Université Lille 1 Sciences et Technologies
Ecole doctorale sciences pour l'ingénieur 072

Numéro d'ordre : 41180

Spécialisations de revêtements et théorie inverse de Galois

THÈSE

présentée et soutenue publiquement le 10 décembre 2013

pour l'obtention du

Doctorat de l'Université Lille 1

(spécialité mathématiques pures)

par

François LEGRAND

Composition du jury

Président :	Michel EMSALEM	Université Lille 1
Directeur de thèse :	Pierre DÈBES	Université Lille 1
Rapporteurs :	Lior BARY-SOROKER	Tel Aviv University
	Jochen KOENIGSMANN	University of Oxford
Examinateurs :	Sinnou DAVID	Université Paris 6
	Bruno DESCHAMPS	Université du Maine
	Lorenzo RAMERO	Université Lille 1

Laboratoire Paul Painlevé - U.M.R. CNRS 8524

Mis en page avec la classe thloria.

Université Lille 1 Sciences et Technologies
Ecole doctorale sciences pour l'ingénieur 072

Numéro d'ordre : 41180

Spécialisations de revêtements et théorie inverse de Galois

THÈSE

présentée et soutenue publiquement le 10 décembre 2013

pour l'obtention du

Doctorat de l'Université Lille 1
(spécialité mathématiques pures)

par

François LEGRAND

Composition du jury

Président :	Michel EMSALEM	Université Lille 1
Directeur de thèse :	Pierre DÈBES	Université Lille 1
Rapporteurs :	Lior BARY-SOROKER	Tel Aviv University
	Jochen KOENIGSMANN	University of Oxford
Examinateurs :	Sinnou DAVID	Université Paris 6
	Bruno DESCHAMPS	Université du Maine
	Lorenzo RAMERO	Université Lille 1

Laboratoire Paul Painlevé - U.M.R. CNRS 8524

Mis en page avec la classe thloria.

Résumé

On s'intéresse dans cette thèse à des questions portant sur les spécialisations de revêtements algébriques (galoisiens ou non). Le thème central de la première partie de ce travail est la construction de spécialisations de n'importe quel revêtement galoisien $f : X \to \mathbb{P}^1$ de groupe G défini sur k dont on impose d'une part le comportement local en un nombre fini d'idéaux premiers de k et dont on assure d'autre part qu'elles restent de groupe G si le corps k est hilbertien. Dans la deuxième partie, on développe une méthode générale pour qu'un revêtement galoisien $f : X \to \mathbb{P}^1$ de groupe G défini sur k vérifie la propriété suivante : étant donné un sous-groupe H de G, il existe au moins une extension galoisienne F/k de groupe H qui n'est pas spécialisation de $f : X \to \mathbb{P}^1$. De nombreux exemples sont donnés. La troisième partie consiste en l'étude de la question suivante : une extension galoisienne F/k, ou plus généralement une k-algèbre étale $\prod_l F_l/k$, est-elle la spécialisation d'un revêtement $f : X \to B$ défini sur k (galoisien ou non) en un certain point non-ramifié $t_0 \in B(k)$? Notre principal outil est un *twisting lemma* qui réduit la question à trouver des points k-rationnels sur certaines k-variétés que nous étudions ensuite pour des corps de base k variés.

Mots-clés : théorie de Galois, problème inverse de Galois, revêtements algébriques, spécialisations, théorème d'irréductibilité de Hilbert, extensions paramétriques, twisting lemma.

Abstract

We are interested in this thesis in some questions concerning specializations of algebraic covers (Galois or not). The main theme of the first part consists in producing some specializations of any Galois cover $f : X \to \mathbb{P}^1$ of group G defined over k with specified local behavior at finitely many given primes of k and which each have in addition Galois group G if k is assumed to be hilbertian. In the second part, we offer a systematic approach for a given Galois cover $f : X \to \mathbb{P}^1$ of group G defined over k to satisfy the following property: given a subgroup $H \subset G$, at least one Galois extension F/k of group H is not a specialization of $f : X \to \mathbb{P}^1$. Many examples are given. The central question of the third part is whether a given Galois extension F/k, or more generally a given k-étale algebra $\prod_l F_l/k$, is the specialization of a given cover $f : X \to B$ defined over k (Galois or not) at some unramified point $t_0 \in B(k)$? Our main tool is a *twisting lemma* which reduces the problem to finding k-rational points on some k-varieties which we then study for various base fields k.

Keywords: Galois theory, inverse Galois problem, algebraic covers, specializations, Hilbert irreducibility theorem, parametric extensions, twisting lemma.

Avant-propos

Le présent travail s'appuie sur les quatre textes suivants :

- *Specialization results and ramification conditions* [Leg13b],
- *Parametric Galois extensions* [Leg13a],
- *Specialization results in Galois theory* [DL13],
- *Twisted covers and specializations* [DL12].

Il comporte trois parties :

- la première (chapitre 1) repose sur les sections 2 et 3 de l'article [Leg13b],
- la deuxième (chapitres 2 et 3) est basée sur la section 4 de l'article [Leg13b] et l'article [Leg13a],
- la troisième (chapitres 4 et 5) reprend les deux articles [DL13] et [DL12].

Chacune d'entre elles, rédigée en anglais, possède une introduction propre ayant pour buts d'en donner une vue d'ensemble et d'en présenter les principaux résultats.

Ces trois parties sont précédées

- d'un résumé en français de la thèse où l'on présente chacune d'entre elles ainsi que les résultats principaux tout en replaçant le présent travail dans le contexte de la théorie inverse de Galois,
- d'un chapitre de préliminaires où l'on présente le matériel utilisé dans ce travail.

Contents

Introduction

A.1 Autour du problème inverse de Galois

A.1.1 Problème inverse de Galois

Le présent travail concerne la théorie inverse de Galois. De manière classique, la théorie de Galois associe à toute extension finie galoisienne $F/\mathbb{Q}$ un groupe fini appelé *groupe de Galois de* $F/\mathbb{Q}$ et noté $\mathrm{Gal}(F/\mathbb{Q})$. La réciproque est la question centrale de la théorie inverse de Galois :

Problème Inverse de Galois. *Tout groupe fini est-il le groupe de Galois d'une certaine extension galoisienne de* $\mathbb{Q}$ *?*

Historiquement, le problème inverse de Galois concerne le corps $\mathbb{Q}$. La question précédente peut néanmoins être posée pour n'importe quel corps k :

Enoncé (IGP/k). *Tout groupe fini est-il le groupe de Galois d'une certaine extension galoisienne de* k *?*

En dépit de la simplicité de son énoncé, la réponse au problème inverse de Galois, *i.e.* à l'énoncé (IGP/$\mathbb{Q}$), est actuellement inconnue.

Remarquons que l'énoncé (IGP/k) n'est *a priori* pas stable par extension des scalaires : si k' est un corps contenant k, une réponse positive à l'énoncé (IGP/k) n'entraîne pas *a priori* une réponse positive à l'énoncé (IGP/k') [1]. On doit donc étudier chaque énoncé (IGP/k) séparément.

Par exemple, si k est algébriquement clos, la réponse est clairement négative : toute extension finie de k étant triviale, seul le groupe trivial peut être réalisé sur k [2]. Si $k = \mathbb{R}$, la réponse est également négative : seuls le groupe trivial et le groupe $\mathbb{Z}/2\mathbb{Z}$ peuvent être réalisés sur $\mathbb{R}$. Un troisième exemple négatif est fourni par les corps finis : seuls les groupes cycliques peuvent être réalisés sur ces corps.

Dans le cas $k = \mathbb{Q}$, on sait réaliser les groupes suivants :
- les groupes abéliens,
- les groupes résolubles,
- certains groupes simples non-abéliens...

Si la preuve dans le cas abélien est élémentaire (*e.g.* [Dèb09, théorème 2.1.3]), le cas des groupes résolubles est beaucoup plus difficile. Il a été résolu par Shafarevich [NSW08, (9.6.1)].

1. En effet, si l'on se donne une extension finie galoisienne F/k, le groupe de Galois de l'extension Fk'/k' n'est en général qu'un sous-groupe de celui de F/k. Ces deux groupes sont égaux si et seulement si les corps F et k' sont linéairement disjoints sur k.

2. Nous dirons dans cette introduction qu'*un groupe fini G est réalisé sur un corps k* s'il existe une extension galoisienne de k de groupe G.

A.1.2 Théorème d'irréductibilité de Hilbert

Dans le cas des groupes simples non-abéliens, l'approche est différente. Etant donné un groupe fini G, elle consiste, au lieu d'essayer de construire « directement » une extension galoisienne $F/\mathbb{Q}$ de groupe G, à d'abord introduire une indéterminée T et à construire une extension galoisienne $E/\mathbb{Q}(T)$ de groupe G, puis à *spécialiser* l'indéterminée T en un nombre rationnel t_0 bien choisi. Cette approche repose sur le théorème d'irréductibilité de Hilbert ci-dessous qui est un pilier de la théorie inverse de Galois :

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

Plus généralement, nous dirons qu'un corps k est *hilbertien* si le théorème précédent reste vrai en remplaçant $\mathbb{Q}$ par k (ainsi $\mathbb{Q}$ est un corps hilbertien).

Le théorème d'irréductibilité de Hilbert a pour corollaire l'énoncé suivant (*e.g.* [Dèb09, proposition 2.2.12]) :

Corollaire. *Soient G un groupe fini et k un corps hilbertien. Si G peut être réalisé sur $k(T)$, alors il peut l'être sur k.*

Ainsi, pour que la réponse à l'énoncé (IGP$/k$) soit positive quand k est hilbertien, il suffit qu'elle le soit pour l'énoncé (IGP$/k(T)$).

A.1.3 Forme régulière du problème inverse de Galois

Dans l'approche présentée au début du §A.1.2, on demande de plus que l'extension $E/\mathbb{Q}(T)$ soit *régulière sur* $\mathbb{Q}$, *i.e.* qu'elle vérifie $E \cap \overline{\mathbb{Q}} = \mathbb{Q}$. Dans ce cas, elle correspond, via le foncteur corps de fonctions, à un revêtement galoisien $f : X \rightarrow \mathbb{P}^1$ de groupe d'automorphismes G, défini sur $\mathbb{Q}$ ainsi que ses automorphismes. Le problème est ainsi replacé dans un cadre géométrique.

Etant donné un corps k, l'énoncé suivant constitue l'approche moderne pour résoudre le problème inverse de Galois :

Enoncé (RIGP$/k$). *Tout groupe fini est-il le groupe de Galois d'une certaine extension régulière galoisienne de $k(T)$?*

Remarquons que

(1) si le corps k est hilbertien, une réponse positive à l'énoncé (RIGP$/k$) entraîne une réponse positive à l'énoncé (IGP$/k$),

(2) l'énoncé (RIGP$/k$) est stable par extension des scalaires (grâce à la condition de régularité) : si k' est un corps contenant k, une réponse positive à l'énoncé (RIGP$/k$) entraîne une réponse positive à l'énoncé (RIGP$/k'$). Il suffit donc d'étudier les énoncés sur les sous-corps premiers, *i.e.* les énoncés (RIGP$/\mathbb{Q}$) et (RIGP$/\mathbb{F}_p$) pour tout nombre premier p.

Si, à l'heure actuelle, on ne connaît pas de corps k tels que la réponse à l'énoncé (RIGP$/k$) soit négative, la plupart de ceux pour lesquels on sait que la réponse est positive est fournie par le théorème suivant [Pop96] :

Théorème. *L'énoncé* (RIGP$/k$) *a une réponse positive si le corps k est ample*[3].

3. Rappelons qu'un corps k est dit *ample* si toute k-courbe lisse, géométriquement irréductible et possédant un point k-rationnel en possède une infinité. Nous renvoyons au §B.2.2 pour des exemples de tels corps.

Le théorème ci-dessus englobe plusieurs résultats antérieurs, notamment de Harbater [Har84] [Har87], Fried et Völklein [FV91], Dèbes et Fried [DF94], Dèbes [Dèb95]. Nous renvoyons à [DD97a, §3.2] pour un point plus précis.

De plus, comme l'énoncé (RIGP/k) est stable par extension des scalaires, le théorème précédent entraîne que la réponse à l'énoncé (RIGP/k) est positive si k contient un corps ample. La situation des corps ne contenant pas de corps amples est à l'heure actuelle beaucoup plus floue. Koenigsmann a néanmoins donné un exemple de corps k ne contenant pas de corps amples et tel que la réponse à l'énoncé (RIGP/k) soit positive [Koe04].

Dans le cas $k = \mathbb{Q}$, on sait montrer que les groupes suivants sont groupes de Galois d'une certaine extension régulière galoisienne de $\mathbb{Q}(T)$:
- les groupes abéliens,
- les groupes symétriques,
- les groupes alternés,
- les groupes linéaires sur des corps finis,
- de nombreuses familles de groupes géométriques comme $\mathrm{PSL}_n(\mathbb{F}_q)$, $\mathrm{PSU}_n(\mathbb{F}_q)$, $\mathrm{PSp}_n(\mathbb{F}_q)$ (avec peut-être des conditions sur n et q),
- 25 des 26 groupes sporadiques...

Nous renvoyons à [MM99] pour un point plus précis et des références.

A.1.4 Problème de Beckmann-Black

Etant donnés un groupe fini G et un corps (hilbertien) k, on peut se demander si la stratégie reposant sur le théorème d'irréductibilité de Hilbert est optimale : est-il restrictif ou non de chercher à construire des extensions galoisiennes de k de groupe G « uniquement » par spécialisation d'extensions régulières galoisiennes de $k(T)$ de même groupe ? Cette question porte le nom de *problème de Beckmann-Black* :

Enoncé (BB/k/G). *Etant donnée une extension galoisienne F/k de groupe G, existe t-il une extension régulière galoisienne $E_F/k(T)$ de même groupe possédant F/k parmi ses spécialisations ?*

Nous rappelons ci-dessous quelques résultats classiques sur le problème de Beckmann-Black et renvoyons à la vaste littérature sur le sujet pour un point plus précis.

(1) Etant donné un groupe fini G, si l'énoncé (BB/k/G) a une réponse positive pour tout corps k de caractéristique nulle, alors il existe une extension régulière galoisienne de $\mathbb{Q}(T)$ de groupe G [Dèb99c, proposition 1.2].

(2) Si k est ample, l'énoncé (BB/k/G) est vrai pour tout groupe fini G [CT00] (en caractéristique nulle) [HJ98] [MB01] (pour le cas général).

(3) L'énoncé (BB/$\mathbb{Q}$/G) est vrai pour les groupes suivants : les groupes abéliens [Bec94], les groupes symétriques [Bec94], les groupes alternés [Mes90] [KM01, théorème 3] et les groupes diédraux D_n (de cardinal $2n$) avec n impair ou $n = 2^d$ avec $d \leq 4$ [Bla98] [Bla99].

Enfin, il est à noter que l'on ne connaît pas, à l'heure actuelle, de couples (k, G) tels que la réponse à l'énoncé (BB/k/G) soit négative.

A.2 Présentation du travail

Cette thèse est composée de trois parties que nous présentons ci-dessous. Elles sont précédées d'un chapitre de préliminaires dans lequel nous introduisons le matériel utilisé dans ce travail.

A.2.1 Présentation de la partie I (chapitre 1)

La première partie porte sur le comportement local des extensions de $\mathbb{Q}$ obtenues par spécialisation d'extensions régulières galoisiennes de $\mathbb{Q}(T)$. Plus précisément, étant donnés un groupe fini G et une extension régulière galoisienne $E/\mathbb{Q}(T)$ de groupe G, peut-on construire des spécialisations de $E/\mathbb{Q}(T)$ en des points non-ramifiés $t_0 \in \mathbb{Q}$ qui d'une part restent de groupe G et dont on impose d'autre part le comportement local en un nombre fini de nombres premiers ?

Cette question a été étudiée par Dèbes et Ghazi dans les deux articles [DG12] et [DG11] dans un cadre non-ramifié : ils montrent que toute extension régulière galoisienne $E/\mathbb{Q}(T)$ de groupe G a des spécialisations de même groupe, qui sont non-ramifiées en chaque nombre premier d'un ensemble fini fixé au préalable (la seule condition étant que chacun de ces nombres premiers doit être assez grand) et dont ils imposent de plus le groupe de décomposition en chacun d'entre eux.

Nous nous intéressons dans un premier temps à un comportement local ramifié, *i.e.* nous cherchons à construire des spécialisations de $E/\mathbb{Q}(T)$ possédant d'une part un groupe de Galois égal à G et dont on impose d'autre part le groupe d'inertie en un nombre fini de nombres premiers fixés au préalable.

Notons $t_1, \dots, t_r$ les points de branchement de $E/\mathbb{Q}(T)$. Etant donnés un nombre premier p assez grand (dépendant de $E/\mathbb{Q}(T)$) et un nombre rationnel $t_0 \notin \{t_1, \dots, t_r\}$, une condition nécessaire classique pour que p se ramifie dans $E_{t_0}/\mathbb{Q}$ est qu'il existe un idéal premier $\mathcal{P}$ de degré résiduel 1 au dessus de p dans l'extension $k(t_{i_p})/k$ pour un certain indice $i_p \in \{1, \dots, r\}$ (nous dirons pour simplifier que "t_{i_p} est rationalisé par p"). De plus, d'autres résultats montrent que le groupe d'inertie de $E_{t_0}/\mathbb{Q}$ en p est engendré par une certaine puissance $g_{i_p}^{a_p}$ (dépendant de t_0 et t_{i_p}) du générateur distingué g_{i_p} d'un certain groupe d'inertie de $E\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ en t_{i_p}.

Le résultat principal de cette partie fournit une certaine réciproque à la dernière conclusion : pour tout nombre premier p assez grand (dépendant de $E/\mathbb{Q}(T)$), si p rationalise t_{i_p}, en particulier si t_{i_p} est lui-même $\mathbb{Q}$-rationnel, alors il est possible d'imposer l'exposant a_p ci-dessus pour certains nombres rationnels t_0 bien choisis. Pour tout $i \in \{1, \dots, r\}$, notons C_i la classe de conjugaison de g_i dans G.

Théorème. *Soit $\mathcal{S}$ un ensemble fini de nombres premiers p assez grands (dépendant de $E/\mathbb{Q}(T)$), chacun étant muni d'un couple (i_p, a_p) où*
- i_p est un élément de $\{1, \dots, r\}$ tel que p rationalise t_{i_p},
- a_p est un entier naturel non-nul.
Alors il existe une infinité de nombres rationnels t_0 deux à deux distincts tels que la spécialisation $E_{t_0}/\mathbb{Q}$ de $E/\mathbb{Q}(T)$ en t_0 vérifie les deux conditions suivantes :
(1) $\mathrm{Gal}(E_{t_0}/\mathbb{Q}) = G$,
(2) *pour chaque nombre premier $p \in \mathcal{S}$, le groupe d'inertie de la spécialisation $E_{t_0}/\mathbb{Q}$ en p est engendré par un élément de $C_{i_p}^{a_p}$.*

Nous montrons dans un second temps qu'il est possible de réunir ce théorème et le résultat de Dèbes et Ghazi précédemment évoqué pour obtenir, pour tout groupe fini G qui est groupe de Galois d'au moins une extension régulière galoisienne de $\mathbb{Q}(T)$, un résultat général d'existence d'extensions galoisiennes de $\mathbb{Q}$ de groupe G et dont on impose de plus le comportement local (ramifié ou non-ramifié) en un nombre fini de nombres premiers.

A.2.2 Présentation de la partie II (chapitres 2 et 3)

Etant donné un groupe fini H et un corps k, on s'intéresse dans cette deuxième partie aux *extensions H-paramétriques sur k*, *i.e.* aux extensions finies régulières galoisiennes $E/k(T)$ de groupe de Galois G contenant H telles que n'importe quelle extension galoisienne F/k de groupe H soit une spécialisation de $E/k(T)$.

A.2.2.1. Chapitre 2. Ce chapitre a trois objectifs principaux.

(a) Dans un premier temps, nous plaçons la notion d'extension paramétrique dans le contexte de la théorie inverse de Galois.

Par exemple, s'il existe une extension G-paramétrique sur k de groupe G, alors l'énoncé (BB$/k/G$) a clairement une réponse positive. *A contrario*, s'il n'existe pas de telles extensions, alors il ne peut exister de *polynômes génériques à un paramètre pour G sur k*, c'est à dire de polynômes $P(T,Y) \in k[T][Y]$ de groupe G et de corps de décomposition E sur $k(T)$ vérifiant la propriété suivante : l'extension $EL/L(T)$ est G-paramétrique sur L pour toute extension L/k.

(b) Dans un deuxième temps, nous donnons quelques premières conclusions sur les extensions paramétriques (basées sur des travaux précédents) sur des corps variés comme par exemple les corps PAC, les corps finis, certains corps de séries de Laurent ou encore le corps $\mathbb{Q}$ et ses complétions.

Par exemple, si k est PAC [4], la situation est très claire : il existe une extension H-paramétrique sur k de groupe G pour n'importe quels groupes finis $H \subset G$. *A contrario*, si $k = \mathbb{Q}$, peu de choses sont connues bien que l'on puisse avoir l'intuition que peu d'extensions sont paramétriques sur $\mathbb{Q}$. D'un côté, on sait qu'il existe une extension G-paramétrique sur $\mathbb{Q}$ de groupe G pour chacun des quatre groupes $\{1\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et S_3. Pour tout autre groupe fini G, on ignore s'il existe ou non une telle extension. D'un autre côté, peu d'exemples d'extensions non-paramétriques sur $\mathbb{Q}$ sont connus à l'heure actuelle.

(c) Dans un dernier temps, nous donnons quelques nouveaux exemples d'extensions non H-paramétriques sur $\mathbb{Q}$ de groupe G à l'aide d'arguments *ad hoc*.

Par exemple, nous utilisons l'absence de solutions à certaines équations diophantiennes pour obtenir le résultat suivant :

Proposition. *Aucune extension régulière galoisienne de $\mathbb{Q}(T)$ de groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ à trois points de branchement n'est $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-paramétrique sur $\mathbb{Q}$.*

A.2.2.2. Chapitre 3. En fait, étant donnés un corps de nombres k et un groupe fini H, déterminer si une extension finie régulière galoisienne $E/k(T)$ de groupe G contenant H est H-paramétrique sur k ou non semble être une question difficile, même dans le cas de groupes « élémentaires » : par exemple, dans le cas $k = \mathbb{Q}$ et $H = G = \mathbb{Z}/3\mathbb{Z}$, il semblerait qu'on ne connaisse la réponse que pour une seule extension régulière galoisienne de $\mathbb{Q}(T)$ de groupe $\mathbb{Z}/3\mathbb{Z}$. Bien entendu, il existe des exemples évidents comme les extensions $\mathbb{Q}(e^{2i\pi/n})(\sqrt[n]{T})/\mathbb{Q}(e^{2i\pi/n})(T)$ $(n \in \mathbb{N} \setminus \{0\})$ et $\mathbb{Q}(T)(\sqrt{T^2+1})/\mathbb{Q}(T)$: la première est $\mathbb{Z}/n\mathbb{Z}$-paramétrique sur $\mathbb{Q}(e^{2i\pi/n})$ en vertu de la théorie de Kummer alors que la seconde n'est pas $\mathbb{Z}/2\mathbb{Z}$-paramétrique sur $\mathbb{Q}$ car aucune de ses spécialisations n'est imaginaire. Mais il semblerait qu'ils soient assez rares.

Dans ce chapitre, nous développons une méthode générale pour donner davantage d'exemples d'extensions non H-paramétriques de groupe G sur des corps variés comme par exemple les corps de nombres ou encore les extensions finies de corps de fractions rationnelles $\kappa(U)$ (la lettre U désignant une indéterminée) à coefficients dans un corps κ de caractéristique nulle.

Etant donnés un tel corps k, deux groupes finis $H \subset G$, une extension régulière galoisienne

4. Rappelons qu'un corps k est dit *Pseudo Algébriquement Clos* (PAC) si toute k-variété non-vide géométriquement irréductible possède un ensemble Zariski-dense de points k-rationnels. Nous renvoyons au §B.2.1 pour des exemples de tels corps.

$E_H/k(T)$ de groupe H et une extension régulière galoisienne $E_G/k(T)$ de groupe G, nous utilisons les résultats de la partie I pour construire des spécialisations de $E_H/k(T)$ de groupe H qui ne peuvent être spécialisation de $E_G/k(T)$ (et donc l'extension $E_G/k(T)$ n'est pas H-paramétrique sur k). Plus précisément, nous donnons deux conditions suffisantes qui chacune garantissent une telle conclusion. La première porte sur l'arithmétique des points de branchement tandis que la seconde est une condition plus géométrique sur l'inertie des extensions $E_H/k(T)$ et $E_G/k(T)$.

Chacune de ces deux conditions fournit de nombreux exemples d'extensions non H-paramétriques de groupe G sur des corps variés. Nous obtenons tout d'abord l'énoncé suivant qui fournit, pour de nombreux groupes finis G, des extensions non G-paramétriques de groupe G sur des corps de nombres assez gros :

Théorème. *Soit G un groupe fini. Supposons qu'il existe un ensemble $\{C_1, \dots, C_r, C\}$ de classes de conjugaison non-triviales de G satisfaisant les deux conditions suivantes :*

(1) *les éléments de $C_1, \dots, C_r$ engendrent G,*

(2) *il n'existe pas d'indice $i \in \{1, \dots, r\}$ tel que C soit égale à une puissance de C_i.*

Alors il existe un corps de nombres k et une extension régulière galoisienne de $k(T)$ de groupe G qui n'est pas G-paramétrique sur k.

De nombreux groupes finis possèdent un ensemble de classes de conjugaison satisfaisant les conditions (1) et (2) ci-dessus. Citons par exemple les groupes abéliens qui ne sont pas cycliques d'ordre une puissance d'un nombre premier, les groupes symétriques S_n ($n \geq 3$), les groupes alternés A_n ($n \geq 4$), les groupes diédraux D_n ($n \geq 2$) ou encore les groupes simples non-abéliens.

Nous obtenons également de nombreux exemples sur des corps de base k fixés au préalable (en particulier sur $\mathbb{Q}$) en appliquant nos critères à quelques extensions finies régulières galoisiennes de $k(T)$ bien connues. En voici trois :

Théorème. (1) *Etant donnés un entier $n \geq 5$ et une extension finie k de n'importe quel corps de fractions rationnelles $\kappa(U)$ à coefficients dans un corps κ de caractéristique nulle, le trinôme $Y^n - Y - T$ fournit une extension régulière galoisienne de $k(T)$ de groupe S_n qui n'est ni S_n-paramétrique sur k, ni A_n-paramétrique sur k.*

(2) *Soient $r \geq 3$ un entier et k un corps de nombres ou une extension finie du corps de fractions rationnelles $\mathbb{C}(U)$. Alors il existe un entier naturel n_r ne dépendant pas du corps de base k et satisfaisant la conclusion suivante : pour tout entier naturel $n > n_r$, aucune extension régulière galoisienne de $k(T)$ de groupe A_n à r points de branchement n'est A_n-paramétrique sur k.*

(3) *Soit k un corps de nombres. Alors, si* Th *désigne le groupe de Thompson, aucune extension régulière galoisienne de $k(T)$ de groupe le Bébé Monstre* B *et d'invariant canonique de l'inertie $(2C, 3A, 55A)$ n'est* Th*-paramétrique sur k.*

A.2.3 Présentation de la partie III (chapitres 4 et 5)

Etant donné un corps k, on s'intéresse dans cette dernière partie aux spécialisations d'extensions régulières de $k(T)$ non nécessairement galoisiennes. Dans cette situation, la propriété de spécialisation de Hilbert est la suivante : étant donnés un entier naturel non-nul n et une extension régulière $E/k(T)$ de degré n, il existe une infinité de points $t_0 \in k$ deux à deux distincts tels que la spécialisation de $E/k(T)$ en t_0 ne soit constituée que d'une seule extension de k de degré n. Une variante non galoisienne du problème de Beckmann-Black serait donnée par l'énoncé suivant : étant donnés un entier naturel non-nul n et une extension F/k de degré n, existe t-il une extension régulière $E_F/k(T)$ de même degré possédant F/k parmi ses spécialisations ?

Le thème principal de cette partie, qui résulte d'une collaboration avec P. Dèbes, est l'étude de la question plus générale suivante :

Une k-algèbre étale $\prod_l F_l/k$ est-elle la spécialisation d'une extension séparable $E/k(T)$ de même degré en un certain point non-ramifié $t_0 \in \mathbb{P}^1(k)$?

Cette question a déjà été étudiée dans les articles [Dèb99c], [DG12] et [DG11] dans le cadre des extensions $E/k(T)$ régulières galoisiennes. Ici on étudie la situation plus générale des extensions non nécessairement régulières et/ou non nécessairement galoisiennes.

A.2.3.1. Le twisting lemma. Comme dans les articles précédemment cités, notre principal outil est un *twisting lemma* qui réduit la question à trouver des points k-rationnels sur certaines k-variétés. *Grosso modo*, on construit, à partir de la k-algèbre étale $\prod_l F_l/k$ et de l'extension $E/k(T)$, une k-variété X vérifiant la propriété suivante : sous certaines hypothèses,

si (1) *il existe un point k-rationnel sur la variété X,*

alors (2) *$\prod_l F_l/k$ est une spécialisation de $E/k(T)$.*

Une première variante de ce *twisting lemma* a été établie dans les articles [Dèb99c] et [DG12] pour les extensions $E/k(T)$ régulières galoisiennes. Dans un premier temps, nous en établissons diverses variantes dans des situations de technicité variable. Le chapitre 4 est consacré à une variante pratique non-galoisienne alors que le chapitre 5 porte sur deux variantes plus techniques, dont une est consacrée à la situation la plus générale des extensions non nécessairement régulières et non nécessairement galoisiennes.

A.2.3.2. Applications. Le *twisting lemma* fournit une approche générale ne dépendant pas du corps de base k : le problème est réduit à trouver des points k-rationnels sur la variété X. Nous étudions dans un second temps cette nouvelle question pour de nombreux corps k sur lesquels des techniques classiques peuvent être utilisées : corps PAC, corps amples, corps finis, corps valués complets et corps de nombres. Nous présentons brièvement la situation des corps PAC et la situation du corps $\mathbb{Q}$ ci-dessous.

(a) *Situation k PAC.* Si k est PAC, la condition (1) ci-dessus est satisfaite par définition. Il existe alors une infinité de points $t_0 \in k$ deux à deux distincts tels que $\prod_l F_l/k$ soit la spécialisation de $E/k(T)$ en t_0. Ceci a un impact fort sur l'arithmétique des corps PAC ; on peut par exemple en déduire l'énoncé suivant :

Théorème. *Soit k un corps PAC de caractéristique nulle. Alors la clôture séparable k^{sep} de k est engendrée par tous les éléments $y \in k^{\mathrm{sep}}$ tels que $y^n - y \in k$ où $n = [k(y) : k]$.*

(b) *Situation $k = \mathbb{Q}$.* La situation du corps $k = \mathbb{Q}$ (et plus généralement des corps de nombres) est très différente de celle des corps PAC. Par exemple, si le genre de l'extension $E/\mathbb{Q}(T)$ vaut au moins 2, le théorème de Faltings entraîne que la variété X n'a qu'un nombre fini de points $\mathbb{Q}$-rationnels. Il suit alors du *twisting lemma* que l'algèbre étale $\prod_l F_l/\mathbb{Q}$ ne peut être spécialisation de l'extension $E/\mathbb{Q}(T)$ qu'en un nombre fini de nombres rationnels t_0 deux à deux distincts (éventuellement aucun).

Néanmoins, des arguments de type « local-global » peuvent être utilisés et mènent par exemple au résultat suivant qui est une version du théorème d'irréductibilité de Hilbert munie d'une conclusion de type Grunwald [5] :

Théorème. *Soient $E/\mathbb{Q}(T)$ une extension de degré n telle que la clôture galoisienne $\widehat{E}/\mathbb{Q}(T)$ vérifie* $\mathrm{Gal}(\widehat{E}\overline{\mathbb{Q}}(T)/\overline{\mathbb{Q}}(T)) = S_n$ *et $\mathcal{S}$ un ensemble fini de nombres premiers p assez grands (dé-*

5. Notons qu'il s'agit d'un analogue non galoisien du résultat de Dèbes et Ghazi évoqué au début du §A.2.1.

pendant de $E/\mathbb{Q}(T)$), chacun étant muni d'entiers naturels tous non-nuls $d_{p,1}, \dots, d_{p,s_p}$ de somme égale à n. Alors il existe une infinité de nombres rationnels t_0 deux à deux distincts vérifiant les deux conditions suivantes :
(1) *la spécialisation de $E/\mathbb{Q}(T)$ en t_0 n'est formée que d'une seule extension de corps $E_{t_0}/\mathbb{Q}$ de degré n,*
(2) *chaque nombre premier $p \in \mathcal{S}$ est non-ramifié dans $E_{t_0}/\mathbb{Q}$ et les entiers $d_{p,1}, \dots, d_{p,s_p}$ sont exactement les degrés résiduels de $E_{t_0}/\mathbb{Q}$ en p.*

Preliminaries

The aim of this chapter consists in setting up the notation and the basic notions we will use in the rest of this thesis. The first section is devoted to covers, function field extensions and their specializations, étale algebras, fundamental groups and their representations. In the second one, we recall the definition and some examples of PAC fields and ample fields. The third one is concerned with some examples of covers of $\mathbb{P}^1$ which will be used in several occasions in this thesis. The reader who is familiar with these notions can skip this chapter and come back to it when needed.

B.1 Basics

Given a field k, we fix an algebraic closure $\overline{k}$ and denote the separable closure of k in $\overline{k}$ by k^{sep} and its absolute Galois group by G_k. If k' is an overfield of k, we use the notation $\otimes_k k'$ for the scalar extension from k to k': for instance, if X is a k-curve, $X \otimes_k k'$ is the k'-curve obtained by scalar extension from k to k'. Let B be a regular projective geometrically irreducible k-variety. For more on this section, we refer for example to [DD97b, §2] or [Dèb09, chapter 3].

B.1.1 Covers and function field extensions

B.1.1.1. Generalities. Recall that a *k-cover of B* is a finite and generically unramified morphism $f : X \rightarrow B$ defined over k with X a normal and irreducible k-variety.

Through the function field functor, k-covers $f : X \rightarrow B$ correspond (up to isomorphism) to finite separable function field extensions $k(X)/k(B)$. The k-cover $f : X \rightarrow B$ is said to be *Galois* if the corresponding function field extension $k(X)/k(B)$ is; if in addition $f : X \rightarrow B$ is given together with an isomorphism from a given finite group G to the Galois group $\mathrm{Gal}(k(X)/k(B))$, it is called a k-G-*Galois cover of group G*, and the corresponding function field extension $k(X)/k(B)$ is then called a G-*Galois extension of group G (of $k(B)$).*

Warning. *Throughout this thesis, we will indifferently use the cover viewpoint or that of function field extensions. In particular, all the notions recalled below for covers are also for field extensions. For example, the branch divisor of a function field extension is that of the corresponding cover.*

A k-cover $f : X \rightarrow B$ is said to be *regular* if $k(X)$ is a regular extension of k, *i.e.* if $k(X) \cap \overline{k} = k$, or, equivalently, if X is geometrically irreducible. In general, there is some *constant extension* in $f : X \rightarrow B$, which we denote by $\widehat{k}_f/k$ and define by $\widehat{k}_f = k(X) \cap k^{\mathrm{sep}}$ (the special case $\widehat{k}_f = k$ corresponds to the situation f is regular).

Remark B.1.1. To make the rest of this thesis simpler, we will use the following terminology: a regular k-G-Galois cover $f : X \rightarrow B$ of group G will be called a k-G-*cover of group G* and the corresponding function field extension will be called a G-*extension of group G (of $k(B)$).*

If $f : X \to B$ is a k-cover, its Galois closure over k is a Galois k-cover $g : Z \to B$ which, *via* the covers-function field extensions dictionary, corresponds to the Galois closure of $k(X)/k(B)$. The Galois group $\mathrm{Gal}(k(Z)/k(B))$ is called the *monodromy group* of f. Denote next by $k^{\mathrm{sep}}(Z)$ the *compositum* of $k(Z)$ and k^{sep} (in a fixed separable closure of $k(B)$) [1]. The Galois group $\mathrm{Gal}(k^{\mathrm{sep}}(Z)/k^{\mathrm{sep}}(B))$ is called the *geometric monodromy group* of f; it is a normal subgroup of the monodromy group $\mathrm{Gal}(k(Z)/k(B))$ (these two groups coincide if and only if g is regular). The *branch divisor* of the k-cover f is the formal sum of all the hypersurfaces of $B \otimes_k k^{\mathrm{sep}}$ such that the associated discrete valuations are ramified in the function field extension $k^{\mathrm{sep}}(Z)/k^{\mathrm{sep}}(B)$.

If $f : X \to B$ is regular, then $f \otimes_k k^{\mathrm{sep}}$ is a (regular) k^{sep}-cover, the Galois closure of its function field extension is $k^{\mathrm{sep}}(Z)/k^{\mathrm{sep}}(B)$ and its branch divisor is the same as that of f, and it is the formal sum of all the hypersurfaces of $B \otimes_k k^{\mathrm{sep}}$ such that the associated discrete valuations are ramified in the function field extension $k^{\mathrm{sep}}(X)/k^{\mathrm{sep}}(B)$. From Purity of the Branch Locus, f is étale above $B \setminus D$.

B.1.1.2. The case $B = \mathbb{P}^1$. In this situation, the branch divisor D of a given k-cover $f : X \to \mathbb{P}^1$ is more simply denoted by $\mathbf{t} = \{t_1, \ldots, t_r\}$. The points $t_1, \ldots, t_r$ are called *the branch points of f*. Moreover, if f is a k-G-cover and k has characteristic zero, one may define the *inertia canonical invariant of f*.

Fix a *coherent system $\{\zeta_n\}_{n=1}^{\infty}$ of roots of unity*, *i.e.* ζ_n is a primitive n-th root of unity and $\zeta_{nm}^n = \zeta_m$ for any positive integers n and m. To each branch point t_i of f can be associated a conjugacy class C_i of the Galois group $\mathrm{Gal}(k(X)/k(T))$, called the *inertia canonical conjugacy class (associated with t_i)*, in the following way. The inertia groups of $\overline{k}(X)/\overline{k}(T)$ at t_i are cyclic conjugate groups of order equal to the ramification index e_i. Furthermore each of them has a distinguished generator corresponding to the automorphism $(T-t_i)^{1/e_i} \mapsto \zeta_{e_i}(T-t_i)^{1/e_i}$ of $\overline{k}(((T-t_i)^{1/e_i}))$ (replace $T - t_i$ by $1/T$ if $t_i = \infty$). Then C_i is the conjugacy class in $\mathrm{Gal}(k(X)/k(T))$ of all the distinguished generators of the inertia groups at t_i. The unordered r-tuple $(C_1, \ldots, C_r)$ is called *the inertia canonical invariant of f*.

B.1.2 Etales algebras and their Galois representations

Given a field k, a *k-étale algebra* is a product $\prod_{l=1}^{s} F_l/k$ of finite subfield extensions $F_1/k, \ldots, F_s/k$ of k^{sep}/k. Set $m_l = [F_l : k]$ for each index $l = 1, \ldots, s$ and $m = \sum_{l=1}^{s} m_l$; call the integer m the *degree of* $\prod_{l=1}^{s} F_l/k$. If N/k is a Galois extension containing the Galois closures of the extensions $F_1/k, \ldots, F_s/k$, the Galois group $\mathrm{Gal}(N/k)$ acts by left multiplication on the left cosets of $\mathrm{Gal}(N/k)$ modulo $\mathrm{Gal}(N/F_l)$ for each index $l = 1, \ldots, s$. The resulting action $\mathrm{Gal}(N/k) \to S_m$ on the set of these m left cosets, which is well-defined up to equivalence, *i.e.* up to conjugation by an element of S_m, is called the *Galois representation of $\prod_{l=1}^{s} F_l/k$ relative to N*. Equivalently it can be defined as the action of $\mathrm{Gal}(N/k)$ on the set of all k-embeddings $F_l \hookrightarrow N$, $l = 1, \ldots, s$.

Conversely an action $\mu : \mathrm{Gal}(N/k) \to S_m$ determines a k-étale algebra in the following way. For each index $i \in \{1, \ldots, m\}$, denote the fixed field in N of the subgroup of $\mathrm{Gal}(N/k)$ consisting of all elements τ such that $\mu(\tau)(i) = i$ by F_i. The product $\prod_l F_l/k$ for l ranging over a set of representatives of the orbits of the action μ is a k-étale algebra of degree m. If two k-étale algebras $\prod_{l=1}^{s} F_l/k$ and $\prod_{l=1}^{s'} F'_l/k$ are obtained in this manner from two different choices of the set of representatives of the orbits of μ, then they are equivalent in the sense that $s = s'$ and there exist $\sigma_1, \ldots, \sigma_s$ in $\mathrm{Gal}(N/k)$ such that $\sigma_l(F_l) = F'_l$ for each index $l \in \{1, \ldots, s\}$. Equivalently an equivalence class of k-étale algebras can be viewed as a product of k-isomorphism classes of

1. Note that, as $g : Z \to B$ is Galois, $k(Z)$ only depends on the $k(B)$-isomorphism class of $k(X)/k(B)$ (but not on $k(X)/k(B)$ itself).

finite subfield extensions of k^{sep}/k.

G-*Galois variant.* If $\prod_{l=1}^{s} F_l/k$ is a single Galois extension F/k, the restriction $\text{Gal}(N/k) \to \text{Gal}(F/k)$ is called *the* G-*Galois representation of* F/k *(relative to* N*)*. Any map $\varphi : \text{Gal}(N/k) \to G$ obtained by composing $\text{Gal}(N/k) \to \text{Gal}(F/k)$ with a monomorphism $\text{Gal}(F/k) \to G$ is called *a G-Galois representation of* F/k *(relative to* N*)*. The extension F/k can be recovered from $\varphi : \text{Gal}(N/k) \to G$ by taking the fixed field in N of $\ker(\varphi)$. One obtains the Galois representation $\text{Gal}(N/k) \to S_n$ of F/k (relative to N) from a G-Galois representation $\varphi : \text{Gal}(N/k) \to G$ (relative to N) by composing it with the left-regular representation of the image group $\varphi(\text{Gal}(N/k))$; here $n = |\varphi(\text{Gal}(N/k))|$.

B.1.3 π_1-representations

Given a reduced effective divisor $D \subset B$ and a base point $t \in B(\overline{k}) \setminus D$ (which corresponds to the choice of an algebraic closure of $k(B)$), denote the *k-fundamental group* of $B \setminus D$ by $\pi_1(B \setminus D, t)_k$.

B.1.3.1. Representations of k-covers. Via the covers-function field extensions and field extensions-Galois representations dictionaries, k-covers $f : X \to B$ of degree n with branch divisor contained in D correspond to transitive morphisms $\phi : \pi_1(B \setminus D, t)_k \to S_n$ [2]. The k-cover f is regular if and only if the restriction of ϕ to $\pi_1(B \setminus D, t)_{k^{\text{sep}}}$ remains transitive and, in this case, this restriction represents the (regular) k^{sep}-cover $f \otimes_k k^{\text{sep}}$.

*B.1.3.2. Representations of k-*G*-Galois covers.* Similarly k-G-Galois covers $f : X \to B$ of group G with branch divisor contained in D correspond to epimorphisms $\phi : \pi_1(B \setminus D, t)_k \to G$. The k-G-Galois cover f is regular if and only if the restriction of ϕ to $\pi_1(B \setminus D, t)_{k^{\text{sep}}}$ remains onto, and, in this case, this restriction represents the k-G-cover $f \otimes_k k^{\text{sep}}$.

Any k-G-Galois cover $f : X \to B$ of group G with branch divisor contained in D and corresponding epimorphism $\phi : \pi_1(B \setminus D, t)_k \to G$ provides a Galois k-cover (with same branch divisor and same Galois group) by composing ϕ with the left-regular representation of G.

These morphisms are called *fundamental group representations* (π_1-representations for short) of the corresponding k-covers and k-G-Galois covers.

B.1.4 Specializations

Each k-rational point $t_0 \in B(k) \setminus D$ provides a section $\mathsf{s}_{t_0} : \text{G}_k \to \pi_1(B \setminus D, t)_k$ to the exact sequence

$$1 \to \pi_1(B \setminus D, t)_{k^{\text{sep}}} \to \pi_1(B \setminus D, t)_k \to \text{G}_k \to 1$$

which is uniquely defined up to conjugation by an element in $\pi_1(B \setminus D, t)_{k^{\text{sep}}}$.

*B.1.4.1. Specializations of k-*G*-Galois covers.* If $\phi : \pi_1(B \setminus D, t)_k \to G$ represents a k-G-Galois cover $f : X \to B$ of group G, the morphism $\phi \circ \mathsf{s}_{t_0} : \text{G}_k \to G$ is a G-Galois representation; it is called the G-*specialization representation of f at t_0*. The fixed field in k^{sep} of $\ker(\phi \circ \mathsf{s}_{t_0})$ is denoted by $k(X)_{t_0}$ and the extension $k(X)_{t_0}/k$ is called *the specialization of f at t_0*. It is a Galois extension of k of group $\text{Im}(\phi \circ \mathsf{s}_{t_0}) \subset G$. The specialization $k(X)_{t_0}/k$ is also the residue field at some prime above t_0 in the extension $k(X)/k(B)$ (in fact at any prime above t_0 since $k(X)/k(B)$ is Galois).

2. *i.e.* such that the image group $\phi(\pi_1(B \setminus D, t)_k)$ is a transitive subgroup of S_n.

If f is a k-G-cover, the field $k(X)_{t_0}$ is the definition field of the points in the fiber $f^{-1}(t_0)$ and $\phi \circ \mathsf{s}_{t_0} : \mathrm{G}_k \to G$ corresponds to the action of G_k on them.

In the case $B = \mathbb{P}^1$ and $f : X \to \mathbb{P}^1$ is given by some polynomial $P(T,Y) \in k[T][Y]$ [3], one has lemma B.1.2 below which will be used in several occasions in the rest of this thesis:

Lemma B.1.2. *Let $P(T,Y) \in k[T][Y]$ be a monic (with respect to Y) separable polynomial of splitting field E over $k(T)$. Then, for any $t_0 \in k$ such that $P(t_0,Y)$ is separable over k, one has the following two conclusions.*
(1) The point t_0 is not a branch point of $E/k(T)$.
(2) The specialization E_{t_0}/k of $E/k(T)$ (viewed as a G*-Galois extension) at t_0 is the splitting extension over k of $P(t_0,Y)$.*

Proof. Denote the degree of $P(T,Y)$ by n and its roots by $y_1(T), \dots, y_n(T)$.

To prove conclusion (1), assume by contradiction that t_0 is a branch point of $E/k(T)$. Then $\langle T - t_0 \rangle$ ramifies in $Ek^{\mathrm{sep}}/k^{\mathrm{sep}}(T)$. From [Dèb09, §1.5.4.4], there exists some prime ideal $\mathcal{P}$ of the integral closure A of $k^{\mathrm{sep}}[T]$ in Ek^{sep} such that $\mathcal{P} \cap k^{\mathrm{sep}}[T] = \langle T - t_0 \rangle$ and the inertia group $I_{\mathcal{P}}$ is not trivial, *i.e.* there exists some $\sigma \in \mathrm{Gal}(Ek^{\mathrm{sep}}/k^{\mathrm{sep}}(T)) \setminus \{\mathrm{id}_{Ek^{\mathrm{sep}}}\}$ such that $\sigma(a) - a \in \mathcal{P}$ for any $a \in A$. Since $\sigma \neq \mathrm{id}_{Ek^{\mathrm{sep}}}$, there exists some index $i \in \{1, \dots, n\}$ such that $\sigma(y_i(T)) - y_i(T) \neq 0$. Then the reductions modulo $\mathcal{P}$ of $y_i(T)$ and $\sigma(y_i(T))$ coincide, thus showing that the specialized polynomial $P(t_0,Y)$ is not separable over k.

To prove conclusion (2), let $\mathcal{P}$ be a prime ideal of the integral closure A of $k[T]$ in E such that $\mathcal{P} \cap k[T] = \langle T - t_0 \rangle$. With $y_i(t_0)$ the reduction modulo $\mathcal{P}$ of $y_i(T)$ ($i = 1, \dots, n$), we show below that $A/\mathcal{P} = k(y_1(t_0), \dots, y_n(t_0))$.

Denote the field $k(T)(y_1(T))$ by E_1, the integral closure of $k[T]$ in E_1 by A_1, the irreducible polynomial of $y_1(T)$ over $k(T)$ by $P_1(T,Y)$, its degree by d_1 and its discriminant by $\Delta_1(T)$. From [Dèb09, theorem 1.3.13], one has $\Delta_1(T)\, A_1 \subset k[T] + k[T]\, y_1(T) + \dots + k[T]\, y_1^{d_1-1}(T)$. As $P(t_0,Y)$ is separable over k from our assumption, this is also true of $P_1(t_0,Y)$. Hence $\Delta_1(t_0) \neq 0$ and one has then $A_1/(\mathcal{P} \cap A_1) = k(y_1(t_0))$.

Denote next the field $k(T)(y_1(T), y_2(T))$ by E_2, the integral closure of A_1 in E_2 by A_2, the irreducible polynomial of $y_2(T)$ over E_1 by $P_2(Y)$, its degree by d_2 and its discriminant by Δ_2. As before, one has $\Delta_2\, A_2 \subset A_1 + A_1\, y_2(T) + \dots + A_1\, y_2^{d_2-1}(T)$ and $\Delta_2 \neq 0$ modulo $\mathcal{P} \cap A_2$. Hence $A_2/(\mathcal{P} \cap A_2) = k(y_1(t_0), y_2(t_0))$. Adding $y_3(T), \dots, y_n(T)$ one by one provides the conclusion. □

B.1.4.2. Specializations of k-covers. If $\phi : \pi_1(B \setminus D, t)_k \to S_n$ represents a k-cover $f : X \to B$ of degree n, the morphism $\phi \circ \mathsf{s}_{t_0} : \mathrm{G}_k \to S_n$ is called *the specialization representation of f at* t_0. The corresponding k-étale algebra is denoted by $\prod_{l=1}^{s} k(X)_{t_0,l}/k$ and called the *specialization algebra of $k(X)/k(B)$ at t_0*. Each field $k(X)_{t_0,l}$ is a residue extension at some prime above t_0 in the extension $k(X)/k(B)$ and *vice-versa*; $k(X)_{t_0,l}$ is called *a specialization of $k(X)/k(B)$ at t_0*. The *compositum* in k^{sep} of the Galois closures of all the specializations at t_0 is *the* specialization at t_0 of the Galois closure of f (viewed as a k-G-Galois cover).

If f is regular, the fields $k(X)_{t_0,l}$ correspond to the definition fields of the points in the fiber $f^{-1}(t_0)$ and $\phi \circ \mathsf{s}_{t_0} : \mathrm{G}_k \to S_n$ to the action of G_k on them.

The counterpart of lemma B.1.2 for k-covers is given by lemma B.1.3 below:

Lemma B.1.3. *Let $P(T,Y) \in k[T][Y]$ be a monic (with respect to Y) separable polynomial which is irreducible over $k(T)$ and E be the field generated over $k(T)$ by one of its roots. Then, for any $t_0 \in k$ such that $P(t_0,Y)$ is separable over k, one has the following two conclusions.*

3. *i.e.* the corresponding function field extension $k(X)/k(T)$ is the splitting extension over $k(T)$ of $P(T,Y)$.

(1) *The point t_0 is not a branch point of $E/k(T)$.*
(2) *Consider the factorization $P(t_0, Y) = P_1(Y) \dots P_s(Y)$ of $P(t_0, Y)$ in irreducible polynomials $P_l(Y) \in k[Y]$ and, for each $l \in \{1, \dots, s\}$, denote the field generated over k by one of the roots of $P_l(Y)$ by F_l. Then the specialization algebra of $E/k(T)$ at t_0 is the k-étale algebra $\prod_{l=1}^{s} F_l/k$.*

Proof. Conclusion (1) easily follows from part (1) of lemma B.1.2. To prove conclusion (2), let y be a root of $P(t_0, Y)$, $y(T)$ be a root of $P(T, Y)$ and denote the integral closure of $k[T]$ in E by A. From [Dèb09, theorem 1.7.1], there exists some morphism $\varphi_y : A \to \overline{k}$ fixing any element of k and such that $T \mapsto t_0$ and $y(T) \mapsto y$. With n the degree of $P(T, Y)$ and $\Delta(T)$ its discriminant, one has $\Delta(T)\, A \subset k[T] + k[T]\, y(T) + \dots + k[T]\, y^{n-1}(T)$ [Dèb09, theorem 1.3.13]. As $\Delta(t_0) \neq 0$ from our assumption, the morphism φ_y is necessarily unique and one has then $\mathrm{Im}(\varphi_y) = k(y)$. The desired conclusion then follows from the one-one correspondence between the root set of $P(t_0, Y)$ modulo the k-conjugation and the set of prime ideals of A above $\langle T - t_0 \rangle$ provided by the map $y \mapsto \ker(\varphi_y)$. $\square$

B.2 Some classical fields

B.2.1 PAC fields

Recall that a field k is said to be *Pseudo Algebraically Closed* (PAC) if every non-empty geometrically irreducible k-variety has a Zariski-dense set of k-rational points. Here are some examples of PAC fields.

(1) Algebraically closed fields are PAC.

(2) Given a countable hilbertian field k, the fixed field $(k^{\mathrm{sep}})^{\sigma}$ is PAC for almost all $\sigma \in \mathrm{G}_k$ (with respect to the Haar mesure) [FJ05, theorem 18.6.1].

(3) A concrete example of PAC field, due to Pop, is the field $\mathbb{Q}^{\mathrm{tr}}(\sqrt{-1})$ (which is also hilbertian and whose absolute Galois group is a free profinite group of countable rank); here $\mathbb{Q}^{\mathrm{tr}}$ denotes the field of totally real numbers (algebraic numbers such that all conjugates are real).

(4) Algebraic extensions of PAC fields are PAC [FJ05, corollary 11.2.5].

We refer to [FJ05] for more on PAC fields.

B.2.2 Ample fields

Recall that a field k is said to be *ample* if every smooth k-curve with a k-rational point has infinitely many distinct k-rational points. Here are some examples of ample fields.

(1) PAC fields are ample.

(2) Complete valued fields (*e.g.* $\mathbb{R}$, $\mathbb{Q}_p$, $\kappa((U))$) are ample.

(3) Given a prime number p, the field $\mathbb{Q}^{\mathrm{t}p}$ is ample; here $\mathbb{Q}^{\mathrm{t}p}$ denotes the field of totally p-adic numbers, *i.e.* the maximal Galois extension of $\mathbb{Q}$ contained in $\mathbb{Q}_p$.

(4) The field $\mathbb{Q}^{\mathrm{tr}}$ of totally real numbers (see §B.2.1) is ample.

(5) Algebraic extensions of ample fields are ample.

We refer to the literature for references and more on ample fields.

B.3 Some classical covers of $\mathbb{P}^1$

Let k be a field and $p \geq 0$ be its characteristic.

B.3.1 Symmetric groups

Let n be an integer ≥ 3. Recall that *the type of a permutation* $\sigma \in S_n$ is the (multiplicative) divisor of all lengths of disjoint cycles involved in the cycle decomposition of σ (for example, an n-cycle is of type n^1). The conjugacy class in S_n of all permutations of type $1^{l_1} \dots n^{l_n}$ is denoted by $[1^{l_1} \dots n^{l_n}]$.

B.3.1.1. Morse polynomials. Recall that a degree n monic polynomial $M(Y) \in k[Y]$ is *a Morse polynomial* if the zeroes $\beta_1, \dots, \beta_{n-1}$ of the derivative $M'(Y)$ are simple and $M(\beta_i) \neq M(\beta_j)$ for $i \neq j$. For example, $M(Y) = Y^n \pm Y$ is a Morse polynomial if $p \not| n-1$.

Given a degree n Morse polynomial $M(Y) \in k[Y]$, denote the splitting field over $k(T)$ of $P(T,Y) = M(Y) - T$ by E. Then $E/k(T)$ is a G-extension of group S_n if $p \not| n$. Its branch points are ∞, $M(\beta_1), \dots, M(\beta_{n-1})$, with corresponding inertia groups generated by an element of type n^1 at ∞ and $1^{n-2}2^1$ at $M(\beta_1), \dots, M(\beta_{n-1})$. See [Ser92, §4.4].

B.3.1.2. Trinomials. Let m, r and s be three positive integers such that $1 \leq m \leq n$, $(m,n) = 1$ and $s(n-m) - rn = 1$. Denote the splitting field over $k(T)$ of the trinomial $Y^n - T^r Y^m + T^s$ by E_k. Then $E_k/k(T)$ is a G-extension of group S_n if $p \not| nm(n-m)$. Its branch points are ∞, 0 and $m^m n^{-n}(n-m)^{n-m}$, with corresponding inertia groups generated by an element of type n^1 at ∞, $m^1(n-m)^1$ at 0 and $1^{n-2}2^1$ at $m^m n^{-n}(n-m)^{n-m}$. See [Sch00, §2.4].

B.3.2 Alternating groups

Recall first that, if the conjugacy class $[1^{l_1} \dots n^{l_n}]$ is contained in A_n, then $[1^{l_1} \dots n^{l_n}]$ is a conjugacy class of A_n if and only if there exists some index $q \in \{1, \dots, n\}$ such that $l_q \geq 2$ or $l_{2q} \geq 1$. Otherwise $[1^{l_1} \dots n^{l_n}]$ splits into two distinct conjugacy classes of A_n, denoted by $[1^{l_1} \dots n^{l_n}]_1$ and $[1^{l_1} \dots n^{l_n}]_2$.

Assume that $p = 0$ and $n \geq 4$. Applying the "double group trick" [Ser92, lemma 4.5.1] to the trinomial realization $E_{\mathbb{Q}}/\mathbb{Q}(T)$ of S_n (§B.3.1.2) provides a G-extension $E'_{\mathbb{Q}}/\mathbb{Q}(T)$ (and then a G-extension $E'_k/k(T)$ by scalar extension from $\mathbb{Q}$ to k) of group A_n, with three branch points and, from the *branch cycle lemma* [Fri77] [Völ96, lemma 2.8], with inertia canonical invariant
- $([m^1(n-m)^1]_1, [m^1(n-m)^1]_2, [(n/2)^2])$ if n is even,
- $([n^1]_1, [n^1]_2, [m^1((n-m)/2)^2])$ if n and m are odd,
- $([n^1]_1, [n^1]_2, [(m/2)^2(n-m)^1])$ if n is odd and m is even.

Note that the branch cycle lemma shows that the branch point corresponding to the following conjugacy class (in each case) is $\mathbb{Q}$-rational:
- $[(n/2)^2]$ if n is even,
- $[m^1((n-m)/2)^2]$ if n and m are odd,
- $[(m/2)^2(n-m)^1]$ if n is odd and m is even.

B.3.3 The Monster group

Assume that $p = 0$ and use below the Atlas [C$^+$85] notation for conjugacy classes of finite groups. Given three distinct points $t_1, t_2, t_3 \in \mathbb{P}^1(\mathbb{Q})$, the *rigidity method* has produced a (unique) G-extension $E_{\mathbb{Q}}/\mathbb{Q}(T)$ (and then a G-extension $E_k/k(T)$) of group the Monster group M, with branch point set $\{t_1, t_2, t_3\}$ and inertia canonical invariant $(2A, 3B, 29A)$ [Ser92, proposition 7.4.8 and theorem 8.2.1].

Part I

Chapter 1

Specializations with specified local behavior

1.1 Introduction

Given a number field k, the *Inverse Galois Problem over* k ((IGP$/k$)) asks whether, for a given finite group G, there exists at least one Galois extension F/k of group G. Refined versions of the (IGP$/k$) impose some further conditions on the local behavior at finitely many primes of k. For example, we may require no prime of a given finite set $\mathcal{S}$ to ramify in F/k. From a theorem of Shafarevich, this is always possible if $k = \mathbb{Q}$ and G is solvable [KM04, theorem 6.1]. Moreover, if G has odd order, one can add the *Grunwald* conclusion: the completion $F_p/\mathbb{Q}_p$ of $F/\mathbb{Q}$ at each prime $p \in \mathcal{S}$ can be prescribed [Neu79] [NSW08, (9.5.5)]. Here we are interested in ramification prescriptions at finitely many given primes of k.

A classical method to obtain Galois extensions of k of group G is by specializing G-extensions of $k(T)$ with the same group (*Hilbert's irreducibility theorem*); many finite groups are known to occur as the Galois group of such an extension. Let $E/k(T)$ be a G-extension of group G and $\{t_1, \dots, t_r\}$ be its branch point set. Our question is whether, for some suitable points $t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \dots, t_r\}$, in addition to $\mathrm{Gal}(E_{t_0}/k) = G$, one can prescribe the inertia groups of the specialization E_{t_0}/k of $E/k(T)$ at t_0 at finitely many given primes.

Given a prime $\mathcal{P}$ of k, not in the finite list of *bad primes for* $E/k(T)$ (definition 1.2.5), and a point $t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \dots, t_r\}$, a classical necessary condition for $\mathcal{P}$ to ramify in E_{t_0}/k is that t_0 *meets some branch point* $t_{i_\mathcal{P}}$ *modulo* $\mathcal{P}$ (definition 1.2.1). A consequence is that $\mathcal{P}$ should admit a prime divisor of residue degree 1 in the extension $k(t_{i_\mathcal{P}})/k$ (say for short that "$t_{i_\mathcal{P}}$ is rationalized by $\mathcal{P}$"). Moreover the inertia group of E_{t_0}/k at $\mathcal{P}$ is known to be generated by some power $g_{i_\mathcal{P}}^{a_\mathcal{P}}$ (depending on t_0 and $t_{i_\mathcal{P}}$) of the distinguished generator $g_{i_\mathcal{P}}$ of some inertia group of the extension $E\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ at $t_{i_\mathcal{P}}$. We refer to §1.2.1 for a precise statement (the "Specialization Inertia Theorem") and more details.

Our main result in §1.3.1 provides some converse to the latter conclusion: for all primes $\mathcal{P}$ but in a certain finite list $\mathcal{S}_{\mathrm{exc}}$, if $\mathcal{P}$ rationalizes $t_{i_\mathcal{P}}$, in particular if $t_{i_\mathcal{P}}$ is itself k-rational, then it is possible to prescribe the above exponent $a_\mathcal{P}$ for some suitable points $t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \dots, t_r\}$. Denote the inertia canonical invariant of $E/k(T)$ by $(C_1, \dots, C_r)$.

Theorem 1. (corollary 1.3.3) *Let $\mathcal{S}$ be a finite set of primes $\mathcal{P}$ of k not in the finite list $\mathcal{S}_{\mathrm{exc}}$, each given with a couple $(i_\mathcal{P}, a_\mathcal{P})$ where*
- $i_\mathcal{P}$ is an index in $\{1, \dots, r\}$ such that $t_{i_\mathcal{P}}$ is rationalized by $\mathcal{P}$,

- $a_{\mathcal{P}}$ is a positive integer.
Then there exist infinitely many distinct points $t_0 \in \mathbb{P}^1(k)\setminus\{t_1, \dots, t_r\}$ such that the specialization E_{t_0}/k of $E/k(T)$ at t_0 satisfies the following two conditions:
(1) $\mathrm{Gal}(E_{t_0}/k) = G$,
(2) *for each prime $\mathcal{P} \in \mathcal{S}$, the inertia group of E_{t_0}/k at $\mathcal{P}$ is generated by some element of $C_{i_{\mathcal{P}}}^{a_{\mathcal{P}}}$.*

Our condition $\mathcal{P} \notin \mathcal{S}_{\mathrm{exc}}$ on the primes is that $\mathcal{P}$ should be *a good prime for $E/k(T)$* such that $t_{i_{\mathcal{P}}}$ and $1/t_{i_{\mathcal{P}}}$ are integral over the localization $A_{\mathcal{P}}$ of the integral closure A of $\mathbb{Z}$ in k at $\mathcal{P}$.

Part (2) of the conclusion is proved in a more general situation with the number field k replaced by the quotient field of any Dedekind domain A of characteristic zero and holds for all (but finitely many) points t_0 in an arithmetic progression (theorem 1.3.1). Furthermore part (1) is satisfied if k is a hilbertian field or if the inertia canonical invariant of $E/k(T)$ satisfies some *g-complete* hypothesis. We refer to §1.3.1.2 for more details and extra conclusions on the set of points t_0 at which conditions (1) and (2) above simultaneously hold.

Related conclusions can be found in an earlier paper of Plans and Vila [PV05], for specific G-extensions of $\mathbb{Q}(T)$ generally derived from the rigidity method. Here theorem 1 applies to any G-extension of $\mathbb{Q}(T)$ and the inertia groups may be specified. However a finite list of primes is excluded from our conclusions; in particular, any wild ramification situation is left aside.

Many finite groups are known to occur as the Galois group of a G-extension of $\mathbb{Q}(T)$ (fix $k = \mathbb{Q}$ for simplicity) with at least one $\mathbb{Q}$-rational branch point (for example, the Monster group does), in which case theorem 1 then produces Galois extensions of $\mathbb{Q}$ with the same group which ramify at any finitely many given large enough primes. Some examples are given in §1.3.2.

Note however that the assumption on the branch points cannot be removed. Indeed, given an odd prime p, Galois extensions of $\mathbb{Q}$ of group $\mathbb{Z}/p\mathbb{Z}$ are known to ramify only at p or at primes q such that $q \equiv 1 \bmod p$ [Tra90, theorem 1]. And it is known from [DF90, corollary 1.3] that there are no G-extension of $\mathbb{Q}(T)$ of group $\mathbb{Z}/p\mathbb{Z}$ with at least one $\mathbb{Q}$-rational branch point.

On the other hand, theorem 1 also includes trivial ramification at $\mathcal{P}$, by taking $a_{\mathcal{P}}$ equal to (a multiple of) the order of the elements of $C_{i_{\mathcal{P}}}$. In this unramified context, similar more precise conclusions are given in the two papers [DG12] and [DG11] of Dèbes and Ghazi: they have some additional control on the decomposition groups. As shown in §1.4, it is in fact possible to conjoin their statement and theorem 1 to obtain, for any finite group G which occurs as the Galois group of a G-extension of $\mathbb{Q}(T)$, *a general existence result of Galois extensions of $\mathbb{Q}$ of group G with specified local behavior (ramified or unramified).* Theorem 1.4.1 gives the precise statement.

1.2 First statements on the ramification in specializations

Given a field k, we review and complement in §1.2.1 some general facts on the ramification in the specializations of any G-extension of $k(T)$. §1.2.2 is devoted to a preliminary ramification criterion at one prime.

1.2.1 Conditions on the ramification in specializations

The aim of this subsection is the "Specialization Inertia Theorem" of §1.2.1.3 which is a slightly more general form of a result of Beckmann [Bec91, proposition 4.2]. We before review and complement some background in §1.2.1.1-1.2.1.2.

Let A be a Dedekind domain of characteristic zero, k be its quotient field and $\mathcal{P}$ be a (non-zero) prime ideal of A. Denote the valuation of k corresponding to $\mathcal{P}$ by $v_{\mathcal{P}}$.

1.2.1.1. Meeting. Throughout this subsection, we will identify $\mathbb{P}^1(k)$ and $k \cup \{\infty\}$ and set

- $1/\infty = 0$,
- $1/0 = \infty$,
- $v_{\mathcal{P}}(\infty) = -\infty$,
- $v_{\mathcal{P}}(0) = \infty$.

Recall now the following definition:

Definition 1.2.1. (1) Let F/k be a finite extension, A_F be the integral closure of A in F, $\mathcal{P}_F$ be a non-zero prime ideal of A_F and $t_0, t_1 \in \mathbb{P}^1(F)$. We say that t_0 *and* t_1 *meet modulo* $\mathcal{P}_F$ if either one of the following two conditions holds:

(a) $v_{\mathcal{P}_F}(t_0) \geq 0$, $v_{\mathcal{P}_F}(t_1) \geq 0$ and $v_{\mathcal{P}_F}(t_0 - t_1) > 0$,

(b) $v_{\mathcal{P}_F}(t_0) \leq 0$, $v_{\mathcal{P}_F}(t_1) \leq 0$ and $v_{\mathcal{P}_F}((1/t_0) - (1/t_1)) > 0$.

(2) Given $t_0, t_1 \in \mathbb{P}^1(\overline{k})$, we say that t_0 *and* t_1 *meet modulo* $\mathcal{P}$ if there exists some finite extension F/k satisfying the following two conditions:

(a) $t_0, t_1 \in \mathbb{P}^1(F)$,

(b) t_0 and t_1 meet modulo some prime ideal of F lying over $\mathcal{P}$.

It is easily checked that $v_{\mathcal{P}_F}(t_0 - t_1) = v_{\mathcal{P}_F}((1/t_0) - (1/t_1))$ in the case $v_{\mathcal{P}_F}(t_0) = v_{\mathcal{P}_F}(t_1) = 0$, thus making the notion of "meeting" well-defined.

Moreover this notion (and some other ones below too) could be defined by using a projective viewpoint, and a little bit more of generality might then be gained in §1.2.1.1-1.2.1.3. We still retain the affine viewpoint which will be more practical for the rest of this chapter.

Remark 1.2.2. (1) Part (2) of definition 1.2.1 does not depend on the choice of a finite extension F/k such that $t_0, t_1 \in \mathbb{P}^1(F)$.

(2) If $t_0 \in \mathbb{P}^1(k)$ and t_0 meets t_1 modulo $\mathcal{P}$, then t_0 meets each k-conjugate of t_1 modulo $\mathcal{P}$.

Throughout this chapter, the irreducible polynomial over k of any point $t_1 \in \mathbb{P}^1(\overline{k})$ will be denoted by $m_{t_1}(T)$ (set $m_{t_1}(T) = 1$ if $t_1 = \infty$). Denote its constant coefficient by a_{t_1}. Then the irreducible polynomial of $1/t_1$ over k is

- $m_{1/t_1}(T) = (1/a_{t_1})\, T^{\deg(m_{t_1}(T))}\, m_{t_1}(1/T)$ if $t_1 \in \overline{k} \setminus \{0\}$,
- $m_{1/t_1}(T) = 1$ if $t_1 = 0$,
- $m_{1/t_1}(T) = T$ if $t_1 = \infty$.

Fix $t_1 \in \mathbb{P}^1(\overline{k})$. Throughout §1.2.1.1, we will assume that $v_{\mathcal{P}}(a_{t_1}) = 0$ if $t_1 \neq 0$ to make the intersection multiplicity well-defined in definition 1.2.3 below. Let $t_0 \in \mathbb{P}^1(k)$.

Definition 1.2.3. *The intersection multiplicity* $I_{\mathcal{P}}(t_0, t_1)$ *of* t_0 *and* t_1 *at* $\mathcal{P}$ is

$$I_{\mathcal{P}}(t_0, t_1) = \begin{cases} v_{\mathcal{P}}(m_{t_1}(t_0)) & \text{if} \quad v_{\mathcal{P}}(t_0) \geq 0, \\ v_{\mathcal{P}}(m_{1/t_1}(1/t_0)) & \text{if} \quad v_{\mathcal{P}}(t_0) \leq 0. \end{cases}$$

In the case $m_{t_1}(T)$ has coefficients in the localization $A_{\mathcal{P}}$ of A at $\mathcal{P}$ (and so $m_{1/t_1}(T)$ too due to our assumption), our intersection multiplicity coincides with that of Beckmann.

Lemma 1.2.4 below will be used in several occasions in this chapter:

Lemma 1.2.4. (1) *If* $I_{\mathcal{P}}(t_0, t_1) > 0$, *then* t_0 *and* t_1 *meet modulo* $\mathcal{P}$.

(2) *The converse is true if* $m_{t_1}(T) \in A_{\mathcal{P}}[T]$.

Proof. First of all, we note the following simple statement which will be used in several occasions in this chapter:

($*$) *Let* $m(T) \in A_{\mathcal{P}}[T]$ *be a non constant monic polynomial,* L/k *be any extension,* $\mathcal{Q}$ *be a prime ideal of* L *above* $\mathcal{P}$ *and* $t \in L$ *such that* $v_{\mathcal{Q}}(m(t)) \geq 0$ *(in particular if* t *is a root of* $m(T)$*). Then* $v_{\mathcal{Q}}(t) \geq 0$.

Indeed assume that $v_{\mathcal{Q}}(t) < 0$. Set $m(T) = a_0 + a_1 T + \cdots + a_{n-1} T^{n-1} + T^n$. Since $m(T) \in A_{\mathcal{P}}[T]$, one then has $v_{\mathcal{Q}}(a_j t^j) > v_{\mathcal{Q}}(t^n)$ for each index $j \in \{0, \dots, n-1\}$. Hence $v_{\mathcal{Q}}(m(t)) = v_{\mathcal{Q}}(t^n) < 0$; a contradiction.

To prove lemma 1.2.4, set $m_{t_1}(T) = \prod_{i=1}^n (T - t_i)$ (if $t_1 \neq \infty$) and fix a prime ideal $\mathcal{Q}$ of $k(t_1, \dots, t_n)$ above $\mathcal{P}$. We successively prove conclusions (1) and (2).

(1) Assume first that $v_{\mathcal{P}}(t_0) \geq 0$. Then $v_{\mathcal{P}}(m_{t_1}(t_0)) > 0$ from our assumption $I_{\mathcal{P}}(t_0, t_1) > 0$ and $t_1 \neq \infty$ (otherwise $1 = m_{t_1}(t_0) \in \mathcal{P}A_{\mathcal{P}}$). Hence one has $\sum_{i=1}^n v_{\mathcal{Q}}(t_0 - t_i) > 0$. Consequently there is an index $i_0 \in \{1, \dots, n\}$ such that $v_{\mathcal{Q}}(t_0 - t_{i_0}) > 0$. Since $v_{\mathcal{Q}}(t_0) \geq 0$, one then has $v_{\mathcal{Q}}(t_{i_0}) \geq 0$. Hence t_0 and t_{i_0} meet modulo $\mathcal{P}$. The conclusion then follows from part (2) of remark 1.2.2.

Assume now that $v_{\mathcal{P}}(t_0) \leq 0$. Then $v_{\mathcal{P}}(m_{1/t_1}(1/t_0)) > 0$ and $t_1 \neq 0$ (otherwise $1 = m_{1/t_1}(1/t_0) \in \mathcal{P}A_{\mathcal{P}}$). If $t_1 = \infty$, then t_0 and t_1 meet modulo $\mathcal{P}$. If $t_1 \neq \infty$, one has $m_{1/t_1}(T) = \prod_{i=1}^n (T - (1/t_i))$. Hence $\sum_{i=1}^n v_{\mathcal{Q}}((1/t_0) - (1/t_i)) > 0$. Consequently there exists some index $i_0 \in \{1, \dots, n\}$ such that $v_{\mathcal{Q}}((1/t_0) - (1/t_{i_0})) > 0$. As before, t_0 and t_{i_0} meet modulo $\mathcal{P}$ and one concludes from part (2) of remark 1.2.2.

(2) Assume now that t_0 and t_1 meet modulo $\mathcal{P}$ and $m_{t_1}(T) \in A_{\mathcal{P}}[T]$. It is easily checked that $I_{\mathcal{P}}(t_0, t_1) > 0$ if $t_1 \in \{0, \infty\}$, so assume that $t_1 \notin \{0, \infty\}$.

Consider first the case $v_{\mathcal{Q}}(t_0) \geq 0$, $v_{\mathcal{Q}}(t_1) \geq 0$ and $v_{\mathcal{Q}}(t_0 - t_1) > 0$. Given an index $i \in \{1, \dots, n\}$, it follows from statement $(*)$ (applied to the polynomial $m_{t_1}(T)$) that one has $v_{\mathcal{Q}}(t_i) \geq 0$, and then $v_{\mathcal{Q}}(t_0 - t_i) \geq 0$. Hence $v_{\mathcal{Q}}(m_{t_1}(t_0)) \geq v_{\mathcal{Q}}(t_0 - t_1) > 0$, *i.e.* $I_{\mathcal{P}}(t_0, t_1) > 0$.

Consider now the case $v_{\mathcal{Q}}(t_0) \leq 0$, $v_{\mathcal{Q}}(t_1) \leq 0$ and $v_{\mathcal{Q}}((1/t_0) - (1/t_1)) > 0$. Given an index $i \in \{1, \dots, n\}$, statement $(*)$ (applied this time to the polynomial $m_{1/t_1}(T)$) shows that one has $v_{\mathcal{Q}}(1/t_i) \geq 0$, and then $v_{\mathcal{Q}}((1/t_0) - (1/t_i)) \geq 0$. Hence $v_{\mathcal{Q}}(m_{1/t_1}(1/t_0)) \geq v_{\mathcal{Q}}((1/t_0) - (1/t_1)) > 0$, *i.e.* $I_{\mathcal{P}}(t_0, t_1) > 0$. □

1.2.1.2. Good primes. Continue with the same notation as before. Let G be a finite group and $E/k(T)$ be a G-extension of group G. Denote its branch point set by $\{t_1, \dots, t_r\}$.

Definition 1.2.5. We say that $\mathcal{P}$ is *a bad prime for $E/k(T)$* if at least one of the following four conditions holds:

(1) $|G| \in \mathcal{P}$,

(2) two different branch points meet modulo $\mathcal{P}$,

(3) *$E/k(T)$ has vertical ramification at $\mathcal{P}$*, *i.e.* the prime ideal $\mathcal{P}A[T]$ of $A[T]$ ramifies in the integral closure of $A[T]$ in E [1],

(4) $\mathcal{P}$ ramifies in $k(t_1, \dots, t_r)/k$.

Otherwise $\mathcal{P}$ is called *a good prime for $E/k(T)$*.

Remark 1.2.6. (1) There exist only finitely many distinct bad primes for $E/k(T)$.

(2) Condition (4) above does not appear in [Bec91], but seems to be missing for the proof of proposition 4.2 of this paper to work. Indeed, although it is stated at the beginning of the proof there, it seems unclear that any prime ramifying in $k(t_1, \dots, t_r)/k$ should be a bad prime for $E/k(T)$. This extra condition (4) will be used in the proof of the Specialization Inertia Theorem.

In fact, if $\mathcal{P}$ satisfies condition (4) and the following extra condition:

(4') *t_i or $1/t_i$ is integral over $A_{\mathcal{P}}$ (i.e. $m_{t_i}(T) \in A_{\mathcal{P}}[T]$ or $m_{1/t_i}(T) \in A_{\mathcal{P}}[T]$) for each non k-rational branch point t_i,*

then $\mathcal{P}$ satisfies condition (2) of definition 1.2.5 [2].

1. According to [Bec91, proposition 2.3], this condition may be removed if G has trivial center.
2. and then is a bad prime in the sense of Beckmann.

Indeed, if $\mathcal{P}$ ramifies in $k(t_1,\dots,t_r)/k$, then $\mathcal{P}$ does in some $k(t_i)/k$ and so t_i is not k-rational. So assume from the extra condition (4') that t_i is integral over $A_{\mathcal{P}}$ (the other case for which it is $1/t_i$ which is integral over $A_{\mathcal{P}}$ is quite similar). Hence $\mathcal{P}A_{\mathcal{P}}$ contains the discriminant of the integral k-basis $\{1, t_i, \dots, t_i^{[k(t_i):k]-1}\}$ of $k(t_i)$, *i.e.* the discriminant of $m_{t_i}(T)$.

This sole condition shows that condition (2) of definition 1.2.5 holds. Indeed note first that $t_i \notin \mathbb{P}^1(k)$ (otherwise $1 \in \mathcal{P}A_{\mathcal{P}}$). Let $\mathcal{Q}$ be a prime ideal of the splitting field over k of $m_{t_i}(T) = \prod_j (T - t_j)$ above $\mathcal{P}$. As $\prod_{j \neq j'} (t_j - t_{j'}) \in \mathcal{P}A_{\mathcal{P}}$, there are two indices $j \neq j'$ such that $v_{\mathcal{Q}}(t_j - t_{j'}) > 0$. If $v_{\mathcal{Q}}(t_j) \geq 0$, then $v_{\mathcal{Q}}(t_{j'}) \geq 0$ and t_j and $t_{j'}$ meet modulo $\mathcal{P}$. If $v_{\mathcal{Q}}(t_j) < 0$, then $v_{\mathcal{Q}}(t_{j'}) < 0$ and $v_{\mathcal{Q}}((1/t_j) - (1/t_{j'})) = v_{\mathcal{Q}}(t_j - t_{j'}) - v_{\mathcal{Q}}(t_j) - v_{\mathcal{Q}}(t_{j'}) > 0$. Hence t_j and $t_{j'}$ meet modulo $\mathcal{P}$.

In particular, we obtain lemma 1.2.7 below which will be used in several occasions:

Lemma 1.2.7. *Let $i \in \{1,\dots,r\}$ and $t_0 \in A_{\mathcal{P}}$. Assume that $m_{t_i}(T) \in A_{\mathcal{P}}[T]$, $v_{\mathcal{P}}(m_{t_i}(t_0)) > 0$ and $v_{\mathcal{P}}(m'_{t_i}(t_0)) > 0$. Then $\mathcal{P}$ is a bad prime for $E/k(T)$.*

1.2.1.3. Ramification in the specializations of $E/k(T)$. Continue with the same notation as before. For each index $i \in \{1,\dots,r\}$, let g_i be the distinguished generator of some inertia group of $E\overline{k}/\overline{k}(T)$ at t_i.

Specialization Inertia Theorem. *Let $t_0 \in \mathbb{P}^1(k) \setminus \{t_1,\dots,t_r\}$.*
(1) If $\mathcal{P}$ ramifies in E_{t_0}/k, then $E/k(T)$ has vertical ramification at $\mathcal{P}$ or t_0 meets some branch point modulo $\mathcal{P}$.
(2) Fix an index $j \in \{1,\dots,r\}$ such that t_0 and t_j meet modulo $\mathcal{P}$. Assume that the following two conditions hold:
(a) $\mathcal{P}$ is a good prime for $E/k(T)$,
(b) t_j and $1/t_j$ are integral over $A_{\mathcal{P}}$.
Then the inertia group of E_{t_0}/k at $\mathcal{P}$ is (conjugate in G to) $\langle g_j^{I_{\mathcal{P}}(t_0,t_j)} \rangle$.

In the case $t_j \notin \{0,\infty\}$, condition (b) in part (2) above is equivalent to t_j being a unit in $\overline{k}$ with respect to any prolongation of $v_{\mathcal{P}}$ to $\overline{k}$ (statement $(*)$). It will be used in several occasions in this chapter; we will say for short that "$\mathcal{P}$ unitizes t_j".

1.2.1.4. Proof of the Specialization Inertia Theorem. As already alluded to at the beginning of §1.2.1, this statement is a version of [Bec91, proposition 4.2] with less restrictive hypotheses. Part (1) may be obtained as a consequence of the algebraic cover theory of Grothendieck while part (2) follows from the original proof of [Bec91, proposition 4.2] and some previous work of Flon [Flo02, theorem 1.3.3] (and the necessary adjustment alluded to in part (2) of remark 1.2.6). We offer below a unified proof[3].

(a) *Proof of part (1).* Let $f : X \to \mathbb{P}^1$ be the k-G-cover of group G corresponding to the G-extension $E/k(T)$. Denote the normalization of $\mathbb{P}^1_A$ in $k(X) = E$ by $f_A : \mathcal{X} \to \mathbb{P}^1_A$, the Zariski closure of the branch locus $\{t_1,\dots,t_r\}$ of f in $\mathbb{P}^1_A$ by $\overline{\{t_1,\dots,t_r\}}$ and, for each prime ideal $\mathcal{P}$ of A at which $E/k(T)$ has vertical ramification, the fiber at $\mathcal{P}$ by $X_{\mathcal{P}}$. Set $\mathcal{D} = \overline{\{t_1,\dots,t_r\}} \bigcup (\cup_{\mathcal{P}} X_{\mathcal{P}})$.

This morphism is unramified above $\mathbb{P}^1_A \setminus \mathcal{D}$. Moreover lemma 1.2.8 below shows that f_A is flat, hence étale above $\mathbb{P}^1_A \setminus \mathcal{D}$. As a consequence, we obtain that $f_A|_{t_0}$ is étale (in particular unramified) above $\overline{\{t_0\}} \bigcap (\mathbb{P}^1_A \setminus \mathcal{D})$ (with $\overline{\{t_0\}}$ the Zariski closure of $\{t_0\}$ in $\mathbb{P}^1_A$), thus ending the proof of part (1).

Lemma 1.2.8. *Let $f : A \to B$ be a finite monomorphism with A and B two domains such that A is regular, $\dim(A) = 2$ and B is normal. Then B is a flat A-module.*

3. I would like to thank Michel Emsalem and Lorenzo Ramero for their help on this proof.

Proof. Note first that one may assume that A is a local ring; denote next its maximal ideal by m_A. As A is regular, the homological dimension $\mathrm{hom.dim}_A(B)$ of the A-module B is finite (this follows from a theorem of Serre; see *e.g.* [Ram13, theorem 12.21]). Then the Auslander-Buchsbaum equality (*e.g.* [Wei94, theorem 4.4.15]) provides

$$\mathrm{hom.dim}_A(B) + \mathrm{depth}(B) = \mathrm{depth}(A) = \dim(A) = 2$$

with $\mathrm{depth}(B)$ the depth of the A-module B (see *e.g.* [Mat86, §16]).

We next claim that $\mathrm{depth}(B)$ is the lower bound of the numbers $\mathrm{depth}(B_{\mathcal{P}'})$ with $\mathcal{P}'$ ranging over all prime ideals $\mathcal{P}'$ of B such that $f^{-1}(\mathcal{P}') = m_A$. Indeed denote these (finitely many distinct) primes by $\mathcal{P}_1, \dots, \mathcal{P}_s$. Given an integer i, one has $\mathrm{Ext}^i_A(A/m_A, B) = 0$ if and only if $\mathrm{Ext}^i_A(A/m_A, B)_{\mathcal{P}_j} = 0$ for each index $j \in \{1, \dots, s\}$, *i.e.* if and only if $\mathrm{Ext}^i_A(A/m_A, B_{\mathcal{P}_j}) = 0$ for each index $j \in \{1, \dots, s\}$. Hence $\mathrm{depth}(B)$ is the lower bound of the numbers $\mathrm{depth}_{m_A}(B_{\mathcal{P}_j})$ ($j = 1, \dots, s$). Conjoining this and the fact that $\mathrm{depth}_{m_A}(B_{\mathcal{P}_j}) = \mathrm{depth}(B_{\mathcal{P}_j})$ for each index $j \in \{1, \dots, s\}$ (see *e.g.* [Mat86, exercise 16.7 and page 293]) provides our claim.

Now, as f is a finite monomorphism and $\dim(A) = 2$, one has $\dim(B) = 2$ too. Conjoining this and the assumption that B is normal shows that $\mathrm{depth}(B_{\mathcal{P}'}) = 2$ for any maximal ideal $\mathcal{P}'$ of B (this follows from the Serre normality criterion; see *e.g.* [Mat86, theorem 23.8]), *i.e.* for any prime ideal $\mathcal{P}'$ of B such that $f^{-1}(\mathcal{P}') = m_A$. Hence $\mathrm{depth}(B) = 2$ and $\mathrm{hom.dim}_A(B) = 0$, thus ending the proof of lemma 1.2.8. □

(b) *Proof of part (2).* Let $L = k(t_1, \dots, t_r)$ and B be the integral closure of A in L. As t_0 and t_j meet modulo $\mathcal{P}$, there exists some prime ideal $\mathcal{Q}$ of B above $\mathcal{P}$ such that t_0 and t_j meet modulo $\mathcal{Q}$. As $\mathcal{P}$ is a good prime for $E/k(T)$, the prime $\mathcal{Q}$ is a good prime for $EL/L(T)$. Indeed it is then obvious that none of conditions (1), (2) and (4) of definition 1.2.5 holds. And condition (3) does not hold either [Bec91, lemma 2.1(a)]. Moreover t_j and $1/t_j$ are integral over the localization $B_{\mathcal{Q}}$ of B at $\mathcal{Q}$ (part (b) of condition (2) and statement $(*)$). As each branch point of $EL/L(T)$ obviously is L-rational, one may conclude from [Flo02, theorem 1.3.3] [Bec91, §3] that the inertia group of $(EL)_{t_0}/L$ at $\mathcal{Q}$ is (conjugate in G to) $\langle g_j^{I_{\mathcal{Q}}(t_0,t_j)} \rangle$.

As $\mathcal{P}$ does not ramify in L/k (condition (4) of definition 1.2.5), one may next apply [Bec91, lemma 3.2] to conclude that the inertia group of E_{t_0}/k at $\mathcal{P}$ is $\langle g_j^{I_{\mathcal{Q}}(t_0,t_j)} \rangle$. It suffices then to show that $I_{\mathcal{P}}(t_0, t_j) = I_{\mathcal{Q}}(t_0, t_j)$. Assume for example that $v_{\mathcal{P}}(t_0) \geq 0$ (the other case for which $v_{\mathcal{P}}(t_0) \leq 0$ is quite similar) and then $v_{\mathcal{Q}}(t_0 - t_j) > 0$ (as t_0 and t_j meet modulo $\mathcal{Q}$). Then $I_{\mathcal{P}}(t_0, t_j) = v_{\mathcal{P}}(m_{t_j}(t_0)) = v_{\mathcal{Q}}(m_{t_j}(t_0))$ (as $\mathcal{P}$ does not ramify in L/k). Given a k-conjugate $t_{j'}$ of t_j distinct from t_j, one has $v_{\mathcal{Q}}(t_0 - t_{j'}) = 0$. Indeed note first that $v_{\mathcal{Q}}(t_{j'}) = 0$ (part (b) of condition (2) and statement $(*)$). Hence $v_{\mathcal{Q}}(t_0 - t_{j'}) \geq 0$. If $v_{\mathcal{Q}}(t_0 - t_{j'}) > 0$, one has $v_{\mathcal{Q}}(t_j - t_{j'}) > 0$ and then the two distinct branch points t_j and $t_{j'}$ meet modulo $\mathcal{Q}$; a contradiction. Hence $v_{\mathcal{Q}}(m_{t_j}(t_0)) = v_{\mathcal{Q}}(t_0 - t_j) = I_{\mathcal{Q}}(t_0, t_j)$, thus ending the proof of part (2).

1.2.2 Ramification criterion at one prime

Our next goal (achieved with theorem 1.3.1) is to show that, for some good choice of the specialization point $t_0 \in \mathbb{P}^1(k)$, ramification can be prescribed at finitely many primes in the specialization E_{t_0}/k of $E/k(T)$ at t_0 within the Specialization Inertia Theorem limitations. We start by the special but useful case there is a single prime and the requirement on it is that it does ramify (corollary 1.2.12).

Continue with the same notation as before. Let $x_{\mathcal{P}}$ be a generator of the maximal ideal $\mathcal{P}A_{\mathcal{P}}$ of $A_{\mathcal{P}}$. Assume in proposition 1.2.9 below that $\mathcal{P}$ is a good prime for $E/k(T)$ unitizing each branch point.

Proposition 1.2.9. *Let $t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \dots, t_r\}$ such that $v_{\mathcal{P}}(t_0) \geq 0$ (resp. $v_{\mathcal{P}}(t_0) \leq 0$) and neither t_0 nor $t_0 + x_{\mathcal{P}}$ is in $\{t_1, \dots, t_r\}$ (resp. neither t_0 nor $t_0/(1 + x_{\mathcal{P}}\, t_0)$ [4] is in $\{t_1, \dots, t_r\}$). Then the following two conditions are equivalent:*

(1) *t_0 meets some branch point modulo $\mathcal{P}$ (in both cases),*

(2) *$\mathcal{P}$ ramifies in E_{t_0}/k or in $E_{t_0+x_{\mathcal{P}}}/k$ (resp. in E_{t_0}/k or in $E_{t_0/(1+x_{\mathcal{P}}\, t_0)}/k$).*

Proof. We may assume that $v_{\mathcal{P}}(t_0) \geq 0$ (the other case for which $v_{\mathcal{P}}(t_0) \leq 0$ is quite similar).

Assume first that condition (2) holds. From part (1) of the Specialization Inertia Theorem, one may assume that $\mathcal{P}$ ramifies in $E_{t_0+x_{\mathcal{P}}}/k$. Hence $t_0 + x_{\mathcal{P}}$ meets some t_i modulo $\mathcal{P}$. Since $m_{t_i}(T) \in A_{\mathcal{P}}[T]$, the converse in part (1) of lemma 1.2.4 holds and $I_{\mathcal{P}}(t_0 + x_{\mathcal{P}}, t_i) > 0$, *i.e.* $v_{\mathcal{P}}(m_{t_i}(t_0 + x_{\mathcal{P}})) > 0$. From Taylor's formula, there exists some $R_{\mathcal{P}} \in A_{\mathcal{P}}$ such that

$$m_{t_i}(t_0) = m_{t_i}(t_0 + x_{\mathcal{P}}) + x_{\mathcal{P}}\, R_{\mathcal{P}}$$

Hence $v_{\mathcal{P}}(m_{t_i}(t_0)) > 0$, *i.e.* $I_{\mathcal{P}}(t_0, t_i) > 0$. It then remains to apply part (1) of lemma 1.2.4 to finish the proof of implication (2) $\Rightarrow$ (1).

Assume that t_0 and t_i meet modulo $\mathcal{P}$ (and then $I_{\mathcal{P}}(t_0, t_i) > 0$ from the converse in part (1) of lemma 1.2.4). From part (2) of the Specialization Inertia Theorem, $\mathcal{P}$ ramifies in E_{t_0}/k if and only if $I_{\mathcal{P}}(t_0, t_i)$ is not a multiple of the order of the distinguished generator g_i, *i.e.* if and only if $v_{\mathcal{P}}(m_{t_i}(t_0))$ is not either. We may then assume that $v_{\mathcal{P}}(m_{t_i}(t_0)) \geq 2$. Taylor's formula yields

$$m_{t_i}(t_0 + x_{\mathcal{P}}) = m_{t_i}(t_0) + x_{\mathcal{P}}\, m'_{t_i}(t_0) + x_{\mathcal{P}}^2\, R_{\mathcal{P}}$$

with $R_{\mathcal{P}} \in A_{\mathcal{P}}$. Then $v_{\mathcal{P}}(m_{t_i}(t_0 + x_{\mathcal{P}})) = 1$ since one has $v_{\mathcal{P}}(m_{t_i}(t_0)) \geq 2$, $v_{\mathcal{P}}(x_{\mathcal{P}}\, m'_{t_i}(t_0)) = 1$ (lemma 1.2.7) and $v_{\mathcal{P}}(x_{\mathcal{P}}^2\, R_{\mathcal{P}}) \geq 2$. Hence $\mathcal{P}$ ramifies in $E_{t_0+x_{\mathcal{P}}}/k$ and condition (2) holds. □

Recall now the following definition:

Definition 1.2.10. Let $P(T) \in k[T]$ be a non constant polynomial. We say that $\mathcal{P}$ is *a prime divisor of* $P(T)$ if there exists some $t_0 \in k$ such that $v_{\mathcal{P}}(P(t_0)) > 0$.

Remark 1.2.11. Assume that $P(T)$ is in $A_{\mathcal{P}}[T]$ and that $v_{\mathcal{P}}(P(t_0)) > 0$. Fix $a \in \mathcal{P}A_{\mathcal{P}}$. As noted in the second paragraph of the proof of proposition 1.2.9, one has $v_{\mathcal{P}}(P(t_0 + a)) > 0$. Moreover, if $v_{\mathcal{P}}(a) > v_{\mathcal{P}}(P(t_0))$, then $v_{\mathcal{P}}(P(t_0 + a)) = v_{\mathcal{P}}(P(t_0))$.

Set $m_{\underline{\mathbf{t}}}(T) = \prod_{i=1}^{r} m_{t_i}(T)$ and $m_{1/\underline{\mathbf{t}}}(T) = \prod_{i=1}^{r} m_{1/t_i}(T)$. Then corollary 1.2.12 below follows:

Corollary 1.2.12. *Assume that $\mathcal{P}$ is a good prime for $E/k(T)$ unitizing each branch point. Then the following two conditions are equivalent:*

(1) *$\mathcal{P}$ ramifies in some specialization of $E/k(T)$,*

(2) *$\mathcal{P}$ is a prime divisor of $m_{\underline{\mathbf{t}}}(T) \cdot m_{1/\underline{\mathbf{t}}}(T)$.*

Proof. Assume first that there exists some $t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \dots, t_r\}$ such that $\mathcal{P}$ ramifies in E_{t_0}/k. Suppose that $v_{\mathcal{P}}(t_0) \geq 0$ (the other case for which $v_{\mathcal{P}}(t_0) \leq 0$ is quite similar). As noted in the second paragraph of the proof of proposition 1.2.9, one has $v_{\mathcal{P}}(m_{t_i}(t_0)) > 0$ for some index $i \in \{1, \dots, r\}$. But $t_0 \in A_{\mathcal{P}}$ and $m_{t_1}(T), \dots, m_{t_r}(T), m_{1/t_1}(T), \dots, m_{1/t_r}(T) \in A_{\mathcal{P}}[T]$. Hence $v_{\mathcal{P}}(m_{\underline{\mathbf{t}}}(t_0) \cdot m_{1/\underline{\mathbf{t}}}(t_0)) > 0$ and condition (2) holds.

Conversely assume that condition (2) holds. Fix $t_0 \in k$ such that $v_{\mathcal{P}}(m_{\underline{\mathbf{t}}}(t_0) \cdot m_{1/\underline{\mathbf{t}}}(t_0)) > 0$. From statement (*), one has $v_{\mathcal{P}}(t_0) \geq 0$. Assume that $v_{\mathcal{P}}(m_{\underline{\mathbf{t}}}(t_0)) > 0$ (the other case for which $v_{\mathcal{P}}(m_{1/\underline{\mathbf{t}}}(t_0)) > 0$ is quite similar). Then there exists some index $i \in \{1, \dots, r\}$ such that $v_{\mathcal{P}}(m_{t_i}(t_0)) > 0$ (and so condition (1) of proposition 1.2.9 holds from part (1) of lemma 1.2.4). From remark 1.2.11, one may assume that neither t_0 nor $t_0 + x_{\mathcal{P}}$ is in $\{t_1, \dots, t_r\}$. The conclusion then follows from proposition 1.2.9. □

4. Replace $t_0/(1 + x_{\mathcal{P}}\, t_0)$ by $1/x_{\mathcal{P}}$ if $t_0 = \infty$.

1.3 Specializations with specified inertia groups

This section is devoted to theorem 1.3.1 (the most general result of this chapter) which is more general than theorem 1 from the introduction; it is the aim of §1.3.1.1. We then give in §1.3.1.2 two more practical forms of this statement (corollaries 1.3.3 and 1.3.4). We next apply these results to some classical G-extensions of $\mathbb{Q}(T)$ in §1.3.2.

1.3.1 Specializations with specified inertia groups

Let A be a Dedekind domain of characteristic zero, k be its quotient field, G be a finite group, $E/k(T)$ be a G-extension of group G, $\{t_1, \dots, t_r\}$ be its branch point set and $(C_1, \dots, C_r)$ be its inertia canonical invariant.

1.3.1.1. General result. Let s be a positive integer, $\mathcal{P}_1, \dots, \mathcal{P}_s$ be s distinct good primes for $E/k(T)$ and $(i_1, a_1), \dots, (i_s, a_s)$ be s couples where, for each index $j \in \{1, \dots, s\}$,
(1) i_j is an index in $\{1, \dots, r\}$ such that $\mathcal{P}_j$ is a prime divisor of the polynomial $m_{t_{i_j}}(T) \cdot m_{1/t_{i_j}}(T)$ and unitizes t_{i_j},
(2) a_j is a positive integer.

Theorem 1.3.1. *There exist infinitely many distinct points $t_0 \in k \setminus \{t_1, \dots, t_r\}$ such that, for each index $j \in \{1, \dots, s\}$, the inertia group at $\mathcal{P}_j$ of the specialization E_{t_0}/k of $E/k(T)$ at t_0 is generated by some element of $C_{i_j}^{a_j}$.*

Addendum 1.3.1. For each index $j \in \{1, \dots, s\}$, let $x_{\mathcal{P}_j} \in A$ be a generator of $\mathcal{P}_j A_{\mathcal{P}_j}$. Denote the set of all $j \in \{1, \dots, s\}$ such that $t_{i_j} \neq \infty$ by S.

There exists some $\theta \in k$ such that the conclusion of theorem 1.3.1 holds at any point $t_{0,u} \in k \setminus \{t_1, \dots, t_r\}$ of the form $t_{0,u} = \theta + u \prod_{l \in S} x_{\mathcal{P}_l}^{a_l+1}$ with u any element of k such that $v_{\mathcal{P}_l}(u) \geq 0$ for each index $l \in \{1, \dots, s\}$. Furthermore, if $S = \{1, \dots, s\}$ (in particular if ∞ is not a branch point), then such an element θ may be chosen in A.

Remark 1.3.2. For some j, there may be no index i such that $\mathcal{P}_j$ is a prime divisor of $m_{t_i}(T) \cdot m_{1/t_i}(T)$. In this case, if $\mathcal{P}_j$ unitizes each branch point, then E_{t_0}/k ramifies at $\mathcal{P}_j$ for no $t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \dots, t_r\}$ (corollary 1.2.12). If there exists at least one such index i_j, theorem 1.3.1 also provides specializations of $E/k(T)$ which each do not ramify at $\mathcal{P}_j$, by taking a_j equal to (a multiple of) the order of the elements of C_{i_j}. Conjoining these two facts yields the following:
Assume that each prime ideal $\mathcal{P}_j$, $j = 1, \dots, s$, is a good prime for $E/k(T)$ unitizing each branch point. Then there exist infinitely distinct many points $t_0 \in k \setminus \{t_1, \dots, t_r\}$ such that the specialization E_{t_0}/k of $E/k(T)$ at t_0 ramifies at $\mathcal{P}_j$ for no index $j \in \{1, \dots, s\}$.
As in theorem 1.3.1, the conclusion holds at all (but finitely many) points in an arithmetic progression.

Theorem 1.3.1 is proved in §1.3.3.

1.3.1.2. Conjoining theorem 1.3.1 and the Hilbert specialization property. Continue with the notation of §1.3.1.1. We give below two practical situations where infinitely many specializations from theorem 1.3.1 have Galois group G.

(a) *Hilbertian base field.* Assume that k is hilbertian and fix an element θ as in addendum 1.3.1. From [Gey78, lemma 3.4], there exist infinitely many distinct elements $u \in \bigcap_{l=1}^{s} A_{\mathcal{P}_l}$ such that the specializations $E_{t_{0,u}}/k$ of $E/k(T)$ at $t_{0,u} = \theta + u \prod_{l \in S} x_{\mathcal{P}_l}^{a_l+1}$ are linearly disjoint and each have Galois group G. Hence corollary 1.3.3 below immediately follows:

Corollary 1.3.3. *For infinitely many distinct points $t_0 \in k \setminus \{t_1, \dots, t_r\}$ in some arithmetic progression, the specializations E_{t_0}/k of $E/k(T)$ at t_0 are linearly disjoint and each satisfy:*
(1) $\mathrm{Gal}(E_{t_0}/k) = G$,
(2) *for each $j \in \{1, \dots, s\}$, the inertia group of E_{t_0}/k at $\mathcal{P}_j$ is generated by some element of $C_{i_j}^{a_j}$.*

(b) *g-complete hypothesis.* Recall that a set Σ of conjugacy classes of G is called *g-complete* (a terminology due to Fried [Fri95]) if no proper subgroup of G intersects each conjugacy class in Σ. From a classical lemma of Jordan [Jor72], the set of all conjugacy classes of G is g-complete.

Assume in corollary 1.3.4 below that k is a number field and that $\{C_1, \dots, C_r\}$ is g-complete.

Corollary 1.3.4. *For any point $t_0 \in k \setminus \{t_1, \dots, t_r\}$ in some arithmetic progression, the specialization E_{t_0}/k of $E/k(T)$ at t_0 satisfies the following two conditions:*
(1) $\mathrm{Gal}(E_{t_0}/k) = G$,
(2) *for each $j \in \{1, \dots, s\}$, the inertia group of E_{t_0}/k at $\mathcal{P}_j$ is generated by some element of $C_{i_j}^{a_j}$.*

Proof. For each index $i \in \{1, \dots, r\}$, pick a prime divisor $\mathcal{P}'_i$ of $m_{t_i}(T) \cdot m_{1/t_i}(T)$ which is a good prime for $E/k(T)$ unitizing t_i (such a prime may be found since, from the Tchebotarev density theorem, $m_{t_i}(T) \cdot m_{1/t_i}(T)$ classically has infinitely many distinct prime divisors). Assume that the primes $\mathcal{P}'_1, \dots, \mathcal{P}'_r, \mathcal{P}_1, \dots, \mathcal{P}_s$ are distinct.

Apply theorem 1.3.1 to the larger set of primes $\{\mathcal{P}_j \,/\, j \in \{1, \dots, s\}\} \cup \{\mathcal{P}'_i \,/\, i \in \{1, \dots, r\}\}$, each $\mathcal{P}_j$ given with the couple (i_j, a_j) of the statement and each $\mathcal{P}'_i$ with the one $(i, 1)$. The conclusion on the primes $\mathcal{P}_1, \dots, \mathcal{P}_s$ is exactly part (2) of corollary 1.3.4 and, according to our g-complete hypothesis, that on the primes $\mathcal{P}'_1, \dots, \mathcal{P}'_r$ provides part (1).

To obtain that t_0 can be any term of some arithmetic progression, we use the more precise conclusion of addendum 1.3.1. This statement provides some $\theta \in k$ such that conditions (1) and (2) simultaneously hold at any point $t_{0,u} = \theta + u\,(\prod_{l \in S} x_{\mathcal{P}_l}^{a_l+1} \cdot \prod_{l \in S'} x_{\mathcal{P}'_l}^2) \notin \{t_1, \dots, t_r\}$ with S' the set of all indices $i \in \{1, \dots, r\}$ such that $t_i \neq \infty$ and u any element of k such that $v_{\mathcal{P}_j}(u) \geq 0$ for each index $j \in \{1, \dots, s\}$ and $v_{\mathcal{P}'_i}(u) \geq 0$ for each index $i \in \{1, \dots, r\}$. □

This trick, which consists in throwing in more primes to add the Hilbert specialization property in our conclusions, will be used in several occasions in the rest of this thesis.

Remark 1.3.5. More generally, the proof shows that the conclusion of corollary 1.3.4 remains true if there exists some subset $I \subset \{1, \dots, r\}$ satisfying the following two conditions:
(1) the set $\{C_i \,/\, i \in I\} \cup \{C_{i_j}^{a_j} \,/\, j = 1, \dots, s\}$ is g-complete,
(2) for each index $i \in I$, $m_{t_i}(T) \cdot m_{1/t_i}(T)$ has infinitely many distinct prime divisors.
In particular, we do not require the base field k to be hilbertian.

1.3.2 Examples over $\mathbb{Q}$

Fix a finite group G. As a straightforward consequence of corollary 1.3.3, we obtain that

$(**)$ *there exists a finite set $\mathcal{S}_{\mathrm{exc}}$ of prime numbers satisfying the following conclusion: given a finite set $\mathcal{S}$ of prime numbers not in $\mathcal{S}_{\mathrm{exc}}$, there exist infinitely many linearly disjoint Galois extensions of $\mathbb{Q}$ of group G which each ramify at each prime of $\mathcal{S}$,*

provided that the following condition is satisfied:

(H1/$\mathbb{Q}$) *the group G occurs as the Galois group of a* G*-extension of $\mathbb{Q}(T)$ with at least one $\mathbb{Q}$-rational branch point*[5].

5. More generally, condition $(**)$ remains true if G occurs as the Galois group of a G-extension of $\mathbb{Q}(T)$ such that all but finitely many primes are a prime divisor of $m_{\underline{\mathbf{t}}}(T) \cdot m_{1/\underline{\mathbf{t}}}(T)$.

Not all finite groups satisfy condition (H1/$\mathbb{Q}$): [DF90, corollary 1.3] shows for example that such a group should be of even order [6]. But some do. We recall below several of them to which we then apply corollary 1.3.3.

1.3.2.1. Symmetric groups. Given an integer $n \geq 3$ and three positive integers m, q and r such that $1 \leq m \leq n$, $(m,n) = 1$ and $q(n-m) - rn = 1$, we apply below corollary 1.3.3 to the G-extension $E_{\mathbb{Q}}/\mathbb{Q}(T)$ of group S_n provided by the trinomial $Y^n - T^rY^m + T^q$ recalled in §B.3.1.2. We use below the notation from there for elements of S_n and their conjugacy classes.

As S_n is centerless, one easily shows that the bad primes for $E_{\mathbb{Q}}/\mathbb{Q}(T)$ are exactly the primes $\leq n$. Then corollary 1.3.6 below immediately follows from corollary 1.3.3 (and lemma B.1.2):

Corollary 1.3.6. *Let s be a positive integer, $p_1, \dots, p_s$ be s distinct primes $> n$ and $(C_1, a_1), \dots, (C_s, a_s)$ be s couples where, for each index $j \in \{1, \dots, s\}$,*
- C_j is a conjugacy class of S_n in $\{[n^1], [m^1(n-m)^1], [1^{n-2}2^1]\}$,
- a_j is a positive integer.
Then, for infinitely many distinct points $t_0 \in \mathbb{Q}$, the splitting extensions $(E_{\mathbb{Q}})_{t_0}/\mathbb{Q}$ over $\mathbb{Q}$ of the trinomials $Y^n - {t_0}^rY^m + {t_0}^q$ are linearly disjoint and each satisfy the following two conditions:
(1) $\mathrm{Gal}((E_{\mathbb{Q}})_{t_0}/\mathbb{Q}) = S_n$,
(2) *for any $j \in \{1, \dots, s\}$, the inertia group of $(E_{\mathbb{Q}})_{t_0}/\mathbb{Q}$ at p_j is generated by an element of $C_j^{a_j}$.*

As the set $\{[n^1], [m^1(n-m)^1], [1^{n-2}2^1]\}$ is g-complete [Sch00, §2.4], one may use corollary 1.3.4 (instead of corollary 1.3.3) to obtain a more precise conclusion on the set of rational numbers t_0 at which conditions (1) and (2) above simultaneously hold (at the cost of dropping the linearly disjointness condition).

1.3.2.2. The Monster and other groups. Let G be a centerless finite group which occurs as the Galois group of a G-extension of $\mathbb{Q}(T)$ with branch point set $\{0, 1, \infty\}$. It is easily checked that the bad primes for such an extension are exactly the prime divisors of the order of G.

From the rigidity method, several centerless finite groups are known to satisfy this property (see *e.g.* [Ser92] and [MM99]). For example, using the G-extension of $\mathbb{Q}(T)$ of group the Monster group M and branch point set $\{0, 1, \infty\}$ recalled in §B.3.3 yields the following:

Corollary 1.3.7. *Let s be a positive integer, $p_1, \dots, p_s$ be s distinct prime numbers ≥ 73 or in $\{37, 43, 53, 61, 67\}$ and $(C_1, a_1), \dots, (C_s, a_s)$ be s couples where, for each index $j \in \{1, \dots, s\}$,*
- C_j is a conjugacy class of M *in $\{2A, 3B, 29A\}$,*
- a_j is a positive integer.
Then there exist infinitely many linearly disjoint Galois extensions of $\mathbb{Q}$ of group M *whose inertia group at p_j is generated by some element of $C_j^{a_j}$ for each index $j \in \{1, \dots, s\}$.*

1.3.3 Proof of theorem 1.3.1

We first show theorem 1.3.1 under the extra assumption that the set S of addendum 1.3.1 satisfies $S = \{1, \dots, s\}$ (§1.3.3.1) and next consider the case $S \neq \{1, \dots, s\}$ (§1.3.3.2). For simplicity, denote in the proof below the irreducible polynomials over k of $t_{i_1}, \dots, t_{i_s}$ (resp. of $1/t_{i_1}, \dots, 1/t_{i_s}$) by $m_{i_1}(T), \dots, m_{i_s}(T)$ (resp. by $m^*_{i_1}(T), \dots, m^*_{i_s}(T)$) respectively.

1.3.3.1. First case: $S = \{1, \dots, s\}$. The main part of the proof consists in showing that there exists some element $\theta \in A$ (not depending on j) such that $v_{\mathcal{P}_j}(m_{i_j}(\theta)) = a_j$ for each index

6. This remains true if $\mathbb{Q}$ is replaced by any number field $k \subset \mathbb{R}$.

$j \in \{1, \dots, s\}$. Then, for such a θ, fix $u \in \bigcap_{l=1}^{s} A_{\mathcal{P}_l}$ such that $t_{0,u} = \theta + u \prod_{l=1}^{s} x_{\mathcal{P}_l}^{a_l+1}$ is not a branch point. For each index $j \in \{1, \dots, s\}$, one has $v_{\mathcal{P}_j}(m_{i_j}(t_{0,u})) = a_j$ (remark 1.2.11), *i.e.* $I_{\mathcal{P}_j}(t_{0,u}, t_{i_j}) = a_j$. Apply next part (1) of lemma 1.2.4 and part (2) of the Specialization Inertia Theorem to conclude.

According to our assumptions, $\mathcal{P}_j$ is a prime divisor of $m_{i_j}(T)$ or of $m_{i_j}^*(T)$ for each $j \in \{1, \dots, s\}$. In fact, from lemma 1.3.8 below, one may drop the polynomials $m_{i_1}^*(T), \dots, m_{i_s}^*(T)$.

Lemma 1.3.8. *For each index $j \in \{1, \dots, s\}$, $\mathcal{P}_j$ is a prime divisor of $m_{i_j}(T)$.*

Proof. Indeed, if $\mathcal{P}_j$ is a prime divisor of $m_{i_j}^*(T)$ for some index j, then there exists some element $t \in A_{\mathcal{P}_j}$ such that $m_{i_j}^*(t) \in \mathcal{P}_j A_{\mathcal{P}_j}$. In particular $t_{i_j} \neq 0$ (otherwise $1 = m_{i_j}^*(t) \in \mathcal{P}_j A_{\mathcal{P}_j}$). Since $\mathcal{P}_j$ unitizes t_{i_j}, the constant coefficient a_0 of $m_{i_j}(T)$ satisfies $v_{\mathcal{P}_j}(a_0) = 0$ and, from $t_{i_j} \neq \infty$, one then has $t \notin \mathcal{P}_j A_{\mathcal{P}_j}$. Hence, from $m_{i_j}^*(t) = (1/a_0)\, t^n\, m_{i_j}(1/t)$ (with $n = \deg(m_{i_j}(T))$), one has $m_{i_j}(1/t) \in \mathcal{P}_j A_{\mathcal{P}_j}$, *i.e.* $\mathcal{P}_j$ is a prime divisor of $m_{i_j}(T)$. □

Remark 1.3.9. In particular, lemma 1.3.8 shows that, if ∞ is not a branch point, then the two polynomials $m_{\underline{\mathbf{t}}}(T)$ and $m_{\underline{\mathbf{t}}}(T) \cdot m_{1/\underline{\mathbf{t}}}(T)$ have the same prime divisors (up to finitely many).

For each index $j \in \{1, \dots, s\}$, fix $\theta_j \in A_{\mathcal{P}_j}$ such that $v_{\mathcal{P}_j}(m_{i_j}(\theta_j)) > 0$. The core of the construction consists in replacing the s-tuple $(\theta_1, \dots, \theta_s)$ by some suitable s-tuple $(\theta'_1, \dots, \theta'_s)$ such that $v_{\mathcal{P}_j}(m_{i_j}(\theta'_j)) = a_j$ for each index $j \in \{1, \dots, s\}$.

Lemma 1.3.10. *Let $j \in \{1, \dots, s\}$ and d be a positive integer. Then there exists some $\theta_{j,d} \in A_{\mathcal{P}_j}$ such that $v_{\mathcal{P}_j}(m_{i_j}(\theta_{j,d})) = d$.*

Proof. We show lemma 1.3.10 by induction. If $v_{\mathcal{P}_j}(m_{i_j}(\theta_j)) = 1$, one can obviously take $\theta_{j,1} = \theta_j$. Otherwise, as noted in the last paragraph of the proof of proposition 1.2.9, one can take $\theta_{j,1} = \theta_j + x_{\mathcal{P}_j} \in A_{\mathcal{P}_j}$.

We now explain how to produce some $\theta_{j,2} \in A_{\mathcal{P}_j}$. From lemma 1.2.7, one has $v_{\mathcal{P}_j}(m'_{i_j}(\theta_{j,1})) = 0$ and then $m'_{i_j}(\theta_{j,1}) \neq 0$. Assume first that one has $(1/2)m''_{i_j}(\theta_{j,1}) \in A_{\mathcal{P}_j} \setminus \mathcal{P}_j A_{\mathcal{P}_j}$ and set $u = -(m_{i_j}(\theta_{j,1})/m'_{i_j}(\theta_{j,1})) + x_{\mathcal{P}_j}^3$. Taylor's formula yields

$$m_{i_j}(\theta_{j,1} + u) = x_{\mathcal{P}_j}^3 m'_{i_j}(\theta_{j,1}) + (1/2)u^2 m''_{i_j}(\theta_{j,1}) + u^3 R_j$$

with $R_j \in A_{\mathcal{P}_j}$. Hence one can take $\theta_{j,2} = \theta_{j,1} + u$ (this is an element of $A_{\mathcal{P}_j}$ since $v_{\mathcal{P}_j}(u) = 1$) since one has $v_{\mathcal{P}_j}(x_{\mathcal{P}_j}^3 m'_{i_j}(\theta_{j,1})) = 3$, $v_{\mathcal{P}_j}((1/2)u^2 m''_{i_j}(\theta_{j,1})) = 2$ and $v_{\mathcal{P}_j}(u^3 R_j) \geq 3$. Assume now that $v_{\mathcal{P}_j}((1/2)m''_{i_j}(\theta_{j,1})) \geq 1$ and set $\widetilde{u} = -(m_{i_j}(\theta_{j,1})/m'_{i_j}(\theta_{j,1})) + x_{\mathcal{P}_j}^2$. Taylor's formula yields

$$m_{i_j}(\theta_{j,1} + \widetilde{u}) = x_{\mathcal{P}_j}^2 m'_{i_j}(\theta_{j,1}) + (1/2)\widetilde{u}^2 m''_{i_j}(\theta_{j,1}) + \widetilde{u}^3 R_j$$

with $R_j \in A_{\mathcal{P}_j}$. Then one can take $\theta_{j,2} = \theta_{j,1} + \widetilde{u}$ (this is an element of $A_{\mathcal{P}_j}$ since $v_{\mathcal{P}_j}(\widetilde{u}) = 1$) since one has $v_{\mathcal{P}_j}(x_{\mathcal{P}_j}^2 m'_{i_j}(\theta_{j,1})) = 2$, $v_{\mathcal{P}_j}((1/2)\widetilde{u}^2 m''_{i_j}(\theta_{j,1})) \geq 3$ and $v_{\mathcal{P}_j}(\widetilde{u}^3 R_j) \geq 3$.

Fix now an integer $d \geq 2$ and assume that some $\theta_{j,d} \in A_{\mathcal{P}_j}$ has been constructed. We produce below some $\theta_{j,d+1} \in A_{\mathcal{P}_j}$. As before, one has $v_{\mathcal{P}_j}(m'_{i_j}(\theta_{j,d})) = 0$ and then $m'_{i_j}(\theta_{j,d}) \neq 0$. Set $u = -(m_{i_j}(\theta_{j,d})/m'_{i_j}(\theta_{j,d})) + x_{\mathcal{P}_j}^{d+1}$. Taylor's formula yields

$$m_{i_j}(\theta_{j,d} + u) = x_{\mathcal{P}_j}^{d+1} m'_{i_j}(\theta_{j,d}) + u^2 R_j$$

with $R_j \in A_{\mathcal{P}_j}$. Then one can take $\theta_{j,d+1} = \theta_{j,d} + u$ (this is an element of $A_{\mathcal{P}_j}$ since $v_{\mathcal{P}_j}(u) = d$) since one has $v_{\mathcal{P}_j}(x_{\mathcal{P}_j}^{d+1} m'_{i_j}(\theta_{j,d})) = d + 1$ and $v_{\mathcal{P}_j}(u^2 R_j) \geq 2d > d + 1$ $(d \geq 2)$. □

For each index $j \in \{1,\ldots,s\}$, fix $\theta'_j \in A_{\mathcal{P}_j}$ such that $v_{\mathcal{P}_j}(m_{i_j}(\theta'_j)) = a_j$. From the chinese remainder theorem, there exist infinitely many distinct $\theta \in A$ such that $\theta - \theta'_j \in \mathcal{P}_j^{a_j+1} A_{\mathcal{P}_j}$ for each index $j \in \{1,\ldots,s\}$. Hence, for such a θ, it follows from remark 1.2.11 that one has $v_{\mathcal{P}_j}(m_{i_j}(\theta)) = a_j$ for each index $j \in \{1,\ldots,s\}$, thus ending the proof in the case $S = \{1,\ldots,s\}$.

1.3.3.2. Second case: $S \neq \{1,\ldots,s\}$. The proof of lemma 1.3.8 shows that $\mathcal{P}_j$ is a prime divisor of $m_{i_j}(T)$ for each index $j \in S$. Use next lemma 1.3.10 to pick a $|S|$-tuple $(\theta_j)_{j\in S} \in \prod_{j\in S} A_{\mathcal{P}_j}$ such that $v_{\mathcal{P}_j}(m_{i_j}(\theta_j)) = a_j$ for each index $j \in S$. Let $S^* = \{1,\ldots,s\} \setminus S$, *i.e.* S^* is the set of all indices $j \in \{1,\ldots,s\}$ such that $t_{i_j} = \infty$. For each index $j \in S^*$, denote $x_{\mathcal{P}_j}^{a_j}$ by θ^*_j.

From the Artin-Whaples theorem (*e.g.* [Lan02, chapter XII, theorem 1.2]), there exists some $\theta \in k$ satisfying the following two conditions:
(i) $v_{\mathcal{P}_j}(\theta - \theta_j) \geq a_j + 1$ (and so $v_{\mathcal{P}_j}(\theta) \geq 0$) for each index $j \in S$,
(ii) $v_{\mathcal{P}_j}(\theta - (1/\theta^*_j)) \geq a_j + 1$ (and so $v_{\mathcal{P}_j}(\theta) < 0$) for each index $j \in S^*$.
Fix $u \in \bigcap_{l=1}^{s} A_{\mathcal{P}_l}$ such that $t_{0,u} = \theta + u \prod_{l\in S} x_{\mathcal{P}_l}^{a_l+1}$ is not a branch point. We show below that $I_{\mathcal{P}_j}(t_{0,u}, t_{i_j}) = a_j$ for each index $j \in \{1,\ldots,s\}$. As in §1.3.3.1, it then remains to apply part (1) of lemma 1.2.4 and part (2) of the Specialization Inertia Theorem to finish the proof.

Let $j \in S$. Since $v_{\mathcal{P}_j}(t_{0,u}) \geq 0$, one has $I_{\mathcal{P}_j}(t_{0,u}, t_{i_j}) = v_{\mathcal{P}_j}(m_{i_j}(t_{0,u}))$ and, as in the case $S = \{1,\ldots,s\}$, one has $v_{\mathcal{P}_j}(m_{i_j}(t_{0,u})) = a_j$.

Let $j \in S^*$. Since $t_{i_j} = \infty$ and $v_{\mathcal{P}_j}(t_{0,u}) = v_{\mathcal{P}_j}(\theta) < 0$, one has $I_{\mathcal{P}_j}(t_{0,u}, t_{i_j}) = v_{\mathcal{P}_j}(1/\theta)$. But $v_{\mathcal{P}_j}(\theta^*_j) = a_j$ and $v_{\mathcal{P}_j}((1/\theta) - \theta^*_j) = v_{\mathcal{P}_j}((1/\theta^*_j) - \theta) - v_{\mathcal{P}_j}(\theta) + v_{\mathcal{P}_j}(\theta^*_j) \geq a_j + 1$. Hence $v_{\mathcal{P}_j}(1/\theta) = a_j$.

1.4 Specializations with specified local behavior

Fix $k = \mathbb{Q}$ for simplicity. As already noted in remark 1.3.2, theorem 1.3.1 also includes trivial ramification. Previous works, namely [DG12] and [DG11], are concerned with this kind of conclusions: it was shown there that, for each finite group G, any G-extension of $\mathbb{Q}(T)$ of group G has specializations with the same group which each are unramified at any finitely many prescribed large enough primes and such that the associated Frobenius at each such prime is in any specified conjugacy class of G.

As stated in theorem 1.4.1 below, it is in fact possible to conjoin this previous statement and theorem 1.3.1 to obtain Galois extensions of $\mathbb{Q}$ of various finite groups with specified local behavior at finitely many given primes.

1.4.1 Statement of the result

Let G be a finite group, $E/\mathbb{Q}(T)$ be a G-extension of group G, $\{t_1,\ldots,t_r\}$ be its branch point set and $(C_1,\ldots,C_r)$ be its inertia canonical invariant.

Let $\mathcal{S}_{\rm ra}$ and $\mathcal{S}_{\rm ur}$ be two disjoint finite sets of good [7] primes for $E/\mathbb{Q}(T)$ such that $\mathcal{S}_{\rm ur} \neq \emptyset$ and each prime p in $\mathcal{S}_{\rm ur}$ satisfies $p \geq r^2|G|^2$ [8]. For each prime $p \in \mathcal{S}_{\rm ur}$, fix a conjugacy class C_p of G. For each prime $p \in \mathcal{S}_{\rm ra}$, let a_p be a positive integer and $i_p \in \{1,\ldots,r\}$ such that $t_{i_p} \neq \infty$, p unitizes t_{i_p} and is a prime divisor of $m_{t_{i_p}}(T) \cdot m_{1/t_{i_p}}(T)$.

Assume in theorem 1.4.1 below that the set $\{C_{i_p}^{a_p} \,/\, p \in \mathcal{S}_{\rm ra}\} \cup \{C_p \,/\, p \in \mathcal{S}_{\rm ur}\}$ is g-complete. At the cost of throwing in more primes in $\mathcal{S}_{\rm ur}$ with appropriate associated conjugacy classes of G, we may assume that this hypothesis holds: with $\mathrm{cc}(G)$ the number of distinct non trivial

7. Condition (4) of definition 1.2.5 may be removed for prime numbers in $\mathcal{S}_{\rm ur}$.
8. The bound in [DG12] is $p \geq 4r^2|G|^2$. This slight difference comes from a slight technical improvement in the bounds obtained from the Lang-Weil estimates (see §4.2.2 for more details).

conjugacy classes of G, one may throw in $\mathcal{S}_{\mathrm{ur}}$ a set $\mathcal{S}_{\mathrm{gc}}$ of $\mathrm{cc}(G)$ distinct good primes disjoint from the original set $\mathcal{S}_{\mathrm{ur}}$ and associate in a one-one way a non trivial conjugacy class C_p of G to each prime $p \in \mathcal{S}_{\mathrm{gc}}$; the g-complete property following then from [Jor72].

Theorem 1.4.1. *There exists some integer θ satisfying the following conclusion. For each integer $t_0 \equiv \theta \mod (\prod_{p\in\mathcal{S}_{\mathrm{ur}}} p \cdot \prod_{p\in\mathcal{S}_{\mathrm{ra}}} p^{a_p+1})$, t_0 is not a branch point and the specialization $E_{t_0}/\mathbb{Q}$ of $E/\mathbb{Q}(T)$ at t_0 satisfies the following three conditions:*
(1) $\mathrm{Gal}(E_{t_0}/\mathbb{Q}) = G$,
(2) *for each prime $p \in \mathcal{S}_{\mathrm{ra}}$, the inertia group of $E_{t_0}/\mathbb{Q}$ at p is generated by some element of $C_{i_p}^{a_p}$,*
(3) *for each prime $p \in \mathcal{S}_{\mathrm{ur}}$, p does not ramify in $E_{t_0}/\mathbb{Q}$ and the associated Frobenius is in the conjugacy class C_p.*

1.4.2 Proof of theorem 1.4.1

We first recall how [DG12] handles condition (3). Let $p \in \mathcal{S}_{\mathrm{ur}}$, $g_p \in C_p$ and e_p be the order of g_p. Let $F_p/\mathbb{Q}_p$ be the unique unramified Galois extension of $\mathbb{Q}_p$ of degree e_p, given together with an isomorphism $f : \mathrm{Gal}(F_p/\mathbb{Q}_p) \to \langle g_p \rangle$ satisfying $f(\sigma) = g_p$ with σ the Frobenius of the extension $F_p/\mathbb{Q}_p$. Let $\varphi : \mathrm{G}_{\mathbb{Q}_p} \to \langle g_p \rangle$ be the corresponding epimorphism. Since $p \geq r^2|G|^2$ and p is a good prime for $E/\mathbb{Q}(T)$, [DG12] provides some integer θ_p such that, for each integer $t \equiv \theta_p \mod p$, t is not a branch point and the specialization $(E\mathbb{Q}_p)_t/\mathbb{Q}_p$ corresponds to φ.

For each prime $p \in \mathcal{S}_{\mathrm{ra}}$, addendum 1.3.1 provides some integer θ'_p such that, for every integer t satisfying $t \equiv \theta'_p \mod p^{a_p+1}$ and $t \notin \{t_1, \dots, t_r\}$, the inertia group of $E_t/\mathbb{Q}$ at p is generated by some element of $C_{i_p}^{a_p}$.

Use next the chinese remainder theorem to find some integer θ satisfying $\theta \equiv \theta_p \mod p$ for each prime $p \in \mathcal{S}_{\mathrm{ur}}$ and $\theta \equiv \theta'_p \mod p^{a_p+1}$ for each prime $p \in \mathcal{S}_{\mathrm{ra}}$. Then, for every integer t_0 such that $t_0 \equiv \theta \mod (\prod_{p\in\mathcal{S}_{\mathrm{ur}}} p \cdot \prod_{p\in\mathcal{S}_{\mathrm{ra}}} p^{a_p+1})$, t_0 is not a branch point and the specialization $E_{t_0}/\mathbb{Q}$ of $E/\mathbb{Q}(T)$ at t_0 satisfies conditions (2) and (3).

Finally, for such a t_0, one has $\mathrm{Gal}(E_{t_0}/\mathbb{Q}) = G$ according to our g-complete hypothesis, thus ending the proof.

Part II

Presentation of part II

The *Inverse Galois Problem* (over $\mathbb{Q}$) asks whether, for a given finite group H, there exists at least one Galois extension of $\mathbb{Q}$ of group H. A classical way to obtain such an extension consists in producing a G-extension of $\mathbb{Q}(T)$ with the same group: from the *Hilbert irreducibility theorem*, such a G-extension of $\mathbb{Q}(T)$ has at least one specialization of group H (in fact infinitely many if H is not trivial).

We are interested in the second part of this thesis in "parametric Galois extensions", *i.e.* in G-extensions of $\mathbb{Q}(T)$ which have all the Galois extensions of $\mathbb{Q}$ of group H among their specializations. More precisely, given a field k and a finite group H, we say that a G-extension $E/k(T)$ with Galois group G containing H is *H-parametric over k* if any Galois extension of k of group H occurs as a specialization of $E/k(T)$ (definition 2.1.1). The special case $H = G$ is of particular interest.

Chapter 2

Connections with some classical notions in inverse Galois theory (§2.1)

Given a field k and a finite group G, the question of whether there exists at least one G-parametric extension over k of group G or not is intermediate between the following classical two questions in inverse Galois theory:

- if there exists at least one such extension, then it obviously solves the *Beckmann-Black problem for G over k*, which asks whether any Galois extension F/k of group G occurs as a specialization of some G-extension $E_F/k(T)$ with the same group,

- if there are no such extension, then there obviously cannot exist a *one parameter generic polynomial over k of group G*, *i.e.* a polynomial $P(T,Y) \in k(T)[Y]$ of group G such that the splitting extension over $L(T)$ is G-parametric over L for any field extension L/k.

We refer to §2.1 for more details.

If studying parametric extensions indeed seems a natural first step to these important topics, it is itself already quite challenging, especially over number fields. The question of deciding whether a given G-extension of $k(T)$ with given group G containing H is H-parametric over a given base field k or not indeed seems to be difficult, even for small groups H and G: for example, in the case $H = G = \mathbb{Z}/3\mathbb{Z}$ and $k = \mathbb{Q}$, the answer seems to be known for only one such extension (it is $\mathbb{Z}/3\mathbb{Z}$-parametric over $\mathbb{Q}$; see below). Of course there are some obvious examples like the extensions $k(\sqrt[n]{T})/k(T)$ $(n \in \mathbb{N} \setminus \{0\})$ and $k(T)(\sqrt{T^2+1})/k(T)$: if k contains the n-th roots of unity (and the characteristic of k does not divide n), the former is $\mathbb{Z}/n\mathbb{Z}$-parametric over k (this follows from the Kummer theory) whereas, if $k \subset \mathbb{R}$, the latter is not $\mathbb{Z}/2\mathbb{Z}$-parametric over k (since none of its specializations is imaginary). But they seem to be quite sparse.

Parametric extensions over various fields (§2.2)

In §2.2, we give some first conclusions on parametric extensions (based on previous works) over various base fields k with good arithmetic properties such as PAC fields, finite fields, formal Laurent series fields or the field $\mathbb{Q}$ and its completions.

For example, in the case k is a PAC[1] field (§2.2.1), the situation is quite clear: there exists at least one H-parametric extension over k of group G for any finite groups $H \subset G$. In contrast, in the case $k = \mathbb{Q}$ (§2.2.5), not much is known although it may be expected that only a few G-extensions of $\mathbb{Q}(T)$ are parametric over $\mathbb{Q}$. On the one hand, it is known that there exists at least one G-parametric extension over $\mathbb{Q}$ of group G if G is one of the four groups $\{1\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$ and S_3. For any other one, it is unknown whether there exists at least one such extension or not. On the other hand, only a few G-extensions of $\mathbb{Q}(T)$ are known not to be parametric over $\mathbb{Q}$.

First examples over $\mathbb{Q}$ (§2.3)

We next use in §2.3 *ad hoc* arguments to obtain some new examples of non H-parametric extensions over $\mathbb{Q}$ with small Galois groups G and small branch point numbers r (propositions 2.3.3, 2.3.9 and 2.3.11):

Theorem 1. (a) *A* G-*extension of* $\mathbb{Q}(T)$ *of group* $\mathbb{Z}/2\mathbb{Z}$ *with* $r = 2$ *branch points is* $\mathbb{Z}/2\mathbb{Z}$-*parametric over* $\mathbb{Q}$ *if and only if both are* $\mathbb{Q}$-*rational.*

(b) *No* G-*extension of* $\mathbb{Q}(T)$ *of group* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *with* $r = 3$ *branch points is* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-*parametric over* $\mathbb{Q}$.

(c) *The splitting field over* $\mathbb{Q}(T)$ *of the trinomial* $Y^3 + T^2Y + T^2$ *provides a* G-*extension of* $\mathbb{Q}(T)$ *of group* S_3, *with* $r = 4$ *branch points and which is* H-*parametric over* $\mathbb{Q}$ *for no subgroup* $H \subset S_3$.

The proof rests on the non-existence of solutions to some diophantine equations (for the first two parts) and on the non totally real behavior of the specializations (for the third part). We also have an example with $G = \mathbb{Z}/6\mathbb{Z}$ and $r = 2$ (proposition 2.3.7).

Chapter 3

A general method (§3.1)

We offer in §3.1 a systematic approach to give more examples of non H-parametric extensions over k of group G containing H. Given a G-extension $E_H/k(T)$ of group H and a G-extension $E_G/k(T)$ of group G, we use the results of part I to produce some specializations of $E_H/k(T)$ of group H which each cannot be a specialization of $E_G/k(T)$ (and so $E_G/k(T)$ is not H-parametric over k). More precisely, we provide two different sufficient conditions which each guarantee such a situation. The first one (*Branch Point Hypothesis*) involves the branch point arithmetic while the second one (*Inertia Hypothesis*) is a more geometric condition on the inertia of the two G-extensions $E_H/k(T)$ and $E_G/k(T)$. Theorem 3.1.1 is our precise result; it is the aim of §3.1.

We most of the time work over base fields k which are the quotient field of any Dedekind domain A of characteristic zero with infinitely many distinct prime ideals, additionaly assumed to be hilbertian. Number fields or finite extensions of rational function fields $\kappa(U)$, with κ an arbitrary field of characteristic zero (and U an indeterminate), are typical examples. We also discuss the cases where the hilbertian assumption is removed or the domain A only has finitely many distinct prime ideals.

1. See §B.2.1 for the definition and some examples of PAC fields.

Applications (§3.2-3.4)

We then use our criteria in §3.2-3.4 to give new examples of non parametric extensions over various base fields.

A general result over various base fields (§3.2). We first obtain the following result (corollary 3.2.2) which leads to non G-parametric extensions of group G over large enough number fields for many finite groups G.

Theorem 2. *Let G be a finite group. Assume that there exists some set $\{C_1, \dots, C_r, C\}$ of non trivial conjugacy classes of G satisfying the following two conditions:*
(1) *the elements of $C_1, \dots, C_r$ generate G,*
(2) *the conjugacy class C is a power of C_i for no index $i \in \{1, \dots, r\}$.*
Then there exist some number field k and some G*-extension of $k(T)$ of group G which is not G-parametric over k.*

Many finite groups admit a conjugacy class set as above: abelian groups which are not cyclic of prime power order, symmetric groups S_n ($n \geq 3$), alternating groups A_n ($n \geq 4$), dihedral groups D_n of order $n \geq 2$, non abelian simple groups, *etc.* (see §3.2.1.1 for more details and references). Moreover the conclusion also holds if the suitable number field k is replaced by any finite extension of the rational function field $\mathbb{C}(U)$ (§3.2.2.1) or of the formal Laurent series field $\mathbb{C}((U))$ (in the case G has trivial center; see corollary 3.2.5) and, under some conjecture of Fried, one can even take $k = \mathbb{Q}$ (corollary 3.2.3). In contrast, we also obtain that, *given a finite extension $k/\mathbb{C}((U))$, any centerless finite group G occurs as the Galois group of a* G*-extension of $k(T)$ which is H-parametric over k for any subgroup $H \subset G$.* (corollary 3.2.6).

Examples over given base fields (§3.3 and §3.4). We then give new examples of non H-parametric extensions of group G containing H over various given base fields k (in particular over $\mathbb{Q}$). To do so, we need to start from two G-extensions of $k(T)$ with groups H and G respectively. This first step depends on the state-of-the-art in inverse Galois theory, especially in the case $k = \mathbb{Q}$, and the involved finite groups then are the classical ones in this context: abelian groups, symmetric groups, alternating groups, some other simple groups... We present our examples below.

(a) *Examples from the Branch Point Criterion* (§3.3). Let k be a number field and G be a finite group. We first give pure branch point arithmetical conditions for any G-extension of $k(T)$ of group G not to be H-parametric over k for any non trivial subgroup $H \subset G$ (corollary 3.3.1).

We then give some concrete examples in the situation $G = \mathbb{Z}/2\mathbb{Z}$ (and so $H = \mathbb{Z}/2\mathbb{Z}$ too) where the existence of at least one G-extension of $k(T)$ of group G satisfying our conditions is guaranteed and which is already of some interest (corollary 3.3.3). We next give some other examples which are concerned with larger abelian groups (corollaries 3.3.4, 3.3.6 and 3.3.7).

(b) *Examples from the Inertia Criterion* (§3.4).

(i) *Symmetric and alternating groups.* Let $n \geq 3$ be an integer and k be one of our allowed [2] base fields. We first give some practical sufficient conditions for a given G-extension of $k(T)$ of group $G = S_n$ not to be $H = S_n$-parametric over k (§3.4.1.2). We also have an analog in each of the two situations $H = G = A_n$ (§3.4.2.2) and ($H = A_n$ and $G = S_n$) (§3.4.3.2). Theorem 3 below is a consequence of our results:

2. *i.e.* k is the quotient field of any Dedekind domain of characteristic zero with infinitely many distinct prime ideals, additionaly assumed to be hilbertian.

Theorem 3. *Let $r \geq 3$ be an integer and k be a number field or a finite extension of the rational function field $\mathbb{C}(U)$. Then there exists some integer n_r not depending on the base field k and satisfying the following conclusion: for any integer $n > n_r$, no* G*-extension of $k(T)$ of group $G = A_n$ with r branch points is $H = A_n$-parametric over k.*

The same conclusion holds in each of the two situations $H = G = S_n$ and ($H = A_n$ and $G = S_n$).

Moreover our results show that several classical G-extensions of $k(T)$ of group S_n (resp. of group A_n) are neither S_n-parametric nor A_n-parametric (resp. not A_n-parametric) over any given of our allowed base fields k. Corollaries 3.4.1, 3.4.3-3.4.4 and 3.4.6-3.4.11 give our main examples.

(ii) *Non abelian simple groups.* We also show that some G-extensions with simple Galois groups G provided by the rigidity method are not G-parametric. For instance, using the Atlas [C+85] notation for conjugacy classes of finite groups, one has the following (corollary 3.4.12):

Let p be a prime number ≥ 5 and k be one of our allowed base fields such that $(-1)^{(p-1)/2}p$ is a square in k. Then no G*-extension of $k(T)$ of group $\mathrm{PSL}_2(\mathbb{F}_p)$ provided by either one of the rigid triples $(2A, pA, pB)$ (if $(\frac{2}{p}) = -1$) and $(3A, pA, pB)$ (if $(\frac{3}{p}) = -1$) of conjugacy classes of $\mathrm{PSL}_2(\mathbb{F}_p)$ is $\mathrm{PSL}_2(\mathbb{F}_p)$-parametric over k.*

We also have a similar result with the Monster group (corollary 3.4.13).

(iii) *Examples with $H \neq G$.* We also have various examples which are specifically devoted to the case $H \neq G$. For instance, one has the following (corollary 3.4.14):

Let k be one of our allowed base fields. Then, with Th *the Thompson group, no* G*-extension of $k(T)$ of group the Baby-Monster group* B *provided by the rigid triple $(2C, 3A, 55A)$ of conjugacy classes of* B *is* Th*-parametric over k.*

Further similar examples with various groups such as symmetric groups, other sporadic groups or p-groups are given (corollaries 3.4.15 and 3.4.16).

Chapter 2

Parametric extensions I

2.1 Definitions

Let k be a field.

2.1.1 Parametric extensions

Definition 2.1.1. Let $E/k(T)$ be a G-extension of branch point set $\{t_1, \dots, t_r\}$.
(1) Let H be a subgroup of $\mathrm{Gal}(E/k(T))$. We say that $E/k(T)$ is *H-parametric over k* if, for every Galois extension F/k of group H, there exists some point $t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \dots, t_r\}$ such that F/k is the specialization E_{t_0}/k of $E/k(T)$ at t_0.
(2) We say that $E/k(T)$ is *parametric over k* if this extension is H-parametric over k for each subgroup $H \subset \mathrm{Gal}(E/k(T))$.

For this subsection, let $H \subset G$ be two finite groups. The notion of H-parametric extensions $E/k(T)$ over k of Galois group $\mathrm{Gal}(E/k(T)) = G$ relates to that of "lifting extensions".

More precisely, given a Galois extension F/k of group H, recall that a *lifting extension of group G for F/k* is a G-extension $E_F/k(T)$ of group G which has the extension F/k among its specializations. Then any H-parametric extension over k of group G obviously is a lifting extension of group G for any Galois extension of k of group H. Moreover, if there exists at least one G-parametric extension over k of group G, then it obviously solves the *Beckmann-Black problem for G over k*, which asks whether any Galois extension of k of group G has a lifting extension with the same group.

We now consider the case $E/k(T)$ is given by a polynomial $P(T,Y) \in k[T][Y]$. First of all, lemma B.1.2 provides the following statement:

Let $E/k(T)$ be a G-*extension of group G, $P(T,Y) \in k[T][Y]$ be a monic (with respect to Y) separable polynomial of splitting field E over $k(T)$ and H be a subgroup of G. Assume that any Galois extension of k of group H occurs as the splitting extension over k of some separable polynomial $P(t_0, Y)$ with $t_0 \in k$. Then $E/k(T)$ is H-parametric over k.*

Remark 2.1.2. We note for later use that the condition requiring $P(t_0, Y)$ to be separable over k is automatic if $|H| > (n-1)!$; here $n = \deg_Y P(T,Y)$.

Conversely one has the following statement whose proof is similar to that of [JLY02, proposition 5.1.8]:

Proposition 2.1.3. *Let $E/k(T)$ be an H-parametric extension over k of group G. Then there exist two monic separable polynomials $P_1(T,Y)$ and $P_2(T,Y)$ in $k[T][Y]$ of splitting field E over $k(T)$ which satisfy the following property: any Galois extension of k of group H occurs as the splitting extension over k of some polynomial $P_i(t_0,Y)$ with $t_0 \in k$ and $i \in \{1,2\}$.*

Proof. Denote the integral closure of $k[T]$ in E by B_k. Pick an integer s and a s-tuple $(b_1,\dots,b_s)$ of elements of B_k such that $B_k = k[T]b_1 + \cdots + k[T]b_s$ [Dèb09, theorem 1.3.13]. Up to reordering, one may assume that there exists some positive integer $s' \leq s$ satisfying these two conditions:
(i) for $1 \leq i \neq j \leq s'$, b_i and b_j are not conjugate over k,
(ii) for $i > s'$, there exists some index $1 \leq j \leq s'$ such that b_i and b_j are conjugate over k.
For each index $i \in \{1,\dots,s'\}$, denote the irreducible polynomial of b_i over $k(T)$ by $m_i(T,Y)$. Set $P_1(T,Y) = \prod_{i=1}^{s'} m_i(T,Y)$. Then $P_1(T,Y)$ is a monic separable polynomial with coefficients in $k[T]$ and its splitting field over $k(T)$ is equal to E.

We show below the following statement which will be used in several occasions in this chapter:

($*$) *For any extension L/k such that the integral closure B_L of $L[T]$ in the compositum EL satisfies $B_L = L[T]b_1 + \cdots + L[T]b_s$ and any point $t_0 \in L$, not a branch point, the specialization $(EL)_{t_0}/L$ of $EL/L(T)$ at t_0 is the splitting extension over L of the specialized polynomial $P_1(t_0,Y)$.*

Indeed fix an extension L/k as in statement ($*$) and a point $t_0 \in L$ which is not a branch point. Pick a prime ideal $\mathcal{P}_L$ of B_L above $\langle T - t_0 \rangle$. As $B_L = L[T]b_1 + \cdots + L[T]b_s$ and with $\overline{b_1},\dots,\overline{b_s}$ the reductions modulo $\mathcal{P}_L$ of $b_1,\dots,b_s$ respectively, one has $(EL)_{t_0} = B_L/\mathcal{P}_L = L(\overline{b_1},\dots,\overline{b_s})$. Hence $(EL)_{t_0}$ is the splitting field over L of the specialized polynomial $P_1(t_0,Y)$.

Do now the same but with the domain $k[T]$ replaced by $k[1/T]$. Denote the integral closure of $k[1/T]$ in E by B_k^*. Pick a positive integer s^* and a s-tuple $(b_1^*,\dots,b_{s^*}^*)$ of elements of B_k^* such that $B_k^* = k[1/T]b_1^* + \cdots + k[1/T]b_{s^*}^*$. By proceeding as before, we obtain a monic separable polynomial $P_2(T,Y) \in k[T][Y]$ of splitting field E over $k(T)$ which satisfies the following property:

($**$) *For any extension L/k such that the integral closure B_L^* of $L[1/T]$ in the compositum EL satisfies $B_L^* = L[1/T]b_1^* + \cdots + L[1/T]b_{s^*}^*$, if ∞ is not a branch point, then the specialization $(EL)_\infty/L$ of $EL/L(T)$ at ∞ is the splitting extension over L of the polynomial $P_2(0,Y)$.*

The proof of proposition 2.1.3 is now quite clear. Fix a Galois extension F/k of group H. From our assumption, there exists some point $t_0 \in \mathbb{P}^1(k)$ such that $E_{t_0}/k = F/k$. In the case $t_0 \neq \infty$, statement ($*$) shows that F is the splitting field over k of the polynomial $P_1(t_0,Y)$. In the case $t_0 = \infty$, F is the splitting field over k of $P_2(0,Y)$ (statement ($**$)) [1]. □

Remark 2.1.4. The conclusion of proposition 2.1.3 holds with a single polynomial $P(T,Y)$ in each of the following three situations:
(1) $E/k(T)$ has at least one k-rational branch point,
(2) k is an ample [2] field: this follows from statement ($***$) of [Dèb99c, §3.3.2] (see also §5.2.3); one may even require the specialized polynomial $P(t_0,Y)$ to be separable over k,
(3) k is infinite and $E/k(T)$ has genus 0 (see §5.2.4.1); as in the ample field situation, one may also require the specialized polynomial $P(t_0,Y)$ to be separable over k.

2.1.2 Generic extensions and generic polynomials

The notion of parametric extensions is also related to that of *one parameter generic polynomials* which we recall below. We first propose the following definition which is the counterpart of definition 2.1.1 in the generic situation:

1. Note that the polynomials $P_1(t_0,Y)$ and $P_2(0,Y)$ are not necessarily separable over k.
2. See §B.2.2 for the definition and some examples of ample fields.

Definition 2.1.5. Let $E/k(T)$ be a G-extension of branch point set $\{t_1, \dots, t_r\}$.
(1) Let H be a subgroup of $\mathrm{Gal}(E/k(T))$. We say that $E/k(T)$ is *H-generic over k* if the extension $EL/L(T)$ is H-parametric over L for any extension L/k.
(2) We say that $E/k(T)$ is *generic over k* if this extension is H-generic over k for each subgroup $H \subset \mathrm{Gal}(E/k(T))$.

Let $H \subset G$ be two finite groups. Note first that any H-generic extension over k of group G obviously is H-parametric over k. We will give three counter-examples to the converse (part (2) of remark 2.1.7, example 2.2.1 and remark 3.4.2).

As in the parametric situation, one has the following statement in the case $E/k(T)$ is given by a polynomial $P(T,Y) \in k[T][Y]$:

Let $E/k(T)$ be a G*-extension of group G, $P(T,Y) \in k[T][Y]$ be a monic separable polynomial of splitting field E over $k(T)$ and H be a subgroup of G. Assume that the following condition holds:*
$(*/H)$ for any extension L/k, any Galois extension of L of group H occurs as the splitting extension over L of some separable polynomial $P(t_0, Y)$ with $t_0 \in L$.
Then $E/k(T)$ is H-generic over k.

Condition $(*/H)$ is involved in the definition of *one parameter generic polynomials over k*. There are several variants of this definition in the literature. We recall below two of them which we will use in the rest of this chapter (and refer to [JLY02] for more on generic polynomials). Let $P(T,Y) \in k[T][Y]$ be a monic separable polynomial of group G.
(1) If $P(T,Y)$ satisfies condition $(*/G)$, but without requiring $P(t_0,Y)$ to be separable over L, it is generic in the sense of *Ledet*,
(2) If $P(T,Y)$ satisfies condition $(*/H')$ for any subgroup $H' \subset G$, but without requiring $P(t_0,Y)$ to be separable over L, it is generic in the sense of *Kemper* (of course any generic polynomial in the sense of Kemper is generic in the sense of Ledet; [Kem01] shows that the converse is true if k is infinite).

The counterpart of proposition 2.1.3 in the generic situation is given by the following:

Proposition 2.1.6. *Assume that k is perfect. Let $E/k(T)$ be an H-generic extension over k of group G.*
(1) *There exist two monic separable polynomials $P_1(T,Y)$ and $P_2(T,Y)$ in $k[T][Y]$ of splitting field E over $k(T)$ satisfying the following property: for any extension L/k, any Galois extension of L of group H occurs as the splitting extension over L of some polynomial $P_i(t_0,Y)$ with $t_0 \in L$ and $i \in \{1,2\}$.*
(2) *Assume that $H = G$ and k is infinite. Then part (1) holds with a single polynomial $P(T,Y)$, in which case this polynomial is generic over k in the sense of Kemper.*

Proof. We first show part (1). As in the proof of proposition 2.1.3, denote the integral closure of $k[T]$ in E by B_k and set as there $B_k = k[T]b_1 + \cdots + k[T]b_s$. Fix an extension L/k and denote the integral closure of $L[T]$ in the *compositum* EL by B_L.

As our base field k is perfect, the extension L/k is separable (in the sense of not necessarily algebraic extensions; see *e.g.* [Lan02, chapter VIII, §4]). Then the morphism $\mathrm{Spec}\, L \to \mathrm{Spec}\, k$ is normal (as said in [Gro65, page 173]). We claim that this is also true of the morphism $\mathrm{Spec}\, L[T] \to \mathrm{Spec}\, k[T]$. Indeed one may assume that L is finitely generated over k and our claim then follows from [Gro65, proposition (6.8.3), statement (iii)]. Hence, from [Gro65, proposition (6.14.4)], we obtain $B_L = L[T]b_1 + \cdots + L[T]b_s$.

Then, with $P_1(T,Y)$ the polynomial introduced from the elements $b_1,\dots,b_s$ in the proof of proposition 2.1.3 and from statement $(*)$ there, any extension of L of group H which occurs as the specialization $(EL)_{t_0}/L$ of $EL/L(T)$ at t_0 with $t_0 \in L$ occurs as the splitting extension over L of the polynomial $P_1(t_0,Y)$. Do the same with the second polynomial $P_2(T,Y)$ to conclude.

To prove part (2), apply [JLY02, corollary 1.1.6] to conclude that $P_1(T,Y)$ (for example) is generic over k in the sense of Ledet, and even in the sense of Kemper (as k is infinite). □

Remark 2.1.7. (1) Part (1) holds with a single polynomial $P(T,Y)$ (with possibly $H \neq G$) if $E/k(T)$ has at least one k-rational branch point or if k is infinite and $E/k(T)$ has genus zero.

(2) One gets this trivial [3] counter-example to the converse in implication "generic ⇒ parametric":

Any G*-extension of* $\mathbb{R}(T)$ *of group* $\mathbb{Z}/4\mathbb{Z}$ *is* $\mathbb{Z}/4\mathbb{Z}$*-parametric but not* $\mathbb{Z}/4\mathbb{Z}$*-generic over* $\mathbb{R}$.

Indeed the existence of a $\mathbb{Z}/4\mathbb{Z}$-generic extension over $\mathbb{R}$ of group $\mathbb{Z}/4\mathbb{Z}$ would imply that of a one parameter generic polynomial over $\mathbb{R}$ for the group $\mathbb{Z}/4\mathbb{Z}$ in the sense of Ledet (part (2) of proposition 2.1.6), which cannot happen as explained in [Led].

We finally note that [Kem01] provides the following statement:

Proposition 2.1.8. *Let $P(T,Y) \in k[T][Y]$ be a monic separable polynomial of group G. Assume that k is infinite. Then one has the following conclusion: if $P(T,Y)$ satisfies condition $(*/G)$, then it satisfies condition $(*/H')$ for any subgroup $H' \subset G$.*

Proof. The proof consists in refining that of [Kem01, theorem 1]. Following the notation from there, it suffices to make the following adjustments to conclude.

(1) In the first display, one may add that the elements $h \in Z$ are distinct (from our assumption).

(2) In the second one, one may add that the set $\{(h-h')^{-1} \,/\, h \neq h' \in Z\}$ is also contained in S.

(3) In the third one, it suffices to show that the elements $\psi(h)$ $(h \in Z)$ are distinct. Let $(h,h') \in Z^2$ such that $h \neq h'$. Since one has $(h-h')\,(h-h')^{-1} = 1$ in S, one has then $(\psi(h)-\psi(h'))\,\psi((h-h')^{-1}) = 1$. Hence $\psi(h) \neq \psi(h')$. □

2.2 Parametric extensions over various fields

For this section, let $H \subset G$ be two finite groups. We investigate below H-parametric extensions of group G over various base fields k.

2.2.1 PAC fields

In the case k is a PAC [4] field, the situation is quite clear: [Dèb99c, theorem 3.2] (see also corollary 5.2.1) shows that any G-extension of $k(T)$ of group G (at least one such extension exists [FV91] [Pop96]) is parametric over k.

2.2.2 Finite fields

Since there are no (resp. only one) Galois extension of k of group H if H is not cyclic (resp. if H is cyclic), we trivially have that any G-extension of $k(T)$ of group G is H-parametric over k if H is not cyclic and H'-parametric over k for at least one cyclic subgroup $H' \subset G$.

Moreover [DG11, corollary 3.5] shows that any G-extension of $k(T)$ of group G with r branch points is parametric over k provided that $|k| \geq r^2\,|G|^2$ (see §4.2.2 for more details). As in addition

3. in the sense that there are no Galois extension of $\mathbb{R}$ of group $\mathbb{Z}/4\mathbb{Z}$.
4. See §B.2.1 for the definition and some examples of PAC fields.

the group G occurs as the Galois group of a G-extension of $k(T)$ provided that k is large enough (depending on G) [FV91] [Pop96] (see [DD97a, remark 3.9(a)] for more details), conclude that there exists at least one parametric extension over k of group G for large enough finite fields k.

In particular, we obtain the following non trivial counter-example to the converse in implication "generic $\Rightarrow$ parametric" in positive characteristic:

Example 2.2.1. Let $p \equiv 3 \bmod 4$ be a prime and $E/\mathbb{F}_p(T)$ be a G-extension of group $\mathbb{Z}/4\mathbb{Z}$ (at least one such extension exists for any prime p; see *e.g.* [Dèb09, theorem 2.3.7]). Denote its branch point number by r. Pick an odd integer n such that $p^n \geq 16r^2$. Then, as recalled above, the extension $E\mathbb{F}_{p^n}/\mathbb{F}_{p^n}(T)$ is $\mathbb{Z}/4\mathbb{Z}$-parametric over $\mathbb{F}_{p^n}$.

We show below that $E\mathbb{F}_{p^n}/\mathbb{F}_{p^n}(T)$ is not $\mathbb{Z}/4\mathbb{Z}$-generic over $\mathbb{F}_{p^n}$. As n is odd and $p \equiv 3 \bmod 4$, -1 is not a square in $\mathbb{F}_{p^n}$ and [Led] then provides the following:

There exist two scalar extensions $L_1/\mathbb{F}_{p^n}$, $L_2/\mathbb{F}_{p^n}$ and two Galois extensions F_1/L_1, F_2/L_2 of group $\mathbb{Z}/4\mathbb{Z}$ such that, for any monic separable polynomial $P(T,Y) \in \mathbb{F}_{p^n}[T][Y]$ of splitting field $E\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^n}(T)$, the following two conditions hold:

(1) *there exists some index $i \in \{1,2\}$ such that F_i/L_i is the splitting extension over L_i of the polynomial $P(t_0,Y)$ for no point $t_0 \in L_i$,*

(2) *given an index $i \in \{1,2\}$, if F_i/L_i occurs as the splitting extension over L_i of some specialized polynomial $P(t_0,Y)$ with $t_0 \in L_i$, then t_0 should be transcendental over $\mathbb{F}_{p^n}$.*

Assume by contradiction that $E\mathbb{F}_{p^n}/\mathbb{F}_{p^n}(T)$ is $\mathbb{Z}/4\mathbb{Z}$-generic over $\mathbb{F}_{p^n}$. For each index $i \in \{1,2\}$, fix $t_{0,i} \in \mathbb{P}^1(L_i)$ such that F_i/L_i is the specialization $(EL_i)_{t_{0,i}}/L_i$ of $EL_i/L_i(T)$ at $t_{0,i}$. Consider the polynomials $P_1(T,Y)$ and $P_2(T,Y)$ provided by the proof of proposition 2.1.3. If neither $t_{0,1} = \infty$ nor $t_{0,2} = \infty$, statement $(*)$ from there shows that, for each index $i \in \{1,2\}$, the extension F_i/L_i is the splitting extension over L_i of the polynomial $P_1(t_{0,i},Y)$ (as explained in the proof of part (1) of proposition 2.1.6). This contradicts condition (1) above. Hence one may assume that $t_{0,2} = \infty$. Statement $(**)$ from the proof of proposition 2.1.3 then shows that F_2/L_2 is the splitting extension over L_2 of $P_2(0,Y)$. One then obtains a contradiction from condition (2) above. Hence $E\mathbb{F}_{p^n}/\mathbb{F}_{p^n}(T)$ is not $\mathbb{Z}/4\mathbb{Z}$-generic over $\mathbb{F}_{p^n}$.

2.2.3 Formal Laurent series fields

Given an algebraically closed field κ of characteristic zero (and U an indeterminate), assume that k is the formal Laurent series field $\kappa((U))$.

As the only finite extensions of k are the cyclic ones $k(\sqrt[d]{U})/k$, $d \in \mathbb{N}\setminus\{0\}$ (this follows from the Puiseux theorem; see *e.g.* [Dèb09, theorem 3.1.1]), we trivially have that any G-extension of $k(T)$ of group G (at least one such extension exists [Pop96]) is H-parametric over k if H is not cyclic and H'-parametric over k for at least one cyclic subgroup $H' \subset G$. In the case G is the cyclic group $\mathbb{Z}/n\mathbb{Z}$ ($n \in \mathbb{N}\setminus\{0\}$), the G-extension $k(\sqrt[n]{T})/k(T)$ of group G is parametric over k (as noted in the presentation).

2.2.4 Completions of $\mathbb{Q}$

2.2.4.1. $k = \mathbb{Q}_p$. Since any finite Galois extension of $\mathbb{Q}_p$ is solvable, we trivially have that any G-extension of $\mathbb{Q}_p(T)$ of group G (at least one such extension exists [Har87]) is H-parametric over $\mathbb{Q}_p$ if H is not solvable.

If H is solvable, this does not hold in general. Indeed, given a G-extension $E/\mathbb{Q}(T)$ of group $\mathbb{Z}/8\mathbb{Z}$, the extension $E\mathbb{Q}_2/\mathbb{Q}_2(T)$ is not $\mathbb{Z}/8\mathbb{Z}$-parametric over $\mathbb{Q}_2$. Otherwise there exists some point $t_0 \in \mathbb{P}^1(\mathbb{Q}_2)$ such that $(E\mathbb{Q}_2)_{t_0}/\mathbb{Q}_2$ is the unique unramified extension of $\mathbb{Q}_2$ of degree 8.

From the Krasner lemma, one may assume that $t_0 \in \mathbb{P}^1(\mathbb{Q})$ and one then obtains a contradiction from [Wan48].

2.2.4.2. $k = \mathbb{R}$. Since the only finite extensions of $\mathbb{R}$ are the trivial one $\mathbb{R}/\mathbb{R}$ and the quadratic one $\mathbb{C}/\mathbb{R}$, we trivially have that any G-extension of $\mathbb{R}(T)$ of group G (at least one such extension exists (Hurwitz)) is H-parametric over $\mathbb{R}$ if neither $H = \{1\}$ nor $H = \mathbb{Z}/2\mathbb{Z}$, and is $\{1\}$-parametric or $\mathbb{Z}/2\mathbb{Z}$-parametric over $\mathbb{R}$. In particular, there exists at least one parametric extension over $\mathbb{R}$ of group G if G has odd order.

2.2.5 The field $\mathbb{Q}$

The situation in the case $k = \mathbb{Q}$ is more unclear.

2.2.5.1. Positive examples. If G is one of the four groups $\{1\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ or S_3, then there exists at least one parametric extension over $\mathbb{Q}$ of group G. This comes from the fact that these four groups (are the only ones to) have a one parameter generic polynomial over $\mathbb{Q}$ in the sense of Ledet [JLY02, page 194] (examples of such polynomials are recalled in the proof below).

Proposition 2.2.2. *The following three conditions are equivalent:*
(1) *there exists at least one generic extension over* $\mathbb{Q}$ *of group* G*,*
(2) *there exists at least one* G*-generic extension over* $\mathbb{Q}$ *of group* G*,*
(3) G *is one of the four groups* $\{1\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, S_3.

Proof. Implication (1) $\Rightarrow$ (2) is a consequence of definition 2.1.5. Assume that condition (2) holds. Then, from part (2) of proposition 2.1.6, there exists a one parameter generic polynomial over $\mathbb{Q}$ of group G in the sense of Ledet. Hence condition (3) holds [JLY02, page 194].

Assume now that condition (3) holds. Let $P(T,Y) = \dots$
(a) $\dots\ Y - T$ if $G = \{1\}$,
(b) $\dots\ Y^2 - T$ if $G = \mathbb{Z}/2\mathbb{Z}$,
(c) $\dots\ Y^3 - TY^2 + (T-3)Y + 1$ if $G = \mathbb{Z}/3\mathbb{Z}$,
(d) $\dots\ Y^3 + TY + T$ if $G = S_3$.
In each case, $P(T,Y)$ has Galois group G over $\mathbb{Q}(T)$ and is generic over $\mathbb{Q}$ in the sense of Ledet ([JLY02, §2.1] for cases (c) and (d)). Conjoining remark 2.1.2 and proposition 2.1.8 shows that $P(T,Y)$ satisfies condition $(*/H')$ of §2.1.2 for any subgroup $H' \subset G$. Hence the splitting extension $E/\mathbb{Q}(T)$ of $P(T,Y)$ over $\mathbb{Q}(T)$ is generic over $\mathbb{Q}$ (note that $E/\mathbb{Q}(T)$ is regular by [JLY02, proposition 3.3.8]). □

If G is none of the previous four groups, it is unknown whether there exists at least one G-parametric extension over $\mathbb{Q}$ of group G or not. In the case $H \neq G$, the proof of [Dèb09, proposition 3.2.4] shows that, for any abelian finite group G and any G-extension $E/\mathbb{Q}(T)$ of group G, there exists another one $E'/\mathbb{Q}(T)$ with the same group and the same branch point set, satisfying $E\overline{\mathbb{Q}} \simeq E'\overline{\mathbb{Q}}$ and with a trivial specialization, thus providing an H-parametric extension over $\mathbb{Q}$ of group G in the case $H = \{1\}$ and G abelian.

2.2.5.2. Negative examples. In addition to the example with $G = \mathbb{Z}/2\mathbb{Z}$ from the presentation, only a few negative examples are known.

(a) *An example of Beckmann.* No G-extension of $\mathbb{Q}(T)$ of group S_7 and branch point set $\{0, 1, \infty\}$ is S_7-parametric over $\mathbb{Q}$: [Bec94, example 1.1] shows indeed that the Galois extension of $\mathbb{Q}$ of group S_7 defined by the polynomial $P(Y) = Y^7 + 42482Y^6 + 5643Y^5 - 21164Y^4 + 2431Y^3 + 46189Y^2 + 46189Y + 46189$ cannot be a specialization of such an extension.

(b) G-*extensions with three branch points.* Given an integer $n \geq 2$, denote the dihedral group of order n by D_n. The statement below is [DF90, proposition 1.2]:

Proposition 2.2.3. *Assume that the following two conditions hold:*
(1) *there exists at least one totally real Galois extension of $\mathbb{Q}$ of group G,*
(2) *G is none of the four dihedral groups D_2, D_3, D_4, D_6.*
Then no G-*extension of $\mathbb{Q}(T)$ of group G with three branch points is G-parametric over $\mathbb{Q}$. In fact no totally real Galois extension of $\mathbb{Q}$ of group G* [5] *is a specialization of such an extension.*

Remark 2.2.4. (1) It is unknown whether there exists a finite group G which does not satisfy condition (1): according to a result of Serre [KM01, proposition 1], the existence of such a group would disprove the Inverse Galois Problem over $\mathbb{Q}$.

(2) For $G = D_3 = S_3$, the conclusion does not hold. Indeed it is easily checked from the Riemann-Hurwitz formula that any G-extension of $\mathbb{Q}(T)$ of group S_3 with three branch points has inertia canonical invariant $([1^1 2^1], [1^1 2^1], [3^1])$ (see §B.3.1 for the notation). Since S_3 has trivial center and this triple is a rigid one of rational conjugacy classes, there exists only one G-extension of $\mathbb{Q}(T)$ of group S_3 with three branch points (up to isomorphism), and it is that given by the trinomial $Y^3 + TY + T$, which is generic over $\mathbb{Q}$ (as recalled in the proof of proposition 2.2.2).

(3) Proposition 2.2.3 may be used to give some examples of non G-parametric extensions over $\mathbb{Q}$ of group G. For instance, pick an integer $n \geq 4$. Then each of the groups S_n and A_n satisfies conditions (1) and (2) of proposition 2.2.3 (*e.g.* [KM01, proposition 2 and corollary 4] for condition (1)). Hence each of the G-extensions of $\mathbb{Q}(T)$ with three branch points recalled in §B.3.1.2 and in §B.3.2 satisfies the conclusion of proposition 2.2.3.

2.3 First examples over $\mathbb{Q}$

This section is devoted to theorem 1 from the presentation. We use below *ad hoc* arguments to give some new examples of non H-parametric extensions over $\mathbb{Q}$ of group G. Our examples have $r \in \{2, 3, 4\}$ branch points (§2.3.2-2.3.4). We also discuss the case $r \geq 5$ in §2.3.5. We first give in §2.3.1 a general statement devoted to abelian groups which will be used in several occasions in the rest of this thesis.

2.3.1 Abelian groups

Let G be an abelian finite group, $E/\mathbb{Q}(T)$ be a G-extension of group G and $\mathbf{t}$ be its branch point set. Given a G-extension $\overline{E}/\overline{\mathbb{Q}}(T)$ of group G, call a G-extension $E'/\mathbb{Q}(T)$ of group G a $\mathbb{Q}$-G-*model of* $\overline{E}/\overline{\mathbb{Q}}(T)$ if $\overline{E}/\overline{\mathbb{Q}}(T)$ and $E'\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ are isomorphic.

Proposition 2.3.1. *The following two conditions are equivalent:*
(1) *any* $\mathbb{Q}$-G-*model of* $E\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ *with branch point set* $\mathbf{t}$ *is parametric over* $\mathbb{Q}$*,*
(2) *any* $\mathbb{Q}$-G-*model of* $E\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ *with branch point set* $\mathbf{t}$ *is* $\{1\}$-*parametric over* $\mathbb{Q}$*.*

Proof. Implication (1) $\Rightarrow$ (2) is a consequence of definition 2.1.1. The converse follows from the "twisting operation" of [Dèb99c, §2] (see also [DG12, §2.2] and part III for more general versions). As the abelian case is in some sense particular [6], we redetail it below.

5. It seems that this remains true for any arbitrary subgroup of G.
6. in the sense that the twisted extensions still are G-extensions.

Fix a $\mathbb{Q}$-G-model $E'/\mathbb{Q}(T)$ of $E\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ with branch point set $\mathbf{t}$, a subgroup $H \subset G$ and a Galois extension $F/\mathbb{Q}$ of group H. Denote the π_1-representation corresponding to $E'/\mathbb{Q}(T)$ by $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\mathbb{Q}} \to G$ and the G-Galois representation of $F/\mathbb{Q}$ (relative to $\overline{\mathbb{Q}}$) by $\varphi : \mathrm{G}_{\mathbb{Q}} \to H$.

With r the restriction $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\mathbb{Q}} \to \mathrm{G}_{\mathbb{Q}}$, consider the map $\widetilde{\phi}^{\varphi} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\mathbb{Q}} \to G$ defined by the following formula: $\widetilde{\phi}^{\varphi} = \phi - \varphi \circ r$. It is easily checked that $\widetilde{\phi}^{\varphi}$ is a group homomorphism (since G is abelian) with the same restriction to the fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{\mathbb{Q}}}$ as ϕ. This shows that $\widetilde{\phi}^{\varphi}$ is the π_1-representation of some $\mathbb{Q}$-G-model of $E\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ with branch point set $\mathbf{t}$; we denote it by $\widetilde{E'}^{\varphi}/\mathbb{Q}(T)$.

From condition (2), there exists some point $t_0 \in \mathbb{P}^1(\mathbb{Q}) \setminus \mathbf{t}$ such that $(\widetilde{E'}^{\varphi})_{t_0} = \mathbb{Q}$. Hence, with $\mathsf{s}_{t_0} : \mathrm{G}_{\mathbb{Q}} \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\mathbb{Q}}$ the section associated with t_0, the G-specialization representation $\widetilde{\phi}^{\varphi} \circ \mathsf{s}_{t_0} : \mathrm{G}_{\mathbb{Q}} \to G$ of $\widetilde{E'}^{\varphi}/\mathbb{Q}(T)$ at t_0, which is the action of $\mathrm{G}_{\mathbb{Q}}$ on the fiber above t_0, is the trivial morphism, *i.e.* one has $\widetilde{\phi}^{\varphi} \circ \mathsf{s}_{t_0}(\tau) = 0$ for any $\tau \in \mathrm{G}_{\mathbb{Q}}$. Then $\phi \circ \mathsf{s}_{t_0} = \varphi$. Conclude that the fields E'_{t_0} and F coincide. □

2.3.2 The case $r = 2$

We study below the situation of G-extensions of $\mathbb{Q}(T)$ with $r = 2$ branch points. We first determine all finite groups which occur as the Galois group of such an extension:

Lemma 2.3.2. *Let G be a finite group. Then the following two conditions are equivalent:*
(1) *G occurs as the Galois group of a* G*-extension of $\mathbb{Q}(T)$ with two branch points,*
(2) *$G = \mathbb{Z}/n\mathbb{Z}$ with $n \in \{2, 3, 4, 6\}$.*

Proof. Implication (2) $\Rightarrow$ (1) easily follows from [Des95, lemma 2.1.3].

For the converse, we first note that G should be cyclic; set $G = \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{a_s}\mathbb{Z}$, where $p_1, \dots, p_s$ are distinct prime numbers and $a_1, \dots, a_s$ are positive integers. As a classical consequence of the branch cycle lemma (*e.g.* [Dèb09, proposition 3.1.19]), one has $p_i^{a_i-1}(p_i-1) \leq 2$ for each index $i \in \{1, \dots, s\}$. Hence either one of the following two conditions holds:
- $s = 1$ and $G = \mathbb{Z}/n\mathbb{Z}$ with $n \in \{2, 3, 4\}$,
- $s = 2$ and $G = \mathbb{Z}/n\mathbb{Z}$ with $n \in \{6, 12\}$.

As the branch points t_1 and t_2 of any G-extension of $\mathbb{Q}(T)$ of group $\mathbb{Z}/3\mathbb{Z}$ (resp. of group $\mathbb{Z}/4\mathbb{Z}$) with two branch points should satisfy $\mathbb{Q}(t_1, t_2) = \mathbb{Q}(i\sqrt{3})$ (resp. $\mathbb{Q}(t_1, t_2) = \mathbb{Q}(i)$) [Des95, lemma 2.1.2], the case $n = 12$ cannot happen. Indeed, if $E/\mathbb{Q}(T)$ is a G-extension of group $\mathbb{Z}/12\mathbb{Z}$ with two branch points t_1 and t_2, then $E^{\mathbb{Z}/4\mathbb{Z}}/\mathbb{Q}(T)$ has Galois group $\mathbb{Z}/3\mathbb{Z}$ and branch point set $\{t_1, t_2\}$. Hence $\mathbb{Q}(t_1, t_2) = \mathbb{Q}(i\sqrt{3})$. One similarly obtains $\mathbb{Q}(t_1, t_2) = \mathbb{Q}(i)$ (by considering $E^{\mathbb{Z}/3\mathbb{Z}}/\mathbb{Q}(T)$ instead of $E^{\mathbb{Z}/4\mathbb{Z}}/\mathbb{Q}(T)$); a contradiction. □

2.3.2.1. The case $n = 2$. Proposition 2.3.3 below provides an explicit description of $\mathbb{Z}/2\mathbb{Z}$-parametric extensions over $\mathbb{Q}$ with the same group and two branch points:

Proposition 2.3.3. *Let $E/\mathbb{Q}(T)$ be a* G*-extension of group $\mathbb{Z}/2\mathbb{Z}$ with two branch points. Then the following three conditions are equivalent:*
(1) *$E/\mathbb{Q}(T)$ is parametric over $\mathbb{Q}$,*
(2) *$E/\mathbb{Q}(T)$ is $\mathbb{Z}/2\mathbb{Z}$-parametric over $\mathbb{Q}$,*
(3) *each branch point is $\mathbb{Q}$-rational.*

Remark 2.3.4. By using proposition 2.3.1, some non $\{1\}$-parametricity condition can be added in proposition 2.3.3 in the following way.

Let t_1 and t_2 be two distinct points in $\mathbb{P}^1(\overline{\mathbb{Q}})$ such that $\{t_1, t_2\}$ is invariant under the action of $\mathrm{G}_{\mathbb{Q}}$. Assume that neither t_1 nor t_2 is $\mathbb{Q}$-rational. Then, from proposition 2.3.3, no G-extension of $\mathbb{Q}(T)$ of group $\mathbb{Z}/2\mathbb{Z}$ with branch point set $\{t_1, t_2\}$ is $\mathbb{Z}/2\mathbb{Z}$-parametric over $\mathbb{Q}$. Conjoining this fact and proposition 2.3.1 shows that at least one of these G-extensions is in addition non $\{1\}$-parametric over $\mathbb{Q}$.

To prove proposition 2.3.3, we need lemma 2.3.5 below which will be used in several occasions in the rest of this thesis. Given a field k of characteristic zero, we first remark that any G-extension $E/k(T)$ of group $\mathbb{Z}/2\mathbb{Z}$ is given by a polynomial $P(T) \in k[T]$ which is separable over k (namely $E = k(T)(\sqrt{P(T)})$) and *vice-versa*.

Lemma 2.3.5. *Let k be a field of characteristic zero, $P(T) \in k[T]$ be a separable polynomial over k, n be its degree and $\{t_1, \dots, t_n\}$ be its root set. Then the branch point set $\mathbf{t}$ of the G-extension $k(T)(\sqrt{P(T)})/k(T)$ of group $\mathbb{Z}/2\mathbb{Z}$ is*
(1) $\mathbf{t} = \{t_1, \dots, t_n\}$ *if n is even,*
(2) $\mathbf{t} = \{t_1, \dots, t_n\} \cup \{\infty\}$ *if n is odd.*

In particular, by conjoining proposition 2.3.3 and lemma 2.3.5, we reobtain that $\mathbb{Q}(\sqrt{T})/\mathbb{Q}(T)$ (resp. $\mathbb{Q}(T)(\sqrt{T^2+1})/\mathbb{Q}(T)$) is parametric (resp. is not $\mathbb{Z}/2\mathbb{Z}$-parametric) over $\mathbb{Q}$.

Proof. Denote the integral closure of $\overline{k}[T]$ in $E\overline{k}$ by $\overline{B}$. We show below that $\overline{B} = \overline{k}[T] + \overline{k}[T]\sqrt{P(T)}$. Hence $\mathbf{t} = \{t_1, \dots, t_n\}$ or $\mathbf{t} = \{t_1, \dots, t_n\} \cup \{\infty\}$. By the Riemann-Hurwitz formula, the branch point number of $k(T)(\sqrt{P(T)})/k(T)$ is even and the conclusion easily follows.

Let $x \in \overline{B}$ and set $x = a(T) + b(T)\sqrt{P(T)}$ with $a(T)$ and $b(T)$ in $\overline{k}(T)$. Then $-2a(T)$ and $a^2(T) - b^2(T)P(T)$ are polynomials with coefficients in $\overline{k}$, and this also holds for $b^2(T)P(T)$. Set $b(T) = u(T)/v(T)$ with $u(T)$ and $v(T)$ two relatively prime polynomials with coefficients in $\overline{k}$. Then there exists some polynomial $r(T) \in \overline{k}[T]$ such that $u^2(T)P(T) = r(T)v^2(T)$. Since $u(T)$ and $v(T)$ are relatively prime and $P(T)$ is separable over k, $v(T)$ is necessarily constant and then $b(T) \in \overline{k}[T]$, thus ending the proof. □

As a consequence, proposition 2.3.3 may be rephrased as follows:

Let a, b and c be three rational numbers such that $b^2 - 4ac \neq 0$. Then the following three conditions are equivalent:
(1') *the G-extension $\mathbb{Q}(T)(\sqrt{aT^2+bT+c})/\mathbb{Q}(T)$ is parametric over $\mathbb{Q}$,*
(2') *the G-extension $\mathbb{Q}(T)(\sqrt{aT^2+bT+c})/\mathbb{Q}(T)$ is $\mathbb{Z}/2\mathbb{Z}$-parametric over $\mathbb{Q}$,*
(3') *$b^2 - 4ac$ is a square in $\mathbb{Q}$.*

Proof of proposition 2.3.3. Set $E = \mathbb{Q}(T)(\sqrt{aT^2+bT+c})$. We successively prove implications (3') ⇒ (1'), (1') ⇒ (2') and (2') ⇒ (3'). Furthermore the proof will show the following:

(a) *if condition (3') is satisfied, then any quadratic or trivial extension of $\mathbb{Q}$ is the splitting extension over $\mathbb{Q}$ of some specialized polynomial $Y^2 - (at_0^2 + bt_0 + c)$ with $t_0 \in \mathbb{Q}$,*

(b) *if condition (3') is not satisfied, then there exist infinitely many distinct quadratic extensions of $\mathbb{Q}$ which each are not a specialization of $E/\mathbb{Q}(T)$.*

(3') ⇒ (1'). Assume first that condition (3') holds. Let $t_1 \in \mathbb{Q}$ be a root of $aT^2 + bT + c$ and $F/\mathbb{Q}$ be a quadratic or trivial extension. Set $F = \mathbb{Q}(\sqrt{d})$ with d a non-zero integer.

The curve defined by the equation $dY^2 = aT^2 + bT + c$ has a (non singular) $\mathbb{Q}$-rational point (for example $(0, t_1)$). Being of genus 0, it is then birational to $\mathbb{P}^1$ over $\mathbb{Q}$. Then there exist two rational numbers y and t_0 such that $y \neq 0$ and $dy^2 = at_0^2 + bt_0 + c$. Hence one has

$F = \mathbb{Q}(\sqrt{at_0^2 + bt_0 + c})$, *i.e.* $F/\mathbb{Q}$ is the splitting extension over $\mathbb{Q}$ of the specialized polynomial $Y^2 - (at_0^2 + bt_0 + c)$ (and so statement (a) holds). Since this polynomial is separable over $\mathbb{Q}$, one may apply lemma B.1.2 and conclude that $F/\mathbb{Q}$ is the specialization $E_{t_0}/\mathbb{Q}$ of $E/\mathbb{Q}(T)$ at t_0.

(1') ⇒ (2'). This is a consequence of definition 2.1.1.

(2') ⇒ (3'). Assume now that condition (2') holds. There are three steps to show that $b^2 - 4ac$ is a square in $\mathbb{Q}$.

- *First step*: $a \in \mathbb{Z} \setminus \{0\}$, $b = 0$ and $c \in \mathbb{Z} \setminus \{0\}$. Remark first that ∞ is not a branch point of $E/\mathbb{Q}(T)$ since $a \neq 0$ (lemma 2.3.5).

Let p be a prime number such that neither a nor c is a multiple of p and p does not ramify in $E_\infty/\mathbb{Q}$. From condition (2'), there exists some rational number t_0 such that $E_{t_0} = \mathbb{Q}(\sqrt{p})$, *i.e.* $\mathbb{Q}(\sqrt{at_0^2 + c}) = \mathbb{Q}(\sqrt{p})$ (lemmas B.1.2 and 2.3.5). Hence there exists some non-zero rational number λ such that $p\lambda^2 = at_0^2 + c$. Then there exist three non-zero integers u, v and w such that $pu^2 = av^2 + cw^2$ and one may assume that w is not a multiple of p (otherwise v and u are also multiples of p and, with n the p-adic valuation of w, one may then replace (u, v, w) by $(u/p^n, v/p^n, w/p^n)$). By reducing modulo p, $-ac$ is a square modulo p.

Hence $Y^2 + 4ac$ has a root modulo p for all but finitely many primes p (note that this also holds if we only assume that all but finitely many quadratic extensions of $\mathbb{Q}$ are a specialization of $E/\mathbb{Q}(T)$, so proving statement (b)). From *e.g.* [Hei67, theorem 9] [7], $-4ac$ is a square in $\mathbb{Q}$.

- *Second step:* $(a, b, c) \in \mathbb{Z}^3$. Condition (3') trivially holds if $a = 0$ or $c = 0$. So assume that $a \neq 0$ and $c \neq 0$. Set $\Delta = b^2 - 4ac$.

Let p be a prime number such that neither a nor Δ is a multiple of p and p does not ramifiy in $E_\infty/\mathbb{Q}$. From condition (2'), there exists some rational number t_0 such that $\mathbb{Q}(\sqrt{p})/\mathbb{Q} = E_{t_0}/\mathbb{Q}$, *i.e.* $\mathbb{Q}(\sqrt{p}) = \mathbb{Q}(\sqrt{at_0^2 + bt_0 + c})$. Set $t'_0 = 2at_0 + b$. Since $at_0'^2 - a\Delta = 4a^2(at_0^2 + bt_0 + c)$, one has $\mathbb{Q}(\sqrt{at_0^2 + bt_0 + c}) = \mathbb{Q}(\sqrt{at_0'^2 - a\Delta})$. From the first step, $4a^2\Delta$ is a square in $\mathbb{Q}$ and so is Δ too.

- *Third step:* $(a, b, c) \in \mathbb{Q}^3$. Set $a = a_1/a_2$, $b = b_1/b_2$ and $c = c_1/c_2$ with integers $a_1, a_2, b_1, b_2, c_1, c_2$ such that $(a_1, a_2) = (b_1, b_2) = (c_1, c_2) = 1$.

Since $a_2^2\, b_2^2\, c_2^2\, (a\, T^2 + b\, T + c) = a_1\, a_2\, b_2^2\, c_2^2\, T^2 + b_1\, b_2\, a_2^2\, c_2^2\, T + \, c_1\, c_2\, a_2^2\, b_2^2$, one has

$$E = \mathbb{Q}(T)(\sqrt{a_1\, a_2\, b_2^2\, c_2^2\, T^2 + b_1\, b_2\, a_2^2\, c_2^2\, T + \, c_1\, c_2\, a_2^2\, b_2^2})$$

From the second step, the discriminant $b_1^2\, b_2^2\, a_2^4\, c_2^4 - 4\, a_1\, c_1\, a_2^3\, c_2^3\, b_2^4 = (a_2\, b_2\, c_2)^4 (b^2 - 4\, ac)$ is a square in $\mathbb{Q}$. Hence condition (3') holds. □

Remark 2.3.6. (1) The proof of implication (3') ⇒ (1') shows that implication (3) ⇒ (1) holds with the field $\mathbb{Q}$ replaced by any field k of characteristic zero. In particular, this shows that the three conditions (1), (2) and (3) are equivalent to the following two ones:

(4) *$E/\mathbb{Q}(T)$ is $\mathbb{Z}/2\mathbb{Z}$-generic over $\mathbb{Q}$,*

(5) *$E/\mathbb{Q}(T)$ is generic over $\mathbb{Q}$.*

(2) By proceeding as in the proof of implication (2') ⇒ (3'), one can also determine whether a given G-extension $E/\mathbb{Q}(T) = \mathbb{Q}(T)(\sqrt{aT^2 + bT + c})/\mathbb{Q}(T)$ of group $\mathbb{Z}/2\mathbb{Z}$ with two branch points is $\{1\}$-parametric over $\mathbb{Q}$ or not.

Indeed note first that the answer obviously is positive if $a = 0$. In the case $a \neq 0$, one may assume as in the proof of proposition 2.3.3 that $b = 0$ and $c \neq 0$. Then the G-extension $E/\mathbb{Q}(T)$ has at least one trivial specialization if and only if there exists some triple $(u, v, w) \in$

7. It seems that more elementary proofs exist in the quadratic case.

$\mathbb{Q}^3 \setminus \{(0,0,0)\}$ such that $au^2+cv^2=w^2$. From the Hasse-Minkowski theorem (*e.g.* [Ser70, chapter IV, theorem 8]), the existence of such a triple of rational numbers is equivalent to the fact that, for any prime p (possibly infinite), the *Hilbert symbol* (a,c) of a and c (viewed as elements of $\mathbb{Q}_p$ [8]) be equal to 1. Using *e.g.* [Ser70, chapter III, theorem 1] makes it possible to make this last condition totally explicit.

2.3.2.2. The case $n=6$. Proposition 2.3.7 below follows from proposition 2.3.3:

Proposition 2.3.7. *Let $E/\mathbb{Q}(T)$ be a* G*-extension of group $\mathbb{Z}/6\mathbb{Z}$ with two branch points and $m \in \{2,6\}$. Then there are infinitely many distinct Galois extensions of $\mathbb{Q}$ of group $\mathbb{Z}/m\mathbb{Z}$ which each are not a specialization of $E/\mathbb{Q}(T)$. In particular, $E/\mathbb{Q}(T)$ is not $\mathbb{Z}/m\mathbb{Z}$-parametric over $\mathbb{Q}$.*

Proof. Consider first the case $m=6$ and assume by contradiction that all but finitely many Galois extensions of $\mathbb{Q}$ of group $\mathbb{Z}/6\mathbb{Z}$ are a specialization of $E/\mathbb{Q}(T)$. Let $F_2/\mathbb{Q}$ be a quadratic extension. Up to excluding finitely many of them, one may assume that there exists at least one extension $F_3/\mathbb{Q}$ of group $\mathbb{Z}/3\mathbb{Z}$ such that the *compositum* $F_2F_3/\mathbb{Q}$ is a specialization of $E/\mathbb{Q}(T)$. Fix such an extension $F_3/\mathbb{Q}$ and pick $t_0 \in \mathbb{P}^1(\mathbb{Q})$ such that $F_2F_3 = E_{t_0} = (E^{\mathbb{Z}/3\mathbb{Z}}E^{\mathbb{Z}/2\mathbb{Z}})_{t_0}$. As $E_{t_0}/\mathbb{Q}$ has Galois group $\mathbb{Z}/6\mathbb{Z}$, the extension $(E^{\mathbb{Z}/3\mathbb{Z}})_{t_0}/\mathbb{Q}$ (resp. $(E^{\mathbb{Z}/2\mathbb{Z}})_{t_0}/\mathbb{Q}$) has Galois group $\mathbb{Z}/2\mathbb{Z}$ (resp. $\mathbb{Z}/3\mathbb{Z}$) and then $(E^{\mathbb{Z}/3\mathbb{Z}}E^{\mathbb{Z}/2\mathbb{Z}})_{t_0} = (E^{\mathbb{Z}/3\mathbb{Z}})_{t_0}(E^{\mathbb{Z}/2\mathbb{Z}})_{t_0}$. Hence $(E^{\mathbb{Z}/3\mathbb{Z}})_{t_0}/\mathbb{Q}$ (resp. $(E^{\mathbb{Z}/2\mathbb{Z}})_{t_0}/\mathbb{Q}$) coincide with $F_2/\mathbb{Q}$ (resp. with $F_3/\mathbb{Q}$).

Then all but finitely many quadratic extensions of $\mathbb{Q}$ are a specialization of $E^{\mathbb{Z}/3\mathbb{Z}}/\mathbb{Q}(T)$. From statement (b) of the proof of proposition 2.3.3, each of the two branch points of $E/\mathbb{Q}(T)$ should be $\mathbb{Q}$-rational. Hence $E^{\mathbb{Z}/2\mathbb{Z}}/\mathbb{Q}(T)$ is a G-extension of group $\mathbb{Z}/3\mathbb{Z}$ with two branch points which each are $\mathbb{Q}$-rational, which cannot happen (as noted in the proof of lemma 2.3.2).

The case $m=2$ is quite similar. Assume by contradiction that all but finitely many quadratic extensions of $\mathbb{Q}$ are a specialization of $E/\mathbb{Q}(T)$. Let $F_2/\mathbb{Q}$ be such a quadratic extension. Then there exists some point $t_0 \in \mathbb{P}^1(\mathbb{Q})$ such that $F_2 = E_{t_0} = (E^{\mathbb{Z}/3\mathbb{Z}}E^{\mathbb{Z}/2\mathbb{Z}})_{t_0}$. As $E_{t_0}/\mathbb{Q}$ has Galois group $\mathbb{Z}/2\mathbb{Z}$, one has $(E^{\mathbb{Z}/3\mathbb{Z}})_{t_0} = F_2$ (and $(E^{\mathbb{Z}/2\mathbb{Z}})_{t_0} = \mathbb{Q}$). Hence all but finitely many quadratic extensions of $\mathbb{Q}$ are a specialization of $E^{\mathbb{Z}/3\mathbb{Z}}/\mathbb{Q}(T)$. Conclude as in the case $m=6$. □

Remark 2.3.8. Denote the unique (up to isomorphism) G-extension of $\overline{\mathbb{Q}}(T)$ of group $\mathbb{Z}/6\mathbb{Z}$ with two branch points by $\overline{E}/\overline{\mathbb{Q}}(T)$ (Riemann's existence theorem). Then it has several $\mathbb{Q}$-G-models (up to isomorphism).

Indeed conjoining propositions 2.3.1 and 2.3.7 provides a $\mathbb{Q}$-G-model of $\overline{E}/\overline{\mathbb{Q}}(T)$ which is not $\{1\}$-parametric over $\mathbb{Q}$. As there exists at least one $\mathbb{Q}$-G-model of $\overline{E}/\overline{\mathbb{Q}}(T)$ which is $\{1\}$-parametric over $\mathbb{Q}$ (as recalled in §2.2.5.1), the conclusion follows.

2.3.2.3. The two cases $n=4$ and $n=3$. The case $n=4$ will be solved in chapter 3. More precisely, we will prove the analog of proposition 2.3.7 (part (2) of corollary 3.3.6). In particular, remark 2.3.8 holds with the group $\mathbb{Z}/6\mathbb{Z}$ replaced by $\mathbb{Z}/4\mathbb{Z}$.

The case $n=3$ is more unclear. To our knowledge, it is unknown whether there exists only one G-extension of $\mathbb{Q}(T)$ of group $\mathbb{Z}/3\mathbb{Z}$ with two branch points or not (note that this is true over $\overline{\mathbb{Q}}$), in which case it would be given by the polynomial $Y^3 - TY^2 + (T-3)Y + 1$ and would be generic over $\mathbb{Q}$ (as recalled in the proof of proposition 2.2.2). Note also that it seems unknown whether there is at least one non $\mathbb{Z}/3\mathbb{Z}$-parametric extension over $\mathbb{Q}$ with the same group or not.

2.3.3 An example with $r=3$

As for any abelian group, the Beckmann-Black problem for $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ over $\mathbb{Q}$ has a positive answer: any Galois extension $F/\mathbb{Q}$ of group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ has a lifting extension $E_F/\mathbb{Q}(T)$ with

8. Set $\mathbb{Q}_\infty = \mathbb{R}$ if $p=\infty$.

the same group. Moreover [Bec94, corollary 2.4] shows that the extension $E_F/\mathbb{Q}(T)$ may be chosen with three branch points.

Proposition 2.3.9 below shows however that none of these lifting extensions $E_F/\mathbb{Q}(T)$ with three branch points is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-parametric over $\mathbb{Q}$:

Proposition 2.3.9. *Let $E/\mathbb{Q}(T)$ be a* G*-extension of group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with three branch points. Then there exist infinitely many distinct Galois extensions of $\mathbb{Q}$ of group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ which each are not a specialization of $E/\mathbb{Q}(T)$* [9].

This statement shows in particular that remark 2.3.8 holds with the group $\mathbb{Z}/6\mathbb{Z}$ replaced by $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the branch point number two by three. Moreover it provides some complement to proposition 2.2.3.

Proof. Let $P_1(T)$ and $P_2(T)$ be two distinct separable polynomials over $\mathbb{Q}$ such that $E = \mathbb{Q}(T)(\sqrt{P_1(T)}, \sqrt{P_2(T)})$.

Given an index $i \in \{1, 2\}$, it follows from the G-extension $E/\mathbb{Q}(T)$ having three branch points and the G-extension $\mathbb{Q}(T)(\sqrt{P_i(T)})/\mathbb{Q}(T)$ having an even branch point number (lemma 2.3.5) that the latter has two branch points. Consequently each branch point of $E/\mathbb{Q}(T)$ is $\mathbb{Q}$-rational. Hence we may assume that these branch points are 0, 1 and ∞. In particular, there exist two non-zero squarefree integers a and b such that $E = \mathbb{Q}(T)(\sqrt{a\,T}, \sqrt{b\,T - b})$ (lemma 2.3.5).

Fix two distinct squarefree integers d_1, d_2 and assume that $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) = \mathbb{Q}(\sqrt{a\,t_0}, \sqrt{b\,t_0 - b})$ for some $t_0 \in \mathbb{Q} \setminus \{0, 1\}$. Then the quadratic subextensions coincide and one of the following six conditions holds:
(i) $a\,d_1\,t_0 \in \mathbb{Q}^2$ and $d_2\,(b\,t_0 - b) \in \mathbb{Q}^2$,
(ii) $a\,d_1\,t_0 \in \mathbb{Q}^2$ and $d_1\,d_2\,(b\,t_0 - b) \in \mathbb{Q}^2$,
(iii) $a\,d_2\,t_0 \in \mathbb{Q}^2$ and $d_1\,(b\,t_0 - b) \in \mathbb{Q}^2$,
(iv) $a\,d_2\,t_0 \in \mathbb{Q}^2$ and $d_1\,d_2\,(b\,t_0 - b) \in \mathbb{Q}^2$,
(v) $a\,d_1\,d_2\,t_0 \in \mathbb{Q}^2$ and $d_1\,(b\,t_0 - b) \in \mathbb{Q}^2$,
(vi) $a\,d_1\,d_2\,t_0 \in \mathbb{Q}^2$ and $d_2\,(b\,t_0 - b) \in \mathbb{Q}^2$.
Hence one of the following six equations has a non trivial solution, *i.e.* a solution $(u, v, w) \in \mathbb{Z}^3$ such that $uvw \neq 0$:
(i) $a\,d_1\,U^2 - b\,d_2\,V^2 - W^2 = 0$,
(ii) $a\,U^2 - b\,d_2\,V^2 - d_1\,W^2 = 0$,
(iii) $a\,d_2\,U^2 - b\,d_1\,V^2 - W^2 = 0$,
(iv) $a\,U^2 - b\,d_1V^2 - d_2\,W^2 = 0$,
(v) $a\,d_2U^2 - b\,V^2 - d_1\,W^2 = 0$,
(vi) $a\,d_1\,U^2 - b\,V^2 - d_2\,W^2 = 0$.
We show below that there exist infinitely many distinct couples (d_1, d_2) of distinct squarefree integers such that none of these six equations has a non trivial solution. In particular, the conclusion holds (lemma B.1.2).

One may assume that $a > 0$ or $b < 0$ (otherwise take $d_1 > 0$ and $d_2 > 0$ to conclude). Assume for example that $a > 0$ and $b > 0$ (the other two cases for which ($a > 0$ and $b < 0$) or ($a < 0$ and $b < 0$) are quite similar).

Assume first that the squarefree integer b satisfies $b \neq 1$. Fix a squarefree integer $d_2 > 0$ such that neither $a\,b\,d_2$ nor $a\,d_2$ is a square in $\mathbb{Q}$. Since $b \neq 1$, the two quadratic fields $\mathbb{Q}(\sqrt{a\,b\,d_2})$ and $\mathbb{Q}(\sqrt{a\,d_2})$ are distinct. Hence there exist infinitely many distinct prime numbers p such that neither $a\,b\,d_2$ nor $a\,d_2$ is a square modulo p (*e.g.* [Nag69, theorem 7]). Then, for such a prime

9. In particular, $E/\mathbb{Q}(T)$ is not $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-parametric over $\mathbb{Q}$.

p, none of the previous six equations with $d_1 = -p$ has a non trivial solution, *i.e.* none of the following six equations has a non trivial solution:
(i) $-a\,p\,U^2 - b\,d_2\,V^2 - W^2 = 0$,
(ii) $a\,U^2 - b\,d_2\,V^2 + p\,W^2 = 0$,
(iii) $a\,d_2\,U^2 + p\,b\,V^2 - W^2 = 0$,
(iv) $a\,U^2 + p\,b\,V^2 - d_2\,W^2 = 0$,
(v) $a\,d_2\,U^2 - b\,V^2 + p\,W^2 = 0$,
(vi) $-a\,p\,U^2 - b\,V^2 - d_2\,W^2 = 0$.
Indeed note first that neither equation (i) nor equation (vi) has such a solution (as all coefficients are negative). If one of equations (ii)-(v) has such a solution (u, v, w), one may assume that u is not a multiple p (otherwise v and w are also multiples of p and, with n the p-adic valuation of u, one may then replace (u, v, w) by $(u/p^n, v/p^n, w/p^n)$). By reducing modulo p, either $a\,d_2$ or $a\,b\,d_2$ is a square modulo p; a contradiction.

Assume now that $b = 1$. Fix a squarefree integer $d_2 > 0$ such that $a\,d_2$ is not a square in $\mathbb{Q}$. Hence there exist infinitely many distinct primes p such that $a\,d_2$ is not a square modulo p (*e.g.* [Hei67, theorem 9]). Then, for such a prime p, a similar argument as that in the case $b \neq 1$ shows that none of the previous six equations with $d_1 = -p$ has a non trivial solution. □

Remark 2.3.10. The proof and proposition 2.3.3 show in particular that any quadratic subextension of $E/\mathbb{Q}(T)$ is parametric (in fact generic; see part (1) of remark 2.3.6) over $\mathbb{Q}$. However their *compositum* is not $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-parametric over $\mathbb{Q}$.

2.3.4 An example with $r = 4$

Proposition 2.3.11. *Let E be the splitting field over $\mathbb{Q}(T)$ of the trinomial $Y^3 + T^2Y + T^2$. Then $E/\mathbb{Q}(T)$ is a* G*-extension of group S_3, with four branch points and which is H-parametric over $\mathbb{Q}$ for no subgroup $H \subset S_3$. More precisely, given a non trivial subgroup $H \subset S_3$, there exist infinitely many distinct Galois extensions of $\mathbb{Q}$ of group H which each are not a specialization of $E/\mathbb{Q}(T)$.*

In particular, conjoining proposition 2.3.3, this statement and part (3) of remark 2.2.4 provides an example of non S_n-parametric extension over $\mathbb{Q}$ with the same group for each $n \geq 2$.

Proof. The trinomial $Y^3 + T^2Y + T^2$ is absolutely irreducible and its discriminant $\Delta(T) = -4T^6 - 27T^4$ is not a square in $\overline{\mathbb{Q}}(T)$. Then the extension $E/\mathbb{Q}(T)$ is regular over $\mathbb{Q}$ and one has $\mathrm{Gal}(E/\mathbb{Q}(T)) = S_3$. Moreover one easily shows that its branch point set $\mathbf{t}$ is contained in $\{0, 3i\sqrt{3}/2, -3i\sqrt{3}/2, \infty\}$. Hence $\mathbf{t}$ contains some $\mathbb{Q}$-rational point and the two complex conjugate points $3i\sqrt{3}/2$, $-3i\sqrt{3}/2$.

Assume that $E/\mathbb{Q}(T)$ has three branch points. The Riemann-Hurwitz formula then shows that it has genus 0. Then there exists some transcendental element U over $\mathbb{Q}$ such that $E\overline{\mathbb{Q}} = \overline{\mathbb{Q}}(U)$. Since S_3 is isomorphic to the finite group $\mathcal{D}$ generated by σ and τ such that $\tau(U) = 1/U$ and $\sigma(U) = e^{2i\pi/3}U$, one has $\overline{\mathbb{Q}}(T) = \overline{\mathbb{Q}}(U)^{\mathcal{D}} = \overline{\mathbb{Q}}(U^3 + U^{-3})$ (since U is a root ot the trinomial $Y^6 - (U^3 + U^{-3})Y^3 + 1$). Moreover the branch point set of $\overline{\mathbb{Q}}(U)/\overline{\mathbb{Q}}(U^3 + U^{-3})$ is contained in $\{-2, 2, \infty\}$. In particular, any branch point of $E\overline{\mathbb{Q}}(T)/\overline{\mathbb{Q}}(T)$ should be $\mathbb{Q}$-rational; a contradiction. Hence $E/\mathbb{Q}(T)$ has four branch points.

Given a non-zero rational number t_0, the specialized polynomial $Y^3 + t_0^2Y + t_0^2$ is separable over $\mathbb{Q}$ and, from lemma B.1.2, the specialization $E_{t_0}/\mathbb{Q}$ is its splitting extension over $\mathbb{Q}$. As this polynomial has only one real root, the specialization $E_{t_0}/\mathbb{Q}$ is not totally real. Hence the conclusion obviously holds for $H = \{1\}$ and $H = \mathbb{Z}/2\mathbb{Z}$. Moreover, as any finite Galois extension of $\mathbb{Q}$ of odd degree is totally real, the conclusion also holds for $H = \mathbb{Z}/3\mathbb{Z}$ [10]. Finally, since it is known that there exist infinitely many distinct totally real Galois extensions of $\mathbb{Q}$ of group S_3 (*e.g.* [KM01, proposition 2]), the conclusion is also true for $H = S_3$, thus ending the proof. □

2.3.5 The case $r \geq 5$

In this situation, it seems difficult to give similar examples. However one has the following general statement:

Let G be a finite group, H be a subgroup of G and $E/\mathbb{Q}(T)$ be a G-*extension of group G with $r \geq 5$ branch points. Then, given a Galois extension $F/\mathbb{Q}$ of group H, there exist only finitely many distinct points $t_0 \in \mathbb{P}^1(\mathbb{Q})$ (possibly none) such that the extension $F/\mathbb{Q}$ is the specialization $E_{t_0}/\mathbb{Q}$ of $E/\mathbb{Q}(T)$ at t_0.*

Indeed denote the genus of $E\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ by g, its degree by d and the ramified prime number of $E\overline{\mathbb{Q}}$ by $\mathcal{R}$. The Riemann-Hurwitz formula yields $2\mathrm{g} - 2 = -2d + rd - \mathcal{R}$. As $\mathcal{R} \leq rd/2$, one obtains $2\mathrm{g} \geq 2 + d((r/2) - 2)$. Hence $\mathrm{g} \geq 2$ and the conclusion then follows from the Faltings theorem as explained in [Dèb99c, §3.3.5] (see also §5.2.4.2).

10. In fact no Galois extension of $\mathbb{Q}$ of group $\mathbb{Z}/3\mathbb{Z}$ is a specialization of $E/\mathbb{Q}(T)$.

Chapter 3

Parametric extensions II

3.1 Criteria for non parametricity

This section is devoted to theorem 3.1.1 below which gives our most general criteria for a given G-extension of $k(T)$ not to be parametric over k; it is the aim of §3.1.1 and is proved in §3.1.3. We also give in §3.1.2 four more practical forms of this statement which each will be used in the next three sections to obtain new examples of such extensions over various base fields.

Here k is the quotient field of any Dedekind domain A of characteristic zero with infinitely many distinct primes. We next discuss in §3.1.4 the case A only has finitely many distinct primes.

3.1.1 General result

For §3.1.1-3.1.3, let A be a Dedekind domain of characteristic zero assumed to have infinitely many distinct prime ideals and k be its quotient field.

3.1.1.1. Notation. Let H be a non trivial finite group and $E_H/k(T)$ be a G-extension of group H, branch point set $\{t_{1,H}, \dots, t_{r_H,H}\}$ and inertia canonical invariant $(C_{1,H}, \dots, C_{r_H,H})$.

Recall some important notation from chapter 1. For each index $i \in \{1, \dots, r_H\}$, denote the irreducible polynomial of $t_{i,H}$ (resp. of $1/t_{i,H}$ [1]) over k by $m_{i,H}(T)$ (resp. by $m^*_{i,H}(T)$). Set $m_{i,H}(T) = 1$ if $t_{i,H} = \infty$ and $m^*_{i,H}(T) = 1$ if $t_{i,H} = 0$. Set finally $m_{E_H}(T) = \prod_{i=1}^{r_H} m_{i,H}(T)$ and $m^*_{E_H}(T) = \prod_{i=1}^{r_H} m^*_{i,H}(T)$.

Let G be a finite group containing H and $E_G/k(T)$ be a G-extension of group G. Define the same notation for $E_G/k(T)$. Moreover, given a conjugacy class C of H, denote the conjugacy class in G of elements of C by C^G.

3.1.1.2. Statement of the result. Consider the following two conditions:

(Branch Point Hypothesis) *there exist infinitely many distinct prime ideals of A which each are a prime divisor[2] of $m_{E_H}(T) \cdot m^*_{E_H}(T)$ but not of $m_{E_G}(T) \cdot m^*_{E_G}(T)$,*

(Inertia Hypothesis) *there exists some index $i \in \{1, \dots, r_H\}$ satisfying these two conditions:*

(a) *$m_{i,H}(T) \cdot m^*_{i,H}(T)$ has infinitely many distinct prime divisors,*

(b) *the set $\{C^a_{1,G}, \dots, C^a_{r_G,G} \,/\, a \in \mathbb{N}\}$ does not contain $C^G_{i,H}$.*

Theorem 3.1.1. *Under either one of these two conditions, the following non parametricity condition holds:*

1. Set $1/t_{i,H} = 0$ if $t_{i,H} = \infty$ and $1/t_{i,H} = \infty$ if $t_{i,H} = 0$.
2. See definition 1.2.10.

(non parametricity) *there exist infinitely many distinct finite Galois extensions of k which each are not a specialization of $E_G/k(T)$* [3].

Moreover these Galois extensions of k may be obtained by specializing $E_H/k(T)$.

Addendum 3.1.1. Furthermore under either one of the following two conditions:

(1) k is hilbertian,

(2) there exists some subset $I \subset \{1, \dots, r_H\}$ satisfying the following two conditions:

  (a) $m_{i,H}(T) \cdot m^*_{i,H}(T)$ has infinitely many distinct prime divisors for each index $i \in I$,

  (b) the set $\{C_{i,H} \,/\, i \in I\}$ is g-complete [4],

the following more precise non H-parametricity condition holds:

(non H-parametricity) *there exist infinitely many distinct Galois extensions of k of group H which each are not a specialization of $E_G/k(T)$.*

Moreover these Galois extensions of k of group H may be obtained by specializing $E_H/k(T)$ and, in the case the base field k is assumed to be hilbertian, they may be further required to be linearly disjoint.

3.1.2 Practical forms of theorem 3.1.1

Continue with the notation of §3.1.1.1. We now give four more practical forms of theorem 3.1.1. The first one rests on a sharp variant of the Branch Point Hypothesis and the other three ones each use the Inertia Hypothesis.

3.1.2.1. Branch Point Criterion. If $E_H/k(T)$ has at least one k-rational branch point $t_{i,H}$, then all but finitely many prime ideals of A obviously are a prime divisor of $m_{i,H}(T) \cdot m^*_{i,H}(T)$, and so of $m_{E_H}(T) \cdot m^*_{E_H}(T)$ too. Hence one obtains the following statement:

Branch Point Criterion. *The* (non H-parametricity) *condition* [5] *holds if the following three conditions are satisfied:*

(BPC-1) *k is a number field,*

(BPC-2) *$E_H/k(T)$ has at least one k-rational branch point,*

(BPC-3) *there exist infinitely many distinct prime ideals of A which each are not a prime divisor of $m_{E_G}(T) \cdot m^*_{E_G}(T)$.*

An obvious necessary condition for condition (BPC-3) to hold is that $E_G/k(T)$ has no k-rational branch point. Moreover condition (BPC-1) may be replaced by either one of the two conditions of addendum 3.1.1.

3.1.2.2. Inertia Criteria. Since part (b) of the Inertia Hypothesis does not depend on the base field k, one obtains the following three criteria in which the (non H-parametricity) condition remains true after any finite scalar extension, *i.e.* in which the following one holds:

(geometric non H-parametricity) *for any finite extension k'/k, there exist infinitely many distinct Galois extensions of k' of group H which each are not a specialization of $E_Gk'/k'(T)$.*

Moreover, given a finite extension k'/k, these Galois extensions of k' of group H may be obtained by specializing $E_Hk'/k'(T)$ and, in the case k is assumed to be hilbertian, they may be further required to be linearly disjoint.

3. In particular, the extension $E_G/k(T)$ is not parametric over k.

4. See part (b) of §1.3.1.2.

5. Here and in the next three criteria, one can add as in theorem 3.1.1 that the Galois extensions of group H whose existence is claimed may be obtained by specialization.

Inertia Criterion 1. *The* (geometric non H-parametricity) *condition holds if the following three conditions are satisfied:*

(IC1-1) *each branch point of $E_H/k(T)$ is k-rational,*

(IC1-2) *there exists $i \in \{1, \dots, r_H\}$ such that $\{C^a_{1,G}, \dots, C^a_{r_G,G} \,/\, a \in \mathbb{N}\}$ does not contain $C^G_{i,H}$,*

(IC1-3) *the set $\{C_{1,H}, \dots, C_{r_H,H}\}$ is g-complete.*

Indeed, given a finite extension k'/k, apply theorem 3.1.1 to the G-extensions $E_Hk'/k'(T)$ and $E_Gk'/k'(T)$. Fix an index $i \in \{1, \dots, r_H\}$ such that the set $\{C^a_{1,G}, \dots, C^a_{r_G,G} \,/\, a \in \mathbb{N}\}$ does not contain $C^G_{i,H}$ (condition (IC1-2)). Then part (b) of the Inertia Hypothesis holds for this index i. From condition (IC1-1), $t_{i,H}$ is k'-rational and then part (a) of the Inertia Hypothesis also holds for this i (as noted at the beginning of §3.1.2.1). As condition (2) of addendum 3.1.1 is satisfied (with $I = \{1, \dots, r_H\}$) from conditions (IC1-1) and (IC1-3), the conclusion follows.

Inertia Criterion 2. *The* (geometric non H-parametricity) *condition holds if the following two conditions are satisfied:*

(IC2-1) *there is some k-rational branch point $t_{i,H}$ such that $\{C^a_{1,G}, \dots, C^a_{r_G,G} \,/\, a \in \mathbb{N}\}$ does not contain $C^G_{i,H}$,*

(IC2-2) *k is hilbertian.*

Indeed, given a finite extension k'/k, apply theorem 3.1.1 to the G-extensions $E_Hk'/k'(T)$ and $E_Gk'/k'(T)$. From condition (IC2-1), the Inertia Hypothesis is satisfied. As k' is hilbertian from condition (IC2-2), *i.e.* condition (1) of addendum 3.1.1 is satisfied, the conclusion follows.

Inertia Criterion 3. *The* (geometric non H-parametricity) *condition holds if the following two conditions are satisfied:*

(IC3-1) *there exists $i \in \{1, \dots, r_H\}$ such that $\{C^a_{1,G}, \dots, C^a_{r_G,G} \,/\, a \in \mathbb{N}\}$ does not contain $C^G_{i,H}$,*

(IC3-2) *k is either a number field or a finite extension of a rational function field $\kappa(U)$ with κ an arbitrary algebraically closed field of characteristic zero (and U an indeterminate).*

Indeed, given a finite extension k'/k, apply theorem 3.1.1 to the G-extensions $E_Hk'/k'(T)$ and $E_Gk'/k'(T)$. Fix an index $i \in \{1, \dots, r_H\}$ such that the set $\{C^a_{1,G}, \dots, C^a_{r_G,G} \,/\, a \in \mathbb{N}\}$ does not contain $C^G_{i,H}$ (condition (IC3-1)). Then part (b) of the Inertia Hypothesis holds for this index i. We show below that part (a) of the Inertia Hypothesis also holds for this i. As condition (1) of addendum 3.1.1 is satisfied from condition (IC3-2), the conclusion follows.

From condition (IC3-2), any non constant polynomial $P(T) \in k'[T]$ has infinitely many distinct prime divisors. Indeed this classically follows from the Tchebotarev density theorem in the case k is a number field (and so is k' too). In the case k is a finite extension extension of a rational function field $\kappa(U)$ with κ an arbitrary algebraically closed field of characteristic zero (and so is k' too), note first that one may obviously assume that $P(T)$ is monic and irreducible over k'. Denote the field generated over k' by some root of $P(T)$ by F. As κ is algebraically closed, any prime of F has residue degree 1 in the extension $F/\kappa(U)$, and then in F/k' too. Conclude that all but finitely many primes of k' are a prime divisor of $P(T)$.

Remark 3.1.2. Part (b) of the Inertia Hypothesis (and similar other of our conditions) has a stronger but more practical variant in terms of ramification indices instead of inertia canonical conjugacy classes.

Indeed, given an index $i \in \{1, \dots, r_H\}$, if the ramification index of $t_{j,G}$ in $E_G\overline{k}/\overline{k}(T)$ is a multiple of that of $t_{i,H}$ in $E_H\overline{k}/\overline{k}(T)$ for no index $j \in \{1, \dots, r_G\}$, then the set $\{C^a_{1,G}, \dots, C^a_{r_G,G} \,/\, a \in \mathbb{N}\}$ does not contain $C^G_{i,H}$.

3.1.3 Proof of theorem 3.1.1

Assume first that the Branch Point Hypothesis holds. Then there exists some index $i \in \{1, \dots, r_H\}$ such that the polynomial $m_{i,H}(T) \cdot m^*_{i,H}(T)$ has infinitely many distinct prime divisors $\mathcal{P}$ which each are not a prime divisor of $m_{E_G}(T) \cdot m^*_{E_G}(T)$. Furthermore, up to excluding finitely many of these prime ideals, one may also assume that such a $\mathcal{P}$ satisfies these two conditions:
(i) $\mathcal{P}$ is a good [6] prime for $E_H/k(T)$ and unitizes [7] $t_{i,H}$,
(ii) $\mathcal{P}$ is a good prime for $E_G/k(T)$ and unitizes each of its branch points.
For such a $\mathcal{P}$, apply theorem 1.3.1 to construct a specialization $F_{\mathcal{P}}/k$ of $E_H/k(T)$ which ramifies at $\mathcal{P}$. From corollary 1.2.12, $F_{\mathcal{P}}/k$ is not a specialization of $E_G/k(T)$ and the conclusion follows.

Assume now that the Inertia Hypothesis holds. From its part (a), there exist infinitely many distinct prime divisors $\mathcal{P}$ of $m_{i,H}(T) \cdot m^*_{i,H}(T)$ which may be assumed as before to further satisfy conditions (i) and (ii) above. For such a $\mathcal{P}$, apply theorem 1.3.1 to construct a specialization $F_{\mathcal{P}}/k$ of $E_H/k(T)$ whose inertia group at $\mathcal{P}$ is generated by some element of $C_{i,H}$. If $F_{\mathcal{P}}/k$ is a specialization of $E_G/k(T)$, then, from the Specialization Inertia Theorem of §1.2.1.3, there exist some index $j \in \{1, \dots, r_G\}$ and some positive integer a such that the inertia group of $F_{\mathcal{P}}/k$ at $\mathcal{P}$ is generated by some element of $C^a_{j,G}$. This contradicts part (b) of the Inertia Hypothesis. Hence $F_{\mathcal{P}}/k$ is not a specialization of $E_G/k(T)$ and the conclusion follows.

Assume further that condition (2) of addendum 3.1.1 holds. Instead of theorem 1.3.1, use corollary 1.3.4 and remark 1.3.5 in the previous two paragraphs. In each case, the extension $F_{\mathcal{P}}/k$ may be required to have Galois group H. Hence the (non H-parametricity) condition holds. In the case condition (1) holds, corollary 1.3.3 should be used (instead of corollary 1.3.4 and remark 1.3.5) to obtain the (non H-parametricity) condition and the extra linearly disjointness condition.

3.1.4 The case A only has finitely many distinct prime ideals

Our method can also work in the case the ring A only has finitely many distinct prime ideals. We consider this situation in §3.1.4.1 below and more precisely study in §3.1.4.2 the special case of finite extensions of some formal Laurent series fields.

3.1.4.1. General case. Fix a Dedekind domain A of characteristic zero and let k be its quotient field. Then, with the notation of §3.1.1.1, our method provides the following statement:

Proposition 3.1.3. *Assume that the following five conditions hold:*
(1) *there exists at least one (non-zero) prime ideal $\mathcal{P}$ of A such that neither $|H|$ nor $|G|$ is in $\mathcal{P}$,*
(2) *H and G are centerless finite groups,*
(3) *$r_H = 3$ and each branch point of $E_H/k(T)$ is k-rational,*
(4) *$r_G = 3$ and each branch point of $E_G/k(T)$ is k-rational,*
(5) *there is some index $i \in \{1, 2, 3\}$ such that $\{C^a_{1,G}, C^a_{2,G}, C^a_{3,G} \,/\, a \in \mathbb{N}\}$ does not contain $C^G_{i,H}$.*
Then $E_G k'/k'(T)$ is parametric over k' for no finite extension k'/k.

Addendum 3.1.3. Fix a prime $\mathcal{P}$ of A as in condition (1), a finite extension k'/k, a prime $\mathcal{P}'$ of k' above $\mathcal{P}$ and an index i as in condition (5). Then the Galois extension of k' which is not a specialization of $E_G k'/k'(T)$ whose existence is claimed may be obtained by specializing $E_H k'/k'(T)$ and required to have inertia group at $\mathcal{P}'$ generated by some element of $C_{i,H}$.

Proof. As conditions (1)-(5) remain true after any finite scalar extension, it suffices to show the conclusion in the case $k' = k$. From conditions (3) and (4), one may assume that $E_H/k(T)$

6. See definition 1.2.5.
7. See §1.2.1.3.

and $E_G/k(T)$ each have branch point set $\{0, 1, \infty\}$. Conjoining this and the first two conditions shows that any prime ideal of A satisfying condition (1) is a good prime for each of the two G-extensions $E_H/k(T)$ and $E_G/k(T)$. Fix such a prime ideal $\mathcal{P}$ and an index i as in condition (5). As the branch point $t_{i,H}$ associated with $C_{i,H}$ is in $\{0, 1, \infty\}$, $\mathcal{P}$ unitizes $t_{i,H}$ and is a prime divisor of the polynomial $m_{i,H}(T) \cdot m^*_{i,H}(T)$. Moreover $\mathcal{P}$ unitizes each branch point of $E_G/k(T)$.

The end of the proof is now clear: theorem 1.3.1 provides a specialization $F_\mathcal{P}/k$ of $E_H/k(T)$ whose inertia group at $\mathcal{P}$ is generated by some element of $C_{i,H}$ and which, according to the Specialization Inertia Theorem and condition (5), cannot be a specialization of $E_G/k(T)$. □

3.1.4.2. The formal Laurent series case. Assume here that k is a finite extension of a formal Laurent series field $\kappa((U))$ with κ an arbitrary algebraically closed field of characteristic zero. In this special case, one can be more precise in addendum 3.1.3 in the following way. Given an index i as in condition (5) of proposition 3.1.3, denote the order of any element of $C_{i,H}$ by n_i. Then, given a finite extension k'/k, the Galois extension of k' from the conclusion which is not a specialization of $E_Gk'/k'(T)$ may be required to have Galois group $\mathbb{Z}/n_i\mathbb{Z}$ (this follows from the Puiseux theorem), *i.e.* the G-extension $E_Gk'/k'(T)$ is not $\mathbb{Z}/n_i\mathbb{Z}$-parametric over k'.

Moreover the branch point number conditions of proposition 3.1.3 can be relaxed:

Proposition 3.1.4. *Assume that the following four conditions hold:*
(1) *H and G are centerless finite groups,*
(2) *each branch point of $E_H/k(T)$ is κ-rational,*
(3) *each branch point of $E_G/k(T)$ is κ-rational,*
(4) *there is some $i \in \{1, \dots, r_H\}$ such that $\{C^a_{1,G}, \dots, C^a_{r_G,G} \,/\, a \in \mathbb{N}\}$ does not contain $C^G_{i,H}$.*
Then the G*-extension $E_Gk'/k'(T)$ is $\mathbb{Z}/n_i\mathbb{Z}$-parametric over k' for no finite extension k'/k and no integer n_i which is the order of any element of $C_{i,H}$ with i any index as in condition (4).*

Proof. As to proving proposition 3.1.3, one may suppose $k' = k$. From conditions (1), (2) and (3), the valuation ideal $\mathcal{P}_k$ is a good prime for each of the G-extensions $E_H/k(T)$ and $E_G/k(T)$. Given an index i as in condition (4), $\mathcal{P}_k$ unitizes $t_{i,H}$ and is a prime divisor of $m_{i,H}(T) \cdot m^*_{i,H}(T)$ (as $t_{i,H}$ is κ-rational). Moreover $\mathcal{P}_k$ unitizes each branch point of $E_G/k(T)$. Hence there is some specialization of $E_H/k(T)$ whose inertia group is generated by some element of $C_{i,H}$ and which is not a specialization of $E_G/k(T)$. As noted above, this specialization has Galois group $\mathbb{Z}/n_i\mathbb{Z}$. □

3.2 A general consequence over various base fields

Our method to obtain examples of non G-parametric extensions over a given base field k with prescribed Galois group G starts with the knowledge of two G-extensions of $k(T)$ of group G with some somehow incompatible ramification data. Over number fields, the state-of-the-art in inverse Galois theory does not always provide such extensions in general. Proposition 3.2.1, our conditional result, provides an inverse Galois theory assumption which makes the method work. This statement leads in particular to corollary 3.2.2 which is theorem 2 from the presentation. Corollary 3.2.3, our conjectural result, is the corresponding result under a conjecture of Fried. We next discuss in §3.2.2 the case of some other base fields.

For this section, let G be a finite group. Denote the set of all conjugacy classes of G by $\mathbf{cc}(G)$.

3.2.1 The number field case

Let k be a number field.

3.2.1.1. Conditional result. To simplify the rest of this section, we will use the following condition:

(H1/k) *each non trivial conjugacy class of G occurs as the inertia canonical conjugacy class associated with some branch point of some* G*-extension of $k(T)$ of group G.*

It is unknown in general if any finite group satisfies the inverse Galois theory condition (H1/k) for a given number field k. However, as recalled below, every finite group satisfies condition (H1/k) for large enough number fields k.

Indeed the Riemann existence theorem classically provides the following (*e.g.* [Dèb01, §12]):

($*$) *Any set $\{C_1, \dots, C_r\}$ of non trivial conjugacy classes of G whose all elements generate G occurs as the inertia canonical conjugacy class set of some* G*-extension of $\overline{\mathbb{Q}}(T)$ of group G.*

In particular, there exists some G-extension $\overline{E}/\overline{\mathbb{Q}}(T)$ of group G whose inertia canonical conjugacy class set is the set of all non trivial conjugacy classes of G. Hence condition (H1/k) holds over any number field k that is a field of definition of $\overline{E}/\overline{\mathbb{Q}}(T)$.

Proposition 3.2.1. *Let $E/k(T)$ be a* G*-extension of group G and inertia canonical invariant $(C_1, \dots, C_r)$. Assume that the following condition holds:*
(H2) $\{C_1^a, \dots, C_r^a \,/\, a \in \mathbb{N}\} \neq \mathbf{cc}(G)$.
Then, under condition (H1/k)*, the* G*-extension $E/k(T)$ satisfies the* (geometric non G-parametricity) *condition.*

In particular, under the sole condition (H2), there exists some number field k' containing k such that the G-extension $Ek'/k'(T)$ satisfies the (geometric non G-parametricity) condition.

Proof. Let C be a (non trivial) conjugacy class of G which is not contained in $\{C_1^a, \dots, C_r^a \,/\, a \in \mathbb{N}\}$ (condition (H2)) and $E'/k(T)$ be a G-extension of group G such that the conjugacy class C occurs as the inertia canonical conjugacy class associated with some of its branch points (condition (H1/k)). Then the two G-extensions $E'/k(T)$ and $E/k(T)$ satisfy condition (IC3-1) of Inertia Criterion 3. As condition (IC3-2) also holds, the conclusion follows. □

Assume now that G has *a generating conjugacy class set satisfying condition* (H2), *i.e.* a set $\{C_1, \dots, C_r\}$ of non trivial conjugacy classes of G satisfying the following two conditions:
(1) the elements of $C_1, \dots, C_r$ generate G,
(2) $\{C_1^a, \dots, C_r^a \,/\, a \in \mathbb{N}\} \neq \mathbf{cc}(G)$.
Then such a set $\{C_1, \dots, C_r\}$ occurs as the inertia canonical conjugacy class set of some G-extension of $k'(T)$ of group G for some number field k' satisfying condition (H1/k') (condition (1) and statement ($*$)). Moreover condition (H2) of proposition 3.2.1 holds (condition (2)). One then obtains the following:

Corollary 3.2.2. *Assume that G has a generating conjugacy class set satisfying condition* (H2)*. Then there exist some number field k' and some* G*-extension of $k'(T)$ of group G satisfying the* (geometric non G-parametricity) *condition.*

Many finite groups admit a generating conjugacy class set satisfying condition (H2) (and then satisfy the conclusion of corollary 3.2.2). Here are some of them.

(a) Given two non trivial finite groups G_1 and G_2, the product $G_1 \times G_2$ does (in particular, any abelian finite group which is not cyclic of prime power order does [8]).

8. Note that this does not hold if G is cyclic of prime power order.

Indeed the elements, and *a fortiori* their conjugacy classes, $(g_1, 1)$ $(g_1 \in G_1)$ and $(1, g_2)$ $(g_2 \in G_2)$ obviously generate the product $G_1 \times G_2$. And no couple of non trivial elements $(g_1, g_2) \in G_1 \times G_2$ is conjugate to a power of one of these couples.

(b) Symmetric groups S_n $(n \geq 3)$, alternating groups A_n $(n \geq 4)$, dihedral groups D_n $(n \geq 2)$ do.

(c) Non abelian simple groups do. Indeed, as shown in [Wag78] and [MSW94], such a group may be generated by involutions. Then, for any odd prime divisor p of the order of the group, no element of order p is conjugate to a power of an involution and the conclusion follows.

3.2.1.2. Conjectural result. By taking $\{C_1, \dots, C_r\}$ to be the set of all non trivial conjugacy classes of G in the following conjecture of Fried, the inverse Galois theory condition (H1/$\mathbb{Q}$) introduced in §3.2.1.1 holds:

Conjecture (Fried). *Let $\{C_1, \dots, C_r\}$ be a set of non trivial conjugacy classes of G satisfying the following two conditions:*
(1) *the elements of $C_1, \dots, C_r$ generate G,*
(2) *$\{C_1, \dots, C_r\}$ is a rational*[9] *set of conjugacy classes.*
Then $\{C_1, \dots, C_r\}$ occurs as the inertia canonical conjugacy class set of some G*-extension of $\mathbb{Q}(T)$ of group G.*

Under Fried's conjecture, one then obtains corollary 3.2.3 below:

Corollary 3.2.3. *Assume that there exists some set $\{C_1, \dots, C_r\}$ of non trivial conjugacy classes of G satisfying the following three conditions:*
(1) *the elements of $C_1, \dots, C_r$ generate G,*
(2) *$\{C_1, \dots, C_r\}$ is a rational set of conjugacy classes,*
(3) $\{C_1^a, \dots, C_r^a \,/\, a \in \mathbb{N}\} \neq \mathbf{cc}(G)$.
Then there exists some G*-extension of $\mathbb{Q}(T)$ of group G satisfying the* (geometric non G-parametricity) *condition.*

Indeed, under Fried's conjecture, conditions (1) and (2) provide a G-extension of $\mathbb{Q}(T)$ of group G whose inertia canonical conjugacy class set is $\{C_1, \dots, C_r\}$. Moreover condition (H2) of proposition 3.2.1 holds (condition (3)) and condition (H1/$\mathbb{Q}$) also holds under Fried's conjecture.

3.2.2 Some other base fields

3.2.2.1. Rational function fields. Assume that k is a finite extension of a rational function field $\kappa(U)$ with κ an arbitrary algebraically closed field of characteristic zero (and U an indeterminate).

In this case, condition (H1/k) holds (statement $(*)$). Conjoining this and the proof of proposition 3.2.1 shows that the conclusion of this result holds under the sole condition (H2). Moreover corollary 3.2.2 holds with the suitable number field k' replaced by our given base field k.

3.2.2.2. Formal Laurent series fields. Assume here that k is a finite extension of a formal Laurent series field $\kappa((U))$ with κ an arbitrary algebraically closed field of characteristic zero. *We suppose below that G has trivial center.* Then the counterpart of proposition 3.2.1 is given by the following:

Proposition 3.2.4. *Let $E/k(T)$ be a* G*-extension of group G and inertia canonical invariant $(C_1, \dots, C_r)$. Assume that any branch point is κ-rational. Then these conditions are equivalent:*

9. *i.e.* $g^m \in \cup_{i=1}^r C_i$ for each element $g \in \cup_{i=1}^r C_i$ and each positive integer m relatively prime to the least common multiple of the orders of the elements of $C_1, \dots, C_r$.

(1) *$Ek'/k'(T)$ is parametric over k' for any finite extension k'/k,*
(2) *$E/k(T)$ is parametric over k,*
(3) $\{C_1^a, \ldots, C_r^a \,/\, a \in \mathbb{N}\} = \mathbf{cc}(G)$.

Addendum 3.2.4. If condition (3) does not hold, then the following holds. Fix a finite extension k'/k, a conjugacy class C of G which is not contained in the set $\{C_1^a, \ldots, C_r^a \,/\, a \in \mathbb{N}\}$ and denote the order of any element of C by n_C. Then $Ek'/k'(T)$ is not $\mathbb{Z}/n_C\mathbb{Z}$-parametric over k'.

Proposition 3.2.4 may be applied to many G-extensions (see remark 3.4.5 for an example).

Proof. As implication (1) $\Rightarrow$ (2) is trivial, we only show implications (2) $\Rightarrow$ (3) and (3) $\Rightarrow$ (1).

Assume first that condition (3) does not hold. Fix a (non trivial) conjugacy class C of G which is not contained in the set $\{C_1^a, \ldots, C_r^a \,/\, a \in \mathbb{N}\}$. Produce from statement $(*)$ of §3.2.1.1 a G-extension $E'/k(T)$ of group G, with any branch point $\overline{\mathbb{Q}}$-rational and such that the conjugacy class C occurs as the inertia canonical conjugacy class associated with some of them. Apply proposition 3.1.4 to the two G-extensions $E'/k(T)$ and $E/k(T)$ to conclude that $Ek'/k'(T)$ is $\mathbb{Z}/n_C\mathbb{Z}$-parametric over k' for no finite extension k'/k, thus proving the conclusion of addendum 3.2.4 (and so condition (2) does not hold).

Assume now that condition (3) holds. Let k'/k be a finite extension, $A_{k'}$ be the integral closure of $\kappa[[U]]$ in k' and $\mathcal{P}_{k'}$ be the valuation ideal. From the Puiseux theorem, it suffices to show that, for any cyclic subgroup $\mathbb{Z}/n\mathbb{Z} \subset G$, the G-extension $Ek'/k'(T)$ has at least one specialization of group $\mathbb{Z}/n\mathbb{Z}$. Fix such a subgroup $\mathbb{Z}/n\mathbb{Z}$ and pick an element $g \in G$ of order n. Denote its conjugacy class in G by C_g. From condition (3), there exist some index $i \in \{1, \ldots, r\}$ and some integer a such that $C_g = C_i^a$. As any branch point is κ-rational and G has trivial center, the valuation ideal $\mathcal{P}_{k'}$ is a good prime for $Ek'/k'(T)$. Produce then from theorem 1.3.1 a specialization of $Ek'/k'(T)$ whose inertia group at $\mathcal{P}_{k'}$ is generated by some element of $C_i^a = C_g$. From the Puiseux theorem, this specialization has Galois group $\mathbb{Z}/n\mathbb{Z}$. □

Conjoining this and statement $(*)$ of §3.2.1.1 provides the following two conclusions.

(a) First of all, we obtain the following counterpart of corollary 3.2.2:

Corollary 3.2.5. *Assume that the centerless finite group G has a generating conjugacy class set satisfying condition* (H2)*. Then there exists some* G*-extension $E/k(T)$ of group G such that $Ek'/k'(T)$ is parametric over k' for no finite extension k'/k.*

Indeed any generating conjugacy class set satisfying condition (H2) occurs as the inertia canonical conjugacy class set of some G-extension $E/k(T)$ of group G with any branch point $\overline{\mathbb{Q}}$-rational and which does not satisfy condition (3) of proposition 3.2.4. Hence $E/k(T)$ may be required to satisfy the conclusion of addendum 3.2.4.

(b) In contrast, by taking $\{C_1, \ldots, C_r\}$ to be the set of all non trivial conjugacy classes of G in statement $(*)$, one obtains the following positive result:

Corollary 3.2.6. *The centerless finite group G occurs as the Galois group of a* G*-extension $E/k(T)$ such that $Ek'/k'(T)$ is parametric over k' for any finite extension k'/k.*

3.3 Applications of the Branch Point Criterion

Given a number field k and a finite group H, we use below the Branch Point Criterion to show that some known G-extensions of $k(T)$ of group G containing H each satisfy the (non H-parametricity) condition.

3.3.1 A general result

The aim of this subsection is corollary 3.3.1 below. Given a field k and a finite group H, we will use the following condition which has already appeared in §1.3.2 in the case $k = \mathbb{Q}$:

(H3/k) *the group H occurs as the Galois group of a* G*-extension of $k(T)$ with at least one k-rational branch point.*

As already noted there, not all finite groups H satisfy condition (H3/k) for a given number field k. However every finite group satisfies condition (H3/k) for large enough number fields k.

Indeed it classically follows from Riemann's existence theorem that, if r is strictly bigger than the rank of H and $t_1, \dots, t_r$ are r distinct points in $\mathbb{P}^1(\overline{\mathbb{Q}})$, then there is a G-extension $\overline{E}/\overline{\mathbb{Q}}(T)$ of group H and branch point set $\{t_1, \dots, t_r\}$ (*e.g.* [Dèb01, §12]). Hence condition (H3/k) holds for every number field k that is a field of definition of $\overline{E}/\overline{\mathbb{Q}}(T)$ and of one of its branch points.

3.3.1.1. Statement of the result. Let k be a number field, G be a finite group and $E/k(T)$ be a G-extension of group G. Denote the orbits of its branch points under the action of G_k by $O_1, \dots, O_s$ and the field generated over k by all points in O_i by F_i ($i = 1, \dots, s$).

Corollary 3.3.1. *Assume that either one of the following two conditions holds:*
(1) $|O_i| \geq 2$ *and the fields F_i and $F_1 \dots F_{i-1}F_{i+1} \dots F_s$ are linearly disjoint over k for each index $i \in \{1, \dots, s\}$,*
(2) $s = 2$ *and* $|O_1| = |O_2| = 2$.
Then the G*-extension $E/k(T)$ satisfies the* (non H-parametricity) *condition for any subgroup $H \subset G$ satisfying condition* (H3/k).

Remark 3.3.2. Assume that G satisfies condition (H3/k) and that $E/k(T)$ has $r \leq 4$ branch points. As a consequence of corollary 3.3.1, we obtain that

if (a) *no branch point is k-rational,*
then (b) *$E_G/k(T)$ satisfies the* (non G-parametricity) *condition.*

Proposition 2.3.9 shows however that the converse (b) $\Rightarrow$ (a) does not hold in general if $r = 3$: the extension $E/\mathbb{Q}(T)$ there has at least one $\mathbb{Q}$-rational branch point (as noted in the proof), but condition (b) holds. Proposition 2.3.11 provides a similar counter-example in the case $r = 4$.

However, for $r = 2$ and number fields $k \subset \mathbb{R}$, this converse (b) $\Rightarrow$ (a) is true. Indeed fix such a number field k and assume that $E/k(T)$ has two branch points with at least one k-rational. Then the other is also k-rational. From [DF94, theorem 1.1], $\mathrm{Gal}(E/k(T))$ is generated by involutions and, since it is cyclic, one then has $\mathrm{Gal}(E/k(T)) = \mathbb{Z}/2\mathbb{Z}$. Conclude from implication (3) $\Rightarrow$ (1) in proposition 2.3.3 that $E/k(T)$ is parametric over k (as explained in part (1) of remark 2.3.6).

3.3.1.2. Proof of corollary 3.3.1. We show below that, under either one of conditions (1) and (2), there exist infinitely many distinct prime ideals of the integral closure A of $\mathbb{Z}$ in k which each are not a prime divisor of the polynomial $m_E(T) \cdot m_E^*(T)$. Given a subgroup $H \subset G$ satisfying condition (H3/k) and a G-extension $E_H/k(T)$ of group H with at least one k-rational branch point, the conclusion then follows from the Branch Point Criterion applied to the G-extensions $E_H/k(T)$ and $E/k(T)$.

For each index $i \in \{1, \dots, s\}$, pick $t_i \in O_i$ and let $m_i(T)$ be the irreducible polynomial of t_i over k and d_i be the degree of $m_i(T)$. Denote the action of $\mathrm{Gal}(F_i/k)$ on the roots of $m_i(T)$ by $\sigma_i : \mathrm{Gal}(F_i/k) \to S_{d_i}$. Let F be the splitting field of $\prod_{i=1}^{s} m_i(T)$ over k.

Assume first that condition (1) holds. From the second part of the hypothesis, the group $\mathrm{Gal}(F/k)$ is isomorphic to $\mathrm{Gal}(F_1/k) \times \dots \times \mathrm{Gal}(F_s/k)$ and $\sigma_1 \times \dots \times \sigma_s : \mathrm{Gal}(F_1/k) \times \dots \times \mathrm{Gal}(F_s/k) \to S_{d_1 + \dots + d_s}$ corresponds to the action of $\mathrm{Gal}(F/k)$ on the roots of $\prod_{i=1}^{s} m_i(T)$. Given an index $i \in \{1, \dots, s\}$, it follows from the assumption $|O_i| \geq 2$ and a classical group theoretical lemma [10] that there exists some $g_i \in \mathrm{Gal}(F_i/k)$ such that $\sigma_i(g_i)$ has no fixed points.

By the Tchebotarev density theorem, there exist infinitely many distinct prime ideals of A such that the associated Frobenius is conjugate in $\mathrm{Gal}(F/k)$ to the element $(g_1, \dots, g_s)$. In particular, there exist infinitely many distinct prime ideals of A which each are not a prime divisor of $\prod_{i=1}^{s} m_i(T)$, and so not of $m_E(T)$ either. Since ∞ is not a branch point of $E/k(T)$, the same conclusion holds for $m_E(T) \cdot m_E^*(T)$ (remark 1.3.9).

Assume now that condition (2) holds. From the last two paragraphs, we may assume that $F_1 = F_2$. Then $m_1(T)$ and $m_2(T)$ have the same prime divisors up to finitely many. Since the polynomial $m_1(T)$ is irreducible over k and has degree ≥ 2, there exist infinitely many distinct prime ideals of A which each are not a prime divisor of $m_1(T)$ (*e.g.* [Hei67, theorem 9]), and so not of $m_1(T) \cdot m_2(T)$ either. Conclude the proof as in the previous paragraph.

If $s = 2$ and $|O_1| \geq 3$ or $|O_2| \geq 3$, then the proof does not work in general. Indeed each prime number is a prime divisor of the polynomial $P(T) = (T^3 - 2)(T^2 + T + 1)$ [Nag69, §7].

3.3.2 Examples

As already said in the presentation, G-extensions of $k(T)$ with given Galois group G (and *a fortiori* satisfying the assumptions of corollary 3.3.1) are not always known yet. Of course such extensions always exist in the case $G = \mathbb{Z}/2\mathbb{Z}$ (and then $H = \mathbb{Z}/2\mathbb{Z}$ too). We focus in part (a) of §3.3.2.1 on this particular situation. We next give in part (b) of §3.3.2.1 another example with $H = G = \mathbb{Z}/2\mathbb{Z}$ and conclude in §3.3.2.2 by some examples with larger abelian groups.

Denote in this subsection the Euler function by φ and, given a positive integer n, the n-th cyclotomic polynomial by $\phi_n(T)$.

3.3.2.1. The case $G = \mathbb{Z}/2\mathbb{Z}$.

(a) *Application of corollary 3.3.1.* Let k be a number field and $P(T) \in k[T]$ be a separable polynomial over k of even degree. Lemma 2.3.5 shows that the branch points of the G-extension $k(T)(\sqrt{P(T)})/k(T)$ are the roots of $P(T)$. Hence the orbits $O_1, \dots, O_s$ of corollary 3.3.1 exactly correspond to the root sets of the irreducible factors $P_1(T), \dots, P_s(T)$ over k of $P(T)$. Thus corollary 3.3.1 yields corollary 3.3.3 below:

Corollary 3.3.3. *Denote the splitting fields over k of the irreducible polynomials $P_1(T), \dots, P_s(T)$ by $F_1, \dots, F_s$ respectively. Assume that either one of the following two conditions holds:*
(1) $\deg(P_i(T)) \geq 2$ *and the fields F_i and $F_1 \dots F_{i-1}F_{i+1} \dots F_s$ are linearly disjoint over k for each index $i \in \{1, \dots, s\}$,*
(2) $s = 2$ *and* $\deg(P_1(T)) = \deg(P_2(T)) = 2$.
Then the G-*extension* $k(T)(\sqrt{P(T)})/k(T)$ *satisfies the* (non $\mathbb{Z}/2\mathbb{Z}$-parametricity) *condition.*

In particular, the (non $\mathbb{Z}/2\mathbb{Z}$-parametricity) condition holds if $\deg(P(T)) = 4$ and $P(T)$ has no root in k. Moreover we reobtain implication (2) $\Rightarrow$ (3) in proposition 2.3.3.

(b) *Cyclotomic polynomials.* Let s be a positive integer and $(n_1, \dots, n_s)$ be a s-tuple of distinct integers ≥ 3.

Corollary 3.3.4. *The* G-*extension* $\mathbb{Q}(T)(\sqrt{\phi_{n_1}(T) \dots \phi_{n_s}(T)})/\mathbb{Q}(T)$ *satisfies the* (non $\mathbb{Z}/2\mathbb{Z}$-parametricity) *condition.*

10. Namely, if a group $\mathcal{G}$ transitively acts on a finite set S of cardinality ≥ 2, then there exists at least one element g of $\mathcal{G}$ such that $g.s = s$ for no element s of S.

Proof. Set $E = \mathbb{Q}(T)(\sqrt{\phi_{n_1}(T)\dots\phi_{n_s}(T)})$. We show below that there exist infinitely many distinct primes which each are not a prime divisor of the polynomial $m_E(T)\cdot m_E^*(T)$. The conclusion then follows from the Branch Point Criterion applied to the G-extensions $\mathbb{Q}(\sqrt{T})/\mathbb{Q}(T)$ (for example) and $E/\mathbb{Q}(T)$.

As $\phi_{n_1}(T)\dots\phi_{n_s}(T)$ has even degree, ∞ is not a branch point of $E/\mathbb{Q}(T)$ (lemma 2.3.5). Hence, from remark 1.3.9, the polynomials $m_E(T)\cdot m_E^*(T)$ and $m_E(T)$ have the same prime divisors (up to finitely many). Moreover the branch points of $E/\mathbb{Q}(T)$ are the roots of $\phi_{n_1}(T)\dots\phi_{n_s}(T)$ and then $m_E(T) = \phi_{n_1}(T)^{\varphi(n_1)}\dots\phi_{n_s}(T)^{\varphi(n_s)}$. Since, for each index $i \in \{1,\dots,s\}$, the prime divisors of $\phi_{n_i}(T)$ are all primes p such that $p \equiv 1 \bmod [n_i]$ (up to finitely many), any prime divisor p of $m_E(T)\cdot m_E^*(T)$ satisfies $p \equiv 1 \bmod n_{i_p}$ for some index $i_p \in \{1,\dots,s\}$ (up to finitely many). From the Dirichlet theorem, there exist infinitely many distinct primes p which each satisfy $p \equiv 1 \bmod n_i$ for no index $i \in \{1,\dots,s\}$, thus ending the proof. □

3.3.2.2. Larger abelian groups.

(a) *Abelian groups of even order.*

Lemma 3.3.5. *Any abelian group of even order satisfies condition* (H3/$\mathbb{Q}$).

Proof. Given an even integer $n \geq 4$, it suffices to show that the group $\mathbb{Z}/n\mathbb{Z}$ satisfies the required condition. From [Des95, lemma 2.1.2], we have to find
- a positive integer r,
- r elements $g_1,\dots,g_r$ in $\mathbb{Z}/n\mathbb{Z}$ such that $\langle g_1,\dots,g_r\rangle = \mathbb{Z}/n\mathbb{Z}$ and $\sum_{i=1}^r g_i = 0$,
- r distinct points $t_1,\dots,t_r$ in $\mathbb{P}^1(\overline{\mathbb{Q}})$ with at least one $\mathbb{Q}$-rational and satisfying the following property: for any $\tau \in \mathrm{G}_\mathbb{Q}$ and any index $i \in \{1,\dots,r\}$, $\chi_\mathbb{Q}(\tau)g_j \equiv g_i \bmod n$ with $t_j = \tau(t_i)$ and $\chi_\mathbb{Q}$ the cyclotomic character of $\mathbb{Q}$.

Take $r = \varphi(n)+2$, $\{g_1,\dots,g_{r-2}\}$ to be the set of all the generators of $\mathbb{Z}/n\mathbb{Z}$ (with $g_1 = 1$) and $g_{r-1} = g_r = n/2$. Let ζ be a primitive n-th root of unity. For each index $i \in \{1,\dots,r-2\}$, set $t_i = \zeta^{g_i}$. Take finally $\{t_{r-1},t_r\}$ as a couple of distinct points in $\mathbb{P}^1(\mathbb{Q})$.

From the proof of [Des95, lemma 2.1.3], it remains to show that $\chi_\mathbb{Q}(\tau)(n/2) \equiv (n/2) \bmod n$ for any $\tau \in \mathrm{G}_\mathbb{Q}$. As $x(n/2) \equiv (n/2) \bmod n$ for odd integer x, the required equality holds. □

Given a positive integer $n \geq 3$, [Des95, lemma 2.1.3] shows that there exists at least one G-extension of $\mathbb{Q}(T)$ of group $\mathbb{Z}/n\mathbb{Z}$ and branch point set $\{e^{2ik\pi/n} \,/\, (k,n)=1\}$. We use below the notation $E_n/\mathbb{Q}(T)$ for such a G-extension.

Corollary 3.3.6. (1) *Let $n \geq 4$ be an (even) integer. Then every* G*-extension $E_n/\mathbb{Q}(T)$ satisfies the* (non $\mathbb{Z}/m\mathbb{Z}$-parametricity) *condition for any even divisor m of n.*

(2) *Let $n \in \{4,6\}$. Then every* G*-extension of $\mathbb{Q}(T)$ of group $\mathbb{Z}/n\mathbb{Z}$ with two branch points satisfies each of the two* (non $\mathbb{Z}/2\mathbb{Z}$-parametricity) *and* (non $\mathbb{Z}/n\mathbb{Z}$-parametricity) *conditions* [11].

(3) *Let G be an abelian group of even order. Then there exists at least one* G*-extension of $\mathbb{Q}(T)$ of group G satisfying the* (non H-parametricity) *condition for any subgroup $H \subset G$ of even order.*

Proof. Part (1) is a straightforward application of part (1) of corollary 3.3.1 and lemma 3.3.5. For part (2), it suffices to remark that any G-extension of $\mathbb{Q}(T)$ of group $\mathbb{Z}/n\mathbb{Z}$ with two branch points satisfies condition (1) of corollary 3.3.1 (as shown in the last paragraph of remark 3.3.2). Conjoining this and lemma 3.3.5 provides the announced conclusion.

To prove part (3), we show below that there exists some G-extension $E'/\mathbb{Q}(T)$ of group G such that there exist infinitely many distinct primes p which each are not a prime divisor of

11. We then reobtain proposition 2.3.7 (which corresponds to the case $n = 6$).

$m_{E'}(T) \cdot m^*_{E'}(T)$. Given a subgroup $H \subset G$ of even order and a G-extension $E_H/\mathbb{Q}(T)$ of group H with at least one $\mathbb{Q}$-rational branch point (lemma 3.3.5), the conclusion then follows from the Branch Point Criterion applied to the G-extensions $E_H/\mathbb{Q}(T)$ and $E'/\mathbb{Q}(T)$.

Set $G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$ where $n_1, \dots, n_s$ are integers ≥ 2. Pick a G-extension $E'_{n_1}/\mathbb{Q}(T)$ of group $\mathbb{Z}/n_1\mathbb{Z}$ in the following way: if $n_1 = 2$, take it to be $\mathbb{Q}(T)(\sqrt{1+T^2})/\mathbb{Q}(T)$ and, if $n_1 \geq 3$, take it to be any of our G-extensions $E_{n_1}/\mathbb{Q}(T)$. Do the same with the integer n_2. Apply next some homography on $E'_{n_2}/\mathbb{Q}(T)$ to make the branch point sets of $E'_{n_1}/\mathbb{Q}(T)$ and $E'_{n_2}/\mathbb{Q}(T)$ disjoint. Then the *compositum* $E'_{n_1}E'_{n_2}/\mathbb{Q}(T)$ has Galois group $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$. By induction, one then obtains a G-extension $E'/\mathbb{Q}(T)$ of group G such that all but finitely many prime divisors p of the polynomial $m_{E'}(T)$ satisfy either one of the following two conditions:
(i) $p \equiv 1 \bmod n_{i_p}$ for some index i_p such that $n_{i_p} \geq 3$,
(ii) $p \equiv 1 \bmod 4$.
From the Dirichlet theorem, there exist infinitely many distinct primes which each satisfy neither condition (i) nor condition (ii), *i.e.* which each are not a prime divisor of $m_{E'}(T)$. As ∞ is not a branch point of $E'/\mathbb{Q}(T)$, this is also true of $m_{E'}(T) \cdot m^*_{E'}(T)$ (remark 1.3.9). □

(b) *Cyclic groups.* Continue with the G-extensions $E_n/\mathbb{Q}(T)$ introduced in part (a).

Corollary 3.3.7. *Let n be an integer ≥ 3. Then every* G*-extension $E_n/\mathbb{Q}(T)$ satisfies the* (non $\mathbb{Z}/m\mathbb{Z}$-parametricity) *condition for any divisor m of n satisfying the following two conditions:*
(1) $m \notin \{1, n\}$,
(2) $m \neq n/2$ *if* $n \equiv 2 \bmod 4$.

In particular, we obtain the following statement:

Let G be an abelian finite group which is not a power of a same prime order cyclic group. Then there exists at least one G*-extension of $\mathbb{Q}(T)$ of group G which is not $\{1\}$-parametric over $\mathbb{Q}$.*

Indeed it follows from the assumption that there exist some integer $n \geq 3$, not a prime, and some abelian group H such that $G = \mathbb{Z}/n\mathbb{Z} \times H$. Pick any of our G-extensions $E_n/\mathbb{Q}(T)$. As n is not a prime, there exists at least one divisor m of n satisfying conditions (1) and (2) of corollary 3.3.7. Conjoining the fact that $E_n/\mathbb{Q}(T)$ is not $\mathbb{Z}/m\mathbb{Z}$-parametric over $\mathbb{Q}$ (corollary 3.3.7) and proposition 2.3.1 shows that one may further assume that $E_n/\mathbb{Q}(T)$ has no trivial specialization. Pick next a G-extension $E_H/\mathbb{Q}(T)$ of group H. Up to applying some homography on $E_H/\mathbb{Q}(T)$, one may assume that the *compositum* $E_nE_H/\mathbb{Q}(T)$ has Galois group G. And this G-extension of group G obviously has no trivial specialization.

Proof of corollary 3.3.7. Remark first that, since ∞ is not a branch point of $E_n/\mathbb{Q}(T)$, the polynomials $m_{E_n}(T) \cdot m^*_{E_n}(T)$ and $m_{E_n}(T)$ have the same prime divisors (up to finitely many; see remark 1.3.9) and, since $m_{E_n}(T) = \phi_n(T)^{\varphi(n)}$, these prime divisors are all primes p such that $p \equiv 1 \bmod n$ (up to finitely many).

Assume first that $m \geq 3$. From the Dirichlet theorem, there exist infinitely many distinct prime numbers p which each satisfy $p \equiv 1 \bmod m$ and $p \not\equiv 1 \bmod n$. Given any of our G-extensions $E_m/\mathbb{Q}(T)$, this shows that the original Branch Point Hypothesis of theorem 3.1.1 applied to $E_m/\mathbb{Q}(T)$ and $E_n/\mathbb{Q}(T)$ holds. As condition (1) of addendum 3.1.1 obviously holds, the conclusion follows.

Assume now that $m = 2$. From the Dirichlet theorem, there exist infinitely many distinct prime numbers p which each satisfy $p \not\equiv 1 \bmod n$, *i.e.* which each are not a prime divisor of $m_{E_n}(T) \cdot m^*_{E_n}(T)$. The conclusion then follows from the Branch Point Criterion applied to the G-extensions $\mathbb{Q}(\sqrt{T})/\mathbb{Q}(T)$ (for example) and $E_n/\mathbb{Q}(T)$. □

3.4 Applications of the Inertia Criteria

For this section, let A be a Dedekind domain of characteristic zero assumed to have infinitely many distinct prime ideals and k be its quotient field.

Given a finite group H, we use below Inertia Criteria 1-3 to show that some known G-extensions of $k(T)$ of group G containing H each satisfy the (geometric non H-parametricity) condition. We first consider the case $H = S_n$ (§3.4.1) and then the case $H = A_n$ (§3.4.2-3.4.3). §3.4.4 is devoted to some other cases H is a non abelian simple group and we conclude our examples in §3.4.5 with the case H is a p-group.

3.4.1 The case $H = S_n$

Let $n \geq 3$ be an integer. The aims of this subsection are corollaries 3.4.1, 3.4.3 and 3.4.4 below which give our main examples in the situation $H = G = S_n$. The first two statements involve the G-extensions of group S_n recalled in §B.3.1. We also use the notation from there for elements of S_n and their conjugacy classes. The three corollaries are stated in §3.4.1.1 and proved in §3.4.1.2.

3.4.1.1. Examples with $G = S_n$.

(a) *Morse polynomials.* Let $P(Y) \in k[Y]$ be a degree n Morse polynomial and E_1 be the splitting field over $k(T)$ of the polynomial $P(Y) - T$ (§B.3.1.1).

Corollary 3.4.1. *Assume that $n \geq 4$. Then the* G-*extension $E_1/k(T)$ satisfies the* (geometric non S_n-parametricity) *condition.*

As noted in part (2) of remark 2.2.4, the conclusion of corollary 3.4.1 (and that of corollary 3.4.3 below too) does not hold if $n = 3$.

Remark 3.4.2. Fix a PAC field κ of characteristic zero and a G-extension $E/\kappa(T)$ of group S_n (with $n \geq 4$) provided by some degree n Morse polynomial with coefficients in κ. As noted in §2.2.1, $E/\kappa(T)$ is S_n-parametric over κ. But, with U an indeterminate, $E(U)/\kappa(U)(T)$ is not (corollary 3.4.1). Hence $E/\kappa(T)$ is not S_n-generic over κ.

(b) *Trinomials.* Let m, r and s be positive integers such that $1 \leq m \leq n$, $(m, n) = 1$ and $s(n-m) - rn = 1$. Denote the splitting field over $k(T)$ of $Y^n - T^r Y^m + T^s$ by E_2 (§B.3.1.2).

Corollary 3.4.3. (1) *Assume that $n \notin \{3, 4, 6\}$. Then the* G-*extension $E_2/k(T)$ satisfies the* (geometric non S_n-parametricity) *condition.*
(2) *Assume that $n = 6$ and k is hilbertian. Then the* G-*extension $E_2/k(T)$ satisfies the* (geometric non S_n-parametricity) *condition.*

(c) *A realization with four branch points.* Assume that $n \geq 6$ is even. From [HRD03], there exists at least one G-extension of $\mathbb{Q}(T)$ of group S_n and inertia canonical invariant $([1^2(n-2)^1], [1^{n-3}3^1], [2^{(n/2)}], [1^2 2^{(n-2)/2}])$. From the branch cycle lemma, each branch point of such a G-extension is $\mathbb{Q}$-rational. Fix such a G-extension $E/\mathbb{Q}(T)$ and set $E_3/k(T) = Ek/k(T)$.

Corollary 3.4.4. *The* G-*extension $E_3/k(T)$ satisfies the* (geometric non S_n-parametricity) *condition.*

3.4.1.2. Proof of corollaries 3.4.1, 3.4.3 and 3.4.4. The proof has two main parts. The first one consists in showing the following general result:

Let $E/k(T)$ be a G*-extension of group S_n and $(C_1, \ldots, C_r)$ be its inertia canonical invariant. Denote the set of all integers m such that $1 \leq m \leq n$ and $(m,n) = 1$ by I_n. Then $E/k(T)$ satisfies the* (geometric non S_n-parametricity) *condition provided that one of the following three conditions holds:*
(1) $[n^1]$ is not in the set $\{C_1, \ldots, C_r\}$,
(2) $[m^1(n-m)^1]$ is not in the set $\{C_1, \ldots, C_r\}$ for some $m \in I_n$,
(3) k is hilbertian, $n \geq 6$ is even and $[1^2(n-2)^1]$ is not in the set $\{C_1, \ldots, C_r\}$.
In particular, $E/k(T)$ satisfies the (geometric non S_n-parametricity) *condition if $r \leq \varphi(n)/2$* [12].

This statement provides in particular theorem 3 from the presentation in the case $H = G = S_n$ (as $\varphi(n)$ tends to ∞ with n).

The second part consists next in checking that each G-extension $E_i/k(T)$ $(i = 1, 2, 3)$ satisfies one of the conditions above.

Part 1. The proof consists in each case in applying Inertia Criterion 1 (if there are no assumption on the base field k) or Inertia Criterion 2 (if k is assumed to be hilbertian) to some suitable G-extension $E_j/k(T)$ $(j = 1, 2, 3)$ and the given one $E/k(T)$.

Assume first that $[n^1]$ is not in the set $\{C_1, \ldots, C_r\}$. Then $[n^1]$ is not in $\{C_1^a, \ldots, C_r^a \,/\, a \in \mathbb{N}\}$ either [13], *i.e.* condition (IC1-2) of Inertia Criterion 1 applied to the G-extensions $E_2/k(T)$ and $E/k(T)$ holds. As conditions (IC1-1) and (IC1-3) also hold [Sch00, §2.4], the conclusion follows. If $[m^1(n-m)^1]$ is not in the set $\{C_1, \ldots, C_r\}$ for some $m \in I_n$, then repeat the same argument with $[n^1]$ replaced by $[m^1(n-m)^1]$.

Assume now that k is hilbertian, $n \geq 6$ is even and $[1^2(n-2)^1]$ is not in the set $\{C_1, \ldots, C_r\}$. Then $[1^2(n-2)^1]$ is not in the set $\{C_1^a, \ldots, C_r^a \,/\, a \in \mathbb{N}\}$ either, *i.e.* condition (IC2-1) of Inertia Criterion 2 applied to the G-extensions $E_3/k(T)$ and $E/k(T)$ holds. As condition (IC2-2) also holds, the conclusion follows.

Part 2. Let $i \in \{1, 2, 3\}$.
(a) If $i = 1$, condition (2) holds (with $m = 1$).
(b) Assume that $i = 2$. If $n \notin \{3, 4, 6\}$, one has $\varphi(n) \geq 4$ and condition (2) holds. In the case $n = 6$, condition (3) holds.
(c) If $i = 3$, condition (1) holds.

Remark 3.4.5. (An example over complete valued fields) Given an algebraically closed field κ of characteristic zero, assume that k is a finite extension of the formal Laurent series field $\kappa((U))$.

Then, in the case $n = 4$, the G-extension $E_2k'/k'(T)$ is parametric over k' for any finite extension k'/k (proposition 3.2.4). However, in the case $n \geq 5$, this does not hold anymore (and the more precise conclusion of addendum 3.2.4 even holds) since, as the proof above shows, at least one conjugacy class of S_n is not in the set $\{[1^{n-2}2^1]^a, [m^1(n-m)^1]^a, [n^1]^a \,/\, a \in \mathbb{N}\}$.

3.4.2 The case $H = A_n$ and $G = A_n$

Let $n \geq 4$ be an integer. The aims of this subsection are corollaries 3.4.6, 3.4.7 and 3.4.8 below which give our main examples in the situation $H = G = A_n$. The second statement involves the G-extension recalled in §B.3.2. We also use the notation from there for elements of A_n and their conjugacy classes. The three corollaries are stated in §3.4.2.1 and proved in §3.4.2.2.

3.4.2.1. Examples with $G = A_n$.

12. Here and in §3.4.2.2 and §3.4.3.2, φ denotes the Euler function.
13. Here and in §3.4.2.2 and §3.4.3.2, we use the following classical fact: if $\sigma \in S_n$ has type $1^{n-l}l^1$ and a is a positive integer, then, with $d = \gcd(l, a)$, σ^a has type $1^{n-l}(l/d)^d$.

(a) *Mestre's realizations.* Assume that n is odd. In [Mes90], Mestre produces some G-extensions of $k(T)$ of group A_n with $n-1$ branch points and inertia canonical invariant $([1^{n-3}3^1], \dots, [1^{n-3}3^1])$. Let $E'_1/k(T)$ be such a G-extension.

Corollary 3.4.6. *Assume that k is hilbertian. Then the* G*-extension $E'_1/k(T)$ satisfies the* (geometric non A_n-parametricity) *condition.*

(b) *From the trinomials.* Let $E'_2/k(T)$ be a G-extension as in §B.3.2.

Corollary 3.4.7. (1) *Assume that $n \notin \{4,6\}$ and k is hilbertian. Then the* G*-extension $E'_2/k(T)$ satisfies the* (geometric non A_n-parametricity) *condition.*
(2) *Assume that $n = 6$ and k is either a number field or a finite extension of a rational function field $\kappa(U)$ with κ an arbitrary algebraically closed field of characteristic zero (and U an indeterminate). Then $E'_2/k(T)$ satisfies the* (geometric non A_n-parametricity) *condition.*

(c) *From the realization with four branch points.* Assume that $n \geq 6$ is even. As explained in [HRD03, §3.3], the G-extension $E_3/k(T)$ of part (c) of §3.4.1.1 provides a G-extension $E'_3/k(T)$ of group A_n with five branch points and inertia canonical invariant
- $([1^2((n-2)/2)^2], [1^{n-3}3^1], [1^{n-3}3^1], [1^2 2^{(n-2)/2}], [1^2 2^{(n-2)/2}])$ if $n/2$ is odd,
- $([1^2((n-2)/2)^2], [1^{n-3}3^1], [1^{n-3}3^1], [1^2 2^{n/2}], [1^2 2^{n/2}])$ if $n/2$ is even.

Note that, if $n \geq 8$, the branch point of $E'_3/k(T)$ corresponding to $[1^2((n-2)/2)^2]$ (in both cases) is $\mathbb{Q}$-rational from the branch cycle lemma.

Corollary 3.4.8. *Assume that k is hilbertian. Then the* G*-extension $E'_3/k(T)$ satisfies the* (geometric non A_n-parametricity) *condition.*

3.4.2.2. Proof of corollaries 3.4.6-3.4.8. As in the case $H = G = S_n$, the proof has two main parts. The first one consists in showing the following general result:

Let $E'/k(T)$ be a G*-extension of group A_n and $(C_1, \dots, C_r)$ be its inertia canonical invariant. Denote the set of all integers m such that $1 \leq m \leq n$ and $(m,n) = 1$ by I_n. Then $E'/k(T)$ satisfies the* (geometric non A_n-parametricity) *condition provided that either one of the following two conditions holds:*

(1) *k is hilbertian and one of the following four conditions holds:*
- (a) *n is odd and $[m^1((n-m)/2)^2]$ is not in the set $\{C_1, \dots, C_r\}$ for some odd $m \in I_n$,*
- (b) *n is odd and $[(m/2)^2(n-m)^1]$ is not in the set $\{C_1, \dots, C_r\}$ for some even $m \in I_n$,*
- (c) *n is even and $[(n/2)^2]$ is not in the set $\{C_1, \dots, C_r\}$,*
- (d) *$n \geq 8$ is even and neither $[2^1(n-2)^1]$ nor $[1^2((n-2)/2)^2]$ is in the set $\{C_1, \dots, C_r\}$.*

(2) *k is either a number field or a finite extension of a rational function field $\kappa(U)$ with κ an arbitrary algebraically closed field of characteristic zero (and U an indeterminate) and one of the following three conditions holds:*
- (a) *n is odd and neither $[n^1]_1$ nor $[n^1]_2$ is in the set $\{C_1, \dots, C_r\}$,*
- (b) *n is even and neither $[m^1(n-m)^1]_1$ nor $[m^1(n-m)^1]_2$ is in the set $\{C_1, \dots, C_r\}$ for some $m \in I_n$,*
- (c) *$n = 6$ and neither $[2^1 4^1]$ nor $[1^2 2^2]$ is in the set $\{C_1, \dots, C_r\}$.*

In particular, $E'/k(T)$ satisfies the (geometric non A_n-parametricity) *condition if $r \leq \varphi(n)/2$ and k is either a number field or a finite extension of a rational function field $\kappa(U)$ with κ an arbitrary algebraically closed field of characteristic zero.*

The second part consists next in checking that each G-extension $E'_i/k(T)$ $(i = 1,2,3)$ satisfies one of the conditions above.

Part 1. The proof is quite similar to that in the case $H = G = S_n$. It consists in each case in applying Inertia Criterion 2 (if k is assumed to be hilbertian) or Inertia Criterion 3 (if k is assumed to be either a number field or a finite extension of $\kappa(U)$) to some suitable G-extension $E'_j/k(T)$ $(j = 1, 2, 3)$ and the given one $E'/k(T)$.

Assume first that k is hilbertian. In case (1)-(a), the conjugacy class $[m^1((n-m)/2)^2]$ is not in the set $\{C_1^a, \dots, C_r^a \ / \ a \in \mathbb{N}\}$, *i.e.* condition (IC2-1) of Inertia Criterion 2 applied to the G-extensions $E'_2/k(T)$ and $E/k(T)$ holds. As condition (IC2-2) also holds, the conclusion follows. In case (1)-(b) (resp (1)-(c)), repeat the same argument with $[m^1((n-m)/2)^2]$ replaced by $[(m/2)^2(n-m)^1]$ (resp. by $[(n/2)^2]$). In case (1)-(d), the conjugacy class $[1^2((n-2)/2)^2]$ is not in the set $\{C_1^a, \dots, C_r^a \ / \ a \in \mathbb{N}\}$, *i.e.* condition (IC2-1) of Inertia Criterion 2 applied to the G-extensions $E'_3/k(T)$ and $E/k(T)$ holds. As condition (IC2-2) also holds, the conclusion follows.

Assume now that k is either a number field or a finite extension of a rational function field $\kappa(U)$ with κ an arbitrary algebraically closed field of characteristic zero. In case (2)-(a), at least one of the two conjugacy classes $[n^1]_1$ and $[n^1]_2$ is not in the set $\{C_1^a, \dots, C_r^a \ / \ a \in \mathbb{N}\}$, *i.e.* condition (IC3-1) of Inertia Criterion 3 applied to the G-extensions $E'_2/k(T)$ and $E/k(T)$ holds. As condition (IC3-2) also holds, the conclusion follows. In case (2)-(b), repeat the same argument with the two conjugacy classes $[n^1]_1$ and $[n^1]_2$ replaced by $[m^1(n-m)^1]_1$ and $[m^1(n-m)^1]_2$. In case (2)-(c), the conjugacy class $[1^2 2^2]$ is not in the set $\{C_1^a, \dots, C_r^a \ / \ a \in \mathbb{N}\}$, *i.e.* condition (IC3-1) of Inertia Criterion 3 applied to the G-extensions $E'_3/k(T)$ and $E/k(T)$ holds. As condition (IC3-2) also holds, the conclusion follows.

Part 2. Let $i \in \{1, 2, 3\}$.

(a) If $i = 1$, condition (1)-(a) holds (with $m = 1$).

(b) Assume that $i = 2$. If n is even and $n \geq 8$ (resp. $n = 6$), condition (1)-(d) (resp. condition (2)-(c)) holds. If n is odd and $m \in \{1, n-1\}$, condition (1)-(b) holds (with $m = 2$). If n is odd and $m \notin \{1, n-1\}$, condition (1)-(a) holds (with $m = 1$).

(c) If $i = 3$, condition (1)-(c) holds.

3.4.3 The case $H = A_n$ and $G = S_n$

Let $n \geq 4$ be an integer. The aims of this subsection are corollaries 3.4.9, 3.4.10 and 3.4.11 which give our main examples in the case $H = A_n$ and $G = S_n$. They involve the G-extensions of group S_n of §3.4.1.1. The three corollaries are stated in §3.4.3.1 and proved in §3.4.3.2.

3.4.3.1. Examples with $G = S_n$.

(a) *Morse polynomials.*

Corollary 3.4.9. (1) *Assume that $n \notin \{4, 6\}$ and k is hilbertian. Then the* G*-extension $E_1/k(T)$ satisfies the* (geometric non A_n-parametricity) *condition.*

(2) *Assume that $n \in \{4, 6\}$ and k is either a number field or a finite extension of a rational function field $\kappa(U)$ with κ an arbitrary algebraically closed field of characteristic zero (and U an indeterminate). Then $E_1/k(T)$ satisfies the* (geometric non A_n-parametricity) *condition.*

(b) *Trinomials.*

Corollary 3.4.10. (1) *Assume that $n \notin \{4, 6\}$ and k is hilbertian. Then the* G*-extension $E_2/k(T)$ satisfies the* (geometric non A_n-parametricity) *condition.*

(2) *Assume that $n = 6$ and k is either a number field or a finite extension of a rational function field $\kappa(U)$ with κ an arbitrary algebraically closed field of characteristic zero. Then the* G*-extension $E_2/k(T)$ satisfies the* (geometric non A_n-parametricity) *condition.*

(c) *A realization with four branch points.*

Corollary 3.4.11. *Assume that $n \geq 6$ is even and k is hilbertian. Then the* G*-extension $E_3/k(T)$ satisfies the* (geometric non A_n-parametricity) *condition.*

3.4.3.2. Proof of corollaries 3.4.9-3.4.11. As in the previous cases, the proof has two main parts. The first one consists in showing the following general result:

Let $E/k(T)$ be a G*-extension of group S_n and $(C_1, \dots, C_r)$ be its inertia canonical invariant. Denote the set of all integers m such that $1 \leq m \leq n$ and $(m, n) = 1$ by I_n. Then $E/k(T)$ satisfies the* (geometric non A_n-parametricity) *condition provided that either one of the following two conditions holds:*

(1) *k is hilbertian and one of the following conditions holds:*

(a) *n is odd and neither $[m^1(n-m)^1]$ nor $[m^1((n-m)/2)^2]$ is in the set $\{C_1, \dots, C_r\}$ for some odd $m \in I_n$,*

(b) *n is odd and neither $[m^1(n-m)^1]$ nor $[(m/2)^2(n-m)^1]$ is in the set $\{C_1, \dots, C_r\}$ for some even $m \in I_n$,*

(c) *n is even and neither $[n^1]$ nor $[(n/2)^2]$ is in the set $\{C_1, \dots, C_r\}$,*

(d) *$n \equiv 2 \bmod 4$, $n \neq 6$ and none of the classes $[1^2(n-2)^1]$, $[2^1(n-2)^1]$ and $[1^2((n-2)/2)^2]$ is in the set $\{C_1, \dots, C_r\}$,*

(e) *$n \equiv 0 \bmod 4$, $n \geq 6$ and none of the four classes $[1^2(n-2)^1]$, $[2^1(n-2)^1]$, $[1^2((n-2)/2)^2]$ and $[2^1((n-2)/2)^2]$ is in $\{C_1, \dots, C_r\}$,*

(2) *k is either a number field or a finite extension of a rational function field $\kappa(U)$ with κ an arbitrary algebraically closed field of characteristic zero (and U an indeterminate) and one of the following three conditions holds:*

(a) *n is odd and $[n^1]$ is not in the set $\{C_1, \dots, C_r\}$,*

(b) *n is even and $[m^1(n-m)^1]$ is not in the set $\{C_1, \dots, C_r\}$ for some $m \in I_n$,*

(c) *$n = 6$ and none of the classes $[1^2 4^1]$, $[2^1 4^1]$ and $[1^2 2^2]$ is in the set $\{C_1, \dots, C_r\}$.*

In particular, $E/k(T)$ satisfies the (geometric non A_n-parametricity) *condition if $r \leq \varphi(n)/2$ and k is either a number field or a finite extension of a rational function field $\kappa(U)$ with κ an arbitrary algebraically closed field of characteristic zero.*

The second part consists next in checking that each G-extension $E_i/k(T)$ $(i = 1, 2, 3)$ satisfies one of the conditions above.

Part 1. The proof is quite similar to those in the previous cases. It consists in each case in applying Inertia Criterion 2 (if k is assumed to be hilbertian) or Inertia Criterion 3 (if k is assumed to be either a number field or a finite extension of $\kappa(U)$) to some suitable G-extension $E'_j/k(T)$ $(j = 1, 2, 3)$ and the given one $E/k(T)$.

Assume first that k is hilbertian. In case (1)-(a), the conjugacy class $[m^1((n-m)/2)^2]$ is not in $\{C_1^a, \dots, C_r^a \ / \ a \in \mathbb{N}\}$, *i.e.* condition (IC2-1) of Inertia Criterion 2 applied to the G-extensions $E'_2/k(T)$ and $E/k(T)$ holds. As condition (IC2-2) also holds, the conclusion follows. In case (1)-(b) (resp (1)-(c)), repeat the same argument with $[m^1((n-m)/2)^2]$ replaced by $[(m/2)^2(n-m)^1]$ (resp. by $[(n/2)^2]$). In either one of cases (1)-(d) and (1)-(e), the conjugacy class $[1^2((n-2)/2)^2]$ is not in $\{C_1^a, \dots, C_r^a \ / \ a \in \mathbb{N}\}$, *i.e.* condition (IC2-1) of Inertia Criterion 2 applied to the G-extensions $E'_3/k(T)$ and $E/k(T)$ holds. As condition (IC2-2) also holds, the conclusion follows.

Assume now that k is either a number field or a finite extension of a rational function field $\kappa(U)$ with κ an arbitrary algebraically closed field of characteristic zero. In case (2)-(a), $[n^1]$ is not in the set $\{C_1^a, \dots, C_r^a \ / \ a \in \mathbb{N}\}$, *i.e.* condition (IC3-1) of Inertia Criterion 3 applied to the

G-extensions $E_2'/k(T)$ and $E/k(T)$ holds. As condition (IC3-2) also holds, the conclusion follows. In case (2)-(b), repeat the same argument with $[n^1]$ replaced by $[m^1(n-m)^1]$. In case (2)-(c), the conjugacy class $[1^2 2^2]$ is not in the set $\{C_1^a, \dots, C_r^a \ / \ a \in \mathbb{N}\}$, *i.e.* condition (IC3-1) of Inertia Criterion 3 applied to the G-extensions $E_3'/k(T)$ and $E/k(T)$ holds. As condition (IC3-2) also holds, the conclusion follows.

Part 2. Let $i \in \{1, 2, 3\}$.
(a) Assume that $i = 1$. If n is odd, condition (1)-(a) holds (with $m = 1$). If $n = 4$ (resp. $n = 6$), condition (2)-(b) (resp. condition (2)-(c)) holds. If $n \geq 8$ is even, either condition (1)-(d) or condition (1)-(e) holds.
(b) Assume that $i = 2$. If n is odd and $m \in \{1, n-1\}$, then condition (1)-(b) holds (with $m = 2$). If n is odd and $m \notin \{1, n-1\}$, then condition (1)-(a) holds (with $m = 1$). If $n \geq 8$ is even, either condition (1)-(d) or condition (1)-(e) holds. If $n = 6$, condition (2)-(c) holds.
(c) If $i = 3$, condition (1)-(c) holds.

3.4.4 Some other cases H is a non abelian simple group

We now give some examples involving some G-extensions of $k(T)$ provided by the rigidity method. We use below standard Atlas [C$^+$85] notation for conjugacy classes of finite groups.

3.4.4.1. Examples with $\mathrm{PSL}_2(\mathbb{F}_p)$. Let p be a prime ≥ 5 such that $(\frac{2}{p}) = -1$ (resp. $(\frac{3}{p}) = -1$) and $E_1/k(T)$ (resp. $E_2/k(T)$) be a G-extension of group $\mathrm{PSL}_2(\mathbb{F}_p)$ and inertia canonical invariant $(2A, pA, pB)$ (resp. $(3A, pA, pB)$) [Ser92, propositions 7.4.3-7.4.4 and theorem 8.2.2].

Corollary 3.4.12. *Assume that k is hilbertian and $(-1)^{(p-1)/2}p$ is a square in k. Then the two* G*-extensions $E_1/k(T)$ (if $(\frac{2}{p}) = -1$) and $E_2/k(T)$ (if $(\frac{3}{p}) = -1$) each satisfy the* (geometric non $\mathrm{PSL}_2(\mathbb{F}_p)$-parametricity) *condition.*

Proof. Let $E/k(T)$ be a G-extension of group $\mathrm{PSL}_2(\mathbb{F}_p)$ with three k-rational branch points and inertia canonical invariant $(2A, 3A, pA)$ [Ser92, proposition 7.4.2 and theorem 8.2.1]. Since 3 does not divide $2p$ (resp. 2 does not divide $3p$), condition (IC2-1) of Inertia Criterion 2 applied to the G-extensions $E/k(T)$ and $E_1/k(T)$ (resp. and $E_2/k(T)$) holds (remark 3.1.2). As condition (IC2-2) also holds, the conclusion follows. □

3.4.4.2. Examples with the Monster group. Let $E_1/k(T)$ be a G-extension of group the Monster group M as in §B.3.3 and $E_2/k(T)$ be a G-extension of group M with three k-rational branch points and corresponding ramification indices 2, 3, 71 [Tho84] (if -71 is a square in k). Applying twice Inertia Criterion 2 (and remark 3.1.2) to these G-extensions leads to corollary 3.4.13 below:

Corollary 3.4.13. *Assume that k is hilbertian and -71 is a square in k. Then the two* G*-extensions $E_1/k(T)$ and $E_2/k(T)$ each satisfy the* (geometric non M-parametricity) *condition.*

3.4.4.3. Examples with $H \neq G$. Let $E/k(T)$ be a G-extension of group the Baby-Monster group B and inertia canonical invariant $(2C, 3A, 55A)$ [MM99, chapter II, proposition 9.6 and chapter I, theorem 4.8].

Corollary 3.4.14. *Assume that k is hilbertian. Then, with* Th *the Thompson group, the* G*-extension $E/k(T)$ satisfies the* (geometric non Th-parametricity) *condition.*

Proof. It suffices to apply Inertia Criterion 2 (and remark 3.1.2) to $E'/k(T)$ and $E/k(T)$ where $E'/k(T)$ is any G-extension of group Th with three k-rational branch points and inertia canonical invariant $(2A, 3A, 19A)$ [MM99, chapter II, proposition 9.5 and chapter I, theorem 4.8]. □

Any finite group H is a subgroup of $G = S_n$ provided that $n \geq |H|$. This allows us to give some examples of non H-parametric extensions of group S_n for some suitable integers n. For instance, the G-extension $E_1/k(T)$ of part (a) of §3.4.1.1 satisfies the following:

Corollary 3.4.15. *Let n be an integer ≥ 604800. Assume that either one of the following two conditions holds:*
(1) $7 \not| n$ *and k is hilbertian,*
(2) $5 \not| n$ *and k is either a number field or a finite extension of a rational function field $\kappa(U)$ with κ an arbitrary algebraically closed field of characteristic zero (and U an indeterminate).*
Then, with J_2 *the Hall-Janko group, the* G*-extension* $E_1/k(T)$ *satisfies the* (geometric non J_2-parametricity) *condition.*

Proof. It suffices to apply Inertia Criterion 2 if condition (1) holds or Inertia Criterion 3 if condition (2) holds (and remark 3.1.2 in both situations) to $E/k(T)$ and $E_1/k(T)$ where $E/k(T)$ denotes any G-extension of group J_2, inertia canonical invariant $(5A, 5B, 7A)$ and such that the branch point corresponding to $7A$ is k-rational [Ser92, proposition 7.4.7 and theorem 8.2.2]. □

3.4.5 The case H is a p-group

Let G be a finite group, p be a prime divisor of the order of G and $E/k(T)$ be a G-extension of group G.

Corollary 3.4.16. *Assume that the following two conditions hold:*
(1) *none of the ramification indices of the branch points is a multiple of p,*
(2) *k is either a number field or a finite extension of a rational function field $\kappa(U)$ with κ an arbitrary algebraically closed field of characteristic zero (and U an indeterminate).*
Then $E/k(T)$ satisfies the (geometric non H-parametricity) *condition for any p-subgroup $H \subset G$ which occurs as the Galois group of a* G*-extension of $k(T)$. Furthermore condition (2) may be removed in the case $p = 2$ and $H = \mathbb{Z}/2\mathbb{Z}$.*

Remark 3.4.17. Assume that k is a number field. Under condition (1), one has the following two conclusions.
(a) *The* G*-extension $E/k(T)$ satisfies the* (geometric non $\mathbb{Z}/p\mathbb{Z}$-parametricity) *condition.*
(b) *There exists some finite extension k'/k such that the* G*-extension $Ek'/k'(T)$ satisfies the* (geometric non H-parametricity) *condition for any p-subgroup $H \subset G$.*
In the case k is a finite extension of a rational function field $\kappa(U)$ with κ an arbitrary algebraically closed field of characteristic zero, then, under condition (1), conclusion (b) holds with $k' = k$.

Corollary 3.4.16 may be applied to various G-extensions of $k(T)$. For example, consider those of group the Conway group Co_1 and inertia canonical invariant $(3A, 5C, 13A)$ [MM99, chapter II, proposition 9.3 and chapter I, theorem 4.8]: the set of prime divisors of $|\mathrm{Co}_1|$ is $\{2, 3, 5, 7, 11, 13, 23\}$ and condition (1) holds for any prime p in $\{2, 7, 11, 23\}$. Moreover many G-extensions of $k(T)$ recalled in this chapter also satisfy condition (1) (for suitable primes p).

Proof. Given a p-subgroup $H \subset G$ as in corollary 3.4.16, the conclusion follows from Inertia Criterion 3 (and remark 3.1.2) applied to any G-extension $E_H/k(T)$ of group H and the given one $E/k(T)$. In the special case $p = 2$ and $H = \mathbb{Z}/2\mathbb{Z}$, take $E_H = k(\sqrt{T})$ and use Inertia Criterion 1 (instead of Inertia Criterion 3). □

Part III

Presentation of part III

The central question

Given a field k, the main theme of the third part of this thesis, which is a joint work with P. Dèbes, is whether a given k-étale algebra $\prod_l F_l/k$ is the specialization of a given k-cover $f : X \to B$ of the same degree at some unramified point $t_0 \in B(k)$. The classical Hilbert specialization property corresponds to the special case k-étale algebras are taken to be single field extensions F/k and the answer is positive for at least one of them.

This question has already been investigated in the three papers [Dèb99c], [DG12] and [DG11] for k-G-covers. The aim of this part is to handle the situation of arbitrary k-covers.

The twisting lemma

Our main tool is a *twisting lemma* which gives a general answer to the question: under certain hypotheses, *the answer is* Yes *if there exist unramified k-rational points on the covering space $\widetilde{X}$ of certain twisted covers $\widetilde{f} : \widetilde{X} \to B$*. This lemma has several variants. A practical first one, for k-G-covers, was established in [Dèb99c] for covers of $\mathbb{P}^1$ and in [DG12] for a general base space. We first use it in chapter 4 to obtain a practical second one, for regular k-covers of degree n and geometric monodromy group S_n (lemma 4.1.1). We then prove in chapter 5 the more general variants shown on the top row of the following diagram, which indicates that they generalize the two previous ones, shown on the bottom row.

$$\begin{array}{ccc} \text{Galois} & \Leftrightarrow & \text{general} \\ \Downarrow & & \Downarrow \\ \text{regular Galois} & \Rightarrow & \text{monodromy } S_n \end{array}$$

The *Galois* variant is for the situation $f : X \to B$ is a k-G-Galois cover (not necessarily regular [1]); it is proved in §5.1.1 (lemma 5.1.2). The *general* variant is proved in §5.1.2 and concerns arbitrary k-covers, regular or not, Galois or not (lemma 5.1.4). Implication $\Rightarrow$ in the upper row means that the general variant will be obtained from the Galois variant. We will also be interested in the converse in the twisting lemma: the answer to the original question is Yes *if and only if* there exist unramified k-rational points on the twisted varieties $\widetilde{X}$.

The twisting lemma is a geometric *avatar* of an argument of Tchebotarev known as the *Field Crossing Argument* and which notably appears in the proof of the Tchebotarev density theorems over global fields and in the theory of PAC fields (see [FJ05]). The twisting lemma formalizes the core of the argument and produces a geometric tool: the variety $\widetilde{X}$. This allows a unifying approach over an arbitrary base field: questions are reduced to finding rational points on $\widetilde{X}$. The twisted cover $\widetilde{f} : \widetilde{X} \to B$, which appeared first in [Dèb99c] and [Dèb99d], could also be

1. Note that the Galois closure of a given k-cover $f : X \to B$ is not regular in general, even if f is regular.

defined by using the language of torsors. Another related approach using an embedding problem presentation has also been recently proposed by Bary-Soroker [BS12].

Varying the base field and applications

We then investigate the remaining problem of finding rational points on $\widetilde{X}$ over various base fields where classical diophantine techniques can be used: PAC fields, finite fields, complete valued fields, global fields, ample fields. We present our main applications below in connection with those of previous works.

PAC fields

Over a PAC [2] field k, the regular Galois variant was first used in [Dèb99c] to prove that, given a finite group G and a subgroup $H \subset G$, any Galois extension F/k of group H occurs as a specialization of any k-G-cover $f : X \to \mathbb{P}^1$ of group G (thereby solving the Beckmann-Black problem over PAC fields). We then prove in chapter 4 a non Galois analog with an arbitrary k-étale algebra $\prod_l F_l/k$ of degree n replacing the Galois extension F/k under the assumption that f is a regular k-cover of degree n and geometric monodromy group S_n (corollary 4.2.1). We refine in chapter 5 the above Galois result (the regularity assumption is relaxed; see corollary 5.2.1) and give a variant of the non Galois one (allowing more general monodromy groups; see corollary 5.2.2). Similar applications over PAC fields can also be found in two papers of Bary-Soroker [BS09] [BS12].

The general spirit of these results is that, over a PAC field, there is no diophantine obstruction [3] to a given étale algebra being a specialization of a given cover; obstructions only come from Galois theory. This has some impact on the arithmetic of PAC fields; one obtains for example the following statement (corollary 4.3.1):

Theorem 1. *Let k be a PAC field of characteristic $p \geq 0$. Then one has the following two conclusions.*
(1) *Any extension of k of degree n with $p \nmid n(n-1)$ can be realized by a trinomial $Y^n - Y + b \in k[Y]$.*
(2) *If $p \neq 2$, the separable closure k^{sep} is generated by all elements $y \in k^{\mathrm{sep}}$ such that $y^n - y \in k$ for some $n \geq 2$, which can be taken to be $n = [k(y) : k]$ if $p = 0$.*

Finite fields

Over a finite field $k = \mathbb{F}_q$, the regular Galois variant was used in [DG11] to prove that, given a finite group G and a cyclic subgroup $H \subset G$, any Galois extension $F/\mathbb{F}_q$ of group H is a specialization of any $\mathbb{F}_q$-G-cover $f : X \to \mathbb{P}^1$ of group G provided that q be large enough. We then prove in chapter 4 a non Galois analog with an arbitrary $\mathbb{F}_q$-étale algebra $\prod_l F_l/\mathbb{F}_q$ of degree n replacing the Galois extension $F/\mathbb{F}_q$ under the assumption that f is a regular $\mathbb{F}_q$-cover of degree n and geometric monodromy group S_n (corollary 4.2.2). Moreover the twisting lemma can be combined with Lang-Weil to obtain an estimate for the number of points $t_0 \in \mathbb{F}_q$ at which $\prod_l F_l/\mathbb{F}_q$ is a specialization of f (corollary 5.2.3). This type of result is known in the literature as *a Tchebotarev theorem for function fields over finite fields.* For example, if $\prod_l F_l/\mathbb{F}_q$ is the single field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ of degree n, the estimate is of the form $q/n + O(\sqrt{q})$. In the specific case

2. See §B.2.1 for the definition and some examples of PAC fields.
3. in the sense that the existence of rational points on some variety, which is a condition of our twisting lemma in general, is automatic over a PAC field.

f is given by the trinomial $Y^n + Y - T$, it yields results of Cohen and Ree proving a conjecture of Chowla. See §5.2.2 for details and references.

Over finite fields $\mathbb{F}_q$, the same general spirit as for PAC fields can be retained - no diophantine obstruction to the problem -, but provided that q be large enough.

Number fields

The local-global situation of a number field k given with some completions k_v was central in [DG12]. The main result there was a *Hilbert-Grunwald* theorem showing that every G-extension $E/k(T)$ of group G has specializations at points $t_0 \in k$ which are Galois extensions of group G (*Hilbert*) with the extra property that they induce prescribed unramified extensions F^v/k_v of Galois group $H_v \subset G$ at each finite place v in a given finite set $\mathcal{S}$ (*Grunwald*), the only condition on the places being that the residue fields be large enough and of order prime to the order of G. We then prove in chapter 4 a non Galois analog for regular extensions of $\mathbb{Q}(T)$ of degree n and geometric monodromy group S_n (corollary 4.3.6):

Theorem 2. *Let $E/\mathbb{Q}(T)$ be a regular extension of degree n and with S_n as Galois group of its Galois closure over $\overline{\mathbb{Q}}$. Let $\mathcal{S}$ be a finite set of large enough prime numbers p (depending on $E/\mathbb{Q}(T)$), each given with positive integers $d_{p,1}, \dots, d_{p,s_p}$ of sum n. Then there exist infinitely many distinct $t_0 \in \mathbb{Q}$ such that the following two conditions hold:*
(1) *the specialization algebra of $E/\mathbb{Q}(T)$ at t_0 consists of a single field extension $E_{t_0}/\mathbb{Q}$ of degree n (Hilbert),*
(2) *$E_{t_0}/\mathbb{Q}$ has residue degrees $d_{p,1}, \dots, d_{p,s_p}$ at each prime $p \in \mathcal{S}$ (Grunwald).*

A refinement of this result is given in chapter 5 for arbitrary regular finite extensions of $k(T)$ with k an arbitrary number field (corollary 5.2.9). On the way, the following typical result of Fried is reproved (and generalized): if the Galois group over $\overline{\mathbb{Q}}(T)$ of a polynomial $P(T, Y) \in \mathbb{Q}[T][Y]$ of degree n (with respect to Y) contains an n-cycle, then the associated Hilbert subset contains infinitely many distinct arithmetic progressions with ratio a prime number. See §5.2.4 for details and references.

Here it is the relative flexibility of the local extensions obtained from global specializations which is the striking phenomenon [4]. In the Galois situation, the existence of global extensions with such local properties may sometimes even be questioned. Recall for example that results of [DG12] lead to some obstruction to the Regular Inverse Galois Problem (yet unproved to be not vacuous) related to some analytic questions around the Tchebotarev density theorem.

Other local-global situations can be considered, for example that of a base field which is a rational function field $\kappa(U)$ with κ a large enough finite field or a PAC field with enough cyclic extensions (and U an indeterminate). We refer to [DG11] where these cases have been considered.

Ample fields

Over an ample [5] field k, the regular Galois variant was first used in [Dèb99c, §3.3.2] to prove that, if a given k-G-cover of $\mathbb{P}^1$ specializes to some Galois extension F/k at some unramified point $t_0 \in \mathbb{P}^1(k)$, then it specializes to the same Galois extension at infinitely many distinct unramified points $t \in \mathbb{P}^1(k)$. We then prove in chapter 5 a refined form of this statement for arbitrary k-covers (corollary 5.2.4).

4. Note indeed that there is some diophantine obstruction to the problem in the number field case as finding rational points on varieties over such fields can be a difficult question.

5. See §B.2.2 field for the definition and some examples of ample fields.

An application to Hurwitz spaces

In addition to theorems 1 and 2 above, we have a third main application. Theorem 3 below concerns Hurwitz moduli spaces of covers of $\mathbb{P}^1$ with fixed branch point number and fixed monodromy group.

Recall that Hurwitz spaces are an important tool of the arithmetic of covers as the fields of definition of their points correspond to the fields of moduli of the covers they represent; in particular, the Regular Inverse Galois Problem over a given field k can be reduced to the search of k-rational points on them. Theorem 3 considers two cases, somewhat opposite to one another: k is PAC field and k is a number field, and shows that points can be found with a field of definition satisfying some more or less restrictive properties.

Let H be a geometrically irreducible component of some Hurwitz space defined over a field k and N be the degree of the definition field of the cover corresponding to the generic point of H over that of its branch point divisor; N is also the degree of the natural cover $\mathsf{H} \rightarrow \mathsf{U}_r$ of the configuration space U_r for finite subsets of $\mathbb{P}^1$ of cardinality r (see §4.3.3). We also make this assumption which can be checked in practice: the Hurwitz braid action restricted to H generates all of S_N (more formally, S_N is the geometric monodromy group of the cover $\mathsf{H} \rightarrow \mathsf{U}_r$).

Theorem 3. (corollary 4.3.8) *Consider the subset $\mathcal{U} \subset \mathsf{U}_r(k)$ of all $\mathbf{t}_0$ such that the set $\mathsf{H}_{\mathbf{t}_0}$ of $\overline{k}$-covers $f : X \rightarrow \mathbb{P}^1$ in H with branch divisor $\mathbf{t}_0$ satisfies the following condition* (in each case)*:*

(1) (case k is a PAC field of characteristic 0) *given s finite extensions F_l/k such that $\sum_{l=1}^{s}[F_l : k] = N$, there are s $\overline{k}$-covers in $\mathsf{H}_{\mathbf{t}_0}$, say $f_1, \ldots, f_s$, which have smallest definition fields $F_1, \ldots, F_s$ respectively, and the $N - s$ others are k-conjugates of $f_1, \ldots, f_s$,*

(2) (case k is a number field) *the following two conditions hold:*

(a) *the field of moduli of each cover $f \in \mathsf{H}_{\mathbf{t}_0}$ is an extension of k of degree N,*

(b) *for each v in a given finite set of finite places of k with large enough residue characteristic (depending on H) and every associated partition $\{d_{v,1} \ldots, d_{v,s_v}\}$ of the integer N, the smallest fields of definition of the covers $f \otimes_{\overline{k}} \overline{k_v}$ ($f \in \mathsf{H}_{\mathbf{t}_0}$) are the unramifed extensions of k_v of degree $d_{v,1}, \ldots, d_{v,s_v}$.*

Then (in each case) *$\mathcal{U}$ is a Zariski-dense subset of $\mathsf{U}_r(k)$.*

Chapter 4

Specialization results in Galois theory

4.1 The monodromy S_n form of the twisting lemma

Let k be a field, $f : X \to B$ be a regular k-cover, n be its degree and $\prod_{l=1}^{s} F_l/k$ be a k-étale algebra of degree n. The question we address is whether $\prod_{l=1}^{s} F_l/k$ is the specialization algebra of f at some unramified point $t_0 \in B(k)$. The twisting lemma 4.1.1 below gives a sufficient condition for the answer to be affirmative.

4.1.1 Statement of the twisting lemma 4.1.1

Let $g : Z \to B$ be the Galois closure of f and N/k be the *compositum* inside k^{sep} of the Galois closures of the extensions $F_1/k, \dots, F_s/k$; set $H = \mathrm{Gal}(N/k)$. Let $\varphi : \mathrm{G}_k \to H$ be the G-Galois representation of N/k (relative to k^{sep}) and $\mu : H \to S_n$ be the Galois representation of $\prod_{l=1}^{s} F_l/k$ relative to N. The map $\mu \circ \varphi : \mathrm{G}_k \to S_n$ is then the Galois representation of $\prod_{l=1}^{s} F_l/k$ relative to k^{sep}.

The *twisted cover* $\widetilde{g}^{\mu\varphi} : \widetilde{Z}^{\mu\varphi} \to B$ in the result below is a regular k-cover obtained by twisting the k-G-cover $g : Z \to B$ by the morphism $\mu \circ \varphi : \mathrm{G}_k \to S_n$. Its definition is given in [DG12, §2.2] and is recalled in §4.1.2. It is in particular a *k-model of* $g \otimes_k k^{\mathrm{sep}}$ (*i.e.* $\widetilde{g}^{\mu\varphi} \otimes_k k^{\mathrm{sep}} \simeq g \otimes_k k^{\mathrm{sep}}$); it depends on the k-étale algebra $\prod_{l=1}^{s} F_l/k$ only *via* the *compositum* N/k.

Twisting lemma 4.1.1 (monodromy S_n form)**.** *Assume that $f : X \to B$ has geometric monodromy group S_n. Then, for each unramified point $t_0 \in B(k)$,*

if (1) *there exists some point $x_0 \in \widetilde{Z}^{\mu\varphi}(k)$ such that $\widetilde{g}^{\mu\varphi}(x_0) = t_0$,*

then (2) *$\prod_l F_l/k$ is the specialization algebra $\prod_l k(X)_{t_0,l}/k$ of f at t_0.*

In the case $B = \mathbb{P}^1$, using lemma B.1.3 provides a polynomial form of the statement for which the regular k-cover f is replaced by a monic polynomial $P(T,Y) \in k[T][Y]$ of degree n (with respect to Y) and Galois group S_n over $\overline{k}(T)$. For any $t_0 \in k$ such that the specialized polynomial $P(t_0, Y)$ is separable over k, implication (1) $\Rightarrow$ (2) holds with condition (2) translated as follows:

(2') *the polynomial $P(t_0,Y)$ factors as a product $\prod_{l=1}^{s} Q_l(Y)$ of irreducible polynomials $Q_l(Y)$ over k such that, for each index $l \in \{1, \dots, s\}$, the extension F_l/k is generated by one of the roots of $Q_l(Y)$.*

4.1.2 Proof of the twisting lemma 4.1.1

Since the regular k-cover $f : X \to B$ is of degree n and the Galois group $\mathrm{Gal}(k^{\mathrm{sep}}(Z)/k^{\mathrm{sep}}(B))$ is assumed to be isomorphic to S_n, the same is true of $\mathrm{Gal}(k(Z)/k(B))$. Hence $k(Z)$ is a regular extension of k, or, in other words, $g : Z \to B$ is a k-G-cover. Let $\phi : \pi_1(B \setminus D, t)_k \to S_n$ be the corresponding π_1-representation (with D the branch divisor of f).

We will now twist the k-G-cover $g : Z \to B$ by the morphism $\mu \circ \varphi : \mathrm{G}_k \to S_n$. We recall below the definition of the twisted cover.

With $\mathrm{Per}(S_n)$ the permutation group of the set S_n, consider then the map

$$\widetilde{\phi}^{\mu\varphi} : \pi_1(B \setminus D, t)_k \to \mathrm{Per}(S_n)$$

defined by the following formula, with r the restriction $\pi_1(B \setminus D, t)_k \to \mathrm{G}_k$: for any $\theta \in \pi_1(B \setminus D, t)_k$ and any $x \in S_n$,

$$\widetilde{\phi}^{\mu\varphi}(\theta)(x) = \phi(\theta)\; x\; (\mu \circ \varphi \circ r)(\theta)^{-1}$$

It is easily checked that $\widetilde{\phi}^{\mu\varphi}$ is a group homomorphism. Moreover its restriction to $\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}$ is obtained by composing that of the original π_1-representation ϕ with the left-regular representation of S_n. Hence the corresponding action of $\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}$ is transitive, thus showing that $\widetilde{\phi}^{\mu\varphi} : \pi_1(B \setminus D, t)_k \to \mathrm{Per}(S_n)$ is the π_1-representation of some regular k-cover. We denote it by $\widetilde{g}^{\mu\varphi} : \widetilde{Z}^{\mu\varphi} \to B$ and call it the *twisted cover* of g by the morphism $\mu \circ \varphi$; it is in particular a k-model of the (regular) k^{sep}-cover $g \otimes_k k^{\mathrm{sep}}$. The twisted cover $\widetilde{g}^{\mu\varphi} : \widetilde{Z}^{\mu\varphi} \to B$ was defined in [DG12] (and originally in [Dèb99c]) where is also given its main property which we use below.

Let $t_0 \in B(k) \setminus D$. Assume that condition (1) holds, *i.e.* there exists some point $x_0 \in \widetilde{Z}^{\mu\varphi}(k)$ such that $\widetilde{g}^{\mu\varphi}(x_0) = t_0$. Then, by [DG12, lemma 2.1], there exists some $\omega \in S_n$ such that, for any $\tau \in \mathrm{G}_k$, we have

$$\phi(\mathsf{s}_{t_0}(\tau)) = \omega\; (\mu \circ \varphi)(\tau)\; \omega^{-1}$$

with $\mathsf{s}_{t_0} : \mathrm{G}_k \to \pi_1(B \setminus D, t)_k$ the section associated with t_0.

Denote next the s orbits of $\mu : H \to S_n$, which are the same as those of $\mu \circ \varphi : \mathrm{G}_k \to S_n$, by $\mathcal{O}_1, \ldots, \mathcal{O}_s$; they correspond to the extensions $F_1, \ldots F_s$. Fix one of these orbits, *i.e.* an index $l \in \{1, \ldots, s\}$, and let $i \in \{1, \ldots, n\}$ be an index such that F_l is the fixed field in k^{sep} of the subgroup of G_k fixing i *via* the action $\mu \circ \varphi$.

Then, for $j = \omega(i)$ and any $\tau \in \mathrm{G}_k$, we have

$$\phi(\mathsf{s}_{t_0}(\tau))(j) = \omega\, (\mu \circ \varphi)(\tau)\, (i)$$

and so j is fixed by $\phi \circ \mathsf{s}_{t_0}(\tau)$ if and only if i is fixed by $(\mu \circ \varphi)(\tau)$. Hence the specialization $k(X)_{t_0,j}$ and the field F_l coincide. The conclusion then follows from the one-one correspondence between the orbits of $\mu \circ \varphi$ and those of $\phi \circ \mathsf{s}_{t_0}$ provided by ω (namely the orbit of i under $\mu \circ \varphi$ is the same as that of $\omega(i)$ under $\phi \circ \mathsf{s}_{t_0}$).

Remark 4.1.2. The proof shows further that, if condition (1) of the twisting lemma 4.1.1 holds for a given point $t_0 \in B(k) \setminus D$, then the Galois group $\mathrm{Gal}(k(Z)_{t_0}/k)$ of the specialization of g at t_0 is conjugate in S_n to the image group $\mu(H)$.

4.2 Varying the base field

We investigate below the remaining problem of finding k-rational points on the twisted variety $\widetilde{Z}^{\mu\varphi}$ over various base fields k. We start in §4.2.1 with the case of PAC fields and next consider the case of finite fields in §4.2.2. These two cases, for which, as already said in the presentation, various forms of the results also exist in the literature, are presented here as special cases of our unifying approach. §4.2.3 and §4.2.4 give newer applications, to the two cases k is a complete valued field and k is a global field. For this section, let n be a positive integer.

4.2.1 PAC fields

In the case k is a PAC [1] field, condition (1) of the twisting lemma 4.1.1 holds for any point t_0 in a Zariski-dense [2] subset of $B(k) \setminus D$; consequently so does condition (2).

Corollary 4.2.1. *Let k be a PAC field, $f : X \to B$ be a regular k-cover of degree n and geometric monodromy group S_n and $\prod_{l=1}^s F_l/k$ be a k-étale algebra of degree n. Then $\prod_{l=1}^s F_l/k$ is the specialization algebra of f at any point t_0 in a Zariski-dense subset of $B(k) \setminus D$ (with D the branch divisor of f).*

We refer to corollary 5.2.2 for a refined statement devoted to arbitrary k-covers of degree n. As a special case, we reobtain [BS09, corollary 1.4]: if $P(T, Y) \in k[T][Y]$ is a monic polynomial of degree n (with respect to Y) and Galois group S_n over $\overline{k}(T)$ and F/k is a separable extension of degree n, then there exist infinitely many distinct $t_0 \in k$ such that the specialized polynomial $P(t_0, Y)$ is irreducible over k and has a root in $\overline{k}$ which generates F over k (lemma B.1.3).

4.2.2 Finite fields

Assume that k is the finite field $\mathbb{F}_q$ and consider the case of covers of $\mathbb{P}^1$ (for simplicity). From the Lang-Weil estimates for the number of rational points on a curve over $\mathbb{F}_q$, condition (1) of the twisting lemma 4.1.1 holds for at least one unramified point $t_0 \in \mathbb{P}^1(\mathbb{F}_q)$ if $q + 1 - 2\widetilde{\mathrm{g}}\sqrt{q} > \widetilde{r}\widetilde{d}$ with $\widetilde{r}$ the branch point number of the regular $\mathbb{F}_q$-cover $\widetilde{g}^{\mu\varphi}$ there, $\widetilde{d}$ its degree and $\widetilde{\mathrm{g}}$ the genus of its covering space $\widetilde{Z}^{\mu\varphi}$.

Corollary 4.2.2. *Let $f : X \to \mathbb{P}^1$ be a regular $\mathbb{F}_q$-cover of degree n, with r branch points and of geometric monodromy group S_n. Assume that $q \geq (rn!)^2$. Then, for every choice of positive integers $m_1, \ldots, m_s$ such that $\sum_{l=1}^s m_l = n$, there exists at least one unramified point $t_0 \in \mathbb{F}_q$ such that $\prod_{l=1}^s \mathbb{F}_{q^{m_l}}/\mathbb{F}_q$ is the specialization algebra of f at t_0.*

We refer to corollary 5.2.3 for an estimate of the number of points $t_0 \in \mathbb{F}_q$ at which the conclusion holds.

Proof. It suffices to show that $q \geq (rn!)^2$ guarantees $q+1-2\widetilde{\mathrm{g}}\sqrt{q} > \widetilde{r}\widetilde{d}+\widetilde{d}$; the extra $\widetilde{d}$ in the right-hand side term is here to assure that t_0 can be chosen different from ∞. As $\widetilde{g}^{\mu\varphi} \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q} \simeq g \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$ (where $g : Z \to \mathbb{P}^1$ is as before the Galois closure of f), $\widetilde{r}$ is the branch point number r of g, which is the same as that of f, $\widetilde{\mathrm{g}}$ is the genus, say g, of Z and one has $\widetilde{d} = n!$.

One may obviously assume that $d = n! > 1$. With $\mathcal{R}$ the ramified point number on $Z \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$, the Riemann-Hurwitz formula provides $2\mathrm{g} - 2 = -2d + rd - \mathcal{R}$ (and then $r \geq 2$). Hence $\mathrm{g} = (rd/2 - 1) + (2 - d - \mathcal{R}/2) < rd/2 - 1$ as $2 - d - \mathcal{R}/2 \leq 2 - d - r/2 < 0$. If $\sqrt{q} \geq rd$, we obtain

$$\begin{aligned} q + 1 - 2\,\mathrm{g}\,\sqrt{q} &> rd\,\sqrt{q} + 1 + \sqrt{q}\,(2 - rd) \\ &\geq 2rd + 1 \\ &\geq rd + d \end{aligned}$$

□

4.2.3 Complete valued fields

Assume that k is the quotient field of some complete discrete valuation ring A. Denote the valuation ideal by $\mathfrak{p}$, the residue field by κ, assumed to be perfect, and its characteristic by $p \geq 0$. A given k-étale algebra $\prod_{l=1}^s F_l/k$ is said to be *unramified* if each extension F_l/k is unramified.

1. See §B.2.1 for the definition and some examples of PAC fields.
2. but not necessarily Zariski-open.

Let B be a smooth projective and geometrically irreducible k-variety given with an integral smooth projective model $\mathcal{B}$ over A. Let $f : X \to B$ be a regular k-cover of degree n and branch divisor D. Denote the Zariski closure of D in $\mathcal{B}$ by $\mathcal{D}$, the normalization of $\mathcal{B}$ in $k(X)$ by $\mathcal{F} : \mathcal{X} \to \mathcal{B}$ and its special fiber by $\mathcal{F}_0 : \mathcal{X}_0 \to \mathcal{B}_0$.

In corollary 4.2.3 below, the constant $c(f, \mathcal{B})$ only depends on f and $\mathcal{B}$. It is the constant c of [DG12, lemma 2.4] for $g : Z \to B$ the Galois closure of f; see remark 4.2.4 for more on this constant. As to condition (good-red), it assures "good reduction" of the cover as more precisely recalled in the proof of corollary 4.2.3; a more elementary characterization of it in the case $\mathcal{B} = \mathbb{P}^1_A$ is given at the beginning of §4.3.2.

Corollary 4.2.3. *Let $\prod_{l=1}^{s} F_l/k$ be an unramified k-étale algebra of degree n. Assume that the geometric monodromy group of $f$is S_n and that these further two conditions hold:*

(good-red) $p = 0$ *or* $p > n$*, each irreducible component of* $\mathcal{D}$ *is smooth over* A*,* $\mathcal{D} \cup \mathcal{B}_0$ *is a sum of irreducible regular divisors with normal crossings over* A *and there is no vertical ramification at* $\mathfrak{p}$ *in the Galois closure* $g : Z \to B$ [3].

(κ-big-enough) κ *is either a PAC field or a finite field of order* $q \geq c(f, \mathcal{B})$.

Then there exist points $t_0 \in B(k) \setminus D$ such that $\prod_{l=1}^{s} F_l/k$ is the specialization algebra of f at t_0. More precisely, the set of such points t_0 contains the preimage via the map $\mathcal{B}(A) \to \mathcal{B}_0(\kappa)$ of a non-empty subset $F \subset \mathcal{B}_0(\kappa) \setminus \mathcal{D}_0$.

Remark 4.2.4. The constant $c(f, \mathcal{B})$ *a priori* depends on q *via* its dependence on $\mathcal{B}$. Thus it is important to have a precise description of it or otherwise the finite field part of corollary 4.2.3 could be vacuous (if $c(f, \mathcal{B}) > q$ for example). From [DG12, addendum 2.5], for each prime $\ell \neq p$, a constant c_ℓ is given there and $c(f, \mathcal{B})$ should be bigger than one of these c_ℓ. For $\mathcal{B} = \mathbb{P}^1_A$, one can be quite explicit: $q \geq c(f, \mathcal{B})$ should imply $q + 1 - 2g\sqrt{q} > r\, n!$; as shown in the proof of corollary 4.2.2, it suffices to take $c(f, \mathcal{B}) = (r n!)^2$ with r the branch point number (and then the desired t_0 can even be chosen $\neq \infty$). In the general case, the description given in [DG12, addendum 2.5] shows that $c(f, \mathcal{B})$ is "geometric", in the sense that it can be kept unchanged if f is replaced by $f \otimes_k k'$ for any separable base extension k'/k. This allows applications for a given cover and large enough base fields. We also recall in addendum 4.2.5 that, in a global situation, $c(f, \mathcal{B})$ can be chosen independent of the place; this leads to other applications for a given cover and "large enough places" (see §4.3.2).

Proof. Let $\widetilde{g}^{\mu\varphi} : \widetilde{Z}^{\mu\varphi} \to B$ be the regular k-cover of the twisting lemma 4.1.1. From there, it suffices to show that $\widetilde{Z}^{\mu\varphi}$ has k-rational points. This (and the more precise conclusion of corollary 4.2.3) is explained in proposition 2.2 and lemma 2.4 of [DG12] which we summarize below.

Denote the normalization of $\mathcal{B}$ in $k(Z)$ by $\mathcal{G} : \mathcal{Z} \to \mathcal{B}$. Assumption (good-red) holds for $\mathcal{G}$ as it holds for $\mathcal{F}$ (f and g have the same branch divisor) and the Galois extension N/k (which is as before the *compositum* inside k^{sep} of the Galois closures of the extensions $F_1/k, \ldots, F_s/k$) is unramified (*compositum* of unramified extensions). These two conditions guarantee that the morphism $\widetilde{\mathcal{G}}^{\mu\varphi} : \widetilde{\mathcal{Z}}^{\mu\varphi} \to \mathcal{B}$ obtained by normalizing $\mathcal{B}$ in $k(\widetilde{Z}^{\mu\varphi})$ has good reduction [DG12, proposition 2.2]; more precisely, the proof of this result shows that $\widetilde{\mathcal{G}}^{\mu\varphi}$ is flat, étale above $\mathcal{B} \setminus \mathcal{D}$ and the special fiber $\widetilde{\mathcal{Z}}_0^{\mu\varphi}$ is normal and geometrically irreducible [DG12, §2.4.1–4]. Assumption (κ-big-enough) shows next that κ-rational points exist on the special fiber $\widetilde{\mathcal{Z}}_0^{\mu\varphi}$ [DG12, §2.4.5];

3. See [DG12, §2.3] for a precise definition of non vertical ramification (and definition 1.2.5 in the case $\mathcal{B} = \mathbb{P}^1_A$). This condition can in fact be removed here if $n \geq 3$: according to [Bec91, proposition 2.3], no vertical ramification may then occur (under the other two assumptions $p = 0$ or $p > n$ and $\mathcal{D}$ smooth) as the geometric monodromy group S_n is of trivial center.

if κ is finite, this follows from the Lang-Weil estimates (see the proof of [DG12, lemma 2.4]). Hensel's lemma is finally used to lift these κ-rational points to k-rational points on $\widetilde{Z}^{\mu\varphi}$. □

4.2.4 Local-global results

Finding rational points on varieties over a global field k is harder than it is over local fields. Nevertheless results of §4.2.3 can be used to obtain local-global statements. We explain below how to globalize local information coming from corollary 4.2.3.

Let k be the quotient field of some Dedekind domain A and $\mathcal{S}$ be a finite set of places of k corresponding to some prime ideals of A. For every place v, the completion of k is denoted by k_v, the valuation ring by A_v, the residue field by κ_v, which we assume to be perfect, and the order (possibly infinite) of κ_v by q_v.

Let B be a smooth projective and geometrically integral k-variety, given with an integral model $\mathcal{B}$ over A such that $\mathcal{B}_v = \mathcal{B} \otimes_A A_v$ is smooth for each place $v \in \mathcal{S}$. The *weak approximation property* below guarantees that k_v-rational points on B ($v \in \mathcal{S}$), which may be provided by corollary 4.2.3, can be approximated by some k-rational point on B.

(weak-approx $/\mathcal{S}$) *$B(k)$ is dense in $\prod_{v\in\mathcal{S}} B(k_v)$.*

Then corollary 4.2.5 below readily follows from corollary 4.2.3:

Corollary 4.2.5. *Let $f : X \to B$ be a regular k-cover of degree n, D be its branch divisor and, for each $v \in \mathcal{S}$, $\prod_{l=1}^{s_v} F_{v,l}/k_v$ be an unramified k_v-étale algebra of degree n. Assume that the following three conditions hold:*
(1) *the geometric monodromy group of f is S_n,*
(2) *the weak approximation condition* (weak-approx $/\mathcal{S}$) *holds,*
(3) *for each place $v \in \mathcal{S}$, conditions* (good-red) *and* (κ-big-enough) *of corollary 4.2.3 hold for the regular k_v-cover $f_v = f \otimes_k k_v$ and the residue field κ_v.*
Then there exist v-adic open subsets $U_v \subset B(k_v) \setminus D$ ($v \in \mathcal{S}$) such that $B(k) \cap \prod_{v\in\mathcal{S}} U_v \neq \emptyset$ and, for each point $t_0 \in B(k) \cap \prod_{v\in\mathcal{S}} U_v$ and each place $v \in \mathcal{S}$, the k_v-étale algebra $\prod_{l=1}^{s_v} F_{v,l}/k_v$ is the specialization algebra of $f \otimes_k k_v$ at t_0.

Addendum 4.2.5. Each condition $q_v \geq c(f_v, \mathcal{B}_v)$ ($v \in \mathcal{S}$) in assumption (κ_v-big-enough) can be guaranteed by some condition $q_v \geq C(f, \mathcal{B})$ with $C(f, \mathcal{B})$ only depending on f and $\mathcal{B}$ (and not on v); see [DG12, lemma 3.1]. The constant $C(f, \mathcal{B})$ here is the constant $C(g, \mathcal{B})$ from there with g the Galois closure of f. In the case $\mathcal{B} = \mathbb{P}^1_A$, it can be taken to be $C(f, \mathcal{B}) = (rn!)^2$ with r the branch point number of f.

4.3 Applications

The three subsections below correspond to the three main theorems from the presentation.

4.3.1 Trinomial realizations and variants

Bary-Soroker's motivation in [BS09] was to obtain analogs of the Dirichlet theorem for polynomial rings. He proved that, if k is a PAC field, then, given two relatively prime polynomials $a(Y)$ and $b(Y) \in k[Y]$ and an integer n, large enough (depending on $a(Y)$ and $b(Y)$) and for which k has at least one separable extension of degree n, there are infinitely many distinct polynomials $c(Y) \in k[Y]$ such that $a(Y) + b(Y)\, c(Y)$ is irreducible over k and of degree n. A first stage is to construct a polynomial $c_0(Y) \in k[Y]$ such that $a(Y) + b(Y)\, c_0(Y)\, T \in k[T][Y]$ is absolutely irreducible, of degree n and Galois group S_n over $\overline{k}(T)$. By using results as in §4.2.1, one can then specialize T in k to obtain the desired polynomials. We develop below other applications.

Given a positive integer n and a field k, we apply some of our results of §4.2 to some classical covers $f : X \to \mathbb{P}^1$ of degree n and geometric monodromy group S_n, given by polynomials $P(T,Y) \in k[T][Y]$ of degree n (with respect to Y) and Galois group S_n over $\overline{k}(T)$. Some of our statements below involve the two ones recalled in §B.3.1. We say below that a finite extension F/k can be *realized by a polynomial* $Q(Y) \in k[Y]$ if $Q(Y)$ is the irreducible polynomial over k of some primitive element of F/k.

4.3.1.1. Special realizations of extensions of PAC fields.

(a) *Morse polynomials.* Applying corollary 4.2.1 to the trinomial $Y^n - Y - T$ of §B.3.1.1 provides theorem 1 from the presentation:

Corollary 4.3.1. *Let k be a PAC field and $p \geq 0$ be its characteristic. Then one has the following two conclusions.*
(1) *Let $n \geq 2$ be an integer. If $p \not| n(n-1)$, then every extension F/k of degree n can be realized by some trinomial $Y^n - Y + b$ with $b \in k$.*
(2) *If $p \neq 2$, the separable closure k^{sep} is generated over k by all elements $y \in k^{\mathrm{sep}}$ such that $y^n - y \in k$ for some integer $n \geq 2$, which can be taken to be $n = [k(y) : k]$ if $p = 0$.*

Proof. For part (1), note first that F/k is separable since $p \not| n$ and that one may obviously assume that $n \geq 3$. The conclusion then follows from corollary 4.2.1 (and lemma B.1.3) applied to the regular k-cover $f : X \to \mathbb{P}^1$ given by the trinomial $P(T,Y) = Y^n - Y - T$ (§B.3.1.1) and the k-étale algebra $\prod_{l=1}^{s} F_l/k$ taken to be the single field extension F/k.

To prove part (2), fix a finite separable extension F/k of degree $m \geq 2$. Pick an integer $n \geq m$ such that p does not divide $n(n-1)$ (at least one such integer exists as $p \neq 2$ and one can even choose $n = m$ if $p = 0$) and do as above but with the k-étale algebra $\prod_{l=1}^{s} F_l/k$ taken to be the product of the extension F/k with $n - m$ copies of the trivial one k/k. Conclude that F/k has a primitive element whose irreducible polynomial over k divides $Y^n - Y + b$ (and is equal to $Y^n - Y + b$ if $p = 0$ and $n = m$) for some $b \in k$. As F/k is an arbitrary finite separable extension, this provides the claimed description of k^{sep}. $\square$

Proceeding as above but using an arbitrary Morse polynomial instead of the particular one $Y^n - Y$ (§B.3.1.1) leads to corollary 4.3.2 below:

Corollary 4.3.2. *Let $n \geq 2$ be an integer, k be a PAC field of characteristic $p \geq 0$ not dividing n and $M(Y) \in k[Y]$ be a Morse polynomial of degree n. Then every extension F/k of degree n can be realized by some polynomial $M(Y) + b$ with $b \in k$.*

(b) *An example of Uchida.* Let k be a field, n be a positive integer and $U_0, \dots, U_3$ be four algebraically independent indeterminates. From [Uch70, corollary 2], the polynomial $F(Y) = Y^n + U_3Y^3 + U_2Y^2 + U_1Y + U_0$ has Galois group S_n over the field $k(U_0, \dots, U_3)$ if $n \geq 4$. Lemma 4.3.3 below makes it possible to derive a polynomial $P(T,Y) = Y^n + u_3(T)Y^3 + u_2(T)Y^2 + u_1(T)Y + u_0(T) \in k[T][Y]$ of Galois group S_n over $\overline{k}(T)$.

Lemma 4.3.3. *Let l be a positive integer, $\underline{U} = (U_1, \dots, U_\ell)$ be a l-tuple of algebraically independent indeterminates, $F(\underline{U}, Y) \in k(\underline{U})[Y]$ be a non constant polynomial (with respect to Y) and n be its degree. Assume that $F(\underline{U}, Y)$ has Galois group S_n over $\overline{k}(\underline{U})$. Then there exist infinitely many distinct ℓ-tuples $\underline{u}(T) = (u_1(T), \dots, u_\ell(T)) \in k[T]^\ell$ such that the polynomial $F(\underline{u}(T), Y)$ has Galois group S_n over $\overline{k}(T)$.*

Proof. As $F(\underline{U}, Y)$ has Galois group S_n over $\overline{k}(T)(\underline{U})$, the conclusion follows from the Hilbert specialization property of the hilbertian field $\overline{k}(T)$, but one needs a version providing good specialisations in $k(T)$ (but still good relative to the irreducibility over $\overline{k}(T)$). This is classical if k is infinite (*e.g.* [FJ05, §13.2]). In the general case, we resort to [Dèb99b, theorem 3.3], which shows that, given a Hilbert subset $\mathcal{H} \subset \overline{k}(T)$, then, for all but finitely many $t_0 \in \overline{k}(T)$, there exists some $a \in \overline{k}(T)$ such that, if $b \in k[T]$ is any non-constant polynomial, then $\mathcal{H}$ contains infinitely many distinct elements of the form $t_0 + ab^m$ ($m \geq 0$). This gives what we want if a can be chosen in $k(T)$. Although it is not stated, the proof shows that such a choice is possible; the main point is to adjust [Dèb99b, lemma 3.2] to show that there are infinitely many cosets of $k(T)$ modulo $\overline{k}(T)^p$ (with p the characteristic of k). $\square$

One then obtains the following statement:

Corollary 4.3.4. *Let $n \geq 4$ be an integer and k be a PAC field. Then every separable extension F/k of degree n can be realized by some polynomial $Y^n + aY^3 + bY^2 + cY + d$ with $a, b, c, d \in k$.*

As pointed out by Bary-Soroker, one may replace the polynomial $F(Y) = Y^n + U_3Y^3 + U_2Y^2 + U_1Y + U_0$ from [Uch70, corollary 2] by more general ones. For example, given a monic polynomial $f(Y) \in k[Y]$ of degree n, the polynomial $F(Y) = f(Y) + U_3Y^3 + U_2Y^2 + U_1Y + U_0$ has Galois group S_n over $k(U_0, \dots, U_3)$ if $n \geq 4$ [BBSR13, proposition 3.6].

4.3.1.2. Variants.

(a) *Finite fields.* Proceeding as above but using corollary 4.2.2 instead of corollary 4.2.1 leads to the following statement for finite fields:

Let q be a prime power, $n \geq 2$ be an integer and $M(Y) \in \mathbb{F}_q[Y]$ be a Morse polynomial of degree n such that $(n, q) = 1$ and $q \geq (nn!)^2$. Then the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ can be realized by some polynomial $M(Y) + b$ with $b \in \mathbb{F}_q$.

(b) *p-adic fields.* The statement below easily follows from (a):

Let $n \geq 2$ be an integer and $p \geq (nn!)^2$ be a prime number. Then, given a monic polynomial $M(Y) \in \mathbb{Z}_p[Y]$ of degree n with reduction modulo p a Morse polynomial in $\mathbb{F}_p[Y]$, the unique unramified extension of $\mathbb{Q}_p$ of degree n can be realized by some polynomial $M(Y) + b$ with $b \in \mathbb{Z}_p$.

This can also be proved in the special case $M(Y) = Y^n - Y$ by using corollary 4.2.3 instead of corollary 4.2.2.

(c) *Trinomials.* The trinomials $Y^n - T^rY^m + T^s$ of §B.3.1.2 can also be used to provide similar conclusions. The assumption on p is that $p \nmid mn(n-m)$ and the bound on q can be replaced by the better one $q = p^f \geq (3n!)^2$.

(d) *Missing characteristics.* Given an integer $n \geq 2$ and a prime number p, corollary 4.2.1, combined with lemma 4.3.3 (and lemma B.1.3), shows in fact that

$(*)$ *given a PAC field k of characteristic p, every separable extension F/k of degree n can be realized by some trinomial $Y^n + aY^m + b$ with $1 \leq m < n$ and $a, b \in k$,*

provided that the following condition holds:

$(**)$ *there exists $1 \leq m < n$ such that the trinomial $Y^n + UY^m + V$ has Galois group S_n over $\overline{\mathbb{F}}_p(U, V)$ (with U and V two indeterminates).*

There are many results about condition $(**)$ in the literature, notably in [Uch70], [Coh80] and [Coh81]. Here are conclusions which can be derived about cases not covered by corollary 4.3.1:

- if $p \neq 2$, $p|n(n-1)$ and n is odd, condition $(**)$ holds with Y^n+UY^2+V or with Y^n-UY+V [Coh81, corollary 3] [Uch70, theorem 2],
- if $p=2$ and n is odd, condition $(**)$ holds with Y^n+UY^2+V if $n \geq 5$ [Coh81, corollary 3] and with Y^n-UY+V if $n=3$ [Uch70, theorem 2],
- if $p=3$ and $n=4$, condition $(**)$ holds with Y^n-UY+V [Uch70, theorem 2],
- if ($p=5$ and $n=6$) or ($p=2$ and $n=6$), condition $(**)$ does not hold: Y^6-UY+V has Galois group $\mathrm{PGL}_2(\mathbb{F}_5)$ over $\mathbb{F}_5(U,V)$ and Y^6-UY+V has Galois group A_5 over $\mathbb{F}_4(U,V)$ [Uch70] (note that the exponent m is necessarily prime to n if condition $(**)$ holds, or otherwise the Galois group of the trinomial is not primitive, and that changing Y to $1/Y$ reduces the check of condition $(**)$ to half of the remaining m).

Remark 4.3.5. From above, condition $(**)$ holds if n is odd and $p|n(n-1)$, and, from [Uch70, theorem 1], it also holds if $p \not| n(n-1)$ (with $m=1$). As a consequence, condition $(**)$, and so condition $(*)$ too, always hold if n is odd.

(e) *Number fields.* Over a number field k, extensions with trinomial realizations are more sparse. For example, Angeli proved that, for every integer $n \geq 3$, there exist (up to some standard equivalence for trinomials) only finitely many trinomials of degree n, with coefficients in k, irreducible over k and of Galois group over k a primitive subgroup $G \subset S_n$ distinct from S_n and A_n [Ang09]. See also [Ang07] where the same is proved with "$G \subset S_n$ primitive" replaced by "G solvable" in the case n is a prime number.

4.3.2 Hilbert's irreducibility theorem

We elaborate below on the local-global result of §4.2.4 in the case $B=\mathbb{P}^1$. In this situation, assumption (weak-approx $/\mathcal{S}$) holds for every finite set $\mathcal{S}$ (this follows from the Artin-Whaples approximation theorem; see *e.g.* [Lan02, chapter XII, theorem 1.2]) and the good reduction assumption (good-red) requires no place $v \in \mathcal{S}$ be bad[4] [DG12, lemma 2.6].

We use below the trick which consists in throwing in more places in $\mathcal{S}$ to further guarantee in corollary 4.2.5 that the Hilbert specialization property holds, *i.e.* that the specialization algebra of f at t_0 consists of a single field extension $k(X)_{t_0}/k$ of degree n.

Namely the idea is to construct a finite set $\mathcal{S}_0$ of finite places of k, disjoint from $\mathcal{S}$, and to attach to each place $v \in \mathcal{S}_0$ a k_v-étale algebra $\prod_l F_{v,l}/k_v$ with any extension $F_{v,l}/k_v$ trivial but one consisting of an unramified cyclic extension F_v/k_v of degree $d_v \leq n$. If the assumptions of corollary 4.2.5 still hold for the set $T=\mathcal{S}\cup\mathcal{S}_0$, then the Galois group $\mathrm{Gal}(k(Z)_{t_0}/k)$ (of the specialization of the Galois closure of f at t_0) contains some cycle of length d_v for each place $v \in \mathcal{S}_0$ (remark 4.1.2). This implies that $\mathrm{Gal}(k(Z)_{t_0}/k)$ is all of S_n if, for example, $\mathcal{S}_0$ contains three places with corresponding degrees d_v equal to 2, $n-1$ and n [Ser92, lemma 4.4.3]. In particular, the specialization algebra of f at t_0 consists of a single field extension $k(X)_{t_0}/k$ of degree n. Of course, for this idea to work, cyclic extensions F_v/k_v of degree d_v should exist, for places v satisfying the assumptions of corollary 4.2.5.

We develop below the number field case for which this trick can be used. Another example would be to work over $k=\kappa(U)$ with κ a PAC field with enough cyclic extensions and U an indeterminate (see [DG11, §4]). We will also use the explicit aspect of [DG12] which makes it possible to be more precise on the constants. Take $k=\mathbb{Q}$ for simplicity.

Corollary 4.3.6. *Let $f: X \to \mathbb{P}^1$ be a regular $\mathbb{Q}$-cover and n be its degree. Assume that f has geometric monodromy group S_n. Then there exist two positive integers m_0 and β only depending*

4. See definition 1.2.5 (condition (4) there can be removed here).

on f and satisfying the following conclusion. Let $\mathcal{S}$ be a finite set of good primes $p > m_0$, each given with positive integers $d_{p,1}\dots,d_{p,s_p}$ such that $\sum_{l=1}^{s_p} d_{p,l} = n$. Then there exists some integer b satisfying the following:

for each integer $t_0 \equiv b \bmod (\beta\prod_{p\in\mathcal{S}} p)$, t_0 is unramified and the specialization algebra of f at t_0 consists of a single field extension $\mathbb{Q}(X)_{t_0}/\mathbb{Q}$ of degree n which has residue degrees $d_{p,1}\dots,d_{p,s_p}$ at p for each prime $p\in\mathcal{S}$ and S_n as Galois group of its Galois closure.

We refer to corollary 5.2.9 for a refined statement which concerns arbitrary regular $\mathbb{Q}$-covers.

Addendum 4.3.6. (on the constants) Denote the branch point number by r and the bad prime number by $\mathrm{br}(\mathbf{t})$. One can take m_0 such that the interval $[(rn!)^2, m_0]$ contains at least $\mathrm{br}(\mathbf{t})+3$ distinct prime numbers and β to be the product of three distinct good primes in $[(rn!)^2, m_0]$.

If the regular $\mathbb{Q}$-cover f is given by a polynomial $P(T,Y)\in\mathbb{Q}[T][Y]$, addendum 4.3.6 (and lemma B.1.3) provides a bound for the least specialization $t_0\geq 0$ making $P(t_0,Y)$ irreducible in $\mathbb{Q}[Y]$ which only depends on $\deg_Y(P)$, $\mathrm{br}(\mathbf{t})$ and the degree of the discriminant $\Delta(T)$ of $P(T,Y)$, and then only on $\deg(P)$ and $\mathrm{br}(\mathbf{t})$. It is conjectured that a bound depending only on $\deg(P)$ exists in general for Hilbert's irreducibility theorem (see [DW08]).

Proof. Take m_0 as in addendum 4.3.6. Then $m_0 \geq (rn!)^2 = C(f,\mathbb{P}^1_{\mathbb{Z}})$ (addendum 4.2.5). Moreover three distinct good primes can be picked in the interval $[(rn!)^2, m_0]$. Given a positive integer d, denote the unique unramified extension of $\mathbb{Q}_p$ of degree d by $F_p^{\mathrm{ur},d}/\mathbb{Q}_p$. For each prime $p\in\mathcal{S}$, consider the $\mathbb{Q}_p$-étale algebra $\underline{F}_p = \prod_{l=1}^{s_p} F_p^{\mathrm{ur},d_{p,l}}/\mathbb{Q}_p$. Denote the set of additional primes by $\mathcal{S}_0=\{p_2,p_{n-1},p_n\}$, and, for each index $i\in\{2,n-1,n\}$, let $\underline{F}_{p_i}=\prod_l F_{p_i,l}/\mathbb{Q}_{p_i}$ be the $\mathbb{Q}_{p_i}$-étale algebra with one term $F_{p_i,l}/\mathbb{Q}_{p_i}$ equal to $F_{p_i}^{\mathrm{ur},i}/\mathbb{Q}_{p_i}$ and all the $n-i$ others trivial.

Apply corollary 4.2.5 to the cover f, the larger set of places $\mathcal{S}\cup\mathcal{S}_0$ and the associated $\mathbb{Q}_p$-algebras $\underline{F}_p$. Let t_0 be in the set $\mathbb{P}^1(\mathbb{Q})\cap\prod_{p\in\mathcal{S}\cup\mathcal{S}_0} U_p$ provided by its conclusion. As already said, the three prime numbers in $\mathcal{S}_0$ guarantee that the specialization of the Galois closure of f at t_0 has Galois group S_n and then that the specialization algebra of f at t_0 consists of a single field extension $\mathbb{Q}(X)_{t_0}/\mathbb{Q}$ of degree n. The conclusion of corollary 4.2.5 relative to any prime p in $\mathcal{S}$ yields that the extension $\mathbb{Q}(X)_{t_0}/\mathbb{Q}$ has residue degrees $d_{p,1}\dots,d_{p,s_p}$ at p.

To obtain that t_0 can be chosen to be any term in the arithmetic progression as in the statement, we use the more precise description of the p-adic open subsets U_p given in corollary 4.2.3: for each prime $p\in\mathcal{S}\cup\mathcal{S}_0$, U_p contains the preimage *via* the map $\mathbb{P}^1_{\mathbb{Z}_p}\to\mathbb{P}^1_{\mathbb{F}_p}$ of a non-empty subset of $\mathbb{P}^1_{\mathbb{F}_p}$, which can further be assumed to be contained in $\mathbb{A}^1_{\mathbb{F}_p}$. The Artin-Whaples theorem then reduces to the chinese remainder theorem and provides the announced conclusion. □

4.3.3 Hurwitz spaces

Given a finite group G (resp. a positive integer n and a subgroup $G\subset S_n$) and an integer $r\geq 3$, there is a coarse moduli space called *Hurwitz space* for G-covers of $\mathbb{P}^1$ of group G (resp. for regular covers of $\mathbb{P}^1$ of degree n and geometric monodromy group $G\subset S_n$) with r branch points. We view it as a (reducible) variety defined over $\mathbb{Q}$; it can be more generally defined as a scheme over some extension ring of $\mathbb{Z}[1/|G|]$. We do not distinguish between the G-cover and regular cover situations and use the same notation $\mathsf{H}_r(G)$ for the Hurwitz space.

A central moduli property is that, for any field k of characteristic zero, there is a one-one correspondence between the set of $\overline{k}$-rational points on $\mathsf{H}_r(G)$ and the set of isomorphisms classes of (regular or G-) covers defined over $\overline{k}$ with the given invariants. Furthermore, for every closed point $[f]\in\mathsf{H}_r(G)$, the field $k([f])$ is the field of moduli of the corresponding (regular or G-) cover

f. We refer to [DD97b] for more on fields of moduli; in standard situations (*e.g.* $Z(G) = \{1\}$ for G-covers, $\mathrm{Cen}_{S_n}(G) = \{1\}$ for regular covers) and in most situations below, the field of moduli is a field of definition of f and is the smallest one.

Denote the configuration space for finite subsets of $\mathbb{P}^1$ of cardinality r by U_r. The map $\Psi_r : \mathsf{H}_r(G) \to \mathsf{U}_r$ which sends each isomorphism class of cover $[f]$ in $\mathsf{H}_r(G)$ to its branch divisor $\mathbf{t} \in \mathsf{U}_r$ is an étale cover defined over $\mathbb{Q}$. The geometrically irreducible components of $\mathsf{H}_r(G)$ correspond to the connected components of $\mathsf{H}_r(G) \otimes_{\mathbb{Q}} \mathbb{C}$, which in turn correspond to the orbits of the so-called *Hurwitz monodromy action*, of the fundamental group of U_r (the *Hurwitz group* $\mathcal{H}_r$) on a fiber $\Psi_r^{-1}(\mathbf{t})$ ($\mathbf{t} \in \mathsf{U}_r(\overline{k})$). See [Völ96] or [Dèb99a] for more on Hurwitz spaces.

The variety U_r is a Zariski open subset of the projective space $\mathbb{P}^r$. For any given component H of $\mathsf{H}_r(G)$, normalizing $\mathbb{P}^r$ in the function field $\overline{\mathbb{Q}}(\mathsf{H})$ provides a (regular) $\overline{\mathbb{Q}}$-cover $(\Psi_r)_{\overline{\mathsf{H}}} : \overline{\mathsf{H}} \to \mathbb{P}^r$. We apply below some of our specialization results to this (regular) cover.

Let k be a field such that $(\Psi_r)_{\overline{\mathsf{H}}} : \overline{\mathsf{H}} \to \mathbb{P}^r$ is defined over k. For $\mathbf{t}_0 \in \mathsf{U}_r(k)$, consider the specialization algebra $\prod_{l=1}^s k(\mathsf{H})_{\mathbf{t}_0,l}/k$ of $(\Psi_r)_{\overline{\mathsf{H}}}$ at $\mathbf{t}_0$. The fields $k(\mathsf{H})_{\mathbf{t}_0,1}, \dots, k(\mathsf{H})_{\mathbf{t}_0,s}$ are the fields of moduli of all the (regular or G-) $\overline{k}$-covers $[f : X \to \mathbb{P}^1]$ in H with branch divisor $\mathbf{t}_0$.

Definition 4.3.7. The k-étale algebra $\prod_{l=1}^s k(\mathsf{H})_{\mathbf{t}_0,\mathsf{l}}/\mathsf{k}$ is called the *k-algebra of fields of moduli* (or *of smallest fields of definition* if fields of moduli are fields of definition) of the (regular or G-) $\overline{k}$-covers $f : X \to \mathbb{P}^1$ in H with branch divisor $\mathbf{t}_0$.

In this situation, we have the following result. In condition (2)-(b) below, where k is a number field and v is a place of k, we use the notation $k_v^{\mathrm{ur},f}$ ($f \in \mathbb{N} \setminus \{0\}$) for the unique unramified extension of k_v of degree f.

Corollary 4.3.8. *Let k be a field of characteristic zero and H be a component of $\mathsf{H}_r(G)$ such that $(\Psi_r)_{\overline{\mathsf{H}}} : \overline{\mathsf{H}} \to \mathbb{P}^r$ is a regular k-cover of geometric monodromy group S_N with $N = \deg((\Psi_r)_{\overline{\mathsf{H}}})$.*

(1) *Assume that k is a PAC field and fix a k-étale algebra $\prod_{l=1}^s F_l/k$ of degree N. Then there exists some Zariski-dense subset $\mathcal{U} \subset \mathsf{U}_r(k)$ such that, for each $\mathbf{t}_0 \in \mathcal{U}$, the k-étale algebra $\prod_{l=1}^s F_l/k$ is the k-algebra of smallest fields of definition of the (regular or* G*-) $\overline{k}$-covers $f : X \to \mathbb{P}^1$ in H with branch divisor $\mathbf{t}_0$.*

(2) *Assume that k is a number field. Then there exist two constants $p(r,G)$ and $q(r,G)$ only depending on r and G (and so not of k) with the following property. Let $\mathcal{S}$ be a finite subset of finite places v of k with residue field of order $q_v \geq q(r,G)$ and residue characteristic $p_v > p(r,G)$, and, for each place $v \in \mathcal{S}$, $d_{v,1} \dots, d_{v,s_v}$ be positive integers such that $\sum_{l=1}^{s_v} d_{v,l} = N$. Then there exists some Zariski-dense subset $\mathcal{U} \subset \mathsf{U}_r(k)$, of the form $\mathcal{U} = \mathsf{U}_r(k) \cap \prod_{v \in \mathcal{S}} U_v$ for some v-adic open subsets $U_v \subset \mathsf{U}_r(k_v)$, such that, for each $\mathbf{t}_0 \in \mathcal{U}$, the following two conditions hold:*

(a) *the field of moduli of each of the (regular or* G*-) $\overline{k}$-covers $f : X \to \mathbb{P}^1$ in H with branch divisor $\mathbf{t}_0$ is an extension of k of degree N,*

(b) *for every place $v \in \mathcal{S}$, the k_v-algebra of smallest fields of definition of the (regular or* G*-) $\overline{k_v}$-covers $f \otimes_{\overline{k}} \overline{k_v}$ (for any given embedding $\overline{k} \hookrightarrow \overline{k_v}$) in H with branch divisor $\mathbf{t}_0$ is the k_v-étale algebra $\prod_{l=1}^{s_v} k_v^{\mathrm{ur},d_{v,l}}/k_v$.*

Proof. Part (1) is a straightforward application of corollary 4.2.1, applied to the regular k-cover $(\Psi_r)_{\overline{\mathsf{H}}}$ and combined with definition 4.3.7 and the fact that, over a PAC field, the field of moduli is always a field of definition [DD97b].

For part (2), we apply corollary 4.2.5 to the regular k-cover $(\Psi_r)_{\overline{\mathsf{H}}}$ (with $\mathcal{B} = \mathbb{P}^r$) and to the k_v-étale algebras $\prod_{l=1}^{s_v} k_v^{\mathrm{ur},d_{v,l}}/k_v$ ($v \in \mathcal{S}$). The geometric monodromy group of $(\Psi_r)_{\overline{\mathsf{H}}}$ being S_N, the first assumption holds. The second one holds too (for any finite set $\mathcal{S}$ of finite places) as $\mathbb{P}^r$

is a k-rational variety. The branch locus $D = \mathbb{P}^r \setminus \mathsf{U}_r$ consists of hyperplane sections which cross normally over k. Only finitely many places of k may not satisfy condition (good-red) of corollary 4.2.3. Take $p(r, G)$ to be the largest characteristic of these exceptional places and $q(r, G)$ to be the constant $C((\Psi_r)_{\overline{\mathsf{H}}}, \mathbb{P}^r)$ of addendum 4.2.5; these constants can indeed be chosen depending on r and G and not on the number field k (remark 4.2.4). Assuming $p_v > p(r, G)$ and $q_v \geq q(r, G)$ ($v \in \mathcal{S}$) then guarantees that the third assumption of corollary 4.2.5 holds. Part (2)-(b) then corresponds to the conclusion of corollary 4.2.5, combined with definition 4.3.7 and the fact that, as a consequence of condition (good-red), the field of moduli of each (regular or G-) $\overline{k_v}$-cover $f \otimes_{\overline{k}} \overline{k_v}$ is a field of definition [DH98]. To obtain part (2)-(a), we use the trick as in §4.3.2: adding to $\mathcal{S}$ well-chosen places v with corresponding k_v-étale algebras and applying corollary 4.2.5 to this larger set of places assures that the specialization algebra of $(\Psi_r)_{\overline{\mathsf{H}}}$ at $\mathbf{t}_0$ consists of a single field extension $k(\mathsf{H})_{\mathbf{t}_0}/k$ of degree N [5]. □

There is in corollary 4.3.8 the assumption that $(\Psi_r)_{\overline{\mathsf{H}}} : \overline{\mathsf{H}} \to \mathbb{P}^r$ be a regular k-cover of geometric monodromy group S_N. This assumption can be checked in practical situations. Indeed the geometric monodromy group is the image group of the Hurwitz monodromy action (restricted to the component H), which can be made totally explicit.

5. and S_N is the Galois group of its Galois closure.

Chapter 5

Twisted covers and specializations

5.1 The twisting lemma

Given a field k, the central question we address is whether a given k-cover specializes to a given k-étale algebra at some unramified k-rational point. We first consider the situation of k-G-Galois covers in §5.1.1 and then handle the situation of k-covers in §5.1.2 by "going to the Galois closure".

5.1.1 The Galois form of the twisting lemma

Let k be a field and $g : Z \to B$ be a k-G-Galois cover. Denote its branch divisor by D, the Galois group $\mathrm{Gal}(k(Z)/k(B))$ by G, the π_1-representation associated with g by $\phi : \pi_1(B\setminus D, t)_k \to G$, the geometric monodromy group $\mathrm{Gal}(k^{\mathrm{sep}}(Z)/k^{\mathrm{sep}}(B))$ by $\overline{G}$ and the constant extension in $g : Z \to B$ by $\widehat{k}_g/k$.

5.1.1.1. Twisting k-G-Galois covers. Let N/k be a finite Galois extension and H be its Galois group, assumed to be isomorphic to some subgroup of G. With no loss of generality, we may and will view H itself as a subgroup of G. The constant extension $\widehat{k}_g/k$ is characterized by this condition: $\widehat{k}_g(B)$ is the fixed field in $k(Z)$ of the geometric monodromy group $\overline{G} \subset G$. We assume the following *compatibility condition* of N/k with the constant extension $\widehat{k}_g/k$:

(const/comp) *the fixed field $N^{H\cap\overline{G}}$ of $H \cap \overline{G}$ in N is the field $\widehat{k}_g$.*

This condition is trivially satisfied if g is a k-G-cover as both fields $N^{H\cap\overline{G}}$ and $\widehat{k}_g$ equal k.

Consider the homomorphism $\Lambda : \mathrm{G}_k \to G/\overline{G}$ induced by ϕ on the quotient $\mathrm{G}_k = \pi_1(B \setminus D, t)_k/\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}$. The map Λ is a G-Galois representation of the constant extension $\widehat{k}_g/k$ (relative to k^{sep}); it is called the *constant extension map* [DD97b, §2.8]. As it is surjective, we have $\mathrm{Gal}(\widehat{k}_g/k) \simeq G/\overline{G}$ and so condition (const/comp) implies that $H\overline{G} = G$.

Let $\varphi : \mathrm{G}_k \to H$ be the G-Galois representation of the Galois extension N/k (relative to k^{sep}) and $\overline{\varphi} : \mathrm{G}_k \to G/\overline{G}$ be the composed map of φ with the canonical surjection $\overline{\cdot} : G \to G/\overline{G}$. Condition (const/comp) rewrites as follows:

(const/comp) *There exists some $\overline{\chi} \in \mathrm{Aut}(G/\overline{G})$ such that $\Lambda = \overline{\chi} \circ \overline{\varphi}$.*

Indeed this follows from $\widehat{k}_g = (k^{\mathrm{sep}})^{\ker(\Lambda)}$ and $(k^{\mathrm{sep}})^{\ker(\overline{\varphi})} = ((k^{\mathrm{sep}})^{\ker(\varphi)})^{\ker(\overline{\varphi})/\ker(\varphi)} = N^{\varphi(\ker(\overline{\varphi}))} = N^{H\cap\overline{G}}$. Note also that, as $\Lambda : \mathrm{G}_k \to G/\overline{G}$ is onto, an automorphism $\overline{\chi}$ satisfying condition (const/comp) is necessarily unique.

Assume that there exists an isomorphism $\chi : H \to H'$ onto a subgroup $H' \subset G$ which induces $\overline{\chi}$ modulo $\overline{G}$. With $\mathrm{Per}(G)$ the permutation group of G, consider then the map

$$\widetilde{\phi}^{\chi\varphi} : \pi_1(B \setminus D, t)_k \to \mathrm{Per}(G)$$

defined by the following formula, with r the restriction $\pi_1(B \setminus D, t)_k \to \mathrm{G}_k$: for any $\theta \in \pi_1(B \setminus D, t)_k$ and any $x \in G$,

$$\widetilde{\phi}^{\chi\varphi}(\theta)(x) = \phi(\theta)\ x\ (\chi \circ \varphi \circ r)(\theta)^{-1}$$

It is easily checked that $\widetilde{\phi}^{\chi\varphi}$ is a group homomorphism. However the corresponding action of $\pi_1(B \setminus D, t)_k$ on G is not transitive in general [1]. More precisely, we have the following statement:

Lemma 5.1.1. *Under condition* (const/comp)*, we have* $\widetilde{\phi}^{\chi\varphi}(\theta)(\overline{G}) \subset \overline{G}$ *for every* $\theta \in \pi_1(B \setminus D, t)_k$.

Proof. For any $\theta \in \pi_1(B \setminus D, t)_k$ and any $x \in \overline{G}$, we have

$$\overline{\widetilde{\phi}^{\chi\varphi}(\theta)(x)} = \overline{\phi(\theta)}\,.\,\overline{x}\,.\overline{(\chi \circ \varphi \circ r)(\theta)}^{-1} = \Lambda(r(\theta))\,.\,\overline{\chi}(\overline{\varphi}(r(\theta)))^{-1} = 1 \qquad \square$$

Consider the morphism, denoted by $\widetilde{\phi}^{\chi\varphi}_{\overline{G}} : \pi_1(B \setminus D, t)_k \to \mathrm{Per}(\overline{G})$, which sends $\theta \in \pi_1(B \setminus D, t)_k$ to the restriction of $\widetilde{\phi}^{\chi\varphi}(\theta)$ on $\overline{G}$. Its restriction $\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}} \to \mathrm{Per}(\overline{G})$ is given by

$$\widetilde{\phi}^{\chi\varphi}_{\overline{G}}(\theta)(x) = \phi(\theta)\ x \qquad (\theta \in \pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}, x \in \overline{G})$$

Thus this restriction is obtained by composing that of the original π_1-representation ϕ with the left-regular representation of $\overline{G}$. Hence the corresponding action of $\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}$ on $\overline{G}$ is transitive, thus showing that $\widetilde{\phi}^{\chi\varphi}_{\overline{G}} : \pi_1(B \setminus D, t)_k \to \mathrm{Per}(\overline{G})$ is the π_1-representation of some regular k-cover. We denote it by $\widetilde{g}^{\chi\varphi} : \widetilde{Z}^{\chi\varphi} \to B$ and call it the *twisted cover* of g by the morphism $\chi \circ \varphi$; it is in particular a k-model of the (regular) k^{sep}-cover $g \otimes_k k^{\mathrm{sep}}$ (*i.e.* $\widetilde{g}^{\chi\varphi} \otimes_k k^{\mathrm{sep}} \simeq g \otimes_k k^{\mathrm{sep}}$).

5.1.1.2. The twisting lemma for k*-*G*-Galois covers.* The following statement gives the main property of the twisted cover.

Some notation is needed. Conjugation automorphisms in a given group $\mathcal{G}$ are denoted by $\mathrm{conj}(\omega)$ for $\omega \in \mathcal{G}$: $\mathrm{conj}(\omega)(x) = \omega\, x\, \omega^{-1}$ for any $x \in \mathcal{G}$. The set of all isomorphisms $\chi : H \to H'$ onto a subgroup $H' \subset G$ which each induce $\overline{\chi}$ modulo $\overline{G}$ is denoted by $\mathrm{Isom}_{\overline{\chi}}(H, H')$.

Fix then a set $\{\chi_\gamma : H \to H_\gamma \,/\, \gamma \in \Gamma\}$ of representatives of all isomorphims $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, H')$ with H' ranging over all subgroups of G isomorphic to H, modulo the equivalence which identifies $\chi_1 \in \mathrm{Isom}_{\overline{\chi}}(H, H'_1)$ and $\chi_2 \in \mathrm{Isom}_{\overline{\chi}}(H, H'_2)$ if $H'_2 = \omega H'_1 \omega^{-1}$ and $\chi_2\chi_1^{-1} = \mathrm{conj}(\omega)$ for some element $\omega \in \overline{G}$.

Twisting lemma 5.1.2 (Galois form)**.** *Under condition* (const/comp)*, we have the following two conclusions.*

(1) *For each subgroup* $H' \subset G$ *isomorphic to* H*, each isomorphism* $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, H')$ *and each unramified point* $t_0 \in B(k)$*, the following two conditions are equivalent:*

(a) *there exists some point* $x_0 \in \widetilde{Z}^{\chi\varphi}(k)$ *such that* $\widetilde{g}^{\chi\varphi}(x_0) = t_0$*,*

(b) *there exists some element* $\omega \in \overline{G}$ *such that* $(\phi \circ \mathsf{s}_{t_0})(\tau) = \omega\,(\chi \circ \varphi)(\tau)\,\omega^{-1}$ *for any* $\tau \in \mathrm{G}_k$ *(with* $\mathsf{s}_{t_0} : \mathrm{G}_k \to \pi_1(B \setminus D, t)_k$ *the section associated with* t_0*).*

(2) *For each point* $t_0 \in B(k) \setminus D$*, the following three conditions are equivalent:*

1. This action is transitive if g is regular.

(c) *the extension N/k is the specialization $k(Z)_{t_0}/k$ of g at t_0,*

(d) *there exists some isomorphism $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, \phi \circ \mathsf{s}_{t_0}(\mathrm{G}_k))$ such that both conditions (a) and (b) hold for this χ,*

(e) *there exists some $\gamma \in \Gamma$ such that conditions (a) and (b) hold for $\chi = \chi_\gamma$.*

Furthermore an element $\gamma \in \Gamma$ as in condition (e) is necessarily unique.

A single twisted cover is involved in part (1) while there are several in part (2). In this respect, the representation viewpoint used in part (1) may look more natural than the field extension one in part (2). The latter however is more useful in practice. Note also that conditions (d) and (e), being equivalent to condition (c), do not depend on the chosen π_1-representation $\phi : \pi_1(B \setminus D, t)_k \to G$ of g modulo conjugation by elements of G.

Remark 5.1.3. (1) The existence of some subgroup $H' \subset G$ such that the set $\mathrm{Isom}_{\overline{\chi}}(H, H')$ is non-empty, which amounts to $\Gamma \neq \emptyset$, is not guaranteed; if $\Gamma = \emptyset$, each of the three conditions (c), (d) and (e) fails. It is however guaranteed under each of the two assumptions $\overline{\chi} = \mathrm{id}_{G/\overline{G}}$ and $\mathrm{Out}(G/\overline{G}) = \{1\}$. Indeed, if $\overline{\chi} = \mathrm{id}_{G/\overline{G}}$, then $\mathrm{id}_H \in \mathrm{Isom}_{\overline{\chi}}(H, H)$ and, if $\mathrm{Out}(G/\overline{G}) = \{1\}$, the automorphism $\overline{\chi} \in \mathrm{Aut}(G/\overline{G})$ is inner, of the form $\mathrm{conj}(\overline{\omega})$ with $\overline{\omega} \in G/\overline{G}$, and, as $H\overline{G} = G$, lifts to some isomorphism $\mathrm{conj}(\omega) : H \to H$ with $\omega \in H$. Both assumptions include the regular case as then $G/\overline{G} = \{1\}$.

(2) If g is a k-G-cover, then condition (const/comp) trivially holds and equivalence (a) $\Leftrightarrow$ (b) holds with $H' = H$ and $\chi = \mathrm{id}_H$ (as noted above). We then reobtain the twisting lemma 2.1 of [DG12] for k-G-covers.

(3) Some uniqueness property can be added to condition (d) as in condition (e). Indeed an isomorphism $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, \phi \circ \mathsf{s}_{t_0}(\mathrm{G}_k))$ satisfying both conditions (a) and (b), as the one in condition (d), is necessarily unique up to left composition by $\mathrm{conj}(\omega)$ with $\omega \in \mathrm{Nor}_{\overline{G}}(\phi \circ \mathsf{s}_{t_0}(\mathrm{G}_k))$. The advantage of condition (e) is that the set $\bigcup_{\gamma \in \Gamma} \widetilde{Z}^{\chi_\gamma \varphi}(k)$, where unramified k-rational points should be found to conclude that condition (c) holds, does not depend on t_0 (although the element $\gamma \in \Gamma$ in condition (e) does). Moreover the uniqueness property in condition (e) makes it easier to count the points $t_0 \in B(k)$ at which condition (c) holds.

(4) The proof of equivalence (a) $\Leftrightarrow$ (b) below shows further that the number of k-rational points on $\widetilde{Z}^{\chi\varphi}$ above a given unramified point $t_0 \in B(k)$, if positive, is equal to the order of the group $\mathrm{Cen}_{\overline{G}}(\chi(H))$.

5.1.1.3. Proof of the twisting lemma 5.1.2.

(1) Fix a subgroup $H' \subset G$ isomorphic to H, an isomorphism $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, H')$ and a point $t_0 \in B(k) \setminus D$. The G-specialization representation $\widetilde{\phi}^{\chi\varphi}_{\overline{G}} \circ \mathsf{s}_{t_0} : \mathrm{G}_k \to \mathrm{Per}(\overline{G})$ of $\widetilde{g}^{\chi\varphi}$ at t_0 is the action of G_k on the fiber $(\widetilde{g}^{\chi\varphi})^{-1}(t_0)$; it is given by

$$\widetilde{\phi}^{\chi\varphi}_{\overline{G}}(\mathsf{s}_{t_0}(\tau))(x) = \phi(\mathsf{s}_{t_0}(\tau))\, x\, (\chi \circ \varphi)(\tau)^{-1} \qquad (\tau \in \mathrm{G}_k, x \in \overline{G})$$

The elements $\widetilde{\phi}^{\chi\varphi}_{\overline{G}}(\mathsf{s}_{t_0}(\tau))$ have a common fixed point $\omega \in \overline{G}$ if and only if $\phi \circ \mathsf{s}_{t_0}(\tau) = \omega\, (\chi \circ \varphi)(\tau)\, \omega^{-1}$ for any $\tau \in \mathrm{G}_k$. This yields equivalence (a) $\Leftrightarrow$ (b). Moreover the set of all elements $\omega \in \overline{G}$ satisfying the preceding condition, if non empty, is a left coset $\omega_0\, \mathrm{Cen}_{\overline{G}}(\chi(H))$, thus proving part (4) of remark 5.1.3.

(2) Fix $t_0 \in B(k) \setminus D$ and a representative of the section $\mathsf{s}_{t_0} : \mathrm{G}_k \to \pi_1(B \setminus D, t)_k$ (defined up to conjugation by an element in $\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}$). We successively prove equivalences (d) $\Leftrightarrow$ (c) and (e) $\Leftrightarrow$ (d).

Implication (d) $\Rightarrow$ (c) follows from the fact that, if $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, \phi \circ \mathsf{s}_{t_0}(\mathrm{G}_k))$ satisfies both conditions (a) and (b), then $\ker(\phi \circ \mathsf{s}_{t_0})$ and $\ker(\varphi)$ are equal, hence so are their fixed fields in k^{sep}. Conversely assume that the extensions $k(Z)_{t_0}/k$ and N/k are equal, *i.e.* $\ker(\phi \circ \mathsf{s}_{t_0})$ and $\ker(\varphi)$ are the same subgroup, say $\mathcal{K}$, of G_k. The two morphisms $\phi \circ \mathsf{s}_{t_0} : \mathrm{G}_k \to \phi \circ \mathsf{s}_{t_0}(\mathrm{G}_k) \subset G$ and $\varphi : \mathrm{G}_k \to H \subset G$ then differ from $\mathrm{G}_k \to \mathrm{G}_k/\mathcal{K}$ by some isomorphisms $\phi \circ \mathsf{s}_{t_0}(\mathrm{G}_k) \to \mathrm{G}_k/\mathcal{K}$ and $H \to \mathrm{G}_k/\mathcal{K}$ respectively. Thus they differ from one another by some isomorphism $\chi : H \to \phi \circ \mathsf{s}_{t_0}(\mathrm{G}_k)$: $\phi \circ \mathsf{s}_{t_0} = \chi \circ \varphi$. It follows from this and from the uniqueness of the automorphism $\overline{\chi}$ satisfying condition (const/comp) that χ automatically induces $\overline{\chi}$ modulo $\overline{G}$. Conclude that χ is in $\mathrm{Isom}_{\overline{\chi}}(H, \phi \circ \mathsf{s}_{t_0}(\mathrm{G}_k))$ and conditions (a) and (b) hold for this χ (with no conjugation factor).

Assume that condition (e) holds, *i.e.*, for some $\gamma \in \Gamma$, conditions (a) and (b) are satisfied for the isomorphism $\chi_\gamma : H \to H_\gamma$ and some $\omega \in \overline{G}$. It readily follows that $\chi = \mathrm{conj}(\omega) \circ \chi_\gamma$ also satisfies condition (b) (with no conjugation factor) and is in $\mathrm{Isom}_{\overline{\chi}}(H, \phi \circ \mathsf{s}_{t_0}(\mathrm{G}_k))$, thus establishing condition (d). Conversely assume that condition (d) holds. Let $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, \phi \circ \mathsf{s}_{t_0}(\mathrm{G}_k))$ be an isomorphism such that both conditions (a) and (b) hold (with conjugation factor $\omega \in \overline{G}$). There exist $\gamma \in \Gamma$ and $\omega' \in \overline{G}$ such that $\chi = \mathrm{conj}(\omega') \circ \chi_\gamma$. It follows that condition (b) holds for χ_γ as well (with conjugation factor $\omega\omega'$). The uniqueness of the element $\gamma \in \Gamma$ in condition (e) readily follows from condition (b) and the definition of the set $\{\chi_\gamma \,/\, \gamma \in \Gamma\}$.

5.1.2 The general form of the twisting lemma

Let k be a field, $f : X \to B$ be a k-cover, n be its degree and $\prod_{l=1}^{s} F_l/k$ be a k-étale algebra of degree n. The question we address is whether *$\prod_{l=1}^{s} F_l/k$ is the specialization algebra of f at some unramified point $t_0 \in B(k)$.*

5.1.2.1. Statement of the result. Denote the branch divisor of $f : X \to B$ by D, its Galois closure by $g : Z \to B$, the Galois group $\mathrm{Gal}(k(Z)/k(B))$ by G, the π_1-representation of the k-G-Galois cover $g : Z \to B$ by $\phi : \pi_1(B \setminus D, t)_k \to G$, the Galois representation of the extension $k(X)/k(B)$ relative to $k(Z)$ by $\nu : G \to S_n$, the geometric monodromy group $\mathrm{Gal}(k^{\mathrm{sep}}(Z)/k^{\mathrm{sep}}(B))$ by $\overline{G}$ and the constant extension in g by $\widehat{k}_g/k$.

Let N/k be the *compositum* inside k^{sep} of the Galois closures of the extensions $F_1/k, \ldots, F_s/k$; set $H = \mathrm{Gal}(N/k)$. A necessary condition for a positive answer to the question requires the extension N/k to be the specialization $k(Z)_{t_0}/k$ of g at t_0. In particular, H should be isomorphic to some subgroup of G. From now on we will assume it. With no loss of generality, we may then and will view H as a subgroup of G. Finally let $\varphi : \mathrm{G}_k \to H$ be the G-Galois representation of N/k (relative to k^{sep}) and $\mu : H \to S_n$ be the Galois representation of $\prod_{l=1}^{s} F_l/k$ relative to N.

Some further notation of §5.1.1 is retained. The constant extension compatibility condition (const/comp) determines a unique automorphism $\overline{\chi}$ of $G/\overline{G}$ (§5.1.1.1). The twisted cover $\widetilde{g}^{\chi\varphi} : \widetilde{Z}^{\chi\varphi} \to B$ is defined for every isomorphism $\chi : H \to H'$ onto a subgroup $H' \subset G$ inducing $\overline{\chi}$ modulo $\overline{G}$ (§5.1.1.1). The set of all such isomorphisms $\chi : H \to H'$ is denoted by $\mathrm{Isom}_{\overline{\chi}}(H, H')$. The isomorphisms $\chi_\gamma : H \to H_\gamma$ ($\gamma \in \Gamma$) are defined in §5.1.1.2.

Twisting lemma 5.1.4 (general form). *Assume that condition* (const/comp) *holds for g. Then, for each unramified point $t_0 \in B(k)$, the following two conditions are equivalent:*

(1) *$\prod_l F_l/k$ is the specialization algebra $\prod_l k(X)_{t_0,l}/k$ of f at t_0.*

(2) *there exist some subgroup $H' \subset G$ isomorphic to H and some isomorphism $\chi \in \mathrm{Isom}_{\overline{\chi}}(H, H')$ satisfying the following two conditions:*

(a) *there exists some point $x_0 \in \widetilde{Z}^{\chi\varphi}(k)$ with $\widetilde{g}^{\chi\varphi}(x_0) = t_0$,*

(b) *there exists some element $\sigma \in S_n$ such that $\nu \circ \chi(h) = \sigma\, \mu(h)\, \sigma^{-1}$ for every $h \in H$.*

Furthermore, if condition (2) holds, then it holds for some isomorphism $\chi_\gamma : H \to H_\gamma$ with $\gamma \in \Gamma$ and the element γ then is necessarily unique.

5.1.2.2. About condition (2)-(b). We focus on condition (2)-(b) which is the group theoretical part of condition (2) (while condition (2)-(a) is the diophantine part).

We first note for later use that, if condition (2)-(b) holds for $\chi = \chi_{\gamma_0}$ with $\gamma_0 \in \Gamma$, then the number of $\gamma \in \Gamma$ for which condition (2)-(b) holds for $\chi = \chi_\gamma$ is equal to the number of isomorphisms χ_γ ($\gamma \in \Gamma$) such that the actions $\nu \circ \chi_\gamma : H \to S_n$ and $\nu \circ \chi_{\gamma_0} : H \to S_n$ are conjugate in S_n.

We give below three standard situations where condition (2)-(b) holds.

(a) *Geometric monodromy group S_n*: $G = \overline{G} = S_n$ (as in chapter 4). Condition (const/comp) holds and $\nu : S_n \to S_n$ is the natural action: $\nu = \mathrm{id}_{S_n}$. Condition $\nu \circ \chi_\gamma(h) = \sigma\, \mu(h)\, \sigma^{-1}$ ($h \in H$) is satisfied with χ_γ the representative of the isomorphism $\mu : H \to \mu(H) \subset S_n$ (and some element $\sigma \in S_n$).

(b) *Galois situation*: $f : X \to B$ is a Galois k-cover, $\prod_l F_l/k$ is a product of $|G|/|H|$ copies of a same Galois extension F/k with Galois group a subgroup $H \subset G$ and $\Gamma \neq \emptyset$. Then ν is the left-regular representation $G \to \mathrm{Per}(G)$ and μ its restriction $H \to \mathrm{Per}(G)$. Note next that, if $\gamma \in \Gamma$, the restriction $\nu|_H : H \to \mathrm{Per}(G)$ and $\nu \circ \chi_\gamma : H \to \mathrm{Per}(G)$ are conjugate actions, thus establishing condition (2)-(b).

(c) *Cyclic specializations*: condition (const/comp) holds, H is a cyclic subgroup of G generated by an element ω such that $\nu(\omega) \in S_n$ is of type [2] equal to the divisor of the degrees $[F_l : k]$ of the extensions in the k-étale algebra $\prod_l F_l/k$.

Indeed, for every integer $a \geq 1$ such that $(a, |H|) = 1$, let $\chi_a : H \to H$ be the morphism which sends ω to ω^a. As condition (const/comp) holds, one has $H\overline{G} = G$ (as noted in §5.1.1.1) and each map χ_a then induces an automorphism of the cyclic group $G/\overline{G}$. Then there necessarily exists some integer $a \geq 1$ such that χ_a induces $\overline{\chi}$ modulo $\overline{G}$ and $(a, |H|) = 1$ [3]. From the hypothesis, the types of $\nu(\omega)$ and $\mu(\omega)$ are the same. But so are the types of $\nu(\omega)$ and $\nu \circ \chi_a(\omega)$. Conclude that the actions $\nu \circ \chi_a$ and μ are conjugate.

5.1.2.3. Comparizon with previous forms. We compare the general form (lemma 5.1.4) with the Galois form (lemma 5.1.2) and the monodromy S_n form (lemma 4.1.1) of the twisting lemma.

(a) *Lemma 5.1.4 (general form) $\Rightarrow$ lemma 5.1.2 (Galois form).* These two forms each have assumption (const/comp). Moreover lemma 5.1.4 provides equivalence (c) $\Leftrightarrow$ (e) in lemma 5.1.2.

Indeed, given a k-G-Galois cover $f : X \to B$ of group G, a subgroup $H \subset G$ and a Galois extension N/k of group H, apply lemma 5.1.4 to the Galois k-cover f and the k-étale algebra $\prod_{l=1}^s F_l/k$ taken to be the product of $|G|/|H|$ copies of the extension N/k. Then condition (1) of lemma 5.1.4 corresponds to condition (c) of lemma 5.1.2. Moreover, from part (b) of §5.1.2.2, condition (2) of lemma 5.1.4 reduces to its part (a) and then corresponds to condition (e) of lemma 5.1.2.

(b) *Lemma 5.1.4 (general form) $\Rightarrow$ lemma 4.1.1 (monodromy S_n form).* In lemma 4.1.1, the k-cover $f : X \to B$ has degree n and geometric monodromy group S_n. Apply lemma 5.1.4 to such a k-cover. Then condition (const/comp) holds. Moreover we are in the standard situation

2. See §B.3.1.

3. This amounts to showing that, if b is an integer prime to $\nu = |G/\overline{G}|$, then there exists some integer $a = b + k\nu$ which is prime to $|G| = \mu\nu$. Take k to be the product of the prime divisors of μ which do not divide b.

(a) of §5.1.2.2 and then condition (2) of lemma 5.1.4 reduces to its part (a) with $\chi = \mu$, and then to condition (1) of lemma 4.1.1. Conclude that implication (2) $\Rightarrow$ (1) in lemma 5.1.4 yields implication (1) $\Rightarrow$ (2) in lemma 4.1.1.

5.1.2.4. Proof of the twisting lemma 5.1.4. We use below the Galois form of the twisting lemma to establish the general form.

(1) $\Rightarrow$ (2). Assume that condition (1) holds. Necessarily N/k is the specialization $k(Z)_{t_0}/k$ of g at t_0. From part (2) of lemma 5.1.2, there exists a unique $\gamma \in \Gamma$ such that χ_γ satisfies condition (2)-(a) of lemma 5.1.4. And, from part (1) of lemma 5.1.2, this last condition is equivalent to the existence of some $\omega \in \overline{G}$ satisfying $(\phi \circ \mathsf{s}_{t_0})(\tau) = \omega\, (\chi_\gamma \circ \varphi)(\tau)\, \omega^{-1}$ for any $\tau \in \mathrm{G}_k$. Thus we have

$$(\nu \circ \phi \circ \mathsf{s}_{t_0})(\tau) = \nu(\omega)\ (\nu \circ \chi_\gamma \circ \varphi)(\tau)\ \nu(\omega)^{-1} \qquad (\tau \in \mathrm{G}_k)$$

But condition (1) provides some $\beta \in S_n$ satisfying $\nu \circ \phi \circ \mathsf{s}_{t_0}(\tau) = \beta\, \mu \circ \varphi(\tau)\, \beta^{-1}$ for any $\tau \in \mathrm{G}_k$. Conjoining these equalities shows that χ_γ also satisfies condition (2)-(b) (with conjugation factor $\nu(\omega^{-1})\beta$).

(2) $\Rightarrow$ (1). Assume that condition (2) holds. From part (1) of lemma 5.1.2, the existence of some $x_0 \in \widetilde{Z}^{\chi\varphi}(k)$ such that $\widetilde{g}^{\chi\varphi}(x_0) = t_0$ implies that $(\phi \circ \mathsf{s}_{t_0})(\tau) = \omega\, (\chi \circ \varphi)(\tau)\, \omega^{-1}$ for some $\omega \in \overline{G}$ and any $\tau \in \mathrm{G}_k$.

Denote the orbits of $\mu \circ \varphi : \mathrm{G}_k \to S_n$, which correspond to the fields $F_1, \dots F_s$, by $\mathcal{O}_1, \dots, \mathcal{O}_s$. Fix one of them, *i.e.* an index $l \in \{1, \dots, s\}$, and let $i \in \{1, \dots, n\}$ be an index such that F_l is the fixed field in k^{sep} of the subgroup of G_k fixing i *via* the action $\mu \circ \varphi$. For $j = \nu(\omega)(\sigma(i))$ (with σ given by condition (2)-(b)) and any $\tau \in \mathrm{G}_k$, we have

$$\begin{aligned}(\nu \circ \phi \circ \mathsf{s}_{t_0})(\tau)(j) &= \nu(\omega)\, (\nu \circ \chi \circ \varphi)(\tau)\, (\sigma(i))\\ &= \nu(\omega)\, (\mathrm{conj}(\sigma) \circ \mu \circ \varphi)(\tau)\, (\sigma(i))\\ &= \nu(\omega)\ \sigma\ (\mu \circ \varphi)(\tau)\, (i)\end{aligned}$$

and so j is fixed by $(\nu \circ \phi \circ \mathsf{s}_{t_0})(\tau)$ if and only if i is fixed by $(\mu \circ \varphi)(\tau)$. Hence the specialization $k(X)_{t_0,j}$ and the field F_l coincide. Then condition (1) holds from the one-one correspondence between the orbits of $\mu \circ \varphi$ and those of $\nu \circ \phi \circ \mathsf{s}_{t_0}$ provided by the map $i \mapsto \nu(\omega)(\sigma(i))$.

5.2 Varying the base field

We investigate below the remaining problem of finding k-rational points on the twisted varieties over various base fields k. We first consider the case of PAC fields (§5.2.1) and then that of finite fields (§5.2.2). §5.2.3 is devoted to the case of ample fields and we conclude this chapter by that of number fields (§5.2.4). For this section, let n be a positive integer.

5.2.1 PAC fields

In the case of PAC [4] fields, the twisting lemma leads to the following two results in the two standard situations (b) and (c) of §5.1.2.2 (the standard situation (a) leads to corollary 4.2.1).

Corollary 5.2.1. *Let k be a PAC field, $g : Z \to B$ be a k-G-Galois cover, G be its monodromy group, $\overline{G}$ be its geometric monodromy group and N/k be a finite Galois extension with Galois group a subgroup of G. Assume that condition* (const/comp) *holds and that* $\mathrm{Out}(G/\overline{G}) = \{1\}$.

4. See §B.2.1 for the definition and some examples of PAC fields.

Then N/k is the specialization of g at any point t_0 in some Zariski-dense[5] subset of $B(k) \setminus D$ (with D the branch divisor of g).

The special case $G = \overline{G}$ and $B = \mathbb{P}^1$ corresponds to [Dèb99c, theorem 3.2].

Proof. As $\mathrm{Out}(G/\overline{G}) = \{1\}$, one has $\Gamma \neq \emptyset$ (part (1) of remark 5.1.3). Pick then $\gamma \in \Gamma$. As k is PAC, the twisted variety $\widetilde{Z}^{\chi_\gamma \varphi}$ has a Zariski-dense subset $\mathcal{Z}$ of k-rational points. From lemma 5.1.2, the Zariski-dense subset $\widetilde{g}^{\chi_\gamma \varphi}(\mathcal{Z}) \setminus D \subset B(k) \setminus D$ satisfies the required condition. □

Corollary 5.2.2. *Let k be a PAC field, $f : X \to B$ be a k-cover of degree n, G be its monodromy group and $1^{\beta_1} \dots n^{\beta_n}$ be the type of some element of G in the Galois representation $\nu : G \to S_n$ of $k(X)/k(B)$. Let $\prod_l F_l/k$ be a k-étale algebra satisfying the following three conditions:*
(1) *the divisor of all the degrees $[F_l : k]$ is $1^{\beta_1} \dots n^{\beta_n}$,*
(2) *condition* (const/comp) *holds,*
(3) *the compositum N/k inside k^{sep} of the Galois closures of all the extensions F_l/k is a cyclic extension of order* $\mathrm{lcm}\{\, i \mid \beta_i \neq 0\}$.
Then $\prod_l F_l/k$ is the specialization algebra of f at any point t_0 in some Zariski-dense subset of $B(k) \setminus D$ (with D the branch divisor of f).

A useful special case is for $1^{\beta_1} \dots n^{\beta_n} = n^1$: it can then be concluded that f specializes to some field extension of k of degree n at each t_0 in some Zariski-dense subset of $B(k) \setminus D$ (*i.e.* the Hilbert specialization property) under the assumptions that there is an n-cycle in $\nu(G)$ and k has a cyclic extension of degree n satisfying condition (const/comp). This can be compared to [BS09, corollary 1.4] (and corollary 4.2.1) which has the same Hilbert conclusion under the assumptions that $G = \overline{G} = S_n$ and there exists at least one separable extension of k of degree n.

Proof. Let $\omega \in G$ such that $\nu(\omega)$ has type $1^{\beta_1} \dots n^{\beta_n}$. Identify the Galois group $H = \mathrm{Gal}(N/k)$ with the subgroup $\langle \omega \rangle \subset G$. We are in the standard situation (c) of §5.1.2.2 and so condition (2)-(b) of the twisting lemma 5.1.4 holds for some isomorphism χ_γ with $\gamma \in \Gamma$. Since k is PAC, condition (2)-(a) holds for any t_0 in a Zariski-dense subset of $B(k) \setminus D$. Hence condition (1) of the twisting lemma 5.1.4 holds as well, thus ending the proof. □

5.2.2 Finite fields

If k is a large enough finite field $\mathbb{F}_q$, the Lang-Weil estimates can be used to guarantee that the twisted covers have $\mathbb{F}_q$-rational points (see §4.2.2). More specifically, we have the following result where we take $B = \mathbb{P}^1$ for simplicity. We use below the notation of §B.3.1 for elements of symmetric groups and their conjugacy classes.

Corollary 5.2.3. *Let $f : X \to \mathbb{P}^1$ be a regular $\mathbb{F}_q$-cover of degree n and r be its branch point number. Assume that $n \geq 2$ [6] and f has geometric monodromy group S_n. Then, for every choice of positive integers $m_1, \dots, m_s$ such that $\sum_{l=1}^{s} m_l = n$, the number $\mathcal{N}(f, m_1, \dots, m_s)$ of unramified points $t_0 \in \mathbb{F}_q$ such that $\prod_{l=1}^{s} \mathbb{F}_{q^{m_l}}/\mathbb{F}_q$ is the specialization algebra of f at t_0 can be evaluated as follows:*

$$\left| \mathcal{N}(f, m_1, \dots, m_s) - \frac{(q+1)\,|m_1^1 \dots m_s^1|}{n!} \right| \leq r\, n! \sqrt{q}$$

with $|m_1^1 \dots m_s^1|$ the cardinality of the conjugacy class $[m_1^1 \dots m_s^1]$.

5. but not necessarily Zariski-open.
6. Note that the statement does not hold if $n = 1$.

This result extends similar estimates which have appeared in the literature for $\mathbb{F}_q$-G-covers under the name of Tchebotarev theorems for function fields over finite fields. See [Wei48], [Fri74], [Eke90], [FJ05, chapter 6] and also [DG11, §3.5] where the analog of corollary 5.2.3 for $\mathbb{F}_q$-G-covers is obtained as the outcome of our approach in the standard situation (b) of §5.1.2.2.

For the type $m_1^1 \dots m_s^1 = n^1$ of the n-cycles, we obtain that the number $\mathcal{N}(f, n)$ is asymptotic to q/n when $q \to +\infty$. For example, if q is a prime p and f is given by the trinomial $Y^n + Y - T$ (which satisfies the assumptions of corollary 5.2.3 if $p \not| n(n-1)$ [Ser92, §4.4]; see also §B.3.1.1), the number of irreducible trinomials $Y^n + Y + a \in \mathbb{F}_p[Y]$ realizing the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$, *i.e.* such that one of its roots generates $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, is asymptotic to p/n as $p \to \infty$, a result due to Cohen [Coh70] and Ree [Ree71] proving a conjecture of Chowla [Cho66].

Proof. We are in the standard situation (a) of §5.1.2.2. Then condition (const/comp) holds. Moreover it follows from the beginning note of §5.1.2.2 that the number of elements $\gamma \in \Gamma$ for which condition (2)-(b) of lemma 5.1.4 holds is 1; denote the corresponding isomorphism by χ_0. From this lemma, the set of unramified $\mathbb{F}_q$-rational points on the twisted curve $\widetilde{Z}^{\chi_0\varphi}$ maps, *via* the regular $\mathbb{F}_q$-cover $\widetilde{g}^{\chi_0\varphi} : \widetilde{Z}^{\chi_0\varphi} \to \mathbb{P}^1$, to the set of points $t_0 \in \mathbb{P}^1(\mathbb{F}_q)$ satisfying the required condition. Moreover, the covers $\widetilde{g}^{\chi_0\varphi}$ and g (where $g : Z \to \mathbb{P}^1$ is as before the Galois closure of f) being isomorphic over $\overline{\mathbb{F}_q}$, they have the same degree, which is $n!$, and the same branch point number, which is the branch point number r of f. Using part (4) of remark 5.1.3 and the fact that $r(n!-1)$ is an upper bound for the number of points on $\widetilde{Z}^{\chi_0\varphi}$ above the ramified points, we obtain

$$0 \leq \frac{|\widetilde{Z}^{\chi_0\varphi}(\mathbb{F}_q)|}{|\mathrm{Cen}_{S_n}(\chi_0(H))|} - \mathcal{N}(f, m_1, \dots, m_s) \leq \frac{r(n!-1)}{|\mathrm{Cen}_{S_n}(\chi_0(H))|} + 1$$

where $H = \mathrm{Gal}(\mathbb{F}_{q^M}/\mathbb{F}_q)$ with $M = \mathrm{lcm}(m_1, \dots, m_s)$.

The cyclic subgroup $\chi_0(H) \subset S_n$ is generated by a permutation of type $m_1^1 \dots m_s^1$ (condition (2)-(b) of the twisting lemma 5.1.4). Hence we have $|\mathrm{Cen}_{S_n}(\chi_0(H))| = n!/|m_1^1 \dots m_s^1|$. Denote next the genus of $\widetilde{Z}^{\chi_0\varphi}$ (which is the same as that of Z) by g. The Lang-Weil estimates give

$$\left| \, |\widetilde{Z}^{\chi_0\varphi}(\mathbb{F}_q)| - (q+1) \right| \leq 2\mathrm{g}\sqrt{q}$$

The Riemann-Hurwitz formula yields $\mathrm{g} \leq (r-2)(n!-1)/2$. Conjoining this and the fact that the largest cardinality of a conjugacy class in S_n is $n(n-2)!$, *i.e.* that of the class $[1^1(n-1)^1]$, provides the announced estimate. □

In the two standard situations (b) and (c) of §5.1.2.2, conjoining the twisting lemma and the Lang-Weil estimates provides analogs of corollaries 5.2.1 and 5.2.2 in the case $B = \mathbb{P}^1$ (for simplicity) where the PAC field k should be replaced by any finite field $\mathbb{F}_q$ such that $q \geq r^2|\overline{G}|^2$ with r the branch point number and $\overline{G}$ the geometric monodromy group of the cover there (see §4.2.2 for more details), and the conclusion holds for at least one unramified point $t_0 \in \mathbb{F}_q$.

5.2.3 Ample fields

In the ample [7] field case, the twisting lemma 5.1.4 yields corollary 5.2.4 below which extends statement $(***)$ of [Dèb99c, §3.3.2] to the most general situation of arbitrary covers:

Corollary 5.2.4. *Let k be an ample field, $f : X \to B$ be a k-cover of curves and $t_0 \in B(k)$ be an unramified point. Then there exist infinitely many distinct unramified points $t \in B(k)$ such that the specialization algebras $\prod_l k(X)_{t,l}/k$ and $\prod_l k(X)_{t_0,l}/k$ at t and t_0 respectively are equal.*

7. See §B.2.2 for the definition and some examples of ample fields.

By using the Galois form of the twisting lemma instead of the general form, one may give a Galois variant of this statement (and of corollaries 5.2.6 and 5.2.7 below too) with the k-cover $f : X \to B$ replaced by any k-G-Galois cover $g : Z \to B$ and the specialization algebra $\prod_l k(X)_{t_0,l}/k$ of f at t_0 by the specialization $k(Z)_{t_0}/k$ of g at t_0.

Proof. Take the k-étale algebra $\prod_{l=1}^s F_l/k$ of the twisting lemma 5.1.4 to be the specialization algebra of f at t_0. With the notation of §5.1.1, we have $\varphi = \phi \circ \mathsf{s}_{t_0}$ and $\overline{\varphi} = \Lambda$. Hence condition (const/comp) holds with $\overline{\chi} = \mathrm{Id}_{G/\overline{G}}$.

By implication (1) $\Rightarrow$ (2) in the twisting lemma 5.1.4, there exists some $\gamma \in \Gamma$ such that conditions (2)-(a) and (2)-(b) are satisfied for t_0 with $\chi = \chi_\gamma$. Condition (2)-(a) is that there exists some $x_0 \in \widetilde{Z}^{\chi\varphi}(k)$ such that $\widetilde{g}^{\chi\varphi}(x_0) = t_0$. As k is ample and $\widetilde{Z}^{\chi\varphi}$ is a smooth k-curve, there exist infinitely many distinct k-rational points x on $\widetilde{Z}^{\chi\varphi}$. The corresponding points $t = \widetilde{g}^{\chi\varphi}(x) \in B(k)$, excluding the ramified points, satisfy conditions (2)-(a) and (2)-(b) of the twisting lemma 5.1.4. Implication (2) $\Rightarrow$ (1) in this lemma finishes the proof. □

Remark 5.2.5. The proof and the result generalize to higher dimensional k-covers $f : X \to B$. It should be assumed however that the covering space Z^{sep} of the (regular) k^{sep}-cover $Z^{\mathrm{sep}} \to B \otimes_k k^{\mathrm{sep}}$ corresponding to the function field extension $k^{\mathrm{sep}}(Z)/k^{\mathrm{sep}}(B)$ is smooth (Z^{sep} is the normalization of B in the field $k^{\mathrm{sep}}(Z)$ and so is *a priori* only normal). The ampleness of k then provides a Zariski-dense subset of k-rational points on $\widetilde{Z}^{\chi\varphi}$ and the conclusion becomes that there exists some Zariski-dense subset $\mathcal{B} \subset B(k) \setminus D$ such that the specialization algebra $\prod_l k(X)_{t,l}/k$ at each $t \in \mathcal{B}$ equals $\prod_l k(X)_{t_0,l}/k$.

5.2.4 Number fields

5.2.4.1. Genus zero curves. In the genus zero situation, the twisting lemma 5.1.4 provides the following statement:

Corollary 5.2.6. *Let k be a number field*[8]*, $f : X \to \mathbb{P}^1$ be a k-cover and $t_0 \in \mathbb{P}^1(k)$ be an unramified point. Assume that the genus g of the covering space Z of the Galois closure $g : Z \to \mathbb{P}^1$ of f satisfies $\mathrm{g} = 0$. Then there exist infinitely many distinct unramified points $t \in \mathbb{P}^1(k)$ such that the specialization algebras $\prod_l k(X)_{t,l}/k$ and $\prod_l k(X)_{t_0,l}/k$ of f at t and t_0 respectively are equal.*

Proof. The proof is exactly the same as that of corollary 5.2.4 at the only difference that, to obtain that there exist infinitely many distinct k-rational points x on $\widetilde{Z}^{\chi\varphi}$ from the existence of at least one such point x_0, the ampleness of k and the smoothness of the curve $\widetilde{Z}^{\chi\varphi}$ should be replaced by the fact that $\widetilde{Z}^{\chi\varphi}$ has genus zero from our assumption and then that it is birational to $\mathbb{P}^1$ over k; the infiniteness of k then providing the desired points. □

5.2.4.2. Using the Faltings theorem. In higher genus situations, conjoining the twisting lemma 5.1.4 and the Faltings theorem provides corollary 5.2.7 below:

Corollary 5.2.7. *Let k be a number field, $f : X \to \mathbb{P}^1$ be a k-cover and $t_0 \in \mathbb{P}^1(k)$ be an unramified point. Assume that the genus g of the covering space Z of the Galois closure $g : Z \to \mathbb{P}^1$ of f satisfies $\mathrm{g} \geq 2$. Then there exist only finitely many distinct unramified points $t \in \mathbb{P}^1(k)$ (possibly none) such that the specialization algebras $\prod_l k(X)_{t,l}/k$ and $\prod_l k(X)_{t_0,l}/k$ of f at t and t_0 respectively are equal.*

8. The statement remains true if k is assumed to be infinite.

Proof. As before, take the k-étale algebra $\prod_{l=1}^{s} F_l/k$ of the twisting lemma 5.1.4 to be the specialization algebra of f at t_0. With the notation of §5.1.1, we have $\varphi = \phi \circ \mathsf{s}_{t_0}$ and $\overline{\varphi} = \Lambda$. Hence condition (const/comp) holds with $\overline{\chi} = \mathrm{Id}_{G/\overline{G}}$.

By implication (1) $\Rightarrow$ (2) in the twisting lemma 5.1.4, it suffices to show that the set $\bigcup_{\gamma\in\Gamma} \widetilde{Z}^{\chi_\gamma\varphi}(k)$ is finite. Since Γ is finite, this amounts to showing that $\widetilde{Z}^{\chi_\gamma\varphi}(k)$ is finite for each $\gamma \in \Gamma$. But each twisted curve $\widetilde{Z}^{\chi_\gamma\varphi}$ has genus ≥ 2 from our assumption and the conclusion then follows from the Faltings theorem. $\square$

5.2.4.3. Local-global results. We follow below a local-global approach as in chapter 4 and in [DG12]. We start with a local result at one prime. We give two versions: a *mere version* for a regular cover $f : X \to \mathbb{P}^1$ and a G-*Galois version* for a G-Galois cover $g : Z \to \mathbb{P}^1$.

We first set up some notation for the next two statements. Let k be a number field, $f : X \to \mathbb{P}^1$ be a regular k-cover of degree n, r be its branch point number, G be its monodromy group, $\overline{G}$ be its geometric monodromy group, $g : Z \to \mathbb{P}^1$ be its Galois closure, $\nu : G \to S_n$ be the Galois representation of $k(X)/k(T)$ relative to $k(Z)$ and $\widehat{k}_g/k$ be the constant extension in g.

Corollary 5.2.8. *Fix*

(mere version) *the type $1^{\beta_1} \dots n^{\beta_n}$ of some element of $\nu(\overline{G}) \subset S_n$,*

(G-Galois version) *an element $\omega \in \overline{G}$.*

Then, for each prime number $p \geq r^2|\overline{G}|^2$, good[9] *and totally split in $\widehat{k}_g/\mathbb{Q}$, there exists some integer b_p such that, for each integer $t_0 \equiv b_p \bmod p$, t_0 is unramified and*

(mere version) *the specialization algebra of $f \otimes_k \mathbb{Q}_p$ at t_0 is an unramified $\mathbb{Q}_p$-étale algebra $\prod_l F_l/\mathbb{Q}_p$*[10] *with degree divisor $\prod_l [F_l : \mathbb{Q}_p]^1 = 1^{\beta_1} \dots n^{\beta_n}$,*

(G-Galois version) *the specialization of the $\mathbb{Q}_p$-*G*-cover $g \otimes_k \mathbb{Q}_p$ at t_0 is the unramified extension $N_p/\mathbb{Q}_p$ of degree $|\langle\omega\rangle|$.*

The mere version extends [Fri74, theorem 4]: if $\nu(\overline{G})$ contains an n-cycle, then, for $1^{\beta_1} \dots n^{\beta_n} = n^1$, the conclusion of corollary 5.2.8, stated as in [Fri74] in the case f is given by a polynomial $P(T, Y)$, is that $P(t_0, Y)$ is irreducible over $\mathbb{Q}_p$, and so over k is too.

Proof. Consider first the mere version. Let p be a totally split prime number in the extension $\widehat{k}_g/\mathbb{Q}$ (infinitely many such primes exist from the Tchebotarev density theorem). In particular, one has $\mathbb{Q}_p\widehat{k}_g = \mathbb{Q}_p$. For each index $i \in \{1, \dots, n\}$ such that $\beta_i > 0$, let $F^{p,i}/\mathbb{Q}_p$ be the unique unramified extension of $\mathbb{Q}_p$ of degree i. Here we use the twisting lemma 5.1.4 in the "cyclic specializations" standard situation (c) of §5.1.2.2; we apply it to the regular $\mathbb{Q}_p$-cover $f \otimes_k \mathbb{Q}_p$ and the $\mathbb{Q}_p$-étale algebra $\prod_i (F^{p,i}/\mathbb{Q}_p)^{\beta_i}$ where the exponent β_i indicates that the extension $F^{p,i}/\mathbb{Q}_p$ appears β_i times. Condition (const/comp) holds by definition of $\widehat{k}_g$ and condition (2)-(b) of lemma 5.1.4 holds for some isomorphism χ_γ with $\gamma \in \Gamma$ (part (c) of §5.1.2.2). If p is a good prime, the twisted curve $\widetilde{Z}^{\chi_\gamma\varphi} \otimes_k \mathbb{Q}_p$ has good reduction [DG12, lemma 2.6] and the Lang-Weil estimates show that, if $p \geq r^2|\overline{G}|^2$, then the special fiber has at least one unramified $\mathbb{F}_p$-rational point (see §4.2.2 for more details). From Hensel's lemma, such a $\mathbb{F}_p$-rational point lifts to a $\mathbb{Q}_p$-rational point on $\widetilde{Z}^{\chi_\gamma\varphi}$. Conclude by lemma 5.1.4 that the $\mathbb{Q}_p$-étale algebra $\prod_i (F^{p,i}/\mathbb{Q}_p)^{\beta_i}$ is the specialization algebra of $f \otimes_k \mathbb{Q}_p$ at each point t_0 in a coset of $\mathbb{Z}_p$ modulo $p\mathbb{Z}_p$.

The G-Galois version is quite similar, but it is the Galois form of the twisting lemma (lemma 5.1.2) which should be applied, to the $\mathbb{Q}_p$-G-cover $g \otimes_k \mathbb{Q}_p$ and the unique unramified extension

9. See definition 1.2.5 (condition (4) there can be removed here).

10. *i.e.* such that any field extension $F_l/\mathbb{Q}_p$ is unramified.

of $\mathbb{Q}_p$ of degree $|\langle\omega\rangle|$. In particular, for each point t_0 in the announced coset, the Galois group $\mathrm{Gal}(\mathbb{Q}_p(Z)_{t_0}/\mathbb{Q}_p)$ of the specialization of $g \otimes_k \mathbb{Q}_p$ at t_0 is conjugate in $\overline{G}$ to $\langle\omega\rangle$. □

Corollary 5.2.8 can be used simultaneously for several types of elements in $\nu(\overline{G}) \subset S_n$ and for several elements of $\overline{G}$. The chinese remainder theorem then provides arithmetic progressions $(am+b)_{m\in\mathbb{Z}} \subset \mathbb{Z}$ with ratio a the product of the corresponding prime numbers. In particular, it can be guaranteed that the specialization at $am+b$ (for every $m \in \mathbb{Z}$) of the $\widehat{k}_g$-G-cover $g \otimes_k \widehat{k}_g$ is a Galois extension of group $\overline{G}$: according to [Jor72] (and the end of the proof of corollary 5.2.8), it suffices to use all the non trivial elements of $\overline{G}$. This implies that the specialization at $am+b$ of the original k-G-Galois cover g is a Galois extension of Galois group a subgroup of G containing $\overline{G}$. As the original k-cover f is assumed to be regular (and so $\nu(\overline{G})$ is a transitive subgroup of S_n), the specialization algebra at $am+b$ of f consists of a single field extension of k of degree n, *i.e.* the Hilbert specialization property holds at $am+b$ (for any $m \in \mathbb{Z}$).

We obtain the following statement which generalizes corollary 4.3.6 to arbitrary regular covers. The constants however are not as good as in the "$G = \overline{G} = S_n$" situation of chapter 4 because of the preliminary condition on the primes which uses the Tchebotarev density theorem.

Corollary 5.2.9. *There exist two positive integers m_0 and β only depending on f and satisfying the following conclusion. Let $\mathcal{S}$ be a finite set of prime numbers $p > m_0$, good and totally split in $\widehat{k}_g/\mathbb{Q}$, each given with positive integers $d_{p,1}, \dots, d_{p,s_p}$ such that $d^1_{p,1} \dots d^1_{p,s_p}$ is the type of some element in $\nu(\overline{G})$. Then there exists some integer b satisfying the following:*

for each integer $t_0 \equiv b \bmod (\beta \prod_{p\in\mathcal{S}} p)$, t_0 is unramified and the specialization algebra of f at t_0 consists of a single field extension of k of degree n which has residue degrees $d_{p,1}, \dots, d_{p,s_p}$ at p for each prime $p \in \mathcal{S}$.

Addendum 5.2.9 (on the constants) Denote the number of non trivial conjugacy classes of $\overline{G}$ by $\mathrm{cc}(\overline{G})$. One can take m_0 such that the interval $[r^2|\overline{G}|^2, m_0]$ contains at least $\mathrm{cc}(\overline{G})$ distinct prime numbers, good and totally split in $\widehat{k}_g/\mathbb{Q}$ and β to be the product of $\mathrm{cc}(\overline{G})$ such primes.

Proof. We use corollary 5.2.8 simultaneaously for several prime numbers: a first set of primes associated to all non trivial elements of $\overline{G}$ as explained in addendum 5.2.9 and the set of primes given in the statement with the associated types. We apply the G-Galois version of corollary 5.2.8 to the former data and the mere version to the latter. This provides an arithmetic progression $(am+b)_{m\in\mathbb{Z}} \subset \mathbb{Z}$ with ratio $a = \beta \prod_{p\in\mathcal{S}} p$ (where $\beta > 0$ is the product of all prime numbers in the first set). The prime numbers dividing β guarantee that the specialization algebra at $am+b$ of the original regular k-cover f consists of a single field extension F/k of degree n (as explained above). And each of the prime numbers $p \in \mathcal{S}$ yields that the $\mathbb{Q}_p$-étale algebra $F \otimes_k \mathbb{Q}_p$ has degree divisor $d^1_{p,1} \dots d^1_{p,s_p}$, thus ending the proof. □

Bibliography

[Ang07] Julien Angeli. Trinômes irréductibles résolubles sur un corps de nombres. *Acta Arith.*, 127(2):169–178, 2007.

[Ang09] Julien Angeli. *Trinômes à petits groupes de Galois*. Thèse de doctorat, Université de Limoges, 2009.

[BBSR13] Efrat Bank, Lior Bary-Soroker, and Lior Rosenzweig. Prime polynomials in short intervals and in arithmetic progressions. *manuscript*, 2013. ArXiv:1302.0625.

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

[Bec94] Sybilla Beckmann. Is every extension of $\mathbb{Q}$ the specialization of a branched covering? *J. Algebra*, 164(2):430–451, 1994.

[Bla98] Elena V. Black. Aritmetical lifting of dihedral extensions. *J. Algebra*, 203(1):12–29, 1998.

[Bla99] Elena V. Black. Deformations of dihedral 2-group extensions of fields. *Trans. Amer. Math. Soc.*, 351(8):3229–3241, 1999.

[BS09] Lior Bary-Soroker. Dirichlet's theorem for polynomial rings. *Proc. Amer. Math. Soc.*, 137(1):73–83, 2009.

[BS12] Lior Bary-Soroker. Irreducible values of polynomials. *Adv. Math.*, 229(2):854–874, 2012.

[C+85] J .H. Conway et al. *Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray.* Oxford University Press, Eynsham, 1985.

[Cho66] Sarvadaman Chowla. A note on the construction of finite Galois fields $\mathrm{GF}(p^n)$. *J. Math. Anal. Appl.*, 15:53–54, 1966.

[Coh70] Stephen D. Cohen. The distribution of polynomials over finite fields. *Acta Arith.*, 17:255–271, 1970.

[Coh80] Stephen D. Cohen. The Galois group of a polynomial with two indeterminate coefficients. *Pacific J. Math.*, 90(1):63–76, 1980.

[Coh81] Stephen D. Cohen. Corrections to [Coh80]. *Pacific J. Math.*, 97(2):483–486, 1981.

[CT00] Jean-Louis Colliot-Thélène. Rational connectedness and Galois covers of the projective line. *Ann. of Math. (2)*, 151(1):359–373, 2000.

[DD97a] Pierre Dèbes and Bruno Deschamps. The regular inverse Galois problem over large fields. In *Geometric Galois actions 2*, volume 243 of *London Math. Soc. Lecture Note Ser.*, pages 119–138. Cambridge Univ. Press, Cambridge, 1997.

[DD97b] Pierre Dèbes and Jean-Claude Douai. Algebraic covers: field of moduli versus field of definition. *Ann. Sci. École Norm. Sup. (4)*, 30(3):303–338, 1997.

[Dèb95] Pierre Dèbes. Covers of $\mathbb{P}^1$ over the p-adics. In *Recent developments in the inverse Galois problem (Seattle, WA, 1993)*, volume 186 of *Contemp. Math.*, pages 217–238. Amer. Math. Soc., Providence, RI, 1995.

[Dèb99a] Pierre Dèbes. Arithmétique et espaces de modules de revêtements. In *Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997)*, pages 75–102. de Gruyter, Berlin, 1999.

[Dèb99b] Pierre Dèbes. Density results for Hilbert subsets. *Indian J. Pure Appl. Math.*, 30(1):109–127, 1999.

[Dèb99c] Pierre Dèbes. Galois covers with prescribed fibers: the Beckmann-Black problem. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 28(2):273–286, 1999.

[Dèb99d] Pierre Dèbes. Some arithmetic properties of algebraic covers. In *Aspects of Galois Theory (Gainesville, FL, 1996)*, volume 256 of *London Math. Soc. Lecture Note Ser.*, pages 66–84. Cambridge University Press, Cambridge, 1999.

[Dèb01] Pierre Dèbes. Méthodes topologiques et analytiques en théorie inverse de Galois: théorème d'existence de Riemann. In *Arithmétique de revêtements algébriques (Saint-Étienne, 2000)*, volume 5 of *Sémin. Congr.*, pages 27–41. Soc. Math. France, Paris, 2001.

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

[Des95] Bruno Deschamps. Existence de points p-adiques pour tout p sur un espace de Hurwitz. In *Recent developments in the inverse Galois problem (Seattle, WA, 1993)*, volume 186 of *Contemp. Math.*, pages 239–247. Amer. Math. Soc., Providence, RI, 1995.

[DF90] Pierre Dèbes and Michael D. Fried. Rigidity and real residue class fields. *Acta Arith.*, 56(4):291–323, 1990.

[DF94] Pierre Dèbes and Michael D. Fried. Nonrigid constructions in Galois theory. *Pacific J. Math.*, 163(1):81–122, 1994.

[DG11] Pierre Dèbes and Nour Ghazi. Specializations of Galois covers of the line. In *"Alexandru Myller" Mathematical Seminar*, volume 1329 of *AIP Conf. Proc.*, pages 98–108. Amer. Inst. Phys., Melville, NY, 2011.

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

[DH98] Pierre Dèbes and David Harbater. Fields of definition of p-adic covers. *J. Reine Angew. Math.*, 498:223–236, 1998.

[DL12] Pierre Dèbes and François Legrand. Twisted covers and specializations. In *Galois-Teichmueller theory and Arithmetic Geometry*, pages 141–162. Proceedings for Conferences in Kyoto (October 2010), H. Nakamura, F. Pop, L. Schneps, A. Tamagawa eds., Advanced Studies in Pure Mathematics 63, 2012.

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

[DW08] Pierre Dèbes and Yann Walkowiak. Bounds for Hilbert's irreducibility theorem. *Pure Appl. Math. Q.*, 4(4):1059–1083, 2008.

[Eke90] Torsten Ekedahl. An effective version of Hilbert's irreducibility theorem. In *Séminaire de Théorie des Nombres, Paris 1988-1989*, volume 91 of *Progr. Math.*, pages 241–249. Birkhäuser Boston, Boston, MA, 1990.

[FJ05] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete.* Springer-Verlag, Berlin, 2005. (first edition 1986).

[Flo02] Stéphane Flon. *Mauvaises places ramifiées dans le corps des modules d'un revêtement.* PhD thesis, Université des Sciences et Technologies de Lille, 2002.

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

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

[Fri95] Michael D. Fried. Introduction to modular towers: generalizing dihedral group–modular curve connections. In *Recent developments in the inverse Galois problem (Seattle, WA, 1993)*, volume 186 of *Contemp. Math.*, pages 111–171. Amer. Math. Soc., Providence, RI, 1995.

[FV91] Michael D. Fried and Helmut Völklein. The inverse Galois problem and rational points on moduli spaces. *Math. Ann.*, 290(4):771–800, 1991.

[Gey78] Wulf-Dieter Geyer. Galois groups of intersections of local fields. *Israel J. Math.*, 30(4):382–396, 1978.

[Gro65] Alexandre Grothendieck. *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II.*, volume 24 of *Inst. Hautes Études Sci. Publ. Math.* 1965.

[Har84] David Harbater. Mock covers and Galois extensions. *J. Algebra*, 91(2):281–293, 1984.

[Har87] David Harbater. Galois covering of the arithmetic line. In *Number theory (New-York, 1984-1985)*, volume 1240 of *Lecture Notes in Math.*, pages 165–195. Springer, Berlin, 1987.

[Hei67] Hans Arnold Heilbronn. Zeta-functions and L-functions. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 204–230. Thompson, Washington, D.C., 1967.

[HJ98] Dan Haran and Moshe Jarden. Regular split embeddings problems over complete valued fields. *Forum Math.*, 10(3):329–351, 1998.

[HRD03] Emmanuel Hallouin and Emmanuel Riboulet-Deyris. Computation of some moduli spaces of covers and explicit S_n and A_n regular $\mathbb{Q}(T)$-extensions with totally real fibers. *Pacific J. Math.*, 211(1):81–99, 2003.

[JLY02] Christian U. Jensen, Arne Ledet, and Noriko Yui. *Generic polynomials. Constructive Aspects of the Inverse Galois Problem.* Cambridge University Press, 2002.

[Jor72] Camille Jordan. Recherches sur les substitutions. *J. Liouville*, 17:351–367, 1872.

[Kem01] Gregor Kemper. Generic polynomials are descent-generic. *Manuscripta Math.*, 105(1):139–141, 2001.

[KM01] Jürgen Klüners and Gunter Malle. A database for field extensions of the rationals. *LMS J. Comput. Math.*, 4:182–196, 2001.

[KM04] Jürgen Klüners and Gunter Malle. Counting nilpotent Galois extensions. *J. Reine Angew. Math.*, 572:1–26, 2004.

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

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, revised third edition, 2002.

[Led] Arne Ledet. *Errata to Generic Polynomials.* at http://www.math.ttu.edu/ aledet/papers/corr.pdf.

[Leg13a] François Legrand. Parametric Galois extensions. *manuscript*, 2013. ArXiv:1310.6682.

[Leg13b] François Legrand. Specialization results and ramification conditions. *manuscript*, 2013. ArXiv:1310.2189.

[Mat86] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986. Translated from the Japanese by M. Reid.

[MB01] Laurent Moret-Bailly. Construction de revêtements de courbes pointées. *J. Algebra*, 240(2):505–534, 2001.

[Mes90] Jean-François Mestre. Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\tilde{A}_n$. *J. Algebra*, 131(2):483–495, 1990.

[MM99] Gunter Malle and B. Heinrich Matzat. *Inverse Galois Theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.

[MSW94] Gunter Malle, Jan Saxl, and Thomas Weigel. Generation of classical groups. *Geom. Dedicata*, 49(1):85–116, 1994.

[Nag69] Trygve Nagell. Sur les diviseurs premiers des polynômes. *Acta Arith.*, 15:235–244, 1969.

[Neu79] Jürgen Neukirch. On solvable number fields. *Invent. Math.*, 53(2):135–164, 1979.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*, volume 323 of *Grundlehren de mathematischen Wissenschaften*. Springer, Berlin, second edition, 2008.

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

[PV05] Bernat Plans and Núria Vila. Galois covers of $\mathbb{P}^1$ over $\mathbb{Q}$ with prescribed local or global behavior by specialization. *J. Théor. Nombres Bordeaux*, 17(1):271–282, 2005.

[Ram13] Lorenzo Ramero. *Grimoire d'algèbre commutative.* 2013. at http://math.univ-lille1.fr/ ramero/CoursAG.pdf.

[Ree71] Rimhak Ree. Proof of a conjecture of S. Chowla. *J. Number Theory*, 3:210–212, 1971.

[Sch00] Andrzej Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2000.

[Ser70] Jean-Pierre Serre. *Cours d'arithmétique.* Collections SUP: "Le Mathématicien", 2. Presses Universitaires de France, Paris, 1970.

[Ser92] Jean-Pierre Serre. *Topics in Galois Theory*, volume 1 of *Research Notes in Mathematics*. Jones and Bartlett Publishers, Boston, MA, 1992.

[Tho84] John G. Thompson. Some finite groups which appear as $\mathrm{Gal}(L/K)$, where $K \subseteq \mathbb{Q}(\mu_n)$. *J. Algebra*, 89(2):437–499, 1984.

[Tra90] Artur Travesa. Nombre d'extensions abéliennes sur $\mathbb{Q}$. *Sém. Théor. Nombres Bordeaux (2)*, 2(2):413–423, 1990.

[Uch70] Koji Uchida. Galois group of an equation $X^n - aX + b = 0$. *Tôhoku Math. J. (2)*, 22:670–678, 1970.

[Völ96] Helmut Völklein. *Groups as Galois groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996.

[Wag78] Ascher Wagner. The minimal number of involutions generating some finite three-dimensional groups. *Boll. Un. Mat. Ital. A (5)*, 15(2):431–439, 1978.

[Wan48] Shianghaw Wang. A counter-example to Grunwald's theorem. *Ann. of Math. (2)*, 49:1008–1009, 1948.

[Wei48] André Weil. *Sur les courbes algébriques et les variétés algébriques qui s'en déduisent.* Hermann et Cie., Paris, 1948.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.

Résumé

On s'intéresse dans cette thèse à des questions portant sur les spécialisations de revêtements algébriques (galoisiens ou non). Le thème central de la première partie de ce travail est la construction de spécialisations de n'importe quel revêtement galoisien $f : X \to \mathbb{P}^1$ de groupe G défini sur k dont on impose d'une part le comportement local en un nombre fini d'idéaux premiers de k et dont on assure d'autre part qu'elles restent de groupe G si le corps k est hilbertien. Dans la deuxième partie, on développe une méthode générale pour qu'un revêtement galoisien $f : X \to \mathbb{P}^1$ de groupe G défini sur k vérifie la propriété suivante : étant donné un sous-groupe H de G, il existe au moins une extension galoisienne F/k de groupe H qui n'est pas spécialisation de $f : X \to \mathbb{P}^1$. De nombreux exemples sont donnés. La troisième partie consiste en l'étude de la question suivante : une extension galoisienne F/k, ou plus généralement une k-algèbre étale $\prod_l F_l/k$, est-elle la spécialisation d'un revêtement $f : X \to B$ défini sur k (galoisien ou non) en un certain point non-ramifié $t_0 \in B(k)$? Notre principal outil est un *twisting lemma* qui réduit la question à trouver des points k-rationnels sur certaines k-variétés que nous étudions ensuite pour des corps de base k variés.

Mots-clés : théorie de Galois, problème inverse de Galois, revêtements algébriques, spécialisations, théorème d'irréductibilité de Hilbert, extensions paramétriques, twisting lemma.

Abstract

We are interested in this thesis in some questions concerning specializations of algebraic covers (Galois or not). The main theme of the first part consists in producing some specializations of any Galois cover $f : X \to \mathbb{P}^1$ of group G defined over k with specified local behavior at finitely many given primes of k and which each have in addition Galois group G if k is assumed to be hilbertian. In the second part, we offer a systematic approach for a given Galois cover $f : X \to \mathbb{P}^1$ of group G defined over k to satisfy the following property: given a subgroup $H \subset G$, at least one Galois extension F/k of group H is not a specialization of $f : X \to \mathbb{P}^1$. Many examples are given. The central question of the third part is whether a given Galois extension F/k, or more generally a given k-étale algebra $\prod_l F_l/k$, is the specialization of a given cover $f : X \to B$ defined over k (Galois or not) at some unramified point $t_0 \in B(k)$? Our main tool is a *twisting lemma* which reduces the problem to finding k-rational points on some k-varieties which we then study for various base fields k.

Keywords: Galois theory, inverse Galois problem, algebraic covers, specializations, Hilbert irreducibility theorem, parametric extensions, twisting lemma.