Aspects commutatifs et non commutatifs de la théorie inverse de Galois

Angelot Behajaina

▶ **To cite this version:**

Angelot Behajaina. Aspects commutatifs et non commutatifs de la théorie inverse de Galois. Algèbre commutative [math.AC]. Normandie Université, 2021. Français. NNT : 2021NORMC212 . tel-03250407

HAL Id: tel-03250407
https://theses.hal.science/tel-03250407

Submitted on 4 Jun 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Normandie Université

THÈSE

Pour obtenir le diplôme de doctorat

Spécialité MATHEMATIQUES

Préparée au sein de l'Université de Caen Normandie

Aspects commutatifs et non commutatifs de la théorie inverse de Galois

Présentée et soutenue par
Angelot BEHAJAINA

Thèse soutenue le 28/05/2021 devant le jury composé de		
M. JEAN-MARC COUVEIGNES	Professeur des universités, Université Bordeaux 1 Sciences et Techno	Rapporteur du jury
M. DAVID HARARI	Professeur des universités, Université Paris 11 Paris-Sud	Rapporteur du jury
Mme SARA CHECCOLI	Maître de conférences, Institut Fourier	Membre du jury
M. PIERRE DEBES	Professeur des universités, Université Lille 1 Sciences Et Technolog	Membre du jury
M. JÉRÔME POINEAU	Professeur des universités, Université Caen Normandie	Membre du jury
M. BRUNO DESCHAMPS	Professeur des universités, Université Le Mans	Directeur de thèse
M. FRANCOIS LEGRAND	Docteur, Université Caen Normandie	Co-directeur de thèse
Mme ANNA CADORET	Professeur des universités, IMJ-PRG	Président du jury

Thèse dirigée par BRUNO DESCHAMPS et FRANCOIS LEGRAND, Laboratoire de Mathématiques 'Nicolas Oresme' (Caen)

UNIVERSITÉ CAEN NORMANDIE

MIIS

LMNO

Avant-propos

Cette thèse porte sur la théorie inverse de Galois. Traditionnellement, cette théorie est étudiée sur un corps commutatif K et la première question en est le problème inverse de Galois : pour tout groupe fini G, existe t-il une extension galoisienne L/K de groupe G ? Dans cette question, L est bien entendu un corps commutatif. Quant à la définition d'extension galoisienne L/K, la plus répandue est celle demandant que L/K soit algébrique, normale et séparable.

Nonobstant, il existe une notion d'extension galoisienne qui s'applique à tous les corps, commutatifs ou non. En effet, d'après Artin, une extension de corps L/H est galoisienne si le sous-corps de L laissé fixe sous l'action de $\mathrm{Aut}(L/H)$ est égal à H. Avec cette définition, la théorie inverse de Galois peut être étudiée sur tous les corps. Alors que le cas des corps commutatifs est étudié depuis Hilbert et Noether, il est frappant que, jusqu'à très récemment, personne ne se soit intéressé aux aspects non commutatifs de la théorie inverse de Galois.

Cette thèse contribue à la fois aux aspects commutatifs et non commutatifs de la théorie et est composée de deux parties. La première partie (chapitre 1) est basée sur l'article [Beh20] et porte sur les corps commutatifs. La deuxième partie porte quant à elle sur les corps quelconques et est constituée de trois chapitres. Le chapitre 2 contient les éléments de théorie des corps nécessaires à la lecture des chapitres 3 et 4, qui sont eux basés sur les articles [Beh21] et [BDL20].

Ces deux parties sont précédées d'une introduction dans laquelle nous présentons rapidement le contenu de chaque chapitre et nos principaux résultats (voir §0.3). Dans le but de relier nos résultats à la littérature, nous présentons au préalable l'état de l'art du domaine, à la fois sur les corps commutatifs (voir §0.1) et sur les corps quelconques (voir §0.2).

Table des matières

Avant-propos **1**

Table des matières **3**

0 Introduction **5**
0.1 Théorie inverse de Galois sur les corps commutatifs : état de l'art 5
0.1.1 Problème inverse de Galois 5
0.1.2 Théorème d'irréductibilité de Hilbert 5
0.1.3 Problème inverse de Galois régulier 6
0.1.4 Problèmes de plongement finis 6
0.2 Théorie inverse de Galois sur les corps quelconques : état de l'art 7
0.3 Présentation du travail 8
0.3.1 Chapitre 1 : Réalisations galoisiennes explicites de certaines familles de 2-groupes 8
0.3.2 Chapitre 2 : Eléments de théorie des corps quelconques 9
0.3.3 Chapitre 3 : Théorie inverse de Galois sur les corps de fractions rationnelles tordus 9
0.3.4 Chapitre 4 : Problèmes de plongement finis sur les corps non commutatifs 10

1 Réalisations galoisiennes explicites de certaines familles de 2-groupes **13**
1.1 Préliminaires 13
1.1.1 Extensions de corps de fonctions 13
1.1.2 Sur les 2-groupes 14
1.1.3 Un lemme sur les racines de l'unité 16
1.2 Produits semi-directs $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ 16
1.2.1 Notations 16
1.2.2 Résultats préparatoires 17
1.2.3 Résultat principal 21
1.2.4 Corollaires 23
1.3 Groupes de quaternions généralisés 23
1.3.1 Notations 23
1.3.2 Réalisations régulières explicites 24
1.3.3 Réalisations explicites de Q_{2^n} sur $\mathbb{Q}$ 25
1.3.3.1 Bons premiers 26
1.3.3.2 Invariant canonique de l'inertie 28
1.3.3.3 Théorème principal 28

2 Eléments de théorie des corps quelconques **31**
2.1 Généralités . . . 31
2.1.1 Corps . . . 31
2.1.2 Corps de fractions . . . 32
2.1.3 Corps tordus . . . 33
2.1.3.1 Anneaux de polynômes et corps de fractions rationnelles tordus . 33
2.1.3.2 Corps de séries tordus . . . 34
2.2 Formes réduites . . . 35
2.3 Théorie de Galois . . . 36
2.3.1 Extensions de corps . . . 37
2.3.2 Extensions galoisiennes . . . 37
2.3.3 Théorie de Galois finie . . . 38
2.3.4 Théorie de Galois infinie . . . 39

3 Théorie inverse de Galois sur les corps de fractions rationnelles tordus **41**
3.1 Preuve du théorème 0.3.5 . . . 41
3.2 Preuve du théorème 0.3.6 . . . 44

4 Problèmes de plongement finis sur les corps gauches **49**
4.1 Préliminaires . . . 49
4.1.1 Extensions galoisiennes de corps quelconques . . . 49
4.1.2 Résultats sur les corps de fractions rationnelles tordus . . . 50
4.1.3 Extensions de corps de fractions rationnelles tordus . . . 51
4.2 Problèmes de plongement finis . . . 53
4.2.1 Applications de restriction . . . 53
4.2.2 Problèmes de plongement finis . . . 57
4.2.2.1 Terminologie . . . 57
4.2.2.2 Passage des corps quelconques aux corps commutatifs et vice-versa 57
4.2.2.3 Solutions géométriques . . . 58
4.3 Résolution de problèmes de plongement finis scindés . . . 59
4.4 A propos de la réduction faible→scindé . . . 60
4.4.1 Extensions de la réduction faible→scindé . . . 60
4.4.2 Extension du théorème 4.3.1 . . . 62
4.4.3 Remarque finale . . . 62

Bibliographie **65**

Chapitre 0

Introduction

0.1 Théorie inverse de Galois sur les corps commutatifs : état de l'art

0.1.1 Problème inverse de Galois

La théorie de Galois usuelle associe à toute extension galoisienne finie $L/\mathbb{Q}$ un groupe fini appelé *groupe de Galois* de $L/\mathbb{Q}$ et noté $\mathrm{Gal}(L/\mathbb{Q})$. La réciproque, remontant à Hilbert et Noether, est appelée *problème inverse de Galois*. Plus précisément, ce problème demande si tout groupe fini est groupe de Galois d'une extension galoisienne finie de $\mathbb{Q}$. D'une manière générale, le problème inverse de Galois se pose sur n'importe quel corps commutatif K :

PIG$_K$: *Tout groupe fini est-il le groupe de Galois d'une extension galoisienne de K ?*

Ce problème admet une réponse négative sur certains corps : $\mathbb{R}$, les corps algébriquement clos, les corps finis, etc. Sur $\mathbb{Q}$, malgré la simplicité de l'énoncé, il demeure encore largement ouvert. On sait cependant réaliser certains groupes finis comme groupes de Galois sur $\mathbb{Q}$. Par exemple, les groupes abéliens (voir, par exemple, [Dèb09, théorème 2.1.3]) et les groupes symétriques sont groupes de Galois sur $\mathbb{Q}$ et les preuves ne sont pas très difficiles. Des résultats plus profonds sont, par exemple, le théorème de Shafarevich, qui affirme que les groupes résolubles sont groupes de Galois sur $\mathbb{Q}$ (voir [NSW08, 9.6.1]), et le résultat de Zywina, qui affirme que $\mathrm{PSL}_2(\mathbb{F}_p)$ est groupe de Galois sur $\mathbb{Q}$ pour tout nombre premier p (voir [Zyw15]).

0.1.2 Théorème d'irréductibilité de Hilbert

La preuve du théorème de Shafarevich utilise des méthodes cohomologiques. Quand au résultat de Zywina, l'approche consiste à étudier certaines représentations du groupe de Galois absolu de $\mathbb{Q}$. Nous n'en dirons pas plus sur ces méthodes dans cette introduction et nous consacrerons davantage à l'approche géométrique au problème inverse de Galois.

L'approche géométrique à la réalisation d'un groupe fini G comme groupe de Galois sur $\mathbb{Q}$ consiste à introduire une indéterminée T et à construire une extension galoisienne $E/\mathbb{Q}(T)$ de groupe G. Si l'on dispose d'une telle extension, il existe une infinité de $t_0 \in \mathbb{Q}$ telle que la spécialisation $E_{t_0}/\mathbb{Q}$ de $E/\mathbb{Q}(T)$ en t_0 (voir §1.1.1 pour la définition) soit galoisienne de groupe G. Cela repose sur le fameux théorème dû à Hilbert suivant :

Théorème d'irréductibilité de Hilbert. *Soit $P(T,X) \in \mathbb{Q}(T)[X]$ un polynôme irréductible sur $\mathbb{Q}(T)$. Alors, il existe une infinité de nombres rationnels t_0 tels que le polynôme $P(t_0,X)$ soit irréductible sur $\mathbb{Q}$.*

Plus généralement, un corps K est dit *hilbertien* s'il vérifie le théorème précédent en remplaçant $\mathbb{Q}$ par K et en supposant P séparable. Par exemple, les corps globaux et les corps de fractions rationnelles sont hilbertiens. L'intérêt d'étudier les corps hibertiens K est que l'on a $\mathrm{PIG}_{K(T)} \Leftrightarrow \mathrm{PIG}_K$. On renvoie, par exemple, à [FJ08] pour plus de détails sur les corps hilbertiens.

0.1.3 Problème inverse de Galois régulier

L'approche précédente admet une version plus forte que l'on appelle *problème inverse de Galois régulier* et que l'on note **PIGR**. Etant donné un corps K, ce problème s'énonce comme suit :

PIGR_K : *Tout groupe fini est-il le groupe de Galois d'une extension galoisienne régulière $L/K(T)$ (c'est-à-dire $L \cap \overline{K} = K$) ?*

De manière équivalente, ce problème revient à se demander si, pour tout groupe fini G, il existe un G-revêtement $f : X \to \mathbb{P}^1$ défini sur K.

Remarque 0.1.1. Par la condition de régularité, le PIGR admet une réponse positive sur tout corps si et seulement s'il en est de même sur $\mathbb{Q}$ et sur tous les $\mathbb{F}_p$ (p premier). De plus, une réponse positive au PIGR_K fournit une réponse positive au PIG_K pour tout corps hilbertien K.

A l'heure actuelle, on ne connaît aucun exemple de corps K ne satisfaisant pas au PIGR. Quant aux résultats positifs, un profond théorème de Pop (voir [Pop96]) affirme que le PIGR_K admet une réponse positive dès que K contient un corps ample. Rappelons qu'un corps K est *ample* si toute courbe lisse définie sur K et géométriquement irréductible possède une infinité de points K-rationnels dès qu'elle en possède un. Par exemple, les corps valués henséliens, la clôture totalement réelle $\mathbb{Q}^{\mathrm{tr}}$ de $\mathbb{Q}$ et les corps algébriquement clos sont des corps amples. Nous renvoyons à [Jar11], [BSF13] et [Pop14] pour plus de détails.

Si le résultat de Pop englobe plusieurs résultats antérieurs dûs à Riemann, Hurwitz, Harbater, Dèbes, etc (voir [DD97]), il existe, comme démontré par Koenigsmann dans [Koe04], des corps K satisfaisant au PIGR mais ne contenant aucun corps ample.

D'un autre côté, il existe des groupes finis G qui sont groupes de Galois réguliers sur tout corps K (en particulier, sur $\mathbb{Q}$). On peut, par exemple, citer les groupes abéliens, les groupes symétriques, les groupes alternés, 25 des 26 groupes sporadiques, etc. Nous renvoyons, par exemple, à [MM18] pour plus de détails. Il nous semble pertinent de rappeler que, pour certains groupes simples non abéliens G, toutes les réalisations de G sur $\mathbb{Q}$ connues à l'heure actuelle sont des spécialisations d'extensions régulières galoisiennes de $\mathbb{Q}(T)$ de groupe G.

0.1.4 Problèmes de plongement finis

Une généralisation du problème inverse de Galois est donnée par les problèmes de plongement finis. Un *problème de plongement fini* sur un corps commutatif K est un épimorphisme $\alpha : G \to \mathrm{Gal}(L/K)$, où G est un groupe fini et L/K une extension galoisienne de corps commutatifs. On dit que α est *scindé* s'il existe un plongement $\alpha' : \mathrm{Gal}(L/K) \to G$ tel que $\alpha \circ \alpha' = \mathrm{id}_{\mathrm{Gal}(L/K)}$. Une *solution* à α est un isomorphisme $\beta : \mathrm{Gal}(F/K) \to G$, où F est un corps commutatif contenant L et qui est une extension galoisienne de K, tel que $\alpha \circ \beta$ soit l'application de restriction $\mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K)$. Une *solution géométrique* à α est un isomorphisme $\beta : \mathrm{Gal}(E/K(T)) \to G$, où E est un corps contenant L et qui est une extension galoisienne de $K(T)$, tel que $\alpha \circ \beta$ soit l'application de restriction $\mathrm{Gal}(E/K(T)) \to \mathrm{Gal}(L/K)$.

Rappelons que la conjecture principale portant sur les problèmes de plongement finis dans le cas commutatif a été proposée par Dèbes et Deschamps (voir [DD97, §2.2.1]) :

Conjecture. *Tout problème de plongement fini scindé $G \to \mathrm{Gal}(L/K)$ sur n'importe quel corps commutatif K possède une solution géométrique $\mathrm{Gal}(E/K(T)) \to G$ vérifiant $E \cap \overline{K} = L$.*

L'intérêt de cette conjecture est qu'elle généralise et unifie plusieurs conjectures en théorie inverse de Galois commutative. D'une part, elle fournit une réponse positive au PIGR_K pour tout corps K. D'autre part, elle permet de résoudre la *conjecture de Shafarevich*, qui affirme que le groupe de Galois absolu de l'extension cyclotomique maximale de $\mathbb{Q}$ est prolibre et qui est abondamment étudiée (voir, par exemple, [Pop96, HS05, Par09, Des15]). A ce jour, la conjecture de Dèbes et Deschamps n'a été démontrée que pour les corps amples (voir [Pop96, Main Theorem A]) et aucun contre-exemple n'est connu.

0.2 Théorie inverse de Galois sur les corps quelconques : état de l'art

Comme déjà indiqué dans l'avant-propos, la théorie inverse de Galois sur des corps quelconques est un sujet beaucoup plus récent. Dans [DL20], Bruno Deschamps et François Legrand s'intéressent à la problématique inverse de Galois sur des corps non nécessairement commutatifs H. En effet, la théorie des corps admet une généralisation dans le cas de ces corps (voir chapitre 2 ou [Coh95, Chapter 3]), qui rend légitime le PIG_H. Cependant, une difficulté majeure est que, sans l'hypothèse de commutativité, la théorie est bien différente de celle que l'on apprend en licence. Nous allons illustrer cela par l'exemple suivant :

Exemple 0.2.1. Soit H un corps de dimension finie sur son centre h. Par le théorème de Skolem–Noether, $\mathrm{Aut}(H/h)$ ne contient que des automorphismes intérieurs. Plus précisément, on a un isomorphisme $x \in H^*/h^* \mapsto I(x) \in \mathrm{Aut}(H/h)$ où $I(x)(y) = xyx^{-1}$ pour tous $x \in H^*$ et $y \in H$. Ainsi on a $H^{\mathrm{Aut}(H/h)} = h$ et donc H/h est galoisienne. Si $H \neq h$, alors $\mathrm{Gal}(H/h)$ est infini et, dans ce cas, on obtient une extension galoisienne finie dont l'ordre du groupe de Galois est plus grand que le degré de l'extension, une situation qui ne se produit pas dans le cas commutatif classique.

Notons que la notion de clôture algébrique n'est pas immédiate pour les corps non commutatifs H, donc le PIGR_H n'a pas de sens. On peut néanmoins s'intéresser au $\mathrm{PIG}_{H(T)}$ dès que l'on sait donner un analogue d'un corps de fractions rationnelles sur un corps non commutatif. La théorie des anneaux de polynômes tordus de Ore en est un cadre idéal. Rappelons que, si H est un corps quelconque, alors l'anneau de polynômes $H[T]$ est le H-espace vectoriel des polynômes sur H muni du produit qui vérifie $Ta = aT$ pour tout $a \in H$ (voir §2.1.3). Cet anneau possède un unique corps de fractions $H(T)$ (voir §2.1.3 ou [Coh95, Chapter 2]). L'un des résultats principaux de [DL20] est le théorème suivant (voir [DL20, Théorème B]), qui fournit un analogue non commutatif du résultat de Pop évoqué dans le §0.1.3.

Théorème 0.2.2. *(Deschamps–Legrand) Si H est un corps de dimension finie sur son centre h contenant un corps ample, alors le $\mathrm{PIG}_{H(T)}$ admet une réponse positive.*

Exemple 0.2.3. On considère le corps des quaternions de Hamilton $\mathbb{H}_{\mathbb{R}}$. Le centre de $\mathbb{H}_{\mathbb{R}}$ est $\mathbb{R}$, qui est ample, donc le $\mathrm{PIG}_{\mathbb{H}_{\mathbb{R}}(T)}$ admet une réponse positive par le théorème 0.2.2.

Une application de ce théorème a été ensuite donnée dans [ALP20], où il est montré que l'anneau $H(X)$ des fonctions polynomials en la variable X et à coefficients dans H est isomorphe à un certain corps $H'(T)$. Les auteurs en déduisent, par [DL20], que le problème inverse de Galois admet une réponse positive sur $H(X)$ dès que h contient un corps ample.

0.3 Présentation du travail

0.3.1 Chapitre 1 : Réalisations galoisiennes explicites de certaines familles de 2-groupes

Une version raffinée du problème inverse de Galois sur un corps K consiste à construire, pour tout groupe fini G, une extension galoisienne explicite de K de groupe G.

Exemples 0.3.1. 1) Si $G = \mathbb{Z}/2\mathbb{Z}$, alors l'extension $F/\mathbb{Q} = \mathbb{Q}(\sqrt{3})/\mathbb{Q}$ est galoisienne de groupe G.
2) Si $G = \mathbb{Z}/4\mathbb{Z}$, alors l'extension $\mathbb{Q}(T)(\sqrt{T^2+1+T\sqrt{T^2+1}})/\mathbb{Q}(T)$ est une extension $\mathbb{Q}$-régulière de groupe G (voir [Ser92]).
3) Si $G = S_n$, alors le corps de décomposition sur $\mathbb{Q}(T)$ du polynôme $Y^n - Y - T$ ($n \geq 3$) est une extension galoisienne régulière de $\mathbb{Q}(T)$ de groupe G (voir [Ser92]).

Nous renvoyons à [MM18] pour d'autres exemples de réalisations explicites de groupes de petit cardinal.

Dans ce chapitre, nous nous intéressons à certains 2-groupes, plus précisément aux groupes non abéliens d'ordre 2^n et d'exposant 2^{n-1}. Pour $n \geq 3$, il existe exactement quatre tels groupes (voir [JLY02, page 127]), à savoir le *groupe diédral* D_{2^n}, le *groupe quasi-diédral* QD_{2^n}, le *groupe modulaire* M_{2^n} et le *groupe de quaternions généralisés* Q_{2^n} (voir §1.1.2 pour une présentation de chacun de ces groupes). Bien entendu, ces groupes étant résolubles, ils sont groupes de Galois sur $\mathbb{Q}$ par le théorème de Shafarevich. Ces groupes sont en fait groupes de Galois réguliers sur $\mathbb{Q}$. En effet, il est connu que tout produit en couronnes $\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/h\mathbb{Z}$ est groupe de Galois d'une extension galoisienne $\mathbb{Q}$-régulière $E/\mathbb{Q}(T_1, \ldots, T_s)$ pour un certain $s \geq 1$, qui est en fait égal à h, et que tout produit semi-direct $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/h\mathbb{Z}$ est quotient de $\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/h\mathbb{Z}$ (voir [FJ08, §16.4]). Un argument de spécialisation (voir [FJ08, Proposition 13.2.1]), en général non explicite, permet alors de prendre $s = 1$ (pour h quelconque). Ceci s'applique en particulier aux 2-groupes ci-dessus puisque les trois premiers sont des produits semi-directs $\mathbb{Z}/2^{n-1}\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ et le dernier est quotient d'un produit semi-direct $\mathbb{Z}/2^{n-1}\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$.

Par contre, l'existence de réalisations explicites de ces groupes est en général inconnue, notamment pour les groupes de quaternions généralisés (voir [JLY02, page 141]). Dans la suite, nous construisons de telles extensions en développant et en rendant explicite la méthode de [FJ08, §16.4]. Nous montrons par exemple le théorème suivant (voir théorème 1.3.2) :

Théorème 0.3.2. *Soient $n \geq 3$ et $\xi = \exp(2\pi i/2^{n-1})$. Pour $l \in [\![1, 2^{n-1}]\!]$ et $\ell \in \{1, 2\}$, on pose*

$$z_{\ell,l} = \sum_{j \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*} \xi^{lj} \prod_{k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*} (T + 1 + (-1)^\ell \sqrt{T^2+1} - \xi^k)^{r(j/k)/2^{n-1}},$$

où $r : (\mathbb{Z}/2^{n-1}\mathbb{Z})^* \to [\![0, 2^{n-1} - 1]\!]$ envoie $k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*$ sur son unique représentant modulo 2^{n-1}. Si l'on note

$$w = \sqrt{T^2+1} + (\sqrt{T^2+1+T\sqrt{T^2+1}} + \sum_{l=1}^{2^{n-1}} z_{1,l} z_{2,l})^2,$$

alors l'extension $\mathbb{Q}(T, w)/\mathbb{Q}(T)$ est galoisienne de groupe Q_{2^n} et $\mathbb{Q}(T, w)/\mathbb{Q}$ est régulière. De plus, les $\mathbb{Q}(T)$-conjugués de w sont les

$$(-1)^a \sqrt{T^2+1} + (\pm\sqrt{T^2 + (-1)^a T\sqrt{T^2+1}} + \sum_{l=1}^{2^{n-1}} z_{2,l} z_{1,l+s})^2, \quad (a, s) \in \{0, 1\} \times [\![0, 2^{n-2} - 1]\!].$$

Nous donnons aussi des analogues pour D_{2^n}, QD_{2^n} et M_{2^n} (voir corollaires 1.2.6, 1.2.7 et 1.2.8).

Nous construisons en fait une réalisation régulière explicite de n'importe quel produit semi-direct $\mathbb{Z}/m\mathbb{Z}\rtimes\mathbb{Z}/2\mathbb{Z}$ ($m \geq 3$), ce qui généralise nos résultats sur D_{2^n}, QD_{2^n} et M_{2^n} (voir théorème 1.2.5). Ce résultat plus général nous permet aussi de construire une réalisation régulière explicite du groupe diédral D_{2m} à $2m$ éléments ($m \geq 3$), voir corollaire 1.2.6. Ceci fournit une variante régulière, valable pour tout m, d'une construction de Martinais et Schneps (voir [MS92]).

Notons toutefois que notre méthode diffère de celle de [FJ08, §16.4] puisque nous construisons "directement" des extensions galoisiennes $E/\mathbb{Q}(T)$ de groupe $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, c'est-à-dire notre méthode ne nécessite pas l'argument de spécialisation nécessaire pour passer de $\mathbb{Q}(T_1, T_2)$ à $\mathbb{Q}(T)$ rappelé plus haut. De plus, la stratégie de la preuve du théorème 0.3.2 ne consiste pas à réaliser explicitement $\mathbb{Z}/2^{n-1}\mathbb{Z}\wr\mathbb{Z}/4\mathbb{Z}$, puis ses quotients $\mathbb{Z}/2^{n-1}\mathbb{Z}\rtimes\mathbb{Z}/4\mathbb{Z}$, puis Q_{2^n}. Elle consiste plutôt à remarquer que Q_{2^n} est quotient d'un produit semi-direct $\mathbb{Z}/2^{n-1}\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ qui est en fait un produit fibré de $\mathbb{Z}/4\mathbb{Z}$ et de D_{2^n}. Nous utilisons alors la réalisation régulière explicite de D_{2^n} obtenue dans le corollaire 1.2.6 pour réaliser explicitement ce produit fibré, et donc Q_{2^n}.

Nous donnons ensuite des progressions arithmétiques explicites d'entiers t_0 tels que la spécialisation de $E/\mathbb{Q}(T)$ en t_0 soit galoisienne de groupe Q_{2^n}, où $E/\mathbb{Q}(T)$ désigne l'extension de groupe Q_{2^n} construite dans le théorème 0.3.2. L'existence de progressions arithmétiques d'entiers satisfaisant à la propriété de spécialisation de Hilbert a été étudiée par de nombreux auteurs, par exemple, par Davenport–Lewis–Schinzel (voir [Sch00]), Fried (voir [Fri74]), Dèbes–Ghazi (voir [DG12]), Dèbes–Legrand (voir [DL13]) et Legrand (voir [Leg16]). Nous explicitons la méthode de [Leg16], qui repose sur l'inertie des spécialisations, et obtenons le théorème suivant :

Théorème 0.3.3. *Soit $n \geq 3$. Soient p et q deux nombres premiers distincts supérieurs ou égaux à $7^{2^{n-2}} + 1$ tels que $p \equiv 1 \pmod{2^{n-1}}$ et $q \equiv 1 \pmod 4$. Alors il existe un $t_0 \in [\![0, p^2q^2 - 1]\!]$ explicite tel que, si t désigne n'importe quel entier positif vérifiant $t \equiv t_0 \pmod{p^2q^2}$, alors la spécialisation $E_t/\mathbb{Q}$ de $E/\mathbb{Q}(T)$ en t est galoisienne de groupe Q_{2^n}.*

Nous renvoyons au théorème 1.3.10 pour un énoncé plus général où l'on explique comment construire un tel t_0. Par ailleurs, il nous paraît plausible que des analogues peuvent être donnés pour les autres 2-groupes considérés dans ce chapitre. Nous laissons ce travail au lecteur intéressé.

0.3.2 Chapitre 2 : Eléments de théorie des corps quelconques

Dans ce chapitre, nous rappelons les éléments de la théorie des corps quelconques, qui seront utilisés dans les chapitres 3 et 4 : anneaux de Ore, corps de fractions rationnelles tordus, théorie de Galois des corps quelconques, etc.

0.3.3 Chapitre 3 : Théorie inverse de Galois sur les corps de fractions rationnelles tordus

Nous expliquons brièvement la méthode utilisée par B. Deschamps et F. Legrand dans [DL20] pour montrer le théorème 0.2.2, qui repose sur l'extension des scalaires. Ils montrent d'abord le résultat suivant (voir [DL20, Théorème B]) faisant intervenir une contrainte polynomiale :

Théorème 0.3.4. *Soient G un groupe fini, K un corps de dimension finie sur son centre k et $\mathcal{F}_K \in k[X_1, \ldots, X_{n^2}]$ la forme polynomiale associée à la norme réduite (voir §2.2 pour la définition) de K/k relativement au choix d'une k-base de K. Alors G est groupe de Galois sur K si et seulement s'il existe une extension galoisienne L/k telle que $\mathcal{F}_K$ ne possède que le zéro trivial sur L. Dans ce cas, l'extension $K \otimes_k L/K$ est galoisienne de groupe G.*

Ensuite, ils déduisent le théorème 0.2.2 en utilisant le théorème 0.3.4 (avec $K = H(T)$ et $k = h(T)$) et le fait que le résultat démontré par Pop dans [Pop96] affirme que la variante forte du PIGR ci-dessous admet une réponse positive sur tout corps h contenant un corps ample.

PIGS$_h$ (Problème Inverse de Galois Sérié) : *Pour tout groupe fini G, existe t-il une extension galoisienne $L/h(T)$ de groupe G telle que $L \subset h((T))$?*

De manière équivalente, ce problème consiste à savoir si, pour tout groupe fini G, il existe un G-revêtement $X \to \mathbb{P}^1$ défini sur h tel que X possède un point h-rationnel non ramifié.

Tout en continuant à utiliser la méthode de l'extension des scalaires, nous introduisons une nouvelle approche utilisant les corps des séries de Laurent tordus, qui nous permet de montrer la généralisation du résultat de Deschamps–Legrand suivante :

Théorème 0.3.5. *Soient H un corps de centre h (H non nécessairement de dimension finie sur h) et σ un automorphisme d'ordre fini de H. Si $h^{\langle\sigma\rangle}$ désigne le corps des invariants de h par σ, alors on a*

$$\mathrm{PIGS}_{h^{\langle\sigma\rangle}} \Longrightarrow \mathrm{PIG}_{H(T,\sigma)}.$$

En particulier, si $h^{\langle\sigma\rangle}$ contient un corps ample, alors le $\mathrm{PIG}_{H(T,\sigma)}$ admet une réponse positive.

Rappelons que $H(T,\sigma)$ est le corps de fractions de l'anneau de polynômes tordu $H[T,\sigma]$ vérifiant $Ta = \sigma(a)T$ pour tout $a \in H$ (voir §2.1.3 pour plus de détails). Quand $\sigma = \mathrm{id}$, on retrouve le corps $H(T)$. Un exemple d'application du théorème 0.3.5 ne rentrant pas dans le cadre des travaux de [DL20] peut être donné en considérant le corps $H = k(Y,\sigma)$ où k/k_0 désigne une extension galoisienne vérifiant $\langle\sigma\rangle = \mathrm{Gal}(k/k_0)$ infini et k_0 ample (e.g. $k_0 = \mathbb{C}((X))$ et $k = \overline{\mathbb{C}((X))}$) (voir exemples 3.1.4 pour plus de détails).

La théorie de Galois des corps quelconques admet aussi une généralisation au cas infini (voir §2.3.4). Dans cette perspective, on s'inspire des travaux de Pierre Dèbes et Bruno Deschamps sur la ψ-liberté des corps (présentés dans [DD04]) pour nous intéresser à la possibilité de réaliser le groupe prolibre $\widehat{F}_\omega$ comme groupe de Galois d'une extension de $H(T,\sigma)$. A cet effet, nous montrons le théorème suivant :

Théorème 0.3.6. *Soient H un corps de centre h et σ un automorphisme d'ordre fini de H. Supposons que le corps des invariants $h^{\langle\sigma\rangle}$ contienne un corps h_0 qui est, soit réel clos, soit hensélien de caractéristique résiduelle nulle et contenant toutes les racines de l'unité. Alors, il existe une extension galoisienne $L/H(T,\sigma)$ de groupe $\widehat{F}_\omega$.*

Ce théorème montre, par exemple, que le groupe $\widehat{F}_\omega$ est groupe de Galois sur $\mathbb{H}_{\mathbb{R}}(T)$, le corps de fractions rationnelles tordu à indéterminée centrale, où $\mathbb{H}_{\mathbb{R}}$ est le corps des quaternions de Hamilton (voir exemple 3.2.5).

0.3.4 Chapitre 4 : Problèmes de plongement finis sur les corps non commutatifs

Dans ce chapitre, nous nous intéressons aux problèmes de plongement finis sur les corps de dimension finie sur leurs centres. D'un point de vue pratique, nous remplissons quatre objectifs.

Premièrement, nous étendons la terminologie des problèmes de plongement finis sur un corps H de dimension finie sur son centre, qui étend naturellement la terminologie du cas commutatif rappelée dans le §0.1.4. Une première difficulté est que, si F/H et L/H sont deux extensions galoisiennes à groupes de Galois finis et telles que $L \subseteq F$, alors il n'est en général pas vrai que $\sigma(x) \in L$ si $\sigma \in \mathrm{Gal}(F/H)$ et $x \in L$, c'est-à-dire il n'y a pas, a priori, d'application de restriction $\mathrm{Gal}(F/H) \to \mathrm{Gal}(L/H)$ comme dans le cas commutatif. Cependant, une telle application de

restriction existe toujours si H est de dimension finie sur son centre (voir [Coh95, Chapter 3] ou §4.2.1). De plus, pour généraliser la notion de solution géométrique, nous devons montrer au préalable que, pour une extension galoisienne L d'un corps H de dimension finie sur son centre à groupe de Galois fini, l'extension $L(T)/H(T)$ est galoisienne et il existe une application de restriction $\mathrm{Gal}(L(T)/H(T)) \to \mathrm{Gal}(L/H)$, qui est un isomorphisme (voir §4.2.1).

Deuxièmement, si $\alpha : G \to \mathrm{Gal}(L/H)$ désigne un problème de plongement fini sur un corps H de dimension finie sur son centre h, nous lui associons un problème de plongement fini $\check{\alpha} : G \to \mathrm{Gal}(\ell/h)$ sur h, où ℓ est le centre de L (voir (4.2.3)). Nous montrons alors le théorème suivant, dont le cas $L = H$ est le théorème 0.3.4 :

Théorème 0.3.7. *Soient $\alpha : G \to \mathrm{Gal}(L/H)$ un problème de plongement fini sur un corps H de dimension finie sur son centre h et $\mathcal{F}_H \in h[X_1, \ldots, X_{n^2}]$ la forme polynomiale associée à la norme réduite de H/h relativement au choix d'une h-base de H. Alors α a une solution $\mathrm{Gal}(F/H) \to G$ si et seulement si $\check{\alpha}$ a une solution $\mathrm{Gal}(f/h) \to G$ telle que $\mathcal{F}_H$ n'ait que le zéro trivial sur f.*

Nous renvoyons au théorème 4.2.9 pour un énoncé plus précis, qui fournit une correspondance explicite entre les solutions à α et celles à $\check{\alpha}$ vérifiant la contrainte polynomiale ci-dessus.

Troisièmement, nous établissons un analogue non commutatif du résultat de Pop résolvant la conjecture de Dèbes et Deschamps sur les corps amples :

Théorème 0.3.8. *Soit H un corps de dimension finie sur son centre h. Tout problème de plongement fini scindé sur H admet une solution géométrique, si h est un corps ample.*

Etant donnés un problème de plongement fini scindé $\alpha : G \to \mathrm{Gal}(L/H)$ sur H et un automorphisme σ de H d'ordre fini, nous donnons en fait, sous l'hypothèse h ample, des conditions suffisantes pour que α acquière une solution sur $H(t, \sigma)$. Nous renvoyons au théorème 4.3.1 pour notre résultat précis. Ce dernier résultat généralise, d'une part, le théorème 0.3.8 et permet, d'autre part, de réobtenir le théorème 0.3.5 dans le cas où H est de dimension finie sur son centre.

Quatrièmement, rappelons que, dans le cas commutatif, la *réduction faible→scindé* (voir [Pop96, §1 B) 2)] et [DD97, §2.1.2]) est un procédé bien connu pour déduire des résultats sur les problèmes de plongement finis admettant une *solution faible* de résultats sur les problèmes de plongement finis scindés. Des applications usuelles de ce procédé sont que la conjecture de Dèbes et Deschamps est équivalente à la conjecture affirmant que tout problème de plongement fini $G \to \mathrm{Gal}(\ell/k)$ sur n'importe quel corps commutatif k possédant une solution faible possède en fait une solution géométrique $\mathrm{Gal}(e/k(T)) \to G$ vérifiant $e \cap \overline{k} = \ell$, et que cette dernière conjecture est vraie si k est ample.

Nous étendons la notion de solution faible et la réduction faible→scindé à la situation des problèmes de plongement finis sur les corps de dimension finie sur leurs centres. Les propositions 4.4.2 et 4.4.3 constituent nos résultats précis. Ceux-ci nous permettent d'étendre le théorème 4.3.1 en montrant, en particulier, que, *si H est un corps de dimension finie sur son centre h, alors tout problème de plongement fini sur H admettant une solution faible possède une solution géométrique, si h est un corps ample* (voir corollaire 4.4.4).

Chapitre 1

Réalisations galoisiennes explicites de certaines familles de 2-groupes

Dans ce chapitre, nous construisons, pour certains 2-groupes G, des extensions galoisiennes $\mathbb{Q}$-régulières explicites $E/\mathbb{Q}(T)$ de groupe G. Nous fournissons aussi des progressions arithmétiques explicites d'entiers t_0 telles que la spécialisation $E_{t_0}/\mathbb{Q}$ de $E/\mathbb{Q}(T)$ en t_0 soit de groupe G.

Ce chapitre est basé sur l'article [Beh20] et est organisé de la manière suivante. La section 1.1 est dédiée aux préliminaires. Dans la section 1.2, nous construisons des réalisations régulières explicites de n'importe quel produit semi-direct $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ ($m \geq 3$). La section 1.3 est non seulement dédiée à la même tâche pour les groupes de quaternions généralisés mais aussi à la construction de réalisations explicites de ces groupes sur $\mathbb{Q}$ par spécialisation. Les théorèmes 0.3.2 et 0.3.3 sont établis dans la section 1.3.

1.1 Préliminaires

1.1.1 Extensions de corps de fonctions

Etant donnés un groupe fini G et un corps K, une *G-extension* de K est une extension galoisienne F/K de groupe G. Si F/K et M/L désignent deux extensions galoisiennes finies telles que $K \subset L$ et $F \subset M$, l'application de restriction $\mathrm{Gal}(M/L) \to \mathrm{Gal}(F/K)$ sera notée $\mathrm{res}^{M/L}_{F/K}$.

Etant donnée une indéterminée T, on dit qu'une extension finie galoisienne $E/K(T)$ est *K-régulière* si E/K est régulière, c'est-à-dire si $E \cap \overline{K} = K$. On dit que $t_0 \in \mathbb{P}^1(\overline{K})$ est un *point de branchement* de $E/K(T)$ si l'idéal $\langle T - t_0 \rangle$ est ramifié dans la clôture intégrale de $\overline{K}[T - t_0]$ dans $E\overline{K}$ (si $t_0 = \infty$, $T - t_0$ doit être remplacé par $1/T$).

On suppose maintenant que $E/K(T)$ est une G-extension K-régulière de points de branchement $t_1, \ldots, t_r$. Etant donné $t_0 \in \mathbb{P}^1(K) \setminus \{t_1, \ldots, t_r\}$, la *spécialisation* de $E/K(T)$ en t_0, notée E_{t_0}/K, est l'extension résiduelle en un idéal premier $\mathcal{P}$ au dessus de $\langle T - t_0 \rangle$. Comme $E/K(T)$ est galoisienne, l'extension E_{t_0}/K ne dépend pas du choix de l'idéal premier $\mathcal{P}$. De plus, E_{t_0}/K est galoisienne et son groupe de Galois est le groupe de décomposition de $E/K(T)$ en $\mathcal{P}$.

On se donne maintenant une G-extension $\mathbb{Q}$-régulière $E/\mathbb{Q}(T)$ de points de branchement $t_1, \ldots, t_r$. Etant donné un nombre premier p, on pose $1/\infty = 0$, $1/0 = \infty$, $v(\infty) = -\infty$ et $v(0) = \infty$, où v désigne la valuation p-adique. Soit $\mathbb{Z}_{p\mathbb{Z}}$ le localisé de $\mathbb{Z}$ en p. Pour chaque $t \in \mathbb{P}^1(\overline{\mathbb{Q}})$, on note $m_t(X) \in \mathbb{Q}[X]$ le polynôme minimal de t sur $\mathbb{Q}$, avec la convention $m_\infty(X) = 1$.

Définition 1.1.1. Soient t_0 et t_1 dans $\mathbb{P}^1(\overline{\mathbb{Q}})$. On dit que t_0 *et* t_1 *se rencontrent modulo* p s'il existe un corps de nombres F et un idéal premier de F au dessus de p de valuation associée w tels que t_0, $t_1 \in \mathbb{P}^1(F)$ et tels que l'une des conditions suivantes soit vérifiée :
1) $w(t_0) \geq 0$, $w(t_1) \geq 0$ et $w(t_0 - t_1) > 0$,
2) $w(t_0) \leq 0$, $w(t_1) \leq 0$ et $w((1/t_0) - (1/t_1)) > 0$.

Le lemme suivant nous sera utile par la suite.

Lemme 1.1.2. *Soient t_0 et t_1 dans $\overline{\mathbb{Q}}$ entiers sur $\mathbb{Z}_{p\mathbb{Z}}$. Si t_0 et t_1 se rencontrent modulo p et si $N(t_0 - t_1)$ désigne la norme de $t_0 - t_1$ dans une extension finie galoisienne $F/\mathbb{Q}$ donnée telle que $t_0, t_1 \in F$, alors $v(N(t_0 - t_1)) > 0$.*

Preuve. On se donne un idéal premier de F au dessus de p de valuation associée w tel que $w(t_0 - t_1) > 0$. On a $w(N(t_0 - t_1)) = \sum_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} w(\sigma(t_0 - t_1)) \geq w(t_0 - t_1) > 0$. □

Définition 1.1.3. On dit que p est un *mauvais premier* (et un *bon premier* sinon) de l'extension $E/\mathbb{Q}(T)$ si l'une des conditions suivantes est vérifiée :
1) $|G| \in p\mathbb{Z}$,
2) deux points de branchement distincts de $E/\mathbb{Q}(T)$ se rencontrent modulo p,
3) p est *verticalement ramifié* dans $E/\mathbb{Q}(T)$, c'est-à-dire l'idéal $p\mathbb{Z}[T]$ se ramifie dans la clôture intégrale de $\mathbb{Z}[T]$ dans E,
4) p se ramifie dans $\mathbb{Q}(t_1, \ldots, t_r)/\mathbb{Q}$, où $t_1, \ldots, t_r$ sont les points de branchement de $E/\mathbb{Q}(T)$.

A chaque point de branchement t_i est associée une classe de conjugaison C_i de G, appelée *classe canonique de l'inertie*. En effet, les groupes d'inertie de $E\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ en t_i sont des groupes cycliques deux à deux conjugués et d'ordre égal à l'indice de ramification e_i. De plus, chacun d'eux admet un générateur distingué correspondant à l'automorphisme $(T - t_i)^{1/e_i} \mapsto \exp(2\pi i/e_i)(T - t_i)^{1/e_i}$ de $\overline{\mathbb{Q}}(((T - t_i)^{1/e_i}))$ (on remplace $T - t_i$ par $1/T$ si $t_i = \infty$). Alors C_i est la classe de conjugaison de tous les générateurs distingués des groupes d'inertie en t_i. Le r-uplet non ordonné $(C_1, \ldots, C_r)$ est appelé *invariant canonique de l'inertie* de $E/\mathbb{Q}(T)$. Pour $i \in [\![1, r]\!]$, notons g_i le générateur distingué d'un certain groupe d'inertie de $E\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ en t_i.

Nous renvoyons à [Bec91, Proposition 4.2] et [Leg16, §2.2.3] pour le théorème suivant.

Théorème 1.1.4. *Soit $t_0 \in \mathbb{P}^1(\mathbb{Q}) \setminus \{t_1, \ldots, t_r\}$. Fixons $j \in [\![1, r]\!]$ tel que t_0 et t_j se rencontrent modulo p. Supposons que p soit un bon premier pour $E/\mathbb{Q}(T)$ et que $m_{t_j}(T)$ et $m_{1/t_j}(T)$ soient dans $\mathbb{Z}_{p\mathbb{Z}}[T]$. Alors le groupe d'inertie de $E_{t_0}/\mathbb{Q}$ en p est conjugué dans G à $\langle g_j^a \rangle$, où $a = v(m_{t_j}(t_0))$ (resp. $a = v(m_{1/t_j}(1/t_0))$) si $v(t_0) \geq 0$ (resp. $v(t_0) \leq 0$).*

1.1.2 Sur les 2-groupes

Dans ce chapitre, le groupe cyclique d'ordre m est noté $\mathbb{Z}/m\mathbb{Z}$ et considéré additivement.

Un produit semi-direct $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est déterminé par l'image d de $1 \in \mathbb{Z}/2\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) = (\mathbb{Z}/m\mathbb{Z})^*$ (on a nécessairement $d^2 = 1$). Une présentation de ce groupe est

$$\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = \langle r, s \mid r^m = s^2 = 1, srs^{-1} = r^d \rangle, \tag{1.1.1}$$

où r (resp. s) correspond à $(1, 0)$ (resp. $(0, 1)$). Dans la suite, on considérera trois cas :
1) m arbitraire et $d = -1$; dans ce cas, $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est le groupe diédral D_{2m},
2) $m = 2^{n-1}$ $(n \geq 3)$ et $d = 2^{n-2} - 1$; dans ce cas, le produit semi-direct $\mathbb{Z}/2^{n-1}\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est le groupe quasi-diédral QD_{2^n},
3) $m = 2^{n-1}$ $(n \geq 3)$ et $d = 2^{n-2} + 1$; dans ce cas, le produit semi-direct $\mathbb{Z}/2^{n-1}\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est le groupe modulaire M_{2^n}.

Etant donné $n \geq 3$, on définit le groupe Δ_n comme étant le produit semi-direct $\mathbb{Z}/2^{n-1}\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ où l'image de $1 \in \mathbb{Z}/4\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/2^{n-1}\mathbb{Z})$ est $-\mathrm{id}$. Ce groupe admet comme présentation

$$\Delta_n = \langle \rho, \sigma \mid \rho^{2^{n-1}} = \sigma^4 = 1, \sigma\rho\sigma^{-1} = \rho^{-1} \rangle, \tag{1.1.2}$$

où ρ (resp. σ) correspond à $(1,0)$ (resp. $(0,1)$). Le groupe de quaternions généralisés d'ordre 2^n, noté Q_{2^n}, est le quotient de Δ_n par le sous-groupe distingué $\langle (2^{n-2}, 2) \rangle$. La présentation (1.1.2) de Δ_n induit la présentation de Q_{2^n} suivante :

$$Q_{2^n} = \langle \Lambda, \Sigma \mid \Lambda^{2^{n-1}} = \Sigma^4 = 1, \Lambda^{2^{n-2}} = \Sigma^2, \Sigma\Lambda\Sigma^{-1} = \Lambda^{-1} \rangle, \tag{1.1.3}$$

où Λ (resp. Σ) est l'image de ρ (resp. σ) modulo $\langle (2^{n-2}, 2) \rangle$.

Pour $m \geq 2$, le produit en couronnes de $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$, noté $\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$, est le produit semi-direct $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$ où l'image de $1 \in \mathbb{Z}/2\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$ est l'automorphisme $(a, b) \mapsto (b, a)$.

Dans ce chapitre, on utilise toujours les présentations ci-dessus.

La proposition suivante nous sera utile par la suite.

Proposition 1.1.5. *Soient $n \geq 3$, K un corps et M/K une D_{2^n}-extension. Notons L le sous-corps de M fixé par r, où r est défini dans la présentation* (1.1.1)*. Supposons que L/K se plonge dans une $\mathbb{Z}/4\mathbb{Z}$-extension H/K et soit τ un générateur de* $\mathrm{Gal}(H/K)$*. D'une part, H/L et M/L sont linéairement disjointes. D'autre part, HM/K est une Δ_n-extension. De plus, il existe un unique relèvement ρ de r dans* $\mathrm{Gal}(HM/H)$ *et celui-ci vérifie ce qui suit : pour tout relèvement σ de τ dans Δ_n, les éléments ρ et σ vérifient la présentation* (1.1.2)*.*

Preuve. Tout d'abord, il est clair que HM/K est galoisienne. De plus, on a $H \not\subset M$ car $\mathbb{Z}/4\mathbb{Z}$ n'est pas quotient de D_{2^n}. Par conséquent, on a $[HM : M] = 2$, les extensions H/L et M/L sont linéairement disjointes et $\mathrm{res}^{HM/H}_{M/L}$ est un isomorphisme. Ainsi, r admet un unique relèvement ρ dans $\mathrm{Gal}(HM/H)$. A partir de maintenant, on se donne un relèvement σ de τ à HM.

Maintenant, σ est d'ordre 4. En effet, on a $o(\sigma) \geq o(\tau) = 4$. De plus, σ ne fixe pas $L = M^{\langle r \rangle}$ et $\mathrm{res}^{HM/K}_{M/K}(\sigma) \in D_{2^n}$. Par conséquent, on a $\mathrm{res}^{HM/K}_{M/K}(\sigma)^2 = \mathrm{id}_M$. Puisque $[HM : M] = 2$, on obtient $o(\sigma^2) \leq 2$. Ainsi $o(\sigma) \leq 4$ et donc $o(\sigma) = 4$.

Ensuite, $\sigma\rho\sigma^{-1} = \rho^{-1}$. En effet, on a $\mathrm{res}^{HM/H}_{M/L}(\sigma\rho\sigma^{-1}) = \mathrm{res}^{HM/K}_{M/K}(\sigma) \cdot r \cdot \mathrm{res}^{HM/K}_{M/K}(\sigma)^{-1} = r^{-1}$ car $\mathrm{res}^{HM/K}_{M/K}(\sigma) \notin \langle r \rangle$. Or $r^{-1} = \mathrm{res}^{HM/H}_{M/L}(\rho^{-1})$ et $\mathrm{res}^{HM/H}_{M/L}$ est injective. Donc $\sigma\rho\sigma^{-1} = \rho^{-1}$.

De plus, on a $\mathrm{Gal}(HM/K) = \langle \rho, \sigma \rangle$. En effet, soit s comme dans (1.1.1). Le morphisme de restriction $\langle \rho, \sigma \rangle \to \langle r, s \rangle = D_{2^n}$ est surjectif puisque l'on a $s = r^a \mathrm{res}^{HM/K}_{M/K}(\sigma)$ pour un certain a. Ainsi $2^n = |D_{2^n}|$ divise $|\langle \rho, \sigma \rangle|$, donc divise $|\mathrm{Gal}(HM/K)| = 2^{n+1}$. Le morphisme n'est pas injectif car $o(\sigma) = 4 \neq 2 = o(r^{-a}s) = o(\mathrm{res}^{HM/K}_{M/K}(\sigma))$. On en déduit donc $\mathrm{Gal}(HM/K) = \langle \rho, \sigma \rangle$.

Enfin, on a $\mathrm{Gal}(HM/K) = \Delta_n$ et ρ, σ vérifient (1.1.2). En effet, les égalités $\rho^{2^{n-1}} = 1$, $\sigma^4 = 1$, $\sigma\rho\sigma^{-1} = \rho^{-1}$ et $|\langle \rho, \sigma \rangle| = 2^{n+1}$ montrent que l'on a $\langle \rho, \sigma \rangle = \Delta_n$. Le paragraphe précédent donne alors $\mathrm{Gal}(HM/K) = \Delta_n$. □

La proposition précédente admet la version régulière suivante :

Proposition 1.1.6. *Soient $n \geq 3$ et $M/\mathbb{Q}(T)$ une D_{2^n}-extension $\mathbb{Q}$-régulière. Notons L le sous-corps de M fixé par r, où r est défini dans* (1.1.1)*. Supposons que $L/\mathbb{Q}(T)$ se plonge dans une $\mathbb{Z}/4\mathbb{Z}$-extension $H/\mathbb{Q}(T)$. Alors $HM/\mathbb{Q}(T)$ est une Δ_n-extension $\mathbb{Q}$-régulière.*

Preuve. Supposons que $H/\mathbb{Q}$ ne soit pas régulière. Alors $[H \cap \overline{\mathbb{Q}} : \mathbb{Q}] = 2$ car $L \subset H$ et $L/\mathbb{Q}(T)$ est une extension de degré 2 $\mathbb{Q}$-régulière. Ainsi, $(H \cap \overline{\mathbb{Q}})(T)/\mathbb{Q}(T)$ et $L/\mathbb{Q}(T)$ sont linéairement disjointes, ce qui entraîne $\mathrm{Gal}(H/\mathbb{Q}(T)) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, une contradiction. Par conséquent, $H/\mathbb{Q}(T)$ est $\mathbb{Q}$-régulière. En appliquant la proposition 1.1.5 aux extensions $M/\mathbb{Q}(T)$ et $H/\mathbb{Q}(T)$ (resp. $M\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ et $H\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$), on obtient que $HM/\mathbb{Q}(T)$ (resp. $HM\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$) est une Δ_n-extension. Ainsi, $HM/\mathbb{Q}(T)$ est $\mathbb{Q}$-régulière. □

1.1.3 Un lemme sur les racines de l'unité

Nous terminons cette section avec un lemme, que nous utiliserons à plusieurs reprises par la suite :

Lemme 1.1.7. *Soient $m \geq 3$ et $\xi = \exp(2\pi i/m)$. Posons $s_k = -(1-\xi^k)/2 + 1/(2(1-\xi^k))$ pour tout $k \in (\mathbb{Z}/m\mathbb{Z})^*$. Soit $\overline{\mathcal{O}}$ la clôture intégrale de $\overline{\mathbb{Q}}[T]$ dans $\overline{\mathbb{Q}}(T)(\sqrt{T^2+1})$.*

a) Pour $k \neq k'$, on a $s_k \neq s_{k'}$.

b) Pour $\epsilon \in \{-1, 1\}$ et $k \in (\mathbb{Z}/m\mathbb{Z})^*$, on a $s_k \neq \epsilon i$.

c) Les idéaux $(T+1+(-1)^\ell\sqrt{T^2+1}-\xi^k)\overline{\mathcal{O}}$ ($k \in (\mathbb{Z}/m\mathbb{Z})^*$ et $\ell \in \{0,1\}$) sont premiers et deux à deux distincts. De plus, pour $k \in (\mathbb{Z}/m\mathbb{Z})^*$, on a $(T+1\pm\sqrt{T^2+1}-\xi^k)\overline{\mathcal{O}} \cap \overline{\mathbb{Q}}[T] = (T-s_k)\overline{\mathbb{Q}}[T]$.

Preuve. a) S'il y avait égalité, on aurait $(1-\xi^k)(1-\xi^{k'}) = -1$ et donc $\xi^k = (\xi^{k'}-2)/(\xi^{k'}-1)$. Ainsi $\xi^{k'}$ serait à la fois sur le cercle unité et la médiatrice du segment $[1, 2]$, une contradiction.

b) S'il y avait égalité, on aurait $\xi^{2k} - 2(1+i\epsilon)\xi^k + 2i\epsilon = 0$ et donc $\xi^k = 1 + i\epsilon$, une contradiction.

c) On a tout d'abord $(T+1+\sqrt{T^2+1}-\xi^k)(T+1-\sqrt{T^2+1}-\xi^k) = 2(1-\xi^k)(T-s_k)$, ce qui donne $(T+1+\sqrt{T^2+1}-\xi^k)\overline{\mathcal{O}} \cdot (T+1-\sqrt{T^2+1}-\xi^k)\overline{\mathcal{O}} = (T-s_k)\overline{\mathcal{O}}$. Puisque $(T-s_k)\overline{\mathbb{Q}}[T] \neq \overline{\mathbb{Q}}[T]$, on a $(T-s_k)\overline{\mathcal{O}} \neq \overline{\mathcal{O}}$. Par conséquent, $T+1+\sqrt{T^2+1}-\xi^k$ et son conjugué $T+1-\sqrt{T^2+1}-\xi^k$ ne sont pas inversibles dans $\overline{\mathcal{O}}$. Puisque $[\overline{\mathbb{Q}}(T)(\sqrt{T^2+1}) : \overline{\mathbb{Q}}(T)] = 2$, on en déduit que $(T+1+\sqrt{T^2+1}-\xi^k)\overline{\mathcal{O}}$ et $(T+1-\sqrt{T^2+1}-\xi^k)\overline{\mathcal{O}}$ sont des idéaux premiers. De plus, ceux-ci sont nécessairement distincts en vertu de [Sti09, Proposition 6.2.3] et du b). Enfin, le a) entraîne que les idéaux $(T-s_k)\overline{\mathbb{Q}}[T]$ ($k \in (\mathbb{Z}/m\mathbb{Z})^*$) sont deux à deux distincts. □

1.2 Produits semi-directs $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

Dans cette partie, nous construisons, pour tout $m \geq 3$ et tout produit semi-direct $G = \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, une extension galoisienne $\mathbb{Q}$-régulière explicite de $\mathbb{Q}(T)$ de groupe G (voir théorème 1.2.5).

1.2.1 Notations

On pose $L = \mathbb{Q}(T)(\sqrt{T^2+1})$ et on note β le générateur de $\mathrm{Gal}(L/\mathbb{Q}(T))$. On note $\mathcal{O}$ (resp. $\overline{\mathcal{O}}$) la clôture intégrale de $\mathbb{Q}[T]$ (resp. $\overline{\mathbb{Q}}[T]$) dans L (resp. $L\overline{\mathbb{Q}}$). On se donne $m \geq 3$ et on note $\xi = \exp(2\pi i/m)$. Pour $\ell \in \{1, 2\}$ et $k \in (\mathbb{Z}/m\mathbb{Z})^*$, on note $\mathcal{P}_{\ell,k}$ l'idéal premier de $\overline{\mathcal{O}}$ engendré par $T+1+(-1)^\ell\sqrt{T^2+1}-\xi^k$ (voir lemme 1.1.7) et on choisit une racine m-ième $x_{\ell,k}$ de $T+1+(-1)^\ell\sqrt{T^2+1}-\xi^k$ dans $\overline{\mathbb{Q}(T)}$. Pour $\ell \in \{1, 2\}$, on note M_ℓ le compositum des corps $L(\xi, x_{\ell,k})$ ($k \in (\mathbb{Z}/m\mathbb{Z})^*$) et, pour tout $j \in (\mathbb{Z}/m\mathbb{Z})^*$, on pose

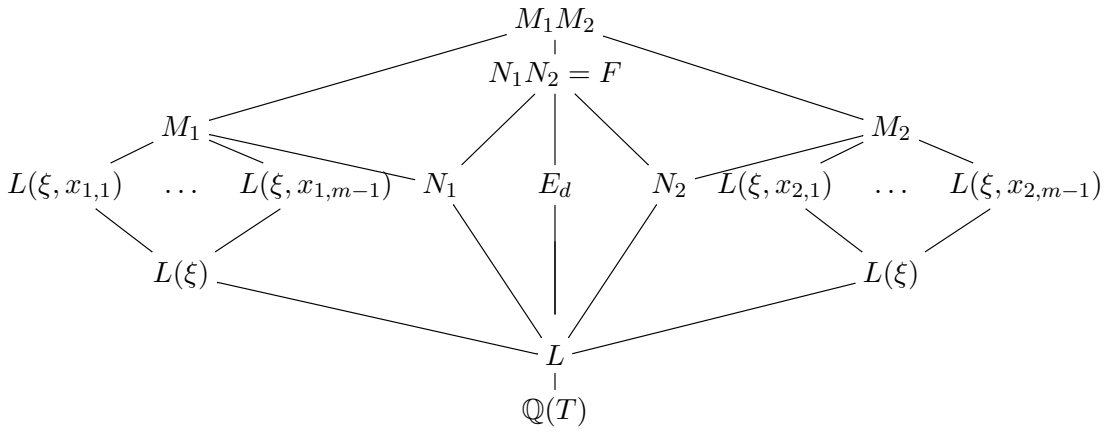
$$y_{\ell,j} = \prod_{k \in (\mathbb{Z}/m\mathbb{Z})^*} x_{\ell,k}^{r_m(j/k)},$$

où $r_m : (\mathbb{Z}/m\mathbb{Z})^* \to [\![0, m-1]\!]$ envoie $k \in (\mathbb{Z}/m\mathbb{Z})^*$ sur son unique représentant modulo m. Pour tout $\ell \in \{1,2\}$ et tout $l \in \mathbb{N}$, on pose

$$z_{\ell,l} = \sum_{j\in(\mathbb{Z}/m\mathbb{Z})^*} \xi^{lj} y_{\ell,j} = \sum_{j\in(\mathbb{Z}/m\mathbb{Z})^*} \xi^{lj} \prod_{k\in(\mathbb{Z}/m\mathbb{Z})^*} x_{\ell,k}^{r_m(j/k)}.$$

Pour tout $\ell \in \{1,2\}$, notons $N_\ell = L(z_{\ell,1})$ et $h_\ell(X) = \prod_{l=1}^m (X - z_{\ell,l})$. Posons $F = N_1N_2 = L(z_{1,1}, z_{2,1})$ et $E_d = \mathbb{Q}(T, \sqrt{T^2+1} + \sum_{l=1}^m z_{2,l} z_{1,-dl})$ pour tout $d \in (\mathbb{Z}/m\mathbb{Z})^*$ vérifiant $d^2 = 1$.

On a le diagramme suivant :



1.2.2 Résultats préparatoires

Commençons par déterminer $\mathrm{Gal}(M_1/L)$ et $\mathrm{Gal}(M_2/L)$.

Lemme 1.2.1. *a) Les deux extensions de corps $(L(\xi, x_{\ell,k})/L(\xi))_{\ell\in\{1,2\},k\in(\mathbb{Z}/m\mathbb{Z})^*}$ et $(\overline{\mathbb{Q}}L(x_{\ell,k})/\overline{\mathbb{Q}}L)_{\ell\in\{1,2\},k\in(\mathbb{Z}/m\mathbb{Z})^*}$ sont cycliques de degré m et linéairement disjointes dans leur ensemble*[1]*. Ainsi, pour $\ell \in \{1,2\}$, l'extension $M_\ell/L(\xi)$ est galoisienne de groupe $(\mathbb{Z}/m\mathbb{Z})^{\varphi(m)}$, où φ est l'indicatrice d'Euler. De plus, pour $\ell \in \{1,2\}$, les idéaux premiers de $\overline{\mathcal{O}}$ ramifiés dans $\overline{\mathbb{Q}}M_\ell$ sont les $\mathcal{P}_{\ell,k}$ ($k \in (\mathbb{Z}/m\mathbb{Z})^*$).*

b) Soit $\ell \in \{1,2\}$. L'extension M_ℓ/L est galoisienne de degré $m^{\varphi(m)}\varphi(m)$. De plus, pour tout $\omega \in \mathrm{Gal}(M_\ell/L)$, il existe un unique $v(\omega) \in (\mathbb{Z}/m\mathbb{Z})^*$ tel que $\omega(\xi) = \xi^{v(\omega)}$ et, pour tout $k \in (\mathbb{Z}/m\mathbb{Z})^*$, il existe un unique $s_k \in \mathbb{Z}/m\mathbb{Z}$ tel que $\omega(x_{\ell,k}) = \xi^{s_k} x_{\ell,v(\omega)k}$. L'application

$$f : \left\{ \begin{array}{ccc} \mathrm{Gal}(M_\ell/L) & \to & (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^{\varphi(m)} \\ \omega & \mapsto & (v(\omega), (s_k)_{k\in(\mathbb{Z}/m\mathbb{Z})^*}) \end{array} \right.$$

est en fait bijective.

Preuve. a) Soient $\ell \in \{1,2\}$ et $k \in (\mathbb{Z}/m\mathbb{Z})^*$. Du fait que $X^m - (T + 1 + (-1)^\ell\sqrt{T^2+1} - \xi^k) \in \overline{\mathcal{O}}[X]$ est d'Eisenstein pour l'idéal premier $\mathcal{P}_{\ell,k}$, on obtient que $\overline{\mathbb{Q}}L(x_{\ell,k})/\overline{\mathbb{Q}}L$ et $L(\xi, x_{\ell,k})/L(\xi)$ sont de degré m. Par la théorie de Kummer, $\overline{\mathbb{Q}}L(x_{\ell,k})/\overline{\mathbb{Q}}L$ et $L(\xi, x_{\ell,k})/L(\xi)$ sont cycliques. De plus, les sous-extensions de $L(\xi, x_{\ell,k})/L(\xi)$ (resp. $\overline{\mathbb{Q}}L(x_{\ell,k})/\overline{\mathbb{Q}}L$) sont les $(L(\xi, x_{\ell,k}^a)/L(\xi))_{a|m}$ (resp. $(\overline{\mathbb{Q}}L(x_{\ell,k}^a)/\overline{\mathbb{Q}}L)_{a|m}$). Pour tout diviseur a de m, différent de m, le seul idéal premier de $\overline{\mathcal{O}}$ ramifié dans $\overline{\mathbb{Q}}L(x_{\ell,k}^a)/\overline{\mathbb{Q}}L$ est $\mathcal{P}_{\ell,k}$. Comme les idéaux premiers $\mathcal{P}_{\ell,k}$ ($\ell \in \{1,2\}$ et $k \in (\mathbb{Z}/m\mathbb{Z})^*$) sont distincts (voir lemme 1.1.7), le lemme d'Abhyankar fournit la conclusion voulue.

1. Rappelons que des extensions galoisiennes finies $M_1/K, \dots, M_n/K$ sont linéairement disjointes dans leur ensemble si, pour toute partition (I, J) de $[\![1, n]\!]$, le compositum des M_i ($i \in I$) est linéairement disjoint sur K du compositum des M_j ($j \in J$).

b) Le corps M_ℓ est le corps de décomposition sur L du polynôme $\prod_{k\in(\mathbb{Z}/m\mathbb{Z})^*}(X^m - x_{\ell,k}^m) \in L[X]$, ce qui montre que M_ℓ/L est galoisienne. De plus, puisque $L/\mathbb{Q}$ est régulière, $\mathbb{Q}(T,\xi)$ et L sont linéairement disjoints sur $\mathbb{Q}(T)$. On a donc $[L(\xi):L] = \varphi(m)$ et, par le a), $[M_\ell : L] = m^{\varphi(m)}\varphi(m)$. Il est alors clair que l'application f est bien définie et que celle-ci est injective. Pour des raisons de cardinalité, elle est aussi surjective. □

La proposition suivante est inspirée de [MM18, Chapter III, Theorem 4.3] et permet de déterminer le groupe de Galois de N_ℓ/L.

Proposition 1.2.2. *Soit $\ell \in \{1,2\}$.*
a) Le polynôme $h_\ell(X)$ est dans $L[X]$ et est irréductible sur $\overline{\mathbb{Q}}L$.
b) L'extension N_ℓ/L est galoisienne de groupe $\mathbb{Z}/m\mathbb{Z}$. De plus, un générateur de $\mathrm{Gal}(N_\ell/L)$ est donné par γ_ℓ, où γ_ℓ vérifie $\gamma_\ell(z_{\ell,l}) = z_{\ell,l+1}$ pour tout $l \in \mathbb{N}$.

Preuve. Ecrivons

$$h_\ell(X) = X^m + \sum_{\iota=1}^{m}(-1)^\iota s_{\ell,\iota}X^{m-\iota}$$

dans $\overline{\mathbb{Q}(T)}[X]$. Pour tout $\varsigma \in [\![1,m]\!]$, notons

$$q_{\ell,\varsigma} = \sum_{l=1}^{m} z_{\ell,l}^{\varsigma}.$$

Des identités de Newton, pour tout $\varsigma \in [\![1,m]\!]$, on a

$$q_{\ell,\varsigma} + \sum_{\iota=1}^{\varsigma-1}(-1)^\iota s_{\ell,\iota}q_{\ell,\varsigma-\iota} + (-1)^\varsigma \varsigma s_{\ell,\varsigma} = 0. \tag{1.2.1}$$

a) Pour $\varsigma \in [\![1,m]\!]$, on a $q_{\ell,\varsigma} \in \mathcal{O}[\xi]$. En effet, soit $\varsigma \in [\![1,m]\!]$. On a

$$\begin{aligned}
q_{\ell,\varsigma} &= \sum_{l=1}^{m}\left(\sum_{j\in(\mathbb{Z}/m\mathbb{Z})^*}\xi^{lj}y_{\ell,j}\right)^\varsigma = \sum_{l=1}^{m}\prod_{\lambda=1}^{\varsigma}\left(\sum_{j_\lambda\in(\mathbb{Z}/m\mathbb{Z})^*}\xi^{lj_\lambda}y_{\ell,j_\lambda}\right)\\
&= \sum_{l=1}^{m}\left(\sum_{(j_1,\dots,j_\varsigma)\in((\mathbb{Z}/m\mathbb{Z})^*)^\varsigma}\left(\prod_{\lambda=1}^{\varsigma}\xi^{lj_\lambda}y_{\ell,j_\lambda}\right)\right)\\
&= \sum_{(j_1,\dots,j_\varsigma)\in((\mathbb{Z}/m\mathbb{Z})^*)^\varsigma}\left(\sum_{l=1}^{m}\prod_{\lambda=1}^{\varsigma}\xi^{lj_\lambda}\right)\left(\prod_{\lambda=1}^{\varsigma}y_{\ell,j_\lambda}\right)\\
&= \sum_{(j_1,\dots,j_\varsigma)\in((\mathbb{Z}/m\mathbb{Z})^*)^\varsigma}\left(\sum_{l=1}^{m}\xi^{l(\sum_{\lambda=1}^{\varsigma}j_\lambda)}\right)\left(\prod_{\lambda=1}^{\varsigma}y_{\ell,j_\lambda}\right).
\end{aligned}$$

Du fait que, pour tout $o \in \mathbb{Z}$, la somme $\sum_{l=1}^{m}\xi^{lo}$ est égale à m si m divise o et est égale à 0 sinon, les seuls termes non nuls dans la somme ci-dessus sont ceux vérifiant $\sum_{\lambda=1}^{\varsigma}j_\lambda \equiv 0 \pmod m$. On obtient alors

$$\begin{aligned}
q_{\ell,\varsigma} &= \sum_{\substack{(j_1,\dots,j_\varsigma)\in((\mathbb{Z}/m\mathbb{Z})^*)^\varsigma\\ \sum_{\lambda=1}^{\varsigma}j_\lambda\equiv 0 \pmod m}} m\prod_{\lambda=1}^{\varsigma}\left(\prod_{k\in(\mathbb{Z}/m\mathbb{Z})^*}x_{\ell,k}^{r_m(j_\lambda/k)}\right)\\
&= \sum_{\substack{(j_1,\dots,j_\varsigma)\in((\mathbb{Z}/m\mathbb{Z})^*)^\varsigma\\ \sum_{\lambda=1}^{\varsigma}j_\lambda\equiv 0 \pmod m}} m\left(\prod_{k\in(\mathbb{Z}/m\mathbb{Z})^*}x_{\ell,k}^{\sum_{\lambda=1}^{\varsigma}r_m(j_\lambda/k)}\right).
\end{aligned}$$

Comme, pour tout $k \in (\mathbb{Z}/m\mathbb{Z})^*$, on a

$$\sum_{\lambda=1}^{\varsigma} r_m(j_\lambda/k) \equiv \left(\sum_{\lambda=1}^{\varsigma} j_\lambda\right)/k \equiv 0 \pmod{m}, \tag{1.2.2}$$

les termes de $q_{\ell,\varsigma}$ appartiennent bien à $\mathcal{O}[\xi]$.

Par conséquent, les $s_{\ell,\iota}$ ($\iota \in [\![1,m]\!]$) sont dans $\mathcal{O}[\xi]$ en utilisant la relation (1.2.1).

De plus, par le lemme 1.2.1, tout $\omega \in \mathrm{Gal}(L(\xi)/L)$ se relève en un unique $\widetilde{\omega} \in \mathrm{Gal}(M_\ell/L)$ tel que, pour tout $k \in (\mathbb{Z}/m\mathbb{Z})^*$, on ait $\widetilde{\omega}(x_{\ell,k}) = x_{\ell,v(\omega)k}$, où $v(\omega)$ est l'unique élément de $(\mathbb{Z}/m\mathbb{Z})^*$ vérifiant $\omega(\xi) = \xi^{v(\omega)}$. Tout $\widetilde{\omega}$ de cette forme fixe les $z_{\ell,l}$ car, pour tout $l \in [\![1,m]\!]$, on a

$$\begin{aligned}
\widetilde{\omega}(z_{\ell,l}) &= \widetilde{\omega}\Bigg(\sum_{j\in(\mathbb{Z}/m\mathbb{Z})^*} \xi^{lj} \prod_{k\in(\mathbb{Z}/m\mathbb{Z})^*} x_{\ell,k}^{r_m(j/k)}\Bigg) = \sum_{j\in(\mathbb{Z}/m\mathbb{Z})^*} \xi^{ljv(\omega)} \prod_{k\in(\mathbb{Z}/m\mathbb{Z})^*} x_{\ell,v(\omega)k}^{r_m(j/k)} \\
&= \sum_{j\in(\mathbb{Z}/m\mathbb{Z})^*} \xi^{lj} \prod_{k\in(\mathbb{Z}/m\mathbb{Z})^*} x_{\ell,k}^{r_m(j/k)} \\
&= z_{\ell,l}.
\end{aligned}$$

Des résultats précédents, on déduit que les $s_{\ell,\iota}$ sont dans $\mathcal{O}$.

Montrons maintenant que $h_\ell(X)$ est irréductible sur $\overline{\mathbb{Q}}L$. Pour cela, il suffit de vérifier que c'est un polynôme d'Eisenstein pour l'idéal premier $\mathcal{P}_{\ell,1}$. En utilisant l'équation (1.2.2), on voit que $q_{\ell,\varsigma} \in \mathcal{P}_{\ell,1}$ pour tout ς. Par conséquent, en utilisant l'identité (1.2.1), on a $s_{\ell,\iota} \in \mathcal{P}_{\ell,1}$ pour tout $\iota \in [\![1,m]\!]$. Donc, il reste à montrer que $s_{\ell,m} \notin \mathcal{P}_{\ell,1}^2$. En utilisant l'identité (1.2.1) avec $\varsigma = m$ et le fait que $s_{\ell,\iota}q_{\ell,m-\iota} \in \mathcal{P}_{\ell,1}^2$ pour tout $\iota \in [\![1,m-1]\!]$, il suffit de vérifier que $q_{\ell,m} \notin \mathcal{P}_{\ell,1}^2$.

Pour cela, notons v la valuation de $\overline{\mathbb{Q}}L$ associée à $\mathcal{P}_{\ell,1}$. Pour tout $(j_1,\dots,j_m) \in ((\mathbb{Z}/m\mathbb{Z})^*)^m$ tel que $\sum_{\lambda=1}^m j_\lambda \equiv 0 \pmod{m}$, on a

$$v\left(x_{\ell,k}^{\sum_{\lambda=1}^m r_m(j_\lambda/k)}\right) = 0$$

pour tout $k \in (\mathbb{Z}/m\mathbb{Z})^* \setminus \{1\}$ par le lemme 1.1.7. Par conséquent, on a

$$\begin{aligned}
v\left(m\Bigg(\prod_{k\in(\mathbb{Z}/m\mathbb{Z})^*} x_{\ell,k}^{\sum_{\lambda=1}^m r_m(j_\lambda/k)}\Bigg)\right) &= v\left(x_{\ell,1}^{\sum_{\lambda=1}^m r_m(j_\lambda)}\right) \\
&= v\left(\left(T+1+(-1)^\ell\sqrt{T^2+1}-\xi\right)^{\frac{\sum_{\lambda=1}^m r_m(j_\lambda)}{m}}\right) \\
&= \frac{1}{m}\Big(\sum_{\lambda=1}^m r_m(j_\lambda)\Big).
\end{aligned}$$

En remarquant que la valuation ci-dessus est égale à 1 si $(j_1,\dots,j_m) = (1,\dots,1)$ et supérieure ou égale à 2 sinon, on obtient $v(q_{\ell,m}) = 1$, ce qui achève la démonstration du a).

b) Pour tout $j \in (\mathbb{Z}/m\mathbb{Z})^*$, l'extension $L(\xi, y_{\ell,j})/L(\xi)$ est cyclique de degré m. En effet, $X^m - \prod_{k\in(\mathbb{Z}/m\mathbb{Z})^*} x_{\ell,k}^{mr_m(j/k)} \in L(\xi)[X]$ annule $y_{\ell,j}$ et est d'Eisenstein pour l'idéal premier $\mathcal{P}_{\ell,j}$. On conclut donc par la théorie de Kummer.

Maintenant, si F_ℓ désigne le compositum des $L(\xi, y_{\ell,j})$ ($j \in (\mathbb{Z}/m\mathbb{Z})^*$), on a $F_\ell = L(\xi, y_{\ell,1})$. En effet, soit $j \in (\mathbb{Z}/m\mathbb{Z})^*$. Pour tout $k \in (\mathbb{Z}/m\mathbb{Z})^*$, il existe $o_{j,k} \in m\mathbb{Z}$ tel que $r_m(j)r_m(1/k) =$

$r_m(j/k)+o_{j,k}$. On a alors

$$y_{\ell,1}^{r_m(j)} = y_{\ell,j}\Bigg(\prod_{k\in(\mathbb{Z}/m\mathbb{Z})^*}\Big(T+1+(-1)^\ell\sqrt{T^2+1}-\xi^k\Big)^{o_{j,k}/m}\Bigg),$$

donc $L(\xi,y_{\ell,j})\subset L(\xi,y_{\ell,1})$. Par conséquent, on a $F_\ell = L(\xi,y_{\ell,1})$.

De plus, F_ℓ/L est galoisienne. En effet, $L(\xi)/L$ est clairement galoisienne et, d'après les deux paragraphes précédents, $F_\ell/L(\xi)$ l'est aussi. Par conséquent, il suffit de montrer que tout élément de $\mathrm{Gal}(L(\xi)/L)$ se relève en un élément de $\mathrm{Aut}(F_\ell/L)$. Fixons pour cela $\omega\in\mathrm{Gal}(L(\xi)/L)$. Notons comme précédemment $\widetilde{\omega}$ l'unique relèvement de ω à M_ℓ tel que, pour tout $k\in(\mathbb{Z}/m\mathbb{Z})^*$, on ait $\widetilde{\omega}(x_{\ell,k}) = x_{\ell,v(\omega)k}$, où $v(\omega)$ est l'unique élément de $(\mathbb{Z}/m\mathbb{Z})^*$ vérifiant $\omega(\xi)=\xi^{v(\omega)}$. Pour tout $j\in(\mathbb{Z}/m\mathbb{Z})^*$, on a $\widetilde{\omega}(y_{\ell,j}) = y_{\ell,v(\omega)j}$, ce qui montre que la restriction de $\widetilde{\omega}$ à F_ℓ est bien un élément de $\mathrm{Aut}(F_\ell/L)$.

En outre, N_ℓ/L est cyclique de degré m. En effet, d'après le a), N_ℓ/L est de degré m. Notons $\Omega = \{\mathrm{res}^{M_\ell/L}_{F_\ell/L}(\widetilde{\omega}) \mid \omega\in\mathrm{Gal}(L(\xi)/L)\}$, où $\widetilde{\omega}$ est défini dans le paragraphe précédent. Vu que $v(\omega\omega') = v(\omega)v(\omega')$ pour tous $\omega,\omega'\in\mathrm{Gal}(L(\xi)/L)$, l'ensemble Ω est un sous-groupe de $\mathrm{Gal}(F_\ell/L)$. Par restriction, Ω est isomorphe à $\mathrm{Gal}(L(\xi)/L)$. De plus, la preuve du a) montre que Ω fixe chaque élément du sous-corps N_ℓ de F_ℓ. Pour des raisons de degrés, on a forcément $N_\ell = F_\ell^\Omega$. De plus, par le a), les L-conjugués de $z_{\ell,1}$ sont les $z_{\ell,l}$ ($l\in[\![1,m]\!]$). Ils sont fixés par Ω par la preuve du a), donc ils sont dans N_ℓ. On en déduit que N_ℓ/L est galoisienne de degré m. On remarque enfin que $L(\xi)\cap N_\ell = L(\xi)\cap F_\ell^\Omega = L(\xi)^{\mathrm{Gal}(L(\xi)/L)} = L$ et donc $F_\ell = N_\ell(\xi)$. On en déduit $\mathrm{Gal}(N_\ell/L)\simeq\mathrm{Gal}(F_\ell/L(\xi))\simeq\mathbb{Z}/m\mathbb{Z}$.

Enfin, γ_ℓ définit bien un générateur de $\mathrm{Gal}(N_\ell/L)$. En effet, avec les notations du lemme 1.2.1, soit ω l'unique élément de $\mathrm{Gal}(M_\ell/L)$ défini par $v(\omega)=1$, $s_1=1$ et $s_k=0$ pour tout $k\in(\mathbb{Z}/m\mathbb{Z})^*\setminus\{1\}$. On vérifie que $\omega(z_{\ell,l}) = z_{\ell,l+1}$ pour tout $l\in[\![1,m]\!]$. Ainsi $\gamma_\ell = \mathrm{res}^{M_\ell/L}_{N_\ell/L}(\omega)$ est un élément de $\mathrm{Gal}(N_\ell/L)$ d'ordre m. □

Nous relevons maintenant le générateur β de $\mathrm{Gal}(L/\mathbb{Q}(T))$ en un élément χ du groupe $\mathrm{Aut}(M_1M_2/\mathbb{Q}(T))$.

Lemme 1.2.3. *Il existe un automorphisme χ de M_1M_2 prolongeant β, fixant ξ et tel que $\chi(x_{2,k}) = x_{1,k}$ et $\chi(x_{1,k}) = x_{2,k}$ pour tout $k\in(\mathbb{Z}/m\mathbb{Z})^*$. En conséquence, $\chi(z_{1,l}) = z_{2,l}$ et $\chi(z_{2,l}) = z_{1,l}$ pour tout $l\in[\![1,m]\!]$. De plus, l'extension $M_1M_2/\mathbb{Q}(T)$ est galoisienne.*

Preuve. On remarque d'abord que l'on peut étendre β en un automorphisme de $L(\xi)$ fixant ξ. Ensuite, on étend β en un isomorphisme $M_2\to M_1$ tel que $\beta(x_{2,k}) = x_{1,k}$ pour tout $k\in(\mathbb{Z}/m\mathbb{Z})^*$. En effet, pour tout $k\in(\mathbb{Z}/m\mathbb{Z})^*$, on a $(X^m-(T+1+\sqrt{T^2+1}-\xi^k))^\beta = X^m-(T+1-\sqrt{T^2+1}-\xi^k)$ et le polynôme minimal de $x_{2,k}$ (resp. $x_{1,k}$) sur le compositum des corps $L(\xi,x_{2,k'})$ (resp. $L(\xi,x_{1,k'})$), pour $k'\in(\mathbb{Z}/m\mathbb{Z})^*\setminus\{k\}$, est $X^m-(T+1+\sqrt{T^2+1}-\xi^k)$ (resp. $X^m-(T+1-\sqrt{T^2+1}-\xi^k)$), d'après le lemme 1.2.1. Enfin, on étend β en un automorphisme χ de M_1M_2 tel que $\chi(x_{1,k}) = x_{2,k}$ pour tout $k\in(\mathbb{Z}/m\mathbb{Z})^*$. En effet, pour tout $k\in(\mathbb{Z}/m\mathbb{Z})^*$, on a $(X^m-(T+1-\sqrt{T^2+1}-\xi^k))^\beta = X^m-(T+1+\sqrt{T^2+1}-\xi^k)$ et le polynôme minimal de $x_{1,k}$ (resp. $x_{2,k}$) sur le compositum des corps M_2 et $L(\xi,x_{1,k'})$ (resp. M_1 et $L(\xi,x_{2,k'})$), pour $k'\in(\mathbb{Z}/m\mathbb{Z})^*\setminus\{k\}$, est $X^m-(T+1-\sqrt{T^2+1}-\xi^k)$ (resp. $X^m-(T+1+\sqrt{T^2+1}-\xi^k)$). □

Nous déterminons enfin le groupe de Galois de $F/\mathbb{Q}(T)$.

Proposition 1.2.4. *a) L'extension $F/\mathbb{Q}(T)$ est galoisienne et $\mathbb{Q}$-régulière.*
b) On a $\mathrm{Gal}(F/L) = \{\mathcal{L}_{a,b}\mid(a,b)\in(\mathbb{Z}/m\mathbb{Z})^2\}$, où $\mathcal{L}_{a,b}(z_{1,l}) = z_{1,l+a}$ et $\mathcal{L}_{a,b}(z_{2,l}) = z_{2,l+b}$ pour tout $(a,b)\in\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ et tout $l\in\mathbb{N}$.

c) Il existe $g \in \mathrm{Gal}(F/\mathbb{Q}(T))$, *d'ordre* 2, *vérifiant* $\mathrm{res}^{F/\mathbb{Q}(T)}_{L/\mathbb{Q}(T)}(g) = \beta$ *et* $g(z_{1,l}) = z_{2,l}$ *(resp.* $g(z_{2,l}) = z_{1,l}$*) pour tout* $l \in [\![1, m]\!]$. *De plus, on a*

$$\mathrm{Gal}(F/\mathbb{Q}(T)) = \{\mathcal{L}_{a,b} \circ g^{\epsilon} \mid (a,b) \in (\mathbb{Z}/m\mathbb{Z})^2, \epsilon \in \{0,1\}\}, \tag{1.2.3}$$

qui est isomorphe à $\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$ *via*

$$\psi : \left\{ \begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z} & \to & \mathrm{Gal}(F/\mathbb{Q}(T)) \\ ((a,b),\epsilon) & \mapsto & \mathcal{L}_{a,b} \circ g^{\epsilon} \end{array} \right. .$$

Preuve. a) Montrons tout d'abord que l'on a $F \cap \overline{\mathbb{Q}} = \mathbb{Q}$. Pour cela, notons que $M_1\overline{\mathbb{Q}}$ et $M_2\overline{\mathbb{Q}}$ sont linéairement disjoints sur $L\overline{\mathbb{Q}}$ en vertu du lemme 1.2.1. En particulier, $N_1\overline{\mathbb{Q}}$ et $N_2\overline{\mathbb{Q}}$ le sont également. On a donc $[N_1N_2\overline{\mathbb{Q}} : L\overline{\mathbb{Q}}] = m^2$ par la proposition 1.2.2. Ainsi, on a $[N_1N_2\overline{\mathbb{Q}} : \overline{\mathbb{Q}}(T)] = 2m^2$, ce qui montre bien $F \cap \overline{\mathbb{Q}} = \mathbb{Q}$ puisque $[F : \mathbb{Q}(T)] \leq 2m^2$. Au passage, on a montré que N_1 et N_2 étaient linéairement disjoints sur L. Ensuite, notons χ un automorphisme de M_1M_2 comme dans le lemme 1.2.3. On a $\chi(z_{1,l}) = z_{2,l}$ et $\chi(z_{2,l}) = z_{1,l}$ pour tout $l \in \mathbb{N}$, donc la restriction de χ à F, que l'on note g, est un automorphisme de F. Ainsi, $F/\mathbb{Q}(T)$ est galoisienne.
b) Soient γ_1 et γ_2 les générateurs de $\mathrm{Gal}(N_1/L)$ et $\mathrm{Gal}(N_2/L)$ de la proposition 1.2.2. Puisque N_1 et N_2 sont linéairement disjoints sur L, on obtient un isomorphisme

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \to & \mathrm{Gal}(F/L) \\ (a,b) & \mapsto & (\gamma_1^a, \gamma_2^b) = \mathcal{L}_{a,b} \end{array} \right. .$$

c) Tout d'abord, on a

$$\mathrm{Gal}(F/\mathbb{Q}(T)) = \mathrm{Gal}(F/L) \rtimes \langle g \rangle. \tag{1.2.4}$$

En effet, notons que $\mathrm{Gal}(F/L)$ est bien un sous-groupe distingué de $\mathrm{Gal}(F/\mathbb{Q}(T))$ et que l'on a $\mathrm{Gal}(F/L) \cap \langle g \rangle = \{\mathrm{id}_F\}$ puisque g est d'ordre 2 et prolonge β. Le b) donne alors (1.2.3).

Considérons maintenant l'application ψ de la proposition. Par le b) et l'égalité (1.2.4), l'application ψ est bijective. Pour montrer que ψ est un isomorphisme, il suffit de vérifier que φ préserve l'action de $\mathbb{Z}/2\mathbb{Z}$. A cet effet, pour $(a,b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, on a

$$\begin{array}{rcccccl} g \circ \varphi(a,b) \circ g^{-1}(z_{1,1}) & = & g \circ \varphi(a,b)(z_{2,1}) & = & g(\gamma_2^b(z_{2,1})) & = & g(z_{2,1+b}) \\ & & & & & = & z_{1,1+b} \\ & & & & & = & \gamma_1^b(z_{1,1}) \\ & & & & & = & \varphi(b,a)(z_{1,1}) \\ & & & & & = & \varphi((a,b)^{\overline{1}})(z_{1,1}) \end{array}$$

et, de même, $g \circ \varphi(a,b) \circ g^{-1}(z_{2,1}) = \varphi((a,b)^{\overline{1}})(z_{2,1})$. □

1.2.3 Résultat principal

Théorème 1.2.5. *On se donne un produit semi-direct* $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, *uniquement déterminé par l'image* d *de* $1 \in \mathbb{Z}/2\mathbb{Z}$ *dans* $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) = (\mathbb{Z}/m\mathbb{Z})^*$. *Pour tout* $\delta \in [\![1, m]\!]$, *posons*

$$v_\delta(d) = \sum_{l=1}^{m} z_{2,l} z_{1,-dl+\delta}.$$

a) L'extension $E_d/\mathbb{Q}(T) = \mathbb{Q}(T, \sqrt{T^2+1} + v_0(d))/\mathbb{Q}(T)$ *est une* $(\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z})$*-extension* $\mathbb{Q}$*-régulière. De plus, on a* $E_d = L(v_0(d))$ *et les* $\mathbb{Q}(T)$*-conjugués de* $\sqrt{T^2+1} + v_0(d)$ *sont les*

$$(-1)^{\epsilon}\sqrt{T^2+1} + v_\delta(d^{(-1)^{\epsilon}}), \quad (\delta, \epsilon) \in [\![1, m]\!] \times \{0,1\}.$$

b) Le groupe $\mathrm{Gal}(E_d/L)$ *est engendré par un automorphisme* r *vérifiant* $r(v_\delta(d)) = v_{\delta+1}(d)$ *pour tout* $\delta \in [\![1, m]\!]$. *En posant* $s = \mathrm{res}^{F/\mathbb{Q}(T)}_{E_d/\mathbb{Q}(T)}(g)$, *où* g *est défini dans la proposition 1.2.4, on a*

$$\mathrm{Gal}(E_d/\mathbb{Q}(T)) = \{r^\delta \circ s^\epsilon \mid \delta \in [\![1, m]\!], \epsilon \in \{0, 1\}\},$$

qui est isomorphe à $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ *via* $(\delta, \epsilon) \mapsto r^\delta \circ s^\epsilon$.

Preuve. D'après [FJ08, Lemma 16.4.3], l'application suivante est un épimorphisme :

$$\begin{array}{rccc} \alpha & : & \mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \\ & & ((a,b),\eta) & \mapsto & (a+db,\eta). \end{array}$$

Son noyau est $\mathrm{Ker}(\alpha) = \{(-da, a) \mid a \in \mathbb{Z}/m\mathbb{Z}\}$. Ci-dessous, on utilise les notations $\mathcal{L}_{a,b}$ ($(a,b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$) et ψ de la proposition 1.2.4.

Le sous-corps de F fixé par $\psi(\mathrm{Ker}(\alpha))$ est $L(v_0(d))$. De plus, $L(v_0(d))/L$ est une $\mathbb{Z}/m\mathbb{Z}$-extension de groupe de Galois engendré par l'automorphisme r vérifiant $r(v_\delta(d)) = v_{\delta+1}(d)$ pour tout $\delta \in [\![1, m]\!]$. En effet, en remarquant que $\psi(\mathrm{Ker}(\alpha)) = \{\mathcal{L}_{-da,a} \mid a \in \mathbb{Z}/m\mathbb{Z}\} \subset \mathrm{Gal}(F/L)$, on obtient

$$\mathrm{Gal}(F^{\psi(\mathrm{Ker}(\alpha))}/L) = \mathrm{Gal}(F/L)/\psi(\mathrm{Ker}(\alpha)) = \{\mathrm{res}^{F/L}_{F^{\psi(\mathrm{Ker}(\alpha))}/L}(\mathcal{L}_{\delta,0}) \mid \delta \in [\![1, m]\!]\} = \langle r \rangle,$$

où $r = \mathrm{res}^{F/L}_{F^{\psi(\mathrm{Ker}(\alpha))}/L}(\mathcal{L}_{1,0})$. On voit que $v_\delta(d) = \mathcal{L}_{\delta,0}(v_0(d))$ pour tout $\delta \in [\![1, m]\!]$, donc les $v_\delta(d)$ sont L-conjugués. Il est immédiat que l'on a $v_0(d) \in F^{\psi(\mathrm{Ker}(\alpha))}$ et donc $L(v_0(d)) \subset F^{\psi(\mathrm{Ker}(\alpha))}$. Pour l'inclusion inverse, puisque $[F^{\psi(\mathrm{Ker}(\alpha))} : L] = m$, il suffit de montrer que les $v_\delta(d)$ sont deux à deux distincts. Pour cela, soient $\delta \not\equiv t \pmod m$. On a

$$\begin{aligned} v_\delta(d) - v_t(d) &= \sum_{l=1}^{m} z_{2,l}(z_{1,-dl+\delta} - z_{1,-dl+t}) \\ &= \sum_{l=1}^{m} z_{2,l} \left(\sum_{j \in (\mathbb{Z}/m\mathbb{Z})^*} \xi^{-dlj}(\xi^{j\delta} - \xi^{jt}) y_{1,j} \right) \\ &= \sum_{l=1}^{m} \left(\sum_{j' \in (\mathbb{Z}/m\mathbb{Z})^*} \xi^{lj'} y_{2,j'} \right) \left(\sum_{j \in (\mathbb{Z}/m\mathbb{Z})^*} \xi^{-dlj}(\xi^{j\delta} - \xi^{jt}) y_{1,j} \right) \\ &= \sum_{l=1}^{m} \sum_{j,j' \in (\mathbb{Z}/m\mathbb{Z})^*} \xi^{l(-dj+j')}(\xi^{j\delta} - \xi^{jt}) \prod_{k \in (\mathbb{Z}/m\mathbb{Z})^*} x_{2,k}^{r_m(j'/k)} x_{1,k}^{r_m(j/k)} \\ &= \sum_{j \in (\mathbb{Z}/m\mathbb{Z})^*} m(\xi^{j\delta} - \xi^{jt}) \prod_{k \in (\mathbb{Z}/m\mathbb{Z})^*} x_{2,k}^{r_m(dj/k)} x_{1,k}^{r_m(j/k)}. \end{aligned}$$

La dernière égalité vient du fait que $\sum_{l=1}^{m} \xi^{lo}$ est égal à 0 si $o \not\equiv 0 \pmod m$ et m sinon. Soit $\mathcal{P}$ un idéal premier au dessus de $\mathcal{P}_{1,1}$ dans $\overline{\mathbb{Q}}M_1M_2/\overline{\mathbb{Q}}L$. Pour $j \neq 1$ (resp. $j = 1$), on a $r_m(j/1) \geq 2$ (resp. $r_m(j/1) = 1$). Donc on a

$$0 < v(v_\delta(d) - v_t(d)) = v\left(m(\xi^\delta - \xi^t) \prod_{k \in (\mathbb{Z}/m\mathbb{Z})^*} x_{2,k}^{r_m(d/k)} x_{1,k}^{r_m(1/k)} \right) < \infty, \tag{1.2.5}$$

où v est la valuation associée à $\mathcal{P}$. Par conséquent, on a $v_\delta(d) - v_t(d) \neq 0$.

Maintenant, on a $E_d = L(v_0(d))$ et $\mathrm{Gal}(E_d/\mathbb{Q}(T)) = \{r^\delta \circ s^\epsilon \mid \delta \in [\![1,m]\!], \epsilon \in \{0,1\}\}$. En effet, pour $\delta \in [\![1,m]\!]$ et $\epsilon \in \{0,1\}$, posons $w_{\epsilon,\delta} = (-1)^\epsilon\sqrt{T^2+1} + v_\delta(d^{(-1)^\epsilon})$. Il est déjà clair que l'on a $E_d = \mathbb{Q}(T)(w_{0,0}) \subset L(v_0(d))$. De plus, pour tout $\epsilon \in \{0,1\}$ et tout $\delta \in [\![1,m]\!]$, on a $w_{\epsilon,\delta} = \mathcal{L}_{\delta,0} \circ g^\epsilon(w_{0,0})$. Il suffit donc de montrer que les $w_{\epsilon,\delta}$ sont deux à deux distincts. Soient donc (ϵ,δ) et (ϵ',δ') tels que $w_{\epsilon,\delta} = w_{\epsilon',\delta'}$. Supposons dans un premier temps $\epsilon = \epsilon'$ et $\delta \neq \delta'$. On a donc $0 = v_\delta(d^{(-1)^\epsilon}) - v_{\delta'}(d^{(-1)^\epsilon})$ et l'on aboutit à une contradiction comme dans le paragraphe précédent. Supposons maintenant $\epsilon \neq \epsilon'$. On a alors

$$0 = ((-1)^\epsilon - (-1)^{\epsilon'})\sqrt{T^2+1} + v_\delta(d^{(-1)^\epsilon}) - v_{\delta'}(d^{(-1)^{\epsilon'}}).$$

Comme dans le paragraphe précédent, soit $\mathcal{P}$ un idéal premier au dessus de $\mathcal{P}_{1,1}$ dans l'extension $\overline{\mathbb{Q}}M_1M_2/\overline{\mathbb{Q}}L$. Si v désigne à nouveau la valuation associée à $\mathcal{P}$, on a $v(v_\delta(d^{(-1)^\epsilon}) - v_{\delta'}(d^{(-1)^{\epsilon'}})) > 0$. Or $v(\sqrt{T^2+1}) = 0$. En effet, si $\sqrt{T^2+1}$ était dans $\mathcal{P}$, alors $T-i$ ou $T+i$ le serait aussi. D'après le lemme 1.1.7, i ou $-i$ serait alors égal à $-(1-\xi)/2+1/(2(1-\xi))$, ce qui est impossible. Puisque $(-1)^\epsilon - (-1)^{\epsilon'} \neq 0$, on en déduit $v(0) = v(w_{\epsilon,\delta} - w_{\epsilon',\delta'}) = 0$, une contradiction. □

1.2.4 Corollaires

Les trois énoncés ci-dessous s'obtiennent à partir du théorème précédent en considérant successivement les cas suivants :

1) m arbitraire et $d = -1$,

2) m égal à une puissance de 2 et $d = (m/2) - 1$,

3) m égal à une puissance de 2 et $d = (m/2) + 1$.

Corollaire 1.2.6. *L'extension $\mathbb{Q}(T, \sqrt{T^2+1} + \sum_{l=1}^m z_{2,l}z_{1,l})/\mathbb{Q}(T)$ est une D_{2m}-extension $\mathbb{Q}$-régulière. De plus, les $\mathbb{Q}(T)$-conjugués de $\sqrt{T^2+1} + \sum_{l=1}^m z_{2,l}z_{1,l}$ sont les*

$$(-1)^\epsilon\sqrt{T^2+1} + \sum_{l=1}^m z_{2,l}z_{1,l+\delta}, \quad (\delta,\epsilon) \in [\![1,m]\!] \times \{0,1\}.$$

Corollaire 1.2.7. *Soit $n \geq 3$. L'extension $\mathbb{Q}(T, \sqrt{T^2+1} + \sum_{l=1}^{2^{n-1}} z_{2,l}z_{1,-(2^{n-2}-1)l})/\mathbb{Q}(T)$ est une QD_{2^n}-extension $\mathbb{Q}$-régulière et les $\mathbb{Q}(T)$-conjugués de $\sqrt{T^2+1} + \sum_{l=1}^{2^{n-1}} z_{2,l}z_{1,-(2^{n-2}-1)l}$ sont les*

$$(-1)^\epsilon\sqrt{T^2+1} + \sum_{l=1}^{2^{n-1}} z_{2,l}z_{1,-(2^{n-2}-1)^{(-1)^\epsilon}l+\delta}, \quad (\delta,\epsilon) \in [\![1,2^{n-1}]\!] \times \{0,1\}.$$

Corollaire 1.2.8. *Soit $n \geq 3$. L'extension $\mathbb{Q}(T, \sqrt{T^2+1} + \sum_{l=1}^{2^{n-1}} z_{2,l}z_{1,-(2^{n-2}+1)l})/\mathbb{Q}(T)$ est une M_{2^n}-extension $\mathbb{Q}$-régulière et les $\mathbb{Q}(T)$-conjugués de $\sqrt{T^2+1} + \sum_{l=1}^{2^{n-1}} z_{2,l}z_{1,-(2^{n-2}+1)l}$ sont les*

$$(-1)^\epsilon\sqrt{T^2+1} + \sum_{l=1}^{2^{n-1}} z_{2,l}z_{1,-(2^{n-2}+1)^{(-1)^\epsilon}l+\delta}, \quad (\delta,\epsilon) \in [\![1,2^{n-1}]\!] \times \{0,1\}.$$

1.3 Groupes de quaternions généralisés

1.3.1 Notations

On considère la $\mathbb{Z}/2\mathbb{Z}$-extension $L/\mathbb{Q}(T) = \mathbb{Q}(T)(\sqrt{T^2+1})/\mathbb{Q}(T)$. On se donne $n \geq 3$ et on note $\xi = \exp(2\pi i/2^{n-1})$. Pour tout $k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*$, on pose $s_k = -(1-\xi^k)/2 + 1/(2(1-\xi^k))$.

Pour tout $k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*$ et tout $\ell \in \{1,2\}$, on choisit une racine 2^{n-1}-ième $x_{\ell,k}$ de $T+1+(-1)^\ell\sqrt{T^2+1}-\xi^k$ dans $\overline{\mathbb{Q}(T)}$. Pour $\ell \in \{1,2\}$, on note M_ℓ le compositum des corps $L(\xi, x_{\ell,k})$ ($k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*$). Pour tout $\ell \in \{1,2\}$ et tout $l \in \mathbb{N}$, on pose

$$z_{\ell,l} = \sum_{j\in(\mathbb{Z}/2^{n-1}\mathbb{Z})^*} \xi^{lj} \prod_{k\in(\mathbb{Z}/2^{n-1}\mathbb{Z})^*} x_{\ell,k}^{r_{2^{n-1}}(j/k)},$$

où $r_{2^{n-1}} : (\mathbb{Z}/2^{n-1}\mathbb{Z})^* \to [\![0, 2^{n-1}-1]\!]$ envoie $k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*$ sur son unique représentant modulo 2^{n-1}. De l'égalité $\xi^{2^{n-2}} = -1 = (-1)^j$ pour tout entier impair j, on déduit

$$z_{1,l+2^{n-2}} = \sum_{j\in(\mathbb{Z}/2^{n-1}\mathbb{Z})^*} \xi^{2^{n-2}j}\xi^{lj} \prod_{k\in(\mathbb{Z}/2^{n-1}\mathbb{Z})^*} x_{1,k}^{r_{2^{n-1}}(j/k)} = -z_{1,l}. \tag{1.3.1}$$

Comme dans le théorème 1.2.5, on pose $v_\delta(-1) = \sum_{l=1}^{2^{n-1}} z_{2,l}z_{1,l+\delta}$ pour tout $\delta \in [\![0, 2^{n-1}-1]\!]$. Pour simplifier, on écrira v_δ au lieu de $v_\delta(-1)$. Les v_δ sont deux à deux distincts et sont conjugués sur L par le théorème 1.2.5. De plus, pour tout $\delta \in \mathbb{N}$, (1.3.1) entraîne

$$v_{\delta+2^{n-2}} = -v_\delta. \tag{1.3.2}$$

Posons $\mu_1 = \sqrt{T^2+1-T\sqrt{T^2+1}}$, $\mu_2 = -\sqrt{T^2+1+T\sqrt{T^2+1}}$, $\mu_3 = -\mu_1$, $\mu_4 = -\mu_2$ et $H = \mathbb{Q}(T)(\mu_4)$. L'extension $H/\mathbb{Q}(T)$ est une $\mathbb{Z}/4\mathbb{Z}$-extension $\mathbb{Q}$-régulière dans laquelle l'extension $L/\mathbb{Q}(T)$ se plonge. Notons τ le générateur de $\mathrm{Gal}(H/\mathbb{Q}(T))$ qui envoie μ_4 sur μ_1.

On note $E/\mathbb{Q}(T)$ la D_{2^n}-extension $\mathbb{Q}$-régulière fournie par le corollaire 1.2.6.

1.3.2 Réalisations régulières explicites

Dans cette partie, nous construisons une extension galoisienne $\mathbb{Q}$-régulière explicite de $\mathbb{Q}(T)$ de groupe Q_{2^n} (voir théorème 1.3.2).

Commençons par déterminer $\mathrm{Gal}(HE/\mathbb{Q}(T))$.

Proposition 1.3.1. *L'extension $HE/\mathbb{Q}(T)$ est une Δ_n-extension $\mathbb{Q}$-régulière. De plus, le groupe $\mathrm{Gal}(HE/\mathbb{Q}(T))$ est engendré par deux éléments ρ et σ vérifiant les propriétés suivantes :*
- $\rho(\mu_4) = \mu_4$ et $\rho(v_\delta) = v_{\delta+1}$ pour tout $\delta \in [\![1, 2^{n-1}]\!]$,
- $\sigma(\mu_4) = \mu_1$ et $\sigma(v_0) = v_0$.
En outre, ρ et σ vérifient la présentation (1.1.2) et σ^2 fixe chaque élément de E.

Preuve. L'extension $L/\mathbb{Q}(T) = E^{\langle r\rangle}/\mathbb{Q}(T)$, où r est défini dans le théorème 1.2.5, se plonge dans la $\mathbb{Z}/4\mathbb{Z}$-extension $\mathbb{Q}$-régulière $H/\mathbb{Q}(T)$. La proposition 1.1.6 assure alors que $HE/\mathbb{Q}(T)$ est une Δ_n-extension $\mathbb{Q}$-régulière. Par la proposition 1.1.5, il existe un unique relèvement ρ de r dans $\mathrm{Gal}(HE/H)$ et celui-ci vérifie ce qui suit : pour tout relèvement $\widetilde{\tau}$ de τ dans Δ_n, les éléments ρ et $\widetilde{\tau}$ engendrent Δ_n et vérifient (1.1.2). Fixons maintenant un tel $\widetilde{\tau}$ et considérons sa restriction à E. Il est alors clair qu'il existe un entier t tel que $\mathrm{res}_{E/\mathbb{Q}(T)}^{HE/\mathbb{Q}(T)}(\widetilde{\tau}) = r^t s$, où s est défini dans le théorème 1.2.5, et que l'on a $\mathrm{res}_{E/\mathbb{Q}(T)}^{HE/\mathbb{Q}(T)}(\widetilde{\tau})(v_0) = r^t(v_0)$. La composée $\sigma = \rho^{-t}\widetilde{\tau}$ est alors un relevé de τ à HE qui fixe v_0. Aussi, non seulement ρ et σ vérifient bien les deux propriétés de l'énoncé, mais ils vérifient aussi (1.1.2) (voir proposition 1.1.5). Pour le dernier point, il suffit de remarquer que $E = L(v_0)$ (voir théorème 1.2.5), que $\mathrm{res}_{L/\mathbb{Q}(T)}^{HE/\mathbb{Q}(T)}(\sigma^2) = \mathrm{id}_L$ et que $\sigma^2(v_0) = v_0$. □

Le théorème suivant est le théorème 0.3.2 de l'introduction :

Théorème 1.3.2. *L'extension* $\mathbb{Q}(T, \sqrt{T^2+1} + (\mu_4 + v_0)^2)/\mathbb{Q}(T)$ *est une* Q_{2^n}*-extension* $\mathbb{Q}$*-régulière. De plus, les* $\mathbb{Q}(T)$*-conjugués de* $\sqrt{T^2+1} + (\mu_4 + v_0)^2$ *sont les*

$$(-1)^a\sqrt{T^2+1} + (\mu_a + v_\delta)^2, \quad (a,\delta) \in [\![1,4]\!] \times [\![0, 2^{n-2}-1]\!].$$

Preuve. La proposition 1.3.1 montre que $HE/\mathbb{Q}(T)$ est une Δ_n-extension $\mathbb{Q}$-régulière. Considérons les générateurs ρ et σ de $\mathrm{Gal}(HE/\mathbb{Q}(T))$ définis dans cette même proposition.

On a $HE = L(\mu_4 + v_0)$. En effet, par construction, le corps HE est le compositum sur L des corps $L(\mu_4) = H$ et $L(v_0) = E$, qui sont linéairement disjoints sur L (voir proposition 1.1.5). Comme $L(\mu_4)/L$ et $L(v_0)/L$ sont galoisiennes, on obtient bien que $\mu_4 + v_0$ est un élément primitif de HE sur L (voir, par exemple, [Wei09, Proposition 3.5.5]).

De plus, $L((\mu_4 + v_0)^2)/\mathbb{Q}(T)$ est une Q_{2^n}-extension $\mathbb{Q}$-régulière. En effet, le polynôme $X^2 - (\mu_4 + v_0)^2$ annule $\mu_4 + v_0$, donc $[HE : L((\mu_4 + v_0)^2)] \leq 2$. D'après (1.3.2), on a

$$\rho^{2^{n-2}} \circ \sigma^2(\mu_4 + v_0) = \rho^{2^{n-2}}(-\mu_4 + v_0) = -\mu_4 + v_{2^{n-2}} = -(\mu_4 + v_0).$$

L'élément $\rho^{2^{n-2}}\sigma^2$ correspond à $(2^{n-2}, 2)$ dans Δ_n, qui est d'ordre 2. Ainsi, pour des raisons de degré, on obtient $L((\mu_4 + v_0)^2) = (HE)^{\langle \rho^{2^{n-2}}\sigma^2 \rangle}$ et $\mathrm{Gal}(L((\mu_4 + v_0)^2)/\mathbb{Q}(T)) = Q_{2^n}$.

Enfin, on a $\mathbb{Q}(T, \sqrt{T^2+1} + (\mu_4 + v_0)^2) = L((\mu_4 + v_0)^2)$. En effet, pour tout $(a,\delta) \in [\![1,4]\!] \times [\![0, 2^{n-2}-1]\!]$, posons $w_{a,\delta} = (-1)^a\sqrt{T^2+1} + (\mu_a + v_\delta)^2$. Il suffit de montrer que $w_{0,0}$ est un élément primitif de $L((\mu_4 + v_0)^2)$ sur $\mathbb{Q}(T)$. Il est clair que $w_{0,0} \in L((\mu_4 + v_0)^2)$. Pour tout $(a,\delta) \in [\![1,4]\!] \times [\![0, 2^{n-2}-1]\!]$, on a $w_{a,\delta} = \rho^\delta \circ \sigma^a(w_{0,0})$. Il suffit donc de montrer que les $w_{a,\delta}$ sont deux à deux distincts. Soient (a,δ) et (b,t) deux éléments distincts de $[\![1,4]\!] \times [\![0, 2^{n-2}-1]\!]$ tels que $w_{a,\delta} = w_{b,t}$. On remarque tout d'abord que l'on a $v_\delta \neq -v_t$. En effet, si ce n'était pas le cas, alors on aurait $v_\delta = -v_t = v_{t+2^{n-2}}$ (par l'égalité (1.3.2)) et donc $\delta = t + 2^{n-2}$ car les v_δ sont deux à deux distincts comme mentionné dans le §1.3.1, une contradiction. De l'égalité $w_{a,\delta} = w_{b,t}$, un petit calcul montre que

$$2(\mu_a v_\delta - \mu_b v_t) = v_t^2 - v_\delta^2 + ((-1)^b - (-1)^a)(T+1)\sqrt{T^2+1} \in E \subset (HE)^{\langle \sigma^2 \rangle}, \tag{1.3.3}$$

où l'inclusion $E \subset (HE)^{\langle \sigma^2 \rangle}$ vient de la proposition 1.3.1. Ainsi, $\mu_a v_\delta - \mu_b v_t = \sigma^2(\mu_a v_\delta - \mu_b v_t) = -(\mu_a v_\delta - \mu_b v_t)$ et donc $\mu_a v_\delta - \mu_b v_t = 0$. On distingue maintenant deux cas.

Supposons d'abord a et b de même parité. L'équation (1.3.3) donne $v_t^2 - v_\delta^2 = 0$. Ainsi on a $v_t = v_\delta$ car $v_t \neq -v_\delta$. En conséquence, on obtient $t = \delta$. De l'égalité $\mu_a v_\delta - \mu_b v_t = 0$, on déduit $a = b$, une contradiction.

Supposons maintenant a et b de parité différente. En remarquant que

$$v_\delta^2 - v_t^2 = (v_\delta - v_t)(v_\delta + v_t) = (v_\delta - v_t)(v_\delta - v_{t+2^{n-2}}),$$

l'égalité (1.3.3) donne $(v_\delta - v_t)(v_\delta - v_{t+2^{n-2}}) = 2(-1)^b(T+1)\sqrt{T^2+1}$. Comme précédemment, soit $\mathcal{P}$ un idéal premier de $\overline{\mathbb{Q}}M_1M_2$ contenant $T + 1 - \sqrt{T^2+1} - \xi$ de valuation associée v. L'équation (1.2.5) dans la preuve du théorème 1.2.5 montre que $v(2(-1)^b(T+1)\sqrt{T^2+1}) = v((v_\delta - v_t)(v_\delta - v_{t+2^{n-2}})) > 0$. Par le lemme 1.1.7, on a $v(2(-1)^b(T+1)\sqrt{T^2+1}) = v((T+1)^2(T^2+1)) = 0$, une contradiction. Par conséquent $w_{a,\delta} \neq w_{b,t}$. □

1.3.3 Réalisations explicites de Q_{2^n} sur $\mathbb{Q}$

Dans cette partie, nous construisons des réalisations explicites de Q_{2^n} sur $\mathbb{Q}$ par spécialisation de la Q_{2^n}-extension $\mathbb{Q}$-régulière $\Gamma/\mathbb{Q}(T)$ fournie par le théorème 1.3.2 (voir théorème 1.3.10).

1.3.3.1 Bons premiers

On donne ici une condition suffisante pour qu'un nombre premier p soit un bon premier pour $\Gamma/\mathbb{Q}(T)$ (voir proposition 1.3.7).

Lemme 1.3.3. *a) Les points de branchement de $H/\mathbb{Q}(T)$ sont contenus dans $\{-i, i, 0, \infty\}$.*
b) L'ensemble des points de branchement de $M_1M_2/\mathbb{Q}(T)$ est contenu dans $\{-i, i, \infty\} \cup \{s_k \mid k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*\}$.
c) L'ensemble des points de branchement de $\Gamma/\mathbb{Q}(T)$ est contenu dans $\{-i, i, 0, \infty\} \cup \{s_k \mid k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*\}$.

Preuve. a) Cela vient du fait que le discriminant du polynôme minimal de μ_4 sur $\overline{\mathbb{Q}}(T)$ est $256T^4(T^2+1)^3$.

b) Soit $\lambda \in \overline{\mathbb{Q}}$ un point de branchement de $M_1M_2/\mathbb{Q}(T)$ qui n'est pas dans $\{-i, i\}$. Par [Sti09, Proposition 6.2.3], λ n'est pas un point de branchement de $L/\mathbb{Q}(T)$. En conséquence, on peut trouver un idéal premier $\mathcal{P}$ de $\overline{\mathbb{Q}}L$ contenant $T - \lambda$ et se ramifiant dans $\overline{\mathbb{Q}}M_1M_2/\overline{\mathbb{Q}}L$. Par le lemme 1.2.1 et le lemme d'Abhyankar, il existe $\ell \in \{1, 2\}$ et $k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*$ tels que $\mathcal{P}$ soit engendré par $T + 1 + (-1)^\ell\sqrt{T^2+1} - \xi^k$. D'où $\lambda = s_k$ par le lemme 1.1.7.

c) Il suffit de remarquer que l'on a $\Gamma \subset HM_1M_2$ et d'utiliser le a) et le b). □

Lemme 1.3.4. *Soit p un nombre premier impair qui ne divise pas $2^{2^{n-2}} + 1$. Alors, pour tout $t \in \{i, -i\} \cup \{s_k \mid k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*\}$ et tout idéal premier de $\mathbb{Z}[\xi]$ au dessus de p de valuation associée v, on a $v(t) = 0$.*

Preuve. Le cas où $t \in \{-i, i\}$ est immédiat. Il reste à considérer le cas où $t \in \{s_k \mid k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*\}$. Soit donc $k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*$. On a

$$s_k = \frac{\xi^k(2 - \xi^k)}{2(1 - \xi^k)}. \tag{1.3.4}$$

On remarque ensuite que le polynôme minimal de $1-\xi^k$ (resp. $2-\xi^k$) sur $\mathbb{Q}$ est $(X-1)^{2^{n-2}}+1$ (resp. $(X-2)^{2^{n-2}}+1$). Donc la norme de $1-\xi^k$ (resp. $2-\xi^k$) dans $\mathbb{Q}(\xi)/\mathbb{Q}$ est 2 (resp. $2^{2^{n-2}}+1$). Par conséquent, si v est comme dans l'énoncé, on a $v(x) = 0$ dès que x est un $\mathbb{Q}$-conjugué de $1 - \xi^k$ ou $2 - \xi^k$. On peut ainsi conclure en vertu de (1.3.4). □

Lemme 1.3.5. *Pour tout $x \in \mathbb{Q}(\xi)$, on note $N(x)$ la norme de x dans $\mathbb{Q}(\xi)/\mathbb{Q}$. Soit p un nombre premier impair tel que*
a) pour tout $k \not\equiv 1 \pmod{2^{n-1}}$, le nombre premier p ne divise pas $N((1 - \xi^k)(1 - \xi) + 1)$,
b) pour tout $k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*$, le nombre premier p ne divise pas $N(\xi^k(2 - \xi) \pm 2i(1 - \xi^k))$.
Alors deux points de branchement quelconques et distincts de $\Gamma/\mathbb{Q}(T)$ ne peuvent se rencontrer modulo p. Cette dernière conclusion est en particulier vraie pour $p \geq 7^{2^{n-2}} + 1$.

Preuve. Par le lemme 1.3.3, il suffit de vérifier que deux éléments quelconques et distincts de $\{-i, i, 0, \infty\} \cup \{s_k \mid k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*\}$ ne peuvent se rencontrer modulo p.

D'après le lemme 1.3.4, on a $v(s_k) = 0$ pour tout $k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*$ et toute valuation v de $\mathbb{Q}(\xi)$ étendant la valuation p-adique. Par conséquent, s_k et 0 ne peuvent se rencontrer modulo p. Il en est de même pour s_k et ∞.

On remarque maintenant que les s_k ($k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*$) sont deux à deux conjugués sur $\mathbb{Q}$. Par conséquent, pour montrer qu'il n'existe pas $k \neq l$ tels que s_k et s_l se rencontrent modulo p, il suffit de le faire pour $k \neq 1$ et $l = 1$. Fixons donc $k \neq 1$. On a

$$s_k - s_1 = \frac{\xi^k - \xi}{2(1 - \xi^k)(1 - \xi)}((1 - \xi^k)(1 - \xi) + 1).$$

D'après l'hypothèse du a), le nombre premier p ne divise pas $N((1-\xi^k)(1-\xi)+1)$. De plus, on montre comme dans la preuve du lemme 1.3.4 que p ne divise, ni $N(2(1-\xi^k)(1-\xi))$, ni $N(\xi^k-\xi)$. Le lemme 1.1.2 montre alors que s_k et s_1 ne se rencontrent pas modulo p.

Ensuite, pour tout $k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*$, on a

$$s_k \pm i = \frac{\xi^k(2-\xi^k) \pm 2i(1-\xi^k)}{2(1-\xi^k)}$$

et on montre comme ci-dessus que s_k et $\pm i$ ne peuvent se rencontrer modulo p.

Pour le dernier point, on remarque que les valeurs absolues des normes de a) et b) sont inférieures ou égales à $7^{2^{n-2}}$. □

Lemme 1.3.6. *Aucun nombre premier impair p n'est verticalement ramifié dans $\Gamma/\mathbb{Q}(T)$.*

Preuve. Il suffit de travailler au dessus du localisé $R = \mathbb{Z}[T]_{p\mathbb{Z}[T]}$ de $\mathbb{Z}[T]$ en $p\mathbb{Z}[T]$. Remarquons que $\Gamma \subset HM_1M_2$ et notons C la clôture intégrale de R dans HM_1M_2.

Tout d'abord, le discriminant du polynôme minimal de μ_4 sur $\mathbb{Q}(T)$ est $256T^4(T^2+1)^3 \notin p\mathbb{Z}[T]$, donc pR est non ramifié dans $H/\mathbb{Q}(T)$.

Soient maintenant $\ell_0 \in \{1,2\}$ et $k_0 \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*$. Les $\mathbb{Q}(T)$-conjugués de x_{ℓ_0,k_0} sont parmi les $\xi^l x_{\ell,k}$ où $l \in [\![1, 2^{n-1}]\!]$, $\ell \in \{1,2\}$ et $k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*$. En posant

$$\eta_{(l,\ell,k),(l',\ell',k')} = \xi^l x_{\ell,k} - \xi^{l'} x_{\ell',k'}$$

pour tous $(l,\ell,k) \neq (l',\ell',k')$, on voit que le discriminant du polynôme minimal de x_{ℓ_0,k_0} sur $\mathbb{Q}(T)$ divise $\prod_{(l,\ell,k)\neq(l',\ell',k')} \eta_{(l,\ell,k),(l',\ell',k')}$ dans C.

Soient $(l,\ell,k) \neq (l',\ell',k')$. Pour simplifier, on pose $\eta = \eta_{(l,\ell,k),(l',\ell',k')}$. Supposons tout d'abord $\ell \neq \ell'$. Par définition des $x_{\ell,k}$, on a $\eta r = 4T^2 + 4 - (\xi^k - \xi^{k'})^2 \in C$, où

$$r = (((-1)^l - (-1)^{l'})\sqrt{T^2+1} - (\xi^k - \xi^{k'})) \prod_{s=0}^{2^{n-2}} ((\xi^l x_{\ell,k})^{2^s} - (\xi^{l'} x_{\ell',k'})^{2^s}) \in C.$$

On peut encore multiplier $4T^2+4-(\xi^k-\xi^{k'})^2$ par ses $\mathbb{Q}(T)$-conjugués pour obtenir qu'il existe un $r' \in C$ tel que $\eta r' = 4^u T^v + a$, où $u \in \mathbb{N}$, $v \in \mathbb{N}$ et $a \in \mathbb{Z}[T]$ de degré inférieur ou égal à $v-1$.

Supposons maintenant $\ell = \ell'$ et $k = k'$. Dans ce cas, on a

$$\eta x_{\ell,k}^{2^{n-1}-1} = \xi^l(1-\xi^{l'-l})(T+1+(-1)^\ell\sqrt{T^2+1} - \xi^k).$$

En multipliant ce dernier élément par $T+1-(-1)^\ell\sqrt{T^2+1}-\xi^k \in C$, on obtient qu'il existe un r' dans C tel que $\eta r' = \xi^l(1-\xi^{l'-l})(2(1-\xi^k)T + (1-\xi)^2 - 1)$. Or, la norme de ξ dans $\mathbb{Q}(\xi)/\mathbb{Q}$ vaut ± 1 et, comme déjà vu, la norme de $1-\xi^k$ dans cette même extension est une puissance de 2 pour tout $k \not\equiv 0 \pmod{2^{n-1}}$. On peut encore multiplier

$$\xi^l(1-\xi^{l'-l})(2(1-\xi^k)T + (1-\xi)^2 - 1)$$

par ses $\mathbb{Q}(T)$-conjugués pour obtenir qu'il existe un $r'' \in C$ tel que $\eta r'' = \pm 2^u T^v + a$, où $u \in \mathbb{N}$, $v \in \mathbb{N}$ et $a \in \mathbb{Z}[T]$ de degré inférieur ou égal à $v-1$.

Supposons enfin $\ell = \ell'$ et $k \neq k'$. Dans ce cas, il existe un élément r de C tel $\eta r = 2^u$ avec $u \in \mathbb{N}$. En effet, le produit de η et $\prod_{s=0}^{2^{n-2}} ((\xi^l x_{\ell,k})^{2^s} - (\xi^{l'} x_{\ell,k'})^{2^s})$ vaut $-\xi^k(1-\xi^{k'-k})$, dont la norme est une puissance de 2.

En considérant les trois cas ci-dessus, il existe donc un élément r de C tel que le produit de r et du discriminant du polynôme minimal de x_{ℓ_0,k_0} sur $\mathbb{Q}(T)$ soit de la forme $2^uT^v+a \in \mathbb{Z}[T]$ avec $u \in \mathbb{N}$, $v \in \mathbb{N}$ et $a \in \mathbb{Z}_{(p)}[T]$ de degré inférieur ou égal à $v-1$. Par conséquent, ce discriminant n'est pas dans pR. En particulier, pR n'est pas ramifié dans $\mathbb{Q}(T)(x_{\ell_0,k_0})$. De plus, pR n'est pas ramifié dans $\mathbb{Q}(T,\xi)/\mathbb{Q}(T)$. Le lemme d'Abhyankar permet alors de conclure. □

Proposition 1.3.7. *Soit p un nombre premier impair qui vérifie les conditions du lemme 1.3.5. Alors p est un bon premier pour $\Gamma/\mathbb{Q}(T)$.*

Preuve. D'après les lemmes 1.3.5 et 1.3.6, p ne vérifie aucune des conditions 2) et 3) de la définition 1.1.3. De plus, p ne vérifie pas la condition 1). Quant à la condition 4), il suffit de voir que le corps engendré par les points de branchement de $\Gamma/\mathbb{Q}(T)$ est contenu dans $\mathbb{Q}(\xi)$. □

1.3.3.2 Invariant canonique de l'inertie

Dans ce qui suit, Λ et Σ sont les générateurs de Q_{2^n} de la présentation (1.1.3). Rappelons que les classes de conjugaison non triviales de Q_{2^n} sont
- les $\mathcal{A}_j = \{\Lambda^j, \Lambda^{-j}\}$ où $j \in [\![1, 2^{n-2}-1]\!]$ et $\mathcal{A}_{2^{n-2}} = \{\Lambda^{2^{n-2}}\}$,
- $\mathcal{B} = \{\Lambda^{2j}\Sigma \mid j \in [\![0, 2^{n-2}-1]\!]\}$,
- $\mathcal{C} = \{\Lambda^{2j+1}\Sigma \mid j \in [\![0, 2^{n-2}-1]\!]\}$.

Lemme 1.3.8. *La classe canonique de l'inertie du point de branchement i de $\Gamma/\mathbb{Q}(T)$ est $\mathcal{B}$ ou $\mathcal{C}$. De plus, il existe un $k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*$ et un $j \in [\![1, 2^{n-2}]\!]$ impair tels que la classe canonique de l'inertie du point de branchement s_k de $\Gamma/\mathbb{Q}(T)$ soit $\mathcal{A}_j$.*

Preuve. Pour tout $t \in \{-i, i, 0, \infty\} \cup \{s_k \mid k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*\}$, notons C_t la classe canonique de l'inertie de t dans $\Gamma/\mathbb{Q}(T)$. Puisque i est point de branchement de $L/\mathbb{Q}(T)$, la classe C_i n'est pas contenue dans $\mathrm{Gal}(\Gamma/L) = \langle\Lambda\rangle$. De plus, on vérifie facilement que l'on a $\mathcal{B}^3 = \mathcal{B}$ et $\mathcal{C}^3 = \mathcal{C}$. Ainsi, par le *Branch Cycle Lemma* (voir [Fri77] et [Völ96, Lemma 2.8]), on a $C_i = C_{-i}$.

Ensuite, puisque les points de branchement de $L/\mathbb{Q}(T)$ sont i et $-i$, la classe C_0 est de type $\mathcal{A}$ ou triviale et il en est de même des classes C_{s_k} (voir lemme 1.1.7). Supposons que toutes ces classes de conjugaison soient triviales ou de la forme $\mathcal{A}_j$ avec j pair. Puisque l'ensemble des points de branchement de $\Gamma/\mathbb{Q}(T)$ est contenu dans $\{-i, i, 0, \infty\} \cup \{s_k \mid k \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^*\}$ (voir lemme 1.3.3), le théorème d'existence de Riemann fournit $(g_i, g_{-i}, g_0, g_\infty, (g_{s_k})_k) \in C_i \times C_{-i} \times C_0 \times C_\infty \times (C_{s_k})_k$ tel que $\langle g_i, g_{-i}, g_0, g_\infty, \{g_k \mid k\}\rangle = Q_{2^n}$ et $g_i \cdot g_{-i} \cdot g_0 \cdot g_\infty \cdot \prod_k g_k = 1$. Notons $g_i = \Lambda^{a_i}\Sigma$, $g_{-i} = \Lambda^{a_{-i}}\Sigma$, avec a_i et a_{-i} de même parité, $g_0 = \Lambda^{2a_0}$, $g_\infty = \Lambda^{a_\infty}$ et $g_{s_k} = \Lambda^{2a_k}$ pour tout k. On obtient alors $1 = g_i \cdot g_{-i} \cdot g_0 \cdot g_\infty \cdot \prod_k g_k = \Lambda^v$ pour un certain entier v de même parité que $a_i + a_{-i} + 2a_0 + a_\infty + \sum_k 2a_k$. Par conséquent, a_∞ est pair. La condition $\langle g_i, g_{-i}, g_0, g_\infty, \{g_k \mid k\}\rangle = Q_{2^n}$ entraîne alors $Q_{2^n} = \langle\Lambda^2, \Sigma\rangle$ (si $C_i = C_{-i} = \mathcal{B}$) ou $Q_{2^n} = \langle\Lambda^2, \Lambda\Sigma\rangle$ (si $C_i = C_{-i} = \mathcal{C}$), ce qui est impossible. En effet, $\langle\Lambda^2\rangle$ est un sous-groupe distingué d'ordre 2^{n-2} et $\Sigma^2 = \Lambda^{2^{n-2}} \in \langle\Lambda^2\rangle$ (resp. $(\Lambda\Sigma)^2 = \Lambda^{2^{n-2}} \in \langle\Lambda^2\rangle$), donc $|\langle\Lambda^2, \Sigma\rangle|$ (resp. $|\langle\Lambda^2, \Lambda\Sigma\rangle|$) est 2^{n-1} alors que Q_{2^n} est d'ordre 2^n. Ainsi, soit la deuxième partie du lemme est vraie, soit l'indice de ramification de $\langle T\rangle$ dans $\Gamma\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ vaut 2^{n-1}. Or, cette dernière conclusion est impossible car 0 n'est pas un point de branchement de $M_1M_2/\mathbb{Q}(T)$ (voir lemme 1.3.3) et l'indice de ramification de $\langle T\rangle$ dans $H\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ vaut au plus 2. □

1.3.3.3 Théorème principal

Notons $m(X) = \prod_{k\in(\mathbb{Z}/2^{n-1}\mathbb{Z})^*}(X - s_k) \in \mathbb{Q}[X]$. Par le lemme 1.3.4, les dénominateurs des coefficients de $m(X)$ sont des puissances de 2.

Lemme 1.3.9. *Pour $p \equiv 1 \pmod{2^{n-1}}$ premier, il existe $t \in \mathbb{Z}$ tel que $v_p(m(t)) > 0$.*

Preuve. Notons O la clôture intégrale du localisé $\mathbb{Z}_{[2]}$ de $\mathbb{Z}$ en la partie multiplicative $\{2^j \mid j \geq 0\}$ dans $\mathbb{Q}(\xi)$. Soit $\mathcal{P}$ un idéal premier de O au dessus de $p\mathbb{Z}_{[2]}$. Puisque $p \equiv 1 \pmod{2^{n-1}}$, le degré résiduel $f(\mathcal{P}/p\mathbb{Z}_{[2]})$ est égal à 1, c'est-à-dire $O/\mathcal{P} = \mathbb{Z}_{[2]}/p\mathbb{Z}_{[2]}$. Il existe donc $t \in \mathbb{Z}_{[2]}$ tel que $m(t) = 0$ modulo $p\mathbb{Z}_{[2]}$. On peut en fait choisir t dans $\mathbb{Z}$, ce qui conclut la démonstration. □

Le théorème suivant est le théorème 0.3.3 de l'introduction :

Théorème 1.3.10. *Soient p et q deux nombres premiers distincts ne divisant pas $2^{2^{n-2}}+1$, qui vérifient les conditions du lemme 1.3.5 et tels que $p \equiv 1 \pmod{2^{n-1}}$ et $q \equiv 1 \pmod 4$. Soit $t_0 \in \mathbb{N}$ vérifiant $v_p(m(t_0)) = 1$ et $v_q(t_0^2+1) = 1$. Alors la spécialisation $\Gamma_t/\mathbb{Q}$ de $\Gamma/\mathbb{Q}(T)$ en t est galoisienne de groupe Q_{2^n} pour tout $t \equiv t_0 \pmod{p^2q^2}$.*

Preuve. Notons tout d'abord que t_0 comme dans l'énoncé existe. En effet, puisque $p \equiv 1 \pmod{2^{n-1}}$, il existe $t_{0,p}$ dans $\mathbb{Z}$ tel que $v_p(m(t_{0,p})) > 0$ (voir lemme 1.3.9). De plus, d'après l'hypothèse $q \equiv 1 \pmod 4$, il existe $t_{0,q}$ dans $\mathbb{Z}$ tel que $v_q(t_{0,q}^2+1) > 0$. D'après [Leg16, Lemma 3.12], quitte à changer $t_{0,p}$ et $t_{0,q}$, on peut supposer $v_p(m(t_{0,p})) = 1$ et $v_q(t_{0,q}^2+1) = 1$. Le théorème chinois fournit alors un $t_0 \in \mathbb{Z}$ tel que $v_p(t_0 - t_{0,p}) \geq 2$ et $v_q(t_0 - t_{0,q}) \geq 2$. Enfin, [Leg16, Remark 2.11] montre que t_0 vérifie les conditions de l'énoncé.

Fixons maintenant $t \equiv t_0 \pmod{p^2q^2}$. D'après les hypothèses $v_p(m(t_0)) = 1$ et $v_q(t_0^2+1) = 1$, on a $v_p(m(t)) = 1$ et $v_q(t^2+1) = 1$. En particulier, t n'est pas un point de branchement de $\Gamma/\mathbb{Q}(T)$ (voir lemme 1.3.3). Par [Leg16, Lemma 2.5], on obtient que t et s_1 (resp. t et i) se rencontrent modulo p (resp. q). En outre, d'après le lemme 1.3.7, les nombres premiers p et q sont de bons premiers pour $\Gamma/\mathbb{Q}(T)$. Enfin, p unitarise s_1 par le lemme 1.3.4 et il est clair que q unitarise i. Si k désigne l'élément de $(\mathbb{Z}/2^{n-1}\mathbb{Z})^*$ fourni par le lemme 1.3.8, le théorème 1.1.4 assure alors que $\mathrm{Gal}(\Gamma_t/\mathbb{Q})$ contient un élément de la classe canonique de l'inertie C_{s_k} (resp. C_i) du point de branchement s_k (resp. i) de $\Gamma/\mathbb{Q}(T)$. Par le lemme 1.3.8, on obtient que $\mathrm{Gal}(\Gamma_t/\mathbb{Q})$ contient un élément de $\mathcal{A}_j$ pour un certain $j \in [\![1, 2^{n-2}]\!]$ impair et, soit un élément de $\mathcal{B}$, soit un élément de $\mathcal{C}$. On obtient alors $\mathrm{Gal}(\Gamma_t/\mathbb{Q}) = Q_{2^n}$, ce qui achève la démonstration. □

Pour conclure ce chapitre, on détermine pour $n = 3$ un exemple explicite de p, q et t_0 comme dans le théorème. D'abord, on remarque que $m(X) = X^2 + X/2 + 5/8$. Ensuite, on s'assure que $p = 53$ et $q = 61$ vérifient les conditions du théorème. Enfin, des exemples de t_0 sont 804, 865 et 1758. Nous laissons au lecteur intéressé le soin de donner davantage d'exemples numériques.

Chapitre 2

Eléments de théorie des corps quelconques

Dans ce chapitre, nous résumons les résultats en théorie des corps quelconques, généralisant ceux connus en arithmétique des corps commutatifs, que nous utiliserons dans les chapitres 3 et 4. A cet effet, nous présentons, d'une part, la construction des anneaux et corps tordus et, d'autre part, la théorie de Galois des corps quelconques.

2.1 Généralités

Des références pour cette section sont [Coh95] et [GW04].

2.1.1 Corps

Un *corps* est un ensemble K, muni de deux lois internes, l'*addition* notée par le signe $+$, et la *multiplication* notée par le signe $\times$ ou $\cdot$ ou seulement une juxtaposition, avec deux éléments 0 et 1 tels que :

1) $(K,+)$ est un groupe abélien d'élément neutre 0,

2) $1 \neq 0$ et l'ensemble $K \setminus \{0\}$ est un groupe d'élément neutre 1 pour la multiplication,

3) la mutiplication est distributive par rapport à l'addition :

$$(a+b)c = ac + bc \quad \text{et} \quad a(b+c) = ab + ac \quad \text{pour tous } a,b,c \in K.$$

Un corps est dit *commutatif* si la loi de multiplication est commutative. Dans le cas contraire, on dit que le corps est *gauche*.

Exemples 2.1.1. 1) Etant donné un sous-corps K de $\mathbb{R}$, on définit *le corps des quaternions* $\mathbb{H}_K$ *à coefficients dans* K comme le K-espace vectoriel de base $1,i,j,k$ vérifiant :

$$ij = -ji = k, jk = -kj = i, ki = -ik = j.$$

Ce corps est gauche. Si $K = \mathbb{R}$, alors le corps des nombres complexes $\mathbb{C}$ s'identifie naturellement au sous-corps de $\mathbb{H}_{\mathbb{R}}$ engendré par $\mathbb{R}$ et i.

2) Les corps des fractions rationnelles tordus, que nous verrons dans le §2.1.3, sont des exemples de corps gauches.

Etant donnés un corps K et un sous-ensemble A de K, le *commutant* de A dans K est le sous-corps de K défini par

$$Z_K(A) = \{b \in K \mid ab = ba \text{ pour tout } a \in A\}.$$

Dans le cas $A = K$, on a le *centre* de K, donné par

$$Z(K) = \{b \in K \mid ab = ba, \text{ pour tout } a \in K\}.$$

Exemples 2.1.2. 1) Le commutant de $\mathbb{C}$ dans $\mathbb{H}_{\mathbb{R}}$ est $\mathbb{C}$.
2) Pour tout sous-corps K de $\mathbb{R}$, le centre de $\mathbb{H}_K$ est K.

2.1.2 Corps de fractions

Etant donné un anneau intègre[1] commutatif R, le *corps de fractions* de R est un corps K contenant R tel que tout $x \in K$ s'écrive $x = rs^{-1}$ pour certains $r \in R$ et $s \in R \setminus \{0\}$. Ce corps est unique à isomorphisme près. En notant j le morphisme d'inclusion de R dans K, cette définition est équivalente à la définition suivante :

Définition 2.1.3. Soit R un anneau intègre. Un *corps de fractions* de R est un corps K muni d'un plongement $j : R \hookrightarrow K$ tel que le sous-corps de K engendré par $j(R)$ soit égal à K.

Contrairement au cas commutatif, l'existence et l'unicité du corps de fractions ne sont pas toujours assurées pour les corps gauches. Par exemple, l'algèbre libre $K\langle X\rangle$ sur un corps quelconque K possède plusieurs corps de fractions non isomorphes (voir [Coh95, Page 54]). De même, en général, l'écriture $x = rs^{-1}$ n'est pas automatique. Néanmoins, Ore a trouvé une condition suffisante qui permet d'assurer à la fois l'écriture $x = rs^{-1}$, l'existence et l'unicité du corps de fractions.

Définition 2.1.4. Soit R un anneau intègre. On dit que R vérifie la *condition de Ore à droite* (resp. *à gauche*) si, pour tous $r, s \in R \setminus \{0\}$, on a

$$sR \cap rR \neq 0 \,(\text{resp. } Rs \cap Rr \neq 0).$$

Dans ce cas, on dit que R est un *anneau de Ore à droite* (resp. *à gauche*). Si R est à la fois de Ore à gauche et de Ore à droite, on dit tout simplement que R est un *anneau de Ore*.

Exemple 2.1.5. 1) Il est clair que tout anneau intègre commutatif est un anneau de Ore.
2) Tout anneau intègre noethérien à droite (resp. à gauche) est un anneau de Ore à droite (resp. à gauche). En particulier, tout anneau principal à droite (resp. à gauche) est un anneau de Ore à droite (resp. à gauche). Voir [Coh95, Propositions 1.3.6 et 1.3.7] pour plus de détails.

Nous renvoyons à [GW04, Chapter 6] et [Coh95, §1.3] pour des preuves des deux propositions suivantes.

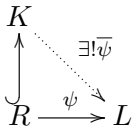
Proposition 2.1.6. *Tout anneau de Ore à droite (resp. à gauche) R admet, à isomorphisme près, un unique corps de fractions K et tout élément x de K s'écrit $x = rs^{-1}$ (resp. $x = s^{-1}r$) pour certains $r \in R$ et $s \in R \setminus \{0\}$.*

Remarque 2.1.7. Avec les notations de la proposition 2.1.6, la condition de Ore assure, d'une part, l'existence d'un dénominateur commun lorsque l'on additionne deux éléments de K et, d'autre part, l'écriture de tout produit d'éléments de K sous la forme rs^{-1} ou $s^{-1}r$.

Etant donné un anneau intègre commutatif R de corps de fractions K, la propriété universelle affirme que tout morphisme injectif de R dans un corps L se prolonge de manière unique en un morphisme de K dans L. Plus généralement, les anneaux de Ore satisfont aussi à une propriété universelle :

1. Un anneau quelconque R est dit *intègre* si $R \neq \{0\}$ et $xy \neq 0$ pour tous $x, y \in R \setminus \{0\}$.

Proposition 2.1.8. *Avec les notations de la proposition 2.1.6, tout morphisme injectif ψ de R dans un corps L se prolonge de manière unique en un morphisme $\overline{\psi} : K \to L$.*



2.1.3 Corps tordus

Dans cette partie, nous présentons la construction de Ore (voir [Ore33]) des anneaux de polynômes tordus (resp. corps de fractions rationnelles tordus, resp. corps de séries tordus) généralisant les anneaux de polynômes (resp. corps de fractions rationnelles, resp. corps de séries) sur les corps commutatifs.

2.1.3.1 Anneaux de polynômes et corps de fractions rationnelles tordus

Etant donné un corps commutatif K, construire une extension algébrique monogène $K(\alpha)/K$ revient à trouver un polynôme irréductible $P(T) \in K[T]$ vérifiant $L = K[T]/(P(T))$. L'anneau de polynômes joue ainsi un rôle important. Il est naturel de se demander s'il existe une généralisation à la situation des corps quelconques. Pour cela, on se donne un corps quelconque H. Le but est de construire un anneau de "polynômes", noté a priori A, comme l'espace vectoriel sur H de base $(T^n)_{n\geq 0}$. Les éléments de A sont alors considérés comme des polynômes $P(T) = \sum_{i=0}^{n} a_i T^i$ où $(a_i)_{i=0}^n \subset H$ et $n \in \mathbb{N}$. On définit le *degré* de P par $\deg(P) = \max\{i | a_i \neq 0\}$. Nous demandons que les conditions ci-dessous, valables pour les anneaux de polynômes sur les corps commutatifs, soient satisfaites.

1) Pour l'addition, on veut que

$$\sum_i a_i T^i + \sum_i b_i T^i = \sum_i (a_i + b_i) T^i \quad \text{pour tous } (a_i)_i, (b_i)_i \subset H.$$

2) Pour la mutiplication, on exige que le degré du produit de deux polynômes soit égal au produit de degrés. Ainsi, on obtient :

a) pour tout $a \in H$, il existe $\sigma(a), \delta(a) \in H$ uniques tels que $Ta = \sigma(a)T + \delta(a)$;

b) pour tous $a, b \in H$, on a

$$\sigma(ab)T + \delta(ab) = T(ab) = (\sigma(a)T + \delta(a))b = \sigma(a)\sigma(b)T + \sigma(a)\delta(b) + \delta(a)b. \tag{2.1.1}$$

De ces conditions, on déduit les faits suivants :

- Comme $1 \cdot T = T = T \cdot 1 = \sigma(1) \cdot T$, on a $\sigma(1) = 1$.
- Pour tous $a, b \in H$, on a $\sigma(ab) = \sigma(a)\sigma(b)$ (par (2.1.1)).
- Pour tous $a, b \in H$, on a

$$\sigma(a+b)T + \delta(a+b) = T(a+b) = \sigma(a)T + \delta(a) + \sigma(b)T + \delta(b) = (\sigma(a) + \sigma(b))T + \delta(a) + \delta(b),$$

donc $\sigma(a+b) = \sigma(a) + \sigma(b)$ et $\delta(a+b) = \delta(a) + \delta(b)$.

On voit que σ est un endomorphisme du corps H et que δ vérifie la définition suivante :

Définition 2.1.9. Soit σ un endomorphisme de H. Une *σ-dérivation* δ de H est un endomorphisme de $(H, +)$ vérifiant

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b,$$

pour tous $a, b \in H$. Si $\sigma = \mathrm{id}_H$, alors on trouve la notion de dérivation classique.

Muni de ces lois, il est facile de montrer que A, noté maintenant $H[T,\sigma,\delta]$, est un anneau intègre appelé *anneau de polynômes tordu associés à σ et δ*. Dans le cas où $\delta = 0$ (resp. $\sigma = \mathrm{id}$ et $\delta = 0$), on note tout simplement $H[T,\sigma]$ (resp. $H[T]$).

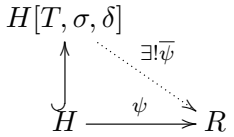
Exemples 2.1.10. 1) Notons τ la conjugaison complexe. Dans $\mathbb{C}[T,\tau]$, on a par exemple

$$(iT^2 + 5T + 1)(2iT + 3) = -2T^3 - 7iT^2 + (15 + 2i)T + 3.$$

2) Soient H un corps et σ un endomorphisme de H. Pour tout $y \in H$, on peut définir la σ-dérivation $\delta_y : x \in H \mapsto yx - \sigma(x)y \in H$, qu'on appelle *dérivation intérieure* associée à y.

Etant donnés un corps commutatif H et un anneau commutatif R, la propriété universelle affirme que se donner un morphisme $\overline{\psi} : H[T] \to R$ équivaut à se donner un morphisme $\psi : H \to R$ et un élément r de R. Dans cette correspondance, $\overline{\psi}(T) = r$ et $\overline{\psi}(x) = \psi(x)$ pour tout $x \in H$. Cette propriété universelle admet une généralisation aux anneaux de polynômes tordus (voir [GW04, Proposition 2.4] pour une preuve) :

Proposition 2.1.11. *Soient H un corps, σ un endomorphisme de H et δ une σ-dérivation de H. Soient R un anneau, $\psi : H \to R$ un morphisme et $r \in R$ vérifiant $r\psi(x) = \psi(\sigma(x))r + \psi(\delta(x))$ pour tout $x \in H$. Alors il existe un unique morphisme $\overline{\psi} : H[T,\sigma,\delta] \to R$ étendant ψ et vérifiant $\overline{\psi}(T) = r$.*



On se donne un corps H, un automorphisme σ de H et une σ-dérivation δ de H. La proposition suivante assure l'existence et l'unicité du corps de fractions de $H[T,\sigma,\delta]$ (voir [Coh95, §2.1] pour une preuve) :

Proposition 2.1.12. *L'anneau $H[T,\sigma,\delta]$ est un anneau de Ore.*

Par les propositions 2.1.12 et 2.1.6, $H[T,\sigma,\delta]$ admet un unique corps de fractions, noté $H(T,\sigma,\delta)$, appelé *corps de fractions rationnelles tordu associé à σ et δ*. Dans le cas où $\delta = 0$ (resp. $\sigma = \mathrm{id}$ et $\delta = 0$), on note simplement $H(T,\sigma)$ (resp. $H(T)$).

2.1.3.2 Corps de séries tordus

Nous allons voir comment se construisent les anneaux de séries tordus et les corps de séries tordus. La construction des anneaux de séries tordus est similaire à celle des anneaux de polynômes tordus. On se donne un corps quelconque H et un endomorphisme σ de H. L'*anneau de séries tordu associé à σ*, noté $H[[T,\sigma]]$, est l'ensemble des séries formelles $\sum_{i\geq 0} a_i T^i$ où $(a_i)_i \subset H$. L'addition sur $H[[T,\sigma]]$ est donnée par :

$$\sum_i a_i T^i + \sum_i b_i T^i = \sum_i (a_i + b_i) T^i. \tag{2.1.2}$$

La multiplication est déterminée par

$$Ta = \sigma(a)T, \tag{2.1.3}$$

pour tout $a \in H$. Dans le cas où $\sigma = \mathrm{id}$, on note simplement $H[[T]]$.

A partir de maintenant, on suppose que σ est un automorphisme. Pour une preuve du lemme suivant, voir [Coh95, Chapter 2].

Lemme 2.1.13. *L'anneau $H[[T,\sigma]]$ est un anneau de Ore.*

Par les propositions 2.1.12 et 2.1.6, $H[[T,\sigma]]$ admet un unique corps de fractions que l'on note $H((T,\sigma))$, appelé *le corps de séries tordu associé à* σ. Le corps $H((T,\sigma))$ peut être défini explicitement de la manière suivante. Il est formé des séries $\sum_{i\geq m} a_i T^i$ avec $m \in \mathbb{Z}$ et $(a_i)_i \subset H$ muni des lois vérifiant (2.1.2) et (2.1.3). Dans le cas où $\sigma = \mathrm{id}$, on note simplement $H((T))$.

En utilisant les propositions 2.1.8 et 2.1.11, nous obtenons le résultat suivant :

Lemme 2.1.14. *L'application définie par* $a \mapsto a$ *(pour tout* $a \in H$*) et* $T \mapsto T$ *est un plongement de* $H[T,\sigma]$ *(resp.* $H(T,\sigma)$*) dans* $H[[T,\sigma]]$ *(resp.* $H((T,\sigma))$*).*

Par l'identification du lemme précédent, il est en fait possible de caractériser les éléments de $H((T,\sigma))$ qui sont dans $H(T,\sigma)$. Cette caractérisation apparaît dans [Coh95, Proposition 2.3.3] sans preuve détaillée. Pour le confort du lecteur, nous en donnons une.

Proposition 2.1.15. *(Critère de rationalité) Soient* H *un corps et* σ *un automorphisme de* H*. Soit* $x = \sum_{n\geq n_0} a_n T^n \in H((T,\sigma))$*, où* $(x_n)_n \subset H$ *et* $a_{n_0} \neq 0$*. Alors* $x \in H(T,\sigma)$ *si et seulement s'il existe* $s \geq 1, n_1 \geq 0$ *et des éléments* $y_1, \ldots, y_s$ *de* H *tels que, pour tout* $n > n_1$*, on ait*

$$a_n = a_{n-1}\sigma^{n-1}(y_1) + a_{n-2}\sigma^{n-2}(y_2) + \cdots + a_{n-s}\sigma^{n-s}(y_s). \tag{2.1.4}$$

Démonstration. D'abord, supposons $x \in H(T,\sigma)$. Comme $H[T,\sigma]$ est un anneau de Ore, on peut écrire $x = P(T)Q(T)^{-1}$ pour certains $P(T) \in H[T,\sigma]$ et $Q(T) \in H[T,\sigma] \setminus \{0\}$. En conséquence, il existe $(y_l)_{l=1}^s \subset H$ $(s \geq 1)$ et $(d_j)_{j=q}^r \subset H$ $(q \in \mathbb{Z}$ et $q \leq r)$ tels que

$$\left(\sum_{n\geq n_0} a_n T^n\right)\left(1 - \sum_{l=1}^{s} y_l T^l\right) = \sum_{j=q}^{r} d_j T^j,$$

ce qui mène à une égalité de la forme

$$\sum_{n\geq n_0} a_n T^n - \sum_{n=n_0+1}^{\infty}\left(\sum_{k=n-1}^{n-s} a_k \sigma^k(y_{n-k})\right) T^n = \sum_{j=q}^{r} d_j T^j.$$

De cette égalité, en posant $n_1 = \max(r, n_0+1)$, on obtient

$$a_n = \sum_{k=n-1}^{n-s} a_k \sigma^k(y_{n-k}) = a_{n-1}\sigma^{n-1}(y_1) + a_{n-2}\sigma^{n-2}(y_2) + \cdots + a_{n-s}\sigma^{n-s}(y_s)$$

pour tout $n > n_1$.

Pour la réciproque, par le calcul précédent, on voit facilement que $x(1 - \sum_{l=1}^s y_l T^l)$ s'écrit $\sum_{j=q}^r d_j T^j$, donc on peut écrire $x = P(T)Q(T)^{-1} \in H(T,\sigma)$ avec $P(T) \in H[T,\sigma]$ et $Q(T) \in H[T,\sigma] \setminus \{0\}$. □

2.2 Formes réduites

Pour plus de détails sur les notions et résultats rappelés dans cette partie, nous renvoyons à [Bou12].

Nous commençons par rappeler la notion d'algèbre simple centrale.

Définition 2.2.1. Soit k un corps commutatif. Une *algèbre simple centrale* sur k est une k-algèbre $\mathcal{A}$ de dimension finie sur k et simple (n'admettant pas d'idéal bilatère non trivial).

Exemples 2.2.2. 1) Tout corps H de dimension finie sur son centre k est une algèbre simple centrale sur k.
2) Etant donné un sous-corps K de $\mathbb{R}$, le corps des quaternions $\mathbb{H}_K$ est une algèbre simple centrale sur K.

On se donne maintenant un corps commutatif k et une algèbre simple centrale $\mathcal{A}$ sur k. Rappelons que la dimension $[\mathcal{A} : k]$ de $\mathcal{A}$ sur k est toujours un carré parfait et notons ainsi $[\mathcal{A} : k] = n^2$. On fixe une k-base $(e_1, \ldots, e_{n^2})$ de $\mathcal{A}$. Rappelons la construction de la *norme réduite*. On se donne un corps neutralisant D de $\mathscr{A}$, c'est-à-dire il existe un isomorphisme de k-algèbres $\varphi : \mathscr{A} \otimes_k D \to \mathscr{M}_n(D)$. La norme réduite $\mathrm{Nrd}_{\mathscr{A}/k}$ est la composée des applications :

$$\mathrm{Nrd}_{\mathscr{A}/k} : \mathscr{A} \xrightarrow{a \mapsto a \otimes 1} \mathscr{A} \otimes_k D \xrightarrow{\varphi} \mathscr{M}_n(D) \xrightarrow{\det} D \ .$$

La norme réduite est indépendante du choix de D et de φ. On montre aussi que $\mathrm{Nrd}_{\mathscr{A}/k}$ est à valeurs dans k. La norme réduite mesure en quelques sortes le défaut d'inversibilité d'un élément dans $\mathscr{A}$. En effet, un élement x de $\mathscr{A}$ est inversible si et seulement si $\mathrm{Nrd}_{\mathscr{A}/k}(x) \neq 0$. L'application $\mathcal{F}_{\mathscr{A}}(X_1, \ldots, X_{n^2})$ donnée par

$$\mathcal{F}_{\mathscr{A}}(X_1, \ldots, X_{n^2}) = \mathrm{Nrd}_{\mathscr{A}/k}(X_1 e_1 + X_2 e_2 + \cdots + X_{n^2} e_{n^2}),$$

pour tout $(X_1, X_2, \ldots, X_{n^2}) \in k^{n^2}$ est une k-forme de degré n, que l'on appelle *forme réduite associée à* $\mathrm{Nrd}_{\mathscr{A}/k}$ *relativement à la* k*-base* $(e_1, e_2, \ldots, e_{n^2})$ de $\mathcal{A}$. A partir de maintenant, on considère $\mathcal{F}_{\mathcal{A}}$ comme un polynôme dans $k[X_1, \ldots, X_{n^2}]$.

Exemple 2.2.3. Etant donné un sous-corps K de $\mathbb{R}$, la forme réduite de $\mathbb{H}_K/K$ (où $\mathbb{H}_K$ désigne le corps des quaternions à coefficients dans K) relative à la base $(1, i, j, k)$ est donnée par

$$\mathcal{F}_{\mathbb{H}_K}(X_1, X_2, X_3, X_4) = X_1^2 + X_2^2 + X_3^2 + X_4^2.$$

Nous obtenons facilement le lemme suivant.

Lemme 2.2.4. *La* k*-algèbre* $\mathcal{A}$ *est un corps si et seulement si* $\mathcal{F}_{\mathcal{A}}$ *ne possède que le zéro trivial sur* k*.*

Nous rappelons enfin quelques résultats établis dans [DL20] que nous utiliserons dans le chapitre 4. On se donne une extension de corps commutatifs L/k et une algèbre simple centrale $\mathcal{A}$ sur k vérifiant $[\mathcal{A} : k] = n^2$. La L-algèbre $\mathcal{A} \otimes_k L$ est simple centrale et l'on a $[\mathcal{A} \otimes_k L : L] = n^2$. De plus, $(e_1 \otimes_k 1, \ldots, e_{n^2} \otimes_k 1)$ est une L-base de $\mathcal{A} \otimes_k L$. Notons $\mathcal{F}_{\mathcal{A} \otimes_k L}$ la forme réduite associée à cette base.

Lemme 2.2.5. *Les formes* $\mathcal{F}_{\mathscr{A}}$ *et* $\mathcal{F}_{\mathscr{A} \otimes_k L}$ *sont égales.*

Le lemme suivant découle immédiatement des deux lemmes précédents.

Lemme 2.2.6. *Supposons que* $\mathscr{A}$ *soit un corps. Alors* $\mathscr{A} \otimes_k L$ *est un corps si et seulement si* $\mathcal{F}_{\mathscr{A}}$ *ne possède que le zéro trivial sur* L

2.3 Théorie de Galois

Dans cette partie, nous présentons la théorie de Galois des corps quelconques. Nous renvoyons à [Coh95] et [Jac56] pour plus de détails sur ce qui suit.

2.3.1 Extensions de corps

On dit qu'un corps E est une *extension* d'un corps K, notée E/K, s'il existe un plongement $j : K \hookrightarrow E$. Dans ce cas, on identifie les éléments de K à leurs images par j dans E et on peut ainsi écrire l'inclusion $K \subset E$ sans ambiguïté.

On se donne maintenant un anneau E contenant un corps K. Naturellement, E est à la fois un K-espace vectoriel à gauche et à droite sur K.

Définition 2.3.1. Le *degré à gauche* (resp. à droite) de E sur K, noté $[E : K]_g$ (resp. $[E : K]_d$), est la dimension de E sur K en tant que K-espace vectoriel à gauche (resp. à droite).

Exemples 2.3.2. 1) Le corps $\mathbb{H}_{\mathbb{R}}$ est de dimension 4 (à droite ou à gauche) sur $\mathbb{R}$.
2) On se donne un corps commutatif k et on note $K = k(T)$ le corps des fractions rationnelles en la variable T sur k. L'anneau $E = K[X, \sigma]/(X^2)$ est de dimension 3 (resp. 2) à gauche (resp. à droite) sur K de K-base $1, X, XT$ (resp. $1, X$) où σ est le k-endomorphisme de K envoyant T sur T^2 (voir [Coh95, Exercise 1, page 96]). Cet exemple montre que, contrairement au cas commutatif, les structures de K-espaces vectoriels à gauche et à droite sur E ne coïncident pas.

Supposons maintenant que E soit un corps. On dit que l'extension E/K est *finie à gauche* (resp. à droite) si $[E : K]_g$ (resp. $[E : K]_d$) est fini. Pour tout $x \in E \setminus \{0\}$, l'*automorphisme intérieur de E associé à x*, noté $I(x)$, est défini par $I(x)(y) = xyx^{-1}$ pour tout $y \in E$. L'*ordre intérieur* d'un automorphisme σ de E est le plus petit $n \geq 1$ tel que σ^n soit un automorphisme intérieur de E (si un tel n existe), et ∞ sinon. Une extension E/K est dite *extérieure* si $\mathrm{Aut}(E/K)$ ne contient aucun automorphisme intérieur non trivial, ou encore $Z_E(K) = Z(E)$ où $Z_E(K)$ (resp. $Z(E)$) désigne le commutant de K dans E (resp. le centre de E). En particulier, si E/K est extérieure, alors on a $Z(K) \subset Z(E)$.

Remarque 2.3.3. Si E/K est une extension de corps commutatifs, alors elle est extérieure.

2.3.2 Extensions galoisiennes

Comme déjà annoncé, nous utilisons le point de vue artinien dans ce manuscrit.

Définition 2.3.4. (Artin) Une extension de corps E/K est dite *galoisienne* si $E^{\mathrm{Aut}(E/K)} = K$ où $E^{\mathrm{Aut}(E/K)}$ désigne le sous-corps de E fixé par tout automorphisme dans $\mathrm{Aut}(E/K)$. Dans ce cas, le *groupe de Galois* de E/K, que l'on note $\mathrm{Gal}(E/K)$, est $\mathrm{Aut}(E/K)$.

Il y a plusieurs intérêts à considérer ce point de vue :

1) D'abord, si E/K est une extension algébrique de corps commutatifs, alors E/K est galoisienne (au sens d'Artin) si et seulement si E/K est normale et séparable. Ainsi le point de vue artinien généralise la définition que l'on apprend habituellement en licence.
2) Ensuite, même dans le cas commutatif, le point de vue artinien est plus général. Par exemple, pour un corps commutatif infini K, l'extension $K(T)/K$ est galoisienne mais n'est pas algébrique. Dans ce cas, le groupe de Galois de $K(T)/K$ est $\mathrm{PGL}_2(K)$ et il agit par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot T = \frac{aT + b}{cT + d}.$$

3) Enfin, les notions d'algébricité sur les corps gauches sont bien différentes. En effet, rappelons que, pour un élément x d'un corps commutatif E contenant un corps K, les deux conditions suivantes sont équivalentes :
i) il existe un entier $n \geq 1$ et $a_0, \ldots, a_{n-1} \in K$ tels que $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} = 0$,
ii) le sous-corps de E engendré par K et x est de dimension finie sur K.

Bien entendu, si ces conditions sont vérifiées, on dit que x est algébrique sur K. Maintenant, si l'on ne suppose plus E et K commutatifs, on dit que x est *algébrique à gauche* sur K si i) est vérifiée. D'une part, on a toujours $ii) \Rightarrow i)$ mais $i) \Rightarrow ii)$ n'est pas claire. D'autre part, les propriétés du type "x, y algébriques sur K impliquent $x+y$ et xy algébriques sur K" ou "F/E et E/K algébriques impliquent F/K algébrique" ne sont pas claires.

Le point de vue artinien est donc le seul raisonnable pour faire de la théorie de Galois des corps quelconques. De plus, pour une extension galoisienne E/K telle que $[E:K]_g < \infty$ ou $[E:K]_d < \infty$, on a toujours $[E:K]_g = [E:K]_d$ (voir [Coh95, Corollary 3.3.4]).

2.3.3 Théorie de Galois finie

Dans cette partie, nous rappelons le théorème fondamental de la théorie de Galois des corps quelconques (voir théorème 2.3.9 ci-dessous). Pour une extension galoisienne finie E/K de corps commutatifs, il existe autant de corps intermédiaires $K \subset F \subset E$ que de sous-groupes H de $\mathrm{Gal}(E/K)$. Comme le montre le théorème 2.3.9, cette affirmation n'est plus vraie en général, à cause de la présence des automorphismes intérieurs.

Nous rappelons d'abord le matériel nécessaire à l'énoncé du théorème. Les sous-groupes qui apparaissent dans la correspondance de Galois sont exactement les sous-groupes qui vérifient la définition suivante :

Définition 2.3.5. Un groupe d'automorphismes G d'un corps K (c'est-à-dire $G \leq \mathrm{Aut}(K)$) est un *N-groupe* (après Noether) si l'ensemble

$$A_{G,K} = \{x \in K \setminus \{0\} \mid I(x) \in G\} \cup \{0\}$$

est une algèbre sur $Z(K)$. Si c'est le cas, on dit que $A_{G,K}$ est l'*algèbre associée* à G.

Remarque 2.3.6. La propriété d'être un N-groupe n'est pas une propriété de groupe mais dépend de l'action du groupe sur un corps.

On remarque que le sous-groupe

$$G_0 = \{I(x) \mid x \in A_{G,K} \setminus \{0\}\}$$

est normal dans G. On définit l'*ordre réduit* de G par

$$|G|_{\mathrm{red}} = [G : G_0][A_{G,K} : Z(K)].$$

Remarque 2.3.7. Supposons K commutatif. Alors $I(x) = \mathrm{id}$ est un élément de G pour tout $x \in K \setminus \{0\}$. Ainsi $G_0 = \{\mathrm{id}\}$ et $A_{G,K} = K$. Donc $|G|_{\mathrm{red}} = |G|$.

Définition 2.3.8. Soit G un N-groupe agissant sur un corps K.

1) Un sous-groupe H de G est un *N-sous-groupe* si H est un N-groupe pour l'action sur K induite par celle de G.

2) Un sous-groupe H de G est dit *N-invariant* si le N-sous-groupe de G engendré par $\mathscr{N}_G(H)$ est égal à G, où $\mathscr{N}_G(H)$ désigne le normalisateur de H dans G.

Théorème 2.3.9. *(Correspondance de Galois) Soit E/K une extension galoisienne de groupe G telle que $[E:K]_g < \infty$.*

1) Il existe une correspondance bijective entre les N-sous-groupes H de G et les sous-corps intermédiaires $K \subset L \subset E$:

$$H \mapsto E^H = \{x \in E \mid \sigma(x) = x \ \textit{pour tout}\ \sigma \in H\}$$

$$L \mapsto \mathrm{Fix}_G(L) = \{\sigma \in G \mid \sigma(x) = x \ \textit{pour tout} \ x \in L\}.$$

Dans cette correspondance, E/E^H est galoisienne de groupe H et on a $[E : E^H]_g = |H|_{\mathrm{red}}$.
2) Si H est un N-sous-groupe, alors $\mathrm{Aut}(E^H/K) = N_G(H)/H$. *De plus, E^H/K est galoisienne si et seulement si H est N-invariant dans G.*

Remarque 2.3.10. 1) La notion de N-groupe est l'équivalent de la notion de sous-groupe normal dans la correspondance de Galois usuelle.
2) Il n'est pas difficile de voir que, si E/K est une extension galoisienne finie extérieure, la correspondance est similaire à la correspondance de Galois usuelle, c'est-à-dire entre tous les sous-groupes du groupe de Galois de E/K et tous les sous-corps intermédiaires.
3) Une conséquence de ce théorème est que, si E/K est une extension galoisienne finie à groupe de Galois d'ordre fini G, alors $[E : K]_g = |G|_{\mathrm{red}} \leq |G|$. En général, il n'y a pas égalité, comme le montre B. Deschamps dans [Des18].
4) Etant donné un corps H de dimension finie sur son centre k, on a vu que H/k était galoisienne de groupe H^*/k^* (voir exemples 0.2.1). Un sous-groupe U/k^* (avec $k^* \subset U \subset H^*$) de H^*/k^* est un N-sous-groupe si seulement si $A_{U,H} = U \cup \{0\}$ est une k-sous-algèbre de H. Cela revient à dire que $U \cup \{0\}$ est un corps (car $[H : k] < \infty$) . La correspondance de Galois associe alors à chaque N-sous-groupe U/k^* le sous-corps $H^{U/k^*} = Z_H(U \cup \{0\})$ de H et à chaque sous-corps intermédiaire $k \subset L \subset H$ le N-sous-groupe $Z_H(L)^*/k^*$.

2.3.4 Théorie de Galois infinie

Nous rappelons enfin la généralisation de la correspondance de Galois profinie. Pour plus de détails, voir [Jac56, Chapter VII].

Définition 2.3.11. Une extension E/K est dite *relativement algébrique à gauche* si pour tout $\xi \in E$, le sous-corps $K(\xi)$ de E engendré par K et ξ est de dimension finie à gauche sur K.

On se donne une extension galoisienne E/K, extérieure et relativement algébrique à gauche de groupe de Galois G. Ce groupe de Galois est en fait un groupe profini (voir [Jac56, Page 167] pour plus de détails).

Théorème 2.3.12. *Les applications*

$$H \mapsto E^H = \{x \in E \mid \sigma(x) = x \ \textit{pour tout} \ \sigma \in H\}$$

et

$$L \mapsto \mathrm{Fix}_G(L) = \{\sigma \in G \mid \sigma(x) = x \ \textit{pour tout} \ x \in L\}.$$

établissent une correspondance bijective entre les sous-groupes fermés H de G et les sous-corps intermédiaires $K \subset L \subset E$. Par cette correspondance, E^H/K est galoisienne si et seulement si H est normal dans G, et dans ce cas, le groupe de Galois de E^H/K s'identifie au groupe G/H.

Remarque 2.3.13. Dans le cas d'une extension galoisienne algébrique de corps commutatifs, le théorème 2.3.12 coïncide avec la correspondance de Galois infinie usuelle.

Chapitre 3

Théorie inverse de Galois sur les corps de fractions rationnelles tordus

Dans ce chapitre, nous montrons que, si H est un corps de centre h et σ un automorphisme d'ordre fini de H tels que le sous-corps $h^{\langle\sigma\rangle}$ de h fixé par σ contienne un corps ample, alors le problème inverse de Galois admet une réponse positive sur le corps $H(T,\sigma)$ des fractions rationnelles tordu. De plus, si $h^{\langle\sigma\rangle}$ contient un corps qui est, soit réel clos, soit hensélien de caractéristique résiduelle nulle et contenant toutes les racines de l'unité, alors le groupe prolibre de rang dénombrable $\widehat{F}_\omega$ est groupe de Galois sur $H(T,\sigma)$.

Ce chapitre est basé sur l'article [Beh21] et est divisé en deux parties. D'abord, dans la section 3.1, nous montrons le théorème 0.3.5. Ensuite, dans la section 3.2, nous prouvons le théorème 0.3.6.

3.1 Preuve du théorème 0.3.5

Commençons par rappeler la stratégie de l'extension galoisienne des scalaires présentée dans [DL20] :

Lemme 3.1.1. *Soient K un corps et k un corps contenu dans le centre $Z(K)$ de K. Si L/k désigne une extension algébrique galoisienne de groupe G telle que la k-algèbre $M = K \otimes_k L$ soit un corps, alors :*

1) Si l'on considère K comme sous-corps de M, l'application

$$\begin{array}{ccccccccc} \Psi & : & \mathrm{Gal}(L/k) & \to & \mathrm{Aut}(M/K) & & & & \\ & & \sigma & \mapsto & \Psi(\sigma) & : & M & \to & M \\ & & & & & & h\otimes x & \mapsto & h\otimes\sigma(x) \end{array} \tag{3.1.1}$$

est un isomorphisme de groupes.

2) L'extension M/K est galoisienne de groupe G.

Démonstration. 1) On voit facilement que Ψ est un monomorphisme de groupes. Pour la surjectivité, considérons $\eta \in \mathrm{Gal}(M/K)$. On remarque tout d'abord que $Z(M)$ est un corps. Vu que $\eta(Z(M)) = Z(M)$, la restriction de η à $Z(M)$ est un k-automorphisme. Or $(k \otimes_k L)/k$ est une sous-extension galoisienne de $Z(M)/k$, donc $\eta(k \otimes_k L) = k \otimes_k L$. Ainsi, on peut définir une application $\sigma_\eta : L \to L$ qui à $l \in L$ associe l'unique $\tilde{l} \in L$ vérifiant $\eta(1 \otimes l) = 1 \otimes \tilde{l}$. On vérifie aisément que σ_η est un isomorphisme d'anneaux, donc $\sigma_\eta \in \mathrm{Gal}(L/k)$. Il reste à vérifier que l'on a $\Psi(\sigma_\eta) = \eta$. A cet effet, pour $h \in K$ et $l \in L$, on a $\Psi(\sigma_\eta)(h \otimes l) = \Psi(\sigma_\eta)(h \otimes 1)\Psi(\sigma_\eta)(1 \otimes l) = (h \otimes 1)(1 \otimes \sigma_\eta(l)) = \eta(h \otimes 1)\eta(1 \otimes l) = \eta((h \otimes 1)(1 \otimes l)) = \eta(h \otimes l)$. Ainsi, on a $\Psi(\sigma_\eta) = \eta$.

2) On voit immédiatement que la sous-algèbre des invariants de M par l'action de $\mathrm{Aut}(M/K)$ vaut K, ce qui conclut la preuve. □

La difficulté dans la méthode de l'extension galoisienne des scalaires consiste à assurer que l'algèbre $M = K \otimes_k L$ reste un corps. Dans [DL20], les auteurs y arrivent en considérant $K = H(T)$, le corps de fractions tordus à indéterminée centrale dont le corps des constantes H est de dimension finie sur son centre h. Ils contrôlent alors les zéros de la norme réduite dans l'extension $L/h(T)$. Ceci limite de manière rédhibitoire l'étude au cas où $K = H(T, \mathrm{id})$ avec $[H : h] < +\infty$. La nouvelle approche que nous proposons pour le cas $K = H(T, \sigma)$ consiste à plonger K, L et M dans un même corps (de séries). Cela va nous permettre d'étendre le résultat de [DL20] à des cas où $\sigma \neq \mathrm{id}$ et $[H : h] = +\infty$.

Proposition 3.1.2. *Soient H un corps de centre h (de dimension non nécessairement finie sur h) et σ un automorphisme de H d'ordre $n \geq 1$. Si $h^{\langle\sigma\rangle}$ désigne le corps des invariants de h par l'action de σ, alors l'application $h^{\langle\sigma\rangle}(T^n)$-linéaire*

$$\tau : H(T, \sigma) \otimes_{h^{\langle\sigma\rangle}(T^n)} h^{\langle\sigma\rangle}((T^n)) \to H((T, \sigma)),$$

qui envoie chaque tenseur $x \otimes l$ sur xl, est un monomorphisme de $h^{\langle\sigma\rangle}(T^n)$-algèbres.

En particulier, pour toute extension intermédiaire $h^{\langle\sigma\rangle}(T^n) \subset L \subset h^{\langle\sigma\rangle}((T^n))$ de dimension finie sur $h^{\langle\sigma\rangle}(T^n)$, l'algèbre $H(T, \sigma) \otimes_{h^{\langle\sigma\rangle}(T^n)} L$ est un corps.

Démonstration. En toute généralité, si A, B, C désignent trois k-algèbres et $f : A \to C$, $g : B \to C$ sont deux morphismes de k-algèbres, alors l'application k-linéaire $A \otimes_k B \longrightarrow C$ qui au tenseur $a \otimes b$ associe $f(a)g(b)$, est un morphisme d'algèbres si et seulement si $\mathrm{Im}(g)$ est inclus dans le commutant dans C de $\mathrm{Im}(f)$ (ce qui équivaut à dire que $\mathrm{Im}(f)$ est inclus dans le commutant dans C de $\mathrm{Im}(g)$). Dans notre situation, $h^{\langle\sigma\rangle}((T^n))$ est inclus dans le centre de $H((T, \sigma))$, ce qui montre que τ est bien un morphisme d'algèbres.

Pour l'injectivité de τ, considérons $h_1, \ldots, h_s \in H(T, \sigma)$ et $z_1, \ldots, z_s \in h^{\langle\sigma\rangle}((T^n))$ tels que $x = \sum_{m=1}^{s} h_m \otimes z_m$ vérifie $\tau(x) = 0$. Puisque $H[T, \sigma]$ est un anneau de Ore (voir lemme 2.1.13), en appliquant s fois la possible écriture $b^{-1}a = a'b'^{-1}$ $(a, b, a', b' \in H[T, \sigma])$, on déduit l'existence d'un polynôme $u \in H[T, \sigma] \setminus \{0\}$ tel que, pour tout $m \in [\![1, s]\!]$, on ait $h_m u \in H[T, \sigma]$. Comme $u \otimes 1$ est inversible et comme $\tau(x)\tau(u \otimes 1) = \tau(\sum_{m=1}^{s} h_m u \otimes z_m)$, pour montrer que $x = 0$, on peut supposer que les h_m sont dans $H[T, \sigma]$. Le même type de manipulation permet de supposer que les z_m sont dans $h^{\langle\sigma\rangle}[[T^n]]$.

Fixons une $h^{\langle\sigma\rangle}$-base $(e_j)_{j\in J}$ de H. En utilisant la centralité de $h^{\langle\sigma\rangle}(T^n)$, on peut écrire chacun des h_m sous la forme d'une somme finie

$$\begin{aligned}
h_m(T) &= \sum_{l=0}^{l_m} T^{ln} \sum_{k=0}^{n-1} a_{l,k,m} T^k \text{ avec } a_{l,k,m} \in H \\
&= \sum_{l=0}^{l_m} T^{ln} \sum_{k=0}^{n-1} \left(\sum_{j\in J_m} \lambda_{l,k,j,m} e_j \right) T^k \text{ avec } J_m \subset J \text{ un sous-ensemble fini choisi} \\
&\quad \text{uniformément pour } l \text{ et } k \text{ variant et } \lambda_{l,k,j,m} \in h^{\langle\sigma\rangle} \\
&= \sum_{k=0}^{n-1} \sum_{j\in J_m} e_j T^k P_{k,j,m}(T^n) \text{ avec } P_{k,j,m}(T^n) \in h^{\langle\sigma\rangle}[T^n].
\end{aligned}$$

On a alors

$$h_m \otimes z_m = \sum_{k=0}^{n-1} \sum_{j\in J_m} (e_j T^k P_{k,j,m}(T^n)) \otimes z_m = \sum_{k=0}^{n-1} \sum_{j\in J_m} (e_j T^k) \otimes (P_{k,j,m}(T^n) z_m)$$

et en sommant pour $m = 1, \dots, s$, on trouve finalement une partie $J_0 = \bigcup_m J_m \subset J$ finie et des séries

$$z_{k,j} = \sum_{m=1}^{s} P_{k,j,m}(T^n) z_m \in h^{\langle\sigma\rangle}[[T^n]]$$

(en ayant pris soin de poser $P_{k,j,m}(T^n) = 0$ si $j \notin J_m$) telles que

$$x = \sum_{m=1}^{s} h_m \otimes z_m = \sum_{k=0}^{n-1} \sum_{j \in J_0} (e_j T^k) \otimes z_{k,j}.$$

En posant formellement $z_{k,j} = \sum_{l \geq 0} \alpha_{k,j,l} T^{ln}$ (avec $\alpha_{k,j,l} \in h^{\langle\sigma\rangle}$) et en utilisant la centralité, on trouve alors

$$\tau(x) = \sum_{k=0}^{n-1} \sum_{j \in J_0} e_j T^k \sum_{l \geq 0} \alpha_{k,j,l} T^{ln} = \sum_{l \geq 0} \sum_{k=0}^{n-1} \left(\sum_{j \in J_0} \alpha_{k,j,l} e_j \right) T^{ln+k} = 0.$$

On en déduit que, pour tout $k \in [\![0, n-1]\!]$ et tout $l \geq 0$, on a $\sum_{j \in J_0} \alpha_{k,j,l} e_j = 0$. La famille $(e_j)_j$ étant une $h^{\langle\sigma\rangle}$-base de H, on a alors $\alpha_{k,j,l} = 0$ pour tous k, j, l. Ainsi, toutes les séries $z_{k,j}$ sont nulles et donc $x = 0$.

Pour le dernier point de la proposition, considérons $h^{\langle\sigma\rangle}(T^n) \subset L \subset h^{\langle\sigma\rangle}((T^n))$ tel que le corps L soit de dimension finie sur $h^{\langle\sigma\rangle}(T^n)$. Puisque l'anneau unitaire $H(T,\sigma) \otimes_{h^{\langle\sigma\rangle}(T^n)} L$ se plonge dans le corps $H((T,\sigma))$, il est donc intègre. En tant que $H(T,\sigma)$-espace vectoriel à gauche, $H(T,\sigma) \otimes_{h^{\langle\sigma\rangle}(T^n)} L$ est de dimension $[L : h^{\langle\sigma\rangle}(T^n)] < +\infty$. Le lemme 3.1.3 qui suit montre alors que $H(T,\sigma) \otimes_{h^{\langle\sigma\rangle}(T^n)} L$ est bien un corps. □

Lemme 3.1.3. *Si A désigne un anneau intègre contenant un corps K (non nécessairement commutatif) tel que A soit de dimension finie en tant que K-espace vectoriel à gauche (pour la multiplication à droite dans A), alors A est un corps.*

Démonstration. Fixons $x \in A \setminus \{0\}$ et notons $m_x : a \mapsto ax$ la multiplication à droite par x. L'application m_x est un K-endomorphisme de A, mais comme A est supposé intègre, cette application linéaire est injective. Rappelons que les théorèmes classiques (théorème du rang, etc.) d'algèbre linéaire sur les corps commutatifs restent valables sur les corps gauches (voir [Ehr11, §3.11] et [Ehr11, §3.12]). En application du théorème du rang et puisque A est supposé de dimension finie sur K, on en déduit que m_x est surjective. Ainsi, il existe $x^{-1} \in A$ tel que $m_x(x^{-1}) = x^{-1}x = 1$. Donc, tout $x \neq 0$ possède un inverse à gauche mais comme 1 est un neutre bilatère, finalement, tout $x \neq 0$ possède un inverse à droite. □

Maintenant, venons-en à la preuve du théorème 0.3.5 dont nous rappelons l'énoncé.

Théorème 0.3.5 *Soient H un corps de centre h (H non nécessairement de dimension finie sur h) et σ un automorphisme d'ordre fini de H. Si $h^{\langle\sigma\rangle}$ désigne le corps des invariants de k par σ, alors on a*

$$\mathrm{PIGS}_{h^{\langle\sigma\rangle}} \Longrightarrow \mathrm{PIG}_{H(T,\sigma)}.$$

En particulier, si $h^{\langle\sigma\rangle}$ contient un corps ample, alors le $\mathrm{PIG}_{H(T,\sigma)}$ admet une réponse positive.

Démonstration. Supposons que le $\mathrm{PIGS}_{h^{\langle\sigma\rangle}}$ admette une réponse positive. Soit G un groupe fini. En notant $n \geq 1$ l'ordre de σ, par hypothèse, il existe une extension galoisienne finie $L/h^{\langle\sigma\rangle}(T^n)$ de groupe G telle que $L \subset h^{\langle\sigma\rangle}((T^n))$. Par la proposition 3.1.2, l'algèbre $H(T,\sigma) \otimes_{h^{\langle\sigma\rangle}(T^n)} L$ reste

un corps. De plus, par le lemme 3.1.1, l'extension $(H(T,\sigma)\otimes_{h^{\langle\sigma\rangle}(T^n)} L)/H(T,\sigma)$ est galoisienne de groupe de Galois G. Par conséquent, le $\mathrm{PIG}_{H(T,\sigma)}$ admet une réponse positive. En particulier, si $h^{\langle\sigma\rangle}$ contient un corps ample, alors, comme rappelé dans l'introduction, le $\mathrm{PIGS}_{h^{\langle\sigma\rangle}}$ admet une réponse positive et il en est donc de même du $\mathrm{PIG}_{H(T,\sigma)}$. □

Remarque. Soient H un corps de centre h et σ un automorphisme d'ordre fini $n \geq 1$ de H. Soit G un groupe fini vérifiant l'un des quatre cas suivants :

1) G abélien et h infini,

2) $G = S_n$ $(n \geq 3)$ et h infini,

3) $G = A_n$ $(n \geq 4)$ et h est de caractéristique nulle,

4) G résoluble et h de caractéristique positive.

Par la preuve de [DL20, proposition 12], il existe $h_0 \subset h^{\langle\sigma\rangle}$ et une extension galoisienne $L/h_0(T^n)$ de groupe G et vérifiant $L \subset h_0((T^n))$. En conséquence, $Lh^{\langle\sigma\rangle}/h^{\langle\sigma\rangle}(T^n)$ est galoisienne de groupe de G vérifiant $Lh^{\langle\sigma\rangle} \subset h^{\langle\sigma\rangle}((T^n))$. Avec le même argument que dans la preuve du théorème 0.3.5, G est groupe de Galois sur $H(T,\sigma)$.

Exemples 3.1.4. Dans [DL20], les auteurs fournissent des exemples de corps gauches, de dimensions finies sur leurs centres et sur lesquels le PIG admet une réponse positive. Ils montrent que si H est un corps gauche contenant un corps ample dans son centre, alors le $\mathrm{PIG}_{H(T)}$ admet une réponse positive, où $H(T)$ est de dimension finie sur son centre. Notre théorème 0.3.5 est bien plus général comme le montre les exemples suivants.

a) En considérant la conjugaison complexe τ sur $\mathbb{C}$, le corps $\mathbb{C}(T,\tau)$ est bien une algèbre simple centrale de centre $\mathbb{R}(T^2)$, qui contient un corps ample. Le corps $\mathbb{C}(T,\tau)$ est bien de dimension finie sur son centre mais les résultats de [DL20] ne peuvent s'appliquer car l'indéterminée n'est pas centrale. Notre théorème 0.3.5 assure cependant une réponse positive au $\mathrm{PIG}_{\mathbb{C}(T,\tau)}$.

b) Lorsque k_0 est un corps ample à groupe de Brauer nul (par exemple lorsque k_0 est PAC [1]), les résultats de [DL20] sont sans intérêt puisqu'il n'existe pas d'algèbre simple centrale non triviale de centre k_0. Pour autant, notre théorème 0.3.5 s'applique non trivialement à des corps H de centre k_0 un corps ample à groupe de Brauer nul. Par exemple, si l'on prend $k_0 = \mathbb{C}((U))$, on a $\overline{k_0} = \mathrm{Puis}(\mathbb{C})$ et $\mathrm{Gal}(\overline{k_0}/k_0) \simeq \widehat{\mathbb{Z}}$. En considérant σ un générateur de $\widehat{\mathbb{Z}}$, on voit que $H = \overline{k_0}(Y,\sigma)$ est de centre k_0 et le théorème 0.3.5 assure que le PIG a une réponse positive sur $H(T)$.

3.2 Preuve du théorème 0.3.6

Dans leur article [DD04], les auteurs introduisent la notion galoisienne de ψ-liberté, dont la définition peut s'adapter au cas des corps gauches. Rappelons en quelques mots de quoi il s'agit. Un corps commutatif H est dit *ψ-libre* si, pour tout système projectif $(G_n, s_n)_{n\in\mathbb{N}}$ de groupes finis où $s_n : G_n \twoheadrightarrow G_{n-1}$ est un épimorphisme pour tout $n \geq 1$ (ce que Dèbes et Deschamps appellent dans leur article un système complet de groupes finis), il existe une tour d'extensions finies galoisiennes $(H_n/H)_{n\in\mathbb{N}}$ et une suite d'isomorphismes $(\epsilon_n : G_n \to \mathrm{Gal}(H_n/H))_{n\in\mathbb{N}}$ tels que, pour tout $n \in \mathbb{N}$, on ait

$$\epsilon_n \circ s_{n+1} = \mathrm{res}^{H_{n+1}/H}_{H_n/H} \circ \epsilon_{n+1},$$

où $\mathrm{res}^{H_{n+1}/H}_{H_n/H} : \mathrm{Gal}(H_{n+1}/H) \to \mathrm{Gal}(H_n/H)$ désigne l'épimorphisme de restriction.

1. On dit qu'un corps K est PAC (Pseudo Algébriquement Clos) si toute variété non vide définie sur K admet au moins un point K-rationnel. Par exemple, le corps $\mathbb{Q}^{\mathrm{tr}}(i)$ est PAC où $\mathbb{Q}^{\mathrm{tr}}$ désigne la clôture totalement réelle de $\mathbb{Q}$. Voir [FJ08] pour plus de détails.

Dans ce cas, on dit que la tour $(H_n/H)_{n\in\mathbb{N}}$ *réalise* le système complet $(G_n, s_n)_{n\in\mathbb{N}}$. Cette définition n'est pas directement applicable dans le cas où H est un corps gauche. En effet (voir §2.3 ou [Coh95, Chapter 3]), si l'on dispose d'une tour d'extensions galoisiennes finies $M/L/H$, la traditionnelle suite exacte

$$1 \to \mathrm{Gal}(M/L) \to \mathrm{Gal}(M/H) \to \mathrm{Gal}(L/H) \to 1,$$

valable dans le cas commutatif, doit être remplacée par la suite

$$1 \to \mathrm{Gal}(M/L) \to \mathscr{N}_{\mathrm{Gal}(M/H)}(\mathrm{Gal}(M/L)) \to \mathrm{Gal}(L/H) \to 1,$$

où $\mathscr{N}_{\mathrm{Gal}(M/H)}(\mathrm{Gal}(M/L))$ désigne le normalisateur de $\mathrm{Gal}(M/L)$ dans $\mathrm{Gal}(M/H)$ (dans cette situation, on sait alors que $\mathrm{Gal}(M/H)$ est le plus petit N-sous-groupe (voir §2.3) contenant le normalisateur). Ainsi, l'application $\mathrm{res}^{M/H}_{L/H}$ n'est pas nécessairement définie. Une manière de pallier à ce problème consiste à considérer des extensions *extérieures*. En effet, dans cette situation, les éléments x de M tels que l'automorphisme intérieur $I(x) : m \in M \mapsto xmx^{-1} \in M$ appartienne au groupe $\mathscr{N}_{\mathrm{Gal}(M/H)}(\mathrm{Gal}(M/L))$ sont exactement les éléments du centre $Z(M)$ de M. Puisque $Z(M)$ est un corps, le groupe $\mathscr{N}_{\mathrm{Gal}(M/H)}(\mathrm{Gal}(M/L))$ est donc un N-groupe et l'on a donc $\mathscr{N}_{\mathrm{Gal}(M/H)}(\mathrm{Gal}(M/L)) = \mathrm{Gal}(M/H)$. On peut donc définir la ψ-liberté d'un corps gauche de la même manière que dans le cas commutatif, mais en demandant que chaque extension H_n/H soit extérieure. Un autre intérêt à ne considérer que des extensions extérieures est que, dans cette situation, la théorie de Krull des extensions galoisiennes infinies reste valide dans le cas relativement algébrique, comme mentionné dans l'introduction (voir aussi §2.3). Pour ces raisons, nous étendons la définition de ψ-liberté comme suit :

Définition 3.2.1. Un corps H est dit *ψ-libre* si, pour tout système complet de groupes finis $(G_n, s_n)_{n\in\mathbb{N}}$, il existe une tour d'extensions $(H_n/H)_{n\in\mathbb{N}}$ telle que :

a) $\Omega = \bigcup_n H_n/H$ est une extension galoisienne extérieure et relativement algébrique à gauche,

b) pour tout $n \in \mathbb{N}$, H_n/H est galoisienne (nécessairement extérieure) de groupe G_n et il existe $\epsilon_n : G_n \simeq \mathrm{Gal}(H_n/H)$ vérifiant

$$\epsilon_n \circ s_{n+1} = \mathrm{res}^{H_{n+1}/H}_{H_n/H} \circ \epsilon_{n+1}$$

pour tout $n \in \mathbb{N}$, où $\mathrm{res}^{H_{n+1}/H}_{H_n/H} : \mathrm{Gal}(H_{n+1}/H) \to \mathrm{Gal}(H_n/H)$ désigne l'épimorphisme de restriction.

Eu égard aux propriétés de la théorie de Galois infinie des corps quelconques, la preuve présentée dans [DD04, proposition 1.2] montre immédiatement que la ψ-liberté d'un corps gauche équivaut juste à l'existence d'une extension relativement algébrique galoisienne extérieure de groupe de Galois le groupe prolibre de rang dénombrable $\widehat{F}_\omega$ (c'est-à-dire à la réalisation d'un système complet de groupes finis particulier qui définit ce groupe).

Proposition 3.2.2. *Soient H un corps, k un corps contenu dans le centre de H et $(L_n/k)_{n\in\mathbb{N}}$ une tour d'extensions galoisiennes qui réalise un système complet de groupes finis $(G_n, s_n)_{n\in\mathbb{N}}$. Supposons que $M_n = H \otimes_k L_n$ reste un corps pour tout $n \in \mathbb{N}$. Alors :*

1) *pour tout $n \in \mathbb{N}$, l'extension M_n/H est galoisienne extérieure relativement algébrique à gauche de groupe G_n,*
2) *si l'on pose $L = \bigcup_{n\in\mathbb{N}} L_n$, alors $M = L \otimes_k H = \bigcup_{n\in\mathbb{N}} M_n$ est un corps qui est une extension galoisienne extérieure relativement algébrique à gauche de H,*
3) *la tour d'extensions galoisiennes $(M_n/H)_{n\in\mathbb{N}}$ réalise le système $(G_n, s_n)_{n\in\mathbb{N}}$ de sorte que*

$$\mathrm{Gal}(M/H) \simeq \varprojlim_n G_n.$$

Démonstration. 1) Soit $n \in \mathbb{N}$. Comme M_n est un corps, l'extension M_n/H est galoisienne de groupe de Galois G_n. En remarquant $[M_n : H] = \mathrm{Gal}(M_n/H)$, on déduit de [Des18, Théorème], que M_n/H est extérieure. Le fait que M_n/H soit relativement algébrique est clair.

2) La suite $(M_n)_{n\in\mathbb{N}}$ filtre M, donc M est un corps. D'une part, l'extension M/H est galoisienne car L/k l'est. D'autre part, M/H est extérieure car tout $x \in M$ est dans un certain M_n. De plus, l'extension M/H est relativement algébrique en étant filtrée par les extensions relativement algébriques M_n/H $(n \in \mathbb{N})$.

3) Par hypothèse, il existe une suite d'isomorphismes $(\epsilon_n : G_n \to \mathrm{Gal}(L_n/k))_{n\in\mathbb{N}}$ telle que pour tout $n \in \mathbb{N}$, on a

$$\epsilon_n \circ s_{n+1} = \mathrm{res}^{L_{n+1}/k}_{L_n/k} \circ \epsilon_{n+1}, \tag{3.2.1}$$

où $\mathrm{res}^{L_{n+1}/k}_{L_n/k}$ désigne le morphisme de restriction. Pour tout $n \in \mathbb{N}$, en considérant l'isomorphisme $\Psi_n : \mathrm{Gal}(L_n/k) \to \mathrm{Gal}(M_n/H)$ défini dans (3.1.1), on vérifie que l'on a

$$\Psi_n \circ \mathrm{res}^{L_{n+1}/k}_{L_n/k} = \mathrm{res}^{M_{n+1}/H}_{M_n/H} \circ \Psi_{n+1} \tag{3.2.2}$$

pour tout $n \in \mathbb{N}$. Pour tout $n \in \mathbb{N}$, on pose $\tilde{\epsilon}_n = \Psi_n \circ \epsilon_n$. Alors, on a

$$\begin{aligned}\tilde{\epsilon}_n \circ s_{n+1} = \Psi_n \circ (\epsilon_n \circ s_{n+1}) = \left(\Psi_n \circ \mathrm{res}^{L_{n+1}/k}_{L_n/k}\right) \circ \epsilon_{n+1} &= \mathrm{res}^{M_{n+1}/H}_{M_n/H} \circ (\Psi_{n+1} \circ \epsilon_{n+1}) \\ &= \mathrm{res}^{M_{n+1}/H}_{M_n/H} \circ \tilde{\epsilon}_{n+1}\end{aligned}$$

pour tout $n \in \mathbb{N}$. La deuxième (resp. troisième) égalité vient de l'égalité (3.2.1) (resp. (3.2.2)). Il reste à montrer l'isomophisme. Pour tout $n \in \mathbb{N}$, on a $\mathrm{res}^{M/H}_{M_{n+1}/H} \circ \mathrm{res}^{M_{n+1}/H}_{M_n/H} = \mathrm{res}^{M/H}_{M_n/H}$, donc on déduit un morphisme $\Phi : \mathrm{Gal}(M/H) \to \varprojlim_n \mathrm{Gal}(M_n/H)$, qui est un isomorphisme car $(M_n/H)_{n\in\mathbb{N}}$ filtre M/H. □

Etant donnés un corps commutatif ψ-libre k et un corps H contenant k dans son centre, on voit que si pour tout système complet de groupes finis (G_n, s_n), on sait trouver une tour (L_n/k) réalisant ce système et telle que $H \otimes_k L_n$ reste un corps pour tout n, alors H sera ψ-libre. C'est cette idée que nous allons utiliser pour montrer le théorème 0.3.6. Nous exploitons à cet effet la construction présentée dans [DD04] pour montrer le résultat suivant :

Proposition 3.2.3. *Soit k un corps commutatif contenant un corps k_0 qui est, soit réel clos, soit hensélien de caractéristique résiduelle nulle et contenant μ_∞. Alors, pour tout système complet de groupes finis $(G_n, s_n)_{n\in\mathbb{N}}$, il existe une tour d'extensions galoisiennes $(L_n/k(T))_{n\in\mathbb{N}}$ qui réalise $(G_n, s_n)_{n\in\mathbb{N}}$ telle que $L_n \subset k((T))$ pour tout $n \in \mathbb{N}$.*

Démonstration. Pour la terminologie sur l'extension de corps de fonctions : régularité, spécialisation, etc, on renvoie au §1.1.1. Pour la proposition, il suffit de montrer le résultat lorsque $k = k_0$. En effet, supposons qu'il existe une tour $(F_n/k_0(T))_n$ qui réalise $(G_n, s_n)_{n\in\mathbb{N}}$ telle que $F_n \subset k_0((T))$ pour tout $n \in \mathbb{N}$. Pour tout $n \in \mathbb{N}$, on pose $L_n = F_n k$. On obtient que la tour $(L_n/k(T))_{n\in\mathbb{N}}$ réalise aussi $(G_n, s_n)_{n\in\mathbb{N}}$ et que l'on a $L_n \subset k((T))$ pour tout $n \in \mathbb{N}$.

Nous remarquons que, quitte à faire le changement de variables $T \mapsto 1/T$, il suffit de trouver une tour $(L_n/k(T))_{n\in\mathbb{N}}$ telle que $L_n \subset k((1/T))$ pour tout $n \in \mathbb{N}$. Pour la preuve, nous allons distinguer selon que le corps k est réel clos ou valué hensélien.

-<u>1er cas</u> : Le corps k est réel clos.

Si $k = \mathbb{R}$, alors cela résulte de [DD04, remarque 2.2]. Dans le cas général, voir la preuve de [DD04, théorème 2.3].

-2ème cas : Le corps k est valué hensélien.

Notons v la valuation sur k et (k_v, v) le complété de (k, v). Par les constructions de [DD04, Partie 3.1], il existe une suite croissante de parties finies non vides $(U_n)_{n\in\mathbb{N}}$ de k et une tour d'extensions galoisiennes $(\tilde{L}_n/k_v(T))_{n\in\mathbb{N}}$ de points de branchement U_n telles que $(\widetilde{L}_n/k_v(T))_{n\in\mathbb{N}}$ réalise régulièrement (c'est-à-dire $\widetilde{L}_n \cap \overline{k_v} = k_v$) le système $(G_n, s_n)_{n\in\mathbb{N}}$ et que pour tout $n \in \mathbb{N}$, la spécialisation $(\widetilde{L}_n)_\infty$ de $\widetilde{L}_n/k_v(T)$ en ∞ est égale à k_v. La preuve du [DD04, Théorème 3.4] montre que la tour $(\widetilde{L}_n/k_v(T))_{n\in\mathbb{N}}$ admet un modèle $(L_n/k(T))_{n\in\mathbb{N}}$ (c'est-à-dire $\widetilde{L}_n = L_n k_v$) qui réalise régulièrement le système complet $(G_n, s_n)_{n\in\mathbb{N}}$. Pour tout $n \in \mathbb{N}$, puisque ∞ n'est pas un point de branchement de $\widetilde{L}_n/k_v(T)$, le point ∞ n'est pas non plus un point de branchement de $L_n/k(T)$. Vu que (k, v) est hensélien pour une valuation de rang 1, on a $k_v \cap \overline{k} = k$. Or la spécialisation $(L_n)_\infty$ de L_n en ∞ est incluse à la fois dans $\overline{k}$ et dans la spécialisation $(\widetilde{L}_n)_\infty$ de $\widetilde{L}_n$ en ∞, donc $(L_n)_\infty = k$. □

Nous avons maintenant les outils nécessaires pour établir la ψ-liberté de certains corps des fractions rationnelles tordus :

Théorème 3.2.4. *Soient H un corps de centre h et σ un automorphisme d'ordre fini de H. Supposons que $h^{\langle\sigma\rangle}$ contienne un corps h_0 qui est, soit réel clos, soit hensélien de caractéristique résiduelle nulle et contenant le groupe des racines de l'unité μ_∞. Alors, le corps $H(T, \sigma)$ est ψ-libre au sens de la définition 3.2.1.*

Démonstration. Considérons un système complet de groupes finis $(G_n, s_n)_{n\in\mathbb{N}}$. Par la proposition 3.2.3, il existe une réalisation $(L_n/h^{\langle\sigma\rangle}(T^n))_{n\in\mathbb{N}}$ du sytème complet $(G_n, s_n)_{n\in\mathbb{N}}$ telle que $L_n \subset h^{\langle\sigma\rangle}((T^n))$ pour tout $n \in \mathbb{N}$. Par la proposition 3.1.2, l'algèbre $M_n = H(T, \sigma) \otimes_{h^{\langle\sigma\rangle}(T^n)} L_n$ reste un corps pour tout $n \in \mathbb{N}$. La proposition 3.2.2 montre que $M/H = (\bigcup_n M_n)/H$ est galoisienne extérieure, relativement algébrique à gauche et que la tour $(M_n/H(T, \sigma))_{n\in\mathbb{N}}$ est galoisienne finie, relativement algébrique à gauche réalisant $(G_n, s_n)_{n\in\mathbb{N}}$. Donc, $H(T, \sigma)$ est ψ-libre. □

Comme remarqué précédemment, on voit que le théorème 3.2.4 est équivalent au théorème 0.3.6' suivant :

Théorème 0.3.6'. *Soient H un corps de centre h et σ un automorphisme d'ordre fini de H. Supposons que le corps des invariants $h^{\langle\sigma\rangle}$ contienne un corps h_0 qui est, soit réel clos, soit hensélien de caractéristique résiduelle nulle et contenant toutes les racines de l'unité. Alors, il existe une extension $L/H(T, \sigma)$ galoisienne extérieure, relativement algébrique et de groupe $\widehat{F}_\omega$.*

Nous précisons que le théorème 0.3.6 est exactement le théorème 0.3.6' sans les conclusions "extérieure" et "relativement algébrique".

Exemple 3.2.5. Dans le théorème 0.3.6', en prenant $H = \mathbb{H}_\mathbb{R}$ le corps des quaternions réels (de centre $\mathbb{R}$) et $\sigma = \mathrm{id}$, on obtient que le groupe $\widehat{F}_\omega$ est groupe de Galois sur $\mathbb{H}_\mathbb{R}(T)$. De même, le groupe $\widehat{F}_\omega$ est groupe de Galois sur $L(T, \sigma)$, où $L/\mathbb{C}((U))$ est une extension finie non triviale et $\sigma \in \mathrm{Gal}(L/\mathbb{C}((U)))$.

Remarque 3.2.6. Dans certaines situations, les corps des fractions rationnelles tordus avec dérivation $H(T, \sigma, \delta)$ peuvent se ramener au cas où $\delta = 0$, ce qui permet d'appliquer les résultats de ce chapitre. En effet, il est par exemple montré dans [Coh95, Theorem 2.3.1] que si $\delta \neq 0$ et $h^{\langle\sigma\rangle} \neq h$, alors les corps $H(T, \sigma, \delta)$ et $H(T, \sigma)$ sont isomorphes. Nous n'avons pas inclus ces cas dans les théorèmes 0.3.5 et 0.3.6 pour ne pas en alourdir artificiellement les énoncés.

Chapitre 4

Problèmes de plongement finis sur les corps gauches

Dans ce chapitre, nous étendons la notion de problème de plongement fini sur les corps commutatifs, une notion centrale de la théorie inverse de Galois, à la situation d'un corps quelconque H de dimension finie sur son centre h. Nous montrons tout d'abord que résoudre un problème de plongement fini sur H équivaut à trouver une solution à un certain problème de plongement fini sur h vérifiant une contrainte polynomiale. Nous montrons ensuite que tout problème de plongement fini scindé constant sur le corps $H(T)$ des fractions rationnelles à indéterminée centrale T admet une solution, si h est un corps ample. Il s'agit d'un analogue non commutatif d'un résultat profond de Pop. Plus généralement, nous résolvons de tels problèmes de plongement finis sur les corps $H(T,\sigma)$ des fractions rationnelles tordus, où σ est un automorphisme de H d'ordre fini. Nos résultats généralisent de précédents travaux sur le problème inverse de Galois sur les corps quelconques.

Ce chapitre est basé sur l'article [BDL20] et est constitué de quatres parties. D'abord, dans la section 4.1, nous présentons les préliminaires. Ensuite, dans la section 4.2, nous étendons la terminologie des problèmes de plongement finis valable pour les corps commutatifs aux corps de dimension finies sur leurs centres. Après, dans la section 4.3. nous résolvons certains problèmes de plongement finis scindés. Enfin, dans la section 4.4, nous généralisons aux corps gauches la réduction faible→scindé.

4.1 Préliminaires

Dans ce chapitre, si $H \subset L$ sont deux corps quelconques, alors nous considérerons toujours L comme espace vectoriel sur H à gauche.

4.1.1 Extensions galoisiennes de corps quelconques

Lemme 4.1.1. *Soit L/H une extension extérieure.*
1) *Si H est commutatif, alors L l'est aussi.*
2) *Pour tout corps intermédiaire $H \subseteq F \subseteq L$, l'extension L/F est extérieure.*

Preuve. 1) Supposons H commutatif. Comme L/H est extérieure, H est contenu dans le centre de L et tout automorphisme intérieur de L est donc dans $\mathrm{Aut}(L/H)$. Comme L/H est extérieure, id_L est donc le seul automorphisme intérieur de L, i.e. L est commutatif.
2) Si $I_L(y)$ $(y \in L^*)$ fixe F point par point, alors $I_L(y)$ fixe H point par point. Comme L/H est extérieure, cela entraîne $I_L(y) = \mathrm{id}_L$. Ainsi L/F est extérieure. □

Soient H un corps et k un sous-corps du centre de H. Soit ℓ/k une extension galoisienne de corps commutatifs à groupe de Galois fini. Supposons que $M = H \otimes_k \ell$ soit un corps. Alors, par le lemme 3.1.1, l'extension M/H est galoisienne (on identifie H et $H \otimes_k k$) et, pour tout $x \in \ell$ et tout $\sigma \in \mathrm{Gal}(M/H)$, on a $\sigma(1 \otimes x) = 1 \otimes \widetilde{x}$ pour un unique $\widetilde{x} \in \ell$. De plus, $\widetilde{\sigma} : x \mapsto \widetilde{x}$ est un élément de $\mathrm{Gal}(\ell/k)$ et l'application suivante est en fait un isomorphisme :

$$\widetilde{\mathrm{res}}_{\ell/k}^{M/H} : \left\{ \begin{array}{ccc} \mathrm{Gal}(M/H) & \longrightarrow & \mathrm{Gal}(\ell/k) \\ \sigma & \longmapsto & \widetilde{\sigma} \end{array} \right. . \tag{4.1.1}$$

Le théorème suivant, qui repose sur [DL20, théorème 7] et sa preuve, décrit les extensions galoisiennes à groupe de Galois fini d'un corps de dimension finie sur son centre :

Théorème 4.1.2. *Soit H un corps de dimension finie sur son centre h.*
1) *Soit L/H une extension galoisienne à groupe de Galois fini. On a :*
   a) *le centre ℓ de L est une extension finie galoisienne de h,*
   b) *$\mathcal{F}_H$ (voir §2.2) ne possède que le zéro trivial sur ℓ,*
   c) *$L = H \otimes_h \ell$,*
   d) *l'application $\widetilde{\mathrm{res}}_{\ell/h}^{L/H}$ (voir (4.1.1)) est un isomorphisme,*
   e) *L/H est extérieure.*
2) *Réciproquement, soit ℓ un corps commutatif qui est une extension galoisienne de h à groupe de Galois fini et sur lequel $\mathcal{F}_H$ ne possède que le zéro trivial. On a :*
   a) *$H \otimes_h \ell$ est un corps de centre ℓ,*
   b) *l'extension $(H \otimes_h \ell)/H$ est galoisienne,*
   c) *l'application $\widetilde{\mathrm{res}}_{\ell/h}^{(H\otimes_h \ell)/H}$ est un isomorphisme.*

4.1.2 Résultats sur les corps de fractions rationnelles tordus

Pour la terminologie sur les anneaux et corps tordus, on peut voir le §2.1.3.

Lemme 4.1.3. *Soient H un corps et σ un automorphisme de H d'ordre fini m. Notons $\widetilde{\sigma}$ la restriction de σ au centre h de H.*
1) *Si H est de dimension finie sur h, alors $H(T, \sigma)$ est de dimension finie sur son centre.*
2) *Supposons que l'ordre intérieur de σ soit égal à m. Alors le centre de $H(T, \sigma)$ vaut $h^{\langle\widetilde{\sigma}\rangle}(T^m)$.*

Preuve. 1) Comme le centre de $H(T, \sigma)$ contient $h^{\langle\widetilde{\sigma}\rangle}(T^m)$, il suffit de montrer que $H(T, \sigma)$ est de dimension finie sur $h^{\langle\widetilde{\sigma}\rangle}(T^m)$. Pour cela, notons que, comme H est de dimension finie sur h et σ est d'ordre fini, la dimension de H sur $h^{\langle\widetilde{\sigma}\rangle}$ est finie. Soit $e_1, \ldots, e_r$ une $h^{\langle\widetilde{\sigma}\rangle}$-base de H et soit Γ l'espace vectoriel engendré sur $h^{\langle\widetilde{\sigma}\rangle}(T^m)$ par tous les éléments de la forme $e_i T^j$ avec $i \in [\![1, r]\!]$ et $j \in [\![0, m-1]\!]$. On a alors $H[T, \sigma] \subseteq \Gamma \subseteq H(T, \sigma)$. De plus, Γ est un anneau et est de dimension finie sur $h^{\langle\widetilde{\sigma}\rangle}(T^m)$. Ainsi Γ est un corps. Comme tout élément de $H(T, \sigma)$ s'écrit sous la forme $P(T)Q(T)^{-1}$ avec $P(T), Q(T) \in H[T, \sigma]$, on obtient $H(T, \sigma) = \Gamma$.
2) Soit $x = \sum_{n \geq n_0} a_n T^n$ un élément du centre de $H(T, \sigma)$ avec $a_{n_0} \neq 0$. Par le *critère de rationalité* (voir proposition 2.1.4), on peut trouver deux entiers $s \geq 1$ et $n_1 \geq 0$ et des éléments $y_1, \ldots, y_s$ de H tels que

$$a_n = a_{n-1}\sigma^{n-1}(y_1) + a_{n-2}\sigma^{n-2}(y_2) + \cdots + a_{n-s}\sigma^{n-s}(y_s) \tag{4.1.2}$$

pour tout $n \geq n_1$. Puisque x est dans le centre de $H(T, \sigma)$, on a $Tx = xT$, c'est-à-dire

$$\sum_{n \geq n_0} \sigma(a_n) T^{n+1} = \sum_{n \geq n_0} a_n T^{n+1}.$$

Cela entraîne $\sigma(a_n) = a_n$, c'est-à-dire $a_n \in H^{\langle\sigma\rangle}$ pour tout n. On a donc $x \in H^{\langle\sigma\rangle}((T))$. De plus, pour tout $a \in H$, on a $ax = xa$, c'est-à-dire

$$\sum_{n\geq n_0} aa_nT^n = \sum_{n\geq n_0} a_n\sigma^n(a)T^n,$$

Pour $n \geq n_0$ tel que $a_n \neq 0$, on a donc $\sigma^n(a) = a_n^{-1}aa_n$, i.e. σ^n est intérieur. Pour un tel n, l'hypothèse sur l'ordre intérieur entraîne alors que m divise n. On a donc $aa_n = a_na$ pour $a \in H$ et n tel que $a_n \neq 0$, i.e. $x \in h^{\langle\widetilde{\sigma}\rangle}((T^m))$. Soit u le quotient de la division euclidienne de s par m. Par (4.1.2), pour $l \in \mathbb{N}$ tel que $ml \geq n_1$, on obtient

$$a_{ml} = a_{m(l-1)}y_m + a_{m(l-2)}y_{2m} + \cdots + a_{m(l-u)}y_{mu}.$$

Ainsi, par le critère de rationalité, $x \in H(T^m)$. Comme x est dans le centre de $H(T,\sigma)$, on obtient en fait que x est dans le centre de $H(T^m)$, c'est-à-dire dans $h(T^m)$ (voir, par exemple, [Coh95, Proposition 2.1.5]). Ainsi $x \in h^{\langle\widetilde{\sigma}\rangle}((T^m)) \cap h(T^m)$. Comme $h^{\langle\widetilde{\sigma}\rangle}((T^m)) \cap h = h^{\langle\widetilde{\sigma}\rangle}$ et $h/h^{\langle\widetilde{\sigma}\rangle}$ est galoisienne finie, $h^{\langle\widetilde{\sigma}\rangle}((T^m))$ et h sont linéairement disjoints sur $h^{\langle\widetilde{\sigma}\rangle}$. Ainsi $h(T^m)$ et $h^{\langle\widetilde{\sigma}\rangle}((T^m))$ sont linéairement disjoints sur $h^{\langle\widetilde{\sigma}\rangle}(T^m)$ (voir [FJ08, Lemma 2.5.3]), i.e. $h(T^m) \cap h^{\langle\widetilde{\sigma}\rangle}((T^m)) = h^{\langle\widetilde{\sigma}\rangle}(T^m)$. On a donc $x \in h^{\langle\widetilde{\sigma}\rangle}(T^m)$. □

4.1.3 Extensions de corps de fractions rationnelles tordus

On s'intéresse enfin aux extensions de corps de la forme $L(T,\tau)/H(T,\sigma)$. Commençons par le lemme élémentaire suivant :

Lemme 4.1.4. *Soient L/H une extension de corps, $\sigma \in \mathrm{Aut}(H)$ et τ un automorphisme de L d'ordre fini prolongeant σ.*

1) *Les conditions suivantes sont équivalentes :*
   i) $\langle\tau, \mathrm{Aut}(L/H)\rangle = \mathrm{Aut}(L/H) \rtimes \langle\tau\rangle$,
   ii) $\mathrm{Aut}(L/H) \cap \langle\tau\rangle = \{\mathrm{id}_L\}$,
   iii) *l'ordre de τ vaut l'ordre de σ.*

2) *Supposons les trois conditions suivantes vérifiées :*
   a) *L est commutatif,*
   b) *L/H est galoisienne,*
   c) *l'ordre de τ vaut l'ordre de σ.*

Alors $L^{\langle\tau\rangle}$ et H sont linéairement disjoints sur $H^{\langle\sigma\rangle}$ et $L = L^{\langle\tau\rangle}H$.

Preuve. 1) Comme $\tau(H) = \sigma(H) = H$, on a $\mathrm{Aut}(L/H) \trianglelefteq \langle\tau, \mathrm{Aut}(L/H)\rangle$ et on a donc $\langle\tau, \mathrm{Aut}(L/H)\rangle = \mathrm{Aut}(L/H)\langle\tau\rangle$. Ainsi i) $\Leftrightarrow$ ii) est vraie. De plus, on a $\mathrm{Aut}(L/H) \cap \langle\tau\rangle = \langle\tau^m\rangle$, où m est l'ordre de σ. Par conséquent, ii) $\Leftrightarrow$ iii) est aussi vraie.
2) Par a) et c), on a $[L^{\langle\tau\rangle} : H^{\langle\sigma\rangle}] = [L : H]$. De plus, $L^{\langle\tau\rangle}H = L^{\langle\tau\rangle}L^{\mathrm{Gal}(L/H)} = L^{\langle\tau\rangle\cap\mathrm{Gal}(L/H)} = L$ par b), c) et 1). Ainsi $[L^{\langle\tau\rangle} : H^{\langle\sigma\rangle}] = [L^{\langle\tau\rangle}H : H]$, ce qui achève la preuve. □

La proposition suivante sera utilisée pour définir des applications de restriction :

Proposition 4.1.5. *Soient H un corps de dimension finie sur son centre h et $\sigma \in \mathrm{Aut}(H)$. Notons $\widetilde{\sigma}$ la restriction de σ à h. Soient L/H une extension galoisienne à groupe de Galois fini et τ un automorphisme de L d'ordre fini étendant σ. Soient ℓ le centre de L et $\widetilde{\tau}$ la restriction de τ à ℓ. Supposons la condition suivante vérifiée :*
$(*)$ *l'ordre de $\widetilde{\tau}$ vaut l'ordre de $\widetilde{\sigma}$.*
Alors $L(T,\tau) \cong H(T,\sigma) \otimes_{h^{\langle\widetilde{\sigma}\rangle}(T^m)} \ell^{\langle\widetilde{\tau}\rangle}(T^m)$, où m est l'ordre de τ.

Preuve. Notons tout d'abord que, par le théorème 4.1.2, ℓ est une extension galoisienne de h. De plus, puisque τ étend σ, on a $h^{\langle\widetilde{\sigma}\rangle} \subseteq \ell^{\langle\widetilde{\tau}\rangle}$. Ainsi $H(T,\sigma) \otimes_{h^{\langle\widetilde{\sigma}\rangle}(T^m)} \ell^{\langle\widetilde{\tau}\rangle}(T^m)$ est bien défini.

Considérons maintenant l'application $h^{\langle\widetilde{\sigma}\rangle}(T^m)$-linéaire

$$\psi : \left\{ \begin{array}{ccc} H(T,\sigma) \otimes_{h^{\langle\widetilde{\sigma}\rangle}(T^m)} \ell^{\langle\widetilde{\tau}\rangle}(T^m) & \longrightarrow & L(T,\tau) \\ y \otimes z & \longmapsto & yz \end{array} \right. .$$

Puisque $\ell^{\langle\widetilde{\tau}\rangle}(T^m)$ est contenu dans le centre de $L(T,\tau)$, ψ est un morphisme d'algèbres. De plus, $\mathrm{Im}(\psi)$ contient $H(T,\sigma)$ et est de dimension finie sur ce corps. Ainsi $\mathrm{Im}(\psi)$ est un corps.

Nous montrons ensuite que ψ est surjective. Pour cela, notons que, par $(*)$ et le lemme 4.1.4, $\ell^{\langle\widetilde{\tau}\rangle}$ et h sont linéairement disjoints sur $h^{\langle\widetilde{\sigma}\rangle}$ et $\ell^{\langle\widetilde{\tau}\rangle}h = \ell$. Par conséquent, si $f_1, \dots, f_r$ est une $h^{\langle\widetilde{\sigma}\rangle}$-base de $\ell^{\langle\widetilde{\tau}\rangle}$, alors $f_1, \dots, f_r$ est une h-base de ℓ. Puisque $L = H \otimes_h \ell$ (voir théorème 4.1.2), on en déduit que $f_1, \dots, f_r$ (que l'on identifie à $1 \otimes f_1, \dots, 1 \otimes f_r$) est une H-base de L.

Maintenant, soit $x = \sum_i a_i T^i \in L[t,\tau]$ ($(a_i)_i \subset L$). Pour tout i, il existe $(a_{i,k})_{k=1}^r \subset H$ tel que $a_i = \sum_{k=1}^r a_{i,k} f_k$. Ainsi

$$x = \sum_i \left(\sum_{k=1}^r a_{i,k} f_k \right) T^i = \sum_i \sum_k \left((a_{i,k} T^i) f_k \right) = \psi \left(\sum_i \sum_k \left((a_{i,k} T^i) \otimes f_k \right) \right).$$

Ainsi $L[T,\tau] \subseteq \mathrm{Im}(\psi)$. Comme $\mathrm{Im}(\psi)$ est un corps et tout élément de $L(T,\tau)$ s'écrit sous la forme $P(T)Q(T)^{-1}$ avec $P(T), Q(T) \in L[T,\tau]$, on en déduit $L(T,\tau) = \mathrm{Im}(\psi)$.

Montrons enfin que ψ est injective. Pour cela, notons que, puisque H est de dimension finie sur h et σ est d'ordre fini, la dimension de H sur $h^{\langle\widetilde{\sigma}\rangle}$ est finie. Considérons une $h^{\langle\widetilde{\sigma}\rangle}$-base $(e_l)_l$ de H. Soit $x = \sum_i x_i \otimes y_i \in H(T,\sigma) \otimes_{h^{\langle\widetilde{\sigma}\rangle}(T^m)} \ell^{\langle\widetilde{\tau}\rangle}(T^m)$ ($(x_i)_i \subset H(T,\sigma)$ et $(y_i)_i \subset \ell^{\langle\widetilde{\tau}\rangle}(T^m)$) tel que $\psi(x) = 0$. Comme $\psi(x) = 0$ et $H[T,\sigma]$ est un anneau de Ore, par itération de la propriété de Ore, on peut supposer $(x_i)_i \subset H[T,\sigma]$ et $(y_i)_i \subset \ell^{\langle\widetilde{\tau}\rangle}[T^m]$. On peut alors écrire

$$x = \sum_l \sum_{j=0}^{m-1} \lambda_{l,j} (e_l T^j \otimes v_{l,j}), \tag{4.1.3}$$

où $(\lambda_{l,j})_{l,j} \subset h^{\langle\widetilde{\sigma}\rangle}$ et $(v_{l,j})_{l,j} \subset \ell^{\langle\widetilde{\tau}\rangle}[T^m] \setminus \{0\}$. Pour tout (l,j), on pose $v_{l,j} = \sum_a b_{l,j,a} T^{ma}$, avec $(b_{l,j,a})_{l,j,a} \subset \ell^{\langle\widetilde{\tau}\rangle}$ et, pour tout (l,j,a), on a $b_{l,j,a} = \sum_k c_{l,j,a,k} f_k$ avec $(c_{l,j,a,k})_{l,j,a,k} \subset h^{\langle\widetilde{\sigma}\rangle}$. Ainsi

$$\psi(x) = \sum_{(j,a)} \left(\sum_k \left(\sum_l (\lambda_{l,j} c_{l,j,a,k})\, e_l \right) f_k \right) T^{ma+j}.$$

L'égalité précédente montre alors que, pour tout (j,a,k,l), on a

$$\lambda_{l,j} c_{l,j,a,k} = 0. \tag{4.1.4}$$

Fixons maintenant (l,j). Comme $v_{l,j} \neq 0$, il existe (a,k) tel que $c_{l,j,a,k} \neq 0$. Ainsi, en utilisant (4.1.4), on obtient $\lambda_{l,j} = 0$. Par (4.1.3), on en déduit $x = 0$. □

Remarque 4.1.6. 1) La condition $(*)$ entraîne que les ordres de σ et τ sont égaux. En effet, par le lemme 4.1.4, il suffit de montrer $\mathrm{Gal}(L/H) \cap \langle\tau\rangle = \{\mathrm{id}_L\}$. Soit donc $j \geq 1$ tel que $\tau^j \in \mathrm{Gal}(L/H)$. En particulier, on a $\widetilde{\tau}^j \in \mathrm{Gal}(\ell/h)$. Si l'on suppose $(*)$, alors, par le lemme 4.1.4, on a $\mathrm{Gal}(\ell/h) \cap \langle\widetilde{\tau}\rangle = \{\mathrm{id}_\ell\}$ et donc $\widetilde{\tau}^j = \mathrm{id}_\ell$. Comme L est de dimension finie sur son centre ℓ, le théorème de Skolem–Noether entraîne que τ^j est intérieur. Or τ^j est dans $\mathrm{Gal}(L/H)$ et L/H est extérieure par le théorème 4.1.2. On a donc $\tau^j = \mathrm{id}_L$.

2) Si, dans la proposition 4.1.5, on suppose aussi que l'ordre de σ vaut l'ordre de $\widetilde{\sigma}$, alors, par le lemme 4.1.3, le théorème de Skolem–Noether et le 1), le centre de $H(T,\sigma)$ vaut $h^{\langle\widetilde{\sigma}\rangle}(T^m)$. Ainsi, dans la preuve, l'injectivité de ψ est une conséquence directe de [Bla72, théorème II-3].

3) En général, la réciproque du 1) est fausse. En effet, rappelons tout d'abord que le *niveau* d'un corps commutatif h est, soit le plus entier $n \geq 1$ pour lequel il existe $(x_1,\ldots,x_n) \in h^{*n}$ tel que $-1 = x_1^2 + \cdots + x_n^2$ (si un tel n existe), soit ∞ (sinon). Par le théorème de Pfister (voir, par exemple, [Lam05, Chapter XI, Theorem 2.2]), le niveau de h est infini ou une puissance de 2. De plus, pour un corps commutatif h de niveau au moins 4, notons H_h le *corps des quaternions* à coefficients dans h, i.e. $H_h = h \oplus hi \oplus hj \oplus hk$ ($i^2 = j^2 = k^2 = ijk = -1$).

On se donne maintenant une extension galoisienne ℓ/h de corps commutatifs telle que ℓ soit de niveau au moins 4 et telle que $\mathrm{Gal}(\ell/h)$ soit fini d'ordre pair (par exemple, $h = \mathbb{Q}$ et $\ell = \mathbb{Q}(\sqrt{2})$). Posons $L = H_\ell$ et $H = H_h$. Par le théorème 4.1.2, L/H est galoisienne à groupe de Galois fini d'ordre pair. Soit τ' un élément d'ordre 2 de $\mathrm{Gal}(L/H)$, soit $\sigma = I_H(i)$ et soit $\tau = I_L(i) \circ \tau'$. Clairement, σ est d'ordre 2 et $\widetilde{\sigma} = \mathrm{id}_h$. De plus, puisque τ' fixe H point par point, τ prolonge σ. Mais, puisque L/H est extérieure (voir théorème 4.1.2), τ' n'est pas intérieur et, ainsi, τ ne l'est pas non plus. Par le théorème de Skolem–Noether, on en déduit $\widetilde{\tau} \neq \mathrm{id}_\ell$. Mais, pour $x \in L$, on a $I_L(i) \circ \tau'(x) = i\tau'(x)i^{-1}$ et donc $\tau^2(x) = I_L(i) \circ \tau'(i\tau'(x)i^{-1}) = i\tau'(i)\tau'^2(x)\tau'(i^{-1})i^{-1} = i^2xi^{-2} = x$, ce qui montre que τ est d'ordre 2.

4.2 Problèmes de plongement finis

Dans cette partie, nous étendons la terminologie des problèmes de plongement finis sur les corps commutatifs à la situation des corps de dimension finie sur leurs centres. Nous démontrons aussi une version plus précise du théorème 0.3.7 (voir théorème 4.2.9).

4.2.1 Applications de restriction

Etant données deux extensions galoisiennes L/H et F/M à groupes de Galois finis et telles que $L \subseteq F$ et $H \subseteq M$, nous notons $\mathrm{res}^{F/M}_{L/H}$ l'application de restriction $\mathrm{Gal}(F/M) \to \mathrm{Gal}(L/H)$ (c'est-à-dire $\mathrm{res}^{F/M}_{L/H}(\sigma)(x) = \sigma(x)$ pour tout $\sigma \in \mathrm{Gal}(F/M)$ et tout $x \in L$), si celle-ci est bien définie.

Contrairement au cas commutatif, l'application $\mathrm{res}^{F/M}_{L/H}$ n'est pas définie en général. Nous donnons maintenant des conditions suffisantes sur L, H, F et M pour qu'elle le soit.

Proposition 4.2.1. *Soient L/H et F/M deux extensions galoisiennes à groupes de Galois finis, telles que $L \subseteq F$ et $H \subseteq M$, et vérifiant les conditions suivantes :*

1) *$F = M \otimes_{k_M} \ell_M$ et $L = H \otimes_{k_H} \ell_H$ pour des extensions galoisiennes ℓ_M/k_M et ℓ_H/k_H de corps commutatifs à groupes de Galois finis et telles que k_M (resp. k_H) soit contenu dans le centre de M (resp. de H),*

2) *il existe une extension galoisienne ℓ_0/k_0 de corps commutatifs de groupe fini telle que*

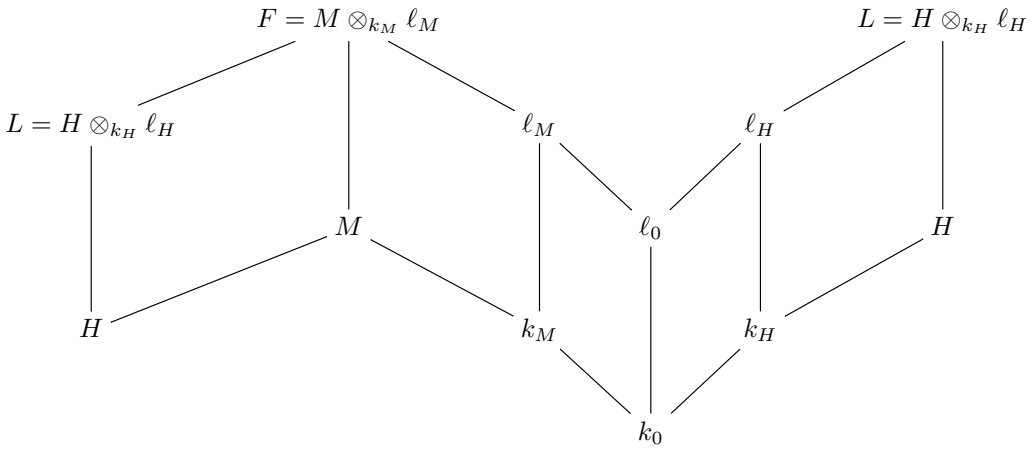
a) *$\ell_0 \subseteq \ell_M \cap \ell_H$ et $k_0 \subseteq k_M \cap k_H$,*

b) *l'extension ℓ_H/k_0 est galoisienne finie et $[\ell_0 : k_0] = [\ell_H : k_H]$,*

c) *$\mathrm{Gal}(\ell_H/\ell_0) \cap \mathrm{Gal}(\ell_H/k_H) = \{\mathrm{id}_{\ell_H}\}$.*

Alors $\mathrm{res}^{F/M}_{L/H}$ est bien définie.

Preuve. On a le diagramme d'extensions de corps suivant :



Puisque ℓ_0/k_0 est galoisienne à groupe de Galois fini et a) est vérifiée, on peut considérer l'application $\mathrm{res}^{\ell_M/k_M}_{\ell_0/k_0}$. De plus, par b), on a $\ell_0 k_H = \ell_H^{\mathrm{Gal}(\ell_H/\ell_0)} \ell_H^{\mathrm{Gal}(\ell_H/k_H)} = \ell_H^{\mathrm{Gal}(\ell_H/\ell_0)\cap\mathrm{Gal}(\ell_H/k_H)} = \ell_H$, la dernière égalité étant le c). Par b), on en déduit $[\ell_0 : k_0] = [\ell_0 k_H : k_H]$, c'est-à-dire ℓ_0 et k_H sont linéairement disjoints sur k_0. En utilisant à nouveau $\ell_0 k_H = \ell_H$, on en déduit que $\mathrm{res}^{\ell_H/k_H}_{\ell_0/k_0}$ est un isomorphisme. En outre, puisque 1) est vraie, les applications $\widetilde{\mathrm{res}}^{F/M}_{\ell_M/k_M}$ et $\widetilde{\mathrm{res}}^{L/H}_{\ell_H/k_H}$ (voir (4.1.1)) sont des isomorphismes bien définis. On peut alors considérer

$$g = (\widetilde{\mathrm{res}}^{L/H}_{\ell_H/k_H})^{-1} \circ (\mathrm{res}^{\ell_H/k_H}_{\ell_0/k_0})^{-1} \circ \mathrm{res}^{\ell_M/k_M}_{\ell_0/k_0} \circ \widetilde{\mathrm{res}}^{F/M}_{\ell_M/k_M} : \mathrm{Gal}(F/M) \to \mathrm{Gal}(L/H). \qquad (4.2.1)$$

Alors $g = \mathrm{res}^{F/M}_{L/H}$. En effet, par ce qui précède, on a $L = H \otimes_{k_H} \ell_H = H \otimes_{k_H} \ell_0 k_H$. Etant donnés $\sigma \in \mathrm{Gal}(F/M)$, $x \in H$, $y \in \ell_0$ et $z \in k_H$, on a donc

$$g(\sigma)(x \otimes yz) = x \otimes ((\mathrm{res}^{\ell_H/k_H}_{\ell_0/k_0})^{-1} \circ \mathrm{res}^{\ell_M/k_M}_{\ell_0/k_0} \circ \widetilde{\mathrm{res}}^{F/M}_{\ell_M/k_M}(\sigma)(yz)).$$

Mais, puisque y est dans ℓ_0, on a $(\mathrm{res}^{\ell_H/k_H}_{\ell_0/k_0})^{-1} \circ \mathrm{res}^{\ell_M/k_M}_{\ell_0/k_0} \circ \widetilde{\mathrm{res}}^{F/M}_{\ell_M/k_M}(\sigma)(y) = \sigma(y)$ et, puisque $z \in k_H$ et σ laisse fixe H point par point, on a

$$(\mathrm{res}^{\ell_H/k_H}_{\ell_0/k_0})^{-1} \circ \mathrm{res}^{\ell_M/k_M}_{\ell_0/k_0} \circ \widetilde{\mathrm{res}}^{F/M}_{\ell_M/k_M}(\sigma)(z) = z = \sigma(z),$$

Ainsi $g(\sigma)(x \otimes yz) = x \otimes \sigma(yz) = \sigma(x \otimes yz)$, ce qui conclut la démonstration. □

Remarque 4.2.2. Avec les notations de la proposition, la définition de $\mathrm{res}^{F/M}_{L/H}$ (voir (4.2.1)) montre que cette application est un isomorphisme si et seulement s'il en est de même de $\mathrm{res}^{\ell_M/k_M}_{\ell_0/k_0}$.

Nous appliquons maintenant notre construction dans quatre situations.

I) Bien entendu, le cas des corps commutatifs est couvert. Plus précisément, soient F/M et L/H deux extensions galoisiennes de corps commutatifs à groupes de Galois finis et telles que $H \subseteq M$ et $L \subseteq F$. Dans ce cas, on a $F = M \otimes_M F$ et $L = H \otimes_H L$. La proposition 4.2.1 s'applique donc avec $\ell_M = F$, $k_M = M$, $\ell_H = \ell_0 = L$ et $k_H = k_0 = H$.

II) Soit F/M une extension galoisienne à groupe de Galois fini. Supposons $F = M \otimes_k \ell$ pour une certaine extension galoisienne ℓ/k de corps commutatifs à groupe de Galois fini et telle que k soit contenu dans le centre de M. On pose $\ell_M = \ell_0 = \ell_H = L = \ell$ et $k_M = k_0 = k_H = H = k$. Alors l'application $\mathrm{res}^{F/M}_{L/H}$ de la proposition 4.2.1 est un isomorphisme, qui vaut $\widetilde{\mathrm{res}}^{F/M}_{\ell/k}$ (voir

(4.1.1)). En particulier, si M est de dimension finie sur son centre m, alors $F = M \otimes_m f$ par le théorème 4.1.2, où f est le centre de F. Ainsi $\mathrm{res}_{f/m}^{F/M}$ est un isomorphisme.

III) Soient L/H et F/H galoisiennes à groupes de Galois finis avec $L \subseteq F$ et H de dimension finie sur son centre h. Par le lemme 4.1.1 et le théorème 4.1.2, F/L est extérieure. Ainsi le centre ℓ de L est un sous-corps du centre f de F. De plus, par le théorème 4.1.2, on a $F = H \otimes_h f$ (resp. $L = H \otimes_h \ell$) et f/h (resp. ℓ/h) est galoisienne finie. En posant $M = H$, $\ell_M = f$, $k_M = h$, $\ell_0 = \ell_H = \ell$ et $k_0 = k_H = h$, la proposition 4.2.1 montre que $\mathrm{res}_{L/H}^{F/H}$ est bien définie.

Remarque 4.2.3. Si L/H et F/H sont deux extensions galoisiennes à groupes de Galois finis, telles que F/H soit extérieure et telles que $L \subseteq F$, alors $\mathrm{res}_{L/H}^{F/H}$ est bien définie (voir le début du §3.2 ou [Coh95]).

IV) Nous appliquons enfin la proposition 4.2.1 aux extensions de corps de fractions rationnelles tordus.

Corollaire 4.2.4. *Soient H un corps de dimension finie sur son centre h et $\sigma \in \mathrm{Aut}(H)$. Soient L/H une extension galoisienne à groupe de Galois fini et τ un automorphisme de L d'ordre fini étendant σ. Notons $\widetilde{\tau}$ la restriction de τ au centre ℓ de L et supposons :*

$$\langle \widetilde{\tau}, \mathrm{Gal}(\ell/h) \rangle \cong \langle \widetilde{\tau} \rangle \times \mathrm{Gal}(\ell/h). \tag{4.2.2}$$

Alors $L(T,\tau)/H(T,\sigma)$ est galoisienne à groupe de Galois fini et $\mathrm{res}_{L/H}^{L(T,\tau)/H(T,\sigma)}$ est un isomorphisme bien défini.

Nous aurons besoin du lemme suivant, qui sera réutilisé dans la suite :

Lemme 4.2.5. *Soient H un corps de dimension finie sur son centre et L/H une extension galoisienne à groupe de Galois fini. Soit h (resp. ℓ) le centre de H (resp. de L), soit $\sigma \in \mathrm{Aut}(H)$ et soit τ un automorphisme de L d'ordre fini prolongeant σ. Soit $\widetilde{\sigma}$ (resp. $\widetilde{\tau}$) la restriction de σ (resp. de τ) à h (resp. à ℓ). Les conditions suivantes sont équivalentes :*
i) $\langle \widetilde{\tau}, \mathrm{Gal}(\ell/h) \rangle = \mathrm{Gal}(\ell/h) \times \langle \widetilde{\tau} \rangle$,
ii) *l'ordre de $\widetilde{\tau}$ vaut l'ordre de $\widetilde{\sigma}$ et l'extension $\ell^{\langle \widetilde{\tau} \rangle}/h^{\langle \widetilde{\sigma} \rangle}$ est galoisienne.*

Preuve du lemme 4.2.5. Par le théorème 4.1.2, ℓ est une extension galoisienne de h. De plus, puisque τ prolonge σ, on a $h^{\langle \widetilde{\sigma} \rangle} \subseteq \ell^{\langle \widetilde{\tau} \rangle}$. Par conséquent, les conditions i) et ii) sont bien définies. De plus, en vertu du lemme 4.1.4, on peut supposer que $\langle \widetilde{\tau}, \mathrm{Gal}(\ell/h) \rangle$ vaut $\mathrm{Gal}(\ell/h) \rtimes \langle \widetilde{\tau} \rangle$ et se contenter de montrer que $\langle \widetilde{\tau} \rangle \trianglelefteq \langle \widetilde{\tau}, \mathrm{Gal}(\ell/h) \rangle$ si et seulement si $\ell^{\langle \widetilde{\tau} \rangle}/h^{\langle \widetilde{\sigma} \rangle}$ est galoisienne. Pour cela, notons que, puisque ℓ/h est galoisienne, on a $h = \ell^{\mathrm{Gal}(\ell/h)}$ et donc $h^{\langle \widetilde{\sigma} \rangle} = \ell^{\langle \widetilde{\tau}, \mathrm{Gal}(\ell/h) \rangle}$. Comme $\langle \widetilde{\tau}, \mathrm{Gal}(\ell/h) \rangle$ est fini, le lemme d'Artin montre que $\ell/h^{\langle \widetilde{\sigma} \rangle}$ est galoisienne et $\mathrm{Gal}(\ell/h^{\langle \widetilde{\sigma} \rangle}) = \langle \widetilde{\tau}, \mathrm{Gal}(\ell/h) \rangle$. Ainsi $\ell^{\langle \widetilde{\tau} \rangle}/h^{\langle \widetilde{\sigma} \rangle}$ est galoisienne si et seulement si $\mathrm{Gal}(\ell/\ell^{\langle \widetilde{\tau} \rangle}) \trianglelefteq \mathrm{Gal}(\ell/h^{\langle \widetilde{\sigma} \rangle})$, c'est-à-dire si et seulement si $\langle \widetilde{\tau} \rangle \trianglelefteq \langle \widetilde{\tau}, \mathrm{Gal}(\ell/h) \rangle$. □

Preuve du corollaire 4.2.4. Notons $\widetilde{\sigma}$ la restriction de σ à h. Par (4.2.2) et le lemme 4.2.5, l'ordre de $\widetilde{\tau}$ vaut l'ordre de $\widetilde{\sigma}$ et $\ell^{\langle \widetilde{\tau} \rangle}/h^{\langle \widetilde{\sigma} \rangle}$ est galoisienne de degré $[\ell : h]$. On peut donc appliquer la proposition 4.1.5 et conclure que $L(T,\tau) = H(T,\sigma) \otimes_{h^{\langle \widetilde{\sigma} \rangle}(T^m)} \ell^{\langle \widetilde{\tau} \rangle}(T^m)$, où m est l'ordre de τ. De plus, $h^{\langle \widetilde{\sigma} \rangle}(T^m)$ est contenu dans le centre de $H(T,\sigma)$ et $\ell^{\langle \widetilde{\tau} \rangle}(T^m)/h^{\langle \widetilde{\sigma} \rangle}(T^m)$ est galoisienne à groupe de Galois fini. Par le §4.1.1, $L(T,\tau)/H(T,\sigma)$ est galoisienne à groupe de Galois fini.

Montrons maintenant que $\mathrm{res}_{L/H}^{L(T,\tau)/H(T,\sigma)}$ est un isomorphisme bien défini. On applique pour cela la proposition 4.2.1 avec $F = L(T,\tau)$, $M = H(T,\sigma)$, $\ell_M = \ell^{\langle \widetilde{\tau} \rangle}(T^m)$, $k_M = h^{\langle \widetilde{\sigma} \rangle}(T^m)$, $\ell_0 = \ell^{\langle \widetilde{\tau} \rangle}$, $k_0 = h^{\langle \widetilde{\sigma} \rangle}$, $\ell_H = \ell$ et $k_H = h$. L'extension $\ell_0/k_0 = \ell^{\langle \widetilde{\tau} \rangle}/h^{\langle \widetilde{\sigma} \rangle}$ est galoisienne finie et, par (4.2.2), $\ell_H/k_0 = \ell/h^{\langle \widetilde{\sigma} \rangle} = \ell/\ell^{\langle \widetilde{\tau}, \mathrm{Gal}(\ell/h) \rangle}$ l'est aussi. De plus, $[\ell_0 : k_0] = [\ell^{\langle \widetilde{\tau} \rangle} : h^{\langle \widetilde{\sigma} \rangle}] = [\ell : h] =$

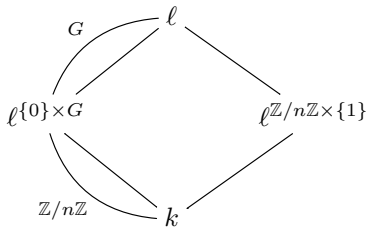
$[\ell_H : k_H]$ et $\mathrm{Gal}(\ell_H/\ell_0) \cap \mathrm{Gal}(\ell_H/k_H) = \mathrm{Gal}(\ell/\ell^{\langle\widetilde{\tau}\rangle}) \cap \mathrm{Gal}(\ell/h) = \{\mathrm{id}_\ell\} = \{\mathrm{id}_{\ell_H}\}$ par (4.2.2). Ainsi $\mathrm{res}_{L/H}^{L(T,\tau)/H(T,\sigma)}$ est bien définie et, par la remarque 4.2.2, c'est un isomorphisme. □

Remarque 4.2.6. Si H est de dimension finie sur son centre et L/H galoisienne à groupe de Galois fini, le corollaire 4.2.4 s'applique immédiatement dans les deux cas suivants :
• $\tau = \mathrm{id}_L$,
• σ est n'importe quel automorphisme de H d'ordre fini, $L = H$ et $\tau = \sigma$.
Nous présentons maintenant trois cas d'application moins immédiats.

1) Soit H un corps de dimension finie sur son centre h, soit L/H une extension galoisienne à groupe de Galois fini et soit $y \in H \setminus \{0\}$ pour lequel il existe $n \geq 1$ tel que $y^n \in h$. Clairement, le corollaire 4.2.4 s'applique si $\sigma = I_H(y)$ et $\tau = I_L(y)$.

2) Soient m et n deux entiers naturels non nuls tels que $n \equiv 1 \pmod{m}$. Pour une indéterminée U, le corps $L = \mathbb{C}((U^{1/n}))$ est une extension galoisienne de $H = \mathbb{C}((U))$ de groupe $\mathbb{Z}/n\mathbb{Z}$. Si σ est l'automorphisme de H d'ordre m défini par $U \mapsto e^{2i\pi/m}U$, on considère l'automorphisme τ de L défini par $U^{1/n} \mapsto e^{2i\pi/m}U^{1/n}$. Alors τ est d'ordre m et, puisque $n \equiv 1 \pmod{m}$, la restriction de τ à H vaut σ. De plus, (4.2.2) est vraie.

3) Soit K un corps de dimension finie sur son centre k. Soient $n \geq 2$ un entier et G un groupe fini non trivial tels qu'il existe une extension galoisienne L/K de groupe $\mathbb{Z}/n\mathbb{Z} \times G$. Par le théorème 4.1.2, si ℓ est le centre de L, on a :



De plus, $H = K \otimes_k \ell^{\{0\}\times G}$ est un corps et H/K est galoisienne de groupe $\mathbb{Z}/n\mathbb{Z}$. Soient $\widetilde{\sigma}$ un générateur de $\mathrm{Gal}(\ell^{\{0\}\times G}/k)$ et σ un générateur de $\mathrm{Gal}(H/K)$ tel que $\mathrm{res}^{H/K}_{\ell^{\{0\}\times G}/k}(\sigma) = \widetilde{\sigma}$. En outre, $\ell^{\{0\}\times G}$ et $\ell^{\mathbb{Z}/n\mathbb{Z}\times\{1\}}$ sont linéairement disjoints sur k et leur compositum vaut ℓ. Ainsi il existe $\widetilde{\tau} \in \mathrm{Gal}(\ell/k)$ d'ordre n et tel que $\mathrm{res}^{\ell/k}_{\ell^{\{0\}\times G}/k}(\widetilde{\tau}) = \widetilde{\sigma}$. Soit $\tau \in \mathrm{Gal}(L/K)$ l'antécédent de $\widetilde{\tau}$ sous $\mathrm{res}^{L/K}_{\ell/k}$. Alors τ étend σ. Enfin, L/H est galoisienne de groupe G (voir théorème 4.1.2) et, par construction, on a $\langle\widetilde{\tau}, \mathrm{Gal}(\ell/\ell^{\{0\}\times G})\rangle \cong \langle\widetilde{\tau}\rangle \times \mathrm{Gal}(\ell/\ell^{\{0\}\times G})$.

Le corollaire 4.2.4 admet la réciproque partielle suivante :

Proposition 4.2.7. *Soient H un corps de dimension finie sur son centre h et $\sigma \in \mathrm{Aut}(H)$. Soient L/H une extension galoisienne à groupe de Galois fini et τ un automorphisme de L d'ordre fini étendant σ. Notons $\widetilde{\tau}$ la restriction de τ au centre ℓ de L. Supposons :*
1) *$L(T,\tau)/H(T,\sigma)$ est galoisienne à groupe de Galois fini,*
2) *l'ordre intérieur de σ (resp. de τ) vaut l'ordre de σ (resp. de τ).*
Alors $\langle\widetilde{\tau}, \mathrm{Gal}(\ell/h)\rangle \cong \langle\widetilde{\tau}\rangle \times \mathrm{Gal}(\ell/h)$.

Preuve. Soit $\widetilde{\sigma}$ la restriction de σ à h. Par 2) et le lemme 4.1.3, les centres de $H(T,\sigma)$ et $L(T,\tau)$ sont $h^{\langle\widetilde{\sigma}\rangle}(T^m)$ et $\ell^{\langle\widetilde{\tau}\rangle}(T^n)$, où m (resp. n) est l'ordre de σ (resp. de τ). Comme $H(T,\sigma)$ est de dimension finie sur son centre (voir lemme 4.1.3), le théorème 4.1.2 et 1) montrent que $\ell^{\langle\widetilde{\tau}\rangle}(T^n)/h^{\langle\widetilde{\sigma}\rangle}(T^m)$ est galoisienne. De plus, comme $T^m \in \ell^{\langle\widetilde{\tau}\rangle}(T^n)$, on a $n \,|\, m$ et donc $n = m$. Ainsi $\ell^{\langle\widetilde{\tau}\rangle}/h^{\langle\widetilde{\sigma}\rangle}$ est galoisienne. En outre, comme $n = m$, le théorème de Skolem–Noether et 2) montrent que les ordres de $\widetilde{\sigma}$ et $\widetilde{\tau}$ sont égaux. Le lemme 4.2.5 permet alors de conclure. □

4.2.2 Problèmes de plongement finis

4.2.2.1 Terminologie

Soit H un corps de dimension finie sur son centre. Un *problème de plongement fini* sur H est un épimorphisme $\alpha : G \to \mathrm{Gal}(L/H)$, où G est un groupe fini et L/H une extension galoisienne. On dit que α est *scindé* s'il existe un plongement $\alpha' : \mathrm{Gal}(L/H) \to G$ tel que $\alpha \circ \alpha' = \mathrm{id}_{\mathrm{Gal}(L/H)}$. Une *solution faible* à α est un monomorphisme $\beta : \mathrm{Gal}(F/H) \to G$, où F/H est une extension galoisienne vérifiant $L \subseteq F$, tel que l'application composée $\alpha \circ \beta$ soit l'application de restriction $\mathrm{res}^{F/H}_{L/H}$ du III) du §4.2.1. Si β est un isomorphisme, on dit *solution* plutôt que solution faible.

Remarque 4.2.8. 1) Plus généralement, on peut définir un problème de plongement fini sur un corps quelconque H (pas nécessairement de dimension finie sur son centre). Cependant, pour la notion de solution faible, nous avons besoin que $\mathrm{res}^{F/H}_{L/H}$ soit bien définie. Comme vu dans la remarque 4.2.3, c'est le cas sans aucune hypothèse sur H, à condition de supposer F/H extérieure. Comme la plupart de nos résultats supposent H de dimension finie sur son centre, nous nous restreignons à cette situation dans la terminologie ci-dessus.

2) Soient H un corps de dimension finie sur son centre et $\alpha : G \to \mathrm{Gal}(L/H)$ un problème de plongement fini sur H. Puisque G est fini, L/H est extérieure (voir théorème 4.1.2) et, par conséquent, le lemme 4.1.1 s'applique : si H est commutatif, alors L l'est aussi. De même, si $\mathrm{Gal}(F/H) \to G$ est une solution faible à α et si H est commutatif, alors F l'est aussi. Par conséquent, notre terminologie étend celle du cas commutatif rappelée dans le §0.1.4 et aucune confusion n'est possible.

4.2.2.2 Passage des corps quelconques aux corps commutatifs et vice-versa

Soit H un corps de dimension finie sur son centre h. Nous renvoyons au §2.2 pour la définition de la forme polynomiale $\mathcal{F}_H$ associée à la norme réduite de H/h.

Soit $\alpha : G \to \mathrm{Gal}(L/H)$ un problème de plongement fini sur H. Puisque $\mathrm{res}^{L/H}_{\ell/h}$ est un isomorphisme, où ℓ est le centre de L (voir le II) du §4.2.1),

$$\check{\alpha} = \mathrm{res}^{L/H}_{\ell/h} \circ \alpha : G \to \mathrm{Gal}(\ell/h) \tag{4.2.3}$$

est un problème de plongement fini sur h. Par le théorème 4.1.2, $\mathcal{F}_H$ n'a que le zéro trivial sur ℓ. De plus, si $\beta : \mathrm{Gal}(F/H) \to G$ est une solution faible à α, alors $\mathrm{res}^{F/H}_{f/h}$ est un isomorphisme, où f est le centre de F. Ainsi

$$\check{\beta} = \beta \circ (\mathrm{res}^{F/H}_{f/h})^{-1} : \mathrm{Gal}(f/h) \to G \tag{4.2.4}$$

est une solution faible à $\check{\alpha}$, car $\mathrm{res}^{L/H}_{\ell/h} \circ \mathrm{res}^{F/H}_{L/H} = \mathrm{res}^{f/h}_{\ell/h} \circ \mathrm{res}^{F/H}_{f/h}$. De plus, $\mathcal{F}_H$ n'a que le zéro trivial sur f et β est une solution à α si et seulement si $\check{\beta}$ est une solution à $\check{\alpha}$.

Réciproquement, soit $\alpha : G \to \mathrm{Gal}(\ell/h)$ un problème de plongement fini sur h tel que $\mathcal{F}_H$ ne possède que le zéro trivial sur ℓ. Par le théorème 4.1.2, $(H \otimes_h \ell)/H$ est galoisienne à groupe de Galois fini et le centre de $H \otimes_h \ell$ vaut ℓ. Ainsi $\mathrm{res}^{(H\otimes_h \ell)/H}_{\ell/h}$ est un isomorphisme et

$$\hat{\alpha} = (\mathrm{res}^{(H\otimes_h \ell)/H}_{\ell/h})^{-1} \circ \alpha : G \to \mathrm{Gal}((H \otimes_h \ell)/H) \tag{4.2.5}$$

est un problème de plongement fini sur H. De plus, si $\beta : \mathrm{Gal}(f/h) \to G$ est une solution faible à α telle que $\mathcal{F}_H$ ne possède que le zéro trivial sur f, alors, par le théorème 4.1.2, $(H \otimes_h f)/H$ est

une extension galoisienne à groupe de Galois fini et le centre de $H \otimes_h f$ vaut f. Ainsi $\mathrm{res}_{f/h}^{(H\otimes_h f)/H}$ est un isomorphisme. Par conséquent, l'application composée

$$\hat{\beta} = \beta \circ \mathrm{res}_{f/h}^{(H\otimes_h f)/H} : \mathrm{Gal}((H \otimes_h f)/H) \to G \tag{4.2.6}$$

est une solution faible à $\hat{\alpha}$, puisque $\mathrm{res}_{\ell/h}^{(H\otimes_h \ell)/H} \circ \mathrm{res}_{(H\otimes_f \ell)/H}^{(H\otimes_h f)/H} = \mathrm{res}_{\ell/h}^{f/h} \circ \mathrm{res}_{f/h}^{(H\otimes_h f)/H}$. Il est également clair que β est une solution à α si et seulement si $\hat{\beta}$ est une solution à $\hat{\alpha}$.

Enfin, soit $\alpha : G \to \mathrm{Gal}(L/H)$ un problème de plongement fini sur H. Puisque $L = H \otimes_h \ell$ (voir théorème 4.1.2), où h (resp. ℓ) est le centre de H (resp. de L), on a $\hat{\check{\alpha}} = \alpha$. De même, si $\beta : \mathrm{Gal}(F/H) \to G$ est une solution faible à α, alors $\hat{\check{\beta}} = \beta$. Réciproquement, soit $\alpha : G \to \mathrm{Gal}(\ell/h)$ un problème de plongement fini sur h tel que $\mathcal{F}_H$ ne possède que le zéro trivial sur ℓ. Puisque le centre de $H \otimes_h \ell$ vaut ℓ, on a $\check{\hat{\alpha}} = \alpha$. De même, si $\beta : \mathrm{Gal}(f/h) \to G$ est une solution faible à α telle que $\mathcal{F}_H$ ne possède que le zéro trivial sur f, alors $\check{\hat{\beta}} = \beta$.

Nous avons donc démontré le théorème suivant, qui généralise à la fois [DL20, théorème 7] et le théorème 0.3.7 de l'introduction :

Théorème 4.2.9. *Soient H un corps de dimension finie sur son centre h et $\alpha : G \to \mathrm{Gal}(L/H)$ un problème de plongement fini sur H. Les applications $\beta \mapsto \check{\beta}$ et $\gamma \mapsto \hat{\gamma}$ sont des bijections réciproques entre l'ensemble des solutions β à α et l'ensemble des solutions $\gamma : \mathrm{Gal}(f/h) \to G$ à $\check{\alpha}$ telles que $\mathcal{F}_H$ ne possède que le zéro trivial sur f.*

4.2.2.3 Solutions géométriques

Soient H un corps de dimension finie sur son centre h et $\sigma \in \mathrm{Aut}(H)$. Soient $\alpha : G \to \mathrm{Gal}(L/H)$ un problème de plongement fini sur H et τ un automorphisme de L d'ordre fini étendant σ. Notons $\widetilde{\tau}$ la restriction de τ au centre ℓ de L et supposons $\langle \widetilde{\tau}, \mathrm{Gal}(\ell/h)\rangle \cong \langle \widetilde{\tau}\rangle \times \mathrm{Gal}(\ell/h)$. Alors $L(T,\tau)/H(T,\sigma)$ est galoisienne à groupe de Galois fini et $\mathrm{res}_{L/H}^{L(T,\tau)/H(T,\sigma)}$ est un isomorphisme bien défini (voir corollaire 4.2.4). Comme le corps $H(T,\sigma)$ est de dimension finie sur son centre (voir lemme 4.1.3), l'application composée

$$\alpha_{\sigma,\tau} = (\mathrm{res}_{L/H}^{L(T,\tau)/H(T,\sigma)})^{-1} \circ \alpha : G \to \mathrm{Gal}(L(T,\tau)/H(T,\sigma)) \tag{4.2.7}$$

est un problème de plongement fini sur $H(T,\sigma)$. Une *solution (σ,τ)-géométrique* à α est une solution $\mathrm{Gal}(E/H(T,\sigma)) \to G$ à $\alpha_{\sigma,\tau}$. Si $\tau = \mathrm{id}_L$, on dit plutôt *solution géométrique*. Comme dans la remarque 4.2.8, E est commutatif dès que $H(T,\sigma)$ l'est. En particulier, il n'y a aucune confusion possible avec la notion de solution géométrique du §0.1.4.

De plus, notons $\widetilde{\sigma}$ la restriction de σ à h. Par les lemmes 4.1.4 et 4.2.5, l'extension $\ell^{\langle\widetilde{\tau}\rangle}/h^{\langle\widetilde{\sigma}\rangle}$ est galoisienne et $\mathrm{res}_{\ell^{\langle\widetilde{\tau}\rangle}/h^{\langle\widetilde{\sigma}\rangle}}^{\ell/h}$ est un isomorphisme. Avec $\check{\alpha}$ comme dans (4.2.3), on peut donc considérer le problème de plongement fini sur $h^{\langle\widetilde{\sigma}\rangle}$ suivant :

$$\overline{\alpha}_{\sigma,\tau} = \mathrm{res}_{\ell^{\langle\widetilde{\tau}\rangle}/h^{\langle\widetilde{\sigma}\rangle}}^{\ell/h} \circ \check{\alpha} : G \to \mathrm{Gal}(\ell^{\langle\widetilde{\tau}\rangle}/h^{\langle\widetilde{\sigma}\rangle}). \tag{4.2.8}$$

Lemme 4.2.10. *On a $\alpha_{\sigma,\tau} = (\mathrm{res}_{\ell^{\langle\widetilde{\tau}\rangle}/h^{\langle\widetilde{\sigma}\rangle}}^{L(T,\tau)/H(T,\sigma)})^{-1} \circ \overline{\alpha}_{\sigma,\tau}$.*

Preuve. Notons m l'ordre de τ. Par la définition de $\mathrm{res}_{L/H}^{L(T,\tau)/H(T,\sigma)}$, on a

$$\begin{aligned}
\alpha_{\sigma,\tau} &= (\mathrm{res}_{L/H}^{L(T,\tau)/H(T,\sigma)})^{-1} \circ \alpha \\
&= (\mathrm{res}_{\ell^{\langle\widetilde{\tau}\rangle}(T^m)/h^{\langle\widetilde{\sigma}\rangle}(T^m)}^{L(T,\tau)/H(T,\sigma)})^{-1} \circ (\mathrm{res}_{\ell^{\langle\widetilde{\tau}\rangle}/h^{\langle\widetilde{\sigma}\rangle}}^{\ell^{\langle\widetilde{\tau}\rangle}(T^m)/h^{\langle\widetilde{\sigma}\rangle}(T^m)})^{-1} \circ \mathrm{res}_{\ell^{\langle\widetilde{\tau}\rangle}/h^{\langle\widetilde{\sigma}\rangle}}^{\ell/h} \circ \check{\alpha} \\
&= (\mathrm{res}_{\ell^{\langle\widetilde{\tau}\rangle}(T^m)/h^{\langle\widetilde{\sigma}\rangle}(T^m)}^{L(T,\tau)/H(T,\sigma)})^{-1} \circ (\mathrm{res}_{\ell^{\langle\widetilde{\tau}\rangle}/h^{\langle\widetilde{\sigma}\rangle}}^{\ell^{\langle\widetilde{\tau}\rangle}(T^m)/h^{\langle\widetilde{\sigma}\rangle}(T^m)})^{-1} \circ \overline{\alpha}_{\sigma,\tau} \\
&= (\mathrm{res}_{\ell^{\langle\widetilde{\tau}\rangle}/h^{\langle\widetilde{\sigma}\rangle}}^{L(T,\tau)/H(T,\sigma)})^{-1} \circ \overline{\alpha}_{\sigma,\tau},
\end{aligned}$$

ce qui démontre le lemme. □

4.3 Résolution de problèmes de plongement finis scindés

Le théorème suivant est l'objectif de cette partie :

Théorème 4.3.1. *Soit H un corps de dimension finie sur son centre h, soit $\sigma \in \mathrm{Aut}(H)$ et soit $\widetilde{\sigma}$ la restriction de σ à h. Soient $\alpha : G \to \mathrm{Gal}(L/H)$ un problème de plongement fini sur H et τ un automorphisme de L d'ordre fini étendant σ. Soit $\widetilde{\tau}$ la restriction de τ au centre ℓ de L. Supposons que les trois conditions suivantes soient vérifiées :*
1) *α est scindé,*
2) *$\langle \widetilde{\tau}, \mathrm{Gal}(\ell/h)\rangle \cong \langle \widetilde{\tau}\rangle \times \mathrm{Gal}(\ell/h)$,*
3) *il existe un sous-corps ample k_0 de $h^{\langle\widetilde{\sigma}\rangle}$ et un corps commutatif ℓ_0 galoisien sur k_0 tels que ℓ_0 et $h^{\langle\widetilde{\sigma}\rangle}$ soient linéairement disjoints sur k_0 et tels que $\ell_0 h^{\langle\widetilde{\sigma}\rangle} = \ell^{\langle\widetilde{\tau}\rangle}$.*
Alors α admet une solution (σ,τ)-géométrique.

Nous aurons besoin du lemme suivant, qui fait le lien avec le cas des corps commutatifs :

Lemme 4.3.2. *En conservant les notations du théorème, supposons que 2) soit vérifiée et notons m l'ordre de τ. Alors α a une solution (σ,τ)-géométrique, pourvu que $\overline{\alpha}_{\sigma,\tau}$ (voir (4.2.8)) possède une solution géométrique $\mathrm{Gal}(e/h^{\langle\widetilde{\sigma}\rangle}(T^m)) \to G$ vérifiant $e \subseteq \ell^{\langle\widetilde{\tau}\rangle}((T^m))$.*

Preuve du lemme 4.3.2. Tout d'abord, notons que $\overline{\alpha}_{\sigma,\tau}$ est bien défini puisque 2) est vraie. Soit $\beta : \mathrm{Gal}(e/h^{\langle\widetilde{\sigma}\rangle}(T^m)) \to G$ une solution géométrique à $\overline{\alpha}_{\sigma,\tau}$ telle que $e \subseteq \ell^{\langle\widetilde{\tau}\rangle}((T^m))$. Puisque la dernière inclusion vaut, la proposition 3.1.2 s'applique : $L(T,\tau)\otimes_{\ell^{\langle\widetilde{\tau}\rangle}(T^m)} e$ est un corps. De plus, puisque 2) est vraie, on a

$$L(T,\tau) = H(T,\sigma)\otimes_{h^{\langle\widetilde{\sigma}\rangle}(T^m)} \ell^{\langle\widetilde{\tau}\rangle}(T^m) \tag{4.3.1}$$

(voir proposition 4.1.5). Ainsi, en vertu de, par exemple, [Des11, proposition 37], on a

$$L(T,\tau)\otimes_{\ell^{\langle\widetilde{\tau}\rangle}(T^m)} e = (H(T,\sigma)\otimes_{h^{\langle\widetilde{\sigma}\rangle}(T^m)} \ell^{\langle\widetilde{\tau}\rangle}(T^m))\otimes_{\ell^{\langle\widetilde{\tau}\rangle}(T^m)} e = H(T,\sigma)\otimes_{h^{\langle\widetilde{\sigma}\rangle}(T^m)} e.$$

En particulier, $E = H(T,\sigma)\otimes_{h^{\langle\widetilde{\sigma}\rangle}(T^m)} e$ est un corps et, par le §4.1.1, l'extension $E/H(T,\sigma)$ est galoisienne. De plus, puisque e contient $\ell^{\langle\widetilde{\tau}\rangle}(T^m)$ et (4.3.1) est vraie, on a $L(T,\tau)\subseteq E$.

Maintenant, le §4.1.1 montre que $\mathrm{res}^{E/H(T,\sigma)}_{e/h^{\langle\widetilde{\sigma}\rangle}(T^m)}$ est un isomorphisme. On peut alors considérer l'isomorphisme composé $\beta\circ\mathrm{res}^{E/H(T,\sigma)}_{e/h^{\langle\widetilde{\sigma}\rangle}(T^m)} : \mathrm{Gal}(E/H(T,\sigma)) \to G$. Le lemme 4.2.10 fournit alors

$$\begin{aligned}
\alpha_{\sigma,\tau}\circ\beta\circ\mathrm{res}^{E/H(T,\sigma)}_{e/h^{\langle\widetilde{\sigma}\rangle}(T^m)} &= (\mathrm{res}^{L(T,\tau)/H(T,\sigma)}_{\ell^{\langle\widetilde{\tau}\rangle}/h^{\langle\widetilde{\sigma}\rangle}})^{-1}\circ\overline{\alpha}_{\sigma,\tau}\circ\beta\circ\mathrm{res}^{E/H(T,\sigma)}_{e/h^{\langle\widetilde{\sigma}\rangle}(T^m)}\\
&= (\mathrm{res}^{L(T,\tau)/H(T,\sigma)}_{\ell^{\langle\widetilde{\tau}\rangle}/h^{\langle\widetilde{\sigma}\rangle}})^{-1}\circ\mathrm{res}^{e/h^{\langle\widetilde{\sigma}\rangle}(T^m)}_{\ell^{\langle\widetilde{\tau}\rangle}/h^{\langle\widetilde{\sigma}\rangle}}\circ\mathrm{res}^{E/H(T,\sigma)}_{e/h^{\langle\widetilde{\sigma}\rangle}(T^m)}\\
&= \mathrm{res}^{E/H(T,\sigma)}_{L(T,\tau)/H(T,\sigma)},
\end{aligned}$$

ce qui conclut la démonstration du lemme. □

Preuve du théorème 4.3.1. Par 3), $\mathrm{res}^{\ell^{\langle\widetilde{\tau}\rangle}/h^{\langle\widetilde{\sigma}\rangle}}_{\ell_0/k_0}$ est un isomorphisme. Considérons le problème de plongement fini

$$\alpha' = \mathrm{res}^{\ell^{\langle\widetilde{\tau}\rangle}/h^{\langle\widetilde{\sigma}\rangle}}_{\ell_0/k_0}\circ\overline{\alpha}_{\sigma,\tau} : G \to \mathrm{Gal}(\ell_0/k_0)$$

sur k_0. Puisque k_0 est ample (par 3)) et α' est scindé (par 1)), on peut appliquer [Pop96, Main Theorem A] (voir aussi [HJ98, Theorem 1]) pour obtenir que α' a une solution géométrique

$\beta : \mathrm{Gal}(e/k_0(T^m)) \to G$ vérifiant $e \subseteq \ell_0((T^m))$, où m est l'ordre de τ. Or, par 3) et puisque $e \cap \overline{k_0} = \ell_0$, l'application de restriction $\mathrm{res}^{eh^{\langle\widetilde{\sigma}\rangle}/h^{\langle\widetilde{\sigma}\rangle}(T^m)}_{e/k_0(T^m)}$ est un isomorphisme. Ainsi l'isomorphisme composé

$$\beta \circ \mathrm{res}^{eh^{\langle\widetilde{\sigma}\rangle}/h^{\langle\widetilde{\sigma}\rangle}(T^m)}_{e/k_0(T^m)} : \mathrm{Gal}(eh^{\langle\widetilde{\sigma}\rangle}/h^{\langle\widetilde{\sigma}\rangle}(T^m)) \to G$$

est une solution géométrique à $\overline{\alpha}_{\sigma,\tau}$. De plus, comme $e \subseteq \ell_0((T^m))$, on a $eh^{\langle\widetilde{\sigma}\rangle} \subseteq \ell_0 h^{\langle\widetilde{\sigma}\rangle}((T^m)) = \ell^{\langle\widetilde{\tau}\rangle}((T^m))$. Il ne reste plus qu'à appliquer le lemme 4.3.2 pour conclure la démonstration. □

Remarque 4.3.3. 1) Pour $\tau = \mathrm{id}_L$, le théorème 4.3.1 affirme que tout problème de plongement fini scindé sur un corps H de dimension finie sur son centre h admet une solution géométrique, si h est ample, comme annoncé dans le théorème 0.3.8 de l'introduction.

2) Si $H = L$ dans le théorème 4.3.1, on a l'énoncé suivant, qui est un cas particulier du théorème 0.3.5 et dont le cas $\sigma = \mathrm{id}_H$ est [DL20, théorème B] :

Soient H un corps de dimension finie sur son centre h et σ un automorphisme de H d'ordre fini. Supposons que $h^{\langle\widetilde{\sigma}\rangle}$ contienne un corps ample, où $\widetilde{\sigma}$ est la restriction de σ à h. Alors tout groupe fini est le groupe de Galois d'une extension galoisienne de $H(T, \sigma)$.

3) Les 1) et 2) de cette remarque correspondent aux deux situations de la remarque 4.2.6 dans lesquelles le corollaire 4.2.4 s'applique immédiatement. Bien entendu, des corollaires du théorème 4.3.1 correspondant aux situations "non triviales" de la remarque 4.2.6 peuvent aussi être donnés. Nous laissons ce travail au lecteur intéressé.

4.4 A propos de la réduction faible→scindé

Dans cette dernière partie, nous étendons la réduction faible→scindé au cas des corps de dimension finie sur leurs centres. Nous donnons aussi une variante du théorème 4.3.1 pour les problèmes de plongement finis admettant une solution faible (voir corollaire 4.4.4).

4.4.1 Extensions de la réduction faible→scindé

Rappelons tout d'abord cette réduction dans le cas commutatif (voir [Pop96, §1 B) 2)] et [DD97, §2.1.2]) :

Proposition 4.4.1. *Soient k un corps commutatif et $\alpha : G \to \mathrm{Gal}(\ell/k)$ un problème de plongement fini sur k. Pour toute solution faible $\mathrm{Gal}(\ell'/k) \to G$ à α, il existe un problème de plongement fini scindé $\alpha' : G' \to \mathrm{Gal}(\ell'/k)$ sur k vérifiant les propriétés suivantes :*

1) $\ker(\alpha) \cong \ker(\alpha')$,

2) *toute solution $\mathrm{Gal}(f'/k) \to G'$ à α' donne une solution $\mathrm{Gal}(f/k) \to G$ à α avec $f \subseteq f'$,*

3) *toute solution géométrique $\mathrm{Gal}(e'/k(T)) \to G'$ à α' fournit une solution géométrique $\mathrm{Gal}(e/k(T)) \to G$ à α vérifiant $e \subseteq e'$.*

Nous démontrons maintenant une première généralisation :

Proposition 4.4.2. *Soient H un corps de dimension finie sur son centre, $\alpha : G \to \mathrm{Gal}(L/H)$ un problème de plongement fini sur H et $\gamma : \mathrm{Gal}(L'/H) \to G$ une solution faible à α. Il existe un problème de plongement fini scindé $\alpha' : G' \to \mathrm{Gal}(L'/H)$ sur H vérifiant :*

1) $\ker(\alpha) \cong \ker(\alpha')$,

2) *toute solution $\mathrm{Gal}(F'/H) \to G'$ à α' donne une solution $\mathrm{Gal}(F/H) \to G$ à α avec $F \subseteq F'$.*

Preuve. Considérons le problème de plongement fini $\check{\alpha} : G \to \mathrm{Gal}(\ell/h)$ sur le centre h de H (voir (4.2.3)), où ℓ est le centre de L. Comme γ est une solution faible à α, $\check{\gamma} : \mathrm{Gal}(\ell'/h) \to G$ (voir (4.2.4)), où ℓ' est le centre de L', est une solution faible à $\check{\alpha}$ et $\mathcal{F}_H$ (voir §2.2) n'a que le zéro trivial sur ℓ'. La proposition 4.4.1 fournit alors un problème de plongement fini scindé $(\check{\alpha})' : G' \to \mathrm{Gal}(\ell'/h)$ sur h qui en vérifie les 1) et 2). Comme $\mathcal{F}_H$ n'a que le zéro trivial sur ℓ', on peut considérer le problème de plongement fini $\widehat{(\check{\alpha})'} : G' \to \mathrm{Gal}(L'/H)$ sur H (voir (4.2.5)), que l'on note α'. Notons que α' est scindé (car $(\check{\alpha})'$ l'est). De plus, puisque $(\check{\alpha})'$ vérifie le 1) de la proposition 4.4.1, on a $\ker(\alpha') = \ker((\check{\alpha})') \cong \ker(\check{\alpha}) = \ker(\alpha)$, ce qui démontre le 1). Maintenant, soit $\beta' : \mathrm{Gal}(F'/H) \to G'$ une solution à α'. Alors $\check{\beta}' : \mathrm{Gal}(f'/h) \to G'$ est une solution à $\check{\alpha}' = (\check{\alpha})'$, où f' est le centre de F', et $\mathcal{F}_H$ n'a que le zéro trivial sur f'. Comme $(\check{\alpha})'$ vérifie le 2) de la proposition 4.4.1, il existe une solution $\beta : \mathrm{Gal}(f/h) \to G$ à $\check{\alpha}$ telle que $f \subseteq f'$. Enfin, puisque $\mathcal{F}_H$ n'a que le zéro trivial sur f, $\hat{\beta} : \mathrm{Gal}((H \otimes_h f)/H) \to G$ (voir (4.2.6)) est une solution à $\hat{\check{\alpha}} = \alpha$ telle que $H \otimes_h f \subseteq H \otimes_h f' = F'$. □

Nous concluons cette partie avec la variante géométrique de la proposition 4.4.2 suivante :

Proposition 4.4.3. *Soient H un corps de dimension finie sur son centre h et $\sigma \in \mathrm{Aut}(H)$. Soient $\alpha : G \to \mathrm{Gal}(L/H)$ un problème de plongement fini sur H et $\tau \in \mathrm{Aut}(L)$ étendant σ et tel que*

$$\langle \widetilde{\tau}, \mathrm{Gal}(\ell/h) \rangle \cong \langle \widetilde{\tau} \rangle \times \mathrm{Gal}(\ell/h), \tag{4.4.1}$$

où $\widetilde{\tau}$ est la restriction de τ au centre ℓ de L. Soit $\gamma : \mathrm{Gal}(L'/H) \to G$ une solution faible à α et soit τ' un automorphisme de L' d'ordre fini étendant τ et tel que

$$\langle \widetilde{\tau'}, \mathrm{Gal}(\ell'/h) \rangle \cong \langle \widetilde{\tau'} \rangle \times \mathrm{Gal}(\ell'/h), \tag{4.4.2}$$

où $\widetilde{\tau'}$ est la restriction de τ' au centre ℓ' de L'. Alors il existe un problème de plongement fini scindé $\alpha' : G' \to \mathrm{Gal}(L'/H)$ sur H vérifiant les deux conditions suivantes :
1) $\ker(\alpha) \cong \ker(\alpha')$,
2) *toute solution (σ, τ')-géométrique $\mathrm{Gal}(E'/H(T,\sigma)) \to G'$ à α' fournit une solution (σ, τ)-géométrique $\mathrm{Gal}(E/H(T,\sigma)) \to G$ à α vérifiant $E \subseteq E'$.*

Preuve. Comme (4.4.1) vaut, on peut considérer le problème de plongement fini

$$\alpha_{\sigma,\tau} : G \to \mathrm{Gal}(L(T,\tau)/H(T,\sigma))$$

sur $H(T,\sigma)$ (voir (4.2.7)). De plus, comme (4.4.2) vaut, $L'(T,\tau')/H(T,\sigma)$ est galoisienne à groupe de Galois fini et $\mathrm{res}_{L'/H}^{L'(T,\tau')/H(T,\sigma)}$ est un isomorphisme bien défini (voir corollaire 4.2.4). Ainsi

$$\gamma_{\sigma,\tau} = \gamma \circ \mathrm{res}_{L'/H}^{L'(T,\tau')/H(T,\sigma)} : \mathrm{Gal}(L'(T,\tau')/H(T,\sigma)) \to G$$

est une solution faible à $\alpha_{\sigma,\tau}$. Puisque $H(T,\sigma)$ est de dimension finie sur son centre (voir lemme 4.1.3), la proposition 4.4.2 s'applique et fournit un problème de plongement fini scindé $\underline{\alpha} : G' \to \mathrm{Gal}(L'(T,\tau')/H(T,\sigma))$ sur $H(T,\sigma)$ qui vérifie le 1) et le 2) de cette dernière proposition. On peut alors considérer le problème de plongement fini

$$\alpha' = \mathrm{res}_{L'/H}^{L'(T,\tau')/H(T,\sigma)} \circ \underline{\alpha} : G' \to \mathrm{Gal}(L'/H)$$

sur H. Comme $\underline{\alpha}$ est scindé, il en est de même pour α' et on a $\ker(\alpha') = \ker(\underline{\alpha}) \cong \ker(\alpha_{\sigma,\tau}) = \ker(\alpha)$. Maintenant, soit $\beta' : \mathrm{Gal}(E'/H(T,\sigma)) \to G'$ une solution (σ,τ')-géométrique à α'. Alors β' est une solution à $\alpha'_{\sigma,\tau'} = \underline{\alpha}$. Comme $\underline{\alpha}$ vérifie le 2) de la proposition 4.4.2, il existe une solution $\beta : \mathrm{Gal}(E/H(T,\sigma)) \to G$ à $\alpha_{\sigma,\tau}$ vérifiant $E \subseteq E'$. Cela conclut la démonstration puisque, par définition, β est une solution (σ,τ)-géométrique à α. □

4.4.2 Extension du théorème 4.3.1

Notre dernier objectif est la variante du théorème 4.3.1 suivante, qui concerne les problèmes de plongement finis admettant une solution faible :

Corollaire 4.4.4. *Soient H un corps de dimension finie sur son centre h, $\sigma \in \mathrm{Aut}(H)$, $\alpha : G \to \mathrm{Gal}(L/H)$ un problème de plongement fini sur H et $\tau \in \mathrm{Aut}(L)$ étendant σ tels que*
1) *α admet une solution faible $\mathrm{Gal}(L'/H) \to G$ et il existe un automorphisme τ' de L' d'ordre fini étendant τ et tel que $\langle \widetilde{\tau'}, \mathrm{Gal}(\ell'/h)\rangle \cong \langle \widetilde{\tau'}\rangle \times \mathrm{Gal}(\ell'/h)$, où $\widetilde{\tau'}$ est la restriction de τ' au centre ℓ' de L',*
2) *$\langle \widetilde{\tau}, \mathrm{Gal}(\ell/h)\rangle \cong \langle \widetilde{\tau}\rangle \times \mathrm{Gal}(\ell/h)$, où $\widetilde{\tau}$ est la restriction de τ au centre ℓ de L,*
3) *$h^{\langle \widetilde{\sigma}\rangle}$ est un corps ample, où $\widetilde{\sigma}$ est la restriction de σ à h.*
Alors α a une solution (σ, τ)-géométrique.

Preuve. Comme 1) et 2) sont vraies, la proposition 4.4.3 s'applique et fournit un problème de plongement fini scindé $\alpha' : G' \to \mathrm{Gal}(L'/H)$ sur H vérifiant le 1) et le 2) de cette dernière proposition. Maintenant, comme 1) et 3) sont vraies et comme α' est scindé, α' a une solution (σ, τ')-géométrique (voir théorème 4.3.1). Il ne reste alors plus qu'à utiliser que le problème de plongement fini α' vérifie le 2) de la proposition 4.4.3 pour achever la démonstration. □

En particulier, si H est un corps de dimension finie sur son centre h et si $\alpha : G \to \mathrm{Gal}(L/H)$ est un problème de plongement fini sur H admettant une solution faible, alors α a une solution géométrique, si h est ample, comme annoncé à la fin de l'introduction.

4.4.3 Remarque finale

Soit $\alpha : G \to \mathrm{Gal}(L/H)$ un problème de plongement fini sur un corps H de dimension finie sur son centre h. Par le lemme 4.3.2, α a une solution géométrique si $\check{\alpha}$ a une solution géométrique $\mathrm{Gal}(e/h(T)) \to G$ avec $e \subseteq \ell((T))$, où ℓ est le centre de L.

La réciproque est fausse en général. En effet, supposons les conditions suivantes vérifiées :
1) h est ample,
2) α possède une solution faible,
3) α n'est pas scindé.
Comme 1) et 2) sont vraies, α a une solution géométrique (voir corollaire 4.4.4). Cependant, supposons que $\check{\alpha}$ possède une solution géométrique $\beta : \mathrm{Gal}(e/h(T)) \to G$ vérifiant $e \subseteq \ell((T))$. Alors 0 n'est pas un point de branchement de $e/\ell(T)$. Puisque 0 n'est pas non plus un point de branchement de $\ell(T)/h(T)$, on en déduit que 0 n'est pas un point de branchement de $e/h(T)$. De plus, le corps résiduel de e en n'importe quel idéal maximal $\mathfrak{P}$ contenant T vaut ℓ. Si $D_{\mathfrak{P}}$ désigne le groupe de décomposition de $e/h(T)$ en l'idéal maximal $\mathfrak{P}$, on a un isomorphisme $\varphi_0 : D_{\mathfrak{P}} \to \mathrm{Gal}(\ell/h)$ défini comme suit. Soit B la clôture intégrale de $h[t]$ dans e et soit $\mathfrak{P}$ un idéal maximal de B contenant T. La réduction modulo $\mathfrak{P}$ de n'importe quel élément x de B est notée $\overline{x}$. On a donc $B/\mathfrak{P} = \ell$ et, pour $\sigma \in D_{\mathfrak{P}}$ et $x \in B$, on pose $\varphi_0(\sigma)(\overline{x}) = \overline{\sigma(x)}$. On vérifie alors facilement que l'on a $\check{\alpha} \circ \beta \circ \varphi_0^{-1} = \mathrm{id}_{\mathrm{Gal}(\ell/h)}$, ce qui contredit 3).

Pour conclure, nous donnons un exemple de problème de plongement fini comme ci-dessus. Considérons le groupe quaternionique Q_8, muni de la présentation $\langle i, j \mid i^4 = 1, i^2 = j^2, jij^{-1} = i^{-1}\rangle$, et le problème de plongement fini $\alpha : Q_8 \to \mathrm{Gal}(\mathbb{Q}((T))(\sqrt{2})/\mathbb{Q}((T)))$ sur le corps ample $\mathbb{Q}((T))$, défini par $\alpha(i)(\sqrt{2}) = -\sqrt{2}$ et $\alpha(j)(\sqrt{2}) = \sqrt{2}$. Puisque Q_8 ne peut s'écrire sous la forme $H_1 \rtimes H_2$, où H_1 et H_2 sont des sous-groupes propres et non triviaux de Q_8, le problème de plongement fini α n'est pas scindé. Cependant, α a une solution faible. En effet, d'après [Ser92, Theorem 1.2.1], $\mathbb{Q}((T))(\sqrt{2+\sqrt{2}})/\mathbb{Q}((T))$ est galoisienne de groupe $\mathbb{Z}/4\mathbb{Z}$ et on

a $\mathbb{Q}((T))(\sqrt{2}) \subseteq \mathbb{Q}((T))(\sqrt{2+\sqrt{2}})$. Si σ est un générateur de $\mathrm{Gal}(\mathbb{Q}((T))(\sqrt{2+\sqrt{2}})/\mathbb{Q}((T)))$, on considère l'isomorphisme $\beta : \mathrm{Gal}(\mathbb{Q}((T))(\sqrt{2+\sqrt{2}})/\mathbb{Q}((T))) \to \langle i \rangle$ défini par $\sigma \mapsto i$. Alors β est une solution faible à α. Enfin, puisque $\mathbb{Q}((T))(\sqrt{2+\sqrt{2}})$ est de niveau infini, $\hat{\beta} : \mathrm{Gal}(H_{\mathbb{Q}((T))(\sqrt{2+\sqrt{2}})}/H_{\mathbb{Q}((T))}) \to Q_8$ est une solution faible au problème de plongement fini $\hat{\alpha} : Q_8 \to \mathrm{Gal}(H_{\mathbb{Q}((T))(\sqrt{2})}/H_{\mathbb{Q}((T))})$ sur le corps des quaternions $H_{\mathbb{Q}((T))}$ à coefficients dans $\mathbb{Q}((T))$ (voir remarque 4.1.6 pour la définition), mais $\hat{\alpha}$ n'est pas scindé.

Bibliographie

[ALP20] Gil Alon, François Legrand, and Elad Paran. Galois groups over rational function fields over skew fields. *Comptes Rendus Mathématique*, 358(7):785–790, 2020.

[BDL20] Angelot Behajaina, Bruno Deschamps, and François Legrand. Problèmes de plongement finis sur les corps non commutatifs. *Manuscript*, 2020. arXiv:2008.08333. A paraître dans Israel Journal of Mathematics.

[Bec91] Sybilla Beckmann. On extensions of number fields obtained by specializing branched coverings. *J. Reine Angew. Math.*, 419:27–53, 1991.

[Beh20] Angelot Behajaina. Réalisations explicites régulières des groupes de quaternions généralisés. *J. Théor. Nombres Bordeaux*, 32(2):605–630, 2020.

[Beh21] Angelot Behajaina. Théorie inverse de Galois sur les corps des fractions rationnelles tordus. (French). *Journal of Pure and Applied Algebra.*, 224(106549), 2021.

[Bla72] André Blanchard. *Les corps non commutatifs. (French).* Collection Sup : Le Mathématicien, No. 9. Presses Universitaires de France, Vendôme, 1972. 135 pp.

[Bou12] Nicolas Bourbaki. *Éléments de mathématique. Algèbre. Chapitre 8. Modules et anneaux semi-simples. (French).* Springer, Berlin, 2012. x+489 pp. Second revised version of the 1958 edition.

[BSF13] Lior Bary-Soroker and Arno Fehm. Open problems in the theory of ample fields. In *Geometric and differential Galois theories*, volume 27 of *Sémin. Congr.*, pages 1–11. Soc. Math. France, Paris, 2013.

[Coh95] Paul Moritz Cohn. *Skew fields. Theory of general division rings.* Encyclopedia of Mathematics and its Applications, 57. Cambridge University Press, Cambridge, 1995. xvi+500 pp.

[DD97] Pierre Dèbes and Bruno Deschamps. The regular inverse Galois problem over large fields. In *Geometric Galois actions, 2*, volume 243 of *London Math. Soc. Lecture Note Ser.*, pages 119–138. Cambridge Univ. Press, Cambridge, 1997.

[DD04] Pierre Dèbes and Bruno Deschamps. Corps ψ-libres et théorie inverse de Galois infinie. (French). *J. Reine Angew. Math.*, 574:197–218, 2004.

[Dèb09] Pierre Dèbes. *Arithmétique des revêtements de la droite.* Lecture notes, 2009. At http://math.univ-lille1.fr/~pde/ens.html.

[Des11] Bruno Deschamps. *Une introduction au groupe de Brauer.* Lecture notes, 2011.

[Des15] Bruno Deschamps. Minimalité et abyssalité des extensions abéliennes et projectives de $\mathbb{Q}$. (French). *J. Algebra*, 441:1–20, 2015.

[Des18] Bruno Deschamps. Des extensions plus petites que leurs groupes de Galois. (French). *Comm. Algebra*, 46(10):4555–4560, 2018.

[DG12] Pierre Dèbes and Nour Ghazi. Galois covers and the Hilbert–Grunwald property. *Ann. Inst. Fourier (Grenoble)*, 62(3):989–1013, 2012.

[DL13] Pierre Dèbes and François Legrand. Specialization results in Galois theory. *Trans. Amer. Math. Soc.*, 365(10):5259–5275, 2013.

[DL20] Bruno Deschamps and François Legrand. Le problème inverse de Galois sur les corps des fractions tordus à indéterminée centrale. (French). *Journal of Pure and Applied Algebra.*, 224(106240), 2020.

[Ehr11] Gertrude Ehrlich. *Fundamental Concepts of Abstract Algebra.* Dover Books on Mathematics. Dover Publications, 2011.

[FJ08] Michael D. Fried and Moshe Jarden. *Field arithmetic.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 11. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden. xxiv+792 pp.

[Fri74] Michael D. Fried. On Hilbert's irreducibility theorem. *J. Number Theory*, 6:211–231, 1974.

[Fri77] Michael D. Fried. Fields of definition of function fields and Hurwitz families-groups as Galois groups. *Comm. Algebra*, 5(1):17–82, 1977.

[GW04] Kenneth R. Goodearl and Jr. Warfield, Robert Breckenridge. *An Introduction to noncommutative Noetherian rings.* London Mathematical Society Student Texts, 61. Cambridge University Press, Cambridge, 2004. Second edition. xxiv+344 pp.

[HJ98] Dan Haran and Moshe Jarden. Regular split embeddings problems over function fields of one variable over ample fields. *J. Algebra*, 208(1):147–164, 1998.

[HS05] David Harbater and Katherine F. Stevenson. Local Galois theory in dimension two. *Adv. Math.*, 198(2):623–653, 2005.

[Jac56] Nathan Jacobson. *Structure of rings.* American mathematical society colloquium publications, 1956.

[Jar11] Moshe Jarden. *Algebraic patching.* Springer Monographs in Mathematics. Springer, Heidelberg, 2011. xxiv + 290 pp.

[JLY02] Christian U. Jensen, Arne Ledet, and Noriko Yui. *Generic polynomials. Constructive Aspects of the Inverse Galois Problem.* Mathematical Sciences Research Institute Publications, 45. Cambridge University Press, 2002. x+258 pp.

[Koe04] Jochen Koenigsmann. The regular inverse Galois problem over non-large fields. *J. Eur. Math. Soc. (JEMS)*, 6(4):425–434, 2004.

[Lam05] Tsit Yuen Lam. *Introduction to quadratic forms over fields.* Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005. xxii+550 pp.

[Leg16] François Legrand. Specialization results and ramification conditions. *Israel J. Math.*, 214(2):621–650, 2016.

[MM18] Gunter Malle and B. Heinrich Matzat. *Inverse Galois theory.* Springer Monographs in Mathematics. Springer, Berlin, 2018. Second edition. xvii+532 pp.

[MS92] Dominique Martinais and Leila Schneps. Polynômes à groupe de Galois diédral. (French). *Sém. Théor. Nombres Bordeaux (2)*, 4(1):141–153, 1992.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der mathematischen Wissenschaften [Fundamental*

Principles of Mathematical Sciences]. Springer-Verlag, Berlin, second edition, 2008. xvi+825 pp.

[Ore33] Oystein Ore. Theory of non-commutative polynomials. *Ann. of Math. (2)*, 34(3):480–508, 1933.

[Par09] Elad Paran. Split embedding problems over complete domains. *Ann. of Math. (2)*, 170(2):899–914, 2009.

[Pop96] Florian Pop. Embedding problems over large fields. *Ann. of Math. (2)*, 144(1):1–34, 1996.

[Pop14] Florian Pop. Little survey on large fields - old & new. In *Valuation theory in interaction*, EMS Ser. Congr. Rep., pages 432–463. Eur. Math. Soc., Zürich, 2014.

[Sch00] Andrzej Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2000. With an appendix by Umberto Zannier. x+558 pp.

[Ser92] Jean-Pierre Serre. *Topics in Galois Theory*, volume 1 of *Research Notes in Mathematics*. Jones and Bartlett Publishers, Boston, MA, 1992. Lecture notes prepared by Henri Darmon [Henri Darmon]. With a foreword by Darmon and the author. xvi+117 pp.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009. xiv+355 pp.

[Völ96] Helmut Völklein. *Groups as Galois groups. An introduction*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996. xviii+248 pp.

[Wei09] Steven Weintraub. *Galois Theory*. Universitext. Springer, 2009.

[Zyw15] David Zywina. The inverse Galois problem for $\mathrm{PSL}_2(\mathbb{F}_p)$. *Duke Math. J.*, 164(12):2253–2292, 2015.