Deux sujets en théorie des nombres : spécialisation de Hilbert de variétés paramétrées et structure galoisienne de la racine carrée de la codifférente

Angelo Iadarola

Université de Lille

Laboratoire Paul Painlevé

THÈSE

présentée pour obtenir le grade de

DOCTEUR DE

L'UNIVERSITÉ DE LILLE

École Doctorale SPI
Faculté des Sciences et Technologies
Spécialité Mathématiques et leurs interactions

par

Angelo IADAROLA

Two topics in Number Theory: Hilbert specialization of parametrized varieties and Galois module structure of the square root of the inverse different

---

Sous la direction de Prof. Pierre DÈBES et de Prof. Bouchaïb SODAÏGUI
Soutenue le 24/06/2021, devant le jury composé de:

Lior BARY-SOROKER	Professor, Tel Aviv University	Rapporteur
Nigel P. BYOTT	Associate Professor, University of Exeter	Rapporteur
Philippe CASSOU-NOGUÈS	Professeur Émérite, Université Bordeaux 1	Examinateur
Sara CHECCOLI	Maître de Conférences, Université Grenoble Alpes	Examinateur
Ilaria DEL CORSO	Professore Associato, Università di Pisa	Examinateur
Bruno DESCHAMPS	Professeur, Université du Maine	Président
Pierre DÈBES	Professeur, Université de Lille	Directeur
Bouchaïb SODAÏGUI	Professeur, UPHF	Directeur

Univ. Lille, CNRS, UMR 8524 - Laboratoire Paul Painlevé, F-59000 Lille, France

Université de Lille

Laboratoire Paul Painlevé

THÈSE

présentée pour obtenir le grade de

DOCTEUR DE

L'UNIVERSITÉ DE LILLE

École Doctorale SPI
Faculté des Sciences et Technologies
Spécialité Mathématiques et leurs interactions

par

Angelo IADAROLA

Deux sujets en théorie des nombres : spécialisation de Hilbert de variétés paramétrées et structure galoisienne de la racine carrée de la codifférente

---

Sous la direction de Prof. Pierre DÈBES et de Prof. Bouchaïb SODAÏGUI
Soutenue le 24/06/2021, devant le jury composé de:

Lior BARY-SOROKER	Professor, Tel Aviv University	Rapporteur
Nigel P. BYOTT	Associate Professor, University of Exeter	Rapporteur
Philippe CASSOU-NOGUÈS	Professeur Émérite, Université Bordeaux 1	Examinateur
Sara CHECCOLI	Maître de Conférences, Université Grenoble Alpes	Examinateur
Ilaria DEL CORSO	Professore Associato, Università di Pisa	Examinateur
Bruno DESCHAMPS	Professeur, Université du Maine	Président
Pierre DÈBES	Professeur, Université de Lille	Directeur
Bouchaïb SODAÏGUI	Professeur, UPHF	Directeur

Univ. Lille, CNRS, UMR 8524 - Laboratoire Paul Painlevé, F-59000 Lille, France

Acknowledgements

First and foremost, I would like to thank my supervisors, Pierre and Bouchaib. Without their aid and their support, I would not have made it until the end. They have always been available for my doubts, my worries and my problems, not only the mathematical ones.

I want to express my gratitude to Nigel Byott and Lior Bary-Soroker for accepting to be the referees of this thesis and dedicating some time to read it. Their suggestions have certainly been useful to improve this text.

I would also like to thank the other members of my jury, Philippe Cassou-Noguès, Sara Checcoli, Ilaria Del Corso and Bruno Deschamps, for accepting to be (virtually) present at my defense.

I would like to thank Monica for her immense patience. During this tough period she has had the ungrateful duty of tolerating me all day long. She has always been there whenever I needed someone to talk to and unload myself.

I would like to thank Fabrizio, Gaia, Giulio and Mariagiulia. Their friendship and their help has really been invaluable to me, both outside and inside the lab.

I would like to thank the rest of the Quai du Wault family, Chaki, Markus and Victoire. During these tough times we have spent a lot of time together and their presence has been very important to get distracted from the world outside.

I would like to thank Ele, Giuliana, Virgi and many others for the uncountable moments we have spent together during these years. Their presence has been fundamental to help me freeing up my mind from the daily problems.

I would like to thank Angelo, Valeria and Vincenzo. Even if from far away, I have always felt their support throughout this journey.

Per ultima, ma assolutamente non per importanza, vorrei ringraziare la mia famiglia. Il loro supporto è stato sempre costante e preziosissimo durante questi anni. Anche se a distanza, non mi hanno mai fatto mancare il loro amore.

To all the people I have mentioned, explicitly or implicitly, and to the ones I may have forgot, I hope that I have been able to give back at least half of what I have received.

Contents

Introduction

Given a number field K, denote by O_K its ring of integers and $\mathrm{Cl}(K)$ its class group.

Consider an extension of number fields E/K: [Nar04, Theorem 1.32], applied in the case of number fields, implies the so-called *Steinitz decomposition*

$$O_E \cong O_K^{[E:K]-1} \oplus I$$

for some ideal I of O_K. Moreover, [Nar04, Theorem 1.39] implies that the isomorphism still holds if we multiply I by a principal ideal. This means that the structure of O_E as an O_K-module is determined by the class $[I] \in \mathrm{Cl}(K)$. We call $[I]$ the *Steinitz class* of E/K and we denote it by $\mathrm{cl}_K(O_E)$.

Now, given a number field K and a finite group Γ, we define the subset of $\mathrm{Cl}(K)$ given by the *tamely realizable* Steinitz classes over K with Galois group isomorphic to Γ as

$$R_m(O, K[\Gamma]) = \{c \in \mathrm{Cl}(K) | c = \mathrm{cl}_K(O_E) \text{ for } E/K \text{ tamely ramified and } \mathrm{Gal}(E/K) \cong \Gamma\}.$$

The following is a classical conjecture in algebraic number theory (see, for example, [BGS06]).

Conjecture. *For every choice of the base number field K and of the finite group Γ, $R_m(O, K[\Gamma])$ is a subgroup of $\mathrm{Cl}(K)$.*

This conjecture is still widely open, in particular in the case where Γ is a non-abelian simple group.

Take, for example, $\Gamma = A_n$ for $n \geq 5$, the *alternating group of degree n* of order $\frac{n!}{2}$, a non-abelian simple group. The original approach was to investigate the problem posed by the above conjecture in an innovative way, using the Hilbert specialization of Galois extensions of number fields.

This approach was, at first, very promising. On the one side, Hilbert specialization lets us construct infinitely many extensions of number fields E/K of Galois group A_n from just one extension $N/K(T)$ by specializing at different values $t_0 \in K$. On the other side, a famous problem in Inverse Galois Theory, the *Beckmann-Black problem* [Bla99], is known to be true for every alternating group A_n thanks to Mestre [Mes90]: this implies that, for every number field K and every extension (in particular the tamely ramified ones) E/K of Galois group A_n, there exists a regular extension $N/K(T)$ of Galois group A_n such that E/K is its specialization at t_0 for some $t_0 \in K$.

Though still promising, this strategy encountered problems at the level of basic tools.

On the side of the Hilbert specialization, some pieces of information about the ramification of ideals of O_K in O_E can be deduced from the branch points of $N/K(T)$, see [Bec91, Leg16], but other aspects are still unclear. For this reason, we want to increase the complexity of the data, by looking at *multivariate Galois extensions* $N/K(T_1, \dots, T_n)$ and by analyzing the specialization at the level of the ideals in $K[T_1, \dots, T_n]$, or even $O_K[T_1, \dots, T_n]$, about which the knowledge is quite scarce. This is, indeed, what we will deal with in Chapter 1.

On the side of the structure of Galois modules and Steinitz classes we approached the problem in a new direction, following recent developments by Tsang [Tsa16, Tsa17], which extended the problem from the ring of integers O_E to other ambiguous fractional ideals of O_E, such as, for example, the square root of the inverse different, which we will denote by $\mathcal{A}_{E/K}$.

We now present two topics through the introductions of the two papers, which will also appear in the appropriate chapter to preserve the wholeness of the two texts. The introduction to the second topic is here translated in English, for the sake of non-francophone readers.

Introduction to the Hilbert specialization of parametrized varieties

The Hilbert Irreducibility Theorem has been a core result in Field Arithmetic for many decades. A simple form, see for example [FJ08, Page 218], says that, given an irreducible polynomial $P(T, Y)$ in $\mathbb{Q}(T)[Y]$, one can find infinitely many $t \in \mathbb{Q}$ such that the so-called *specialized* polynomial $P(t, Y)$ is irreducible in $\mathbb{Q}[Y]$.

This result has been generalized under many aspects. First of all, the notion of *Hilbertian field* has been introduced to identify all those fields K for which the previous statement is verified in the case of polynomials, which are separable in Y, if we replace $\mathbb{Q}$ with K, see for example [FJ08, Page 218]. Moreover, if K is of characteristic 0 or imperfect, the same result holds if we replace a separable irreducible polynomial in two variables $P(T, Y)$ in $K(T)[Y]$ with several irreducible polynomials $P_1(\underline{T}, \underline{Y}), \dots, P_n(\underline{T}, \underline{Y})$ in $K(\underline{T})[\underline{Y}]$ in two arrays of variables, $\underline{T} = (T_1, \dots, T_r)$ and $\underline{Y} = (Y_1, \dots, Y_s)$ for r, s positive integers: we can find a Zariski-dense subset $H \subset \mathbb{A}^r_K$ such that the polynomial $P_i(\underline{t}, \underline{Y})$ is irreducible in $K[\underline{Y}]$ for every $\underline{t} \in H$ and $i = 1, \dots, n$, see for example [FJ08, Section 12.1].

If we look at this statement from a geometric point of view, another potential generalization arises naturally. Giving an irreducible polynomial $P(\underline{T}, \underline{Y})$ in $K(\underline{T})[\underline{Y}]$ is equivalent to giving an irreducible $K(\underline{T})$-hypersurface[1] $V_{K(\underline{T})}(P(\underline{T}, \underline{Y}))$ in the s-dimensional

[1] The precise definition will be given later.

affine space $\mathbb{A}^s_{K(\underline{T})}$ over $K(\underline{T})$. In these terms, for K Hilbertian and of characteristic 0 or imperfect, Hilbert Irreducibility says that for a Zariski-dense set of choices $\underline{t}$ of the variables $\underline{T}$ in K^r, the *specialized* algebraic set $V_K(P(\underline{t},\underline{Y})) \subset \mathbb{A}^s_K$ is an irreducible K-hypersurface. It is then natural to ask if an analogous result holds in the case of a $K(\underline{T})$-variety of codimension bigger than 1. In algebraic terms this is equivalent to finding values $\underline{t}$ in K^r of $\underline{T}$ such that a nonzero prime ideal $\mathfrak{p}_T$ in $K(\underline{T})[\underline{Y}]$ remains a nonzero prime ideal of $K[\underline{Y}]$ when *specializing* $\underline{T}$ at $\underline{t}$. This is indeed one of the problems we are addressing in Chapter 1.

We want to make another step further. Until now the Hilbert *specialization* has typically been intended for scalar values in K^r. However, there is a recent result, see [BDN20], in which a polynomial version of the Schinzel hypothesis is proved by specializing at polynomial values instead of scalar values. Given irreducible polynomials $P_i(\underline{T},\underline{Y})$, for $i = 1,\dots,n$, in a polynomial ring $R[\underline{T},\underline{Y}]$ for R an integral domain, the variables $\underline{T}$ are replaced by polynomials $\underline{Q}(\underline{Y}) = (Q_1(\underline{Y}),\dots,Q_r(\underline{Y}))$, in the other variables and, under appropriate assumptions, all the *specialized* polynomials $P_i\left(\underline{Q}(\underline{Y}),\underline{Y}\right)$ are shown to remain irreducible in $R[\underline{Y}]$. This recent development encourages us to pursue the study of the specialization at polynomials. Indeed, another goal of Chapter 1 will be to apply the results of the first part to obtain a more general version of them where the *specialization* of the variables $\underline{T}$ occurs at polynomials in $(K[\underline{Y}])^r$ instead of scalars in K^r.

Introduction to the Galois module structure of the square root of the inverse different for metacyclic non-abelian extensions

In Chapter 2, if K is a number field, O_K indicates its ring of integers and $\mathrm{Cl}(K)$ its class group. If I is a fractional ideal of K, we denote its class in $\mathrm{Cl}(K)$ by $\mathrm{cl}_K(I)$, or simply by $\mathrm{cl}(I)$ if there cannot be any ambiguity.

Let k be a number field and Γ a finite group. Let $\mathcal{M}$ be a maximal O_k-order in the semisimple algebra $k[\Gamma]$ containing $O_k[\Gamma]$; sometimes, to be more precise, we will denote it by $\mathcal{M}(k[\Gamma])$. Let $\mathrm{Cl}(O_k[\Gamma])$ (resp. $\mathrm{Cl}(\mathcal{M})$) be the class group of the locally free $O_k[\Gamma]$-modules (resp. $\mathcal{M}$-modules) (see [Frö83, Chap. I]). Let M be a locally free $O_k[\Gamma]$-module. We can associate to M a class, denoted by $[M]$, in $\mathrm{Cl}(O_k[\Gamma])$ and, by scalar extension, the class of $\mathcal{M} \otimes_{O_k[\Gamma]} M$, denoted by $[\mathcal{M} \otimes_{O_k[\Gamma]} M]$, in $\mathrm{Cl}(\mathcal{M})$.

Let N/k be a Galois extension having Galois group isomorphic to Γ; we will often say that N/k is a Γ-extension. Let π be an isomorphism between $\mathrm{Gal}(N/k)$ and Γ. For every $\gamma \in \Gamma$, we will denote $\pi^{-1}(\gamma) \in \mathrm{Gal}(N/k)$ just by γ.

Let $\mathcal{D}_{N/k}$ be the different of N/k. Assume that the square root of the inverse different $\mathcal{D}^{-1}_{N/k}$ exists and denote it by $\mathcal{A}_{N/k}$. Immediately, $\mathcal{A}_{N/k}$ is an ambiguous fractional ideal

of the extension N/k (i.e. it is stable under the action of $\mathrm{Gal}(N/k)$, so it is a Γ-module).

We note that, by the Hilbert formula (see [Ser68, Proposition 4, p. 72]), if N/k is tamely ramified, $\mathcal{A}_{N/k}$ exists if, and only if, the ramification indices in N/k are odd; in particular this holds if Γ has odd order.

Using π, we endow $\mathcal{A}_{N/k}$ with a structure of $O_k[\Gamma]$-module defined by: for every $x \in \mathcal{A}_{N/k}$ and every $\gamma \in \Gamma$, $\gamma x = \gamma(x)$. We denote by $\mathcal{A}_{N/k,\pi}$, or simply $\mathcal{A}_{N/k}$ if there cannot be any ambiguity, the $O_k[\Gamma]$-module we have just defined. We note that the number of such structures is equal to the order of the group of automorphisms of Γ.

From [Ull74, Proposition 1.3], if N/k is tamely ramified, then $\mathcal{A}_{N/k}$ is a projective $O_k[\Gamma]$-module, so it is a locally free $O_k[\Gamma]$-module (by a result of Swan).

We know that, if N/k is tamely ramified, then O_N is a locally free $O_k[\Gamma]$-module. We briefly recall the definition of the realisable classes by the ring of integers. We denote by $\mathcal{R}(O, O_k[\Gamma])$ (resp. $\mathcal{R}(O, \mathcal{M})$) the set of classes c of $\mathrm{Cl}(O_k)[\Gamma]$ (resp. $\mathrm{Cl}(\mathcal{M})$) such that there exists a tamely ramified extension N/k having Galois group isomorphic to Γ, with $[O_N] = c$ (resp. $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] = c$).

In a similar manner, we denote by $\mathcal{R}(\mathcal{A}, O_k[\Gamma])$ (resp. $\mathcal{R}(\mathcal{A}, \mathcal{M})$) the set of classes c of $\mathrm{Cl}(O_k[\Gamma])$ (resp. $\mathrm{Cl}(\mathcal{M})$) such that there exists a tamely ramified extension N/k having Galois group isomorphic to Γ, with $[\mathcal{A}_{N/k}] = c$ (resp. $[\mathcal{M} \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k}] = c$). We will say that $\mathcal{R}(\mathcal{A}, O_k[\Gamma])$ (resp. $\mathcal{R}(\mathcal{A}, \mathcal{M})$) is the set of realisable classes by the square root of the inverse different. We note that these two sets are linked by the relation $\mathrm{Ex}(\mathcal{R}(\mathcal{A}, O_k[\Gamma])) = \mathcal{R}(\mathcal{A}, \mathcal{M})$, where $\mathrm{Ex} : \mathrm{Cl}(O_k[\Gamma]) \to \mathrm{Cl}(\mathcal{M})$ is the surjective morphism induced by the scalar extension from $O_k[\Gamma]$ to $\mathcal{M}$.

Let $\mathrm{Tr}_{N/k}$ be the trace in N/k. We have that $\mathrm{Tr}_{N/k}(\mathcal{A}_{N/k}) = O_k$ because $O_N \subset \mathcal{A}_{N/k} \subset \mathcal{D}_{N/k}^{-1}$, $\mathrm{Tr}_{N/k}(O_N) = O_k$ (N/k is tamely ramified) and $\mathrm{Tr}_{N/k}(\mathcal{D}_{N/k}^{-1}) \subset O_k$ (by definition of $\mathcal{D}_{N/k}^{-1}$).

Denote by $\mathrm{Cl}^\circ(O_k[\Gamma])$ (resp. $\mathrm{Cl}^\circ(\mathcal{M})$) the kernel of the morphism $\mathrm{Cl}(O_k[\Gamma]) \to \mathrm{Cl}(k)$ (resp. $\mathrm{Cl}(\mathcal{M}) \to \mathrm{Cl}(k)$) induced by the augmentation morphism $O_k[\Gamma] \to O_k$ (resp. $\mathcal{M} \to O_k$). It follows from $\mathrm{Tr}_{N/k}(\mathcal{A}_{N/k}) = O_k$ that $\mathcal{R}(\mathcal{A}, O_k[\Gamma]) \subset \mathrm{Cl}^\circ(O_k[\Gamma])$ and $\mathcal{R}(\mathcal{A}, \mathcal{M}) \subset \mathrm{Cl}^\circ(\mathcal{M})$.

In the same manner to some conjectures about $\mathcal{R}(O, O_k[\Gamma])$ and $\mathcal{R}(O, \mathcal{M})$ (see for example [BGS06]), we conjecture:

Conjecture 1. *The set* $\mathcal{R}(\mathcal{A}, O_k[\Gamma])$ *is a subgroup of* $\mathrm{Cl}^\circ(O_k[\Gamma])$.

Conjecture 2. *The set* $\mathcal{R}(\mathcal{A}, \mathcal{M})$ *is a subgroup of* $\mathrm{Cl}^\circ(\mathcal{M})$.

In the whole Chapter 2, we will assume that Γ has odd order.

On the one hand, as the group Γ is solvable (by Feit-Thompson), from the (famous) theorem of Shafarevich (see [NSW08, Theorem 9.6.1, p. 574, and Exercice (b), p. 597]), there exists a tamely ramified Galois extension N/k whose Galois group is isomorphic to Γ. On the other hand, $\mathcal{A}_{N/k}$ exists. We deduce, in particular, that the sets $\mathcal{R}(\mathcal{A}, O_k[\Gamma])$ and $\mathcal{R}(\mathcal{A}, \mathcal{M})$ are non-empty.

If $k = \mathbb{Q}$, we have that $\mathcal{R}(\mathcal{A}, O_k[\Gamma]) = \{1\}$ by [Ere91]: the proof is an adaptation of the proof of a theorem of M.J. Taylor (previously a conjecture of Fröhlich) about the structure of O_N as a $\mathbb{Z}[\Gamma]$-module (see [Tay81, Theorem 1]).

For every k and Γ abelian, Conjecture 1 holds [Tsa16, Theorem 1.3]. The proof is an adaptation of a theorem of McCulloh about the realisable classes by the ring of integers (see [McC87, Theorem 6.17 and Corollary 6.20]).

We recall the definition of Steinitz class. Let K be a number field. Let M be an O_K-module of finite type, without torsion and of rank n. Then, there exists an ideal I of O_K such that $M \simeq O_K^{n-1} \oplus I$ as an O_K-module. The class of I in $\mathrm{Cl}(K)$ is called the Steinitz class of M; we denote it by $\mathrm{cl}_K(M)$. We note that if M is a fractional ideal of K, $\mathrm{cl}_K(M)$ is the class of M in $\mathrm{Cl}(K)$. Thus, the structure of M, as an O_K-module, is fully determined by its rank and its Steinitz class. It is clear that M is a free O_K-module if, and only if, $\mathrm{cl}_K(M) = 1$.

We define $R_m(O, k[\Gamma])$ as the set of $c \in \mathrm{Cl}(k)$ such that there exists a tamely ramified Galois extension N/k whose Galois group is isomorphic to Γ and $\mathrm{cl}_k(O_N) = c$. We conjecture (see for example [BGS06]) that $R_m(O, k[\Gamma])$ is a subgroup of $\mathrm{Cl}(k)$ (with the order of Γ not necessarily odd).

In a similar manner, we define $R_m(\mathcal{A}, k[\Gamma])$ by replacing O_N with $\mathcal{A}_{N/k}$ in the above definition.

Proposition 0.1. *Let N/k be a Galois extension (tamely ramified or not) whose Galois group is isomorphic to Γ of odd order. Then, $\mathcal{A}_{N/k}$ is a free O_k-module.*

Proof. From [Mar69, Théorème I.4, p. 9] (it is a generalization of a theorem of Artin in [Art50]):

$$\mathrm{cl}_k(\mathcal{A}_{N/k}) = \mathrm{cl}_k\left(\sqrt{\frac{\Delta(\mathcal{A}_{N/k})}{d}}\right),$$

where $\Delta(\mathcal{A}_{N/k})$ is the discriminant, relative to the trace form $\mathrm{Tr}_{N/k}$, of the lattice $\mathcal{A}_{N/k}$ of the k-vector space N (see [Ser68, Chap. III, §2 and §3]) and d is the discriminant of a basis of k-vector space N.

As N/k is a Galois extension of odd degree,

$$\mathrm{cl}_k(\mathcal{A}_{N/k}) = \mathrm{cl}\left(\sqrt{\Delta(\mathcal{A}_{N/k})}\right),$$

because d is a square in k.

As $\mathcal{A}_{N/k}$ is a fractional ideal of N, from [Mar69, Théorème I.5, p. 10] we have that:

$$\Delta(\mathcal{A}_{N/k}) = \Delta(N/k) N'_{N/k}(\mathcal{A}_{N/k})^2,$$

where $\Delta(N/k)$ is the discriminant of N/k and $N'_{N/k}$ is the norm in N/k. We deduce that

$$\Delta(\mathcal{A}_{N/k}) = O_k,$$

because $\mathcal{A}_{N/k}^2 = \mathcal{D}_{N/k}^{-1}$ and $N'_{N/k}(\mathcal{D}_{N/k}) = \Delta(N/k)$. We conclude that $\mathrm{cl}_k(\mathcal{A}_{N/k}) = 1$. □

Corollary 0.2. *We have that* $R_m(\mathcal{A}, k[\Gamma]) = \{1\}$.

In Chapter 2, we will treat Conjecture 2. In Section 2.2, we will describe in an explicit way the set $\mathcal{R}(\mathcal{A}, \mathcal{M})$ where $\Gamma = C_l$ is the cyclic group of order an odd prime number l and k is linearly disjoint over $\mathbb{Q}$ with the l-th cyclotomic field over $\mathbb{Q}$ and we prove that $\mathcal{R}(\mathcal{A}, \mathcal{M})$ is a subgroup of $\mathrm{Cl}^\circ(\mathcal{M})$; the proof is an adaptation of a proof in [Sod88]. Then, in Section 2.3, we will apply the results obtained in Section 2.2 to describe a subset of $\mathcal{R}(\mathcal{A}, \mathcal{M})$ when Γ is a non-abelian metacyclic group of order lq, where q is a prime number, in the same situation as in [SS10, Sod97]. Adapting the proofs in those papers, we prove that that subset is a subgroup of $\mathrm{Cl}^\circ(\mathcal{M})$. In Section 2.3, we will give a non-explicit generalization of the main results of Section 2.2.

We finishe this section with a remark.

It is well known (see [Ere91, Théorème 1,§1]) that $\mathcal{A}_{N/k}$ is a locally free $O_k[\Gamma]$-module if, and only if, N/k is weakly ramified (i.e. the second ramification group is trivial).

Let $\mathcal{R}_f(\mathcal{A}, \mathcal{M})$ be the set of classes c of $\mathrm{Cl}(\mathcal{M})$ such that there exists a weakly ramified extension N/k whose Galois group is isomorphic to Γ, satisfying $[\mathcal{M} \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k}] = c$. When Γ is abelian, from [Tsa17, Theorem 1.2] we have that $\mathcal{R}_f(\mathcal{A}, \mathcal{M}) = \mathcal{R}(\mathcal{A}, \mathcal{M})$. So, in the abelian case, when we work in $\mathrm{Cl}(\mathcal{M})$, we do not lose anything by limiting the study to the tamely ramified extensions when we look at the realisable classes by the square root of the inverse different.

1 Hilbert specialization of parametrized varieties

1.1 Introduction

The Hilbert Irreducibility Theorem has been a core result in Field Arithmetic for many decades. A simple form, see for example [FJ08, Page 218], says that, given an irreducible polynomial $P(T,Y)$ in $\mathbb{Q}(T)[Y]$, one can find infinitely many $t \in \mathbb{Q}$ such that the so-called *specialized* polynomial $P(t,Y)$ is irreducible in $\mathbb{Q}[Y]$.

This result has been generalized under many aspects. First of all, the notion of *Hilbertian field* has been introduced to identify all those fields K for which the previous statement is verified in the case of polynomials, which are separable in Y, if we replace $\mathbb{Q}$ with K, see for example [FJ08, Page 218]. Moreover, if K is of characteristic 0 or imperfect, the same result holds if we replace a separable irreducible polynomial in two variables $P(T,Y)$ in $K(T)[Y]$ with several irreducible polynomials $P_1(\underline{T},\underline{Y}),\dots,P_n(\underline{T},\underline{Y})$ in $K(\underline{T})[\underline{Y}]$ in two arrays of variables, $\underline{T} = (T_1,\dots,T_r)$ and $\underline{Y} = (Y_1,\dots,Y_s)$ for r,s positive integers: we can find a Zariski-dense subset $H \subset \mathbb{A}^r_K$ such that the polynomial $P_i(\underline{t},\underline{Y})$ is irreducible in $K[\underline{Y}]$ for every $\underline{t} \in H$ and $i = 1,\dots,n$, see for example [FJ08, Section 12.1].

If we look at this statement from a geometric point of view, another potential generalization arises naturally. Giving an irreducible polynomial $P(\underline{T},\underline{Y})$ in $K(\underline{T})[\underline{Y}]$ is equivalent to giving an irreducible $K(\underline{T})$-hypersurface[1] $V_{K(\underline{T})}(P(\underline{T},\underline{Y}))$ in the s-dimensional affine space $\mathbb{A}^s_{K(\underline{T})}$ over $K(\underline{T})$. In these terms, for K Hilbertian and of characteristic 0 or imperfect, Hilbert Irreducibility says that for a Zariski-dense set of choices $\underline{t}$ of the variables $\underline{T}$ in K^r, the *specialized* algebraic set $V_K(P(\underline{t},\underline{Y})) \subset \mathbb{A}^s_K$ is an irreducible K-hypersurface. It is then natural to ask if an analogous result holds in the case of a $K(\underline{T})$-variety of codimension bigger than 1. In algebraic terms this is equivalent to finding values $\underline{t}$ in K^r of $\underline{T}$ such that a nonzero prime ideal $\mathfrak{p}_T$ in $K(\underline{T})[\underline{Y}]$ remains a nonzero prime ideal of $K[\underline{Y}]$ when *specializing* $\underline{T}$ at $\underline{t}$. This is indeed one of the problems we are addressing in Chapter 1.

We want to make another step further. Until now the Hilbert *specialization* has typically been intended for scalar values in K^r. However, there is a recent result, see [BDN20], in which a polynomial version of the Schinzel hypothesis is proved by specializ-

[1] The precise definition will be given later.

ing at polynomial values instead of scalar values. Given irreducible polynomials $P_i(\underline{T}, \underline{Y})$, for $i = 1, \dots, n$, in a polynomial ring $R[\underline{T}, \underline{Y}]$ for R an integral domain, the variables $\underline{T}$ are replaced by polynomials $\underline{Q}(\underline{Y}) = (Q_1(\underline{Y}), \dots, Q_r(\underline{Y}))$, in the other variables and, under appropriate assumptions, all the *specialized* polynomials $P_i\left(\underline{Q}(\underline{Y}), \underline{Y}\right)$ are shown to remain irreducible in $R[\underline{Y}]$. This recent development encourages us to pursue the study of the specialization at polynomials. Indeed, another goal of Chapter 1 will be to apply the results of the first part to obtain a more general version of them where the *specialization* of the variables $\underline{T}$ occurs at polynomials in $(K[\underline{Y}])^r$ instead of scalars in K^r.

1.1.1 Notation and main results

In this chapter, given a field F, a set of variables $\underline{X} = (X_1, \dots, X_m)$ and polynomials $f_1, \dots, f_n$ in $F[\underline{X}]$, we denote by $V_F(f_1, \dots, f_n)$ the *affine subvariety* of $\mathbb{A}^m_F$ of equations $\{f_i(x_1, \dots, x_m) = 0, i = 1, \dots, n\}$. More formally, following [Liu02, Definition 3.4.7], it is the affine scheme associated to the finitely generated F-algebra $F[\underline{X}]/\langle f_1, \dots, f_n\rangle$. As, by extension of scalars, the same set of elements gives rise to different varieties over different fields, to avoid any ambiguity, we use the word *F-variety* to specify the base field. If the ideal $\langle f_1, \dots, f_n\rangle$ is prime in $F[\underline{X}]$, we say that the F-variety is *irreducible*. Moreover, if the F-variety has codimension[2] 1, we call it an *F-hypersurface*. Finally we say that an irreducible F-variety is *separable* if $\mathrm{Frac}\left(F[\underline{X}]/\langle f_1, \dots, f_n\rangle\right)$ is a separable extension of F, in the general sense as in [FJ08, Lemma 2.6.1].

We state the first result of the chapter.

Theorem 1.1.1. *Let K be a Hilbertian field, $\underline{P}(\underline{T}, \underline{Y}) = \{P_1(\underline{T}, \underline{Y}), \dots, P_l(\underline{T}, \underline{Y})\}$ a set of polynomials in $K[\underline{T}, \underline{Y}]$ such that $V_T = V_{K(\underline{T})}(\underline{P}(\underline{T}, \underline{Y}))$ is a separable irreducible $K(\underline{T})$-variety. Then for every $\underline{t} = (t_1, \dots, t_r) \in K^r$ in some Zariski-dense subset of $\mathbb{A}^r_K$, the K-variety $V_t = V_K(\underline{P}(\underline{t}, \underline{Y})) \subset \mathbb{A}^s_K$, where $\underline{P}(\underline{t}, \underline{Y})$ is the set made of the specialized polynomials at $\underline{t}$, is irreducible and its dimension $\dim_K V_t$ is equal to $\dim_{K(\underline{T})} V_T$, the dimension of V_T as a $K(\underline{T})$-variety.*

Remarks 1.1.2. (a) Even if the polynomials in $\underline{P}$ are irreducible, it is not enough that the corresponding specialized polynomials $P_i(\underline{t}, \underline{Y})$ are irreducible to conclude that the variety $V_K(\underline{P}(\underline{t}, \underline{Y}))$ is irreducible. Generally speaking, it may be that an ideal is generated by irreducible polynomials in $K[\underline{Y}]$ but is not a prime ideal. Take for example the ideal $\langle Y - X, Y - X^2\rangle$, which contains the product $X(X - 1)$.

(b) Hilbert specialization in the case of polynomials can be also performed over rings instead of fields, as in [BDKN20, Theorem 1.6 and Remark 4.4]. It is then natural to ask if we can extend Theorem 1.1.1 to a ring R as well, at least when R is a Unique

[2] We define the dimension of a variety as the Krull dimension of the ring $F[\underline{X}]/\langle f_1, \dots, f_n\rangle$.

Factorization Domain. As our proof and [BDKN20] suggest, it may be possible that such a version holds if a nonzero element $\varphi \in R$ is inverted, i.e. if R is replaced by $R[\varphi^{-1}]$ (a restriction that cannot be avoided in general). This, however, remains unclear at the moment.

(c) Theorem 1.1.1 can be seen as a Hilbertian version of Bertini's Theorem. If we look at the statement of Bertini's Theorem given in [FJ08, Corollary 10.4.3], we can see the similarity between the two statements. However, the two statements go on parallel routes. Bertini's Theorem demands an algebraically closed base field K. In particular the case $s = 1$ is excluded in the Bertini context while it is a significant situation in the Hilbert context of Theorem 1.1.1.

A recurrent tool in the chapter will be the *generic* polynomial. Given an integer $D \geq 0$ we define the *generic* polynomial of degree D:

$$\mathcal{Q}_D(\underline{\Lambda}, \underline{Y}) = \sum_{i=1}^{N_D} \Lambda_i Q_i(\underline{Y})$$

where $Q_i(\underline{Y})$ varies over all the power products $Y_1^{\beta_1} \cdots Y_s^{\beta_s}$, $\beta_i \geq 0$, in the variables $\underline{Y}$ of degree smaller or equal than D and N_D is the number of such power products and $\underline{\Lambda} = (\Lambda_1, \ldots, \Lambda_{N_D})$ is a set of auxiliary variables, which correspond to the "generic" coefficients.

The application of Theorem 1.1.1, with these variables $\underline{\Lambda}$ playing the role of the variables $\underline{T}$ in the statement of Theorem 1.1.1, is the main tool of the proof of the next two statements.

The first one is about the intersection between an irreducible K-variety and a "generic" $K(\underline{T})$-hypersurface.

Theorem 1.1.3. *Let K be a Hilbertian field of characteristic 0. Let $P_1(\underline{Y}), \ldots, P_l(\underline{Y})$, for $l \geq 1$, be polynomials in $K[\underline{Y}]$ such that $V = V_K(P_1, \ldots, P_l)$ is an irreducible K-variety of positive dimension d. Then, for every $\underline{\lambda} \in K^{N_D}$ in a Zariski-dense subset of $\mathbb{A}_K^{N_D}$, the K-variety $V \cap V_K(\mathcal{Q}_D(\underline{\lambda}, \underline{Y}))$ is irreducible and $\dim_K V \cap V_K(\mathcal{Q}_D(\underline{\lambda}, \underline{Y}))) = d - 1$.*

We will see that a more general result, in fact, holds. If we replace the "generic" hypersurface by an intersection of ρ "generic" hypersurfaces, with $\rho \leq d$, the intersection with the original variety V will "often" be an irreducible K-variety of dimension $d - \rho$, see Corollary 1.3.6.

The generic polynomial will be central also in the proof of the last main result of this chapter, where the goal is to generalize Theorem 1.1.1 to the situation in which the variables are specialized at polynomials.

We note that the set $K[\underline{Y}]_D$ of all the polynomials of degree smaller or equal than D can be endowed with a Zariski topology through the natural isomorphism with $\mathbb{A}_K^{N_D}$ which associates to a polynomial $P(\underline{Y})$ the point in $\mathbb{A}_K^{N_D}$ having the coefficients of P as coordinates.

Theorem 1.1.4. *Let K be a Hilbertian field of characteristic 0. Let $P_1(\underline{T},\underline{Y}),\dots,P_l(\underline{T},\underline{Y})$, for $l \geq 1$, be polynomials in $K[\underline{T},\underline{Y}]$ such that $V_T = V_{K(\underline{T})}(P_1,\dots,P_l)$ is an irreducible $K(\underline{T})$-variety of dimension d. Fix non-negative integers $D_1,\dots,D_r$. Then for every $\underline{U} = (U_1(\underline{Y}),\dots,U_r(\underline{Y}))$ in a Zariski-dense subset of $\prod_{i=1}^r K[\underline{Y}]_{D_i}$, the K-variety $V_U = V_K(P_1(\underline{U},\underline{Y}),\dots,P_l(\underline{U},\underline{Y}))$ is an irreducible K-variety of dimension $\dim_K V_U = d$.*

Remarks 1.1.5. (a) The case $l = r = 1$ (i.e. one polynomial and one variable T) yields the Schinzel hypothesis for the polynomial ring $K[\underline{Y}]$, as stated in [BDN20, Section 1.1]: given an irreducible polynomial $P(T,\underline{Y})$ in $K[T,\underline{Y}]$, for every $U(\underline{Y})$ in some Zariski-dense subset of $K[\underline{Y}]_D$, the polynomial $P(U(\underline{Y}),\underline{Y})$ is irreducible in $K[\underline{Y}]$.

(b) By taking $D_i = 0$, for every i, Theorem 1.1.4 implies Theorem 1.1.1 in characteristic 0 (see Remark 1.3.9).

1.1.2 Hilbert sets

In this introduction, we have restricted the choice of the base field to a Hilbertian field. However, these statements can be generalized to every field thanks to the notion of *Hilbert sets*. We are giving only a quick review on this topic; refer to [FJ08, Sections 12,13] for more details.

Given a set of irreducible polynomials $P_1(\underline{T},\underline{Y}),\dots,P_l(\underline{T},\underline{Y})$ in $K(\underline{T})[\underline{Y}]$, we define the following set:

$$H_K(P_1,\dots,P_l) = \{\underline{t} \in K^r | P_i(\underline{t},\underline{Y}) \text{ is irreducible in } K[\underline{Y}] \text{ for each } i = 1,\dots,l\}.$$

Such sets and their intersections with non-empty open Zariski-subsets are called *Hilbert subsets* of K^r. Or else, if we do not specify the dimension r, we say that $H_K(P_1,\dots,P_l)$ is a *Hilbert set* of K to say that it is a Hilbert subset of K^r for some r. This definition does not require any hypothesis on the field.

These sets can be empty: take for example $K = \mathbb{C}$ and $P(T,Y) \in \mathbb{C}(T)[Y]$, an irreducible complex monic polynomial, such that $\deg_Y P > 1$.

Therefore we define the *Hilbertian fields*, which we have already mentioned, as the fields for which all these sets are Zariski-dense in $\mathbb{A}^r_K$. Of course Hilbertian fields are the most convenient setting because the sets of elements for which our results hold are generally as big as possible.

By definition, Hilbert sets are stable under finite intersection. We will show, in the next sections, that the Zariski-dense subsets involved in Theorems 1.1.1, 1.1.3 and 1.1.4 are, in fact, Hilbert sets, with no assumption on the field K. Consequently, our main results hold, in fact, for a finite number of varieties/ideals.

In particular, the original Hilbert irreducibility property in its full form, i.e. for several polynomials $P_1,\dots,P_l$, follows from Theorem 1.1.1: just apply it to each of the prime ideals $\langle P_i\rangle$ and then take the intersection of the Hilbert sets.

The chapter is organized as follows. In Section 1.2 we will focus on Theorem 1.1.1: we will see the two steps of its proof and some further remarks. Some more preliminary tools will be added when convenient. In Section 1.3 we will first give some results about generic polynomials and then, finally, we will use them to obtain the proofs of Theorems 1.1.3 and 1.1.4.

1.2 Proof of Theorem 1.1.1

The cornerstone of the chapter is the proof of Theorem 1.1.1, which will be essential to prove Theorems 1.1.3 and 1.1.4. The statement we are actually going to prove hereinafter is a more general version of Theorem 1.1.1.

Theorem 1.2.1. *Let K be a field. Assume that $\mathfrak{p}_T = \langle P_1(\underline{T},\underline{Y}),\dots,P_l(\underline{T},\underline{Y})\rangle$ is a prime ideal in $K[\underline{T},\underline{Y}]$ such that $\mathfrak{p}_T \cap K[\underline{T}] = \{0\}$ and $\operatorname{Frac}\left(K[\underline{T},\underline{Y}]/\mathfrak{p}_T\right)$ is separable over $K(\underline{T})$. Denote by d the dimension of $K[\underline{T},\underline{Y}]/\mathfrak{p}_T$ as a $K[\underline{T}]$-algebra. Then for every $\underline{t}$ in a Hilbert subset of K^r, the following equivalent statements hold:*

(i) *The quotient $K[\underline{Y}]/\mathfrak{p}_t$ is an integral algebra of dimension d over K, where $\mathfrak{p}_t = \langle P_1(\underline{t},\underline{Y}),\dots,P_l(\underline{t},\underline{Y})\rangle$ is the specialized ideal.*

(ii) *The ideal $\mathfrak{p}_t$ is prime and its height $\operatorname{ht}\mathfrak{p}_t$ is equal to the height $\operatorname{ht}\mathfrak{p}_T$ of $\mathfrak{p}_T$.*

(iii) *The K-variety $V_t = V(\underline{P}(\underline{t},\underline{Y}))$, where $\underline{P}(\underline{t},\underline{Y})$ is the set made of the specialized polynomials at $\underline{t}$, is irreducible and its dimension $\dim_K V_t$ is equal to $\dim_{K(\underline{T})} V_T$, the dimension of V_T as a $K(\underline{T})$-variety.*

Remark 1.2.2. Consider the extreme case for which the ideal $\mathfrak{p}_T$ in Theorem 1.2.1 is maximal as an ideal in $K(\underline{T})[\underline{Y}]$. Then the quotient $K(\underline{T})[\underline{Y}]/\mathfrak{p}_T$ is an algebraic separable field extension of $K(\underline{T})$ of finite degree. In this case, Theorem 1.2.1 implies the well-known fact that the degree of the extension is preserved under specialization at every $\underline{t}$ in a Hilbert set of K. Moreover, if the extension is Galois, then also the Galois group of the extension is preserved. The study of the specialization of Galois extensions is central in Inverse Galois Theory, see for example [Völ96, FJ08].

The equivalence between the three statements is easy. The proof is given right after the following lemma, which we will frequently use in the chapter.

Lemma 1.2.3. *Let K be a field. Then, given a prime ideal*

$$\mathfrak{p} = \langle P_1(\underline{T},\underline{Y}),\dots,P_l(\underline{T},\underline{Y})\rangle \subset K[\underline{T},\underline{Y}]$$

such that $\mathfrak{p}\cap K[\underline{T}] = \{0\}$, the ideal

$$\tilde{\mathfrak{p}} = \langle P_1(\underline{T},\underline{Y}),\dots,P_l(\underline{T},\underline{Y})\rangle \subset K(\underline{T})[\underline{Y}]$$

is prime and its height $\operatorname{ht}\tilde{\mathfrak{p}}$ is equal to the height $\operatorname{ht}\mathfrak{p}$ of $\mathfrak{p}$.

Proof. Denoting $S = K[\underline{T}] \setminus \{0\}$, we remark that S is a multiplicative subset and $S^{-1}K[\underline{T},\underline{Y}] = K(\underline{T})[\underline{Y}]$. The natural morphism sending an element a in $K[\underline{T},\underline{Y}]$ to $\frac{a}{1}$ in $S^{-1}K[\underline{T},\underline{Y}]$ induces a bijective correspondence between prime ideals in $K[\underline{T},\underline{Y}]$ having empty intersection with S and prime ideals in $K(\underline{T})[\underline{Y}]$ [AM69, Proposition 3.11(iv)]. So we can consider the prime ideal $\tilde{\mathfrak{p}}$ associated to $\mathfrak{p}$ by this correspondence, which is the ideal generated by the image of $\mathfrak{p}$ under the aforementioned morphism: the ideal

$$\tilde{\mathfrak{p}} = \langle P_1(\underline{T},\underline{Y}), \ldots, P_l(\underline{T},\underline{Y})\rangle \subset K(\underline{T})[\underline{Y}]$$

is prime.

Now we want to check that the height is preserved by this extension. Consider a maximal chain of primes in $\mathfrak{p}$ in $K[\underline{T},\underline{Y}]$,

$$\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \ldots \subset \mathfrak{p}.$$

As $\mathfrak{p}_i \subset \mathfrak{p}$ for each i, we have $\mathfrak{p}_i \cap S = \emptyset$, so $\tilde{p}_i$ is prime in $K(\underline{T})[\underline{Y}]$. Since the inclusions are conserved for $\tilde{\mathfrak{p}}_i$, we have $\operatorname{ht}\mathfrak{p} \leq \operatorname{ht}\tilde{\mathfrak{p}}$. Vice versa, assume that a chain of primes $\tilde{\mathfrak{p}}_i$ inside $\tilde{\mathfrak{p}}$ is longer than $\operatorname{ht}\mathfrak{p}$: by the previous correspondence we can build a chain of ideals inside $\mathfrak{p}$ longer than $\operatorname{ht}\mathfrak{p}$, which is a contradiction. So $\operatorname{ht}\mathfrak{p} = \operatorname{ht}\tilde{\mathfrak{p}}$. □

We can now give the proof of the equivalence between the three statements of Theorem 1.2.1.

Proof. (i)⇔(ii) It easily follows from the fact that the height of the ideal is equal to the codimension of the quotient algebra by the ideal.

(ii)⇔(iii) Assume that (ii) holds. By Lemma 1.2.3, $\operatorname{ht}\mathfrak{p}_T = \operatorname{ht}\tilde{\mathfrak{p}}_T$. By statement (ii), $\operatorname{ht}\mathfrak{p}_t = \operatorname{ht}\mathfrak{p}_T$. So $\operatorname{ht}\mathfrak{p}_t = \operatorname{ht}\tilde{\mathfrak{p}}_T$. As the height of a prime ideal is the codimension of the associated variety and the rings $K(\underline{T})[\underline{Y}]$ and $K[\underline{Y}]$ have the same Krull dimension, statement (iii) follows. The converse is easily shown in the same manner. □

There are two requirements for statement (i) of Theorem 1.2.1: we want $K[\underline{T},\underline{Y}]/\mathfrak{p}_T$ to be integral and of the correct dimension. We are going to prove the two parts separately: first we show that each integral component of $K[\underline{Y}]/\mathfrak{p}_t$ is of dimension d, then that there is only one such component.

1.2.1 First part

This part is mostly geometric. We are quickly recalling some tools that we are going to use. The statements are taken from [FGI+05].

Lemma 1.2.4 (Local freeness, Lemma 5.11)**.** *Let A be a Noetherian domain and B a finite-type A-algebra. Let M be a finite B-module. Then there exists $c \in A$, $c \neq 0$ such that the localisation $M\left[c^{-1}\right]$ is a free module over $A\left[c^{-1}\right]$.*

This result, due to Grothendieck, has a deep consequence, the so-called *Generic flatness*.

Theorem 1.2.5 (Generic flatness, Theorem 5.12)**.** *Let S be a Noetherian and integral scheme. Let $p : X \to S$ be a finite type morphism and let $\mathcal{F}$ be a coherent sheaf of $\mathcal{O}_X$-modules. Then there exists a non-empty open subscheme $U \subset S$ such that the restriction of $\mathcal{F}$ to $X_U = p^{-1}(U)$ is flat over $\mathcal{O}_U$.*

We do not want to go into the details of this statement, as it falls outside of the aim of this chapter. The only things we need to know are, first, that if a ring A is Noetherian, then the structural sheaf of $\operatorname{Spec} A$ is coherent as a sheaf of modules over itself [Har77, 5.2.1]. Moreover, if S is an affine integral scheme, i.e. $S = \operatorname{Spec} A$ for some domain A, then the open subscheme U in Theorem 1.2.5 is, indeed, $\operatorname{Spec} A\left[c^{-1}\right]$ for some c coming from local freeness.

Now we can begin the actual proof of Theorem 1.2.1.

Here is a diagram including all the maps involved, so to give also the necessary notation:

$$\begin{array}{ccc} K[\underline{T},\underline{Y}]\big/\mathfrak{p}_T & \xrightarrow{\mathrm{sp}_t} & K[\underline{Y}]\big/\mathfrak{p}_t \\ \uparrow{\scriptstyle i_T} & & \uparrow{\scriptstyle i_t} \\ K[\underline{T}] & \xrightarrow{\mathrm{sp}_t} & K \end{array}.$$

Here sp_t is the specialization map at the fixed point $\underline{t} \in K^r$. We will show that both maps $i_\bullet$ are injective.

As, by assumption, $\mathfrak{p}_T \cap K[\underline{T}] = \{0\}$, we have that i_T is an injection.

For i_t to be well defined and injective, we show that $\mathfrak{p}_t \cap K = \{0\}$, which is equivalent to showing that $\mathfrak{p}_t \neq K[\underline{Y}]$. Consider the ideal $\tilde{\mathfrak{p}}_T$, which, by Lemma 1.2.3, satisfies $\tilde{\mathfrak{p}}_T \subsetneq K(\underline{T})[\underline{Y}]$. By Weak Nullstellensatz [FJ08, Proposition 9.4.1], if $1 \notin \tilde{\mathfrak{p}}_T \subset K(\underline{T})[\underline{Y}]$, then there exists

$$\underline{x}(\underline{T}) = (x_1(\underline{T}), \dots, x_s(\underline{T})) \in \overline{K(\underline{T})}^s$$

such that

$$P_i(\underline{T}, \underline{x}(\underline{T})) = 0 \quad \forall i = 1, \dots, l.$$

For every $\underline{t}$ outside of a proper Zariski-closed set C of values, we can extend the morphism of specialization sp_t to the x_i's (e.g. [Dèb09, Lemma 1.7.3]). Then, denoting $\underline{x}(\underline{t}) = (\mathrm{sp}_t(x_1(\underline{T})), \dots, \mathrm{sp}_t(x_s(\underline{T}))) \in \overline{K}^s$, we have that

$$P_i(\underline{t}, \underline{x}(\underline{t})) = 0 \quad \forall i = 1, \dots, l \tag{1.2.1}$$

which implies that $1 \notin \mathfrak{p}_t$, so $\mathfrak{p}_t \neq K[\underline{Y}]$.

The above diagram of ring morphisms induces a diagram of scheme morphisms on the spectra of the rings

$$\begin{array}{ccc} \operatorname{Spec}\left(K[\underline{T},\underline{Y}]/\mathfrak{p}_T\right) & \xleftarrow{\mathrm{sp}_t^*} & \operatorname{Spec}\left(K[\underline{Y}]/\mathfrak{p}_t\right) \\ \downarrow{\scriptstyle i_T^*} & & \downarrow{\scriptstyle i_t^*} \\ \operatorname{Spec} K[\underline{T}] & \xleftarrow{\mathrm{sp}_t^*} & \operatorname{Spec} K \end{array}$$

We look at the map i_T^*.

- As $K[\underline{T}]$ is a Noetherian domain, $\operatorname{Spec} K[\underline{T}]$ is a Noetherian and integral scheme;
- As $K[\underline{T},\underline{Y}]/\mathfrak{p}_T$ is an algebra of finite type over $K[\underline{T}]$, i_T^* is a morphism of finite type;
- Let $\mathcal{F}$ be the structural sheaf of $\operatorname{Spec} K[\underline{T}]$. Then $\mathcal{F}$ is coherent on itself.

Then we can apply Generic Flatness (Theorem 1.2.5): there exists $c(\underline{T}) \in K[\underline{T}]$ such that the following restriction of i_T^*

$$i_T^* : \operatorname{Spec}\left(K[\underline{T},\underline{Y}]/\mathfrak{p}_T\left[c(\underline{T})^{-1}\right]\right) \to \operatorname{Spec}\left(K[\underline{T}]\left[c(\underline{T})^{-1}\right]\right)$$

is flat. This implies, by [Har77, Proposition 9.5, Corollary 9.6], that every irreducible component of $\operatorname{Spec}\left(K[\underline{T},\underline{Y}]/\mathfrak{p}_T\left[c(\underline{T})^{-1}\right]\right)$ has dimension d.

This yields the following restriction of the initial diagram for every $t \in K^r$ such that $c(\underline{T}) \neq 0$ and $t \notin C$:

$$\begin{array}{ccc} \operatorname{Spec}\left(K[\underline{T},\underline{Y}]/\mathfrak{p}_T\left[c(\underline{T})^{-1}\right]\right) & \xleftarrow{\mathrm{sp}_t^*} & \operatorname{Spec}\left(K[\underline{Y}]/\mathfrak{p}_t\right) \\ \downarrow{\scriptstyle i_T^*} & & \downarrow{\scriptstyle i_t^*} \\ \operatorname{Spec}\left(K[\underline{T}]\left[c(\underline{T})^{-1}\right]\right) & \xleftarrow{\mathrm{sp}_t^*} & \operatorname{Spec} K \end{array}$$

As the dimension of the fiber at a point is preserved by base change, we can conclude that every irreducible component of $\operatorname{Spec} K[\underline{Y}]/\mathfrak{p}_t$ has dimension d for every value of $\underline{t} \in K^r$ such that $c(\underline{t}) \neq 0$ and $\underline{t} \notin C$, i.e. for every value of $\underline{t} \in K^r$ outside of two proper Zariski-closed sets, whose union is still a Zariski-closed set. Denote this set by C_1.

1.2.2 Second part

The second stage of the proof is to find $\underline{t}$ in $K^r \setminus C_1$ such that the specialized quotient $K[\underline{Y}]/\mathfrak{p}_t$ is integral. This part has a more algebraic approach and relies on the Noether Normalization Lemma. We are stating below a complete version of this result, which is obtained by merging the statements in [Hoc10] and [Eis95, Corollary 13.18]. It is readily checked that the two proofs can also be merged to yield the following statement.

Lemma 1.2.6 (Noether Normalization Lemma)**.** *Let A be an algebra of finite type of dimension d over a domain R. Then there exist a nonzero element $c \in R$ and elements $z_1, \dots, z_d$ in $A\left[c^{-1}\right]$, algebraically independent over $R\left[c^{-1}\right]$, such that $A\left[c^{-1}\right]$ is a module of finite type over its subring $R\left[c^{-1}\right][\underline{z}] \coloneqq R\left[c^{-1}\right][z_1, \dots, z_d]$.*
Moreover, set $F = \operatorname{Frac} R$ and $L = \operatorname{Frac} A$. If L is separable over F, then $\underline{z}$ can be chosen so to be a separating transcendence basis of the extension.

An interesting remark is that the element c satisfying Lemma 1.2.4 and Theorem 1.2.5 can also be chosen to satisfy Lemma 1.2.6. This is clear by looking at the proofs of these results.

Therefore, going back to the proof of Theorem 1.1.3, we can apply Lemma 1.2.6 to the situation $A = {}^{K[\underline{T},\underline{Y}]}\!/_{\mathfrak{p}_T}$ and $R = K[\underline{T}]$. We get that

$$K[\underline{T},\underline{Y}]\!/_{\mathfrak{p}_T}\left[c(\underline{T})^{-1}\right] = K[\underline{T}]\left[c(\underline{T})^{-1}\right][\underline{z}(\underline{T})][\underline{\theta}(\underline{T})]$$

for $c(\underline{T}) \in K[\underline{T}]$ the same as in Section 1.2.1, $\underline{z}(\underline{T}) = (z_1(\underline{T}), \dots, z_d(\underline{T}))$ a separating transcendence basis in ${}^{K[\underline{T},\underline{Y}]}\!/_{\mathfrak{p}_T}$ and $\underline{\theta}(\underline{T}) = (\theta_1(\underline{T}), \dots, \theta_m(\underline{T}))$ the elements generating $K[\underline{T},\underline{Y}]\!/_{\mathfrak{p}_T}\left[c(\underline{T})^{-1}\right]$ as a $K[\underline{T}]\left[c(\underline{T})^{-1}\right][\underline{z}(\underline{T})]$-module. Moreover, $\underline{z}(\underline{T})$ is also separating, i.e. the field $\operatorname{Frac}\left(K[\underline{T},\underline{Y}]\!/_{\mathfrak{p}_T}\left[c(\underline{T})^{-1}\right]\right)$ is algebraically separable over $K(\underline{T}, \underline{z}(\underline{T}))$.

Set $R_T \coloneqq K[\underline{T}]\left[c(\underline{T})^{-1}\right]$ and $A_T \coloneqq {}^{K[\underline{T},\underline{Y}]}\!/_{\mathfrak{p}_T}\left[c(\underline{T})^{-1}\right]$. We apply the Primitive Element Theorem as in [Mil20, Theorem 5.1]: there exists an element $\alpha(\underline{T}) \in \operatorname{Frac}(A_T)$ such that

$$\operatorname{Frac}(A_T) = K(\underline{T}, \underline{z}(\underline{T}))(\underline{\theta}(\underline{T})) = K(\underline{T}, \underline{z}(\underline{T}))(\alpha(\underline{T})). \tag{1.2.2}$$

Moreover, by [Mil20, Remark 5.2], $\alpha(\underline{T})$ can be written as a linear combination

$$\alpha(\underline{T}) = \sum_{i=1}^{m} \alpha_i(\underline{T})\theta_i(\underline{T}) \tag{1.2.3}$$

with $\alpha_i(\underline{T}) \in K[\underline{T}, \underline{z}(\underline{T})]$ and chosen to be integral over $R_T[\underline{z}(\underline{T})]$ (up to multiplying the $\alpha_i(\underline{T})$ by some element of $K[\underline{T}, \underline{z}(\underline{T})]$).

For $i = 1, \dots, m$, let $\delta_i \in R_T[\underline{z}(\underline{T})]$ such that $\delta_i\theta_i(\underline{T})$ is integral over $R_T[\underline{z}(\underline{T})]$.

Let $d(\underline{T}) \in R_T[\underline{z}(\underline{T})]$ be the product of $\delta_1 \cdots \delta_m$ with the discriminant of the $K(\underline{T}, \underline{z}(\underline{T}))$-basis

$$1, \alpha(\underline{T}), \dots, \alpha(\underline{T})^{m-1}$$

of the m-dimensional $K(\underline{T}, \underline{z}(\underline{T}))$-vector space $K(\underline{T}, \underline{z}(\underline{T}))(\alpha(\underline{T}))$.

As $R_T[\underline{z}(\underline{T})]$ is integrally closed, it is classical (e.g. [Dèb09, Theorème 1.3.15(a)]) that

$$d(\underline{T})\theta_i(\underline{T}) \in R_T[\underline{z}(\underline{T})][\alpha(\underline{T})] \quad \forall i = 1, \dots, m. \tag{1.2.4}$$

Moreover, our choice of $\alpha(\underline{T})$ implies that its minimal polynomial $p(\underline{T}, \underline{z}(\underline{T}), Y)$ over $K(\underline{T}, \underline{z}(\underline{T}))$ is in $R_T[\underline{z}(\underline{T}), Y]$.

The field $K(\underline{T}, \underline{z}(\underline{T}), Y)$ is isomorphic to the field $K(\underline{T}, \underline{W}, Y)$ where $\underline{W}$ is a new set of variables independent of $\underline{T}$. Consider the polynomial $p(\underline{T}, \underline{W}, Y)$ image of $p(\underline{T}, \underline{z}(\underline{T}), Y)$ via this isomorphism and let

$$H = \{\underline{t} \in K^r |\ p(t, \underline{W}, Y) \text{ is irreducible in } K[\underline{W}, Y]\}$$

be the Hilbert set of p.

For every $\underline{t} \in H \subseteq K^r$, the polynomial $p(\underline{t}, \underline{W}, Y)$ is irreducible in $K[\underline{W}, Y]$.

It is important to remark that, for every $\underline{t} \in K^r \setminus (C_1 \cup C_2)$, where C_2 is the closed set defined by $c(\underline{t}) = 0$, a specialization morphism can be defined that maps A_T to $A_t\left[c(\underline{t})^{-1}\right]$ where $A_t = {}^{K[\underline{Y}]}\!/_{\mathfrak{p}_t}\left[c(\underline{t})^{-1}\right]$. We denote the images of $\underline{z}(\underline{T})$ and $\underline{\theta}(\underline{T})$ via this morphism by $\underline{z}(\underline{t})$ and $\underline{\theta}(\underline{t})$ respectively.

Furthermore, after specialization in $\underline{T} = \underline{t} \in K^s \setminus (C_1 \cup C_2)$, the elements $\underline{z}_i(\underline{t})$ are still algebraically independent as Section 1.2.1 implies that the transcendence degree is preserved through specialization at $\underline{t}$, i.e.

$$d = \operatorname{trdeg}_{K(\underline{T})} \operatorname{Frac}(A_T) = \operatorname{trdeg}_K \operatorname{Frac}(A_t) = \operatorname{trdeg}_K K(z_1(\underline{t}), \ldots, z_d(\underline{t}))$$

Therefore, for $\underline{t}$ outside of $(C_1 \cup C_2)$, $K[\underline{z}(\underline{t})]$ is still a polynomial ring of dimension d, hence isomorphic to $K[\underline{W}]$. As a result, denoting by $\alpha(\underline{t})$ the specialization of $\alpha(\underline{T})$ given by (1.2.3), the polynomial $p(\underline{t}, \underline{z}(\underline{t}), Y) \in K[\underline{z}(\underline{t}), Y]$ must also be irreducible for $\underline{t} \in H \setminus (C_1 \cup C_2)$ so

$$K(\underline{z}(\underline{t}))[\alpha(\underline{t})] \cong {}^{K(\underline{z}(\underline{t}))[Y]}\!/_{\langle p(\underline{t}, \underline{z}(\underline{t}), Y)\rangle}$$

is a field.

Specializing $\underline{T}$ in $\underline{t} \in K^r$ outside of the Zariski-closed set C_3 defined by $d(\underline{t}) = 0$, conclusion (1.2.4) implies that $\theta_i(\underline{t}) \in K(\underline{z}(\underline{t}))[\alpha(\underline{t})]$ for every i.

Finally, for $\underline{t} \in H \setminus (C_1 \cup C_2 \cup C_3)$, which is a Hilbert set, $\theta_i(\underline{t}) \in K(\underline{z}(\underline{t}))[\alpha(\underline{t})]$ for $i = 1, \ldots, m$ so $K[\underline{z}(\underline{t})][\underline{\theta}(\underline{t})]$ is a subring of $K(\underline{z}(\underline{t}))[\alpha(\underline{t})]$, which is a field, so

$$K[\underline{z}(\underline{t})][\underline{\theta}(\underline{t})] \cong {}^{K[\underline{Y}]}\!/_{\mathfrak{p}_t}$$

must be integral. This proves statement (i) of Theorem 1.2.1.

1.3 Theorems 1.1.3 and 1.1.4

Before discussing the other two main results, we want to focus on an important tool for their proofs: *quasi-generic* polynomials.

1.3.1 Quasi-generic polynomials

In the Introduction, we have briefly talked about generic polynomials. In fact, we want to define a larger class of polynomials, the *quasi-generic polynomials*, of which the generic polynomial is the principal example.

Definition 1.3.1. *Let K be a field, $K[\underline{Y}]$ the ring of polynomials with coefficients in K and variables $\underline{Y}$. Given an integer $D \geq 0$, a set*

$$S = \{Q_1(\underline{Y}), \dots, Q_{|S|}(\underline{Y})\} \subseteq \{Y_1^{\beta_1} \cdots Y_s^{\beta_s}, \beta_i \geq 0 \text{ and } \sum_{i=1}^{s} \beta_i \leq D\}$$

of power products of degree at most D, which always contains $Q_1(\underline{Y}) = 1$, and a polynomial $R(\underline{Y}) \in K[\underline{Y}]$, we define the quasi-generic polynomial of base S, R:

$$\mathcal{Q}_{S,R}(\underline{\Lambda}, \underline{Y}) = \sum_{i=1}^{|S|} \Lambda_i Q_i(\underline{Y}) + R(\underline{Y})$$

where $\underline{\Lambda} = (\Lambda_1, \dots, \Lambda_{|S|})$ is a new set of variables called the set of parameters.

We note that, by taking all the power products for $i = 1, \dots, |S|$ and $R(\underline{Y}) = 0$, we obtain the generic polynomial of degree D.

The importance of such polynomials is shown in the following lemma.

Lemma 1.3.2. *Let K be a field. Let $\mathfrak{p}$ be a prime ideal in $K[\underline{Y}]$ of height $\operatorname{ht}\mathfrak{p}$ and $\mathcal{Q}_{S,R}(\underline{\Lambda}, \underline{Y})$ a quasi-generic polynomial. Assume that S, $\mathfrak{p}$ and $R(\underline{Y})$ satisfy hypothesis* (H) *stated below. Denote by $\mathfrak{P}$ the ideal $\langle \mathfrak{p}, \mathcal{Q}_{S,R} \rangle \subseteq K[\underline{\Lambda}, \underline{Y}]$ and by $\tilde{\mathfrak{P}}$ the ideal $\langle \mathfrak{p}, \mathcal{Q}_{S,R} \rangle \subseteq K(\underline{\Lambda})[\underline{Y}]$. Then $\tilde{\mathfrak{P}}$ is a prime ideal of height $\operatorname{ht}\tilde{\mathfrak{P}} = \operatorname{ht}\mathfrak{p} + 1$.*

To state hypothesis (H), consider the set E of elements in $B := K[\underline{Y}]/\mathfrak{p}$ which are algebraic over K. Clearly E is a field containing K. Let then

$$\varphi_{S,R} : K^{|S|-1} \to B/E$$

be the map sending an $(|S|-1)$-uple $(a_2, \dots, a_{|S|})$ to the coset modulo E of the element $\sum_{i=2}^{|S|} a_i Q_i(\underline{Y}) + R(\underline{Y})$.

Definition 1.3.3. *The triple $(\mathfrak{p}, S, R(\underline{Y}))$ satisfies hypothesis* (H) *if*

(H) $\varphi_{S,R}$ *is not identically zero.*

Lemma 1.3.4. (i) *If the triple $(\mathfrak{p}, S, R(\underline{Y}))$ satisfies hypothesis* (H)*, then $\mathfrak{p}$ is a non-maximal ideal of $K[\underline{Y}]$.*

(ii) *If $\mathfrak{p}$ is a non-maximal of $K[\underline{Y}]$ and $\{Y_1, \dots, Y_s\} \subset S \cup \{R(\underline{Y})\}$, then the triple $(\mathfrak{p}, S, R(\underline{Y}))$ satisfies hypothesis* (H).

Proof. (i) By contradiction, assume that $\mathfrak{p}$ is maximal. Then B is a K-algebra of finite type and a field, so by [AM69, Corollary 5.24] B is an algebraic extension of K, hence $B = E$ and $\varphi_{S,R}$ is identically zero.

(ii) By contradiction, assume that $\varphi_{S,R}$ is identically zero. Then, $\varphi_{S,R}(0,\dots,0) = 0$ and $\varphi_{S,R}(e_i) = 0$ for every i, where $\{e_i,\ i = 1,\dots,|S|-1\}$ is the canonical base of $K^{|S|-1}$ as a K-vector space. Then $Y_i \in E$ for every i, but $\{Y_i,\ i = 1,\dots,s\}$ generates B over K, hence $B = E$, i.e. B is a field, which is a contradiction with $\mathfrak{p}$ being non-maximal. □

Proof of Lemma 1.3.2. **First step.** We show that $\mathfrak{P}$ is a prime ideal of $K[\underline{\Lambda}, \underline{Y}]$.

Using a similar strategy as in [BDN20, Lemma 2.1(a)], consider the ring automorphism

$$f : K[\underline{\Lambda}, \underline{Y}] \to K[\underline{\Lambda}, \underline{Y}] \tag{1.3.5}$$

which is the identity on $K[\Lambda_2,\dots,\Lambda_{|S|},\underline{Y}]$ and sends Λ_1 to $\Lambda_1 - \sum_{i=2}^{|S|} \Lambda_i Q_i(\underline{Y}) - R(\underline{Y})$. The ideal $\langle \mathfrak{p}, \mathcal{Q}_{S,R}\rangle$ is then sent to the ideal $\langle \mathfrak{p}, \Lambda_1\rangle$.

Now consider the specialization morphism, $f_0 : K[\underline{\Lambda}, \underline{Y}] \to K[\Lambda_2,\dots,\Lambda_{|S|},\underline{Y}]$ sending Λ_1 to 0. The ideal $\langle \mathfrak{p}\rangle$ in $K[\Lambda_2,\dots,\Lambda_{|S|},\underline{Y}]$ is prime as the following isomorphism shows

$$K[\Lambda_2,\dots,\Lambda_{|S|},\underline{Y}]\big/_{\langle \mathfrak{p}\rangle} \cong \left(K[\underline{Y}]\big/_{\mathfrak{p}}\right)[\Lambda_2,\dots,\Lambda_{|S|}]. \tag{1.3.6}$$

So its preimage under f_0, i.e. the ideal $\mathfrak{p} + \ker f_0 = \langle \mathfrak{p}, \Lambda_1\rangle$ is also prime.

As a result, the ideal $\mathfrak{P} = \langle \mathfrak{p}, \mathcal{Q}_{S,R}\rangle$ is prime in $K[\underline{\Lambda}, \underline{Y}]$, being sent to a prime ideal by f.

Second step. We show that $\mathcal{Q}_{S,R}$ is not invertible in the ring $B_\Lambda \coloneqq K(\underline{\Lambda})[\underline{Y}]\big/_{\tilde{\mathfrak{p}}_\Lambda}$, where $\tilde{\mathfrak{p}}_\Lambda$ is the extension of $\mathfrak{p}$ to $K(\underline{\Lambda})[\underline{Y}]$.

We note that the quotient B_Λ is integral and non-trivial. Indeed, the ideal $\tilde{\mathfrak{p}}_\Lambda$ is prime in $K(\underline{\Lambda})[\underline{Y}]$: the ideal $\mathfrak{p}_\Lambda = \langle \mathfrak{p}\rangle \subset K[\underline{\Lambda}, \underline{Y}]$ is prime (proceed similarly as in (1.3.6)) and $\mathfrak{p}_\Lambda \cap K[\underline{\Lambda}] = \{0\}$ because, otherwise, if there was some nonzero $P(\underline{\Lambda})$ in $\mathfrak{p}_\Lambda$, then for every $\underline{\lambda} \in K^{|S|}$ such that $P(\underline{\lambda}) \neq 0$, $P(\underline{\lambda}) \in \mathfrak{p}$, which is a contradiction because $\mathfrak{p} \neq K[\underline{Y}]$.

Now, by contradiction, assume that $\mathcal{Q}_{S,R}$ is invertible in B_Λ.

Then, there exists $\alpha \in B_\Lambda$ such that $\alpha\,\mathcal{Q}_{S,R} = 1$. As $B_\Lambda = S^{-1}B[\underline{\Lambda}]$ with $S = K[\underline{\Lambda}]$, we can write $\alpha = \frac{N(\underline{\Lambda})}{P(\underline{\Lambda})}$ for $N \in B[\underline{\Lambda}]$ and $P \in K[\underline{\Lambda}]$, $P \neq 0$.

As, by hypothesis (H), $\varphi_{S,R}$ is not identically 0, the linear subvariety $V = \varphi_{S,R}^{-1}(0)$ is of dimension strictly smaller that $|S| - 1$.

Define the set

$$Z \coloneqq \{\underline{a} = (a_2,\dots,a_r) \in K^{|S|-1} : P(\Lambda_1, a_2,\dots,a_{|S|}) = 0\}.$$

If we write $P(\underline{\Lambda}) = \sum_{i=1}^{k} p_i(\Lambda_2,\dots,\Lambda_{|S|})\Lambda_1^i$, then we see that $Z = \bigcap_{i=0}^{k} V(p_i)$, where $V(p_i)$ is the zero locus of p_i in $K^{|S|-1}$. We distinguish two cases.

First case. Assume that K is infinite.

The polynomial $P(\underline{\Lambda})$ is nonzero, so, in particular, there exists i such that $p_i \neq 0$. As $Z \subseteq V(p_i)$, then $Z \cup V \subset V(p_i) \cup V$. The set $V(p_i) \cup V$ is a proper closed set because it is the union of two proper closed sets. Thus, if K is infinite, $V(p_i) \cup V \neq K^{|S|-1}$, hence $V \cup Z \neq K^{|S|-1}$.

Take then $\underline{a} \in K^{|S|-1} \setminus (V \cup Z)$. Recall that $N(\underline{\Lambda})\mathcal{Q}_{S,R}(\underline{\Lambda}, \underline{Y}) = P(\underline{\Lambda})$. So, as $\mathcal{Q}_{S,R}(\underline{\Lambda}, \underline{Y})$ divides $P(\underline{\Lambda})$ in $B[\underline{\Lambda}]$, it follows that $m(\Lambda_1) \coloneqq \mathcal{Q}_{S,R}(\Lambda_1, \underline{a}, \underline{Y})$ divides $p(\Lambda_1) \coloneqq P(\Lambda_1, \underline{a})$ in $B[\Lambda_1]$.

By construction of $\underline{a}$, we have $p(\Lambda_1) \neq 0$ and $m(\Lambda_1) = \Lambda_1 + Q(\underline{Y})$ with $Q(\underline{Y}) = \sum_{i=2}^{|S|} a_i Q_i(\underline{Y}) + R(\underline{Y})$. Then $\Lambda_1 = -Q(\underline{Y})$ is a root of $p(\Lambda_1) = 0$ which, by construction, has coefficients in K so its roots are algebraic over K. But $Q(\underline{Y})$ is transcendental over K: the coset modulo E of $Q(\underline{Y})$ is $\varphi_{S,R}(\underline{a}) \neq 0$ because $\underline{a} \notin V$, so $Q(\underline{Y}) \notin E$. This is a contradiction.

Second case. Assume that K is finite. Let K' be an algebraic closure of K. By [AM69, Theorem 5.10], there exists a prime ideal $\mathfrak{p}'$ in $K'[\underline{Y}]$ such that $\mathfrak{p}' \cap K[\underline{Y}] = \mathfrak{p}$. Moreover, by the Going-up Theorem [AM69, Theorem 5.11] and the incomparability property [AM69, Corollary 5.9] we have $\operatorname{ht} \mathfrak{p}' = \operatorname{ht} \mathfrak{p}$.

Replacing K and $\mathfrak{p}$ by K' and $\mathfrak{p}'$ we can get back to the first case. Indeed, define $B' \coloneqq {}^{K'[\underline{Y}]}\!/_{\mathfrak{p}'}$ and $B'_\Lambda \coloneqq K(\underline{\Lambda}) \otimes_{K[\underline{\Lambda}]} B'[\underline{\Lambda}]$ and apply the first case to the image of $\mathcal{Q}_{S,R}$ under the induced homomorphism $B_\Lambda \to B'_\Lambda$. The image of the polynomial $\mathcal{Q}_{S,R}$ is then not invertible in B'_Λ, which implies that $\mathcal{Q}_{S,R}$ is not invertible in B_Λ, for otherwise the previous homomorphism yields an invertible element in B'_Λ.

Third step. The fact that $\mathcal{Q}_{S,R}$ is not invertible in the ring B_Λ implies that $\mathfrak{P} \cap K[\underline{\Lambda}] = \{0\}$. If this was not the case, we would have $\tilde{\mathfrak{P}} = K(\underline{\Lambda})[\underline{Y}]$. But, then, we could find $A(\underline{\Lambda}, \underline{Y}), B(\underline{\Lambda}, \underline{Y}) \in K(\underline{\Lambda})[\underline{Y}]$ and $P(\underline{Y}) \in \mathfrak{p}$ such that

$$A(\underline{\Lambda}, \underline{Y})P(\underline{Y}) + B(\underline{\Lambda}, \underline{Y})\mathcal{Q}_{S,R}(\underline{\Lambda}, \underline{Y}) = 1.$$

Reducing this equality modulo $\tilde{\mathfrak{p}}_\Lambda$, we would obtain that $\mathcal{Q}_{S,R}$ is invertible in B_Λ, which is a contradiction.

Saying that that $\mathfrak{P} \cap K[\underline{\Lambda}] = \{0\}$ is also equivalent to saying that $\tilde{\mathfrak{P}}$ is a prime ideal of $K(\underline{\Lambda})[\underline{Y}]$, by bijective correspondence [AM69, Proposition 3.11(iv)].

Fourth step. The polynomial $\mathcal{Q}_{S,R}$ is not contained in $\tilde{\mathfrak{p}}_\Lambda$, i.e. $\tilde{\mathfrak{p}}_\Lambda \subsetneq \tilde{\mathfrak{P}}$. Otherwise, we could write the following relation

$$\mathcal{Q}_{S,R}(\underline{\Lambda}, \underline{Y}) = \sum_{i=1}^{n} A_i(\underline{\Lambda}, \underline{Y})P_i(\underline{Y})$$

for $A_i \in K(\underline{\Lambda})[\underline{Y}]$ and $P_i(\underline{Y}) \in \mathfrak{p}$. Specializing this equality in $\underline{\lambda} = \underline{0}$ and $\underline{\lambda} = (1, 0, \ldots, 0)$, we would find that R and $1 + R$, respectively, belong to $\mathfrak{p}$, so $1 \in \mathfrak{p}$, which is a contradiction.

Fifth step. It follows from $\tilde{\mathfrak{P}}$ being a prime ideal and $\tilde{\mathfrak{p}}_\Lambda \not\subseteq \tilde{\mathfrak{P}}$ that the quotient $\tilde{\mathfrak{P}}/\tilde{\mathfrak{p}}_\Lambda$ is a nonzero prime ideal of B_Λ.

The ring B_Λ is integral and Noetherian by construction and the element $\mathcal{Q}_{S,R} \mod \tilde{\mathfrak{p}}_\Lambda$ is nonzero and is not invertible in B_Λ. By Krull's Height Theorem [Har77, Theorem 1.11A], the ideal $\tilde{\mathfrak{P}}/\tilde{\mathfrak{p}}_\Lambda \subset B_\Lambda$ has height 1, so the ideal $\tilde{\mathfrak{P}}$ has height $\operatorname{ht}\tilde{\mathfrak{p}}_\Lambda + 1 = \operatorname{ht}\mathfrak{p} + 1$ in $K(\underline{\Lambda})[\underline{Y}]$. □

Now, consider the ideal $\mathfrak{P} = \langle \mathfrak{p}, \mathcal{Q}_{S,R} \rangle \subset K[\underline{\Lambda}, \underline{Y}]$. If we assume that K has characteristic 0, we have just showed that $\mathfrak{P}$ satisfies all the hypotheses of Theorem 1.2.1. Its conclusion already proves Theorem 1.1.3 as it is stated in the Introduction. As promised we will establish a more general version using several quasi-generic polynomials.

In the following sections we present two recursive generalizations of Lemma 1.3.2 and see how they imply Theorem 1.1.3 (generalized) and Theorem 1.1.4.

1.3.2 Intersection of varieties

Fix $\rho > 0$. For $i = 1, \ldots, \rho$, fix a non-negative integer D_i and then consider the quasi-generic polynomial $\mathcal{Q}_{S_i,R_i}(\underline{\Lambda}_i, \underline{Y})$ of basis the set S_i of all the power products in the variables $\underline{Y}$ of degree $\leq D_i$ and $R_i = 0$; the additional variables $\underline{\Lambda}_i$ form the "set of parameters" of Definition 1.3.1. In fact, given this choice of S_i and R_i, the polynomial $\mathcal{Q}_{S_i,R_i}(\underline{\Lambda}_i, \underline{Y})$ is the generic polynomial of degree D_i, so, in this section, we will denote it by $\mathcal{Q}_{D_i}(\underline{\Lambda}_i, \underline{Y})$.

Set $K[\underline{\underline{\Lambda}}, \underline{Y}] = K[\underline{\Lambda}_1, \ldots, \underline{\Lambda}_\rho, \underline{Y}]$ where $\underline{\underline{\Lambda}} = (\underline{\Lambda}_1, \ldots, \underline{\Lambda}_\rho)$.

The following statement generalizes Lemma 1.3.2 for this set of data.

Theorem 1.3.5. *Let K be a field. Let $\mathfrak{p}$ be a non-maximal prime ideal of $K[\underline{Y}]$ such that $\dim_K \left(K[\underline{Y}]/\mathfrak{p}\right) = d > 0$. Let $\mathcal{Q}_{D_i}(\underline{\Lambda}_1, \underline{Y}), \ldots, \mathcal{Q}_{D_\rho}(\underline{\Lambda}_\rho, \underline{Y})$ be the generic polynomials defined above for $0 < \rho \leq d$. Then the ideal $\mathfrak{P}_\rho = \langle \mathfrak{p}, \mathcal{Q}_{D_1}, \ldots, \mathcal{Q}_{D_\rho} \rangle$ is a prime ideal of $K[\underline{\underline{\Lambda}}, \underline{Y}]$ such that $\mathfrak{P}_\rho \cap K[\underline{\underline{\Lambda}}] = \{0\}$ and*

$$\dim_{K(\underline{\underline{\Lambda}})} \left(K(\underline{\underline{\Lambda}})[\underline{Y}] / \tilde{\mathfrak{P}}_\rho \right) = d - \rho,$$

where $\tilde{\mathfrak{P}}_\rho$ is the extension of $\mathfrak{P}_\rho$ to $K(\underline{\underline{\Lambda}})[\underline{Y}]$.

Proof. We proceed by recursion on ρ.

The case $\boldsymbol{\rho = 1}$ is exactly Lemma 1.3.2 where $\mathfrak{P}_1$ is the ideal $\mathfrak{P}$ in the statement of the lemma and, consequently, $\tilde{\mathfrak{P}}_1$ is the ideal $\tilde{\mathfrak{P}}$. As previously remarked, the fact that $\operatorname{ht}\tilde{\mathfrak{P}}_1 = \operatorname{ht}\mathfrak{p} + 1$ is equivalent to saying that

$$\dim_{K(\underline{\underline{\Lambda}})} \left(K(\underline{\underline{\Lambda}})[\underline{Y}] / \tilde{\mathfrak{P}}_1 \right) = \dim_K \left(K[\underline{Y}]/\mathfrak{p} \right) - 1 = d - 1.$$

For simplicity in the notation, we only explain the case $\boldsymbol{\rho = 2}$. It will then be clear how to prove the case for an arbitrary $\rho \leq d$.

Let $\mathfrak{P}_1 = \langle \mathfrak{p}, \mathcal{Q}_{D_1} \rangle \subset K[\underline{\Lambda}_1, \underline{Y}]$ be the ideal obtained as in the case $\rho = 1$. As $\dim K[\underline{\Lambda}_1, \underline{Y}] > \dim K[\underline{Y}]$ and $\operatorname{ht} \mathfrak{P}_1 = \operatorname{ht} \mathfrak{p} + 1$, the ideal $\mathfrak{P}_1$ is not maximal. Moreover, by Lemma 1.3.4(ii), the triple $(\mathfrak{P}_1, S_2, 0)$ satisfies hypothesis (H) because $\mathcal{Q}_{D_2}$ is the generic polynomial of degree D_2. Therefore, we can apply Lemma 1.3.2 to $\mathfrak{P}_1$ and $\mathcal{Q}_{D_2}$ and obtain that $\mathfrak{P}_2 = \langle \mathfrak{p}, \mathcal{Q}_{D_1}, \mathcal{Q}_{D_2} \rangle$ is prime in $K[\underline{\Lambda}_1, \underline{\Lambda}_2, \underline{Y}]$ and has height $\operatorname{ht} \mathfrak{P}_2 = \operatorname{ht} \mathfrak{p} + 2$, i.e.

$$\dim_{K(\underline{\underline{\Lambda}})} \left(K(\underline{\underline{\Lambda}})[\underline{Y}] \big/ \tilde{\mathfrak{P}}_2 \right) = \dim_K \left(K[\underline{Y}] \big/ \mathfrak{p} \right) - 2 = d - 2.$$

□

Denote by $V_{\rho,\underline{\underline{\Lambda}}}$ the variety defined by $\mathcal{Q}_{D_1}(\underline{\Lambda}_1, \underline{Y}), \ldots, \mathcal{Q}_{D_\rho}(\underline{\Lambda}_\rho, \underline{Y})$. If $0 < \rho \leq s$, as it is the case if $0 < \rho \leq d$ as above, a recursive application of Lemma 1.3.2, starting with $\mathfrak{p} = \langle \mathcal{Q}_{D_1}(\underline{\Lambda}_1, \underline{Y}) \rangle$, easily shows that $V_{\rho,\underline{\underline{\Lambda}}}$ is, in fact, an irreducible $K(\underline{\underline{\Lambda}})$-variety of codimension ρ, i.e. $\langle \mathcal{Q}_{D_1}(\underline{\Lambda}_1, \underline{Y}), \ldots, \mathcal{Q}_{D_\rho}(\underline{\Lambda}_\rho, \underline{Y}) \rangle$ is a prime ideal of height ρ in $K[\underline{\underline{\Lambda}}, \underline{Y}]$. We call $V_{\rho,\underline{\underline{\Lambda}}}$ the *generic $K(\underline{\underline{\Lambda}})$-subvariety of codimension ρ.*

Using this remark, a general version of Theorem 1.1.3 follows from conjoining Theorem 1.3.5 and Theorem 1.2.1.

Corollary 1.3.6. *Let K be a field of characteristic 0. Let $V = V_K(\mathfrak{p})$ be an irreducible K-variety such that $\dim_K \left(K[\underline{Y}] \big/ \mathfrak{p} \right) = d > 0$. Let $V_{\rho,\underline{\underline{\Lambda}}}$ be the generic $K(\underline{\underline{\Lambda}})$-subvariety defined above. Then for $\underline{\underline{\lambda}} = (\underline{\lambda}_1, \ldots, \underline{\lambda}_\rho)$ in some Hilbert subset of $K^{N_{D_1} + \ldots + N_{D_\rho}}$, the intersection $V \cap V_{\rho,\underline{\underline{\lambda}}}$ of V with the K-variety $V_{\rho,\underline{\underline{\lambda}}}$, obtained by specializing $\underline{\underline{\Lambda}}$ at $\underline{\underline{\lambda}}$, is an irreducible K-variety of dimension $d - \rho$.*

Theorem 1.1.3 is the special case for which $\rho = 1$ and $\mathcal{Q}_{S,R}(\underline{\Lambda}, \underline{Y})$ is the generic polynomial of degree D.

Proof. By Theorem 1.3.5, the ideal $\mathfrak{P}_\rho = \langle \mathfrak{p}, \mathcal{Q}_{D_1}, \ldots, \mathcal{Q}_{D_\rho} \rangle$ is prime in $K[\underline{\underline{\Lambda}}, \underline{Y}]$ and $\mathfrak{P}_\rho \cap K[\underline{\underline{\Lambda}}] = \{0\}$. Moreover, as K has characteristic 0, $\operatorname{Frac}\left(K[\underline{\underline{\Lambda}}, \underline{Y}] \big/ \mathfrak{P}_{\underline{S}} \right)$ is separable over $K(\underline{\underline{\Lambda}}, \underline{Y})$. Then we can apply Theorem 1.2.1 to $\mathfrak{P}_\rho$: using statement (iii) of the theorem, for $\underline{\underline{\lambda}} = (\underline{\lambda}_1, \ldots, \underline{\lambda}_\rho)$ in a Hilbert subset of $K^{N_{D_1} + \ldots + N_{D_\rho}}$, the K-variety

$$V_K(\mathfrak{p}, \mathcal{Q}_{D_1}(\underline{\lambda}_1, \underline{Y}), \ldots, \mathcal{Q}_{D_\rho}(\underline{\lambda}_\rho, \underline{Y})) = V \cap V_{\rho,\underline{\underline{\lambda}}}$$

is an irreducible K-variety of dimension $d - \rho$. □

Remark 1.3.7. At the beginning of the section, we chose to take as $\mathcal{Q}_{S_i,R_i}(\underline{\Lambda}_i, \underline{Y})$ the generic polynomial of degree D_i. However, if we fix the ideal $\mathfrak{p}$ at the beginning, Corollary 1.3.6 holds more generally if we take for S_i a subset of all possible monomials such that the triple $(\mathfrak{p}, S_i, 0)$ satisfies hypothesis (H) and Theorem 1.3.5.

1.3.3 Specialization at polynomials

In the previous sections the base ring used to define the quasi-generic polynomials was $K[\underline{Y}]$, while in this section it will be $K[\underline{T},\underline{Y}]$.

Fix $\rho > 0$. For $i = 1,\dots,\rho$, fix a non-negative integer D_i and then consider the quasi-generic polynomial $\mathcal{Q}_{S_i,R_i}(\underline{\Lambda}_i,\underline{Y})$ of basis the set S_i of all the power products in the variables $\underline{Y}$ of degree $\leq D_i$ and $R_i = -T_i$; the additional variables $\underline{\Lambda}_i$ form the "set of parameters" of Definition 1.3.1. Thus, we have

$$\mathcal{Q}_{S_i,R_i}(\underline{\Lambda}_i,\underline{T},\underline{Y}) = \sum_{j=1}^{N_{D_i}} \Lambda_{i,j}\, Q_j(\underline{Y}) - T_i = \mathcal{U}_{D_i}(\underline{\Lambda}_i,\underline{Y}) - T_i.$$

Note that $\mathcal{U}_{D_i}(\underline{\Lambda}_i,\underline{Y})$, as defined above, is the generic polynomial of degree D_i in the variables $\underline{Y}$.

According to the definition of quasi-generic polynomial, the power products could be taken in the variables $\underline{T}$ and $\underline{Y}$, but we take them only in the variables $\underline{Y}$ for our purpose.

The following statement generalizes Lemma 1.3.2 for this set of data.

Theorem 1.3.8. *Let K be a field. Let $\mathfrak{p}$ be a prime ideal of $K[\underline{T},\underline{Y}]$ such that $\mathfrak{p}\cap K[\underline{T}] = \{0\}$ and $\dim_{K(\underline{T})}\left(K(\underline{T})[\underline{Y}]/\tilde{\mathfrak{p}}\right) = d > 0$, where $\tilde{\mathfrak{p}}$ is the extension of $\mathfrak{p}$ to $K(\underline{T})[\underline{Y}]$. Let $\mathcal{Q}_{S_1,R_1}(\underline{\Lambda}_1,\underline{T},\underline{Y}),\dots,\mathcal{Q}_{S_\rho,R_\rho}(\underline{\Lambda}_\rho,\underline{T},\underline{Y})$ be the quasi-generic polynomials defined above for $0 < \rho \leq r$. Then the ideal $\mathfrak{P}_{\underline{S}} = \langle \mathfrak{p}, \mathcal{Q}_{S_1,R_1},\dots,\mathcal{Q}_{S_\rho,R_\rho}\rangle$ is a prime ideal of $K[\underline{\underline{\Lambda}},\underline{T},\underline{Y}]$ such that $\mathfrak{P}_{\underline{S}}\cap K[\underline{\underline{\Lambda}}] = \{0\}$ and*

$$\dim_{K(\underline{\underline{\Lambda}})}\left(K(\underline{\underline{\Lambda}})[\underline{T},\underline{Y}]/\tilde{\mathfrak{P}}_{\underline{S}}\right) = d + r - \rho$$

where $\tilde{\mathfrak{P}}_{\underline{S}}$ is the extension of $\mathfrak{P}_{\underline{S}}$ to $K(\underline{\underline{\Lambda}})[\underline{T},\underline{Y}]$.

Proof. We proceed by recursion on ρ.

Assume $\boldsymbol{\rho = 1}$. As $\mathfrak{p}\cap K[\underline{T}] = \{0\}$, in particular, $\mathfrak{p}\cap K[T_2,\dots,T_r] = \{0\}$, so the ideal $\tilde{\mathfrak{p}}_{T_2} = \langle\mathfrak{p}\rangle \subset K(T_2,\dots,T_r)[T_1,\underline{Y}]$ is non-maximal by Lemma 1.2.3.

By construction, the set S_1 contains all the power products in the variables $\underline{Y}$ of degree $\leq D_1$, hence Y_j, for all $j = 1,\dots,s$, and we have set $R_1(\underline{T},\underline{Y}) = -T_1$. So, by Lemma 1.3.4(ii), the triple $(\tilde{\mathfrak{p}}_{T_2}, S_1, -T_1)$ satisfies hypothesis (H) with the ring $K[\underline{Y}]$ in Lemma 1.3.4 replaced by $K(T_2,\dots,T_r)[T_1,\underline{Y}]$.

Therefore, by Lemma 1.3.2, the ideal

$$\tilde{\mathfrak{P}}_{T_2,S_1} = \langle \mathfrak{p}, \mathcal{Q}_{S_1,R_1}\rangle \subset K(\underline{\Lambda}_1,T_2,\dots,T_r)[T_1,\underline{Y}]$$

is a prime ideal and $\operatorname{ht}\tilde{\mathfrak{P}}_{T_2,S_1} = \operatorname{ht}\mathfrak{p} + 1$.

By the classical bijective correspondence between extended and contracted ideals in rings of fractions (e.g. [AM69, Proposition 3.11(iv)]), to the ideal $\tilde{\mathfrak{P}}_{T_2,S_1}$ we associate the prime ideal

$$\tilde{\mathfrak{P}}_{S_1} = \langle \mathfrak{p}, \mathcal{Q}_{S_1,R_1} \rangle \subset K(\underline{\Lambda}_1)[\underline{T}, \underline{Y}].$$

In the same manner, we associate the prime ideal

$$\mathfrak{P}_{S_1} = \langle \mathfrak{p}, \mathcal{Q}_{S_1,R_1} \rangle \subset K[\underline{\Lambda}_1, \underline{T}, \underline{Y}]$$

and, in addition, we have $\mathfrak{P}_{S_1} \cap K[\underline{\Lambda}_1] = \{0\}$.

Moreover, by Lemma 1.2.3, $\operatorname{ht} \tilde{\mathfrak{P}}_{S_1} = \operatorname{ht} \tilde{\mathfrak{P}}_{T_2,S_1} = \operatorname{ht} \mathfrak{p} + 1$, so

$$\dim_{K(\underline{\Lambda}_1)} \left(K(\underline{\Lambda}_1)[\underline{T}, \underline{Y}] \big/ \tilde{\mathfrak{P}}_{S_1} \right) = r + s - (\operatorname{ht} \mathfrak{p} + 1) = d + r - 1.$$

For simplicity in the notation, we explain only the case $\boldsymbol{\rho = 2}$. The case of an arbitrary $\rho \leq r$ can be easily deduced.

Consider the prime ideal

$$\tilde{\mathfrak{P}}_{T_3,S_1} = \langle \mathfrak{p}, \mathcal{Q}_{S_1,R_1} \rangle \subset K(\underline{\Lambda}_1, T_3, \ldots, T_r)[T_1, T_2, \underline{Y}]$$

deduced from $\mathfrak{P}_{S_1}$ by applying the classical bijective correspondence. Denote by

$$\tilde{\mathfrak{P}}_{T_1^*,T_3} \subset K(\underline{\Lambda}_1, T_3, \ldots, T_r)[T_2, \underline{Y}]$$

the ideal obtained by replacing T_1 with the generic polynomial, previously denoted by $\mathcal{U}_{D_1}(\underline{\Lambda}_1, \underline{Y})$, in $\tilde{\mathfrak{P}}_{T_3,S_1}$. For $\rho = 2$, the ideal $\tilde{\mathfrak{P}}_{T_1^*,T_3}$ will play the role played by $\tilde{\mathfrak{p}}_{T_2}$ in the case $\rho = 1$.

The ideal $\tilde{\mathfrak{P}}_{T_1^*,T_3}$ is formally constructed through the quotient morphism, which we denote by π_1, sending $\tilde{\mathfrak{P}}_{T_3,S_1}$ to

$$\tilde{\mathfrak{P}}_{T_3,S_1} \big/ \langle \mathcal{Q}_{S_1,R_1} \rangle \cong \tilde{\mathfrak{P}}_{T_1^*,T_3}.^3$$

It follows that $\tilde{\mathfrak{P}}_{T_1^*,T_3}$ is prime. Moreover, by [Eis95, Proposition 9.2], we have $\operatorname{ht} \tilde{\mathfrak{P}}_{T_1^*,T_3} = \operatorname{ht} \tilde{\mathfrak{P}}_{T_3,S_1} - 1$. Now, by Lemma 1.2.3 and the case $\rho = 1$, we have $\operatorname{ht} \tilde{\mathfrak{P}}_{T_3,S_1} = \operatorname{ht} \mathfrak{P}_{S_1} = \operatorname{ht} \mathfrak{p} + 1$. Therefore, we obtain:

$$\operatorname{ht} \tilde{\mathfrak{P}}_{T_1^*,T_3} = \operatorname{ht} \mathfrak{p}, \tag{1.3.7}$$

so $\tilde{\mathfrak{P}}_{T_1^*,T_3}$ is a non-maximal prime ideal of $K(\underline{\Lambda}_1, T_3, \ldots, T_r)[T_2, \underline{Y}]$.

Consider the polynomial $\mathcal{Q}_{S_2,R_2}(\underline{\Lambda}_2, \underline{T}, \underline{Y})$. By construction, S_2 contains Y_j for all $j = 1, \ldots, s$ and $R_2(\underline{T}, \underline{Y}) = -T_2$. By Lemma 1.3.4(ii), the triple $(\tilde{\mathfrak{P}}_{T_1^*,T_3}, S_2, -T_2)$ satisfies hypothesis (H) with the ring $K[\underline{Y}]$ in Lemma 1.3.4 replaced by $K(\underline{\Lambda}_1, T_3, \ldots, T_r)[T_2, \underline{Y}]$.

[3] Recall that $\mathcal{Q}_{S_1,R_1} = \mathcal{U}_{D_1}(\underline{\Lambda}_1, \underline{Y}) - T_1$.

From Lemma 1.3.2 applied to $\tilde{\mathfrak{P}}_{T_1^*,T_3}$ and $\mathcal{Q}_{S_2,R_2}$, we deduce that the ideal

$$\tilde{\mathfrak{P}}_{T_1^*,T_3,S_2} \coloneqq \langle \tilde{\mathfrak{P}}_{T_1^*,T_3}, \mathcal{Q}_{S_2,R_2} \rangle \subset K(\underline{\Lambda}_1, \underline{\Lambda}_2, T_3, \dots, T_r)[T_2, \underline{Y}]$$

is prime and has height $\operatorname{ht} \tilde{\mathfrak{P}}_{T_1^*,T_3,S_2} = \operatorname{ht} \mathfrak{p} + 1$.

Using the morphism π_1, we obtain that the ideal

$$\tilde{\mathfrak{P}}_{T_1^*,T_3,S_2} + \ker \pi_1 = \langle \tilde{\mathfrak{P}}_{T_3,S_1}, \mathcal{Q}_{S_2,R_2} \rangle = \langle \mathfrak{p}, \mathcal{Q}_{S_1,R_1}, \mathcal{Q}_{S_2,R_2} \rangle$$

is a prime ideal of $K(\underline{\Lambda}_1, \underline{\Lambda}_2, T_3, \dots, T_r)[T_1, T_2, \underline{Y}]$ and that its height is equal to

$$\operatorname{ht} \tilde{\mathfrak{P}}_{T_1^*,T_3,S_2} + 1 = \operatorname{ht} \mathfrak{p} + 2.$$

Applying the classical bijective correspondence, the ideal

$$\mathfrak{P}_{S_1,S_2} = \langle \mathfrak{p}, \mathcal{Q}_{S_1,R_1}, \mathcal{Q}_{S_2,R_2} \rangle \subset K[\underline{\Lambda}_1, \underline{\Lambda}_2, \underline{T}, \underline{Y}]$$

is prime and such that $\mathfrak{P}_{S_1,S_2} \cap K[\underline{\Lambda}_1, \underline{\Lambda}_2] = \{0\}$. Moreover, the ideal

$$\tilde{\mathfrak{P}}_{S_1,S_2} = \langle \mathfrak{p}, \mathcal{Q}_{S_1,R_1}, \mathcal{Q}_{S_2,R_2} \rangle \subset K(\underline{\Lambda}_1, \underline{\Lambda}_2)[\underline{T}, \underline{Y}]$$

is prime. By Lemma 1.2.3, both these ideals have height $\operatorname{ht} \mathfrak{p} + 2$.

In terms of dimensions, this is equivalent to saying that

$$\dim_{K(\underline{\Lambda}_1,\underline{\Lambda}_2)} \left(K(\underline{\Lambda}_1, \underline{\Lambda}_2)[\underline{T}, \underline{Y}] \Big/ \tilde{\mathfrak{P}}_{S_1,S_2} \right) = d + r - 2.$$

□

Fix $\rho = r$. Theorem 1.1.4 follows from Theorem 1.3.8 conjoined with Theorem 1.2.1. Differently from Theorem 1.1.1, we need to assume K of characteristic 0 to guarantee the separability required in the statement of Theorem 1.1.1.

Proof of Theorem 1.1.4. By assumption, V_T is a $K(\underline{T})$-variety so the ideal $\tilde{\mathfrak{p}} \coloneqq \langle P_1, \dots, P_l \rangle$ is a prime ideal of $K(\underline{T})[\underline{Y}]$. Equivalently, $\mathfrak{p} \coloneqq \langle P_1, \dots, P_l \rangle$ is a prime ideal of $K[\underline{T}]$ and $\mathfrak{p} \cap K[\underline{T}] = \{0\}$.

For $i = 1, \dots, r$, let $\mathcal{Q}_{S_i,R_i}$ be the quasi-generic polynomials defined at the beginning of the section, i.e.

$$\mathcal{Q}_{S_i,R_i}(\underline{\Lambda}_i, \underline{T}, \underline{Y}) = \sum_{j=1}^{N_{D_i}} \Lambda_{i,j} Q_j(\underline{Y}) - T_i = \mathcal{U}_{D_i}(\underline{\Lambda}_i, \underline{Y}) - T_i.$$

The polynomials $\mathcal{Q}_{S_i,R_i}$ and $\mathfrak{p}$ satisfy the hypotheses of Theorem 1.3.8, so the ideal $\mathfrak{P}_{\underline{S}} = \langle \mathfrak{p}, \mathcal{Q}_{S_1,R_1}, \dots, \mathcal{Q}_{S_r,R_r} \rangle$ is a prime ideal of $K[\underline{\Lambda}, \underline{T}, \underline{Y}]$ such that $\mathfrak{P}_{\underline{S}} \cap K[\underline{\Lambda}] = \{0\}$ and $\operatorname{ht} \mathfrak{P}_{\underline{S}} = \operatorname{ht} \mathfrak{p} + r$.

Denote by $\tilde{\mathfrak{P}}_{\underline{S}}$ the extension of $\mathfrak{P}_{\underline{S}}$ to $K(\underline{\underline{\Lambda}})[\underline{T},\underline{Y}]$. By the classical bijective correspondence the ideal $\tilde{\mathfrak{P}}_{\underline{S}}$ is prime.

For $i=1,\dots,r$, denote by π_i the quotient morphism by the ideal $\langle \mathcal{Q}_{S_i,R_i}\rangle$. Denote by $\tilde{\mathfrak{P}}_{\Lambda}$ the ideal of $K(\underline{\underline{\Lambda}})[\underline{Y}]$ obtained by replacing T_i with $\mathcal{U}_{D_i}$ for every i. Applying, recursively, all the morphisms π_i to the ideal $\tilde{\mathfrak{P}}_{\underline{S}}$, in the same manner as for (1.3.7), we obtain that $\tilde{\mathfrak{P}}_{\Lambda}$ is a prime ideal of $K(\underline{\underline{\Lambda}})[\underline{Y}]$ and

$$\operatorname{ht}\tilde{\mathfrak{P}}_{\Lambda}=\operatorname{ht}\mathfrak{p}.$$

By bijective correspondence, the ideal

$$\mathfrak{P}_{\Lambda}=\langle P_1(\underline{\mathcal{U}}(\underline{\underline{\Lambda}},\underline{Y}),\underline{Y}),\dots,P_l(\underline{\mathcal{U}}(\underline{\underline{\Lambda}},\underline{Y}),\underline{Y})\rangle,$$

where $\underline{\mathcal{U}}(\underline{\underline{\Lambda}},\underline{Y})=(\mathcal{U}_{D_1}(\underline{\Lambda}_1,\underline{Y}),\dots,\mathcal{U}_{D_r}(\underline{\Lambda}_r,\underline{Y}))$, is a prime ideal of $K[\underline{\underline{\Lambda}},\underline{Y}]$ such that $\mathfrak{P}_{\Lambda}\cap K[\underline{\underline{\Lambda}}]=\{0\}$ and $\operatorname{ht}\mathfrak{P}_{\Lambda}=\operatorname{ht}\mathfrak{p}$.

Finally, we can apply Theorem 1.2.1 to $\mathfrak{P}_{\Lambda}$. For $\underline{\underline{\lambda}}$ in $K^{D_1+\dots+D_r}$, consider the ideal

$$\mathfrak{P}_{\lambda}=\langle P_1(\underline{\mathcal{U}}(\underline{\underline{\lambda}},\underline{Y}),\underline{Y}),\dots,P_l(\underline{\mathcal{U}}(\underline{\underline{\lambda}},\underline{Y}),\underline{Y})\rangle=\langle P_1(\underline{U}(\underline{Y}),\underline{Y}),\dots,P_l(\underline{U}(\underline{Y}),\underline{Y})\rangle$$

where $\underline{\mathcal{U}}(\underline{\underline{\lambda}},\underline{Y})=(\mathcal{U}_1(\underline{\lambda}_1,\underline{Y}),\dots,\mathcal{U}_r(\underline{\lambda}_r,\underline{Y}))$ and $\underline{U}(\underline{Y})=(U_1(\underline{Y}),\dots,U_r(\underline{Y}))$ with $U_i(\underline{Y})=\mathcal{U}_i(\underline{\lambda}_i,\underline{Y})$. By Theorem 1.2.1, for every $\underline{\underline{\lambda}}$ in some Hilbert subset of $K^{D_1+\dots+D_r}$, the ideal $\mathfrak{P}_{\lambda}$ is prime and has height $\operatorname{ht}\mathfrak{p}$, i.e. $V_U=V_K(\mathfrak{P}_{\lambda})$ is an irreducible K-variety and

$$\dim_K V_U=\dim_K\left(K[\underline{Y}]\big/\mathfrak{P}_{\lambda}\right)=s-\operatorname{ht}\mathfrak{p}=d.$$

Recalling the isomorphism between $\mathbb{A}_K^{D_1+\dots+D_r}$ and $\prod_{i=1}^r K[\underline{\Lambda}_i]_{D_i}$ that we mentioned in the Introduction, taking a Hilbert subset of $K^{D_1+\dots+D_r}$ is equivalent to taking a Hilbert subset of $\prod_{i=1}^r K[\underline{\Lambda}_i]_{D_i}$. □

Remark 1.3.9. As we mentioned in Remark 1.1.5(b), taking $D_i=0$, for every i, implies Theorem 1.1.1 in characteristic 0. Indeed, for every $i=1,\dots,r$, take

$$\mathcal{Q}_{S_i,R_i}=\Lambda_{i,1}-T_i.$$

The map φ_{R_i,S_i} sends 0, the only point of K^0, to $-T_i$. The element $-T_i$ is clearly transcendental over K and, by hypothesis, $-T_i$ is not in $\mathfrak{p}$, so φ_{R_i,S_i} is not identically 0 for every i. Therefore, we apply Theorem 1.1.4 and Theorem 1.1.1 follows.

2 Structure galoisienne relative de la racine carrée de la codifférente d'extensions métacycliques non abéliennes

2.1 Introduction

Dans tout ce chapitre, si K est un corps de nombres, O_K désigne son anneau d'entiers et $\mathrm{Cl}(K)$ son groupe des classes. Si I est un idéal fractionnaire de K, on note $\mathrm{cl}_K(I)$ sa classe dans $\mathrm{Cl}(K)$, ou simplement $\mathrm{cl}(I)$ si aucune confusion n'est possible.

Soient k un corps de nombres et Γ un groupe fini. Soient $\mathcal{M}$ un O_k-ordre maximal dans l'algèbre semi-simple $k[\Gamma]$ contenant $O_k[\Gamma]$; parfois, pour plus de précision, on le notera $\mathcal{M}(k[\Gamma])$. Soit $\mathrm{Cl}(O_k[\Gamma])$ (resp. $\mathrm{Cl}(\mathcal{M})$) le groupe des classes des $O_k[\Gamma]$-modules (resp. $\mathcal{M}$-modules) localement libres (voir [Frö83, Chap. I]). Soit M un $O_k[\Gamma]$-module localement libre. On peut associer à M une classe, notée $[M]$, dans $\mathrm{Cl}(O_k[\Gamma])$, et par extension des scalaires la classe de $\mathcal{M} \otimes_{O_k[\Gamma]} M$, notée $[\mathcal{M} \otimes_{O_k[\Gamma]} M]$, dans $\mathrm{Cl}(\mathcal{M})$.

Soit N/k une extension galoisienne à groupe de Galois isomorphe à Γ ; parfois on dira simplement que N/k est une Γ-extension. Soit π un isomorphisme défini sur $\mathrm{Gal}(N/k)$ et à valeurs dans Γ. Pour tout $\gamma \in \Gamma$, nous noterons $\pi^{-1}(\gamma) \in \mathrm{Gal}(N/k)$ simplement par γ.

Soit $\mathcal{D}_{N/k}$ la différente de N/k. Supposons que la racine carrée de la codifférente $\mathcal{D}_{N/k}^{-1}$ existe et notons la par $\mathcal{A}_{N/k}$. Immédiatement, $\mathcal{A}_{N/k}$ est un idéal fractionnaire ambige de l'extension N/k (i.e., stable par les éléments de $\mathrm{Gal}(N/k)$; donc c'est un Γ-module).

Signalons que, par la formule de Hilbert (voir [Ser68, Proposition 4, p. 72]), lorsque N/k est modérement ramifiée, $\mathcal{A}_{N/k}$ existe si, et seulement si, les indices de ramifications dans N/k sont impairs ; c'est le cas, par exemple, lorsque Γ est d'ordre impair.

A l'aide de π, on munit $\mathcal{A}_{N/k}$ d'une structure de $O_k[\Gamma]$-module défini par : pour tout $x \in \mathcal{A}_{N/k}$ et tout $\gamma \in \Gamma$, $\gamma x = \gamma(x)$. On désigne par $\mathcal{A}_{N/k,\pi}$, ou simplement $\mathcal{A}_{N/k}$ si aucune ambiguïté n'est possible, le $O_k[\Gamma]$-module ainsi défini. Notons que le nombre de structures possibles est égal à l'ordre du groupe des automorphismes de Γ.

D'après [Ull74, Proposition 1.3], si N/k est modérément ramifiée, alors $\mathcal{A}_{N/k}$ est un $O_k[\Gamma]$ module projectif, et donc c'est un $O_k[\Gamma]$-module localement libre (par un résultat

de Swan).

On sait que si N/k est modérément ramifiée, alors O_N est un $O_k[\Gamma]$-module localement libre. Rappelons brièvement la définition de l'ensemble des classes réalisables par les anneaux d'entiers. On désigne par $\mathcal{R}(O, O_k[\Gamma])$ (resp. $\mathcal{R}(O, \mathcal{M})$) l'ensemble des classes c de $\mathrm{Cl}(O_k[\Gamma])$ (resp. $\mathrm{Cl}(\mathcal{M})$) telles qu'il existe une extension N/k modérément ramifiée, à groupe de Galois isomorphe à Γ, avec $[O_N] = c$ (resp. $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] = c$).

D'une façon similaire, on désigne par $\mathcal{R}(\mathcal{A}, O_k[\Gamma])$ (resp. $\mathcal{R}(\mathcal{A}, \mathcal{M})$) l'ensemble des classes c de $\mathrm{Cl}(O_k[\Gamma])$ (resp. $\mathrm{Cl}(\mathcal{M})$) telles qu'il existe une extension N/k modérément ramifiée, à groupe de Galois isomorphe à Γ, avec $[\mathcal{A}_{N/k}] = c$ (resp. $[\mathcal{M} \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k}] = c$). Nous dirons que $\mathcal{R}(\mathcal{A}, O_k[\Gamma])$ (resp. $\mathcal{R}(\mathcal{A}, \mathcal{M})$) est l'ensemble des classes galoisiennes réalisables par la racine carrée de la codifférente. Signalons que ces derniers sont liés par la relation : $\mathrm{Ex}(\mathcal{R}(\mathcal{A}, O_k[\Gamma])) = \mathcal{R}(\mathcal{A}, \mathcal{M})$, où $\mathrm{Ex} : \mathrm{Cl}(O_k[\Gamma]) \to \mathrm{Cl}(\mathcal{M})$ est le morphisme surjectif induit par l'extension des scalaires de $O_k[\Gamma]$ à $\mathcal{M}$.

Soit $\mathrm{Tr}_{N/k}$ la trace dans N/k. On a $\mathrm{Tr}_{N/k}(\mathcal{A}_{N/k}) = O_k$, car $O_N \subset \mathcal{A}_{N/k} \subset \mathcal{D}_{N/k}^{-1}$, $\mathrm{Tr}_{N/k}(O_N) = O_k$ (N/k est modérée) et $\mathrm{Tr}_{N/k}(\mathcal{D}_{N/k}^{-1}) \subset O_k$ (par définition de $\mathcal{D}_{N/k}^{-1}$).

Notons $\mathrm{Cl}^\circ(O_k[\Gamma])$ (resp. $\mathrm{Cl}^\circ(\mathcal{M})$) le noyau du morphisme $\mathrm{Cl}(O_k[\Gamma]) \to \mathrm{Cl}(k)$ (resp. $\mathrm{Cl}(\mathcal{M}) \to \mathrm{Cl}(k)$) induit par l'augmentation $O_k[\Gamma] \to O_k$ (resp. $\mathcal{M} \to O_k$). Il découle de $\mathrm{Tr}_{N/k}(\mathcal{A}_{N/k}) = O_k$ que $\mathcal{R}(\mathcal{A}, O_k[\Gamma]) \subset \mathrm{Cl}^\circ(O_k[\Gamma])$ et $\mathcal{R}(\mathcal{A}, \mathcal{M}) \subset \mathrm{Cl}^\circ(\mathcal{M})$.

D'une façon analogue à des conjectures sur $\mathcal{R}(O, O_k[\Gamma])$ et $\mathcal{R}(O, \mathcal{M})$ (voir par exemple [BGS06]), on conjecture :

Conjecture 1. *L'ensemble* $\mathcal{R}(\mathcal{A}, O_k[\Gamma])$ *est un sous-groupe de* $\mathrm{Cl}^\circ(O_k[\Gamma])$.

Conjecture 2. *L'ensemble* $\mathcal{R}(\mathcal{A}, \mathcal{M})$ *est un sous-groupe de* $\mathrm{Cl}^\circ(\mathcal{M})$

Dans tout ce chapitre, on suppose Γ d'ordre impair.

D'une part, le groupe Γ étant résoluble (par Feit-Thompson), d'après le (célèbre) théorème de Shafarevich (voir [NSW08, Théorème 9.6.1, p. 574, et Exercice (b), p. 597]), il existe des extensions galoisiennes N/k, modérées dont le groupe de Galois est isomorphe à Γ. D'autre part, $\mathcal{A}_{N/k}$ existe. On en déduit en particulier que $\mathcal{R}(\mathcal{A}, O_k[\Gamma])$ et $\mathcal{R}(\mathcal{A}, \mathcal{M})$ sont non vides.

Lorsque $k = \mathbb{Q}$, on a $\mathcal{R}(\mathcal{A}, O_k[\Gamma]) = \{1\}$ par [Ere91, Théorème 3] : la preuve est une adaptation de celle d'un théorème de M.J. Taylor (ancienne conjecture de Fröhlich) concernant la structure de O_N en tant que $\mathbb{Z}[\Gamma]$ module (voir [Tay81, Théorème 1]).

Pour k quelconque et Γ abélien, on a la Conjecture 1 par [Tsa16, Théorème 1.3]. La démonstraion est une adaptation d'un théorème de McCulloh sur les classes galoisiennes réalisables par les anneaux d'entiers (voir [McC87, Théorème 6.17 et Corollaire 6.20]).

Rappelons la définition de la classe de Steinitz. Soit K un corps de nombres. Soit M un O_K-module de type fini, sans torsion et de rang n. Alors, il existe un idéal I de O_K tel que $M \simeq O_K^{n-1} \oplus I$ en tant que O_K-module. La classe de I dans $\mathrm{Cl}(K)$ est appelée la classe de Steinitz de M ; on la note $\mathrm{cl}_K(M)$. Notons que si M est un idéal fractionnaire de

K, $\mathrm{cl}_K(M)$ est la classe de M dans $\mathrm{Cl}(K)$. La structure de M, en tant que O_K-module, est complètement déterminée par son rang et sa classe de Steinitz. Il est clair que M est un O_K-module libre si, et seulement, si $\mathrm{cl}_K(M) = 1$.

On définit $R_m(O, k[\Gamma])$ comme étant l'ensemble des $c \in \mathrm{Cl}(k)$ telles qu'il existe une extension galoisienne modérée à groupe de Galois isomorphe à Γ, avec $\mathrm{cl}_k(O_N) = c$. On conjecture (voir par exemple [BGS06]) que $R_m(O, k[\Gamma])$ est un sous-groupe de $\mathrm{Cl}(k)$ (avec l'ordre de Γ non nécéssairement impair).

D'une façon similaire on définit $R_m(\mathcal{A}, k[\Gamma])$, en remplaçant ci-dessus O_N par $\mathcal{A}_{N/k}$.

Proposition 2.1.1. *Soit N/k une extension galoisienne (modérée ou non) à groupe de Galois isomorphe à Γ d'ordre impair. Alors, $\mathcal{A}_{N/k}$ est un O_k-module libre.*

Démonstration. D'après [Mar69, Théorème I.4, p. 9] (c'est une généralisation du Théorème d'Artin dans [Art50]) :

$$\mathrm{cl}_k(\mathcal{A}_{N/k}) = \mathrm{cl}_k\left(\sqrt{\frac{\Delta(\mathcal{A}_{N/k})}{d}}\right),$$

où $\Delta(\mathcal{A}_{N/k})$ est le discriminant, par rapport à la forme trace $\mathrm{Tr}_{N/k}$, du réseau $\mathcal{A}_{N/k}$ du k-espace vectoriel N (voir [Ser68, Chap III, §2 et §3]), et d est le discriminant d'une base de ce dernier.

Puisque N/k est galoisienne de degré impair,

$$\mathrm{cl}_k(\mathcal{A}_{N/k}) = \mathrm{cl}\left(\sqrt{\Delta(\mathcal{A}_{N/k})}\right),$$

car d est un carré dans k.

Comme $\mathcal{A}_{N/k}$ est un idéal fractionnaire de N, d'après [Mar69, Théorème I.5, p. 10] :

$$\Delta(\mathcal{A}_{N/k}) = \Delta(N/k) N'_{N/k}(\mathcal{A}_{N/k})^2,$$

où $\Delta(N/k)$ est le discriminant de N/k et $N'_{N/k}$ est la norme dans N/k. On en déduit :

$$\Delta(\mathcal{A}_{N/k}) = O_k,$$

car $\mathcal{A}_{N/k}^2 = \mathcal{D}_{N/k}^{-1}$ et $N'_{N/k}(\mathcal{D}_{N/k}) = \Delta(N/k)$. On conclut que $\mathrm{cl}_k(\mathcal{A}_{N/k}) = 1$. □

Corollaire 2.1.2. *On a $R_m(\mathcal{A}, k[\Gamma]) = \{1\}$.*

Dans ce chapitre on s'interesse à la Conjecture 2. Dans la Section 2.2, on décrit d'une façon assez explicite, $\mathcal{R}(\mathcal{A}, \mathcal{M})$ lorsque $\Gamma = C_l$ est le groupe cyclique d'ordre un nombre premier l impair, et k est linéairement disjoint sur $\mathbb{Q}$ du l-ième corps cyclotomique sur $\mathbb{Q}$ et nous prouvons que $\mathbb{R}(\mathcal{A}, \mathcal{M})$ est un sous groupe de $\mathrm{Cl}^\circ(\mathcal{M})$; la preuve est une adaptation de quelques unes dans [Sod88]. Ensuite, dans la Section 2.3, on applique le résultat obtenu dans la Section 2.2 pour décrire un sous-ensemble de $\mathcal{R}(\mathcal{A}, \mathcal{M})$ lorsque

Γ est un groupe métacyclique non abélien d'ordre lq, où q est un nombre premier en se plaçant dans la situation de [SS10, Sod97]. En adaptant leurs preuves, nous démontrons que ce sous ensemble est un sous groupe de $\mathrm{Cl}^\circ(\mathcal{M})$. Dans la Section 2.4, on donne une généralisation non explicite des principaux résultats de la Section 2.3.

Nous terminons cette section par une remarque.

Il est bien connu (voir [Ere91, Théorème 1, §1]) que $\mathcal{A}_{N/k}$ est un $O_k[\Gamma]$ module localement libre si, et seulement si, N/k est faiblement ramifiée (i.e., les seconds groupes de ramifications sont triviaux).

Soit $\mathcal{R}_f(\mathcal{A},\mathcal{M})$ l'ensemble des classes c de $\mathrm{Cl}(\mathcal{M})$ telles qu'il existe une extension N/k faiblement ramifiée, à groupe de Galois isomorphe à Γ, avec $[\mathcal{M}\otimes_{O_k[\Gamma]}\mathcal{A}_{N/k}] = c$. Lorsque Γ est abélien, d'après [Tsa17, Théorème 1.2], $\mathcal{R}_f(\mathcal{A},\mathcal{M}) = \mathcal{R}(\mathcal{A},\mathcal{M})$. Donc, dans le cas abélien, on ne perd rien, lorsqu'on travaille dans $\mathrm{Cl}(\mathcal{M})$, en se restreignant aux extensions modérées pour l'étude des classes réalisables par la racine carrée de la codifférente.

2.2 Groupe cyclique d'ordre premier impair

Dans toute cette section : l est un nombre premier impair, $\Gamma = C_l = \langle\sigma\rangle$ est le groupe cyclique d'ordre l de générateur σ, ξ est une racine primitive l-ième de l'unité et k est linéairement disjoint de $\mathbb{Q}(\xi)$ sur $\mathbb{Q}$. Si $m \in \mathbb{Z}$, on désigne par $\underline{m}$ l'entier : $0 \leq \underline{m} \leq l-1$ congru à m modulo l. Nous identifierons des groupes isomorphes pour simplifier les notations.

Notons χ le caratère de Γ défini par $\chi(\sigma) = \xi$. Alors les caractères absolument irréductibles de Γ sont les χ^i, $0 \leq i \leq l-1$. Puisque k est linéairement disjoint de $\mathbb{Q}(\xi)$ su $\mathbb{Q}$, on peut choisir χ^0 et χ comme représentants de leurs classes de conjugaison sur k. On désigne par $k(\chi^i)$ l'extension de k obtenue par adjonction à k les valeurs de χ^i.

Il est immédiat que la décomposition de Wedderburn de l'algèbre semi-simple $k[\Gamma]$ en un produit d'algèbres simples est la suivante :

$$k[\Gamma] \simeq k(\chi^0) \times k(\chi) \simeq k \times k(\xi).$$

Soit $\mathcal{M}$ le O_k-ordre maximal dans l'algèbre semi-simple $k[\Gamma]$ contenant $O_k[\Gamma]$ ($\mathcal{M}$ est unique puisque $k[\Gamma]$ est commutative). On a :

$$\mathcal{M} \simeq O_k \times O_{k(\xi)}.$$

D'où

$$\mathrm{Cl}(\mathcal{M}) \simeq \mathrm{Cl}(k) \times \mathrm{Cl}(k(\xi)),$$

et

$$\mathrm{Cl}^\circ(\mathcal{M}) \simeq \mathrm{Cl}(k(\xi)).$$

Notons que comme $k/\mathbb{Q}$ et $\mathbb{Q}(\xi)/\mathbb{Q}$ sont linéairement disjointes, $\mathrm{Gal}(k(\xi)/k)$ est isomorphe par restriction à $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$.

Soit

$$S = \mathrm{Gal}(k(\xi)/k) = \{s_i \mid \ 1 \leq i \leq l-1\}, \text{où} \ \ s_i(\xi) = \xi^i.$$

Soit l'élément de Stickelberger

$$\theta = \sum_{i=1}^{l-1} i s_i^{-1},$$

et soit l'idéal de Stickelberger

$$\mathcal{S} = \frac{1}{l}\theta\mathbb{Z}[S] \cap \mathbb{Z}[S].$$

On modifie θ et $\mathcal{S}$ de la manière suivante : soient

$$\theta_* = \sum_{i=-\frac{l-1}{2}, i\neq 0}^{\frac{l-1}{2}} i s_{\underline{i}}^{-1},$$

$$\mathcal{S}_* = \frac{1}{l}\theta_*\mathbb{Z}[S] \cap \mathbb{Z}[S].$$

L'action naturelle de S sur les idéaux fractionnaires de $k(\xi)$ induit une structure de $\mathbb{Z}[S]$-module sur le groupe des idéaux fractionnaire de $k(\xi)$ et sur $\mathrm{Cl}(k(\xi))$. On note $\mathcal{S}\,\mathrm{Cl}(k(\xi))$ (resp. $\mathcal{S}_*\,\mathrm{Cl}(k(\xi))$) le sous-groupe de $\mathrm{Cl}(k(\xi))$ engendré par les éléments de la forme $\mathfrak{s}c$, où $\mathfrak{s} \in \mathcal{S}$ (resp. $\mathfrak{s} \in \mathcal{S}_*$) et $c \in \mathrm{Cl}(k(\xi))$.

Dans cette section nous démontrons le théorème suivant.

Théorème 2.2.1. *Sous les hypothèses et notations précédentes, et en identifiant* $\mathrm{Cl}^\circ(\mathcal{M})$ *et* $\mathrm{Cl}(k(\xi))$ *on a :* $\mathcal{R}(\mathcal{A}, \mathcal{M})$ *est un sous-groupe de* $\mathrm{Cl}^\circ(\mathcal{M})$ *égal à* $\mathcal{S}_*\,\mathrm{Cl}(k(\xi))$.

Nous allons énoncer ou établir quelques lemmes avant de faire la démonstration.

Dans la suite N/k est une extension galoisienne modérée à groupe de Galois isomorphe à Γ. Il est clair que N/k et $k(\xi)/k$ sont linéairement disjointes. D'où

$$\mathrm{Gal}(N(\xi)/k) \simeq \mathrm{Gal}(N/k) \times \mathrm{Gal}(k(\xi)/k),$$

et par restriction :

$$\mathrm{Gal}(N(\xi)/k(\xi)) \simeq \mathrm{Gal}(N/k), \mathrm{Gal}(N(\xi)/N) \simeq \mathrm{Gal}(k(\xi)/k)).$$

Si π est un isomorphisme de $\mathrm{Gal}(N/k)$ dans Γ, tout caractère χ' de Γ induit un caractère $\chi' \circ \pi$ de $\mathrm{Gal}(N/k)$ que l'on notera aussi χ'. Rappelons la définition de la résolvante de Lagrange de $x \in N$ et χ' :

$$\langle x, \chi' \rangle = \sum_{\gamma \in \Gamma} \chi'(\gamma^{-1})\gamma(x).$$

Immédiatement on a :

$$\sigma(\langle x, \chi' \rangle) = \chi'(\sigma)\langle x, \chi' \rangle, \quad s_i(\langle x, \chi' \rangle) = \langle x, \chi'^i \rangle.$$

D'après [Sod88, Théorème 2.2 (1)] on a :

Lemme 2.2.2. *Soit a une base normale de N/k. Alors, on peut écrire d'une manière unique*

$$\langle a,\chi\rangle^l O_{k(\xi)} = I(\chi)^l \theta J(\chi),$$

où $I(\chi)$ est un idéal fractionnaire de $k(\xi)$, et $J(\chi)$ est un idéal entier de $k(\xi)$ sans facteur carré et tel que les idéaux $s_i(J(\chi))$, $1 \leq i \leq l-1$, sont premiers entre eux deux à deux.

Un calcul simple nous donne :

$$\theta_* = \theta - l \sum_{i=\frac{l-1}{2}+1}^{l-1} s_i^{-1}.$$

Posons

$$R = \sum_{i=\frac{l+1}{2}}^{l-1} s_i^{-1},$$

de sorte que

$$\theta_* = \theta - lR \ \text{ et } \ R = \frac{1}{l}(\theta - \theta_*).$$

Lemme 2.2.3. *Sous les notations du lemme précédent, notons*

$$I_*(\chi) = I(\chi) R J(\chi).$$

Alors, la composante de la classe de $\mathcal{M} \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k}$ (plus précisément $\mathcal{M} \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k,\pi}$, avec χ identifié à $\chi \circ \pi$) dans $\mathrm{Cl}(k(\xi))$ est égale à la classe de $(I_*(\chi))^{-1}$.

Démonstration. Puisque pour tout $x \in N$, $\sigma(\langle x,\chi\rangle) = \chi(\sigma)\langle x,\chi\rangle$, on a : $\frac{\langle x,\chi\rangle}{\langle a,\chi\rangle}$ est un élément de $k(\xi)$.

Suivant le dernier paragraphe de la page 38 de [Ull74] on considère l'application

$$f : N \to k(\xi), \quad x \mapsto \frac{\langle x,\chi\rangle}{\langle a,\chi\rangle}.$$

Soit $X = \{\chi^0, \chi\}$; c'est un ensemble de représentants de toutes les classes de conjugaison sur k des caractères absolument irréductibles de Γ. D'après le dernier paragraphe de la page 36 et le début de la page 37 de [Ull74]

$$\mathcal{M} \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k} \simeq \left(O_k \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k}\right) \times \left(O_{k(\xi)} \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k}\right).$$

On a : $\mathcal{A}_{N/k}$ est un $O_k[\Gamma]$-module, $\mathcal{A}_{N/k}k = N$ ($\mathcal{A}_{N/k}$ est un idéal fractionnaire) et les idéaux premiers au dessus du degré l de N/k ne sont pas ramifiés dans N/k (N/k est modérée). Donc, le corollaire de la page 36 dans [Ull74] nous donne :

$$\frac{\langle \mathcal{A}_{N/k}, \chi^0\rangle}{\langle a, \chi^0\rangle} \simeq \left(O_k \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k}\right)$$

et

$$f(\mathcal{A}_{N/k}) \simeq \left(O_{k(\xi)} \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k}\right).$$

On en déduit (rappelons que $\mathrm{Cl}(\mathcal{M}) \simeq \mathrm{Cl}(k) \times \mathrm{Cl}(k(\xi))$) que les composantes de la classe de $\mathcal{M} \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k}$ dans $\mathrm{Cl}(k)$ et $\mathrm{Cl}(k(\xi))$ sont respectivement les classes de

$$\frac{\mathrm{Tr}_{N/k}(\mathcal{A}_{N/k})}{\mathrm{Tr}_{N/k}(a)} = \frac{O_k}{\mathrm{Tr}_{N/k}(a)} \text{ et } f(\mathcal{A}_{N/k}).$$

Notons qu'on retrouve la classe triviale dans $\mathrm{Cl}(k)$.

Le but de la suite est le calcul de $f(\mathcal{A}_{N/k})$ en utilisant [Ull74].

Notons $\mathfrak{p}_i$, $1 \leq i \leq n$, les idéaux premiers de O_k ramifiés dans l'extension N/k. Pour tout i, $1 \leq i \leq n$, on note $\mathfrak{P}_i$ l'idéal premier de O_N au dessus de $\mathfrak{p}_i$, de sorte que $\mathfrak{p}_i O_N = \mathfrak{P}_i^l$.

Comme l'extension N/k est modérée, on a : $v_{\mathfrak{P}_i}(\mathcal{D}_{N/k}) = l-1$. Donc :

$$\mathcal{D}_{N/k} = \prod_{i=1}^{n} \mathfrak{P}_i^{l-1}, \quad \text{et} \quad \mathcal{A}_{N/k} = \prod_{i=1}^{n} \mathfrak{P}_i^{-\frac{l-1}{2}}.$$

On a :

$$\mathcal{A}_{N/k} = \left(\prod_{i=1}^{n} \mathfrak{P}_i\right)^{-l} \left(\prod_{i=1}^{n} \mathfrak{P}_i\right)^{\frac{l+1}{2}} = \left(\left(\prod_{i=1}^{n} \mathfrak{p}_i\right)^{-1} O_N\right) \left(\prod_{i=1}^{n} \mathfrak{P}_i\right)^{\frac{l+1}{2}}.$$

Posons

$$\mathfrak{b} = \left(\prod_{i=1}^{n} \mathfrak{p}_i\right)^{-1}, \quad \text{et} \quad \mathfrak{U}_0 = \left(\prod_{i=1}^{n} \mathfrak{P}_i\right)^{\frac{l+1}{2}};$$

d'où

$$\mathcal{A}_{N/k} = \mathfrak{b} O_N \mathfrak{U}_0.$$

(Dans la terminologie de [Ull74], $\mathfrak{U}_0$ est un idéal primitif ambige de N/k.)

Comme f est k-linéaire on obtient

$$f(\mathcal{A}_{N/k}) = \mathfrak{b} O_{k(\xi)} f(\mathfrak{U}_0).$$

Nous allons déterminer $\mathfrak{b} O_{k(\xi)}$ et $J(\chi)$.

Immédiatement $N(\xi) = N(\langle a, \chi \rangle)$, le degré de $N(\xi)/k(\xi)$ est l, et elle est modérée car N/k l'est. Comme N/k et $k(\xi)/k$ sont arithmétiquement disjointes, on a

$$\Delta(N/k) O_{k(\xi)} = \Delta(N(\xi)/k(\xi)).$$

D'une part, par la théorie de Kummer (voir [Hec81, §39] ou [Bru09, Théorème 2.1])

$$\Delta(N(\xi)/k(\xi)) = \left(\left(\sum_{i=1}^{l-1} s_i\right) J(\chi)\right)^{l-1}.$$

D'autre part

$$\Delta(N/k) = N_{N/k}(\mathcal{D}_{N/k} = \prod_{i=1}^{n} \mathfrak{P}_i^{l-1}) = \prod_{i=1}^{n} \mathfrak{p}_i^{l-1}.$$

Par conséquent

$$\left((\prod_{i=1}^{n} \mathfrak{p}_i)O_{k(\xi)}\right)^{l-1} = ((\sum_{i=1}^{l-1} s_i)J(\chi))^{l-1},$$

D'où

$$\mathfrak{b}O_{k(\xi)} = ((\sum_{i=1}^{l-1} s_i)J(\chi))^{-1}.$$

Il est bien connu que les $\mathfrak{p}_i$ sont totalement décomposés dans $k(\xi)/k$, car ils sont premiers avec lO_k (voir par exemple [Bru09, Proposition 2.4]). De $(\prod_{i=1}^{n} \mathfrak{p}_i)O_{k(\xi)} = ((\sum_{i=1}^{l-1} s_i)J(\chi))$, on déduit que $J(\chi)$ peut s'écrire :

$$J(\chi) = \prod_{i=1}^{n} \mathfrak{p'}_i,$$

où $\mathfrak{p'}_i$ un idéal premier de $O_{k(\xi)}$ au dessus de $\mathfrak{p}_i$.

Puisque N/k est une extension cyclique de degré un nombre premier l dans laquelle tout idéal premier ramifié est totalement ramifié, les idéaux premiers de O_k au dessus de l ne sont pas ramifiés (car N/k est modérée), χ est fidèle et $J(\chi) = \prod_{i=1}^{n} \mathfrak{p'}_i$, d'après [Ull74, Theorème 1, p. 40] et dans ses notations

$$f(\mathfrak{U}_0) = f(O_N)u\left(\frac{l+1}{2}\right)\left(\prod_{i=1}^{n} \mathfrak{p'}_i\right)$$

où

$$u\left(\frac{l+1}{2}\right) = \sum_{i=1}^{l-1} c_i\left(\frac{l+1}{2}\right)s_i^{-1}, \quad \text{et} \quad c_i\left(\frac{l+1}{2}\right) = 1 + \left[\left(\frac{l+1}{2} - i - 1\right)/l\right],$$

où $[x]$ est la partie entière de x.

Posons $R' = \sum_{i=1}^{\frac{l-1}{2}} s_i^{-1}$. Immédiatement, $u(\frac{l+1}{2}) = R'$. D'où

$$f(\mathfrak{U}_0) = f(O_N)R'J(\chi).$$

D'après la démonstration du Théorème 2.3 de [Sod88, p. 193] :

$$f(O_N) = I(\chi)^{-1}.$$

Comme $R + R' = \sum_{i=1}^{l-1} s_i^{-1} = \sum_{i=1}^{l-1} s_i$, et $\mathfrak{b}O_{k(\xi)} = ((R + R')J(\chi))^{-1}$, on obtient :

$$\begin{aligned} f(\mathcal{A}_{N/k}) &= I(\chi)^{-1}(R + R')J(\chi)^{-1}R'J(\chi) \\ &= (I(\chi)RJ(\chi))^{-1} \\ &= (I_*(\chi))^{-1}. \end{aligned}$$

Ce qui termine la démonstration du lemme. □

Le groupe $\mathrm{Aut}(\Gamma)$ des automorphismes de Γ est isomorphe au groupe cyclique des éléments inversibles de $\mathbb{Z}/l\mathbb{Z}$. Soient π un isomorphisme de $\mathrm{Gal}(N/k)$ dans Γ et φ un générateur de $\mathrm{Aut}(\Gamma)$. Immédiatement les isomorphismes de $\mathrm{Gal}(N/k)$ dans Γ sont les $\pi_i = \varphi^i \circ \pi$, $0 \leq i \leq l-1$, et $\chi \circ \pi_i = (\chi \circ \pi)^i$.

Corollaire 2.2.4. *Sous les notations du lemme précédent, on a : la composante de la classe de $\mathcal{M} \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k,\pi_i}$ dans $\mathrm{Cl}(k(\xi))$ est égale à la classe de $s_i(I_*(\chi))^{-1}$.*

Démonstration. Cela découle de : $\langle a, \chi\circ\pi_i\rangle = s_i(\langle a, \chi\circ\pi\rangle)$ et l'unicité de la décomposition de $\langle a, \chi \circ \pi_i\rangle^l O_{k(\xi)}$. □

Lemme 2.2.5. *Soit $\mathcal{S}'$ l'idéal de $\mathbb{Z}[S]$ engendré par les éléments de la forme $c - s_{\underline{c}}$, où c est premier avec l.*

(1) *Soit $\mathfrak{s} \in \mathbb{Z}[S]$. Alors : $\frac{1}{l}\theta\mathfrak{s} \in \mathbb{Z}[S] \Longleftrightarrow \mathfrak{s} \in \mathcal{S}'$.*

(2) $\mathcal{S} = \frac{1}{l}\theta\mathcal{S}'$.

(3) $\mathcal{S} + \mathcal{S}' = \mathbb{Z}[S]$.

Démonstration. Les assertions (1) et (2) proviennent du [Was97, Lemme 6.8, p. 93]. Pour (3), il suffit de voir qu'on a

$$-\theta + \left(l + \sum_{i=1}^{l-1}(i - s_i)s_i^{-1}\right) = 1,$$

et $l \in \mathcal{S}'$, car $l = (l+1) - s_{\underline{l+1}}$. □

Lemme 2.2.6. *Sous les notations précédentes, on a :*

(1) $\mathcal{S}_* = \frac{1}{l}\theta_*\mathcal{S}'$.

(2) $\mathcal{S}_* + \mathcal{S}' = \mathbb{Z}[S]$.

(3) *Soit $c \in \mathrm{Cl}(k(\xi))$. Si pour tout $\mathfrak{s}' \in \mathcal{S}'$, $\mathfrak{s}'c \in \mathcal{S}_* \mathrm{Cl}(k(\xi))$, alors $c \in \mathcal{S}_* \mathrm{Cl}(k(\xi))$.*

Démonstration. (1) Soit $x = \frac{1}{l}\theta_*\mathfrak{s}' \in \frac{1}{l}\theta_*\mathcal{S}'$, où $\mathfrak{s}' \in \mathcal{S}'$. Comme $\theta_* = \theta - lR$, on obtient $x = \frac{1}{l}\theta\mathfrak{s}' - R\mathfrak{s}'$. D'où $x \in \mathbb{Z}[S]$ par l'assertion (1)(ou (2)) du lemme précédent et donc $x \in \mathcal{S}_*$; on en déduit $\frac{1}{l}\theta_*\mathcal{S}' \subset \mathcal{S}_*$.

Soit $x = \frac{1}{l}\theta_*\mathfrak{s} \in \mathcal{S}_*$, où $\mathfrak{s} \in \mathbb{Z}[S]$. On a

$$x = \frac{1}{l}(\theta - lR)\mathfrak{s} = \frac{1}{l}\theta\mathfrak{s} - R\mathfrak{s}.$$

D'où $\frac{1}{l}\theta\mathfrak{s} \in \mathbb{Z}[S]$. Par le lemme précédent $\mathfrak{s} \in \mathcal{S}'$. Donc $\mathcal{S}_* \subset \frac{1}{l}\theta_*\mathcal{S}'$.

(2) Par (3) du Lemme 2.2.5, il existe $\mathfrak{s} \in \mathcal{S}$ et $\mathfrak{s}' \in \mathcal{S}'$ tels que $\mathfrak{s} + \mathfrak{s}' = 1$. Il existe $x \in \mathcal{S}'$ tel que $\mathfrak{s} = \frac{1}{l}\theta x$. De $\theta = \theta_* + lR$ et $\mathfrak{s} + \mathfrak{s}' = 1$ on tire

$$\frac{1}{l}\theta_* x + (Rx + \mathfrak{s}') = 1,$$

d'où $\mathcal{S}_* + \mathcal{S}' = \mathbb{Z}[S]$.

(3) D'après (2) il existe $\mathfrak{s} \in \mathcal{S}_*$ et $\mathfrak{s}' \in \mathcal{S}'$ tels que $\mathfrak{s} + \mathfrak{s}' = 1$. On a (3) puisque $c = (\mathfrak{s}'c)(\mathfrak{s}c)$ et $\mathcal{S}_* \operatorname{Cl}(k(\xi))$ est un sous-groupe de $\operatorname{Cl}(k(\xi))$. □

Démonstration du Théorème 2.2.1. (1) $\mathcal{R}(\mathcal{A}, \mathcal{M}) \subset \mathcal{S}_* \operatorname{Cl}(k(\xi))$.

Sous les notations et hypothèses du Lemme 2.2.2 on a :

$$\langle a, \chi\rangle^l O_{k(\xi)} = I(\chi)^l \theta J(\chi).$$

On en déduit sous les notations du Lemme 2.2.3 :

$$\langle a, \chi\rangle^l O_{k(\xi)} = I_*(\chi)^l \theta_* J(\chi).$$

Soit $\mathfrak{s}' \in \mathcal{S}'$. Immédiatement $\mathfrak{s}'\langle a, \chi\rangle \in k(\xi)$. D'où

$$(\mathfrak{s}'\langle a, \chi\rangle) O_{k(\xi)} = \mathfrak{s}' I_*(\chi) \frac{1}{l}\theta_* \mathfrak{s}' J(\chi).$$

Par suite la classe de $\mathfrak{s}' I_*(\chi)^{-1}$ appartient à $\mathcal{S}_* \operatorname{Cl}(k(\xi))$. Donc, par le Lemme 2.2.6 (3), la classe de $I_*(\chi)^{-1}$ appartient à $\mathcal{S}_* \operatorname{Cl}(k(\xi))$. On conclut grâce au Lemme 2.2.3.

(2) $\mathcal{S}_* \operatorname{Cl}(k(\xi)) \subset \mathcal{R}(\mathcal{A}, \mathcal{M})$.

Nous allons adapter la seconde partie de la preuve du Théorème 2.4 dans ([Sod88, p. 195]) à notre situation.

Précisons un allègement d'une notation pour la suite : si I est un idéal fractionnaire de $k(\xi)$, on désigne par $\operatorname{cl}(I)$ sa classe dans $\operatorname{Cl}(k(\xi))$ (au lieu de $\operatorname{cl}_{k(\xi)}(I)$).

Soit $c \in \mathcal{S}_* \operatorname{Cl}(k(\xi))$. D'après le Lemme 2.2.6 (1), il existe un entier j, des idéaux fractionnaires I_i de $k(\xi)$, $1 \leq i \leq j$, qu'on peut choisir premiers avec $lO_{k(\xi)}$ par le Théorème de densité de Chebotarev, et des éléments $\mathfrak{s}'_i$, $1 \leq i \leq j$, de $\mathcal{S}'$ tels que :

$$c = \operatorname{cl}\left(\prod_{i=1}^{j} (1/l)\mathfrak{s}'_i \theta_* I_i\right).$$

Posons $I = \prod_{i=1}^{j} (1/l)\mathfrak{s}'_i \theta_* I_i$ et $J = \prod_{i=1}^{j} \mathfrak{s}'_i I_i$. Alors :

$$I^l = \theta_* J, \quad c = \operatorname{cl}(I).$$

Soit le cycle $\mathcal{C} = (1-\xi)^l O_{k(\xi)}$. Soit $\operatorname{Cl}(k(\xi), \mathcal{C})$ le groupe de classes de rayon de $k(\xi)$ modulo $\mathcal{C}$. On a J est premier avec $\mathcal{C}$, en effet : d'une part pour tout i', $1 \leq i' \leq l-1$, et tout i, $1 \leq i \leq j$, $s_{i'}(I_i)$ est premier avec $s_{i'}(lO_{k(\xi)}) = lO_{k(\xi)}$; d'autre part, comme

$lO_{k(\xi)} = (1-\xi)^{l-1}O_{k(\xi)}$, les idéaux premiers de $O_{k(\xi)}$ divisant toute puissance non triviale de $(1-\xi)O_{k(\xi)}$ sont exactement ceux divisant $lO_{k(\xi)}$. Par le Théorème de densité de Chebotarev dans $\mathrm{Cl}(k(\xi),\mathcal{C})$, il existe un idéal premier $\mathfrak{p}$ de $O_{k(\xi)}$, avec $\mathfrak{p}\cap O_k$ totalement décomposé dans $k(\xi)/k$ et tel que $\mathrm{cl}(\mathfrak{p}) = \mathrm{cl}(J)$ dans $\mathrm{Cl}(k(\xi),\mathcal{C})$. Il s'ensuit qu'il existe $a' \in k(\xi)$ satisfaisant :

$$\mathfrak{p} = a'J, \quad a' \equiv 1 \mod^* (1-\xi)^l O_{k(\xi)},$$

où $\mod^*$ est la congruence habituelle dans la théorie du corps de classes.

D'une part

$$\begin{aligned} I^l &= \theta_* J = (\theta - lR)J \\ &= \theta J (RJ)^{-l}. \end{aligned}$$

D'autre part, de $\mathfrak{p} = a'J$ on tire

$$\theta J = \theta\mathfrak{p}(\theta a')^{-1}.$$

Posons

$$a'' = \theta a'.$$

Alors

$$a''O_{k(\xi)} = ((IRJ)^{-1})^l \theta\mathfrak{p}.$$

L'élément a'' n'est pas une puissance l-ième dans $k(\xi)$, car par exemple on a que $v_{\mathfrak{p}}(a'') \equiv 1 \ mod\ l$, où $v_{\mathfrak{p}}$ est la valuation $\mathfrak{p}$-adique.

Soit α un élément de $\overline{k}$ vérifiant

$$\alpha^l = a''.$$

Posons

$$N' = k(\xi)(\alpha).$$

Alors $N'/k(\xi)$ est une extension cyclique (de Kummer) de degré l. Elle est modérée, car $\theta a' \equiv 1 \mod^* (1-\xi)^l O_{k(\xi)}$; donc N'/k est modérée car $k(\xi)/k$ l'est. L'extension N'/k est galoisienne abélienne par [Lon71, Corollaire 1.3, p. 89] (ou [Bru09, Proposition 2.3]), car $a'' = \theta a'$; elle admet une (unique) sous-extension N/k galoisienne, de degré l. Il est clair que N/k est modérée et $N' = N(\xi)$.

On a $\mathrm{Gal}(N'/k(\xi)) \simeq C_l$. Nous identifions C_l avec $\mathrm{Gal}(N(\xi)/k(\xi))$ en faisant agir σ sur $N(\xi)$ de sorte que $\sigma(\alpha) = \xi\alpha$. Puisque $\mathrm{Gal}(N(\xi)/k(\xi))$ est isomorphe (par restriction) à $\mathrm{Gal}(N/k)$, on identifie aussi C_l et $\mathrm{Gal}(N/k)$, d'où un caractère φ_0 de $\mathrm{Gal}(N/k)$, défini par

$$\varphi_0(\sigma) = \xi.$$

Notons qu'en fait, si l'on note π_0 l'isomorphisme $\mathrm{Gal}(N/k) \simeq C_l$ ci-dessus, alors

$$\varphi_0 = \chi \circ \pi_0.$$

Dans la suite, on identifie φ_0 et χ.

Posons $\alpha' = (1/l)\,\mathrm{Tr}_{N(\xi)/N}(\alpha)$. Alors, immédiatement $\langle \alpha', \chi\rangle_{N/k} = \alpha$. Donc

$$\langle \alpha', \chi\rangle^l O_{k(\xi)} = ((IRJ)^{-1})^l \theta \mathfrak{p}.$$

Rappelons que pour tout $x \in N$,

$$\sigma(\langle x, \chi\rangle) = \chi(\sigma)\langle x, \chi\rangle.$$

On en déduit que, si a est une base normale de N/k, alors $\langle a, \chi\rangle / \langle \alpha', \chi\rangle$ est fixe par σ ; donc il existe $\lambda \in k(\xi)$ tel que $\langle a, \chi\rangle = \lambda \langle \alpha', \chi\rangle$. Par conséquent

$$\langle a, \chi\rangle^l O_{k(\xi)} = (\lambda (IRJ)^{-1})^l \theta \mathfrak{p}.$$

D'où

$$I_*(\chi) = \lambda (IRJ)^{-1} R \mathfrak{p}.$$

Comme $\mathrm{Cl}(\mathfrak{p}) = \mathrm{cl}(J)$, on a :

$$\mathrm{cl}(I_*(\chi))^{-1} = \mathrm{cl}(I) = c.$$

D'après le Lemme 2.2.3, la composante de la classe de $\mathcal{M} \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k}$ (plus précisément $\mathcal{M} \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k,\pi_0}$) dans $\mathrm{Cl}(k(\xi)$ est égale à c. Donc $c \in \mathcal{R}(\mathcal{A}, \mathcal{M})$. Par conséquent $\mathcal{S}_* \,\mathrm{Cl}(k(\xi)) \subset \mathcal{R}(\mathcal{A}, \mathcal{M})$. □

Remarque. L'extension N/k obtenue ci-dessus a pour discriminant $\Delta(N/k) = (\mathfrak{p} \cap O_k)^{l-1}$, car $J(\chi) = \mathfrak{p}$. Soit X un idéal entier de O_k, Il est immédiat qu'on peut réaliser c par une extension modérée N'/k dont le discriminant est premier à X ; il suffit de partir dans la démonstration ci-dessus avec le cycle $\mathcal{C}' = (1-\xi)^l X O_{k(\xi)}$.

Nous terminons cette section par comparer θ, $\mathcal{S}$, $\mathcal{R}(O, \mathcal{M})$ et θ_*, $\mathcal{S}_*$, $\mathcal{R}(\mathcal{A}, \mathcal{M})$.

Proposition 2.2.7. *On a :*

(1) $\theta_* = (s_2 - 1)\theta$. *(Donc* $\theta_* \in \mathcal{S}$.*)*

(2) $\mathcal{S}_* = (s_2 - 1)\mathcal{S}$. *(Donc* $\mathcal{S}_* \subset \mathcal{S}$.*)*

(3) $\mathcal{R}(\mathcal{A}, \mathcal{M}) \subset \mathcal{R}(O, \mathcal{M})$ *; l'inclusion pouvant être stricte.*

Démonstration. (1) On a $s_2\theta = \sum_{i=1}^{l-1} i s^{-1}_{\underline{2^{-1}i}}$. En effectuant le changement de variable : $j \equiv \underline{2^{-1}i} \mod l$, on obtient :

$$\begin{aligned} s_2\theta &= \sum_{j=1}^{(l-1)/2} 2j s_j^{-1} + \sum_{j=(l+1)/2}^{l-1} (2j-l) s_j^{-1} \\ &= 2\theta - l \sum_{j=(l+1)/2}^{l-1} s_j^{-1} \\ &= 2\theta - lR \end{aligned}$$

Par suite $\theta - lR = (s_2 - 1)\theta$. Donc $\theta_* = (s_2 - 1)\theta$.

(2) On a $\mathcal{S}_* = \frac{1}{l}\theta_*\mathcal{S}' = (s_2 - 1)\frac{1}{l}\theta\mathcal{S}' = (s_2 - 1)\mathcal{S}$.

(3) D'après [Sod88, Théorème 2.4], $\mathcal{R}(O, \mathcal{M}) = \mathcal{S}\,\mathrm{Cl}(k(\xi))$. Comme $\mathcal{S}_* \subset \mathcal{S}$ et

$$\mathcal{R}(\mathcal{A}_{N/k}, \mathcal{M}) = \mathcal{S}_*\,\mathrm{Cl}(k(\xi)),$$

on a $\mathcal{R}(\mathcal{A}, \mathcal{M}) \subset \mathcal{R}(O, \mathcal{M})$.

Immédiatement

$$N_{k(\xi)/k}(\mathcal{S}\,\mathrm{Cl}(k(\xi))) = N_{k(\xi)/k}(\mathrm{Cl}(k(\xi))^{(l-1)/2}.$$

d'où

$$N_{k(\xi)/k}(\mathcal{S}_*\,\mathrm{Cl}(k(\xi))) = (s_2 - 1)N_{k(\xi)/k}(\mathrm{Cl}(k(\xi))^{(l-1)/2} = \{1\}.$$

Il suffit donc que $N_{k(\xi)/k}(\mathrm{Cl}(k(\xi)))^{(l-1)/2}$ soit non trivial pour que l'inclusion dans (3) soit stricte. Signalons que, d'après [Lon71, Théorème 2.6],

$$R_m(O, k[\Gamma]) = N_{k(\xi)/k}(\mathrm{Cl}(k(\xi))^{(l-1)/2}.$$

En particulier, si $k \neq \mathbb{Q}$, il est en général non trivial. Par exemple si l ne se ramifie pas dans k, $N_{k(\xi)/k}(\mathrm{Cl}(k(\xi)) = \mathrm{Cl}(k)$ ($k(\xi)/k$ est totalement ramifiée au dessus des premiers divisant l, d'où la surjection de $N_{k(\xi)/k}$ sur $\mathrm{Cl}(k(\xi))$; on ajoute la condition : le nombre de classe de k est différent de 1 et est premier avec $(l-1)/2$. □

Remarque. Si $k = \mathbb{Q}$, alors $\mathcal{R}(\mathcal{A}, \mathcal{M}) = \{1\}$, car $\mathcal{S}_*\,\mathrm{Cl}(\mathbb{Q}(\xi)) = \{1\}$ puisque $\mathcal{S}_* \subset \mathcal{S}$ et il est bien connu que $\mathcal{S}\,\mathrm{Cl}(\mathbb{Q}(\xi)) = \{1\}$.

2.3 Groupe métacyclique non abélien d'ordre un produit de deux nombres premiers impairs

Dans toute cette section : l (resp. q) est un nombre premier impair, Γ est un groupe métacyclique non abélien d'ordre lq, ξ_l (resp. ξ_q) est une racine primitive l (resp. q)-ième de l'unité, nous identifierons des groupes isomorphes pour simplifier les notations.

Le groupe Γ peut être défini par la présentation suivante :

$$\Gamma = \langle \sigma, \tau : \sigma^l = \tau^q = 1, \tau\sigma\tau^{-1} = \sigma^r \rangle,$$

où r est un entier, avec $1 \leq r \leq l-1$, et la classe de r dans $(\mathbb{Z}/l\mathbb{Z})^*$ est d'ordre q. C'est un produit semi-direct de $C_l = \langle\sigma\rangle$ et $C_q = \langle\tau\rangle$:

$$\Gamma = C_l \rtimes C_q.$$

L'objectif de cette section est l'application de la section 2.2 à l'étude des classes réalisables de racines carrées de codifférentes d'extensions métacycliques non abéliennes de degré lq.

Le thème de l'article [SS10] (resp. [Sod97]) est l'étude des classes réalisables d'anneaux d'entiers d'extensions métacycliques de degré lm (resp. lq, avec q pouvant être pair).

Dans la suite, nous utiliserons des notations et résultats de [SS10] ; nous notons m par q comme dans [Sod97]. Nous adapterons les preuves dans [SS10] à notre situation. Nous avons préféré suivre [SS10] que [Sod97] car dans le premier il y a une correction du second dans [SS10, Remarque (2), p. 1822] et, pour la convenance du lecteur, il y a plus de détails nécessaires et suffisants que dans [Sod97].

Le groupe dérivé de Γ étant C_l, l'abelianisé de Γ est Γ/C_l ($\simeq C_q$). Donc il y a q caractères absolument irréductibles de Γ de degré 1 : on les obtient en composant les caractères de degré 1 de Γ/C_l avec la surjection canonique de Γ sur Γ/C_l. Supposons que $k/\mathbb{Q}$ et $\mathbb{Q}(\xi_q)/\mathbb{Q}$ soient linéairement disjointes, alors il y a deux classes de conjugaison sur k de ces caractères. Notons $\{\psi_i, 0 \leq i \leq 1\}$ un système de leurs représentants, avec ψ_0 le caractère trivial.

Pour tout i, $0 \leq i \leq 1$, la restriction de ψ_i à C_q définit un caractère de C_q, qu'on note χ_i. Il est clair que $\{\chi_i, 0 \leq i \leq 1\}$ est un système de représentants des classes de conjugaison sur k des caractères absolument irréductibles de C_q. Soit $k(\psi_i)$ (resp. $k(\chi_i)$) l'extension de k obtenue par adjonction à k les valeurs de ψ_i (resp. χ_i) ; alors $k(\psi_i) = k(\chi_i)$ pour tout i, $0 \leq i \leq 1$.

D'après les deux derniers paragraphes et la remarque (2) dans [SS10, p. 1820], en supposant que $k/\mathbb{Q}$ et $\mathbb{Q}(\xi_l)/\mathbb{Q}$ linéairement disjointes il reste une seule classe de conjugaison sur k des caractères irréductibles de Γ dont on note χ son représentant. Le caractère χ est de degré q, n'est pas symplectique et est induit par un caractère ψ de degré 1 et d'ordre l de C_l

$$\chi = \mathrm{Ind}_{C_l}^{\Gamma} \psi.$$

Dans toute la suite de ce chapitre, on suppose que k est linéairement disjoint de $\mathbb{Q}(\xi_l, \xi_q)$ sur $\mathbb{Q}$ et l'on note par E_0 le sous-corps de $k(\xi_l)$ tel que le degré de $k(\xi_l)/E_0$ est q. Signalons que le corps K défini dans [Sod97, p. 88] est égal à E_0.

Soit $\mathcal{M}$ un O_k-ordre maximal dans l'algèbre semi-simple $k[\Gamma]$ contenant $O_k[\Gamma]$. On a (voir [SS10, p. 1821]) :

- D'une part, la décomposition de Wedderburn de l'algèbre semi-simple $k[\Gamma]$ en un produit d'algèbres simples est la suivante :

$$\begin{aligned} k[\Gamma] &\simeq k(\psi_0) \times k(\psi_1) \times M_q(E_0) = k(\chi_0) \times k(\chi_1) \times M_q(E_0) \\ &\simeq k \times k(\xi_q) \times M_q(E_0), \end{aligned}$$

où $M_q(E_0)$ est l'anneau des matrices carrées d'ordre q à coefficients dans E_0.

- D'autre part, comme $E_0 = k(\chi)$ l'extension de k obtenue par adjonction à k des valeurs de χ et aucun caratère de Γ n'est symplectique,

$$\mathrm{Cl}(\mathcal{M}) \simeq \mathrm{Cl}(k) \times \mathrm{Cl}(k(\xi_q)) \times \mathrm{Cl}(E_0).$$

D'où

$$\mathrm{Cl}^\circ(\mathcal{M}) \simeq \mathrm{Cl}(k(\xi_q)) \times \mathrm{Cl}(E_0).$$

On note :

$$S_l = \mathrm{Gal}(k(\xi_l)/k) = \{s_i \mid \ 1 \leq i \leq l-1\}, \text{où} \ \ s_i(\xi_l) = \xi_l^i,$$
$$S_q = \mathrm{Gal}(k(\xi_q)/k) = \{s'_i \mid \ 1 \leq i \leq q-1\}, \text{où} \ \ s'_i(\xi_q) = \xi_q^i.$$

Soient les éléments de Stickelberger

$$\theta_l = \sum_{i=1}^{l-1} i s_i^{-1}, \quad \theta_q = \sum_{i=1}^{q-1} i s_i'^{-1},$$

et soient les idéaux de Stickelberger

$$\mathcal{S}_l = \frac{1}{l}\theta_l \mathbb{Z}[S_l] \cap \mathbb{Z}[S_l], \quad \mathcal{S}_q = \frac{1}{q}\theta_q \mathbb{Z}[S_q] \cap \mathbb{Z}[S_q].$$

On modifie θ_l, θ_q, $\mathcal{S}_l$ et $\mathcal{S}_q$ de la manière suivante : soient

$$(\theta_l)_* = \sum_{i=-\frac{l-1}{2}, i\neq 0}^{\frac{l-1}{2}} i s_{\underline{i}}^{-1}, \quad (\theta_q)_* = \sum_{i=-\frac{q-1}{2}, i\neq 0}^{\frac{q-1}{2}} i s_{\underline{i}}'^{-1}$$

$$(\mathcal{S}_l)_* = \frac{1}{l}(\theta_l)_* \mathbb{Z}[S_l] \cap \mathbb{Z}[S_l], \quad (\mathcal{S}_q)_* = \frac{1}{q}(\theta_q)_* \mathbb{Z}[S_q] \cap \mathbb{Z}[S_q].$$

On définit $\mathcal{R}_1(\mathcal{A}, \mathcal{M})$ comme étant l'ensemble des classes réalisables par les racines carrées des codifférentes des extensions métacycliques N/k de degré lq, telles que la sous-extension k_1/k de N/k de degré q est linéairement disjointe de $k(\xi_l)/k$.

L'extension E_0/k étant galoisienne, S_l opère par restriction de façon naturelle sur le groupe des idéaux fractionnaires de E_0, d'où une structure de $\mathbb{Z}[S_l]$ sur $\mathrm{Cl}(E_0)$.

Dans cette section nous démontrons le théorème suivant.

Théorème 2.3.1. *Sous les hypothèses et notations précédentes, et en identifiant* $\mathrm{Cl}^\circ(\mathcal{M})$ *et* $\mathrm{Cl}(k(\xi_q)) \times \mathrm{Cl}(E_0)$*, on a :* $\mathcal{R}_1(\mathcal{A}, \mathcal{M})$ *est un sous-groupe de* $\mathrm{Cl}^\circ(\mathcal{M})$ *et*

$$\mathcal{R}_1(\mathcal{A}, \mathcal{M}) = (\mathcal{S}_q)_* \,\mathrm{Cl}(k(\xi_q)) \times (\mathcal{S}_l)_* \,\mathrm{Cl}(E_0).$$

Soient G un groupe fini et M/K une G-extension galoisienne de corps de nombres. En utilisant la terminologie de [McC85], M/K est dite domestique si les idéaux premiers au dessus des diviseurs premiers de l'ordre de G ne sont pas ramifiés ; il est clair qu'une telle extension est modérée.

Soit $\mathcal{R}_d(O, O_k[G])$ (resp. $\mathcal{R}_d(O, \mathcal{M}(K[G]))$ le sous-ensemble des classes réalisables par des anneaux d'entiers des G-extensions domestiques. D'une façon similaire on définit $\mathcal{R}_d(\mathcal{A}, O_k[G])$ et $\mathcal{R}_d(\mathcal{A}, \mathcal{M}(K[G]))$.

Dans [McC85, Théorème 3.3, p. 198], comme une étape vers l'article définitif [McC87], il est montré que lorsque G est abélien, $\mathcal{R}_d(O, O_k[G])$ est un sous-groupe de $\mathrm{Cl}(O_k[G])$, donc $\mathcal{R}_d(O, \mathcal{M}(K[G]))$ est aussi un sous-groupe de $\mathrm{Cl}(\mathcal{M}(K[G])$.

Corollaire 2.3.2. *Supposons l non ramifié dans $k/\mathbb{Q}$. Alors, $\mathcal{R}_d(\mathcal{A}, \mathcal{M})$ est égal au sous-groupe $\mathcal{R}_1(\mathcal{A}, \mathcal{M})$.*

Soient K un corps de nombres quelconque et Γ' un groupe fini. Supposons qu'aucun caractère absolument irreductible de Γ' ne soit symplectique (notre groupe Γ vérifie cette condition) ; en particulier $K[\Gamma']$ satisfait la condition d'Eichler. Soit $\mathcal{M}'$ un O_K-ordre maximal de $K[\Gamma']$ contenant $O_K[\Gamma']$. Ci-dessous, nous rappelons brièvement la Hom-description de Fröhlich du groupe des classes $\mathrm{Cl}(\mathcal{M}')$ et la notion de résolvante de Fröhlich-Lagrange(voir [Frö83]).

On désigne par $R_{\Gamma'}$ le groupe des caractères virtuels de Γ'. Soient $\overline{K}$ une clôture algébrique de K, $\overline{K}^\times = \overline{K} \setminus \{0\}$, $\Omega_K = \mathrm{Gal}(\overline{K}/K)$, $J(\overline{K})$ le groupe des idèles de $\overline{K}$, et $U(\overline{K})$ le sous-groupe des idèles unités de $J(\overline{K})$. Alors

$$\mathrm{Cl}(\mathcal{M}') \simeq \frac{\mathrm{Hom}_{\Omega_K}(R_{\Gamma'}, J(\overline{K}))}{\mathrm{Hom}_{\Omega_K}(R_{\Gamma'}, \overline{K}^\times)\,\mathrm{Hom}_{\Omega_K}(R_{\Gamma'}, U(\overline{K}))}.$$

Soit M/K une extension galoisienne à groupe de Galois isomorphe à Γ'. Si π est un isomorphisme défini sur $\mathrm{Gal}(M/K)$ et à valeurs dans Γ', alors tout caractère χ' de Γ' induit un caractère $\chi' \circ \pi$ de $\mathrm{Gal}(M/K)$ que l'on notera aussi χ'. Si $\gamma \in \Gamma'$, nous noterons $\pi^{-1}(\gamma) \in \mathrm{Gal}(M/K)$ simplement par γ. Soit B une K-algèbre commutative, alors $M \otimes_K B$ est un $B[\Gamma']$-module libre de rang 1 ; soit $a \in M \otimes_K B$ une base de ce module. Soit $T : \Gamma' \to GL_n(\overline{K})$ une représentation linéaire de Γ' de caractère χ'. On appelle résolvante de Fröhlich-Lagrange de a et de χ', l'élément de $\overline{K} \otimes_K B$, noté $\langle a, \chi' \rangle_{M/K}$ (ou $\langle a, \chi' \rangle$ si aucune confusion n'est possible), défini par :

$$\langle a, \chi' \rangle_{M/K} = \mathrm{Det}(\sum_{\gamma \in \Gamma'} \gamma(a) T(\gamma^{-1})),$$

où Det désigne le déterminant.

Pour tout idéal premier $\mathfrak{p}$ de O_K, soit $K_\mathfrak{p}$ (resp. $O_{K,\mathfrak{p}}$) la complétion de K (resp. O_K) en $\mathfrak{p}$. Si K'/K est une sous-extension de M/K, on note $K'_\mathfrak{p} = K' \otimes_K K_\mathfrak{p}$ et $O_{K',\mathfrak{p}} = O_{K'} \otimes_{O_K} O_{K,\mathfrak{p}}$ les semi-complétés respectifs de K' et $O_{K'}$.

Faisons quelques rappels (voir [Frö83, §2, p.17]). Un $O_K[\Gamma']$-module X est dit localement libre si c'est un $O_K[\Gamma']$-module de type fini tel que pour tout premier $\mathfrak{p}$ de O_k, le $O_{K,\mathfrak{p}}[\Gamma']$-module $X_\mathfrak{p} = X \otimes_{O_K} O_{K,\mathfrak{p}}$ (le semi- complété de X) est libre. Le rang de X est défini comme étant le rang du $K[\Gamma']$-module libre $(X \otimes_{O_K} K) = KX$. Ce rang est fini et il est égal au rang de $X_\mathfrak{p}$ sur $O_{K,\mathfrak{p}}[\Gamma']$ pour tout $\mathfrak{p}$.

Signalons que le Théorème 4 de Fröhlich dans [Frö83, Théorème 4, p. 30] est valable, non seulement pour O_M, mais pour tout $O_K[\Gamma]$-module localement libre X de rang 1, avec

b de son énoncé une base du $K[\Gamma']$-module libre $(X \otimes_{O_K} K) = KX$. Pour le prouver, il suffit de copier la démonstration de ce théorème en remplaçant O_M par X et en utilisant [Frö83, Théorème 1, p. 20] (Théorème 1 est valable pour tout $O_K[\Gamma']$-module localement libre de rang 1).

Supposons M/K modérée. On sait que $\mathcal{A}_{M/K}$ est un $O_K[\Gamma']$-module localement libre. Comme $\mathcal{A}_{M/K}$ est un idéal fractionnaire de M, on a $K\mathcal{A}_{M/K} = M$. Par le théorème de la base normale, M est un $K[\Gamma']$-module libre de rang 1. Donc le rang de $\mathcal{A}_{M/K}$ est 1.

Pour tout idéal premier $\mathfrak{p}$ de O_K, soit $\alpha_\mathfrak{p}$ une base (normale locale) du $O_{K,\mathfrak{p}}[\Gamma']$-module $\mathcal{A}_{M/K,\mathfrak{p}}$. Soit a une base (normale) du $K[\Gamma']$-module M. D'après [Frö83, Théorème 4, p. 30] et ce qui vient d'être dit ci-dessus sur sa généralisation, un représentant de la classe de $\mathcal{M}' \otimes_{O_K[\Gamma']} \mathcal{A}_{M/K}$ dans $\mathrm{Cl}(\mathcal{M}')$ est l'application f définie par :

$$f(\chi') = \left(\frac{\langle \alpha_\mathfrak{p}, \chi' \rangle}{\langle a, \chi' \rangle}\right)_\mathfrak{p}.$$

Désormais N/k désigne une extension modérément ramifiée à groupe de Galois isomorphe à Γ, où k et Γ vérifient les hypothèses du Théorème 2.3.1. Rappelons que nous notons par k_1 le sous-corps de N fixe par C_l ; on a : k_1/k est galoisienne et $\mathrm{Gal}(k_1/k) \simeq C_q$. Soit a une base du $k[\Gamma]$-module N. Pour tout idéal premier $\mathfrak{p}$ de O_k, soit $\alpha_\mathfrak{p}$ une base du $O_{k,\mathfrak{p}}[\Gamma]$-module $\mathcal{A}_{N/k,\mathfrak{p}}$.

Soit i, $0 \leq i \leq 1$. Les égalités suivantes découlent facilement de la définition des résolvantes de Fröhlich-Lagrange :

$$\langle \alpha_\mathfrak{p}, \psi_i \rangle = \langle \mathrm{Tr}_{N_\mathfrak{p}/(k_1)_\mathfrak{p}}(\alpha_\mathfrak{p}), \chi_i \rangle_{k_1/k}, \quad \langle a, \psi_i \rangle = \langle \mathrm{Tr}_{N/k_1}(a), \chi_i \rangle_{k_1/k}.$$

Il est facile de voir que $\mathrm{Tr}_{N_\mathfrak{p}/(k_1)_\mathfrak{p}}(\alpha_\mathfrak{p})$ et $\mathrm{Tr}_{N/k_1}(a)$ sont des bases respectives du $O_{k,\mathfrak{p}}[C_q]$-module $\mathcal{A}_{k_1/k,\mathfrak{p}}$ et du $k[C_q]$-module k_1. Signalons que $\mathrm{Tr}_{N/k_1}(\mathcal{A}_{N/k}) = \mathcal{A}_{k_1/k}$.

Un résultat de Fröhlich (voir [Frö76, Théorème 10 et (5.12), p. 401] ou [Frö77, Theorem 12, p. 165]) donne un lien entre la résolvante d'un caractère et celle de son caractère induit pour les anneaux d'entiers de corps de nombres. Une démonstration plus détaillée et son énoncé se trouvent dans [BS13, Lemme 2.4.1, Corollaire 2.4.3, pp. 315–318].

Brièvement, le Lemme 2.4.1 se généralise de la manière suivante. Dans ses notations, soient H un sous-groupe de $\mathrm{Gal}(N/k)$ et $F = N^H$; ce lemme reste vrai en remplaçant :

- O_N en tant que $O_k[\Gamma]$-module par un idéal ambige A dans N/k en tant que $O_k[\Gamma]$-module de la forme (multiplicative) $A = BA'$, où B (resp. A') est un idéal fractionnaire de F (resp. N).

- O_N en tant que $O_F[H]$-module par A' en tant que $O_F[H]$-module (noter que A' est un idéal ambige dans N/F).

- O_F par B.

En particulier, le lemme généralisé s'applique à $\mathcal{A}_{N/k}$ puisque $\mathcal{A}_{N/k} = \mathcal{A}_{k_1/k}\mathcal{A}_{N/k_1}$ (ici $H = C_l$, $F = k_1$, $B = \mathcal{A}_{k_1/k}$, $A' = \mathcal{A}_{N/k_1}$).

Soient b et $b_{\mathfrak{p}}$ des bases respectives du $k_1[C_l]$-module N et du $O_{k_1,\mathfrak{p}}[C_l]$-module $\mathcal{A}_{N/k_1,\mathfrak{p}}$. Soit S un système de représentants des classes d'équivalence des éléments de $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$ modulo $\mathrm{Gal}(\overline{\mathbb{Q}}/k_1)$.

Comme $\chi = \mathrm{Ind}_{C_l}^{\Gamma} \psi$, on déduit du lemme généralisé qu'il existe λ et $\lambda_{\mathfrak{p}}$ des éléments inversibles respectifs des anneaux $k[C_l]$ et $O_{k,\mathfrak{p}}[C_l]$ tels que :

$$\langle a, \chi\rangle\psi(\lambda) = \mathfrak{N}_{k_1/k}(\langle b, \psi\rangle_{N/k_1}) e(k_1/k)^{\deg\psi=1},$$

et

$$\langle \alpha_{\mathfrak{p}}, \chi\rangle\psi(\lambda_{\mathfrak{p}}) = \mathfrak{N}_{k_1/k}(\langle b_{\mathfrak{p}}, \psi\rangle_{N/k_1}) e((k_1)_{\mathfrak{p}}/k_{\mathfrak{p}})^{\deg\psi=1},$$

où ψ a été prolongé par linéarité à $k_{\mathfrak{p}}[C_l]$, $e(k_1/k)^2$ est le discriminant d'une base du k-espace vectoriel k_1, $e((k_1)_{\mathfrak{p}}/k_{\mathfrak{p}})^2 O_{k,\mathfrak{p}} = \Delta(\mathcal{A}_{k_1/k}) O_{k,\mathfrak{p}}$, où $\Delta(\mathcal{A}_{k_1/k})$ est le discriminant du réseau $\mathcal{A}_{k_1/k}$ par rapport à la forme trace $\mathrm{Tr}_{k_1/k}$ (c'est une modification du résultat de Fröhlich, dans lequel $e((k_1)_{\mathfrak{p}}/k_{\mathfrak{p}})^2 O_{k,\mathfrak{p}} = \Delta(k_1/k) O_{k,\mathfrak{p}}$, voir [BS13, Remarque 2.4.2, p. 16]), et

$$\mathfrak{N}_{k_1/k}(\langle x, \psi\rangle_{N/k_1}) = \prod_{\gamma\in S} \gamma(\langle x, \gamma^{-1}\psi\rangle_{N/k_1}).$$

Supposons que k_1/k et $k(\xi_l)/k$ soient linéairement disjointes. On peut donc choisir un prolongement $\overline{\tau}$ de τ à $\overline{\mathbb{Q}}$ vérifiant $\overline{\tau}(\xi_l) = \xi_l$. Il est clair qu'on peut supposer $S = \{\overline{\tau}^i, 0 \leq i \leq q-1\}$. Alors

$$\mathfrak{N}_{k_1/k}(\langle x, \psi\rangle_{N/k_1}) = \prod_{\gamma\in S} \gamma(\langle x, \psi\rangle_{N/k_1}) = \prod_{i=0}^{q-1} \overline{\tau}^i(\langle x, \psi\rangle_{N/k_1}).$$

Une démonstration similaire à celle de la Proposition 2.1 dans [SS10] nous donne :

Proposition 2.3.3. *Sous les hypothèses et notations ci-dessus, un représentant de la classe de* $\mathcal{M} \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k}$ *dans* $\mathrm{Cl}(\mathcal{M})$ *est l'élément* f *de* $\mathrm{Hom}_{\Omega_k}(R_\Gamma, J(\overline{k}))$ *défini par :*

$$f(\psi_0) = (1)$$
$$f(\psi_1) = \left(\frac{\langle \mathrm{Tr}_{N_{\mathfrak{p}}/(k_1)_{\mathfrak{p}}}(\alpha_{\mathfrak{p}}), \chi_i\rangle_{k_1/k}}{\langle \mathrm{Tr}_{N/k_1}(a), \chi_i\rangle_{k_1/k}}\right)_{\mathfrak{p}}$$
$$f(\chi) = \left(\frac{e((k_1)_{\mathfrak{p}}/k_{\mathfrak{p}})}{e(k_1/k)} \prod_{i=0}^{q-1} \overline{\tau}^i \left(\frac{\langle b_{\mathfrak{p}}, \psi\rangle_{N/k_1}}{\langle b, \psi\rangle_{N/k_1}}\right)\right)_{\mathfrak{p}}$$

Nous allons utilisé les résultats et notations de [SS10, pp. 1825–1826] pour énoncer une proposition analogue à [SS10, Proposition 2.2].

Il découle de k_1/k et $k(\xi_l)/k$ linéairement disjointes que $\mathrm{Gal}(k_1(\xi_l)/k)$ est isomorphe à $\mathrm{Gal}(k(\xi_l)/k) \times \mathrm{Gal}(k_1/k)$. On peut donc noter

$$\mathrm{Gal}(k_1(\xi_l)/k) = \{s_i \tau^j \mid \ 1 \leq i \leq l-1, 0 \leq j \leq q-1\}.$$

Soit Z/k la sous-extension de $k_1(\xi_l)/k$ fixe par τs_r. Alors :
- Z/E_0 et $k(\xi_l)/E_0$ sont linéairement disjointes et

$$\mathrm{Gal}(Z/E_0) \simeq \mathrm{Gal}(k_1(\xi_l)/k(\xi_l))(\simeq \mathrm{Gal}(k_1/k)).$$

- Z/k et k_1/k sont linéairement disjointes, et

$$\mathrm{Gal}(Z/k) \simeq \mathrm{Gal}(k_1(\xi_l)/k_1) \simeq \mathrm{Gal}(k(\xi_l)/k)(= S_l).$$

Les extensions N/k et $k(\xi_l)/k$ sont linéairement disjointes. Donc $\mathrm{Gal}(N(\xi_l)/k)$ est isomorphe à $\mathrm{Gal}(N/k) \times \mathrm{Gal}(k(\xi_l)/k)$.

On a les isomorphismes de restriction :

$$\begin{gathered}\mathrm{Gal}(N(\xi_l)/N) \simeq \mathrm{Gal}(k_1(\xi_l)/k_1) \simeq \mathrm{Gal}(k(\xi_l)/k) = S_l,\\ \mathrm{Gal}(N(\xi_l)/k(\xi_l)) \simeq \mathrm{Gal}(N/k) = \langle\sigma,\tau\rangle,\\ \mathrm{Gal}(N(\xi_l)/k_1(\xi_l)) \simeq \mathrm{Gal}(N/k_1) = \langle\sigma\rangle = C_l,\\ \mathrm{Gal}(k_1(\xi_l)/k(\xi_l)) \simeq \mathrm{Gal}(k_1/k) \simeq C_q = \langle\tau\rangle.\end{gathered}$$

Soit K_0/k la sous-extension de degré l de N/k fixe par $\langle\tau\rangle$. Il existe $b \in K_0$ (donc $\tau(b) = b$) telle que $(g(b))_{g\in C_l}$ est une base normale de N/k_1.

On a $\langle b,\psi\rangle^l_{N/k_1}$ est un élément de Z et

$$\langle b,\psi\rangle^l_{N/k_1} O_Z = (I(\psi))^l \theta_l J_1(\psi),$$

où $I(\psi)$ est un idéal fractionnaire de Z, et les $s_i\,(J_1(\psi))$, $1 \le i \le l-1$, sont des idéaux entiers de O_Z, sans facteur carré et premiers entre eux deux à deux.

La décomposition de Wedderburn de l'algèbre semi-simple $k[C_q]$ en un produit d'algèbres simples est la suivante :

$$k[C_q] \simeq \prod_{i=0}^{1} k(\chi_i) = k \times k(\xi_q).$$

Soit $\mathcal{M}(k[C_q])$ l'ordre maximal de O_k dans $k[C_q]$. Alors :

$$\mathrm{Cl}(\mathcal{M}(k[C_q])) \simeq \mathrm{Cl}(k) \times \mathrm{Cl}(k(\xi_q)),$$

et donc

$$\mathrm{Cl}^\circ(\mathcal{M}(k[C_q])) \simeq \mathrm{Cl}(k(\xi_q)).$$

Proposition 2.3.4. *Soient c_i, $0 \le i \le 2$, les composantes de $[\mathcal{M} \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k}]$ dans $\mathrm{Cl}(\mathcal{M}) \simeq \mathrm{Cl}(k) \times \mathrm{Cl}(k(\xi_q)) \times \mathrm{Cl}(E_0)$. Alors :*

(1) *c_0 est la classe triviale dans $\mathrm{Cl}(k)$.*

(2) c_1 *est la classe de* $[\mathcal{M}(k[C_q]) \otimes_{O_k[C_q]} \mathcal{A}_{k_1/k}]$ *dans* $\mathrm{Cl}(k(\xi_q))$.

(3) $c_2 = N_{Z/E_0}\left((\mathrm{cl}_Z(I(\psi)RJ_1(\psi))^{-1})\right)$ *dans* $\mathrm{Cl}(E_0)$.

Démonstration. (1) C'est évident.

(2) La démonstration est analogue à celle de l'assertion (ii) de la Proposition 2.2 dans [SS10, p. 1828].

(3) La preuve consiste en la détermination de la classe du contenu de l'idèle suivant, lequel est défini dans la Proposition 2.3.3 :

$$f(\chi) = \left(\frac{e((k_1)_\mathfrak{p}/k_\mathfrak{p})}{e(k_1/k)} \prod_{i=0}^{m-1} \overline{\tau}^i \left(\frac{\langle b_\mathfrak{p}, \psi \rangle_{N/k_1}}{\langle b, \psi \rangle_{N/k_1}} \right) \right)_\mathfrak{p}.$$

Comme dans le Lemme 2.2.2, on peut écrire d'une manière unique :

$$\langle b, \psi \rangle_{N/k_1}^l O_{k_1(\xi)} = (I'(\psi))^l \theta J_1'(\psi),$$

où $I'(\psi)$ est un idéal fractionnaire de $k_1(\xi_l)$, et les $s_i J_1'(\psi)$, $1 \leq i \leq (l-1)$, sont des idéaux entiers de $O_{k_1(\xi_l)}$, sans facteur carré et premiers entre eux deux à deux.

La classe dans $\mathrm{Cl}(k_1(\xi_l))$ du contenu de l'idèle $(\langle b_\mathfrak{p}, \psi \rangle_{N/k_1} / \langle b, \psi \rangle_{N/k_1})_\mathfrak{p}$ est la classe de l'idéal fractionnaire

$$\langle \mathcal{A}_{N/k_1}, \psi \rangle_{N/k_1} / \langle b, \psi \rangle_{N/k_1}.$$

Mais la classe de ce dernier dans $\mathrm{Cl}(k_1(\xi_l))$ est égale à $\mathrm{cl}_{k_1(\xi_l)}(I'(\psi)RJ_1'(\psi))^{-1}$ par le Lemme 2.2.3.

Par [SS10, Lemme 2.3], $I'(\psi) = I(\psi)O_{k_1(\xi_l)}$ et $J_1'(\psi) = J_1(\psi)O_{k_1(\xi_l)}$.

Comme dans le troisième paragraphe de la démonstration de l'assertion (iii) de la Proposition 2.2 dans [SS10, p. 1828], on obtient : la classe $N_{Z/E_0}\left((\mathrm{cl}_Z(I(\psi)RJ_1(\psi))^{-1})\right)$ dans $\mathrm{Cl}(E_0)$ est celle du contenu de l'idèle $(\prod_{i=0}^{q-1} \overline{\tau}^i (\langle b_\mathfrak{p}, \psi \rangle_{N/k_1} / \langle b, \psi \rangle_{N/k_1}))_\mathfrak{p}$.

Soit I l'idéal fractionnaire de k qui est le contenu de l'idèle $(e((k_1)_\mathfrak{p}/k_\mathfrak{p})/e(k_1/k))_\mathfrak{p}$. De $e(k_1/k)^2$ est le discriminant d d'une base du k-espace vectoriel k_1 et $e((k_1)_\mathfrak{p}/k_\mathfrak{p})^2 O_{k,\mathfrak{p}} = \Delta(\mathcal{A}_{k_1/k}) O_{k,\mathfrak{p}}$ on déduit :

$$I^2 = \frac{\Delta(\mathcal{A}_{k_1/k})}{d}.$$

Donc $\mathrm{Cl}_k(I) = \mathrm{cl}_k(\mathcal{A}_{k_1/k})$. Par la Proposition 2.1.1, $\mathrm{cl}_k(\mathcal{A}_{k_1/k}) = 1$. Donc $\mathrm{Cl}_k(I) = 1$. □

Maintenant nous pouvons démontrer le Théorème 2.3.1 et le Corollaire 2.3.2.

Démonstration du Théorème 2.3.1. Rappelons qu'on veut montrer l'égalité $\mathcal{R}_1(\mathcal{M}) = A$, où A est le sous-ensemble de $\mathrm{Cl}(k(\xi_q)) \times \mathrm{Cl}(E_0)$ suivant :

$$A = (\mathcal{S}_q)_* \mathrm{Cl}(k(\xi_q) \times (\mathcal{S}_l)_* \mathrm{Cl}(E_0).$$

(1) Montrons l'inclusion $\mathcal{R}_1(\mathcal{M}) \subset A$.

On utilise les hypothèses et notations de la Proposition 2.3.4. Par le Théorème 2.2.1, $c_1 \in (\mathcal{S}_q)_* \operatorname{Cl}(k(\xi_q))$. D'une façon analogue à la démonstration du Théorème 2.2.1, partie (1), on obtient la classe de $I_*(\psi)^{-1} = I(\psi)RJ_1(\psi))^{-1}$ appartient à $(\mathcal{S}_l)_* \operatorname{Cl}(Z)$. Par suite $c_2 \in (\mathcal{S}_l)_* \operatorname{Cl}(E_0)$.

(2) Montrons l'inclusion $A \subset \mathcal{R}_1(\mathcal{M})$.

Soit $X = (c_1, c_2)$ un élément de A. Tout d'abord on considère l'élément c_1. La remarque après la fin de la démonstration de la partie (2) du Théorème 2.2.1 nous affirme l'existence d'une extension modérée k_1/k à groupe de Galois isomorphe à $C_q = \langle\tau\rangle$, telle que $[\mathcal{M}(C_q) \otimes_{O_k[C_q]} \mathcal{A}_{k_1/k}] = c_1$, k_1/k est ramifiée en une place finie (donc la seule sous-extension de k_1/k non ramifiée sur k est k lui-même puisque son degré est premier), et dont le discriminant est premier à lO_k. Signalons que la dernière condition sur le discriminant implique que k_1/k et $k(\xi_l)/k$ sont linéairement disjointes.

Notons

$$\operatorname{Gal}(k_1(\xi_l)/k) = \{s_i\tau^j \mid \ 1 \leq i \leq l-1, 0 \leq j \leq q-1\}.$$

Soit Z le sous-corps de $k_1(\xi_l)/k$ fixe par $\langle\tau s_r\rangle$. Par [SS10, Proposition 2.4] toute sous-extension de Z/E_0 différente de E_0 est ramifiée. Ce dernier fait entraîne que N_{Z/E_0} : $\operatorname{Cl}(Z) \to \operatorname{Cl}(E_0)$ est surjective grâce à [Was97, Théorème 10.1, p. 400]. On en déduit que N_{Z/E_0} induit un morphisme surjectif de $(\mathcal{S}_l)_* \operatorname{Cl}(Z)$ sur $(\mathcal{S}_l)_* \operatorname{Cl}(E_0)$.

Ensuite on considère l'élément c_2 de $(\mathcal{S}_l)_* \operatorname{Cl}(E_0)$. Soit $y \in (\mathcal{S}_l)_* \operatorname{Cl}(Z)$ vérifiant

$$N_{Z/E_0}(y) = c_2.$$

D'après l'assertion (1) du Lemme 2.2.6, il existe un entier j, des idéaux fractionnaires I_i de Z, $1 \leq i \leq j$, qu'on peut choisir premiers avec lO_Z par le théorème de densité de Chebotarev, et des éléments $\mathfrak{s}'_i$, $1 \leq i \leq j$, de $\mathcal{S}'$ tels que :

$$I = \prod_{i=1}^{j} (1/l)\mathfrak{s}'_i(\theta_l)_* I_i, \quad \text{et } y = \operatorname{cl}_Z(I) \text{ dans } \operatorname{Cl}(Z).$$

Posons $J = \prod_{i=1}^{j} \mathfrak{s}'_i I_i$. Alors :

$$I^l = (\theta_l)_* J.$$

Soit le cycle $\mathcal{C} = l^2 O_Z$. Soit $\operatorname{Cl}(Z, \mathcal{C})$ le groupe des classes de rayon de Z modulo $\mathcal{C}$. Par la surjection canonique de $\operatorname{Cl}(Z, \mathcal{C})$ sur $\operatorname{Cl}(Z)$ et le théorème de densité de Chebotarev, il existe un idéal premier $\mathfrak{p}$ de O_Z, totalement décomposé dans Z/k et tel que $\operatorname{cl}_Z(\mathfrak{p}) = \operatorname{cl}_Z(J)$ dans $\operatorname{Cl}(Z, \mathcal{C})$. Il s'ensuit qu'il existe $\alpha' \in Z$ satisfaisant :

$$\mathfrak{p} = \alpha' J \text{ for } \alpha' \equiv 1 \bmod^* l^2 O_Z.$$

Posons

$$\alpha = \theta_l \alpha'.$$

Comme $(\theta_l)_* = \theta_l - lR$, on a :

$$\alpha O_Z = ((IRJ)^{-1})^l \theta \mathfrak{p}.$$

On continue exactement comme dans les pages [SS10, pp. 1831–1832] (avec $\theta = \theta_l$ et $m = q$). Pour la convenance du lecteur, afin de faciliter la lecture de cette section on reprend de façon concise les principales idées de ces pages. Signalons qu'on a modifié les éléments α et α' de ces pages.

L'élément α n'est pas une puissance l-ième dans Z et dans $k_1(\xi_l)$.

Soit ω un élément d'une clôture algébrique de k vérifiant $\omega^l = \alpha$. Posons $L = k_1(\xi_l)(\omega)$. Alors $L/k_1(\xi_l)$ est une extension cyclique (de Kummer) de degré l.

Rappelons que ψ est un caractère de degré 1 et d'ordre l du groupe C_l. Chosissons un générateur σ de C_l tel que $\psi(\sigma) = \xi_l$. Ensuite identifions C_l avec $\mathrm{Gal}(L/k_1(\xi_l))$ en faisant agir σ sur L de sorte que $\sigma(\omega) = \xi_l \omega$.

On montre que L/k_1 est galoisienne abélienne de degré $l(l-1)$. D'où l'existence d'une sous-extension galoisienne N/k_1 de L/k_1 de degré l.

On montre aussi que N/k est galoisienne modérée à groupe de Galois isomorphe à Γ.

Soit K/k la sous-extension de degré l de N/k fixe par $\langle\tau\rangle$. Soit b un élément de K engendrant une base normale de N/k_1. On a $L = k_1(\xi_l)(\langle b, \psi\rangle)$. Par la théorie de Kummer, il existe $g \in k_1(\xi_l)$ et i, $1 \leq i \leq (l-1)$, tels que $\alpha = g^l \langle b, \psi\rangle^{li}$. On montre que $i = 1$, car $\sigma(\omega) = \xi_l \omega$. Donc

$$\alpha = g^l \langle b, \psi\rangle^l.$$

Mais $\langle b, \psi\rangle^l \in Z$ et $\alpha \in Z$, par suite $g \in Z$ (sinon $Z(g)/Z$ serait une sous-extension de $k_1(\xi_l)/Z$ de degré l, et l diviserait q). En utilisant la décomposition (de façon unique) $\alpha O_Z = ((IRJ)^{-1})^l \theta \mathfrak{p}$ on obtient :

$$\langle b, \psi\rangle^l O_Z = ((gIRJ)^{-1})^l \theta \mathfrak{p}$$

est la décomposition (de façon unique) de $\langle b, \psi\rangle^l O_Z$.

Par l'assertion (3) de la Proposition 2.3.4 : la composante X de la classe de $\mathcal{M} \otimes_{O_k[\Gamma]} \mathcal{A}_{N/k}$ dans $\mathrm{Cl}(E_0)$ est

$$\begin{aligned} X &= N_{Z/E_0}\left(\mathrm{cl}_Z((gIRJ)^{-1} R\mathfrak{p})^{-1})\right) \\ &= N_{Z/E_0}\left(\mathrm{cl}_Z(I)\,\mathrm{cl}_Z(RJ)\,\mathrm{cl}_Z(R\mathfrak{p})^{-1}\right). \end{aligned}$$

Rappelons que $\mathrm{cl}_Z(\mathfrak{p}) = \mathrm{cl}_Z(J)$, $y = \mathrm{cl}_Z(I)$ et $N_{Z/E_0}(y) = c_2$. Alors

$$X = N_{Z/E_0}(\mathrm{cl}_Z(I)) = c_2.$$

Donc $A \subset \mathcal{R}_1(\mathcal{M})$. Ceci termine la démonstration du Théorème 2.3.1. □

Démonstration du Corollaire 2.3.2. (1) Soit N/k une Γ-extension domestique. Comme l est non ramifié dans $k/\mathbb{Q}$, il est immédiat que les premiers au dessus de l dans O_k sont totalement ramifiés dans $k(\xi_l)/k$. Puisque ces derniers sont non ramifiés dans k_1/k, on obtient k_1/k et $k(\xi_l)/k$ sont linéairement disjointes. Par suite, $\mathcal{R}_d(\mathcal{A},\mathcal{M}) \subset \mathcal{R}_1(\mathcal{A},\mathcal{M})$.

(2) Pour l'autre inclusion, on suit la partie (2) de la démonstration du Théorème 2.3.1 en faisant quelques modifications.

On garde k_1/k ; elle est non ramifiée en l et q. Ensuite on remplace le cycle $\mathcal{C} = l^2 O_Z$ par $\mathcal{C} = l^2 q O_Z$. L'extension N/k_1 obtenue a pour discriminant $((\mathfrak{p}O_{k_1(\xi_l)}) \cap O_{k_1})^{l-1}$, donc elle est aussi non ramifiée en l et q. On conclut que N/k est domestique. On en déduit $\mathcal{R}_1(\mathcal{A},\mathcal{M}) \subset \mathcal{R}_d(\mathcal{A},\mathcal{M})$. Ce qui termine la démonstration du corollaire. □

2.4 Une généralisation non explicite du Théorème 2.3.1

Dans toute cette section : l (resp. m) est un nombre premier impair (resp. un entier naturel impair), Γ est un groupe métacyclique non abélien d'ordre lm (comme dans [SS10, p. 1819]). Le groupe Γ est un produit semi-direct des groupes cycliques $C_l = \langle\sigma\rangle$ et $C_m = \langle\tau\rangle$ et l'action de C_m sur C_l est fidèle :

$$\Gamma = C_l \rtimes C_m.$$

On peut le définir par la présentation suivante :

$$\Gamma = \langle \sigma, \tau : \sigma^l = \tau^m = 1, \tau\sigma\tau^{-1} = \sigma^r \rangle,$$

où r est un entier, avec $1 \leq r \leq (l-1)$, et la classe de r dans $(\mathbb{Z}/l\mathbb{Z})^*$ est d'ordre m.

Supposons $k/\mathbb{Q}$ et $\mathbb{Q}(\xi_l)/\mathbb{Q}$ linéairement disjointes. D'après [SS10, p. 1821]

$$\mathrm{Cl}^\circ(\mathcal{M}(k[\Gamma])) \simeq \mathrm{Cl}^\circ(\mathcal{M}(k[C_m])) \times \mathrm{Cl}(E_0).$$

On définit $\mathcal{R}_1(\mathcal{A},\mathcal{M}(k[\Gamma]))$ et $\mathcal{R}_d(\mathcal{A},\mathcal{M}(k[\Gamma]))$ comme dans la section 2.3 en remplaçant q par m. D'après [Tsa16, Théorème 1.3], $\mathcal{R}(\mathcal{A},\mathcal{M}(k[C_m]))$ est un sous-groupe de $\mathrm{Cl}^\circ(\mathcal{M}(k[C_m]))$.

Théorème 2.4.1. *Supposons les extensions $k/\mathbb{Q}$ et $\mathbb{Q}(\xi_l)/\mathbb{Q}$ linéairement disjointes. Identifions $\mathrm{Cl}^\circ(\mathcal{M}(k[\Gamma]))$ avec $\mathrm{Cl}^\circ(\mathcal{M}(k[C_m])) \times \mathrm{Cl}(E_0)$. Alors, $\mathcal{R}_1(\mathcal{A},\mathcal{M}(k[\Gamma]))$ est le sous-groupe de $\mathrm{Cl}^\circ(\mathcal{M}(k[\Gamma]))$ suivant :*

$$\mathcal{R}_1(\mathcal{A},\mathcal{M}(k[\Gamma])) = \mathcal{R}(\mathcal{A},\mathcal{M}(k[C_m])) \times (\mathcal{S}_l)_* \,\mathrm{Cl}(E_0).$$

Démonstration. Elle est similaire à celle du Théorème 2.3.1, avec les modifications suivantes.

On remplace l'assertion (2) de la Proposition 2.3.4 par : c_1 est la classe de

$$[\mathcal{M}(k[C_m]) \otimes_{O_k[C_m]} \mathcal{A}_{k_1/k}]$$

dans $\mathrm{Cl}^\circ(\mathcal{M}(k[C_m]))$.

Maintenant on suit la démonstration du Théorème 2.3.1.

Dans la partie (1) on remplace "par le Théorème 2.2.1, $c_1 \in (\mathcal{S}_q)_* \mathrm{Cl}(k(\xi_q)$", par : D'après [Tsa16, Théorème 1.3], $c_1 \in \mathcal{R}(\mathcal{A}, \mathcal{M}(k[C_m]))$.

Dans la partie (2), la seule modification concerne l'élément c_1.

Considérons c_1. Le [Tsa16, Théorème 1.3] nous affirme l'existence d'une extension modérée k_1/k à groupe de Galois isomorphe à $C_m = \langle\tau\rangle$, telle que $[\mathcal{M}(C_q) \otimes_{O_k[C_q]} \mathcal{A}_{k_1/k}] = c_1$, et dont le discriminant est premier à lO_k.

Mais la démonstration du [Tsa16, Théorème 1.3] est une adaptation de celle [McC87, Théorème 6.7]. Il n'est pas difficile de voir, que dans la preuve du [Tsa16, Preuve du Théorème 1.3, p.791], on peut trouver k_1/k satisfaisant en plus (comme dans [McC87, Théorème 6.7]) : la seule sous-extension de k_1/k non ramifiée est k, ce qui nous donne en utilisant [SS10, Proposition 2.4] : $N_{Z/E_0} : \mathrm{Cl}(Z) \to \mathrm{Cl}(E_0)$ est surjective.

On termine en continuant exactement comme dans la démonstration du Théorème 2.3.1. □

Corollaire 2.4.2. *Si l ne se ramifie pas dans k, alors $\mathcal{R}_d(\mathcal{A}, \mathcal{M}(k[\Gamma])) = \mathcal{R}_1(\mathcal{A}, \mathcal{M}(k[\Gamma]))$.*

Démonstration. Elle est similaire à celle du Corollaire 2.3.2.

La partie (1) est la même.

Dans la partie (2), on peut choisir k_1/k de discriminant premier à lmO_k par [Tsa16, Théorème 1.3]. Ensuite on remplace le cycle $\mathcal{C} = l^2O_Z$ par $\mathcal{C} = l^2mO_Z$. □

Bibliography

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[Art50] E. Artin, *Questions de base minimale dans la théorie des nombres algébriques*, Algèbre et Théorie des Nombres, Colloques Internationaux du Centre National de la Recherche Scientifique, no. 24, Centre National de la Recherche Scientifique, Paris, 1950, pp. 19–20.

[BDKN20] A. Bodin, P. Dèbes, J. König, and S. Najib, *The Hilbert-Schinzel specialization property*, 2020, Available at `http://arxiv.org/pdf/2009.07254.pdf`.

[BDN20] A. Bodin, P. Dèbes, and S. Najib, *The Schinzel hypothesis for polynomials*, Trans. Amer. Math. Soc. **373** (2020), no. 12, 8339–8364.

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

[BGS06] N.P. Byott, C. Greither, and B. Sodaïgui, *Classes réalisables d'extensions non abéliennes*, J. Reine Angew. Math. **601** (2006), 1–27.

[Bla99] E.V. Black, *On semidirect products and the arithmetic lifting property*, J. London Math. Soc. (2) **60** (1999), no. 3, 677–688.

[Bru09] C. Bruche, *Classes de Steinitz d'extensions non abéliennes de degré p^3*, Acta Arith. **137** (2009), no. 2, 177–191.

[BS13] N.P. Byott and B. Sodaïgui, *Realizable Galois module classes over the group ring for non abelian extensions*, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 1, 303–371.

[Dèb09] P. Dèbes, *Arithmétique des revêtements de la droite*, Available at `http://math.univ-lille1.fr/~pde/rev_www.pdf`, 2009.

[Eis95] D. Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry.

[Ere91] B. Erez, *The Galois structure of the square root of the inverse different*, Math. Z. **208** (1991), no. 2, 239–255.

[FGI+05] B. Fantechi, L. Göttsche, L. Illusie, S. L. Kleiman, N. Nitsure, and A. Vistoli, *Fundamental algebraic geometry*, Mathematical Surveys and Monographs, vol. 123, American Mathematical Society, Providence, RI, 2005, Grothendieck's FGA explained.

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

[Frö76] A. Fröhlich, *Arithmetic and Galois module structure for tame extensions*, J. Reine Angew. Math. **286(287)** (1976), 380–440.

[Frö77] ———, *Galois module structure*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), 1977, pp. 133–191.

[Frö83] ———, *Galois module structure of algebraic integers*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 1, Springer-Verlag, Berlin, 1983.

[Har77] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977, Graduate Texts in Mathematics, No. 52.

[Hec81] E. Hecke, *Lectures on the theory of algebraic numbers*, Graduate Texts in Mathematics, vol. 77, Springer-Verlag, New York-Berlin, 1981, Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen.

[Hoc10] M. Hochster, *Noether normalization and Hilbert's Nullstellensatz*, Available at `http://www.math.lsa.umich.edu/~hochster/615W10/supNoeth.pdf`, 2010.

[Leg16] F. Legrand, *Specialization results and ramification conditions*, Israel J. Math. **214** (2016), no. 2, 621–650.

[Liu02] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications.

[Lon71] R.L. Long, *Steinitz classes of cyclic extensions of prime degree*, J. Reine Angew. Math. **250** (1971), 87–98.

[Mar69] J. Martinet, *Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre* $2p$, Ann. Inst. Fourier (Grenoble) **19** (1969), no. fasc. 1, 1–80, ix.

[McC85] L.R. McCulloh, *Stickelberger ideals, monoid rings, and Galois module structure*, Orders and their applications (Oberwolfach, 1984), Lecture Notes in Math., vol. 1142, Springer, Berlin, 1985, pp. 190–204.

[McC87] ———, *Galois module structure of abelian extensions*, J. Reine Angew. Math. **375/376** (1987), 259–306.

[Mes90] Jean-François Mestre, *Extensions régulières de* $\mathbf{Q}(T)$ *de groupe de Galois* $\tilde{A}_n$, J. Algebra **131** (1990), no. 2, 483–495.

[Mil20] J.S. Milne, *Fields and Galois Theory*, Available at `http://www.jmilne.org/math/CourseNotes/FT.pdf`, 2020.

[Nar04] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, third ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008.

[Ser68] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[Sod88] B. Sodaïgui, *Structure galoisienne relative des anneaux d'entiers*, J. Number Theory **28** (1988), no. 2, 189–204.

[Sod97] ———, *Classes réalisables par des extensions métacycliques non abéliennes et éléments de Stickelberger*, J. Number Theory **65** (1997), no. 1, 87–95.

[SS10] F. Sbeity and B. Sodaïgui, *Classes réalisables d'extensions métacycliques de degré* lm, J. Number Theory **130** (2010), no. 8, 1818–1834.

[Tay81] M.J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. **63** (1981), no. 1, 41–79.

[Tsa16] C. Tsang, *On the Galois module structure of the square root of the inverse different in abelian extensions*, J. Number Theory **160** (2016), 759–804.

[Tsa17] ———, *Galois module structure of the square root of the inverse different over maximal orders*, Bull. Lond. Math. Soc. **49** (2017), no. 1, 71–88.

[Ull74] S. Ullom, *Integral representations afforded by ambiguous ideals in some abelian extensions*, J. Number Theory **6** (1974), 32–49.

[Völ96] H. Völklein, *Groups as Galois groups*, Cambridge Studies in Advanced Mathematics, vol. 53, Cambridge University Press, Cambridge, 1996, An introduction.

[Was97] L.C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

Abstract. In this thesis, we discuss two topics in number theory: the Hilbert specialization of parametrized varieties and the Galois module structure of the square root of the inverse different for metacyclic non-abelian extensions.

Hilbert specialization is an important tool in Field Arithmetic and Arithmetic Geometry, which has usually been intended for polynomials, hence hypersurfaces, and at scalar values. In the first part of this thesis, we extend this tool to prime ideals, hence affine varieties. Then we give an application to the study of the irreducibility of the intersection of varieties. Finally, encouraged by recent results, we consider the more general situation in which the specialization is done at polynomial values, instead of scalar values.

In the second part of the thesis we will study the Galois module structure of the square root of the inverse different. Given a number field K and a group Γ, we consider a tamely ramified Galois extension N/K of Galois group isomorphic to Γ. If we take Γ of odd order, we can define a fractional ideal of N called the *square root of the inverse different* $\mathcal{A}_{N/K}$. This fractional ideal is ambiguous, so it can be endowed in a natural way with an $O_K[\Gamma]$-module structure. Moreover, it is a locally free $O_K[\Gamma]$-module. So we can consider its class $[\mathcal{A}_{N/K}]$ in $\mathrm{Cl}(O_K[\Gamma])$, the class group of the locally free $O_K[\Gamma]$-modules. Now, let $\mathcal{M}$ be a maximal O_K-order in the semisimple algebra $K[\Gamma]$ containing $O_K[\Gamma]$ and $\mathrm{Cl}(\mathcal{M})$ its class group. Thus, we can consider the class $[\mathcal{M} \otimes_{O_K[\Gamma]} \mathcal{A}_{N/K}]$ in $\mathrm{Cl}(\mathcal{M})$. Denote by $\mathcal{R}(\mathcal{A}, O_K[\Gamma])$ and $\mathcal{R}(\mathcal{A}, \mathcal{M})$ the set of all the classes $[\mathcal{A}_{N/K}]$ and $[\mathcal{M} \otimes_{O_K[\Gamma]} \mathcal{A}_{N/K}]$, respectively, as N varies over all the tamely ramified extensions of K whose Galois group is isomorphic to Γ. We conjecture that $\mathcal{R}(\mathcal{A}, O_K[\Gamma])$ and $\mathcal{R}(\mathcal{A}, \mathcal{M})$ are subgroups of $\mathrm{Cl}(O_K[\Gamma])$ and $\mathrm{Cl}(\mathcal{M})$, respectively. Under suitable assumptions, we prove, first, that $\mathcal{R}(\mathcal{A}, \mathcal{M})$ is a subgroup of $\mathrm{Cl}(\mathcal{M})$ when Γ is a cyclic group of order an odd prime number. Then, when Γ is a non-abelian metacyclic group of odd order lq, for q an odd prime, we define a subset of $\mathcal{R}(\mathcal{A}, \mathcal{M})$ and, using the first result, we prove that it is a subgroup of $\mathrm{Cl}(\mathcal{M})$.

Résumé. Dans cette thèse, nous traitons de deux sujets en théorie des nombres : la spécialisation de Hilbert de variétés paramétrées et la structure galoisienne de la racine carrée de la codifférente d'extensions non abéliennes métacycliques.

La spécialisation de Hilbert est un outil important en Géométrie Arithmétique et en Arithmétique des Corps qui a généralement été appliqué aux polynômes, donc aux hypersurfaces, et en valeurs scalaires. Dans la première partie de cette thèse, nous étendons cet outil aux idéaux premiers, donc aux variétés affines. Nous donnons ensuite une application à l'étude de l'irréductibilité de l'intersection des variétés. Enfin, encouragé par des résultats récents, nous considérons la situation plus générale dans laquelle la spécialisation est faite en des valeurs polynomiales, au lieu de valeurs scalaires.

Dans la deuxième partie de la thèse, nous étudierons la structure galoisienne de la racine carrée de la codifférente. Étant donné un corps de nombres K et un groupe Γ, nous considérons une extension de Galois modérément ramifiée N/K à groupe de Galois isomorphe à Γ. Si nous prenons Γ d'ordre impair, nous pouvons définir un idéal fractionnaire de N qu'on appele la *racine carrée de la codifférente* $\mathcal{A}_{N/K}$. Cet idéal fractionnaire est ambige, il peut donc être muni de manière naturelle d'une structure de $O_K[\Gamma]$-module. De plus, c'est un $O_K[\Gamma]$-module localement libre. Donc nous pouvons considérer sa classe $[\mathcal{A}_{N/K}]$ dans $\mathrm{Cl}(O_K[\Gamma])$, le groupe des classes des $O_K[\Gamma]$-modules localement libres. Maintenant, soient $\mathcal{M}$ un O_K-ordre maximal dans l'algèbre semi-simple $K[\Gamma]$ contenant $O_K[\Gamma]$ et $\mathrm{Cl}(\mathcal{M})$ son group des classes. Ainsi, on peut considérer la classe $[\mathcal{M} \otimes_{O_K[\Gamma]} \mathcal{A}_{N/K}]$ dans $\mathrm{Cl}(\mathcal{M})$. On note $\mathcal{R}(\mathcal{A}, O_K[\Gamma])$ et $\mathcal{R}(\mathcal{A}, \mathcal{M})$ l'ensemble de toutes les classes $[\mathcal{A}_{N/K}]$ et $[\mathcal{M} \otimes_{O_K[\Gamma]} \mathcal{A}_{N/k}]$, respectivement, lorsque N varie parmi toutes les extensions modérément ramifiées de K à groupe de Galois isomorphe à Γ. On conjecture que $\mathcal{R}(\mathcal{A}, O_K[\Gamma])$ et $\mathcal{R}(\mathcal{A}, \mathcal{M})$ sont des sous-groupes de $\mathrm{Cl}(O_K[\Gamma])$ et $\mathrm{Cl}(\mathcal{M})$, respectivement. Sous des hypothèses appropriées, nous prouvons d'abord que $\mathcal{R}(\mathcal{A}, \mathcal{M})$ est un sous-groupe de $\mathrm{Cl}(\mathcal{M})$ lorsque Γ est un groupe cyclique d'ordre un nombre premier impair. Ensuite, quand Γ est un groupe métacyclique non abélien d'ordre impair lq, pour q un premier impair, on définit un sous-ensemble de $\mathcal{R}(\mathcal{A}, \mathcal{M})$ et, en utilisant le premier résultat, nous démontrons qu'il est un sous-groupe de $\mathrm{Cl}(\mathcal{M})$.