au plus dénombrable. Alors il existe une unique structure de surface de Riemann sur Y tel que α est holomorphe. En outre, si α a des fibres finies, alors elle est propre.*

Démonstration. On vérifie d'abord que Y est séparé et à base dénombrable d'ouverts. Soient $x, y \in Y$ deux points différents de Y. Si $\alpha(x) = \alpha(y)$, on prend un voisinage distingué (voir la Proposition 3) U de $\alpha(x)$ et un décomposition $\alpha^{-1}(U) = \cup_{i \in I} U_i$ en feuillets. Alors il existe $i, j \in I$, $i \neq j$ tels que $x \in U_i$ et $y \in U_j$. Les deux ouverts U_i et U_j fournissent une séparation de x et y par des ouverts disjoints de Y. Dans le cas où $\alpha(x) \neq \alpha(y)$, on prend des ouverts disjoints de X, O et W, tels que $\alpha(x) \in O$ et $\alpha(y) \in W$. Leurs pré-images, $\alpha^{-1}(O)$ et $\alpha^{-1}(W)$ conviennent comme séparation de x et y. Ceci montre que Y est séparé. Maintenant, soit $\mathcal{B}$ une base dénombrable de X par des ouverts connexes et distingués par rapport à α. Pour chaque $U \in \mathcal{B}$, $\alpha^{-1}(U)$ n'a qu'une quantité dénombrable de composantes connexes. L'ensemble des composantes connexes des $\alpha^{-1}(U)$, pour $U \in \mathcal{B}$, fournit une base dénombrable d'ouverts de Y.

Chaque point $y \in Y$ admet un voisinage V dans Y dont la restriction $\alpha \mid V \to \alpha(V)$ est un homéomorphisme (voir 4). Notons $U = \alpha(V)$. Quitte a prendre V plus petit, on peut supposer qu'il existe une carte $\varphi : U \to U'$ de X. On prend comme atlas de Y l'ensemble des $\varphi \circ \alpha_{|V}$ ainsi obtenues. Ces applications sont bien des homéomorphismes dont les sources recouvrent Y. Les transitions sont holomorphes parce qu'elles correspondent avec des transitions des cartes de X. L'application α est clairement holomorphe avec cette atlas. L'unicité de la structure de surface de Riemann vient du fait que si α holomorphe, alors les $\varphi \circ \alpha_{|V}$ sont des biholomorphismes (voir la proposition 35 de l'application inverse), donc des cartes de Y.

Supposons maintenant que α a des fibres finies. Soit $K \subset X$ compact. Recouvrons K par un nombre fini d'ouverts $V_1, \ldots, V_n$ dont l'adhérence de chaque V_i est compacte et contenue dans un ouverte distingué U_i. Alors $\alpha^{-1}(K) = \cup_{i=1}^n \alpha^{-1}(K \cap \overline{V_i})$, et chaque $\alpha^{-1}(K \cap \overline{V_i})$ est compact, en tant que union finie d'espaces homéomorphes à $K \cap \overline{V_i}$. On conclut que $\alpha^{-1}(K)$ est compact et donc que α est propre. $\square$

Lemme 42 (Somme amalgamée des surfaces de Riemann)**.** *On se donne un diagramme*

$$\begin{tikzcd} Y_0 \arrow[r, hook, "l_1"] \arrow[d, hook, "l_2"'] & Y_1 \\ Y_2 & \end{tikzcd}$$

d'applications holomorphes injectives entre surfaces de Riemann et on suppose vraie la propriété suivante :

$(*)$ *Pour tout compact K dans Y_1, la partie $l_2(l_1^{-1}(K))$ est fermée dans Y_2.*

Alors la colimite Y (ou somme amalgamé) de ce diagramme dans **Top** *admet une structure de surface de Riemann avec laquelle Y devient la colimite dans la catégorie des surfaces de Riemann. Plus concrètement, il existe une surface de Riemann Y et des applications holomorphes injectives $m_1 : Y_1 \to Y$, $m_2 : Y_2 \to Y$ telles que $m_1 \circ l_1 = m_2 \circ l_2$ et $m_1(Y_1) \cup m_2(Y_2) = Y$.*

Démonstration. On pose $Y = (Y_1 \sqcup Y_2)/\sim$, où $\sim$ est la relation d'équivalence dans l'union disjointe $Y_1 \sqcup Y_2$ engendré par les relations $l_1(x) \sim l_2(x)$, pour $x \in Y_0$. On munit $Y_1 \sqcup Y_2$ de la topologie union disjointe et Y de la topologie quotient. On pose, pour $i = 1, 2$, $m_i : Y_i \to Y$ la composition de l'inclusion $Y_i \to Y_1 \sqcup Y_2$ et la projection $Y_1 \sqcup Y_2 \to Y$. L'espace Y muni des applications m_1 et m_2 est bien la colimite du diagramme dans **Top**. Un ensemble $A \subset Y$ est ouvert dans Y si et seulement si $m_i^{-1}(A)$ est ouvert dans Y_i pour $i = 1, 2$.

Pour $\{i,j\} = \{1,2\}$, on a $m_j^{-1}m_i(U) = l_2 l_1^{-1}(U)$, et l_1 et l_2 sont ouvertes par le théorème 34 de l'application ouverte. Alors m_1 et m_2 le sont aussi. Ce sont aussi des homéomorphismes sur leurs images, par injectivité.

Vérifions tout d'abord que Y est bien séparé et à base dénombrable d'ouverts. La deuxième propriété découle du fait que Y s'écrit comme l'union $Y = m_1(Y_1) \cup m_2(Y_2)$ de deux ouverts qui sont des images homéomorphes des espaces à base dénombrable d'ouverts. Pour montrer que Y est bien séparé on va se servir de la propriété $(*)$. Soient x_1 et x_2 deux points différents de Y. Si les deux points sont dans un des $m_i(Y_i)$, on peut utiliser que Y_i est séparé pour trouver une séparation de x et y par des ouverts disjoints. On suppose donc que $x_i \in m_i(Y_i) \setminus m_j(Y_j)$ pour $\{i,j\} = \{1,2\}$. On prend $y_1 \in Y_1$ tel que $m_1(y_1) = x_1$ et un voisinage V de y_1 dans Y_1 à adhérence compacte dans Y_1. Les voisinages $m_1(V)$ et $m_2(Y_2 \setminus l_2(l_1^{-1}(\overline{V})))$ fournissent une séparation de x_1 et x_2 par des ouverts disjoints de Y.

On munit Y des cartes de la forme $\varphi \circ m_i^{-1}|_{m_i(U)}$, où $\varphi : U \to U'$ est une carte de Y_i, pour $i = 1, 2$. On vérifie sans peine que ceci donne à Y une structure de surface de Riemann telle que m_1 et m_2 sont holomorphes.

□

Le théorème n'est pas vrai sans l'hypothèse $(*)$. Comme contre-exemple, regardons le diagramme

$$\begin{tikzcd} \mathbb{D} \arrow[r, hook] \arrow[d, hook] & \mathbb{C} \\ \mathbb{C} & \end{tikzcd}$$

Par le principe d'identité 36, sa colimite dans la catégorie des surfaces de Riemann est $\mathbb{C}$. Pourtant, sa colimite dans **Top** n'est pas séparé. On peut aussi trouver un diagramme sans colimite dans la catégorie des surfaces de Riemann. On prend

$$\begin{tikzcd} \mathbb{D} \arrow[r, hook, "a"] \arrow[d, hook, "b"'] & \mathbb{C}/\mathbb{Z}^2 \\ \mathbb{P}^1 & \end{tikzcd} \tag{1}$$

Pour définir a et b, on prend $u \colon \mathbb{C} \to \mathbb{C}/\mathbb{Z}^2$ la projection, $v \colon \mathbb{C} \to \mathbb{P}^1$ l'inclusion (qui couvre tout $\mathbb{P}^1$ sauf le point ∞), et une injection $j \colon \mathbb{D} \to \mathbb{C}$ telle que $u \circ j \colon \mathbb{D} \to \mathbb{C}/\mathbb{Z}^2$ soit injective. On définit alors $a = u \circ j$ et $b = v \circ j$. On prétend que tout cocône du diagramme 1 est formé par des applications constantes. On se donne un carré commutatif

$$\begin{tikzcd} \mathbb{D} \arrow[r, hook, "a"] \arrow[d, hook, "b"'] & \mathbb{C}/\mathbb{Z}^2 \arrow[d, "f"] \\ \mathbb{P}^1 \arrow[r, "g"] & X \end{tikzcd}$$

Les applications $f \circ u$ et $g \circ v$ coïncident sur $j(\mathbb{D})$, donc elles sont égales, par le principe d'identité. On a,

$$\lim_{\substack{t \to +\infty \\ t \in \mathbb{R}}} g \circ v(t) = g(\infty)$$

Mais $f \circ u|_{\mathbb{R}}$ est périodique, parce qu'elle factorise par le tore. La limite en $+\infty$ existe si et seulement si $f \circ u|_{\mathbb{R}}$ est constante. Par le principe d'identité, $f \circ u = g \circ v$ est constante, donc $f = g$ et f et g sont constantes. Le diagramme 1 n'admet pas de colimite, parce que s'il en existait, il factoriserait par soi-même de deux façons : avec l'application identité et avec une application constante.

$$\begin{tikzcd}
\mathbb{C} \arrow[drr, bend left, "u"] \arrow[dr, bend right, "v"'] & & \\
& \mathbb{D} \arrow[ul, "j"'] \arrow[r, hook, "a"] \arrow[d, hook, "b"'] & \mathbb{C}/\mathbb{Z}^2 \arrow[d, "f"] \\
& \mathbb{P}^1 \arrow[r, "g"] & X
\end{tikzcd}$$

Lemme 43. *Soit $\alpha : E \to \mathbb{D}^\times$ un revêtement connexe avec des fibres finies de cardinal $k \in \mathbb{N} \setminus \{0\}$. Alors il existe un homéomorphisme $g : \mathbb{D}^\times \to E$ tel que $\alpha \circ g(z) = z^k$ pour tout $z \in \mathbb{D}^\times$.*

Démonstration. Le disque pointé $\mathbb{D}^\times$ est homotopiquement équivalent au cercle $\mathbb{S}^1$, dont le groupe fondamental est $\mathbb{Z}$. Un ensemble muni d'une action transitive de $\mathbb{Z}$ est caractérisé par son cardinal. On remarque que le disque pointé $\mathbb{D}^\times$ est connexe et localement simplement connexe. Alors, par le théorème 14 de classification des revêtements, un revêtement connexe non vide de $\mathbb{D}^\times$ est caractérisé par le cardinal de ses fibres. Or, pour $n \in \mathbb{N} \setminus \{0\}$, le revêtement connexe $\mathbb{D}^\times \to \mathbb{D}^\times : z \mapsto z^n$ a toutes ses fibres de cardinal n, donc il est isomorphe à tout autre revêtement connexe de $\mathbb{D}^\times$ avec fibres de cardinal n. $\square$

Proposition 44. *Soient X une surface de Riemann connexe, S un sous-ensemble fermé discret de X et notons $X' = X \setminus S$. Soit $\alpha' : Y' \to X'$ un revêtement topologique fini. Alors il existe une surface de Riemann Y, un revêtement ramifié $\alpha : Y \to X$ et un biholomorphisme $\beta \colon Y \setminus \alpha^{-1}(S) \to Y'$ tels que le diagramme*

$$\begin{tikzcd}
Y \setminus \alpha^{-1}(S) \arrow[rr, "\beta"] \arrow[dr, "\alpha"'] & & Y' \arrow[dl, "\alpha'"] \\
& X' &
\end{tikzcd}$$

commute.

Démonstration. La surface X étant à base dénombrable d'ouverts, l'ensemble S est au plus dénombrable. Par une récurrence, on trouve pour chaque $s \in S$ un voisinage ouvert U_s de s biholomorphe à $\mathbb{D}$, de telle façon que les U_s soient deux à deux disjoints. On munit $\mathbb{D} \times S$ de la structure évidente de surface de Riemann, où S est muni de la topologie discrète, et on note $\mathbb{D}_s = \mathbb{D} \times \{s\}$. On note $U'_s = U_s \setminus \{s\}$ et on choisit des biholomorphismes $h_s : U_s \to \mathbb{D}_s$ tels que $h_s(s) = 0$, où $\mathbb{D}_s$ est une copie du disque complexe $\mathbb{D}$. On note h'_s la restriction $h_s \mid U'_s \to \mathbb{D}_s^\times$. Soit $(V_i)_{i \in I}$ la famille des composantes connexes de $\alpha'^{-1}(\cup_{s \in S} U'_s)$. Pour chaque $i \in I$ il existe un unique $s(i) \in S$ tel que $\alpha'(V_i) \subset U'_{s(i)}$. On note α'_i la restriction $\alpha' \mid V_i \to U'_{s(i)}$, qui est un revêtement. comme précédemment, on munit I de la topologie discrète et pour $A \subset \mathbb{D}$ on note $A_i = A \times \{i\} \subset A \times I$. Comme la composée $h'_{s(i)} \circ \alpha'_i \colon V_i \to \mathbb{D}^\times_{s(i)}$ est un revêtement connexe, par le lemme précédent, il existe un homéomorphisme $g_i : \mathbb{D}_i^\times \to V_i$ et un entier positif k_i tels que, en notant p_i l'application $\mathbb{D}_i \to \mathbb{D}_{s(i)} \colon z \mapsto z^{k_i}$ et p'_i sa restriction $p_i \mid \mathbb{D}_i^\times \to \mathbb{D}^\times_{s(i)}$, le carré suivant est commutatif

$$\begin{tikzcd} V_i \arrow[d, "\alpha'_i"'] & \mathbb{D}_i^\times \arrow[l, "g_i"'] \arrow[d, "p'_i"] \\ U'_{s(i)} \arrow[r, "h_{s(i)}"] & \mathbb{D}^\times_{s(i)} \end{tikzcd}$$

Comme tous les flèches sauf peut être g_i, sont des biholomorphismes locaux, g_i l'est aussi. En recollant tous les g_i en une application $g : \mathbb{D}^\times \times I \to Y'$ et en notant $j : \mathbb{D}^\times \times I \to \mathbb{D} \times I$ l'inclusion évidente, on obtient un diagramme

$$\begin{tikzcd} \mathbb{D}^\times \times I \arrow[r, hook, "j"] \arrow[d, hook, "g"'] & \mathbb{D} \times I \\ Y' & \end{tikzcd} \tag{2}$$

des applications holomorphes injectives dont on veut faire sa somme amalgamée. Vérifions la propriété $(*)$ du lemme 42. Soit $K \subset \mathbb{D} \times I$ compact, on veut montrer que $g(j^{-1}(K)) = g(K \setminus \{0\} \times I)$ est fermé dans Y'. Chaque $K \cap \mathbb{D}_i$ est compact, donc K n'intersecte qu'un nombre finie des $\mathbb{D}_i$ et on se ramène au cas $K \subset \mathbb{D}_i$ pour un i. Supposons par l'absurde qu'il existe une suite $x_\bullet \in (K \setminus \{0\}_i)^{\mathbb{N}}$ tel que $g_i(x_\bullet)$ converge vers un élément $y \in Y' \setminus g(K \setminus \{0\}_i)$. Soit $0 < r < 1$ tel que $K \subset \{z \in \mathbb{D}_i : |z| \leq r\}$ et notons $R_n = \{z \in \mathbb{D} : r/(n+1) \leq |z| \leq r\}_i$, pour $n \in \mathbb{N}$. Dès que $g_i(R_n)$ est compact et Y' est séparé, chaque $g_i(R_n)$ ne contient qu'un nombre fini de termes de $g_i(x_\bullet)$ (sinon, on aurait $y \in g(K \setminus \{0\}_i)$. Ceci implique que $x_\bullet$ tends vers $0 \in \mathbb{D}_i$. On a $\alpha'(y) = \alpha'(\lim g_i(x_\bullet)) = \lim \alpha'(g_i(x_\bullet)) = \lim h^{-1}_{s(i)}(p_i(x_\bullet)) = s(i)$. C'est une contradiction, parce que $\alpha'(Y') \subset X'$, qui ne contiens pas $s(i)$.

On a un diagramme commutatif.

$$\begin{tikzcd}
& \mathbb{D}^\times \times I \arrow[rr, hook, "j"] \arrow[dl, hook', "g"'] \arrow[dd, "p'"] & & \mathbb{D} \times I \arrow[dl, hook', "v"] \arrow[dd, "p"] \\
Y' \arrow[rr, hook, "u"] \arrow[dd, "\alpha'"'] & & Y \arrow[dd, "\alpha"] & \\
& \mathbb{D}^\times \times S \arrow[rr, hook, "k"] \arrow[dl, hook', "b'"'] & & \mathbb{D} \times S \arrow[dl, hook', "b"] \\
X' \arrow[rr, hook, "a"'] & & X &
\end{tikzcd}$$

On explique les objets du diagramme : k est l'inclusion évidente ; p est le recollement de tous les p_i ; p' est le recollement de tous les p'_i ; a est l'inclusion ; b est le recollement de tous les h_s^{-1} ; b' est le recollement de tous les ${h'}_s^{-1}$; Y est la somme amalgamée du diagramme (2) via u et v. Finalement, α est l'application induite par la propriété universelle de la somme amalgamée. Pour la façon dont on construit la somme amalgamé, $Y = u(Y') \sqcup \{v(0_i) : i \in I\}$, et par commutativité du diagramme, $\alpha(v(0_i)) = s(i)$. Par injectivité et puisque v est ouvert, l'ensemble $\{v(0_i) : i \in I\} = \alpha^{-1}(S)$ est fermé et discret, et la restriction $u \mid Y' \to Y \setminus \alpha^{-1}(S)$ est un biholomorphisme. On peut prendre son inverse comme le β dans l'énoncé du théorème. Par construction, Y est connexe.

Il reste à montrer que α est propre, dont il découle que c'est un revêtement ramifié. Soit K un compact dans X. Comme X est localement compact et X' et $b(\mathbb{D} \times S)$ sont des ouverts recouvrant X, il existe des compacts $K_1 \in X'$ et $K_2 \in b(\mathbb{D} \times S)$ tels que $K = K_1 \cup K_2$. Alors $\alpha^{-1}(K) = u({\alpha'}^{-1}(K_1)) \cup v(p^{-1}(b^{-1}(K_2)))$, et c'est un compact parce que α' est propre (voir le lemme 41) et p aussi (parce que chaque p_i l'est). $\square$

Maintenant on a des outils suffisants pour établir la relation entre revêtements ramifiés et revêtements topologiques des surfaces de Riemann.

Définition 45. *Soit X une surface de Riemann connexe et non vide et soit S un sous-ensemble fermé discret de X.*

On définit la catégorie $\mathbf{Hol}X$ *des revêtements ramifiés de X. Pour deux objets $\alpha_1 \colon Y_1 \to X$ et $\alpha_2 \colon Y_2 \to X$, un morphisme de α_1 à α_2 est une application holomorphe $\varphi \colon Y_1 \to Y_2$ telle que*

$$\begin{tikzcd}
Y_1 \arrow[rr, "\varphi"] \arrow[dr, "\alpha_1"'] & & Y_2 \arrow[dl, "\alpha_2"] \\
& X &
\end{tikzcd}$$

commute.

On définit $\mathbf{Hol}_S X$ comme la sous-catégorie pleine de $\mathbf{Hol}_S$ où les objets sont les revêtements ramifiés de X avec tous leur points de branchement dans S.

Proposition et définition 46 (Degré d'un revêtement ramifié)**.** *Soit α : $Y \to X$ un revêtement ramifié. Notons, pour $y \in Y$, n_y l'indice de ramification de y. Il existe un nombre $d \in \mathbb{N} \setminus \{0\}$ tel que pour tout $x \in X$ on a $\sum_{y \in \alpha^{-1}(x)} n_y = d$. On appelle tel d le* ***degré*** *du revêtement ramifié α. Le degré est invariant par isomorphisme de revêtements ramifiés.*

Démonstration. Par le théorème de forme locale 33, la valeur de $\sum_{y \in \alpha^{-1}(x)} n_y$ pour $x \in X$, est localement constant. On a le résultat par connexité de X. □

La relation entre revêtements ramifiés et revêtements topologiques est établie par

Théorème 47. *Soit X une surface de Riemann connexe et non vide et soit S un sous-ensemble fermé discret de X. On dispose d'un foncteur*

$$\mathbf{\Gamma} \colon \mathbf{Hol}_S X \to \mathbf{Revfc}(X \setminus S)$$

qui à un revêtement ramifié $\alpha \colon Y \to X$ associe la restriction $\alpha \mid Y \setminus \alpha^{-1}(S) \to X \setminus S$, et à un morphisme $\varphi \colon Y_1 \to Y_2$ entre deux objets $\alpha_1 \colon Y_1 \to X$ et $\alpha_2 \colon Y_2 \to X$ de $\mathbf{Hol}_S X$ associe la restriction $\varphi \mid Y_1 \setminus \alpha_1^{-1}(S) \to Y_2 \setminus \alpha_2^{-1}(S)$, qui est bien un morphisme entre les revêtements $\mathbf{\Gamma}(\alpha_1)$ et $\mathbf{\Gamma}(\alpha_2)$.

Le foncteur $\mathbf{\Gamma}$ est une équivalence de catégories qui préserve le degré.

Si l'on veut spécifier, on notera ce foncteur $\mathbf{\Gamma}_{X,S}$. Il préserve le degré évidemment. On rappelle que $\mathbf{Revfc}(X \setminus S)$ est la catégorie des revêtements finis connexes non vides de $X \setminus S$, définie dans la section sur les revêtements. Comme $X \setminus S$ est connexe et localement simplement connexe, on peut se servir des résultats de classification des revêtements.

Démonstration. Le foncteur $\mathbf{\Gamma}$ est bien défini par la proposition 40. La proposition 44 affirme exactement que $\mathbf{\Gamma}$ est essentiellement surjectif. Il reste à montrer que $\mathbf{\Gamma}$ est pleinement fidèle. Soient $\alpha_1 \colon Y_1 \to X$ et $\alpha_2 \colon Y_2 \to X$ deux objets de $\mathbf{Hol}_S X$. On note $X' = X \setminus S$, $S_i = \alpha_i^{-1}(S)$ et $Y_i' = Y_i \setminus S_i$ et pour $i = 1, 2$. On veut montrer que l'application

$$\mathrm{Hom}_{\mathbf{Hol}_S X}(\alpha_1, \alpha_2) \to \mathrm{Hom}_{\mathbf{Revfc} X'}(\mathbf{\Gamma}(\alpha_1), \mathbf{\Gamma}(\alpha_2))$$

induite par $\mathbf{\Gamma}$ est une bijection. Elle est injective, par densité de Y_1' dans Y_1.

Pour la surjectivité, on se donne un morphisme $\varphi \colon Y_1' \to Y_2'$ dans $\mathbf{Revfc}(X')$ entre $\mathbf{\Gamma}(\alpha_1)$ et $\mathbf{\Gamma}(\alpha_2)$. Soit $x \in S_1$ et $\alpha_1(x) = s \in S$ et soit $\{y_1, \ldots, y_n\} = \alpha_2^{-1}(s)$. Soient $U_1, \ldots, U_n$ et $V_1, \ldots, V_n$ des ouverts de Y_2 tels que pour tout $i = 1, \ldots, n$,

1. U_i et V_i sont des voisinages de y_i,

2. $\overline{V_i} \subset U_i$,
3. il existe un biholomorphisme $\lambda_i \colon U_i \to \mathbb{D}$ et
4. $U_1, \ldots, U_n$ sont deux à deux disjoints.

Soit $V = \cap_{i=1}^n \alpha_2(V_i)$, qui est un voisinage ouvert de s dans X. Soit U un ouvert connexe de Y_1 tel que $U \cap S_1 = \{x\}$ et $\alpha_1(U) \subset V$. Comme $\alpha_2 \circ \varphi = \alpha_1|_{Y_1'}$, la partie $\varphi(U \setminus \{x\}) \subset \cup_{i=1}^n V_i$. Comme $U \setminus \{x\}$ est connexe, il existe un $i \in \{1, \ldots, n\}$ tel que $\varphi(U \setminus \{x\}) \subset V_i$. Alors, par la proposition 37 (Élimination des singularités), la fonction $\lambda_i \circ \varphi|_{U \setminus \{x\}}$ se prolonge en une application holomorphe $f_x \colon U \to \mathbb{C}$. Par continuité, $f(x) \in \overline{\lambda_i(V_i)} = \lambda_i(\overline{V_i}) \subset \lambda_i(U_i)$, donc $g_x = \lambda_i^{-1} \circ f_x \colon U \to U_i$ prolonge $\varphi|_{U \setminus \{x\}}$. On prolonge φ en une application holomorphe $\widehat{\varphi} \colon Y_1 \to Y_2$ en posant, pour $x \in S_1$, $\widehat{\varphi}(x) = g_x(x)$. Comme $\alpha_2 \circ \widehat{\varphi}|_{Y_1'} = \alpha_1|_{Y_1'}$, par densité de Y_1' dans Y_1, on a aussi $\alpha_2 \circ \widehat{\varphi} = \alpha_1$. L'application $\widehat{\varphi}$ est donc un morphisme entre les revêtements ramifiés α_1 et α_2 tel que $\mathbf{\Gamma}(\widehat{\varphi}) = \varphi$, ce qui conclut. □

Grâce à l'équivalence de catégories ci-dessus on peut définir une notion de revêtement ramifié galoisien.

Proposition et définition 48. *Soit X une surface de Riemann connexe et non vide et soit $\alpha \in \mathbf{Hol}(X)$ de degré d. Alors le cardinal du groupe d'automorphismes $\#Aut(\alpha) \leq d$. Si $\#Aut(\alpha) = d$ on dit que le revêtement ramifié α est **galoisien**.*

Démonstration. Il suffit de prendre $S \subset X$ fermé discret tel que $\alpha \in \mathbf{Hol}_S X$, utiliser que $\mathbf{\Gamma}_{X,S}$ est une équivalence de catégories préservant le degré et la proposition 26. □

Corollaire 49. *Soient X et S comme dans le théorème 47. Pour $\alpha \in \mathbf{Hol}_S X$, α est galoisien si et seulement si $\mathbf{\Gamma}_{X,S}(\alpha)$ est galoisien.*

2.3 Surfaces de Riemann et corps

Définition 50 (Fonction méromorphe). *Une fonction méromorphe sur une surface de Riemann X est une application holomorphe $f : X' \to \mathbb{C}$, où X' est un ouvert de X tel que $S = X \setminus X'$ est un ensemble fermé discret de X et pour chaque $s \in S$ on a*

$$\lim_{z \to s} f(z) = \infty$$

On note $\mathcal{M}(X)$ l'ensemble des fonctions méromorphes sur X.

Par le théorème 37 d'élimination des singularités et par le principe d'identité 36, on peut prolonger $f \colon X' \to \mathbb{C}$ en une fonction holomorphe $X \to \mathbb{P}^1$ de façon unique. Réciproquement, si on se donne une application holomorphe $f \colon X \to \mathbb{P}^1$ qui n'est constante à valeur ∞ sur aucune composante connexe de X, on récupère une fonction méromorphe en prenant la restriction à $X \setminus f^{-1}(\infty)$.

On dispose de plusieurs critères pour montrer qu'une fonction est méromorphe.

Proposition 51. *Soit X une surface de Riemann et soit S un sous ensemble fermé discret de X. Posons $X' = X \setminus S$. Soit $f\colon X' \to \mathbb{C}$ une fonction holomorphe. On a les équivalences :*

1. *La fonction f s'étend en une fonction méromorphe. (Si c'est le cas, l'extension est unique.)*
2. *Pour tout $s \in S$, il existe un voisinage ouvert U connexe de s dans X et une fonction holomorphe $g\colon U \to \mathbb{C}$ non nulle telle que le produit $(g|_{U\setminus S}) \cdot (f|_{U\setminus S})$ s'étende de façon holomorphe à U (c'est le cas si ce produit est borné).*
3. *Pour tout $s \in S$, il existe un voisinage ouvert U de s dans X, une carte $\varphi\colon U \to \mathbb{D}$, un entier $n \in \mathbb{Z}$ et une fonction holomorphe $g\colon \mathbb{D} \to \mathbb{C}$ tels que $f \circ \varphi = z^n \cdot g$.*

Démonstration. Tout découle facilement de [Rudin, 1987], Theorem 10.21, et de la proposition 37. □

La première relation avec les corps est fournie par la

Proposition 52. *Si X est connexe et non vide, alors $\mathcal{M}(X)$ admet naturellement une structure de corps commutatif.*

Démonstration. Comme X n'est pas vide, $\mathcal{M}(X)$ non plus, et on a les fonctions constantes à valeurs 1 et 0, qui seront les éléments neutres. On définit le produit et la somme dans $\mathcal{M}(X)$. Soient $f, g \in \mathcal{M}(X)$. Comme l'union de deux sous-ensembles fermés discrets de X l'est aussi, il existe un sous-ensemble fermé discret $S \subset X$ tel que f et g sont définies sur $X' = X \setminus S$. Maintenant, on peut sommer ou multiplier les restrictions $f, g \mid X' \to \mathbb{C}$. Soit a un point de S et $\varphi : U \to \mathbb{D}$ une carte autour de a avec $\varphi(a) = 0$. Par la proposition 51, on a

$$\forall z \in \mathbb{D}', \quad f \circ \varphi^{-1}(z) = z^n u(z) \text{ et } g \circ \varphi^{-1}(z) = z^m v(z)$$

pour $n, m \in \mathbb{Z}$ et $u, v : \mathbb{D} \to \mathbb{C}$ holomorphes. Pour le produit, on a

$$(f \cdot g) \circ \varphi^{-1} = z^{n+m} u \cdot v,$$

donc $f \cdot g$ se prolonge bien en une fonction holomorphe vers $\mathbb{P}^1$ près de a, selon que $n + m$ est négatif ou positif. Pour la somme, en supposant par exemple que $n \geq m$, on a

$$(f + g) \circ \varphi^{-1} = z^m (z^{n-m} u + v),$$

donc $f + g$ se prolonge bien en une fonction holomorphe vers $\mathbb{P}^1$ près de a, selon le cas. Tous ces prolongements son uniques, et les opérations sont donc bien définies.

La commutativité et la distributivité des opérations viennent du fait qu'on a ces propriétés sur des ouverts appropriés (dépendant des fonctions choisies à chaque fois), et du principe d'identité. Ceci montre que $\mathcal{M}(X)$ est un anneau commutatif.

Pour l'existence d'inverses, soit $f \in \mathcal{M}(X)$ non nulle. Encore pour le principe d'identité, $f^{-1}(0)$ est fermé et discret dans X. On peut définir $1/f$ sur $X \setminus f^{-1}(0)$ et prolonger en une fonction méromorphe comme précédemment en regardant la forme locale. □

Le corps des fonctions méromorphes de la sphère de Riemann est bien connu.

Proposition 53. *Le corps $\mathcal{M}(\mathbb{P}^1)$ des fonctions méromorphes sur la sphère de Riemann est canoniquement isomorphe à $\mathbb{C}(t)$.*

Démonstration. Une fraction rationnelle non nulle $f/g \in \mathbb{C}(t)$, où f et g sont des polynômes non nuls dans $\mathbb{C}[t]$ premiers entre eux correspond à une fonction méromorphe sur $\mathbb{P}^1$ où l'ensemble des pôles est l'ensemble des zéros de g avec ∞ si deg $f >$ deg g. Ceci nous donne un monomorphisme canonique $\mathbb{C}(t) \to \mathcal{M}(\mathbb{P}^1)$. Montrons qu'il est surjectif. Soit $h \in \mathcal{M}(\mathbb{P}^1)$ non nulle. Quitte à remplacer h par $1/h$, on peut supposer que ∞ n'est pas un pôle de h. Par compacité de $\mathbb{P}^1$, h n'a qu'un nombre fini de pôles $a_1, \ldots, a_n \in \mathbb{C}$. Par [Rudin, 1987], Theorem 10.21, pour chaque $i = 1, \ldots, n$ il existe un nombre naturel m_i et des nombres complexes $c_1, \ldots, c_{m_i}$ tels que

$$h - \sum_{j=1}^{m_i} \frac{c_j}{(z - a_i)^j}$$

n'a pas de pôle dans a_i. Alors la fonction

$$h - \sum_{i=1}^{n} \sum_{j=1}^{m_i} \frac{c_j}{(z - a_i)^j}$$

est holomorphe sur $\mathbb{C}$ et bornée, donc elle est constante, par le théorème de Liouville. Ceci implique que h est une fraction rationnelle.

□

Étant donné un revêtement ramifié $\varphi : Y \to X$, où X et Y sont connexes et non vides, le tiré en arrière $\varphi^* : \mathcal{M}(X) \to \mathcal{M}(Y) : f \mapsto f \circ \varphi$ est un morphisme de corps qui définit une extension de $\mathcal{M}(Y)$ sur $\mathcal{M}(X)$.

Soit X une surface de Riemann connexe et non vide et $u : Y \to Z$ un morphisme entre deux revêtements ramifiés $\varphi : Y \to X$ et $\sigma : Z \to X$. Le tiré en arrière par u, $u^* : \mathcal{M}(Z) \to \mathcal{M}(Y)$, donne un morphisme entre les extensions σ^* et φ^*. On note **EF**-$\mathcal{M}(X)$ la catégorie des extensions finies du corps $\mathcal{M}(X)$. Le théorème suivant est fondamental et donne le lien entre revêtements ramifiés et extensions finies du corps de fonctions méromorphes.

Théorème 54 (Anti-équivalence entre revêtements ramifiés et extensions finies)**.** *Soit X une surface de Riemann compacte, connexe et non vide. Le foncteur contravariant*

$$\mathbf{\Theta}_X : \mathbf{Hol}X \to \mathbf{EF}\text{-}\mathcal{M}(X)$$

qui, à un revêtement ramifié $\varphi : Y \to X$, associe l'extension φ^* et, à chaque morphisme de revêtement ramifié $u : Y \to Z$, associe le tiré en arrière u^* est bien défini et établit une anti-équivalence de catégories.

Si le degré de $\varphi : Y \to X$ comme revêtement ramifié est d, alors le degré de l'extension $\mathbf{\Theta}_X(\varphi)$ est aussi d.

Démonstration. On montre d'abord que le foncteur est bien défini, c'est-à-dire que φ^* est bien une extension finie de $\mathcal{M}(X)$. Ensuite, la fonctorialité ($u^* \circ v^* = (v \circ u)^*$) est immédiate. On commence par un lemme.

Lemme 55. *Soit $\varphi : Y \to X$ un revêtement ramifié connexe de degré d de X. Tout élément de $\mathcal{M}(Y)$ est algébrique sur $\mathcal{M}(X)$ (au moyen de φ^*) et son polynôme minimal a pour degré au plus d.*

Démonstration. On définit les polynômes symétriques élémentaires $s_1, \dots, s_d$ en les variables $x_1, \dots, x_d$ par la formule

$$\prod_{i=1}^{d}(x - x_i) = x^d - s_1(x_1, \dots, x_d)x^{d-1} + \cdots + (-1)^d s_d(x_1, \cdots, x_d)$$

où x est une indéterminée. On a aussi, pour $1 \leq n \leq d$, la formule explicite

$$s_n(x_1, \dots, x_d) = \sum_{\substack{S \subset \{1,\dots,d\} \\ |S|=n}} \prod_{i \in S} x_i$$

Soit $A \subset Y$ l'ensemble des points de branchement de φ et des pôles de f. Étant fermé et discret, et par compacité de Y, A est fini. On définit, pour des entiers $1 \leq n \leq d$, des fonctions

$$a_n : X \setminus \varphi(A) \to \mathbb{C} : x \mapsto s_n(f(y_1), \dots, f(y_d))$$

où $y_1, \dots, y_d$ sont les différents éléments de la fibre $\varphi^{-1}(x)$. Par symétrie de s_n, la valeur de a_n ne dépend pas de la numérotation de $\varphi^{-1}(x)$, donc a_n est bien défini.

Montrons que a_n est holomorphe sur $X \setminus \varphi(A)$. Soit $x_0 \in X \setminus \varphi(A)$ et soient $y_1, \dots, y_d$ les éléments de la fibre $\varphi^{-1}(x_0)$. Soient $V_1, \dots, V_d \subset Y \setminus A$ des voisinages deux à deux disjoints de $y_1, \dots, y_d$ respectivement tels que chaque $\varphi|_{V_i}$ est injective (voir la proposition 33). Puisque φ est ouverte (voir la proposition 34), $U = \cap_i \varphi(V_i)$ est un voisinage ouvert de x_0. En remplaçant chaque V_i par $V_i \cap \varphi^{-1}(U)$, les applications $\varphi_i = \varphi \mid V_i \to U$

sont des biholomorphisme (voir la proposition 35). On peut alors exprimer la restriction de a_n à U comme

$$a_{n|U} = s_n(f \circ \varphi_1^{-1}, \dots, f \circ \varphi_d^{-1}),$$

ce qui montre bien que a_n est holomorphe.

Voyons que a_n admet une extension méromorphe à X. Par la proposition 51, il suffit de montrer que chaque point $a \in \varphi(A)$ admet un voisinage ouvert U disjoint de $\varphi(A) \setminus \{a\}$ et une fonction holomorphe $u : U \to \mathbb{C}$ tel que $a_{n|U'} \cdot u|_{U'}$ est bornée, où $U' = U \setminus \{a\}$. Soient $y_1, \dots, y_l \in Y$ les différents points de $\varphi^{-1}(a)$. On peut trouver des voisinages ouverts V_i deux à deux disjoints de y_i dans Y, un voisinage U de a dans X et une fonction holomorphe $r : U \to \mathbb{C}$ tels que

(i) U est disjoint de $\varphi(A) \setminus \{a\}$ et on note $U' = U \setminus \{a\}$.

(ii) Pour tout $1 \leq i \leq l$, $\varphi(V_i) \subset U$.

(iii) Pour tout $1 \leq i \leq l$, le produit $f|_{V_i} \cdot (r \circ \varphi|_{V_i})$ est bornée, par une constante que l'on appellera M.

Soit $x \in U'$, on a

$$a_n(x)r(x)^n = \sum_{\substack{S \subset \varphi^{-1}(x) \\ |S|=n}} \prod_{y \in S} f(y) \cdot r(x) = \sum_{\substack{S \subset \varphi^{-1}(x) \\ |S|=n}} \prod_{y \in S} f(y) \cdot (r \circ \varphi)(y),$$

qui est borné par $\binom{d}{n} \cdot M^n$.

Pour finir il faut juste remarquer que, par notre choix des a_n, pour tout $b \in Y \setminus A$ on a

$$0 = \prod_{y \in \varphi^{-1}(\varphi(b))} (f(b) - f(y)) = f(b)^d - a_1(\varphi(b))f(b)^{d-1} + \cdots + (-1)^d a_d(\varphi(b)),$$

donc par le principe d'identité, f est une racine du polynôme

$$x^d - \varphi^*(a_1)x^{d-1} + \cdots + (-1)^d \varphi^*(a_d),$$

qui a ses coefficients dans $\varphi^*(\mathcal{M}(X))$, ce qui conclut.

□

Lemme 56. *Soit $\varphi : Y \to X$ un revêtement ramifié connexe de degré d de X. Alors $\varphi^* : \mathcal{M}(X) \to \mathcal{M}(Y)$ induit une extension finie $\mathcal{M}(Y)|\mathcal{M}(X)$ de degré d.*

Démonstration. Pour la preuve de ce lemme on doit utiliser un résultat analytique profond, le théorème d'existence de Riemann, que l'on énonce sans démonstration.

Théorème 57 (Théorème d'existence de Riemann)**.** *Soient X une surface de Riemann compacte, $x_1, \dots, x_n$ un nombre fini de points deux à deux distincts de X et $a_1, \dots, a_n$ des nombres complexes. Il existe une fonction méromorphe $f \in \mathcal{M}(X)$ tel que pour tout $1 \leq i \leq n$, $f(x_i) = a_i$.*

Pour une preuve, voir par exemple [Forster, 1991], Corollary 14.13.

Soient x un point de X qui n'est pas un point de ramification de φ et $y_1, \dots, y_d$ les points de sa fibre. A l'aide du théorème d'existence de Riemann, on prend une fonction méromorphe $f \in \mathcal{M}(Y)$ telle que les $f(y_i)$ sont tous distincts. Soit $t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in \mathcal{M}(X)[t]$ le polynôme minimal de f, qui par le lemme précédent a pour degré $n \leq d$. Soit $S \subset X$ l'ensemble des pôles des a_i. Comme il n'y a qu'un nombre fini de points de ramification de φ, par continuité de f et parce que φ est ouverte, on peut trouver un voisinage U de x dans X tel que U ne contient pas des points de ramification et tel que pour tout $c \in U$, $f(\varphi^{-1}(c))$ est un ensemble à d éléments. Comme S est fini, il existe un point $c \in U \setminus S$. Tout élément de $f(\varphi^{-1}(c))$ est une racine de $t^n + a_{n-1}(c)t^{n-1} + \cdots + a_0(c) \in \mathbb{C}[t]$, ce qui implique $d = n$.

On montre que $\mathcal{M}(X)(f) = \mathcal{M}(Y)$. Soit $g \in \mathcal{M}(Y)$. Par le théorème de l'élément primitif, il existe $h \in \mathcal{M}(Y)$ tel que $\mathcal{M}(X)(f, g) = \mathcal{M}(X)(h)$. Par le lemme précédent, $\mathcal{M}(X)(h)|\mathcal{M}(X)$ est une extension finie de degré au plus d, mais elle contient $\mathcal{M}(X)(f)$, qui est de degré d, ce qui implique $\mathcal{M}(X)(f) = \mathcal{M}(X)(h)$ et en conséquence $g \in \mathcal{M}(X)(f)$. □

On développe le reste de la preuve en plusieurs étapes.

Lemme 58. *Le foncteur $\mathbf{\Theta}_X$ est essentiellement surjectif.*

Démonstration. On utilisera plus bas :

Lemme 59. *Soit $\tau \colon U \to V$ une application continue à fibres finies telle que V est séparé et pour tout $v \in V$ et tout $u \in \tau^{-1}(v)$ il existe un voisinage ouvert O de v et une section locale $s \colon O \to U$ de τ telle que $s(v) = u$. Alors τ est un revêtement.*

On ne donne pas la preuve, car elle est facile. On veut juste remarquer que le résultat est faux si on ne suppose pas que U est séparé. La projection de la droite à deux origines sur la droite est un contre-exemple.

Soit $L|\mathcal{M}(X)$ une extension finie de degré d. Soit $\alpha \in L$ un élément primitif et soit $F \in \mathcal{M}(X)[x]$ son polynôme minimal, où x est une indéterminée. Le polynôme F est séparé, donc il existe $A, B \in \mathcal{M}(X)[x]$ tels que

$$FA + F'B = 1 \tag{3}$$

où F' est la dérivée formelle de F. Soit $S \subset X$ l'ensemble fermé discret des pôles des coefficients de F, A et B, et posons $X' = X \setminus S$. Pour $a \in X'$, on note F_a la spécialisation de F en a, c'est-à-dire le polynôme $F_a \in \mathbb{C}[x]$ qui résulte de l'évaluation de tous les coefficients de F en a. Soit $Y' = \{(a, z) \in$

$X' \times \mathbb{C} : F_a(z) = 0\}$, muni de la topologie induite comme sous-ensemble de $X' \times \mathbb{C}$. Posons $p' \colon Y' \to X' \colon (a, z) \mapsto a$, qui est bien continue. Montrons que p' est un revêtement. Comme p' est à fibres finies et Y' est séparé, par le lemme 59 il suffit de montrer que pour tout point $a_0 \in X'$ et pour tout $(a_0, z_0) \in p'^{-1}(a_0)$, il existe un voisinage U de a_0 dans X' et une application continue $s \colon U \to Y'$ avec $s(a_0) = (a_0, z_0)$ et $p' \circ s = id_U$. Si un tel a_0 et un tel b_0 sont donnés, on a $F_{a_0}(z_0) = 0$ et $F_{a_0}(z_0) \neq 0$, par (3). Comme $(a, z) \to F_a(z)$ est C^∞, par le théorème de la fonction inverse, il existe un voisinage ouvert U de a_0 et une fonction $\xi \colon U \to \mathbb{C}$ de classe C^∞ telle que $\xi(a_0) = z_0$ et $F_a(\xi(a)) = 0$, pour tout $a \in U$. Alors la fonction s définie comme $s(a) = (a, \xi(a))$, pour tout $a \in U$, convient.

L'espace Y' admet une structure de surface de Riemann qui fait de p' une application holomorphe. Par la proposition 44, Y' se plonge dans une autre surface Y de façon telle que $Y \setminus Y'$ est un sous-ensemble fermé discret de Y et p' est la restriction d'un revêtement ramifié $p \colon Y \to X$. On définit sur Y' la fonction $f \colon Y' \to \mathbb{C} \colon (a, z) \mapsto z$. Elle est holomorphe, car en précomposant par une section s comme précédemment (qui est un biholomorphisme sur son image), on obtient ξ. Cette dernière est holomorphe, parce que sa différentielle, qui peut se calculer a l'aide des différentielles partielles de $(a, z) \to F_a(z)$, est $\mathbb{C}$-linéaire. Montrons que f s'étend en une fonction méromorphe. On écrit

$$F = x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

avec $a_0, \ldots, a_{d-1} \in \mathcal{M}(X)$. Soit $s \in Y \setminus Y'$. Il existe un voisinage U de $p(s)$ dans X, une fonction holomorphe $r \colon U \to \mathbb{C}$ et une constante $M > 0$ tels que r et $a_0 \cdot r, \ldots, a_{d-1} \cdot r$ sont bornés par M sur $U \setminus \{p(s)\}$. On peut borner las racines d'un polynôme unitaire par ses coefficients :

Lemme 60. *Soit $P = x^n + b_{n-1}x^{n-1} \cdots + b_0 \in \mathbb{C}[x]$. Toute racine de P est bornée par $n \cdot (\max_i |b_i| + 1)$.*

Démonstration. Si $|z| > n \cdot (\max_i |b_i| + 1)$,

$$\frac{|P(z)|}{|z|^n} \geq 1 - \frac{|b_{n-1}|}{|z|} - \cdots - \frac{|b_0|}{|z|} \geq 1 - \frac{1}{n}\left(\frac{|b_{n-1}|}{|b_{n-1}| + 1} - \cdots - \frac{|b_0|}{|b_0| + 1}\right) > 0$$

□

Soit V un voisinage de s dans $Y' \cup \{s\}$ tel que $p(V) \subset U$. Pour tout $v \in V \setminus \{s\}$, on a

$$|f(v) \cdot r \circ p(v)| \leq n \cdot \left(\max_i |a_i(p(v))| + 1\right) \cdot |r(p(v))| \leq 2M$$

Par la proposition 51, f se prolonge à une fonction méromorphe sur Y. Le revêtement p' est à fibres de cardinal d, donc le revêtement ramifié p est de degré d. Montrons que Y est connexe. Soit Y_1 une composante connexe de Y. Le polynôme minimal de $f|_{Y_1} \in \mathcal{M}(Y_1)$ divise F, mais ce dernier est irréductible. Le polynôme minimal de $f|_{Y_1}$ est donc F. Ceci implique que le degré de $\mathcal{M}(Y_1)|\mathcal{M}(X)$ est d, donc le degré du revêtement ramifié $p|_{Y_1}$ est d, et $Y_1 = Y$, c'est-à-dire que Y est connexe. Par le lemme 55, l'extension $\mathcal{M}(Y)|\mathcal{M}(X)$ est de degré d, et f est un élément de degré d. Le polynôme minimal de f est F, et comme F est irréductible, il existe un isomorphisme de $\mathcal{M}(Y)|\mathcal{M}(X)$ à $L|\mathcal{M}(X)$ qui envoie f sur α. Ceci montre que le foncteur $\mathbf{\Theta}_X$ est essentiellement surjectif. $\square$

Pour finir la preuve, il reste à montrer que le foncteur $\mathbf{\Theta}_X$ est pleinement fidèle. Soient $\varphi\colon Y \to X$ et $\sigma\colon Z \to X$ des éléments de $\mathbf{Hol}X$. Soit $c \in X$ un point que n'est pas de branchement ni pour φ ni pour σ. Par le théorème d'existence de Riemann, soient f et g dans $\mathcal{M}(Y)$ et $\mathcal{M}(Z)$ telles qu'elles séparent les points de $\varphi^{-1}(c)$ et $\sigma^{-1}(c)$, respectivement. Soient $F, G \in \mathcal{M}(X)[x]$ les polynômes minimaux de f et g respectivement. Soit S l'ensemble des points de branchement de φ et σ, des images par φ des pôles de f et des pôles des coefficients de F, et des images par σ des pôles de g et des pôles des coefficients de G. Posons $X' = X \setminus S$, $Y' = Y \setminus \varphi^{-1}(S)$ et $Z' = Z \setminus \sigma^{-1}(S)$. On note φ' et σ' les restrictions de φ et σ au dessus de X', qui sont des revêtements topologiques. Quitte à remplacer c par un point très voisin de c, on peut supposer que $c \in X'$. Par la preuve du lemme 56, f et g sont des éléments primitifs de $\mathcal{M}(Y)$ et $\mathcal{M}(Z)$ respectivement. On définit,

$$X_F = \{(a, z) \in X' \times \mathbb{C} : F_a(z) = 0\}$$

$$X_G = \{(a, z) \in X' \times \mathbb{C} : G_a(z) = 0\}$$

et on note $\pi_F\colon X_F \to X$ et $\pi_G\colon X_G \to X$ les projections sur la première composante. Comme dans la preuve de 58, on peut ajouter des points à S pour que toutes les spécialisations de F et G dans X' soient séparées. Quitte à décaler c un peu, on peut supposer que $c \in X'$. Par la preuve du lemme 58, π_F et π_G sont des revêtements topologiques connexes non vides. On a un morphisme de revêtements $u_F\colon Y' \to X_F\colon b \mapsto (\varphi(b), f(b))$ entre φ' et π_F qui, étant bijectif sur la fibre de c, est un isomorphisme, par le théorème de classification des revêtements 14. De même on a un isomorphisme $u_G\colon Z' \to X_G\colon b \mapsto (\sigma(b), g(b))$ entre σ' et π_G.

Montrons que $\mathbf{\Theta}_X$ est plein. Soit $v\colon \mathcal{M}(Z) \to \mathcal{M}(Y)$ un morphisme de $\mathcal{M}(X)$-algèbres. Il existe un polynôme $R \in \mathcal{M}(X)[x]$ tel que $v(g) = R(f)$. On a $G \circ R(f) = G(v(g)) = v(G(g)) = 0$, donc il existe $V \in \mathcal{M}(X)[x]$ tel que $G \circ R = F \cdot V$. Quitte à ajouter des points à S et à décaler c un peut, on peut supposer que tous les coefficients de R et de V sont définis sur X'. On définit un morphisme de revêtements u entre π_F et π_G par $u\colon X_F \to X_G\colon (a, z) \mapsto (a, R_a(z))$. C'est bien défini, car si $(a, z) \in X_F$, alors $G_a(R_a(z)) = F_a(z) \cdot$

$V_a(z) = 0$, donc $(a, R_a(z)) \in X_G$. Comme c'est clairement continu et il préserve les fibres, u est bien un morphisme de revêtements.

$$\begin{tikzcd} Y' \arrow[r, "u_F"] \arrow[dr, "\varphi'"'] & X_F \arrow[r, "u"] \arrow[d, "\pi_F"] & X_G \arrow[dr, "\pi_G"'] & Z' \arrow[l, "u_G"'] \arrow[d, "\sigma"] \\ & X' & & X' \end{tikzcd}$$

La composé $w' = (u_G)^{-1} \circ u \circ u_F$ est un morphisme de revêtements entre φ' et σ. Le tiré en arrière par w' de $g|_{Z'}$ en $a \in Y'$ est $g(w'(a)) = \pi_G(u_G(w'(a))) = \pi_G(u(u_F(a)) = \pi_G\left(\varphi(a), R_{\varphi(a)}(f(a))\right) = v(g)(a)$. Par le théorème 47, w' s'étend de façon unique en un morphisme de revêtements ramifiés $w\colon Y \to Z$. Par densité, $w^*(g) = v(g)$, et comme g est un générateur de $\mathcal{M}(Z)$, on a $w^* = v$.

Montrons que $\mathbf{\Theta}_X$ est fidèle. Notons $o_1 = \varphi^{-1}(c)$ et $o_2 = \sigma^{-1}(c)$. Soient $u_1, u_2\colon Y \to Z$ deux morphismes entre φ et σ qui ont le même tiré en arrière, $u_1^* = u_2^*\colon \mathcal{M}(Z) \to \mathcal{M}(Y)$. On a $g \circ u_1 = g \circ u_2$, d'où $g \circ u_1|_{o_1} = g \circ u_2|_{o_1}$. Comme g est injective sur o_2, $u_1|_{o_1} = u_2|_{o_1}$. Comme le foncteur fibre est pleinement fidèle (théorème 14), les deux morphismes $u_1|_{Y'}$ et $u_2|_{Y'}$ entre les revêtements φ' et σ' sont égaux. Par densité, $u_1 = u_2$.

Ceci conclut la preuve du théorème 54.

□

C'est un fait connu de théorie de Galois des corps que pour une extension finie de corps $L|K$ de degré d, le cardinal $\#\mathrm{Aut}(L|K) \leq d$ et qu'on a l'égalité si et seulement si $L|K$ est une extension galoisienne. En utilisant le fait que l'équivalence de catégories $\mathbf{\Theta}_X$ préserve le degré, on en déduit

Corollaire 61. *Soit X une surface de Riemann compacte, connexe et non vide et φ un revêtement ramifié de X. L'extension φ^* de corps associé est galoisienne si et seulement si φ est galoisien.*

2.4 Résumé des équivalences

Soit X une surface de Riemann compacte, connexe et non vide. Soit $S \subset X$ fini, $X' = X \setminus S$ et $b \in X'$. On a étudié les catégories suivantes

1. La catégorie $\mathbf{Hol}X$ des revêtements ramifiés de X.
2. La catégorie $\mathbf{Hol}_S X$ des revêtements ramifiés de X non ramifiés au-dessus de X', qui est une sous-catégorie pleine de $\mathbf{Hol}X$.
3. La catégorie $\mathbf{EF}\text{-}\mathcal{M}(X)$ des extensions finies du corps des fonctions méromorphes sur X.
4. La catégorie $\mathbf{Revfc}(X')$ des revêtements finis connexes non vides de $X \setminus S$.
5. La catégorie $\pi_1(X', b)$-$\mathbf{Ensft}$ des actions finis transitifs non vides de $\pi_1(X', b)$.

Dans chacune de ces catégories on a une notion de degré et une notion d'être galoisien. Parmi les trois foncteurs suivants le premier est une anti-équivalence et les autres sont des équivalences de catégories. Touts préservant le degré et les objets galoisiens.

1. $\mathbf{\Theta}_X \colon \mathbf{Hol}X \to \mathbf{EF}\text{-}\mathcal{M}(X)$,
2. $\mathbf{\Gamma}_{X,S} \colon \mathbf{Hol}_S X \to \mathbf{Revfc}(X')$,
3. $\mathbf{\Omega}_{X',b} \colon \mathbf{Revfc}(X') \to \pi_1(X',b)\text{-}\mathbf{Ensft}$

Ils ont été définis dans les théorèmes 54, 47 et 14 respectivement.

2.5 Application au problème de Galois inverse sur $\mathbb{C}(t)$

Soit K un corps commutatif. On dit qu'un groupe fini est **réalisable** sur K s'il est isomorphe au groupe de Galois d'une extension fini galoisienne de K. *Le problème de Galois inverse sur le corps K* consiste à tenter de classifier les groupes finis réalisables sur K. La conjecture principale autour du problème de Galois inverse est

Conjecture 62. *Tout groupe fini est réalisable sur $\mathbb{Q}$.*

Cela reste encore un problème ouvert et un sujet actif de recherche. Cependant, on a développé des outils suffisants pour résoudre le problème de Galois inverse sur le corps des fractions rationnelles complexes $\mathbb{C}(t)$.

Théorème 63. *Tout groupe fini est réalisable sur $\mathbb{C}(t)$.*

Démonstration. Soit G un groupe fini et soit G' son groupe opposé. Par le corollaire 30, il existe un sous-ensemble fini $S \subset \mathbb{P}^1$ et un revêtement connexe fini galoisien p de $\mathbb{P}^1 \setminus S$ tel que $\mathrm{Aut}_{\mathbf{Revfc}(\mathbb{P}^1 \setminus S)}(p)$ est isomorphe à G'. Par surjectivité essentielle de $\mathbf{\Gamma}_{\mathbb{P}^1,S}$, il existe q dans $\mathbf{Hol}_S\mathbb{P}^1$ tel que $\mathbf{\Gamma}_{\mathbb{P}^1,S}(q)$ est isomorphe à p. Comme $\mathbf{\Theta}_{\mathbb{P}^1}$ est une anti-équivalence, le groupe $\mathrm{Aut}_{\mathbf{EF}\text{-}\mathcal{M}(\mathbb{P}^1)}(\mathbf{\Theta}_{\mathbb{P}^1}(q))$ est anti-isomorphe à $\mathrm{Aut}_{\mathbf{Hol}\mathbb{P}^1}(q)$. Ce dernier groupe est isomorphe à $\mathrm{Aut}_{\mathbf{Revfc}(\mathbb{P}^1 \setminus S)}(p)$ via $\mathbf{\Gamma}_{\mathbb{P}^1,S}$. Ceci nous donne un anti-isomorphisme entre $\mathrm{Aut}_{\mathbf{EF}\text{-}\mathcal{M}(\mathbb{P}^1)}(\mathbf{\Theta}_{\mathbb{P}^1}(q))$ et G', donc un isomorphisme entre $\mathrm{Aut}_{\mathbf{EF}\text{-}\mathcal{M}(\mathbb{P}^1)}(\mathbf{\Theta}_{\mathbb{P}^1}(q))$ et G.

Les équivalences préservent les objets galoisiens. Ainsi, q est galoisien parce que $\mathbf{\Gamma}_{\mathbb{P}^1,S}(q)$, qui est isomorphe à p, est galoisien. L'extension $\mathbf{\Theta}_{\mathbb{P}^1}(p)$ est aussi galoisienne. Le fait que $\mathbb{C}(t)$ et $\mathcal{M}(\mathbb{P}^1)$ soient isomorphes (voir 53) nous permet de conclure. □

En fait, le cas du groupe du corps $\mathbb{C}(t)$ est essentiel. Il nous permet de montrer que sur un corps de la forme $K(t)$ tout groupe fini est réalisable, où K est algébriquement clos et de caractéristique 0. En particulier tout groupe fini est réalisable sur $\overline{\mathbb{Q}}(t)$. Ensuite, la méthode de rigidité permet de montrer que, sous certains conditions, un groupe fini réalisable sur $\overline{\mathbb{Q}}(t)$ est aussi réalisable sur $\mathbb{Q}(t)$. Finalement, le théorème d'irréductibilité de Hilbert montre que tout groupe fini réalisable sur $\mathbb{Q}(t)$ est aussi réalisable sur $\mathbb{Q}$. Cela permet de prouver que certains familles de groupes finis sont réalisables sur $\mathbb{Q}$, donnant une solution partielle à la conjecture principale du problème de Galois inverse. Pour une exposition à cette histoire, nous renvoyons à [Malle and Matzat, 1999].

3 Extensions infinies de corps

Définition 64 (Ordre filtrant croissant)**.** *Un **ordre filtrant croissant** est un ensemble ordonné $(\Lambda, \leq)$ (vu comme une petite catégorie où il y a une flèche de a à b si et seulement si $a \leq b$) avec la propriété suivante*

$$\forall a, b \in \Lambda, \quad \exists c \in \Lambda, \quad a \leq c \text{ et } b \leq c$$

Définition 65 (Système projectif, cône)**.** *Étant donné un ordre filtrant croissant Λ, et une catégorie $\mathcal{C}$, un **système projectif** dans $\mathcal{C}$ indexé par Λ est un foncteur contravariant $\psi \colon \Lambda \to \mathcal{C}$. Pour $a \leq b$ dans Λ, on note $\psi_{ab} : \psi(b) \to \psi(a)$ le morphisme associé.*

*Un **cône** de ψ est une transformation naturelle entre δ_N et ψ, où N est un objet de $\mathcal{C}$ et δ_N est le foncteur $\Lambda \to \mathcal{C}$ qui envoie tous les objets sur N et toutes les flèches sur id_N. L'objet N s'appelle **sommet** du cône ψ.*

Plus concrètement, un cône de ψ est la donnée d'un objet N de $\mathcal{C}$ et d'une famille de morphismes $(c_a \colon N \to \psi(a))_{a \in \Lambda}$ telle que pour tous $a \leq b$ dans Λ, on a $\psi_{ab} \circ c_b = c_a$. On utilise la notation (N, c) pour designer un tel cône. Un morphisme entre cônes (N, c) et (M, d) est la donnée d'un morphisme $u \colon N \to M$ dans $\mathcal{C}$ tel que pour tout $a \in \Lambda$, on ait $d_a \circ u = c_a$. On obtient de cette façon la **catégorie des cônes de** ψ.

Définition 66 (Limite projective)**.** *Une **limite projective** d'un système projectif ψ est un cône final dans la catégorie des cônes de ψ.*

On rappelle que, dans une catégorie $\mathcal{D}$, un objet a est dit final si pour tout objet b de $\mathcal{D}$, il existe un unique morphisme de b dans a. L'exemple typique est le point dans **Top**. On vérifie facilement que deux objets finaux dans une catégorie sont isomorphes d'une unique façon. Deux limites projectives de ψ sont alors canoniquement isomorphes. On utilise la notation $\varprojlim \psi$ pour désigner une limite projective de ψ lorsqu'elle existe. On se permettra d'utiliser des notations plus vagues comme $\varprojlim \psi(a)$. Parfois on appellera aussi *limite projective* au sommet du cône qui est la limite projective au sens précédent.

Pour certains catégories la limite projective existe toujours.

Proposition 67. *Dans les catégories* **Grp** *des groupes,* **Grptp** *des groupes topologiques,* **Top** *des espaces topologiques et* **Ens** *des ensembles, il existe la limite projective de tout système projectif.*

Démonstration. Montrons le résultat par exemple pour la catégorie **Grp**. Pour les autres le principe est le même : on peut considérer un produit et certain sous-ensemble de ce produit.

Soit $\psi \colon \Lambda \to$ **Grp** un système projectif de groupes. On prendre le produit $H = \prod_{a \in \Lambda} \psi(a)$ et on note $p_a \colon H \to \psi(a)$ la projection, pour $a \in \Lambda$. On définit,

$$G = \{(g_a)_{a \in \Lambda} : \psi_{ab}(g_b) = g_a, \text{ si } a \leq b\}$$

On voit que G est un sous-groupe de H, et on note $i\colon G \to H$ l'inclusion. Alors $(G,(p_a \circ i)_{a\in\Lambda})$ convient comme limite projective. En effet, c'est bien un cône et si (N,c) est un autre cône de ψ, l'image du produit (au but) d'applications $\prod_{a\in\Lambda} c_a$ est contenu dans G et factorise donc en une application $N \to G$ qui fournit bien un morphisme de cônes. On vérifie sans peine l'unicité de ce morphisme. $\square$

Supposons que $\mathcal{C}$ admet des limites projectives. On a une catégorie $\underleftarrow{\mathcal{C}_\Lambda}$ où les objets sont les systèmes projectifs indexés par Λ et où les morphismes sont les transformations naturelles entre eux. On a aussi un foncteur $\underleftarrow{\mathcal{C}_\Lambda} \to \mathcal{C}$ qui, à un système projectif, associe sa limite et, à une transformation naturelle entre systèmes projectifs, associe le morphisme induit entre les limites.

Le lemme suivant sera utile dans le chapitre suivant. On ne le montre pas, la démonstration étant facile.

Lemme 68. *Soit $\psi\colon \Lambda \to \mathcal{C}$ un système projectif qui a pour limite $a \in \mathcal{C}$. Soit $j\colon \Lambda' \to \Lambda$ un morphisme d'ensembles ordonnés qui admet une section. Alors la composée $\psi' = \psi \circ j$ est un système projectif qui a pour limite a.*

Le résultat suivant repose sur le Théorème de Tychonoff (et donc sur l'axiome du choix). Il sera utile pour le chapitre suivant.

Proposition 69. *La limite dans* **Top** *d'un système projectif d'espaces topologiques compacts non vides est non vide et compacte. En particulier la limite dans* **Ens** *d'un système projectif d'ensembles finis non vides est non vide.*

Démonstration. Soit $\psi\colon \Lambda \to \mathbf{Top}$ un tel système. La limite projective est le sous-espace X du produit $P = \Pi_{c\in\Lambda}\psi(c)$ formé des tuples $(x_c)_{c\in\Lambda}$ tels que $\psi_{ab}(x_b) = (x_a)$ pour tous $a \leq b$ dans Λ. Pour tout couple $a \leq b$ dans Λ, on considère l'ensemble X_{ab} des tuples $(x_c)_{c\in\Lambda}$ tels que $\psi_{ab}(x_b) = (x_a)$. Comme chaque $\psi(c)$ est séparé, X_{ab} est fermé. Comme Λ est filtrant croissant, une intersection finie des X_{ab} est non vide. Par le théorème de Tychonoff, le produit P est compact. On conclut que X, étant l'intersection de tous les X_{ab}, est non vide. Il est aussi compact, comme fermé dans le compact P. $\square$

Remarquons que l'hypothèse que l'ordre soit filtrant croissant est cruciale dans la proposition précédente.

Définition 70 (Groupe profini)**.** *Un groupe profini est un groupe topologique qui peut s'écrire comme la limite d'un système projectif de groupes finis discrets.*

Définition 71 (Complété profini)**.** *Soit un groupe G quelconque. Les quotients G/N, où N est un sous-groupe distingué et d'indice fini de G, munis de la topologie discrète, forment un système projectif (indexé par l'ensemble des sous-groupes de ce type, avec l'ordre opposé à l'inclusion) dans* **Grptp***. La limite projective de ce système s'appelle le* ***complété profini*** *de G, et elle est notée $\widehat{G}$.*

Un homomorphisme $f\colon G \to H$ de groupes induit un morphisme $\widehat{f}\colon \widehat{G} \to \widehat{H}$ entre les complétés profinis de la façon suivante. Pour un sous-groupe distingué N dans H, l'application $G/f^{-1}(N) \to H/N$ est injective, donc $f^{-1}(N)$ est un sous-groupe distingué d'ordre fini de G. Les applications $\widehat{G} \to G/f^{-1}(N) \to H/N$ forment un cône du système projectif définissant $\widehat{H}$. Par la propriété universelle, ceci induit une application $\widehat{f}\colon \widehat{G} \to \widehat{H}$.

Désormais le terme *corps* veut dire *corps commutatif*. Si $K|k$ est une extension de corps, on note $\mathrm{Gal}(K|k)$ le groupe d'automorphismes de l'extension, aussi appelé le groupe de Galois. Si H est un sous-groupe de $\mathrm{Gal}(K|k)$, on note $K^H = \{x \in K : \sigma(x) = x,\ \forall \sigma \in H\}$, qui est un sous-corps de K contenant k. On suppose connue la théorie des extensions galoisiennes finies. On peut généraliser la notion pour des extensions algébriques quelconques de la façon suivante.

Définition 72. *Une extension algébrique de corps $K|k$ de groupe de Galois G est dit* ***galoisienne*** *si $K^G = k$.*

Définition 73. *Une clôture algébrique d'un corps k est une extension $\overline{k}$ de k qui est algébriquement clos (c'est-à-dire qui n'admet pas d'extension algébrique non trivial)*

On résume les faits les plus importants des clôtures algébriques dans la proposition suivant.

Proposition 74. *Soit k un corps. Alors, il existe une clôture algébrique $\overline{k}$ de k. Si L est une extension de k et $\overline{L}$ est une clôture algébrique de L, un morphisme d'extensions $L \to \overline{k}$ s'étend en un isomorphisme $\overline{L} \to \overline{k}$.*

Pour la preuve voir [Lang, 1993], corollaire 2.6 et théorème 2.8.

On peut déduire, par exemple avec la proposition 74, les critères suivantes.

Proposition 75. *Une extension algébrique $K|k$ est galoisienne si et seulement si pour tout $x \in K$, le polynôme minimal de x sur k est séparable et a tous ses racines dans K.*

Si k est un corps parfait, une clôture algébrique de k est galoisienne sur k.

Soit $K|k$ une extension de corps galoisienne, et soit Λ l'ensemble des sous-extensions $L|k$ finies et galoisiennes, ordonné par inclusion. On note $G = \mathrm{Gal}(K|k)$. Pour $L \subset M$ dans Λ, on dispose du morphisme $\psi_{LM}\colon \mathrm{Gal}(M|k) \to \mathrm{Gal}(L|k)\colon \sigma \mapsto \sigma|_L$. Le fait que $L|k$ est galoisienne assure que cette application est bien définie. En posant $\psi(L) = \mathrm{Gal}(L|k)$, on définit un système projectif de groupes finis $\psi\colon \Lambda \to \mathbf{Grp}$. On dispose aussi d'un cône (G, c), où $c_L\colon G \to \mathrm{Gal}(L|k)$. En fait, ce cône exprime G comme un groupe profini.

Proposition 76. *Le cône* (G, c) *est la limite projective du système* ψ *défini ci-dessus. En particulier, le groupe de Galois d'une extension galoisienne s'écrit comme un groupe profini et il est naturellement muni d'une topologie, parfois appelée la topologie de Krull.*

Démonstration. Soit (H, d) un autre cône du système. Une fois que l'on arrive à définir le bon morphisme de cônes $f \colon H \to G$, tout est trivial. Pour $h \in H$, on définit $f(h)$ comme l'application

$$f(h) : K \to K : x \mapsto d_L(h)(x), \text{ si } x \in L \in \Lambda$$

On vérifie que $f(h)$ est bien définie. Si $x \in K$, il existe $L \in \Lambda$ avec $x \in L$. En effet, on peut prendre comme L le corps de décomposition dans K du polynôme minimal de x sur k. Supposons maintenant que $x \in L, M$ pour deux $L, M \in \Lambda$. On veut montrer que $d_L(h)(x) = d_M(h)(x)$. Dès que $L \cap M \in \Lambda$, on peut supposer que $L \subset M$. Alors $\psi_{LM} \circ d_M = d_L$, donc $d_L(h) = d_M(h)|_L$ et $d_L(h)(x) = d_M(h)(x)$.

Ainsi, $f(h)$ est bien définie pour tout $h \in H$. Montrons que c'est un automorphisme de $K|k$. Soient $x, y \in K$, et soit $L \in \Lambda$ tel que $x, y \in L$. Alors $f(h)(x+y) = d_L(h)(x+y) = d_L(h)(x) + d_L(h)(y) = f(h)(x) + f(h)(y)$. De même on vérifie $f(h)(x \cdot y) = f(h)(x) \cdot f(h)(y)$, et $f(h)(1) = 1$.

Montrons que f est un morphisme de groupes. Pour $g, h \in H$ et $x \in K$ avec $x \in L \in \Lambda$, on a bien $f(gh)(x) = d_L(gh)(x) = d_L(g)(d_L(h)(x)) = f(g)(f(h)(x))$.

Finalement, on vérifie que f est un morphisme de cônes. Pour cela il faut voir que $c_L \circ f = d_L$, pour tout $L \in \lambda$. Or, pour $h \in H$, on a $c_L(f(h)) = f(h)|_L = d_L$, par définition de f.

□

Même si ce ne sera pas nécessaire pour la suite, il est convenable de mentionner la généralisation du Théorème de Galois au cas des extensions galoisiennes infinies. Il faut juste ajouter le mot « fermé » à la version pour des extensions finies.

Théorème 77 (Krull)**.** *Soit* $K|k$ *une extension galoisienne de corps. On note* $G = Gal(K|k)$ *son groupe de Galois.*

L'application

$$H \mapsto K^H$$

entre l'ensemble des sous-groupes fermés de G *et l'ensemble des sous-extensions de* $K|k$ *est une bijection renversant les inclusions. Son inverse est l'application*

$$L \mapsto Gal(K|L)$$

Pour une sous-extension L*, l'extension* $K|L$ *est toujours galoisienne. D'autre part, l'extension* $L|k$ *est galoisienne si et seulement si* $Gal(K|L)$ *est un sous-groupe distingué de* G*, et dans ce cas, la projection* $G \to Gal(L|k)$ *induit un isomorphisme* $G/Gal(K|L) = Gal(L|k)$*.*

Pour la preuve, voir par exemple [Szamuely, 2009], Theorem 1.2.11.

4 Le groupe de Galois absolu de $\mathbb{C}(t)$

Dans ce chapitre on utilise toute la théorie qu'on a développé pour calculer le groupe de Galois absolu de $\mathbb{C}(t)$, c'est-à-dire le groupe $\mathrm{Gal}(\overline{\mathbb{C}(t)}|\mathbb{C}(t))$, où $\overline{\mathbb{C}(t)}$ est une clôture algébrique de $\mathbb{C}(t)$.

Dans la suite, X est une surface de Riemann compacte, connexe et non vide. Notons $k = \mathcal{M}(X)$ et fixons une clôture algébrique K de k.

4.1 Extension maximale non ramifiée au-dessus de $X \setminus S$

Proposition et définition 78. *Soit $L|k$ une extension finie. Soit p dans $\mathbf{Hol}X$ tel que $\mathbf{\Theta}_X(p)$ est isomorphe à $L|k$. L'ensemble des points de branchement de p ne dépend que de la classe d'isomorphisme de $L|k$ dans $\mathbf{EF}$-k. On l'appelle l'ensemble des* ***points de branchement*** *de $L|k$.*

Démonstration. $\mathbf{\Theta}_X$ est une anti-équivalence de catégories et deux revêtements ramifiés de X isomorphes ont le même ensemble de points de branchement. □

Définition 79 (Catégorie des extensions finies de k non ramifiées au-dessus de $X \setminus S$)**.** *Soit S un sous-ensemble fini de X. On note $\mathbf{EF}$-k-S la catégorie des extensions finies L de k telles que ses points de branchement sont inclus dans S. C'est une sous-catégorie pleine de $\mathbf{EF}$-k, appelée la catégorie des extensions finies de k non ramifiées au-dessus de $X \setminus S$.*

On note $\mathbf{\Theta}_{X,S} : \mathbf{Hol}_S X \to \mathbf{EF}$-$k$-$S$ la restriction du foncteur $\mathbf{\Theta}_X$. C'est une anti-équivalence de catégories. On choisit un quasi-inverse $\mathbf{\Theta}_X^{-1}$ de $\mathbf{\Theta}_X$ et on note $\mathbf{\Theta}_{X,S}^{-1}$ la restriction de $\mathbf{\Theta}_X^{-1}$ à $\mathbf{EF}$-k-S, qui est bien une quasi-inverse de $\mathbf{\Theta}_{X,S}$. On fait cela de telle façon que pour une extension $L|k$ non ramifiée ni au-dessus de $X \setminus S$ ni au-dessus de $X \setminus T$ on ait $\mathbf{\Theta}_{X,S}^{-1}(L) = \mathbf{\Theta}_{X,T}^{-1}(L)$.

Lemme 80. *Soit S un sous-ensemble fini de X.*

(i) Soit $L|k$ une extension dans $\mathbf{EF}$-k-S. Toute sous-extension de L est aussi dans $\mathbf{EF}$-k-S.

(ii) Toute extension $L|k$ dans $\mathbf{EF}$-k-S est contenue dans une extension galoisienne dans $\mathbf{EF}$-k-S.

(iii) Soient L et L' deux extensions finies de k non ramifiées au-dessus de $X \setminus S$ et contenues dans K de k. Alors la composée LL' de L et L' dans K est aussi non-ramifiée au-dessus de $X \setminus S$.

Démonstration. Partie (i). Soit T une sous-extension de L. Soient $p\colon Y \to X$ et $q\colon Z \to X$ des revêtements ramifiés de X tels que $\mathbf{\Theta}_X(p)$ est isomorphe à L et $\mathbf{\Theta}_X(q)$ est isomorphe à T. Le monomorphisme de T dans L induit un morphisme $\varphi\colon Y \to Z$ entre p et q. Il suffit de montrer que si $a \in X$ est un point de branchement de q, alors il est aussi un point de branchement de p. Soit $b \in Z$ un point de ramification de q avec $q(b) = a$, et soit $c \in Y$ tel que $\varphi(c) = b$ (φ est surjective). Soit U un voisinage ouvert de c, alors $\varphi(U)$ est un voisinage ouvert de b, parce que φ est ouverte. Comme b est un point de ramification de q, la restriction $q|_{\varphi(U)}$ n'est pas injective. Comme $q \circ \varphi = p$, la restriction $p|_U$ n'est pas injective non plus. Ceci étant vrai pour tout voisinage ouvert U de c, la seule possibilité est que c soit un point de ramification de p. Alors $a = q(\varphi(c)) = p(c)$ est un point de branchement de p, ce qui conclut.

Partie (ii). On choisit un point $b \in X \setminus S$ et on note $G = \pi_1(X \setminus S, b)$. La composée $\boldsymbol{\mu} = \boldsymbol{\Omega}_{X \setminus S, b} \circ \boldsymbol{\Gamma}_{X,S} \circ \boldsymbol{\Theta}_{X,S}^{-1} \colon \mathbf{EF}\text{-}k\text{-}S \to G\text{-}\mathbf{Ensft}$ est une anti-équivalence de catégories qui préserve degrés et objets galoisiens. Le fait que toute extension dans $\mathbf{EF}$-k-S soit contenue dans une extension galoisienne dans $\mathbf{EF}$-k-S équivaut au fait que pour tout objet A dans G-$\mathbf{Ensft}$ il existe un morphisme $f \colon B \to A$ dans G-$\mathbf{Ensft}$ avec B galoisien. Par la proposition 17 il suffit de montrer que tout sous-groupe H de G d'indice fini contient un sous-groupe N distingué dans G et d'indice fini. On peut prendre $N = \cap_{g \in G} gHg^{-1}$. L'intersection est finie parce que H est d'indice fini. Finalement, N est d'indice fini parce que c'est une intersection finie de sous-groupes d'indice fini.

Partie (iii). Par les parties *(i)* et *(ii)*, on peut supposer que L et L' sont galoisiennes. Le carré des inclusions

$$\begin{tikzcd} L \cap L' \arrow[r] \arrow[d] & L \arrow[d] \\ L' \arrow[r] & LL' \end{tikzcd} \tag{4}$$

est cocartésien [1] dans la catégorie $\mathbf{EF}$-k. Pour montrer que LL' appartient à $\mathbf{EF}$-k-S, il suffit de voir que le carré

$$\begin{tikzcd} L \cap L' \arrow[r] \arrow[d] & L \\ L' & \end{tikzcd} \tag{5}$$

admet un cocône dans $\mathbf{EF}$-k-S. En effet, si c'est le cas, comme le carré 4 est cocartésien, LL' se plonge dans un élément de $\mathbf{EF}$-k-S. La partie *(i)* permet alors de conclure. Par l'anti-équivalence $\boldsymbol{\mu}$, il suffit de montrer que l'image par $\boldsymbol{\mu}$ du diagramme précédent admet un cône dans G-$\mathbf{Ensft}$. Montrons que

1. C'est un argument de théorie de Galois des corps. Avec la correspondance de Galois, on montre que $\#\mathrm{Gal}(L|L \cap L') \cdot \#\mathrm{Gal}(L'|L \cap L') = \#\mathrm{Gal}(LL'|L \cap L')$. Le résultat en découle facilement.

ce dernier est isomorphe à un diagramme de la forme

$$\begin{tikzcd} G/(NN') & G/N \arrow[l] \\ G/N' \arrow[u] & \end{tikzcd}$$

avec N et N' des sous-groupes distingués de G et les flèches étant les projections. Ensuite, le carré commutatif

$$\begin{tikzcd} G/(NN') & G/N \arrow[l] \\ G/N' \arrow[u] & G/(N \cap N') \arrow[l] \arrow[u] \end{tikzcd}$$

convient. Soit Δ la sous-catégorie **EF**-k-S où les objets sont les sous-extensions de K contenues dans L ou dans L' et où les morphismes sont les inclusions. On peut choisir un élément dans chaque $\boldsymbol{\mu}(T)$, $T \in \Delta$, de façon compatible avec les morphismes de $\boldsymbol{\mu}(\Delta)$. Grâce à la proposition 17, ceci nous donne un isomorphisme dans G-**Ensft** entre le diagramme $\boldsymbol{\mu}(\Delta)$ et le diagramme Λ des G-ensembles de la forme G/H, avec H un sous-groupe contenant N ou N', où N et N' sont des sous-groupes distingués de G, $\boldsymbol{\mu}(L)$ correspond à G/N, $\boldsymbol{\mu}(L')$ correspond à G/N', et les morphismes de Λ sont les projections. Dans Δ, tout objet muni de morphismes vers L et L' factorise par $L \cap L'$. La propriété duale dans Λ implique que $\boldsymbol{\mu}(L \cap L')$ correspond à $G/(NN')$, d'où le résultat. □

Proposition et définition 81. *Soit $S \subset X$ fini. On définit K_S comme la composée de toutes les sous-extensions finies de $K|k$ non ramifiées au-dessus de $X \setminus S$. C'est une extension galoisienne (en général infinie) de k et toute sous-extension finie de K_S est non ramifiée au-dessus de $X \setminus S$.*

Démonstration. Par la partie *(iii)* du lemme précédent, K_S est en fait l'*union* de toutes les sous-extensions finies de $K|k$ non ramifiées au-dessus de $X \setminus S$. Par la partie *(ii)* du lemme, K_S est globalement fixé par les automorphismes de K, donc elle est galoisienne. La dernière propriété découle aussi de la partie la partie *(iii)* du lemme. □

4.2 Un système cohérent de points de base

On notera $\beth$ la catégorie où les objets sont les sous-ensembles finis de X et où il y a une flèche pour chaque inclusion. $\beth$ est un ordre filtrant croissant. Soit $\beta :]0,1] \to X$ un chemin injectif dans X. Pour $S \in \beth$, soit $c_S = \frac{1}{2} \min\left(\beta^{-1}(S) \cup \{1\}\right)$ et soit $b_S = \beta(c_S)$. Notons $G_S = \pi_1(X \setminus S, b_S)$ le groupe fondamental basé en b_S. Si $S \subset T$ sont deux éléments de $\beth$, $c_T \leq c_S$, et on a un morphisme $p_{ST}\colon G_T \to G_S$ défini comme la composition

$$G_T = \pi_1(X \setminus T, b_T) \to \pi_1(X \setminus S, b_T) \to \pi_1(X \setminus S, b_S) = G_S$$

Ci-dessus, le premier homomorphisme est induit par l'inclusion $X \setminus T \subset X \setminus S$ et le deuxième est induit par le chemin $\beta|_{[c_T, c_S]}$. Nos choix nous permettent de définir un foncteur $p\colon \beth \to \mathbf{Grp}$ qui à chaque $S \in \beth$ associe le groupe G_S et qui à chaque flèche $S \subset T$ dans $\beth$ associe le morphisme p_{ST}. C'est un système projectif de groupes. Il induit un autre système projectif $\widehat{p}\colon \beth \to \mathbf{Grptp}$ en passant aux complétés profinis des G_S.

Ci-dessous on va montrer que la limite projective $\varprojlim \widehat{p}$ et le groupe de Galois absolu $\mathrm{Gal}(K|k)$ sont isomorphes en tant que groupes topologiques.

4.3 Le groupe de Galois absolu de $\mathcal{M}(X)$

On désignera $\Pi\colon \beth \to \mathbf{Grp}$ le système projectif des groupes $\mathrm{Gal}(K_S|k)$ ($S \in \beth$) où les morphismes sont les homomorphismes restriction.

Proposition 82. *Le groupe de Galois absolu Gal($K|k$) est isomorphe à la limite projective du système Π en tant que groupe topologique.*

Idée de la preuve. Toute sous-extension finie de $K|k$ est incluse dans un des K_S. Ensuite on peut raisonner comme dans la proposition 76. $\square$

Pour un $S \in \beth$, on introduit le foncteur

$$\boldsymbol{\mu}_S = \boldsymbol{\Omega}_{X \setminus S, b_S} \circ \boldsymbol{\Gamma}_{X,S} \circ \boldsymbol{\Theta}_{X,S}^{-1}\colon \mathbf{EF}\text{-}k\text{-}S \to G_S\text{-}\mathbf{Ensft}$$

(voir le paragraphe après la définition 79 pour la définition de $\boldsymbol{\Theta}_{X,S}^{-1}$). Rappelons que pour $S \subset T$ dans $\beth$, l'homomorphisme p_{ST} induit un foncteur $p_{ST}^*\colon G_S\text{-}\mathbf{Ensft} \to G_T\text{-}\mathbf{Ensft}$ (voir la définition 15).

Lemme 83. *Soient $S \subset T$ dans $\beth$. Le carré*

$$\begin{array}{ccc} \mathbf{EF}\text{-}k\text{-}S & \xrightarrow{\boldsymbol{\mu}_S} & G_S\text{-}\mathbf{Ensft} \\ {\scriptstyle i_{ST}}\downarrow & & \downarrow{\scriptstyle p_{ST}^*} \\ \mathbf{EF}\text{-}k\text{-}T & \xrightarrow{\boldsymbol{\mu}_T} & G_T\text{-}\mathbf{Ensft} \end{array}$$

où i_{ST} est l'inclusion, est essentiellement commutatif. C'est-à-dire qu'il existe un isomorphisme naturel η_{ST} entre $\boldsymbol{\mu}_T \circ i_{ST}$ et $p_{ST}^* \circ \boldsymbol{\mu}_S$ (c'est une famille d'applications $\eta_{ST}(L)\colon \boldsymbol{\mu}_T(L) \to \boldsymbol{\mu}_S(L)$, pour $L \in \mathbf{EF}\text{-}k\text{-}S$).

En plus, si $R \subset S$, on a $\eta_{RS}(L) \circ \eta_{ST}(L) = \eta_{RT}(L)$, pour toute L dans $\mathbf{EF}\text{-}k\text{-}R$.

Démonstration. Le carré ci-dessus se décompose en

$$\begin{tikzcd}
\mathbf{EF}\text{-}k\text{-}S \arrow[r, "\mathbf{\Theta}_{X,S}^{-1}"] \arrow[d, "i_{ST}"'] & \mathbf{Hol}_S X \arrow[r, "\mathbf{\Gamma}_{X,S}"] \arrow[d] & \mathbf{Revfc}(X \setminus S) \arrow[r, "\mathbf{\Omega}_{X\setminus S, b_S}"] \arrow[d, "q_{ST}"'] & G_S\text{-}\mathbf{Ensft} \arrow[d, "p_{ST}^*"] \\
\mathbf{EF}\text{-}k\text{-}T \arrow[r, "\mathbf{\Theta}_{X,T}^{-1}"] & \mathbf{Hol}_S X \arrow[r, "\mathbf{\Gamma}_{X,T}"] & \mathbf{Revfc}(X \setminus T) \arrow[r, "\mathbf{\Omega}_{X\setminus T, b_T}"] & G_T\text{-}\mathbf{Ensft}
\end{tikzcd}$$

où q_{ST} envoie chaque revêtement de $X \setminus S$ sur la restriction au-dessus de $X \setminus T$. Le premier carré commute parce que $\mathbf{\Theta}_{X,S}^{-1}$ et $\mathbf{\Theta}_{X,T}^{-1}$ sont des restrictions de $\mathbf{\Theta}_X^{-1}$. Le deuxième carré commute clairement. Il faut juste écrire une équivalence entre $b = \mathbf{\Omega}_{X\setminus T, b_T} \circ q_{TS}$ et $a = p_{TS}^* \circ \mathbf{\Omega}_{X\setminus S, b_S}$. Pour $\varphi \in \mathbf{Revfc}(X \setminus S)$, $a(\varphi) = \varphi^{-1}(b_S)$ et $b(\varphi) = \varphi^{-1}(b_T)$. Le chemin $\beta|_{[c_T, c_S]}$ induit alors une bijection $\varphi^{-1}(b_T) \to \varphi^{-1}(b_S)$ entre les fibres qui convient. La formule $\eta_{RS}(L) \circ \eta_{ST}(L) = \eta_{RT}(L)$ découle du fait que $[\beta|_{[c_T,c_S]}] \cdot [\beta|_{[c_S,c_R]}] = [\beta|_{[c_T,c_R]}]$, où le crochet désigne la classe d'homotopie des chemins. □

Soit $S \in \beth$. Soit Δ_S la catégorie où les objets sont les sous-extensions finies galoisiennes de $K|k$ non ramifiées au-dessus de $X \setminus S$ et où les flèches sont les inclusions. C'est un ordre filtrant croissant d'après le lemme 80. On a un système projectif $\psi_S \colon \Delta_S \to \mathbf{Grp}$ qui à chaque extension L associe le groupe de Galois $\mathrm{Gal}(L|k)$ et qui à une paire d'extensions $L' \subset L$ associe l'homomorphisme restriction $\mathrm{Gal}(L|k) \to \mathrm{Gal}(L'|k)$. Par la proposition 76, le groupe de Galois $\mathrm{Gal}(K_S|k)$ est isomorphe à la limite projective $\varprojlim \psi_S$.

Pour $L \in \Delta_S$, on note N_L^S le stabilisateur de l'action $\boldsymbol{\mu}_S(L)$, qui est un sous-groupe distingué d'indice fini de G_S. L'inclusion de Δ_S dans la sous-catégorie des objets galoisiens de $\mathbf{EF}$-k-S est essentiellement surjective. Comme $\boldsymbol{\mu}_S$ est une anti-équivalence, cela implique que tout sous-groupe distingué d'indice fini de G_S est de la forme N_L^S pour un certain (unique) $L \in \Delta_S$. Pour deux extensions $L' \subset L$, on a l'inclusion $N_L^S \subset N_{L'}^S$. On définit un autre système projectif indexé par Δ_S, $\Upsilon_S \colon \Delta_S \to \mathbf{Grp}$, qui à chaque L associe le groupe G/N_L^S et qui à chaque paire $L' \subset L$ associe la projection $G/N_L^S \to G/N_{L'}^S$.

Lemme 84 (Choix cohérent des représentants)**.** *Pour chaque $S \in \beth$ et $L \in \Delta_S$, on peut choisir un élément $x_{L,S} \in \boldsymbol{\mu}_S(L)$. La famille des $x_{L,S}$ satisfait (avec les notations du lemme précédent) :*

1. *Si $L' \subset L$ sont dans Δ_S, l'application induite $\boldsymbol{\mu}_S(L) \to \boldsymbol{\mu}_S(L')$ envoie $x_{L,S}$ sur $x_{L',S}$.*
2. *Si $L \in \Delta_S$ et $S \subset T$ sont dans $\beth$, alors l'application $\eta_{ST}(L) \colon \boldsymbol{\mu}_S(L) \to \boldsymbol{\mu}_T(L)$ envoie $x_{L,S}$ sur $x_{L,T}$.*

Démonstration. Soit $\daleth$ l'ensemble des couples (L, S) avec $S \in \beth$ et $L \in \Delta_S$. On définit un ordre sur $\daleth$: $(L', S) \leq (L, T)$ si et seulement si $S \subset T$ et $L' \subset L$.

Pour $a = (L', S)$ dans $\daleth$, on pose $\alpha(a) = \boldsymbol{\mu}_S(L)$ en tant que ensemble. Si $b = (L, T)$ est tel que $a \leq b$, on définit $\alpha_{ab} \colon \alpha(b) \to \alpha(a)$ comme la composée

$$\boldsymbol{\mu}_T(L) \to \boldsymbol{\mu}_T(L') \to \boldsymbol{\mu}_S(L')$$

où la première application est l'image par $\boldsymbol{\mu}_T$ de l'inclusion de L' dans L, et la deuxième est $\eta_{ST}(L')$. Le fait que α est un système projectif découle de la fonctorialité des $\boldsymbol{\mu}_S$, du fait que les η_{ST} sont des transformations naturelles et de la compatibilité des η_{ST} au sens de lu lemme précédent. Par la proposition 69, la limite projective de α est non vide. Ceci implique le lemme.

□

Le choix des représentants va nous permettre de définir des isomorphismes entre G_S/N_L^S et $\mathrm{Gal}(L|k)$ qui passent bien à la limite projective (deux fois, comme on verra). On définit

$$v_{L,S} \colon G_S/N_L^S \to \mathrm{Aut}_{G_S\text{-}\mathbf{Ensft}}(\boldsymbol{\mu}_S(L)) \colon g_0 N_L^S \mapsto (g \cdot x_{L,S} \mapsto g g_0 \cdot x_{L,S})$$

C'est un anti-isomorphisme de groupes (voir la preuve de 18). On définit l'isomorphisme $u_{L,S} \colon G_S/N_L^S \to \mathrm{Gal}(L|k)$ comme la composée de $v_{L,S}$ et de l'inverse $w_{L,S}$ de l'anti-isomorphisme $\mathrm{Gal}(L|k) \to \mathrm{Aut}_{G_S\text{-}\mathbf{Ensft}}(\boldsymbol{\mu}_S(L))$ induit par $\boldsymbol{\mu}_S$.

Lemme 85. *Soient $L' \subset L$ dans Δ_S, pour un $S \in \gimel$. Le diagramme suivant est commutatif :*

$$\begin{array}{ccc} G_S/N_L^S & \xrightarrow{u_{L,S}} & \mathit{Gal}(L|k) \\ \downarrow & & \downarrow \\ G_S/N_{L'}^S & \xrightarrow{u_{L',S}} & \mathit{Gal}(L'|k) \end{array}$$

où la flèche verticale à gauche est la projection (rappelons que $N_L^S \subset N_{L'}^S$) et la flèche verticale à droite est l'homomorphisme restriction. Comme conséquence, les systèmes projectifs Υ_S et ψ_S sont isomorphes via la famille d'applications $(u_{L,S})_{L \in \Delta_S}$. Ceci induit un isomorphisme $u_S \colon \widehat{G}_S \to Gal(K_S|k)$ (en tant que groupes profinis).

Démonstration. Regardons le diagramme

$$\begin{array}{ccccc} G_S/N_L^S & \xrightarrow{v_{L,S}} & \mathrm{Aut}(\boldsymbol{\mu}_S(L)) & \xrightarrow{w_{L,S}} & \mathrm{Gal}(L|k) \\ \downarrow & & \downarrow{\scriptstyle\gamma} & & \downarrow \\ G_S/N_{L'}^S & \xrightarrow{v_{L',S}} & \mathrm{Aut}(\boldsymbol{\mu}_S(L')) & \xrightarrow{w_{L',S}} & \mathrm{Gal}(L'|k) \end{array}$$

où γ est est la flèche qui fait le carré a droite commutatif. Il faut montrer que le carré à droite est commutatif. Soit $g_0 \in G$, et soit $\sigma = v_{L,S}(g_0 N_L^S)$, qui est l'automorphisme de $\boldsymbol{\mu}_S(L)$ défini par la formule $\sigma(g \cdot x_{L,S}) = gg_0 \cdot x_{L,S}$. Par définition de γ, le carré

$$\begin{tikzcd} \boldsymbol{\mu}_S(L) \arrow[r, "f"] \arrow[d, "\sigma"'] & \boldsymbol{\mu}_S(L') \arrow[d, "\gamma(\sigma)"] \\ \boldsymbol{\mu}_S(L) \arrow[r, "f"] & \boldsymbol{\mu}_S(L') \end{tikzcd}$$

commute, où f est l'image par $\boldsymbol{\mu}_S$ de l'inclusion de L' dans L. On a

$$\gamma(\sigma)(x_{L',S}) = \gamma(\sigma)(f(x_{L,S})) = f(\sigma(x_{L,S})) = g_0 \cdot x_{L',S}$$

ce qui montre que $\gamma(\sigma) = v_{L',S}(g_0 N^S_{L'})$, d'où le résultat. □

Lemme 86. *Soient $S \subset T$ dans $\beth$ et soit $L \in \Delta_S$. Alors $p_{ST}^{-1}(N_L^S) = N_L^T$ et le carré*

$$\begin{tikzcd} G_T/N_L^T \arrow[r, "u_{L,T}"] \arrow[d] & Gal(L|k) \arrow[d] \\ G_S/N_L^S \arrow[r, "u_{L,S}"] & Gal(L|k) \end{tikzcd}$$

est commutatif. Ci-dessus, la flèche verticale à gauche est induite par p_{ST} et la flèche verticale à droite est l'identité.

Démonstration. Le stabilisateur de $\boldsymbol{\mu}_S(L)$, muni de l'action de G_T induite par $p_{ST} \colon G_T \to G_S$, est $p_{ST}^{-1}(N_L^S)$, tandis que celui de $\boldsymbol{\mu}_T(L)$ est N_L^T. L'existence de l'isomorphisme $\eta_{ST}(L) \colon \boldsymbol{\mu}_T(L) \to \boldsymbol{\mu}_S(L)$ implique alors $p_{ST}^{-1}(N_L^S) = N_L^T$.

À nouveau, on regarde le diagramme plus grand

$$\begin{tikzcd} G_T/N_L^T \arrow[r, "v_{L,T}"] \arrow[d] & \mathrm{Aut}_{G_T\text{-}\mathbf{Ensft}}(\boldsymbol{\mu}_T(L)) \arrow[r, "w_{L,T}"] \arrow[d, "\gamma"] & \mathrm{Gal}(L|k) \arrow[d] \\ G_S/N_L^S \arrow[r, "v_{L,S}"] & \mathrm{Aut}_{G_S\text{-}\mathbf{Ensft}}(\boldsymbol{\mu}_S(L)) \arrow[r, "w_{L,S}"] & \mathrm{Gal}(L|k) \end{tikzcd}$$

où γ est la flèche qui fait que le carré à droite soit commutatif. Montrons que le carré à gauche est aussi commutatif.

Soit $g_0 \in G_T$, et $\sigma = v_{L,T}(g_0 N_L^T)$. Il existe $\widehat{\sigma} \in \mathrm{Gal}(L|k)$ tel que $\sigma = \boldsymbol{\mu}_T(\widehat{\sigma})$. Par définition de γ, $\gamma(\sigma) = \boldsymbol{\mu}_S(\widehat{\sigma})$. Par naturalité de η_{ST}, ceci implique la commutativité du diagramme

$$\begin{tikzcd} \boldsymbol{\mu}_T(L) \arrow[r, "\sigma"] \arrow[d, "\eta_{ST}(L)"'] & \boldsymbol{\mu}_T(L) \arrow[d, "\eta_{ST}(L)"] \\ \boldsymbol{\mu}_S(L) \arrow[r, "\gamma(\sigma)"] & \boldsymbol{\mu}_S(L) \end{tikzcd}$$

Alors, en appelant $f = \eta_{ST}(L)$, on a

$$\gamma(\sigma)(x_{L,S}) = \gamma(\sigma)(f(x_{L,T})) = f(\sigma(x_{L,T})) = f(g_0 \cdot x_{L,T}) = p_{ST}(g_0) \cdot x_{L,S}$$

ce qui montre que $\gamma(\sigma) = v_{L,S}(g_0 N_L^S)$.

□

Lemme 87. *Pour toute paire $S \subset T$ dans $\beth$, le diagramme suivant est commutatif :*

$$\begin{tikzcd} \widehat{G}_T \arrow[r, "u_T"] \arrow[d, "\widehat{p}_{ST}"'] & \mathit{Gal}(K_T|k) \arrow[d] \\ \widehat{G}_S \arrow[r, "u_S"] & \mathit{Gal}(K_S|k) \end{tikzcd}$$

où la flèche verticale à droite est l'homomorphisme restriction.

Démonstration. D'abord, on montre qu'on peut exprimer chaque groupe profini dans le diagramme comme la limite projectif d'un système indexé par Δ_T. On sait déjà que $\widehat{G}_T$ et $\mathrm{Gal}(K_T|k)$ sont la limite des systèmes Υ_T et ψ_T, respectivement, qui sont indexés par Δ_T. D'autre part, $\widehat{G}_S$ et $\mathrm{Gal}(K_S|k)$ sont la limite des systèmes Υ_S et ψ_S, mais ils sont indexés par Δ_S. Cependant, on a un morphisme d'ordres $j\colon \Delta_T \to \Delta_S\colon L \mapsto L \cap K_S$ qui admet une section (l'inclusion de Δ_S dans Δ_T). Par le lemme 68, $\widehat{G}_S$ et $\mathrm{Gal}(K_S|k)$ sont aussi les limites de $\Upsilon'_S = \Upsilon_S \circ j$ et $\psi'_S = \psi_S \circ j$.

On introduit quelques morphismes de systèmes projectifs. Le morphisme $\mathring{p}\colon \psi_T \to \psi'_S$ est donné par les applications $G_T/N_L^T \to G_S/N^S_{L\cap K_S}$ induites par p_{ST}, pour $L \in \Delta_T$ (rappelons que $N_L^T \subset N^T_{L\cap K_S} = p_{ST}^{-1}(N^S_{L\cap K_S})$). Le morphisme $\mathring{r}\colon \psi_T \to \psi'_S$ est donné par les homomorphismes restriction $\mathrm{Gal}(L|k) \to \mathrm{Gal}(L \cap K_S|k)$, pour $L \in \Delta_T$. Le morphisme $\mathring{u}_T : \Upsilon_T \to \psi_T$ est donné par les applications $u_{L,T}$, pour $L \in \Delta_T$. Finalement, le morphisme $\mathring{u}_S\colon \Upsilon'_S \to \psi'_S$, donné par les applications $u_{L\cap K_S,S}$, pour $L \in \Delta_T$.

C'est une vérification simple que le passage à la limite projective du diagramme

$$\begin{tikzcd} \Upsilon_T \arrow[r, "\mathring{u}_T"] \arrow[d, "\mathring{p}"'] & \psi_T \arrow[d, "\mathring{r}"] \\ \Upsilon'_S \arrow[r, "\mathring{u}_S"] & \psi'_S \end{tikzcd}$$

donne le diagramme de l'énoncé du lemme, donc il suffit de montrer que ce dernier est commutatif. Cela équivaut à la commutativité, pour tout $L \in \Delta_T$, du diagramme

$$\begin{tikzcd} G_T/N_L^T \arrow[r, "u_{L,T}"] \arrow[d] & \mathrm{Gal}(L|k) \arrow[d] \\ G_S/N^S_{L\cap K_S} \arrow[r, "u_{L\cap K_S,S}"] & \mathrm{Gal}(L \cap K_S|k) \end{tikzcd}$$

On le décompose en deux carrés comme

$$\begin{tikzcd}
G_T/N_L^T \arrow[r, "u_{L,T}"] \arrow[d] & \mathrm{Gal}(L|k) \arrow[d] \\
G_T/N_{L\cap K_S}^T \arrow[r, "u_{L\cap K_S,T}"] \arrow[d] & \mathrm{Gal}(L\cap K_S|k) \arrow[d] \\
G_S/N_{L\cap K_S}^S \arrow[r, "u_{L\cap K_S,S}"] & \mathrm{Gal}(L\cap K_S|k)
\end{tikzcd}$$

Le premier carré commute par le lemme 85, et le deuxième, par le lemme 86. Ceci conclut.

□

Théorème 88. *La limite projective* $\varprojlim \widehat{G}_S$ *du système* $\widehat{p}$ *est isomorphe, en tant que groupe topologique, au groupe de Galois absolu de* k*, Gal*$(K|k)$*.*

Démonstration. C'est en réalité un corollaire aux résultats de cette section. Par le lemme précédent, la famille des $(u_S)_{S\in\beth}$ est un isomorphisme entre les systèmes projectifs $\widehat{p}$ et Π. La proposition 82 permet de conclure. □

4.4 Le groupe de Galois absolu de $\mathbb{C}(t)$

On commence par introduire la notion de groupe profini libre sur un ensemble.

Définition 89 (Groupe profini libre)**.** *Soit* C *un ensemble. Le groupe profini libre* $\widehat{F}(C)$ *sur* C *est construit de la façon suivante. Soit* Λ *l'ensemble des sous-ensembles finis de* C*, ordonné par inclusion (c'est un ordre filtrant croissant). Pour* $S \in \Lambda$*, on note* $\widehat{F(S)}$ *le complété profini du groupe libre sur* S*,* $F(S)$*. Pour* $S, T \in \Lambda$ *avec* $S \subset T$*, on a un morphisme* $F(T) \to F(S)$ *qui est l'identité sur* S *et qui envoie* $T \setminus S$ *sur l'élément neutre. Cela induit un morphisme* $\widehat{F(T)} \to \widehat{F(S)}$*. Ces morphismes forment un système projectif* δ *indexé par* Λ*. Finalement, on définit* $\widehat{F}(C)$ *comme la limite projective de* δ *(dans la catégorie des groupes topologiques).*

Le groupe $\widehat{F}(C)$ s'écrit aussi comme la limite projective des quotients finis $F(C)/N$ où N est distingué et où la projection $F(C) \to F(C)/N$ se factorise par $F(S)$ pour un $S \in \Lambda$. Ainsi, $\widehat{F}(C)$ est bien un groupe profini. Le groupe $\widehat{F}(C)$ est libre dans un sens qu'on ne précisera pas ici (voir [Douady and Douady, 2005], 6.4.1).

On arrive au résultat principal de ce chapitre.

Théorème 90. *Le groupe de Galois absolu de* $\mathbb{C}(t)$ *est isomorphe au groupe profini libre sur l'ensemble des nombres complexes* $\widehat{F}(\mathbb{C})$*.*

Démonstration. Comme $\mathbb{C}(t)$ s'identifie à $\mathcal{M}(\mathbb{P}^1)$ (voir la proposition 53) on montrera que le groupe de Galois de $\mathcal{M}(\mathbb{P}^1)$ est isomorphe à $\widehat{F}(\mathbb{C})$. Prenons le chemin $\beta\colon]0,1] \to \mathbb{P}^1 : t \mapsto e^{i\pi t}$. On utilisera les notations de cette section avec $X = \mathbb{P}^1$, mais on change légèrement la définition de c_S pour S un sous-ensemble fini de $\mathbb{P}^1$, en posant

$$c_S = \frac{1}{2}\min(\beta^{-1}(S) \cup \beta^{-1}(A) \cup \{1\})$$

où A est l'ensemble des points a de $\beta(]0,1])$ tels qu'il existe une droite réelle dans $\mathbb{C}$ contenant deux points distincts de $S \setminus \{\infty\}$ et a. Comme $\beta(]0,1])$ est contenu dans $\mathbb{S}^1$, A est fini. Comme avant, on a $c_T \leq c_S$ si $S \subset T$, donc cette nouvelle définition ne change pas notre développement postérieur.

Soit Λ l'ensemble des sous-ensembles finis de $\mathbb{C}$, ordonné par inclusion, et soit δ le système projectif décrit à la définition 89. Soit $\Sigma \in \Lambda$ et $S = \Sigma \cup \{\infty\}$. Soit $\varepsilon = \frac{1}{2}\min\{|a-b| : a, b \in \Sigma, a \neq b\}$. Pour $z \in \Sigma$, soit γ_Σ^z le lacet basé en b_S qui va de b_S vers z en droite ligne, s'arrête à distance ε de z, décrit un cercle de rayon ε autour de z dans le sens trigonométrique et revient à b_S en parcourant en sens inverse sa trace. Soit $r_\Sigma\colon F(\Sigma) \to G_S$ l'isomorphisme qui envoie chaque z sur la classe de γ_Σ^z (voir la proposition 28), et soit $\widehat{r}_\Sigma\colon \widehat{F(\Sigma)} \to \widehat{G}_S$ l'isomorphisme induit par passage au complété profini. Grâce à la nouvelle définition de c_S, la famille des $\widehat{r}_\Sigma$ forme un isomorphisme entre les systèmes projectifs δ et $\widehat{p}$ (reindexé par Λ). Ceci nous donne un isomorphisme entre $\widehat{F}(\mathbb{C})$ et $\varprojlim G_S$. Ce dernier est isomorphe au groupe de Galois absolu de $\mathcal{M}(\mathbb{P}^1)$, par le théorème 88. $\square$

Références

[Douady and Douady, 2005] Douady, R. and Douady, A. (2005). *Algèbre et théories galoisiennes*. Cassini, nouvelle bibliothèque mathématique.

[Forster, 1991] Forster, O. (1991). *Lectures on Riemann Surfaces*. Springer.

[Lang, 1993] Lang, S. (1993). *Algebra, third edition*. Addison-Wesley.

[Malle and Matzat, 1999] Malle, G. and Matzat, B. H. (1999). *Inverse Galois Theory*. Springer.

[Rudin, 1987] Rudin, W. (1987). *Real and Complex Analysis*. Mc Graw Hill.

[Szamuely, 2009] Szamuely, T. (2009). *Galois Groups and Fundamental Groups*. Cambridge University Press.