Université des sciences et technologies de Lille

Thèse de doctorat de mathématiques

Aspects de la Théorie Inverse de Galois

soutenue le 25 juin 1997 par

Bruno DESCHAMPS

Membres du Jury:
Pierre Dèbes (directeur de thèse, université Lille I)
Jean-Claude Douai (université Lille I)
Michel Emsalem (université Lille I)
Michael Fried (université de Californie, Irvine USA)
David Harbater (université de Pensylvanie, Philadelphie USA)
Michel Waldschmidt (université Paris VI)

Rapporteurs:
Michael Fried (université de Californie, Irvine USA)
David Harbater (université de Pensylvanie, Philadelphie USA)

Aspects de la Théorie Inverse de Galois

Bruno DESCHAMPS

A mon oncle Jacques,
à sa mémoire.

Table des matières

Chapitre 1

Introduction

1.1 De Lascaux au testament d'Evariste Galois

Il est fort probable que le premier effort intellectuel de l'humanité ait eu à voir avec les mathématiques. L'aperception des nombres entiers naturels a du être une nécessité pour la création des premières communautés. Il fallait bien faire la correspondance entre le *nombre*, objet concret (1 bison, 2 mammouths etc.), et le *nombre*, objet abstrait (je vois 2 bisons et j'ai 2 flêches dans les mains pour les tuer). Une fois accepté le fait que dans la relation entre 2 mammouths et 2 peintures de mammouth il existait un lien qui dépasse le simple mammouth, l'arithmétique pouvait naître. Je suis un chasseur cro-magnon, j'ai 10 femmes et 50 enfants, sachant qu'avec un auroch je peux nourrir 20 personnes, combien dois-je en tuer pour le déjeuner? (Notons que le problème se complique si je chasse en même temps plusieurs espèces différentes qui ne représentent pas la même quantité de nourriture...) Additionner, soustraire, multiplier, diviser, sont donc visiblement des concepts premiers de l'intelligence.

Les grecs s'intéressaient déjà à la notion de quantité proportionnelle dans leurs considérations géométriques (théorème de Thalès, etc.), c'est à dire finalement à $\mathbb{Q}$. A cette époque où la philosophie imposait à l'homme l'idée d'une nature ordonnée et *rationnelle* dans sa structure profonde, on admettait mal que la longueur de l'hypothénuse d'un triangle rectangle dessinée sur le sable ne soit pas toujours un nombre rationnel. Pourtant le théorème de Pythagore est formel! Cette idée que l'on ne puisse pas "attraper" certaines quantités "naturelles" par les simples opérations arithmétiques sur $\mathbb{Q}$ est à relier à la notion de polynôme ($x^2 + y^2 = z^2$, intersections de cercles et de droites). Diophante et ses congénères seraient à l'origine de ce genre de considération. Il existe dans la nature des quantités qui bien que n'étant pas rationnelles, peuvent être obtenues à partir de quantités rationnelles: Les polynômes sont construits grâce à la simple arithmétique sur $\mathbb{Q}$, mais leurs racines dépassent parfois cet ensemble. Par exemple $\sqrt{2}$ (qui n'est pas rationnel) représente la longueur de l'hypothénuse d'un triangle rectangle isocèle de côté 1, c'est à dire, d'après le théorème de pythagore, une racine du polynôme $X^2 - 2$.

La recherche de racines de polynômes allait devenir une obsession frustrante, comme en atteste les travaux des algébristes arabes et européens du moyen-age. Dès la renaissance, on savait "résoudre" les équations de degré $1, 2, 3, 4$ (méthode de Cardan et Ferrari). On se heurta pendant des siècles au rang 5. Et pour cause puisqu'il fallut attendre le XIX^e siècle avec Galois pour montrer que ce n'était pas possible pour les rangs plus grand que 4.

La théorie de Galois allait révolutionner les mathématiques à jamais. Certains attribuent à Galois l'invention de la notion de groupes voire de l'algèbre moderne. En tous cas, il est vrai qu'il est difficile de travailler maintenant dans un domaine mathématique sans entendre parler de groupe de Galois! Avec Galois l'arithmétique allait prendre une nouvelle dimension: on n'allait plus étudier les opérations élémentaires uniquement sur $\mathbb{Q}$, mais sur toute extension finie de $\mathbb{Q}$. L'arithmétique des corps allait alors se développer sur cette idée de correspondance entre racines de polynômes, extensions de corps et automorphismes. Je sais "trouver" les racines d'un polynôme irréductible à condition que ce polynôme engendre une extension galoisienne de $\mathbb{Q}$ ayant un groupe de Galois résoluble. D'où la nécessité d'étudier plus précisement les groupes finis et en particulier de savoir ceux qui ont une chance d'être groupe de Galois sur $\mathbb{Q}$. La théorie inverse de Galois allait naître...

1.2 Aspects de la théorie inverse de Galois

Nous présentons dans cette thèse des travaux concernant certains aspects de la théorie inverse de Galois. On pourrait résumer l'objet de cette théorie à l'étude des deux questions suivantes: 1/ Etant donné un corps K, pouvons-nous décrire les groupes finis qui apparaissent comme groupes de Galois d'extensions galoisiennes finies de K? 2/ Etant donné un corps K, pouvons-nous décrire la structure algébrique du *groupe de Galois absolu* de K (i.e. le groupe de Galois $Gal(K^{sep}/K)$, de l'extension K^{sep}/K où K^{sep} désigne la clôture séparable de K)? La deuxième question, qui semble à priori la plus difficile (puisque la simple description des quotients finis d'un groupe profini ne suffit généralement pas à en donner l'exacte structure), admet dans certain cas une réponse affirmative. Ceci permet alors de répondre à la première question, qui semblait, de prime abord, très compliquée. Bien évidemment, beaucoup d'autres questions connexes se posent à ce sujet, soulignant l'extrême richesse de l'arithmétique des corps. Chaque chapitre de ce travail correspond, à peu de choses près, à un article ([DebDes], [Des2], [Des3]).

Le premier, rédigé en collaboration avec mon directeur de thèse Pierre Dèbes, présente les conjectures modernes liées au problème inverse. La plus célèbre est la suivante: Etant donné un corps K quelconque, tout groupe fini est groupe de Galois d'une extension *régulière* de $K(T)$ (i.e. une extension $L/K(T)$ telle que $\overline{K} \cap L = K$)? Cette conjecture s'appelle le problème inverse de Galois régulier. L'intérêt premier de cette conjecture est qu'elle permet de considérer le problème sous un angle géométrique. En effet, à une telle extension $L/K(T)$, on peut naturellement associer un revêtement galoisien de la droite projective, défini sur K. Face à cette conjecture, existent d'autres conjectures liées à des problèmes de plongement pour le groupe de Galois absolu de $K(T)$, qui ont à terme pour conséquences de décrire efficacement ce groupe. D'un point de vue logique, il n'existe pas de connections évidentes entre toutes ces conjectures. Nous présentons donc une (méta-)conjecture due à P.Dèbes (et à F.Pop indépendamment) qui a pour objectif d'unifier toutes ces questions et leurs conséquences. Pour résumer, on peut dire que cette conjecture étudie les extensions galoisiennes finies de $K(T)$ en précisant ce qui se passe sur $\overline{K}(T)$. Nous indiquons comment les conjectures se positionnent entre elles et on introduit dans ce chapitre la notion récente de corps amples, notion due à Florian Pop. L'omniprésence des méthodes géométriques, souligne la nécessité de se placer dans un cadre plus général pour aborder efficacement ces problèmes. Le nécessaire emploi de techniques nouvelles en montre aussi l'extrême complexité. Le résultat le plus significatif de ce chapitre est

que le problème inverse de Galois régulier sur $K(T)$ est vrai, pourvu que K soit un corps ample. Ce résultat est dû à F.Pop, nous en donnons une démonstration. En fait, Pop a prouvé que la conjecture principale de ce chapitre est vraie si K est un corps ample. Nous montrons alors comment la plupart des résultats récents de théorie inverse de Galois peuvent être retrouvés à partir de ce résultat.

Le deuxième chapitre se place dans le cadre de la théorie des espaces de modules de revêtements (espaces de Hurwitz). Cette théorie, introduite par Michael Fried pour l'étude du problème inverse, a montré son efficacité en s'appliquant à d'autres problèmes diophantiens (problème de Hilbert-Siegel, problème de Davenport [Deb4]). Grâce aux travaux de M.Fried et H.Völklein, on sait que la réalisation d'un groupe fini G donné, comme groupe de Galois d'une extension régulière de $\mathbb{Q}(T)$, se ramène à l'existence d'un point $\mathbb{Q}$-rationnel sur une certaine variété irréductible, lisse et définie sur $\mathbb{Q}$. Nous nous sommes intéressés à l'existence de points rationnels sur ces espaces. Nous montrons en fait que pour tout groupe fini G, il existe une variété (en fait une infinité) vérifiant les propriétés précédemment énoncées et possédant des points $\mathbb{Q}_p$-rationnels pour tout premier p. Ce résultat est aussi présenté, de façon un peu moins précise, comme corollaire de l'étude du problème régulier dans le premier chapitre. On est alors amené à considérer un problème local-global, type problème de Hasse: si sur une variété, il existe des points p-adiques pour tout p, en existe-t-il un rationnel? Une réponse affirmative résoudrait alors le problème inverse de Galois régulier. Hélas, il est célèbre que le problème de Hasse est faux dans le cadre général, même quand les variétés considérées sont des espaces de Hurwitz. Chronologiquement parlant, l'article qui correspond au deuxième chapitre est antérieur à celui qui correspond au premier chapitre. Dans un souci de clarté nous avons inversé dans cette thèse cet ordre en estimant que le premier chapitre avait un caractère plus général que le second.

Dans le troisième chapitre, nous avons voulu appliquer la théorie d'Artin et Schreier pour généraliser la construction et l'étude du corps $\mathbb{Q}^{tr}$ des nombres algébriques totalement réels. L'idée a été d'utiliser les méthodes et les résultats que nous présentons précédemment, notament ceux du premier chapitre. Essentiellement, on y utilise des résultats d'arithmétique sur les corps hilbertiens, PAC ou amples. On introduit dans cette partie la notion de clôture totalement réelle d'un corps ordonnable et l'on regarde la structure de son groupe de Galois absolu. La clôture totalement réelle d'un corps ordonnable K est le corps $\widetilde{K_{tr}}$ obtenu en prenant l'intersection de toutes les extensions algébriques ordonnées maximales de K. Dans tous les exemples dont nous disposons, le groupe de Galois absolu du corps $\widetilde{K_{tr}}(\sqrt{-1})$ (ce dernier corps est en fait la clôture cyclotomique de $\widetilde{K_{tr}}$) est pro-libre (de rang variable). D.Haran et M.Jarden ont apporté d'autres exemples allant dans ce sens. Nous conjecturions qu'il en était toujours ainsi, mais D.Haran et M.Jarden ont aussi donné un contre exemple à cette propriété. Ils proposent maintenant d'étudier la conjecture dans le cas où K est ordonnable, dénombrable et hilbertien. Nous nous intéressons aussi à la structure du groupe de Brauer de $\widetilde{K_{tr}}$. Nous montrons par exemple que le groupe de Brauer de $\mathbb{Q}^{tr}$ est isomorphe à $\varinjlim_{n\in\mathbb{N}} (\mathbb{Z}/2)^n$. Nous montrons aussi ce curieux résultat: si K est une extension ordonnable et algébrique de $\mathbb{Q}$ alors pour que $Br(\widetilde{K_{tr}})$ soit égal à $\mathbb{Z}/2$, il faut et il suffit que le groupe de Klein $G = \mathbb{Z}/2 \times \mathbb{Z}/2$ ne soit pas groupe de Galois sur $\widetilde{K_{tr}}$. Ce travail s'inscrit dans le cadre de l'étude des corps ordonnés et de la connection de cette théorie avec la théorie inverse de Galois.

Enfin nous présentons deux appendices. Le premier tente d'appréhender sous plusieurs formes le problème inverse de Galois. Il représente un complément à cette introduction.

Nous avons tenté de donner des exemples variés, parfois pathologiques touchant à la théorie inverse de Galois. Le deuxième introduit la notion de corps P-réduisant et veut généraliser la notion de corps pythagoricien dont nous parlons dans le troisième chapitre. C'est donc un complément de ce chapitre et des notions qui y sont évoquées.

1.3 Remerciements

Je voudrais remercier l'ensemble des membres du jury pour avoir accepté de participer à la soutenance de ma thèse. Plus spécialement, merci à David Harbater et à Mike Fried, les rapporteurs de cette thèse, d'avoir pris sur leur précieux temps pour effectuer ce travail.

Merci à celui sans qui tout ceci n'aurait jamais vu le jour. Merci pour ses conseils, ses enseignements et sa connaissance. Toujours prêt à m'écouter et à me soutenir, il était là quand tout allait bien et surtout quand tout n'allait pas forcement bien! C'est à son contact que j'ai appris le métier de la recherche. Je lui dois bien plus que les connaissances mathématiques qu'il m'a transmises, mais ces quelques lignes ne suffiraient pas à lui exprimer toute ma reconnaissance. Merci à vous, Pierre.

Chapitre 2

Problème inverse de Galois régulier sur les corps amples

2.1 Introduction

La plupart des résultats récents en théorie inverse de Galois concerne la structure du groupe de Galois absolu de $K(T)$, $G_{K(T)}$, quand K est un corps possédant certaines "bonnes" propriétés arithmétiques. Ce chapitre présente un aperçu de ces progrès récents. Notre but est aussi d'essayer d'unifier les questions et résultats qui ont émergé ces dernières années dans ce domaine.

Historiquement, le *Problème Inverse de Galois* (PIG) est le suivant: est-ce que tout groupe fini est groupe de Galois d'une extension galoisienne de $\mathbb{Q}$? L'approche moderne de ce problème consiste plutôt en l'étude du *Problème Inverse de Galois Régulier* (PIGR): est-ce que tout groupe fini est groupe de Galois d'une extension galoisienne $E/\mathbb{Q}(T)$ avec $E/\mathbb{Q}$ extension régulière? (on dit plus rapidement que $E/\mathbb{Q}(T)$ est régulière). Régulière signifie que $E \cap \overline{\mathbb{Q}} = \mathbb{Q}$, ou de façon équivalente que $Gal(E/\mathbb{Q}(T)) = Gal(E\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T))$. Voici trois raisons pour lesquelles il est plus naturel de considérer ce problème:

(1) Une réponse positive au (PIGR) implique une réponse positive au (PIG). Ceci résulte classiquement du théorème d'irréductibilité d'Hilbert.

(2) Les extensions galoisiennes régulières de $\mathbb{Q}(T)$ correspondent aux revêtements galoisiens de $\mathbb{P}^1$ définis sur $\mathbb{Q}$ avec leurs automorphismes. De là, le (PIGR) se ramène à l'étude de l'action de $G_{\mathbb{Q}}$ sur la droite projective. Ceci renforce le sentiment général qui consiste à penser que l'action de $G_{\mathbb{Q}}$ sur certains objets géométriques est susceptible de très bien décrire sa structure.

(3) Le (PIGR) peut être reformulé plus généralement pour n'importe quel corps K (éventuellement de caractéristique > 0). Etant donné un corps K, tout groupe fini pourrait bien être groupe de Galois d'une extension galoisienne régulière de $K(T)$: aucun contre exemple n'est connu à ce jour. Au contraire du (PIG), le (PIGR) pourrait bien ne pas dépendre du corps de base, mais uniquement de propriétés universelles du corps $K(T)$.

En raison de la propriété de régularité, résoudre le (PIGR) (dans le sens positif) sur un corps donné, résoud ce même problème sur tout surcorps. Ainsi, il est suffisant de résoudre le (PIGR) sur tous les corps premiers Q. Le (PIGR) a été résolu sur tout corps algébriquement clos: le réel problème est de "descendre" de $\overline{Q}$ à Q. En résumant, il y a alors deux

directions de travail. Les théoriciens des groupes fixent un groupe fini et essayent de le réaliser sur $Q(T)$ de façon régulière (i.e., comme groupe de Galois d'une extension galoisienne régulière de $Q(T)$). Grâce au critère dit de rigidité et à ses développements, il y a eu depuis les années 70 beaucoup de résultats dans cette direction notamment en ce qui concerne les groupes simples. Nous renvoyons le lecteur aux travaux de Matzat ([Mat],[MatMa]) et de ses étudiants pour cet aspect de la question (voir aussi [Deb1]). D'un autre côté, les géomètres arithméticiens essayent de réaliser de façon régulière tous les groupes finis sur $K(T)$ avec K une extension algébrique (aussi petite que possible) de Q. Il y a eu, encore plus récemment, des progrès significatifs dans cette direction. Nous nous focaliserons sur ce deuxième aspect du problème, qui fut développé en particulier par Fried, Harbater et Pop. Bien entendu, cette distinction est quelque part artificielle en ce sens que dans la pratique, il y a une forte interaction entre les théoriciens des groupes et les arithméticiens.

En simplifiant, la majeure partie de ces progrès récents peuvent se résumer en disant que le (PIGR) est résolu quand le corps de base K est "large". Par large nous entendons la propriété précise suivante, introduite par Pop: toute courbe géométrique, lisse et irréductible définie sur K a une infinité de points K-rationnels pourvu qu'elle en ait au moins un. Nous étudierons plus précisément cette propriété dans le paragraphe 2.3.1 de ce chapitre. Haran et Jarden appellent cette propriété "ample" dans [HaJa1], ce qui exprime une certaine tendance qu'ont ces corps à développer abondamment le nombre de points sur une variété. Nous utiliserons ici cette terminologie.

Le résultat précédent ne rend pas compte d'une seconde série de résultats du même esprit. De même, le (PIGR) n'inclut pas une seconde série de conjectures classiques du domaine. Ces résultats et conjectures donnent ou prédisent, sous certaines conditions, la structure exacte de certains groupes de Galois absolus. Historiquement, le problème de départ de ce second cercle de questions est la conjecture de Shafarevich: le groupe de Galois absolu, $G_{Q^{ab}}$, de $\mathbb{Q}^{ab}$ est pro-libre de rang dénombrable.

Ces deux cercles d'idées sont intimement liés. Les méthodes abordées utilisent les mêmes types de techniques, à savoir des procédés de découpage et recollement de revêtements analytiques et des arguments de spécialisation pour les corps amples. Notre sentiment était que la connection entre ces deux cercles n'avait jamais été établie clairement et totalement. L'objectif de ce chapitre est:

(1) établir une conjecture qui unifie toutes les questions classiques. C'est la conjecture principale du chapitre. Dans la première partie, nous l'énonçons et décrivons comment elle se connecte avec les autres.

(2) d'énoncer un théorème qui résume la plupart des résultats récents dans le domaine. C'est le théorème principal, il assure que la conjecture principale est vraie dans le cas où le corps de base est ample. Ceci contient le fait que le (PIGR) est vrai si K est ample. Le théorème principal est énoncé dans le paragraphe 2.3.2 où nous montrons comment on peut en déduire, comme cas particulier, la plupart des résultats récents. Une preuve générale du théorème principal a été donnée par Pop [Pop4].

(3) d'expliquer l'argument central de la preuve du théorème principal. Pour une question de simplicité, nous nous restreindrons à la solution du (PIGR) sur un corps ample.

2.2 Conjectures

2.2.1 Conjectures classiques

Premier cercle de conjectures

Nous rappellons ici, comme dans l'introduction, un certain nombre de conjectures tournant autour du problème inverse de Galois. Comme d'habitude, pour un corps K donné, nous noterons K_s (resp. $\overline{K}$) la clôture séparable (resp. algébrique) de K et G_K le groupe de galois absolu, $Gal(K_s/K)$, de K.

Conjecture 2.2.1 ($\mathbf{PIGR}/_{K(T)}$) *Pour tout corps K et tout groupe fini G, il existe une extension galoisienne régulière $E_G/K(T)$ telle que $Gal(E_G/K(T)) = G$.*

Conjecture 2.2.2 ($\mathbf{PIG}/_{K\ hilb}$) *Pour tout corps K hilbertien et tout groupe fini G, il existe une extension galoisienne E_G/K telle que $Gal(E_G/K) = G$. De façon équivalente, tout groupe fini est un quotient de G_K.*

Conjecture 2.2.3 (**PIG**) *Pour tout groupe fini G, il existe une extension galoisienne $E_G/\mathbb{Q}$ telle que $Gal(E_G/\mathbb{Q}) = G$.*

On a: $$(\mathbf{PIGR}/_{K(T)}) \Longrightarrow (\mathbf{PIG}/_{K\ hilb}) \Longrightarrow (\mathbf{PIG})$$

Preuve: En effet, il vient de la propriété d'Hilbert que, si $E_T/K(T)$ est une extension galoisienne régulière de groupe de Galois G, alors il existe une spécialisation $t \in K$ de T telle que l'extension "spécialisée" E_t/K soit galoisienne de groupe de Galois G. De là $(\mathbf{PIGR}/_{K(T)}) \Longrightarrow (\mathbf{PIG}/_{K\ hilb})$. Le théorème d'irréductibilité de Hilbert dit que $\mathbb{Q}$ est hilbertien. Donc $(\mathbf{PIG}/_{K\ hilb}) \Longrightarrow (\mathbf{PIG})$. □

Second cercle de conjectures

Le second cercle de conjectures concerne les problèmes de plongements. Rappelons qu'un *problème de plongement* pour un groupe Γ est un diagramme d'homomorphismes de groupes

$$\begin{array}{ccccccccc} & & & & & & \Gamma & & \\ & & & & & & \downarrow f & & \\ 1 & \longrightarrow & N & \longrightarrow & G & \xrightarrow{\alpha} & H & \longrightarrow & 1 \end{array}$$

où la ligne horizontale est une suite exacte et l'application $f : \Gamma \to H$ est un homomorphisme surjectif. Une *solution forte* est un homomorphisme surjectif $g : \Gamma \to G$ tel que $\alpha g = f$. Sans la condition "g surjective", un tel homomorphisme est appellé *solution faible*. Le problème de plongement est dit *fini* si G est fini. Il est dit *scindé* si $\alpha : G \to H$ possède une section.

Un groupe profini Γ est dit *projectif* si tout problème de plongement pour Γ admet une solution faible. Notons que dans le cas où Γ désigne le groupe de Galois absolu d'un corps K, il y a équivalence entre Γ projectif et $cd(K) \leq 1$ ([Ser3]). Les groupes

pro-libres sont un exemple de groupes projectifs. Enfin, rappelons que, étant donné une solution faible à un problème de plongement pour Γ, il existe une procédure standard qui de manière générale ramène le problème de plongement de départ à un problème de plongement scindé. De manière plus précise, cette procédure (e.g. [Po4,§1 B) 2)]) utilise une solution faible pour construire un problème de plongement scindé pour Γ tel que l'existence d'une solution forte pour ce deuxième problème de plongement implique l'existence d'une solution forte pour le problème de départ. Nous utiliserons ce procédé à plusieurs reprises. Par commodité, nous l'appelerons la réduction *faible* $\rightarrow$ *scindé.*

Conjecture 2.2.4 (Fried-Völklein [FrVo2]) *Soit K un corps hilbertien et dénombrable tel que G_K soit projectif, alors G_K est pro-libre.*

Conjecture 2.2.5 (Shafarevich) *$G_{\mathbb{Q}^{ab}}$ est pro-libre.*

Ces conjectures sont plus ou moins classiques. Nous les noterons respectivement **(FrVo)** et **(SHA)**. La seconde est en fait un cas particulier de la première. En effet, d'après un résultat de Kuyk, $\mathbb{Q}^{ab}$ est hilbertien, voir [FrJa, Th.15.6]; et $\mathbb{Q}^{ab}$ est de dimension cohomologique ≤ 1 (voir [CaFr]). De même, **(FrVo)** est une conséquence des deux conjectures équivalentes suivantes:

Conjecture 2.2.6 (Split EP/$_{K(T)}$) *Soit K un corps quelconque. Tout problème de plongement scindé pour $G_{K(T)}$ possède une solution forte.*

Conjecture 2.2.7 (Split EP/$_{K\ hilb}$) *Soit K un corps hilbertien. Tout problème de plongement scindé pour G_K possède une solution forte.*

Nous appelerons ces conjectures, *conjectures des problèmes de plongements scindés* sur $K(T)$ (resp. sur les corps hilbertiens). On a:

$$\textbf{(Split EP/}_{K(T)}\textbf{)} \Longleftrightarrow \textbf{(Split EP/}_{K\ hilb}\textbf{)} \Longrightarrow \textbf{(FrVo)} \Longrightarrow \textbf{(SHA)}$$

Preuve de (Split EP/$_{K(T)}$) $\Leftrightarrow$ (Split EP/$_{K\ hilb}$): ($\Leftarrow$) vient du fait que pour tout corps K, le corps $K(T)$ est hilbertien [FrJa; Th.12.10].
($\Rightarrow$): Soit un problème de plongement scindé pour G_K avec K un corps hilbertien. Considérons le problème de plongement pour $G_{K(T)}$ obtenu par composition avec l'application naturelle $G_{K(T)} \rightarrow G_K$. La conjecture **(Split EP/$_{K(T)}$)** donne une solution forte à ce problème. Alors, comme dans la preuve de **(PIGR/$_{K(T)}$)** $\Rightarrow$**(PIG/$_{K\ hilb}$)**, on utilise l'hypothèse K *hilbertien* pour spécialiser cette solution forte en une solution forte du problème de départ pour G_K. □

Preuve de (Split EP/$_{K\ hilb}$) $\Rightarrow$ (FrVo): Nous allons montrer que tout problème de plongement pour G_K a une solution forte. La conclusion "G_K pro-libre" viendra alors du théorème d'Iwasawa rappelé ci-après. Comme G_K est supposé être projectif, un problème de plongement a toujours une solution faible. Grâce à la réduction faible $\rightarrow$ scindé, on peut supposer que le problème de plongement est scindé. De là, grâce à la conjecture **(Split EP/$_{K\ hilb}$)**, ces problèmes de plongements ont tous une solution forte. □

Théorème 2.2.1 (Iwasawa [Iw], [FrJa; Cor.24.2]) *Soit K un corps dénombrable, G_K est pro-libre ssi tout problème de plongement fini pour G_K a une solution forte.*

Conclusion

Pour finir, notons que l'on a (**Split EP**$/_{K\ hilb}$) $\Rightarrow$ (**PIG**$/_{K\ hilb}$). En effet, pour réaliser le groupe G comme groupe de Galois sur K il suffit de trouver une solution forte au problème de plongement pour G_K (visiblement scindé) dans lequel la suite exacte est $1 \to G \to G \to 1 \to 1$. Le diagramme suivant résume ce paragraphe:

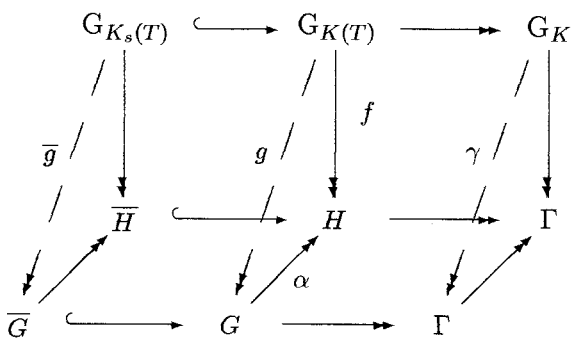
$$\begin{array}{ccccccc} \textbf{PIGR}/_{K(T)} & \Longrightarrow & \textbf{PIG}/_{K\ hilb.} & \Longrightarrow & \textbf{PIG} \\ & & \Uparrow & & \\ \textbf{Split EP}/_{K(T)} & \Longleftrightarrow & \textbf{Split EP}/_{K\ hilb.} & \Longrightarrow & \textbf{FrV} & \Longrightarrow & \textbf{SHA} \end{array}$$

Remarque 1: Les conjectures du deuxième cercle semblent être plus fortes en ce qu'elles donnent des résultats sur la structure des groupes de Galois absolu alors que celles du premier cercle parlent seulement des quotients finis de ces groupes de Galois absolus. Pourtant, il n'existe pas de lien logique évident, excepté (**Split EP**$/_{K\ hilb}$) $\Rightarrow$ (**PIG**$/_{K\ hilb}$), entre ces deux cercles. Par exemple, il n'existe pas de lien entre (**FrVo**) et (**PIG**)[1], de même qu'il n'existe pas de lien entre (**Split EP**$/_{K(T)}$) et (**PIGR**$/_{K(T)}$). L'objectif du prochain paragraphe est d'établir une conjecture plus générale qui unifiera ces deux cercles de conjectures. La différence entre les deux conjectures (**Split EP**$/_{K(T)}$) et (**PIGR**$/_{K(T)}$) deviendra alors plus claire (voir remarque 3).

2.2.2 Conjecture principale

Enoncé de la conjecture principale

Supposons donné un diagramme commutatif de groupes



où les trois lignes sont exactes et les flêches $\hookrightarrow$ (resp. $\twoheadrightarrow$) représentent des homomorphismes injectifs (resp. surjectifs). Un tel diagramme est appellé *problème de plongement pour suites exactes de* $K(T)$. Une solution forte est un triplet $(\overline{g}, g, \gamma)$ d'homomorphismes surjectifs (flêches en pointillés du diagramme précédent) faisant commuter le diagramme. Si l'on enlève la condition surjective, le triplet $(\overline{g}, g, \gamma)$ est appellé solution faible.

[1]Le point à remarquer est que $G_{\mathbb{Q}}$ n'est pas projectif, car il possède des éléments d'ordre 2. Ainsi (**FrVo**) ne peut pas être directement appliqué à $G_{\mathbb{Q}}$.

Conjecture 2.2.8 *(Conjecture Principale) Soit K un corps quelconque. Tout problème de plongement pour suites exactes de $K(T)$ ayant une solution faible a une solution forte.*

Remarques 2:

(a) Les solutions faibles $(\overline{g}, g, \gamma)$ correspondent en fait de façon biunivoque aux applications $g : G_{K(T)} \to G$ telles que $\alpha g = f$. En effet, étant donné g prenons pour $\overline{g}$ la restriction de g à $G_{K_s(T)}$. On a bien l'inclusion $g(G_{K_s(T)}) \subset \overline{G}$, car les deux groupes de droite du diagramme (sur les lignes) sont égaux à Γ. Par conséquent, il existe un unique γ faisant commuter le diagramme. Le triplet $(\overline{g}, g, \gamma)$ est donc une solution faible.

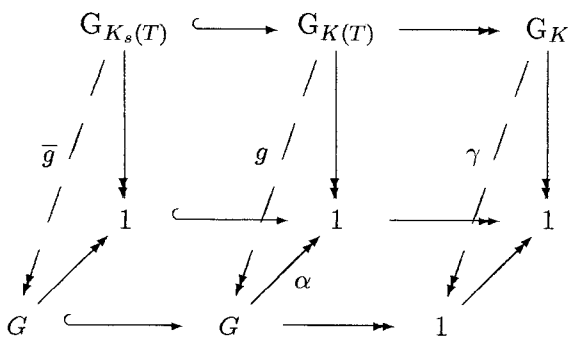
(b) Nous dirons que le problème de plongement pour suite exacte de $K(T)$ est scindé si l'application α admet une section. Dans ce cas, le problème admet une solution faible. Réciproquement, si un problème de plongement pour suite exacte de $K(T)$ admet une solution faible, alors il existe un problème de plongement pour suite exacte de $K(T)$ scindé pour lequel l'existence d'une solution forte implique l'existence d'une solution forte au problème de départ. En effet, l'argument de réduction faible $\to$ scindé, se généralise sans difficulté dans notre situation. Ainsi, dans la conjecture principale, on peut remplacer l'hypothèse "existence d'une solution faible" par "problème de plongement pour suite exacte de $K(T)$ scindé".

Relations avec les autres conjectures

La conjecture principale contient celles exposées dans le paragraphe 2.2.1. En résumé, on a:

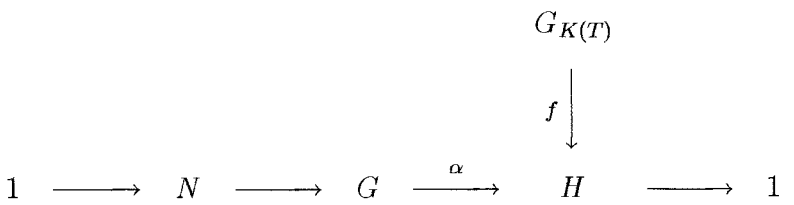
$$\begin{array}{lccccccc} & \Longrightarrow & \textbf{PIGR}/_{K(T)} & \Longrightarrow & \textbf{PIG}/_{K\ hilb.} & \Longrightarrow & \textbf{PIG} & \\ \textbf{Conj. Prin.} & & & & \Uparrow & & & \\ & \Longrightarrow & \textbf{Split EP}/_{K(T)} & \Longleftrightarrow & \textbf{Split EP}/_{K\ hilb.} & \Longrightarrow & \textbf{FrVo} & \Longrightarrow \quad \textbf{SHA} \end{array}$$

Preuve de Conj. Prin. $\Rightarrow$ PIGR$/_{K(T)}$: D'après la conjecture principale, le problème de plongement pour suite exacte de $K(T)$ suivant

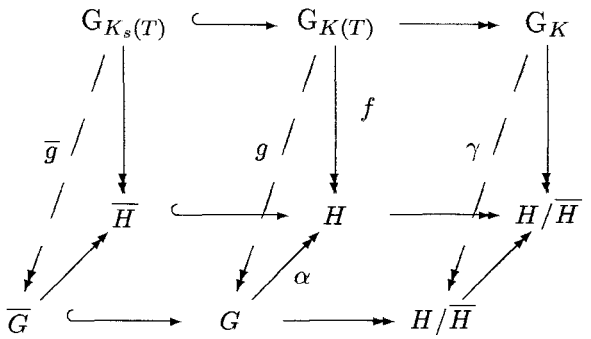


qui est visiblement scindé, a une solution forte. Ceci veut exactement dire qu'il existe une extension $E_G/K(T)$ telle que $Gal(E_G/K(T)) = Gal(E_G K_s/K_s(T)) = G$.

Preuve de Conj. Prin. $\Rightarrow$ Split EP/$_{K(T)}$: Considérons le problème de plongement scindé suivant:



Notons $\overline{H}$ le groupe $f(G_{K_s(T)})$, p l'application naturelle $H \to H/\overline{H}$ et $\overline{G}$ le noyau de l'application surjective $p\alpha$. Il est clair que α est une surjection de $\overline{G}$ sur $\overline{H}$. Ainsi, on peut parler du problème de plongement pour suite exacte de $K(T)$ suivant:



Ce problème de plongement est scindé. D'après la conjecture principale, il existe une solution forte $(\overline{g}, g, \gamma)$. En particulier l'application g est une solution forte au problème de plongement pour $G_{K(T)}$ de départ. □

Remarque 3: La conjecture principale affirme que tout problème de plongement pour $G_{K(T)}$ donné avec certaines contraintes sur K_s a une solution forte. Les conjectures **Split EP/**$_{K(T)}$ et **PIGR/**$_{K(T)}$ correspondent à des cas particuliers. La conjecture **Split EP/**$_{K(T)}$ est obtenue en levant les contraintes sur K_s alors que la conjecture **PIGR/**$_{K(T)}$ a une contrainte sur K_s. Toutefois, le **PIGR/**$_{K(T)}$ ne concerne que les problèmes de plongements scindés pour lesquels le quotient est $H = 1$.

Autres commentaires

(a) La conjecture principale peut être généralisée dans deux directions. Premièrement, le corps $K(T)$ peut être remplacé par le corps des fonctions $K(C)$ de n'importe quelle K-courbe projective lisse. C'est à dire que l'on peut remplacer la ligne exacte "du haut" par la ligne exacte

$$1 \longrightarrow G_{K_s(C)} \longrightarrow G_{K(C)} \longrightarrow G_K \longrightarrow 1$$

Harbater [Har4] et Pop [Pop2] travaillent dans ce contexte plus général. Une difficulté supplémentaire vient se greffer: cette suite n'est pas forcément scindée au contraire du cas particulier $C = \mathbb{P}^1$.

Une seconde généralisation possible est de remplacer le groupe de Galois absolu $G_{K(C)}$

par le groupe algébrique fondamental $\pi_1(C - D)$ où D désigne un diviseur G_K-invariant de C. On remplace alors la "ligne du haut" par la suite exacte

$$1 \longrightarrow \pi_1(\overline{C} - \overline{D}) \longrightarrow \pi_1(C - D) \longrightarrow G_K \longrightarrow 1$$

où $\overline{C} - \overline{D} = (C - D) \otimes_K K_s$. Toutefois, avec ce changement, la conjecture est fausse. En effet, prenons $K = \mathbb{C}$, $C = \mathbb{P}^1$ et $|D| > 0$. Comme $\pi_1(\mathbb{P}^1 - D)$ est pro-libre de rang $|D| - 1$, un problème de plongement

$$\begin{array}{ccccccccc} & & & & & & \pi_1(\mathbb{P}^1 - D) & & \\ & & & & & & \downarrow & & \\ 1 & \longrightarrow & N & \longrightarrow & G & \xrightarrow{\alpha} & H & \longrightarrow & 1 \end{array}$$

avec G de rang $\geq |D|$ ne peut pas avoir de solution forte. Pourtant la conjecture principale peut prédire que le problème de plongement a une solution forte si certains points de ramification supplémentaires sont possibles. De façon plus précise, la conjecture principale peut-être reformulée de la manière suivante:

(*) Etant donné un problème de plongement fini pour suites exactes du groupe fondamental, il existe un ensemble fini $D' \subset C$ tel que le problème de plongement pour la suite exacte:

$$1 \to \pi_1(\overline{C} - (\overline{D} \cup \overline{D'})) \to \pi_1(C - (D \cup D')) \to G_K \to 1$$

obtenu par composition avec l'application $\pi_1(C - (D \cup D')) \to \pi_1(C - D)$ a une solution propre.

L'équivalence "(*)$\Leftrightarrow$ Conj.Prin." vient du fait que $\varprojlim_D \pi_1(C-D) = G(K(C))$. D'autres questions se posent alors: Comment choisir les points de ramification supplémentaires? combien en faut-il? etc.

(b) Conjecturellement parlant, si K est un corps quelconque, $\mathbf{Split\ EP}/_{K(T)}$ et $\mathbf{PIGR}/_{K(T)}$ sont vraies toutes deux sur $K(T)$. Ceci n'est plus vrai si l'on remplace $K(T)$ par K. Plus exactement, il existe un corps K tel que tout groupe fini est groupe de Galois sur K et pourtant, il existe des problèmes de plongements pour G_K sans solution forte. Un contre exemple a été donné par Fried et Völklein [FrVo2;§2 Examples] (voir aussi [Ja1;Ex.3.5]).

Fried et Völklein disent qu'un corps K est RG-hilbertien si la propriété de spécialisation d'Hilbert est vraie pour tous les polynômes irréductibles $P(T, Y) \in K(T)[Y]$ tels que l'extension associée soit galoisienne et régulière. Ils ont montré qu'il existait un corps dénombrable K qui est PAC, RG-hilbertien mais sans être hilbertien. Le corollaire 2.3.4 à venir montre que tout groupe fini est groupe de Galois sur K. (Pour les corps PAC de caractéristique 0, la propriété RG-hilbertienne et celle d'avoir tout les groupes finis pour groupes de Galois sont en fait équivalentes [FrVo2;Th.B]).

Supposons maintenant que tout problème de plongement pour G_K a une solution forte. Alors par le procédé de réduction faible $\to$ scindé, tout problème de plongement pour G_K ayant une solution faible, a une solution forte. Mais, d'après un résultat de Ax, comme K est PAC, G_K est projectif [FrJa;Th.10.17] et donc tout problème de plongement pour G_K admet une solution forte. D'après le théorème d'Iwasawa, G_K est pro-libre.

Mais Roquette a montré qu'un corps K PAC tel que G_K est pro-libre est nécessairement hilbertien [FrJa;Cor.24.38], d'où la contradiction.

2.3 Résultats

2.3.1 Corps ample

Définition 2.3.1 *Un corps K est dit ample si pour toute courbe géométriquement irréductible et lisse C, définie sur K, on a:*

$$C(K) \neq \emptyset \Rightarrow C(K) \text{ infini}$$

Cette définition est due à Pop qui appelle ces corps *larges*. Avant de donner des exemples de tels corps, nous donnons un joli résultat de Pop, que nous utiliserons dans la preuve du théorème principal: les corps K amples sont exactement les corps existentiellement clos dans leur corps de séries de Laurent $K((X))$.

Définition 2.3.2 *Soit Ω/K une extension régulière. Le corps K est dit existentiellement clos dans Ω s'il vérifie une des propriétés équivalentes suivantes:*

(1) Pour toute K-variété géométriquement irréductible et lisse V,

$$V(\Omega) \neq \emptyset \Rightarrow V(K) \neq \emptyset$$

(2) Pour toute K-variété géométriquement irréductible et lisse V,

$$K(V) \subset \Omega \Rightarrow V(K) \neq \emptyset$$

(3) Pour toute K-variété géométriquement irréductible et lisse V,

$$V(\Omega) \text{ Zariski-dense} \Rightarrow V(K) \text{ Zariski-dense}$$

Preuve de l'équivalence:

(3)⇒ (1): Prenons $\xi \in V(\Omega)$. Considérons W, la clôture de Zariski de ξ dans la K-variété V: C'est un sous-schéma fermé irréductible de V. Comme $K(W) = K(\xi) \subset \Omega$ et que l'extension Ω/K est régulière, il vient que $K(W)/K$ est régulière. De là, W est une sous-variété irréductible de V. Il vient de (3) que $W(K) \neq \emptyset$ et donc $V(K) \neq \emptyset$.

(1)⇒ (2): Si $K(V) \subset \Omega$, le point générique ξ de V est dans $V(\Omega)$ (car $K(\xi) = K(V)$). Il vient de (1) que $V(K) \neq \emptyset$.

(2)⇒ (3): Prenons $\xi \in V(\Omega)$. Considérons la clôture de Zariski de ξ dans la K-variété V. Comme expliqué précédement, W est une sous-variété irréductible de V. Il vient de (2) que $W(K) \neq \emptyset$ et donc $V(K) \neq \emptyset$. Le même argument fonctionne si l'on remplace V par un ouvert de V. Ainsi $V(K)$ est Zariski-dense. □

Théorème 2.3.1 (Pop,[Pop4;Prop.1.1]) *Un corps K est ample ssi il est existentiellement clos dans son corps des séries de Laurent $K((X))$.*

Exemples de corps amples:

(1) Les corps PAC sont amples. Ceci vient directement de la définition: un corps K est dit P(seudo) A(lgébriquement) C(los) si $V(K) \neq \emptyset$ pour toute variété irréductible définie

sur K. Les corps algébriquement clos sont bien évidemment PAC. Il existe de nombreux autres exemples de tels corps, même à l'intérieur de $\overline{\mathbb{Q}}$, par exemple $K = \mathbb{Q}^{tr}(\sqrt{-1})$ (voir chapitre IV).

(2) Les corps valués complets sont amples (e.g. $K = \mathbb{Q}_p, \mathbb{R}, k((X))$, etc.). Ceci vient du théorème des fonctions implicites. L'argument suivant montre directement (i.e. sans le théorème 2.3.1) qu'un corps valué complet (K, ν) est existentiellement clos dans $K((X))$. Soit V une variété définie sur K. Supposons la condition du (2) de la définition 2.3.2 satisfaite (i.e. $K(V) \subset K((X))$). Notons $\widetilde{K(X)}$ la clôture hensélienne de $K(X)$ dans $K((X))$. Le corps $\widetilde{K(X)}$ est existentiellement clos dans $K((X))$ [Ja1;Lemmas 2.2 et 2.3]. De là $V(\widetilde{K(X)}) \neq \emptyset$. Maintenant, $\widetilde{K(X)}$ est la clôture algébrique de $K(X)$ dans $K((X))$. Donc les éléments de $\widetilde{K(X)}$ sont les séries formelles ayant un rayon de convergence positif ([Deb3;Prop.p.387]). Prenons un point $M_X \in V(\widetilde{K(X)})$. La spécialisation de X à un élément $\xi \neq 0$ dans le disque de convergence des séries présentes dans les coordonnées de M_X donne un point $M_\xi \in V(K)$.

(3) Pour tout p premier, notons $\mathbb{Q}^{tp}$ le corps des nombres totalement p-adiques (i.e. l'ensemble des éléments de $\overline{\mathbb{Q}}$ dont tous les conjugués vivent dans une même copie de $\mathbb{Q}_p$). On utilise la notation $\mathbb{Q}^{tr}$ pour parler du corps des nombres algébriques totalement réels, qui correspond au cas $p = \infty$. Alors pour tout premier p, y compris $p = \infty$, $\mathbb{Q}^{tp}$ est ample. Ceci vient immédiatement du précédent exemple et du résultat suivant de Pop [Pop5] (voir aussi [GrPoRo], [Pop4;App.I.], [Ja3]).

Théorème 2.3.2 (Pop) *Soit V une variété géométriquement irréductible et lisse définie sur $\mathbb{Q}^{tp}$, si $V(\mathbb{Q}_p^\sigma) \neq \emptyset$ pour tout $\sigma \in G_{\mathbb{Q}_p}$, alors $V(\mathbb{Q}^{tp}) \neq \emptyset$. (La condition peut-être remplacée par $V(\mathbb{Q}_p) \neq \emptyset$ si V est définie sur $\mathbb{Q}$.)*

Cet exemple peut se généraliser au corps K^S des éléments totalement S-adiques d'un corps global K. Ici S désigne un ensemble fini de places de K et K^S est le sous-corps de K_s composé des éléments qui pour tout $\nu \in S$ ont des conjugués restant dans une copie donnée du complété K_ν. Le résultat de Pop reste vrai dans cette généralisation et alors K^S est ample.

(4) Le corps $\mathbb{Q}$ n'est pas ample. Plus généralement, d'après le théorème de Faltings, aucun corps de nombres n'est ample. Jarden nous a signalé qu'en utilisant le théorème de Faltings et celui de Manin et Grauert, on peut montrer qu'aucun corps finiment engendré sur son sous-corps premier, n'est ample. Récemment Pietro Corvaja nous a communiqué l'exemple d'une extension algébrique infinie de $\mathbb{Q}$ qui n'est pas ample. Son exemple repose sur le lemme suivant:

Lemme 2.3.1 *Il existe une courbe lisse telle que pour tout corps de nombres k, l'ensemble des points $P \in X(k)$ quadratiques sur k (i.e. tels que $[k(P) : k] \leq 2$) est fini.*

(Corvaja nous a signalé qu'une preuve de ce théorème pouvait être trouvée dans un article de Vojta et qu'elle repose sur le théorème de finitude de Faltings pour les points rationnels sur une sous-variété d'une variété abélienne ne contenant pas de translaté de sous-variétés abéliennes.)

Une fois établi ce résultat, on prend une telle courbe X (qui peut-être choisi de manière à ce que $X(\mathbb{Q})$ soit non vide). L'ensemble des extensions quadratiques de $\mathbb{Q}$ étant infini, il en existe une, k_1, avec $X(k_1) = X(\mathbb{Q})$. Par récurrence, ayant construit k_n de degré 2^n sur $\mathbb{Q}$, avec $X(k_n) = X(\mathbb{Q})$, il existe k_{n+1} tel que $[k_{n+1} : k_n] = 2$ et $X(k_{n+1}) = X(k_n) = X(\mathbb{Q})$. La réunion des k_n donne l'exemple de corps recherché.

2.3.2 Résultat principal

Théorème 2.3.3 (Théorème Principal) *La conjecture principale est vraie si K est un corps ample.*

Le théorème principal est conséquence d'une série de résultats. La contribution principale est due à Fried, Harbater et Pop. L'idée de travailler avec des familles de revêtements revient à Fried [Fr]. Harbater [Har2] a introduit des méthodes très efficaces de découpages et recollements de revêtements, en particulier sur les corps complets ou algébriquement clos. Pop a développé ces méthodes de recollements et l'aspect arithmétique de cette technique. En particulier, il a introduit et étudié la notion de corps ample. Un énoncé équivalent au théorème principal ainsi qu'une preuve peuvent être trouvés dans les travaux de Pop ([Pop2],[Pop4]). D'autres mathématiciens ont pris une part importante dans le théorème principal, en particulier, Dèbes, Jarden, Haran, Liu, Völklein. Le théorème principal a deux conséquences majeures (Cor.2.3.1 et Cor.2.3.2). Nous allons montrer plus bas qu'il contient en fait la majeure partie des résultats connus dans ce domaine.

Corollaire 2.3.1 *La conjecture* $\mathbf{PIGR}/_{K(T)}$ *est vraie si K est ample. C'est à dire que si K est un corps ample, alors tout groupe fini est groupe de Galois d'une extension régulière de $K(T)$.*

Ce résultat contient les cas particuliers suivants:

- $K = \mathbb{C}$ (Riemann),
- $K = \mathbb{R}$ (Hurwitz, 1890),
- K algébriquement clos (Harbater, 1984, [Har1]),
- $K = \mathbb{Q}_p$ (Harbater, 1985, [Har2]),
- K PAC (Fried-Völklein pour la caractéristique nulle, 1991, [FrVo1] — Pop dans le cas général, 1993, [Pop4]),
- $K = \mathbb{Q}^{tr}$ (Dèbes-Fried, 1991, [DeFr]),
- $K = \mathbb{Q}^{tp}$ (Dèbes, 1993, [Deb2] — Pop, 1993, [Pop4]),
- K ample (Pop, 1995, [Pop4]).

Corollaire 2.3.2 *La conjecture* **Split EP**$/_{K(T)}$ *est vraie si le corps K est ample. En particulier la conjecture de Fried-Völkein* **(FrVo)** *est vraie si K est ample.*

Corollaire 2.3.3 *Pour tout corps dénombrable, $G_{\overline{K}(T)}$ est pro-libre.*

Preuve: D'après le théorème d'Iwasawa, nous avons besoin de prouver que tout problème de plongement pour $G_{\overline{K}(T)}$ admet une solution forte. D'après le théorème de Tsen, $G_{\overline{K}(T)}$ est projectif. Ainsi tout problème de plongement pour $G_{\overline{K}(T)}$ admet une solution faible. Grâce au procédé de réduction faible $\rightarrow$ scindé, on peut supposer que le problème est scindé. Mais comme les corps algébriquement clos sont amples, la conjecture **Split EP**$/_{K(T)}$ est vraie pour $\overline{K}(T)$. Donc tout problème de plongement admet une solution forte. □

Le corollaire 2.3.3 est dû à:

- Douady en caractéristique nulle [Do], 1964,
- Harbater [Har4] and Pop [Pop2] en général, 1993.

Corollaire 2.3.4 *Pour tout corps dénombrable, hilbertien et PAC, G_K est pro-libre.*

Preuve: D'après un résultat d'Ax [FrJa;Th.10.17], si K est PAC alors G_K est projectif. De plus les corps PAC sont amples. La conjecture de Fried-Völklein, qui est vraie pour les corps amples, donne le résultat. □

Le corollaire 2.3.4 est dû à:

- Fried-Völklein en caractéristique nulle [FrVo2], 1992,
- Pop dans le cas général [Pop4], 1993.

Remarques 4:

(a) La conjecture $\mathbf{PIGR}/_{K(T)}$ prévoit, en particulier, qu'étant donné un groupe fini G, G est groupe de Galois d'une extension régulière $E/F(T)$, pour tout corps fini F. Le corollaire 2.3.1 permet de montrer que ceci est vrai pour presque tous les corps finis. La preuve utilise un argument de théorie des modèles: supposons que pour un groupe fini donné G, l'ensemble $\mathcal{F}$ des corps finis F pour lesquels G n'est pas groupe de galois d'une extension régulière de $F(T)$ est infini. Considérons alors l'ultra-produit K de l'ensemble des corps de $\mathcal{F}$ [FrJa;Ch.6]. Alors [FrJa;Cor.10.6] affirme que K est un corps PAC (ceci provient essentiellement de l'estimation de Lang-Weil du nombre de points d'une courbe sur un corps fini [FrJa;Th.4.9]). Ainsi, d'après le corollaire 2.3.1, G est groupe de Galois d'un extension régulière de $K(T)$. Mais, tout énoncé du premier ordre vrai sur K est vrai sur presque tous les F de $\mathcal{F}$ [FrJa;Cor.6.12], donc au moins sur un. D'où la contradiction.

Cette conséquence du corollaire 2.3.1 a été mise à jour en 1991 dans un article de Fried-Völklein [FrVo1;Cor.2], dans une forme légèrement plus faible où seuls les corps finis premiers étaient considérés. Dans ce cas, l'ultra-produit considéré K est un corps PAC de caractéristique 0 et l'argument fonctionne alors dans le cas particulier du corollaire 2.3.1 prouvé par Fried et Völklein. Dans leur article, ils donnent aussi une présentation plus géométrique de l'argument précédent. Le cas général de l'argument précédent, requiert la version du corollaire 2.3.1 pour un corps PAC de caractéristique quelconque, version prouvée par Pop [Pop4]. Ce résultat de Pop apparaissait déjà sous une certaine forme dans une lettre de Roquette en 1991.

(b) Pour $K = \mathbb{Q}^{ab}$, la conclusion "G_K pro-libre" du corollaire 2.3.4 donnerait une réponse affirmative à la conjecture de Shafarevich. Mais Frey a remarqué que $\mathbb{Q}^{ab}$ n'est pas un corps PAC [FrJa;Cor.10.15]. Ainsi le corollaire 2.3.4 ne peut pas s'appliquer à $K = \mathbb{Q}^{ab}$. D'un autre coté, le corollaire 2.3.3 montre que $G_{\overline{\mathbb{F}_p}(T)}$ est pro-libre. Ce résultat peut-être vu comme un analogue de la conjecture de Shafarevich: $\overline{\mathbb{F}_p}(T)$ est en effet la clôture cyclotomique $\mathbb{F}_p{}^{cycl}(T)$ de $\mathbb{F}_p(T)$ (exactement comme $\mathbb{Q}^{ab} = \mathbb{Q}^{cycl}$). De manière similaire le groupe de Galois absolu de la clôture cyclotomique de $K = \mathbb{Q}^{tr}$ est pro-libre. En effet $(\mathbb{Q}^{tr})^{cycl} = \mathbb{Q}^{tr}(\sqrt{-1})$ et d'après le corollaire 2.3.4 $G_{\mathbb{Q}^{tr}(\sqrt{-1})}$ est pro-libre (une des conséquences du théorème 2.3.2 est que $\mathbb{Q}^{tr}(\sqrt{-1})$ est PAC. Ce corps est hilbertien par le théorème de Weissauer [FrJa]). On consultera le chapitre IV de cette thèse pour une généralisation de cet analogie à la conjecture de Shafarevich.

(c) Le corollaire 2.3.3 reste vrai dans le cas indénombrable: pour tout corps K, le groupe $G_{\overline{K}(T)}$ est pro-libre (de rang $card(K)$). Ceci peut-être montré par les mêmes arguments mais certains ajustements sont nécessaires. De façon plus précise, on peut utiliser la généralisation de théorème d'Iwasawa suivante: si $\aleph$ est un cardinal infini, alors une condition nécessaire et suffisante pour qu'un groupe F soit pro-fini de rang $\aleph$ est que tout problème de plongement fini pour F avec un noyau non trivial possède exactement $\aleph$ so-

lutions fortes (voir [Ja2;lemma 2.1] où cette généralisation est attribuée à Z.Chatzidakis). Ainsi pour la généralisation du corollaire 2.3.3 nous avons besoin de prouver que tout problème de plongement fini pour $G_{\overline{K(T)}}$ ayant un noyau non trivial a exactement $card(K)$ solutions fortes. Ceci requiert des résultats plus précis que la simple existence d'une solution propre donnée par le théorème principal (voir [Har4] et [Pop2]).

(d) Un corps K est dit "ω-libre" si tout problème de plongement pour G_K admet une solution forte. D'après le théorème d'Iwasawa, si K est dénombrable, il y équivalence entre ω-libre et pro-libre. Jarden [Ja3;Rem.11.3] observe que l'on peut remplacer la conclusion "G_K pro-libre" du corollaire 2.3.4 par la conclusion "G_K ω-libre" si l'on considère des corps indénombrables. C'est à dire que l'on a dans le cas général "PAC + hilbertien $\Rightarrow$ ω-libre". Il est à noter que l'implication "PAC + hilbertien $\Rightarrow$ pro-libre" est fausse dans le cas général. Il y existe des corps K, PAC et hilbertiens, tels que G_K ne soit pas pro-libre [Ja2;Ex.3.2].

2.4 Arguments principaux

Dans cette partie nous donnons un schéma de la démonstration du corollaire 2.3.1. Nous allons montrer que, si K est un corps ample, alors tout groupe fini G est groupe de Galois d'une extension régulière de $K(T)$. La preuve de ce cas particulier du théorème principal contient les arguments principaux de la méthode. Il y a deux étapes. La première consiste à résoudre le problème sur le corps $K((X))$ des séries de Laurent à coefficients dans K. La seconde utilise un argument de spécialisation pour descendre de $K((X))$ à K.

2.4.1 Le problème inverse de Galois régulier sur $K((X))(T)$

Le point principal est le résultat suivant:

Théorème 2.4.1 *Soit k un corps local. Soit G un groupe engendré par 2 de ses sous-groupes G_1 et G_2. Supposons que pour $i = 1, 2$, il existe une extension galoisienne régulière $F_i/k(T)$ de groupe de Galois G_i ayant un premier non ramifié de degré 1. Alors il existe une extension galoisienne régulière $F/k(T)$ de groupe de Galois G ayant un premier non ramifié de degré 1.*

Ce résultat réduit le problème à la réalisation des groupes cycliques (comme groupes de Galois d'une extension régulière de $k(T)$ avec un premier non ramifié de degré 1). Dans [Har2], Harbater utilise un résultat de Saltman pour traiter ce cas (voir aussi [Liu] et [Vo;Ch.11]). En caractéristique 0, nous donnons dans le chapitre III de cette thèse une méthode plus simple pour réaliser les groupes cycliques, qui nous apporte, de surcroit, des informations plus précises sur la ramification des extensions obtenues.

Le théorème 2.4.1 est dû à Harbater. L'argument principal est une méthode de découpage et recollement d'espaces analytiques utilisée avec le théorème GAGA formel. Ce résultat d'Harbarter à été traduit en termes géométriques rigides par Liu ([Liu] voir aussi [Des1]), après une suggestion de Serre [Ser1;p.93]. Pop et Harbater ont alors développé de façon indépendante ces méthodes de découpages et recollements: en particulier ils ont montré qu'il était possible d'utiliser ces méthodes non seulement pour réaliser des groupes finis mais aussi pour résoudre des problèmes de plongements. Pop réussit aussi à garder un contrôle arithmétique sur cette méthode, cela le mena à son "1/2-théorème

d'existence de Riemann" [Pop1]. La méthode de découpage et recollement est aussi un ingrédient essentiel de la preuve de la conjecture d'Abhyankar sur les groupes de Galois sur les courbes: le cas affine a été démontré en premier par Raynaud [Ra], Harbater put alors prouver le cas général [Har3] par méthode de recollement; une preuve alternative du cas général utilisant le résultat de Raynaud fut apportée un peu plus tard par Pop [Pop3]. Il existe maintenant une preuve du théorème 2.4.1 par Haran et Völklein ([HaVo], [Vo;Ch.11]) qui n'utilise aucune base géométrique.

2.4.2 Argument de spécialisation

(On pourra aussi consulter [Ja4;Prop.2.2] pour cette partie.) Soit Q un corps premier. D'après la partie précédente, on sait que pour tout groupe fini G, il existe une extension galoisienne régulière $E_X/Q((x))(T)$ de groupe de Galois G. Notons y un élément primitif de cette extension.

Soit F/Q une extension de type fini avec $F \subset Q((x))$, telle que le polynôme minimal de y sur $Q((x))(T)$ soit dans $F(T)[Y]$ et telle que tous les conjugués de y sur $Q((x))(T)$ soient dans $F(T,y)$. Posons $E = F(T,y)$, alors l'extension $E/F(T)$ est une extension galoisienne régulière de $F(T)$ avec $Gal(E/F(T)) = G$.

L'inclusion $F \subset Q((X))$ implique en particulier que $F \cap \overline{Q} = Q$. Ainsi, F est le corps des fonctions d'une variété V géométriquement irréductible et définie sur Q. L'égalité $Gal(E/F(T)) = G$ peut se réécrire $Gal(E/Q(V)(T)) = G$.

L'extension $E/Q(V)(T)$ est régulière, donc on peut appliquer le théorème de Bertini-Noether (voir [FrJa;Prop.8.8]). Il existe un fermé de Zariski $Z \subset V$ tel que, pour tout $\nu \in V(\overline{Q}) - Z$, l'extension $E/Q(V)(T)$ se spécialise en une extension $E_\nu/Q(\nu)(T)$ de degré $[E_\nu : Q(\nu)(T)] = [E : Q(V)(T)]$. En grossissant éventuellement Z, on peut:

- conclure que l'extension $E_\nu/Q(\nu)(T)$ est aussi galoisienne. On a alors $Gal(E_\nu/Q(\nu)(T)) = G$ (pour $\nu \in V(\overline{Q}) - Z$).

- supposer que la variété est lisse.

Finalement, comme $F = Q(V) \subset Q((x))$, l'ensemble $V(Q((x)))$ est Zariski-dense. On a donc prouvé le théorème suivant:

Théorème 2.4.2 *Soit Q un corps premier. Pour tout groupe fini G il existe une variété irréductible et lisse définie sur Q telle que:*

(1) Pour tout corps K contenant Q, si $V(K)$ est Zariski-dense alors G est groupe de Galois d'une extension régulière de $K(T)$.

(2) $V(Q((x)))$ est Zariski-dense.

Supposons maintenant que K est un corps ample. D'après le théorème 2.3.1, K est existentiellement clos dans $K((x))$. Ainsi, d'après le (2) du théorème précédent, $V(K)$ est Zariski-dense. Ceci permet de conclure, d'après le (1), que G est groupe de Galois d'une extension régulière de $K(T)$. Le $(\mathbf{PIGR}/_{K(T)})$ est donc vrai sur les corps amples.

Nous avons montré que $\mathbb{R}$ et les corps locaux étaient des corps amples, le théorème précédent donne le résultat suivant:

Corollaire 2.4.1 *Pour tout groupe fini, il existe une variété V irréductible, lisse et définie sur $\mathbb{Q}$ telle que:*

(1) Si $V(\mathbb{Q}) \neq \emptyset$ *alors* G *est groupe de Galois d'une extension régulière de* $\mathbb{Q}(T)$.

(2) $V(\mathbb{Q}_p) \neq \emptyset$ *pour tout premier* p *(y compris* $p = \infty$*).*

Dans la propriété (2), on peut en fait remplacer $\mathbb{Q}_p$ par n'importe quel corps valué complet de caractéristique 0. Il est à noter que la condition (2) ne permet pas de conclure en général que $V(\mathbb{Q}) \neq \emptyset$ (Voir [Deb2;Ex.4.2]).

Ce résultat a été démontré en premier dans [Des2]. Cette preuve originale utilise la théorie des espaces de Hurwitz de Fried [Fr]. Cette approche a l'avantage d'être nettement plus explicite, elle permet aussi de donner de bons renseignements sur la ramification des extensions considérées. L'objet du chapitre suivant est la présentation de cette autre preuve.

Chapitre 3

Existence de points p-adiques sur un espace de Hurwitz

3.1 Introduction

3.1.1 Rappel de la situation.

D'après un résultat fondamental de M.Fried et H.Völklein [FVol] on sait que pour tout groupe fini G donné, il existe une variété algébrique irréductible, définie sur $\mathbb{Q}$ vérifiant:
(A) *Pour tout corps commutatif K contenant $\mathbb{Q}$, à un point K-rationnel de cette variété on peut associer une extension galoisienne régulière de $K(T)$ de groupe de Galois G.*

En fait à un point K-rationnel on associe un G-revêtement défini sur K et de groupe de Galois G.

P.Dèbes en reprenant ce résultat et en le combinant avec ceux de D.Harbater et de Q.Liu ([Har], [Liu]) prouve que pour tout p premier (y compris $p = \infty$) il existe une variété $\mathcal{H}_p$ irréductible et définie sur $\mathbb{Q}$ vérifiant la propriété (A) et possédant un point $\mathbb{Q}_p$-rationnel (resp. $\mathbb{R}$-rationnel pour $p = \infty$),(cf [Deb1]). Grâce à un résultat de Pop, il en déduit l'existence d'un point $\mathbb{Q}^{tp}$-rationnel (on rappelle que $\mathbb{Q}^{tp}$ est le corps des nombres totalement p-adiques, i.e l'ensemble des nombres algébriques p-adiques qui n'ont que des conjugués p-adiques par l'action de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$) et donc que tout groupe fini est groupe de Galois d'une extension de $\mathbb{Q}^{tp}(T)$. Il pose ensuite la question de savoir si l'on peut choisir $\mathcal{H}_p$ indépendament de p.

L'objet de ce chapitre est d'apporter une réponse positive à cette question et de donner en même temps, une forme plus précise du corollaire 2.4.1 du chapitre précédent. Plus précisément:

Théorème 3.1.1 *Pour tout groupe fini G, il existe une variété algébrique, irréductible et définie sur $\mathbb{Q}$ (vérifiant la propriété (A)) et vérifiant en outre:*

1. *Pour réaliser G comme groupe de Galois sur $\mathbb{Q}(T)$ il suffit de trouver un point $\mathbb{Q}$-rationnel sur cette variété.*

2. *Pour tout p premier (y compris $p = \infty$) il existe un point $\mathbb{Q}_p$-rationnel, x_p, sur cette variété (il existe même des points $\mathbb{Q}^{tp}$-rationnels).*

3. *Le G-revêtement défini sur $\mathbb{Q}_p$ associé au point x_p, a des points de ramifications dans $\mathbb{P}^1(\mathbb{Q}^{ab})$ qui sont globalement invariants par l'action de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$.*

Il est naturel de se demander si on peut déduire de l'existence de points $\mathbb{Q}_p$-rationnels, pour tout p, l'existence d'un point $\mathbb{Q}$-rationnel sur les espaces de Hurwitz? Il s'agit d'un problème "local-global", type principe de Hasse qui est aussi évoqué dans [Deb1]: un exemple tiré de [DeFr] montre que ce n'est pas toujours possible.

3.1.2 Rappels, préliminaires.

Espace de Hurwitz.

On rappelle ici brièvement les propriétés des espaces de Hurwitz, on trouvera tous les détails dans [FrVol].

Soit G un groupe fini de centre $Z(G)$ trivial et $r > 2$ un entier. Prenons un r-uplet $\mathbf{C} = (C_1, \cdots, C_r)$ de classes de conjugaison d'éléments de G, on suppose que $\mathbf{C}$ est rationnel (i.e., invariant à l'ordre près par élévation à toute puissance première à $card(G)$).

Proposition 3.1.1 *Sous les conditions précédentes, il existe une variété $\mathcal{H}(\mathbf{C}, G)$ définie sur $\mathbb{Q}$ telle que pour tout corps commutatif K contenant $\mathbb{Q}$, les propriétés suivantes soient équivalentes:*

i) $\mathcal{H}(K) \neq \emptyset$

ii) *Il existe un G-revêtement (i.e., un revêtement galoisien de $\mathbb{P}^1$ de groupe de Galois G donné avec l'action de G) défini sur K, non ramifié en dehors de r points distincts de $\mathbb{P}^1$ et tel que l'invariant canonique de l'inertie (Cf. [Deb1] (2.2 page 3)) de ce G-revêtement est égal ,à l'ordre près, à $\mathbf{C} = (C_1, \cdots, C_r)$.*

On appelle cette variété l'espace de Hurwitz associé à G et à $\mathbf{C}$, on le note parfois simplement $\mathcal{H}(\mathbf{C})$.

Rappellons aussi, le résultat concernant l'irréductibilité de $\mathcal{H}(\mathbf{C})$, dû a J.H. Conway et R.A. Parker (cf [CP] et [FrV,appendix]):

Proposition 3.1.2 *Sous les conditions de la proposition précédente et en supposant de plus que le groupe des multiplicateurs de Schur est engendré par les commutateurs (Cf. [FrVo1]), il existe un entier b_0 dépendant de G tel que si chaque classe de conjugaison de G apparaît au moins b_0 fois dans $\mathbf{C}$, alors $\mathcal{H}(\mathbf{C})$ est irréductible.*

On se placera désormais dans le cas où G vérifie les conditions ci-dessus et on démontrera le théorème suivant:

Théorème 3.1.2 *Soit G un groupe fini de centre trivial, tel que le groupe des multiplicateurs de Schur soit engendré par les commutateurs. Il existe un entier r et un r-uplet de classes de conjugaison $\mathbf{C}$ de G tels que l'espace de Hurwitz $\mathcal{H}(\mathbf{C})$ soit une variété irréductible, définie sur $\mathbb{Q}$ et vérifiant (outre l'équivalence i) $\Leftrightarrow$ ii) de la Prop. 3.1.1) les propriétés suivantes:*

- *Pour tout p premier (y compris $p = \infty$) $\mathcal{H}(\mathbf{C})$ possède un point x_p, $\mathbb{Q}_p$-rationnel. Il existe même des points $\mathbb{Q}^{tp}$-rationnels.*

- *Le G-revêtement associé à x_p a des points de ramification dans $\mathbb{P}^1(\mathbb{Q}^{ab})$ et ceux-ci sont globalement invariants par l'action de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$.*

Ce théorème implique le théorème 3.1.1. En effet grâce au lemme 2 de [FrVo1], on sait que tout groupe fini est quotient d'un groupe vérifiant les hypothèses du théorème 3.1.2. La théorie de Galois permet alors de passer du théorème 2 au théorème 1.

Théorème d'Harbater

Le théorème d'Harbater peut se résumer par l'affirmation suivante:

Tout groupe fini est groupe de Galois d'une extension régulière de $\mathbb{Q}_p(T)$

Liu dans [Liu] démontre ce résultat en reprenant les travaux d'Harbater, mais en utilisant la théorie des espaces analytiques rigides. Voila le théorème qui lui permet d'arriver à ses fins:

On dit que la fibre au dessus d'un point t_0 d'un revêtement $\phi : X \to \mathbb{P}^1$ définie sur K, est totalement K-rationnelle, si $\phi^{-1}(t_0)$ est composée uniquement de points K-rationnels.

Proposition 3.1.3 *Soit p un nombre premier, G un groupe fini engendré par deux de ses sous-groupes H_1, H_2. On suppose donnés deux G-revêtements: $\pi_i : X_i \to \mathbb{P}^1$, $i = 1, 2$ définis sur $\mathbb{Q}_p$ de groupe de Galois respectifs H_1, H_2, ayant respectivement r_1 et r_2 points de ramification et $\mathbf{C_1} = (C_{11}, \cdots, C_{1r_1})$, $\mathbf{C_2} = (C_{21}, \cdots, C_{2r_2})$ pour invariant canonique de l'inertie. On suppose que chacun des deux revêtements possède un point $\mathbb{Q}_p$-rationnel non ramifié t_i, $i = 1, 2$ au dessus duquel la fibre est totalement $\mathbb{Q}_p$-rationnelle.*

Alors, il existe un G-revêtement: $\pi : X \to \mathbb{P}^1$ défini sur $\mathbb{Q}_p$ de groupe de Galois G avec $r = r_1 + r_2$ points de ramification, ayant $\mathbf{C} = (C_{11}^G, \cdots, C_{1r_1}^G, C_{21}^G, \cdots, C_{2r_2}^G)$ (où C_{ij}^G représente la classe de conjugaison dans G de C_{ij}) pour invariant canonique de l'inertie et possédant un point $\mathbb{Q}_p$-rationnel non ramifié au dessus duquel la fibre est totalement $\mathbb{Q}_p$-rationnelle.

Cette proposition permet de construire "à la main" des G-revêtements de $\mathbb{P}^1$ de groupe de Galois donnés (Cf [Har], [Liu], [Des1]).

3.2 Démonstration du théorème 3.1.2.

Soit G un groupe fini vérifiant les hypothèses du théorème 3.1.2. Prenons pour chaque $x \in G/\{1\}$ le sous-groupe $H_x =< x >$. On a $H_x \simeq \mathbb{Z}/\sharp x\mathbb{Z}$, où $\sharp x$ est l'ordre de x dans G. Notons $g_{x_1}, \cdots, g_{x_{\varphi(\sharp x)}} \in (\mathbb{Z}/\sharp x\mathbb{Z})^*$ (φ étant l'indicateur d'Euler) les générateurs de H_x et $C_{g_{x_1}}, \cdots, C_{g_{x_{\varphi(\sharp x)}}}$ leurs classes de conjugaisons respectives dans G. Notons $C_x = (C_{g_{x_1}}, \cdots, C_{g_{x_{\varphi(\sharp x)}}})$ le r-uplet de ces classes de conjugaisons. Notons $y_1, \cdots, y_{\sharp G}$ les éléments de G (avec $y_1 = 1$). Considérons l'uplet $C = (C_{y_2}, \cdots, C_{y_{\sharp G}})$ obtenu en mettant bout à bout les uplet C_{y_i}, $i = 2, \cdots, \sharp G$ (on élimine la classe de conjugaison triviale C_{y_1}). Pour b entier notons à présent $\mathbf{C}_b = (C, \cdots, C)$ le uplet obtenu en répétant b fois le uplet C. On a la proposition suivante:

Proposition 3.2.1 *Pour b assez grand (par exemple le b_0 de la proposition 3.1.2) l'espace de Hurwitz $\mathcal{H}(\mathbf{C}_b)$ associé à $\mathbf{C}_b$ est une variété qui vérifie les propriétés du théorème 3.1.2.*

Les parties suivantes ont pour but de démontrer cette proposition.

3.2.1 Construction de G-revêtements de $\mathbb{P}^1$.

Pour tout groupe fini G fixé, nous allons montrer qu'il est toujours possible de construire un G-revêtement de $\mathbb{P}^1$ défini sur $\mathbb{Q}_p$, de groupe de Galois G tel que le nombre de points de ramification et l'invariant canonique de l'inertie de ces revêtements soient des données indépendantes de p.

Réalisation pour $G = \mathbb{Z}/n\mathbb{Z}$.

Soit K un corps commutatif de caractéristique nulle. Il est classique que l'on puisse réaliser tout groupe fini sur $\overline{K}(T)$. Le véritable problème est celui de la descente de $\overline{K}$ à K. La théorie du groupe fondamentale algébrique permet de poser le problème de la façon suivante. On pourra consulter [Deb2] pour plus de détails.

Etant donné r points distincts $\{t_1, \cdots, t_r\}$ dans $\mathbb{P}^1(\overline{K})$ globalement invariants par $Gal(\overline{K}/K)$, on note Ω l'extension algébrique maximale de $\overline{K}(T)$ non ramifiée en dehors de $t_1, \cdots, t_r$. On note Π^{alg} le groupe de Galois $Gal(\Omega/\overline{K}(T))$, et x_i le générateur canonique des groupe d'inertie au dessus de t_i, $i = 1, \cdots, r$ (Cf [Deb2] page 231 "structure des groupes d'inertie). Le groupe Π^{alg} est le groupe profini libre engendré par $x_1, \cdots, x_r$ modulo l'unique relation $x_1 \cdots x_r = 1$.

Proposition 3.2.2 *Un groupe fini G est groupe de Galois d'une extension régulière de $K(T)$ si et seulement si, il existe:*

- *un entier $r > 0$, r points distincts $t_1, \cdots, t_r$ dans $\mathbb{P}^1(\overline{K})$ globalement invariants par $Gal(\overline{K}/K)$ et $t_0 \in \mathbb{P}^1(K)\backslash\{t_1, \cdots, t_r\}$,*
- *des éléments $g_1, \cdots, g_r$ de G engendrant G et de produit $g_1 \cdots g_r = 1$,*
- *un morphisme de groupes $\tau \to f_\tau$ de $Gal(\overline{K}/K)$ dans G, tels que le morphisme de groupe $f : \Pi^{alg} \to G$ défini par $f(x_i) = g_i$ verifie:*

$$(1) \qquad f(x_i^\tau) = f_\tau g_i f_\tau^{-1} \text{ pour tout } i = 1, \cdots, r \text{ et tout } \tau \in Gal(\overline{K}/K)$$

Le G-revêtement de $\mathbb{P}^1$ associé à cette extension de $K(T)$ est alors de groupe de Galois G, non ramifié en dehors de $t_1, \cdots, t_r$ et a pour invariant canonique de l'inertie le r-uplet $\mathbf{C} = (C_1, \cdots, C_r)$ où C_i est la classe de conjugaison de g_i dans G, $i = 1, \cdots, r$.

Rappellons un lemme dont la démonstration pourra être trouvée dans [Deb2]:

Lemme 3.2.1 *Avec les notations précédentes on a:*
Pour tout $i = 1, \cdots, r$, x_i^τ est conjugué dans Π^{alg} à $(x_j)^{\chi_K(\tau)}$, où $t_j = t_i^\tau$ et $\chi_K : Gal(\overline{K}/K) \to \prod_{n>0} Gal(K(\xi_n)/K)$ (ξ_n racine primitive n-ième de l'unité), désigne le caractère cyclotomique du corps K.

D'après ce qui précède, pour réaliser $\mathbb{Z}/n\mathbb{Z}$ comme groupe de Galois sur $\mathbb{Q}(T)$ il faut et il suffit de trouver $r \in \mathbb{N}$, $\{t_1, \cdots, t_r\} \in \mathbb{P}^1(\overline{\mathbb{Q}})$ et des générateurs $(g_1, \cdots, g_r) \in (\mathbb{Z}/n\mathbb{Z})^r$ vérifiants $g_1 + \cdots + g_r = 0$ tel que:

$$(2) \qquad \forall \tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q}),\ \chi_{\mathbb{Q}}(\tau) g_j = g_i \text{ avec } t_j = t_i^\tau$$

En effet, le lemme 3.2.1 donne que $f(x_i^\tau)$ est conjugué dans G à $f(x_j)^{\chi_{\mathbb{Q}}(\tau)}$. Mais le groupe G étant commutatif, on a $f(x_i^\tau) = f((x_j)^{\chi_{\mathbb{Q}}(\tau)}) = g_j^{\chi_{\mathbb{Q}}(\tau)}$. La formule (1) à réaliser se réduit donc à

$$(3) \qquad g_j^{\chi_{\mathbb{Q}}(\tau)} = f_\tau g_i f_\tau^{-1} = g_i \text{ pour tout } i = 1, \cdots, r \text{ et tout } \tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$$

ce qui correspond bien à la condition (2) (en notation additive). De plus, tout morphisme $\tau \to f_\tau$ convient. Nous prendrons le morphisme trivial, i.e., $f_\tau = 1$ pour tout $\tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Pour ce choix, le G-revêtement associé possède un point $\mathbb{Q}$-rationnel non ramifié au dessus duquel sa fibre est totalement $\mathbb{Q}$-rationnelle. Cela résulte du fait général suivant ([Deb1], Prop.2.1): pour tout $\tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, l'élément f_τ, vu dans S_d par la représentation régulière $G \hookrightarrow S_d$ de G, correspond à l'action de τ sur la fibre au dessus de t_0.

Lemme 3.2.2 *On peut réaliser $\mathbb{Z}/n\mathbb{Z}$ sur $\mathbb{Q}(T)$ en prenant $r = \varphi(n)$ (φ étant l'indicateur d'Euler) $t_i = \xi_i$ où ξ_i est la i-ième racine n-ième primitive de l'unité $i = 1, \cdots, r$ si $n \neq 2$. Si $n = 2$ il suffit de prendre t_1, t_2 deux points rationnels distincts quelconques pour réaliser $\mathbb{Z}/2\mathbb{Z}$.*

Preuve:

1) $n \neq 2$: On va réaliser la condition (2) en prenant pour g_i les éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ indicés correctement. Plus précisément, notons $g_1, \cdots, g_r$ les éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ avec $g_1 = 1$. Soit ξ une racine primitive n-ième de l'unité. On pose $t_i = \xi^{g_i}$. Alors on a:

$$\forall \tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q}),\ (\xi)^\tau = \xi^{\chi_{\mathbb{Q}}(\tau)}$$

et ainsi si $(t_i)^\tau = t_j$, c'est à dire si $((\xi)^{g_i})^\tau = \xi^{g_j}$, alors comme $(\xi^{g_i})^\tau = (\xi^\tau)^{g_i}$, on a nécessairement $\chi_{\mathbb{Q}}(\tau) g_i = g_j$, ce qui est bien ce que l'on demande.

De plus les g_i engendrent $\mathbb{Z}/n\mathbb{Z}$ (chacun d'eux le faisant). Il reste juste à vérifier que $\sum_{1 \leq i \leq r} g_i = 0$.
Prenons un élément $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Alors, comme on a $n \neq 2$, on a $-x \neq x$ et $-x \in (\mathbb{Z}/n\mathbb{Z})^*$, ce qui assure bien que:

$$\sum_{x \in (\mathbb{Z}/n\mathbb{Z})^*} x = 0$$

2) $n = 2$: Réaliser $\mathbb{Z}/2\mathbb{Z}$ ne pose pas vraiment de problème: On prend ξ_1, ξ_2 deux points rationnels et alors pour tout $\tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on a ${\xi_i}^\tau = \xi_i$, $i = 1, 2$. On prend alors $g_1 = g_2 = 1$ dans $(\mathbb{Z}/2\mathbb{Z})^* = 1$. □

On vient donc de réaliser les $\mathbb{Z}/n\mathbb{Z}$ comme groupes de Galois de G-revêtements de $\mathbb{P}^1$ définis sur $\mathbb{Q}$ possédant un point rationnel au dessus duquel la fibre est totalement $\mathbb{Q}$-rationnelle.

Par extension des scalaires on obtient donc, pour tout p premier, un G-revêtement de $\mathbb{P}^1$ défini sur $\mathbb{Q}_p$, de groupe de Galois $\mathbb{Z}/n\mathbb{Z}$ et possédant un point $\mathbb{Q}_p$-rationnel au dessus duquel sa fibre est totalement $\mathbb{Q}_p$-rationnelle. Le nombre de points de ramification vaut $r = \varphi(n)$ (indépendant de p) et son invariant canonique de l'inertie vaut $\mathbf{C} = (C_1, \cdots, C_{\varphi(n)})$ (indépendant de p) où $C_i = \{g_i\}$ et $g_i \in (\mathbb{Z}/n\mathbb{Z})^*$. On appelle ce revêtement le $\mathbb{Z}/n\mathbb{Z}$-revêtement élémentaire de $\mathbb{P}^1$.

Note: Ce n'est pas un résultat nouveau, on sait déjà depuis longtemps réaliser les groupes abéliens sur $\mathbb{Q}(T)$ (e.g. [Ser]), mais ici on a un contrôle explicite sur la ramification.

Réalisation pour un groupe fini quelconque.

Prenons un nombre premier p quelconque et un groupe fini G. Dans la suite, pour tout élément x donné dans un groupe G donné, on note n_x l'ordre de x et $H_x \simeq \mathbb{Z}/n_x\mathbb{Z}$ le sous-groupe engendré par x dans G.

Pour tout $x \in G$, on prend le H_x-revêtement élémentaire de $\mathbb{P}^1$, $\phi_x^{elem} : X_x \to \mathbb{P}^1$. On "recolle" ces revêtements grâce à la proposition 3.1.3 et on obtient un G-revêtement $\phi^{HL} : X \to \mathbb{P}^1$ de groupe de Galois G. Le nombre de points de ramification et l'invariant canonique de l'inertie de ce revêtement sont indépendants de p (voir que cet invariant canonique de l'inertie est le uplet C du préambule de la partie 2). On note à présent ce revêtement le revêtement HL de $\mathbb{P}^1$ associé à G.

Lemme 3.2.3 *L'invariant canonique de l'inertie du revêtement HL associé à G est un uplet rationnel.*

Preuve: On pose $r = \sharp G$ (ordre de G) et $G = (y_1, \cdots, y_r)$ avec $y_1 = 1$ et on écrit l'invariant canonique de l'inertie $\mathbf{C}$ ainsi:

$$\mathbf{C} = (C_{y_2,1}, \cdots, C_{y_2,\varphi(n_{y_2})}, \cdots\cdots, C_{y_r,1}, \cdots, C_{y_r,\varphi(n_{y_r})})$$

où les $C_{y_i,j}$ sont les classes de conjugaisons des générateurs du groupe $< y_i >$. En fait, si on pose $C_i = (C_{y_i,1}, \cdots, C_{y_i,\varphi(n_{y_i})})$ on a alors

$$\mathbf{C} = (C_2, \cdots, C_r)$$

Montrons que pour $a \in \mathbb{N}$ premier avec $\sharp G$ et tout indice $i = 2, \cdots, r$, C_i^a reste globalement invariant. L'application $\psi_a : (\mathbb{Z}/n_{y_i}Z)^* \to (\mathbb{Z}/n_{y_i}Z)^*$ qui à t associe t^a est une bijection. Toute classe $C_{y_i,j}$, $j = 1, \cdots, \varphi(n_{y_i})$, est la classe de conjugaison d'un générateur $t \in < y_i >$. La classe $(C_{y_i,j})^a$ est la classe de conjugaison dans G de t^a qui est aussi un générateur de $< y_i >$. Donc il existe k tel que $(C_{y_i,j})^a = C_{y_i,k}$. Cette correspondance se fait de façon biunivoque du fait de la bijectivité de ψ_a. Ceci achève la preuve.

De façon plus précise on vient de montrer que pour tout entier a premier avec $\sharp G$, il existe $(\sigma_2, \cdots, \sigma_r) \in S_{\varphi(n_{y_2})} \times \cdots \times S_{\varphi(n_{y_r})}$ tel que:

$$\begin{aligned} \mathbf{C}^a &= (C_{y_2,1}, \cdots, C_{y_2,\varphi(n_{y_2})}, \cdots\cdots, C_{y_r,1}, \cdots, C_{y_r,\varphi(n_{y_r})})^a \\ &= (C_{y_2,\sigma_2(1)}, \cdots, C_{y_2,\sigma_2(\varphi(n_{y_2}))}, \cdots\cdots, C_{y_r,\sigma_r(1)}, \cdots, C_{y_r,\sigma_r(\varphi(n_{y_r}))}) \end{aligned}$$

Pour tout entier b, on "recolle" (par 3.1.3) b fois le revêtement HL associé à G en regardant b fois G comme un de ses sous-groupe. On obtient alors un G-revêtement de $\mathbb{P}^1$ de groupe de Galois G avec un nombre de point de ramification indépendant de p et un invariant canonique de l'inertie égale au $\mathbf{C}_b$ du préambule de la partie 2. Cet uplet reste évidemment rationnel.

3.2.2 Fin de la preuve

Grâce au théorème 3.1.2 pour b assez grand (par exemple $b \geq b_0$), l'espace de Hurwitz $\mathcal{H}(\mathbf{C}_b)$ défini sur $\mathbb{Q}$ est irréductible. On vient de montrer que pour tout nombre premier p, il existe un G-revêtement de $\mathbb{P}^1$ défini sur $\mathbb{Q}_p$, de groupe de Galois G, ayant autant de points de ramification qu'il y a de classes dans $\mathbf{C}_b$ et $\mathbf{C}_b$ pour invariant canonique de l'inertie. Ceci prouve donc qu'il existe un point $\mathbb{Q}_p$-rationnel sur $\mathcal{H}(\mathbf{C}_b)$.

Il nous reste à traiter le cas où $p = \infty$. C'est à dire qu'il nous faut prouver l'existence d'un G-revêtement $\beta : X \to \mathbb{P}^1$ défini sur $\mathbb{R}$ ayant autant de points de ramification qu'il y a de classes dans $\mathbf{C}_b$, G comme groupe de Galois et $\mathbf{C}_b$ pour invariant canonique de l'inertie.

Pour ce, nous rappellons ce résultat (e.g. [FrD,Th.3.1]):

Lemme 3.2.4 *Soit* $\mathbf{C} = (C_1, C_1^{-1} \cdots, C_r, C_r^{-1})$ *un r-uplet de couple inverse deux à deux de classes de conjugaison d'éléments de* G. *Supposons qu'il existe* $(g_1, \cdots, g_r) \in C_1 \times \cdots \times C_r$ *tel que* $< g_1, \cdots, g_r >= G$. *Alors il existe un* G*-revêtement de* $\mathbb{P}^1$ *défini sur* $\mathbb{R}$ *de groupe de Galois* G, *ayant* $2r$ *points de ramification et* C *pour invariant canonique de l'inertie.*

Ce lemme nous permet de conclure. En effet reprenons le uplet $\mathbf{C}_b$ précédent. On rappelle que si $G = \{e = y_1, y_2, \cdots, y_{\sharp G}\}$ alors $\mathbf{C}_b = (C, \cdots, C)$ (b fois C) avec $C = (C_{y_2}, \cdots, C_{y_{\sharp G}})$ où:

- $C_{y_i} = (\{g_{1,y_i}\}^G, \cdots, \{g_{n_{y_i},y_i}\}^G)$ où les g_{j,y_i} sont les générateurs du sous-groupe $< y_i >$, si $n_{y_i} \neq 2$.
- $C_{y_i} = (\{y_i\}^G, \{y_i\}^G)$ si $n_{y_i} = 2$.

Dans les deux cas il est clair que l'on peut grouper par paires (C_{ij}, C_{ij}^{-1}) les composantes du uplet C_{y_i}, $i = 2 \cdots, \sharp G$. Ceci assure donc que C_b vérifie les conditions du lemme 3.2.4. Par conséquent il existe un G-revêtement de $\mathbb{P}^1$ défini sur $\mathbb{R}$, de groupe de Galois G ayant $\mathbf{C}_b$ pour invariant canonique de l'inertie. En conclusion il existe un point $\mathbb{R}$-rationnel sur l'espace de Hurwitz $\mathcal{H}(C_b)$.

Rappellons le résultat de Pop ([PRG]) qui achevera la preuve de la première assertion du théorème 3.1.2:

Proposition 3.2.3 *Dans toute variété lisse, irréductible, définie sur* $\mathbb{Q}$, *l'ensemble des points* $\mathbb{Q}^{tp}$*-rationnel est dense dans l'ensemble des points* $\mathbb{Q}^p$*-rationnels.*

Ainsi, pour tout p (y compris $p = \infty$) il existe au moins un point $\mathbb{Q}^{tp}$-rationnel sur $\mathcal{H}(\mathbf{C}_{b_0})$.

3.2.3 Comportement des points de ramification sous l'action de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$.

Cette partie, qui a pour but de prouver la deuxième assertion du théorème 3.1.2, regarde plus précisément comment sont modifiés les points de ramification quand on "recolle" par le théorème 3.1.3 les $\mathbb{Z}/n\mathbb{Z}$-revêtements élémentaires. Il faut rappeler (Cf [Liu], [Des1]) que la première étape de ce théorème de recollement consiste à mettre les points de ramification des deux revêtements que l'on souhaite rencontrer en "bonne position". On utilise pour cela des automorphismes de $\mathbb{P}^1$, i.e. des homographies $\dfrac{az+b}{cz+d}$ avec $a, b, c, d \in \mathbb{Q}_p$. Le corps $\mathbb{Q}$ étant dense dans $\mathbb{Q}_p$, on peut choisir a, b, c, d dans $\mathbb{Q}$. On obtient donc la conclusion suivante:

Lemme 3.2.5 *Soient $\pi_i : X_i \to \mathbb{P}^1$, $i = 1, 2$ deux G-revêtements définis sur $\mathbb{Q}_p$ vérifiants les hypothèses de la proposition 3.2.1. Supposons que $t_1^i, t_2^i, \cdots, t_{n_i}^i$, $i = 1, 2$ soient leurs point de ramification respectifs. Alors il existe $a_1, b_1, c_1, d_1 . a_2, b_2, c_2, d_2 \in \mathbb{Q}$ (dépendants des données précédentes et notament de p) tel que l'ensemble des points $v_{i,j} = \dfrac{a_i t_j^i + b_i}{c_i t_j^i + d_i}$ soit l'ensemble des point de ramification du revêtement $\pi : X \to \mathbb{P}^1$ obtenu en recollant π_1 et π_2.*

Il est clair que les $\mathbb{Z}/n\mathbb{Z}$-revêtements élémentaires ont des points de ramification définis sur $\mathbb{Q}^{ab}$ et globalement invariants par l'action de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$: c'est toujours l'ensemble des racines primitives n-ième de l'unité pour un certain n. Grâce au lemme précédent, il est alors clair que le revêtement obtenu au paragraphe 3.2.1 à des points de ramification dans $\mathbb{Q}^{ab}$ globalement invariant par $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Ceci achève la preuve du théorème 3.1.2.

Chapitre 4

Clôture totalement réelle des corps ordonnables

4.1 Introduction

Nous avons vu dans le chapitre II, que $\mathbb{Q}^{tr}$ est un corps ample. Nous avons vu aussi que $\mathbb{Q}^{tr}(\sqrt{-1})$ est un corps PAC. Ceci nous a permis de déduire que le groupe de Galois absolu, $G_{\mathbb{Q}^{tr}(\sqrt{-1})}$, de $\mathbb{Q}^{tr}(\sqrt{-1})$ est pro-libre. Comme nous l'avons signalé, ce résultat peut-être vu comme un analogue de la conjecture de Shafarevic qui prévoit que le groupe de Galois absolu de $\mathbb{Q}^{ab}$ est pro-libre. En effet la clôture cyclotomique $(\mathbb{Q}^{tr})^{cycl}$ de $\mathbb{Q}^{tr}$ est $\mathbb{Q}^{tr}(\sqrt{-1})$ (de même que $\mathbb{Q}^{cycl} = \mathbb{Q}^{ab}$).

Un des objets de ce chapitre, est d'essayer de généraliser ce résultat à certains corps construits de façon similaire à $\mathbb{Q}^{tr}$. Plus exactement, le corps $\mathbb{Q}^{tr}$ peut être vu comme l'intersection de toutes les extensions ordonnées maximales algébriques de $\mathbb{Q}$. On introduit dans la première partie la notion de *clôture totalement réelle* d'un corps ordonnable K (Définition 4.2.2), comme étant l'intersection de toutes les extensions ordonnées maximales algébriques de K, on note $\widetilde{K}_{tr}$ ce corps. La théorie d'Artin-Schreier permet de mieux décrire cet objet en faisant le rapprochement entre $\widetilde{K}_{tr}$ et les extensions galoisiennes ordonnables de K.

La deuxième partie présente quelques propriétés arithmétiques de $\widetilde{K}_{tr}$. Notamment ce corps est toujours un corps pythagoricien, d'autre part dans le cas où K est une extension algébrique ordonnable de $\mathbb{Q}$, le résultat de Pop entraine que $\widetilde{K}_{tr}(\sqrt{-1})$ est un corps PAC. Nous faisons le lien avec une question posée par Ribenboïm, lors de la conférence de Lille 96, sur le rapport pouvant exister entre la notion de corps pythagoricien, celle de corps ample et celle de corps hilbertien.

Une autre propriété remarquable de $\widetilde{K}_{tr}$ est que $(\widetilde{K}_{tr})^{cycl} = \widetilde{K}_{tr}(\sqrt{-1})$ (Proposition 4.3.1). On s'intéresse donc à l'analogue de la conjecture de Shafarevic pour les clôtures totalement réelles des corps ordonnés; c'est l'objet de la troisième partie où l'on regarde la pro-liberté du groupe de Galois absolu de $\widetilde{K}_{tr}(\sqrt{-1})$. Dans certains cas (corps de nombres ordonnables, corps ordonnés maximaux ou corps de séries de Laurent à coefficients dans un corps ordonné maximal) ce groupe est bien pro-libre. Récement, Dan Haran et Moshe Jarden [HaJa2] on donné d'autres exemples où ce résultat reste vrai, mais ils donnent aussi un contre exemple qui prouve que l'on ne peut pas généraliser ce résultat à toute les clôtures totalement réelles, comme nous l'avions conjecturé en premier. Ils proposent

alors la conjecture moins générale suivante: Pour tout corps K ordonnable, dénombrable et hilbertien, le groupe de Galois absolu de $\widetilde{K}_{tr}(\sqrt{-1})$ est pro-libre.

Enfin nous montrons que si K est une extension algébrique et ordonnable de $\mathbb{Q}$, alors le groupe de Brauer de $\widetilde{K}_{tr}$ est un groupe de 2-torsion. De manière plus générale on a en fait que si le groupe de Galois absolu de $\widetilde{K}_{tr}(\sqrt{-1})$ est projectif alors $Br(\widetilde{K}_{tr})$ est un groupe de 2-torsion. L'étude de la réciproque permetrait de ramener la conjecture à une étude cohomologique.

4.2 Clôtures totalement réelles des corps ordonnables.

Dans cette partie nous utiliserons les résultats principaux de la théorie d'Artin-Schreier sur les corps ordonnés. Nous renvoyons le lecteur à [R,ch IX] dont nous utilisons la terminologie. Dans tout ce qui suit, K désignera un corps ordonnable et G_K le groupe de Galois absolu $Gal(\overline{K}/K)$ de K.

4.2.1 Généralités.

On considère ici les classes de conjugaison des éléments d'ordre 2 de G_K. Ainsi deux éléments c, c' d'ordre 2 de G_K sont conjugués ssi il existe $\sigma \in G_K$ tel que $c = \sigma c' \sigma^{-1}$. Notons alors que si $K_c = \overline{K}^{<c>}$ et $K_{c'} = \overline{K}^{<c'>}$, on a $\sigma(K_c) = K_{c'}$. Réciproquement, rappellons cet élément de la théorie d'Artin-Schreier: l'ensemble des corps K_0 extensions algébriques de K tels que $[\overline{K} : K_0] < +\infty$ est exactement l'ensemble des extensions ordonnées maximales de K. Dans ce cas, on a toujours $[\overline{K} : K_0] = 2$.

Définition 4.2.1 *On appelle pré-clôture totalement réelle de K tout corps obtenu comme intersection des extensions ordonnées maximales de K appartenant à la même classe de conjugaison, en d'autres termes L est une pré-clôture totalement réelle de K ssi il existe $c \in G_K$ d'ordre 2 tel que:*

$$L = \bigcap_{\sigma \in G_K} \overline{K}^{<\sigma c \sigma^{-1}>}$$

Dans le cas de $\mathbb{Q}$ il n'y a qu'une seule pré-clôture totalement réelle, c'est $\mathbb{Q}^{tr}$.

Proposition 4.2.1 *Les propriétés suivantes sont équivalentes:*

i) L est une pré-clôture totalement réelle de K.

ii) L est une extension galoisienne ordonnable maximale (pour ces deux conditions) de K.

iii) Il existe $c \in G_K$ d'ordre 2 tel que $L \subset K_c = \overline{K}^{<c>}$ et telle que

$$L = \{x \in K_c / \forall \sigma \in G_K,\ \sigma(x) \in K_c\}$$

Preuve:

i) $\Rightarrow$ *ii)* Par définition, il existe $c \in G_K$ d'ordre 2 tel que L soit le sous-corps de $\overline{K}$ laissé fixe par le sous-groupe G de G_K engendré par les $\sigma c \sigma^{-1}$. Le groupe G est visiblement distingué, son adhérence (pour la topologie de Krull) l'est donc aussi. Par conséquent l'extension L/K est galoisienne.

Soit maintenant L'/K une extension galoisienne ordonnable telle que $L \subset L'$. Soit K_0 un corps ordonné maximal contenant L' de groupe de Galois absolu $\{1, c\}$. Comme

$L' \subset \overline{K}^{<c>}$ et que L'/K est extension galoisienne, on en déduit que pour tout $\sigma \in G_K$, $L' \subset \overline{K}^{<\sigma c \sigma^{-1}>}$. Donc $L' \subset L$

ii) $\Rightarrow$ *iii)* Soit L/K une extension galoisienne ordonnable maximale. Il existe une extension K_c ordonnée maximale contenant L. Soit

$$L' = \{x \in K_c / \forall \sigma \in G_K,\ \sigma(x) \in K_c\}$$

Soit $x \in L$ et $\sigma \in G_K$, on a $\sigma(x) \in L \subset K_c$, donc $L \subset L'$.

Maintenant, il est clair que L'/K est une extension ordonnable et galoisienne. Donc $L = L'$

iii) $\Rightarrow$ *i)* Evident. □

Définition 4.2.2 *Soit K un corps ordonnable. On appelle clôture totalement réelle de K, l'intersection de ses pré-clôtures totalement réelles, ou de manière équivalente, l'intersection de toute les extensions algébriques ordonnées maximales de K. On note ce corps $\widetilde{K}_{tr}$.*

Le groupe de Galois absolu de la clôture totalement réelle d'un corps ordonné K est donc l'adhérence du sous-groupe de G_K généré par les éléments de 2-torsion (qui sont exactement les éléments de torsion de G_K d'après la théorie d'Artin-Schreier).

4.2.2 Exemples

Le premier exemple est, comme nous l'avons remarqué plus haut, $\widetilde{\mathbb{Q}}_{tr} = \mathbb{Q}^{tr}$. Regardons maintenant $\mathbb{Q}(\sqrt{2})$; il est facile de voir que $\widetilde{\mathbb{Q}(\sqrt{2})}_{tr} = \mathbb{Q}^{tr}$. De manière générale, on a:

Proposition 4.2.2 *Si K est un corps ordonnable tel que $K \subset \mathbb{Q}^{tr}$ (en particulier si K est une extension galoisienne ordonnable de $\mathbb{Q}$), alors $\widetilde{K}_{tr} = \mathbb{Q}^{tr}$.*

Preuve: Comme $K \subset \mathbb{Q}^{tr}$, on a donc $\widetilde{K}_{tr} \subset \widetilde{\mathbb{Q}^{tr}}_{tr} = \mathbb{Q}^{tr}$ (en effet, si L/K est une extension algébrique ordonnable, alors $\widetilde{K}_{tr} \subset \widetilde{L}_{tr}$; de plus, on a toujours $(\widetilde{K}_{tr})_{tr} = \widetilde{K}_{tr}$). De plus, $\mathbb{Q} \subset K$, donc $\mathbb{Q}^{tr} \subset \widetilde{K}_{tr}$. □

Remarque 1: Lorsque $K = \mathbb{Q}(\alpha)$ est un corps de nombres ordonnable non inclus dans $\mathbb{Q}^{tr}$ (par exemple $K = \mathbb{Q}(\sqrt[3]{2})$) le problème est plus délicat. On sait que $\mathbb{Q}^{tr}(\alpha) \subset \widetilde{K}_{tr}$. On peut affirmer que cette inclusion est toujours stricte et même que $[\widetilde{K}_{tr} : \mathbb{Q}^{tr}(\alpha)]$ est infini. En effet, d'après le théorème de Weissauer, toute extension finie de $\mathbb{Q}^{tr}(\alpha)$ est hilbertienne. Mais $\widetilde{K}_{tr}$ est pythagoricien (proposition 4.3.2) donc ne peut pas être hilbertien (remarque 3). Il semble difficile, a priori, de décrire simplement $\widetilde{K}_{tr}$. On verra (cf 4.4.1) que dans ce cas on a toutefois de bonnes informations sur le groupe de galois absolu de $\widetilde{K}_{tr}(\sqrt{-1})$: il est pro-libre.

Regardons maintenant le cas d'une extension transcendante de $\mathbb{Q}$. On pose $\mathbb{Q}^r = \overline{\mathbb{Q}} \cap \mathbb{R}$. Soit alors $K = \mathbb{Q}^r((X))$ le corps des séries de Laurent à coefficients dans $\mathbb{Q}^r$ (c'est un corps ordonnable, par exemple par l'ordre lexicographique).

Proposition 4.2.3 *On a $\widetilde{\mathbb{Q}^r((X))}_{tr} = \mathbb{Q}^r((X))$. De manière plus précise, $\mathbb{Q}^r((X))$ ne possède que deux pré-clôtures totalement réelles qui sont $\mathbb{Q}^r((\sqrt{X}))$ et $\mathbb{Q}^r((\sqrt{-X}))$.*

Preuve: Soit $E/\mathbb{Q}^r((X))$ une extension galoisienne ordonnable maximale. Il est clair que $E \cap \overline{\mathbb{Q}} = \mathbb{Q}^r$: sinon cette intersection vaut $\overline{\mathbb{Q}}$ tout entier et alors E n'est plus ordonnable (car $\sqrt{-1} \in E$). On en déduit alors que E est une extension régulière sur $\mathbb{Q}^r$.

Considérons une extension galoisienne $F/\mathbb{Q}^r((X))$ de degré fini $n > 1$, avec $F \subset E$ et posons $F' = \overline{\mathbb{Q}}.F$. Comme $F/\mathbb{Q}^r((X))$ est régulière, il s'ensuit que $F'/\overline{\mathbb{Q}}((X))$ est galoisienne de degré n. D'après le théorème de Puiseux, $F' = \overline{\mathbb{Q}}((X^{1/n}))$ et $Gal(F'/\overline{\mathbb{Q}}((X)))$ est le groupe cyclique $\mathbb{Z}/n$ engendré par l'automorphisme σ_0 qui laisse invariant $\overline{\mathbb{Q}}$ et qui envoie $X^{1/n}$ sur $\zeta_n X^{1/n}$ (ζ_n désigne une racine primitive n-ième de l'unité fixée une fois pour toutes).

Il est clair que $F \subset F'$. On a les extensions:

$$\begin{array}{ccc} \mathbb{Q}^r((X)) & \xrightarrow{\mathbb{Z}/2} & \overline{\mathbb{Q}}((X)) \\ {\scriptstyle \mathbb{Z}/n}\downarrow & & {\scriptstyle \mathbb{Z}/n}\downarrow \\ F & \xrightarrow{\mathbb{Z}/2} & F' \end{array}$$

L'extension $F'/\mathbb{Q}^r((X))$ est galoisienne et son groupe de Galois est isomorphe au groupe diédral D_n. En effet, la conjugaison complexe c est un automorphisme de $Puis(\overline{\mathbb{Q}})$ qui relève l'élément non trivial de $Gal(\overline{\mathbb{Q}}((X))/\mathbb{Q}^r((X)))$ dans $Gal(F'/\mathbb{Q}^r((X)))$. On vérifie facilement que l'action de c sur σ_0 est ${\sigma_0}^c = \sigma_0^{-1}$.

Le groupe $Gal(\overline{\mathbb{Q}}((X^{1/n}))/F)$ est un sous-groupe distingué d'ordre 2 de D_n. Par conséquent n est pair et si $n > 2$ alors ce groupe est le centre $Z(D_n)$ de D_n. Mais dans $Z(D_n) \subset \mathbb{Z}/n$ laisse fixe $\overline{\mathbb{Q}}$, ce qui contredit $F \cap \overline{\mathbb{Q}} = \mathbb{Q}^r$, donc $n = 2$

Ainsi, il existe $S(X) \in \mathbb{Q}^r((X))$ qui n'est pas un carré et tel que $F = \mathbb{Q}^r((X))(\sqrt{S(X)})$. Deux cas se présentent alors,

1/ Soit $S(X) = X^\alpha(1 + \sum_{n>0} a_n X^n)$ (α impair) et dans ce cas $F = \mathbb{Q}^r((\sqrt{X}))$.

2/ Soit $S(X) = -X^\alpha(1 + \sum_{n>0} a_n X^n)$ (α impair) et dans ce cas $F = \mathbb{Q}^r((\sqrt{-X}))$.

Ces deux corps sont bien ordonnables puisqu'ils sont tout deux isomorphes à $\mathbb{Q}^r((X))$. Maintenant, E ne peut pas contenir simultanément $\mathbb{Q}^r((\sqrt{X}))$ et $\mathbb{Q}^r((\sqrt{-X}))$, sinon E contiendrait $\sqrt{-1}$, ce qui est impossible puisque E est ordonnable. Comme E est limite inductive de ses sous-extensions galoisiennes finies, E est soit $\mathbb{Q}^r((\sqrt{X}))$, soit $\mathbb{Q}^r((\sqrt{-X}))$. L'intersection de ces deux corps est bien réduite à $\mathbb{Q}^r((X))$ □

Remarque 2: L'exemple précédent se généralise à $K((X))$ quand K désigne une extension ordonnée maximale d'un corps ordonnable quelconque (par exemple $\mathbb{R}((X))$). Dans le cas de $\mathbb{Q}((X))$, le problème est plus délicat car nous possédons moins de renseignements sur la nature des extensions finies de ce corps.

Il reste de nombreux cas où $\widetilde{K_{tr}}$ semble difficile à déterminer. Prenons par exemple $K = \mathbb{Q}(X)$, si l'on pose $\Omega = \widetilde{K_{tr}} \cap \overline{\mathbb{Q}}$, alors on a $\mathbb{Q}^{ab} \cap \mathbb{Q}^{tr} \subset \Omega \subset \mathbb{Q}^{tr}$ (voir proposition 4.3.1 pour la première inclusion). Le corps $\widetilde{K_{tr}}$ est donc une extension régulière infinie de $\Omega(X)$. Car $\widetilde{K_{tr}}$ est un corps pythagoricien et que toute extension finie de $\Omega(X)$ est hilbertienne. Que dire de $\widetilde{\mathbb{Q}(X)}_{tr}$ et plus généralement de $\widetilde{K(X)}_{tr}$ quand K est un corps ordonnable quelconque?

4.3 Propriétés arithmétiques.

4.3.1 Clôture cyclotomique.

Une propriété importante des clôtures totalement réelles est que, bien que ne possédant aucune autre racine de l'unité que 1 et -1 on a:

Proposition 4.3.1 *Soit K un corps ordonné, alors*

$$(\widetilde{K_{tr}})^{cycl} = \widetilde{K_{tr}}(\sqrt{-1})$$

Preuve: Remarquons tout d'abord le fait suivant: Soit K_0 un corps ordonné et $c \in G_{K_0}$ d'ordre 2. Si ζ_n est une racine n-ième de l'unité alors $c(\zeta_n) = \zeta_n^{-1}$. En effet, soit $K = \overline{K_0}^{<c>}$, K est une extension algébrique ordonnée maximale. On a $\zeta_n c(\zeta_n) \in K$, mais comme $\zeta_n c(\zeta_n)$ est aussi une racine de l'unité, on en déduit que $\zeta_n c(\zeta_n) = \pm 1$. (En effet, un corps ordonné K_0 ne possède pas d'autre racine de l'unité que 1 et -1 car si $\zeta \in K_0$ est tel que $\zeta^p = 1$ pour un certain $p \in \mathbb{N}$, alors si $|\zeta| \neq 1$, comme K_0 est ordonné, $|\zeta^p| \neq 1$). Maintenant, il existe un couple unique $(\alpha, \beta) \in K^2$ tel que $\zeta_n = \alpha + \sqrt{-1}\beta$, donc $\zeta_n c(\zeta_n) = \alpha^2 + \beta^2$. Si $\zeta_n c(\zeta_n) = -1$ alors $\alpha^2 + \beta^2 = -1$ et K n'est plus ordonnable. Par conséquent $\zeta_n c(\zeta_n) = 1$.
Une fois ce fait établi, on prend ζ_n une racine primitive n-ième de l'unité, on note $\alpha_n = \zeta_n + \zeta_n^{-1}$ et $\beta_n = \sqrt{-1}(\zeta_n - \zeta_n^{-1})$. D'après ce qui précède, pour toute extension algébrique ordonnée maximale R, de groupe de Galois $Gal(\overline{K}/R) = \{1, c\}$, on a $\alpha_n = \zeta_n + \zeta_n^{-1} = \zeta_n + c(\zeta_n) \in R$ et $\beta_n = \sqrt{-1}(\zeta_n - \zeta_n^{-1}) = \sqrt{-1}(\zeta_n - c(\zeta_n)) \in R$. Donc α_n et β_n sont dans $\widetilde{K_{tr}}$. Or $\zeta_n = \frac{1}{2}(\alpha_n - \sqrt{-1}\beta_n) \in \widetilde{K_{tr}}(\sqrt{-1})$. □

4.3.2 Sommes de carrés.

Rappellons tout d'abord qu'un corps K est dit pythagoricien ssi toute somme de carrée d'éléments de K est un carré dans K. i.e. $K^2 = K^2 + K^2$.

Proposition 4.3.2 *Soit K un corps ordonnable. $\widetilde{K_{tr}}$ est un corps pythagoricien. Plus généralement, toute pré-clôture totalement réelle K est un corps pythagoricien.*

Preuve: Les extensions algébriques ordonnées maximales de K sont toujours des corps pythagoriciens. En effet soit K_0 une extension ordonnée maximale de K, on a $\overline{K} = K_0(\sqrt{-1})$. Soit x, y deux éléments de K. Il existe α, β dans K_0 tel que $x^2 + y^2 = (\alpha + \sqrt{-1}\beta)^2$, en développant on trouve $\alpha\beta = 0$. Si $\beta \neq 0$ alors $\alpha = 0$ et alors $x^2 + y^2 + \beta^2 = 0$ ce qui est absurde car K_0 est ordonné. Donc $x^2 + y^2 = \alpha^2$ et K_0 est pythagoricien.

La clôture totalement réelle ainsi que toutes les pré-clôtures totalement réelles sont des intersections de corps pythagoriciens inclus dans un corps algébriquement clos donné; elles sont donc pythagoriciennes. □

Remarques 3:

a) Si K un corps ordonnable, alors $\widetilde{K_{tr}}$ n'est jamais hilbertien. Ceci vient du fait qu'un corps ne peut pas être à la fois pythagoricien et hilbertien. En effet, soit K un corps pythagoricien. Sur $K(X)$ considérons le polynôme $P(X, Y) = Y^2 - (1 + X^2)$. Ce polynôme étant irréductible si K était hilbertien il existerait $x \in K$ tel que $P(x, Y) \in K[Y]$ soit irréductible. En conséquence $x^2 + 1$ ne serait pas un carré.

b) A l'inverse un corps non pythagoricien peut-être hilbertien ou non:

$\mathbb{Q}$ ou bien même tout corps de nombres, est hilbertien sans être pythagoricien.

Maintenant, prenons un nombre premier $p > 2$, alors $\mathbb{Q}_p$ n'est pas hilbertien (c'est un corps henselien). Il n'est pas pythagoricien non plus (il suffit de prendre $a \in \mathbb{F}_p$ qui n'est pas un carré, alors a est somme de deux carré dans $\mathbb{F}_p$, $a = \overline{x}^2 + \overline{y}^2$. Relevé dans $\mathbb{Q}_p$, $x^2 + y^2$ ne peut pas être un carré).

4.3.3 Points $\widetilde{K}_{tr}$-rationnels sur les courbes.

Rappelons qu'un corps K est dit ample ssi toute courbe lisse et définie sur K possédant un point K-rationnel en possède une infinité (pour plus de détail, consulter par exemple [DD]). Un corps PAC est toujours ample. Pop à montré que $\mathbb{Q}^{tr}$ est un corps ample. Cette propriété nous apporte un renseignement fondamental sur $\widetilde{K}_{tr}$:

Proposition 4.3.3 *Soit K un corps ordonnable algébrique sur $\mathbb{Q}$, alors $\widetilde{K}_{tr}$ est un corps ample et $\widetilde{K}_{tr}(\sqrt{-1})$ est un corps PAC*

Preuve: Dans ce cas $\widetilde{K}_{tr}$ est une extension algébrique de $\mathbb{Q}^{tr}$ qui est ample d'après le théorème de Pop. Toute extension algébrique d'un corps ample est encore ample [Pop4]. De même $\widetilde{K}_{tr}(\sqrt{-1})$ est une extension algébrique de $\mathbb{Q}^{tr}(\sqrt{-1})$ et toute extension algébrique d'un corps PAC est encore PAC [FJ]. □

Remarque 4: On peut se demander si dans le cas général, $\widetilde{K}_{tr}$ est ample. Il est pythagoricien, mais existe-t-il un lien entre la propriété d'être pythagoricien et celle d'être hilbertien? Voici quelques exemples:

1/ $\mathbb{Q}$ est un corps qui n'est ni ample ni pythagoricien.

2/ $\mathbb{Q}^{tr}(\sqrt{-1})$ est un corps qui est ample et non pythagoricien. En effet ce corps est PAC donc ample, il est hilbertien donc non pythagoricien.

3/ $\mathbb{Q}^{tr}$ ou bien même tout corps algébriquement clos sont des corps qui sont amples et pythagoriciens: .

4/ La question de Ribenboïm est de savoir si les corps pythagoriciens sont nécessairement amples. Dans le cas algébrique sur $\mathbb{Q}$, cela revient à savoir si $\mathbb{Q}^{pyth}$, la clôture pythagoricienne de $\mathbb{Q}$ (i.e le plus petit corps pythagoricien contenant $\mathbb{Q}$) est ample. On peut déjà remarquer que $\mathbb{Q}^{pyth}$, n'est pas un corps PAC car $\mathbb{Q}^{pyth}$ est un corps ordonné (en effet le polynôme $X^2 + Y^2 + 1$ n'a aucun zéro).

Dans cette perspective, signalons cette propriété de $\mathbb{Q}^{pyth}$ suivante: Aucune extension finie et stricte de $\mathbb{Q}^{pyth}$ n'est pythagoricienne. Cela résulte du fait que, d'après Weissauer, ces extensions sont hilbertiennes ($\mathbb{Q}^{pyth}/\mathbb{Q}$ est une extension galoisienne). On pourra consulter l'annexe 2 de cette thèse pour une généralisation de ce résultat.

4.4 Propriétés galoisiennes.

4.4.1 Groupe de Galois absolu.

Nous avons rappellé que $\mathbb{Q}^{tr}(\sqrt{-1})$ est un corps PAC et hilbertien et que donc $G_{\mathbb{Q}^{tr}(\sqrt{-1})}$ est pro-libre de rang dénombrable. Comme nous l'avons montré, pour tout corps ordonnable K, on a $(\widetilde{K}_{tr})^{cycl} = \widetilde{K}_{tr}(\sqrt{-1})$. Nous regardons alors l'analogue de la conjecture de Shafarevic pour les clôtures totalement réelles:

Problème: *Pour tout corps ordonnable K, le groupe de Galois absolu de $\widetilde{K}_{tr}(\sqrt{-1})$ est-il pro-libre?*

Le problème admet une réponse affirmative dans les cas suivants:

1/ Lorsque K est une extension ordonnée maximale d'un corps ordonnable quelconque (par exemple $\mathbb{R}$). Dans ce cas, si K désigne un tel corps, on a $\widetilde{K}_{tr} = K$ et par Artin-Schreier, on a $K(\sqrt{-1}) = \overline{K}$. Dans ce cas le groupe de Galois absolu est trivial; c'est donc un groupe pro-libre (de rang 0).

2/ Lorsque que $K = k((X))$, où k désigne une extension ordonnée maximale d'un corps ordonnable donné. En effet nous avons vu précédement que dans ce cas $\widetilde{K}_{tr} = K$. Alors $\widetilde{K}_{tr}(\sqrt{-1}) = \overline{k}((X))$ et d'après le théorème de Puiseux, le groupe de Galois absolu de ce corps est $\widehat{\mathbb{Z}}$, c'est à dire un groupe pro-libre de rang 1.

3/ Lorsque K est une extension algébrique, ordonnable et hilbertienne de $\mathbb{Q}$ (en particulier les corps de nombres ordonnables). En effet, dans ce cas $\widetilde{K}_{tr}(\sqrt{-1})$ est hilbertien d'après le théorème de Weissauer et il est PAC (proposition 6). Donc d'après le théorème de Fried-Volklein/Pop $G_{\widetilde{K}_{tr}(\sqrt{-1})}$ est pro-libre de rang dénombrable.

Dans cet exemple, on peut remplacer la condition K hilbertien par $\widetilde{K}_{tr}(\sqrt{-1})$ hilbertien. Ce résultat plus général peut par exemple s'appliquer à $K = \mathbb{Q}^{tr}$ qui n'est pas hilbertien.

Remarque 5: Le corps $\widetilde{K}_{hr}(\sqrt{-1})$ n'est pas toujours un corps hilbertien: il suffit de considérer une extension ordonnée maximale K de $\mathbb{Q}$ alors $K(\sqrt{-1}) = \overline{\mathbb{Q}}$ et $\overline{\mathbb{Q}}$ n'est bien évidement pas hilbertien. Dans le cas où K est une extension algébrique de $\mathbb{Q}$, le théorème de Roquette [FV] permet alors d'affirmer que $G_{\widetilde{K}_{tr}(\sqrt{-1})}$ est pro-libre (non trivial) ssi $\widetilde{K}_{tr}(\sqrt{-1})$ est hilbertien.

Haran et Jarden ont donné [HaJa] d'autres exemples où le problème admet une réponse positive:

Théorème 4.4.1 *(Haran-Jarden) Pour tout entier non nul e, il existe une extension ordonnable K de $\mathbb{Q}(T)$ telle que*

$$G_{\widetilde{K}_{tr}(\sqrt{-1})} \simeq \widehat{F_e}$$

Ils ont aussi donné un contre exemple. Il propose alors la conjecture moins générale suivante:

Conjecture: *Pour tout corps ordonnable, dénombrable et hilbertien K, le groupe de Galois absolu de $\widetilde{K}_{tr}(\sqrt{-1})$ est pro-libre.*

Nous nous sommes intéressés à la structure de $G_{\widetilde{K}_{tr}(\sqrt{-1})}$, que peut-on dire de celle de $G_{\widetilde{K}_{tr}}$? Fried, Haran et Volklein ont montré dans $[FHV]$ que $G_{\mathbb{Q}^{tr}}$ était isomorphe à Δ, la complétion profinie du groupe libre sur un ensemble de générateurs d'ordre 2 homéomorphe à l'ensemble de Cantor dans $G_{\mathbb{Q}}$. Pop a généralisé par la suite ce résulat à certains corps. De manière générale, peut-on trouver une structure équivalente à $G_{\widetilde{K}_{tr}}$ sachant que $G_{\widetilde{K}_{tr}(\sqrt{-1})}$ est pro-libre?

Remarque 6: Il est à noter que le fait que $G_{\mathbb{Q}^{tr}(\sqrt{-1})} = \widehat{F_\omega}$ ($\widehat{F_\omega}$ désigne le groupe pro-libre à une infinité dénombrable de générateurs) ne permet pas de décrire proprement $G_{\mathbb{Q}^{tr}}$. En effet, la suite d'extensions $\mathbb{Q}^{tr} \subset \mathbb{Q}^{tr}(\sqrt{-1}) \subset \overline{\mathbb{Q}}$ donne la suite exacte suivante:

$$1 \longrightarrow \widehat{F_\omega} \longrightarrow G_{\mathbb{Q}^{tr}} \longrightarrow \mathbb{Z}/2 \longrightarrow 1$$

Cette suite est scindée, puisque l'élément non trivial de $\mathbb{Z}/2$ se relève (par exemple) en la conjugaison complexe dans $G_{\mathbb{Q}}$. De là, il est tentant d'écrire que

$$G_{\mathbb{Q}^{tr}} \simeq \widehat{F_\omega} \rtimes \mathbb{Z}/2$$

bien que ceci soit vrai, cela n'apporte pas de renseignements significatifs sur la structure de $G_{\mathbb{Q}^{tr}}$:

Considérons le corps $K = \mathbb{Q}^r(T)$ (on rappelle que $\mathbb{Q}^r = \overline{\mathbb{Q}} \cap \mathbb{R}$). Le corps $\mathbb{Q}^r$ est un corps ample, car c'est une extension algébrique de $\mathbb{Q}^{tr}$ qui est un corps ample. Le corollaire 2.3.3 du chapitre II montre alors que $G_{\overline{\mathbb{Q}(T)}} \simeq \widehat{F_\omega}$. Les mêmes remarques que précédemment montrent que

$$G_{\mathbb{Q}^r(T)} \simeq \widehat{F_\omega} \rtimes \mathbb{Z}/2$$

Pourtant, malgré l'apparente similitude on a $G_{\mathbb{Q}^r(T)} \not\simeq G_{\mathbb{Q}^{tr}}$. En effet, tous les groupes finis sont groupes de Galois sur $\mathbb{Q}^r(T)$ (conséquence du corollaire 2.3.1 du chapitre II), alors que seuls les groupes finis pouvant être engendrés par des éléments d'ordre 2 sont groupes de Galois sur $\mathbb{Q}^{tr}$ (conséquence immédiate de la structure de $G_{\mathbb{Q}^{tr}}$ vu plus haut).

Le point délicat consiste à bien décrire l'action de la conjugaison complexe sur $\widehat{F_\omega}$.

4.4.2 Groupe de Brauer.

On vient de voir que les groupes de Galois absolus des clôtures totalement réelles semblaient posséder de nombreux points communs. Ces corps partagent d'autres propriétés:

Proposition 4.4.1 *Soit K une extension algébrique ordonnable de $\mathbb{Q}$. Alors le groupe de Brauer, $Br(\widetilde{K_{tr}})$, de $\widetilde{K_{tr}}$ est isomorphe au groupe quotient $(\widetilde{K_{tr}}^*)/(\widetilde{K_{tr}}^*)^2$. C'est un groupe commutatif dénombrable dont tous les éléments sont d'ordre 2, il est par conséquent isomorphe soit à $(\mathbb{Z}/2)^n$ pour un certain $n \in \mathbb{N}$, soit à $\varinjlim_{n\in\mathbb{N}} (\mathbb{Z}/2)^n$. En particulier $Br(\mathbb{Q}^{tr}) = \varinjlim_{n\in\mathbb{N}} (\mathbb{Z}/2)^n$.*

Preuve: Nous avons noté (proposition 4.3.3) que $\widetilde{K_{tr}}(\sqrt{-1})$ était un corps PAC, il s'ensuit que $Br(\widetilde{K_{tr}}(\sqrt{-1})) = 0$ (en fait $\widetilde{K_{tr}}(\sqrt{-1})$ est un corps de dimension cohomologique plus petite que 1). La suite exacte $1 \to H^2(E/L) \to Br(L) \to Br(E)$ où E/L est un extension algébrique, donne alors l'isomorphisme $Br(\widetilde{K_{tr}}) \simeq H^2(\widetilde{K_{tr}}(\sqrt{-1})/\widetilde{K_{tr}})$. Reste à calculer ce dernier groupe de cohomologie:

Soit $x \in \widetilde{K_{tr}}^*(\sqrt{-1})$, on note $N(x) = x\overline{x} = |x|^2$ et $T(x) = \overline{x}x^{-1}$. On a alors $H^2(\widetilde{K_{tr}}(\sqrt{-1})/\widetilde{K_{tr}}) \simeq T^{-1}(1)/N(\widetilde{K_{tr}}^*(\sqrt{-1}))$. Ceci vient d'un lemme de cohomologie des groupes classique (voir par exemple [Ser2] ou [B,lemme IV.5,page 107]). On a clairement $T^{-1}(1) = \widetilde{K_{tr}}^*$ et puisque $\widetilde{K_{tr}}$ est pythagoricien, on a $N(\widetilde{K_{tr}}(\sqrt{-1})) = \widetilde{K_{tr}}^{*2}$. On obtient bien $Br(\widetilde{K_{tr}}) \simeq (\widetilde{K_{tr}}^*)/(\widetilde{K_{tr}}^*)^2$.

Vu sous cette forme, il est clair que $Br(\widetilde{K_{tr}})$ est au plus dénombrable et a tous ces éléments d'ordre 2. La donnée du cardinal d'un tel groupe commutatif définit à isomorphisme près ce groupe:
1/ Dans le cas où ce groupe est fini la structure est claire.
2/ Dans le cas où il est infini, il suffit de remarquer que $\varinjlim_{n\in\mathbb{N}} (\mathbb{Z}/2)^n$ est un groupe abélien dénombrable dont tous les éléments sont de 2-torsion et que 2 tels groupes sont isomorphes. En effet, prenons G un tel groupe et considérons C une famille d'éléments de G

maximale pour la propriété suivante : Pour toute sous-famille finie $C_f \subset C$, $\sum_{g \in C_f} g \neq 0$. C existe d'après Zorn, est infinie et engendre G sinon si $g_0 \in G - < C >$ alors la famille $C \cup \{g_0\}$ vérifie la propriété précédente et C n'est plus maximale.
Soit G' un autre groupe abélien dénombrable dont tous les éléments sont de 2-torsion et $C' \subset G'$ une famille d'éléments de G' maximale pour la propriété énoncée précédement. N'importe quelle bijection de C sur C' définit un isomorphisme entre G et G'.

Reste à voir que $Br(\mathbb{Q}^{tr})$ est bien infini. Pour cela il suffit de considérer les éléments $\sqrt{p}$ de $\mathbb{Q}^{tr}$ où p est un nombre premier. Chacun d'eux définit une classe distincte modulo $\mathbb{Q}^{tr*2}$: en effet si p et q sont deux nombres premiers distincts, il n'existe pas d'éléments $x \in \mathbb{Q}^{tr}$ tel que $\sqrt{p/q} = x^2$ car $\sqrt[4]{p/q}$ n'a pas tous ces conjugués dans $\mathbb{R}$. □

De manière générale, la question du cardinal de $Br(\widetilde{K}_{tr})$ se pose. Cette étude est reliée à celle des carrés de $\widetilde{K}_{tr}$. Par exemple, si l'on veut déterminer les extensions K algébriques de $\mathbb{Q}$, telles que $Br(\widetilde{K}_{tr}) = \mathbb{Z}/2$, il faut déterminer les corps K tels que $\widetilde{K}_{tr} = (\widetilde{K}_{tr}^2) \cup (-\widetilde{K}_{tr}^2)$. On sait déja que les extensions K ordonnées maximales de $\mathbb{Q}$ (e.g. $K = \overline{\mathbb{Q}} \cap \mathbb{R}$) vérifient $\widetilde{K}_{tr} = K$ et $Br(\widetilde{K}_{tr}) = \mathbb{Z}/2$. Le théorème de Whaples ([Rib]), permet de donner une caractérisation plus fine:

Proposition 4.4.2 *Soit K une extension algébrique ordonnable de $\mathbb{Q}$, alors $Br(\widetilde{K}_{tr}) = \mathbb{Z}/2$ ssi le groupe de Klein $G = \mathbb{Z}/2 \times \mathbb{Z}/2$ n'est pas groupe de Galois sur $\widetilde{K}_{tr}$.*

Preuve: En effet le théorème de Whaples affirme, entre autres choses, qu'il y a équivalence pour un corps K qui ne contient pas $\sqrt{-1}$ entre:

i) K n'a pas d'extension abélienne de degré 4 et

ii) $K = K^2 \cup (-K^2)$ et K est pythagoricien

Le corps $\widetilde{K}_{tr}$ étant toujours pythagoricien, d'après le théorème de Diller et Dress ([Rib]), $\widetilde{K}_{tr}$ n'a aucune extension cyclique de degré 4. Donc les seules extensions abéliennes à éviter pour $\widetilde{K}_{tr}$ sont celle de groupe $G = \mathbb{Z}/2 \times \mathbb{Z}/2$. □

Qu'en est-il des extensions transcendantes de $\mathbb{Q}$? Si on reprend l'exemple $K = \mathbb{Q}^r((X))$, la même démonstration que précédement (en remarquant que $\overline{\mathbb{Q}}((X))$ est de dimension cohomologique plus petite que 1) montre que $Br(\mathbb{Q}^r((X))) = \mathbb{Q}^r((X))^*/\mathbb{Q}^r((X))^{*2}$. On en déduit que $Br(\mathbb{Q}^r((X))) = \mathbb{Z}/2 \times \mathbb{Z}/2$, les éléments de ce groupe étant les classes de $1, -1, X, -X$. Cet exemple montre encore que les éléments du groupe de Brauer sont de 2-torsion. Ce point semble décisif pour l'étude de $G_{\widetilde{K}_{tr}(\sqrt{-1})}$. En effet si l'on considère les deux propositions:

i) $G_{\widetilde{K}_{tr}(\sqrt{-1})}$ est projectif.

ii) $Br(\widetilde{K}_{tr})$ est de 2-torsion.

la preuve de la proposition 4.4.1 s'étend sans problème pour montrer que $i) \Longrightarrow ii)$. La réciproque donnerait un angle d'attaque cohomologique pour notre conjecture. Remarquons que pour $ii) \Longrightarrow i)$, il suffit de prouver que toute extension galoisienne de $\widetilde{K}_{tr}$ contenant $\sqrt{-1}$ a un groupe de Brauer nul, c'est à dire que la 2-torsion est tuée par les extensions de $\widetilde{K}_{tr}$ de degré pair.

Appendice I
Problème(s) Inverse(s) de Galois

Finalement, qu'est-ce que le *problème inverse de la théorie de Galois*? Ce problème correspond à une conjecture célèbre et bien définie, mais nous voudrions suggérer que ce *problème*, ou tout du moins la façon dont on l'énonce d'habitude n'a rien d'implicite et qu'il y a peut-être des *problèmes inverses à la théorie de Galois*.

De manière générale, la théorie de Galois associe a un type d'objets, que sont les extensions galoisiennes finies (resp. infinies) de corps, un autre type d'objets, que sont les groupes finis (resp. pro-finis). Se poser la question inverse, ce serait donc regarder la correspondance réciproque. Mais c'est là qu'il peut y avoir plusieurs façons de considérer le(s) problème(s) inverse(s). Le premier chapitre de cette thèse à été consacré en partie, à l'exposé des conjectures modernes liées au problème inverse. Nous voulons présenter dans cette partie quelques autres questions, parfois naïves, parfois complexes, qui rentrent dans cette approche:

Problème 1: *Soit G un groupe fini. Existe-t-il une extension galoisienne finie L/K, telle que $Gal(L/K) = G$?*

Ce problème admet toujours une réponse affirmative. Donnons-en une preuve élémentaire: Si $card(G) = n$, on plonge G dans le groupe symétrique S_n par la représentation canonique. On considère alors le corps $L = \mathbb{Q}(X_1, \cdots, X_n)$ des fractions rationnelles sur $\mathbb{Q}$ à n indéterminées. Le groupe S_n agit sur K par permutation des variables. Si K désigne le sous-corps de L laissé fixe par S_n, alors L/K est galoisien de groupe S_n. Il est facile de voir que $K = \mathbb{Q}(\sigma_1, \cdots, \sigma_n)$ où σ_i désigne la i-ème fonction symétrique élémentaire. K est une extension transcendante pure de $\mathbb{Q}$ de degré n (c'est à dire $\mathbb{Q}$ isomorphe à L). Le corps $\mathbb{Q}$ étant un corps hilbertien, on peut "descendre" l'extension L/K à une extension $N/\mathbb{Q}$ tel que $N/\mathbb{Q}$ soit galoisienne de groupe de Galois S_n. On pose alors $M = N^G$ et l'extension N/M est galoisienne de groupe de Galois G.

On peut donc toujours trouver une extension galoisienne de corps de nombres de groupe de Galois un groupe fini donné. Mais on remarque alors qu'il n'y a aucun contrôle sur le corps de base ni même sur l'extension, ces deux données variant en fonction de G. Cela nous amène donc a considérer un autre type de problème:

Problème 2.1: *"Existe-t-il un corps L tel que pour tout groupe fini G, on puisse trouver un sous-corps $K \subset L$, avec L/K galoisien et $Gal(L/K) = G$?"*

Ce problème semble assez délicat, on pourrait penser que plus L est "gros", plus il a une chance de satisfaire à cette propriété. Il n'en est rien: en effet si L est un corps algébriquement clos de caractéristique 0, d'après la théorie d'Artin et Schreier, les seuls sous-corps $K \subset L$ tels que $[L : K] < \infty$ sont de degré 2.

En reprenant le même argument que pour le problème 1, on peut construire un corps qui satisfait à ce problème. Soit k un corps quelconque et $L = k(X_n)_{n\in\mathbb{N}}$ le corps des fractions rationnelles sur k à $\aleph_0$ variables. Comme précédement, pour tout $n \in \mathbb{N}$ le groupe S_n agît sur L. Si l'on plonge un groupe fini G dans S_n, alors G agit sur L et $K = L^G$ vérifie que L/K est galoisien de groupe G.

Problème 2.2: *"Existe-t-il un corps K tel que tout groupe fini soit groupe de Galois d'une extension galoisienne de K?"*

Ce problème admet une réponse positive depuis Riemann: le corps $K = \mathbb{C}(T)$ satisfait à cette propriété. D'après les résultats du chapitre 2, on peut remarquer qu'un corps ample et hilbertien répond à ce problème.

Plus généralement, on peut se demander quels sont les corps K qui satisfont à ce problème et quels sont leur groupe de Galois absolu.

Problème 3: "Pour tout groupe fini G, existe-t-il une extension galoisienne de $\mathbb{Q}$ ayant G pour groupe de Galois?"

Ce problème est ce que l'on appelle d'habitude le problème inverse de Galois. C'est donc le problème 2.2 pour $K = \mathbb{Q}$. A l'heure actuelle, on sait réaliser beaucoup de groupes finis sur $\mathbb{Q}$ (hélas pas tous). Notamment, la méthode de rigidité (voir par exemple [Ser1] ou [Ser4]) a permi dans les années 70 d'en augmenter sensiblement le nombre. Enoncons-en une liste (non exhaustive):

1) Les groupes abéliens. Ceci résulte du théorème de progression arithmétique et du fait que l'on sait réaliser $(\mathbb{Z}/n\mathbb{Z})^*$, grâce aux extensions cyclotomiques.

2) Les groupes résolubles. Ceci à été prouvé par Shafarevich en 1956 ([Sha]).

3) Les groupes symétriques S_n. Nous en avons donné un argument précédement.

4) Les groupes alternés A_n.

5) Certaines familles de groupes simples, en particulier tous les groupes sporadiques, sauf le groupe de Mathieu M_{23}.

On pourra consulter l'ouvrage de Matzat et de Malle [MatMa] pour une liste plus détaillée.

Problème 4: *"Pour tout groupe fini, existe-t-il une infinité d'extensions galoisiennes de $\mathbb{Q}$ ayant G pour groupe de Galois?".*

Ce problème bien qu'à priori plus compliqué que le problème inverse de Galois, lui est équivalent. En effet supposons que le problème inverse de Galois soit vrai. Prenons un groupe fini G et considérons $G(n) = G \times \cdots \times G$ le groupe obtenu en prenant n fois le produit cartésien de G. Par hypothèse il existe un corps de nombres L tel que $L/\mathbb{Q}$ soit galoisien de groupe de Galois G_n. Considérons le sous-groupe distingué de $G(n)$, $G^i = G \times \cdots \times 0 \times \cdots \times G$ et notons $G_i = G(n)/G^i \simeq G$. Posons alors $L_i = L^{G^i}$, on a que $L_i/\mathbb{Q}$ est galoisien de groupe de Galois G, mais comme pour $i \neq j$ les sous-groupe G^i et G^j engendre $G(n)$ il s'ensuit que $L_i \cap L_j = \mathbb{Q}$. Les extensions L_i sont donc linéairement disjointes sur $\mathbb{Q}$. Comme n est quelconque, on peut donc trouver une famille infinie d'extensions galoisiennes de $\mathbb{Q}$ de groupe G, linéairement disjointes deux à deux.

Les problèmes que nous venons d'exposer prévoient que tout les groupes finis apparaissent d'une façon où d'une autre comme groupe de Galois d'une extension. Il existe des corps (à commencer par les corps algébriquement clos) qui n'admettent pas tous les groupes finis pour groupes de Galois. L'exemple élémentaire est le cas des extensions K algébriques ordonnées maximales d'un corps ordonné donné (par exemple $\mathbb{R}$). La théorie d'Artin-Schreier prouve que le seul groupe Galois non trivial sur K est $\mathbb{Z}/2$. On pourrait se demander si en dehors de ces cas extrêmes, tous les corps K n'admettent pas tout les groupes finis comme groupe de Galois. La réponse est bien évidement non. L'étude de

groupe de Galois absolu de $\mathbb{Q}^{tr}$ ([FHV]) montre en particulier que les groupes finis qui sont groupes de Galois sur $\mathbb{Q}^{tr}$ sont exactement les groupes finis qui peuvent être générés par des éléments d'ordre 2 (en particulier $\mathbb{Z}/3$ n'est pas groupe de Galois sur $\mathbb{Q}^{tr}$). L'exemple suivant montre la complexité du sujet:

Proposition.— *Soit n un entier. Il existe un corps K_n tel que les groupes finis qui sont groupes de Galois sur K_n soient exactement les groupes finis pouvant être générés par moins de n éléments.*

Preuve: Soit K un corps à groupe de Galois absolu pro-libre F_ω de rang dénombrable (d'après Pop et Harbater, $K = \overline{\mathbb{Q}}(T)$ est un corps satisfaisant à cette propriété). Considérons $F_n \subset F_\omega$ le groupe libre à n générateurs. Alors $\widehat{F_n}$, la fermeture de F_n dans $\widehat{F_\omega}$ est un sous-groupe fermé de $\widehat{F_\omega}$. Posons

$$K_n = \overline{K}^{\widehat{F_n}}$$

Alors $G_{K_n} = \widehat{F_n}$. Maintenant soit G un groupe fini de rang au moins $n+1$ éléments. Soit $\varphi : \widehat{F_n} \to G$, considérons $\varphi_{|F_n}$ la restriction à F_n de φ. Soit $x_1, \cdots x_n$ les générateurs de F_n et $g_i = \varphi_{|F_n}(x_i) \in G$, notons $H =< g_1, \cdots, g_n >$. Par hypothèse H est un sous-groupe strict de G. Mais on a $\varphi_{|F_n}(F_n) = H$ et comme H est fini on a $\varphi(\widehat{F_n}) = H$, donc φ ne peut pas être surjective. Ainsi, si G est groupe de Galois sur K_n, il peut-être généré par moins de n éléments.
Réciproquement, soit G un groupe fini généré par n éléments $g_1, \cdots g_n$. On pose $\varphi : \widehat{F_n} \to G$ définie par $\varphi(x_i) = g_i$. φ est bien une surjection et donc G est groupe de Galois sur K_n. □

A la lueur de cette exemple, on peut se poser un autre problème inverse:

Problème 5: *Soit $\mathcal{G} = (G_1, G_2, \cdots)$ une famille de groupes finis, existe-t-il un corps qui admette pour groupes de Galois finis exactement cet ensemble?*

Il est clair que pour certaines familles $\mathcal{G}$, il n'existe pas de tel corps: une condition minimale que doit réaliser $\mathcal{G}$ est que si $G \in \mathcal{G}$ alors tout les quotients de G appartiennent à $\mathcal{G}$!

On peut déjà remarquer le phénomène suivant: Soit K un corps, on note $\mathcal{G}_K$ l'ensemble des groupes finis qui sont groupes de Galois sur K, alors

Théorème.— *Soit un corps K tel que $\mathcal{G}_K$ soit fini. Alors $\mathcal{G}_K = \{\mathbb{Z}/2\mathbb{Z}\}$ et $\overline{K} = K(\sqrt{-1})$*

Preuve: Soit $(L_i)_{i\in I}$ l'ensemble des extensions finies de K. Par hypothèse leur degré est borné par le max des ordres des $G_k \in \mathcal{G}$. Supposons que ce maximum soit atteint par G_1. Alors, soit par exemple $Gal(L_1/K) = G_1$, on a $\forall i \in I$, $L_i \subset L_1$ car sinon $L_1.L_i$ serait une extension galoisienne fini de K de degré strictement plus grand que celui de L_1/K, ce qui est absurde par hypothèse. Donc, par limite inductive, on a $L_1 = \overline{K}$. Mais le théorème d'Artin-Schreier assure alors que K est "réel clos" et que $\overline{K} = K(\sqrt{-1})$ donc $[\overline{K} : K] = 2$ et $\mathcal{G} = \{\mathbb{Z}/2\mathbb{Z}\}$. □

Dans cette voie, une nouvelle question se pose alors: soit K un corps, et $(G_1, G_2, \cdots) \subset \mathcal{G}_K$. Peut-on décrire, par des lois élémentaires indépendantes de K, ce qu'il faut "rajouter" à $(G_1, G_2, \cdots)$ pour obtenir $\mathcal{G}_K$, ou encore, ce qu'on peut "rajouter" pour être sûr de rester dans $\mathcal{G}_K$?

Nous avons vu précédemment qu'il fallait ajouter tout les quotients finis des éléments

de $(G_1, G_2, \cdots)$. Peut-on trouver d'autres règles? Par exemple, faut-il imposer que les produits (cartésiens) soient aussi présents? La réponse est non: Reprenons K_n, le produit cartésiens de deux groupes générés par au minimum n éléments, ne peut pas en général être généré par moins de n éléments...

Notons aussi que dans cette perspective, il y a une différence fondamentale entre le problème inverse de Galois et le problème inverse de Galois régulier:

Soit K un corps, on note comme précédemment $\mathcal{G}_K$ l'ensemble des groupes finis qui sont groupes de Galois sur K. On désigne par $\mathcal{GR}_K$ l'ensemble des groupes finis qui sont groupes de Galois d'une extension régulière de $K(T)$. Enfin on appelle $\mathcal{P}(Groupes)$ l'ensemble des ensembles de groupes finis et $\mathcal{E}_K$ l'ensemble des extensions algébriques de K; ces deux ensembles étant ordonnés par l'inclusion.

Avec ces notations, l'application de $\mathcal{E}_K$ dans $\mathcal{P}(Groupes)$ qui à un corps K associe $\mathcal{GR}_K$, est une application croissante. Notons que $\mathcal{GR}_{\overline{K}}$ est égal à l'élément maximal (voir chapitre I) et que le problème inverse de Galois régulier conjecture que cette application est constante.

Considérons maintenant l'application de $\mathcal{E}_K$ dans $\mathcal{P}(Groupes)$ qui à un corps $K \subset \overline{\mathbb{Q}}$ associe $\mathcal{G}_K$. Il est clair que $\mathcal{G}_{\overline{K}} = \{1\}$, on pourrait donc imaginer que cette application est décroissante et que plus K est "petit" plus $\mathcal{G}_K$ est "gros", il n'en est pourtant rien: si $K = \mathbb{Q}$, $L_1 = \mathbb{Q}^{tr}$, $L_2 = \mathbb{Q}^{tr}(\sqrt{-1})$ et $L_3 = \overline{\mathbb{Q}}$, on a $K < L_1 < L_2 < L_3$ et pourtant $\mathcal{G}_{L_1} < \mathcal{G}_{L_2}$ et $\mathcal{G}_{L_3} < \mathcal{G}_{L_2}$ (j'ignore si $\mathcal{G}_{L_1} < \mathcal{G}_K$).

Le problème de Galois inverse ne mesure pas le comportement des extensions galoisiennes de $\mathbb{Q}$, qui ont un groupe fini donné pour groupe de Galois, entre elles. Si G est un groupe fini, On considère l'ensemble $(L_i)_{i\in I}$ des extensions galoisiennes de $\mathbb{Q}$ de groupe de Galois G.

$$\mathbb{Q} \xrightarrow{G} (L_i)_{i\in I} \longrightarrow \overline{\mathbb{Q}}$$

I est nécessairement dénombrable, sinon $\overline{\mathbb{Q}}$ ne serait plus dénombrable.
Notations: Pour tout $i \in I$ il existe $a_i \in \overline{\mathbb{Q}}$ tel que $L_i \simeq \mathbb{Q}(a_i)$; on note alors:

$$L_G = \mathbb{Q}((a_i)_{i\in I})$$

Il est clair que L_G est une extension galoisienne de $\mathbb{Q}$, on note $Gal(G)$ son groupe de Galois. Voici un exemple avec $G = \mathbb{Z}/2$:

$L_{\mathbb{Z}/2\mathbb{Z}}$ est donc engendré par toutes les racines carrées de rationnels (i.e $L_{\mathbb{Z}/2\mathbb{Z}} = \mathbb{Q}((\sqrt{r})_{r\in\mathbb{Q}})$). Il est alors clair que l'on a finalement:

$$L_{\mathbb{Z}/2\mathbb{Z}} = \mathbb{Q}(i, \sqrt{2}, \sqrt{3}, \sqrt{5}, \cdots, \sqrt{p}, \cdots) \ p \ premier$$

Pour calculer $Gal(\mathbb{Z}/2\mathbb{Z})$ rappellons le lemme suivant:

Lemme S.— *Soit K/K_0 une extension galoisienne. Pour tout $i = 1, 2, \cdots$ soit $K \longrightarrow L_i \longrightarrow K$ une extension galoisienne satisfaisant:*

1. *si L_i' est le sous-corps de K engendré par $\bigcup_{j\neq i} L_j$ alors $L_i \cap L_i' = K_0$.*
2. *K est engendré par $\bigcup_{i=1}^{\infty} L_i$.*

Alors il existe un isomorphisme de groupes topologiques

$$Gal(K/K_0) \simeq \prod_{i=1}^{\infty} Gal(L_i/K_0)$$

Preuve: Cf. [Rib] VII k). □

En posant avec les notations du lemme $K_0 = \mathbb{Q}$, $K = L_{\mathbb{Z}/2\mathbb{Z}}$, $L_1 = \mathbb{Q}(i)$, $L_k = \mathbb{Q}(\sqrt{p}_{k-1})$, p_k le k-ième nombre premier, nous obtenons que:

$$Gal(\mathbb{Z}/2\mathbb{Z}) \simeq Gal(\mathbb{Q}(i)/\mathbb{Q}) \times \prod_{p \text{ premier}} Gal(\mathbb{Q}(\sqrt{p})/\mathbb{Q})$$

c'est-à-dire:

$$Gal(\mathbb{Z}/2\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$$

Regardons maintenant le lien avec la théorie inverse de Galois:

Théorème.— *Si la conjecture de Galois inverse est vraie alors pour tout groupe fini simple G, on a:*

$$Gal(G) \simeq G^{\mathbb{N}}$$

Preuve: Nous avons vu dans l'étude du problème 4 que si le problème de Galois était vrai, on pouvait trouver une famille infinie d'extensions galoisiennes de $\mathbb{Q}$ de groupe de Galois G linéairement disjointes deux à deux.

Soit maintenant une famille $(a_1, a_2, \cdots)$ maximale (au sens de l'inclusion) de nombres algébriques telle que:

1. $Gal(\mathbb{Q}(a_i)/\mathbb{Q})$ galoisienne et $Gal(\mathbb{Q}(a_i)/\mathbb{Q}) \simeq G \ \forall i \in \mathbb{N}$
2. $\mathbb{Q}(a_i) \cap \mathbb{Q}(a_j) = \mathbb{Q}$ pour $i \neq j$

Une telle famille existe d'après Zorn. On a alors $L_G = \mathbb{Q}(a_1, a_2, \cdots)$. En effet soit $\alpha \in \overline{\mathbb{Q}}$ tel que $Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) \simeq G$ et $\alpha \notin \mathbb{Q}(a_1, a_2, \cdots)$. Alors par hypothèse sur $(a_i)_{i\in\mathbb{N}}$ il existe $j \in \mathbb{N}$ tel que $W = \mathbb{Q}(a_i) \cap \mathbb{Q}(\alpha) \neq \mathbb{Q}$. Mais W est une extension galoisienne de $\mathbb{Q}$. Donc $Gal(W/\mathbb{Q})$ est un quotient de G qui est simple. Donc $W = \mathbb{Q}(\alpha)$ ou $W = \mathbb{Q}$. Dans ces deux cas, on contredit l'hypothèse.

Il ne nous reste plus qu'a appliquer le lemme S à la famille $(\mathbb{Q}(a_i))_{i\in\mathbb{N}}$ pour conclure. □

Appendice II
Corps P-réduisants

Nous avons parlé dans le chapitre 4 de la notion de corps pythagoriciens. On peut aussi parler de corps fermatiens: ceux sont les corps K tels que toutes sommes de puissances n-ièmes restent une puissance n-ième (i.e. $K^n = K^n + K^n$). Nous avons prouvé dans le chapitre 4 qu'aucune extension finie stricte de $\mathbb{Q}^{pyth}$ n'est pythagoricienne. Nous voulons généraliser dans cet appendice ces notions et résultats.

Définition.— *Soit n un entier positif et $P \in \mathbb{Q}[X_1, \cdots X_n, X]$, un corps K de caractéristique 0 est dit P-réduisant si pour tout n-uplet $(x_1, \cdots, x_n) \in K^n$ le polynôme $P(x_1, \cdots, x_n, X)$ se décompose totalement dans K.*

Lemme.— *Si K et K' sont deux corps de caractéristique 0 et isomorphes alors si K est P-réduisant, K' l'est aussi.*

Preuve: Soit $\sigma : K \to K'$ un isomorphisme (c'est en particulier un $\mathbb{Q}$-isomorphisme) et $(y_1, \cdots, y_n) \in K'^n$. Si on pose $x_i = \sigma^{-1}(y_i)$, alors par hypothèse les racines $r_1, \cdots, r_k$ de $P(x_1, \cdots, x_n, X)$ sont dans K, donc les racines de $P(y_1, \cdots, y_n, Y)$ sont $\sigma(r_1), \cdots, \sigma(r_k)$ et vivent dans K'. □

Théorème-définition.— *Soit K un corps de caractéristique 0 et $(K_i)_{i\in I}$ une famille d'extensions algébriques de K, P-réduisante. Le corps $K_P = \bigcap_{i\in I} K_i$ est un corps P-réduisant.*

En particulier, parmis les extensions algébriques P-réduisantes de K, il en existe une plus petite (pour l'inclusion) notée K_P et appellée clôture P-réduisante de K. L'extension K_P/K est galoisienne.

Preuve: Soit $(x_1, \cdots, x_n) \in K^n$, alors par hypothèse les racines $r_1, \cdots, r_k$ de $P(x_1, \cdots, x_n, X)$ sont dans chaque K_i, donc dans K.
Le corps K_P est alors obtenu en prenant l'intersection de toutes les extensions algébriques P-réduisantes de K.
Soit $\sigma \in G_K$, le corps $\sigma^{-1}(K_P)$ est P-réduisant donc $K_P \subset \sigma^{-1}(K_P)$, donc $\sigma(K_P) \subset K_P$ et par suite K_P/K est une extension normale. Comme K est supposé de caractéristique nulle, K_P/K est séparable et par suite galoisienne. □

Lemme.— *Soit P et Q deux éléments de $\mathbb{Q}[X_1, \cdots X_n, X]$, alors si K est un corps de caractéristique 0, les deux propriétés suivantes sont équivalentes:*

i) K est PQ-réduisant.

ii) K est P-réduisant et Q-réduisant.

On a alors $K_P.K_Q \subset K_{PQ}$.

Preuve: Pour tout $(x_1, \cdots, x_n) \in K^n$ le polynome $P(x_1, \cdots, x_n, X)Q(x_1, \cdots, x_n, X)$ se décompose totalement dans K, donc $P(x_1, \cdots, x_n, X)$ et $Q(x_1, \cdots, x_n, X)$ aussi, et réciproquement.

K_{PQ} est P-réduisant et Q-réduisant, donc $K_P \subset K_{PQ}$ et $K_Q \subset K_{PQ}$, donc $K_P.K_Q \subset K_{PQ}$. □

Exemples:

1/ Si $n = 0$ et $P \in \mathbb{Q}[X]$, alors K est P-réduisant ssi il contient le corps de décomposition C de P sur $\mathbb{Q}$, ainsi $\mathbb{Q}_P = C$.

2/ Si $P = X^2 - X_1$, alors $\mathbb{Q}_P = \mathbb{Q}(i, \sqrt{2}, \sqrt{3}, \cdots, \sqrt{p}, \cdots)$.

3/ Si $n \geq 2$ et $P = X^2 - X_1^2 - \cdots - X_n^2$ alors K est P-réduisant ssi K est pythagoricien.

4/ Si K est algébriquement clos, alors K est P-réduisant pour tout P.

5/ Soit $n > 1$ et $P_n(X_1, \cdots, X_n, X) = X^n + X_1 X^{n-1} + \cdots + X_n$. Alors un corps K est P_n-réduisant ssi il ne possède aucune extension stricte de degré $\leq n$.
On pose $K_n = \mathbb{Q}_{P_n}$. Les corps K_n sont galoisiens sur $\mathbb{Q}$, on note alors $G_n = Gal(K_n/\mathbb{Q})$. On a alors la suite d'inclusions $\mathbb{Q} = K_1 \subset K_2 \subset \cdots \subset K_n \subset \cdots$ et $\overline{\mathbb{Q}} = \varinjlim_{n \geq 1} K_n$.
En effet, comme on vient de le remarquer, un corps K est P_n-réduisant ssi il ne possède aucune extension stricte de degré $\leq n$, ce qui justifie le suite d'inclusions. Soit maintenant $\alpha \in \overline{\mathbb{Q}}$, si n_0 est le degré du polynôme minimal de α sur $\mathbb{Q}$, alors $[K_{n_0}(\alpha) : K_{n_0}] \leq n_0$ donc $\alpha \in K_{n_0}$. Ainsi, on a $Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \simeq \varprojlim_{n \geq 1} G_n$.

Voici maintenant un résultat sur les extensions finies des clôture P-réduisantes des corps hilbertiens. Ce théorème est une généralisation de la remarque 4.4 du chapitre 4, puisque les corps pythagoriciens sont un cas particulier des corps P-réduisants.

Théorème.— *Soit $P \in \mathbb{Q}[X_1, \cdots, X_n, X]$ un polynôme irréductible de degré en X plus grand que 1. Alors si K est un corps P-réduisant, il ne peut pas être hilbertien.*
En conséquence de quoi, si K est un corps hilbertien et $P \in \mathbb{Q}[X_1, \cdots, X_n, X]$ est un polynôme irréductible de degré en X plus grand que 1, alors aucune extension finie et stricte de K_P n'est P-réduisante.
En particulier si K est P-réduisant et que $K \neq \mathbb{Q}_P$ alors $[K : \mathbb{Q}_P] = +\infty$.

Preuve: Le polynôme P est irréductible sur K, si K était hilbertien alors il existerait un n-uplet $(x_1, \cdots, x_n) \in K^n$ tel que $P(x_1, \cdots, x_n, X)$ soit irréductible. Comme ce polynôme est de degré plus grand que 1, cela contredit le fait que K est P-réduisant.
Par application du critère de Weissauer, K_P/K étant galoisien et K étant hilbertien, toutes extensions finies et strictes de K_P sont hilbertiennes et donc ne peuvent être P-réduisantes. □

BIBLIOGRAPHIE

[**Bla**] A.Blanchard, *"Les corps non commutatifs"*, Collection Sup, PUF (1972).

[**CaFr**] J.W.S.Cassels and A.Frölich, *Algebraic number theory*, Academic press (1967).

[**CP**] J.H.Conway and R.A.Parker, *On the Hurwitz number of arrays of group elements*, preprint.

[**Deb1**] P.Dèbes, *Groupes de Galois sur $K(T)$*, Séminaire de théorie des nombres, Bordeaux 2 (1990), 229-243.

[**Deb2**] P.Dèbes, *Covers of $\mathbb{P}^1$ over the p-adics*, Contemporary Mathematics, 186 (1995), 217-238.

[**Deb3**] P.Dèbes, *G-fonctions et Théorème d'irréductibilité de Hilbert*, Acta Arithmetica, 47 $n°4$ (1986), 81-122.

[**Deb4**] P.Dèbes, *Arithmétique sur des Espaces de Modules de Revêtements*, préprint, (1997).

[**DebDes**] P.Dèbes and B.Deschamps, *"The Inverse Galois Problem over Large Field"*, in Geometric Galois action II — London Math. Soc. Lecture Note Series, Cambridge univ. press, 243 (1997).

[**DeFr**] P.Dèbes and M.Fried, *Non rigid constructions in Galois theory*, Pacific Journal of Math., 163 ♯1 (1994), 81-122.

[**Des1**] B.Deschamps, *Autour d'un théorème d'Harbater*, Mémoire de DEA, Université Paris VI (1993).

[**Des2**] B.Deschamps, *Existence de points p-adiques pour tout p sur un espace de Hurwitz*, Contemporary Mathematics, 186 (1995), 239-247.

[**Des3**] B.Deschamps, *Théorie inverse de Galois et clôture totalement réelle d'un corps ordonné*, préprint (1996).

[**Dou**] A.Douady, *Détermination d'un groupe de Galois*, Note au C.R.A.S Paris, 258 (1964), 5305-5308.

[**Ems**] M.Emsalem, *Familles de revêtements de la droite projective*, Bulletin de la S.M.F, 123 (1995).

[**Fr1**] M.Fried, *Field of definition of function fields and Hurwitz families - Groups as Galois groupes*, Communication in Algebra, 5(1) (1977), 17-82.

[**Fr2**] M.Fried, *Introduction to Modular Towers*, Contemporary Mathematics, 186 (1995).

[**FrJa**] M.Fried and M.Jarden, *Field arithmetic*, Springer-Verlag (1986).

[**FrHaVo**] M.Fried, D.Haran and H.Völklein, *"Absolute Galois group of the totally real numbers"*, Note au C.R.A.S, 317 Série I, page 995-999 (1993).

[**FrVo1**] M.Fried and H.Völklein, *The inverse Galois problème and rational points on moduli spaces*, Math. Ann., 290 (1991), 771-800.

[**FrVo2**] M.Fried and H.Völklein, *The embedding problem over Hilbertian PAC-field*, Ann. of Math., 135 (1992), 469-481.

[**GrPoRo**] B.Green, F.Pop and P.Roquette *On Rumely's local-global principle*, Jahresbericht der DMV, 95 (1995), 43-74.

[**HaJa1**] D.Haran and M.Jarden, *Regular split embedding problems over complete valued fields*, manuscript (1995).

[**HaJa2**] D.Haran and M.Jarden, *On a conjecture of Deschamps*, manuscript (1997).

[**HaVo**] D.Haran and H.Völklein, *Galois groups over complete valued fields*, Israel J. of Math., to appear.

[**Har1**] D.Harbater, *Mock covers and Galois extensions*, J. Algebra, 91 (1984), 281-293.

[**Har2**] D.Harbater, *Galois covering of the arithmetic line*, Lecture Notes in Math., 1240 (1987), 165-195.

[**Har3**] D.Harbater, *Abhyankar's conjecture on Galois groups over curves*, Invent. Math., 117 (1994), 1-25.

[**Har4**] D.Harbater, *Fondamental groups and embedding problems in characteristic p*, Contemporary Mathematics, 186 (1995), 353-369.

[**Iw**] K.Iwasawa, *On solvable extensions of algebraic number fields*, Annals of Math., 58 (1953), 548-572.

[**Ja1**] M.Jarden, *The inverse Galois problem over formal power series fields*, Israel J. Math., 85 (1994), 353-369.

[**Ja2**] M.Jarden, *On free profinite groups of uncountable rank*, Contemporary Mathematics, 186 (1995), 371-383.

[**Ja3**] M.Jarden, *Totally S-adic extensions of hilbertian fields*, manuscript (1994).

[**Ja4**] M.Jarden, *Large normal extensions of Hilbertian fields*, Mathematishe Zeitschrift.

[**Liu**] Quing Liu, *Tout groupe fini est groupe de Galois sur* $\mathbb{Q}_p(T)$, Contemporary Mathematics, 186 (1995), 261-265.

[**Mat**] B.H.Matzat, *Konstruktive Galoistheorie*, LNM 1284, Springer (1987).

[**MatMa**] B.H.Matzat and G.Malle, *Inverse Galois Theory*, (1996).

[**Pop1**] F.Pop, *Half Riemann's existence theorem*, Algebra and number theory (G.Frey and J.Ritter, eds), de Gruyter Proceedings in Mathematics (1994).

[**Pop2**] F.Pop, *The geometric case of a conjecture of Shafarevich — $G_{\overline{k}(t)}$ is profinite free —*, Heidelberg-Mannheim Preprint Series "arithmetik", Heft 8 (1993).

[**Pop3**] F.Pop, *Etale Galois covers of affine smooth curves*, Invent. Math., 120 (1995), 555-578.

[**Pop4**] F.Pop, *Embedding problems over large fields*, Annals of Math., 144 (1996), 1-35.

[**Pop5**] F.Pop, *Fields of totally Σ-adic numbers*, Heidelberg-Mannheim Preprint (1990).

[**Ra**] M.Raynaud, *Revêtement de la droite affine en caractéristique p et conjecture d'Abhyankar*, Invent. Math., 116 (1990), 425-462.

[**Rib**] P.Ribenboïm, *"Arithmétique des corps"*, Hermann (1973).

[**Ser1**] J.P.Serre, *Topics in Galois theory*, Note written by H.Darmon, Jones and Bartlett Publ., Boston (1992).

[**Ser2**] J.P.Serre, *Corps locaux*, Hermann (1968).

[**Ser3**] J.P.Serre, *Cohomologie galoisienne*, Lecture Note in Mathematics, Springer-Verlag (1965).

[**Ser4**] J.P.Serre, *Groupes de Galois sur* $\mathbb{Q}$, Séminaire Boubaki, $n°689$ (1987-88).

[**Vo**] H.Völklein, *Groups as Galois groups - an introduction*, Cambridge Univ. Press (1996).

LEXIQUE

— **Ample (corps):** Un corps K est dit *ample* quand toute courbe lisse irréductible et définie sur K possède une infinité de points K-rationnels pourvu qu'elle en possède au moins 1.

— **Clôture totalement réelle:** Si K désigne un corps ordonnable, on appelle *clôture totalement réelle* de K, le corps $\widetilde{K}_{tr}$ obtenu en prenant l'intersection de toutes les extensions algébriques ordonnées maximales de K.

— **Existentiellement clos:** Un corps K est dit *existentiellement clos* dans un corps L quand toute variété lisse irréductible et définie sur K possèdant un point L-rationnel, en possède un K-rationnel.

— **Fried-Völklein (conjecture):** Conjecture qui prévoit que tout corps hilbertien et dénombrable a un groupe de Galois absolu pro-libre, pourvu que celui-ci soit déjà projectif.

— **Groupe de Galois absolu:** Si K est un corps, on appelle groupe de Galois absolu de K le groupe de Galois $Gal(K^{sep}/K)$, où K^{sep} désigne la clôture séparable de K.

— **Hilbertien (corps):** Un corps K est dit *hilbertien* quand il vérifie la propriété d'Hilbert: pour tout polynôme $P(T,Y) \in K(T)[Y]$ irréductible, il existe un $t \in K$ (en fait une infinité) tel que le polynôme "spécialisé" $P(t,Y) \in K[Y]$ reste irréductible.

— **Hurwitz (espaces de):** Espace de module paramétrant les revêtements de $\mathbb{P}^1$ défini sur $\mathbb{C}$ à groupe de Galois fixé.

— **Invariant canonique de l'inertie (d'un revêtement):** Uplet des classes de conjugaisons des générateurs des groupes d'inerties au dessus des points de ramification d'un revêtement.

— **Iwasawa (théorème de):** Pour un corps K dénombrable, il y a équivalence entre G_K pro-libre et tout problème de plongement fini pour G_K a une solution forte.

— **PAC (corps):** Un corps K est dit *P(seudo)-A(lgébriquement)-C(los)* lorsque toute variété lisse irréductible et définie sur K possède un point K-rationnel.

— **P-réduisant (corps):** Si P désigne un polynôme de $\mathbb{Q}[X_1, \cdots X_n, X]$, un corps K de caractéristique 0 est dit *P-réduisant* si pour tout n-uplet $(x_1, \cdots, x_n) \in K^n$, le polynôme "spécialisé" $P(x_1, \cdots, x_n, X)$ est totalement décomposé dans $K[X]$.

— **Problème inverse de Galois:** Conjecture qui prévoit que tout groupe fini est groupe de Galois d'une extension galoisienne de $\mathbb{Q}$.

— **Problème inverse régulier de Galois (sur K):** Conjecture qui prévoit que tout groupe fini est groupe de Galois d'une extension galoisienne et régulière de $K(T)$.

— **Projectif (groupe):** Un groupe profini G est dit *projectif* si tout problème de plongement pour G admet une solution faible. De manière équivalente, G est projectif ssi $cd(G) \leq 1$.

— **Pythagoricien (corps):** Un corps K est dit *pythagoricien* si toute somme de carrés de K est encore un carré dans K (i.e $K^2 + K^2 = K^2$).

— **Régulière (extension):** Une extension $L/K(T)$ est dite *régulière* si $L \cap \overline{K} = K$.

— **G-revêtement:** Revêtement galoisien de $\mathbb{P}^1$ donné avec l'action de son groupe de Galois.

— **Shafarevich (conjecture de):** Conjecture qui prévoit que le groupe de Galois absolu de $\mathbb{Q}^{ab}$ est pro-libre.

— **Totalement réel, (resp. p-adique) (nombre algébrique):** Elément de $\overline{\mathbb{Q}}$ qui n'a que des conjugués réels (resp. p-adiques). L'ensemble de ces éléments est un corps noté $\mathbb{Q}^{tr}$ (resp. $\mathbb{Q}^{tp}$).

— **Totalement S-adique (élément):** Soit K un corps global et S un ensemble fini de places. On dit que $x \in K_s$ est un élément *totalement S-adique* si tout ses conjugués restent dans une copie donnée du complété K_ν, pour tout $\nu \in S$. L'ensemble de ces éléments est un corps noté K^S

— **Weissauer (théorème de):** Toute extension finie et stricte d'une extension galoisienne d'un corps hilbertien est hilbertienne.

Résumé

Cette thèse présente quelques aspects de la théorie inverse de Galois. Dans la première partie, nous présentons une conjecture (due à P.Dèbes) et montrons que celle-ci contient la plupart des conjectures célèbres concernant la théorie inverse de Galois (Problème de Galois inverse, problème inverse régulier, problèmes de plongement, conjecture de Fried-Völklein, conjecture de Shafarevich etc.). Nous donnons un théorème de F.Pop concernant cette conjecture et montrons comment à partir de ce théorème on peut retrouver la plupart des résultats récents de la théorie inverse.

Dans la deuxième partie, nous abordons le cadre de la théorie des espaces de modules de revêtements. Nous montrons que pour tout groupe fini G, il existe un espace de Hurwitz (en fait une infinité) attaché à G, lisse, irréductible et défini sur $\mathbb{Q}$ possédant un point $\mathbb{Q}_p$-rationnel pour tout premier p (y compris $p = \infty$). La théorie des espaces de Hurwitz montre que le problème inverse de Galois régulier se ramène à trouver des points $\mathbb{Q}$-rationnels sur certaines variétés. D'après notre résultat, on peut ajouter que ces variétés possèdent des points $\mathbb{Q}_p$-rationnels pour tout p.

Dans la troisième partie nous généralisons la construction du corps $\mathbb{Q}^{tr}$ des nombres algébriques totalement réels. Nous y introduisons la notion de clôture totalement réelle d'un corps ordonnable K (notée $\widetilde{K}_{tr}$). Nous prouvons que dans les cas suivants: a) K corps réel clos, b) K corps de nombres ordonnable, c) $K = k((X))$ avec k réel clos; le groupe de Galois absolu de $\widetilde{K}_{tr}(\sqrt{-1})$ est pro-libre. Ce résultat constitue un analogue de la conjecture de Shafarevich pour les corps $\widetilde{K}_{tr}$. D.Haran et M.Jarden ont récemment donné un exemple où ce groupe n'est pas pro-libre. Nous conjecturons maintenant que cette propriété est vraie si K est dénombrable et hilbertien. Nous complétons ce travail par une étude du groupe de Brauer de $\widetilde{K}_{tr}$, notamment nous prouvons que $Br(\mathbb{Q}^{tr}) \simeq \varinjlim_{n\in\mathbb{N}} (\mathbb{Z}/2)^n$.

Pour finir nous présentons deux petits appendices. Le premier regarde sous plusieurs angles *l'idée* de problème inverse à la théorie de Galois. Le deuxième essaie de généraliser la notion de corps pythagoriciens dont nous parlons un peu dans la troisième partie.