Université de Montréal

PROBLÈME INVERSE DE GALOIS : CRITÈRE DE RIGIDITÉ

par

Amalega Bitondo François

Département de mathématiques et de statistique
Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître ès sciences (M.Sc.)
en Discipline

août 2014

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé

PROBLÈME INVERSE DE GALOIS : CRITÈRE DE RIGIDITÉ

présenté par

Amalega Bitondo François

a été évalué par un jury composé des personnes suivantes :

Prof. Abraham Broer
(directeur de recherche)

Prof. Lalin Matilde
(membre du jury)

Prof. Benabdallah Khalid
(membres du jury)

Mémoire accepté le :
15 septembre 2014

PROBLÈME INVERSE DE GALOIS : CRITÈRE DE RIGIDITÉ.

SOMMAIRE

Dans ce mémoire, on étudie les extensions galoisiennes finies de $\mathbb{C}(x)$. On y démontre le théorème d'existence de Riemann. Les notions de rigidité faible, rigidité et rationalité y sont développées. On y obtient le critère de rigidité qui permet de réaliser certains groupes comme groupes de Galois sur $\mathbb{Q}$. Plusieurs exemples de types de ramification sont construis.

Mots clefs : Type de ramification, revêtements galoisiens, uplet de classes de conjugaison κ-rationnelle.

SUMMARY

In this master thesis we study finite Galois extensions of $\mathbb{C}(x)$. We prove Riemann existence theorem. The notions of rigidity, weak rigidity, and rationality are developed. We obtain the rigidity criterion which enable us to realise some groups as Galois groups over $\mathbb{Q}$. Many examples of ramification types are constructed.

Key words : Ramification type, galois covering, κ-rational tuple of conjugacy classes.

TABLE DES MATIÈRES

Ce mémoire n'aurait pas vu le jour sans la contribution de près ou de loin de plusieurs personnes. Je tiens à remercier premièrement, mon directeur de mémoire Abraham Broer. Ses conseils éclairés ont guidé et façonné mon parcours de maitrise. Je remercie aussi tout le personnel du Département de Mathématiques et Statistiques de l'Université de Montréal pour leurs disponibilités. Et enfin à tous mes camarades et amis sans qui la réalisation de ce projet aurait été très douloureuse, je dis merci.

INTRODUCTION

Une équation algébrique sur un corps k est une équation du type $f(x) = 0$ avec $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in k[x], a_n \neq 0$. Résoudre une telle équation par radicaux revient à déterminer les racines à partir des coéfficients de $f(x)$ en utilisant l'extraction des racines m-ième et les quatre opérations élémentaires (de k). La théorie de Galois nous permet de savoir qu'une telle équation est résoluble par radicaux si et seulement si le groupe de Galois du polynôme $f(x)$ (qui est un groupe fini) est résoluble. Ce résultat d'Evariste Galois (1832) est le point final de longues pérégrinations de plusieurs mathématiciens. Malgré sa beauté ce résultat pose un nouveau défi, le calcul du groupe de Galois d'un polynôme. On peut se poser la question suivante : Tout groupe fini est-il groupe de Galois (sur k) d'un polynôme $f(x) \in k[x]$? C'est le problème inverse de Galois sur le corps k. Si pour un groupe donné G, il existe une extension galoisienne E/k telle que $G = Gal(E/k)$, on dit que G se réalise sur k. Le problème est simple d'énoncer mais reste largement ouvert en particulier pour $k = \mathbb{Q}$.

0.1. Hilbert et le théorème d'irréductibilité.

Hilbert (1892) est le premier à faire une étude systématique de la question. Il démontre le théorème d'irréductibilité de Hilbert et l'utilise pour réaliser S_n et A_n comme groupe de Galois sur $\mathbb{Q}$. Pour énoncer ce théorème, on définit d'abord ce qu'est un corps Hilbertien. Un corps k est dit Hilbertien si pour tous entiers non nuls r, s et pour tout polynôme irréductible $p(t_1, ..., t_r, x_1, ..., x_s) \in k(t_1, ..., t_r)[x_1, ..., x_s]$, il existe une infinité de $(a_1, ..., a_r) \in k^r$ tel que $p(a_1, ..., a_r, x_1, ..., x_s) \in k[x_1, ..., x_s]$ est irréductible. Le théorème d'irréductibilité de Hilbert stipule que le corps $\mathbb{Q}$ est Hilbertien, voir [14, th. 2.2.1 et th. 2.2.4].

Comme conséquence, si G est groupe de Galois d'un polynôme irréductible $p(t, x) \in k(t)[x]$, il existe une infinité de valeurs de $a \in k$ tels que $p(a, x) \in k[x]$ est irréductible et a pour groupe de Galois G lorsque k est Hilbertien, voir [14, prop.

2.2.12]. Ainsi sur les corps Hilbertien, réaliser un groupe sur $k(t)$ nous assure de sa réalisation sur k.
Pour le cas de S_n, on montre que le sous-corps de $k(t_1, ..., t_n)$ fixé par S_n est $k(s_1, ..., s_n)$ où les s_i sont les fonctions symétriques élémentaires en t_i. Par suite $Gal(k(t_1, ..., t_n)/k(t_1, ..., t_n)^{S_n}) = S_n$. En fixant les valeurs de s_i on obtient une réalisation de S_n sur k. S_n peut-être vu comme le groupe de Galois du polynôme $p(x) = x^n + s_1x^{n-1} + ... + s_{n-1}x + s_n$. Son corps de décomposition est $k(t_1, ..., t_n)$.

0.2. Le programme de Noether.

Noether (1918) dans l'article [12] généralise l'approche de Hilbert. Au lieu de S_n, elle considère un groupe fini G quelconque (que l'on peut voir comme un sous-groupe d'un S_n via sa représentation regulière).
Comme $Gal(k(t_1, ..., t_n)/k(t_1, ..., t_n)^G) \cong G$, si $k(t_1, ..., t_n)^G$ est une extension transcendante pure de k, alors G serait groupe de Galois sur k. C'est-à-dire qu'il existe des éléments algébriquement indépendants $x_1, ..., x_r$ tels que $k(t_1, ..., t_n)^G = k(x_1, ..., x_r)$. Malheureusement Swan (1969) a montré qu'il existe des groupes finis pour lesquelles ce n'est pas vrai (voir[15]), même pour quelques groupes cycliques dans leur représentation régulière.

0.3. Les groupes résolubles.

Scholz et Reichardt (1937) ont permis de passer à une étape décisive en montrant que tout p-groupe avec p premier impair est groupe de Galois sur $\mathbb{Q}$. Ceci en considérant plusieurs problèmes de plongements. En utilisant la même approche Shafarevich (1954, 1989) a démontré que tout groupe résoluble est groupe de Galois sur $\mathbb{Q}$, voir [4, page III].

0.4. La rigidité.

Dans l'article [9], Thompson définit et utilise la rigidité pour réaliser le monstre comme groupe de Galois sur $\mathbb{Q}$. La notion de rigidité est apparue pour la première fois de façon implicite dans la thèse de Shih (1974). La notion a ensuite été reprise et developpée de façon indépendante par Fried (1977), Belyi (1979), Matzat (1979) et Thompson (1984). Elle a été utilisée pour réaliser plusieurs groupes comme groupes de Galois sur $\mathbb{Q}$.
Un des résultats important sur lequel s'appuit la rigidité est le fait que tout

groupe fini est groupe de Galois sur $\mathbb{C}(x)$. Ceci est une conséquence du théorème d'existence de Riemann (Théorème 3.2.1), qui établit une correspondance bijective entre les extensions galoisiennes $E/\mathbb{C}(x)$ non ramifiées en dehors d'un nombre fini de points et certains uplets de classes de conjugaison. Pour établir le résultat, on montre que toute extension galoisienne finie $E/\mathbb{C}(x)$ est le corps des fonctions méromorphes d'une surface de Riemann compacte qui elle est issue d'un revêtement $f : X \to \mathbb{P}^1_{\mathbb{C}}$. L'espace totale X hérite de la structure de surface de Riemann compacte de $\mathbb{P}^1_{\mathbb{C}}$ avec un morphisme vers $\mathbb{P}^1_{\mathbb{C}}$. Un point crucial est le fait que le corps des fonctions méromorphes de $\mathbb{P}^1_{\mathbb{C}}$ est $\mathbb{C}(x)$. On peut voir X comme la variété définie par le polynôme minimal d'un élément primitif de $E/\mathbb{C}(x)$.
Après avoir réalisé tous les groupes finis comme groupes de Galois sur $\mathbb{C}(x)$, le reste est un problème de descente sur $\mathbb{Q}(x)$.

0.5. Plan du mémoire.

L'un des objets de ce mémoire est de présenter une preuve du théorème d'existence de Riemann. L'autre est d'étudier le concept de rigidité. La rigidité couplée à la rationalité nous fournissent un critère de descente pour plusieurs familles de groupes finis. Dans le chapitre 1, on étudie les extensions galoisiennes finies de $E/\mathbb{C}(x)$. Ceci nous permet de ressortir la notion de type de ramification d'une extension galoisienne finie de $E/\mathbb{C}(x)$ qui est un triplet $[G, P, (C_p)_{p\in P}]$. G est le groupe de Galois de $E/\mathbb{C}(x)$, P une partie finie de $\mathbb{C}$ (les points de ramification de l'extension) et $(C_p)_{p\in P}$ les classes de conjugaison associées aux éléments de P. Le premier problème est de savoir si à tout type de ramification correspond une extension galoisienne finie. La réponse négative est donnée par le théorème d'existence de Riemann (TER) (Théorème 3.2.1) qui caractérise les types de ramification qui correspondent aux extensions galoisiennes finies de $\mathbb{C}(x)$. Les chapitres 2 et 3 sont donc consacrés à la preuve de ce théorème (théorème d'existence de Riemann (TER)). Au chapitre 2, on considère les revêtements galoisiens de la sphère de Riemann privée d'un nombre fini de points. On y dégage la notion de type de ramification d'un revêtement galoisien fini de la droite projective privée d'un nombre fini de points. Ceci aboutit à la preuve du TER sous sa forme topologique. Dans l'appendice A, certaines notions sur les revêtements et surtout les revêtements galoisiens sont répertoriés. L'appendice A se place dans la progression entre les chapitres 1 et 2. Au chapitre 3, on définit la notion de surface de Riemann. Le TER y est démontré en utilisant les résultats du chapitre 2 et surtout le théorème d'existence de Riemann sous sa forme analytique (proposition 3.1.3). Le théorème d'existence de Riemann (algébrique) établit une correspondance entre certains types de ramification et toutes les extensions galoisiennes finies de $\mathbb{C}(x)$.

Cette correspondance n'est malheureusement pas bijective. La rigidité faible que l'on étudie au chapitre 4, donne une condition sur un type de ramification pour qu'il corresponde à une unique classe d'isomorphisme d'extensions galoisiennes finies.

Au chapitre 4, on définit et étudie les notions de corps de définition, rationalité, rigidité faible et de rigidité. On y énonce et prouve le résultat principal de ce mémoire qui est le critère de rigidité rationnel (théorème 4.3.1).

Les contributions de l'auteur ce situent à deux niveaux. La première est la construction de plusieurs exemples non évidents particulièrement à la section 4.2.1.2, on y a des extensions non isomorphes ayant même type de ramification. Exemple que l'on n'a pu trouver dans la littérature. La deuxième contribution est l'introduction d'une opération sur les types de ramification (le produit direct). On utilise le produit direct de deux types de ramification rigides et κ-rationnels pour réaliser régulièrement un produit direct de groupes comme groupe de Galois sur κ. Ainsi la définition 1.4.1, les propositions 4.1.6, 4.2.3 et le corollaire 4.2.1 sont des résultats que l'auteur n'a trouvé nulle part dans la littérature.

Chapitre 1

TYPE DE RAMIFICATION D'UNE EXTENSION GALOISIENNE FINIE DE $\mathbb{C}(X)$.

On s'intéresse dans ce chapitre aux extensions galoisiennes finies de $\mathbb{C}(x)$. L'objectif est de dégager la notion de type de ramification d'une extension galoisienne finie $E/\mathbb{C}(x)$, qui joue un rôle important dans le problème inverse de Galois. Son importance comme on le verra au chapitre 4, est qu'il permet entre autre d'avoir une condition sur les groupes qui nous permet de savoir s'ils sont groupes de Galois sur un sous corps de $\mathbb{C}$ et en particulier sur $\mathbb{Q}$.

1.1. Théorème de Puiseux (Théorème de Newton).

Soit $E/\mathbb{C}(x)$ une extension galoisienne finie. On sait qu'il existe un élément primitif $\theta(x) \in E$ (c'est-à-dire $E = \mathbb{C}(x)(\theta(x))$) et un polynôme irréductible $F(x, y) \in \mathbb{C}(x)[y]$ tel que $F(x, \theta(x)) = 0$.

Exemple 1.1.1. *$E_0 = \mathbb{C}(x)(\sqrt{x})$ est une extension galoisienne de degré 2 de $\mathbb{C}(x)$ et $\theta(x) = x^{\frac{1}{2}}$ satisfait le polynôme irréductible (sur $\mathbb{C}(x)$) $F(x, y) = y^2 - x$.*
Exemple 1.1.2. *$E_1 = \mathbb{C}(x)([(x-i)(x-1)^3x]^{\frac{1}{4}})$ est une extension galoisienne de degré 4 et $\theta(x) = ((x-i)(x-1)^3x)^{\frac{1}{4}}$ satisfait le polynôme irréductible (sur $\mathbb{C}(x)$) $F(x, y) = y^4 - (x-i)(x-1)^3x$.*

Les exemples ci-dessous suggèrent qu'un élément primitif d'une extension galoisienne $E/\mathbb{C}(x)$ est une fonction de x. Bien qu'on ne puisse pas toujours avoir une expression de $\theta(x)$, on peut envisager un developpement en série entière de $\theta(x)$.

1.1.1. Série de Laurent, Série de Puiseux.

Une série formelle à coéfficients dans $\mathbb{C}$ est une généralisation de la notion de polynôme à coéfficients dans $\mathbb{C}$. La forme générale d'une série formelle est $\sum_{n=0}^{\infty} a_n x^n$ avec $a_n \in \mathbb{C}$ et $n \in \mathbb{N}$. L'ensemble des séries formelles à coéfficients dans $\mathbb{C}$ est noté $\mathbb{C}[[x]]$, c'est un anneau intègre. Son corps des fractions est noté $\mathbb{C}((x))$ et est appelé corps des séries de Laurent. Ses éléments ont la forme générale $\sum_{n=n_0}^{\infty} a_n x^n$ avec $n_0 \in \mathbb{Z}$. Ce sont les séries de Laurent formelles.
En considérant les puissances rationnelles de dénominateur fixe, on a les séries de Puiseux.

Exemple 1.1.3. $\sum_{n=-3}^{\infty} n^2 x^{\frac{n}{5}}$ *est une série de Puiseux. C'est un élément de* $\mathbb{C}((x^{\frac{1}{5}}))$. *Ce sont les séries de Laurent en l'indéterminée* $x^{\frac{1}{5}}$.

1.1.2. Théorème de Puiseux.

Posons $\mathbb{C}((x))^* = \bigcup_{n>0} \mathbb{C}((x^{\frac{1}{n}}))$. On a le théorème de Puiseux suivant dont une preuve constructive se trouve dans [5,th. 3.1 pp 98-102].

Théorème 1.1.1. $\mathbb{C}((x))^*$ *est un corps algébriquement clos.*

Le résultat reste vrai même si l'on remplace $\mathbb{C}$ par un corps algébriquement clos k. Dans le théorème de Puiseux, il y a entre autre le fait intéressant que $\mathbb{C}((x))^*$ qui est une réunion de corps est un corps ce qui n'est pas vrai en général. Dans le cadre de l'étude des éléments primitifs des extensions galoisiennes finies de $\mathbb{C}(x)$ nous allons considérer une partie de ce théorème : le théorème de Newton.

Proposition 1.1.1. *Pour tout polynôme* $F(x,y) \in \mathbb{C}[[x]][y]$ *non constant, il existe un entier* $n > 0$ *tel que* $F(x,y)$ *possède une racine dans* $\mathbb{C}((x^{\frac{1}{n}}))$.

On a aussi :

Proposition 1.1.2. *L'extension* $\mathbb{C}((x^{\frac{1}{n}}))/\mathbb{C}((x))$ *est une extension galoisienne de degré n, son groupe de Galois est cyclique et est engendré par l'élément* ϖ : $\sum_{i\in\mathbb{Z}} b_i x^{\frac{i}{n}} \mapsto \sum_{i\in\mathbb{Z}} b_i.\zeta_n^i x^{\frac{i}{n}}$. *(où* ζ_n *désigne une racine primitive n-ième de l'unité).*

Démonstration. ϖ est un automorphisme de $\mathbb{C}((x^{\frac{1}{n}}))$.

Soit $\sum_{j\in\mathbb{Z}} a_j x^{\frac{j}{n}}$ et $\sum_{j\in\mathbb{Z}} a'_j x^{\frac{j}{n}}$ deux eléments de $\mathbb{C}((x^{\frac{1}{n}}))$,

$\varpi(\sum_{j\in\mathbb{Z}} a_j x^{\frac{j}{n}} + \sum_{j\in\mathbb{Z}} a'_j x^{\frac{j}{n}}) = \varpi(\sum_{j\in\mathbb{Z}}(a_j + a'_j)x^{\frac{j}{n}}) = \sum_{j\in\mathbb{Z}}(a_j + a'_j)\zeta_n^j x^{\frac{j}{n}} = \sum_{j\in\mathbb{Z}}(a_j\zeta_n^j + a'_j\zeta_n^j)x^{\frac{j}{n}} = \sum_{j\in\mathbb{Z}} a_j\zeta_n^j x^{\frac{j}{n}} + \sum_{j\in\mathbb{Z}} a'_j\zeta_n^j x^{\frac{j}{n}} = \varpi(\sum_{j\in\mathbb{Z}} a_j x^{\frac{j}{n}}) + \varpi(\sum_{j\in\mathbb{Z}} a'_j x^{\frac{j}{n}})$
et $\varpi(\sum_{j\in\mathbb{Z}} a_j x^{\frac{j}{n}}.\sum_{j\in\mathbb{Z}} a'_j x^{\frac{j}{n}}) = \varpi(\sum_{j\in\mathbb{Z}}(\sum_{i+s=j} a_i.a'_s)x^{\frac{j}{n}}) = \sum_{j\in\mathbb{Z}}(\sum_{i+s=j} a_i.a'_s)\zeta_n^j x^{\frac{j}{n}} = \sum_{j\in\mathbb{Z}}(\sum_{i+s=j}(a_i\zeta_n^i).(a'_s\zeta_n^s))x^{\frac{j}{n}} = (\sum_{i\in\mathbb{Z}}(a_i\zeta_n^i)x^{\frac{i}{n}})(\sum_{i\in\mathbb{Z}}(a'_s\zeta_n^s)x^{\frac{s}{n}}) = \varpi(\sum_{j\in\mathbb{Z}} a_j x^{\frac{j}{n}})\varpi(\sum_{j\in\mathbb{Z}} a'_j x^{\frac{j}{n}})$.
D'autre part $\varpi(1) = \varpi(\sum_{j\in\mathbb{Z}} b_j x^{\frac{j}{n}}) = \sum_{j\in\mathbb{Z}} b_j\zeta_n^j x^{\frac{j}{n}} = 1$ avec $b_0 = 1$ et $b_j = 0$ pour

tout $j \neq 0$. ϖ est donc un morphisme de corps qui est forcément injectif. Montrons qu'il est surjectif. Considérons la série de puiseux $\sum_{j\in\mathbb{Z}} a_j x^{\frac{j}{n}} \in \mathbb{C}((x^{\frac{j}{n}}))$ posons $b_j = a_j\zeta_n^{-j}$. On a $\sum_{j\in\mathbb{Z}} b_j x^{\frac{j}{n}} \in \mathbb{C}((x^{\frac{j}{n}}))$ et $\varpi(\sum_{j\in\mathbb{Z}} b_j x^{\frac{j}{n}}) = \sum_{j\in\mathbb{Z}} b_j\zeta_n^j x^{\frac{j}{n}} = \sum_{j\in\mathbb{Z}} a_j x^{\frac{j}{n}}$ donc ϖ est surjectif et par suite est un automorphisme de $\mathbb{C}((x^{\frac{1}{n}}))$.

Le corps fixe de ϖ est $\mathbb{C}((x))$.
Soit $\sum_{j\in\mathbb{Z}} a_j x^{\frac{j}{n}} \in \mathbb{C}((x^{\frac{j}{n}}))$ tel que $\varpi(\sum_{j\in\mathbb{Z}} a_j x^{\frac{j}{n}}) = \sum_{j\in\mathbb{Z}} a_j x^{\frac{j}{n}}$.

On a donc $\sum_{j\in\mathbb{Z}} a_j\zeta_n^j x^{\frac{j}{n}} = \sum_{j\in\mathbb{Z}} a_j x^{\frac{j}{n}} \Leftrightarrow a_j\zeta_n^j = a_j$ pour tout $j \in \mathbb{Z} \Leftrightarrow a_j = 0$ ou $\zeta_n^j = 1 \Leftrightarrow a_j = 0$ ou n/j dans ce cas $\sum_{j\in\mathbb{Z}} a_j x^{\frac{j}{n}} \in \mathbb{C}((x))$.

D'après le lemme d'Artin, $\mathbb{C}((x^{\frac{1}{n}}))/\mathbb{C}((x))$ est une extension galoisienne de groupe de Galois $<\varpi>$. Soit $l \in \mathbb{N}^*$, $\varpi^l(\sum_{j\in\mathbb{Z}} a_j x^{\frac{j}{n}}) = (\varpi \circ \underset{l fois}{\ldots} \circ \varpi)(\sum_{j\in\mathbb{Z}} a_j x^{\frac{j}{n}}) = \sum_{j\in\mathbb{Z}} a_j\zeta_n^{jl} x^{\frac{j}{n}}$ ce qui montre que ϖ est un élément d'ordre n.
Par suite $[\mathbb{C}((x^{\frac{1}{n}})) : \mathbb{C}((x))] = n$.

En particulier $\varpi^l(x^{\frac{1}{n}}) = \zeta_n^l x^{\frac{l}{n}}$, pour avoir $\varpi^l(x^{\frac{1}{n}}) = x^{\frac{1}{n}}$, on doit avoir l multiple de n. Le seul élément de $<\varpi>$ qui fixe $x^{\frac{1}{n}}$ est $id = \varpi^0$ par suite $\mathbb{C}((x^{\frac{1}{n}})) = \mathbb{C}((x))(x^{\frac{1}{n}})$.

□

Remarque 1.1.1. *ϖ est appelé le générateur distingué de $Gal(\mathbb{C}((x^{\frac{1}{n}}))/\mathbb{C}((x)))$. Il vérifie $\varpi(x^{\frac{1}{n}}) = \zeta_n x^{\frac{1}{n}}$.*

Grâce à l'inclusion $\mathbb{C}(x) \subset \mathbb{C}((x))$ on peut voir un polynôme $F(x,y) \in \mathbb{C}(x)[y]$ comme polynôme de $\mathbb{C}((x))[y]$ et ses racines comme des éléments de $\mathbb{C}((x^{\frac{1}{n}}))$ pour une valeur de n. Dans le cas où $F(x,y)$ est le polynôme minimal d'un élément primitif d'une extension $E/\mathbb{C}(x)$, cela permet de voir $E/\mathbb{C}(x)$ comme un sous corps d'une extension $\mathbb{C}((x^{\frac{1}{n}}))/\mathbb{C}((x))$(c'est l'objet de la proposition 1.2.1).

Exemple 1.1.4. *Le polynôme $F(x,y) = y^4 - 2x^3y^2 - 4x^5y + x^6 - x^7 \in \mathbb{C}((x))[y]$ a pour racines $\alpha_1(x) = x^{3/2} + x^{7/4}, \alpha_2(x) = x^{3/2} - x^{7/4}, \alpha_3(x) = -x^{3/2} + ix^{7/4}, \alpha_4(x) = -x^{3/2} - ix^{7/4} \in \mathbb{C}((x^{\frac{1}{4}}))$.*

Les racines sont obtenues par le polygone de Newton. Ces racines sont des éléments de $\mathbb{C}((x))^*$ Voir [6, exemple 1, pp 113].

1.2. Points de branchement et classes de conjugaison associées à une extension galoisienne finie.

Définition 1.2.1. *Un système compatible de racines primitives de l'unité dans* $\mathbb{C}$ *est une famille* $(\zeta_n)_{n\in\mathbb{N}}$ *de racines primitives de l'unité telle que pour tout* $n = n'n''$ *on a* $\zeta_n^{n''} = \zeta_{n'}$.

On va considérer comme système de racines primitives de l'unité $\zeta_n = e^{\frac{2\pi i}{n}}$.

Posons $\mathbb{P}^1_{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. Pour $p \in \mathbb{P}^1_{\mathbb{C}}$, on pose $v_p : \mathbb{C}(x) \to \mathbb{C}(t)$, $x \mapsto t + p$ si $p \neq \infty$ et $x \mapsto \frac{1}{t}$ si $p = \infty$. Ceci correspond à remplacer dans une fraction rationnelle de $\mathbb{C}(x)$ la variable x par $t + p$ pour $p \neq \infty$ et x par $\frac{1}{t}$ si $p = \infty$, donc à se ramener à zéro. Dans le cas du polynôme $F(x, y) = y^2 - x \in \mathbb{C}(x)[y]$, on a $F(t + 5, y) = y^2 - t - 5 \in \mathbb{C}(t)[y]$.

Proposition 1.2.1. *Soit* $E/\mathbb{C}(x)$ *une extension galoisienne finie et* $G = Gal(E/\mathbb{C}(x))$. *Soit* $p \in \mathbb{P}^1_{\mathbb{C}}$, *on peut étendre* $v_p : \mathbb{C}(x) \to \mathbb{C}(t)$ *en un isomorphisme* $v : E \to E_v$ *où* E_v *est un sous-corps d'une extension galoisienne finie* L *de* $\mathbb{C}((t))$. *Le groupe* $Gal(L/\mathbb{C}((t)))$ *laisse invariant* E_v. *Posons* $g_v = v^{-1} \circ \varpi \circ v$ *où* ϖ *est le générateur distingué de* $Gal(L/\mathbb{C}((t)))$. *Supposons qu'il existe une autre extension galoisienne finie* L_1 *de* $\mathbb{C}((t))$, *ayant* E_{v_1} *comme sous-corps et* $v_1 : E \to L_{v_1}$ *l'isomorphisme qui prolonge* v_p, *alors* g_{v_1} *et* g_v *sont dans la même classe de conjugaison de* G. *Cette classe de conjugaison ne depend que de* p.

Démonstration. Voir [1, prop. 2.6]. □

A défaut de faire une preuve de la proposition ci-dessous, nous allons en faire un commentaire. Soit $\theta(x) \in E$ un élément primitif de E, en d'autres termes $E = \mathbb{C}(x)(\theta(x))$. On a $E_v = \mathbb{C}(t)(v(\theta(x))) \subset \mathbb{C}((t^{\frac{1}{n_0}})) = L$ pour un certain $n_0 \in \mathbb{N}$(d'après les propositions 1.1.1 et 1.1.2) ($v(\theta(x))$ est une fonction de t). Si on prend un autre élément primitif $\alpha(x)$ de E ($E = \mathbb{C}(x)(\alpha(x))$) alors on aura un autre plongement v_1 de E et $E_{v_1} = \mathbb{C}(t)(v_1(\alpha(x))) \subset \mathbb{C}((t^{\frac{1}{n_1}})) = L_1$ pour un certain $n_1 \in \mathbb{N}$ ($v_1(\alpha(x))$ est une fonction de t). L'inclusion $\mathbb{C}(t)(v(\theta(x))) \subset \mathbb{C}((t^{\frac{1}{n_0}}))$ signifie qu'on à remplacé x par $t + p$ dans $\theta(x)$ et on a fait son développement en série de Puiseux. Comme g_v, g_{v_1} ont même ordre (comme éléments du groupe G et cet ordre est celui de ϖ) alors $n_0 = n_1 = e$. En d'autres termes le dénominateur commun des puissances dans le développement en série de Puiseux d'un élément primitif de E, ne dépend que de p.

Définition 1.2.2. *(1) On appelle classe de $Gal(E/\mathbb{C}(x))$ associée à p la classe de conjugaison de g_v. On la note C_p.*

(2) L'ordre des éléments de C_p est appelé l'indice de ramification de E en p. On le note $e_{E,p}$.

Définition 1.2.3. *Soit $E/\mathbb{C}(x)$ une extension galoisienne finie et $p \in \mathbb{P}^1_{\mathbb{C}}$. On dit que p est un point de branchement (ou un point de ramification) de $E/\mathbb{C}(x)$ si $e_{E,p} > 1$ (en d'autres termes la classe C_p de $Gal(E/\mathbb{C}(x))$ est non triviale).*

La proposition ci-dessous nous montre où chercher les points de ramification distincts de l'infini d'une extension galoisienne finie de $\mathbb{C}(x)$. En particulier elle dit qu'il n'y a qu'un nombre fini de tels points.

Proposition 1.2.2. *On peut choisir un élément primitif $\theta(x)$ de $E/\mathbb{C}(x)$ tel que son polynôme minimal $F(y) = F(x, y) \in \mathbb{C}[x, y]$ soit unitaire en y. Alors le discriminant $D(x)$ de $F(y)$ sur $\mathbb{C}(x)$ est un élément de $\mathbb{C}[x]$. Si $p \in \mathbb{C}$ et $D(p) \neq 0$ alors $e_{E,p} = 1$.*

Démonstration. Voir [1, prop. 2.6]. □

Proposition 1.2.3. *Si $E'/\mathbb{C}(x)$ est une extension galoisienne finie avec $E' \subset E$ (où $E/\mathbb{C}(x)$ est une extension galoisienne finie) alors la restriction des éléments de G en ceux de $G' = Gal(E'/\mathbb{C}(x))$ applique la classe de C_p à la classe de C'_p de G' associée à p.*

Démonstration. Soit $v : E \to E_v$ l'isomorphisme qui prolonge v_p. Alors $v' = v_{/E'}$ est un isomorphisme de E' sur $v'(E') \subset E_v$ qui prolonge v_p. Donc $g_{v'} = (v')^{-1} \circ \varpi \circ v_{/E'} = (g_v)_{/E'}$. □

Pour chaque extension galoisienne finie $E/\mathbb{C}(x)$, on a les trois invariants suivants :

(1) Le groupe de Galois $G = Gal(E/\mathbb{C}(x))$.

(2) Les points de branchement $p \in \mathbb{P}^1_{\mathbb{C}}$.

(3) Les classes de conjugaison C_p.

Exemple 1.2.1. *$E_0 = \mathbb{C}(x)(\sqrt{x})$ son groupe de Galois est $G = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$. Il a deux points de branchement 0 et ∞. La classe associée à 0 est $C_0 = \{-1\}$ et celle associée à ∞ est $C_\infty = \{-1\}$. En effet en 0, le developpement en série de Laurent de $\sqrt{t}$ est $t^{1/2}$. A l'infini on a $t^{-1/2}$ et en $p \neq 0$ on a $\sqrt{t+p}$ est indéfiniment dérivable ce qui va donner un developpement en série entiere et par suite un indice de ramification égal à 1.*

Cet exemple est un cas particulier d'extension cyclique de $\mathbb{C}(x)$, dont on détermine les points de ramification et leur indices comme suit (la justication que l'on peut retrouver dans [1, exemple 2.9 pp 35 et 36] utilise le lemme de Hensel).

Exemple 1.2.2. *Soit $f(x) \in \mathbb{C}(x)$ et $n > 1$.*
Considérons l'extension $E = \mathbb{C}(x)(f(x)^{\frac{1}{n}})$. On peut toujours supposer que $f(x) = \prod_j (x - p_j)^{m_j}$ avec $p_j \in \mathbb{C}$ deux à deux distincts et $0 < m_j < n$ alors

$$e_{E,p_i} = \frac{n}{pgcd(n,m_i)} \text{ et } e_{E,\infty} = \frac{n}{pgcd(n,m)} \text{ où } m = deg(f(x)).$$

En identifiant $g \in G = Gal(E/\mathbb{C}(x))$ avec $g(f^{\frac{1}{n}}).f^{-\frac{1}{n}}$ ($(g(f^{\frac{1}{n}}).f^{-\frac{1}{n}})^n = 1$). Ce qui revient à plonger G dans $< \zeta_n >$ (où ζ_n est une racine primitive d'ordre n de l'unité), on a :

$$C_{p_j} = \{\zeta_n^{m_j}\} \text{ et } C_\infty = \{\zeta_n^{-m}\} \ .$$

De plus $[E : \mathbb{C}(x)] = n$ (équivalent à $y^n - f$ est irréductible dans $\mathbb{C}(x)[y]$) si et seulement si le pgcd de tous les m_j et de n est 1.

Si on l'applique à l'extension $E_1 = \mathbb{C}(x)([(x-i)(x-1)^3 x]^{\frac{1}{4}})$ alors les points de ramification sont $p_1 = i, p_2 = 1, p_3 = 0$ et ∞ . Son groupe de Galois est $G = \mathbb{Z}/4\mathbb{Z}$ et les classes de conjugaison sont $C_{p_1} = \{\zeta_4\}, C_{p_2} = \{\zeta_4^3\}, C_{p_3} = \{\zeta_4\}, C_\infty = \{\zeta_4^{-1}\}$.

1.3. Type de ramification d'une extension galoisienne finie.

Le paragraphe précédent nous amène à considérer la notion de type de ramification d'un groupe.

On s'intéresse aux triplets $(G, P, (C_p)_{p\in P})$ où G est un groupe fini, $P \subset \mathbb{P}^1_{\mathbb{C}}$ une partie finie et $(C_p)_{p\in P}$ une famille de classes de conjugaison de G indicé par P.
On définit la relation (qui est une relation d'équivalence) par :
deux triplets $(G, P, (C_p)_{p\in P})$ et $(G', P', (C'_p)_{p\in P'})$ sont dits équivalents si $P = P'$ et s'il existe un isomorphisme $\varphi : G \to G'$ tel que $\varphi(C_p) = C'_p$.

Définition 1.3.1. *Une classe d'équivalence pour cette relation est appelée un type de ramification. On note $[G, P, (C_p)_{p\in P}]$ le type du triplet $(G, P, (C_p)_{p\in P})$.*

Exemple 1.3.1. *(1) $[\mathbb{Z}/2\mathbb{Z}, \{0, \infty\}, (\{-1\}, \{-1\})]$ est un type de ramification.*

(2) $[\mathbb{Z}/4\mathbb{Z}, \{i, 1, 0, \infty\}, (\{\zeta_4\}, \{\zeta_4^3\}, \{\zeta_4\}, \{\zeta_4^{-1}\})]$ est un type de ramification.

(3) Dans S_n (les classes de conjugaison sont déterminées par les différents types de décompositions en cycles) posons $C^{(i)}$ la classe de conjugaison des

i -cycles de S_n avec $n > 2$ alors $[S_n, \{0, 5, -1\}, (C^{(n-1)}, C^{(2)}, C^{(n)})]$ est un type de ramification.

(4) Considérons le groupe des quaternions $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ avec $i.j = -j.i = k, i^2 = j^2 = -1$. Les classes de conjugaison de Q_8 sont $\{1\}, \{-1\}, C_1 = \{i, -i\}, C_2 = \{j, -j\}, C_3 = \{k, -k\}$. $[Q_8, \{0, 1, 2\}, \{C_1, C_2, C_3\}]$ est un type de ramification.

Définition 1.3.2. *Soit $E/\mathbb{C}(x)$ une extension galoisienne finie. $P \subset \mathbb{P}^1_{\mathbb{C}}$ l'ensemble des points de ramification de $E/\mathbb{C}(x)$. On appelle type de ramification de $E/\mathbb{C}(x)$, le type de ramification du triplet $(G, P, (C_p)_{p\in P})$ où $G = Gal(E/\mathbb{C}(x))$, C_p la classe de conjugaison associée à p.*

Exemple 1.3.2. *(1) $[\mathbb{Z}/2\mathbb{Z} = \{0, 1\}, \{0, \infty\}, (\{-1\}, \{-1\}]$ est le type de ramification de l'extension $E_0 = \mathbb{C}(x)(\sqrt{x})$.*

(2) $(\mathbb{Z}/4\mathbb{Z}, \{i, 1, 0, \infty\}, (\{\zeta_4\}, \{\zeta_4^3\}, \{\zeta_4\}, \{\zeta_4^{-1}\}))$ est le type de ramification de l'extension $E_1 = \mathbb{C}(x)(((x - i)(x - 1)^3 x)^{\frac{1}{4}})$.

La proposition suivante montre l'éffet sur le type de ramification d'une déformation de $\mathbb{C}$ par un automorphisme α de $\mathbb{C}$. Pour une classe de conjugaison C de G et pour un entier m, on pose $C^m = \{g^m | g \in C\}$.

Proposition 1.3.1 (Branch cycle argument)**.** *Soient $E/\mathbb{C}(x), E'/\mathbb{C}(x)$ deux extensions galoisiennes finies de $\mathbb{C}(x)$ de degré n. Pour chaque $p \in \mathbb{P}^1_{\mathbb{C}}$, posons C_p la classe de $G = Gal(E/\mathbb{C}(x))$ associée à p et C'_p la classe de $G' = Gal(E'/\mathbb{C}(x))$ associée à p. Soit α un automorphisme de $\mathbb{C}$ et soit m un entier tel que $\alpha^{-1}(\zeta_n) = \zeta_n^m$. Supposons que α s'étend en un isomorphisme $\lambda : E \to E'$ avec $\lambda(x) = x$. Soit $\lambda^* : Gal(E/\mathbb{C}(x)) \to Gal(E'/\mathbb{C}(x)), g \mapsto \lambda g \lambda^{-1}$ l'isomorphisme induit sur les groupes de Galois. Alors $C'_{\alpha(p)} = \lambda^*(C_p)^m$.*

Démonstration. Voir [1, lemme 2.8]. □

Proposition 1.3.2. *Deux corps $\mathbb{C}(x)$-isomorphes ont même type de ramification.*

Démonstration. Soit $\lambda : E \to E'$ un $\mathbb{C}(x)$-isomorphisme et $\lambda^* : Gal(E/\mathbb{C}(x)) \to Gal(E'/\mathbb{C}(x)), g \mapsto \lambda g \lambda^{-1}$ l'isomorphisme induit sur les groupes de Galois. Posons $[G, P, (C_p)_{p\in P}]$ et $[G', P', (C'_p)_{p\in P'}]$ les types de ramifications respectifs de $E/\mathbb{C}(x)$ et $E'/\mathbb{C}(x)$. D'après le «branch cycle argument» $C'_p = \lambda^*(C_p)$ car λ prolonge l'identité de $\mathbb{C}$. Pour un $p \in \mathbb{C}$ les classes C_p, C'_p ont donc même ordre. Ce qui implique que $P = P'$ et λ^* est l'isomorphisme cherché. □

Remarque 1.3.1. *La reciproque n'est pas vrai, voir chapitre 4 (section 4.1.2).*

1.4. Type de ramification produit direct.

A partir de deux ou plusieurs types de ramification, on aimerait définir un troisième type de ramification. Nous allons dans cette partie nous intéresser au produit direct de types de ramification.

1.4.1. Classes de conjugaison dans un produit direct de groupes.

Soit $(g,h) \in G \times H$. Posons C, K les classes de conjugaison respectives de g et h dans G et H. La proposition ci-dessous nous donne la classe de $(g,h) \in G \times H$ en fonction C et K.

Proposition 1.4.1. *Le produit cartésien $C \times K$ est la classe de conjugaison de (g,h) dans $G \times H$.*

Démonstration. Soit $(g',h') \in G \times H$.

$$(g',h').(g,h).(g',h')^{-1} = (g'gg'^{-1}, h'hh'^{-1}) \in C \times K.$$

Donc la classe de conjugaison de (g,h) est contenue dans $C \times K$.
Soit $(l,t) \in C \times K$, il existe $(g_0,h_0) \in G \times H$ tel que $l = g_0 g g_0^{-1}, t = h_0 h h_0^{-1}$. Ainsi

$$(l,t) = (g_0 g g_0^{-1}, h_0 h h_0^{-1}) = (g_0,h_0).(g,h).(g_0,h_0)^{-1} \in [(g,h)]$$

où $[(g,h)]$ désigne la classe de conjugaison de (g,h). Donc $[(g,h)] = C \times K$. □

1.4.2. Type de ramification produit direct.

Soit $T = [G, P, (C_p)_{p\in P}]$ et $T' = [G', P', (C'_q)_{q\in P'}]$ deux types de ramification. Suppose que $P \cap P' = \emptyset$. On pose $P = \{p_1, ..., p_r\}, P' = \{q_1, ..., q_t\}$.

Définition 1.4.1. *On appelle type de ramification produit direct de T et T' que l'on note $T \times T'$, le type de ramification du triplet $(G \times G', P \cup P', (C_{p_1} \times \{1\}, ..., C_{p_r} \times \{1\}, \{1\} \times C_{q_1}, ..., \{1\} \times C_{q_t})$.*

Chacune des classes $C_{p_1} \times \{1\}, ..., C_{p_r} \times \{1\}, \{1\} \times C_{q_1}, ..., \{1\} \times C_{q_t}$ est associée à un élément de $P \cup P'$ de facon évidente. On peut étendre cette définition à n types de ramification $1 < n$.

Remarque 1.4.1. *Les deux premiers cas dans l'exemple 1.3.1, sont les types de ramification d'extensions galoisiennes finies, mais les deux suivants sont des types de ramification qui ne sont à priori liés à aucune extension galoisienne. On peut donc se poser deux questions :*

(1) Peut-on associer une extension galoisienne finie à tout type de ramification ?

(2) Dans le cas où la réponse est négative, peut-on à partir d'un type de ramification déterminer une condition qui permet de savoir s'il est le type de ramification d'une extension galoisienne finie ?

C'est l'objet des deux chapitres suivants. On verra que la réponse à la première question est négative et le Théorème 3.2.1 nous donnera la condition que doivent satisfaire les types de ramification qui correspondent aux extensions galoisiennes finies.

Remarque 1.4.2. *Dans ce chapitre, nous avons dégagé la notion de type de ramification d'une extension galoisienne finie $E/\mathbb{C}(x)$. Cette notion et les résultats qui lui sont liés restent vraies lorsque l'on remplace $\mathbb{C}$ par un corps algébriquement clos k de caractéristique 0. Dans $\mathbb{C}$ nous avons choisi un système compatible de racines primitives de l'unité (definition 1.2.1). Dans k, on suppose fixé un tel système. Dorénavant la notion de type de ramification d'une extension galoisienne finie $E/k(x)$ où k est un corps algébriquement clos de caractéristique 0 à un sens.*

Chapitre 2

THÉORÈME D'EXISTENCE DE RIEMANN : FORME TOPOLOGIQUE.

Dans ce chapitre on étudie les revêtements galoisiens de la droite projective $\mathbb{P}^1$ privée d'un nombre fini de points. L'étude du comportement de ces revêtements aux voisinages des points manquants de la droite (les trous de la sphère de Riemann) permet de définir le type de ramification d'un revêtement galoisien fini. Le résultat principal qu'on y démontre est la forme topologique du théorème d'existence de Riemann (TER) Théorème 2.2.1. Ce théorème établit une correspondance entre certains types de ramification et tous les revêtements galoisiens fini de la droite projective $\mathbb{P}^1 = \mathbb{P}^1_{\mathbb{C}}$ privée d'un nombre fini de points. Les notions préalables sur les revêtements et les revêtements galoisiens sont developpés dans l'annexe A.

2.1. Revêtements de la droite projective privée d'un nombre fini de points.

2.1.1. Revêtements du disque privé de son centre.

La proposition suivante donne le groupe fondamental de $D^* = D^*(0,1) = \{z \in \mathbb{C} | 0 < |s| < 1\}$. Comme $D^*(0,r)$ pour $r > 0$ est homéomorphe à D^* ces résultats s'étendent aussi à $D^*(0,r)$. Ensuite la proposition suivante montre que les seuls revêtements finis de D^* sont les $f_e : z \mapsto z^e$.

Proposition 2.1.1. *Soit* $\mathbb{H} = \{z \in \mathbb{C} | Re(z) < 0\}$.

(1) L'application $f_\infty : \mathbb{H} \to D^*, z \mapsto exp(z)$ *est un revêtement.*

(2) $Aut(f_\infty)$ *est un groupe cyclique infini et est constitué des applications* $\lambda_m : \mathbb{H} \to \mathbb{H}, z \mapsto z + 2m\pi i$ *avec* $m \in \mathbb{Z}$ *et* f_∞ *est un revêtement galoisien.*

(3) Soit $x \in \mathbb{H}$ *et* $b = f_\infty(x)$. *L'application* $\Phi_x : \pi_1(D^*, b) \to Aut(f_\infty)$ *(de la proposition A.4.7) est un isomorphisme. Il applique la classe* $[\gamma]$ *du*

chemin $\gamma(t) = be^{2\pi it}, t \in [0,1]$ *à l'application* $z \mapsto z - 2\pi i$. *Donc le groupe fondamental* $\pi_1(D^*, b)$ *est cyclique et infini engendré par* $[\gamma]$.

DÉMONSTRATION. (1) On a $f_\infty(z) = f_\infty(z') \Leftrightarrow z' = \lambda_m(z)$, pour un $m \in \mathbb{Z}$. Donc $f_\infty = f_\infty \circ \lambda_m$. De plus f_∞ est une surjection.
Montrons que f_∞ est un revêtement. Soit $z \in \mathbb{H}$ et $b = f_\infty(z) \in D^*$ On a $f'_\infty(z) = f_\infty(z) = b \neq 0$ donc il existe un voisinage ouvert V de z et un voisinage ouvert U de b tel que f_∞ soit un homéomorphisme de V vers U. On peut supposer que V est un disque de rayon < 1 et de centre z. On a $U = f_\infty(V)$. Les $\lambda_m(V)$ sont des disques deux à deux distincts disjoints. De plus $f_\infty : \lambda_m(V) \to U$ et un homéomorphisme pour tout $m \in \mathbb{Z}$ car $f_\infty \circ \lambda_m = f_\infty$. Comme $f^{-1}(U) = \bigcup_{m\in\mathbb{Z}} \lambda_m(V)$ alors U est un voisinage distingué de b donc f_∞ est un revêtement .

(2) Soit $m \in \mathbb{Z}$, λ_m est une bijection de réciproque λ_{-m}, chacune de ces deux applications est holomorphe donc ouverte par suite λ_m est un homéomorphisme de plus $f_\infty = f_\infty \circ \lambda_m$ donc $\lambda_m \in Aut(f_\infty)$ Comme $\{\lambda_m, m \in \mathbb{Z}\}$ permute transitivement $f^{-1}(\{b\})$ alors $\{\lambda_m, m \in \mathbb{Z}\} = Aut(f_\infty)$ d'après la proposition A.4.6 -(2). Comme $\mathbb{H}$ est connexe par arcs alors f_∞ est un revêtement galoisien.

(3) Soit $[\gamma] \in ker(\Phi_x)$,$([\gamma]x = x)$ δ se relève en un lacet $\widetilde{\delta}$ ayant comme point initial x, comme $\mathbb{H}$ est étoilé par n'importe lequel de ses points alors $\pi_1(B, b) = \{1\}$, donc $\widetilde{\delta}$ est homotope au chemin constant basé en x par suite $f_\infty \circ \widetilde{\delta} = \delta$ est homotope au chemin constant basé en $b = f_\infty(x)$. Donc Φ_x est injectif et donc un isomorphisme.
Soit $\widetilde{\gamma}$ le chemin de $\mathbb{H}$ defini par $\widetilde{\gamma}(t) = x + 2\pi it, t \in I$. Alors $f_\infty \circ \widetilde{\gamma}$ est le chemin de la proposition. Donc $f_\infty \circ \widetilde{\gamma} = \gamma$ d'où $[\gamma]x = \widetilde{\gamma}(1) = x + 2\pi i$. Par définition de Φ_x on sait que l'automorphisme $\Phi_x([\gamma])$ applique $[\gamma]x = x + 2\pi i$ à x. Donc $\Phi_x([\gamma])$ est la transformation de deck $z \mapsto z - 2\pi i, (m = -1)$ comme λ_1 engendre $Aut(f_\infty)$, alors $[\gamma]$ engendre $\pi_1(D^*, b)$.

□

On a donc que $\pi_1(D^*, b) \cong \mathbb{Z}$.

Dans le premier annexe nous avons vu que $f_e : D^*(0, r^{\frac{1}{e}}) \to D^*(0, r), z \mapsto z^e$ est un revêtement galoisien, la proposition suivante énonce que c'est le seul revêtement galoisien (à équivalence près) de degré e de $D^*(0, r)$.

Proposition 2.1.2. *Soit* $f : X \to D^*(0, r)$ *un revêtement fini de degré* e *avec* X *connexe par arcs.*

(1) f est équivalent au revêtement $f_e : D^*(0, r^{\frac{1}{e}}) \to D^*(0, r), z \mapsto z^e$. Il existe donc un homéomorphisme $\chi : X \to D^*(0, r^{\frac{1}{e}})$ avec $\chi(x)^e = f(x)$ pour tout $x \in E$ (on écrit $\chi^e = f$). Ce χ est unique à multiplication près par une racine e -ième ς de 1, cet-à-dire si χ' à la même propriété alors $\chi' = \varsigma\chi$, pour une racine e -ième ς de 1.

(2) Le groupe $Aut(f)$ est cyclique d'ordre e. Il a un unique élément σ ayant la propriété suivante : Pour chaque $\chi : X \to D^*(0, r^{\frac{1}{e}})$ vérifiant $\chi^e = f$, on a $\chi \circ \sigma^{-1} = \varsigma_e\chi$ avec ς_e une racine primitive de l'unité. Ce σ engendre $Aut(f)$ et est appelé générateur distingué.

(3) Soit $x \in X, b = f(x)$. Considérons le σ du (2). Alors $\gamma(t) = b.exp(2\pi it), t \in [0, 1]$ est un chemin fermé dans $D^*(0, r)$ basé en b, et son relèvement ayant pour point initial $\sigma(x)$ a pour extrémité x.

(4) Soit $0 < r' < r, X' = f^{-1}(D^*(0, r'))$ et $f' = f_{|X'}$. Alors X' est connexe par arcs et $f' : X' \to D^*(0, r')$ est un revêment de degré e. De plus le générateur distingué de $Aut(f')$ est la restriction à X' de celui de $Aut(f)$.

Démonstration. Voir [1, cor. 4.22]. □

2.1.2. Revêtements de la droite projective privée d'un nombre fini de points.

Soit $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$ la droite projective complexe. Soit $P \subset \mathbb{P}^1$ un ensemble fini de points. On se propose d'étudier les revêtements galoisiens finis de $\mathbb{P}^1 - P$. Soit $f : X \to \mathbb{P}^1 - P$ un revêtement galoisien fini connexe par arcs. Soit $p \in P$, on pose $\Gamma = \{z \in \mathbb{C} | \, |z - p| < r\} = D(p, r)$ le disque de centre p et de rayon r tel que $\Gamma \cap P = \{p\}$, on dit que $r > 0$ est suffisamment petit. Donc $\Gamma - \{p\} = \Gamma^* \subset \mathbb{P}^1 - P$. Posons aussi $s_p : \Gamma^* \to D^*(0, r)$, l'homéomorphisme définie par $z \mapsto z - p$ si $p \neq \infty$ et $z \mapsto \frac{1}{z}$ si $p = \infty$ (Dans le cas où $p = \infty$, Γ est en fait le complémentaire d'un disque centré en 0).

Proposition 2.1.3. *Pour chaque composante connexe par arcs C de $f^{-1}(\Gamma^*)$ l'application $f_C = s_p \circ f_{|C}$ est un revêtement $f_C : C \to D^*(0, r)$ de degré fini.*

Démonstration. Comme Γ^* est un ouvert de $\mathbb{P}^1 - P$ alors la restriction de f à $f^{-1}(\Gamma^*)$ est un revêtement de Γ^* d'après la proposition A.1.2 du premier annexe. En composant avec l'homéomorphisme $s_p : \Gamma^* \to D^*(0, r)$, on a un revêtement $f^{-1}(\Gamma^*) \to D^*(0, r)$. Et d'après la proposition A.2.2, la restriction de ce revêtement à une composante connexe C de $f^{-1}(\Gamma^*)$ est un revêtement qui est de degré fini car f l'est.

□

Définition 2.1.1. *C de la proposition ci-dessus est appelé une composante circulaire de niveau r de f au dessus de p.*

Proposition 2.1.4. *Soit $0 < r' < r$. Il y a une correspondance bijective entre les composantes circulaires C de niveau r et les composantes circulaires C' de niveau r' donné par l'inclusion. Si $C' \subset C$ alors $f_{C'}$ est la restriction de f_C à C' et $C' = f_C^{-1}(D^*(0, r'))$.*

Démonstration. Soit $X' = f^{-1}(D(p, r') - \{p\})$, $\widetilde{C} = f_C^{-1}(D^*(0, r')) = C \cap X'$ est connexe par arcs d'après la proposition 2.1.2-(4). $\widetilde{C}$ est ouvert et fermé dans X' c'est donc une composante connexe de X. $\widetilde{C}$ est donc une composante circulaire de niveau r' contenue dans C.
Soit $C' \subset C$ une composante circulaire de niveau r' au dessus de p contenue dans C. Alors $f_{C'} = f_{C|C'}$ donc $C' \subset f_C^{-1}(D^*(0, r')) = f_C^{-1}(D^*(0, r'))$. Donc $f_C^{-1}(D^*(0, r')) = C$ car ce sont des composantes connexes, ce qui prouve que chaque composante circulaire de niveau r contient exactement une composante circulaire de niveau r'. Inversement chaque composante circulaire de niveau r' de f au dessus de p est contenue dans $f^{-1}(\Gamma^*)$ il est donc dans un C.(car sinon on pourra l'écrire comme réunion disjointe d'ouverts non vide).

□

Proposition 2.1.5. *Le groupe $G = Aut(f)$ permute transitivement les composantes circulaires C de $f^{-1}(\Gamma^*)$. Posons G_C le stabilisateur de C dans G. La restriction de l'action de G_C à C fournie un isomorphisme $G_C \to Aut(f_C)$. Ainsi G_C est cyclique. Soit $h_C \in G_C$ l'élément correspondant au générateur distingué de $Aut(f_C)$. h_C est appelé générateur distingué de G_C.*

Démonstration. Le groupe G opère sur $f^{-1}(\Gamma^*)$ car pour tout $\chi \in G$, $f \circ \chi = f$ donc si $x \in f^{-1}(\Gamma^*)$ alors $f(\chi(x)) = f(x) \in \Gamma^*$ donc $\chi(x) \in f^{-1}(\Gamma^*)$. Comme G opère sur $f^{-1}(\Gamma^*)$ alors il permute les composantes connexes par arcs de $f^{-1}(\Gamma^*)$. Comme les composantes connexes par arcs sont disjointes, si $\chi \in G$ transforme un point de C en un point de C alors $\chi \in G_C$. Soit $p^* \in \Gamma^*$ l'ensemble $K_C = f^{-1}(\{p^*\}) \cap C$ est une fibre du revêtement f_C. Comme G agit transitivement sur $f^{-1}(\{p^*\})$ alors pour deux points quelconques de K_C il existe un automorphisme $\chi \in G$ qui applique l'un sur l'autre, mais comme les deux points sont dans C alors $\chi \in G_C$. Donc G_C opère transitivement sur K_C. La restriction $G_C \to Aut(f_C)$ est un morphisme de groupes. Ce morphisme est injectif. Comme G_C opère transitivement sur $f^{-1}(\{p^*\})$ alors d'après la proposition A.4.6, $G_C = Aut(f_C)$ (l'injection $G_C \to Aut(f_C)$ fait de G_C un sous groupe

de $Aut(f_C)$). Comme G opère transitivement sur chaque fibre $f^{-1}(\{p^*\})$ et que $f^{-1}(\{p^*\}) \cap C \neq \emptyset$ alors G permute transitivement les C.

□

Proposition 2.1.6. *(1) Soit $\chi \in Aut(f)$ et $C' = \chi(C)$. Alors $\chi \circ h_C \circ \chi^{-1} = h_{C'}$. Les h_C forment une classe de conjugaison C_p de $Aut(f)$. La classe C_p ne dépend que de p et est invariante par le rayon de Γ. Soit e l'ordre commun des éléments de C_p. Alors e est égal au degré du revêtement $f_C : C \to D^*(0,r)$, pour tout C de $f^{-1}(\Gamma^*)$. En particulier, $C_p = \{1\}$ si et seulement si f_C est un isomorphisme.*

(2) Soit $p^* \in \Gamma^*$ et $\overline{p} = s_p(p^*)$. Posons $\lambda(t) = s_p^{-1}(\overline{p}.exp(2\pi it))$ un lacet de Γ^* basé en p^*. Soit $x \in X, q_0 = f(x)$, δ un chemin de $\mathbb{P}^1 - P$ joignant q_0 à p^*. Alors $\gamma = \overline{\delta}\lambda\delta$ est un lacet en q_0, et l'application $\Phi_x : \pi_1(\mathbb{P}^1 - P, q_0) \to Aut(f)$ envoie $[\gamma]$ sur un élément de la classe C_p.

Démonstration. (1) (Preuve du deuxième point.) Le relèvement $\widetilde{\delta}$ de δ via f ayant pour point initial x à son extrémité x^* dans une composante connexe par arcs $C \subset f^{-1}(\Gamma^*)$ car $x^* \in f^{-1}(\{p^*\})$. Soit $\widetilde{\lambda}$ le relèvement de λ via f ayant pour point initial $h_C(x^*)$. Donc $\widetilde{\lambda}$ est égal au relevé du chemin $\overline{p}.exp(2\pi it)$ via f_C, ayant pour point initial $h_C(x^*)$. L'extrémité de $\widetilde{\lambda}$ est x^*. Le chemin $h_C \circ \widetilde{\delta}$ est le relèvement de δ via f ayant pour point initial $h_C(x)$ (son extrémité est $h_C(x^*)$). Donc $\overline{\widetilde{\delta}}\widetilde{\lambda}(h_C \circ \widetilde{\delta})$ est le relèvement de γ ayant pour point initial $h_C(x)$. Son extrémité est x. Donc $\Phi_x([\gamma])([\gamma]h_C(x)) = h_C(x)$ d'ou $\Phi_x([\gamma])(x) = h_C(x)$ car $[\gamma]h_C(x) = x$ ainsi $\Phi_x([\gamma]) = h_C \in C_p$.

(2) (Preuve du premier point.) Soit $\chi \in G$, $\chi \circ \widetilde{\lambda}$ est un relèvement de λ via f de point initial $\chi(h_C(x^*)) \in \chi(C) = C'$. Le chemin $\chi \circ \widetilde{\lambda}$ a pour extrémité $\chi(x^*)$ comme dans le 2) ci-dessus $h_{C'}$ applique l'extrémité de $\chi \circ \widetilde{\lambda}$ a son point initial donc $h_{C'}(\chi(x^*)) = \chi(h_C(x^*))$. Ainsi $h_C^{-1} \circ \chi^{-1} \circ h_{C'} \circ \chi$ fixe x^*, c'est donc l'identité d'après la proposition A.4.6. d'où $h_{C'} = \chi \circ h_C \circ \chi^{-1}$. Lorsque $C' \subset C$, on a $h_{C'} = h_C$. Donc la classe C_p ne dépend pas du rayon r du disque Γ. On $e = deg(f_C)$ car h_C engendre $G_C \cong Aut(f_C$ qui est cyclique d'ordre e. Si $C_p = \{1\}$ alors $e = 1$ et f_C est équivalent à $f_1 : z \mapsto z$qui est un homéomorphisme alors c'est un revêtement de degré 1 car toutes ses fibres ont un seul élément par suite $e = 1, C_p = \{1\}$.

□

On fixe un point $p \in P$, on définit une relation parmi les composantes circulaires au dessus de p de niveau suffisamment petit.

$$C\mathfrak{R}C' \Leftrightarrow C \subset C' \text{ou } C' \subset C$$

Ceci definit une relation d'équivalence par la proposition 2.1.4.

Définition 2.1.2. *Une classe d'équivalence de cette relation est appelée point idéal de $f : X \to \mathbb{P}^1 - P$ au dessus de p.*

Un point idéal de X au dessus de p correspond à une classe d'équivalence de composantes circulaires au dessus de p. Si on se fixe un r suffisamment petit, on voit que le nombre de points idéaux correspond au nombre de composantes circulaires de niveau r. L'action de $Aut(f)$ permute transitivement les composantes circulaires de niveau r donc il y a au plus $|Aut(f)| = deg(f)$ points idéaux. Les composantes circulaires sont homéomorphes à un disque privé de son centre par la proposition 2.1.2. Un point idéal apparaît comme le centre manquant du disque. On se propose maintenant de fermer les trous causés par les éléments de P sur $\mathbb{P}^1$.

Soit $f : X \to \mathbb{P}^1 - P$ un revêtement galoisien fini. Posons S l'ensemble de tous les points idéaux au dessus de tous les $p \in P$. On pose $\overline{X} = X \cup S$.

Topologie sur $\overline{X}$.

Considérons les parties $V \subset \overline{X}$ qui ont la propriété α suivante :

$V \cap X$ est un ouvert de X et pour tout point idéal $m \in V$, il existe une composante connexe circulaire de $C \in m$ tel que $C \subset V$.

Posons $O = \{V \subset \overline{X} | V \text{a la propriété } \alpha\}$.

Proposition 2.1.7. *O est l'ensemble des ouverts d'une topologie sur $\overline{X}$ qui coincide avec la topologie de X. De plus pour chaque point idéal $m \in \overline{X}$ et pour chaque composante circulaire $C \in m$, $C \cup \{m\}$ est un ouvert de $\overline{X}$ qui contient m. Cette topologie est séparée au sens de Hausdorff. De plus X est dense dans $\overline{X}$.*

Démonstration. O est l'ensemble des ouverts d'une topologie.

$\emptyset$ et $\overline{X}$ vérifient la propriété α, ils sont donc dans O. Soit $(V_i)_{i\in I}$ une famille quelconque d'éléments de O. $(\bigcup_{i\in I} V_i) \cap X = \bigcup_{i\in I}(V_i \cap X)$ est un ouvert de X car chaque $V_i \cap X$ est un ouvert de X. Soit $m \in \bigcup_{i\in I} V_i$ alors il existe $i_0 \in I$ tel que $m \in V_{i_0}$ comme V_{i_0} a la propriété α il existe $C \in m$ tel que $C \subset V_{i_0}$ par suite $C \subset \bigcup_{i\in I} V_i$ d'où ${}_{i\in I}V_i$ possède la propriété α.

Soit $(V_i)_{i\in\{1,...,n\}}$ une famille finie d'éléments de O. $(\bigcap_{i=1}^{i=n} V_i) \cap X = \bigcap_{i=1}^{i=n}(V_i \cap X)$ est un ouvert de X car chaque $V_i \cap X$ est un ouvert de X.

Soit $m \in \bigcup_{i=1}^{i=n} V_i$, on a $m \in V_i$ pour tout $i \in \{1, ..., n\}$ il existe $C_i \in m$ composante circulaire tel que $C_i \subset V_i$ alors $\bigcup_{i=1}^{i=n} C_i$ est une composante circulaire de niveau $r_0 = \min r_i$ où r_i est le niveau de C_i et on a $\bigcap_{i=1}^{i=n} C_i \subset \bigcap_{i=1}^{i=n} V_i$ donc $\bigcap_{i=1}^{i=n} V_i \in O$.

Donc O est l'ensemble des ouverts d'une topologie. Elle coincide avec celle de X car $V \cap X$ est un ouvert de X pour tout $V \in O$. De plus $C \cup \{m\}$ possède la propriété α pour tout $m \in \overline{X}$ et $C \in m$.

La topologie de O est séparée.
Soit $(x, y) \in \overline{X}^2$ avec $x \neq y$.
Si $(x, y) \in X^2$ alors cela découle du fait que X est séparée et des ouverts de X sont aussi des ouverts de $\overline{X}$.
Si x, y sont deux points idéaux distincts au dessus de p_1 et p_2 respectivement. Soit $C_x \in x, C_y \in y$ deux composantes circulaires de niveau r, si $p_1 \neq p_2$, on a $D^*(p_1, r) \cap D^*(p_2, r) = \emptyset$ car r est suffisament petit d'autre part $C_x \subset f^{-1}(D^*(p_1, r)), C_y \subset f^{-1}(D^*(p_2, r))$ donc $C_x \cap C_y = \emptyset$ par suite $(C_x \cup \{x\}) \cap (C_y \cup \{y\}) = \emptyset$. Si $p_1 = p_2$ alors on sait que C_x n'est pas inclus dans C_y et C_y n'est pas inclus dans C_x car sinon on aurait $x = y$, mais ce sont des composantes connexes de $f^{-1}(D^*(p_1, r))$ donc $C_x \cap C_y = \emptyset$.
Si x est un point idéal (au dessus de p)et $y \in X$. On a $f(y) \in \mathbb{P}^1 - P$ donc $p \neq f(y)$. Il existe $r > 0$ tel que $D(p, r) \cap D(f(y), r) = \emptyset$, on peut en plus choisir r suffisamment petit donc $y \in f^{-1}(D^*(p, r))$ pour n'importe quelle composante circulaire de niveau r, C_x au dessus de p, on a $(\{x\} \cup C_x) \cap f^{-1}(D(f(y), r)) = \emptyset$ or $\{x\} \cup C_x$ et $f^{-1}(D(f(y), r))$ sont des voisinages de x et y respectivement dans $\overline{X}$ la toplogie est donc séparée. Comme tout ouvert de $\overline{X}$ rencontre X alors X est dense dans $\overline{X}$. □

Proposition 2.1.8. *(1) Le revêtement f s'étend en une application surjective et continue $\overline{f} : \overline{X} \to \mathbb{P}^1$ avec $\overline{f}(m) = p$ pour tout point idéal m au dessus de $p \in P$.*

(2) Tout $\chi \in Aut(f)$ s'étend de manière unique en un homéomorphisme $\overline{\chi} : \overline{X} \to \overline{X}$ avec $\overline{f} \circ \overline{\chi} = \overline{f}$.

(3) $\overline{X}$ est un espace compact et connexe par arcs.

Démonstration. (1) $\overline{f}$ est surjective.

Comme $f : X \to \mathbb{P}^1 - P$ est surjective, il en est de même de $\overline{f} : \overline{X} \to \mathbb{P}^1$ car les antécédents des points de P sont les points idéaux.

$\overline{f}$ est continue.

Soit O un ouvert de $\mathbb{P}^1$, si $O \cap P = \emptyset$ alors $\overline{f}^{-1}(O) = f^{-1}(O)$ qui est un ouvert de X donc de $\overline{X}$ car f est continue. Si $O \cap P \neq \emptyset$, comme P est un

ensemble fini, on peut supposer que O ne possède qu'un point de $p \in P$ et on peut le choisir sous la forme $D(p,r)$ avec r suffisamment petit. Posons $m_1, ..., m_t$ les points idéaux au dessus de p et $C_1, ..., C_t$ les composantes circulaires de niveau r au dessus de p. On a $\overline{f}^{-1}(D(p,r)) = \bigcup_{i=1}^{i=t}(C_i \cup \{m_i\})$, comme $C_i \cup \{m_i\}$ est un ouvert de $\overline{X}$, il en est de même de $\overline{f}^{-1}(D(p,r))$ donc $\overline{f}$ est continue.

(2) Soit $\chi \in Aut(f)$, soit $p \in P$, $C_1, ..., C_t$ les composantes circulaires au dessus de p et $m_1, ..., m_t$ les points idéaux associées. χ permute les C_i, on pose $\overline{\chi}(m_j) = m_k$ si $\chi(C_j) = C_k$.

$\overline{\chi} : \overline{X} \to \overline{X}$ est une bijection. En effet $\overline{\chi}_{|X} = \chi$ qui est une bijection. Sur $\{m_1, ..., m_t\}$, $\overline{\chi}(m_i) = \overline{\chi}(m_j) \Leftrightarrow \chi(C_i) = \chi(C_j) \Leftrightarrow C_i = C_j$ car χ est une bijection et les C_i sont des composantes connexes par arcs.

On a $f \circ \chi = f$ donc sur X, $\overline{f} \circ \overline{\chi} = \overline{f}$ sur les points idéaux comme ils sont permutés au dessus d'un point. On peut donc se restreindre à $\{m_1, ..., m_t\}$. On a $\overline{f}(m_i) = \overline{f}(m_j) = p$ pour tout $i, j \in \{1, ..., t\}$. Si $m_k = \overline{\chi}(m_j)$ on aura $\overline{f}(m_j) = (\overline{f} o \overline{\chi})(m_j)$ ce qui induit $\overline{f} \circ \overline{\chi} = \overline{f}$ sur $\overline{X}$.

Comme $\chi : X \to X$ est un homéomorphisme et $\overline{\chi} : \overline{X} \to \overline{X}$ est une bijection il suffit de s'intéresser aux voisinages du type $C_i \cup \{m_i\}$. Or $\overline{\chi}(C_i \cup \{m_i\}) = C_j\{m_j\}$ avec $\overline{\chi}(m_i) = m_j$ donc $\overline{\chi}$ est ouverte sur $\overline{X}$ et par suite $\overline{\chi}$ est un homéorphisme car son inverse (qui est aussi du 'même type') est ouverte.
Supposons qu'il existe un autre homéomorphisme $\overline{\chi}' : \overline{X} \to \overline{X}$ tel que $\overline{\chi}'_X = \overline{\chi}_X = \chi$. On aura $\overline{\chi}' \circ \overline{\chi}^{-1} : \overline{X} \to \overline{X}$ est un homéomorphisme, de plus $(\overline{\chi}' \circ \overline{\chi}^{-1})_{/X} = id_X (= \chi \circ \chi^{-1})$ pour tout $y \in \overline{X}$ on a $y = lim_{n\to\infty} y_n$ avec $y_n \in X$ donc $(\overline{\chi}' \circ \overline{\chi}^{-1})(y) = lim_{n\to\infty}(\overline{\chi}' \circ \overline{\chi}^{-1})(y_n)$ car $\overline{\chi}' \circ \overline{\chi}^{-1}$ est continue. Par suite $(\overline{\chi}' \circ \overline{\chi}^{-1})(y) = lim_{n\to\infty} y_n = y$ d'où $\overline{\chi}' \circ \overline{\chi}^{-1} = id_{\overline{X}}$ et $\overline{\chi}' = \overline{\chi}$.

(3) Comme X est connexe par arcs alors $\overline{X}$ est connexe par arcs.
Montrons que $\overline{X}$ est compact. Pour cela nous allons d'abord montrer que $\overline{X}$ est à base dénombrable d'ouverts et ensuite on montrera que toute suite de $\overline{X}$ a une limite. Considérons les voisinages admissibles de la forme $U = D(q,r) \subset \mathbb{P}^1 - P$ avec $q \in \mathbb{Q}$ (ou $q = \infty$), $r \in \mathbb{Q}$. Prenons toutes les composantes connexes de $f^{-1}(U)$ en plus des ouverts du type $C_i \cup \{m_i\}$ avec le niveau de C_i un $r \in \mathbb{Q}$ suffisamment petit. Cette collection forme

une base dénombrable d'ouverts de $\overline{X}$. Soit $(a_n)_{n\in\mathbb{N}}$ une suite de $\overline{X}$. Alors $(\overline{f}(a_n))_{n\in\mathbb{N}}$ est une suite de $\mathbb{P}^1$ qui a donc une limite car $\mathbb{P}^1$ est compact et à base dénombrable de voisinage. On a deux cas : 1) $p \in P$ et 2) $p \notin P$.

(a) Si $p \in P$.
Soit $m_1, ..., m_t$ les points idéaux au dessus de p alors la limite de $(a_n)_{n\in\mathbb{N}}$ est l'un des m_i. Supposons le contraire. Donc aucun des m_i n'est la limite de $(a_n)_{n\in\mathbb{N}}$, chaque m_i possède un voisinage $C_i \cup \{m_i\}$ qui ne contient aucun des a_n on peut supposer que tous les C_i ont le même niveau r (en prenant $r = \min r_i$ où r_i est le niveau de C_i). On a $f^{-1}(D(p,r)) = \bigcup_{i=1}^{i=t}(C_i \cup \{m_i\})$ qui ne contient aucun a_n. Par suite $D(p,r)$ ne contient aucun $f(a_n)$ ce qui est absurde.

(b) Si $p \notin P$.
Posons $f^{-1}(\{p\}) = \{x_1, ..., x_t\}$ ($f^{-1}(\{p\})$ est fini car le revêtement est fini).Soit U un voisinage ouvert admissible de p on a $f^{-1}(U) = \bigcup_{i=1}^{i=t} V_i$ on suppose que l'on a ordonné les V_i de telle sorte que $x_i \in V_i$. La suite $(a_n)_{n\in\mathbb{N}}$ converge vers l'un des x_i. Supposons le contraire donc chaque x_i posse un voisinage V_i' qui n'a aucun a_n. Posons $V_i'' = V_i' \cap V_i$, V_i'' est un voisinage ouvert de x_i qui ne contient aucun a_n. Comme $f_{/V_i} : V_i \to U$ est un homéomorphisme alors $p \in f(V_i'') \subset U$ est un ouvert de U et donc de $\mathbb{P}^1 - P$. Posons $U_0 = \bigcap_{i=1}^{i=t} f(V_i'')$, $p \in U_0$ est un ouvert de $\mathbb{P}^1 - P$ et $U_0 \subset U$ de plus $f^{-1}(U_0) \subset \bigcup_{i=1}^{i=t} V_i$ il ne contient donc aucun a_n d'ou U_0 ne contient aucun $f(a_n)$ ce qui est absurde car $lim_{n\to\infty} f(a_n) = p$.

□

2.1.3. Groupe fondamental de la droite projective privée d'un nombre fini de points.

Soit $p_1, ..., p_n \in \mathbb{C}$, $n(\geq 1)$ points distincts. Posons $B = \mathbb{C} - \{p_1, ..., p_n\}$. Soit $q_0 \in B$ tel que les demi-droites $[q_0 p_k)$ ne contiennent aucun p_l pour tout $l \neq k$. On suppose $p_k = q_0 + \rho_k \exp(iv_k)$ avec $\rho_k \in \mathbb{R}_+, 0 \leq v_k < 2\pi$ (pour $k = 1, ..., n$). On suppose de plus que $v_1 > v_2 > ... > v_n$. La disposition que l'on a donné aux p_k a les conséquences suivantes lorsqu'on se déplace dans le sens des aiguilles d'une montre, on rencontre les p_k dans l'ordre suivant $p_1, ..., p_n$ et en plus aucune demi-droites $[Op_k)$ ne contient un autre p_t ($t \neq k$).

On prend des demi-droites d'origine q_0, $M_1, ..., M_n$ dans $\mathbb{C}$ telles que les composantes connexes de $\mathbb{C} - \{M_1, ..., M_n\}$ contiennent exactement un p_k. Soit S_k la composante connexe qui contient p_k, $q_0 \notin S_k$ et la frontière de S_k est constituée de certains M_j. Soit D_k un disque autour de p_k dont l'adhérence est contenue

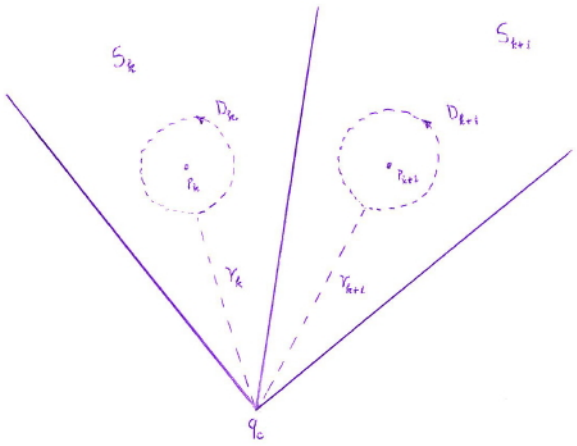

FIGURE 2.1

dans S_k. On pose γ_k le chemin $S_k \cup \{q_0\}$ qui va de q_0 vers p_k jusqu'à la frontière de D_k (en suivant une portion du segment $[q_0p_k]$) et tourne une fois autour de cette frontière dans le sens contraire des aiguilles d'une montre et rentre à q_0 en suivant la même portion du segment $[q_0p_k]$. Voir Figure 2.1.

Proposition 2.1.9. *Les classes des chemins (lacets basés en q_0) $\gamma_1, ..., \gamma_n$ engendrent $\pi_1(B, q_0)$.*

DÉMONSTRATION. Posons $S'_k = \{z \in \mathbb{C} | d(z, S_k) < \epsilon\}$ (on élargie un peu S_k d'un $\epsilon > 0$, sans qu'il ne contienne un autre p_t). On a $S_k \subset S'_k, q_0 \in S'_k$ et deux des M_j sont contenues dans S'_k et il est convexe. On a $\mathbb{C} = \bigcup_{k=1}^{k=n} S'_k$ donc $B = \bigcup_{k=1}^{k=n}(S'_k - \{p_k\})$. Soit γ un lacet de B basé en q_0 alors γ est homotope au produit de δ_μ ($\mu = 1, ..., s$) avec chaque δ_μ contenu dans un $T_\mu = S'_{j_\mu} - \{p_{j_\mu}\}$ (d'après le lemme ci-dessous). Supposons de plus que l'on parcoure les δ_μ dans l'ordre $\delta_1, \delta_2, ...$

Soit k_μ le chemin (segment) qui joint q_0 au point initial de δ_μ. Par convexité $k_\mu([0, 1]) \subset T_\mu \cap k_{\mu-1}$ pour tout $\mu > 1$ (on peut choisir δ_μ de tel sorte qu'il ne rencontre pas p_{j_μ}. Ainsi k_μ est un chemin de $T_\mu \cap k_{\mu-1}$. On pose k_{s+1} le chemin constant en q_0. Soit $\omega_\mu = \overline{k_{\mu+1}}\delta_\mu k_\mu$ pour $\mu = 1, ..., s$. ω_μ est un lacet basé en q_0 contenu dans T_μ et γ est homotope au produit des ω_μ qui est le produit des δ_μ. L'espace T_μ est homéomorphe au disque $D^*(0, 1)$ dont le groupe fondamental est engendré le chemin γ_{j_μ} d'après la proposition 2.1.1. Donc il existe $m \in \mathbb{Z}$ tel que $[\omega_\mu] = [\gamma_{j_\mu}]^m$, comme $[\gamma] = [\omega_1]...[\omega_s]$ alors $[\gamma]$ est le produit des $[\gamma_j]$. D'où $\pi_1(B, q_0)$ est engendré par les classes de γ_j.

□

Lemme 2.1.1. *Soit $(X_j)_{j\in J}$ une famille d'ouverts d'un espace topologique X tel que $X = \bigcup_{j\in J} X_j$. Chaque chemin δ de X est homotope au produit d'un nombre fini de chemins δ_μ tel que δ_μ est un chemin dans l'un des X_j.*

Démonstration. $\delta^{-1}(X_j)$ est un ouvert de I donc est une réunion dénombrable d'intervalles ouverts (les intervalles ouverts forment une base dénombrable d'ouverts de $[0,1]$). La réunion de tous les intervalles qui recouvrent $\delta^{-1}(X_j)$ pour tout les j recouvre $I = [0,1]$. Comme I est compact on peut recouvrir I avec un nombre fini de telles intervalles notons les $I_1, ..., I_s$. Supposons que s est minimal cet-à-dire qu'aucun I_μ n'est contenu dans la réunion des autres. Supposons de plus que l'on a ordonné les I_μ de tel sorte que $inf(I_\mu) < inf(I_{\mu+1})$ pour tout $\mu = 1, ..., s-1$. On a $I_\mu \cap I_{\mu+1} \neq \emptyset$. Soit $t_\mu \in I_\mu \cap I_{\mu+1}$ avec $t_0 = 0, t_s = 1$. Alors l'intervalle $[t_\mu, t_{\mu+1}] \subset I_{\mu+1}$. Ainsi $\delta([t_\mu, t_{\mu+1}])$ est contenu dans un X_i. Soit $\theta_\mu : [0,1] \to [t_\mu, t_{\mu+1}]$ un homéomorphisme alors $\delta_\mu = \delta \circ \theta_\mu$ est un chemin contenu dans X_i et $[\delta] = [\delta_1 .... \delta_s]$. □

2.1.4. Revêtement ayant un groupe d'automorphismes isomorphe à un groupe finiment engendré donné G.

Dans $B = \mathbb{C} - \{p_1, ..., p_n\}$, on considère la demi-droite L_k porté par la droite $(q_0 p_k)$ d'origine p_k et ne contenant pas p_k ne contenant pas q_0. On pose $Q = B - (L_1 \cup L_2 \cup ... \cup L_n)$, Q est connexe par arcs. Voir figure 2.2.

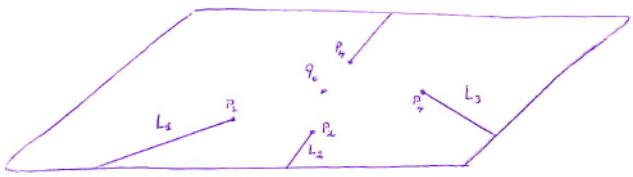

Figure 2.2

Soit G un groupe engendré par n éléments distincts $g_1, ..., g_n$. Posons $X = B \times G$ (on a des copies de B paramétrées par G).

Topologie sur X.

On va définir sur X une topologie en précisant pour chaque point une base de voisinage. Soit $(q, g) \in X$. On a deux cas $q \in Q$ ou $q \notin Q$.

(1) Si $q \in Q$, un voisinage de (q, g) est $D \times \{g\}$ où D est un disque de centre q contenu dans Q.

(2) Si $q \notin Q$, donc $q \in L_k$ pour un certain $k \in \{1, ..., n\}$. Avant de construire un voisinage de (q, g), on va pour un disque D centré en q et ne rencontrant aucun autre L_j pour $j \neq k$ le séparé en deux demi-disques. Voir figure 2.3.

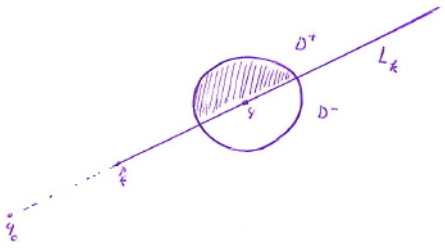

FIGURE 2.3

D^+ est le demi-disque ouvert constitué des points p tel que pour aller de (q_0p_k) à (q_0p), on effectue une rotation d'un angle θ avec $0 \leq \theta < \frac{\pi}{2}$.
D^- est l'autre demi-disque fermé. Un voisinage de (q, g) est $\hat{D}_g = (D^- \times \{g\}) \cup (D^+ \times \{gg_k^{-1}\}$. En réalité un voisange de (q, g) a une partie dans $B \times \{g\}$ et l'autre dans $B \times \{gg_k^{-1}\}$ avec k correspondant à L_k tel que $q \in L_k$.

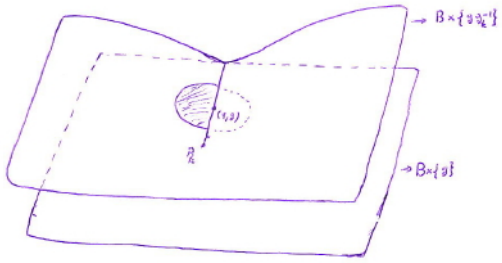

FIGURE 2.4

donc les copies $B \times \{g\}$ et $B \times \{gg_k^{-1}\}$ sont donc collées au travers de L_k. Ceci peut se faire pour $..., gg_k^2, gg_k, g, gg_k^{-1}, gg_k^{-2}, ...$ toutes ces copies sont jointes entre elles.

Tels que défini, pour deux voisinages quelconques de (q, g) l'un est dans l'autre. Et ils forment une base de voisinage de (q, g).

Proposition 2.1.10. *L'application $f : X \to B, (q, g) \mapsto q$ est un revêtement.*

DÉMONSTRATION. Soit $q \in Q$ et D un disque ouvert avec $D \subset Q$, on a $f^{-1}(D) = \bigcup_{g \in G} D \times \{g\}$ par définition de f. Si $q \in L_k$ pour un certain k, $f^{-1}(D) = \bigcup_{g \in G} \hat{D}_g$ donc f est continue et de plus chaque $D \times \{g\}$ où $\hat{D}_g$ sont des ouverts de X homéomorphes à D donc D est un voisinage distingué de q et par suite f est un revêtement.

□

Proposition 2.1.11. *Soit $h \in G$, on pose $\alpha_h : X \to X, (q,g) \to (q,hg)$, α_h est un automorphisme de f et de plus $\alpha_h \circ \alpha_{h'} = \alpha_{hh'}$.*

DÉMONSTRATION. Il est claire que l'on a $\alpha_h \circ \alpha_{h'} = \alpha_{hh'}$. Donc α_h est une bijection d'inverse $\alpha_{h^{-1}}$ pour tout $h \in G$. Chaque α_h est une application ouverte car $\alpha_h(D \times \{g\}) = D \times \{hg\}$ et $\alpha(\hat{D}_g) = \hat{D}_{hg}$ donc α_h est un homéomorphisme de X. De plus $(f \circ \alpha_h)((q,g)) = f(q,hg) = q = f(q,g)$ donc $f \circ \alpha_h = f$ et par suite $\alpha_h \in Aut(f)$. □

Proposition 2.1.12. *L'application $f : X \to B$ est un revêtement galoisien et $Aut(f) \cong G$.*

DÉMONSTRATION. Montrons que X est connexe par arcs.
Chaque copies $Q \times \{g\}$ est homéomorphe à Q par f donc $Q \times \{g\}$ est connexe par arcs car Q l'est. Soit C la composante connexe par arcs de X contenant $Q \times \{1\}$. Soit D un disque ouvert de centre $q \in L_k$. On a $\hat{D}_1 = (D^- \times \{1\}) \cup (D^+ \times \{g_k^{-1}\}$ $(g = 1)$. Soit $a_0 \in D^-$ et $a_1 \in D^+$, posons $s : [0,1] \to D \subset B$ un chemin tel que $\gamma(0) = a_0, \gamma(1) = a_1$ et tel que s rencontre L_k en un unique point en t_k.

$$\varrho(t) = \begin{cases} (s(t),1) & si \quad t \leq t_k \\ (s(t), g_k^{-1}) & si \quad t > t_k \end{cases}$$

$f_{/\hat{D}_1} : \hat{D}_1 \to D$ est un homéomorphisme et $\varrho(t) = ((f_{/\hat{D}_1})^{-1} \circ s)(t)$ donc ϱ est continue. De plus $\varrho(0) = (a_0,1) \in Q \times \{1\}$ et $\varrho(1) = (a_1, g_k^{-1}) \in Q \times \{g_k^{-1}\}$. Donc $Q \times \{g_k^{-1}\} \subset C$. Comme $\alpha_{g_k^{-1}}$ applique $Q \times \{1\}$ à $Q \times \{g_k^{-1}\}$ alors α_g fixe C pour tout $g \in G$ (car les g_k engendrent G). Donc C contient tous les $Q \times \{g\}$ or $\overline{Q} = B$ donc $\overline{Q \times \{g\}} = B \times \{g\}$. Par suite $\bigcup_{g \in G} \overline{Q \times \{g\}} \subset \overline{C} = C$ d'où $\bigcup_{g \in G} B \times \{g\} = C = X$.

Montrons que $Aut(f) \cong G$. L'ensemble $\{\alpha_g, g \in G\} \subset Aut(f)$ et il permute transitivement chaque fibre $f^{-1}(\{b\}), b \in B$ donc $G \cong \{\alpha_g, g \in G\} = Aut(f)$ d'après la proposition A.4.6.

□

Proposition 2.1.13. *Le relèvement de γ_k ayant comme point initial $(q_0,1)$ a pour extrémité (q_0, g_k^{-1}).*

DÉMONSTRATION. Le chemin γ_k rencontre L_k en un seul point pour tout $t = t_k$. Posons

$$\tilde{\gamma}_k(t) = \begin{cases} (\gamma_k(t),1) & si \quad t \leq t_k \\ (\gamma_k(t), g_k^{-1}) & si \quad t > t_k \end{cases}$$

$\tilde{\gamma}_k$ est continue et $f \circ \tilde{\gamma}_k = \gamma_k$, d'autre part $\tilde{\gamma}_k(0) = (\gamma_k(0), 1) = (q_0, 1)$ et $\tilde{\gamma}_k(1) = (\gamma_k(1), 1) = (q_0, g_k^{-1})$. □

Proposition 2.1.14. *Posons $x = (q_0, 1)$, $\Phi_x([\gamma_k]) = g_k$ pour tout $k \in \{1, ..., n\}$. Donc $g_k \in C_k$ la classe de conjugaison de $G = Aut(f)$ associée à p_k.*

Démonstration. Par définition de Φ_x (proposition A.4.7), $\Phi_x([\gamma_k])$ applique l'extrémité (q_0, g_k^{-1}) de $\tilde{\gamma}_k$ à son origine $(q_0, 1)$ donc $\Phi_x([\gamma_k]) = g_k (= \alpha_{g_k})$. Le chemin γ_k possède la propriété de γ de la proposition 2.1.6 donc $\Phi_x([\gamma_k]) \in C_{p_k}$. □

Proposition 2.1.15. *Soit $\rho > 0$ suffisamment grand pour contenir q_0 et tous les p_k dans le cercle K_0 et de centre O(zéro) et de rayon $\rho > 0$. Alors le chemin $\gamma_\infty = \gamma_1 ... \gamma_n$ est homotope dans B au chemin γ' qui va de q_0 en suivant une ligne droite jusqu'à K_0, se déplace sur K_0 dans le sens contraire des auiguilles d'une montre et revient à q_0.*

Démonstration. Soit D un disque ouvert de centre q_0 qui contient tous les p_k. Posons $S_k^* = S_k \cap D$ et γ_k^* le chemin dont l'image est la fontière de S_k^* (parcouru dans le sens contraire des aiguilles d'une montre) allant de q_0 à q_0. γ_k et γ_* sont homotopes. Donc γ_∞ est homotope à $\gamma_1^* ... \gamma_n^*$. Or $\gamma_1^* ... \gamma_n^*$ est homotopes dans B au chemin γ^* qui va de q_0 à la frontière de D par une ligne droite parcours cette frontière (dans le sens trigonométrique) et revient à q_0 par ce même chemin (les autres chemins inverses s'annulent puisqu'ils viennent l'un après l'autre) γ^* et γ' sont homotopes, par suite γ_∞ est homotope à γ'. □

Proposition 2.1.16. $(g_1 ... g_n)^{-1} \in C_\infty$.

Démonstration. Posons $p = \infty$, alors $B - D$ est un voisinage de $p = \infty$ de plus $\gamma = \overline{\gamma'}$ à la propriété de γ dans la proposition 2.1.6. Donc $\Phi_x([\gamma_\infty]) = \Phi_x([\overline{\gamma'}]) = g_1 ... g_n$ d'après les propositions 2.1.13 et 2.1.14. □

On a le résultat suivant :

Proposition 2.1.17. *Pour tout groupe G ayant $g_1, ..., g_n$ comme générateurs. Il existe un revêtement galoisien $f : Y \to B = \mathbb{C} - \{p_1, ..., p_n\}$ et un isomorphisme $\theta : Aut(f) \to G$ et un point $x_0 \in f^{-1}(\{q_0\})$ tel que $(\Phi_{x_0} \circ \theta)([\gamma_k]) = g_k$ pour tout $k = 1, ..., n$. De plus si G est fini $f : Y \to \mathbb{P}^1 - \{p_1, ..., p_n, \infty\}$ est un revêtement galoisien fini et les classes de conjugaisons $C_{p_1}, ..., C_{p_n}, C_\infty$ de G associée à f vérifient $g_k \in C_{p_k}, (g_1 ... g_n)^{-1} \in C_\infty$ pour tout $k \in \{1, ..., n\}$.*

Démonstration. Ceci découle directement des propositions 2.1.10 à 2.1.15. □

2.2. Type de ramification d'un revêtement galoisien fini.

Soit $f : X \to \mathbb{P}^1 - P$ un revêtement galoisien fini avec $P \subset \mathbb{P}^1$ une partie finie. Pour chaque $p \in P$, on a défini à la proposition 2.1.6 une classe de conjugaison C_p de $Aut(f)$.

Définition 2.2.1. *On dit que $p \in P$ est un point de ramification ou une place de branchement de f si $C_p \neq \{1\}$.*

On a donc un nombre fini de tels points.

Définition 2.2.2. *Soit $P' \subset P$, l'ensemble des places de ramification du rêvement f. On appelle type de ramification du revêment galoisien fini f, le type de ramification du triplet $(Aut(f), P', (C_p)_{p\in P'})$.*

Étudions ce qui se produit sur le type de ramification d'un revêtement lorsque l'on bouge les éléments de $\mathbb{P}^1 - P$ par un homéomorphisme $g : \mathbb{P}^1 \to \mathbb{P}^1$. On a la proposition suivante :

Proposition 2.2.1. *Soit $f : X \to \mathbb{P}^1 - P$ un revêtement et $g : \mathbb{P}^1 \to \mathbb{P}^1$ un homéomorphisme. Le type de ramification de $g \circ f$ est celui de f.*

Démonstration. Soit $p \in P$ et γ un chemin comme dans la proposition 2.1.6-(2) autour de p et $x \in f^{-1}(\{q_0\})$ où q_0 est l'origine de γ, on a $\Phi_x([\gamma]) \in C_p$ (où $\Phi_x : \pi(\mathbb{P}^1 - P, q_0) \to Aut(f)$). $\gamma_1 = g \circ \gamma$ à la propriété du chemin de la proposition 2.1.6 -(2) autour de $g(p)$ donc $\Phi_x([\gamma]) \in C_{g(p)}$ (où $\Phi_x : \pi(\mathbb{P}^1 - P, q_0) \to Aut(g \circ f)$). Le relèvement $\widetilde{\gamma}$ de γ d'origine x via f est aussi le relèvement de γ_1 d'origine x via $g \circ f$ de plus $Aut(f) = Aut(g \circ f)$ (par la remarque A.4.1 - (2)) donc les classes C_p et $C_{g(p)}$ de $Aut(f)$ ont un même $\Phi_x([\gamma])$ et sont donc égales. Ce qui donne $C_{g(p)} = C_p$.

□

Dans la preuve du théorème, on va supposer que $\infty \in P$. Ce qui est toujours possible par l'usage des homéomorphismes $z \mapsto z - p_0$ et $z \mapsto \frac{1}{z}, 0 \mapsto \infty, \infty \mapsto 0$.

Théorème 2.2.1 (Théorème d'existence de Riemann : Forme topologique)**.** *Soit $\mathfrak{T} = [G, P, (K_p)_{p\in P}]$ un type de ramification. Soit $r = |P|$, on pose $p_1, ..., p_r$ les éléments de P. Il existe un revêtement galoisien (de $\mathbb{P}^1$ privée des éléments de P)de type $\mathfrak{T}$ si et seulement si il existe des générateurs $g_1, ..., g_r$ de G avec $g_1....g_r = 1$ et $g_i \in K_{p_i}$ pour tout $i \in \{1, ..., r\}$.*

Démonstration. ($\Leftarrow$) Soit $\mathfrak{T} = [G, P, (K_p)_{p\in P}]$ un type de ramification qui vérifie les conditions du théorème, on veut construire un revêtement qui a pour type $\mathfrak{T}$. Si $r = 1$ le résultat est immédiat car alors $G = \{1\}$. On suppose $r > 1$ posons

$n = r - 1$ et posons $p_r = \infty$ d'après la proposition 2.1.17, il existe un revêtement fini $f : X \to \mathbb{P}^1 - P$ tel que $G \cong Aut(f), g_i \in K_{p_i}$ et $g_r = (g_1...g_{r-1})^{-1} \in K_{p_r}$ d'où f a $\mathfrak{T}$ comme type de ramification.

($\Rightarrow$) Supposons que $f : X \to \mathbb{P}^1 - P$ est un revêtement ayant comme type de ramification $\mathfrak{T}$. On doit montrer que $g_1....g_r = 1$ et les $g_1, ..., g_r$ engendrent G. On a $G = Aut(f)$. Posons $B = \mathbb{P}^1 - P, n = r - 1$ et $q_0 \in B$, on prend des chemins $\gamma_1, ..., \gamma_n$ comme a la proposition 2.1.9, posons $\gamma_r = (\gamma_1...\gamma_{r-1})^{-1}$. Soit $x \in f^{-1}(\{q_0\})$, l'application surjective $\Phi_x : \pi_1(B, q_0) \to G = Aut(f)$ vérifie $\Phi_x([\gamma_i]) = g_i \in K_{p_i}$ d'après la proposition 2.1.14. Comme les $[\gamma_i]$ engendrent $\pi_1(B, q_0)$ et $\Phi_x : \pi_1(B, q_0) \to G = Aut(f)$ est surjective alors les $g_1, ..., g_{r-1}$ engendrent G. Et on a $g_r = (g_1....g_{r-1})^{-1}$.

□

Chapitre 3

THÉORÈME D'EXISTENCE DE RIEMANN : FORME ALGÉBRIQUE.

Dans ce chapitre, nous démontrons le théorème d'existence de Riemann (TER) dans sa forme algébrique. Ce théorème permet de décider si un type de ramification est celui d'une extension galoisienne finie. Pour le démontrer, on utilise les formes topologique (Théorème 2.2.1) et analytique (Proposition 3.1.3) du théorème d'existence de Riemann. L'idée est qu'étant donnée une extension galoisienne finie $E/\mathbb{C}(x)$, un élément primitif $\theta(x) \in E/\mathbb{C}(x)$ est localement une fonction analytique. On ne peut pas toujours étendre cette fonction sur $\mathbb{C}$ tout entier, mais grace à la théorie des surfaces de Riemann, $\theta(x)$ est définie sur une surface de Riemann X et E est isomorphe aux corps des fonctions méromorphes sur X. Le lien avec la forme topologique vient du fait que $X \to \mathbb{P}^1 - P$ est un revêtement topologique où $P \subset \mathbb{P}^1$ est une partie finie. La forme algébrique du TER (Théorème 3.2.1) nous permet de montrer que le problème inverse de Galois à une réponse positive sur $\mathbb{C}(x)$.

3.1. Surfaces de Riemann.

3.1.1. Définitions.

Définition 3.1.1. *Une variété topologique réelle de dimension n ($n \in \mathbb{N}$) est un espace topologique séparé X dans lequel tout point possède un voisinage homéomorphe à $\mathbb{R}^n$.*

On pose $\dim_{\mathbb{R}} X = n$. Lorsque $n = 2$, on dit que X est une surface. Nous allons dans la suite nous intéresser essentiellement aux surfaces.

Définition 3.1.2. *Soit X une surface.*

(1) Une carte complexe sur X est un homéomorphisme $\phi : U \to V$ où $U \subset X$ est un ouvert de X et $V = \phi(U) \subset \mathbb{C}$ est un ouvert de $\mathbb{C}$.

(2) *Deux cartes complexes* $(U_1, \phi_1), (U_2, \phi_2)$ *sont dites holomorphiquement compatibles si l'application de transition* $\phi_2 \circ \phi_1^{-1} : \phi_1(U_1 \cap U_2) \to \phi_2(U_1 \cap U_2)$ *est un biholomorphisme c'est-à-dire bijective, holomorphe et d'inverse holomorphe.*

(3) *Un atlas complexe sur* X *est un système* $\mathfrak{A} = (U_i, \phi_i)_{i \in I}$ *de cartes complexes compatibles et tel que* $X = \bigcup_{i \in I} U_i$

(4) *Deux atlas* $\mathfrak{A}$ *et* $\mathfrak{A}'$ *sont analytiquement équivalents si toute carte de* $\mathfrak{A}$ *est compatible à toute carte de* $\mathfrak{A}'$.

Remarque 3.1.1. *(1) La relation* $\mathfrak{A}$ *et* $\mathfrak{A}'$ *sont analytiquement équivalents est une relation d'équivalence.*

(2) Chaque classe contient un atlas maximal qui est la réunion de tous les atlas de cette classe.

Définition 3.1.3. *(1) Une structure complexe sur une surface* X *est une classe d'équivalence d'atlas complexe.*

(2) Une structure complexe étant fixée, une carte de la structure est toute carte de son atlas maximal.

Exemple 3.1.1. *Si* (U, ϕ) *est une carte de l'atlas qui definit la structure complexe, alors pour tout ouvert* $U_1 \subset U$ *et* $\phi_1 = \phi_{/U_1}$, (U_1, ϕ_1) *est une carte de la structure complexe.*

Définition 3.1.4. *Une Surface de Riemann est une paire* (X, Σ) *où* X *est une surface connexe et* Σ *est une structure complexe sur* X.

Remarque 3.1.2. *Localement une surface de Riemann n'est rien d'autre qu'un ouvert du plan complexe.*

3.1.2. Exemples de surfaces de Riemann.

Exemple 3.1.2 (Le plan complexe)**.** $\mathbb{C}$ *est une surface de Riemann (avec sa topologie naturelle), muni de l'atlas* $\mathfrak{A} = \{(\mathbb{C}, id_{\mathbb{C}})\}$ *à une carte.*

Exemple 3.1.3 (La sphère de Riemann)**.** *On pose* $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$.

Topologie sur $\mathbb{P}^1$.

On défini sur $\mathbb{P}^1$ *une topologie qui coincide avec celle de* $\mathbb{C}$*. Un voisinage de* ∞ *est un ensemble qui contient un disque* $D(\infty, r) = \{z \in \mathbb{C} / |z| > \frac{1}{r}\} \cup \{\infty\}$ *(cette topologie fait de* $\mathbb{P}^1$ *un espace topologique homéomorphe à la sphère de* $\mathbb{R}^3$ *par la projection stéréographique). Les ouverts de* $\mathbb{P}^1$ *sont les ouverts* $U \subset \mathbb{C}$ *usuels, les ensembles* $V \cup \{\infty\}$ *où* V *est le complémentaire d'un compact de* $\mathbb{C}$*.*

Atlas sur $\mathbb{P}^1$*.*
$U_1 = \mathbb{P}^1 - \{\infty\} = \mathbb{C}$*,* $\phi_1 = id_{\mathbb{C}}$*,* $U_2 = \mathbb{P}^1 - \{0\} = \mathbb{C}^* \cup \{\infty\}$ *et*

$$\phi_2 : U_2 \to \mathbb{C}, z \to \begin{cases} \frac{1}{z} & si \quad z \in \mathbb{C}^* \\ 0 & si \quad z = \infty \end{cases}$$

ϕ_1 *et* ϕ_2 *sont des homéomorphismes. On a* $\phi_2 \circ \phi_1^{-1} : \mathbb{C}^* \to \mathbb{C}^*, z \mapsto \frac{1}{z}$ *et* $\phi_1 \circ \phi_2^{-1} : \mathbb{C}^* \to \mathbb{C}^*, z \mapsto \frac{1}{z}$ *qui sont des biholomorphismes.* $\mathbb{P}^1$ *muni de sa structure de surface de Riemann est appelée la Sphère de Riemann.*

3.1.3. Fonctions méromorphes sur une surface de Riemann.

Définition 3.1.5. *Soit* X, Y *deux surfaces de Riemann. On appelle morphisme de surfaces de Riemann (ou application holomorphe ou application analytique) de* X *vers* Y *toute application continue* $f : X \to Y$ *telle que pour toutes cartes* (V, ϕ) *de* X *et* (V', ϕ') *de* Y *avec* $f(V) \subset V'$ *l'application* $\phi' \circ f \circ \phi^{-1} : \phi(V) \subset \mathbb{C} \to \phi'(V') \subset \mathbb{C}$ *est holomorphe (dans le sens classique).*

En prenant $Y = \mathbb{P}^1$, on peut définir

Définition 3.1.6. *Soit* X *une surface de Riemann, une fonction méromorphe sur* X *est un morphisme de surfaces de Riemann* $f : X \to \mathbb{P}^1$ *distinct de l'application constante* ∞*.*

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

Exemple 3.1.4. *Étant donné une surface de Riemann* X *toute application constante* $f_a : X \to \mathbb{P}^1, x \mapsto f(x) = a$ *(avec* $a \in \mathbb{C}$*) est une fonction méromorphe sur* X*.*

L'ensemble $\mathfrak{M}(X)$ est donc toujours non vide.

Définition 3.1.7. *Soit* $f : X \to \mathbb{P}^1$ *une fonction méromorphe sur une surface de Riemann* X*.*

(1) On appelle zéro de f *tout* $x \in X$ *tel que* $f(x) = 0$*.*

(2) On appelle pôle de f *tout* $x \in X$ *tel que* $f(x) = \infty$*.*

Les fonctions méromorphes héritent des propriétés locales des fonctions méromorphes à variable complexe. On sait que si une fonction est méromorphe sur un ouvert de $\mathbb{C}$ et si $z_0 \in \mathbb{C}$ est un point de cet ouvert, la fonction admet dans un voisinage de z_0 un developpement en série de Laurent. Soit $f : X \to \mathbb{P}^1$ une fonction méromorphe et $x_0 \in X$, considérons une carte (V, ϕ) avec $x_0 \in V$. $f \circ \phi^{-1}$ est une fonction méromorphe en $\phi(x_0)$, elle admet donc dans un voisinage de $\phi(x_0)$ un developpement en série de Laurent : $(f \circ \phi^{-1})(z) = \sum_{k=N}^{\infty} a_k(z - \phi(x_0))^k$ avec $a_N \neq 0$. On peut écrire $f(x) = \sum_{k=N}^{\infty} a_k(\phi(x) - \phi(x_0))^k$ (où $\phi(x) = z$ et x dans un voisinage de x_0).

Lorsque $N < 0$, x_0 est un pôle d'ordre N, lorsque $N > 0$, x_0 est un zéro d'ordre N. L'ensemble des zéros $f^{-1}(\{0\})$ d'une fonction méromorphe non constante f est un espace fermé discret. De même l'ensemble des pôles $f^{-1}(\{\infty\})$ d'une fonction méromorphe non constante f est un espace fermé discret. Lorsque X est une surface de Riemann compacte les ensembles $f^{-1}(\{0\})$ et $f^{-1}(\{\infty\})$ sont finis. On a aussi le théorème de Liouville : toute fonction holomorphe et bornée $f : X \to \mathbb{C}$ est constante.

Proposition 3.1.1. *Soit X une surface de Riemann. L'ensemble $\mathfrak{M}(X)$ est un corps.*

Démonstration. Voir [8, Remarque 1.16]. □

Proposition 3.1.2. $\mathfrak{M}(\mathbb{P}^1) = \mathbb{C}(z)$.

Démonstration. La fonction identité de $\mathbb{P}^1$, $\mathbb{P}^1 \to \mathbb{P}^1, z \mapsto z$ que l'on notera z est une fonction méromorphe de $\mathbb{P}^1$ donc $z \in \mathfrak{M}(\mathbb{P}^1)$ d'après l'exemple C.3.1 $\mathbb{C}(z) \subset \mathfrak{M}(\mathbb{P}^1)$.
Soit $f \in \mathfrak{M}(\mathbb{P}^1)$, posons $x_1, ..., x_s$ les pôles de f. On peut supposer qu'aucun d'eux n'est ∞. Pour tout $k \in \{1, ..., s\}$, il existe une fonction f_i telle que $f - f_i$ n'a aucun pôle en x_i et x_i est le seul pôle de f_i (on peut prendre f_i à être par exemple les puisances négatives du developpement en série de Laurent de f au voisinage de x_i). La fonction $g = f - \sum_{i=1}^{s} f_i \in \mathfrak{M}(\mathbb{P}^1)$ n'a aucun pôle. L'image de $\mathbb{P}^1$ par g à $\mathbb{C}$ est une fonction constante d'après le théorème de Liouville par suite $f = g + \sum_{i=1}^{s} f_i \in \mathbb{C}(z)$ et $\mathfrak{M}(\mathbb{P}^1) = \mathbb{C}(z)$. □

On finit cette section avec l'énoncé du théorème d'existence de Riemann (forme analytique) dont une preuve se trouve dans [1] et qui sera utile dans la preuve de la forme algébrique du théorème d'existence de Riemann.

Proposition 3.1.3 (Théorème d'existence de Riemann-forme analytique)**.** *Soit X une surface de Riemann compact $x_1, ..., x_n \in X$ (n points distincts) et $a_1, ..., a_n \in \mathbb{C}$. Il existe une fonction méromorphe $g \in \mathfrak{M}(X)$ telle que $g(x_i) = a_i$ pour tout $i \in \{1, ..., n\}$.*

Démonstration. Voir [1, chap 6], la preuve du TER qui y est proposé utilise l'homologie et l'analyse fonctionnelle. Elle y occupe tout un chapitre. □

3.2. Surface de Riemann issue d'un revêtement fini de la sphère de Riemann privée d'un nombre fini de points.

Au chapitre 2 (proposition 2.1.8), on a vu qu'à partir d'un revêtement galoisien fini $f : X \to \mathbb{P}^1 - P$, on a une application continue et surjective $f : \overline{X} \to \mathbb{P}^1$ où $\overline{X}$ est un espace compacte. Dans ce qui suit on voudrait transférer la structure de surface de Riemann compacte de $\mathbb{P}^1$ à $\overline{X}$.

3.2.1. Surface de Riemann (compacte) issue d'un revêtement fini de la sphère de Riemann.

Soit $P \subset \mathbb{P}^1$ une partie finie et $f : X \to \mathbb{P}^1 - P$ un revêtement galoisien fini. Posons $G_0 = Aut(f)$ le groupe des automorphismes de f. Pour tout point $b \in \mathbb{P}^1_k - P$, on peut trouver un voisinage admissible $U \subset \mathbb{P}^1_k - P$ de b tel que $\{0, \infty\}$ n'est pas contenu dans U. On peut écrire $f^{-1}(U) = \bigcup_{i \in I} V_i$ (I fini) et on sait de plus que $f_{|V_i} : V_i \to U$ est un homéomorphisme. Posons $\varphi_{|V_i} = f_{|V_i}$ si $\infty \notin U$ et $\varphi_{|V_i} = \frac{1}{f_{|V_i}}$ si $\infty \in U$.

Proposition 3.2.1. *Les cartes $(V, \varphi_{|V})$ definies ci-dessus forment un atlas de X qui fait de X une surface de Riemann. Pour cette structure de surface de Riemann, l'application $f : X \to \mathbb{P}^1$ est analytique. De plus tout $\chi \in G_0$ est une application analytique de X vers X.*

Démonstration. Comme tout point de $\mathbb{P}^1_k - P$ possède un voisinage admissible alors $X = \bigcup V$ (donc les V recouvrent X). Soit $(V, \varphi), (V', \varphi')$ deux cartes définies ci-dessus, déterminons $\varphi \circ \varphi'^{-1}$ dans le cas où $V \cap V' \neq \emptyset$. On a 4 cas :

(1) $\varphi = f_{|V}$ et $\varphi' = f_{|V'}$
Soit $y \in \varphi'(V \cap V')$, $(\varphi \circ \varphi'^{-1})(y) = \varphi(f^{-1}_{|V'}(y)) = f_{|V}(f^{-1}_{|V'}(y)) = y$ donc $\varphi \circ \varphi'^{-1} = id_{\varphi(V \cap V')}$.

(2) $\varphi = f_{|V}$ et $\varphi' = \frac{1}{f_{|V'}}$ ($0 \notin V'$) Soit $y \in \varphi'(V \cap V')$, $(\varphi \circ \varphi'^{-1})(y) = \varphi((\frac{1}{f_{|V'}})^{-1}(y)) = \varphi(f^{-1}_{|V'}(\frac{1}{y})) = (f_{|V} \circ f^{-1}_{|V'})(\frac{1}{y}) = \frac{1}{y}$.

(3) $\varphi = \frac{1}{f_{|V}}$ et $\varphi' = f_{|V'}$.
Dans ce cas on a $(\varphi \circ \varphi'^{-1})(y) = \frac{1}{y}$.

(4) $\varphi = \frac{1}{f_{|V}}$ et $\varphi' = \frac{1}{f_{|V'}}$.
Dans ce cas on a $(\varphi \circ \varphi'^{-1})(y) = y$.

Dans tous les cas $\varphi \circ \varphi'^{-1} : z \to z$ ou $z \to \frac{1}{z}$ qui donne un biholomorphisme. Les cartes ci- dessus forment donc un atlas de X. Soit $\chi \in G_0$ comme $\chi(f^{-1}(\{b\}) = f^{-1}(\{b\})$ alors on n'a que deux cas pour $\varphi' \circ \chi \circ \varphi^{-1}$ cet-à-dire $\varphi' = f_{|V'}, \varphi = f_{|V}$ ou $\varphi' = \frac{1}{f_{|V'}}, \varphi = \frac{1}{f_{|V}}$. Ce qui donne donc $\varphi' \circ \chi \circ \varphi^{-1} = id$. Par suite χ est analytique. Localement on a :$f : z \to z$ ou $f : z \to \frac{1}{z}$ qui est analytique. □

Remarque 3.2.1. *Pour que les cartes soient conformes à notre définition (définition 3.1.2 (1)), on peut supposer que $\infty \in P$. Ce qui empêcherait d'avoir $\infty \in U$. Et donc $U \subset \mathbb{C}$.*

On a vu au chapitre précédent qu'à partir d'un revêtement $f : X \to \mathbb{P}^1 - P$ avec P fini, on obtient une application surjective continue $\overline{f} : \overline{X} \to \mathbb{P}^1$ et $\overline{X}$ est un espace topologique compact et connexes par arcs. On se propose de munir $\overline{X}$ d'une structure de surface de Riemann (compacte).

On sait que $\overline{X} - X$ est l'ensemble des points idéaux de X, il reste donc à définir une carte contenant un point idéal. Soit $m \in \overline{X} - X$, posons $b = \overline{f}(m)$ pour chaque $C \in m$ de niveau r on considère le revêtement $f_C = s_b \circ f_{|C} : C \to D^*(0, r)$ qui est fini. Posons e son degré. Il existe un homéomorphisme $\chi : C \to D^*(0, r^{\frac{1}{e}})$ tel que $\chi^e = f_{|C}$ ($z^e \circ \chi = f_{|C}$). L'homomorphisme χ s'étend en une application $\chi_m : C \cup \{m\} \to D(0, r^{\frac{1}{e}})$ telle que $\chi(m) = 0$. χ_m est une bijection qui de plus est un homéomorphisme car $\chi_m(C' \cup \{m\}) = D(0, r'^{\frac{1}{e}})$ où C' est une composante circulaire de niveau $r' < r$ au dessus de b. On prendra comme carte de m un couple $(C \cup \{m\}, \chi_m)$.

Proposition 3.2.2. *Les couples (V, φ) dans la proposition 3.1.1. et les $(C \cup \{m\}, \chi_m)$ ci-dessus forment un atlas de $\overline{X}$ qui fait de $\overline{X}$ une surface de Riemann compact. De plus l'application $\overline{f} : \overline{X} \to \mathbb{P}^1$ (de la proposition 2.1.8) est analytique et tout $\chi \in G_0$ s'étend de façon unique en un homéomorphisme analytique $\overline{\chi} : \overline{X} \to \overline{X}$ avec $\overline{f} = \overline{\chi} \circ \overline{f}$.*

Démonstration. $\overline{X}$ est une surface de Riemann compacte.

Pour montrer que les (V,φ) et $(C\cup\{m\},\chi_m)$ forment un atlas de $\overline{X}$ il suffit de montrer qu'une carte du type (V,φ) est compatible avec une carte du type $(C\cup\{m\},\chi_m)$ et que deux cartes du type $(C\cup\{m\},\chi_m)$ sont compatibles.

Soit (V,φ) et $(C\cup\{m\},\chi_m)$ avec $V\cap(C\cup\{m\})\neq\emptyset$. Sur $V\cap(C\cup\{m\})$, on a : $\chi_m^e=f_{|C}=s_b\circ f$ (on rappelle que $s_b:D(b,r)\to D(0,r), z\mapsto z-b$ si $b\neq\infty$ et $z\mapsto\frac{1}{z}$ si $b=\infty$) Soit $z\in\chi_m(V\cap C_m)$, il existe $y\in V\cap C_m$ tel que $z=\chi_m(y)$ on a deux cas $\varphi=f_{|V}$ ou $\varphi=\frac{1}{f_{|V}}$.
Si on est dans le premier cas $(\varphi\circ\chi_m^{-1})(z)=\varphi(y)=f(y)=(s_b^{-1}\circ\chi_m^e)(y)=s_b^{-1}((\chi_m(y))^e)=s_b^{-1}(z^e)=z^e-b$. Dans le deuxième cas $(\varphi\circ\chi_m^{-1})(z)=\varphi(y)=\frac{1}{f(y)}=\frac{1}{s_b^{-1}(z^e)}=\frac{1}{z^e}$. On voit que $\varphi\circ\chi_m^{-1}$ est holomorphe et est un homéomorphisme car φ et χ le sont. De plus $(\varphi\circ\chi_m^{-1})'(z)\neq 0$ dans tous les cas alors $\varphi\circ\chi_m^{-1}$ est un biholomorphisme.

Soit $(C_1\cup\{m_1\},\chi_{m_1})$ et $(C_2\cup\{m_2\},\chi_{m_2})$, si $m_1\neq m_2$ et $(C_1\cup\{m_1\})\cap(C_2\cup\{m_2\})\neq\emptyset$ alors $(C_1\cup\{m_1\})\cap(C_2\cup\{m_2\})\subset X$ donc peut etre recouvert par des cartes du type (V,φ) et comme chaque (V,φ) est compatible à chaque carte du type $(C\cup\{m\},\chi_m)$ d'apres ce qui précède. Alors $(C_1\cup\{m_1\},\chi_{m_1})$ et $(C_2\cup\{m_2\},\chi_{m_2})$ seront compatibles car $\chi_{m_1}\circ\chi_{m_2}^{-1}=\chi_{m_1}\circ\varphi^{-1}\circ\varphi\circ\chi_{m_2}$ est un biholomorphisme sur $(C_1\cup\{m_1\})\cap(C_2\cup\{m_2\})\cap V$.
Si $m_1=m_2$ on peut supposer $C_1\cup\{m_1\}\subset C_2\cup\{m_2\}$ si $C_1\cup\{m_1\}$ est de niveau r alors $C_2\cup\{m_2\}$ est de niveau $r'\geq r$. Les homéomorphismes $\chi_{m_1}:C_1\cup\{m_1\}\to D(0,r^{\frac{1}{e}})$ et $\chi_{m_2|C_1\cup\{m_1\}}:C_1\cup\{m_1\}\to D(0,r^{\frac{1}{e}})$ satisfont aux conditions de la proposition 2.4.2. (1). Donc il existe une racine de l'unité ζ telle que $\chi_{m_2|C_1\cup\{m_1\}}=\zeta\chi_{m_1}$. Donc $(\chi_{m_2}\circ\chi_{m_1}^{-1})(z)=\chi_{m_2}((\frac{1}{\zeta}\chi_{m_2})^{-1}(z))=\chi_{m_2}(\chi_{m_2}^{-1}(\zeta z))=\zeta z$ (voir remarque ci-dessous). Donc $\chi_{m_2}\circ\chi_{m_1}^{-1}$ est la multiplication par ζ qui est un biholomorphisme. D'où $\overline{X}$ est une surface de riemann compact.

$\overline{f}:\overline{X}\to\mathbb{P}^1$ est analytique .

Il reste à montrer que $\overline{f}$ est analytique sur les points idéaux. Soit $m\in\overline{X}-X$, on a deux cas $\overline{f}(m)=\infty$ et $\overline{f}(m)\neq\infty$. Supposons $\overline{f}(m)=b\neq\infty$. Soit $(C\cup\{m\},\chi_m)$ une carte de m, $(\chi_m:C\cup\{m\}\to D(0,r^{\frac{1}{e}}))$, soit $z\in D(0,r^{\frac{1}{e}})$ il existe $y\in D(0,r^{\frac{1}{e}})$ tel que $\chi_m(y)=z$, $(f\circ\chi_m^{-1})(z)=f(y)=s_b^{-1}(z^e)=z^e+b$ (car $s_b\circ f=\chi_m^e$). Si on plutôt $\overline{f}(m)=b=\infty$, soit $z\in D(0,r^{\frac{1}{e}})$ il existe $y\in D(0,r^{\frac{1}{e}})$ tel que $\chi_m(y)=z$. On a $\frac{1}{(f\circ\chi_m^{-1})(z)}=\frac{1}{f(y)}=\frac{1}{s_b^{-1}(z^e)}=\frac{1}{\frac{1}{z^e}}=z^e$. Dans les deux cas on voit que $\overline{f}$ est analytique sur $\overline{X}$.

χ s'étend en un homéomorphisme analytique.

On sait d'après la proposition 2.4.8 que chaque $\chi \in G_0$ s'étend en un unique homéomorphisme $\overline{\chi} : \overline{X} \to \overline{X}$ qui vérifie $\overline{f} = \overline{\chi} \circ \overline{f}$. Il reste à montrer que $\overline{\chi}$ est analytique en les points idéaux d'après la proposition 3.3.1. Soit $m \in \overline{X} - X$ et $(C \cup \{m\}, \chi_m)$ une carte de m. Alors $(\overline{\chi}(C \cup \{m\}), \chi_m \circ \overline{\chi}^{-1})$ est encore une carte en le point idéal $\overline{\chi}(m)$. On regarde donc $\overline{\chi}$ sur les deux cartes.

On a : $\chi_m^e = f$ donc $(\chi_m(\chi^{-1}))^e = f$, ainsi χ_m et $\chi_m \circ \chi^{-1}$ satisfont à la condition (1) de la proposition 2.4.2. Donc $\chi_m \circ \chi^{-1} = \zeta\chi_m$ avec (ζ une racine e-ième de l'unité). Dans ce système de coordonnées, $\overline{\chi}$ s'écrit $(\chi_m \circ \overline{\chi}^{-1}) \circ \overline{\chi} \circ \chi_m^{-1} = id$ donc $\overline{\chi}$ est analytique.

□

3.2.2. Équivalence entre types de ramification topologiques et types de ramification algébriques.

Dans la proposition 3.2.2, on a vu que chaque $\chi \in G_0$ s'étend de façon unique en un isomorphisme analytique $\overline{\chi} : \overline{X} \to \overline{X}$. En effet l'inverse de $\overline{\chi}$ correspond au prolongement de χ^{-1}. Considérons $G_0' = \{\overline{\chi} | \chi \in G_0\}$. $(G_0', \circ)$ est un groupe isomorphe à G_0 par l'isomorphisme $G_0 \to G_0', \chi \mapsto \overline{\chi}$. On peut considérer G_0 comme un groupe d'isomorphismes de $\overline{X}$. Ce groupe permute transitivement les éléments des fibres $f^{-1}(\{b\}), b \in \mathbb{P}^1$.

Proposition 3.2.3. *Soit $g \in \mathfrak{M}(\overline{X})$ avec $g \circ \chi = g$ pour tout $\chi \in G_0$ alors il existe $g' \in \mathfrak{M}(\mathbb{P}^1)$ tel que $g = g' \circ \overline{f}$.*

Démonstration. (On confond f à $\overline{f}$)
Comme G_0 opère transitivement sur les fibres $f^{-1}(\{b\})$, il s'ensuit que g est constant sur $f^{-1}(\{b\})$. Posons $g'(b)$ cette valeur. Soit $U \subset \mathbb{P}^1 - (P \cup \{\infty\})$ un voisinage admissible de f et V une composante connexe de $f^{-1}(U)$. On a $g' \circ f|V = g$ donc $g' = g \circ (f|V)^{-1}$. Comme g est méromorphe sur $\overline{X}$ et $(V, f|V)$ est une carte locale, alors g' est une fonction méromorphe sur U. Par suite g' est méromorphe sur $\mathbb{P}^1 - (P \cup \{\infty\})$. Comme g' est continue sur chaque $p \in P \cup \{\infty\}$ donc g' s'étend en une fonction méromorphe sur tout $\mathbb{P}^1$.

□

Proposition 3.2.4. *Soit $f : X \to \mathbb{P}^1 - P$, un revêtement galoisien fini. Soit $\overline{f} : \overline{X} \to \mathbb{P}^1$ son prolongement analytique sur la surface de Riemann compacte $\overline{X}$. On identifie G_0 à G_0' comme ci-dessus et on pose $\mathbb{C}(\overline{f})$ le corps engendré par $\overline{f}$ et les fonctions constantes sur $\overline{X}$ à valeurs complexes. Pour chaque $\chi \in G_0$ l'application $t_\chi : \mathfrak{M}(\overline{X}) \to \mathfrak{M}(\overline{X}), g \mapsto g \circ \chi^{-1}$ est un automorphisme du corps*

$\mathfrak{M}(\overline{X})$. *Le corps* $\mathfrak{M}(\overline{X})$ *est une extension galoisienne de* $\mathbb{C}(\overline{f})$ *et l'application* $t : G_0 \to G(\mathfrak{M}(\overline{X})/\mathbb{C}(\overline{f})), \chi \mapsto t_\chi = t(\chi)$ *est un isomorphisme.*

DÉMONSTRATION. $\underline{t_\chi \text{ est bien définie.}}$

Soit $g \in \mathfrak{M}(\overline{X})$, $g \circ \chi^{-1} \in \mathfrak{M}(\overline{X})$ car χ est un isomorphisme analytique de $\overline{X}$.
$\underline{t_\chi \text{ est un automorphisme de corps.}}$

$t_\chi(g_1 + g_2) = (g_1 + g_2) \circ \chi^{-1} = g_1 \circ \chi^{-1} + g_2 \circ \chi^{-1} = t_\chi(g_1) + t_\chi(g_2)$

$t_\chi(g_1 g_2) = (g_1 g_2) \circ \chi^{-1} = (g_1 \circ \chi^{-1})(g_2 \circ \chi^{-1}) = t_\chi(g_1).t_\chi(g_2)$
$t_\chi(1_{\overline{X}}) = 1_{\overline{X}} \circ \chi^{-1} = 1_{\overline{X}}(\chi^{-1}) = 1_{\overline{X}}$ car $1_{\overline{X}}(x) = 1$ pour tout x.
$(t_{\chi^{-1}} \circ t_\chi)(g) = t_{\chi^{-1}}(g \circ \chi^{-1}) = (g \circ \chi^{-1}) \circ \chi = g$ donc $(t_\chi)^{-1} = t_{\chi^{-1}}$.
$\underline{t_{\chi/\mathbb{C}(\overline{f})} = id_{\mathbb{C}(\overline{f})}.}$
Pour une constante $a \in \mathbb{C}$, $t_\chi(a) = a \circ \chi^{-1} = a$. Pour $t_\chi(\overline{f}) = \overline{f} \circ \chi^{-1} = \overline{f}$ d'où le résultat.
$\underline{t : G_0 \to Gal(\mathfrak{M}(\overline{X})/\mathbb{C}(\overline{f})) \text{ est un isomorphisme.}}$
$t(\chi \circ \chi')(g) = t_{\chi\circ\chi'}(g) = g \circ (\chi \circ \chi')^{-1} = g \circ (\chi'^{-1} \circ \chi^{-1}) = (g \circ \chi'^{-1}) \circ \chi^{-1} = t_\chi(t_{\chi'}(g)) = (t_\chi \circ t_{\chi'})(g) = (t(\chi) \circ t(\chi'))(g)$ ainsi $t(\chi \circ \chi') = t(\chi) \circ t(\chi')$ donc t est un morphisme de G_0 dans $Aut(\mathfrak{M}(\overline{X}))$ de plus $t_{\chi/\mathbb{C}(\overline{f})} = id_{\mathbb{C}(\overline{f})}$ donc $t(\chi) \in Aut(\mathfrak{M}(\overline{X})/\mathbb{C}(\overline{f}))$.

Montrons que t est injective. Soit $\chi \in G_0$ tel que $t(\chi) = id_{G_0} (= t_\chi)$. Soit $x \in \overline{X}$ et $b = f(x)$ par le théorème d'existence de Riemann »(version analytique) proposition 3.1.3, il existe une fonction méromorphe $g \in \mathfrak{M}(\overline{X})$ telle que les valeurs de g sur les éléments de $f^{-1}(\{b\})$ soient distinctes. Posons $y = \chi(x) \in f^{-1}(\{b\})$, on a $t(\chi)(g) = g$ car $t(\chi) = id_{G_0}$ donc $t(\chi)(g)(y) = g(y) \Leftrightarrow (g \circ \chi^{-1})(y) = g(y) \Leftrightarrow g(\chi^{-1}(y)) = g(y) \Leftrightarrow g(x) = g(y)$ or $x, y \in f^{-1}(\{b\})$ et g y prend des valeurs distinctes donc $x = y$. Comme $\chi(x) = x$ alors $\chi = id$ d'après la proposition A.4.6 et le fait que $G_0 \cong G_0'$ et t est injective. Ainsi t est un isomorphisme de G_0 vers un sous groupe $Aut(\mathfrak{M}(\overline{X})/\mathbb{C}(\overline{f}))$.

$\underline{\mathfrak{M}(\overline{X})^{G_0} = \mathbb{C}(\overline{f}).}$
On a $\mathbb{C}(\overline{f}) \subset \mathfrak{M}(\overline{X})^{G_0}$. Soit $g \in \mathfrak{M}(\overline{X})$ tel que $t_\chi(g) = g$ pour tout g. On a $t_\chi(g) = g \Leftrightarrow g \circ \chi^{-1} = g \Leftrightarrow g = g \circ \chi$, on peut donc écrire $g = g' \circ \overline{f}$ avec $g' \in \mathfrak{M}(\mathbb{P}^1)$ (proposition 3.2.3) or $\mathbb{P}^1 = \mathbb{C}(\overline{f})$ par suite $\mathfrak{M}(\overline{X})^{G_0} = \mathbb{C}(\overline{f})$. D'après le lemme d'Artin $\mathfrak{M}(\overline{X})/\mathfrak{M}(\overline{X})^{G_0} = \mathfrak{M}(\overline{X})/\mathbb{C}(\overline{f})$ est une extension galoisienne de groupe de Galois G_0. □

Remarque 3.2.2. *La proposition 3.2.4 ci-dessus et la proposition 3.2.6 ci-dessous sont les clefs de la preuve du TER sous sa forme algébrique (théorème 3.2.1). C'est la proposition 3.2.4 qui utilise la forme analytique du TER.*

Soit $f : X \to \mathbb{P}^1 - P$ un revêtement galoisien fini avec $P \subset \mathbb{P}^1$ une partie finie. On pose $\overline{f} : \overline{X} \to \mathbb{P}^1$ le prolongement de f. On a defini la classe de conjugaison C_p de $G_0 = Aut(f)$ associée à p lorsque $p \in P$. On désigne cette classe par C_p^{top}. On considère l'extension qui provient de f. On a une extension du type $E/\mathbb{C}(x)$ où l'élément $x = \overline{f}$ et $E = \mathfrak{M}(\overline{X})$ le corps des fonctions méromorphes sur $\overline{X}$. Pour tout $p \in \mathbb{P}^1$, on a defini la classe de conjugaison C_p de $Gal(E/\mathbb{C}(x)) = Gal(\mathfrak{M}(\overline{X})/\mathbb{C}(\overline{f}))$ associée à p. On désigne cette classe par C_p^{alg}.

Proposition 3.2.5. *(1) Si $p \notin P$ alors $C_p^{alg} = \{1\}$.*

(2) Pour tout $p \in P$, l'isomorphisme $t : Aut(f) \to Gal(\mathfrak{M}(\overline{X})/\mathbb{C}(\overline{f}))$ applique C_p^{top} à C_p^{alg}.

Démonstration. (1) On a deux cas.

Cas 1 : Soit $p \in \mathbb{P}^1 - P$ et $x \in f^{-1}(\{p\})$. Il existe une carte (V, φ) de X contenant x. Si $p \neq \infty$, on peut choisir V de telle sorte que $\infty \notin \varphi(V)$ et $\varphi = f_{/V}$, si $p = \infty$, on prend $\varphi = \frac{1}{f_{/V}}$.

Chaque $g \in \mathfrak{M}(\overline{X})$ à un developpement en série de Laurent autour de x de la forme $g = \sum_{i=N}^{\infty} a_i(\varphi - \varphi(x))^i$. L'application $v : \mathfrak{M}(\overline{X}) \to \mathbb{C}((t)), g \to \sum_{i=N}^{\infty} a_i t^i$ est un morphisme de corps qui est donc injectif donc $\mathfrak{M}(\overline{X})$ peut-être vu comme un sous-corps de $\mathbb{C}((t))$. Déterminons $v(f)$, si $p \neq \infty$, on a $f = \varphi = \varphi(x) + (\varphi - \varphi(x)) = p + (\varphi - \varphi(x))$ donc $v(f) = p + t$.

Si $p = \infty$, $f = \frac{1}{\varphi} = \frac{1}{\varphi - \varphi(x)}$ $(\varphi(x) = \frac{1}{f(x)} = \frac{1}{\infty} = 0)$ donc $v(f) = t^{-1}$. Ainsi $v : \mathfrak{M}(\overline{X}) \to \mathbb{C}((t))$ est le prolongement de $v_p : \mathbb{C}(\overline{f}) \to \mathbb{C}(t)$ $(x = \overline{f})$. L'indice de ramification de $\mathfrak{M}(\overline{X})/\mathbb{C}(\overline{f})$ en p est donc 1 et $C_p^{alg} = \{1\}$.

Cas 2 : Soit $p \in P$, soit $m \in f^{-1}(\{p\})$ (un point idéal). Soit (C_m, χ_m) une carte centré en m. On a $C_m = C \cup \{m\}$ où C est une composante circulaire au dessus de p. D'autre part : $\chi_m^e = s_p \circ f$ sur C_m. Chaque $g \in \mathfrak{M}(\overline{X})$ a une serie de Laurent de la forme $g = \sum_{i=N}^{\infty} a_i(\chi_m - \chi_m(m))^i = \sum_{i=N}^{\infty} a_i \chi_m^i$ car $\chi_m(m) = 0$. L'application $v : \mathfrak{M}(\overline{X}) \to \mathbb{C}((t^{\frac{1}{e}})), g \mapsto \sum_{i=N}^{\infty} a_i t^{\frac{i}{e}}$ est un morphisme de corps. Calculons $v(f)$ si $p \neq \infty$, on a $\chi_m^e = s_p \circ f$ donc $f = s_p^{-1} \circ \chi_m^e = p + \chi_m^e$ et $v(f) = p + t^{\frac{e}{e}} = p + t$.

Si $p = \infty$, on a $f = \frac{1}{\chi_m^e}$ donc $v(f) = t^{-1}$ donc v prolonge v_p.

(2) Soit ω le générateur distingué de $G(\mathbb{C}((t^{\frac{1}{e}}))/\mathbb{C}((t)))$, on sait que : $\omega(\sum_{i=N}^{\infty} a_i t^{\frac{i}{e}}) = \sum_{i=N}^{\infty}(a_i\zeta_e^i)t^{\frac{i}{e}}$ par définition de $v^{-1}\circ\omega\circ v \in C_p^{alg}$. Par définition $h_C \in C_p^{top}$ générateur distingué du stabilisateur de C dans $G_0 = Aut(f)$. On a : $t(h_C) = v^{-1}\circ\omega\circ v$. En effet h_C fixe C et induit le générateur distingué du revêtement $f_C = s_p \circ f$. Comme $\chi_m^e = f_C$ alors $\chi_m \circ h_C^{-1} = \zeta_e\chi_m$.
Soit $g \in \mathfrak{M}(\overline{X})$, on a $t(h_C)(g) = g\circ h_C^{-1} = \sum_{i=N}^{\infty} a_i(\chi_m\circ h_C^{-1})^i = \sum_{i=N}^{\infty} a_i(\zeta_e\chi_m)^i = \sum_{i=N}^{\infty}(a_i\zeta_e^i)\chi_m^i = (v^{-1}\circ\omega\circ v)(g)$ d'où $t(h_C) = v^{-1}\circ\omega\circ v$ par suite C_p^{top} est appliqué à C_p^{alg}.

□

3.2.3. Théorème d'existence de Riemann (algébrique).

Il nous reste un ingrédient pour avoir la forme algébrique du TER, c'est le fait de pouvoir voir toute extension galoisienne finie $E/\mathbb{C}(x)$ comme corps de fonctions d'une surface de Riemann compacte.

Soit $E/\mathbb{C}(x)$ une extension galoisienne finie. Soit $F(x,y) \in \mathbb{C}[x,y]$ un polynôme irréductible en y à coéfficients dans $\mathbb{C}(x)$ tel que E soit sont corps de décomposition dans $\mathbb{C}(x)$. Posons $n = deg_y F$. On sait qu'il existe un nombre fini de complexes p tel que le polynôme $F(p,y) \in \mathbb{C}[y]$ n'ait pas de racines distinctes. posons P l'ensemble de ces complexes en plus de ∞.

Posons $X' = \{(a, y_1, ..., y_n) \in \mathbb{C}^{n+1} | a \in \mathbb{P}^1 - P$ et $F(a,y_1) = ... = F(a,y_n) = 0$ et les y_i sont deux à deux distincts $\}$. En fait les y_i sont les racines du polynôme séparable $F(a,y)$. X' est muni de la toplogie naturelle induite par celle de $\mathbb{C}^{n+1}$.
Proposition 3.2.6. *L'application $f' : X' \to \mathbb{P}^1 - P, (a, y_1, ..., y_n) \mapsto a$ est un revêtement. Le groupe symétrique S_n opère comme groupe d'automorphismes de f' sur $y_1, ..., y_n$.*

Démonstration. Pour chaque $a_0 \in \mathbb{P}^1 - P$ il existe des fonctions holomorphes $\Psi_1, ..., \Psi_n$ definies sur un voisinage U de a_0 tel que $\Psi_1(a), ..., \Psi_n(a)$ sont exactement les racines de $F(a,y) \in \mathbb{C}[y]$, pour tout $a \in U$ Pour $\sigma \in S_n$, posons $V_\sigma = \{(a, \Psi_{\sigma(1)}(a), ..., \Psi_{\sigma(n)}(a)), a \in U\}$ on a : $(f')^{-1}(U) = \bigcup_{\sigma\in S_n} V_\sigma$ (la réunion est disjointe). L'application $U \to V_\sigma, a \mapsto (a, \Psi_{\sigma(1)}(a), ..., \Psi_{\sigma(n)}(a))$ est l'inverse de $f'_{|V_\sigma} : V_\sigma \to U$. Les fonctions $id_U, \Psi_1, ..., \Psi_n$ étant continues alors $f'_{|V_\sigma}$ (qui est une projection)et son inverse sont continues et se sont des homéomorphismes. On suppose U compacte et connexe par arcs donc les V_σ sont aussi compactes et connexes par arcs. Le complémentaire de chaque V_σ dans $(f')^{-1}(U)$ est la réunion des autres V_σ (qui sont fermés) donc V_σ est un ouvert de $(f')^{-1}(U)$. Les V_σ sont donc les composantes connexes de $(f')^{-1}(U)$. Si D est un disque ouvert contenu dans U alors D est admissible pour f' et f' est un revêtement.

Soit $\sigma \in S_n$, $(f \circ \sigma)((u, v_1, ..., v_n)) = f(u, v_{\sigma(1)}, ..., v_{\sigma(n)}) = u = f(u, v_1, ..., v_n)$ donc $f \circ \sigma = f$. Tout $\sigma : X' \to X'$ est une bijection . Soit $D = D((a, y_1, ...y_n), r)$ et $(b, y'_1, ..., y'_n) \in D$, on a $\sigma(D) = D(\sigma(a, y_1, ...y_n), r)$
car $|\sigma(a, y_1, ..., y_n) - \sigma(b, y'_1, ..., y'_n)| = |(a, y_1, ..., y_n) - (b, y'_1, ..., y'_n)|$. Donc l'image d'un disque par σ est un disque et par suite σ est ouverte et est donc continue car σ^{-1} est aussi ouverte. Ainsi chaque $\sigma \in S_n$ est un automorphisme de X' . L'action de S_n s'étend transitivement sur chaque fibre alors $Aut(f') = S_n$.

□

Proposition 3.2.7. *Soit X une composante connexe par arcs de X'. La restriction de f' à X est un revêtement galoisien fini f.*

Démonstration. Comme X est une composante connexe par arcs alors d'après la proposition 2.2.7, $f = f'_{|X}$ est un revêtement. Soit $b \in \mathbb{P}^1 - P$ et $x, y \in f^{-1}(\{b\}), \chi \in Aut(f')$ avec $\chi(x) = y$ (ce qui est toujours possible car l'action de S_n est transitive). Comme χ est un homéomorphisme et X est une composante connexe alors $\chi(X) = X$ (puisque $\chi(x) = y \in X$), on a le même résultat pour χ^{-1} car $\chi^{-1}(y) = x$ donc $\chi^{-1}(X) = X$. Donc $\chi_{|X} \in Aut(f)$ et $Aut(f)$ agit transitivement sur chaque fibre. De plus $|f^{-1}(\{b\})| \leq n! = deg(f')$ donc f est un revêtement galoisien fini.

□

Proposition 3.2.8. *$\mathfrak{M}(\overline{X})$ est algébriquement fermé dans $\mathfrak{M}(X)$.*

Démonstration. Voir [1, lemme 5.5] □

Proposition 3.2.9. *Pour tout $i \in \{1, ..., n\}$ les fonctions $g_i : X \to \mathbb{C}, (a, y_1, ..., y_n) \mapsto y_i$ se prolonge en des fonctions méromorphes $\overline{g_i} : \overline{X} \to \mathbb{C}$ telles que $F(\overline{f}, \overline{g_i}) = 0$.*

Démonstration. Les $(V_\sigma, f_{|V_\sigma})$ forment un système de cartes de X. Dans ce système g_i est représentée par $\Psi_{\sigma(i)}$. Donc g_i est une fonction méromorphe sur X. Soit $x = (a, y_1, ..., y_n) \in X$, on a $F(a, y_i) = 0$. Donc $F(f(x), g_i(x)) = 0$ pour tout $x \in X$ d'où $F(\overline{f}(x), \overline{g_i}(x)) = 0$ pour tout $x \in X$, $\overline{g_i}$ est donc une racine d'un polynôme à coéfficient dans $\mathfrak{M}(\overline{X})$ qui est algébriquement fermé dans $\mathfrak{M}(X)$ donc $g_i \in \mathfrak{M}(\overline{X})$.

□

Proposition 3.2.10. *Les fonctions $g_1, ..., g_n$ engendrent $\mathfrak{M}(\overline{X})$ sur $\mathbb{C}(\overline{f})$.*

Démonstration. D'après la proposition 3.2.4, tout élément de $G(\mathfrak{M}(\overline{X})/\mathbb{C}(\overline{f}))$ est de la forme t_χ avec $\chi \in G_0$. Supposons $t_\chi(g_i) = g_i$ alors pour tout $x \in X$, $g_i(x) = g_i(\chi^{-1}(x))$ de plus $f(x) = f(\chi^{-1}(x))$ car $\chi \in Aut(f)$, on a ($x =$

$(a, y_1, ...y_n)$ et $\chi^{-1}(x) = (a', y'_1, ..., y'_n))$ ce qui précède implique $a = a', y_i = y'_i$ ou encore $x = \chi^{-1}(x)$ donc $\chi = id_X$ d'où le corps $\mathbb{C}(\overline{f})(g_1, ..., g_n) = \mathfrak{M}(\overline{X})$. □

Proposition 3.2.11. *Soit $E/\mathbb{C}(x)$ une extension galoisienne finie. Alors il existe une partie finie $P \subset \mathbb{P}^1$ un revêtement galoisien fini $f : X \to \mathbb{P}^1 - P$ et un isomorphisme $\mathbb{C}$ - linéaire entre E et $\mathfrak{M}(\overline{X})$ qui envoie x sur $\overline{f}$.*

Démonstration. Nous avons dans la proposition 3.2.7 construit un revêtement $f : X \to \mathbb{P}^1 - P$ et dans la proposition 3.2.10 on a vu que le corps des fonctions méromorphes $\mathfrak{M}(\overline{X})$ de $\overline{X}$ a pour générateurs les fonctions $g_1, ..., g_n$ sur $\mathbb{C}(\overline{f})$ posons $\alpha_1(x), ..., \alpha_n(x)$ les racines de $F(x, y) \in \mathbb{C}[x, y]$ (où F est le polynôme dont $E/\mathbb{C}(x)$ est le corps de décomposition), on définit $s : E/\mathbb{C}(x) \to \mathfrak{M}(\overline{X})/\mathbb{C}(\overline{f})$ par $s(x) = \overline{f}, s(\alpha_i) = g_i$ .On a $E = \mathbb{C}(x, \alpha_1(x), ..., \alpha_n(x))$, $\mathfrak{M}(\overline{X}) = \mathbb{C}(\overline{f}, g_1, ..., g_n)$ et s est un isomorphisme $\mathbb{C}$ -linéaire. □

On a vu qu'à chaque extension galoisienne $E/\mathbb{C}(x)$ il existe un type de ramification. Peut-on trouver une extension $E/\mathbb{C}(x)$ associée à tout type de ramification $T = [G, P, (C_p)_{p\in P}]$? La forme algébrique du théorème d'existence de Riemann donne une condition nécéssaire et suffisante pour qu'un type de ramification soit le type de ramification d'une extension galoisienne finie.

Théorème 3.2.1 (T.E.R. forme algébrique)**.** *Soit $T = [G, P, (C_p)_{p\in P}]$ un type de ramification. Soit $r = |P|$ posons $p_1, ...p_r$ les éléments de P. Il existe une extension galoisienne finie de $\mathbb{C}(x)$ de type T si et seulement si il existe des générateurs $g_1, ..., g_n$ de G avec $g_1....g_n = 1$ et $g_i \in C_{p_i}$ pour tout $i \in \{1, ..., r\}$.*

Démonstration. ($\Rightarrow$) On suppose que l'on a un type $T = [G, P, (C_p)_{p\in P}]$ qui est le type de ramification d'une extension $E/\mathbb{C}(x)$. On sait qu'il existe d'après la proposition 3.2.6 un revêtement $f : X \to \mathbb{P}^1 - P$ et un morphisme $\mathbb{C}$-linéaire de E vers $\mathfrak{M}(\overline{X})$. Par la proposition 3.2.5 les points de ramification de $E/\mathbb{C}(x)$ sont ceux pour lesquelles $C_p^{top} \neq 1$. D'après le théorème 2.2.1, il existe des générateurs $h_1, ..., h_r$ avec $h_1.....h_r = 1$ et $h_i \in C_{p_i}^{top}$ pour tout i. Les images de ces générateurs sous l'isomorphisme $t : G_0 \to G(\mathfrak{M}(\overline{X})/\mathbb{C}(\overline{f})), \chi \mapsto t_\chi = t(\chi)$ de la proposition 3.2.4 nous donne les générateurs recherchés.

($\Leftarrow$) On suppose que l'on a un type de ramification $T = [G, P, (C_p)_{p\in P}]$ qui satisfait aux conditions du théorème. D'après la forme topologique du théorème d'existence de Riemann (théorème 2.2.1), il existe un revêtement $f : X \to \mathbb{P}^1 -$

P de type $T = [G, P, (C_p)_{p\in P}]$. Par les propositions 3.2.4 et 3.2.5, l'extension $\mathfrak{M}(\overline{X})/\mathbb{C}(\overline{f})$ a le même type. □

3.3. Problème inverse de Galois sur $\mathbb{C}(x)$.

3.3.1. Réalisation des groupes finis comme groupes de Galois sur $\mathbb{C}(x)$.

Nous allons à l'aide de la forme algébrique du théorème d'existence de Riemann montrer que le problème inverse de Galois a une réponse positive pour le corps $k = \mathbb{C}(x)$.

Soit G un groupe fini, $g_1, ..., g_r$ des générateurs de G, posons $g_{r+1} = (g_1...g_r)^{-1}$ on a $g_1...g_r.g_{r+1} = 1$. Soit $p_1, ..., p_{r+1}$ des éléments distincts de $\mathbb{C}$ et C_{p_i} la classe de conjugaison de g_i. Le type de ramification $T = [G, P, (C_p)_{p\in P}]$ où $P = \{p_1, ..., p_{r+1}\}$, vérifié la condition du théorème. Il existe donc une extension $E/\mathbb{C}(x)$ de type $T = [G, P, (C_p)_{p\in P}]$. Donc G est groupe de Galois sur $\mathbb{C}(x)$.

Remarque 3.3.1 (Nombre minimal de points de branchement)**.** *Si le nombre r de points de ramification est < 2 alors l'extension $E/\mathbb{C}(x)$ est triviale. En effet le cas $r = 0$ implique qu'il n'y a pas de point de branchement le groupe a donc 0 générateurs, ce qui correspond au groupe trivial. Le cas $r = 1$ correspond à un générateur égal à l'élément neutre du groupe ce qui donne encore le groupe trivial. Dans le cas où le nombre de points de ramification est $r = 2$ on a deux générateurs $g_1, g_2 \in G$ avec $g_1.g_2 = 1$, ce qui donne $g_2 = g_1^{-1}$ donc le groupe est cyclique.*
Pour donc espérer atteindre tous les groupes le premier cas le plus intéressant est celui où $r = 3$.

3.3.2. Types de ramification et revêtements galoisiens finis.

À la fin du chapitre 1, nous avons donné quatre exemples de types de ramification. Les deux premiers ont été vite vu comme les types de ramification de certaines extensions et les deux derniers n'étaient liés à aucune extension galoisienne finie.

(1) Dans les deux premiers cas les classes de conjugaison sont des singletons, on voit que le produit des éléments de ces classes donne 1 (dans le deuxième exemple $\zeta_4.\zeta_4^3.\zeta_4.\zeta_4^{-1} = 1$) et de plus ces classes engendrent les groupes de Galois considérés.

(2) Pour le cas 3, considérons $\sigma_1 = (n-1, n), \sigma_2 = (1...n-1), \sigma_3 = (n-1, n, n-2, ...2, 1)$ on a $\sigma_1.\sigma_2.\sigma_3 = 1$ et $< \sigma_1, \sigma_2, \sigma_3 >= S_n$ ceci est une conséquence immédiate de proposition B.0.10 de l'appendice B. Par le théorème 3.2.1, le type de ramification $[S_n, \{0, 5, -1\}, (C^{(n-1)}, C^{(2)}, C^{(n)})]$ est celui d'une extension galoisienne finie de $\mathbb{C}(x)$.

(3) Dans le quatrième exemple on a : $i \in C_1, j \in C_2, -k \in C_3$ et $i.j.(-k) = 1$ de plus $Q_8 =< i, j, -k >$, par le théorème 3.2.1, il existe donc une extension galoisienne finie de $\mathbb{C}(x)$ dont le type est $[Q_8, \{0, 1, 2\}, \{C_1, C_2, C_3\}]$.

Chapitre 4

CRITÈRE DE RIGIDITÉ RATIONNELLE.

On sait déjà grâce au T.E.R (Théorème 3.2.1), si un type de ramification est le type de ramification d'une extension galoisienne finie de $\mathbb{C}(x)$. Comme conséquence de ce théorème on sait que tout groupe fini est groupe de Galois sur $\mathbb{C}(x)$. On aimerait partant d'une extension galoisienne finie de $\mathbb{C}(x)$ ayant pour groupe G obtenir une extension galoisienne de $\mathbb{Q}(x)$ ayant le même groupe, ce qui par le théorème d'irréductibilité de Hilbert nous donnerait une extension galoisienne de $\mathbb{Q}$ ayant G comme groupe de Galois. C'est la «descente» de $\mathbb{C}$ à $\mathbb{Q}$.
On élargit un peu le problème. Etant donnée une extension galoisienne finie $E/k(x)$ où k est un corps algébriquement clos (de caractéristique 0) et $\kappa \subset k$ un sous-corps, peut-on toujours «descendre» vers $\kappa(x)$? (La notion de descente est précisée dans la section 4.1, où on parle de corps de définition.) On procède en trois étapes. Dans la première, on montre que l'on peut toujours descendre vers une extension finiment engendrée $\kappa(t_1, ..., t_s)$ de κ. C'est l'objet de la proposition 4.1.2 (1). Dans cette proposition les $t_1, ..., t_s$ ne sont pas forcément algébriquement indépendants. En d'autres termes l'extension $\kappa(t_1, ..., t_s)/\kappa$ n'est pas forcément transcendante pure. La deuxième étape permet de résoudre le problème avec des conditions très particulières le type de ramification de $E/k(x)$ doit-être rigide et κ-rationnel et surtout $k = \overline{\kappa}$, c'est la proposition 4.2.1. A la dernière étape on revient au cas où $k = \mathbb{C}$. On montre que l'on peut descendre vers une extension transcendante pure $\kappa(t_1, ..., t_s)$ de κ lorsque le type de ramification est rigide et κ-rationnel c'est le théorème 4.2.2. L'avantage est qu'une extension transcendante pure est isomorphe à un corps de fractions, ce qui permet d'utiliser le théorème d'irréductibilité de Hilbert. Notre principal résultat, le théorème 4.3.1 a l'avantage de travailler sur les classes de conjugaison sans s'intéresser aux points de ramification. Ce qui devient un problème de théorie des groupes.

Toutes les clôtures algébriques des sous corps de $\mathbb{C}$ dans ce chapitre sont les fermetures algébriques dans $\mathbb{C}$ de ces corps.

4.1. Descente.

4.1.1. Corps de définition.

Soit k un sous-corps de $\mathbb{C}$, κ un sous-corps de k.

Définition 4.1.1. *On dit qu'une extension galoisienne finie $E/k(x)$ est définie sur κ s'il existe un sous-corps $E_\kappa \subset E$ tel que :*

(1) $E_\kappa/\kappa(x)$ est une extension galoisienne,

(2) $[E_\kappa : \kappa(x)] = [E : k(x)]$,

(3) $E_\kappa \cap \overline{\kappa} = \kappa$.

Remarque 4.1.1. *Une extension E/k est dite régulière si $E \cap \overline{k} = k$. La troisième condition signifie que E_κ est une extension régulière de κ.*

Exemple 4.1.1. *L'extension $E = \mathbb{C}(x)(\sqrt{x})$ est définie sur $\mathbb{Q}$, il suffit de prendre $E_\mathbb{Q} = \mathbb{Q}(\sqrt{x})$.*

Proposition 4.1.1. *On suppose E/k est définie sur κ.*

(1) Soit θ un élément primitif de $E_\kappa/\kappa(x)$ c'est-à-dire $E_\kappa = \kappa(x)(\theta)$. On a $E = k(x)(\theta)$. De plus E est défini sur tout corps κ' entre κ et k, et on peut prendre $E_{\kappa'} = \kappa'(x)(\theta)$.

(2) Le groupe $G = Gal(E/k(x))$ est isomorphe au groupe $Gal(E_\kappa/\kappa(x))$ via l'application de restriction à E_κ. Donc G se réalise régulièrement sur κ.

(3) Les points de ramification de E distinct de l'infini sont algébriques sur κ.

(4) Supposons que G à un centre trivial ou κ est algébriquement clos. Alors E_κ est unique, c'est-à-dire qu'il existe une unique extension E_κ qui est galoisienne sur $\kappa(x)$ de degré $n = [E : k(x)]$ et régulière sur κ.

(5) Si κ est algébriquement fermé alors les extensions $E/k(x)$ et $E_\kappa/\kappa(x)$ ont même type de ramification.

Démonstration. (1) L'élément θ est une racine d'un polynôme $F(y) \in \kappa(x)[y]$. Ce polynôme reste irréductible sur $\kappa'(x)[y]$ à cause de la régularité de E_κ sur κ. Ceci est vrai pour tout corps κ' tel que $\kappa \subset \kappa' \subset k$. L'extension $E_{\kappa'}$ est galoisienne sur $\kappa'(x)$, car elle contient toutes les racines de $F(y)$ et est de degré $n = [E : k(x)] = [E_\kappa : \kappa(x)]$, de plus elle est régulière sur κ' (voir [1, lemme 1.1]). Ainsi E est définie κ'. Le corps $k(x)[\theta]$ est donc une extension de degré n de $k(x)$ contenue dans E d'où $E = k(x)[\theta]$.

(2) Le groupe de Galois $G = Gal(E/k(x))$ permute les racines du polynôme $F(y)$ dans E. Ces racines engendrent E_κ sur κ, ainsi G laisse invariant E_κ. La restriction $G \to Gal(E_\kappa/\kappa(x))$ induit un monomorphisme de groupe : en effet si $g \in G$ fixe E_κ point par point (ou encore $g_{|E_\kappa} = id_{E_\kappa}$, on a $g(\theta) = \theta$ et par suite $g = id_E$. Comme les deux groupes ont le même ordre alors c'est un isomorphisme.

(3) On suppose sans nuire à la généralité que le polynôme $F(y)$ est unitaire et à coéfficients dans $\kappa[x]$. Son discriminant $D(x) \in \kappa[x] - \{0\}$. Les points de ramification de E distincts de l'infini sont les racines de $D(x)$. Ils sont donc dans $\overline{\kappa}$.

(4) Soit E^0_κ un autre sous-corps de E ayant la même propriété. Posons K le corps composé de E^0_κ et de E_κ. K est une extension galoisienne de $\kappa(x)$. Si κ' est la clôture algébrique de κ dans K, alors κ' et par suite $\kappa'(x)$ est invariant par $Gal(K/\kappa(x))$. Ceci implique que $Gal(K/\kappa'(x))$ est un sous groupe distingué de $Gal(K/\kappa(x))$ et donc que $\kappa'(x)/\kappa(x)$ est une extension galoisienne. Si θ_0 est un elément primitif de $K/\kappa'(x)$ son polynôme minimal reste irréductible sur $k(x)$ donc son degré est plus petit ou égal à n. Donc $[K : \kappa'(x)] \leq n$. D'autre part K contient θ ainsi $[K : \kappa'(x)] \geq [\kappa'(x)[\theta] : \kappa'(x)] = n$ par (1). Par suite $K = \kappa'(x)(\theta)$. Si donc κ est algébriquement clos alors $K = \kappa(x)(\theta) = E_\kappa$.
Supposons que G a un centre trivial. Le corps $K = \kappa'(x)(\theta)$ est engendré par $\kappa'(x)$ et E_κ. D'autre part $\kappa'(x) \cap \overline{\kappa} = \kappa$. De même pour E^0_κ à la place de E_κ. Par la correspondance de Galois on a

$$Gal(K/\kappa(x)) = Gal(K/E_\kappa)Gal(K/\kappa'(x)) = Gal(K/E^0_\kappa)Gal(K/\kappa'(x)).$$

On a $Gal(K/\kappa'(x)) \cong Gal(K/\kappa(x))$ par (1) et (2) donc $Gal(K/\kappa'(x))$ a un centre trivial. Par suite $Gal(K/E_\kappa) = Gal(K/E^0_\kappa)$ le centralisateur de $Gal(K/\kappa'(x))$ dans $Gal(K/\kappa(x))$. D'où $E_\kappa = E^0_\kappa$.

(5) Soit θ comme dans (1). Soit $p \in \kappa \cup \{\infty\}$ et $v : E \to \Delta$ un prolongement de $v_p : k(x) \to k(t)$ dans une extension galoisienne finie de $k((t))$. Posons $\theta' = v(\theta)$. Alors $v(\kappa(x)) = \kappa(t)$, d'où $v(E_\kappa) = \kappa(t)(\theta')$. La restriction de v induit un plongement $\widehat{v}$ de E_κ dans $\Delta_\kappa = \kappa((t))(\theta')$. La restriction du générateur distingué de $Gal(\Delta/k((t)))$ à Δ_κ est le générateur distingué de $Gal(\Delta_\kappa/\kappa((t)))$. Par suite $g_{\widetilde{v}} \in \widetilde{G} = Gal(E_\kappa/\kappa(x))$ est la restriction de $g_v \in G$. Le morphisme de restriction $G \to \widetilde{G}$ applique la classe C_p de G associée à p à la classe $\widetilde{C_p}$ de $\widetilde{G}$ associée à p, pour tout $p \in \kappa \cup \{\infty\}$. Comme les points de ramification de $E/k(x)$ (et de $E_\kappa/\kappa(x)$) sont dans

$\kappa \cup \{\infty\}$ par (3), on voit en particulier que $E/k(x)$ a les mêmes points de ramification que $E_\kappa/\kappa(x)$.

□

Proposition 4.1.2. *(1) Toute extension $E/k(x)$ est définie sur une extension finiment engendré de κ.*

(2) Si E_0 est une extension galoisienne finie de $\kappa(x)$, régulière sur κ. Alors il existe une extension galoisienne $E/k(x)$, définie sur κ avec E_κ, $\kappa(x)$-isomorphe à E_0.

Démonstration. (1) Soit θ un élément primitif de $E/k(x)$ et $F(y) \in k(x)[y]$ son polynôme minimal. Chaque racine de $F(y)$ peut s'écrire $\theta_i = f_i(\theta)$ avec $f_i \in k(x)[y]$. Les coéfficients de F et f_i sont éléments de $k(x)$. Ils appartiennent donc à une extension galoisienne finiment engendré κ' de κ. Le corps $E_{\kappa'} = \kappa'(x)(\theta)$ est une extension galoisienne $\kappa'(x)$ car il contient tous les θ_i. Il vérifie les conditions de la définition 4.1.1. Donc E est définie sur κ'.

(2) On peut choisir E_0 sous la forme $E_0 = \kappa(x)[y]/(F)$ avec $F(y) \in \kappa(x)[y]$ un polynôme irréductible. Alors $E = k(x)[y]/(F)$ est une extension galoisienne finie de $k(x)$ telle que $E_\kappa = E_0$.

□

Ainsi pour tout corps κ la descente de $\mathbb{C}$ vers une certaine extension de type fini $\kappa_1 = \kappa(t_1, ..., t_s)$ (qui n'est pas forcément une extension transcendante pure) est assurée par la proposition ci-dessus. En particulier lorsque $k = \mathbb{C}$ et $\kappa = \mathbb{Q}$. Toute extension $E/\mathbb{C}(x)$ est définie sur un $\kappa_1 = \mathbb{Q}(t_1, ..., t_s)$ où $t_1, ..., t_s$ sont des complexes convenablement choisit.

Soit k un sous corps de $\mathbb{C}$ et $\alpha \in Aut(k)$. α peut être vu comme un automorphisme de $k(x)$ qui fixe l'indéterminée x.

Définition 4.1.2. *Un α-isomorphisme est un isomorphisme de corps $\lambda : E \to E'$ tel que $\lambda_{|k(x)} = \alpha$ (E et E' sont deux extensions galoisiennes finies de $k(x)$).*

En particulier un $k(x)$-isomorphisme est un α-isomorphisme avec $\alpha = id$. On note λ^* l'isomorphisme induit par λ sur les groupes $Gal(E/k(x))$ et $Gal(E'/k(x))$.

Proposition 4.1.3. *Soit $E/k(x)$ une extension galoisienne finie. Pour chaque $\alpha \in Aut(k)$, il existe un α-isomorphisme λ de E vers une extension galoisienne finie E' de $k(x)$. Si E est définie sur un sous-corps κ de k et $\alpha_{|\kappa} = id$, on peut prendre $E = E'$ et $\lambda^* = id$.*

DÉMONSTRATION. On peut étendre α en un automorphisme l_α de $k(x)[y]$ qui fixe x et y par $l_\alpha(f) = f^\alpha$ où f^α est le polynôme obtenu en appliquant α aux coéfficients de f . On peut écrire $E = k(x)[y]/(F)$ avec $F(y) \in k(x)[y]$. Posons $E' = k(x)[y]/(F^\alpha)$. l_α induit un isomorphisme d'anneaux $\lambda : E \to E'$. Ainsi $E'/k(x)$ est une extension galoisienne finie et λ est un α-isomorphisme.
Si E est définie sur κ, on peut choisir $E_\kappa = \kappa(x)[\theta]$ donc $E = k(x)[\theta]$ d'après la propriété 4.1.1.(Où le polynôme minimal F de θ est un élément de $\kappa(x)[y]$). Si de plus $\alpha_\kappa = id$ alors $F^\alpha = F$ et $E = E'$ et $\lambda_{|E_\kappa} = id_{E_\kappa}$ car $l_{\alpha|\kappa(x)[y]} = id_{|\kappa(x)[y]}$ d'où $\lambda^*(\theta) = \theta$ et par suite $\lambda^* = id$.

□

La proposition ci-dessous est notre principal critère de descente.

Proposition 4.1.4. *Soit κ un sous corps de $\mathbb{C}$ et $k = \overline{\kappa}$. Soit $E/k(x)$ une extension galoisienne finie dont le groupe de Galois $G = Gal(E/k(x))$ a un centre trivial. Alors E est définie sur κ si et seulement si pour chaque $\alpha \in Gal(\overline{\kappa}/\kappa)$, il existe un α-automorphisme λ de E avec $\lambda^* = id$.*

DÉMONSTRATION. La condition est nécessaire par la proposition 4.1.3. On sait que E est définie sur une extension finiment engendré κ_1 de κ. Comme $\kappa_1 \subset k = \overline{\kappa}$ alors on peut prendre κ_1 à être une extension galoisienne finie de κ. Posons $E_1 = E_{\kappa_1}$.

$\underline{E_1/\kappa(x) \text{ est une extension galoisienne finie.}}$

Soit $\alpha_1 \in Gal(\kappa_1/\kappa)$, on peut le prolonger en un $\alpha \in Gal(\overline{\kappa}/\kappa)$. Par hypothèse, il existe un α-automorphisme λ de E tel que $\lambda^* = id$. Comme G a un centre trivial, d'après la proposition 4.1.1 (4), E_1 est unique et donc $\lambda(E_1) = E_1$. Posons $\lambda_1 = \lambda_{|E_1}$, $\lambda_1 \in Aut(E_1/k(x))$ est un prolongement de $\alpha_1 \in Gal(\kappa_1(x)/\kappa(x)) \cong Gal(\kappa_1/\kappa)$ (par la remarque ci-dessous). Ceci est vrai pour tout $\alpha_1 \in Gal(\kappa_1/\kappa)$, par suite $E_1/\kappa(x)$ car $E_1/\kappa_1(x)$ est une extension galoisienne finie.

Posons $H = Gal(E_1/\kappa(x))$, $G_1 = Gal(E_1/\kappa_1(x))$, C le entralisateur de G_1 dans H et $f : H \to Gal(\kappa_1(x)/\kappa(x))$ la restriction.

$\underline{H = G_1.C \text{ (produit direct).}}$
Pour tout $g \in G$, $\lambda^*(g) = g$ (car $\lambda^* = id$), donc $\lambda g = g\lambda$. Par restriction à E_1, on a $\lambda_1 g_1 = g_1 \lambda_1$ pour tout $g_1 \in G_1$. Donc $\lambda_1 \in G$. Comme chaque $\alpha_1 \in Gal(\kappa_1/\kappa)$ se prolonge en un λ_1 alors $f_{|C}$ est surjective. Or $Gal(\kappa_1(x)/\kappa(x)) \cong H/G_1$ ceci implique que $H = G_1.C$. D'autre part $G_1 \cap C \subset Z(G_1)$ et $G_1 \cong G$ par la

proposition 4.1.1 (2) et $Z(G) = \{1\}$ donc $G_1 \cap C = \{1\}$ et par suite le produit $H = G_1.C$ est direct.
Posons $E_\kappa = E_1^C$, comme C est un sous groupe normal de H alors $E_\kappa/\kappa(x)$ est une extension galoisienne de groupe de Galois $H/C \cong G_1$. D'où $[E_\kappa : \kappa(x)] = |G_1| = |G| = [E : k(x)]$. D'autre part $E_\kappa \cap \kappa_1(x) = \kappa(x)$, en effet $E_\kappa \cap \kappa_1(x) = E_1^C \cap E_1^{G_1} = E_1^{G_1.C} = E_1^H = \kappa(x)$. Comme E_1 est régulier sur κ_1 et $E_\kappa \subset E_1$ alors E_κ est régulier κ. Par suite E_κ est définie sur κ. □

Remarque 4.1.2. *Soit κ'/κ une extension galoisienne alors $G = Gal(\kappa'/\kappa) \cong Gal(\kappa'(x)/\kappa(x))$. Ceci vient du fait que l'action naturelle de G sur $\kappa'(x)$ (en fixant x) a pour corps fixe $\kappa(x)$.*

4.1.2. Type de ramification κ-rationnel.

Définition 4.1.3. *Soit $T = [G, P, (C_p)_{p\in P}]$ un type de ramification, $n = |G|$. T est dit κ- rationnel si :*

(1) $P \subset \overline{\kappa} \cup \{\infty\}$,

(2) pour chaque $p \in P$ et pour chaque $\alpha \in Gal(\overline{\kappa}/\kappa)$, on a $\alpha(p) \in P$ et $C_{\alpha(p)} = C_p^m$ où m est un entier tel que $\alpha^{-1}(\zeta_n) = \zeta_n^m$ (ζ_n est une racine primitive n-ième de l'unité.).

Une classe de conjugaison C de G est dite rationnelle si $C^m = C$ pour tout entier m premier avec l'ordre de G. En d'autres termes pour tout $g \in C, g^m \in C$ lorsque le pgcd de m et $|G|$ est 1.

Remarque 4.1.3. *Comme cas particulier de notre définition un type de ramification $T = [G, P, (C_p)_{p\in P}]$ est κ-rationnel si $P \subset \kappa \cup \{\infty\}$ et chaque classe C_p est rationnelle.*

La proposition ci-dessous donne la relation qu'il y a entre les deux notions «corps de définition» et « κ-rationnalité ».

Proposition 4.1.5. *Si $E/k(x)$ est définie sur κ alors son type de ramification est κ - rationnel.*

Démonstration. On suppose que $E/k(x)$ est définie sur κ et posons $T = [G, P, (C_p)_{p\in P}]$ son type de ramification. D'après la proposition 4.1.1 (3) $P \subset \overline{\kappa}$. Soit $\alpha \in Gal(\overline{\kappa}/\kappa)$, on sait d'après la proposition 4.1.3 que α se prolonge en un automorphisme $\lambda : E \to E$ tel que $\lambda^* = id$. D'après la proposition 1.3.1, $C_{\alpha(p)} = \lambda^*(C_p^m) = C_p^m$. Ainsi $C_{\alpha(p)}$ est une classe non triviale et $\alpha(p) \in P$. □

Exemple 4.1.2. *Considérons le groupe diédral* $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ *et ses* 5 *classes de conjugaison qui sont :* $C_0 = \{1\}, C_1 = \{r, r^3\}, C_2 = \{r^2\}, C_3 = \{s, sr^2\}, C_4 = \{sr, sr^3\}$.
Un entier m *est premier avec l'ordre de* D_8 *si et seulement si* m *est impair. On peut donc écrire* $m = 2t + 1$.
On a $1^m = 1, (r^2)^{2t+1} = r^{4t}.r^2 = r^2$ *donc les classes* $C_0 = \{1\}, C_2 = \{r^2\}$ *sont rationnelles.*
D'autre part, $r^{2t+1} = (r^2)^t r = \begin{cases} r & si \quad t \quad est \quad pair \\ r^3 & si \quad t \quad est \quad impair \end{cases}$

et $(r^3)^{2t+1} = r^{6t}r^3 = \begin{cases} r^3 & si \quad t \quad est \quad pair \\ r & si \quad t \quad est \quad impair \end{cases}$

Donc C_1 *est rationnelle.*

De plus les éléments de C_3 *et* C_4 *étant d'ordre* 2*, leurs classes sont aussi rationnelles. Donc toutes les classes de conjugaison de* D_8 *sont rationnelles. Ainsi les type de ramification* $[D_8, \{1, -1, -3\}, (C_2, C_3, C_3)]$ *et* $[D_8, \{17/2, -1, -4\}, (C_2, C_4, C_4)]$ *sont* $\mathbb{R}$*-rationnels.*

Exemple 4.1.3. *Dans* S_n*, les classes de conjugaison sont toutes rationnelles.*

Soit $\sigma \in S_n$, et m un entier premier avec $n!$.
Supposons tout d'abord que σ est un l-cycle. On peut écrire $m = lq + r$ avec $0 < r < l$ (car m est premier avec l), $\sigma^m = \sigma^r$ et comme $0 < r < l$ alors σ^r est encore un l-cycle. Les classes des cycles sont rationnelles.
Supposons maintenant que $\sigma = \sigma_1....\sigma_t$ où σ_i est un cycle de longueur n_i, la décomposition de σ en produit de cycles disjoints. On a $\sigma^m = \sigma_1^m....\sigma_t^m$. Comme m est premier avec chaque n_i alors σ_i^m est un cycle de longueur n_i. Donc σ^m et σ sont dans la même classe de conjugaison.

Proposition 4.1.6. *Soit* $T = [G, P, (C_p)_{p\in P}]$ *et* $T' = [G', P', (C'_q)_{q\in P'}]$ *avec* $P = \{p_1, ..., p_r\}, P' = \{q_1, ..., q_t\}$ *deux types de ramification* κ*-rationnelles et* $P \cap P' = \emptyset$*. Alors le produit* $T \times T'$ *est* κ*-rationnel.*

Démonstration. On a $P \cup P' \subset \overline{\kappa} \cup \{\infty\}$ car $P, P' \subset \overline{\kappa} \cup \{\infty\}$ par κ-rationnalité. Soit $\alpha \in G(\overline{\kappa}/\kappa)$, on a $\alpha(p) \in P \cup P'$ pour tout $p \in P \cup P'$ car les types T et T' sont κ-rationnels. Si m vérifie $\alpha^{-1}(\zeta_n) = \zeta_n^m$ alors $C_{\alpha(p)} \times \{1\} = C_p^m \times \{1\} = (C_p \times \{1\})^m$ de même pour $\{1\} \times C_{\alpha(p)} = \{1\} \times C_p^m = (\{1\} \times C_p)^m$ donc $T \times T'$ est κ rationnel. □

4.2. Rigidité faible et Rigidité.

4.2.1. Extensions Galoisiennes finies de $\mathbb{C}(x)$ ayant un type de ramification donné.

4.2.1.1. *Extensions ne se ramifiant pas en dehors d'un ensemble donné et ayant un groupe fixé.*

On commence par s'intéresser aux extensions galoisiennes ayant un groupe fixé G et ne se ramifiant pas en dehors d'un ensemble fini $P \subset \mathbb{P}^1$. On ne réquiert pas qu'elles aient forcément le même type de ramification. Le théorème ci-dessus en donne une description complète.

Proposition 4.2.1. *Soit G un groupe fini et $P \subset \mathbb{P}^1$ une partie finie, $q \in \mathbb{P}^1 - P$. Il y a une correspondance bijective entre :*

(1) Les classes de $\mathbb{C}(x)$-isomorphisme entre extensions galoisiennes $E/\mathbb{C}(x)$ ayant un groupe de Galois isomorphe à un groupe G et des points de ramifications contenues dans P.

(2) Les classes d'équivalences de revêtements galoisiens $f : X \to \mathbb{P}^1 - P$ ayant un groupe de transformations de deck isomorphes à G.

(3) Les sous-groupes normaux du groupe fondamental $\pi_1(\mathbb{P}^1 - P, q)$ ayant un quotient isomorphe à G.

De plus les objets correspondants en (1) *et* (2) *ont même type de ramification.*

Démonstration. Voir [1,th. 5.14]. La correspondance entre (1) et (2) est donnée en associant à chaque revêtement f les extensions galoisiennes $E/\mathbb{C}(x)$ pour lesquelles il existe un isomorphisme $\mathbb{C}$-linéaire entre $\mathfrak{M}(\overline{X})$ et $E/\mathbb{C}(x)$ qui applique x sur f. La correspondance entre (2) et (3) est donnée en associant à f le noyau de la surjection $\Phi_x : \pi_1(\mathbb{P}^1 - P, q) \to Aut(f_\infty)$ pour n'importe quel $x \in f^{-1}(\{q\})$. □

La dernière catégorie d'objets va nous permettre de calculer le nombre θ de classes d'extensions galoisiennes $\mathbb{C}(x)$-isomorphes qui ont un groupe fixé G et qui ne se ramifient pas en dehors de P.

On sait qu'un sous-groupe normal de $\pi_1(\mathbb{P}^1 - P, q)$ dont le quotient est G correspond au noyau d'un morphisme surjectif $\varphi : \pi_1(\mathbb{P}^1 - P, q) \to G$. Posons $n = |P| - 1$. Le groupe $\pi_1(\mathbb{P}^1 - P, q)$ est engendré par les classes de chemins $\gamma_1, ..., \gamma_n$ par une légère modification de la proposition 2.1.9. Il y a donc une bijection entre les morphismes surjectifs $\varphi : \pi_1(\mathbb{P}^1 - P, q) \to G$ et les systèmes

générateurs $(g_1, ..., g_n)$ de G de longueur n, cette correspondance est donnée par $g_i = \varphi(\gamma_i)$. Deux tels morphismes φ, φ' ont le même noyau si et seulement si il existe un automorphisme $\alpha \in Aut(G)$ tel que $\varphi' = \alpha\varphi$. Pour les systèmes générateurs correspondants $(g_1, ..., g_n)$ et $(g'_1, ..., g'_n)$ de G ceci implique que $(g'_1, ..., g'_n) = (g_1, ..., g_n)^\alpha$. Ainsi

$\theta =$ Nombre de $Aut(G)$-orbites sur les systèmes générateurs de longueur n.

4.2.1.2. *Exemples d'extensions non isomorphes ayant même type de ramification.*

Considérons le groupe diédral $D_{10} = \{1, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4\}$. On a les relations $r^i s = sr^{-i}, r^5 = s^2 = 1$ pour tout $i \in \mathbb{N}$. D_{10} à 4 classes de conjugaison $C_0 = \{1\}, C_1 = \{r, r^4\}, C_2 = \{r^2, r^3\}, C_3 = \{s, sr^2, sr^3, sr, sr^4\}$.

Le T.E.R. nous permet de constater que le type de ramification $[D_{10}, \{-1, 0, 1, 2, 5\}, (C_1, C_2, C_3, C_3, C_3)]$ est le type de ramification d'une extension galoisienne finie de $\mathbb{C}(x)$.

Par le paragraphe précédent, on sait que le nombre de classes d'extensions galoisiennes $\mathbb{C}(x)$-isomorphes correspond aux nombre de $Aut(G)$-orbites sur les systèmes générateurs de longueurs 4. Les systèmes $(r, r^2, s, sr^2) \in C_1 \times C_2 \times C_3 \times C_3, (r, r^3, sr^4, s) \in C_1 \times C_2 \times C_3 \times C_3$ sont des systèmes générateurs de longeurs 4 de D_{10}, et il n'existe pas d'automorphismes α tel que $(r, r^2, s, sr^2)^\alpha = (r, r^3, sr^4, s)$. En effet si tel était le cas on aurait $\alpha(r) = r, \alpha(r^2) = r^3, \alpha(s) = sr^4, \alpha(sr^2) = s$ égalités qui ne sont pas compatibles avec le fait que α est un morphisme de groupes. Ainsi les deux 4-uplets $(r, r^2, s, sr^2), (r, r^3, sr^4, s)$ définissent deux extensions non isomorphes de $\mathbb{C}(x)$ qui ont un même type de ramification à savoir $[D_{10}, \{-1, 0, 1, 2, 5\}, (C_1, C_2, C_3, C_3, C_3)]$.

4.2.2. Rigidité faible et Rigidité.

4.2.2.1. *Définitions et exemples.*

D'après l'exemple qui précède, un type de ramification ne définit pas forcément une unique extension galoisienne de $\mathbb{C}(x)$. Mais les $Aut(G)$-orbites sur les systèmes de générateurs de longueur $n = |P| - 1$ définissent de façon unique les extensions galoisiennes qui sont non ramifiées en dehors de P. Ceci motive la définition suivante :

Définition 4.2.1. *Soit $(C_1, ..., C_r)$ un uplet de classes de conjugaison d'un groupe fini G. On dit que $(C_1, ..., C_r)$ est faiblement rigide si :*

(1) Il existe des générateurs $g_1, ..., g_r$ de G avec $g_1....g_r = 1, g_i \in C_i$ pour tout $i = 1, ..., r$.

(2) Si $g'_1, ..., g'_r$ est un autre système de générateurs de G ayant la même propriété, il existe un automorphisme γ de G tel que $\gamma(g_i) = g'_i$.

Définition 4.2.2. *Un type $T = [G, P, (C_p)_{p\in P}]$ est faiblement rigide si les éléments de P peuvent être écris $p_1, ..., p_r$ ($r = |P|$)tels que les classes $C_i = C_{p_i}$ forment un uplet de classes de conjugaison faiblement rigides.*

Exemple 4.2.1. *Considérons le groupe diédral $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ avec les relations $r^i s = sr^{-i}, r^4 = s^2 = 1$. Son centre est $Z(D_8) = \{1, r^2\}$. Il a 5 classes de conjugaisons qui sont : $C_0 = \{1\}, C_1 = \{r, r^3\}, C_2 = \{r^2\}, C_3 = \{s, sr^2\}, C_4 = \{sr, sr^3\}$.*
Les types de ramification $[D_8, \{i, -1, -i\}, (C_2, C_3, C_3)]$ et $[D_8, \{i, -1, -i\}, (C_2, C_4, C_4)]$ sont faiblement rigides.

Proposition 4.2.2. *Pour chaque type faiblement rigide, il existe une unique extension galoisienne finie (à $\mathbb{C}(x)$-isomorphisme près) de $\mathbb{C}(x)$ ayant ce type.*

Démonstration. L'existence du type de ramification découle du théorème d'existence de Riemann 3.2.1. Supposons que l'on a $E_1/\mathbb{C}(x)$, $E_2/\mathbb{C}(x)$ deux extensions galoisiennes finies ayant un même type de ramification faiblement rigide. On peut supposer qu'il existe une extension galoisienne $E/\mathbb{C}(x)$ telle que $E_1 \subset E$ et $E_2 \subset E$. Posons $G = Gal(E/\mathbb{C}(x))$, $G_i = Gal(E_i/\mathbb{C}(x))$ et $\rho_i : G \to G_i$ l'application de restriction (avec $i \in \{1, 2\}$). Pour $p \in \mathbb{P}^1$, posons $C_p, C_p^{(1)}, C_p^{(2)}$ les classes de conjugaisons associées à G, G_1, G_2. On a $\rho_i(C_p) = C_p^{(i)}$ par la prop 1.2.3. Posons $p_1, ..., p_r$ les points de ramifications de E. Par le théorème d'existence de Riemann, il existe des générateurs $g_1, ..., g_r$ de G avec $g_1.....g_r = 1$ et $g_i \in C_{p_i}$ pour $i \in \{1, ..., r\}$. Alors $\rho_j(g_1), ..., \rho_j(g_r)$ sont des générateurs de G_j avec les mêmes propriétés que celles de $g_1, ..., g_r$. Comme E_1 et E_2 ont le même type de ramification, par définition il existe un isomorphisme $\theta : G_2 \to G_1$ qui applique $C_p^{(2)}$ sur $C_p^{(1)}$ pour tout p. Alors $\theta(\rho_2(g_1)), ..., \theta(\rho_2(g_r))$ ont les mêmes propriétés que $\rho_j(g_1), ..., \rho_j(g_r)$. Par rigidité faible il existe un automorphisme f de G_1 tel que $f(\theta(\rho_2(g_i))) = \rho_1(g_i)$. $\delta = f \circ \theta$ est un isomorphisme de G_2 vers G_1 qui applique $\rho_2(g_i)$ à $\rho_1(g_i)$ et par suite $\delta \circ \rho_2 = \rho_1$. Ainsi ρ_1 et ρ_2 ont même noyau N. On a $E^N = E_1$, en effet soit $x \in E_1$ et $g \in N$, $g(x) = \rho_1(g)(x) = x$ car $g \in N = ker(\rho_1)$ d'où $x \in E^N$. Ainsi $E_1 \subset E^N$ ils ont même dimension

car $Gal(E^N/\mathbb{C}(x)) \cong G/N = G_1$ alors E_1 et E^N ont même degré et par suite $E^N = E_1$. On a de même $E^N = E_2$. D'où $E_1 = E_2$. □

Les types faiblement rigides définissent donc de façon unique leurs extensions à isomorphisme près.

Définition 4.2.3. *Soit $(C_1, ..., C_r)$ un uplet de classes de conjugaison d'un groupe fini G. On dit que $(C_1, ..., C_r)$ est rigide si :*

(1) Il existe des générateurs $g_1, ..., g_r$ de G avec $g_1....g_r = 1, g_i \in C_i$ pour tout $i = 1, ..., r$.

(2) Si $g'_1, ..., g'_r$ est un autre système de générateurs de G ayant la même propriété, il existe un unique $g \in G$ tel que $g.g_i.g^{-1} = g'_i$.

Définition 4.2.4. *Un type $T = [G, P, (C_p)_{p\in P}]$ est rigide si les éléments de P peuvent être écrits $p_1, ..., p_r$ ($r = |P|$)tels que les classes $C_i = C_{p_i}$ forment un uplet de classes de conjugaisons rigide.*

Un type rigide est donc faiblement rigide, prendre comme γ l'automorphisme intérieur défini par g. Ceci implique que la proposition ci-dessus reste vrai en remplaçant faiblement rigide par rigide.

Remarque 4.2.1. *L'unicité dans la deuxième condition de la définition 4.2.3 est équivalente au fait que G à un centre trivial. (On ne peut donc avoir de type rigide qu'avec les groupes à centres triviaux.)*

($\Rightarrow$) Supposons que G a un centre trivial et que l'on a $h_1 \neq h_2$ vérifiant $h_1 g_i h_1^{-1} = g'_i, h_2 g_i h_2^{-1} = g'_i$ pour tout $i = 1, ..., r$. Ceci donne $h_1 g_i h_1^{-1} = h_2 g_i h_2^{-1}$ ou encore $(h_2^{-1}h_1)g_i = g_i(h_2^{-1}h_1)$ pour tout $i = 1, ..., r$. Comme les g_i sont des générateurs alors ceci reste vrai pour tout $h \in G$ donc $h_2^{-1}h_1 \in Z(G) = \{1\}$ ce qui est absurde.

($\Leftarrow$) Supposons l'unicité vérifée dans la deuxième condition, soit $h \in Z(G)$, on a $hg_ih^{-1} = g_i$ pour tout $i = 1, ..., r$. D'autre part on sait qu'il existe un unique $g \in G$ tel que $gg_ig^{-1} = g'_i$ pour tout $i = 1, ..., r$. Donc $g(hg_ih^{-1})g^{-1} = gg_ig^{-1} = g'_i$ ou encore $(gh)g_i(gh)^{-1} = g'_i$ par unicité de g on a $gh = g$ donc $h = g^{-1}g = 1$.

Remarque 4.2.2. *Le fait d'avoir un centre trivial n'est pas suffisant pour qu'un type soit rigide. (On peut considérer le cas de D_{10}).*

Remarque 4.2.3. *Soit $(C_1, ..., C_r)$ un uplet rigide d'un groupe G. Tout automorphisme γ de G tel que $\gamma(C_i) = C_i$ (qui fixe les classes du uplet) est un automorphisme intérieur. En effet supposons que l'on a un tel automorphisme, soit*

$g_i \in C_i$ avec $g_1....g_r = 1$, on a $\gamma(g_1)....\gamma(g_r) = 1$ et $\gamma(g_i) \in C_i$ car γ fixe les C_i. A cause de la rigidité il existe un unique $g \in G$ tel que $\gamma(g_i) = gg_ig^{-1}$ car $(C_1, ..., C_r)$ est rigide. Par suite γ est un automorphisme intérieur car définit sur un système de générateurs.

Exemple 4.2.2. *Le type d'une extension abélienne fini est faiblement rigide mais n'est pas rigide.*

Le fait qu'il ne soit pas rigide vient de ce que $Z(G) = G$ et la remarque 4.2.1. Montrons qu'il est faiblement rigide. Soit $T = [G, P, (C_p)_{p\in P}]$ le type d'une extension abélienne. D'après le théorème d'existence de Riemann, il existe des générateurs $g_1, ..., g_r$ de G avec $g_1....g_r = 1, g_i \in C_i$ pour tout $i = 1, ..., r$. Soit $g'_1, ..., g'_r$ un autre système de générateurs de G ayant la même propriété, comme G est abélien alors les classes de conjugaisons sont des singletons ce qui donne $g'_i \in \{g_i\}$ ou encore $g'_i = g_i$, l'automorphisme recherché est l'identité.

Dans les lignes qui suivent, on se propose de montrer que le triplet $(C^{(n-1)}, C^{(2)}, C^{(n)})$ est rigide dans S_n. Pour cela on a besoin du lemme suivant :

Lemme 4.2.1. *Soit C_1, C_2, C_3 trois classes de conjugaisons d'un groupe G tel qu'il existe des générateurs g_1, g_2, g_3 de G avec $g_i \in C_i$ et $g_1.g_2.g_3 = 1$.*

Le triplet (C_1, C_2, C_3) est rigide
si et seulement si

(1) G a un centre trivial.

(2) pour chaque $g'_2 \in C_2$ tel que $(g_1g'_2)^{-1} \in C_3$ et $< g_1, g'_2 >= G$, il existe $h \in G$ tel que $hg_1h^{-1} = g_1$ et $hg'_1h^{-1} = g_2$.

Démonstration. ($\Rightarrow$) Comme le triplet est rigide alors G a un centre trivial. Soit $g'_2 \in C_2$ avec $(g_1g'_2)^{-1} \in C_3$ posons $g'_3 = (g_1g'_2)^{-1}$ le triplet (g_1, g'_2, g'_3) vérifie les mêmes conditions que le triplet (g_1, g_2, g_3) donc il existe $h \in G$ tel que

$$\begin{cases} hg_1h^{-1} = g_1 \\ hg'_2h^{-1} = g_2 \end{cases}$$

($\Leftarrow$) Soit $(g''_1, g''_2, g''_3) \in C_1 \times C_2 \times C_3$ avec

$$\begin{cases} g''_1g''_2g''_3 = 1 \\ < g''_1, g''_2, g''_3 >= G \end{cases}$$

Comme $g''_1 \in C_1$ alors il existe $g_0 \in G$ tel que $g''_1 = g_0g_1g_0^{-1}$.
Ainsi $g''_1g''_2g''_3 = 1 \Rightarrow g_1(g_0^{-1}g''_2g_0) = g_0^{-1}(g''_3)^{-1}g_0$. Posons $g'_2 = g_0^{-1}g''_2g_0$, on a $g'_2 \in C_2$ et $(g_1g'_2)^{-1} \in C_3$.

$G =< g_1'', g_2'' >=< g_0^{-1}g_1''g_0, g_0^{-1}g_2''g_0, g_0 >=< g_1, g_0^{-1}g_2''g_0, g_0 >=< g_1, g_2', g_0 >$.
D'autre part $g_0 \in G =< g_1'', g_2'' >$ donc il existe $\alpha_1, ..., \alpha_2, \beta_1, ..., \beta_2$ des entiers tel que $g_0 = (g_1'')^{\alpha_1}(g_2'')^{\beta_1}...(g_1'')^{\alpha_t}(g_2'')^{\beta_t} = g_0 g_1^{\alpha_1} g_0^{-1}(g_2'')^{\beta_1} g_0 g_1^{\alpha_2} g_0^{-1}(g_2'')^{\beta_2}...g_0 g_1^{\alpha_t} g_0^{-1}(g_2'')^{\beta_t}$.
En composant par g_0^{-1} et en ajustant le dernier terme, on a
$1 = g_1^{\alpha_1}(g_0^{-1}g_2''g_0)^{\beta_1} g_1^{\alpha_2}(g_0^{-1}g_2''g_0)^{\beta_2}...g_1^{\alpha_t}(g_0^{-1}g_2''g_0)^{\beta_t} g_0^{-1}$
d'où $g_0 = g_1^{\alpha_1}(g_0^{-1}g_2''g_0)^{\beta_1} g_1^{\alpha_2}(g_0^{-1}g_2''g_0)^{\beta_2}...g_1^{\alpha_t}(g_0^{-1}g_2''g_0)^{\beta_t}$.

Ce qui donne $g_0 = g_1^{\alpha_1}(g_2')^{\beta_1}...g_1^{\alpha_t}(g_2')^{\beta_t}$ d'où $g_0 \in < g_1, g_2' >$ par suite $G =< g_1, g_2' >$. Il existe donc $h \in G$ tel que $hg_1h^{-1} = g_1$ et $hg_2'h^{-1} = g_2$. En posant $g = hg_0^{-1}$ on a $gg_1''g^{-1} = g_1, gg_2''g^{-1} = g_2, gg_3''g^{-1} = g_3$, l'unicité de g vient du fait que G à un centre trivial. □

On peut donc appliquer le lemme ci-dessus pour montrer que le triplet $(C^{(n-1)}, C^{(2)}, C^{(n)})$ est rigide. On sait que S_n a un centre trivial. En posant $\sigma_1 = (n-1, n), \sigma_2 = (1, ..., n-1), \sigma_3 = (n-1, n, n-2, ...2, 1)$ (comme dans 3.3.2). Soit $\tau' \in C^{(2)}$ tel que $\sigma_2\tau' \in C^{(n)}$ on a $\tau' = (j, n)$ avec $j \in \{1, ..., n-1\}$ (sinon $\sigma_2\tau'$ n'est pas un n-cycle). $\sigma^{n-1-j}(j) = n-1, \sigma^{n-1-j}(n) = n$ donc $\sigma^{n-1-j}\tau'\sigma^{-(n-1-j)} = \tau$ et $\sigma^{n-1-j}\sigma\sigma^{-(n-1-j)} = \sigma$ le h du lemme ci-dessus est σ^{n-1-j} donc $(C^{(n-1)}, C^{(2)}, C^{(n)})$ est rigide dans S_n.

On sait que si $E/k(x)$ est definie sur κ alors son type de ramification est κ-rationnel (proposition 4.1.5). Dans le cas rigide, on a l'équivalence.

Théorème 4.2.1. *Soit $k = \overline{\kappa}$ et soit $E/k(x)$ une extension galoisienne finie. Si le type de ramification de $E/k(x)$ est rigide et κ-rationnel alors E est définie sur κ.*

Démonstration. Comme le type de ramification de E est rigide alors $G = Gal(E/k(x))$ a un centre trivial. Soit $\alpha \in Gal(\overline{\kappa}/\kappa)$, il existe un α-isomorphisme $\lambda : E \to E'$ où $E'/k(x)$ est une extension galoisienne finie par la proposition 4.1.3. Posons $G' = Gal(E'/k(x))$, C_p la classe de conjugaison de G associée à p et C_p' la classe de conjugaison de G' associée à p. Par la proposition 1.3.1 et le fait que le type de ramification est κ-rationnel pour p, q avec $q = \alpha(p)$, on a $C_q' = \lambda^*(C_p^m) = \lambda^*(C_q)$ avec le m convenable. E et E' sont donc du même type via $\lambda^* : G \to G'$ comme ce type est rigide alors E et E' son $k(x)$-isomorphe (voir [1, corollaire 3.4]). Soit donc $\mu : E \to E$ un $k(x)$-isomorphisme. Posons $\chi = \mu\lambda$. χ est un automorphisme de E de plus pour tout $a \in k$, $\chi(a) = \alpha(a)$ donc χ est un α-automorphisme de E. Comme μ est un $k(x)$-isomorphisme alors $\mu^*(C_q') = C_q$ donc $\chi^*(C_q) = \mu^*(\lambda^*(C_q)) = \mu^*(C_q') = C_q$. Ainsi χ^* est un automorphisme de G

qui fixe toutes les classes C_q par suite χ^* est un automorphisme intérieur d'après la remarque 4.2.3. Il existe donc $g \in G$ tel que $\chi^* = g^*$. Considérons $\psi = g^{-1}\chi$, ψ est un α-automorphisme et surtout $\psi^* = id$. □

Définition 4.2.5. *Un groupe G se réalise régulièrement sur un corps k s'il existe un entier m et une extension $E/k(x_1, ..., x_m)$ régulière sur k telle que $Gal(E/k(x_1, ..., x_m)) \cong G$.*

Une des caractéristiques des réalisations régulières est leur invariance par le corps de base en d'autres termes : Si G se réalise régulièrement sur k alors il se réalise régulièrement sur toute extension k_1 de k, Voir [1, cor. 1.15].

Théorème 4.2.2. *Soit $T = [G, P, (C_p)_{p\in P}]$ un type de ramification rigide et κ-rationnel. Il existe une unique extension galoisienne finie $M/\mathbb{C}(x)$ ayant ce type. Elle est définie sur une extension transcendante pure $\kappa(t_1, ..., t_s)$. Ainsi le groupe G se réalise régulièrement sur κ.*

Démonstration. Comme T est rigide (donc faiblement rigide), on a une unique extension $M/\mathbb{C}(x)$ ayant ce type par le proposition 4.2.2. Elle est définie sur une extension finiment engendré κ_1 de κ par la proposition 4.1.2. Et ce κ_1 est de degré fini sur une extension transcendante pure $\kappa_0 = \kappa(t_1, ..., t_s)$. Posons $k = \overline{\kappa_0} = \overline{\kappa_1}$, M est définie sur k. Posons $E = M_k$. Alors $E/k(x)$ est aussi de type T par la proposition 4.1.1 (5). Comme le type de E est rigide et κ_0-rationnel (car κ-rationnel), il est défini sur κ_0 (d'après le théorème 4.2.1).M est aussi définie sur κ_0 avec $M_{\kappa_0} = E_{\kappa_0}$. Donc $G = Gal(M_{\kappa_0}/\kappa_0(x)) = Gal(M_{\kappa_0}/\kappa(t_1, ..., t_s, x))$ d'après proposition 4.1.1 (2). M_{κ_0} est régulier sur κ car il l'est sur κ_0 et $\kappa \subset \kappa_0$. x est transcendant sur $\kappa(t_1, ..., t_s)$. Donc $\kappa(t_1, ..., t_s, x)$ est une extension transcendante pure de κ_0. □

4.2.2.2. *Rigidité et type de ramification produit.*

Soit $\alpha \in Aut(G_1)$ et $\beta \in Aut(G_2)$, on définit l'application

$$\alpha \times \beta : G_1 \times G_2 \to G_1 \times G_2, (\alpha \times \beta)(x, y) = (\alpha(x), \beta(y)).$$

Cette application est un automorphisme de $G_1 \times G_2$.

En effet, $(\alpha\times\beta)((g_1, g_2).(g'_1, g'_2)) = (\alpha\times\beta)((g_1.g'_1, g_2.g'_2)) = (\alpha(g_1.g'_1), \beta(g_2.g'_2)) = (\alpha(g_1).\alpha(g'_1), \beta(g_2).\beta(g'_2)) = (\alpha(g_1), \beta(g_2)).(\alpha(g'_1), \beta(g'_2)) = (\alpha \times \beta)((g_1, g_2)).(\alpha \times \beta)((g'_1, g'_2))$. Soit $(g_1, g_2) \in G_1 \times G_2$ tel que $\alpha \times \beta((g_1, g_2)) = (1, 1)$ ceci donnera $\alpha(g_1) = 1, \beta(g_2) = 1$ donc $g_1 = 1, g_2 = 1$ par suite $\alpha \times \beta$ est injectif donc bijectif

car $G_1 \times G_2$ est fini.

Proposition 4.2.3. *Soit T et T' deux types de ramification (qui remplissent les critères de 1.4.2).*

(1) Si T et T' sont faiblement rigides alors $T \times T'$ est faiblement rigide.

(2) Si T et T' sont rigides alors $T \times T'$ est rigide.

DÉMONSTRATION. (1) Posons $T = [G, P, (C_p)_{p\in P}]$ et $T' = [G', P', (C'_q)_{q\in P'}]$ avec $P = \{p_1, ..., p_r\}, P' = \{q_1, ..., q_t\}$. Comme T est faiblement rigide alors il existe un r-uplet $(g_1, ..., g_r)$ d'éléments de G tel que

$$\begin{cases} g_1...g_r = 1 \\ < g_1, ..., g_r >= G \\ g_i \in C_{p_i} \end{cases}$$

de même pour T', il existe un t-uplet $(h_1, ..., h_t)$ d'éléments de G' tel que

$$\begin{cases} h_1...h_t = 1 \\ < h_1, ..., h_t >= G' \\ h_i \in C'_{q_i} \end{cases}$$

Considérons le $r + t$-uplet $((g_1, 1), ..., (g_r, 1), (1, h_1), ..., (1, h_t))$ de $G \times G'$. On a :

$$\begin{cases} (g_1, 1)...(g_r, 1)...(1, h_1)...(1, h_t) = (1, 1) \\ < (g_1, 1), ..., (g_r, 1), ..., (1, h_1), ..., (1, h_t) >= G \times G' \\ (1, h_i) \in \{1\} \times C'_{q_i}, (g_i, 1) \in C_{p_i} \times \{1\} \end{cases}$$

Soit maintenant (u_i, v_i) un système générateur de $G \times G'$ qui vérifie les mêmes conditions. On aura alors $v_i = 1$ pour $1 \leq i \leq r$ et $u_i = 1$ pour $r + 1 \leq i \leq r + t$ de plus $\prod_{i=1}^{i=r} u_i = 1$ et $\prod_{i=r+1}^{i=r+t} v_i = 1$ et $u_i \in C_{p_i}$, $v_i \in C'_{q_i}$. Comme T et T' sont faiblement rigides, on en déduit l'existence d'un automorphisme γ de G tel que $\gamma(g_i) = u_i$ pour $1 \leq i \leq r$ de même on a un automorphisme $\delta(h_i) = v_{i+r}$ pour $1 \leq i \leq t$.
L'automorphisme $\gamma \times \delta$ permet de passer du $r + t$-uplet
$((g_1, 1), ..., (g_r, 1), (1, h_1), ..., (1, h_t))$ au du $r + t$-uplet (u_i, v_i). Ce qui implique que $T \times T'$ est faiblement rigide.

(2) Le deuxième point se fait de la même façon.

□

On aimerait utiliser les réalisations régulières de G_1 et G_2 comme groupes de Galois sur κ, pour en déduire celle de $G_1 \times G_2$. Ceci grâce au type de ramification produit. Comme conséquence les produits comme $M_{12} \times M, M_{12} \times M_{11}, ...$ (ici M désigne le monstre $M_{12}, M_{11}, ...$ les groupes de Mathieu) apparaissent comme groupes de Galois sur $\mathbb{Q}$ et les extensions qui en découlent sont régulières.

Corollaire 4.2.1. *Si deux types de ramification $T = [G, P, (C_p)_{p\in P}]$ et $T' = [G', P', (C'_q)_{q\in P'}]$ (qui admettent un produit) sont rigides et κ-rationnelles, alors $G_1 \times G_2$ se réalise régulièrement sur κ.*

Démonstration. Découle des propositions 4.1.6 et 4.2.3. □

4.3. Critère de rigidité rationnelle

Le théorème 4.2.2 nous fournit une condition nécéssaire et suffisante sur le type de ramification d'une extension galoisienne pour qu'elle soient définie sur un sous-corps $\kappa \subset k$. On cherche maintenant une condition sur un groupe G pour qu'il existe une extension définie sur $\mathbb{Q}$.

Définition 4.3.1. *Soit $(C_1, ..., C_r)$ un uplet de classes de conjugaison dans un groupe G. On dit qu'il est κ-rationnel si $C_1^m, ..., C_r^m$ est une permutation de $C_1, ..., C_r$ pour chaque entier m ayant la propriété suivante : il existe $\alpha \in Gal(\overline{\kappa}/\kappa)$ avec $\alpha^{-1}(\zeta_n) = \zeta_n^m$ où $n = |G|$*

Si le uplet est κ-rationnel pour $\kappa = \mathbb{Q}$, on l'appelle rationnel. En d'autres termes pour tout entier m premier avec l'ordre de G, les classes $C_1^m, ..., C_r^m$ sont une permutation de $C_1, ..., C_r$.

Exemple 4.3.1. *Considérons le groupe diédral D_{10}, il à 4 classes de conjugaison $C_0 = \{1\}, C_1 = \{r, r^4\}, C_2 = \{r^2, r^3\}, C_3 = \{s, sr^2, sr^3, sr, sr^4\}$.*
Un entier m est premier avec l'ordre de D_{10} s'il n'est pas divisible par 2 et 5. La première condition impose qu'il soit impair et la deuxième implique qu'on n'a que 4 cas parmi les classes modulo 10, c'est-à-dire $10k+1, 10k+3, 10k+7, 10k+9$. On a $C_3^m = C_3$ pour tout m ayant l'une de ces valeurs car ses éléments sont d'ordre 2. $C_1^{10k+1} = C_1, C_2^{10k+1} = C_2, C_1^{10k+3} = C_2, C_2^{10k+3} = C_1, C_1^{10k+7} = C_2, C_2^{10k+7} = C_1, C_1^{10k+9} = C_2, C_2^{10k+9} = C_1$. Les classes C_1 et C_2 sont donc échangées par suite le 5-uplet $(C_1, C_2, C_3, C_3, C_3)$ est rationnel.

La proposition suivante nous permet de restreindre la recherche de types de ramifcation κ-rationnels à celle d'uplets κ-rationnels. Nous épargnant des vérifications sur les points de ramification.

Proposition 4.3.1. *Si un uplet de classes de conjugaison $(C_1, ..., C_r)$ est κ-rationnel alors il existe un ensemble fini $P = \{p_1, ..., p_r\} \subset \overline{\kappa}$ tel que le type $T = [G, P, (C_p)_{p\in P}]$ est κ-rationnel, où $C_{p_i} = C_i$ pour tout $i = 1, ..., r$.*

Démonstration. Posons $n = |G|$ et $S = G(\kappa(\zeta_n)/\kappa)$. On définit l'action de S sur les classes de conjugaison C de G comme suit : pour chaque $\sigma \in S$, il existe un entier m tel que $\sigma^{-1}(\zeta_n) = \zeta_n^m$. Posons $\sigma(C) = C^m$. Cette action est bien définie car si $\sigma^{-1}(\zeta_n) = \zeta_n^{m'}$ alors $m \equiv m'(\mod n)$ donc $C^{m'} = C^m$.
Posons S_1 le stabilisateur de C_1 par cette action et $\sigma_1, ..., \sigma_l$ des représentants des classes modulo S_1. Les classes $\sigma_1(C_1), ..., \sigma_l(C_1)$ sont distinctes et sont parmi les classes $C_1, ..., C_r$ par κ- rationnalité. On suppose de plus que $C_i = \sigma_i(C_1)$ ainsi $C_1, ..., C_l$ est l'orbite de C_1 sous l'action de S.
Soit $\kappa_1 = \kappa(\zeta_n)^{S_1}$ le corps fixe de S_1 et p_1 un élément primitif de κ_1, posons $p_i = \sigma_i(p_1)$ pour $i \in \{1, ..., l\}$. Alors S permute $p_1, ..., p_l$ en effet, soit $\sigma \in S$, $\sigma(p_j) = (\sigma.\sigma_j)(p_1)$ or comme $\sigma.\sigma_j \in S = \bigcup \sigma_i S_1$ donc il existe t tel que $\sigma\sigma_j = \sigma_t$ par suite $\sigma(p_j) = p_t$. D'autre part $Stab_S(p_1) = S_1 = Stab_S(C_1)$. L'application

$$\theta : \{p_1, ..., p_l\} \to \{C_1, ..., C_l\}, p_i \mapsto C_i$$

est un isomorphisme de S-ensembles. En effet $\theta(\sigma(p_i)) = \theta(p_j) = C_j$ (1)
avec $p_j = \sigma(p_i) = \sigma\sigma_i(p_1)$ ceci implique que $p_j = (\sigma\sigma_i)(p_1)$ donc $\sigma\sigma_i \in \sigma_j S_1$. Ainsi $\sigma(C_i) = \sigma\sigma_i(C_i) = \sigma_j(C_1) = C_j$ d'où $\sigma(\theta(p_i)) = C_j$ (2).
De (1) et (2) on a $\theta(\sigma(p_i)) = \sigma(\theta(p_i))$. Ainsi $C_{\sigma(p)} = \theta(\sigma(p)) = \sigma(\theta(p)) = \sigma(C_p) = C_p^m$ où m vérifie $\sigma^{-1}(\zeta_n) = \zeta_n^m$.
On recommence le même processus, en posant S_2 le stabilisateur de C_{l+1}, p_{l+1} un élément primitif de $\kappa(\zeta_n)^{S_2}$. $C_{l+1}, ..., C_t$ l'orbite de C_{l+1} sous l'action de S et $p_{l+1}, ..., p_t$ l'orbite de p_{l+1} sous l'action de S. On arrête lorsque $C_1, ..., C_l, C_{l+1}, ..., C_t, ...$ recouvre $C_1, ..., C_r$. □

On peut donc énoncer le critère de rigidité général suivant :

Théorème 4.3.1. *Supposons que κ est un sous-corps de $\mathbb{C}$, et G est un groupe fini. Si G a des classes de conjugaisons $C_1, ..., C_r$ qui forment un uplet rigide et κ-rationnel alors G se réalise régulièrement sur κ.*

Démonstration. La preuve est la combinaison du proposition 4.3.1 et du théorème 4.2.2. □

Comme application on a :

Proposition 4.3.2. *Tous les groupes symétriques se réalisent régulièrement sur $\mathbb{Q}$.*

Démonstration. Ceci est une conséquence du théorème 4.3.1 et de l'exemple 4.1.3 appliqué au triplet rigide $(C^{(n-1)}, C^{(2)}, C^{(n)})$. □

Remarque 4.3.1. *Groupes Alternés et groupe de Mathieu M_{12}.*

On montre (Voir [1, lemme 3.20]) que si un groupe G possède un triplet (C_1, C_2, C_3) rigide et rationnel alors tout sous-groupe d'indice 2 se réalise régulièrement sur $\mathbb{Q}$. Grâce à cette proposition, on voit que tous les groupes alternés A_n se réalisent régulièrement sur $\mathbb{Q}$.
Pour le cas du groupe de Mathieu M_{12} (Voir [16]), on pose $G = Aut(M_{12})$. On a $[G : M_{12}] = 2$. On montre que G possède un triplet (C_1, C_2, C_3) rigide et rationnel (les ordres des éléments de ces classes sont respectivement 2, 3 et 12). Ceci implique que G et M_{12} se réalise régulièremnt sur $\mathbb{Q}$.

Exemple 4.3.2. *Le Monstre.*

Dans le cas du monstre, on montre qu'il possède un triplet rigide et rationnel (C_1, C_2, C_3) les ordres des éléments des classes sont 2, 3, 29 respectivement. En appliquant le Théorème 4.3.1, il se réalise régulièrement sur $\mathbb{Q}$.

BIBLIOGRAPHIE

[1] Völklein, H. Groups as Galois Groups, an Introduction. Cambridge University Press (1996).

[2] Serre, J.-P . Topics in Galois Theory. Research Notes in Mathematics 1. Jones and Bartlett (1992).

[3] Dummit D. S. and Foote, R. M. Abstract algebra. John Wiltey & Sons Inc., Hoboken, NJ, third edition (2004).

[4] Malle G. and Matzat H. Inverse Galois theory. Springer Monographs in Mathematics Berlin Heidelberg (1999).

[5] Walker R. J. Algebraic Curves. Springer-Verlag, New York Heidelberg Berlin (1978).

[6] Chenciner A. Courbes algébriques planes. Springer-Verlag Berlin Heidelberg (2008).

[7] Félix,Y. Tanré , D. Topologie algébrique : cours et exercices corrigés. Paris Dunod (2010).

[8] Forster, O. Lectures on Riemann surfaces. Graduate texts in mathematics no 81. Springer-Verlag (1981).

[9] Thompson, J, G. Some finite groups which appear as $Gal(L/K)$, where $K \subset \mathbb{Q}(\mu_n)$. Journal of Algebra, vol. 89, no 2, 437–499 (1984).

[10] Christian, U. Jensen, Arne Ledet et Noriko Yui. Generic Polynomials. Cambridge : Cambridge University Press (2002).

[11] Swan, R. G. Invariant rational functions and a problem of Steenrod, Inventiones math. Math.7 , 148-158 (1969).

[12] Noether, E. Gleichungen mit Vorgeschriebener Gruppe. Math. Ann., 78, 221-229 (1910).

[13] Débes, P. Revêtements Topologiques. Séminaires et Congrès 5. Disponible en ligne à l'adresse : www.emis.de/journals/SC/2001/5/ps (2001).

[14] Débes, P. Arithmétique des revêtements de la droite. Cours donnée à l'université de Lille. Disponible en ligne à l'adresse : www. math.univ-lille1.fr/ pde/M2debes.pdf (2007/2008).

[15] Martinet J. Un contre-exemple à une conjecture d'Emmy Noether. Séminaire N. Bourbaki. Disponible en ligne à l'adresse : www.numdam.org/item (1970).

[16] Hunt D. C. Rational rigidity and the sporadic groups. Journal of Algebra, 99, 577-592 (1986).

Annexe A

REVÊTEMENTS TOPOLOGIQUE.

A.1. Généralités.

Définition A.1.1. *(1) Soit B un espace topolgique. Un revêtement de B est la donnée d'un espace topologique X d'une application continue $f : X \to B$ ayant la propriété de trivialisation locale suivante : pour tout point $b \in B$ il existe un voisinage ouvert U de b, un espace discret non vide D et un homéomorphisme $\varphi : f^{-1}(U) \to U \times D$ tel que $p_1 \circ \varphi = f$ où $p_1 : U \times D \to U, (u, d) \mapsto u$ est la première projection.*

(2) B est appelé la base du revêtement, X l'espace totale, $f^{-1}(\{b\})$ la fibre de f au dessus de b, U est un voisinage admissible ou distingué de b et φ une trivialisation de f au dessus de U.

Définition A.1.2. *(1) Un revêtement $f : X \to B$ est dit connexe si l'espace totale X est connexe.*

(2) Un revêtement $f : X \to B$ est dit connexe par arcs si l'espace totale X est connexe par arcs.

On a des définitions similaires avec localement connexes etc...
$U \times D$ est muni de la topologie produit.

Proposition A.1.1. *Soit $f : X \to B$ une application continue. Les propriétés suivantes sont équivalentes :*

(1) f est un revêtement.

(2) Pour tout $b \in B$, il existe un voisinage ouvert U de b et une famille d'ouverts $(V_d)_{d \in D}$ de X paramétrées par un ensemble non vide D vérifiant :

(a) Les V_d sont des ouverts deux à deux disjoints de X.

(b) $f^{-1}(U) = \bigcup_{d \in D} V_d$.

(c) Pour tout $d \in D$, l'application f induit un homéomorphisme $f_d : V_d \to U$.

DÉMONSTRATION. Voir [13, prop. 1.1] □

Autour de chaque $b \in B$ il y a un voisinage admissible U et au dessus une pile de copies V_d de ce voisinage paramétrées par un espace discret D. Les V_d sont appelés les feuillets du revêtement au dessus de U.

Remarque A.1.1. *(1) un revêtement $f : X \to B$ est un homéomorphisme local. Donc les espaces X et B partagent les mêmes propriétés locales.*

(2) Si U est un voisinage admissible et $U' \subset U$ alors U' est un voisinage admissible. En effet,on a $f^{-1}(U') \subset f^{-1}(U) = \bigcup_{d\in D} V_d$ donc $f^{-1}(U') = \bigcup_{d\in D}(V_d \cap f^{-1}(U'))$ posons $V'_d = V_d \cap f^{-1}(U')$ alors les V'_d sont des ouverts deux à deux disjoints de plus la restriction de f à V'_d est un homéomorphisme sur U'.

(3) Si on suppose U connexe par arcs alors V_d sera connexe par arcs pour tout $d \in D$. Les feuillets V_d sont les composantes connexes par arcs de $f^{-1}(U)$ car ils sont deux à deux disjoints.

Proposition A.1.2. *Pour tout ouvert $B' \subset B$, $f_{/f^{-1}(B')} : f^{-1}(B') \to B'$ est un revêtement.*

DÉMONSTRATION. Découle directement de la remarque (2). ci-dessus. □

Exemple A.1.1. *(1) <u>Revêtements triviaux.</u>*

Soit B un espace topologique. Pour tout ensemble non vide D (que l'on muni de la topologie discrète), l'application $f : B \times D \to B$ définie par $f(b, d) = b$ est un revêtement de B. Un tel revêtement est appelé revêtement trivial. (il y a donc une infinité de revêtement triviaux).

(2) <u>Revêtement du disque privé de son centre.</u>

Considérons l'ensemble $D^*(0, r) = \{z \in \mathbb{C}/0 < |z| < r\}$, c'est le disque complexe de rayon r privé de son centre 0. On suppose que $D^*(0, r)$ est munit de la topologie induite par celle de $\mathbb{C}$. Soit $e \in \mathbb{N}^*$, l'application $f_e : D^*(0, r^{\frac{1}{e}}) \to D^*(0, r), z \mapsto z^e$ est un revêtement de $D^*(0, r)$.En effet : f_e est un polynôme complexe donc une application continue. Soit $b \in D^*(0, r)$ et ς une racine primitive e-ème de 1.

(preuve)

(a) Soit $a \in D^*(0, r^{\frac{1}{e}})$ tel que $a^e = b$ et V un voisinage ouvert de a contenu dans $D^*(0, r^{\frac{1}{e}})$ tel que les $V_j = \varsigma^j V$ soient deux à deux disjoints pour $j \in \{0, 1, ..., e - 1\}$.$V_j = \varsigma^j V$ est un ouvert homéomorphe à V car la multiplication par ς^j est une application ouverte et injective.

(b) Posons $f_e(V) = U$, U est un ouvert homéomorphe à V car f_e est une application injective et ouverte (puisque c'est une application holomorphe donc la dérivée ne s'annule pas sur $D^*(0, r^{\frac{1}{e}})$) et $b \in U$.On a $f_e^{-1}(U) = \bigcup_{j=0}^{e-1} V_j$.

(c) La restriction de f_e à V_j est un homéomorphisme sur U.
Donc f_e est une revêtement de $D^*(0, r^{\frac{1}{e}})$.

Définition A.1.3. *(1) Un revêtement est dit localement fini si toutes ses fibres sont des ensembles finis.*

(2) Si toutes les fibres d'un revêtement $f : X \to B$ sont en bijections, on appelle degré du revêtement le nombre d'éléments pouvant être infini d'une fibre $f^{-1}(\{b\})$ avec $b \in B$. On le note $deg(f)$.

(3) Un revêtement est dit fini s'il est localement fini et toutes ses fibres sont en bijections.

Si la base B d'un revêtement est connexe. Alors les fibres de f sont toutes en bijections. En particulier $f : X \to B$ est un revêtement fini s'il est localement fini.

A.2. Relèvements des homotopies de chemins.

Définition A.2.1. *Soit $f : X \to B$ un revêtement et $g : Y \to B$ une application continue. Un relevement (ou relevé)de g est une application continue $\widetilde{g} : Y \to E$ telle*

$g = f \circ \widetilde{g}$.

Les revêtements relèvent les chemins et les homotopies de chemins.

Proposition A.2.1. *(1) Soit $f : X \to B$ un revêtement. Pour tout chemin $\gamma : I \to B$ d'origine $b \in B$, pour tout $x \in f^{-1}(\{b\})$, il existe un unique relèvement $\widetilde{\gamma} : I \to X$ de d'origine x.*

(2) Si deux chemins sont homotopes alors leurs relèvements ayant même point initial ont même extrémité et sont homotopes.

Démonstration. Voir [7, th. 4.5 et 4.6] □

Proposition A.2.2. *Soit $f : X \to B$ un revêtement, on suppose B connexe par arcs et localement connexe par arcs. Soit X_1 une composante connexe de X. Alors la restriction de f à X_1 est un revêtement . Si de plus $f^{-1}(\{b\}) \subset X_1$ pour tout $b \in B$, alors $X = X_1$.*

Démonstration. Voir [1, cor. 4.13] □

A.3. Action de la monodromie.

Soit $f : X \to B$ un revêtement, $b \in B$ et $\pi_1(B, b)$ le groupe fondamental basé en b. Pour tout $[\gamma] \in \pi_1(B, b)$, on a une application $T_{f,b}([\gamma]) : f^{-1}(\{b\}) \to f^{-1}(\{b\})$ qui à tout $x \in f^{-1}(\{b\})$ associe l'extrémité $\widetilde{\gamma}(1)$ du relèvement $\widetilde{\gamma}$ de γ d'origine x. D'après la proposition A.2.1, l'extrémité $\widetilde{\gamma}(1)$ ne dépend pas du représentant de la classe $[\gamma]$. D'autre part $f \circ \widetilde{\gamma} = \gamma$ donc $(f \circ \widetilde{\gamma})(1) = \gamma(1) = b$, d'où $T_{f,b}([\gamma])$ est bien définie.
Considérons l'application $T = T_{f,b} : \pi_1(B, b) \to Perm(f^{-1}(\{b\})), [\gamma] \mapsto T_{f,b}([\gamma])$.

Proposition A.3.1. *L'application T est une action de $\pi_1(B, b)$ sur la fibre $f^{-1}(\{b\})$. On suppose B connexe par arcs, alors T est transitive si et seulement si X est connexe par arcs.*

Démonstration. (1) <u>T est une action</u>.

Soit $[\gamma], [\delta] \in \pi_1(B, b)$, posons $T([\gamma])(x) = y, T([\delta])(y) = z, T([\delta][\gamma])(x) = l$. On a : $l = T([\delta\gamma])(x)$ d'où l est l'extrémité du relèvement $\widetilde{\delta\gamma}$ de $\delta\gamma$ d'origine x. D'autre part y est l'extrémité du relèvement $\widetilde{\gamma}$ de γ d'origine x et z est l'extrémité du relèvement $\widetilde{\delta}$ d'origine y. On a $\widetilde{\delta}\widetilde{\gamma} = \widetilde{\delta\gamma}$, par suite $l = z$ ou encore $T([\delta])(T([\gamma])(x) = T([\delta][\gamma])(x)$, ce qui donne $T([\delta]) \circ T([\gamma]) = T([\delta][\gamma])$.

(2) Supposons X connexe par arcs.

Soit $x, y \in f^{-1}(\{b\})$, il existe un chemin γ dans X de x vers y. $[f \circ \gamma] \in \pi_1(B, b)$ et $T([f \circ \gamma])(x) = y$. Donc l'action T est transitive.
Inversement supposons que T est une action transitive. Soit $(x, y) \in X^2$, comme B est connexe par arcs, il existe un chemin δ_1 qui joint $f(x)$ à b et δ_2 qui joint $f(y)$ à b dans B. Posons $x_0 = \widetilde{\delta}_1(1)$ et $y_0 = \widetilde{\delta}_2(1)$ où $\widetilde{\delta}_1$ et $\widetilde{\delta}_2$ sont les relèvements respectifs de δ_1, δ_2 d'origine respective x et y. On a $x_0 \in f^{-1}(\{b\})$. Par hypothèse il existe $\gamma \in \pi_1(B, b)$ tel que $T([\gamma])(x_0) = y_0$. Considérons $\widetilde{\gamma}$ le relèvement de γ tel que $\widetilde{\gamma}(0) = x_0, \widetilde{\gamma}(1) = y_0$, on a : $\widetilde{\delta}_2\widetilde{\gamma}\widetilde{\delta}_1$ qui joint x à y et X est connexe par arcs.

□

Comme on a supposé B connexe par arcs, on a $\pi_1(B) = \pi_1(B, b)$ pour tout $b \in B$. L'action de T est appelée action de la monodromie sur la fibre $f^{-1}(\{b\})$. Le groupe $G = T(\pi_1(B))$ est appelé le groupe de monodromie.

A.4. Revêtements galoisiens.

A.4.1. Morphismes de revêtements.

Définition A.4.1. *(1) Soit $f : X \to B$ et $f' : X' \to B$ deux revêtements. On appelle morphisme de f vers f' toute application continue $\chi : X \to X'$ tel que $f' \circ \chi = f$.*

(2) Un isomorphisme de revêtements est un morphisme de revêtement qui est en plus un homéomorphisme.

Si $\chi : X \to X'$ est un isomorphisme de revêtement alors sa réciproque $\chi^{-1} : X' \to X$ est aussi un morphisme de revêtement. En effet χ^{-1} est continue et comme $f' \circ \chi = f$ alors $f' = f \circ \chi^{-1}$. L'existence d'un isomorphisme de revêtement entre deux revêtements définie une relation d'équivalence entre les revêtements ayant une base B fixée.

Définition A.4.2. *Deux revêtements sont dits équivalents s'il existe un isomorphisme de revêtement entre eux.*

Nous avons vu que le groupe fondamental $\pi_1(B, b)$ agit sur $f^{-1}(\{b\})$. En réalité cette action détermine une classe d'équivalence sur l'ensemble des revêtements de B dont la fibre est en bijection avec $f^{-1}(\{b\})$, comme le montre les deux propriétés suivantes :

Proposition A.4.1. *Soit $f : X \to B$ et $f' : X' \to B$ deux revêtements équivalents alors les actions de $\pi_1(B, b)$ sur $f^{-1}(\{b\})$ et sur $f'^{-1}(\{b\})$ sont équivalentes.*

Démonstration. Voir [13, prop. 3.1]. □

Proposition A.4.2. *Soit $f_1 : X_1 \to B$ et $f_2 : X_2 \to B$ deux revêtements, on suppose X_1, X_2, B connexes par arcs et localement connexes par arcs. Soit $x_i \in X_i$ ($i \in \{1, 2\}$) avec $f_1(x_1) = f_2(x_2) = b$. Supposons que pour tout $[\gamma] \in \pi_1(B, b)$ on a : $T_f([\gamma])(x_1) = x_1 \Leftrightarrow T_{f'}([\gamma])(x_2) = x_2$. Alors les revêtements f_1 et f_2 sont équivalents. En d'autres termes il existe un homéomorphisme $\chi : X_1 \to X_2$ avec $f_2 \circ \chi = f_1$ et $\chi(x_1) = x_2$.*

Démonstration. Voir [1, cor. 4.14]. □

En supposant que les fibres sont finis de degré n ce qui nous sera utile pour la suite, on a le résultat suivant :

Proposition A.4.3. *Soit B un espace topologique connexe par arcs, localement connexe par arcs et localement simplement connexe. Les classes d'équivalence de revêtements $f : X \to B$ connexe de degré n de B correspondent de façon buinivoque aux classes d'équivalence d'actions transitives $T : \pi_1(B) \to S_n$ ou encore aux classes d'équivalence de sous-groupes d'indices n de $\pi_1(B)$.*

DÉMONSTRATION. Voir [13, th. 3.2] □

A.4.2. Groupe des automorphismes d'un revêtement.

Définition A.4.3. *Soit $f : X \to B$ un revêtement, un automorphisme de f ou une transformation de deck est un isomorphisme de revêtement de f vers f.*

On note $Deck(f)$ ou $Aut(f)$ l'ensemble des automorphismes de f. $Aut(f)$ muni de la composition des applications est un groupe. On l'appelle groupe des automorphismes de f ou groupe des transformations de deck de f.

Proposition A.4.4. *Le groupe $Aut(f)$ opère sur chaque fibre $f^{-1}(\{b\})$ pour tout $b \in B$.*

DÉMONSTRATION. Soit $\chi \in Aut(f)$ pour tout $x \in f^{-1}(\{b\})$, on a $(f \circ \chi)(x) = f(x) = b$ donc $\chi(x) \in f^{-1}(\{b\})$ d'autre part $\chi_{/f^{-1}(\{b\})}$ est une bijection car χ l'est donc $\chi_{/f^{-1}(\{b\})} \in Perm(f^{-1}(\{b\}))$. L'application $Aut(f) \to Perm(f^{-1}(\{b\})), x \mapsto \chi_{/f^{-1}(\{b\})}$ est un morphisme de groupe. En effet $(\chi \circ \psi)_{/f^{-1}(\{b\})} = \chi_{/f^{-1}(\{b\})} \circ \psi_{/f^{-1}(\{b\})}$. □

Nous avons donc deux groupes qui opèrent sur $f^{-1}(\{b\})$, le groupe fondamental de l'espace B (où la partie agissante le groupe de monodromie) et le groupes des automorphismes $Aut(f)$ de f. Quelle relation y a t-il entre ces actions ?

Proposition A.4.5. *Soit $f : X \to B$ un revêtement.*

(1) Soit $(a, b) \in B^2$ et γ un chemin de a vers b. Pour chaque $x \in f^{-1}(\{a\})$ posons $\gamma x = \widetilde{\gamma}(1)$ où $\widetilde{\gamma}$ est le relèvement de γ de point initial x. Alors l'application $x \mapsto \gamma x$ est une bijection entre $f^{-1}(\{a\})$ et $f^{-1}(\{b\})$. Cette bijection commute avec l'action de $Aut(f)$ cet-à-dire $\chi(\gamma(x)) = \gamma(\chi(x))$ pour tout $\chi \in Aut(f)$.

(2) L'action de $Deck(f)$ sur $f^{-1}(\{b\})$ commute avec celle de $\pi_1(B, b)$.

DÉMONSTRATION. (1) Posons $l_\gamma : f^{-1}(\{a\}) \to f^{-1}(\{b\}), x \mapsto \gamma x$ et $s_{\overline{\gamma}} : f^{-1}(\{b\}) \to f^{-1}(\{a\}), x \mapsto \overline{\gamma} x$ ($\overline{\gamma} x$ se défini comme γx), montrons que $s_{\overline{\gamma}} = l_\gamma^{-1}$ Soit $t \in [0, 1]$, $(f \circ \overline{\widetilde{\gamma}})(t) = f(\overline{\widetilde{\gamma}}(t)) = f(\widetilde{\gamma}(1-t)) = (f \circ \widetilde{\gamma})(1-t) = \gamma(1-t) = \overline{\gamma}$. Donc $f \circ \overline{\widetilde{\gamma}} = \overline{\gamma}$ ce qui implique $\overline{\widetilde{\gamma}}$ est le relèvement de $\overline{\gamma}$ d'origine $\gamma x = \widetilde{\gamma}(1)$. Ainsi $\overline{\gamma}(\gamma x) = \overline{\widetilde{\gamma}}(1) = \widetilde{\gamma}(1-1) = \widetilde{\gamma}(0) = x$ d'où $s_{\overline{\gamma}}(l_\gamma(x)) = x$ par suite $s_{\overline{\gamma}} \circ l_\gamma = id$. On montre de même que $l_\gamma \circ s_{\overline{\gamma}} = id$ Pour la deuxième partie du 1) , on a $f \circ (\chi \circ \widetilde{\gamma}) = f \circ \widetilde{\gamma} = \gamma$ donc $\chi \circ \widetilde{\gamma}$ est le relèvement de γ de point initial $\chi(\widetilde{\gamma}(0)) = \chi(x)$ donc $\gamma(\chi(x))$ est l'extrémité de $\chi \circ \widetilde{\gamma}$ d'où $\gamma(\chi(x)) = (\chi \circ \widetilde{\gamma})(1) = \chi(\widetilde{\gamma}(1)) = \chi(\gamma(x))$.

(2) Le 2) découle du 1) en prenant $a = b$.

□

Proposition A.4.6. *Soit $f : X \to B$ un revêtement.*

(1) On suppose que X est connexe par arcs. Si $\chi \in Aut(f)$ fixe un point $x \in X$ alors $\chi = id$.

(2) On suppose que X est connexe par arcs et que $Aut(f)$ a un sous groupe G qui opère transitivement sur la fibre $f^{-1}(\{b\})$. Alors $G = Aut(f)$.

DÉMONSTRATION. (1) Soit $x \in X$ tel que $\chi(x) = x$ et $y \in X$. Soit $\widetilde{\gamma}$ un chemin qui joint x à y, $f \circ \widetilde{\gamma} = \gamma$ est un chemin de B qui joint $f(x)$ à $f(y)$ et $\widetilde{\gamma}$ est l'unique relèvement de γ de point initial x. D'autre part on a $f \circ (\chi \circ \widetilde{\gamma}) = (f \circ \chi) \circ \widetilde{\gamma} = f \circ \widetilde{\gamma} = \gamma$ donc $\chi \circ \widetilde{\gamma}$ est le relèvement de γ de point initial $(\chi \circ \widetilde{\gamma})(0) = \chi(\widetilde{\gamma}(0)) = \chi(x) = x$ d'où $\chi \circ \widetilde{\gamma} = \widetilde{\gamma}$ par suite $\chi(\widetilde{\gamma}(1)) = \widetilde{\gamma}(1)$ ce qui donne $\chi(y) = y$ et $\chi = id$.

(2) Soit $x \in f^{-1}(\{b\})$ pour tout $\chi \in Aut(f)$ il existe $\psi \in G$ tel que $\psi(\chi(x)) = x$ donc $(\psi \circ \chi)(x) = x$ d'après 1) $\psi \circ \chi = id$ donc $\chi = \psi^{-1} \in G$.

□

Définition A.4.4. *Un revêtement $f : X \to B$ est dit galoisien si X est connexe par arcs et $Aut(f)$ opère transitivement sur une fibre $f^{-1}(\{b\})$ $(b \in B)$.*

Si X est connexe par arcs, il en est de même de B. En conséquence $Aut(f)$ opère transitivement sur toutes les fibres $f^{-1}(\{b\})$.

Exemple A.4.1. *L'application $f_e : D^*(0, r^{\frac{1}{e}}) \to D^*(0, r), z \mapsto z^e$ est un revêtement galoisien de degré e, pour chaque $e \in \mathbb{N}^*$ et $r > 0$. Son groupe des automorphismes est cyclique d'ordre e et est formé des applications $l_\varsigma : z \mapsto \varsigma z, \varsigma \in \mu_e$.*

(preuve) On sait que f_e est un revêtement (exemple A.1.1) pour $\varsigma \in \mu_e$, l'application $l_\varsigma : D^*(0, r^{\frac{1}{e}}) \to D^*(0, r^{\frac{1}{e}}), z \mapsto \varsigma z$ est une application holomorphe et bijective donc c'est un homéomorphisme. De plus $(f_e \circ l_\varsigma)(z) = f_e(\varsigma z) = (\varsigma z)^e = z^e = f_e(z)$ donc l_ς est un automorphisme de f_e. De plus $\{l_\varsigma, \varsigma \in \mu_e\}$ opère transitivement sur les fibres de f_e (en effet soit z_1, z_2 tels que $z_1^e = z_2^e$ alors$(\frac{z_1}{z_2})^e = 1$, il existe $\varsigma \in \mu_e$ tel que $\varsigma = \frac{z_1}{z_2}$) donc $Aut(f_e) = \{l_\varsigma, \varsigma \in \mu_e\}$.

Proposition A.4.7. *Soit $f : X \to B$ un revêtement galoisien.*

(1) Le degré de f est égal à l'ordre de n (pouvant être infini)de $Aut(f)$. Pour chaque voisinage admissible et connexe par arcs U de B(resp chaque point $b \in B$), l'ensemble $f^{-1}(\{U\})$ (resp $f^{-1}(\{b\})$) à n feuillets (resp n éléments) et ils sont permutés transitivement par $Aut(f)$.

(2) Soit $x \in X$ et $b = f(x)$. Il existe un unique morphisme surjectif $\Phi_x : \pi_1(B,b) \to Aut(f)$ tel que $\Phi_x([\gamma])$ applique $T_f([\gamma])(x) = [\gamma]x$ à x pour chaque $[\gamma] \in \pi_1(B,b)$.

DÉMONSTRATION. Voir [1, prop. 4.19] □

Remarque A.4.1. *Soit $f : X \to B$ un revêtement et $g : B \to B$ un homéomorphisme.*

(1) $g \circ f$ est un revêtement de B.

En effet, $g \circ f$ est une application continue. Soit $b \in B$, il existe $a \in B$ tel que $b = g(a)$. Considérons V un ouvert trivialisant de a pour f, on a $f^{-1}(V) = \bigcup_{d\in D} V_d$ avec les V_d deux à deux disjoints et homéomorphes à V via f. Posons $U = g(V)$, on a $g^{-1}(U) = V$ donc $f^{-1}(g^{-1}(U)) = f^{-1}(V)$. Ainsi $(g \circ f)^{-1}(U) = \bigcup_{d\in D} V_d$ donc $g \circ f$ est un revêtement.

(2) Si $f : X \to B$ un revêtement galoisien fini alors $g \circ f$ est un revêtement galoisien fini et $Aut(f) = Aut(g \circ f)$.
Si f est galoisien fini alors X est connexe par arcs et $g\circ f$ est un revêtement fini car ses fibres sont évidemment finies. Soit $\chi \in Aut(f)$, on a $f \circ \chi = f$, donc $(g \circ f) \circ \chi = g \circ (f \circ \chi) = g \circ f$ d'où $Aut(f) \subset Aut(g \circ f)$. Soit $x, y \in (g \circ f)^{-1}(\{b\}) = f^{-1}(\{a\})$ (ou $g^{-1}(b) = a$) il existe $\chi \in Aut(f)$ tel que $\chi(x) = y$ donc $Aut(f)$ opère transitivement sur les fibres de $g \circ f$ et par suite $Aut(f) = Aut(g \circ f)$ d'après la proposition A.4.6.

Annexe B

GÉNÉRATEURS DE S_N.

Proposition B.0.8. *S_n est engendré par les transpositions (t, n) pour tout $t \in \{1, ..., n-1\}$.*

DÉMONSTRATION. On sait que toute permutation se décomposent de facon unique comme produit de cycles disjoints et qu'un cycle $(a_1, ..., a_t)$ s'écrit comme produit de transpositions $(a_1a_2)(a_2a_3)...(a_{t-1}a_t)$. Il suffit donc de montrer qu'une transposition (ab) s'écrit comme produit de transpositions (kn). Ce qui est le cas avec $(ab) = (an)(bn)(an)$. □

Proposition B.0.9. *Tout sous-groupe G de S_n qui contient σ_2 et σ_3 est transitif.(Où $\sigma_2 = (1, ..., n-1), \sigma_3 = (n-1, n, n-2...1)$).*

DÉMONSTRATION. En effet soit $a < b$ deux éléments de $\{1, ..., n\}$. Si $b \leq n-1$ on a $b = \sigma_2^{b-a}(a)$ et $\sigma_2^{b-a} \in G$. Si $b = n$ alors $\sigma_2^{n-1-a}(a) = n-1$ et $(\sigma_3 \circ \sigma_2^{n-1-a})(a) = n = b$. Les inverses des applications ci-dessus marchent pour $b < a$.

□

Proposition B.0.10. *Soit G sous-groupe transitif de S_n qui contient un $(n-1)$-cycle et une transposition alors $G = S_n$.*

DÉMONSTRATION. On peut numéroter les éléments de telle facon que le $(n-1)$-cycle soit $\theta = (12...n-1)$. Posons (i_0j_0) la transposition de G.
Comme G est transitif, il existe dans G une permutation σ telle que $\sigma(j_0) = n$. On a $\sigma(i_0j_0)\sigma^{-1} = (\sigma(i_0)\sigma(j_0)) = (\sigma(i_0)n)$. Posons $t_0 = \sigma(i_0)$, $t_0 \neq n$ car σ est injective et $\sigma(j_0) = n$. G contient donc la transposition (t_0n) avec $1 \leq t_0 \leq n-1$ car G est un groupe.
D'autre part $\theta^k.(t_0n).\theta^{-k} = (\theta^k(t_0)\theta^k(n)) = (\theta^k(t_0)n)$ où k est un entier. En faisant varier k on a $\theta^k(t_0)$ qui prend toutes les valeurs de $\{1, ..., n-1\}$ ce qui donne $G = S_n$.

□