https://doi.org/10.15388/vu.thesis.726
https://orcid.org/0000-0002-2719-0903

VILNIUS UNIVERSITY

Mickaël Montessinos

The Explicit Isomorphism Problem on Global Fields

DOCTORAL DISSERTATION

Natural Sciences,
Mathematics N 001

VILNIUS 2025

This dissertation was written in 2020-2024 at Vilnius University.

Academic supservisor:
Prof. Habil. Dr. Artūras Dubickas (Vilnius University, Natural Sciences, Mathematics – N 001).
Academic consultant:
Prof. Dr. Paulius Drungilas (Vilnius University, Natural Sciences, Mathematics – N 001).

Dissertation Defence Panel:
Chairman – Prof. Habil. Dr. Antanas Laurinčikas (Vilnius University, Natural Sciences, Mathematics – N 001)
Members:
Prof. Dr. Igoris Belovas (Vilnius University, Natural Sciences, Mathematics – N 001),
Prof. Dr. Paulius Drungilas (Vilnius University, Natural Sciences, Mathematics – N 001),
Prof. Dr. Ramūnas Garunkštis (Vilnius University, Natural Sciences, Mathematics – N 001),
Assoc. Prof. Dr. Alar Leibak (Tallinn University of Technology, Natural Sciences, Mathematics - N 001).

The dissertation shall be defended at a public meeting of the Dissertation Defense Panel at 16:00 on the 24th of February 2025, in the auditorium 103 of the Faculty of Mathematics and Informatics of Vilnius University.
Address: Naugarduko str. 24, LT-03225, Vilnius, Lithuania.
Phone: +370052193050; e-mail: mif@mif.vu.lt.

The text of this dissertation can be accessed at the Library of Vilnius University, or on the website of Vilnius university: `www.vu.lt/naujienos/ivykiu-kalendorius`.

https://doi.org/10.15388/vu.thesis.726
https://orcid.org/0000-0002-2719-0903

VILNIAUS UNIVERSITETAS

Mickaël Montessinos

Išreikštinio izomorfizmo problema globaliuose kūnuose

DAKTARO DISERTACIJA

Gamtos mokslai,
Matematika N 001

VILNIUS 2025

Disertacija rengta 2020-2024 metais Vilniaus universitete.

Mokslinis vadovas:
Prof. habil. dr. Artūras Dubickas (Vilniaus universitetas, gamtos mokslai, matematika – N 001)
Mokslinis konsultantas:
Prof. dr. Paulius Drungilas (Vilniaus universitetas, gamtos mokslai, matematika – N 001)

Gynimo taryba:
Pirmininkas – Prof. habil. dr. Antanas Laurinčikas (Vilniaus universitetas, gamtos mokslai, matematika – N 001)
Nariai:
Prof. dr. Igoris Belovas (Vilniaus universitetas, gamtos mokslai, matematika – N 001),
Prof. dr. Paulius Drungilas (Vilniaus universitetas, gamtos mokslai, matematika – N 001),
Prof. dr. Ramūnas Garunkštis (Vilniaus universitetas, gamtos mokslai, matematika – N 001),
Doc. dr. Alar Leibak (Talino technikos universitetas, gamtos mokslai, matematika - N 001).

Disertacija ginama viešame Gynimo tarybos posėdyje 2025m. vasario 24, 16 valandą, Vilniaus universiteto Matematikos ir informatikos fakultete, 103 auditorijoje.
Adresas: Naugarduko g. 24, LT-03225, Vilnius, Lietuva.
Tel. +37052193050; el. paštas mif@mif.vu.lt.

Disertaciją galima peržiurėti Vilniaus universiteto bibliotekoje ir Vilniaus universiteto interneto svetainėje adresu
`www.vu.lt/lt/naujienos/ivykiu-kalendorius`.

"Careful. We don’t want to learn from this."

Bill Waterson

To the memory of Irena Toliušienė

Contents

Notations **10**

1 Introduction **13**
1.1 Research topic 13
1.2 Actuality 13
1.3 Aims 15
1.4 Main Results 15
1.5 Methods 18
1.6 Novelty 22
1.7 Dissemination 24
1.8 Publications 24
1.9 Structure of the thesis 25

Acknowledgments **27**

2 Computing in global fields **28**
2.1 Background on algebraic number theory 28
2.1.1 Local Field 28
2.1.2 Global Fields 31
2.1.3 The ring of integers of a number field 35
2.1.4 Global function fields 35
2.1.5 Étale algebras 39
2.1.6 Lattices and orders 46
2.2 Algorithms 46
2.2.1 Computational Model 47
2.2.2 Lattice reduction 48
2.2.3 Main algorithms for global fields 52

3 The explicit isomorphism problem **58**
3.1 Algebras and algorithms 58
3.1.1 Structure constants 58
3.1.2 The structure of algebras 59
3.1.3 Computing maximal orders 61
3.2 Central simple algebra 62
3.2.1 General properties 62
3.2.2 Algebraic presentations of central simple algebras . . . 66
3.3 Computational representations of central simple algebras . . . 76
3.3.1 Computational representations 76
3.3.2 Finding an algebraic representation of an algebra . . . 77
3.4 The explicit isomorphism problem and its variants 80
3.4.1 Problem statements and reductions 80
3.4.2 Algorithms for the explicit isomorphism problem . . . 83
3.4.3 Solving algebraic versions of the explicit isomorphism problem 83

4 Computational Amitsur cohomology and the explicit isomorphism problem **85**
4.1 Amitsur cohomology 85
4.2 Amitsur algebras 88
4.2.1 Embedding S into $A(S,c)$ 90
4.2.2 Amitsur cocycles give central simple algebras 92
4.2.3 Central simple algebras come from Amitsur cocycles . 93
4.2.4 Tensor product and product of cocycles 95
4.3 Computational results 98
4.3.1 Algorithmic representation of Amitsur algebras 99
4.3.2 Computing a cocycle representing a given algebra . . . 99
4.3.3 Trivialisation of Amitsur cocycles 102

5 Lattices pairs in global function fields **109**
5.1 Vector bundles and lattices 109
5.1.1 $\mathcal{O}_X$-lattices and $\mathcal{O}_R$-lattices 111
5.1.2 Cohomology of $\mathcal{O}_R$-lattices 113
5.1.3 Extensions of $\mathcal{O}_R$-lattices 115
5.1.4 Restriction and conorm of an $\mathcal{O}_R$-lattice 118
5.1.5 Indecomposable $\mathcal{O}_R$-lattices 120
5.2 Explicit computations with lattice pairs 122

5.2.1 Algorithmic representation of lattice pairs 122
5.2.2 Restriction and conorm of a lattice pair 124
5.2.3 Computing cohomology groups and extensions 126
5.2.4 Computing isomorphisms between lattice pairs 132
5.2.5 Algorithms for homomorphisms of lattice pairs 134
5.3 Applications 138
5.3.1 Maximal orders and the explicit isomorphism problem 138
5.3.2 Vector bundles on an elliptic curve 140
5.3.3 Algebraic geometry codes 143

Conclusions **147**

Santrauka (Summary in Lithuanian) **158**
Tyrimo objektas 158
Aktualumas 158
Tikslai 160
Pagrindinai rezultatai 160
Metodai 163
Naujumas 167
Išvada 169
Aprobacija 170
Publikacijos 170
Trumpai apie autorių 171

Publications by the author **173**

Notations

$\circ$ The composition operator for maps.

$\simeq$ The isomorphy relation.

$\oplus$ The direct sum operator.

$\otimes$ The tensor product operator.

$\times$ The direct product operator.

A_S The scalar extension S-algebra $A \otimes_R S$ for R a commutative ring, S a commutative R-algebra and A an R-algebra.

$A_{\geq 0}$ The set of nonnegative elements of A, where A is a subset of the real numbers.

$\mathbb{C}$ The field of complex numbers.

$\mathcal{D}(k)$ The divisor group of a global field k.

D^{op} The opposite algebra of D. The product of ab in D^{op} is the product ba of D.

deg The degree valuation, extended from the ring of polynomials to the field of rational functions. May also denote the degree of a central simple algebra, vector bundle, $\mathcal{O}_X$-lattice, $\mathcal{O}_R$-lattice, or of a lattice pair.

$E^\vee$ The dual of E, where E is a module (resp. vector bundle, sheaf of modules, lattice, lattice pair).

$\mathrm{End}(E)$ The algebra of endomorphisms of a module, vector bundle, $\mathcal{O}_X$-lattice, $\mathcal{O}_R$-lattice, or lattice pair E.

$\mathcal{E}nd(E)$ The vector bundle (resp. $\mathcal{O}_X$-lattice, $\mathcal{O}_R$-lattice, lattice pair) of endomorphisms of the vector bundle (resp. $\mathcal{O}_X$-lattice, $\mathcal{O}_R$-lattice, lattice pair) E.

f_* The pullback of f on coherent sheaves, where f is a morphism of schemes

f_* The pushforward of f on coherent sheaves, where f is a morphism of schemes

$\mathbb{F}_q$ The finite field with q elements, where q is a power of a prime integer.

$\overline{F}$ The Galois closure of a field F

$F((X))$ The field of formal power series $\sum_{n\geq\nu} a_n X^n$ with $\nu \in \mathbb{Z}$ and the coefficients a_n lying in the field F.

$F(X)$ The field of rational functions in one variable, with coefficients in the field F.

$F(X)_\infty$ The valuation ring of the degree valuation in a field of rational functions $F(X)$.

$\mathrm{Gal}(K/k)$ The Galois group of a Galois field extension K/k.

$GL_d(R)$ The group of invertible square matrices of size d with coefficients in R.

GRH The generalised Riemann hypothesis.

$\mathrm{Hom}(E, E')$ The algebra of homomorphisms between two vector bundles, $\mathcal{O}_X$-lattices, $\mathcal{O}_R$-lattices, or lattice pairs E and E'.

$\mathcal{H}om(E, E')$ The vector bundle (resp. $\mathcal{O}_X$-lattice, $\mathcal{O}_R$-lattice, lattice pair) of homomorphisms between the vector bundles (resp. $\mathcal{O}_X$-lattices, $\mathcal{O}_R$-lattices, lattice pairs) E and E'.

κ_k The residue field of a local field k.

$K^{\otimes n}$ The iterated n-fold tensor product $K \otimes_k K \otimes_k \ldots \otimes_k K$, when K is a k-algebra.

M_k The set of places of a global field. Superscrits na, a, fi, ∞ may indicate, respectively, the subset of non-archimedean places, archimedean places, finite places and infinite places.

$M_d(R)$ The R-algebra of square matrices of size d with coefficients in R.

$M_{m,n}(R)$ The R-algebra of matrices of size $m \times n$ with coefficients in R.

$[n]$ The set of integers $\{1, 2, \ldots, n\}$.

$[n]_0$ The set of integers $\{0, 1, \ldots, n\}$.

$\mathbb{N}$ The set of natural numbers $\{1, 2, \ldots\}$.

$N_{K/k}$ The norm map of the field extension K/k.

$\mathcal{O}_{fi}$ When k is an extension of a field of rational functions $F(X)$, $\mathcal{O}_{fi}$ is the integral closure of $F[X]$ in k.

$\mathcal{O}_\infty$ When k is an extension of a field of rational functions $F(X)$, $\mathcal{O}_{fi}$ is the integral closure of $F(X)_\infty$ in k.

$\mathcal{O}_{R_k}$ The ring of integral répartitions of a function field k. The subscript k may be omitted when the field is clear from context.

ord_P The normalized valuation associated to a non-archimedean place P of a global field.

$\mathcal{O}_X$ The structural sheaf of a scheme X.

$\mathbb{Q}$ The field of rational numbers.

$\mathbb{Q}_p$ The field of p-adic numbers.

$R^\times$ The group of units of the ring R.

$\mathbb{R}$ The field of real numbers.

R_k The ring of répartitions of a function field k. The subscript k may be omitted when the fiels is clear from context.

$R[X]$ The ring of polynomials with coefficients in the ring R.

$\mathrm{Tr}_{B/A}$ The trace map of A-Algebra B, when B is free as an A-module.

U_S The group of S-units of a global field.

$[V : k]$ The dimension of the k-vector space V.

$\mathbb{Z}$ The ring of integers.

Chapter 1

Introduction

1.1 Research topic

This work focuses on the explicit isomorphism problem and related algorithmic problems.

Problem 1.1.1 (The explicit isomorphism problem)**.** *Given a field k and a k-algebra A isomorphic to the matrix algebra $M_d(k)$ for some $d \in \mathbb{N}$, compute an explicit isomorphism $\varphi\colon A \to M_d(k)$.*

The explicit isomorphism problem is usually studied over a specific field or class of fields. In our case, we focus on solving the explicit isomorphism problem for global fields. That is, for number fields and global function fields, finite extensions of the rational function field $F(X)$, where F is a finite field.

As we find that vector bundles over normal projective curves are relevant in studying the explicit isomorphism problem over function fields, we also consider the algorithmic theory of such vector bundles.

1.2 Actuality

The explicit isomorphism problem emerges as a natural problem in computational representation theory. Given a k-algebra A, one may wish to describe its structure explicitly. That is, compute the Jacobson radical of A, and the decomposition of the semi-simple part of A as a sum of simple k-algebras, themselves isomorphic to some $M_n(D)$, for D a division k-algebra. In general, the hard part of this task is to find an isomorphism $A \to M_n(D)$ when A is simple. A general recipe for solving this problem is to identify the Brauer

class of D over its centre K/k, find structure constants for $M_d(D^{\mathrm{op}})$ and then compute an explicit isomorphism $A \otimes M_d(D^{\mathrm{op}}) \simeq M_{n^2}(K)$ [23, 37, 49].

Applications of the explicit isomorphism problem go beyond the mere computational theory of associative algebras. In arithmetic geometry, the problem is relevant for trivialising obstruction algebras in explicit descent over elliptic curves [19, 20, 22, 30] and computation of Cassel-Tate pairings [32, 96]. The problem also applies to the parametrisation of Severi-Brauer surfaces [24]. Recent work in algebraic complexity theory reduced the determinant equivalence test to the explicit isomorphism problem [35]. Finally, the explicit isomorphism problem over a rational function field $F(X)$ (F finite) is also relevant to error correcting codes [37].

In the case of a finite base field, Ronyái introduced a polynomial-time algorithm for the explicit isomorphism problem in [70].

Instances of the explicit isomorphism problem for $\mathbb{Q}$-algebras were first treated separately for small values of d. When $d = 2$, the problem reduces to finding a rational point on a projective conic [91, Theorem 5.5.4], which is solved for instance in [21]. Then, [24] presented a subexponential algorithm when $d = 3$ by finding a cyclic presentation and solving a cubic norm equation. The case $d = 4$ is tackled in [66] by reducing the problem to the case of quaternion algebras over $\mathbb{Q}$ and quadratic number fields and then solving a quadratic norm equation.

In [22], an algorithm was given and studied mostly for the cases $d = 3$ and $d = 5$. It was then generalised in [47, 49] to a K-algebra isomorphic to $M_d(K)$, where d is a natural number and K is a number field. The complexity of this last algorithm is polynomial in the size of the structure constants of the input algebra. However, it depends exponentially on d, the degree of K and the size of the discriminant of K.

In 2018, [46] exhibited a polynomial-time algorithm for the explicit isomorphism problem over $F(X)$, where F is a finite field.

For the case of fixed d and varying base field, [31, 54] independently gave an algorithm for an algebra isomorphic to $M_2(K)$, where K is a quadratic number field. The complexity of this algorithm is polynomial in the size of the discriminant of K.

While the methods of [46] are entirely algebraic, we argue in Section 5.3.1 that the main theoretical result supporting the algorithm admits a natural interpretation as a famous theorem of Grothendieck on the structure of vector bundles over the projective line. As Grothendieck's theorem does not hold for

function fields of higher genus, the method of [46] does not generalise directly to such fields. However, our geometric interpretation of this method suggests that progress may follow from existing results on the structure of vector bundles over normal projective curves of higher genus. This observation suggests the relevance of developing an algorithmic theory for representing vector bundles over normal projective curves using pairs of lattices.

1.3 Aims

This thesis presents new methods for solving the explicit isomorphism problem over global fields. Over number fields, we aim to provide a novel cohomological description of central simple algebras that is fit for practical computations and to study the impact of such a tool in solving the explicit isomorphism problem over number fields. Over function fields, we aim to develop an algorithmic theory of vector bundles, relying on the theory of lattices over maximal orders.

1.4 Main Results

For a field k and an étale k-algebra K, we define a group $Z^2_{Am}(k,K) \subset (K^{\otimes 3})^\times$, a subgroup $B^2_{Am}(k,K)$ and we consider the factor group $H^2_{Am}(k,K) = Z^2_{Am}(k,K)/B^2_{Am}(k,K)$. We then define the Amitsur algebra $A(K,c)$ for $c \in Z^2_{Am}(k,K)$ whose underlying k-vector space is $K^{\otimes 2}$, and prove the following classification result:

Theorem 1.4.1. *Let k be a field and let K be an étale k-algebra of dimension d. Let $c \in K^{\otimes 3}$. Then, $A(K,c)$ is a central simple k-algebra if and only if $c \in Z^2_{Am}(k,K)$. In this case, $A(K,c)$ has degree d and contains K as a maximal commutative subalgebra. Conversely, if A is a central simple k-algebra containing K as a maximal commutative subalgebra, there exists $c \in Z^2_{Am}(k,K)$ such that the algebra $A(K,c)$ is isomorphic to A.*

This yields an isomorphism $H^2_{Am}(k,K) \simeq \mathrm{Br}(K/k)$ with the relative Brauer group of K over k.

Fix a polynomial $\chi \in k[X]$ such that there is an isomorphism $K \simeq k[X]/(\chi(X))$. We consider the algebras $K_1 = k[X,Y]/(\chi(X),\chi(Y))$ and $K_2 = k[X,Y,Z]/(\chi(X),\chi(Y),\chi(Z))$. Observe that for $n \in [2]$, the algebra K_n is naturally isomorphic to $K^{\otimes n+1}$ and that its elements may be represented

computationally as residue classes of polynomials. We prove algorithmic results on Amitsur algebras:

Theorem 1.4.2. *Identifying elements of $Z^2_{Am}(k, K)$ with their images in K_2 and identifying $A(K, c)$ with K_1 as a k-vector space, we have the following results:*

1. *There is a polynomial algorithm which, given $\chi, c \in Z^2_{Am}(k, K)$, and α and β in $A(K, c)$, computes $\alpha\beta$;*

2. *There is a probabilistic polynomial algorithm which, given a central simple k-algebra A, computes a maximal commutative subalgebra $K \subset A$, a polynomial χ such that $K \simeq k[X]/(\chi(X))$, $c \in Z^2_{Am}(k, K)$ and an isomorphism of k-algebras from A to $A(K, c)$.*

As an application of our construction of Amitsur algebras, we prove the following result:

Theorem 1.4.3. *Under GRH, Algorithm 2 is a polynomial quantum algorithm that solves the explicit isomorphism problem over number fields.*

Let X be a normal projective curve over a finite field F, and let k be its function field. Let $\mathcal{O}_{fi}$ and $\mathcal{O}_\infty$ be the integral closures in k respectively of $F[X]$ and of $F(X)_\infty = \{R \in k(X) : \deg R \leq 0\}$. A lattice pair of rank n on k is the data of a projective $\mathcal{O}_{fi}$-submodule L_{fi} of k^n and a free $\mathcal{O}_\infty$-submodule L_∞ of k^n such that $kL_{fi} = kL_\infty = k^n$. We prove the following:

Theorem 1.4.4. *The category of vector bundles over X is equivalent to the category of lattice pairs of k.*

We provide a computational representation of lattice pairs over a function field k. We let LP be the functor from the category of vector bundles to that of lattice pairs discussed above. We then get several algorithmic results. Unless specified otherwise, in the theorem stated below, E and E' are vector bundles over X.

Theorem 1.4.5.

1. *There is a polynomial algorithm which, given* $\mathrm{LP}(E)$*, computes* $\mathrm{LP}(\det(E))$.

2. *There is a polynomial algorithm which, given* $\mathrm{LP}(E)$*, computes* $\deg(E)$.

3. *There is a polynomial algorithm which, given* $\mathrm{LP}(E)$ *and* $\mathrm{LP}(E')$*, computes* $\mathrm{LP}(E \otimes E')$.

4. *There is a polynomial algorithm which, given* $\mathrm{LP}(E)$ *and* $\mathrm{LP}(E')$*, computes* $\mathrm{LP}(E \oplus E')$.

5. *There is a polynomial algorithm which, given* $\mathrm{LP}(E)$*, computes* $\mathrm{LP}(E^\vee)$.

6. *There is a polynomial algorithm which, given* $\mathrm{LP}(E)$ *and* $\mathrm{LP}(E')$*, computes* $\mathrm{LP}(\mathcal{H}om(E, E'))$.

7. *Let* $f : Y \to X$ *be a morphism of normal projective curves. There is a polynomial algorithm which, given* $\mathrm{LP}(E)$ *for* E *a vector bundle over* Y*, computes* $\mathrm{LP}(f_*(E))$.

8. *Let* f *and* Y *be as above. There is a polynomial algorithm which, give* $\mathrm{LP}(E)$ *for* E *a vector bundle over* X*, computes the lattice pair* $\mathrm{LP}(f^*(E))$ *over the function field of* Y.

9. *There is a polynomial algorithm which, given* $\mathrm{LP}(E)$*, computes a basis of* $H^0(X, E)$.

10. *There is a polynomial algorithm which, given* $\mathrm{LP}(E)$*, computes a basis of* $H^1(X, E)$.

11. *There is a polynomial algorithm which, given* $\mathrm{LP}(E)$, $\mathrm{LP}(E')$ *and* $\xi \in H^1(\mathcal{H}om(E, E'))$*, computes* $\mathrm{LP}(E'')$*, where* E'' *is the extension of* E *by* E' *corresponding to* ξ.

12. *There is a polynomial algorithm which, given an oracle for computing Hermite normal form of pseudo matrices over* $\mathcal{O}_{fi}$*, lattice pairs* $\mathrm{LP}(E)$ *and* $\mathrm{LP}(E')$*, and a matrix representing* $\mathrm{LP}(f)$*, for a homomorphism* $f : E \to E'$*, computes* $\mathrm{LP}(\mathrm{Ker}(f))$.

13. *There is a polynomial algorithm which, given an oracle for computing Hermite normal form of pseudo matrices over* $\mathcal{O}_{fi}$*, lattice pairs* $\mathrm{LP}(E)$ *and* $\mathrm{LP}(E')$*, and a matrix representing* $\mathrm{LP}(f)$*, for a homomorphism* $f : E \to E'$*, computes* $\mathrm{LP}(\mathrm{Im}(f))$.

14. *There is a polynomial algorithm which, given an oracle for computing Hermite normal forms of pseudo-matrices over* $\mathcal{O}_{fi}$ *and a lattice pair* $\mathrm{LP}(E)$*, computes* $\mathrm{LP}(E_1), \ldots, \mathrm{LP}(E_r)$ *such that the vector bundles* $E_1, \ldots, E_r$ *are indecomposables, and an isomorphism* $\mathrm{LP}(f)$ *between* $\mathrm{LP}(E)$ *and* $\mathrm{LP}(E_1 \oplus \ldots \oplus E_r)$.

15. *There is a polynomial algorithm which, given an oracle for computing Hermite normal forms of pseudo-matrices over $\mathcal{O}_{fi}$, and two lattice pairs* $\mathrm{LP}(E)$ *and* $\mathrm{LP}(E')$*, decides whether E and E' are isomorphic and, if they are, computes an isomorphism* $\mathrm{LP}(f)$.

The algorithms for lattice pairs discussed above were all implemented as a package[1] for Sagemath. [89]

1.5 Methods

In [55], Theorem 1.4.1 is proved by showing that our construction of Amitsur algebras is equivalent to the construction of Brauer algebras, and then leveraging existing results on Brauer algebras, which appear in [51, Chapter 2]. In this work, we give a direct proof instead, as suggested in [55, Remark 3.8].

Let k be a global field, let R be an étale k-algebra and let S be an R-algebra which is étale over k and free as an R-module. Letting $S^{\otimes n}$ be the n-fold tensor product $S \otimes_R \ldots \otimes_R S$, we recall the definition of the Amitsur complex. For $n \in \mathbb{Z}_{\geq 0}$ and $i \in [n+1]_0$, we define the R-algebra homomorphisms

$$\begin{array}{rccc} \varepsilon_i^n\colon & S^{\otimes n+1} & \to & S^{\otimes n+2} \\ & a_0 \otimes \ldots \otimes a_n & \mapsto & a_0 \ldots a_{i-1} \otimes 1 \otimes a_i \otimes \ldots \otimes a_n \end{array}$$

and the group homomorphisms

$$\begin{array}{rccc} \partial_{Am}^n\colon & (S^{\otimes n+1})^\times & \to & (S^{\otimes n+2})^\times \\ & x & \mapsto & \prod_{i\in[n+1]_0} \varepsilon_i^n(x)^{-1^i}. \end{array}$$

The Amitsur complex of S over R is the following sequence of group homomorphisms:

$$S^\times \xrightarrow{\partial_{Am}^0} (S^{\otimes 2})^\times \xrightarrow{\partial_{Am}^1} (S^{\otimes 3})^\times \xrightarrow{\partial_{Am}^2} \ldots$$

For $n \in \mathbb{Z}_{\geq 0}$, we may then set $Z_{Am}^n(R,S) = \operatorname{Ker} \partial_{Am}^n$ and, if $n \geq 1$, $B_{Am}^n(R,S) = \operatorname{Im} \partial_{Am}^{n-1}$. If $c \in S^{\otimes 3}$, the Amitsur algebra $A(S,c)$ is defined as the R-module $S^{\otimes 2}$ with multiplication

$$xy = \mathrm{Tr}_1^1(\varepsilon_2^1(x)c\varepsilon_0^1(y)), \tag{1.1}$$

where Tr_1^1 is the trace map $S^{\otimes 3} \to S^{\otimes 2}$, where $S^{\otimes 3}$ is seen as a $S^{\otimes 2}$-algebra via the map $\varepsilon_1^1\colon S^{\otimes 2} \to S^{\otimes 3}$.

[1] `https://git.disroot.org/montessiel/vector-bundles-sagemath`

The various statements of Theorem 1.4.1 are proved by detailed algebraic computations, but a pivotal argument relies on the sequence of isomorphisms coming from extending scalars to S. That is, for any R-algebra A, we let A_S be the S-algebra $A \otimes_R S$. Then, we show that

$$A(S, c)_S \simeq A(S_S, c \otimes 1) \simeq \mathrm{End}_S(S_S).$$

Many results about $A(S, c)$ are then inherited from $\mathrm{End}_S(S_S)$.

Theorem 1.4.2 is proved in two parts. The existence of an algorithm for computing products in Amitsur algebras follows directly from the straightforward statement of Equation (1.1) and the fact that

$$\mathrm{Tr}_1^1(a_0 \otimes a_1 \otimes a_2) = \mathrm{Tr}_{S/R}(a_1)a_0 \otimes a_2.$$

In order to construct a representation of a given central simple algebra as an Amitsur algebra, we rely on two facts:

1. If A is a central simple k-algebra, elements $u \in A$ such that $K = k[u]$ is a maximal commutative subalgebra of A and $v \in A$ such that $A = KvK$ may be computed efficiently.

2. Once u, K, and v are given as above, we get an isomorphism $K^{\otimes 2} \simeq A$ sending $a_0 \otimes a_1$ to $a_0 v a_1$. Finding $c \in K^{\otimes 3}$ such that multiplication in A matches Equation (1.1) is then a matter of solving a system of linear equations.

The method to prove Theorem 1.4.3 relies on the existence of a polynomial quantum algorithm for computing groups of S-units in number fields [9]. We prove a theorem that generalises [29, Theorem 7] to our setting of Amitsur cohomology. That is, we prove that if $c \in B^2_{Am}(k, K)$, then there are certain sets $S^{(1)}, S^{(2)}$ of places respectively of $K^{\otimes 2}$ and $K^{\otimes 3}$ such that c lies in the group of $S^{(2)}$-units of $K^{\otimes 3}$ and a preimage a of c by ∂^1_{Am} lies in the group of $S^{(1)}$-units of $K^{\otimes 2}$. Since such groups of units are finitely generated abelian groups, the map ∂^1_{Am}, once restricted, may be seen as a linear map between $\mathbb{Z}$-modules, and one may compute a preimage using existing algorithms for linear algebra over $\mathbb{Z}$. We note that the dependence on GRH stems from the necessity for the $S^{(n)}$ to contain all the places lying above a set of places of K that generate its class group. GRH provides a polynomial upper bound on the minimal size of a set of generators of the class group of a number field and, therefore, of an étale algebra over a number field.

Our proof of a generalisation of [29, Theorem 7] follows the structure of Fieker's proof, but we face new difficulties owing to our more general setting. The fundamental lemma in the original proof, [29, Lemma 9], is a vanishing theorem of the H^1 group over the group of divisors of a number field. This generalises Hilbert's Theorem 90 on the triviality of the H^1 group of the multiplicative group of a field. In our case, we must handle both number fields and étale algebras over number fields. Therefore, we must introduce definitions of places and divisors for étale algebra and prove some primary results we could not locate in the literature.

Theorem 1.4.4 is straightforward to prove from definitions. Lattice pairs are convenient to represent computationally because $\mathcal{O}_{fi}$-lattices and $\mathcal{O}_\infty$-lattices are so. Indeed, $\mathcal{O}_{fi}$ is a Dedekind domain, so an $\mathcal{O}_{fi}$-lattice is of the form $\mathfrak{a}_1 x_1 \oplus \ldots \oplus \mathfrak{a}_n x_n$, where the $\mathfrak{a}_i$ are fractional $\mathcal{O}_{fi}$-ideals in k and the x_i form a basis of k^n. Such a lattice may be represented by the data of a matrix in $GL_n(k)$ and a tuple $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ of fractional $\mathcal{O}_{fi}$-ideals. Since the ring $\mathcal{O}_\infty$ is a PID, an $\mathcal{O}_\infty$-lattice admits a basis and may be represented by a matrix in $GL_n(k)$.

Several algorithms presented in Theorem 1.4.5 follow directly from definitions. Some others require more sophisticated methods, which we discuss below. In what follows, for a lattice pair L, we denote by L_{fi} the corresponding $\mathcal{O}_{fi}$-lattice and by L_∞ the corresponding $\mathcal{O}_\infty$-lattice.

- In Item 9, we compute the H^0 group of a lattice pair L. This algorithm is a generalisation of the Riemann-Roch problem for divisors of function fields. The method we use relies on the computation of the Popov reduced form of a matrix over $F(X)$ and is a generalisation of the method of [45]. We note that this method also serves in [46] for a pair of maximal orders in a $F(X)$-algebra, which is a particular case of lattice pair. As we prove that $H^0(L) = L_{fi} \cap L_\infty$, we compute the intersection of lattices using a Popov reduced basis of L_{fi} with respect to a basis of L_∞. A Popov reduced basis is analogous to an orthogonal basis of a $\mathbb{Z}$-module and allows for a straightforward computation of $L_{fi} \cap L_\infty$ as a set of small elements of L_{fi}.

- In Item 10, computing the 1st cohomology group $H^1(L)$ of a lattice pair L of rank n presents more difficulties. Adapting the approach from [94], the H^1 group of a lattice pair is defined as the quotient F-vector space $R_k^n/(L' + k^n)$, where R_k is the ring of répartitions of k, and L' is a certain

lattice contained in R_k^n and determined by L. This computation presents several difficulties: elements of R_k are infinite tuples of elements of k and are therefore not generally computationally representable. There is also no obvious way to check that representable elements of R_k^n lie in the same equivalence class or to produce a complete system of representatives. The most obvious way to circumnavigate these difficulties is to rely on Serre duality, which gives an isomorphism between the group $H^1(L)$ and the dual F-vector space of $H^0(L'')$, where L'' is a lattice pair determined by L. While this is sufficient for computing the F-dimension of $H^1(L)$, we need the representation of elements of $H^1(L)$ as residue classes of vectors of répartitions for computing extensions of lattice pairs (see Item 11). To achieve this, we linearise an explicit Serre duality formula by restricting it to a subset of R_k^n, which is a finite-dimensional F-vector space. We may then efficiently compute preimages of elements lying in the dual of an H^0 space and obtain computational representations of elements lying in each equivalence class of $H^1(L)$.

- Let ξ be an extension of vector bundles over X given by the exact sequence

$$0 \to G \to E \to F \to 0.$$

  A straightforward application of the snake lemma to a commutative diagram built using flasque resolutions of the vector bundles $\mathcal{H}om(F, G)$, $\mathcal{H}om(F, E)$ and $\mathcal{H}om(F, F)$, we may associate to the extension ξ an element of $H^1(\mathcal{H}om(F, G))$, whose description as a residue class of vectors of répartitions itself yields an explicit description of $\mathrm{LP}(E)$.

- Computing kernels and images of homomorphisms is a straightforward application of known results on the Hermite Normal Form.

- The category of vector bundles, and therefore that of lattice pairs, is a Krull-Schmidt category [4]. It follows that the structure of a lattice pair's endomorphism algebra entirely determines how it splits as a direct sum of indecomposables. More specifically, let A be the semi-simple quotient of the F-algebra of endomorphisms of L. We have an isomorphism

$$A \simeq M_{n_1}(D_1) \oplus \ldots \oplus M_{n_s}(D_s),$$

  where the D_i are division F-algebras. Then, L has the following splitting pattern:

$$L \simeq L_1^{n_1} \oplus \ldots \oplus L_s^{n_s},$$

where the L_i are indecomposable and D_i is the semi-simple quotient of the endomorphism algebra of L_i. Therefore, computing the splitting of a lattice pair reduces to the tasks of computing its endomorphism algebra, computing the central idempotents of its semi-simple quotient and then computing the images of these idempotent endomorphisms. The endomorphism algebra is the H^0 space of the lattice pairs of homomorphisms and is therefore computed by combining Items 6 and 9. Computing the structure of an algebra over a finite field is the object of [70]. Finally, we may compute images of endomorphisms by Item 13.

- When the base field F is large enough (larger than the rank of L, that is), finding an isomorphism between lattice pairs may be done by taking random homomorphisms. With enough trials, either an isomorphism is found, or the two lattice pairs are not isomorphic with overwhelming probability. When the base field is small, computing the splitting pattern of both input lattice pairs reduces the problem to computing isomorphisms between indecomposable objects. This task, in turn, is done by computing the structure of the endomorphism algebra of their direct sum. Indeed, if both lattice pairs are isomorphic, the semi-simple part of the endomorphism algebra will have the form $M_2(D)$, with D a division F-algebra. Furthermore, the morphism corresponding to $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ yields an isomorphism. On the other hand, if the lattice pairs are not isomorphic, the semi-simple quotient of the endomorphism algebra will be of the form $D_1 \oplus D_2$, where the D_i are division F-algebras.

1.6 Novelty

The Amitsur algebras we introduce are novel, although presentations of central simple algebras and Azumaya algebras using Amitsur (or étale) cohomology are already known [2, 14, 18, 73]. Our construction stands out as we sacrifice generality for practicality: multiplication in an Amitsur algebra follows a straightforward formula involving its defining Amitsur cocycle. This Amitsur algebra presentation generalises existing cyclic and crossed-product presentations and is, in fact, equivalent to the Brauer algebra presentation [55]. Our presentation, however, hits a sweet spot given by Theorem 1.4.2. Indeed, cyclic and crossed-product presentations only satisfy the first item of the theorem, but computing a cyclic (resp. crossed-product) presentation of a given central

simple algebra requires the knowledge of a maximal commutative subalgebra that is a cyclic extension (resp. a Galois extension) of the base field. To our knowledge, there is no efficient algorithm to compute such a subalgebra.

On the other hand, while constructing a Brauer presentation theoretically only requires the knowledge of any maximal commutative subalgebra, the representation of Brauer algebras and Brauer factor sets involves elements of a normal splitting field of this subalgebra. Results in arithmetic statistics suggest that, with overwhelming probability, a random commutative maximal subalgebra of a matrix algebra of degree d is an extension of the base field with Galois group $\mathfrak{S}_d$ [28]. Computation in a normal splitting field for such an extension is therefore not tractable, as the degree of such a field is $d!$. Therefore, the fact that both items of Theorem 1.4.2 hold is a novel property of our Amitsur algebra construction.

Theorem 1.4.3 is essentially a generalisation to Amitsur cohomology of results from [29, 82]. While our proof strategy is analogous to that of [29, Theorem 7], our setting presents additional difficulties. Indeed, it requires a theory of divisors of étale algebras over global fields and their splitting behaviour. While the results we prove and use are certainly very accessible to experts, we could not locate a reference to them in the literature, and they may be of independent interest.

To our knowledge, no conditional polynomial quantum algorithm is known for the explicit isomorphism problem on number fields. Known classical algorithms either focus on restricted versions of the problem (restricting either the base field or the degree of the algebra) or have exponential complexity in some parameters. Therefore, our algorithm is the first polynomial quantum algorithm and the first subexponential classical algorithm to solve the explicit isomorphism problem for number fields under GRH.

Computations on vector bundles on projective curves are a particular case of computation on coherent sheaves over projective schemes, where algorithms using Gröbner bases follow from Serre's description of coherent sheaves as graded modules [78]. This is the representation that, for instance, Sagemath and Magma [10,89] use. Increasingly efficient methods have been developed to compute the cohomology groups of such sheaves, for instance, in [27, 61, 83].

Our approach is smaller in scope but allows for more specialised algorithms and representations. To our knowledge, this approach of computationally representing vector bundles as pairs of lattices is novel. Our representation of vector bundles as lattices over a ring of integral répartitions is similar to Weng's

unpublished work on so-called adelic vector bundles [93]. The computation of 0th cohomology groups is a generalisation of known methods for computing Riemann-Roch spaces [45] and intersections of orders [46]. Our method for explicitly computing Serre duality isomorphisms is also novel to our knowledge.

1.7 Dissemination

Talks given by the author

1. Finding Nontrivial Zeros of Quadratic Forms over Rational Function Fields of Characteristic 2. International Symposium on Symbolic and Algebraic Computation, Université de Lille, France. July 2022.

2. The Explicit Isomorphism Problem. Arithmetic Geometry Seminar, Bayreuth University, Germany. January 2023.

3. The Splitting Problem in Central Simple Algebras. 19th Atelier PARI/GP 2024, ENS Lyon, France. January 2024.

Talks given by a coauthor

1. Explicit Isomorphisms of Quaternion Algebras over Quadratic Global Fields. Algorithmic Number Theory Symposium XV. University of Bristol, United Kingdom. July 2022. Presentation given by Péter Kutas.

Other international events attended by the author

1. Isogeny-based Cryptography School. Online. July 2021.

2. Isogeny-based Cryptography Workshop. University of Birmingham, United Kingdom. March 2022.

3. Park City Mathematics Institute Graduate Summer School: Number Theory Informed by Computation. Park City, Utah, USA. July 2022

1.8 Publications

1. Tímea Csahók, Péter Kutas, Mickaël Montessinos and Gergely Zábrádi. Finding Nontrivial Zeros of Quadratic Forms over Rational Function

Fields of Characteristic 2. ISSAC '22—Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation, 235–244. https://doi.org/10.1145/3476446.3535485

2. Tímea Csahók, Péter Kutas, Mickaël Montessinos and Gergely Zábrádi. Explicit isomorphisms of quaternion algebras over quadratic global fields. Research in Number Theory 8, 4 (2022), 77, 24 p. https://doi.org/10.1007/s40993-022-00380-3

3. Péter Kutas, Mickaël Montessinos. Efficient computations in central simple algebras using Amitsur cohomology. Journal of Algebra 665 (2025), 255-281. https://doi.org/10.1016/j.jalgebra.2024.10.045

4. Mickaël Montessinos. Algebraic algorithms for vector bundles over curves. Journal of Algebra and its Applications, 2024. https://doi.org/10.1142/S0219498826500210

1.9 Structure of the thesis

We recall the basic theory of global fields and then present existing algorithms used in the sequel in Chapter 2. Section 2.1 presents theoretical results. In particular, Section 2.1.5 present several results that are likely well-known by experts but which we could not locate in the literature and may be of independent interest. Section 2.2 then presents known algorithms for the computational treatment of global fields.

We recall well-known results on finite-dimensional algebras, central simple algebras and the Brauer group in Chapter 3. Section 3.1 presents known results on the structure and algorithmic treatment of finite-dimensional associative algebras, Section 3.2 introduces the theory of central simple algebras, with a focus on cohomological presentations, Section 3.3 discussed the computational treatment of these cohomological presentations, and Section 3.4 presents variants of the explicit isomorphism problem and discusses some of the main known algorithms solving it.

We present our cohomological presentation of central simple algebra and our polynomial quantum algorithm for solving the explicit isomorphism problem under GRH in Chapter 4. Section 4.1 recalls the definitions of Amitsur cohomology, Section 4.2 introduces our version of Amitsur algebras and proofs

that they classify central simple algebras, while Section 4.3 gives our algorithmic treatment of Amitsur algebras.

We discuss our algorithmic treatment of vector bundles in Chapter 5. Section 5.1 presents the theoretical results, representing vector bundles as lattices over a ring of integral répartitions, Section 5.2 presents the algorithmic treatment of lattice pairs, our computational representation of vector bundles, and Section 5.3 presents some examples of practical computations made using our algorithms.

Acknowledgments

I am grateful to my advisor, Artūras Dubickas, for supervising my work. I am also thankful to all the teachers and professors who helped me grow as a mathematician. I am particularly grateful to Gabriel Dospinescu and Philippe Gille for sharing helpful advice at the beginning of my doctoral studies.

I owe much to my coauthors, Tímea Csahók, Péter Kutas and Gergely Zábrádi, who helped me discover the explicit isomorphism problem. I am particularly grateful to Péter Kutas for many hours of conversation and exchanging ideas.

I am also obliged to many members of the international mathematical community. I thank Aurel Page, Lin Weng, Sean Eberhard and many others for fruitful and enlightening conversations on their work. I am indebted to Himanshu Shukla and Florent Bréhard for hosting me when I attended seminars and conferences they organised.

This thesis might not have existed without the benevolent care of my parents, both mathematics teachers, who were the first to teach me that mathematics are fun. I also owe much to many of my friends, whose presence and shared hobbies have helped me maintain the will to move forward. I am particularly thankful to Fabrice and Vincent for maintaining regular contact despite the distance, and to Andrew, Dug, James, Karl, and Nick for teaching me that when in doubt, I should stick to the plan.

Finally, I am eternally grateful to my wife and best friend, Simona, for sharing my life, being supportive, and constantly helping me grow.

Chapter 2

Computing in global fields

This this chapter briefly recalls some results in the algorithmic theory of global fields.

2.1 Background on algebraic number theory

We recall the basic definitions and results of algebraic number theory.

2.1.1 Local Field

A *local field* is a topological field that is non-discrete and locally compact. By [92, Section I.3], such a field is always isomorphic to one of the following variants:

1. The field of real numbers $\mathbb{R}$.
2. The field of complex numbers $\mathbb{C}$.
3. A finite extension of the field $\mathbb{Q}_p$ of p-adic numbers, for p a prime number.
4. A field $\mathbb{F}((X))$ of formal power series over a finite field $\mathbb{F}$.

The fields of real and complex numbers are called *Archimedean local fields* while the others are *non-Archimedean local fields*. The topology of any local field is metric and comes from an absolute value (among a class of equivalent absolute values).

Definition 2.1.1 ([63, Definition II.3.1])**.** *Let k be a field. An* absolute value *over k is a map $|\cdot|\colon k \to \mathbb{R}_{\geq 0}$ such that*

1. *for* $a \in k$, $|a| = 0$ *if and only if* $a = 0$*;*

2. *for* $a, b \in k$, $|ab| = |a||b|$*;*

3. *for* $a, b \in k$, $|a + b| \leq |a| + |b|$.

If, furthermore, for $a, b \in k$, $|a + b| \leq \max(|a|, |b|)$*, then the absolute value* $|\cdot|$ *is said to be* non-Archimedean*. Two absolute values* $|\cdot|_1$ *and* $|\cdot|_2$ *over a field* k *are said to be* equivalent *if there exists* $\alpha \in \mathbb{R}_{>0}$ *such that* $|\cdot|_1 = |\cdot|_2^{\alpha}$.

If k is a local field with absolute value $|\cdot|_k$, and K is a finite extension of k, then by [13, Section II.11], K is a local field when given the topology induced by the absolute value $|\cdot|_K$ defined by

$$|a|_K = \left|N_{K/k}(a)\right|_k .$$

Observe that if $a \in k$,

$$|a|_K = |a|_k^{[K:k]}.$$

Let k be a non-Archimedean local field with absolute value $|\cdot|_k$. As in [13, Section II.7], the *valuation ring* of k is the discrete valuation ring

$$\mathcal{O}_k = \{a \in k : |a|_k \leq 1\}.$$

The unique maximal ideal of $\mathcal{O}$ is

$$\mathfrak{m}_k = \{a \in k : |a|_k < 1\},$$

and the *residue field* of k is

$$\kappa_k = \mathcal{O}/\mathfrak{m}.$$

Note that κ is always a finite field, and its characteristic is p, where k is either an extension of $\mathbb{Q}_p$ or of the form $\mathbb{F}_q((t))$, where q is a power of p.

For a local field k, we define its *normalised absolute value* as in [13, Section II.11]:

1. If $k \simeq \mathbb{R}$, the normalised absolute value of k is the usual real absolute value.

2. If $k \simeq \mathbb{C}$, the normalised absolute value of k is the square of the usual complex absolute value.

3. If k is non-Archimedean, set $q = |\kappa_k|$. Then, the normalised absolute value of k is the unique absolute value of k, whose values are precisely the integral powers of q.

We now consider a finite extension K/k of non-archimedean local fields and follow [13, Section I.5]. Then, we have $\mathcal{O}_k \subset \mathcal{O}_K$ and $\mathfrak{m}_k \subset \mathfrak{m}_K$, so κ_K is a field extension of κ_k. It is finite, and its degree, which we denote by $f_{K/k}$, is called the *inertia degree of the extension* K/k. Furthermore, if the field k is non-Archimedean, $\mathfrak{m}_k\mathcal{O}_K$ is an ideal of $\mathfrak{m}_K$, and we have $\mathfrak{m}_k\mathcal{O}_K = \mathfrak{m}_K^{e_{K/k}}$ for some $e_{K/k} \in \mathbb{N}$. Then $e_{K/k}$, is called the *ramification degree of the extension* K/k, and we have [13, Proposition I.5.3]:

$$e_{K/k} f_{K/k} = [K : k].$$

If L is a finite extension of K, we have [13, Proposition I.5.1]:

$$f_{K/k} = f_{L/K} f_{K/k},$$

and

$$e_{L/k} = e_{L/K} e_{K/k}$$

if k is non-Archimedean.

We next prove a lemma on the tensor product of unramified extensions of local fields.

Lemma 2.1.2. *Let k be a non-Archimedean local field, and let K and L be finite non-ramified separable extensions of k. Then, the direct factors of $K \otimes_k L$ are unramified extensions of k.*

Proof. By [13, Proposition I.7.1], there exist an irreducible monic polynomial $\chi \in \mathcal{O}_k[X]$ such that $L \simeq k[X]/(\chi(X))$ and the respective residue polynomial $\bar{\chi}$ of χ in $\kappa_k[X]$ is irreducible and separable. Then, we have

$$K \otimes_k L \simeq K[X]/(\chi(X)).$$

Consider the factorisation $\chi(X) = \chi_1(X) \dots \chi_r(X)$ in $\mathcal{O}_K[X]$, and set $K_i = K[X]/(\chi_i(X))$. The factors χ_i are pairwise coprime since χ is a separable polynomial, so

$$K \otimes_k L \simeq K_1 \times \dots \times K_r.$$

Now, fix $i \in [r]$. The residue polynomial $\bar{\chi}_i$ is a factor of $\bar{\chi}$ in $\kappa_K[X]$, and is therefore separable. Then, by Hensel's lemma (see e.g [63, Lemma II.4.6]), $\bar{\chi}_i$ is irreducible in $\kappa_K[X]$ because χ_i is so in $\mathcal{O}_K[X]$. It follows by [13, Proposition I.7.1 (ii)] that K_i is a non ramified extension of K, and therefore of k. □

2.1.2 Global Fields

As in [92, Section III.1], a *global field* (*A*-field in the terminology of Weil's book) is a field of one of the two forms below:

1. A *number field*. That is a finite extension of the rational field $\mathbb{Q}$.
2. A *global function field*. That is, a finitely generated extension of a finite field $\mathbb{F}$, with transcendence degree 1 over $\mathbb{F}$.

Places of a global field

We follow here the exposition from [92, Section III.1]. Let k be a global field. Two embeddings $\lambda\colon k \to K$ and $\mu\colon k \to L$ into field extensions are called equivalent if there exists an isomorphism $\varphi\colon K \to L$ such that $\mu = \varphi \circ \lambda$. A fundamental concept in the theory of global fields is that of a place:

Definition 2.1.3 ([92, Definition III.1.2])**.** *A* place *of k is an equivalence class of embeddings $\lambda\colon k \to K$, where k is a local field and $\lambda(k)$ is dense in K. The class of λ is called an* Archimedean (resp. non-Archimedean) place *if K is itself Archimedean (resp. non-Archimedean).*

We denote the set of places of k by M_k. We also write M_k^a for the set of Archimedean places of k and M_k^{na} for the set of non-Archimedean places of k.

Let $P \in M_k$. We let k_P be a local field that is the codomain of an embedding contained in the class P. Then k_P and a subfield isomorphic to k are defined up to isomorphism. We let $|\cdot|_P$ be the absolute value on k defined as the restriction to k of the normalised absolute value of k_P. This absolute value is independent of the choice of k_P. If P is a non-Archimedean place, we also set

$$\mathcal{O}_P = \{a \in k : |a|_P \leq 1\} = \mathcal{O}_{k_P} \cap k,$$

$$\mathfrak{m}_P = \{a \in k : |a|_P < 1\} = \mathfrak{m}_{k_P} \cap k,$$

and

$$\kappa_P = \mathcal{O}_P/\mathfrak{m}_P \simeq \kappa_{k_P}.$$

For any $a \in k^\times$, we have $|a|_P = |\kappa_P|^n$ for some $n \in \mathbb{Z}$. We set $\mathrm{ord}_P(a) = -n$. We then have $\mathrm{ord}_P(ab) = \mathrm{ord}_P(a) + \mathrm{ord}_P(b)$ and $\mathrm{ord}_P(a+b) \geq \min(\mathrm{ord}_P(a), \mathrm{ord}_P(b))$. We call ord_P the *valuation* of k at P.

We observe that for any non-trivial absolute value $|.|$ of k, there is a place P of k such that $|.|$ is equivalent to $|.|_P$. Indeed, the completion of k for the topology induced by $|.|$ is a local field, and the natural embedding of k into its completion belongs to a place P of k.

Extensions of global fields

Let k be a global field and let K be a finite separable extension of k. Let $Q \in M_K$, and fix a corresponding embedding $\lambda\colon K \to K_Q$. Let L be the closure of $\lambda(k)$ in K_Q. Then, L is a local field and the embedding $\lambda\colon k \to L$ defines a place P of k [92, Proposition III.1.1]. The place P does not depend on the choice of λ, and we call it the *place of k lying below Q* [92, Definition III.1.4]. We also write $Q \mid P$ and say that Q lies *above* P. We also set $f_{Q/P} = f_{K_Q/L}$ and, if P is a non-Archimedean place, $e_{Q/P} = e_{K_Q/L}$, and call these numbers respectively the *inertia degree of Q over P* and the *ramification degree of Q over P*.

We now consider the converse situation. Let $P \in M_k$. Then, only finitely many places of K lie above P. In fact, the extension of scalars algebra K_{k_P} splits as a direct product of finite extensions of k_P (see [92, Theorem III.4.4])):

$$K_{k_P} = K_1 \times \ldots \times K_r.$$

Let p_i be the projection map from K_{k_P} to K_i, and let ι be the embedding $K \to K_{k_P}$. Then each map $p_i \circ \iota$ defines a distinct place Q_i of K above P, and the Q_i are the only places of K above P. Furthermore, if P is a non-Archimedean place, we have [63, Theorem II.8.5]:

$$\sum_{i=1}^{r} e_{Q_i/P} f_{Q_i/P} = [K : k].$$

We say that the non-Archimedean place P *ramifies in K* if any of the $e_{Q_i/P}$ is greater than 1, and we say that a place Q_i is *ramified over k* if $e_{Q_i/P} > 1$. In the other case, we say that the relevant place is *unramified*.

Following the similar result for extension of local fields, if L is a finite extension of K, and we have places $P \in M_k$, $Q \in M_K$ and $R \in M_L$ such that $P \mid Q \mid R$, we have

$$f_{R/P} = f_{R/Q} f_{Q/P},$$

and

$$e_{R/P} = e_{R/Q} e_{Q/P}$$

if the place P is non-Archimedean.

S-Integral elements and S-units

In this paragraph, we fix a global field k and a nonempty set $S \subset M_k$, which contains all the Archimedean places of k. We may then define the ring of

S-integral elements of k as follows:

$$\mathcal{O}_S = \{a \in k : \forall P \in M_k \setminus S,\ |a|_P \leq 1\} = \bigcap_{P \in M_k \setminus S} \mathcal{O}_P.$$

The ring $\mathcal{O}_S$ is known to be a Dedekind domain.

We also define the group of S-units [13, Section II.18]:

$$U_S = \{a \in k : \forall P \in M_k \setminus S,\ |a|_P = 1\} = \mathcal{O}_S^\times.$$

If the set S is finite, the structure of U_S is well known. The group U_S is a finitely generated abelian group of rank $|S| - 1$, and its torsion subgroup is the group of roots of unity of k. We may abuse notations and write $\mathcal{O}_S$ and U_S for $\mathcal{O}_{S'}$ and $U_{S'}$ respectively for $S' = S \cup M_k^a$ even if S does not contain the Archimedean places of k.

Divisors

Let k be a global field. The *divisor group* of k, denoted by $\mathcal{D}(k)$, is the free abelian group on M_k^{na}. In this section, we follow the exposition from [13, Section II.17], except we use the term *divisor group* for both number fields and function fields. A *divisor* of k is a formal sum

$$D = \sum_{P \in M_k^{na}} n_P P,$$

where the n_P are integers, and all but finitely many of them are zero. The *support* of the divisor D is the finite set

$$\mathrm{Supp}(D) = \{P \in M_k^{na} : n_P \neq 0\},$$

and we say that D is supported by $S \subset M_k$ if $\mathrm{Supp}(D) \subset S$.

If $a \in k^\times$, it is known that $\mathrm{ord}_P(a) \neq 0$ for only finitely many places $P \in M_k$. It follows that we have a group homomorphism

$$\begin{array}{ccc} k^\times & \to & \mathcal{D}(k) \\ a & \mapsto & \mathcal{D}(a) = \sum_{P \in M_k^{na}} \mathrm{ord}_P(a) P. \end{array}$$

A divisor thus obtained from an element of $k^\times$ is called a *principal divisor*, and the principal divisors of k form a subgroup of $\mathcal{D}(k)$ denoted by $\mathcal{P}(k)$. Then, the *class group* of k is defined by

$$\mathrm{Cl}(k) = \mathcal{D}(k)/\mathcal{P}(k).$$

An important theorem of algebraic number theory states that the class group $\mathrm{Cl}(k)$ of a global field is finite.

We now let K/k be a finite separable field extension. Then, we have a map $\iota_{K/k}$ from M_k^{na} to $\mathcal{D}(K)$ which sends a place P of k to the divisor

$$\sum_{\substack{Q \in M_K^{na} \\ P|Q}} e_{Q/P} Q.$$

Proposition 2.1.4. *The map $\iota_{K/k}$, extended to the divisor group of k, is an injective group homomorphism. Furthermore, if L is a finite separable extension of L, we have*

$$\iota_{L/k} = \iota_{L/K} \circ \iota_{K/k}.$$

Proof. By the universal property of the free abelian group, any map from the set M_k^{na} to an abelian group such as $\mathcal{D}(K)$ extends to a group homomorphism $\mathcal{D}(k) \to \mathcal{D}(K)$. By uniqueness of the place of k below a place of K, it follows that the supports of the images of distinct elements of M_k^{na} in $\mathcal{D}(K)$ are disjoint. The injectivity of the map $\iota_{k/K} \colon \mathcal{D}(k) \to \mathcal{D}(K)$ follows readily.

The functoriality statement is a straightforward consequence of the facto that for $P \in M_k^{na}$, $Q \in M_K^{na}$ and $R \in M_L^{na}$, we have $e_{R/P} = e_{R/Q} e_{Q/P}$. □

Divisors and fractional ideals

Let k be a global field and let $S \subset M_k$ be a nonempty set of places which contains all the Archimedean places. Then the prime ideals of $\mathcal{O}_S$ are exactly the $\mathfrak{m}_P$ where P is an element of $M_k \setminus S$ [13, Section II.17].

We let $\mathcal{D}(k)_S$ be the subgroup of divisors with support in S. As $\mathcal{O}_S$ is a Dedekind domain, any fractional $\mathcal{O}_S$-ideal (*i.e.* a sub $\mathcal{O}_S$-module of k) factors uniquely as a product of prime ideals. It follows that there is a bijection between the group of fractional ideals of $\mathcal{O}_S$ and the quotient group $\mathcal{D}(k)/\mathcal{D}(k)_S$. As the group of principal ideals of $\mathcal{O}_S$ is in bijection with $(\mathcal{P}(k)/(\mathcal{P}(k) \cap \mathcal{D}(k)_S)$, the class group of $\mathcal{O}_S$ may be expressed as the quotient

$$\mathrm{Cl}(k)_S \coloneqq \mathrm{Cl}(\mathcal{O}_S) = \frac{\mathcal{D}(k)}{\mathcal{P}(k) + \mathcal{D}(k)_S}.$$

We also call this group the *S-class group of k*. In particular, if S is such that for every nontrivial class of $\mathrm{Cl}(k)$ has an element with support in S, then $\mathrm{Cl}(k)_S$ is the trivial group, and $\mathcal{O}_S$ is a PID.

2.1.3 The ring of integers of a number field

Let k be a number field. Since k is a finite extension of $\mathbb{Q}$, k has Archimedean places, which are all the places above the unique Archimedean place of $\mathbb{Q}$. As a result, the set $S = M_k^a \subset M_k$ is the minimal nonempty subset of M_k which contains all the Archimedean places. We then write $\mathcal{O}_k$ for the ring of S-integers of k, and we call this ring the *ring of integers of* k. It is a $\mathbb{Z}$-lattice of full rank in k [92, Theorem V.2.1].

For any prime ideal $\mathfrak{p}$ of $\mathcal{O}_k$, we may define the $\mathfrak{p}$-adic absolute value on k, and the $\mathfrak{p}$-adic completion $k_\mathfrak{p}$ of k. Thus, every prime ideal of $\mathcal{O}_k$ is associated with a non-Archimedean place of k.

There is a bijective correspondence between the non-Archimedean places of a global field and the prime ideals of its ring of integers.

2.1.4 Global function fields

The situation for a function field k is different from that of a number field in that there does not exist a ring whose prime ideals are in bijection with the non-Archimedean places of k. Instead, one must consider a regular projective curve, a generalisation of a Dedekind domain in the language of schemes. Since our treatment focuses on the algebraic language of function fields, we do not recall the theory of algebraic curves. Instead, we direct the reader to [81, Chapter 1 and 2] for an elementary introduction to algebraic curves and to [38, 42] for a presentation of the language of schemes. References for the theory of function fields are [72, 84].

For the remainder of this section, the field k is an algebraic function field with constant field F. Some results are valid even when F is not a finite field. Without loss of generality, we may assume that F is algebraically closed in k.

Places of function fields

We first recall the definition of a projective space. Let $n \in \mathbb{N}$. Let $\overline{F}$ be an algebraic closure of F. Then we define the projective space $\mathbb{P}^n_F$ as the quotient set $(\overline{F}^{n+1} \setminus \{0\})/\sim$ where $x = (x_0, \ldots, x_n) \sim y = (y_0, \ldots, y_n)$ if there exist $\lambda \in \overline{F}^\times$ and $\sigma \in \mathrm{Gal}(\overline{F}/F)$ such that $x_i = \lambda\sigma(y_i)$ for $i \in [n]_0$. If $x = (x_0, \ldots, x_n) \in F^{n+1} \setminus \{0\}$, we write $(x_0 : \ldots : x_n)$ for the class of x in $\mathbb{P}^n_F$.

If $k = F(X)$, we set $C_k = \mathbb{P}^1_F$. Otherwise, as discussed in the beginning of [72, Chapter 5], the field k is isomorphic to a field of the form $k \simeq F[X,Y]/(\chi(X,Y))$, where $\chi \in F[X,Y]$ is irreducible as an element

of $F(X)[Y]$. In this case, we set $\chi = \sum_{i,j\in\mathbb{N}} c_{ij}X^iY^j$, and we let $d = \deg\chi$ be the maximal value of $i + j$ such that $c_{ij} \neq 0$. Then, the homogeneisation of χ is the polynomial

$$\widetilde{\chi}(X, Y, Z) = \sum_{i,j\in\mathbb{N}} c_{ij}X^iY^jZ^{d-i-j}.$$

The projective curve corresponding to the polynomial χ is the set

$$C_\chi = \{(x : y : z) \in \mathbb{P}^2_F \mid \widetilde{\chi}(x, y, z) = 0\}.$$

We note that, in the language of schemes, C_P is the set of closed points of a regular projective curve X_P over F with function field k.

By [38, Theorem 15.21], the regular projective curve X_P is unique up to isomorphism. We, therefore, usually refer to this curve as X_k and to its set of closed points as C_P, understanding that it is fixed up to isomorphism.

We then have a bijection between the set M_k of places of k and the set C_k defined above [38, Remark 15.23]. Let $P = M_k$ correspond to a point $(x : y : z)$, we have $\kappa_P \simeq \bigcap_{(x,y,z)\in[x:y:z]} F(x, y, z)$ [38, Exercise 15.10], and we set $\deg P = [\kappa_P : F]$.

If we identify k with the field $F[X, Y]/P(X, Y)$, k naturally presents as a finite extension of the rational function field $F(X)$. The places of the rational function field are the *finite places* corresponding to the Galois orbits of elements $\alpha \in \overline{k}$ via the points $(\alpha : 1)$ and one *infinite place* ∞ corresponding to the point $(1 : 0)$ of the curve $C_{F(X)} = \mathbb{P}^1_F$. We note that if $S = \{\infty\}$, then the integer ring $\mathcal{O}_S$ is in fact the polynomial ring $F[X]$. The valuation ring $F(X)_\infty$ of the infinite place is the PID $\{R \in F(X) \mid \deg R \leq 0\}$. We set $M^\infty_{F(X)} = \{\infty\}$ and $M^{fi}_{F(X)} = M_{F(X)} \setminus M^\infty_{F(X)}$. Then we write M^{fi}_k for the set of places lying above the finite places of $F(X)$, and we likewise set M^∞_k to be the set of places of k lying above the infinite place of $F(X)$. We call the places of k finite or infinite depending on whether they belong to M^{fi}_k or M^∞_k. When the field k is clear from context, we will write $\mathcal{O}_{fi} = \mathcal{O}_{M^\infty_k}$ and $\mathcal{O}_\infty = \mathcal{O}_{M^{fi}_k}$. We note that $\mathcal{O}_{fi}$ is the integral closure of $F[X]$ in k and $\mathcal{O}_\infty$ is the integral closure of $F(X)_\infty$ in k. Observe that the Dedekind domain $\mathcal{O}_\infty$ has finitely many prime ideals and is, therefore, a PID.

Répartitions

The words répartition and adèles are sometimes used interchangeably in the literature. When working over a global field, they always mean to take a

restricted product over the set of places of the field. Usually, this is the product of the completions of the field, but one may also work with mere copies of the field. Since our work is computational, we avoid taking completions to preserve exact computational representations. In this work, we use the term *répartition* to emphasise this. In this work we shall only use répartitions over function fields. References for répartitions in algebraic function fields are [79, 84].

Definition 2.1.5. *The ring R_k of répartitions of k (simply written R when there is no ambiguity on the choice of field k) is the restricted product*

$$R = \tilde{\prod_{P \in M_k}} k,$$

where the restriction means that for an element $(r_P) \in R$, all but finitely many of the r_P lie in $\mathcal{O}_P$.

The subring of R of integral répartitions is the product

$$\mathcal{O}_R = \prod_{P \in M_k} \mathcal{O}_P.$$

We may now define the degree of an invertible répartition

Definition 2.1.6. *Let $r \in R^\times$. If $P \in M_k$, we set* $\mathrm{ord}_P(r) = \mathrm{ord}_P(r_P)$. *Then, we set*

$$\deg(r) = \sum_{P \in M_k} \mathrm{ord}_P(r) \deg(P).$$

The degree is well defined since, for all but finitely many $P \in M_k$, an invertible répartition $r \in R^\times$ lies in $\mathcal{O}_P^\times$ and therefore has valuation zero at P.

In our statement of Serre duality, we will use residues of répartitions, which we define as follows:

Definition 2.1.7. *Let $r \in R$. The* residue *of r is defined as the sum*

$$\mathrm{res}(r) = \sum_{P \in M_k} \mathrm{Tr}_{\kappa_P/F}(\mathrm{res}_P(r_P)),$$

where $\mathrm{res}_P(r_P)$ is the coefficient of degree -1 in the formal series in π_P representing r_P.

In Section 5.2.3, we must compute répartitions with prescribed residues. Our strategy will focus on an infinite place of k. We introduce the following useful notation:

Definition 2.1.8. *An* infinite répartition *is a répartition $r \in R$ such that $r_P = 0$ for all $P \in M_k^{fi}$ and there exists $a \in k$ such that $r_P = a$ for all $P \in M_k^{\infty}$. We denote such a répartition r by a_∞. We also extend this notation to vectors with coefficients in R.*

In order to use répartitions to describe vector bundles of rank larger than 1, we will use matrices taking coefficients in R. Such techniques were already discussed in [86,93–95] for matrices with coefficients in the ring of adèles. The properties we need to establish are often analogous to some results from the references above, but we give our own proofs for completeness and to account for the change from adèles to répartitions.

A matrix $M \in M_{r_1,r_2}(R)$ is the same thing as a family $(M_P)_{P \in M_k}$ of matrices in $M_{r_1,r_2}(k)$ with the extra condition that at most finitely many of the M_P do not lie in $M_{r_1,r_2}(\mathcal{O}_P)$.

We take note of an easy lemma.

Lemma 2.1.9. *A matrix $M \in M_n(R)$ is invertible if and only if it lies in $\prod_{P \in M_k} GL_n(k)$ and all but finitely many of the M_P lie in $GL_n(\mathcal{O}_P)$.*

Proof. The determinant $d = \det M$ is invertible in R if and only in it lies in $\prod_{P \in M_k} k^\times$ and for all but finitely many P, $d_P \in \mathcal{O}_P^\times$. The result follows readily. □

Differentials

Here we recall definitions and basic facts about the differentials of function fields. Details and omitted proofs may be found in [84, Chapter 4].

Let $\widetilde{\Omega}_k$ to be the free k-vector space with basis the set of symbols $\{da : a \in k\}$, and then we set $\Omega^1_{k/F}$ to be the quotient space $\widetilde{\Omega}_k / V$, where V is the subspace of $\widetilde{\Omega}_k$ generated by the $d(a+b) - da - db$, the $d(ab) - adb - bda$ and the $d\alpha$, for $a, b \in k$ and $\alpha \in F$. We call $\Omega^1_{k/F}$ the space of *differentials* of K. It is canonically isomorphic to the space Δ_k as introduced in [84, Definition 4.1.7] (both spaces satisfy the universal property stated in [84, Proposition 4.1.8.(d)]).

The space $\Omega^1_{k/F}$ is 1-dimensional as a k-vector space, and da is a basis for any separable element $a \in k$. That is for any $a \in k$ such that $k/F(a)$ is a finite separable field extension.

If $\omega \in \Omega^1_{k/F}$ and $P \in M_k$, we let π_P be a local uniformiser at P, and write $\omega = f_P d\pi_P$. Then, we may embed f_P into the local field k_P, which is the field of formal series $\kappa_P((\pi_P))$. We let $f_P = \sum_{n \in \mathbb{Z}} a_n \pi_P^n$ and we set

$\mathrm{res}_P(\omega) = a_{-1} \in \kappa_P$. It is well known that the value of $\mathrm{res}_P(\omega)$ does not depend on the choice of uniformiser π_P. We may then state the Residue Theorem: for any $\omega \in \Omega^1_{k/F}$,

$$\sum_{P \in M_k} \mathrm{Tr}_{\kappa_P/F}\left(\mathrm{res}_P(\omega)\right) = 0. \tag{2.1}$$

In the literature, this theorem is usually stated in the case that F is algebraically closed. In this case, $\kappa_P = F$ and it is useless to take the trace of the residues. The more general Equation (2.1) is well known to experts and is, for instance, used as an example for testing the computation of residues of a differential in the documentation of Sagemath [89]. The Residue Theorem for a general ground field is proved in [87], in a slightly different form equivalent to Equation (2.1). Indeed, [87] gives a definition of the residue $\mathrm{res}_P(\omega)$ as a trace over F of a related k-linear endomorphism of K_P (restricted to a finite-dimensional F-subspace of K_P). In the proof of [87, Theorem 2], the author argues that if $\deg P = 1$, *i.e.* $\kappa_P = F$, then the residue takes the same form as our definition. When $\deg P > 1$, the argument shows that the trace mentioned above, this time taken over κ_P, takes the value that we defined as $\mathrm{res}_P(\omega)$. Since that is the case, the residue according to Tate's definition, as a trace, decomposes as $\mathrm{Tr}_{\kappa_P/F}(\mathrm{res}_P(\omega))$. Equation (2.1) then follows from the corollary to [87, Theorem 3].

Fix a local uniformiser π_P for every place $P \in M_k$. We define an injective k-linear map $\iota\colon \Omega^1_{k/F} \to R_k$. Let $\omega \in \Omega^1_{k/F}$, and let $f_P \in K$ such that $\omega = f_P d\pi_P$ for all $P \in M_k$. We then set $\iota(\omega) = (f_P)_{P \in M_k}$.While the répartition $\iota(\omega)$ depends on the choice of uniformisers π_P, we always have

$$\mathrm{res}(\iota(\omega)) = \sum_{P \in M_k} \mathrm{Tr}_{\kappa_P/F}(\mathrm{res}_P(\omega)) = 0.$$

2.1.5 Étale algebras

In this section, we fix a field k. We will recall some usual definitions and properties of étale k-algebras and prove some less common results which will be needed later.

Definition 2.1.10. *Let R be a k-algebra. We say that R is* diagonalisable *if there exists $d \in \mathbb{N}$ such that R is isomorphic to k^d, the direct product of d copies of k. An extension K/k* diagonalises *the k-algebra R if the K-algebra R_K is diagonalisable. The algebra R is said to be* étale *if there exists a finite*

separable field extension K/k such that K diagonalises R. Such an extension is called a splitting field *for R.*

Lemma 2.1.11. *Let R be an étale k-algebra of dimension d, and let K be a Galois splitting field of R, with splitting isomorphism $\varphi\colon R \otimes K \to K^d$. Let $x \in R$ such that for any two nonzero maps φ, φ' from R to K,*

$$\varphi(x) = \varphi'(x).$$

Then $x \in k$.

Proof. Consider the sequence of maps

$$R \xrightarrow{\cdot\otimes 1} R \otimes_k K \simeq K^d \xrightarrow{p_i} K,$$

where p_i is the projection of K^d to its i-th factor. We let f_i be the composition of these maps. Then f_i is non-zero since $f_i(t) = t$ for $t \in k$.

Now, for $i, j \in [d]$, we have $f_i(x) = f_j(x)$, and it follows that $\varphi(x \otimes 1)$ lies in the diagonal of K^d. Furthermore, if $i \in [d]$ and ψ is a k-automorphism of K, we have $\psi(f_i(x)) = f_i(x)$, and it follows that the $f_i(x)$ lie in k. Put together, we get $\varphi(x \otimes 1) = (t, t, \ldots, t)$ with $t \in k$. However, since the composite map $R \to K^n$ is injective, we get $x = t \in k$. □

Proposition 2.1.12 ([11, Corollary V.6.5.1])**.** *Let R, S be two commutative finite-dimensional k-algebras. Let $C = R \otimes_k S$. Then C is étale if and only if R and S are étale.*

Proposition 2.1.13 ([11, Theorem V.6.7.4])**.** *Let R be a k-algebra. The algebra R is étale if and only if there exist finite separable extensions $K_1, \ldots, K_r$ of k such that $R \simeq K_1 \times \ldots \times K_r$.*

Observe that the $K_1, \ldots, K_r$ are the minimal ideals of R and are therefore entirely determined by R up to reindexing.

Proposition 2.1.13 suggests that if R is an étale k-algebra, the category of R-modules is almost as well behaved as that of vector spaces over a field. We will need the following result:

Corollary 2.1.14. *Let R be an étale k-algebra, and let M be a faithful R-module such that $[M : k] = [R : k]$. Then, M is isomorphic to R as an R-module.*

Proof. Let $K_1, \ldots, K_r$ be the minimal ideals of R as in Proposition 2.1.13. We let $d = [R : k]$, $d_i = [K_i : k]$. We also set $r_i = [K_i M : K_i]$. The faithfulness

of M implies that every r_i is nonzero and that $M = \bigoplus_{i=1}^{r} K_i M$. Then, we have $[M : k] = \sum_{i=1}^{r} r_i n_i$. Since $[M : k] = [R : k] = \sum_{i=1}^{n} n_i$, it follows that $r_i = 1$ for all $1 \leq i \leq r$. Then, $K_i M$ is isomorphic to K_i as a K_i-module, and therefore M is isomorphic to R as an R-module. □

Proposition 2.1.13 also permits a description of homomorphisms of étale algebras.

Corollary 2.1.15. *Let $K = K_1 \times \ldots \times K_r$ and $L = L_1 \times \ldots \times L_s$ be étale k-algebras, and let $f \colon K \to L$ be a homomorphism of k-algebras. Then $f = \sum_{i \in [r]} f_i$, where $f_i \colon K_i \to L$ is either zero or a multiplicative k-linear map from K_i to L. Furthermore, the sets*

$$J_i = \{j \in [s] \colon p_j \circ f_i \neq 0\},$$

where p_j is the projection map from L to L_j, are pairwise disjoint.

Proof. Since $K = K_1 \times \ldots \times K_r$, the map f decomposes uniquely as a sum $f = \sum_{i \in [r]} f_i$, where f_i is a k-linear map from K_i to L, and it is clear that f_i is multiplicative since f_i is the restriction of f to K_i.

Now, fix $j \in [s]$. Let $i, i' \in [r]$, and set e_i (resp. $e_{i'}$) be the identity of K_i (resp. $K_{i'}$) in K. We then have $e_i e_{i'} = 0$, so

$$p_j(f(e_i))p_j(f(e_{i'})) = 0.$$

Since the codomain of p_j is L_j, a field, it follows that either $p_j(f(e_i))$ or $p_j(f(e_{i'}))$ is 0. Assuming that $p_j(f(e_i)) = 0$, it is easy to see that $p_j \circ f_i = 0$, and therefore $j \notin J_i$. □

Corollary 2.1.16. *Let $K = K_1 \times \ldots \times K_r$ be an étale k-algebra. A field extension E/k is a splitting field for K if and only if E contains subfields isomorphic to each of the K_i.*

Proof. We have

$$K \otimes_k E = \bigoplus_{i=1}^{r} K_i \otimes_k E.$$

Therefore, E is a splitting field for K if and only if it is a splitting field for all of the K_i. Now, fix $i \in [r]$. Let $\chi \in k[X]$ be irreducible (necessarily separable) polynomials such that $K_i \simeq k[X]/(\chi)$. Then, consider the factorisation $\chi = \xi_1 \ldots \xi_s$ of χ in $E[X]$. We get $K_i \otimes_k E \simeq \bigoplus_{j=1}^{s} E[X]/(\xi_j)$. Since E must be a splitting field for K_i, it follows that $\deg \xi_j = 1$ for all $j \in [s]$. That is, the polynomial χ splits in E, and therefore E contains a copy of K_i. □

Corollary 2.1.17. *Let $K = K_1 \times \ldots \times K_r$ be an étale k-algebra of dimension d, and let E be a Galois splitting field for K. Then, there are exactly d distinct nonzero maps from K to E.*

Proof. By Corollary 2.1.15, a nonzero map $\varphi\colon K \to E$ is zero on all but one of the factors K_i. Furthermore, by Corollary 2.1.16, E contains all of the K_i. Now, if we set $d_i = [K_i : k]$, we have $d = \sum_{i=1}^{r} d_i$, and there are exactly d_i nonzero k-algebra homomorphisms from K_i to E. The result follows. □

Example 2.1.18. Let k be a field, and let $\chi \in k[X]$ be a separable polynomial. Then $K = k[X]/(\chi)$ is an étale algebra. We say that such an étale algebra is *monogeneous*.

Proposition 2.1.19. *If the field k is infinite, every étale k-algebra is isomorphic to a monogeneous étale k-algebra.*

Proof. Let K be an étale k-algebra, isomorphic to the product $K_1 \times \ldots \times K_r$ of separable extensions of k. And let $\chi_i \in k[X]$ for $i \in [r]$ be irreducible polynomials such that $K_i \simeq k[X]/(\chi_i(X))$. Then, for $i, i' \in [r]$, either χ_i and $\chi_{i'}$ are distinct and therefore coprime, or they are equal. In that case, there exist only finitely many pairs $\alpha, \beta \in k$ such that $\chi_i(X + \alpha)$ and $\chi_{i'}(X + \beta)$ are not coprime. Since the field k is infinite, one may therefore pick the χ_i to be pairwise coprime, and then $K \simeq k[X]/(\prod_{i \in [s]} \chi_i)$. □

In Chapter 4, we will need to consider étale algebras over étale algebras.

Definition 2.1.20. *Let R be an étale k-algebra. An R-algebra S is said to be* étale *if it is étale as a k-algebra. We further say that S is a* free étale *R-algebra if S is étale and free as an R-module.*

Remark 2.1.21. A definition of étale R-algebras exists for a general commutative ring R. In the case that R is an étale k-algebra, the general definition coincides with our own (See [33, Definition 9.2.3, Proposition 9.2.5 and Corollary 9.2.6]).

Moreover, we will need the following result:

Lemma 2.1.22. *Let R be an étale k-algebra, and let S be an étale R-algebra. Then, there is a trace map $S \to R$. Let $S^\vee$ be the dual of S as an R-module. Then, the map*

$$\begin{array}{ccc} S & \to & S^\vee \\ a & \mapsto & (b \mapsto \mathrm{Tr}(ab)) \end{array}$$

is an isomorphism of R-modules.

Proof. By Remark 2.1.21, S is an étale R-algebra in the sense of [33, Definition 9.2.3]. It is, therefore, separable as an R-algebra, and then the result is a particular case of [33, Corollary 4.6.8]. □

Proposition 2.1.23. *Let R be an étale k-algebra and let S be a free étale R-algebra. Let S_1, S_2 be k-subalgebras of* $\mathrm{End}_R(S)$ *that are isomorphic to S. Then, there exists an R-algebra automorphism of* $\mathrm{End}_R(S)$ *which sends S_1 to S_2.*

Proof. Let φ_i be an isomorphism from S to S_i for $i \in [2]$. For $i \in [2]$, we let S_{φ_i} be the S-module isomorphic to S as a k-vector space and such that $a \cdot x = \varphi_i(a)(x)$ for $a, x \in S$. Then, the faithful S-modules S_{φ_1} and S_{φ_2} are isomorphic by Corollary 2.1.14. Let ψ be an isomorphism of S-modules from S_{φ_1} to S_{φ_2}. Since both S_{φ_1} and S_{φ_2} are identified with S as k-vector spaces, we may see ψ as a k-linear endomorphism of S. Then, for any $a, x \in S$, we have

$$(\psi \circ \varphi_1(a))(x) = (\varphi_2(a) \circ \psi)(x).$$

It follows that conjugation by ψ is an R-algebra automorphism of $\mathrm{End}_R(S)$ which sends S_1 to S_2. □

Divisors of étale algebras over global fields

For what follows, we assume that k is a global field.

Definition 2.1.24. *Let $K = K_1 \times \ldots \times K_r$ be an étale k-algebra. We define the set of* places *of K as the disjoint union*

$$M_K = \bigsqcup_{i=1}^{r} M_{K_i}.$$

We likewise define the sets of Archimedean, non-Archimedean, finite *and* infinite places *of K.*

By analogy with Section 2.1.2, we define the divisor group *of K, denoted by $\mathcal{D}(K)$, as the free abelian group over M_K^{na}. We define the* support *of a divisor, the subgroup of* principal divisors $\mathcal{P}(K)$ *and the* class group $\mathrm{Cl}(K)$ *likewise.*

Observe that $\mathcal{P}(K) = \mathcal{P}(K_1) \times \ldots \times \mathcal{P}(K_r)$. It follows that

$$\mathrm{Cl}(K) = \mathrm{Cl}(K_1) \times \ldots \times \mathrm{Cl}(K_r).$$

In particular, we get the following result:

Proposition 2.1.25. *Let K be an étale k-algebra. Then, the class group of K is finite.*

In what follows, we adapt results from Section 2.1.2 to the setting of étale algebra.

We will prove that $\mathcal{D}$ is a functor from the category of étale k-algebras to the category of abelian groups. Let $K = K_1 \times \ldots \times K_r$ and $L = L_1 \times \ldots \times L_s$ be étale k-algebras, and let $f\colon K \to L$ be a homomorphism of k-algebras. We also let p_j be the projection from L to L_j for any $j \in [s]$ and let $J_i \subset [s]$ be defined as in Corollary 2.1.15. For $i \in [r]$, $j \in [s]$, we have a map $f_{ij} = p_j \circ f_i$ from K_i to L_j, which is either the zero map if $j \notin J_i$ or a k-homomorphism of field extensions if $j \in J_i$. If $j \in J_i$, we then have a group homomorphism $\mathcal{D}(f_{ij})\colon \mathcal{D}(K_i) \to \mathcal{D}(L_j) \subset \mathcal{D}(L)$. We extend this mapping to $\mathcal{D}(K)$ linearly by setting $\mathcal{D}(f_{ij}))(P) = 0$ if $P \in M^{na}_{K_{i'}}$ and $i' \neq i$. Then, we set

$$\mathcal{D}(f) = \sum_{\substack{i\in[r]\\ j\in J_i}} \mathcal{D}(f_{ij}).$$

Now, let $N = N_1 \times \ldots \times N_t$ be another étale algebra, and let $g\colon L \to N$ be a homomorphism of k-algebras. The fact that $\mathcal{D}(g \circ f) = \mathcal{D}(g) \circ \mathcal{D}(f)$ follows from the similar fact for divisor groups of global fields.

If f is an automorphism of K as a k-algebra and $P \in M^{na}_K$, the divisor $\mathcal{D}(f)(P)$ is also primitive, in the sense that if $\mathcal{D}(f)(P) = \sum_{Q\in M^{na}_K} n_Q Q$, $n_Q = 0$ for all but one $Q \in M^{na}_K$, and then $n_Q = 1$. We denote by P^f the place Q as above.

We record one result for later purposes:

Lemma 2.1.26. *Let K, L be étale k-algebras, and let $f\colon K \to L$ be a homomorphism of k-algebras such that, with $[r], [s]$ and the J_i as in Corollary 2.1.15, $\bigcup_{i\in[r]} J_i = [s]$. Let $Q \in M^{na}_L$. Then there exists a unique $P \in M^{na}_K$ such that $Q \in \mathrm{Supp}(\mathcal{D}(f)(P))$.*

Proof. We set $K = K_1 \times \ldots \times K_r$ and $L = L_1 \times \ldots \times L_s$ as usual. Then, we may assume that $Q \in M_{K_1}$, and we let p_1 be the projection map $L \to L_1$. By Corollary 2.1.15, there is a unique $i \in [r]$, such that $p_1 \circ f_{|K_i} \neq 0$. It follows from definition of $\mathcal{D}(f)$ that if $P \in M_K$ is such that $Q \in \mathrm{Supp}(\mathcal{D}(f)(P))$, then $P \in M_{K_i}$. As $p_1 \circ f_{|K_i}$ corresponds to a k-homomorphism of field extensions, the result follows from the uniqueness of the place below Q in a subfield of K_1. □

When f, Q and P are as in the statement of Lemma 2.1.26, we write $Q_f \coloneqq P$.

Definition 2.1.27. *With notations as in the proof of Lemma 2.1.26, if $Q \in M_{L_j}^{na} \subset M_L^{na}$, let $i \in [r]$ such that $Q_f \in M_{L_i}$. Then, the* ramification index of Q by f, *denoted by $e_{Q,f}$ is the index e_{Q/Q_f} where L_j is seen as an extension of K_i via the map $p_j \circ f_{|K_i}$.*

A place $Q \in M_L^{na}$ is called unramified with respect of f *if $e_{Q,f} = 1$. A place $P \in M_K^{na}$ is called* unramified with respect to f *if $e_{Q,f} = 1$ for all $Q \in \mathrm{Supp}(\mathscr{D}(f)(P))$.*

Local completions of étale algebras over global fields

We assume that k is a global field. Using completions, we may give a Galois theoretical description of the splitting behaviour of the places of an étale k-algebras.

Definition 2.1.28. *Let $K = K_1 \times \ldots \times K_r$ be an étale k-algebra, and let $P \in M_K$. Let $i \in [r]$ be such that $P \in M_{K_i}$. Then, the* local completion of K at P *is the completion of the field K_i at the place P. It is a K-algebra via the composite map*

$$K \to K_i \to K_P,$$

where the left map is the projection map and the second is the natural injection of K_i into its completion.

Proposition 2.1.29. *Let K, L be étale k-algebras, let $f\colon K \to L$ be a homomorphism of k-algebras, and let $P \in M_K^{na}$. Then, the scalar extension algebra L_{K_P} is a direct product of finite extensions of K_P, and there is a bijection between its direct factors and the support of $\mathscr{D}(f)(P)$.*

Proof. Set $K = K_1 \times \ldots \times K_r$ and $L = L_1 \times \ldots \times L_s$. Without loss of generality, we assume that $P \in M_{K_1}$. Then, the K-algebra K_P is killed by the maximal ideal $0 \times K_2 \times \ldots \times K_r$. It follows that

$$L_{K_P} = K_P \otimes_K L \simeq K_P \otimes_{K_1} (K_1 \otimes_F L) \simeq \prod_{j \in J_1} K_P \otimes_{K_1} L_j.$$

However, by the discussion in Section 2.1.2, if $j \in J_i$, $K_P \otimes_K L_j$ is a direct product of local field, whose factors are in bijection with the support of $\mathscr{D}(p_j \circ f_1)(P)$ in $\mathscr{D}(L_j)$. The result follows since $\mathscr{D}(f)(P)$ is the sum of the $\mathscr{D}(p_j \circ f_1)(P)$, and the supports of these maps are pairwise disjoint. □

2.1.6 Lattices and orders

Let k be a global field, and let $S \subset M_k$ be a nonempty subset which contains all the Archimedean places of k. Let V be a finite-dimensional k-vector space. An $\mathcal{O}_S$-lattice in V is a finitely generated $\mathcal{O}_S$-submodule L of V such that $kL = V$. Such a lattice is torsion-free. As $\mathcal{O}_S$ is a Dedekind domain, it follows that L is a projective $\mathcal{O}_S$-module.

Such a projective module is not necessarily free. However, it admits a pseudo-basis [91, Theorem 9.3.6]. If $n = [V : k]$, a pseudo-basis of an $\mathcal{O}_S$-lattice L in V is a pair

$$PB = ((\mathfrak{a}_1, \ldots, \mathfrak{a}_n), (x_1, \ldots, x_n))$$

such that the $\mathfrak{a}_i$ are fractional $\mathcal{O}_S$-ideals, the x_i are elements of V, and

$$L = \mathfrak{a}_1 x_1 \oplus \ldots \oplus \mathfrak{a}_n x_n.$$

A well-known result on Dedekind domains states that for any lattice admits a pseudo-basis of the form $((\mathcal{O}_S, \ldots, \mathcal{O}_S, \mathfrak{a}), (x_1, \ldots, x_n))$. Furthermore, if $\mathfrak{a}$ and $\mathfrak{a}'$ are two fractional $\mathcal{O}_S$-ideals such that there exists a pseudo-basis of L of this form, then $\mathfrak{a}$ and $\mathfrak{a}'$ have the same class in $\mathrm{Cl}(k)_S$. The class of $\mathfrak{a}$ is called the *Steinitz class* of L. Two lattices are isomorphic if and only if they have the same Steinitz class. In particular, if $\mathcal{O}_S$ is a PID, then all $\mathcal{O}_S$-lattices are free [91, Theorem 9.3.9].

If we assume that V is in fact the underlying vector space of a k-algebra A, the lattice L is said to be an $\mathcal{O}_S$-*order* of A if it also a subring of A [91, Definition 10.2.1]. An $\mathcal{O}_S$-order is then naturally an $\mathcal{O}_S$-algebra. An order is called *maximal* if not contained in a strictly larger order.

We now present two examples of orders.

1. The ring $M_d(\mathcal{O}_S)$ is a maximal $\mathcal{O}_S$-order in $M_d(k)$.
2. If K/k is a finite extension and T is the set of places of K lying above the elements of S, then the ring $\mathcal{O}_T$ of T-integral elements of K is an $\mathcal{O}_S$-order in K. It is the integral closure of $\mathcal{O}_S$ in K. It is also the only maximal $\mathcal{O}_S$-order in K.

2.2 Algorithms

We present various algorithmic problems for algebraic number theory and the complexity of existing algorithms that solve them. For brevity, we do not give the details of the algorithms but instead give references.

Many of these algorithms (or others solving the same problems) are implemented in computer algebra software such as PARI/gp [88], Sage [89] and Magma [10].

2.2.1 Computational Model

When we state the complexity of an algorithm, we mean the number of bit operations necessary for the computation, expressed as a function of the size of the input. By *polynomial algorithm*, we mean a deterministic algorithm whose complexity is dominated by a polynomial in the size of the input. A *subexponential algorithm* is an algorithm whose complexity is asymptotically larger than any polynomial but smaller than any exponential function of the input. We also consider probabilistic algorithms, which require the generation of random numbers and whose behaviour and success may be random. We distinguish algorithms of the *Monte Carlo* type, whose complexity is fixed but success is uncertain, and algorithms of the *Las Vegas* type, whose success is guaranteed but complexity is random. We say that a Las Vegas algorithm is polynomial if the expectation of its complexity is polynomial.

A polynomial Monte Carlo algorithm may turn into a polynomial Las Vegas algorithm under two conditions: that the probability of success is larger than $1/p(n)$ for some polynomial p and n the size of the input; and that the validity of its output may be checked in polynomial time. Indeed, if these conditions are satisfied, a polynomial Las Vegas algorithm is obtained by repeatedly executing the Monte Carlo algorithm and checking for the validity of its output. In the sequel, we will use this transformation freely.

When describing an algorithm, we may refer to an *oracle* for a specific algorithmic task. An oracle here is a subroutine which solves the algorithmic task in question, and its complexity is considered polynomial in the size of its input.

Many algorithms we will discuss are deterministic and run in polynomial time, except for one or several factorisation steps. An f*-algorithm* is a deterministic polynomial algorithm with access to an oracle for factoring polynomials over finite fields. An ff*-algorithm* is a deterministic polynomial algorithm with access to an oracle for factoring integers and polynomials over finite fields. [71].

2.2.2 Lattice reduction

Many of our algorithms involve lattices and orders. In order to handle such objects, it is often necessary to compute a reduced basis or pseudo-basis with desirable properties. Below, we define such reductions and present algorithms to compute them.

Popov reduction

In order to relate lattices over the rings $F[X]$ and $F(X)_\infty$, we need to compute bases that are orthogonal in some sense. While LLL reduction would be used over $\mathbb{Z}$, the function field equivalent we use here is the Popov form of matrices. We follow the exposition given in [75] up to transposition since our convention will be to have the columns of matrices represent basis elements. Note that since the rings $F[X]$ and $F(X)_\infty$ are PIDs, any lattice over these rings is a free module. In particular, it admits a basis in $F(X)^n$, and may be represented by an element of $GL_n(F(X))$.

Definition 2.2.1. *Let $v = (v_i) \in M_{n,1}(F[x])$ be a column vector. We define the following:*

- *The* norm *of v as $|v| = \max_{i=1}^{n} \deg(v_i)$.*
- *The vector $\mathrm{lc}(v) \in M_{n,1}(F)$ is the vector whose i-th entry is the coefficient of degree $|v|$ of the polynomial v_i.*
- *The* pivot index *of vector v, denoted by $\mathrm{piv}(v)$ is the largest i such that $\deg v_i = |v|$.*

Definition 2.2.2 ([75, Definition 2])**.** *Let $M \in M_n(F[x])$, and let $v_1, \ldots, v_n$ be the columns of M. We say that the matrix M is* reduced *if the matrix*

$$\mathrm{lc}(M) = \begin{pmatrix} \mathrm{lc}(v_1) & \ldots & \mathrm{lc}(v_n) \end{pmatrix}$$

is invertible. We say that the matrix M is in Popov form *if it is reduced and the following conditions are satisfied:*

1. *The pivot indices $\mathrm{piv}(v_1), \ldots, \mathrm{piv}(v_n)$ are distinct.*
2. *The pivot entries $v_{i,\mathrm{piv}(v_i)}$ are monic.*
3. *For $i \in [n]$, $|v_i| \leq |v_{i+1}|$, and if $|v_i| = |v_{i+1}|$, then $\mathrm{piv}(v_i) < \mathrm{piv}(v_{i+1})$.*

4. *The entries of v that are not the pivot of their column have degree lesser than the entry of the same row which is the pivot of its column.*

The reason reduced matrices are relevant to us is the following statement, which is a form of orthogonality:

Proposition 2.2.3 ([52, Theorem 6.3-13])**.** *Let $v_1, \ldots, v_n$ be the columns of a reduced matrix. Let $a_1, \ldots, a_n \in F[x]$. Then*

$$\left| \sum_{i=1}^{n} a_i v_i \right| = \max_{i \in [n]} \left(\deg(a_i) + |v_i| \right).$$

Computing reduced matrices would be sufficient for most applications, but a matrix may be right-equivalent to several different reduced matrices. Instead, computing the Popov form of a matrix ensures uniqueness and may be desirable in a computational context.

Proposition 2.2.4. *Let $M \in M_n(k[x])$ be nonsingular. Then there exist unique matrices $U \in GL_n(k[x])$ and $P \in M_n(k[x])$ such that $P = MU$ and the matrix P is in Popov form.*

Reduced and Popov forms of matrices may be computed efficiently. In the following, the notation $\tilde{O}$ means we omit logarithmic factors, ω is the exponent of the cost of matrix multiplication in k, $M(d)$ is the cost of multiplication of two polynomials of degree at most d and $B(d)$ is the cost of an extended gcd computation for two polynomials of degree at most d.

Proposition 2.2.5. *Let $M \in M_n(k[x])$ with entries of degree no larger than $d \in \mathbb{N}$.*

- *A reduced matrix right-equivalent to M may be computed at a cost of $\tilde{O}(n^\omega(M(d) + B(d)))$ operations in k. [41]*
- *If M is reduced, the Popov form of M maybe computed at a cost of $\tilde{O}(n^\omega d)$ operations in k. [75]*

Hermite form

Many basic algorithms for algebraic number theory require computing the Hermite normal form of matrices with coefficients in rings of S-integers of global fields. We first recall the definitions. If R is a PID, elements a and b of $R \setminus \{0\}$ are said to be *associated* if there exists a unit $u \in R^\times$ such that $a = ub$.

Our definition of the Hermite normal form over a PID is a mix of the definition given in [64, Section II.6] and [15, Definition 2.4.2].

Definition 2.2.6. *Let R be a PID. Fix a maximal set A of nonassociated elements of R, and for each $a \in A$, fix a complete set B_a of residues modulo a. Then, a matrix $M = (m_{ij})_{\substack{i\in[m]\\ j\in[n]}} \in M_{m,n}(R)$ is in* Hermite normal form *if there exist $r \in [n]$ and a strictly increasing map f from $\{r+1, r+2, \ldots, n\}$ to $[m]$ such that the following conditions are satisfied:*

1. *For $r+1 \leq j \leq n$, $m_{f(j),j} \in A$, $m_{i,j} = 0$ if $i > f(j)$ and $m_{f(i),j} \in B_{m_{f(k),k}}$ if $i < j$.*
2. *The first r columns of M are equal to 0.*

It is well-known that a matrix admits a Hermite normal form.

The problem of computing the Hermite normal form of a matrix with integer or polynomial coefficients is well studied and may be solved in polynomial time [41, 85]. The ring $k(x)_\infty$ is a DVR, so the Hermite normal form may also easily be computed over this ring.

The algorithms given in Section 5.2.5 will rely on the computation of Hermite normal forms of matrices and pseudo-matrices over rings $\mathcal{O}_{fi}$ and $\mathcal{O}_\infty$ lying in a global function field. We briefly recall the relevant definitions and results and refer the reader to [17, Sections 1.4 and 1.5] for details. Note that we include the case of matrices that are not of full rank.

For the rest of this section, R is a Dedekind domain with fraction field K. We first give a definition of pseudo-matrices:

Definition 2.2.7 ([17, Definition 1.4.5])**.**

1. *A pseudo-matrix of size $m \times n$ over A is a pair $PM = (\mathfrak{a}, M)$, where $\mathfrak{a} = (\mathfrak{a}_j)_{j\in[n]}$ are fractional ideals of R and $M \in M_{m,n}(K)$.*
2. *The map associated with such a pseudo-matrix is the map $f\colon \mathfrak{a}_1 \oplus \ldots \oplus \mathfrak{a}_n \to K^m$ defined by $f(a_1, \ldots, a_n) = \sum_{j=1}^n a_j M_j$, where the M_j are the columns of M.*
3. *The module associated with this pseudo-matrix is the module*

$$L = \sum_{j=1}^{n} \mathfrak{a}_j M_j.$$

It is the image of the map f in K^n, and is denoted by $PM(R^n)$.

4. *The kernel of the pseudo-matrix $(\mathfrak{a}, M)$ is the kernel of the map f.*

Remark 2.2.8. If A is a PID, we may always turn a pseudo-matrix into a matrix by computing generators of its coefficient ideals.

For the following definition, we assume that for each fractional ideal $\mathfrak{a}$ of R, there is a fixed set $B_{\mathfrak{a}}$ of representatives of the residue classes of $K/\mathfrak{a}$.

Definition 2.2.9 ([8, 17]). *Let $PM = (\mathfrak{a}, M)$ be a pseudo-matrix of size $m \times n$, with coefficients in R, let $r = \operatorname{rank} M$. A Hermite normal form of $(\mathfrak{a}, M)$ is the data of a matrix $U = (u_{ij})_{i,j\in[n]} \in GL_n(K)$ and a pseudo-matrix $(\mathfrak{b}, N)$ with $\mathfrak{b} = (\mathfrak{b}_1, \ldots, \mathfrak{b}_n)$ and $N \in M_{m,n}(K)$ such that*

1. *$u_{ij} \in \mathfrak{a}_i\, \mathfrak{b}_j^{-1}$ for all $i, j \in [n]$;*
2. *we have $\prod_{i\in[n]} \mathfrak{a}_i = \det(U) \prod_{i\in[n]} \mathfrak{b}_i$;*
3. *the matrix N is of the form $\begin{pmatrix} \mathbf{0} & H \end{pmatrix}$, with $\mathbf{0}$ the zero matrix in $M_{m,n-r}(K)$ and $H = (h_{ij})_{\substack{i\in[m]\\ j\in[r]}} \in M_{m,r}(K)$ such that there exists an increasing function $f\colon [r] \to [m]$ such that for $j \in [r]$ and $f(i) < j \leq m$, $h_{ij} = 0$ and for $j \in [r]$, $h_{f(j)j} = 1$.*
4. *with H_i the i-th column of H for $i \in [r]$,*
$$PM(R^n) = \mathfrak{b}_{n-r+1} H_1 \oplus \ldots \oplus \mathfrak{b}_n H_r;$$
5. *with U_i the i-th column of U, $((\mathfrak{b}_1, \ldots, \mathfrak{b}_{n-r}), (U_1, \ldots, U_{n-r}))$ is a pseudo-basis of the kernel of PM;*
6. *if $j \in [r]$ and $i \in [f(j) - 1]$, $h_{ij} \in B_{\mathfrak{b}_{n-r+i}\, \mathfrak{b}_{n-r+j}^{-1}}$.*

More than the exact definition, what matters to us is the useful algorithmic properties of the Hermite Normal Form:

Proposition 2.2.10.
1. *Let $(\mathfrak{a}, M), (\mathfrak{a}', M')$ be two pseudo-matrices over a Dedekind domain R. Then, the modules generated by these pseudo-matrices are equal if and only if their Hermite normal forms are equal as well [17, 1.5.2 (2)].*
2. *The image and kernel of a pseudo-matrix may be computed in polynomial time from its Hermite normal form [17, 1.5.2 (5)].*

We now discuss the problem of computing Hermite normal forms for pseudo-matrices over the rings $\mathcal{O}_{fi}$ and $\mathcal{O}_\infty$ of a global function field. The

analogue problem for rings of integers of number fields was conjectured in [16] to be feasible in polynomial time, and it was proved in [8] for pseudo-matrices of full rank. Since the ring $\mathcal{O}_\infty$ has only finitely many prime ideals, a polynomial algorithm for computing Hermite normal forms may easily be found. In the case of rings $\mathcal{O}_{fi}$ in function field and matrices of lower rank, no such result exists in the literature to the best of our knowledge. It seems plausible that the methods of [8] may be adapted to the function field setting, replacing the use of LLL-reduction with Popov reduction. However, Remark 36 of the work cited argue that the modular methods used there do not adapt to pseudo-matrices that are not of full rank. We, therefore, define the following problem:

Problem 2.2.11. *Given a global function field K and a pseudo-matrix PM over $\mathcal{O}_{fi}$, compute a Hermite normal form of PM.*

We state the following conjecture, hoping that further research may fully tackle the problem.

Conjecture 2.2.12. *There exists a polynomial-time algorithm that solves Problem 2.2.11.*

2.2.3 Main algorithms for global fields

This section discusses algorithms for representing and manipulating elements of global fields. The standard references for most of these results are the books [15, 17]. These books focus on number fields, but some algorithms are also valid for function fields. A more recent and different approach to several algorithmic problems is [40].

Representing elements and computing algebraic operations

We assume efficient algorithms for representing elements of the rational field $\mathbb{Q}$ and any rational function field $\mathbb{F}(X)$, when $\mathbb{F}$ is a finite field. A rational number $r = a/b \in \mathbb{Q}$, with a and b coprime integers, has a representation of size $\lceil \log_2(a) \rceil + \lceil \log_2(b) \rceil$. Likewise, an element $r = a/b \in \mathbb{F}(X)$, where a and b are coprime polynomials, has a representation size proportional to $\deg a + \deg b$. We also assume that algebraic operations between elements may be computed in polynomial time.

In what follows, k is a global field for which we assume we may represent elements and compute algebraic operations. With the paragraph above, this is already the case if k is the field of rational numbers or a rational function field.

Let K be a finite monogeneous extension of k. That is, we assume that an irreducible polynomial $\chi[X]$ of degree d is given such that K may be identified with $k[X]/(\chi(X))$. Then, denoting by θ the image of X in K, any element of K may be uniquely written as

$$x = \sum_{i=0}^{d-1} x_i \theta^i,$$

and this element may be represented computationally as the tuple $x_0, \ldots, x_{d-1}$. Additions and substractions may then be computed componentwise. Multiplication of elements may be computed using polynomial multiplication and reduction modulo χ. Finally, computing inverses of elements, and thus divisions, requires a slightly more involved computation: The polynomial $\xi(X) = c_0 + \ldots + c_{d-1}X^{d-1}$ representing an element x of K (*i.e* $x = \xi(\theta)$) is coprime to χ, since χ is irreducible. Then, one may compute Bezout coefficients $U, V \in k[X]$ such that

$$\xi U + \chi V = 1,$$

and $U \mod \chi$ is the inverse of x in K. These algorithms allow us to represent any global field presented as a separable extension of one of the rational global fields. As inseparable extensions of function fields are unnecessary for our purposes, we do not consider them here. We note that several optimisations are done in practice when these algorithms are implemented.

The references given at the beginning of the section present a variety of possible representations for number field elements, some of them generalising directly to global function fields. Different representations present various advantages depending on the situation. Discussing them is, however, out of the scope of this work, and we refer the reader to the sources for more details.

Heights in function fields

Let k be a global function field with field of constants F. Let $a \in k^\times$. We define the *height* of a as

$$\mathrm{ht}_k(a) = \sum_{P \in M_k} \max(\mathrm{ord}_P(a), 0) = \sum_{P \in M_k} -\min(\mathrm{ord}_P(a), 0).$$

We simply write $\mathrm{ht}(a)$ if the field k is clear from context. Observe that for a finite separable extension K/k, if $a \in k^\times$, $\mathrm{ht}_K(a) = [K : k]\,\mathrm{ht}_k(a)$.

While analogous to heights in number fields, this is more usually called degree in the literature on function fields. In this work, we consider degrees of

vector bundles in various forms and connect them to degrees of divisors and répartitions. We use the word height for this notion to avoid overloading the term.

We observe readily that for $a, b \in k^\times$, $\mathrm{ht}(a+b) \leq \mathrm{ht}(a) + \mathrm{ht}(b)$ and $\mathrm{ht}(ab) \leq \mathrm{ht}(a) + \mathrm{ht}(b)$.

In the case $k = F(x)$, let $r = \frac{a}{b} \in F(x)$ with a and b coprime non-zero polynomials in $k[x]$. Then $\mathrm{ht}(r) = \deg(a) + \deg(b)$. This equation suggests a connection between the height of an element $a \in K^\times$ and the size of its computational representation:

Proposition 2.2.13. *Let $a \in K^\times$. Then $\mathrm{ht}(a)$ is polynomial in the size of the representation of the field K and of the function a.*

Proof. Let $d = [K : k]$. First, we compute $\mathrm{ht}(y)$. Let $\chi_y = \sum_{i=0}^{d} c_i T^i$ be the minimal polynomial of y over $k(x)$. Observe that $[K : k(y)] \leq \max_i \mathrm{ht}(c_i)$. Thus, by [84, Theorem 1.4.11], $\mathrm{ht}_K(y) \leq \max_i \mathrm{ht}(c_i)$. The size of the representation of the field K is bounded by $\sum_{i=0}^{n} \mathrm{ht}(c_i)$, so $\mathrm{ht}(y)$ is bounded by the size of the representation of K. Let $a = \sum_{i=0}^{d-1} a_i y^i$. Then we compute

$$\begin{aligned}\mathrm{ht}(a) &\leq \sum_{i=0}^{d-1} \mathrm{ht}_K(a_i) + i\,\mathrm{ht}(y) \\ &\leq \sum_{i=0}^{d-1} (\mathrm{ht}(a_i)) + \frac{d(d-1)}{2}\,\mathrm{ht}(y).\end{aligned}$$

□

We will need the following easy lemma:

Lemma 2.2.14. *Let $g \in GL_n(K)$. Then $\mathrm{ht}(\det(g))$ is polynomial in the size of the representation of g.*

Proof. A representation of the determinant of g in the basis $1, y, \ldots, y^{d-1}$ may be computed in polynomial time and therefore has polynomial size. The result then follows from Proposition 2.2.13. □

Places and ideals

Following [40], we may represent places of a global field k and fractional ideals over any ring of integers of k. Given places $P_1, \ldots, P_r \in M_k$, integers $\nu_1, \ldots, \nu_r \in \mathbb{Z}$ and $a_1, \ldots, a_r \in k^\times$, we may also solve the Chinese Remainder Problem and compute $a \in k$ such that $\mathrm{ord}_{P_i}(a - a_i) \geq \nu_i$ for $i \in [r]$.

Completions

A computational task for global fields is to compute embeddings into their completions. In this work, we only need to compute the embedding of a global function field k at a given place $P \in M_k$. Such an embedding may be computed in polynomial time using, for instance, [44, Lemma 9 and Algorithm 27].

Factorisation problems

The task of factoring integers into a product of primes is known to be feasible in subexponential time. The task of factoring polynomials over finite fields is known to be feasible in probabilistic polynomial time.

The Montes algorithm [39] allows to factor a prime number p in a ring of integers of a number field, and generalises to factoring a place P of $\mathbb{F}(X)$ into a divisor of a function field. We note that this algorithm is polynomial.

As discussed in [40], it follows that there is an f-algorithm for computing the divisor of an element of a global function field, and an ff-algorithm for computing the divisor of an element of a number field. This work also yields a polynomial algorithm for computing the image of a divisor $D \in \mathcal{D}(k)$ in the group $\mathcal{D}(K)$, where K is a finite extension of k. Finally, if k is a global field, a polynomial in $k[X]$ may be factored in polynomial time as a product of irreducible polynomials [59].

Computing rings of integers

Zassenhaus' Round 2 Algorithm is a well-known ff-algorithm for computing the ring of integers of a number field and may also adapt into an f-algorithm for computing the rings $\mathcal{O}_{fi}$ and $\mathcal{O}_\infty$ of a global function field [15, Section 6.1]. As discussed in [40, Section 8.2], the Montes algorithm also provides a ff-algorithm for computing the ring of integers of a number field, and an f-algorithm for computing the finite and infinite rings of integers of a function field.

Once such rings are computed, any ideal may be represented using a basis over, respectively, $\mathbb{Z}$, $F[X]$, and $F(X)_\infty$.

Class group and unit group

Computing class groups and unit groups is a well-studied problem of algorithmic number theory. In this section, we restrict ourselves to the case that k is a

number field. We first observe that under the *generalised Riemann hypothesis* (henceforth *GRH*), there exists a polynomial-sized set of prime ideals which generate the class group of k [9, Fact 4.1]. More precisely, the class group Cl_k is generated by the set

$$\mathcal{B} = \{\mathfrak{p} \in M_k^{na} \colon N(\mathfrak{p}) \leq 12 \log(|\Delta_k|)^2\},$$

where Δ_k is the discriminant of k and $N(\mathfrak{p})$ is the cardinality of the (finite) field $\mathcal{O}_k/\mathfrak{p}$.

The problem of computing the class group of k is then to compute relations for the elements of $\mathcal{B}$ (or of another generating set) in the class group.

The problem of computing units or S-units in a number field is usually solved as a byproduct of the class group computation. One key question is the choice of representation for the units computed, as there is no guarantee that generators with a polynomial-sized representation in the usual form exist. Instead, the work [7] introduces a compact representation of algebraic integers:

Definition 2.2.15 ([9, Definition 3.1])**.** *Let $l > 0$ be a constant, a* compact representation *of $\alpha \in \mathcal{O}_k$ with respect to the integral basis $(\omega_j)_{j \leq d}$ of $\mathcal{O}_k$ is a positive integer n of polynomial size, and algebraic numbers $\gamma_0, \ldots, \gamma_n$ of polynomial size (in the integral basis (ω_j)) such that*

$$\alpha = \gamma_0 \gamma_1^l \ldots \gamma_n^{l^n}.$$

Then, [7] provides a subexponential algorithm for computing compact representations of generators of the group of units of a number field. While an algorithm exists for computing generators of the group of S-units of a number field, it relies on solving the so-called principal ideal problem. [82, Section 6.1]. We introduce the following problem:

Problem 2.2.16 (S-units computation)**.** *Given a number field k and a finite set S containing the Archimedean places of k, compute compact representations for $\alpha_1, \ldots, \alpha_{|S|-1}$ which generate the torsion-free part of U_S, and the usual representations of a generator of the torsion part of U_S.*

Given generators $\alpha_1, \ldots, \alpha_{|S|-1}$ of the group of S-units in compact representation, [57, Theorem 1.11] provides a polynomial algorithm for computing a representation of a given S-unit as a product of powers of the α_i. We may efficiently compute the isomorphism $U_S \simeq \mathbb{Z}^{|S|-1} \times \mathbb{Z}/n\mathbb{Z}$.

Quantum algorithms

In [80], Shor proposed a polynomial quantum algorithm for factoring integers. While the theory of quantum algorithms is out of the scope of this work, we shall take note of several algorithmic tasks for which a polynomial quantum algorithm is known.

As discussed above, an ff-algorithm is known for computing the ring of integers of a number field. Using Shor's algorithm, we get a polynomial quantum algorithm for computing the ring of integers of a number field.

Also of interest to us, [9] provides a polynomial quantum algorithm for solving Problem 2.2.16.

Chapter 3

The explicit isomorphism problem

This chapter introduces notions related to the explicit isomorphism and presents some existing results on the topic and the methods that they use. A general reference for central simple algebras is [36].

For the remainder of this chapter, k is a field. The k-algebras considered here are assumed to be unital, associative, and finite-dimensional unless specified otherwise.

3.1 Algebras and algorithms

Here, we recall some results on algebras over a field particularly a global field. Let k be a field.

3.1.1 Structure constants

In order to give an algorithmic treatment of k-algebra, we must be able to represent their elements and compute the usual algebraic operations: addition, scalar multiplication and multiplication. Let A be a k-algebra with underlying vector space V of dimension n. Then, any basis of V provides an isomorphism $V \simeq k^n$. We fix such a basis $B = (e_1, \ldots, e_n)$ and identify V with k^n. The bilinear map $V \times V \to V$, which describes the multiplication operation of A, corresponds to a tensor in $V^\vee \otimes V^\vee \otimes V$. If we let $(e_1^\vee, \ldots, e_n^\vee)$ be the basis of $V^\vee$ dual to B, then $(e_i^\vee \otimes e_j^\vee \otimes e_\ell)_{1 \leq i,j,\ell \leq n}$ is a basis of $V^\vee \otimes V^\vee \otimes V$. The structure constants of A with respect to the basis B are then the coordinates

of the multiplication operation of A in this basis. We give a more elementary version of this definition:

Definition 3.1.1. *Let A be a k-algebra of dimension n, and let $(e_i)_{1\leq i\leq n}$ be a basis of A. The* structure constants *of A with respect to the basis (e_i) are the $(c_{ij\ell}) \in k^{n^3}$ such that for all $i, j \in [n]$,*

$$e_i e_j = \sum_{\ell=1}^{n} c_{ij\ell} e_\ell.$$

For such a k-algebra A with structure constants $c_{ij\ell}$, we may represent an element $a = \sum_{i=1}^{n} a_i e_i \in A$ as the vector $(a_i)_{1\leq i\leq n}$. In this setting, computing additions and scalar multiplications is straightforward. The product of two elements is computed using the natural formula

$$\left(\sum_{i=1}^{n} a_i e_i\right)\left(\sum_{j=1}^{n} a'_j e_j\right) = \sum_{\ell=1}^{n}\left(\sum_{\substack{1\leq i,j\leq n\\ i+j=\ell}} a_i a'_j c_{ij\ell}\right) e_\ell.$$

Remark 3.1.2. While more efficient representations may exist for specific classes of algebras, we note that structure constants are universal in the following sense: every method of representation which allows one to efficiently compute the usual algebraic operations in A and find a basis of A allows one to compute structure constants in polynomial time.

3.1.2 The structure of algebras

We briefly recall some well-known results on the structure of k-algebras. For instance, these results may be found in [12].

Definition 3.1.3. *Let A be a k-algebra. The* left regular module ${}_A A$ *of A is the left A-module A, where scalar multiplication is taken on the left. That is, the module action of A on itself gives, for $t \in A$ and $a \in {}_A A$, $t \cdot a = ta$.*

Definition 3.1.4. *Let A be a k-algebra.*

- *An A-module is* simple *if it contains no non-trivial submodule*
- *An A-module is* semisimple *if it is isomorphic to a direct sum of simple modules.*
- *The algebra A is* semisimple *if the left regular module ${}_A A$ is a semisimple A-module.*

- *The algebra A is* simple *if its only two-sided ideals are $\{0\}$ and A itself.*
- *The algebra A is* separable *if it is semisimple and its centre is an étale k-algebra.*
- *The* Jacobson radical of A, *denoted by $J(A)$ is the two-sided ideal*

$$\{x \in A : \exists n \in \mathbb{N} \mid (xA)^n = 0\}.$$

- *The* center *of A is the subalgebra $C(A) = \{x \in A \colon \forall y \in A,\ xy = yx\}$.*
- *The k-algebra A is said to be* central *if $C(A) = k$.*

We then have the following results:

Proposition 3.1.5. *Let A be a k-algebra.*

1. *The algebra $A/J(A)$ is semisimple. In particular, if $J(A) = 0$, then A is semisimple.*
2. *If $A/J(A)$ is a separable k-algebra, there is a semisimple subalgebra W of A such that $A = W \oplus J(A)$. The subalgebra W is unique up to conjugation by an element of $1 + j(A)$.*
3. *If A is semisimple, then $A = A_1 \oplus \ldots \oplus A_r$, where the A_r are the minimal two-sided ideals of A.*
4. *If A is simple, it is isomorphic to an algebra of the form $M_n(D)$, where $n \in \mathbb{N}$ and D is a division k-algebra.*
5. *The algebra A is simple if and only if for any k-algebra B and homomorphism of k-algebra $f \colon A \to B$, f is either zero or injective.*
6. *If A is semisimple, it is in fact simple if and only if the center of A is a field. [70, Section 3]*

In summary, the algebra A has the following structure:

$$A \simeq J(A) \oplus \bigoplus_{i=1}^{s} M_{n_i}(D_i), \tag{3.1}$$

where the D_i are division k-algebras. Such a decomposition is unique up to conjugation and reindexing.

Definition 3.1.6. *A semisimple subalgebra W as in Item 2 of Proposition 3.1.5 is called a* Wedderburn-Malcev complement of A. *We denote by $D(A)$ an arbitrarily chosen Wedderburn-Malcev complement of A.*

The algorithmic task of computing the isomorphism in Equation (3.1) decomposes in several subtasks. We discuss them in the special case that the field k is finite.

Proposition 3.1.7. *Let A be a k-algebra, given by structure constants.*

1. *A basis of $J(A)$ can be computed in polynomial time. [70, Theorem 2.7]*
2. *A basis of a Wedderburn-Malcev complement of A can be computed in polynomial time. [26, Theorem 3.1].*
3. *If A is semisimple, there is an* f*-algorithm for computing bases for the minimal ideals of A. [70, Theorem 3.1]*
4. *The explicit isomorphism problem over a finite field can be solved by an* f*-algorithm. [70, Theorem 5.2]*

3.1.3 Computing maximal orders

Let k be a global field, $M_k^a \subset S \subset M_k$ be non-empty and A be a separable k-algebra. We focus here on computing an $\mathcal{O}_S$-maximal order in A. As opposed to the commutative case, where A is an étale algebra, a maximal $\mathcal{O}_S$-order in A needs not be unique.

Known algorithms for computing maximal orders in separable algebras are generalisations of Zassenhaus' algorithm for computing the ring of integers of a number field. The case $k = \mathbb{Q}$ was first treated in [48]. A general statement for the general case of a Dedekind domain R and a separable algebra over the quotient field of R is given in [34, Section 3.5]. A similar algorithm for the case $k = \mathbb{F}(X)$ is also described in [46], although it is only stated in the case that A is a matrix algebra. We note that the algorithm starts with the factorisation of a discriminant. It follows that this algorithm is an ff-algorithm when k is a number field and an f-algorithm when k is a function field.

While the algorithms described above already cover all global fields, the computation for k a number field or a separable extension of $F(X)$ (F a finite field) may directly reduce to the cases $k = \mathbb{Q}$ and $k = F(X)$. Indeed, we have the following result:

Proposition 3.1.8. *Let K be a finite separable extension of k. Let T be the set of places of K lying above the elements of S. Let A be a separable K-algebra. A maximal $\mathcal{O}_S$-order of A contains the image of $\mathcal{O}_T$ in A. Furthermore, it is a maximal $\mathcal{O}_T$-order.*

Proof. Let $\mathcal{O}$ be a maximal $\mathcal{O}_S$-order in A. Then, $\mathcal{O} \cap K$ is an $\mathcal{O}_S$-submodule and a subring of K. Furthermore, if $x \in A \setminus K$ and $\lambda \in k^\times$, then $\lambda x \notin K$. Since $k\mathcal{O} = A$, it follows that $k(\mathcal{O} \cap K) = K$. That is, $\mathcal{O} \cap K$ is an $\mathcal{O}_S$-order in K. This order is in equal to $\mathcal{O}_T$. Indeed, $\mathcal{O}_T\mathcal{O}$ is also an $\mathcal{O}_S$-order in A which contains $\mathcal{O}$. Since $\mathcal{O}$ is maximal, we have $\mathcal{O} = \mathcal{O}_T\mathcal{O}$, and therefore $\mathcal{O}_T \subset \mathcal{O}$.

Then, $\mathcal{O}$ is an $\mathcal{O}_T$-submodule of A, and we have $A = k\mathcal{O} \subset K\mathcal{O}$, so $\mathcal{O}$ is an $\mathcal{O}_T$-lattice in A, and since it is also a subring, it is an $\mathcal{O}_T$-order. Furthermore, it is also a maximal $\mathcal{O}_T$-order, since any $\mathcal{O}_T$-order is also naturally an $\mathcal{O}_S$-order. □

Applying this result, we may compute a maximal $\mathcal{O}_S$-order and obtain a maximal $\mathcal{O}_T$-order. This method is the approach used, for instance, in Magma. [10]

3.2 Central simple algebra

3.2.1 General properties

We present fundamental properties of central simple algebra. We loosely follow the presentation of [36] for this section. Fundamental examples of central simple algebra are matrix algebras $A = M_d(k)$ and central division algebra.

Example 3.2.1 ([36, Example 2.1.2]). Let D be a central division algebra over k. Then the k-algebra $M_n(D)$ is central simple.

As discussed briefly in Proposition 3.1.5, a famous theorem by Wedderburn states the converse: all central simple algebras are of this form.

Theorem 3.2.2 ([36, Theorem 2.1.3])**.** *A k-algebra A is central simple if and only if there exist $n \in \mathbb{N}$ and a central division k-algebra D such that $A \simeq M_n(D)$. Furthermore, the number n and algebra D are uniquely determined (up to isomorphism) by the property.*

Central simple algebras are characterised as so-called *forms* of matrix algebras. By this, we mean the following:

Theorem 3.2.3. *Let A be a k-algebra. Then the following are equivalent*

1. *A is central simple.*
2. *There exists a finite field extension K/k such that $A \otimes_k K \simeq M_d(K)$.*
3. *There exists a commutative k-algebra R such that $A \otimes_k R \simeq M_d(R)$.*

Proof. The equivalence Item 1 $\iff$ Item 2 is the content of [36, Theorem2.2.1].

Item 2 clearly implies Item 3.

Now, let R be a commutative k-algebra such that $A \otimes R \simeq M_d(R)$. It follows by [33, Proposition 7.1.10] that $A \otimes_k R$ is a so-called central separable R-algebra. By [33, Corollary 4.3.5], it follows that A is a central separable k-algebra. Since k is a field, a central separable k-algebra is the same thing as a central simple k-algebra by [33, Corollary 4.5.4]. □

For this reason, matrix algebras play a pivotal role in the theory of central simple algebras.

Definition 3.2.4. *Let A be a central simple k-algebra. A field extension K/k is called a* splitting field *of A if $A \otimes K \simeq M_d(K)$ for some $n \in \mathbb{N}$. Then, $d = \sqrt{[A : k]}$ is called the* degree *of A and denoted by* $\deg A$. *Furthermore, a* splitting *of A over K is an isomorphism $\varphi \colon A \otimes_k K \to M_d(K)$. If k is a splitting field for A, we say that A is* split.

We give a valuable characterisation of split central simple algebras based on the existence of a rank one element.

Definition 3.2.5. *Let A be a central simple k-algebra, and let $z \in A$. The* rank *of z, denoted by* $\operatorname{rank} z$, *is the number*

$$\operatorname{rank} z = \frac{[Az : k]}{\deg A}$$

Proposition 3.2.6. *Let A be a central simple k-algebra. Then A is split if and only it contains an element of rank* 1.

Proof. When $A \simeq M_d(k)$, the rank defined above coincides with the usual rank of a matrix (which is invariant up to isomorphism), and then A contains elements of rank one. Conversely, let $z \in A$ have rank one. Then we set $V = Az$, and V is a d-dimensional k-vector space, where $d = \deg A$. Since V is a left-ideal of A, we get a k-algebra homomorphism $A \to \operatorname{End}_k(V)$ by

sending $a \in A$ to the *multiplication-by-a-on-the-left* linear map L_a. Since A is a simple algebra, the map $a \mapsto L_a$ is injective. By equality of dimensions, it is an isomorphism. □

A well-known fact is that the tensor product of central simple algebras remains central simple.

Lemma 3.2.7 ([36, Lemma 2.2.5])**.** *Let A and B be central simple k-algebras. Then $A \otimes_k B$ is also a central simple k-algebra.*

Central simple algebras form a group under this operation when considered up to a specific equivalence relationship. This group, called the Brauer group, is an algebraic invariant of the field k. We summarize the results that lead to the construction of the Brauer group:

Definition 3.2.8. *Let A be a k-algebra. The* opposite algebra *of A is the k-algebra A^{op} defined as follows: As a k-vector space, A^{op} is isomorphic to A. If $a \in A$, we write a^{op} for the corresponding element in A^{op}. Then, the multiplication in A^{op} is defined as follows: for $a, b \in A^{\mathrm{op}}$, $a^{\mathrm{op}} b^{\mathrm{op}} = (ba)^{\mathrm{op}}$.*

Definition 3.2.9. *Two central simple k-algebras A and B are said to be* Brauer-equivalent*, denoted by $A \sim_{\mathrm{Br}} B$, if there exist $d, d' \in \mathbb{N}$ such that*

$$A \otimes_k M_d(k) \simeq B \otimes_k M_{d'}(k).$$

We denote the equivalence class of an algebra A for this relation by $[A]_{\mathrm{Br}}$.

We state a lemma which gives a criterion for proving Brauer equivalence:

Lemma 3.2.10 ([74, Lemma 3.4])**.** *Let A be a central simple k-algebra, and let $e \in A$ be idempotent. Then eAe is a central simple k-algebra which is Brauer-equivalent to A.*

We now present the construction of the Brauer group:

Proposition 3.2.11 ([36, Proposition 2.4.7])**.** *If A, A', B, B' are central simple k-algebras, such that $A \sim_{\mathrm{Br}} A'$ and $B \sim_{\mathrm{Br}} B'$, then $A \otimes_k B \sim_{\mathrm{Br}} A' \otimes_k B'$. The set of Brauer-equivalence classes of central simple k-algebras forms an abelian group. Its neutral element is the class of split algebras, and the inverse of the class of A is the class of A^{op}.*

Definition 3.2.12. *The group formed by Brauer equivalence classes of central simple k-algebras with the tensor product is called the* Brauer group of k. *It is denoted by* $\mathrm{Br}(k)$. *If K/k is a field extension, there is a map* $\mathrm{Res}_{K/k}\colon \mathrm{Br}(k) \to \mathrm{Br}(K)$ *sending the class of some k-algebra A to the class of A_K. The kernel of this map is called the* relative Brauer group of k with respect to K, *denoted by* $\mathrm{Br}(K/k)$.

More generally, if K is a commutative k-algebra, we may define the group $\mathrm{Br}(K/k)$ *as the subgroup of* $\mathrm{Br}(k)$ *of classes of algebras A such that $A_K \simeq \mathrm{End}_K(P)$, for some projective K-module P.*

Remark 3.2.13. The Brauer group is also defined for a general commutative ring and even for a scheme in the literature, but we shall not need such generality in this work (see [18, 33] for details). We note that our definition of $\mathrm{Br}(K/k)$ then coincides with the kernel of the map sending a k-algebra A to A_K for any commutative k-algebra K.

Next, we record two fundamental theorems on central simple algebras. First is the Skolem-Noether theorem:

Theorem 3.2.14 ([69, Theorem 7.21])**.** *Let A be a central simple k-algebra and let B be a simple k-subalgebra of A (e.g a field extension). Then, if $\tilde{B}$ is a k-subalgebra of A and $\varphi\colon B \to \tilde{B}$ is an isomorphism, there exists $a \in A^\times$ such that the restriction of the inner automorphism $x \mapsto axa^{-1}$ to B coincides with φ.*

The second is the double centraliser theorem. We first define the centraliser and then state the theorem.

Definition 3.2.15. *Let A be a k-algebra and let $B \subset A$. Then, the* centralizer *of B in A is the subalgebra*

$$C_A(B) \coloneqq \{x \in A\colon \forall b \in B,\ xb = bx\}.$$

Theorem 3.2.16. *Let A be a central simple k-algebra, and let $B \subset A$ be a simple subalgebra. Then,*

1. *$C_A(B)$ is simple.*
2. *$[B : k][C_A(B) : k] = [A : k]$.*
3. *$C_A(C_A(B)) = B$.*
4. *If B is central simple, then $C_A(B)$ is central simple, and $A = B \otimes C_A(B)$.*

A useful corollary is the following:

Corollary 3.2.17. *Let A be a central simple k-algebra of degree d, and let $K \subset A$ be a subalgebra such that K/k is a degree d field extension. Then*

$$C_A(K) = K.$$

Proof. This is Item 2 of Theorem 3.2.16, coupled with the fact that $[K : k]^2 = [A : k]$). □

Finally, we give a useful characterisation of $\mathrm{Br}(K/k)$ when K is an étale k-algebra:

Proposition 3.2.18. *If K is an étale k-algebra of dimension d and A is a central simple k-algebra of degree d, then the class of A is in $\mathrm{Br}(K/k)$ if and only if A contains a subalgebra isomorphic to K.*

Proof. If K is a field, then this is [36, Proposition 2.2.9]. Otherwise, this is a consequence of [33, Theorem 7.4.2]. □

3.2.2 Algebraic presentations of central simple algebras

Early XXth century investigations on division algebras led to several constructions of central simple algebras, relying on simpler algebraic objects. Such constructions would yield a presentation for the algebra, and the question of finding an isomorphism between thus presented algebras would translate into a multiplicative equation expressed over the centre. This section recalls three such constructions introduced by Dickson, Noether and Brauer. In modern references, the constructions of Dickson and Noether (respectively of cyclic and crossed-product algebras) are discussed with the language of Galois cohomology (see e.g. [36, 74]). The construction of Brauer also admits a cohomological interpretation once the definitions of Galois cohomology are extended to non-Galois field extensions. [1].

While the cohomological formulation allows for a powerful theory, the computational nature of our concerns leads us to prefer elementary and explicit presentations. As we will not need the powerful machinery of Galois cohomology, we present the constructions mentioned above in elementary language. Historically minded accounts of these constructions in modern language are given in [58] for Dickson's cyclic algebras and in [50] for Noether's crossed products and Brauer's factor sets.

The three constructions we discuss below are related in the following way: cyclic algebras are a particular case of crossed-product algebras, which are themselves a particular case of algebras defined by a Brauer factor set. For each construction, we get similar structural results. While these results may be proved in a self-contained manner for each construction, we chose for simplicity to prove the results for the particular cases as consequences of the results for the more general construction.

Brauer factor sets

For this paragraph, K is an étale k-algebra of degree d. We let E be a splitting field of K over k and $G = \mathrm{Gal}(E/k)$. We also let Φ be the set of nonzero homomorphisms of k-algebra from K to E. We note that the cardinal of Φ is d by Corollary 2.1.17. We define Brauer factor sets as algebraic objects which classify central simple algebras of degree n that contain a copy of K as a subalgebra. We also explicitly describe $\mathrm{Br}(K/k)$. The exposition, again, follows loosely that of [51, Chapter 2].

Definition 3.2.19. *A* Brauer factor set *for the k-algebra K is a map*

$$\begin{array}{rccc} c\colon & \Phi\times\Phi\times\Phi & \to & E^\times \\ & (\rho,\sigma,\tau) & \mapsto & c_{\rho,\sigma,\tau} \end{array}$$

which satisfies the following conditions: for $\alpha,\beta,\gamma\in\Phi$ and $\pi\in G$,

$$c_{\pi\alpha,\pi\beta,\pi\gamma} = \pi(c_{\alpha,\beta,\gamma}), \tag{3.2}$$

and for $\alpha,\beta,\gamma,\delta\in\Phi$,

$$c_{\alpha,\beta,\gamma}c_{\alpha,\gamma,\delta} = c_{\alpha,\beta,\delta}c_{\beta,\gamma,\delta}. \tag{3.3}$$

The Brauer factor sets form a group, which we denote by $Z^2_{\mathrm{Br}}(K/k,E^\times)$.

The condition defined by Equation (3.2) is called homogeneity. It extends in an obvious manner to maps from Φ^n to A, for any $n\in\mathbb{N}$ and $A\subset E$ stable by the action of Galois.

Definition 3.2.20. *Let $c\in Z^2_{\mathrm{Br}}(K/k,E^\times)$ be a Brauer factor set. We let V be the k-vector space of homogeneous maps $\ell\colon\Phi\times\Phi\to E$. For $\ell,\ell'\in V$, we define the product as follows:*

$$(\ell\ell')_{\alpha,\beta} = \sum_{\gamma\in\Phi}\ell_{\alpha,\gamma}c_{\alpha,\gamma,\beta}\ell'_{\gamma,\beta}. \tag{3.4}$$

This yields a k-algebra of dimension n^2 called the Brauer algebra determined by *c, and denoted by $B(K, c)$.*

Proposition 3.2.21 ([51, Theorem 2.5.6])**.** *If $c \in Z^2_{\mathrm{Br}}(K/k, K^\times)$, the algebra $B(K, c)$ is a central simple k algebra of degree n containing K as a subalgebra. Conversely, if A is such an algebra, then there exists $c \in Z^2_{\mathrm{Br}}(K/k, K^\times)$ such that $A \simeq B(K, c)$.*

Definition 3.2.22. *A Brauer factor set $c \in Z^2_{\mathrm{Br}}(K/k, E^\times)$ is called* associated *if there exists a homogeneous map $a \colon \Phi \times \Phi \to E^\times$ such that for $\alpha, \beta, \gamma \in \Phi$,*

$$c_{\alpha,\beta,\gamma} = \partial_{\mathrm{Br}}(a) \coloneqq a_{\alpha,\beta} a_{\beta,\gamma} a^{-1}_{\alpha,\gamma}.$$

Such a map a is called a trivialisation *of c. The group of associated Brauer factor sets is denoted by $B^2_{\mathrm{Br}}(K/k, E^\times)$, and we define the factor group*

$$H^2_{\mathrm{Br}}(K/k, E^\times) = Z^2_{\mathrm{Br}}(K/k, E^\times)/B^2_{\mathrm{Br}}(K/k, E^\times).$$

Proposition 3.2.23 ([51, Theorem 2.3.21])**.** *Let $c, c' \in Z^2_{\mathrm{Br}}(K/k, E^\times)$. Then the algebras $B(K, c)$ and $B(K, c')$ are isomorphic if and only if $c(c')^{-1} = \partial_{\mathrm{Br}}(a)$ for some homogeneous maps $a \colon \Phi \times \Phi \to E^\times$. In that case, the map*

$$\begin{array}{ccc} B(K, c) & \to & B(K, c') \\ \ell & \mapsto & (a_{\alpha,\beta} \ell_{\alpha,\beta})_{\alpha,\beta \in G} \end{array}$$

is an isomorphism.

Remark 3.2.24. In [51], the author introduces the notion of a reduced factor set. A factor set c is reduced if $c_{\alpha,\alpha,\alpha} = 1$ for all $\alpha \in \Phi$. Propositions 3.2.21 and 3.2.23 are stated with the additional hypothesis that the factor sets involved be reduced. This hypothesis is, in fact, not necessary for our relaxed statement of Proposition 3.2.23, where we do not impose that the isomorphism between $B(K, c)$ and $B(K, c')$ fixes the image of K in these algebras.

The multiplication of factor sets is compatible with the multiplication operation in the Brauer group of k:

Proposition 3.2.25 ([51, Theorem 2.4.6])**.** *Let $c, c' \in Z^2_{\mathrm{Br}}(K/k, E^\times)$. Then we have the Brauer equivalence*

$$B(K, cc') \sim_{\mathrm{Br}} B(K, c) \otimes B(K, c').$$

We will see that the map $c \mapsto B(K, c)$ yields a group homomorphism from $H^2_{\mathrm{Br}}(K/k, E^\times)$ to $\mathrm{Br}(K/k)$. In order to prove that, it remains to see that the algebra $Br(K, \mathbf{1})$ is split.

Example 3.2.26 (The trivial factor set). The trivial Brauer factor set is the factor set $\mathbf{1}$ defined by $\mathbf{1}_{\alpha,\beta,\gamma} = 1$ for all $\alpha, \beta, \gamma \in \Phi$. Set $\Phi = \{\varphi_1, \ldots, \varphi_d\}$, so that a map $\Phi \times \Phi \to E$ identifies with a matrix in $M_d(E)$. Then, the vector space $B(K, c)$ of homogeneous maps is identified with a subspace of $M_d(E)$. Applying Equation (3.4) to the trivial factor set, we find that multiplication in $B(K, c)$ coincides with multiplication in $M_d(E)$. Now, $B(K, c)$ contains the rank one matrix $z = (1)_{i,j\in[n]}$. Since $[M_n(E)z : E] = d$, we have $[B(K, c)z : k] = d$. Then, z has rank one as an element of $B(K, c)$ and therefore, the algebra $B(K, c)$ is split by Proposition 3.2.6.

We may gather the results of this section in the following theorem:

Theorem 3.2.27. *If $c \in Z^2_{\mathrm{Br}}(K/k, E^\times)$, the algebra $B(K, c)$ is central simple of degree d. Then the map $c \mapsto [B(K, c)]_{\mathrm{Br}}$ factors through $H^2_{\mathrm{Br}}(K/k, E^\times)$ and yields an isomorphism between $H^2_{\mathrm{Br}}(K/k, E^\times)$ and $\mathrm{Br}(K/k)$.*

Crossed-product algebras

Here, we let K/k be a Galois field extension of degree d. We also let G be the Galois group $\mathrm{Gal}(K/k)$. We will define the so-called Noether factor sets for the extension K/k and the crossed-product algebra associated with such a factor set. Then, we will show that Noether factor sets coincide with Brauer factor sets for the extension K/k, and we will recover Theorem 3.2.27 in terms of Noether factor sets, as well as the explicit expression for isomorphisms given in Proposition 3.2.23. We loosely follow the exposition from [51, Section 2.6].

Definition 3.2.28. *A* Noether factor set *for the extension K/k is a map*

$$\begin{array}{rccc} c\colon & G \times G & \to & K^\times \\ & (\sigma, \tau) & \mapsto & c_{\sigma,\tau} \end{array}$$

which satisfies the following condition: for $\sigma, \tau, \rho \in G$,

$$c_{\sigma,\tau} c_{\sigma\tau,\rho} = c_{\sigma,\tau\rho}\sigma(c_{\tau,\rho}) \tag{3.5}$$

The Noether factor sets form a group, denoted by $Z^2(K/k, K^\times)$.

Definition 3.2.29. *Let $c \in Z^2(K/k, K^\times)$ be a Noether factor set. We let V be the K-vector space K^d and denote the elements of it canonical basis by*

$(u_\sigma)_{\sigma\in G}$. *Then, V admits a natural structure of k-vector space of dimension n^2. We define a product on V as follows: For $\alpha, \beta \in K^G$,*

$$\left(\sum_{\sigma\in G} \alpha_\sigma u_\sigma\right)\left(\sum_{\tau\in G} \beta_\tau u_\tau\right) = \sum_{\sigma,\tau\in G} c_{\sigma,\tau}\alpha_\sigma\sigma(\beta_\tau)u_{\sigma\tau}. \tag{3.6}$$

This yields a k-algebra of dimension n^2 which we call the crossed-product of K with c. *It is denoted by $\Delta(K/k, c)$.*

Definition 3.2.30. *A Noether factor set $c \in Z^2(K/k, K^\times)$ is called* associated *if there exists a map $a\colon G \to K^\times$ such that for $\sigma, \tau \in G$,*

$$c_{\sigma,\tau} = \partial(a) \coloneqq a_\sigma\sigma(a_\tau)a_{\sigma\tau}^{-1}.$$

The subgroup of associated Noether factor sets is denoted by $B^2(K/k, K^\times)$, and we define the factor group

$$H^2(K/k, K^\times) = Z^2(K/k, K^\times)/B^2(K/k, K^\times).$$

Now, we wish to recover the results from the previous section. For this, we will give a map $\iota\colon Z^2(K/k, K^\times) \to Z^2_{\mathrm{Br}}(K/k, K^\times)$ (here we have $E = K$ and $\Phi = G$ since K/k is a Galois extension) and prove that it induces an isomorphism $H^2(K/k, K^\times) \simeq H^2_{\mathrm{Br}}(K/k, K^\times)$. We will also show that $\Delta(K/k, c) \simeq B(K/k, \iota(c))$, and get an explicit expression for an isomorphism from $\Delta(K/k, c)$ to $\Delta(K/k, c')$ when $c(c')^{-1} \in B^2(K/k, K^\times)$.

We define the following maps:

$$\begin{array}{rccc} \iota\colon & Z^2(K/k, K^\times) & \to & Z^2_{\mathrm{Br}}(K/k, K^\times) \\ & (c_{\sigma,\tau})_{\sigma,\tau\in G} & \mapsto & (\iota(c)_{\rho,\sigma,\tau})_{\rho,\sigma,\tau\in G} \coloneqq (\rho(c_{\rho^{-1}\sigma,\sigma^{-1}\tau}))_{\rho,\sigma,\tau\in G} \end{array}$$

$$\begin{array}{rccc} \kappa\colon & Z^2_{\mathrm{Br}}(K/k, K^\times) & \to & Z^2(K/k, K^\times) \\ & (c_{\rho,\sigma,\tau})_{\rho,\sigma,\tau\in G} & \mapsto & (\kappa(c))_{\sigma,\tau\in G} \coloneqq (c_{1,\sigma,\sigma\tau})_{\sigma,\tau\in G} \end{array}$$

One can easily check that the maps ι and κ are mutually inverse group isomorphisms. Furthermore, assume that $c = \partial(a) \in B^2(K/k, K^\times)$ and consider the homogeneous map

$$\begin{array}{rccc} b\colon & G\times G & \to & K^\times \\ & (\sigma,\tau) & \mapsto & b_{\sigma,\tau} \coloneqq \sigma(a_{\sigma^{-1}\tau}) \end{array}.$$

The map b is homogeneous, and we get

$$\begin{aligned}\iota(c) &= \iota\left((a_\sigma\sigma(a_\tau)a_{\sigma\tau}^{-1})_{\sigma,\tau\in G}\right)\\ &= \left(\rho(a_{\rho^{-1}\sigma})\sigma(a_{\sigma^{-1}\tau})\rho(a_{\rho^{-1}\tau})^{-1}\right)_{\rho,\sigma,\tau\in G}\\ &= (\partial_{\mathrm{Br}}(b)_{\rho,\sigma,\tau})_{\rho,\sigma,\tau\in G}.\end{aligned}$$

That is, $\iota(B^2(K/k,K^\times)) \subset B^2_{\mathrm{Br}}(K/k,K^\times)$. Conversely, we prove that

$$\kappa(B^2_{\mathrm{Br}}(K/k,K^\times)) \subset B^2(K/k,K^\times).$$

Let $c = \partial_{\mathrm{Br}}(a) \in B^2_{\mathrm{Br}}(K/k,K^\times)$. We set

$$\begin{array}{rccc} b\colon & G & \to & K^\times \\ & \sigma & \mapsto & b_\sigma \coloneqq a_{1,\sigma}. \end{array}$$

We compute:

$$\begin{aligned}\kappa(c) &= \kappa\left((a_{\rho,\sigma}a_{\sigma,\tau}a_{\rho,\tau}^{-1})_{\rho,\sigma,\tau\in G}\right)\\ &= \left(a_{1,\sigma}a_{\sigma,\sigma\tau}a_{1,\sigma\tau}^{-1}\right)_{\sigma,\tau\in G}\\ &= \left(a_{1,\sigma}\sigma(a_{1,\tau})a_{1,\sigma\tau}^{-1}\right)_{\sigma,\tau\in G}\\ &= \left(b_\sigma\sigma(b_\tau)b_{\sigma\tau}^{-1}\right)_{\sigma,\tau\in G}\\ &= \partial(b)\end{aligned}$$

and we get

$$\kappa\left(B^2_{\mathrm{Br}}(K/k,K^\times)\right) \subset B^2(K/k,K^\times).$$

It follows that the maps ι and κ yield mutually inverse group isomorphisms of $H^2(K/k,K^\times)$ and $H^2_{\mathrm{Br}}(K/k,K^\times)$.

Next, we prove that for $c \in Z^2(K/k,K^\times)$, $\Delta(K/k,c) \simeq B(K,\iota(c))$. Consider the map

$$\begin{array}{rccc} \eta\colon & B(K,c) & \to & \Delta(K/k,\kappa(c)) \\ & \ell & \mapsto & \sum_{\sigma\in G}\ell_{1,\sigma}u_\sigma. \end{array}$$

The map η is clearly k-linear. We check that it is a homomorphism of

k-algebras. Let $\ell, \ell' \in B(K,c)$, and we compute:

$$\begin{aligned}
\eta(\ell\ell') &= \sum_{\sigma\in G} (\ell\ell')_{1,\sigma} u_\sigma \\
&= \sum_{\sigma\in G}\sum_{\tau\in G} \ell_{1,\tau}\ell'_{\tau,\sigma} c_{1,\tau,\sigma} u_\sigma \\
&= \sum_{\sigma,\tau\in G} \ell_{1,\tau}\tau(\ell'_{1,\tau^{-1}\sigma})\kappa(c)_{\tau,\tau^{-1}\sigma} u_\sigma \\
&= \sum_{\sigma,\tau\in G} \ell_{1,\tau} u_\tau \ell'_{1,\tau^{-1}\sigma} u_{\tau^{-1}\sigma} \\
&= \sum_{\rho,\tau\in G} \left(\ell_{1,\tau}u_\tau\right)\left(\ell'_{1,\rho}u_\rho\right) \\
&= \left(\sum_{\tau\in G} \ell_{1,\tau}u_\tau\right)\left(\sum_{\rho\in G} \ell'_{1,\rho}u_\rho\right) \\
&= \eta(\ell)\eta(\ell').
\end{aligned}$$

Now, since $[B(K,c) : k] = [\Delta(K/k, \kappa(c)) : k]$ and $B(K,c)$ is a simple algebra, the map η is in fact an isomorphism. One may check easily that its inverse is

$$\begin{array}{rccc}
\xi\colon & \Delta(K/k,c) & \to & B(K,\iota(c)) \\
& a = \sum_{\sigma\in G} a_\sigma u_\sigma & \mapsto & \xi(a)\colon (\sigma,\tau) \mapsto \sigma(a_{\sigma^{-1}\tau}).
\end{array}$$

This entire discussion proved the following as a consequence of Theorem 3.2.27:

Theorem 3.2.31. *If $c \in Z^2(K/k, K^\times)$, the algebra $\Delta(K/k,c)$ is central simple of degree n. The map $c \mapsto [\Delta(K/k,c)]_{\mathrm{Br}}$ factors through $H^2(K/k,K^\times)$ yields an isomorphism between $H^2(K/k,K^\times)$ and $\mathrm{Br}(K/k)$.*

As with the Brauer factor set, we have an explicit expression for an isomorphism between crossed-products with associated Noether factor sets.

Proposition 3.2.32. *Let $c, c' \in Z^2(K/k,K^\times)$, and let $b\colon G \to K^\times$ such that $cc'^{-1} = \partial(b)$. Then an isomorphism $\Delta(K/k,c) \to \Delta(K/k,c')$ is given by the map that is the map*

$$\sum_{\sigma\in G} a_\sigma u_\sigma \mapsto \sum_{\sigma\in G} a_\sigma b_\sigma u_\sigma$$

Proof. This isomorphism is $\eta^{-1}\circ\varphi\circ\xi$, where φ is the isomorphism from $B(K,\kappa(c))$ to $B(K/,\kappa(c'))$ given by Proposition 3.2.23 and the fact that b' is a trivialisation of $\kappa(cc'^{-1})$, where $b'_{\sigma,\tau} = \sigma(b_{\sigma^{-1}\tau})$. □

It is implied by Example 3.2.26 and the discussion above that the algebra $\Delta(K, 1)$ is isomorphic to $M_d(k)$. In the example below, we give an independent proof of this fact and give an explicit isomorphism.

Example 3.2.33 (The trivial crossed-product algebra). Fix a basis $(e_1, \dots, e_d)$ of K. Then, any k-linear endomorphism of K may be identified with a matrix in $M_d(k)$. If $\alpha \in K$, write L_α for the matrix corresponding to multiplication on the left by α. For $\sigma \in G$, we also write T_σ for the matrix corresponding to the automorphism σ of K. Then, by a well-known theorem of Artin (see, e.g. [11, Theorem V.66.3]), the family $(L_{e_i} T_\sigma)_{\substack{1 \le i \le d \\ \sigma \in G}}$ gives a basis of $M_d(k)$.

Now, observe that if $\alpha, \beta \in K$ and $\sigma, \tau \in G$,

$$L_\alpha T_\sigma L_\beta T_\tau = L_\alpha L_{\sigma(\beta)} T_{\sigma\tau}.$$

It follows directly that the map

$$\begin{array}{ccc} \Delta(K, 1) & \to & M_n(k) \\ \sum_{\sigma \in G} a_\sigma u_\sigma & \mapsto & \sum_{\sigma \in G} L_{a_\sigma} T_\sigma \end{array}$$

is an isomorphism of k-algebras.

Cyclic algebras

Let k be a field and let K/k be a cyclic extension of k of degree d. That is, K/k is a finite Galois field extension and the Galois group $G := \mathrm{Gal}(K/k)$ is cyclic. We fix a generator θ of G.

Definition 3.2.34. *Let $a \in k^\times$. We let V be the left K-vector space K^n, and we name the elements of its canonical basis $1, y, \dots, y^{d-1}$. Then V naturally has a structure of d^2-dimensional k-vector space. We define a multiplication on V by linearly extending the rule*

$$(\alpha y^i)(\beta y^j) = a^{\lfloor (i+j)/d \rfloor} \alpha \theta^i(\beta) y^{i+j \mod d}$$

for $0 \le i, j \le n-1$ and $\alpha, \beta \in K$.

To put it more simply, the multiplication on V is given by the following rules: for $i, j \in [d]$,

$$y^i y^j = y^{i+j},$$

$$y^n = a,$$

and for $\alpha \in K$,

$$y\alpha = \theta(\alpha) y.$$

The algebra formed by the k-vector space V with the product defined above is called a cyclic algebra. *We denote it by the symbol $\langle K/k, \theta, a\rangle$.*

We will prove that every class in $\mathrm{Br}(K/k)$ contains an algebra of this form and that this yields an isomorphism $k^\times/N_{K/k}(K^\times) \simeq \mathrm{Br}(K/k)$. We will obtain this result as a consequence of Theorem 3.2.31 once we give a compatible isomorphism $k^\times/N_{K/k}(K^\times) \simeq H^2(K/k, K^\times)$.

Consider the map

$$\begin{array}{rccc} \chi\colon & k^\times & \to & Z^2(K/k, K^\times) \\ & b & \mapsto & \chi(b), \end{array}$$

where

$$\chi(b)_{\theta^i,\theta^j} = \begin{cases} 1 & \text{if } i+j < d \\ b & \text{otherwise.} \end{cases}$$

First, we prove that $\chi(b) \in B^2(K/k, K^\times)$ if and only if $b \in N_{K/k}(K^\times)$. Let $a \in K^\times$, and let $\alpha\colon G \to K^\times$ defined by $\alpha_{\theta^i} = \prod_{j=0}^{i-1} \theta^i(a)$ for $i \in [d-1]_0$. We show that $\chi(N_{K/k}(a)) = \partial(\alpha)$. Indeed, we let $i, j \in [n-1]_0$. We note that

$$\alpha_{\theta^i}\theta^i(\alpha_{\theta^j}) = \prod_{\ell=0}^{i-1} \theta^i(a) \prod_{\ell=0}^{j-1} \theta^{i+\ell}(a) = \prod_{\ell=0}^{i+j-1} \theta^\ell(a),$$

and

$$\alpha_{\theta^i\theta^j} = \begin{cases} \prod_{\ell=0}^{i+j-1} \theta^\ell(a) = \alpha_{\theta^i}\theta^i(\alpha_{\theta^j}) & \text{if } i+j < d \\ \prod_{\ell=0}^{i+j-n-1} \theta^\ell(a) = a_{\theta^i}\theta^i(\alpha_{\theta^j})N_{K/k}(a)^{-1} & \text{otherwise.} \end{cases}$$

It follows that $\chi(N_{K/k}(a)) = \partial(\alpha) \in B^2(K/k, K^\times)$.

Conversely, let $c \in k^\times$ such that $\chi(c) \in B^2(K/k, K^\times)$. Let $\alpha\colon G \to K^\times$ such that $\chi(c) = \partial(\alpha)$. Then, we know that if $i + j < d$, for $i, j \in [d-1]_0$, $\partial(\alpha)_{\theta^i,\theta^j} = 1$. That is,

$$\alpha_{\theta^i}\theta^i(\alpha_{\theta^j}) = \alpha_{\theta^{i+j}}.$$

Setting $i = 0$, we get $a_1 = 1$. Setting $i = 1$ and $j < d-1$, we show that

$$a_{\theta^{j+1}} = a_\theta\theta(a_{\theta^j}),$$

and by a straightforward induction, it follows that for $i \in [d-1]_0$,

$$a_{\theta^i} = \prod_{\ell=0}^{i-1} \theta^\ell(a_\theta).$$

It is then easy to check that $c = N_{K/k}(a_\theta)$.

Putting things together, we have proved that the map χ yields an injective group homomorphism from $k^\times/N_{K/k}(K^\times)$ to $H^2(K/k, K^\times)$. Unfortunately, the map χ, seen as a map from $k^\times$ to $Z^2(K/k, K^\times)$ is not surjective. In order to prove that its factor from $k^\times/N_{K/k}(K^\times)$ to $H^2(K/k, K^\times)$ is, we must prove that for any $c \in Z^2(K/k, K^\times)$, there exist $b \in k^\times$ and $\alpha\colon G \to K$ such that $\chi(b)\partial(a) = c$.

Let $c \in Z^2(K/k, K^\times)$, and we let $\alpha\colon G \to K^\times$ be defined by $\alpha_1 = 1$ and $\alpha_{\theta^i} = \prod_{\ell=1}^{i-1} c_{\theta^\ell,\theta}$ for $i \in [n-1]$. We may quickly observe that if i or j is zero, $\partial(\alpha)_{\theta^i,\theta^j} = 1$. Otherwise, we let $i, j \in [d-1]$ and we first compute

$$\begin{aligned}
\alpha_{\theta^i}\theta^i(\alpha_{\theta^j}) &= \prod_{\ell=1}^{i-1} c_{\theta^\ell,\theta} \prod_{\ell=1}^{j-1} \theta^i(c_{\theta^\ell,\theta}) \\
&= \prod_{\ell=1}^{i-1} c_{\theta^\ell,\theta} \prod_{\ell=1}^{j-1} c^{-1}_{\theta^i,\theta^{\ell+1}} c_{\theta^i,\theta^\ell} c_{\theta^{i+\ell},\theta} \quad \text{(by Equation (3.5))} \\
&= c^{-1}_{\theta^i,\theta^j} \prod_{\ell=1}^{i+j} c_{\theta^\ell,1}
\end{aligned}$$

Now, observe that

$$\alpha_{\theta^{i+j}} = \begin{cases} \prod_{\ell=1}^{i+j-1} c_{\theta^\ell,\theta} & \text{if } i+j < n \\ 1 \quad \text{if } i+j = d & \\ \prod_{\ell=1}^{i+j-d-1} c_{\theta^\ell,\theta} & \text{otherwise.} \end{cases}$$

It follows that

$$c_{\theta^i,\theta^j}\partial(a)_{\theta^i,\theta^j} = \begin{cases} 1 & \text{if } i+j < d \\ b & \text{otherwise,} \end{cases}$$

where $b = \prod_{\sigma\in G} c_{\sigma,\theta}$. Now, using Equation (3.5) again, one may check that for $\tau \in G$, $\tau(b) = b$, and therefore $b \in k^\times$, and

$$c = \chi(b)\partial(a^{-1}).$$

We showed that the map χ factors into an isomorphism from $k^\times/N_{K/k}(K^\times)$ to $H^2(K/k, K^\times)$. Now, it remains for us to show that if $c \in k^\times$, $\langle K/k, \theta, c\rangle \simeq \Delta(K, \chi(c))$. Let $c \in k^\times$ and consider the map

$$\begin{array}{rccc} \psi\colon & \Delta(K,\chi(c)) & \to & \langle K/k,\theta,c\rangle \\ & \sum_{i=0}^{d-1} a_i u_{\theta^i} & \mapsto & \sum_{i=0}^{d-1} a_i y^i \end{array}$$

One may check directly that this map is a homomorphism of k-algebras, and since the algebra $\Delta(K, \chi(c))$ is simple and $[\Delta(K, \chi(c)) : k] = [\langle K/k, \theta, c\rangle : k]$, it is an isomorphism. From the discussion above and Theorem 3.2.31, we get the following:

Theorem 3.2.35. *If $c \in k^\times$, the algebra $\langle K/k, \theta, c\rangle$ is central simple of degree n. The map $c \mapsto [\langle K/k, \theta, c\rangle]_{\mathrm{Br}}$ yields an isomorphism from $k^\times/N_{K/k}(K^\times)$ to $\mathrm{Br}(K/k)$.*

Applying the isomorphisms defined above to Proposition 3.2.32, we get the following:

Proposition 3.2.36. *Let $c, c' \in k^\times$, and let $b \in K^\times$ such that $cc'^{-1} = N_{K/k}(b)$. Then, an isomorphism from $\langle K/k, \theta, c\rangle$ to $\langle K/k, \theta, c'\rangle$ is given by the map defined by*

$$\sum_{i=0}^{d-1} a_i y^i \mapsto \sum_{i=0}^{d-1} a_i \left(\prod_{j=0}^{i-1} \theta^j(b)\right) y^i.$$

3.3 Computational representations of central simple algebras

In order to fully define the explicit isomorphism problem, we need to state how algebras are represented computationally. In this section, we present several possible representations, and in the next section, we discuss how these affect the explicit isomorphism problem.

3.3.1 Computational representations

If K/k is a cyclic extension of degree d with fixed generator θ of its Galois group, any central simple k-algebra of degree d (and thus dimension d^2) which contains a subalgebra isomorphic to K admits a presentation as a cyclic algebra $\langle K/k, \theta, c\rangle$ for some $c \in k^\times$. An element $\sum_{i=0}^{d-1} a_i y^i$ of $\langle K/k, \theta, c\rangle$ may then be represented by the coordinate vector $(a_i)_{0\le i\le d-1} \in K^d$. The sum of elements of this algebra is then represented by the sum of their coordinate vectors, and the representation of the product may be computed via the formula

$$\left(\sum_{i=0}^{d-1} a_i y^i\right)\left(\sum_{j=0}^{d-1} a'_j y^j\right) = \sum_{\ell=0}^{d-1}\left(\sum_{\substack{0\le i,j\le d-1\\ i+j=\ell \mod d}} a_i a'_j \delta_{i+j}\right) y^\ell,$$

where

$$\delta_{i+j} = \begin{cases} 1 & \text{if } i+j < d \\ c & \text{otherwise.} \end{cases}$$

If K/k is a Galois extension of degree d, whose Galois group is $G = \{\sigma_0, \ldots, \sigma_{d-1}\}$, any central simple k-algebra which contains a subalgebra isomorphic to K admits a presentation as a crossed-product algebra $\Delta(K, c)$ for some $Z^2(K/k, K^\times)$. An element $\sum_{i=0}^{d-1} a_i u_{\sigma_i}$ of $\Delta(K, c)$ may then represented by the vector $(a_i)_{0 \le i \le d-1} \in K^d$. The sum of elements of this algebra is then represented by the sum of their coordinate vectors, and the representation of the product may be computed via Equation (3.6).

In the general case that K/k is an étale algebra of degree d, and $B(K, c)$ is a Brauer algebra, the degree of the smallest splitting field E may be as large as $d!$, preventing us from representing the algebra $B(K, c)$ in a straightforward manner as in the case of cyclic and crossed-product algebras. In Chapter 4, we find a different algebraic presentation isomorphic to $B(K, c)$, which admits an efficient computational representation.

3.3.2 Finding an algebraic representation of an algebra

There are obvious polynomial-time algorithms which, taking respectively as input a cyclic presentation and a crossed-product presentation of an algebra, output structure constants for this algebra. Indeed, multiplications may be computed in polynomial time, so one may pick a convenient basis and compute the coordinates of every product of pairs of basis elements. We also note that one may efficiently compute a crossed-product presentation of a cyclic algebra by the discussion given in Section 3.2.2. In this section, we consider the reduction problems stated below. We specialise to the case that k is a global field. Then, by the Albert-Brauer-Hasse-Noether theorem, every central simple k-algebra admits a cyclic presentation and, therefore, also a crossed-product presentation. Hence, the following problems always have a solution:

Problem 3.3.1. *Let k be a global field, $d \in \mathbb{N}$ and $(c_{ij\ell}) \in k^{(d^2)^3}$ be structure constants for a central simple k-algebra A of degree d. Find a cyclic extension K/k of degree d, a generator θ of $\mathrm{Gal}(K/k)$, $c \in k^\times$ and an isomorphism from A to $\langle K/k, \theta, c \rangle$.*

Problem 3.3.2. *Let k be a global field, $d \in \mathbb{N}$ and $(c_{ij\ell}) \in k^{(d^2)^3}$ be structure constants for a central simple k-algebra A of degree d. Find a Galois field*

extension K/k of degree d, a Noether factor set $c \in Z^2(K/k, K^\times)$ and an isomorphism from A to $\Delta(K, c)$.

While to the best of our knowledge, there is no efficient solution to either problem, they each reduce to the following respective weakenings:

Problem 3.3.3. *Let k be a global field, $d \in \mathbb{N}$ and $(c_{ik\ell}) \in k^{(d^2)^3}$ be structure constants for a central simple k-algebra A of degree d. Find a subalgebra $K \subset A$ such that K/k is a cyclic field extension of degree d, and compute the Galois group of K/k.*

Problem 3.3.4. *Let k be a global field, $d \in \mathbb{N}$ and $(c_{ik\ell}) \in k^{(d^2)^3}$ be structure constants for a central simple k-algebra A of degree d. Find a subalgebra $K \subset A$ such that K/k is a Galois field extension, and compute the Galois group of K/k.*

We have the following reductions:

Theorem 3.3.5. *Problem 3.3.1 reduces to Problem 3.3.3.*

Theorem 3.3.6. *Problem 3.3.2 reduces to Problem 3.3.4.*

Before we prove the theorems, we need an effective version of the Skolem-Noether Theorem, Theorem 3.2.14:

Lemma 3.3.7. *Let k be a field, $d \in \mathbb{N}$ and $(c_{ij\ell}) \in k^{(d^2)^3}$ be structure constants for a central simple k-algebra A. Let $(b_1, \ldots, b_r)$ and $(b'_1, \ldots, b'_r)$ be bases for simple k-subalgebras B and B' of A, and let $M \in GL_r(k)$ be the matrix of an isomorphism from B to B' with respect to these bases. Then, an element $a \in A$ such that, for any $X = \begin{pmatrix} x_1 & \ldots & x_r \end{pmatrix}^t \in k^r$ and $\begin{pmatrix} y_1 & \ldots & y_r \end{pmatrix}^t = MX$,*

$$a\left(\sum_{i=1}^{r} x_i b_i\right)a^{-1} = \sum_{i=1}^{r} y_i b'_i,$$

may be computed in polynomial time.

Proof. Such an a is a solution of the following linear system of equations:

$$ab_j - \sum_{i=1}^{r} M_{ij} b'_i a = 0 \quad \text{for all } j \in [r].$$

Such a system may be solved in polynomial time. □

The way we prove Theorems 3.3.5 and 3.3.6 is to leverage Lemma 3.3.7 to turn usual constructions of cyclic and crossed-product algebras into algorithms.

Proof of Theorem 3.3.5. Here, we adapt the proof of [36, Proposition 2.5.3]. Let $k, d, (c_{ij\ell}), A$ be as in the statement of Problem 3.3.1, and assume that we know a subalgebra $K \subset A$ such that K/k is a cyclic extension of degree d. We also assume that we know a generator θ of the Galois group of K and that we know how to efficiently compute a representation of $\theta(x)$ for $x \in K$.

Then, by Lemma 3.3.7, we may compute $a \in A$ such that $axa^{-1} = \theta(x)$ for all $x \in K$. Then, for $x \in K$, $ax = \theta(x)a$. Furthermore, by induction we have $a^\ell x a^{-\ell} = \theta^\ell(x)$ for all $x \in K$.

In particular, $a^d x a^{-d} = x$ for $x \in K$. That is, $a^d \in C_A(K)$. By Corollary 3.2.17, it follows that $a^d \in K^\times$. Since a^d commutes with a, we also get $\theta(a^d) = a^d$, so in fact, $a^d \in k^\times$. We let $c = a^d$.

The discussion above proves that the map

$$\begin{array}{ccc} \langle K/k, \theta, c\rangle & \to & A \\ \sum_{i=0}^{d-1} x_i y^i & \mapsto & \sum_{i=0}^{d-1} x_i a^i \end{array}$$

is a k-algebra homomorphism. Since $\langle K/k, \theta, c\rangle$ is simple and the dimensions of $\langle K/k, \theta, c\rangle$ and A are equal, the map above is an isomorphism. □

Proof of Theorem 3.3.6. Here, we adapt the construction discussed in [51, Section 2.6]. Let $k, d, (c_{ij\ell}), A$ be as in the statement of Problem 3.3.2, and assume that we know a subalgebra $K \subset A$ such that K/k is a Galois field extension of degree n. We also assume that we know the Galois group G of K/k in the sense that we may represent its elements, compute their multiplication and compute their action on K. Then, for $\sigma \in G$, we may apply Lemma 3.3.7 to find $a_\sigma \in A$ such that for all $x \in K$, $a_\sigma x a \sigma^{-1} = \sigma(x)$. For $x \in K$, we have:

$$a_{\sigma\tau}^{-1} a_\sigma a_\tau x (a_{\sigma\tau}^{-1} a_\sigma a_\tau)^{-1} = x.$$

As in the proof of Theorem 3.3.5, this shows that $c_{\sigma,\tau} \coloneqq a_{\sigma\tau}^{-1} a_\sigma a_\tau \in K^\times$. A straightforward computation shows that $(c_{\sigma,\tau}) \in Z^2(K/k, K^\times)$. Then, the map

$$\begin{array}{ccc} \Delta(K, c) & \to & A \\ \sum_{\sigma\in G} x_\sigma u_\sigma & \mapsto & \sum_{\sigma\in G} x_\sigma a_\sigma \end{array}$$

is a homomorphism of k-algebra. This map is an isomorphism by simplicity of $\Delta(K, c)$ and equality of dimensions. □

3.4 The explicit isomorphism problem and its variants

In this section, we discuss the explicit isomorphism problem in different forms.

3.4.1 Problem statements and reductions

Various versions of the explicit isomorphism problem

We introduce the following variants:

Problem 3.4.1 (The explicit isomorphism problem)**.** *Let k be a field, $d \in \mathbb{N}$ and $(c_{ij\ell}) \in k^{(d^2)^3}$ be structure constants for an algebra A isomorphic to $M_d(k)$, with respect to some basis $(e_i)_{1\le i\le d^2}$ of A. Find an isomorphism from A to $M_d(k)$. That is, output d^2 matrices $M_i \in M_d(k)$, such that the linear map sending e_i to M_i gives a k-algebra isomorphism.*

Problem 3.4.2 (The explicit isomorphism problem (cyclic version))**.** *Let k be a field, and K/k be a cyclic extension of degree $d \in \mathbb{N}$. Let θ be a generator of the Galois group $\mathrm{Gal}(K/k)$ and let $c \in N_{K/k}(K^\times)$. Find an explicit isomorphism from $\langle K/k, \theta, c\rangle$ to $M_n(k)$. That is, find an embedding $\iota\colon K \to M_d(k)$ and a matrix $Y \in M_d(K)$ such that $\iota(K)$ and Y generate $M_d(k)$ as an algebra, $Y^d = cI_d$ and for any $\alpha \in K$,*

$$Y\iota(\alpha) = \iota(\theta(\alpha))Y.$$

Problem 3.4.3 (The explicit isomorphism problem (crossed-product version))**.** *Let k be a field, and K/k be a Galois extension of degree $d \in \mathbb{N}$. Let $c \in B^2(K/k, K^\times)$. Find an explicit isomorphism from $\Delta(K, c)$ to $M_d(k)$. That is, find an embedding $\iota\colon K \to M_d(K)$ and matrices U_σ for $\sigma \in G = \mathrm{Gal}(K/k)$ such that $\iota(K)$ and the U_σ generate $M_d(k)$ as an algebra, and for $\alpha, \beta \in K$ and $\sigma, \tau \in G$,*

$$\iota(\alpha)U_\sigma\iota(\beta)U_\tau = \iota(\alpha)\iota(\beta)c_{\sigma,\tau}U_{\sigma\tau}.$$

Remark 3.4.4. Generally, we speak of the explicit isomorphism problem for a specific class of fields. In this case, we assume algorithms for representing such fields, and thus, the size of the representation of the base field k is part of the size of the input to the problem.

In general, one version of the explicit isomorphism problem reduces to another if one may deduce one computational representation of an algebra A from another. By the results of Section 3.3.2, we have the following:

Theorem 3.4.5. *1. Problem 3.4.1 reduces to Problems 3.3.4 and 3.4.3.*

2. Problem 3.4.1 reduces to Problems 3.3.3 and 3.4.2.

3. Problem 3.4.3 reduces to Problem 3.4.1.

4. Problem 3.4.3 reduces to Problems 3.3.3 and 3.4.2.

5. Problem 3.4.2 reduces to Problem 3.4.3.

6. Problem 3.4.2 reduces to Problem 3.4.1.

It follows that the cyclic version of the explicit isomorphism problem is weaker than the crossed-product version, which is weaker than the main version. In practice, we will show in the next section that subexponential algorithms exist that solve both the cyclic and the crossed-product versions. However, to the best of our knowledge, there is no known subexponential algorithm which solves Problem 3.3.3, Problem 3.3.4, or Problem 3.4.1. In Chapter 4, we define a new variant of the explicit isomorphism problem, which may be solved in subexponential time and is equivalent to the explicit isomorphism problem.

Zero divisors

If A is an algebra isomorphic to $M_d(k)$, knowing a zero divisor $z \in A$ may help reduce the problem of finding an explicit isomorphism. If a rank one zero divisor is known, it leads directly to a solution to the problem.

We give a generic definition of the rank one element problem, understanding that different versions exist for any possible way to represent the algebra A:

Problem 3.4.6 (The rank one element problem)**.** *Let $A \simeq M_d(k)$ be a k algebra, find a rank one element in A.*

Then, we always have the reduction

Proposition 3.4.7. *Any version of the explicit isomorphism problem reduces to the corresponding version of the rank one element problem.*

Proof. This is a direct consequence of Proposition 3.2.6 and its proof. Indeed, if a rank one element z is known in an algebra A, one may compute a basis of the left ideal Az and then compute the matrix of the multiplication on the left by any $a \in A$. This algorithm only involves a polynomial amount of computations in A and linear algebraic operations. □

If only that a higher rank zero divisor is known, the problem may not instantly be solved, but it reduces to a version of lower degree. This fact is a consequence of the following lemmas:

Lemma 3.4.8. *Given an algebra $A \simeq M_d(k)$ and an element $z \in A$, which is a zero-divisor of rank r, one may compute in polynomial time an idempotent in A of rank* $\min(r, d-r)$.

Proof. If $z \in M_n(k)$ is a zero divisor of rank r, then the left ideal $M_d(k)z$ admits a right unit e. We claim that e is idempotent and has rank r. Then, $1-e$ is an idempotent of rank $n-r$.

We prove the claim: If $z \in M_d(k)$, the left ideal $M_d(k)z$ is the set of matrices M whose image is contained in $\mathrm{Im}(z)$. Then, let e be the matrix of the projection onto $\mathrm{Im}(z)$. It follows that e is an idempotent matrix of rank r. □

The following is a specific version of Lemma 3.2.10.

Lemma 3.4.9. *Let $A \simeq M_d(k)$ be a k-algebra, and let $e \in A$ be an idempotent of rank r. Then eAe is an algebra isomorphic to $M_r(k)$.*

Proof. It is enough to prove the result for $A = M_d(k)$. However, then, e is a projection matrix onto a subspace $V \subset k^n$, and eAe bijectively maps onto $\mathrm{End}_k(V)$ in a way that preserves multiplication. □

We may then express the following weaker variant of Problem 3.4.6:

Problem 3.4.10 (The zero divisor problem)**.** *Let $A \simeq M_d(k)$ be a k algebra, find a zero divisor in A.*

It may seem that the explicit isomorphism problem should reduce to the zero divisor problem. One may repeatedly find a zero divisor $z \in A$, produce an idempotent e of rank $r \leq (\deg A)/2$ and repeat the process with the algebra eAe of degree lesser or equal to $(\deg A)/2$. However, this reduction is only polynomial if one may ensure that the size of the representation of eAe only grows at most sublinearly. To work around this caveat, we may define the problem of reducing the representation size of an algebra $A \simeq M_d(k)$. This problem makes sense since A admits representations of fixed size by virtue of being isomorphic to a matrix algebra,.

3.4.2 Algorithms for the explicit isomorphism problem

Here, we discuss known algorithms for solving Problem 3.4.1 over a global field. One algorithm pertains to number fields. While its complexity is polynomial in the size of the structure constants, it is not in terms of the degree of the algebra A. We also present a polynomial algorithm for rational function fields.

Both algorithms rely on Proposition 3.4.7 and, in fact, solve the rank one element problem (Problem 3.4.6).

For an algebra $A \simeq M_d(k)$, where k is a number field and A is given by structure constants, an algorithm was first proposed in [22], and later generalised in [49] and further improved in [47]. While the complexity of this algorithm is not polynomial in d or the discriminant of k, it is subexponential if these two quantities are bounded. More precisely, it provides an ff-algorithm for the explicit isomorphism problem over a fixed number field with bounded degree. The method is to compute a maximal $\mathcal{O}_k$-order R in A, and to split $A \otimes_k k_P$, where P ranges over M_k^a. These splitting allow one to compute Frobenius norms over A, and one may search for a rank-one element among the small elements of R. The exponential complexity comes from the large search space size in the last step of the algorithm.

For an algebra $A \simeq M_d(k)$, where $k = \mathbb{F}_q(x)$ is a rational function field, a polynomial algorithm was given in [46]. The method is similar to the method for number fields but also allows for a geometric interpretation. One computes a maximal $\mathcal{O}_{fi}$-order R_{fi} and a maximal $\mathcal{O}_\infty$-order R_∞ in A. Then, a rank-one element is found in $R_{fi} \cap R_\infty$. The order R_{fi} plays the role of the maximal order R in the number field case, and elements of $R_{fi} \cap R_\infty$ are analogous to small elements of R_{fi}. While this result is proved in purely algebraic terms in [46], it admits a simple geometric interpretation. After introducing the necessary definitions, we discuss it in Section 5.3.1.

3.4.3 Solving algebraic versions of the explicit isomorphism problem

Here, we discuss known techniques for solving Problems 3.4.2 and 3.4.3 in subexponential time in the case that k is a number field. Both algorithms rely on similar strategies: solving a multiplicative equation and applying either Proposition 3.2.36 or Proposition 3.2.32 to get an isomorphism to $M_d(k)$. More precisely, we have the following problems:

Problem 3.4.11 (Cyclic norm equation)**.** *Let K be a cyclic extension of a global field k. Let $b \in N_{K/k}(K^\times)$. Compute $a \in K^\times$ such that*

$$b = N_{K/k}(a).$$

Problem 3.4.12 (Noether factor set trivialisation)**.** *Let K be a Galois extension of a global field k. Let $b \in B^2(K/k, K^\times)$. Compute $a\colon G \to K^\times$ such that*

$$b = \partial(a).$$

Then, we have the following reductions:

Theorem 3.4.13. *1. Problem 3.4.2 reduces to Problem 3.4.11*

2. Problem 3.4.3 reduces to Problem 3.4.12

Proof. We only state the proof of the first point, as the proof for the second one is similar. Let k, K, d, c be as in the statement of Problem 3.4.3. Then if $a\colon G \to K^\times$ is given such that $c = \partial(a)$, an isomorphism from $A = \Delta(K, c)$ to $\Delta(K, 1)$ may be computed by Proposition 3.2.32. Then, by Example 3.2.33, this yields an isomorphism from A to $M_d(k)$. □

Then, subexponential algorithms solving Problems 3.4.2 and 3.4.3 over a number field follow from the following results:

Theorem 3.4.14. *If k is a number field, Problem 3.4.11 over k may be solved in subexponential time under GRH.*

Theorem 3.4.15. *If k is a number field, Problem 3.4.12 may be solved over k in subexponential time under GRH.*

The first theorem is a particular case of the results of [82]. The second theorem either reduces to factoring and S-unit group computation by [29] or to solving norm equations in relative extensions of number fields by [67]. Note that the problem of solving norm equations reduces to the problems of factoring and computing S-units by [82].

Chapter 4

Computational Amitsur cohomology and the explicit isomorphism problem

This chapter presents results published in [55]. We introduce an algebraic presentation of a central simple algebra using Amitsur cohomology. This representation is as a rephrasing of Brauer algebras. As discussed in Section 3.3, the usual definition of a Brauer algebra does not suggest a reasonable computational representation when the splitting field of K has a large degree. Our equivalent representation relies only on computations in $K^{\otimes 2}$ and $K^{\otimes 3}$, and therefore has polynomial size. Using this representation, we provide a polynomial reduction of the explicit isomorphism problem (Problem 3.4.1) to factorisation and Problem 2.2.16 under GRH, which yields a polynomial quantum algorithm (still under GRH). We prove that we may compute a representation of an algebra from its structure constants in polynomial time (whereas this is not known for cyclic and crossed-product presentations). Then, we prove results analogous to Theorems 3.4.13 and 3.4.15.

4.1 Amitsur cohomology

Definition 4.1.1. *Let R be a ring and S be an R-algebra. We let $C^n_{Am}(R,S)$ be the group $(S^{\otimes(n+1)})^\times$ of units in $S^{\otimes(n+1)}$. Elements of $C^n_{Am}(R,S)$ are called* Amitsur n-cochains of S*, or simply* n-cochains of S *if there is no ambiguity on the type of cohomology.*

We will define a complex

$$\ldots \to C^n_{Am}(R,S) \xrightarrow{\partial^n} C^{n+1}_{Am}(R,S) \to \ldots$$

as follows: let $n \in \mathbb{Z}_{\geq 0}$ and let $i \in [n+1]_0$. We define the R-algebra homomorphism

$$\begin{array}{rccc} \varepsilon^n_i : & S^{\otimes(n+1)} & \to & S^{\otimes(n+2)} \\ & a_0 \otimes a_1 \otimes \ldots \otimes a_n & \mapsto & a_0 \otimes a_1 \otimes \ldots \otimes a_{i-1} \otimes 1 \otimes a_i \otimes \ldots \otimes a_n. \end{array}$$

We may then define the group homomorphism

$$\begin{array}{rccc} \partial^n : & C^n_{Am}(R,S) & \to & C^{n+1}_{Am}(R,S) \\ & a & \mapsto & \prod_{i=0}^{n+1} \varepsilon^n_i(a)^{(-1)^i}. \end{array}$$

We observe that for $n \in \mathbb{N}$, $0 \leq j \leq i \leq n+1$, we have

$$\varepsilon^{n+1}_j \circ \varepsilon^n_i = \varepsilon^{n+1}_{i+1} \varepsilon^n_j. \tag{4.1}$$

We may then prove

Proposition 4.1.2. *Let R be a ring and S an R-algebra, and let $n \in \mathbb{Z}_{\geq 0}$. Then the map $\partial^{n+1} \circ \partial^n : C^n_{Am}(R,S) \to C^{n+2}_{Am}(R,S)$ is the trivial map $a \mapsto 1$. That is, ∂^* is a complex of abelian groups.*

Proof. Applying Equation (4.1), we compute:

$$\begin{aligned} \partial^{n+1} \circ \partial^n &= \left(\prod_{j=0}^{n+2} (\varepsilon^{n+1}_j)^{(-1)^j} \right) \circ \left(\prod_{i=0}^{n+1} (\varepsilon^n_i)^{(-1)^i} \right) \\ &= \left(\prod_{0 \leq j \leq i \leq n+1} (\varepsilon^{n+1}_j \circ \varepsilon^n_i)^{(-1)^{i+j}} \right) \left(\prod_{0 \leq i < j \leq n+2} (\varepsilon^{n+1}_j \circ \varepsilon^n_i)^{(-1)^{i+j}} \right) \\ &= \left(\prod_{0 \leq j \leq i \leq n+1} (\varepsilon^{n+1}_{i+1} \circ \varepsilon^n_{j-1})^{(-1)^{i+j}} \right) \left(\prod_{0 \leq i < j \leq n+2} (\varepsilon^{n+1}_j \circ \varepsilon^n_i)^{(-1)^{i+j}} \right) \\ &= \left(\prod_{0 \leq i < j \leq n+2} (\varepsilon^{n+1}_j \circ \varepsilon^n_i)^{(-1)^{i+j-1}} \right) \left(\prod_{0 \leq i < j \leq n+2} (\varepsilon^{n+1}_j \circ \varepsilon^n_i)^{(-1)^{i+j}} \right) \\ &= \mathbf{1} \end{aligned}$$

□

Using Proposition 4.1.2, we may define the groups of Amitsur cohomology of an R-algebra:

Definition 4.1.3. *Let $n \in \mathbb{Z}_{\geq 0}$. Let R be a ring and S an R-algebra, and let $n \in \mathbb{Z}_{\geq 0}$. We define the following groups:*

- $Z^n_{Am}(R,S) = \text{Ker } \partial^n$ *is the group of* Amitsur n-cocycles *of S.*
- *If $n \geq 1$, we set $B^n_{Am}(R,S) = \text{Im } \partial^{n-1}$ is the group of* Amitsur n-coboundaries *of S if $n \in \mathbb{N}$. We let $B^0(R,S)$ be the trivial group.*
- $H^n_{Am}(R,S) = Z^n_{Am}(R,S)/B^n_{Am}(R,S)$ *is the n-th Amitsur cohomology group of S.*

Applying [33, Theorem 5.5], we get the following base-change result:

Proposition 4.1.4. *Let R be a ring and let S, S' be R-algebras. Let $c = \sum_{i\in I} a_{0i} \otimes \ldots \otimes a_{ni} \in S^{\otimes(n+1)}$. We set*

$$c_{S'} = \sum_{i\in I} (a_{0i} \otimes_R 1) \otimes_{S'} \ldots \otimes_{S'} (a_{ni} \otimes_R 1).$$

Then, $c \in C^n_{Am}(R,S)$ if and only if $c_{S'} \in C^n_{Am}(S', S_{S'})$ and we get a map of complexes:

$$\begin{array}{ccccccc} \ldots & \longrightarrow & C^n_{Am}(R,S) & \xrightarrow{\partial^n} & C^{n+1}_{Am}(R,S) & \longrightarrow & \ldots \\ & & \downarrow{\scriptstyle (\cdot)_{S'}} & & \downarrow{\scriptstyle (\cdot)_{S'}} & & \\ \ldots & \longrightarrow & C^n_{Am}(S', S_{S'}) & \xrightarrow{\partial^n_{S'}} & C^{n+1}_{Am}(S', S_{S'}) & \longrightarrow & \ldots \end{array} \tag{4.2}$$

where $\partial^n_{S'} = \partial^n \otimes Id_{S'}$. It follows that if $c \in Z^2_{Am}(R,S)$, then $c_{S'} \in Z^2_{Am}(S', S_{S'})$, and likewise if $c \in B^2_{Am}(R,S)$, then $c_{S'} \in B^2_{Am}(S', S_{S'})$. This also defines a map from $H^n(R,S)$ to $H^n(S', S_{S'})$ sending the class of c to that of $c_{S'}$.

Proof. The only part that does not follow from [33, Theorem 5.5] is that c is a unit if and only if $c_{S'}$ is. However, if c admits an inverse $c^{-1} \in S^{\otimes(n+1)}$, then $(c^{-1})_{S'}$ is an inverse of $c_{S'}$. □

In the case that $S = S'$, the base-change sends $H^n_{Am}(R,S)$ to the trivial class:

Proposition 4.1.5. *Let $n \in \mathbb{N}$. Let R be a ring and let S be an R-algebra. Let $c \in Z^n_{Am}(R,S)$ be a cocycle. Then, $c_S \in B^n_{Am}(S, S_S)$.*

Proof. Observe that in this case, $S_S = S^{\otimes 2}$, seen as an S-algebra via the map $\varepsilon_0^0 \colon S \to S^{\otimes 2}$. In general, we have $(S_S)^{\otimes_S n} \simeq S^{\otimes_R n+1}$ as R algebras. We may therefore identify $C^n_{Am}(S, S_S)$ and $C^{n+1}_{Am}(R, S)$ as abelian groups. Then, if $c \in C^n_{Am}(R, S)$, we get

$$c_S = \varepsilon^n_{n+1}(c).$$

Furthermore, if $c \in C^{n+1}_{Am}(R, S)$, then

$$\partial^n_S(c) = \prod_{i=0}^{n+1} (\varepsilon^{n+1}_i(c))^{(-1)^i},$$

Observe that if $c \in C^n_{Am}(R, S) = C^{n-1}_{Am}(S, S_S)$, we get

$$\partial^n(c) = \partial^{n-1}_S(c)(\varepsilon^n_{n+1}(c))^{(-1)^{n+1}}.$$

It follows that if $c \in Z^n_{Am}(R, S)$, so that $\partial^n(c) = 1$, we get

$$c_S = \varepsilon^n_{n+1}(c) = \partial^{n-1}_S(c^{(-1)^n}) \in B^2_{Am}(S, S_S)$$

□

4.2 Amitsur algebras

In this section, we fix a field k. We will prove Theorem 4.2.4, which gives an isomorphism between the cohomology group $H^2_{Am}(k, K)$ and the relative Brauer group $\mathrm{Br}(K/k)$. This theorem is comparable to the results of Section 3.2.2. In [55], the authors prove this result as a consequence of Proposition 3.2.21, and an equivalence between Brauer algebras and the Amitsur algebras defined below. Here, as suggested in [55, Remark 3.8], we give a direct proof, which, while inspired by the techniques used in [51, Chapter 2], is independent of the theory of Brauer factor sets.

In this section, we will consider two settings. The first is the case where $R = k$ and S is an étale k-algebra K, as in the discussion of Brauer factor sets. In this first setting, we state and prove Theorem 4.2.4. Some intermediate results require us to consider Amitsur algebras in the more general setting where R is an étale k-algebra and S is a free étale R-algebra.

In either case, since S is free as a R-module, we may see $S^{\otimes(n+1)}$ as an $S^{\otimes n}$-algebra via any map ε^{n-1}_i for $i \in [n+1]_0$. This algebra is always free as a $S^{\otimes n}$-module. In this case, we write Tr^{n-1}_i for the corresponding trace map. This section will focus on the trace map Tr^1_1, as it plays a central role in defining Amitsur algebras.

Definition 4.2.1. *Let $c \in S^{\otimes 3}$. Then, we define a bilinear map*

$$\pi_c \colon S^{\otimes 2} \times S^{\otimes 2} \to S^{\otimes 2}$$

as follows: for $a, a' \in S^{\otimes 2}$,

$$\pi_c(a, a') = \mathrm{Tr}_1^1(\varepsilon_2^1(a)c\varepsilon_0^1(a')).$$

The R-algebra with underlying vector space $S^{\otimes 2}$ and product π_c is called the Amitsur algebra *associated to S and c, and is denoted by $A(S, c)$.*

Remark 4.2.2. The algebra $A(S, c)$ needs not be unital or associative.

We stress that for the remainder of this section, unless specified otherwise, the notation aa', when $a, a' \in S^{\otimes 2}$ means the usual product in the tensor product algebra $S^{\otimes 2}$. We use the maps π_c when we mean multiplication in the algebra $A(S, c)$.

Observe that in general, for $a = \sum_{i \in I} a_{i0} \otimes a_{i1} \otimes a_{i2} \in S^{\otimes 3}$, we have

$$\mathrm{Tr}_1^1(a) = \sum_{i \in I} \mathrm{Tr}_{S/R}(a_{i1})a_{i0} \otimes a_{i2}. \tag{4.3}$$

It follows that if $c \in S^{\otimes 3}$, $a, a' \in S^{\otimes 2}$ and $b \in S$, we have the following:

$$\pi_c(\varepsilon_1^0(b)a, a') = \varepsilon_1^0(b)\pi_c(a, a') \tag{4.4}$$

$$\pi_c(a, \varepsilon_0^0(b)a') = \varepsilon_0^0(b)\pi_c(a, a') \tag{4.5}$$

Example 4.2.3 (The trivial Amitsur algebra). Let d be the rank of S as a free R-module. The algebra $A = A(S, 1)$ is isomorphic to $M_d(R)$. Indeed, there is an isomorphism $\mathrm{End}_R(S) \simeq M_n(R)$. Since S is free as an R module, we have $\mathrm{End}_R(S) \simeq S \otimes S^\vee$, given by $a \otimes \varphi \mapsto (b \mapsto a\varphi(b))$. By Lemma 2.1.22, we get an isomorphism $\simeq S^{\otimes 2} \simeq \mathrm{End}_R(S)$, where the multiplication on $S^{\otimes 2}$ is not the usual, but is rather defined by the following: for $a, a', b, b' \in S$,

$$(a \otimes a') \cdot (b \otimes b') = \mathrm{Tr}_{S/R}(a'b)a \otimes b'.$$

Now, we need to check that this coincides with the bilinear map π_1, and it is enough to check on simple tensor elements. Let $a, a', b, b' \in S$. We compute:

$$\begin{aligned}
\pi_1(a \otimes a', b \otimes b') &= \mathrm{Tr}_1^1(\varepsilon_2^1(a \otimes a')\varepsilon_0^1(b \otimes b')) \\
&= \mathrm{Tr}_1^1(a \otimes a'b \otimes b') \\
&= \mathrm{Tr}_{S/R}(a'b)a \otimes b' \quad \text{(by Equation (4.3)).}
\end{aligned}$$

The main result of this section is the following, stated as Theorem 1.4.1:

Theorem 4.2.4. *Let k be a field and let K be an étale k-algebra of degree d. Let $c \in K^{\otimes 3}$. Then, $A(K,c)$ is a central simple k-algebra if and only if $c \in Z^2_{Am}(k,K)$. In this case, $A(K,c)$ has degree d and contains K as a maximal commutative subalgebra. Conversely, if A is a central simple k-algebra of degree d containing K as a maximal commutative subalgebra, there exists $c \in Z^2_{Am}(k,K)$ such that the Amitsur algebra $A(K,c)$ is isomorphic to A.*

This factors into an isomorphism between $H^2_{Am}(k,K)$ and the relative Brauer group of k with respect to K.

Proof. Theorem 4.2.4 is the combination of the following results proved in this section: Example 4.2.3 and Propositions 4.2.5, 4.2.7 and 4.2.10 to 4.2.14 □

4.2.1 Embedding S into $A(S,c)$

Proposition 4.2.5. *Let $c \in S^{\otimes 3}$. Assume that the algebra $A(S,c)$ is unital and let $\mathbf{1}_c$ be its unit. Then S embeds into $A(S,c)$ as an R-algebra via the mapping*

$$\iota_c(a) = \varepsilon_1^0(a)\mathbf{1}_c.$$

Proof. First, we prove that if $\iota_c(a) = 0$, then $a = 0$. Indeed, applying Equation (4.4), we get

$$\varepsilon_1^0(a) = \varepsilon_1^0(a)(1 \otimes 1) = \pi_c(\iota_c(a), 1 \otimes 1),$$

and it follows that if $\iota_c(a) = 0$, then $\varepsilon_1^0(a) = 0$ and therefore $a = 0$.

Now, it remains for us to prove that if $a, a' \in S$, then

$$\iota_c(aa') = \pi_c(\iota_c(a), \iota_c(a')).$$

We compute:

$$\begin{aligned}
\pi_c(\iota_c(a), \iota_c(a')) &= \varepsilon_1^0(a)\pi_c(\mathbf{1}_c, \iota_c(a')) \\
&= \varepsilon_1^0(a)\pi_c(\iota_c(a'), \mathbf{1}_c) \\
&= \varepsilon_1^0(aa')\pi_c(\mathbf{1}_c, \mathbf{1}_c) \\
&= \iota_c(aa').
\end{aligned}$$

□

Lemma 4.2.6. *Let $c \in S^{\otimes 3}$, and let $\alpha \in S$. Then*

$$\iota_c(\alpha) = \varepsilon_0^0(\alpha)\mathbf{1}_c.$$

Proof. We set

$$c = \sum_{\ell \in L} c_{\ell 0} \otimes c_{\ell 1} \otimes c_{\ell 2}$$

and

$$\mathbf{1}_c = \sum_{i \in I} a_i \otimes b_i.$$

We first prove that for a general $\alpha \in S$,

$$\varepsilon_1^0(\alpha) = \sum_{\substack{i \in I \\ \ell \in L}} \mathrm{Tr}_{S/R}(b_i c_{\ell 1} \alpha)(c_{\ell 0} a_i) \otimes c_{\ell 2}.$$

Indeed, we compute

$$\begin{aligned}
\varepsilon_1^0(\alpha) &= \pi_c(\mathbf{1}_c, \varepsilon_1^0(\alpha)) \\
&= \sum_{\substack{i \in I \\ \ell \in L}} \mathrm{Tr}_{S/R}(b_i c_{\ell 1} \alpha)(c_{\ell 0} a_i) \otimes c_{\ell 2}.
\end{aligned}$$

Now,

$$\begin{aligned}
\varepsilon_0^0(\alpha)\mathbf{1}_c &= \pi_c(\mathbf{1}_c, \varepsilon_0^0(\alpha)\mathbf{1}_c) \\
&= \sum_{\substack{i,j \in I \\ \ell \in L}} \mathrm{Tr}_{S/R}(b_i c_{\ell 1} a_j \alpha)(c_{\ell 0} a_i) \otimes (c_{\ell 2} b_j) \\
&= \sum_{j \in J} (1 \otimes b_j) \sum_{\substack{i \in I \\ \ell \in L}} \mathrm{Tr}_{S/R}(b_i c_{\ell 0}(\alpha a_j))(c_{\ell 0} a_i) \otimes c_{\ell 2} \\
&= \sum_{j \in J} (1 \otimes b_j)\varepsilon_1^0(\alpha a_j) \\
&= \sum_{j \in J} \varepsilon_1^0(\alpha)(a_j \otimes b_j) \\
&= \iota_c(\alpha).
\end{aligned}$$

□

Combining Proposition 4.2.5 and Lemma 4.2.6, we observe that for any $a \in A(S, c)$ and $\alpha \in S$, we have

$$\pi_c(\iota_c(\alpha), a) = \varepsilon_1^0(\alpha)a, \tag{4.6}$$

and

$$\pi_c(a, \iota_c(\alpha)) = \varepsilon_0^0(\alpha)a. \tag{4.7}$$

4.2.2 Amitsur cocycles give central simple algebras

Proposition 4.2.7. *Let R be an étale k-algebra, and let S be a free étale R-algebra. Let $c, c' \in S^{\otimes 3}$. Assume that there exists $b \in B^2_{Am}(R,S)$ such that $c = bc'$, and let $a \in C^1_{Am}(R,S)$ such that $b = \partial^1(a)$. Then, the map $x \mapsto ax$ gives an R-algebra isomorphism from $A(S,c)$ to $A(S,c')$.*

Proof. It is clear that multiplication-by-a is an R-linear automorphism of $S^{\otimes 2}$. Let $\alpha, \beta \in S^{\otimes 2}$, we compute:

$$\begin{aligned}
a\pi_c(\alpha,\beta) &= a\,\mathrm{Tr}_1^1(\varepsilon_2^1(\alpha)c'\varepsilon_0^1(\beta)\\
&= a\,\mathrm{Tr}_1^1(\varepsilon_2^1(\alpha)c\varepsilon_0^1(a)\varepsilon_2^1(a)\varepsilon_1^1(a^{-1})\varepsilon_0^1(\beta))\\
&= a\,\mathrm{Tr}_1^1(\varepsilon_1^1(a^{-1})\varepsilon_2^1(a\alpha)c\varepsilon_0^1(a\beta))\\
&= aa^{-1}\,\mathrm{Tr}_1^1(\varepsilon_2^1(a\alpha)c\varepsilon_0^1(a\beta)) \quad \text{(by linearity of } \mathrm{Tr}_1^1)\\
&= \mathrm{Tr}_1^1(\varepsilon_2^1(a\alpha)c\varepsilon_0^1(a\beta)\\
&= \pi_{c'}(a\alpha, a\beta).
\end{aligned}$$

□

Lemma 4.2.8. *Let A be a (non necessarily unital or associative) k-algebra, and let K be an étale k-algebra. If A_K is a unital associative K-algebra, then A is itself associative and unital.*

Proof. As there is an injective mapping from A to A_K, A is associative. It remains to prove that A is unital.

Let $n = [A : k]$. We fix a k-basis $(e_1, \dots, e_n)$ of A, and $(e_i \otimes 1)_{i\in[n]}$ is a K-basis of A_K. We let $\mathbf{1}$ be the unit of A_K and we set

$$\mathbf{1} = \sum_{i\in[n]} e_i \otimes a_i.$$

Then, we fix an algebraic closure $\overline{k}$ of k. If φ is an embedding of K into $\overline{k}$, then the map

$$\tilde{\varphi}\colon \sum_{i\in[n]} e_i \otimes x_i \mapsto \sum_{i\in[n]} e_i \otimes \varphi(x_i)$$

is an embedding of A_K into $A_{\overline{k}}$.

Now, let φ_1 and φ_2 be two embeddings of K into $\overline{k}$. We have $\tilde{\varphi_1}(\mathbf{1}) = \tilde{\varphi_2}(\mathbf{1})$, and it follows that for $i \in [n]$, $\varphi_1(a_i) = \varphi_2(a_i)$. Then, by Lemma 2.1.11, $a_i \in k$ for all $i \in [n]$, and it follows that $\mathbf{1} \in A$, and that the algebra A is unital. □

Lemma 4.2.9. *Let R be an étale algebra and let S be a free étale R-algebra. Let $c \in R^{\otimes 3}$. Then*

$$A(R,c)_S \simeq A(S,c_S).$$

Proof. We have an isomorphism of S-modules

$$\begin{array}{ccc} (R^{\otimes 2})_S & \simeq & (R_S)^{\otimes 2} \\ \sum_{i\in I}(u_i \otimes v_i) \otimes t_i & \mapsto & \sum_{i\in I}(u_i \otimes 1) \otimes (v_i \otimes t_i). \end{array}$$

Now, we prove that if $\alpha, \beta \in R^{\otimes 2}$,

$$\pi_c(\alpha,\beta) \otimes 1 = \pi_{c_S}(\alpha \otimes 1, \beta \otimes 1).$$

Indeed,

$$\begin{aligned} \pi_{c_S}(\alpha \otimes 1, \beta \otimes 1) &= \mathrm{Tr}_1^1((\varepsilon_2^1(\alpha) \otimes 1)(c \otimes 1)(\varepsilon_0^1(\beta) \otimes 1)) \\ &= \mathrm{Tr}_1^1((\varepsilon_2^1(\alpha) c \varepsilon_0^1(\beta)) \otimes 1) \\ &= \mathrm{Tr}_1^1(\varepsilon_2^1(\alpha) c \varepsilon_0^1(\beta)) \otimes 1 \\ &= \pi_c(\alpha,\beta) \otimes 1. \end{aligned}$$

□

Proposition 4.2.10. *Let K be an étale k-algebra of dimension d, and let $c \in Z^2_{Am}(k,K)$. Then $A(K,c)$ is a central simple K-algebra.*

Proof. By Proposition 4.1.5, c_K lies in $B^2_{Am}(K,K_K)$. Then, by Proposition 4.2.7, Example 4.2.3, and Lemma 4.2.9, $A(K,c)_K \simeq A(K_K,c_K) \simeq \mathrm{End}_K(K_K) \simeq M_d(K)$. Now, it will follow from Theorem 3.2.3 that $A(K,c)$ is a central simple algebra if it is associative and unital, which itself follows from Lemma 4.2.8. □

4.2.3 Central simple algebras come from Amitsur cocycles

Proposition 4.2.11. *If K is an étale k-algebra, $c \in K^{\otimes 3}$ and $A(K,c) \simeq \mathrm{End}_k(K)$, then $c \in B^2_{Am}(k,K)$.*

Proof. By Example 4.2.3, there is an isomorphism $\varphi\colon A(K,c) \to A(K,1)$. Since the algebras $A(K,1)$ and $A(K,c)$ are unital, we have subalgebras $K_1 = \iota_c(K)$ and $K_2 = \varphi^{-1}(\iota_1(K))$ of $A(K,c)$, and both are isomorphic to K. By Proposition 2.1.23, there is a k-algebra automorphism ψ of $A(K,c)$ which sends K_1 to K_2. Replacing φ with $\varphi \circ \psi$, we get $\varphi \circ \iota_c = \iota_1$.

Then, it follows from Equations (4.6) and (4.7) that φ is also an isomorphism of $K^{\otimes 2}$-module, where $A(K,c)$ and $A(K,1)$ are both seen as free $K^{\otimes 2}$ of rank 1 generated by $1 \otimes 1$. It follows that there exists $a \in C^1_{Am}(K)$ such that for all $\alpha \in A(K,c)$,

$$\varphi(\alpha) = \alpha a.$$

Then, for any $\alpha, \beta \in A(K,c)$, we have

$$\begin{aligned}
\mathrm{Tr}^1_1(\varepsilon^1_2(\alpha)c\varepsilon^1_0(\beta)) &= \pi_c(\alpha,\beta) \\
&= a^{-1}\pi_1(a\alpha, a\beta) \\
&= a^{-1}\,\mathrm{Tr}^1_1(\varepsilon^1_2(a\alpha)\varepsilon^1_0(a\beta)) \\
&= \mathrm{Tr}^1_1(\varepsilon^1_2(\alpha)(\varepsilon^1_2(a)\varepsilon^1_0(a)\varepsilon^1_1(a)^{-1})\varepsilon^1_0(\beta) \\
&= \mathrm{Tr}^1_1(\varepsilon^1_2(\alpha)\partial^1(a)\varepsilon^1_0(\beta)).
\end{aligned}$$

Since the images of ε^1_0 and ε^1_2 span $K^{\otimes 3}$ as a $K^{\otimes 2}$-module, it follows from Lemma 2.1.22 that $c = \partial^1(a) \in B^2_{Am}(k,K)$. □

Proposition 4.2.12. *If K is an étale k-algebra and $c \in K^{\otimes 3}$ is such that $A(K,c)$ is a central simple k-algebra, then $c \in Z^2_{Am}(k,K)$.*

Proof. Let L be a splitting field for $A(K,c)$. Then, by Lemma 4.2.9 and Proposition 4.2.11, $c_L \in B^2_{Am}(L,K_L)$. Now, this means that c_L is a unit in $K_L^{\otimes 3}$. Since $K^{\otimes 3}$ is an étale k-algebra, it follows from Proposition 2.1.13 that c is a unit if and only if it is not a zero divisor. However, if it were, c_L would also be one. Therefore, $c \in C^2_{Am}(k,K)$. Furthermore, $1 = \partial^2_L(c_L) = \partial^2(c) \otimes 1$, so $\partial^2(c) = 1$, and $c \in Z^2_{Am}(k,K)$. □

Proposition 4.2.13. *Let K be an étale algebra of degree d, and let A be a central simple algebra of degree d which contains a subalgebra isomorphic to K. Then there exists $c \in Z^2_{Am}(k,K)$ such that $A \simeq A(K,c)$.*

Proof. By Proposition 4.2.12, it is enough to prove that there exists $c \in K^{\otimes 3}$ such that $A \simeq A(K,c)$.

Let $A^e = A \otimes_k A^{op}$ be the envelopping algebra of A. Then A is an A^e-module via the multiplication $(\alpha \otimes \beta)x = \alpha x \beta$. The k-algebra A^e is central simple by Lemma 3.2.7, and therefore A is a faithful A^e-module by [33, Theorem 3.2.5]. Since $K^{\otimes 2}$ is a subalgebra of A^e, A is also a faithful $K^{\otimes 2}$-module.

By Corollary 2.1.14, there exists $v \in A$ such that $A = KvK$ (this is also the content of [51, Theorem 2.2.2]). We let $\varphi\colon K^{\otimes 2} \to A$ be the $K^{\otimes 2}$-module isomorphism defined by

$$\varphi(a \otimes b) = avb,$$

and we consider the bilinear map

$$\begin{array}{rccc} \Gamma\colon & (K^{\otimes 2})^2 & \to & K^{\otimes 3} \\ & (\alpha_0 \otimes \alpha_1, \beta_0 \otimes \beta_1) & \mapsto & \alpha_0 \otimes \alpha_1\beta_0 \otimes b_1 \end{array}.$$

We see $K^{\otimes 3}$ as a $K^{\otimes 2}$-algebra via the map ε_1^1, and we define the $K^{\otimes 2}$-module homomorphism

$$\begin{array}{rccc} \psi\colon & K^{\otimes 3} & \to & A \\ & a_0 \otimes a_1 \otimes a_2 & \mapsto & a_0va_1va_2 \end{array}.$$

It may easily be seen that for $\alpha, \beta \in K^{\otimes 2}$, we have

$$\varphi(\alpha)\varphi(\beta) = \psi(\Gamma(\alpha, \beta)).$$

The map $\varphi^{-1} \circ \psi$ is a $K^{\otimes 2}$-module homomorphism from $K^{\otimes 3}$ to $K^{\otimes 2}$. By Lemma 2.1.22, there exists $c \in K^{\otimes 3}$ such that for all $\alpha \in K^{\otimes 3}$,

$$\varphi^{-1}(\psi(\alpha)) = \mathrm{Tr}_1^1(c\alpha).$$

Therefore, there is an isomorphism $A(K, c) \simeq A$. □

4.2.4 Tensor product and product of cocycles

Proposition 4.2.14. *Let K be an étale k-algebra. Let $c, c' \in Z^2_{Am}(k, K)$. Then the algebra $A(K, cc')$ is Brauer equivalent to $A(K, c) \otimes A(K, c')$.*

Fix an étale k-algebra K. Let $c, c' \in Z^2_{Am}(k, K)$, which we denote by

$$c = \sum_{\ell \in L} c_{\ell 0} \otimes c_{\ell 1} \otimes c_{\ell 2}$$

and

$$c' = \sum_{\ell' \in L'} c'_{\ell' 0} \otimes c'_{\ell' 1} \otimes c'_{\ell' 2}.$$

Now, we set

$$c \otimes c' \coloneqq \sum_{\substack{\ell \in L \\ \ell' \in L'}} c_{\ell 0} \otimes c'_{\ell' 0} \otimes c_{\ell 1} \otimes c'_{\ell' 1} \otimes c_{\ell 2} \otimes c'_{\ell' 2}.$$

Proposition 4.2.14 follows immediately from Lemmas 4.2.15 and 4.2.17 below.

Lemma 4.2.15. *The tensor product $A(K,c)\otimes A(K,c')$ is isomorphic to $A(K\otimes K, c\otimes c')$.*

Proof. Both algebras are isomorphic to $K^{\otimes 4}$ as k-vector spaces. We consider the linear isomorphism $\varphi\colon A(K,c)\otimes A(K,c')\to A(K\otimes K, c\otimes c')$ defined on simple tensor elements by

$$\varphi(a\otimes b\otimes c\otimes d) = a\otimes c\otimes b\otimes d.$$

All that remains to prove is that for $\alpha,\beta\in A(K,c), \alpha',\beta'\in A(K,c')$,

$$\varphi(\pi_c(\alpha,\beta)\otimes\pi_{c'}(\alpha',\beta')) = \pi_{c\otimes c'}(\varphi(\alpha\otimes\alpha',\beta\otimes\beta')).$$

We prove the equation above for simple tensor elements, and the general result follows. We let $\alpha = a_0\otimes a_1$ and $\beta = b_0\otimes b_1$ be in $A(K,c)$ and $\alpha' = a'_0\otimes a'_1$ and $\beta' = b'_0\otimes b'_1$ be in $A(K,c')$. Applying Equation (4.3), we get

$$\begin{aligned}
&\pi_{c\otimes c'}(\varphi(\alpha\otimes\alpha'),\varphi(\beta\otimes\beta'))\\
&= \sum_{\substack{\ell\in L\\ \ell'\in L'}} \mathrm{Tr}_{K\otimes K/k}(a_1b_0c_{\ell 1})\otimes(a'_1b'_0c'_{\ell' 1})(a_0c_{\ell 0}\otimes a'_0c'_{\ell' 0}\otimes b_1c_{\ell 2}\otimes b'_1c'_{\ell' 2})\\
&= \sum_{\substack{\ell\in L\\ \ell'\in L'}} \mathrm{Tr}_{K/k}\left(a_1b_0c_{\ell 1}\right)\mathrm{Tr}_{K/k}\left(a'_1b'_0c'_{\ell' 1}\right)\varphi(a_0c_{\ell 0}\otimes c_{\ell 2}b_1\otimes a'_0c'_{\ell' 0}\otimes c'_{\ell' 2}b'_1)\\
&= \varphi\left(\left(\sum_{\ell\in L}\mathrm{Tr}_{K/k}(a_1c_{\ell 1}b_0)a_0c_{\ell 0}\otimes b_1c_{\ell 2}\right)\right.\\
&\left.\otimes\left(\sum_{\ell'\in L'}\mathrm{Tr}_{K/k}(a'_1c'_{\ell' 1}b'_0)a'_0c'_{\ell' 0}\otimes b'_1c'_{\ell' 2}\right)\right)\\
&= \varphi(\pi_c(\alpha,\beta)\otimes\pi_{c'}(\alpha',\beta')).
\end{aligned}$$

□

For $n\in\mathbb{N}$, we consider the multiplication map

$$\begin{array}{rccc}
\mu_n\colon & K^{\otimes 2n} & \to & K^{\otimes n}\\
& a_0\otimes a_1\otimes\ldots\otimes a_{2n-1} & \mapsto & a_0a_1\otimes\ldots\otimes a_{2n-2}a_{2n-1}
\end{array}$$

Now, by [33, Proposition 4.1.2 and Exercise 4.1.8], there exists a separability idempotent $e_n\in K^{\otimes 2n}$ such that $\mu_n(e_n)=1$ and $\ker\mu_n$ is generated by $(1-e)$. It follows directly that $K^{\otimes 2n} = eK^{\otimes 2n}\oplus(1-e)K^{\otimes 2n}$ and that μ_n is an isomorphism from $eK^{\otimes 2n}$ to $K^{\otimes n}$. Furthermore, it is clear that $e_{n+1} = e_n\otimes e$.

As usual, we see $K^{\otimes 3}$ as a $K^{\otimes 2}$-algebra via the map ε_1^1 and write Tr_1^1 for the associated trace map. Likewise, we see $K^{\otimes 6}$ as a $K^{\otimes 4}$-algebra via the map

$$\begin{array}{rccc} \varepsilon_1^{'1}: & K^{\otimes 4} & \to & K^{\otimes 6} \\ & a_0 \otimes a_1 \otimes a_2 \otimes a_3 & \mapsto & a_0 \otimes a_1 \otimes 1 \otimes 1 \otimes a_2 \otimes a_3 \end{array}$$

and we write $\mathrm{Tr}_1^{'1}$ for the corresponding trace map. We also define maps $\varepsilon_i^{'n}$ for $0 \leq i \leq n+1$ in a similar manner, by analogy with the maps ε_i^n. If $c, c' \in Z^2_{Am}(k, K)$, and $c \otimes c'$ is defined as above, we have

$$\mu_3(c \otimes c') = cc'. \tag{4.8}$$

It may also be easily observed that for $0 \leq i \leq 2$, if $\alpha \in K^{\otimes 4}$,

$$\mu_3(\varepsilon_i^{'1}(\alpha)) = \varepsilon_i^1(\mu_2(\alpha)). \tag{4.9}$$

Lemma 4.2.16. *With notations as above, if $\alpha \in e_3 K^{\otimes 6}$, then*

$$\mu_2(\mathrm{Tr}_1^{'1}(\alpha)) = \mathrm{Tr}_1^1(\mu_3(\alpha)).$$

Proof. Observe that

$$K^{\otimes 4} = e_2 K^{\otimes 4} \oplus (1 - e_2) K^{\oplus 4}$$

and

$$K^{\otimes 6} = e_3 K^{\otimes 6} \oplus (1 - e_3) K^{\otimes 6}.$$

Under these identifications, we have

$$\varepsilon_1^{'1} = e(\varepsilon_1^{'1})_{|e_2 K^{\otimes 4}} + (1 - e_3)(\varepsilon_1^{'1})_{|e_2 K^{\otimes 4}}.$$

It follows that for $\alpha \in K^{\otimes 6}$,

$$\mathrm{Tr}_1^{'1}(\alpha) = \mathrm{Tr}_{e_3 K^{\otimes 6}/e_2 K^{\otimes 4}}(e_3\alpha) + \mathrm{Tr}_{(1-e_3)K^{\otimes 6}/(1-e_2)K^{\otimes 4}}((1 - e_3)\alpha)$$

In particular, if $\alpha \in e_3 K^{\otimes 6}$,

$$\mathrm{Tr}_1^{'1}(\alpha) = \mathrm{Tr}_{e_3 K^{\otimes 6}/e_2 K^{\otimes 4}}(\alpha).$$

The result follows from the fact that the diagram below commutes and its horizontal arrows are isomorphisms.

$$\begin{array}{ccc} e_3 K^{\otimes 6} & \xrightarrow{\mu_3} & K^{\otimes 3} \\ {\scriptstyle e_3\varepsilon_1^{'1}}\uparrow & & \uparrow{\scriptstyle \varepsilon_1^1} \\ e_2 K^{\otimes 4} & \xrightarrow{\mu_2} & K^{\otimes 2} \end{array}$$

This diagram commutes by a combination of Equation (4.9) and the fact that $\mu_3(e_3) = 1$. □

Lemma 4.2.17. *The algebra $A(K, cc')$ is Brauer equivalent to $A(K \otimes K, c \otimes c')$.*

Proof. We let $f = \iota_{c\otimes c'}(e_1)$ and we will show that $A(K, cc') \simeq \pi_{c\otimes c'}(f, A(K \otimes K, c \otimes c'), f)$ (abusing notation by associativity of $\pi_{c\otimes c'}$). Since f is idempotent, the result will follow by Lemma 3.2.10. By Equations (4.6) and (4.7),

$$\pi_{c\otimes c'}(f, A(K \otimes K, c \otimes c'), f) = e_2 A(K \otimes K, c \otimes c'),$$

and it follows that the map μ_2 restricts to an isomorphism from this subspace (of $A(K \otimes K, c \otimes c')$ identified with $K^{\otimes 4}$ as a $K^{\otimes 2}$-module) to $K^{\otimes 2}$. It remains for us to show that for $\alpha, \beta \in e_2 A(K \otimes K, c \otimes c')$,

$$\mu_2(\pi_{c\otimes c'}(\alpha, \beta)) = \pi_{cc'}(\mu_2(\alpha), \mu_2(\beta)).$$

We let $\alpha, \beta \in e_2 A(K \otimes K', c \otimes c')$ and we compute:

$$\begin{aligned}
\mu_2(\pi_{c\otimes c'}(\alpha, \beta) &= \mu_2\left(\mathrm{Tr}_1^{\prime 1}(\varepsilon_0^{\prime 1}(\alpha c \otimes c' \varepsilon_2^{\prime 1}(\beta)\right) \\
&= \mathrm{Tr}_1^1(\mu_3(\varepsilon_0^{\prime 1}(\alpha)(c \otimes c')\varepsilon_2^{\prime 1}(\beta))) \quad \text{(Lemma 4.2.16)} \\
&= \mathrm{Tr}_1^1(\varepsilon_0^1(\mu_2(\alpha))cc'\varepsilon_2^1(\mu_2(\beta))) \quad \text{(Equations (4.8) and (4.9))} \\
&= \pi_{cc'}(\mu_2(\alpha), \mu_2(\beta))
\end{aligned}$$

□

4.3 Computational results

This section presents a computational representation of central simple algebras as Amitsur algebras. We also give an algorithm for computing such a representation in polynomial time for any central simple algebra. Finally, under GRH, we give a polynomial quantum algorithm for solving the explicit isomorphism problem for an Amitsur algebra (Problem 4.3.1 below). We then obtain, still under GRH, a polynomial quantum algorithm for solving the explicit isomorphism problem (Problem 3.4.1).

Problem 4.3.1 (The explicit isomorphism problem (Amitsur version))**.** *Let k be a field, and let K be an étale k-algebra of degree $d \in \mathbb{N}$. Let $c \in B^2_{Am}(k, K)$. Find an explicit isomorphism from $A(K, c)$ to $M_d(k)$.*

4.3.1 Algorithmic representation of Amitsur algebras

Once a field k and a monogeneous étale k-algebra $K = k[X]/(\chi(X))$ are fixed, we have isomorphisms

$$K_n \coloneqq k[X_0, \ldots, X_n]/(\chi(X_0), \ldots, \chi(X_n)) \simeq K^{\otimes(n+1)},$$

for all $n \in \mathbb{N}$. Therefore, an element of $K^{\otimes(n+1)}$, and in particular of $C^n_{Am}(k, K)$, may be represented uniquely as a polynomial $\xi(X_0, \ldots, X_n)$ in $k[X_0, \ldots, X_n]$ whose individual degrees in the indeterminates X_i for $i \in [d]_0$ are all bounded by $d - 1$.

In this setting, the map ε^n_i becomes the map sending $\xi(X_0, \ldots, X_n)$ to $\xi(X_0, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)$. That is,

$$\varepsilon^n_i(X_j) = \begin{cases} X_j \text{ if } j < i \\ X_{j+1} \text{ otherwise.} \end{cases}$$

The trace map Tr_{K_2/K_1} corresponding to Tr^1_1 may easily be computed in the K_1-basis $(X^i_1)_{0 \le i < d}$ of K_2 using the fact that

$$\mathrm{Tr}_{K_2/K_1}(X^i_0 X^j_1 X^\ell_2) = X^i_0 X^\ell_2 \, \mathrm{Tr}_{K/k}(X^j).$$

It follows that if $\xi_1, \xi_2 \in R_1$ represent elements a_1, a_2 of $A(F, c)$, where we see c as an element of R_2, then the element $\xi \in R_2$ representing the product $a_1 a_2$ may be computed practically as:

$$\xi(X_0, X_1) = \mathrm{Tr}_{K_2/K_1}\left(\xi_1(X_0, X_1) c(X_0, X_1, X_2) \xi_2(X_1, X_2)\right).$$

We record the discussion above in the following:

Theorem 4.3.2. *There exist polynomial algorithms for computing additions and multiplications in $A(K, c)$ when its elements are represented as elements of K_n.*

For the remainder of this section, if K is an étale k-algebra, an element of $K^{\otimes(n+1)}$ is represented as an element of K_n using the algorithms described above.

4.3.2 Computing a cocycle representing a given algebra

Here we present an Algorithm 1, which, given a central simple algebra A, computes a representation of an isomorphism Amitsur algebra $A(K, c)$, together with an isomorphism between A and $A(K, c)$.

Input: A field k

Input: Structure constants for a central simple k-algebra A such that $|k| > [A : k] = n$

Output: $u \in A$ such that $K = k[u]$ is a maximal separable commutative subalgebra of A

Output: The minimal polynomial χ of u

Output: $c \in Z^2_{Am}(K, k)$

Output: An isomorphism e from $A(K, c)$ to A

1 Find $u \in A$ such that $K \coloneqq k[u]$ is a maximal separable commutative subalgebra of A;

2 Compute χ, the minimal polynomial of u;

3 Find $v \in A$ such that $A = KvK$;

4 Compute the matrix of the isomorphism $e : K^{\otimes 2} \to A$ sending $f_1 \otimes f_2$ to $f_1 v f_2$;

5 Compute $c \in K^{\otimes 3}$ such that for all $a, b \in K^{\otimes 2}$, $e(a)e(b) = \mathrm{Tr}^1_1(\varepsilon^1_2(a)c\varepsilon^1_0(b))$;

6 **return** (u, χ, c, e)

Algorithm 1: Computing a 2-cocycle representing a given central simple algebra

Before we prove the correctness and efficiency of Algorithm 1, we need a lemma:

Lemma 4.3.3. *Let k be a field and let A be a central simple k-algebra. Assume that $|k| > [A : k]$. Let $u \in A$ be such that $K \coloneqq k[u]$ is a maximal commutative subalgebra of A. Then an element $v \in A$ such that $A = KvK$ may be found in probabilistic polynomial time.*

Proof. For v in A, by an argument of dimensions over k, we observe that $A = KvK$ if and only if the map

$$e\colon \begin{array}{ccc} K \otimes K & \to & A \\ a_1 \otimes a_2 & \mapsto & a_1 v a_2 \end{array}$$

is injective.

We fix the bases $(u^i \otimes u^j)_{0 \leq i,j \leq \deg A - 1}$ of $K^{\otimes 2}$ and $B = (b_1, \ldots, b_{[A:k]})$ the input basis of A (that is, the basis with respect to which the structure constants of A are defined). The determinant of e is a homogeneous polynomial on the coordinates of v in the basis B, and $A = KvK$ if and only if v is not a zero of this polynomial.

Letting S be a finite subset of k, the Schwartz-Zippel lemma ensures that a random v in $Sb_1 \oplus \ldots \oplus Sb_{[A:k]}$ satisfies this condition with probability larger than $1 - \frac{[A:k]}{|S|}$.

Therefore, if $|k| > [A : k]$, we may pick S large enough that v has the desired property with positive probability and small enough that we may sample a random element in $Sb_1 \oplus \ldots \oplus Sb_{[A:k]}$. For instance, take $|S| = [A : k] + 1$ and v has the desired property with probability larger than $\frac{1}{[A:k]+1}$. □

Theorem 4.3.4. *If k is a field over which linear algebra may be performed efficiently, and A is a central simple k-algebra such that $|k| > [A : k]$, then Algorithm 1 returns $u \in A$, a cocycle $c \in Z^2_{Am}(k, k(u))$ and an isomorphism $e\colon A(F, c) \to A$ in probabilistic polynomial time.*

Proof. The correctness of the algorithm follows directly for the proof of Proposition 4.2.13. The element $u \in A$ in Line 1 may be found using the polynomial algorithm given in [25]. The element $v \in A$ of Line 3 may be found in probabilistic polynomial time using Lemma 4.3.3. The remaining lines involve arithmetic in A and bounded tensor powers of K, as well as the computation of the solution of a system of linear equations. All in all, this makes Algorithm 1 a polynomial probabilistic algorithm. □

Corollary 4.3.5. *There is a probabilistic polynomial reduction from the explicit isomorphism problem (Problem 3.4.1) to its Amitsur version (Problem 4.3.1).*

4.3.3 Trivialisation of Amitsur cocycles

In this section, we present an algorithm for computing the trivialisation of a coboundary using S-units group computation. This result is reminiscent of results such as Simon's algorithm for solving norm equations in cyclic extensions [82] and Fieker's result on finding trivialisation of Galois coboundaries in groups of S-units [29, Theorem 7].

Our strategy is similar to that of [29]: We prove Lemma 4.3.8, a vanishing lemma for the first Amitsur cohomology group with coefficients in the divisor group. Such a result is analogous to [29, Lemma 9] and allows us to adapt the proof strategy of [29, Theorem 7] to our setting.

Let k be a global field, and let K be an étale k-algebra. For $n \in \mathbb{N}$, we set

$$\partial_{\mathcal{D}}^n = \sum_{i=0}^{n+1} (-1)^i \, \mathcal{D}(\varepsilon_i^n).$$

For a place $Q \in M^{na}_{K^{\otimes(n+2)}}$ and $i \in [n+1]_0$, we set $Q_i = Q_{\varepsilon_i^n}$ and $e_{Q,i} = e_{Q,\varepsilon_i^n}$. Then, for a divisor $D = \sum_{P \in M^{na}_{K^{\otimes(n+1)}}} n_P P$, we get

$$\partial_{\mathcal{D}}^n(D) = \sum_{Q \in M^{na}_{K^{\otimes(n+2)}}} \sum_{i=0}^{n+1} (-1)^i n_{Q_i} e_{Q,i} Q.$$

We first need a few lemmas:

Lemma 4.3.6. *Let Q, Q' be finite places of $K^{\otimes 2}$ such that $Q_0 = Q'_0$. Then there exists a place $R \in M^{fi}_{K^{\otimes 3}}$ such that $R_1 = Q$ and $R_0 = Q'$.*

Proof. We must prove that

$$\mathcal{D}(\varepsilon_1^1)(Q) \cap \mathcal{D}(\varepsilon_2^1(Q')) \neq \emptyset.$$

Let $\chi \in k[X]$ be a defining polynomial for K, and we identify K with $k[X]/(\chi(X))$. Now, we may identify the algebra $K^{\otimes 2}$ with $K[X]/(\chi(X))$, where the identification of K with the rings of scalars in $K[X]$ is ε_0^0. We also identify the algebra $K^{\otimes 3}$ with $K[X,Y]/(\chi(X), \chi(Y))$, where the identification of K with the ring of scalars in $K[X,Y]$ is the map $\varepsilon_1^1 \circ \varepsilon_0^0 = \varepsilon_0^1 \circ \varepsilon_0^0$.

Furthermore, under this identification, the ε maps become:

$$\begin{array}{rccc} \varepsilon_1^1\colon & K[X]/(\chi(X)) & \to & K[X,Y]/(\chi(X),\chi(Y)) \\ & X & \mapsto & X \\ \varepsilon_0^1\colon & K[X]/(\chi(X)) & \to & K[X,Y]/(\chi(X),\chi(Y)) \\ & X & \mapsto & Y \end{array}$$

With this in place, we have $(K^{\otimes 2})_{K_P} \simeq K_P[X]/(\chi(X))$. Let $\chi = \prod_{i\in[r]} \xi_i$ be the factorisation of the polynomial χ in $K_P[X]$, and the ξ_i are distinct since χ is separable. By Proposition 2.1.29, the ξ_i are in bijection with the support of $\mathcal{D}(\varepsilon_0^0)(P)$, so that if $Q \in \mathrm{Supp}(\mathcal{D}(\varepsilon_0^0)((P)))$, the place Q is identified ξ_i such that $K_Q^{\otimes 2} \simeq K_P(X)/(\chi_i(X))$.

Likewise, we have $(K^{\otimes 3})_{K_P} \simeq K_P[X,Y]/(\chi(X),\chi(Y))$. Since $K_{K_P}^{\otimes 3}$ is a product of finitely many field extensions of K_P, the ideal $(\chi(X),\chi(Y))$ of $K_P[X,Y]$ is contained in finitely many distinct maximal ideals $\mathfrak{m}_1,\dots,\mathfrak{m}_s$ and we have in fact $(\chi(X),\chi(Y)) = \cap_{\ell\in[s]}\mathfrak{m}_\ell$. Then, the $\mathfrak{m}_\ell$ are in bijection with $\mathrm{Supp}(\mathcal{D}(\varepsilon_1^1\circ\varepsilon_0^0)(P)) = \mathrm{Supp}(\mathcal{D}(\varepsilon_2^1\circ\varepsilon_0^0)(P))$ (since $\varepsilon_1^1\circ\varepsilon_0^0 = \varepsilon_0^1\circ\varepsilon_0^0$). Furthermore, if $Q \in \mathrm{Supp}(\mathcal{D}(\varepsilon_0^0)(P))$ corresponds to a factor ξ of χ, and $R \in \mathrm{Supp}(\mathcal{D}(\varepsilon_1^1\circ\varepsilon_0^0)(P))$ corresponds to a maximal ideal $\mathfrak{m} \supset (\chi(X),\chi(Y))$ of $K_P\otimes K^{\otimes 3}$, then $R_1 = Q$ if and only if the map ε_1^1 extended to $K_P\otimes K^{\otimes 2}$ maps $K_P[X]/(\xi(X))$ into $K_P[X,Y]/\mathfrak{m}$. That is the case if and only if $\xi(X)\subset\mathfrak{m}$. Likewise, $R_0 = Q$ if and only if $\xi(Y)\subset\mathfrak{m}$. Then, let ξ,ξ' be the factors of χ corresponding respectively to Q and Q'. Any maximal ideal containing the ideal $(\xi(X),\xi'(Y))$ corresponds to a place $R \in M_{K^{\otimes 3}}$ such that $R_1 = Q$ and $R_0 = Q'$. □

If S is a set of places of k and $n \geq 0$, we write $S^{(n)}$ for the set of places of $K^{\otimes(n+1)}$ lying above the elements of S. We also let S_r be the set of non-archimedean places of k that ramify in K.

Lemma 4.3.7. *Let $n \in \mathbb{N}$ be an integer and let $P \in M_K^{\otimes n} \setminus S_r^{(n-1)}$. Then, we have the following:*

1. *The place P is non ramified over k.*
2. *Assume that $n \geq 2$. For $i \in [n-1]_0$, $e_{P,i} = 1$.*

Proof. The second point follows directly from the first since the map $k \to K^{\otimes n}$ factors as $k \to K^{\otimes n-1} \xrightarrow{\varepsilon_i^{n-2}} K^{\otimes n}$.

Now, the first point is a straightforward induction. It is valid for $n = 1$ by hypothesis, and then, if it is true when $n = k$, for some $k \in \mathbb{N}$, it is valid for $n = k + 1$ by Lemma 2.1.2. □

We may now prove a generalised version of Hilbert's theorem 90 in our setting.

Lemma 4.3.8. *Let $D = \sum_{Q \in M_{K^{\otimes 2}}^{na}} n_Q Q \in \operatorname{Ker} \partial_{\mathcal{D}}^1$ be supported by places outside of $S_r^{(1)}$. Then, there exists $E \in \mathcal{D}(K)$ such that $D = \partial_{\mathcal{D}}^0(E)$.*

Proof. We set

$$E = \sum_{P \in M_K^{na}} \left(\min_{Q \in \operatorname{Supp}(\mathcal{D}(\varepsilon_0^0)(P))} n_Q \right) P.$$

Then, by Lemma 4.3.7, we get

$$\mathcal{D}(\epsilon_0^0)(E) = \sum_{Q \in M_{K^{\otimes 2}}^{na}} \left(\min_{Q' \in \operatorname{Supp}(\mathcal{D}(\varepsilon_0^0)(Q_0)} n_{Q'} \right) Q$$

and

$$\mathcal{D}(\epsilon_1^0)(E) = \sum_{Q \in M_{K^{\otimes 2}}^{na}} \left(\min_{Q' \in \operatorname{Supp}(\mathcal{D}(\varepsilon_0^0)(Q_1)} n_{Q'} \right) Q.$$

It follows that

$$D + \mathcal{D}(\epsilon_1^0)(E) = \sum_{Q \in M_{K^{\otimes 2}}^{na}} \left(\min_{Q' \in \operatorname{Supp}(\mathcal{D}(\varepsilon_0^0)(Q_1)} n_Q + n_{Q'} \right) Q.$$

We introduce the following automorphisms:

$$\begin{array}{rccc} \sigma\colon & K^{\otimes 2} & \to & K^{\otimes 2} \\ & a \otimes b & \mapsto & b \otimes a \\ \tau\colon & K^{\otimes 3} & \to & K^{\otimes 3} \\ & a \otimes b \otimes c & \mapsto & a \otimes c \otimes b. \end{array}$$

We have:

$$\tau \circ \varepsilon_0^1 = \varepsilon_0^1 \circ \sigma \tag{4.10}$$

$$\tau \circ \varepsilon_2^1 = \varepsilon_1^1 \tag{4.11}$$

$$\varepsilon_1^0 = \sigma \circ \varepsilon_0^0 \tag{4.12}$$

Let $Q, Q' \in M_{F^{\otimes 2}}^{fi}$ be such that $Q' \in \operatorname{Supp}(\mathcal{D}(\varepsilon_0^0)(Q_1)$. That is, we have $Q_0' = Q_1$, and therefore, by Equation (4.12), $Q_0' = Q_0^{\sigma}$. We apply Lemma 4.3.6

to Q^σ and Q' and we get $R \in M^{fi}_{F^{\otimes 3}}$ such that $R_1 = Q'$ and $R_0 = Q^\sigma$. By Equation (4.11), $R_2^\tau = (R_1) = Q'$ and by Equation (4.10), $R_0^\tau = (R_0)^\sigma = Q$. We may then set $Q'' = R_1^\tau$. Consider the coefficient of R^τ in $\mathcal{D}(\partial^1_{Am})(D) = 0$ and get ($n_Q + n_{Q'} = n_{Q''}$ since $R \notin S_r^{(2)}$. Now, $\varepsilon_0^1 \circ \varepsilon_0^0 = \varepsilon_1^1 \circ \varepsilon_0^0$, so we get

$$\begin{aligned}\mathcal{D}(\varepsilon_1^1 \circ \varepsilon_0^0)(Q_0) &= \mathcal{D}(\varepsilon_0^1)(\mathcal{D}(\varepsilon_0^0)(Q_0)) \\ &= \mathcal{D}(\varepsilon_0^1)(Q) \\ &= R\end{aligned}$$

Furthermore,

$$\begin{aligned}\mathcal{D}(\varepsilon_1^1 \circ \varepsilon_0^0)(Q_0'') &= \mathcal{D}(\varepsilon_1^1)(\mathcal{D}(\varepsilon_0^0)(Q_0'')) \\ &= \mathcal{D}(\varepsilon_1^1)(Q'') \\ &= R\end{aligned}$$

Since $\mathcal{D}(\varepsilon_1^1 \circ \varepsilon_0^0)(Q_0) = \mathcal{D}(\varepsilon_1^1 \circ \varepsilon_0^0)(Q_0'')$, we have $Q_0 = Q_0''$ by Lemma 2.1.26. Conversely, if we fix $Q, Q'' \in M^{fi}_{K^{\otimes 2}}$ such that $Q_0 = Q_0''$, then there exists $R \in M^{fi}_{K^{\otimes 3}}$ such that $R_0 = Q$ and $R_1 = Q''$. We set $Q' = R_2$ and, again, we get that $n_Q + n_{Q'} = n_{Q''}$. As above, we use the fact that $\varepsilon_0^1 \circ \varepsilon_1^0 = \varepsilon_2^1 \circ \varepsilon_0^0$ to prove that $Q_1 = Q_0'$.

This shows that for $Q \in M^{na}_{K^{\otimes 2}}$,

$$\min_{Q' \in \mathrm{Supp}(\mathcal{D}(\varepsilon_1^1)(Q_1))} n_Q + n_{Q'} = \min_{Q' \in \mathrm{Supp}(\mathcal{D}(\varepsilon_0^0)(Q_0))} n_{Q'}.$$

Therefore, $D + \epsilon_1^0(E) = \epsilon_0^0(E)$. That is, $D = \mathcal{D}(\partial^0_{Am})(E)$. □

We now get our main theorem for this section:

Theorem 4.3.9. *Let $b \in B^2_{Am}(k, K)$ be a coboundary. Let S be a finite set of places of k such that:*

- *S contains the archimedean places of K.*
- *S is non-empty.*
- *S contains S_r*
- *The non-archimedean places of $S^{(0)}$ generate the class group* $\mathrm{Cl}(K)$.
- $\mathrm{Supp}(\mathcal{D}(b)) \subset S^{(2)}$.

Then there exists a cochain σ in the group of $S^{(1)}$-units of $K^{\otimes 2}$ such that $b = \partial^1_{Am}(\sigma)$

Proof. Let $\alpha \in C^1_{Am}(k, K)$ be such that $\partial^1_{Am}(\alpha) = b$. We consider the divisor $D = \mathcal{D}(\alpha) = \sum_{Q \in M^{fi}_{K^{\otimes 2}}} n_Q Q$ of α. We set $D_S = \sum_{Q \in S^{(1)}} n_Q Q$ and $D'_S = \sum_{Q \notin S^{(1)}} n_Q Q$. Now, $\partial^1_{\mathcal{D}}(D) = \mathcal{D}(b)$, and therefore is supported by $S^{(2)}$. Observe that by Lemma 2.1.26, if $Q \in M^{na}_{K^{\otimes 2}} \setminus S^{(1)}$, then $\mathcal{D}(\partial^1_{Am})(Q)$ has support disjoint from $S^{(2)}$. It follows that $\partial^1_{\mathcal{D}}(D_{\bar{S}}) = 0$.

The support of D'_S is disjoint from $S^{(1)}_r$. We apply Lemma 4.3.8 and get a divisor $E \in \mathcal{D}(K)$ such that $D'_S = \partial^0_{\mathcal{D}}(E)$. Now, as $S^{(0)}$ generates the class group of K, there exists $E' \in \mathcal{D}(K)$ with support in $S^{(0)}$ and $\gamma \in K^\times$ such that $E = \mathcal{D}(\gamma) + E'$. Then, we get that

$$\partial^0_{\mathcal{D}}(\mathcal{D}(\gamma)) + \partial^0_{\mathcal{D}}(E') = D'_S = D - D_S$$

and therefore

$$\partial^0_{\mathcal{D}}(E') + D'_S = \mathcal{D}(\alpha \partial^0_{Am}(\gamma^{-1})).$$

This shows that $\mathrm{Supp}(\mathcal{D}(\alpha \partial^0(\gamma^{-1}))) \subset S^{(1)}$. That is, $\alpha \partial^0_{Am}(\gamma^{-1})$ is a $S^{(1)}$-unit. Furthermore,

$$\partial^1_{Am}(\alpha \partial^0_{Am}(\gamma^{-1})) = \partial^1_{Am}(\alpha) = b,$$

and $\alpha \partial^0_{Am}(\gamma^{-1})$ is a cochain with the required properties. □

From Theorem 4.3.9, we directly get an algorithm for computing a trivialisation of a 2-coboundary:

Theorem 4.3.10. *Under GRH, Algorithm 2 is correct and runs in polynomial time with access to an oracle for Problem 2.2.16 and for factoring integers.*

Proof. Using a polynomial-time algorithm for factoring polynomials over number fields, one may compute splitting isomorphisms

$$K \simeq \bigoplus_{\alpha} K^{(0)}_\alpha,$$

$$K^{\otimes 2} \simeq \bigoplus_{\beta} K^{(1)}_\beta,$$

and

$$K^{\otimes 3} \simeq \bigoplus_{\gamma} K^{(2)}_\gamma.$$

Input: A number field k
Input: A separable polynomial $P \in k[X]$ defining an étale algebra $K = k[X]/(P)$
Input: $b \in B^2_{Am}(k, K)$
Compute S_1, the set of places of k that ramify in K;
Compute S_2, a set of places of k such that the elements of $S^{(0)}$ generate the class group $\mathrm{Cl}(K)$;
Compute S_3, the set of places of k lying below the elements of $\mathrm{Supp}(\mathcal{D}(b))$;
Set $S = S_1 \cup S_2 \cup S_3$;
Compute the sets $S^{(2)}$ and $S^{(3)}$;
Compute an isomorphism ϕ from the group of $S^{(2)}$-units of $F^{\otimes 2}$ to $\mathbb{Z}^r \oplus \mathbb{Z}/m\mathbb{Z}$;
Compute an isomorphism ψ from the group of $S^{(3)}$-units of $F^{\otimes 3}$ to $\mathbb{Z}^{r'} \oplus \mathbb{Z}/m'\mathbb{Z}$;
Solve the linear equation $(\psi \circ \partial^1_{Am} \circ \phi^{-1})(\alpha) = \psi(b)$;
return α

Algorithm 2: Computing a trivialisation of a 2-coboundary

Then, S_1 may be computed by computing and factoring the discriminants of the number fields $K^{(0)}_\alpha$. This may be done in polynomial time using an oracle for factoring integers. Under GRH, one may set $S_2 = \{\mathfrak{p} \in M^{na}_k : N(\mathfrak{p}) \leq \max_\alpha 12 \log(|\Delta_{K^{(0)}_\alpha}|)^2$. The divisor $\mathcal{D}(b)$ may be computed using an algorithm for factoring ideals in the fields $K^{(2)}_\gamma$. This may be done in polynomial time using an oracle for factoring integers. Then, S-units are computed using an oracle for Problem 2.2.16, and we get isomorphisms ϕ and ψ. Finally, the last step is simple linear algebra over $\mathbb{Z}$.

The correctness of the algorithm relies on the fact that a cochain α such that $b = \partial^1_{Am}(\alpha)$ exists and may be found in the group of $S^{(2)}$-units, which is the content of Theorem 4.3.9. □

Corollary 4.3.11. *Under GRH, Algorithm 2 is correct and is a polynomial quantum algorithm.*

Corollary 4.3.12. *Under GRH, there is a polynomial quantum algorithm for Problem 4.3.1.*

Proof. This result is a combination of Algorithm 2 with the explicit formulas

for isomorphisms given in Proposition 4.2.7 and Example 4.2.3. □

Theorem 4.3.13. *Under GRH, there exists a polynomial quantum algorithm which solves the explicit isomorphism problem (Problem 3.4.1) for number fields.*

Proof. By Corollary 4.3.5, Problem 3.4.1 reduces to Problem 4.3.1 in probabilistic polynomial time and by Corollary 4.3.12, there exists a polynomial quantum algorithm for Problem 4.3.1. □

Chapter 5

Lattices pairs in global function fields

5.1 Vector bundles and lattices

This section we presents results from [60]. As a motivation and for some proofs, use the language of schemes and locally free coherent sheaves, including results on their cohomology. We direct the reader to [42] for an exposition of the necessary material on the topic. For the remainder of the section, we let X be an integral smooth projective curve over a finite field F (we note that most results are valid over a more general field). Unless specified otherwise, k is the field of rational functions of X.

We begin with a definition of four equivalent categories:

Definition 5.1.1. *1. A* vector bundle *over X is a coherent locally free $\mathcal{O}_X$-module. A map of vector bundles is simply a homomorphism of $\mathcal{O}_X$-modules.*

*2. Let k_X be the constant sheaf equal to k over X, and let $n \in \mathbb{N}$. An $\mathcal{O}_X$-*lattice *of rank n is a subsheaf of k_X^n that is a locally free $\mathcal{O}_X$-module of rank n. A map between $\mathcal{O}_X$-lattices $\mathcal{L}$ and $\mathcal{L}'$ of respective ranks n and n' is an $\mathcal{O}_X$-module homomorphism $f\colon k_X^n \to k_X^{n'}$ such that $f(\mathcal{L}) \subset \mathcal{L}'$.*

*3. Let $n \in \mathbb{N}$. An $\mathcal{O}_R$-*lattice *of rank n is a free $\mathcal{O}_R$-submodule $(L_P)_{P \in M_k}$ of R_k^n. A map between $\mathcal{O}_R$-lattices L and L' of ranks n and n' is a map $f\colon k^n \to k^{n'}$ such that $f(L) \subset L'$ when f is extended to R^n by pointwise application.*

4. *A* lattice pair *L of k is the data of an $\mathcal{O}_{fi}$-lattice L_{fi} and an $\mathcal{O}_\infty$-lattice L_∞ of equal ranks. A map between lattice pairs L of rank r and L' of rank r' is a linear map $f\colon k^r \to k^{r'}$ such that $f(L_{fi}) \subset f(L'_{fi})$ and $f(L_\infty) \subset L'_\infty$.*

Theorem 5.1.2. *The four categories introduced in the definition above are equivalent.*

Proof. We describe fully faithful, essentially surjective functors between the categories:

- $2 \to 1$: The forgetful functor from the category of $\mathcal{O}_X$-lattices to that of vector bundles is faithful. It is essentially surjective because any vector bundle E is isomorphic to a lattice once one fixes a basis of its generic stalk E_η: this yields an isomorphism $E_\eta \simeq k^n$, and we get injective maps $\Gamma(U, E) \to k^n$ compatible with restriction maps. These maps yield an injective homomorphism $E \to k^n_X$. Since a map between vector bundles induces a map between generic stalks, it is clear that this functor is full.

- $2 \to 3$: The functor sending an $\mathcal{O}_X$-lattice $\mathcal{L}$ to $\prod_{P\in M} \mathcal{L}_P$ is fully faithful from the definitions of homomorphisms and the fact that a global homomorphism from k^n_X to $k^{n'}_X$ is the same thing as a linear map from k^n to $k^{n'}$. By the local-global principle for $\mathcal{O}_X$-lattices [91, Exercise 9.16], all but finitely many of the $\mathcal{L}_P$ are equal to $\mathcal{O}_P$. Furthermore, all products of $\mathcal{O}_P$-lattices with this property are reached. Such a product of lattices is the same thing as an $\mathcal{O}_R$-lattice by Lemma 2.1.9 and (essential) surjectivity follows.

- $3 \to 4$: By the local-global principle for lattices on a Dedekind domain [91, Theorem 9.4.9], if $L = (L_P)$ is an $\mathcal{O}_R$-lattice, the restriction $(L_P)_{P\in M_k^{fi}}$ determines a unique $\mathcal{O}_{fi}$-lattice which we denote by L_{fi}, furthermore every $\mathcal{O}_{fi}$-lattice can bet obtained this way. We likewise define L_∞ as the unique $\mathcal{O}_\infty$-lattice defined by $(L_P)_{P\in M_k^\infty}$. It is straightforward to deduce that sending an $_R$-lattice L to the pair (L_{fi}, L_∞) yields an equivalence of categories.

□

Remark 5.1.3. By our definitions, the categories 2,3 and 4 are small (their objects form a set), and the equivalence of categories we described are not merely surjective, but they induce a bijection between the sets of objects. As

a result, we may unambiguously fix an object in one of these categories and talk about the associated objects in the other two categories. If L is any type of lattice, we write L_X for the corresponding $\mathcal{O}_X$-lattice, L_R for the corresponding $\mathcal{O}_R$-lattice and L_{LP} for the corresponding lattice pair.

Remark 5.1.4. If L is an $\mathcal{O}_X$-lattice and U is an open subset of X, we observe that $\Gamma(U, L)$ is the subset $\bigcap_{P\in U} L_P$ of $\Gamma(U, k_X) = k$. Indeed, a section $s \in \Gamma(U, L)$ has its stalk in L_P for all $P \in U$ and is therefore sent there by the restriction maps of the sheaf k_X. However, these maps are the identity. Conversely, an element $s \in \bigcap_{P\in U} L_P$ directly glue back into an element of $\Gamma(U, L)$.

5.1.1 $\mathcal{O}_X$-lattices and $\mathcal{O}_R$-lattices

Proposition 5.1.5. *There is a bijection between the set of isomorphism classes of rank n vector bundles and the double quotient*

$$GL_n(k)\backslash GL_n(R)/GL_n(\mathcal{O}_R).$$

Proof. This proposition is an easier version of [94, Proposition 22]. We prove the result for isomorphism classes of rank n. For any $g \in GL_n(R)$, there is an $\mathcal{O}_R$-lattice $R(n) \coloneqq g(\mathcal{O}_R^n)$. This lattice is determined by g up to an automorphism of $\mathcal{O}_R^n$. So, the set of $\mathcal{O}_R$-lattices is in bijection with $GL_n(R)/GL_n(\mathcal{O}_R)$. Furthermore, two lattices in this set are isomorphic if one is the image of the other by an automorphism of k^r applied pointwise. That is, the set of isomorphism classes of $\mathcal{O}_R$-lattices, and therefore of vector bundles over X, is in bijection with the double quotient $GL_n(k)\backslash GL_n(R)/GL_n(\mathcal{O}_R)$. □

As we represent an $\mathcal{O}_R$-lattice L by a matrix g such that $L = R(g)$, we establish how properties of L may be described algebraically using g.

Definition 5.1.6. *Let $g \in GL_n(R)$, let $L = R(g)$. We define* $\det(L) = R(\det(g))$ *and* $\deg(L) = -\deg(\det(g))$.

In order to express the tensor product of $\mathcal{O}_R$-lattices as a lattice, we identify the tensor product $R^r \otimes_R R^{r'}$ with $R^{rr'}$ via the tensor product of the canonical bases. That is, if $(e_1, \ldots, e_n)$ is the canonical basis of R^n and $(e'_1, \ldots, e'_{n'})$ is that of $R^{n'}$, we identify $R^n \otimes R^{n'}$ with $R^{nn'}$ via the basis $(e_1 \otimes e'_1, e_1 \otimes e'_2, \ldots, e_1 \otimes e'_{n'}, e_2 \otimes e'_1, \ldots, e_n \otimes e'_{n'})$.

Proposition 5.1.7. *Let $g \in GL_n(R)$ and $g' \in GL_{n'}(R)$. Let $L = R(g)$.*

1. *The rank one lattice* $\det(L)$ *is independent of the choice of* g *such that* $L = R(g)$. *Furthermore,* $\det(L)_X = \det(L_X)$.

2. *The number* $\deg(L)$ *is independent of the choice of* g *such that* $L = R(g)$. *Furthermore,* $\deg(L_X) = \deg(L)$.

3. $R(g) \otimes_{\mathcal{O}_R} R(g') = R(g \otimes g')$.

4. $R(g) \oplus R(g') = R(g \oplus g')$.

5. *Let* $M \in M_{n',n}(k)$. *Then* M *describes a map from* $R(g)$ *to* $R(g')$ *if and only if* $g'^{-1}Mg \in M_{r',r}(\mathcal{O}_R)$. *That is,* $\mathrm{Hom}(R(g), R(g')) = M_{n',n}(k) \cap g'M_{n',n}(\mathcal{O}_R)g^{-1}$.

Proof. The matrix g such that $L = R(g)$ is defined up to a factor in $GL_n(\mathcal{O}_R)$. Such a factor has a determinant in $\mathcal{O}_R^\times$. Multyplying a répartition by an element of $\mathcal{O}_R^\times$ does not change the $\mathcal{O}_R$-lattice of rank 1 it generates. Thus, $\det(L)$ is independent of the choice of g, and so is $\deg(L)$.

Then, each item is proved by observing that the result holds locally at each $P \in M$. We note that the degree of a rank 1 $\mathcal{O}_R$-lattice is the opposite of the degree of its generator: if $r \in R$ is invertible and $D = \sum_{P \in X} v_P(r_P)P$ is the associated divisor of r, the line bundle associated to $R(r)$ is in fact $\mathcal{L}(-D)$, and by the definition of the degree of a répartition, $\deg r = \deg D$. □

Definition 5.1.8. *If* L *is an* $\mathcal{O}_R$*-lattice of rank* n*, the set*

$$L^\vee = \left\{ a \in R^n \mid \forall b \in L, \sum_{i=1}^{n} a_i b_i \in \mathcal{O}_R \right\}$$

is called the dual lattice of L.

Proposition 5.1.9. *Let* L *be an* $\mathcal{O}_R$*-lattice. The dual* $L^\vee$ *is an* $\mathcal{O}_R$*-lattice. This duality is the same as that of vector bundles:*

$$(L^\vee)_X \simeq (L_X)^\vee.$$

Proof. If $g \in GL_n(R)$ is such that $L = R(g)$, then $L^\vee = R({}^t g^{-1})$ and therefore $L^\vee$ is an $\mathcal{O}_R$-lattice.

Let $U \subset X$ be an open subset, and let $a = (a_1, \ldots, a_n) \in \Gamma(U, (L^\vee)_X) \subset \Gamma(U, k_X^n) = k^n$. For any $s = (s_1, \ldots, s_n) \in \Gamma(U, L_X)$, define $a(s) = \sum_{i=1}^r a_i s_i \in \Gamma(U, k_X)$. Then, for all $P \in U$, $a(s) \in \mathcal{O}_P$ since $a \in (L^\vee)_P$ and $s \in L_P$. Thus, $a(s) \in \Gamma(U, \mathcal{O}_X)$ seen as a subset of $\Gamma(U, k_X)$, and a does

define a homomorphism $\Gamma(U, L) \to \Gamma(U, \mathcal{O}_X)$. It is clear from the definition of this homomorphism that it is compatible with restriction maps.

This yields a homomorphism $\Gamma(U, (L^\vee)_X) \to \Gamma(U, (L_X)^\vee)$. The fact that it is an isomorphism may be checked locally. □

Remark 5.1.10. We record from the proof of Proposition 5.1.9 that if $g \in GL_n(R)$, $R(g)^\vee = R({}^t g^{-1})$. For convenience, when $g \in GL_n(R)$, we set $g^\vee = {}^t g^{-1}$.

Remark 5.1.11. Item 5 of Proposition 5.1.7 suggests that if $g \in GL_n(R)$ and $g' \in GL_{n'}(R)$, then $\mathrm{Hom}(R(g), R(g'))$ is the set of global sections of the $\mathcal{O}_X$-lattice corresponding to the free $\mathcal{O}_R$-submodule $g' M_{n',n}(\mathcal{O}_R) g^{-1}$ of $M_{n',n}(R)$. For any commutative ring B, the dual of the regular B-module B is identified with B itself, via the isomorphism $b \mapsto (a \mapsto ab)$. Then, there is a natural identification $M_{n',n}(B) = B^n \otimes B^{n'}$. The basis $e_1 \otimes e'_1, e_1 \otimes e'_2, \ldots, e_2 \otimes e'_1, \ldots, e_n \otimes e'_{n'}$ we use in general for $B^n \otimes_B B^{n'}$ then identifies with the basis of elementary matrices $(E_{11}, E_{12}, \ldots, E_{r1}, E_{21}, \ldots, E_{nn'})$. One checks easily that upon identifying $M_{n',n}(R)$ with $R^{n'n}$, $g' M_{n',n}(\mathcal{O}_R) g^{-1}$ is sent to $L^\vee \otimes L'$. For this reason, we set $\mathcal{H}om(R(g), R(g')) = g' M_{n',n}(\mathcal{O}_R) g^{-1}$ which we also identify with $R(g)^\vee \otimes_{\mathcal{O}_R} R(g')$.

5.1.2 Cohomology of $\mathcal{O}_R$-lattices

We may explicitly describe the cohomology of vector bundles in terms of répartitions. We first introduce some notation and then quote a result of [86,94], which generalises [79, Proposition II.5.3].

Definition 5.1.12. *If L is an $\mathcal{O}_R$-lattice of rank n, we define the cohomology groups*

$$H^0(L) = L \cap k^n$$

and

$$H^1(L) = R^n / (L + k^n).$$

As usual, this definition is compatible with the analogous definition on X-lattices:

Proposition 5.1.13. *Let L be an $\mathcal{O}_R$-lattice of rank n. Then $H^0(X, L_X) = \Gamma(X, L_X)$ injects in k^n and we get:*

$$H^0(L) = H^0(X, L_X).$$

Furthermore, there is an isomorphism

$$H^1(L) \simeq H^1(X, L_X).$$

We first need a lemma:

Lemma 5.1.14. *Let L be an $\mathcal{O}_X$-lattice of rank n. Then for any open subset $U \subset X$, $\Gamma(U, k_X^n/L) = \bigoplus_{P\in U} k^n/L_P$. In particular, the sheaf k_X/L is flasque.*

Proof. It is enough to prove the result on an open cover of X, so we may assume without loss of generality that $U = \mathrm{Spec}(A)$ is an affine open subset of X over which L is free. Then, L_A may be seen as an A-lattice isomorphic to A^n, and we must prove that $k^n/L_A \simeq \bigoplus_{\mathfrak{p}\in\mathrm{Spec}(A)} k^n/L_P$. Fix $(a_1, \ldots, a_n)$ a basis of L_A and then $k^n/L_A = \bigoplus_{i=1}^r ka_i/Aa_i$. It is enough to prove the result for $L_A = A$. However, if A is a Dedekind domain and k is its fraction field, then $k/A \simeq \bigoplus_{\mathfrak{p}\in\mathrm{Spec}(A)} k/A_{\mathfrak{p}}$ by the Chinese Remainder Theorem. □

Proof of Proposition 5.1.13. We rephrase Serre's argument and adapt it to our broader context. By Lemma 5.1.14, the middle and right terms of the exact sequence

$$0 \to L_X \to k_X^n \to k^n/L_X \to 0$$

are flasque sheaves, so $H^1(X, k_X^n) = H^1(X, k_X^n/L_X) = 0$ [42, Proposition III.2.5]. Therefore, the cohomology of L_X may be computed as the kernel and cokernel of the map $\Gamma(X, k_X^n) \to \Gamma(X, k_X^n/L_X)$. Now, $\Gamma(k, k_X^n) = k^n$ and by Lemma 5.1.14, $\Gamma(X, k_X^n/L_X) \simeq \bigoplus_{P\in X} k^n/L_P = R/L$.

This gives isomorphisms $H^*(L) \simeq H^*(X, L_X)$. The fact that the isomorphism of H^0 groups is an equality under the identification of $H^0(X, L_X)$ with its image in k^r is a consequence of Remark 5.1.4. □

We conclude this subsection by explicitly describing Serre duality in our setting. This is a rephrased version of a theorem for adèles proved in [86]. It would be possible to adapt Serre's proof given in [79, Section II.8] and prove the theorem using only the theory of répartitions and differentials. However, for efficiency purposes, we will assume that the statement of Serre duality for coherent sheaves on projective curves is already known and content ourselves with giving concrete formulas for computation.

Theorem 5.1.15 (Serre Duality)**.** *Let ω be a differential of k. For any $\mathcal{O}_R$-lattice L of rank n, there is a perfect pairing*

$$\begin{array}{rccc} \theta_\omega\colon & H^0(\iota(\omega)^{-1}L^\vee) \times H^1(L) & \to & F \\ & (a, b) & \mapsto & \mathrm{res}\left(\sum_{i=1}^n a_i b_i \iota(\omega)\right). \end{array}$$

Proof. We first prove that θ is a well-defined pairing. For $a \in H^0(\iota(\omega)^{-1}L^\vee)$, consider the map

$$\begin{array}{rccc} \theta'_\omega(a,\cdot): & R^n & \to & F \\ & b & \mapsto & \operatorname{res}\left(\sum_{i=1}^n a_i b_i \iota(\omega)\right). \end{array}$$

We prove that $L + k^n \subset \operatorname{Ker}(\theta'_\omega(a,\cdot))$. Observe that

$$H^0(\iota(\omega)^{-1}L^\vee) = \left\{ f \in k^n \mid \forall b \in L, \sum_{i=1}^n \iota(\omega) a_i b_i \in \mathcal{O}_R \right\}.$$

If $b \in L$, $ab\iota(\omega) \in \mathcal{O}_R^n$, so $\theta'_\omega(a,b) = \operatorname{res}\left(\sum_{i=1}^n a_i b_i \iota(\omega)\right) = 0$ since $\operatorname{res}(x) = 0$ for any $x \in \mathcal{O}_R$. If $b \in k^n$, then $\sum_{i=1}^n a_i b_i \iota(\omega) = \iota(\sum_{i=1}^n a_i b_i \omega)$ since the set of differentials of k is a k-vector space. Therefore, $\theta'_\omega(a,b) = 0$ by the Residue Theorem. It follows that $\theta'_\omega(a,\cdot)$ factors into a unique map $\theta_\omega(a,\cdot)$ from $H^1(L)$ to k. The pairing θ_ω is well defined.

We prove that the map $a \mapsto \theta_\omega(a,\cdot)$ is injective. Let $a \in H^0(\iota(\omega)^{-1}L^\vee)$ Assume that $a_{i,P} \neq 0$ for some $i \in [r]$, $P \in X$ and set $\nu = \operatorname{ord}_P(a\iota(\omega)) + 1$, $b_j = 0$ for $j \neq i$, $b_{i,Q} = 0$ for $Q \neq P$ and $b_{i,P} = 1/\pi_P^\nu$. Then $\theta_a(b) = \operatorname{res}_P(\iota(\omega) a_i b_i) \neq 0$. Therefore, the map θ_a is non-zero over R^n and therefore over $H^1(L) = R^n/(L + k^n)$.

Since $H^0(\omega^{-1}L^\vee)$ and $H^1(L)$ are finite-dimensional F-vector spaces of equal dimensions (for instance by Serre duality for coherent sheaves), it follows that the map $a \mapsto \theta_a$ is an isomorphism. That is, θ is a perfect pairing. □

Remark 5.1.16. The pairing θ_ω behaves naturally with the change of differential. More precisely, if $\omega' = f\omega$ is a different differential of the field k, then multiplication by f gives an isomorphism $H^0(\iota(\omega')^{-1}L^\vee) \simeq H^0(\iota(\omega)L^\vee)$. We easily check that for any $a \in H^0(\iota(\omega')^{-1}L^\vee)$, $\theta_{\omega'}(a) = \theta_\omega(fa)$.

5.1.3 Extensions of $\mathcal{O}_R$-lattices

We briefly recall the general theory of extension of vector bundles. We then give an explicit construction of an extension of $\mathcal{O}_R$-lattices. A reference for extensions of vector bundles is [56, Section 7.3].

Definition 5.1.17. *Let F, G be vector bundles over X. Then an extension of F by G is an exact sequence*

$$0 \to G \to E \to F \to 0.$$

A map of extensions is a map of exact sequences. We note that two extensions of F by G may not be isomorphic as extensions, even though the vector bundles in the middle of the sequences are. It is well known that module extensions are generally classified by the cohomology group $\mathrm{Ext}^1(F, G)$. In the case of vector bundles, this group is naturally isomorphic to $H^1(X, F^\vee \otimes G)$, with the isomorphism given as follows:

Proposition 5.1.18. *Let F and G be vector bundles over X. Then, there is a bijection δ between the set of isomorphy classes of extensions of F by G and $H^1(X, F^\vee \otimes G)$. The map δ is defined as follows: let ξ be an extension given by the exact sequence*

$$0 \to G \to E \to F \to 0.$$

Then, the following sequence is also exact.

$$0 \to F^\vee \otimes G \to F^\vee \otimes E \to F^\vee \otimes F \to 0.$$

This sequence yields a map $\partial\colon \mathrm{Hom}(F, F) = H^0(F^\vee \otimes F) \to H^1(F^\vee \otimes G)$. Then, $\delta(\xi) = \partial(Id_F)$.

This result is usually proved using injective resolutions of sheaves, which yields a construction of the map δ^{-1}. However, this is impractical in a computational setting. Instead, we adapt the methods from [93, Section 2] and redo the computation using the exact sequence from the proof of Proposition 5.1.13.

Theorem 5.1.19. *Let $g' \in GL_{n'}(R)$ and $g'' \in GL_{n''}(R)$. Let $\kappa \in M_{n',n''}(R)$. Then κ represents an element of $H^1(\mathcal{H}om(R(g''), R(g')))$ and therefore an extension of $R(g'')$ by $R(g')$. The following exact sequence represents this extension.*

$$0 \to R(g') \xrightarrow{\iota} R(g) \xrightarrow{\pi} R(g'') \to 0,$$

where

$$g = \begin{pmatrix} g' & -\kappa g'' \\ 0 & g'' \end{pmatrix} \in GL_n(R)$$

and ι and π are respectively given by the injection of $k^{n'}$ into the n' first summands of k^n and by the projection of k^n onto its last n'' summands.

Proof. Recall from the proof of Proposition 5.1.13 that for any $\mathcal{O}_X$-lattice L, we have the exact sequence

$$0 \to L_X \to K_X^r \to K_X^r/L_X \to 0,$$

which gives rise to the following long exact sequence:

$$H^0(L) \to K^r \to R^r/L \to H^1(L). \tag{5.1}$$

Indeed, R^r/L is none other than $\bigoplus_{P\in X} K^r/L_P$, which is the group $H^0(X, K_X/L_X)$ by Lemma 5.1.14.

Let $L = R(g)$, $L' = R(g')$ and $L'' = R(g'')$. Writing (5.1) vertically for each term of the short exact sequence

$$0 \to \mathcal{H}om(L''_X, L'_X) \to \mathcal{H}om(L''_X, L_X) \to \mathcal{E}nd(L''X) \to 0,$$

we get the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}(L'', L') & \longrightarrow & \mathrm{Hom}(L'', L) & \longrightarrow & \mathrm{End}(L'') & \xrightarrow{\partial} & \dots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_{n',n''}(k) & \longrightarrow & M_{n,n''}(k) & \longrightarrow & M_{n''}(k) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_{n',n''}(R)/\mathcal{H}om(L'', L') & \longrightarrow & M_{n,n''}(R)/\mathcal{H}om(L'', L) & \longrightarrow & M_{n''}(R)/\mathcal{E}nd(L'') & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\dots & \xrightarrow{\partial} & H^1(\mathcal{H}om(L'', L')) & \longrightarrow & H^1(\mathcal{H}om(L'', L)) & \longrightarrow & H^1(\mathcal{E}nd(L'')) & \longrightarrow & 0.
\end{array}$$

At each line, the maps are between rings of matrices with coefficients either in k or in R. Either way, the first map always sends a matrix M' of size $n' \times n''$ to the matrix $\begin{pmatrix} M \\ 0 \end{pmatrix}$ of size $n' + n'' \times n''$ and the second map sends a matrix $M = \begin{pmatrix} M_1 \\ M_2 \end{pmatrix}$ of size $n' + n'', n''$ to the matrix M_2 of size $n'' \times n''$. Regardless of the coefficient ring, we denote this injection and projection by ι' and π'. We wish to compute $\delta(\xi) = \partial(Id''_L)$. By the usual proof of the snake lemma, $\partial(Id''_L) \in H^1((L'')^\vee_R)$ is represented by a matrix $c \in M_{n',n''}(R)$ such that there exist $U \in M_{n',n''}(k)$ and $V \in \mathcal{H}om(L'', L) = gM_{n,n''}(\mathcal{O}_R)g''^{-1}$ such that $\iota'(c + U) = \begin{pmatrix} 0 \\ I_{n''} \end{pmatrix} + V$. Now, if $M = \begin{pmatrix} M_1 \\ M_2 \end{pmatrix} \in M_{n,n''}(\mathcal{O}_R)$ (with M_1 having n' lines and M_2 having n''), we get

$$\begin{aligned} gMg''^{-1} &= \begin{pmatrix} g' & -\kappa g'' \\ 0 & g'' \end{pmatrix} \begin{pmatrix} M_1 g''^{-1} \\ M_2 g''^{-1} \end{pmatrix} \\ &= \begin{pmatrix} g'M_1 g''^{-1} + -\kappa g'' M_2 g''^{-1} \\ g'' M_2 g''^{-1} \end{pmatrix}. \end{aligned}$$

Therefore, setting $M_2 = -I_{n''}$ and $M_1 = 0$, we construct $V = \begin{pmatrix} \kappa \\ -I_{n''} \end{pmatrix} \in \mathcal{H}om(L'', L)$, and observe that $\iota'(\kappa) = \begin{pmatrix} 0 \\ I_{n''} \end{pmatrix} + V$. It follows

directly that the class $\delta(\xi) = \partial(Id_{L''})$ in $H^1(\mathcal{H}om(L'', L'))$ is represented by the matrix κ. □

5.1.4 Restriction and conorm of an $\mathcal{O}_R$-lattice

This section considers a finite separable function field extension K/k. We also set $d = [K : k]$. As this separable extension corresponds to a separable morphism of algebraic curves, we define the restriction and conorm of an $\mathcal{O}_R$-lattice as the counterpart of respectively the direct and inverse image of a vector bundle.

The first convention we adopt for the rest of this section is that we assume a fixed k-basis of K denoted by $c_1, \ldots, c_d$. Using this, we identify K with k^d and more generally $(K)^n$ with k^{nd} as k-vector spaces. That is, if $e_1, \ldots, e_n$ is a basis of K^n, the corresponding basis of k^{nd} is $(e_1c_1, e_1c_2, \ldots, e_1c_d, e_2c_1, \ldots, e_nc_d)$. If $Q \in M_K$, we let Q_k be the place in M_k lying below Q.

Definition 5.1.20. *Let L be an $\mathcal{O}_{R_k}$-lattice of rank n and let L' be an $\mathcal{O}_{R_K}$-lattice of rank n'.*

- *The* restriction *of L' to k is the $\mathcal{O}_{R_k}$-lattice of rank dn' defined locally at $P \in M_k$ by*
$$(\mathrm{Rest}(L'))_P \coloneqq \bigcap_{\substack{Q \in M_K \\ Q|P}} L'_Q.$$
- *The* conorm *of L over K is the $\mathcal{O}_{R_K}$-lattice of rank n defined locally at $Q \in M_K$ by*
$$(\mathrm{CoN}(L))_Q \coloneqq \mathcal{O}_Q L_{Q_K}.$$

Proposition 5.1.21. *Let $f : X \to X'$ be a morphism of curves corresponding to the function field extension K/k. Let L be an $\mathcal{O}_{R_k}$-lattice and L' be an $\mathcal{O}_{R_K}$-lattice. Then,*
$$\mathrm{Rest}(L')_{X'} = f_*(L'_{X'})$$
and
$$\mathrm{CoN}(L)_X = f^*(L_X).$$

Proof. This result is directly checked on stalks. □

It is well known that for quasi-coherent sheave, and therefore for vector bundles, there exist natural isomorphisms $H^*(X', L'_{X'}) \simeq H^*(X, f_*(L'_{X'}))$. This isomorphism becomes equality for H^0 in our setting.

Regarding H^1, we will identify the space R_k^{nd} with its image in R_K^n by the injective map φ defined as follows: First identify R_k^{nd} with the restricted product $\left(\tilde{\prod}_{P\in M_k} K\right)^n$, and then send a vector $(v_P)_{P\in M_k}$ to $(v_{Q_k})_{Q\in M_K}$. We then get the following identification.

Proposition 5.1.22. *Let L' be an $\mathcal{O}_{R_K}$-lattice. Then under the usual identification $(K)^r = k^{rn}$,*

$$H^0(L') = H^0(\mathrm{Rest}(L')).$$

Furthermore, the map φ described above factors into an isomorphism

$$\tilde{\varphi}\colon H^1(\mathrm{Rest}(L')) \simeq H^1(L').$$

Proof. A direct computation proves the first result:

$$\begin{aligned} H^0(L') &= \bigcap_{Q\in M_K} L'_Q \\ &= \bigcap_{P\in M_k} \bigcap_{\substack{Q\in M_K \\ Q|P}} L'_Q \\ &= \bigcap_{P\in M_k} \mathrm{Rest}(L')_P \\ &= \bigcap_{P\in M_k} H^0(X, \mathrm{Rest}(L')_X) \\ &= H^0(\mathrm{Rest}(L')). \end{aligned}$$

For the second result, we prove that $\varphi^{-1}(L' + k^{nd}) = \mathrm{Rest}(L') + k^n$. First, observe that $\varphi(R^{nd})$ is the space of répartition vectors v such that $v_Q = v_{Q'}$ if Q and Q' lie above the same place of k. It is also clear that $\varphi(k^{nd}) = K^n$.

Next, we observe that $\varphi(\mathrm{Rest}(L')) = L' \cap \varphi(R_k^{nd})$. Indeed, let $v \in L' \cap \varphi(R_k^{nd})$, and fix $P \in M_k$. Then, for all $i \in [n]$, the $v_{i,Q}$ are equal for all $Q \mid P$, and we denote their common value by $v_{i,P}$. It follows that

$$(v_{1,P}, \ldots, v_{n,P}) \in \cap_{Q|P} L'_Q = (\mathrm{Rest}(L'))_P.$$

Therefore, $v \in \varphi(\mathrm{Rest}(L'))$ and $L' \cap \varphi(R_k^{nd}) \subset \mathrm{Rest}(L')$. The converse inclusion is clear enough.

As $\varphi(k^{nd}) = (K)^n$ and $\varphi(\mathrm{Rest}(L')) = L' \cap \varphi(R_k^{nd})$, we have

$$\mathrm{Rest}(L') + k^{nd} = \varphi^{-1}(L' + K^n).$$

Indeed, let $r \in R_k^{nd}$ such that $\varphi(r) = s + t$, with $s \in L'$ and $t \in K^n$. Set $u \in k^{nd}$ such that $\varphi(u) = t$ and observe that $\varphi(r - u) \in L' \cap \varphi(R_k^{nd})$. So, $r - u \in \mathrm{Rest}(L')$ and $r \in \mathrm{Rest}(L') + k^{nd}$.

This shows that φ factors into an injective map from $H^1(\mathrm{Rest}(L'))$ to $H^1(L')$. Surjectivity follows from equality of dimensions, as it is known that these two finite-dimensional F-vector spaces are isomorphic from general results on quasi-coherent sheaves. □

5.1.5 Indecomposable $\mathcal{O}_R$-lattices

Since the Krull-Schmidt theorem applies to the category of vector bundles over X [4], and as the direct sum of two $\mathcal{O}_R$-lattices is easily constructed, we are primarily concerned with constructing vector bundles that do not split into a direct sum of vector bundles. We recall here results from [3] and interpret them in terms of $\mathcal{O}_R$-lattices. Results stated without proof in this section are simple restatements of results from the sources above.

Definition 5.1.23. *An $\mathcal{O}_R$-lattice L is indecomposable if for any $\mathcal{O}_R$-lattices L' and L'' such that $L \simeq L' \oplus L''$, either L' or L'' is the zero module.*

An $\mathcal{O}_R$-lattice L is absolutely indecomposable if its conorm over $\overline{F}k$ is an indecomposable $\mathcal{O}_{R_{\overline{F}k}}$-lattice.

Remark 5.1.24. Since the objects of the category of $\mathcal{O}_R$-lattices are free $\mathcal{O}_R$-modules this notion may seem trivial. However, since we restrict the maps to homomorphisms that are globally defined (that is, defined by a matrix with coefficients in k), our notion of direct sum is also restricted, and there may exist indecomposable $\mathcal{O}_R$-lattices of rank larger that 1.

Proposition 5.1.25 (Krull-Schmidt-Atiyah)**.** *Any $\mathcal{O}_R$-lattice L admits a decomposition into a direct sum of indecomposable $\mathcal{O}_R$-lattices*

$$L \simeq \bigoplus_{i=1}^{s} L_i^{n_i}.$$

Furthermore, such a decomposition is unique up to reindexing the summands.

Let L be an $\mathcal{O}_R$-lattice L. Then, $\mathrm{End}(L)$ is an F-algebra. We denote by $D(L)$ the Wedderburn-Malcev complement $D(\mathrm{End}(L))$. We get the following description of the structure of L:

Proposition 5.1.26. *Let L be an $\mathcal{O}_R$-lattice, and let*

$$D(L) = \bigoplus_{i=1}^{s} M_{n_i}(D_i)$$

be the splitting of $D(L)$ into a direct sum of simple F-algebras. Then it is well known that

$$L \simeq \bigoplus_{i=1}^{s} L_i^{n_i},$$

where L_i is an indecomposable $\mathcal{O}_R$-lattice and $D(L_i) \simeq D_i$. Furthermore, the action of $D(L)$ on L is compatible with this isomorphism. In particular, L is indecomposable if and only if $D(L)$ is a division algebra.

Following [3], and since the field F is perfect, we also have

Proposition 5.1.27. *An $\mathcal{O}_R$ lattice is absolutely indecomposable if and only if $D(L) \simeq F$.*

In order to represent indecomposable vector bundles in terms of absolutely indecomposable vector bundles, the authors introduce the notion of trace of a vector bundle:

Definition 5.1.28. *Let F' be a finite extension of F, let $X_{F'} = X \times_F \mathrm{Spec}(F')$ and let $p\colon X_{F'} \to X$ be the projection map. Let E be a vector bundle over $X_{F'}$, then the* trace of E *is set to be* $\mathrm{Tr}_{F'/F}(E) = p_*(E)$.

They then prove the following result:

Proposition 5.1.29. *Let F be an indecomposable vector bundle on X and let F' be a maximal field contained in $D(F)$. Then, there is an absolutely indecomposable vector bundle E on $X_{F'}$ such that $F = \mathrm{Tr}_{F'/F}(E)$.*

In order to translate Proposition 5.1.29 in terms of $\mathcal{O}_R$-lattice, we only need to give an interpretation of the trace defined above, which is a restriction:

Definition 5.1.30. *Let F'/F be a separable extension of F, and let $F'k$ be the corresponding constant field extension of k. Then if L' is an $\mathcal{O}_{R_{F'k}}$-lattice, we set*

$$\mathrm{Tr}_{F'/F}(L') = \mathrm{Rest}(L').$$

5.2 Explicit computations with lattice pairs

5.2.1 Algorithmic representation of lattice pairs

Definition 5.2.1. *A matrix pair of rank n is a tuple $g = (\mathfrak{a}, g_{fi}, g_\infty)$, where $PM = (\mathfrak{a}, g_{fi})$ is an invertible square pseudo-matrix of size n over $\mathcal{O}_{fi}$ and $g_\infty \in GL_n(k)$. Given such a matrix pair g, we define the lattice pair $\mathrm{LP}(g)$ as the pair of lattices $(PM(\mathcal{O}_{fi}^n), g_\infty(\mathcal{O}_\infty^n))$, and say that g is a matrix pair for L if $L = \mathrm{LP}(g)$.*

Theorem 5.2.2. *Let $L = (L_{fi}, L_\infty)$ be a lattice pair over k. Then, there exists a matrix pair g such that $L = \mathrm{LP}(g)$.*

Proof. Since the ring $\mathcal{O}_{fi}$ is a Dedekind domain and the ring $\mathcal{O}_\infty$ is a PID, the lattice L_{fi} admits a pseudo-basis and the lattice L_∞ admits a basis. Representing the pseudo-basis of L_{fi} as a pseudo-matrix $(\mathfrak{a}, g_{fi})$ and the basis of L_∞ as a matrix g_∞, we obtain a matrix pair $g = (\mathfrak{a}, g_{fi}, g_\infty)$ such that $L = \mathrm{LP}(g)$. □

This section aims to translate the results from Section 5.1 in terms of matrix representations of lattice pairs. While there is no one-to-one translation from répartition matrices to matrix pairs, a matrix pair may be represented as a répartition matrix in the following manner:

Definition 5.2.3. *Let $g = (\mathfrak{a}, g_{fi}, g_\infty)$ be a matrix pair. We call $x_1, \ldots, x_n$ the columns of g_{fi} For any $P \in M$, we set:*

$$g_P = \begin{cases} g_\infty \text{ if } P \in M^\infty \\ \begin{pmatrix} \pi_P^{\mathrm{ord}_P(\mathfrak{a}_1)} x_1 & \ldots & \pi_P^{\mathrm{ord}_P(\mathfrak{a}_n)} x_n \end{pmatrix} \text{ otherwise} \end{cases}$$

and we let $\mathrm{rép}(g) = (g_P)_{P \in X}$ be the répartition matrix associated to g.

Remark 5.2.4. It is clear that the $\mathcal{O}_R$-lattice $R(\mathrm{rép}(g))$ corresponds to the lattice pair $\mathrm{LP}(g)$. Therefore, in order to give an algorithm to realise any construction discussed in Section 5.1, it is enough to give an algorithmic construction of a matrix pair g such that $\mathrm{rép}(g)$ corresponds to the same construction in terms of répartition matrices. In particular, any construction directly compatible with localisations is compatible with this correspondence.

We get a first batch of straightforward constructions:

Definition 5.2.5. *Let $g = (\mathfrak{a}, g_{fi}, g_\infty)$ and $g' = (\mathfrak{a}', g'_{fi}, g'_\infty)$ be matrix pairs of respective ranks n and n'.*

1. *We define* $\det(g) = \left(\prod_{i=1}^{n} \mathfrak{a}_i, \det(g_{fi}), \det(g_\infty)\right)$.

2. *If I is a fractional ideal of $\mathcal{O}_{fi}$, we set* $\deg(I) = \sum_{P \in X_{fi}} \operatorname{ord}_P(I)$. *If $a \in k^\times$, we set* $\deg_{fi}(a) = \deg(a\mathcal{O}_{fi})$ *and* $\deg_\infty(a) = -\deg_{fi}(a) = \sum_{P \in X_\infty} v_P(a)$.

3. *If $n = 1$, we set* $\deg(g) = \deg(\mathfrak{a}) + \deg_{fi}(g_{fi} + \deg_\infty(g_\infty)$. *If $r > 1$, we set* $\deg(g) = \deg(\det(g))$. *Then, we define* $\deg(\mathrm{LP}(g)) = -\deg(g)$.

4. *We define*

$$g \otimes g' = \left((\mathfrak{a}_1\mathfrak{a}'_1, \mathfrak{a}_1\mathfrak{a}'_2 \ldots, \mathfrak{a}_1\mathfrak{a}'_{n'}, \mathfrak{a}_2\mathfrak{a}'_1, \ldots, \mathfrak{a}_n\mathfrak{a}'_{n'}), g_{fi} \otimes g'_{fi}, g_\infty \otimes g'_\infty\right).$$

5. *We define* $g \oplus g' = \left((\mathfrak{a}_1, \ldots, \mathfrak{a}_n, \mathfrak{a}'_1, \ldots, \mathfrak{a}'_{n'}), g_{fi} \oplus g'_{fi}, g_\infty \oplus g'_\infty\right)$.

6. *We define* $g^\vee = \left((\mathfrak{a}_1^{-1}, \ldots, \mathfrak{a}_r^{-1}), (g_{fi}^t)^{-1}, (g_\infty^t)^{-1}\right)$.

Theorem 5.2.6. *Let g and g' be matrix pairs. We have*

1. $\mathrm{rép}(\det(g)) = \det(\mathrm{rép}(g))$.

2. $\deg(g) = \deg(\mathrm{rép}(g))$.

3. $\mathrm{rép}(g \otimes g') = \mathrm{rép}(g) \otimes \mathrm{rép}(g')$.

4. $\mathrm{rép}(g \oplus g') = \mathrm{rép}(g) \oplus \mathrm{rép}(g')$.

5. $\mathrm{rép}(g^\vee) = \mathrm{rép}(g)^\vee$.

Proof. All of these constructions may be checked locally. One must check that the operation done on the tuple of ideals matches the movements of the columns of g_{fi}. □

Remark 5.2.7. It is more tedious to translate our statement on homomorphisms of lattices directly. Instead, we may simply define $\mathcal{H}om(L, L') = L^\vee \otimes L'$ and recall the isomorphism $M_{n',n}(k) \simeq k^{nn'}$ given by the basis of elementary matrices. Then, an algorithm for computing the lattice pair of homomorphisms follows from Theorem 5.2.6.

Example 5.2.8. We let $F = \mathbb{F}_7$ and consider the genus 1 function field $k = F(x, y)/(y^2 - x^3 - x)$. We let $\pi = \frac{y}{x^2}$ be a local uniformiser at infinity. Observe that $\mathfrak{p} = \langle x, y\rangle$ is a prime ideal of $\mathcal{O}_{fi}$. We consider the lattice pair

$$L = \mathrm{LP}\left(\left(\mathcal{O}_{fi}, \mathfrak{p}^{-1}\right), \begin{pmatrix} \frac{x^2}{x^2+4} & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -\pi^{-1} \\ 0 & 1 \end{pmatrix}\right).$$

We compute

$$\det(L) = \mathrm{LP}\left(\mathfrak{p}^{-1}, \frac{x^2}{x^2+4}, 1\right),$$

and therefore

$$\deg(L) = -\deg(\mathfrak{p}^{-1}) = 1.$$

5.2.2 Restriction and conorm of a lattice pair

We adopt the same notations and setting as in Section 5.1.4. We also write $\mathcal{O}'_{fi}$ and $\mathcal{O}'_\infty$ for the respective integral closures of $\mathcal{O}_{fi}$ and $\mathcal{O}_\infty$ in K.

Definition 5.2.9. *Let $L' = (L'_{fi}, L'_\infty)$ be a lattice pair of rank n over K. We define* $\mathrm{Rest}(L')$ *as the pair* $(\mathrm{Rest}(L'_{fi}), \mathrm{Rest}(L'_\infty))$*, where* $\mathrm{Rest}(L'_*)$ *is the lattice L'_* seen as an $\mathcal{O}_*$-lattice under the identification $K^n = k^{nd}$ (where $*$ is either fi or ∞).*

Let $L = (L_{fi}, L_\infty)$ be a lattice pair of rank r over k. We define $\mathrm{CoN}(L)$ *as the pair* $(\mathrm{CoN}(L_{fi}), \mathrm{CoN}(L_\infty))$*, where* $\mathrm{CoN}(L_*) = \mathcal{O}'_* L_* \subset K^r$ *is an $\mathcal{O}'_*$-lattice.*

One checks readily that these definitions are compatible with the equivalent definitions on $\mathcal{O}_R$-lattices.

Matrix pairs for $\mathrm{Rest}(L)$ and $\mathrm{CoN}(L)$ may easily be computed.

Definition 5.2.10. *Let $g = (\mathfrak{a}, g_{fi}, g_\infty)$ be a matrix pair of rank n defined over k. We set*

$$\mathrm{CoN}(g) = \left((\mathfrak{a}_1\mathcal{O}'_{fi}, \ldots, \mathfrak{a}_n\mathcal{O}'_{fi}), g_{fi}, g_\infty\right).$$

The definition of the restriction of a matrix-pair is more tedious to write down. First, we define the restriction of a pseudo-matrix. The definition is given over any Dedekind domain with fraction field K, as it applies to both $\mathcal{O}_{fi}$ and $\mathcal{O}_\infty$, with the specificity that we only consider pseudo matrices with trivial coefficient ideals over $\mathcal{O}_\infty$, since it is a PID.

Definition 5.2.11. *Let $\mathcal{O}'_*$ be a Dedekind domain with fraction field K, and set $\mathcal{O}_* = \mathcal{O}'_* \cap k$. Let $PM = (\mathfrak{a}, g)$ be a pseudo-matrix of rank n over $\mathcal{O}'_*$. The ideals $\mathfrak{a}_i$ each admit a pseudo-basis $(\mathfrak{b}_{i1}, \ldots, \mathfrak{b}_{id}), (a_{i1}, \ldots, a_{id})$ over $\mathcal{O}_*$.*

Then, we define the pseudo-matrix $\mathrm{Rest}(PM)$ *of rank nd over $\mathcal{O}_*$ with*

coefficient ideals $(\mathfrak{b}_{11}, \mathfrak{b}_{12}, \ldots, \mathfrak{b}_{1d}, \mathfrak{b}_{21}, \ldots, \mathfrak{b}_{nd})$ *and matrix*

$$\begin{pmatrix} a_{11}g_{11} & a_{12}g_{11} & \ldots & a_{1n}g_{11} & a_{21}g_{12} & \ldots & a_{nd}g_{1n} \\ a_{11}g_{21} & a_{12}g_{21} & \ldots & a_{1n}g_{21} & a_{21}g_{22} & \ldots & a_{nd}g_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{11}g_{n1} & a_{12}g_{n1} & \ldots & a_{1n}g_{n1} & a_{21}g_{n2} & \ldots & a_{nd}g_{nn} \end{pmatrix},$$

where each $a_{ij}g_{\ell m}$ *is understood as a column vector in* k^d *representing an element of* K *in the usual fixed basis.*

Now, if $g' = (\mathfrak{a}', g'_{fi}, g'_\infty)$ *is a matrix pair over* K*, we may define*

$$\mathrm{Rest}(g') = (\mathfrak{a}, g_{fi}, g_\infty),$$

where $(\mathfrak{a}, g_{fi}) = \mathrm{Rest}((\mathfrak{a}', g'_{fi}))$*, and likewise* $g_\infty = \mathrm{Rest}(g'_\infty)$*, where it is understood that all coefficient ideals of* g'_∞ *are equal to* A'_∞*, which admits a basis over* $\mathcal{O}_\infty$*.*

Theorem 5.2.12. *Let* g *be a matrix pair over* k*. Then,*

$$\mathrm{CoN}(\mathrm{LP}(g)) = \mathrm{LP}(\mathrm{CoN}(g)).$$

Let g' *be a matrix pair over* K*. Then,*

$$\mathrm{Rest}(\mathrm{LP}(g')) = \mathrm{LP}(\mathrm{Rest}(g')).$$

Proof. The first claim is straightforward. For the second one, the definition of the matrix pair $\mathrm{Rest}(g')$ is simply an explicit writing of pseudo-bases of lattices L'_{fi} and L'_∞ in K^n identified with k^{dn}. □

This last theorem allows us to construct traces of vector bundles as defined in Section 5.1.5, but also to express the restriction to $F(x)$ of a lattice pair, which will be a vital tool in the computation of global sections.

Example 5.2.13. We compute the restriction $\mathrm{Rest}(L)$ over $F(x)$ of the lattice pair L from Example 5.2.8. A basis of $\mathcal{O}_{fi}$ over $F[x]$ is $(1, y)$, a $F[x]$-basis of $\mathfrak{p}^{-1}$ is $(1, \frac{y}{x})$ and a basis of $\mathcal{O}_\infty$ over the valuation ring at infinity of $F(x)$ is $(1, \pi) = (1, \frac{y}{x^2})$. It follows that $\mathrm{Rest}(L) = \big(\mathfrak{a}, g_{fi}, g_\infty\big)$, with

$$\mathfrak{a} = (F[x], F[x], F[x], F[x]),$$

$$g_{fi} = \begin{pmatrix} \frac{x^2}{x^2+4} & 0 & 0 & 0 \\ 0 & \frac{x^2}{x^2+4} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{1}{x} \end{pmatrix},$$

and

$$g_\infty = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & \frac{1}{x^2} & \frac{-x}{x^2-1} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{1}{x^2} \end{pmatrix}.$$

5.2.3 Computing cohomology groups and extensions

If L is a lattice pair, we define $H^i(L)$ as $H^i(L_R)$ for $i \in \{0, 1\}$. Given a matrix pair g, we aim to compute F-bases for the spaces $H^0(\mathrm{LP}(g))$ and $H^1(\mathrm{LP}(g))$.

Computing global sections of a lattice pair

The computation of $H^0(L)$ relies on the following simple observation:

Lemma 5.2.14. *Let $L = (L_{fi}, L_\infty)$ be a lattice pair. Then $H^0(L) = L_{fi} \cap L_\infty$.*

Proof. This lemma is clear using Remark 5.1.4. □

We first assume that $k = F(x)$. In this case, note that $\mathcal{O}_{fi} = F[x]$ is a PID and every projective $\mathcal{O}_{fi}$-module is free. Therefore, we omit the tuple of ideals $\mathfrak{a}$ in every matrix pair and assume that all ideals involved are equal to $\mathcal{O}_{fi}$. Then, the computation of the intersection $L_{fi} \cap L_\infty$ reduces to matrix reduction as discussed in Section 2.2.2. The method discussed here is adapted from [46, Lemma 25] and [45].

Let (g_{fi}, g_∞) be a matrix pair of k of rank n. Then, the matrix pair $g' = (g_\infty^{-1} g_{fi}, I_r)$ represents an isomorphic lattice pair, and $H^0(\mathrm{LP}(g)) = g_\infty \left(H^0(\mathrm{LP}(g'))\right)$. Upon applying the global isomorphism g_∞^{-1}, we may assume without loss of generality that g_∞ is the identity matrix.

Then, a vector $v \in k^n$ lies in L_∞ if and only it $|v| \leq 0$ (see Definition 2.2.1). Assume that $e_1, \ldots, e_r$ is a reduced basis of L_{fi}, in the sense that the matrix $\begin{pmatrix} e_1 & \ldots & e_r \end{pmatrix}$ is reduced. Then, by Proposition 2.2.3, $\sum_{i=1}^r a_i e_i \in L_\infty$ if and only if $\deg(a_i) \leq -|e_i|$ for all $1 \leq i \leq r$. Since $\sum_{i=1}^r a_i e_i \in L_{fi}$ if and only if $a_i \in F[x]$ for all $1 \leq i \leq r$, a basis of $H^0(\mathrm{LP}(g))$ is

$$(x^j e_i)_{\substack{1 \leq i \leq r \\ 0 \leq j \leq -|e_i|}}.$$

We write this algorithm as Algorithm 3 for the reader's convenience.

Theorem 5.2.15. *If $k = F(x)$, Algorithm 3 outputs a F-basis of $H^0(\mathrm{LP}(g))$. If F is a finite field, then Algorithm 3 runs in polynomial time.*

Input: a matrix pair $g = (g_{fi}, g_\infty)$ over F(X)
Output: A F-basis of $H^0(\mathrm{LP}(g))$
1 Set $M = (g_\infty)^{-1} g_{fi}$;
2 Compute $d \in F[x]$ such that $dM \in M_n(F[x])$;
3 Compute a reduced basis $\mathcal{B} = (b_1, \ldots, b_n)$ of the $F[x]$-lattice generated by the columns of dM;
4 **return** $\left\{ \frac{x^j}{d} g_\infty(b_i) : 1 \leq i \leq n \text{ and } 0 \leq j \leq \deg(d) - |b_i| \right\}$;

Algorithm 3: Computing the global sections of a lattice pair over $\mathbb{P}^1_F$.

Proof. The correctness of Algorithm 3 has already been discussed above. Since there exist efficient algorithms for computing a reduced basis (see Section 2.2.2), and since the size of the output is at most $n(\deg(d) + 1)$, the algorithm runs in polynomial time. □

Corollary 5.2.16. *For a general separable extension $k/F(x)$ of degree d and a matrix pair g, a basis of $H^0(\mathrm{LP}(g))$ may be computed in polynomial time.*

Proof. First, compute $H^0(\mathrm{Rest}(\mathrm{LP}(g)))$ using Algorithm 3. Then, applying Proposition 5.1.22, a basis of $H^0(\mathrm{Rest}(\mathrm{LP}(g)))$ is a basis of $H^0(\mathrm{LP}(g))$ upon the identification $k^n = F(x)^{nd}$. A representation of the vectors of the basis in k^n may be computed using the basis $1, y, \ldots, y^{d-1}$. □

Remark 5.2.17. In Algorithm 3, we may compute the Popov normalised form of the matrix M instead of a mere reduced equivalent matrix if we want the algorithm to output a more predictable basis of $H^0(\mathrm{LP}(g))$.

Example 5.2.18. We gather again notations from Examples 5.2.8 and 5.2.13. Compute

$$M \coloneqq g_\infty^{-1} g_{fi} = \begin{pmatrix} \frac{x^2}{x^2+4} & 0 & 0 & 0 \\ 0 & \frac{x^4}{x^2+4} & 0 & 0 \\ 0 & \frac{x^3}{x^2-1} & 1 & 0 \\ x & 0 & 0 & x \end{pmatrix}.$$

We compute the Popov form of its numerator and obtain the reduced form

$$M' = \begin{pmatrix} \frac{x^2}{x^2+4} & 0 & 0 & \frac{4x}{x^2+4} \\ 0 & \frac{x^3}{x^2-1} & \frac{2x^4}{x^4+3x^2+3} & 0 \\ 0 & 1 & -x & 0 \\ 0 & 0 & 0 & x \end{pmatrix}.$$

It follows that a basis of $H^0(\mathrm{Rest}(L))$ is

$$g_\infty \begin{pmatrix} \frac{x^2}{x^2+4} \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{x^2}{x^2+4} \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Therefore, a basis of $H^0(L)$ is

$$\begin{pmatrix} \frac{x^2}{x^2+4} \\ 0 \end{pmatrix}.$$

We also observe that given an element $f \in H^0(L)$ for some lattice pair L, we may compute the coordinates of f in terms of a given basis of $H^0(L)$ (for instance the one computed by the algorithm of Corollary 5.2.16).

Lemma 5.2.19. *Let L be a lattice pair of rank n and let $f \in H^0(L) \subset k^n$. Let $m_1, \dots, m_s$ be a F-basis of $H^0(L)$. We may compute in polynomial time a vector $a \in F^s$ such that $f = \sum_{i=1^s} a_i m_i$.*

Proof. Fix a place P of k and a local uniformiser π_P at P. For any element $\alpha \in k$ and $i \in \mathbb{Z}$, we write $\alpha^{(i)}$ for the coefficient of degree i of α written as a formal series in the variable π_P. For each $1 \leq i \leq n, 1 \leq j \leq s$, let m_{ij} be the ith component of m_j. We write $v_i = \min_{1 \leq j \leq s} \mathrm{ord}_P(m_{ij})$ (if all the m_{ij} are zero, simply set $v_i = 0$). Then, for any $\ell \in \mathbb{N}$ we define the map

$$\begin{array}{rccc} \varphi_{P,\ell}\colon & k^n & \to & F^{n\ell} \\ & f & \mapsto & (f_i^{(v_i+j)})_{\substack{1 \leq i \leq r \\ 0 \leq j \leq \ell-1}}. \end{array}$$

Now, consider the matrix $N_{P,\ell}$ of size $n\ell \times s$ whose columns are the $\varphi_{P,\ell}(m_j)$. The matrix $N_{P,\ell}$ has rank s if and only if the restriction of $\varphi_{P,\ell}$ to $H^0(L)$ is injective and in this case, the coordinates of an element $f \in H^0(L)$ with respect to basis $m_1, \dots, m_s$ may be computed as a vector $a \in F^s$ such that $N_{P,\ell} a = \varphi_{P,\ell}(f)$.

All that is left is to prove that the restriction of $\varphi_{P,\ell}$ to $H^0(L)$ is injective for some ℓ bounded by a polynomial in the size of the input. Let $f = \sum_{i=j}^s a_j m_j \in H^0(L)$. Then, for $i \in [r]$, if $f_i \neq 0$ then $\mathrm{ht}(f_i) \leq \sum_{j=1}^s \mathrm{ht}(m_{ij})$, and thus $\mathrm{ord}_P(f_i) \leq \sum_{j=1}^s \mathrm{ht}(m_{ij})$. It follows that if $\ell > \max_{1 \leq i \leq n} v_i + \sum_{j=1}^s \mathrm{ht}(m_{ij})$, the map $\varphi_{P,\ell}$ is injective over $H^0(L)$. Since v_i is itself bounded by $\max_{1 \leq j \leq s} \mathrm{ht}(m_{ij})$, ℓ may indeed be chosen of polynomial size in the input. □

Computing the group H^1

By Serre duality, computing the group $H^1(L)$ for a lattice pair L can be done by computing the F-vector space $H^0(\iota(\omega)^{-1}L^\vee)$ for some differential ω. However, for applications such as computing extensions of vector bundles, it is desirable to be able to find an element of R^n representing a given element of $H^1(L)$.

Our strategy will be to adapt the linearisation technique introduced in Lemma 5.2.19 to turn the inversion of the Serre duality map into a linear equation.

Fix $Q_0 \in M^\infty$, and a local uniformiser π_{Q_0} such that $\mathrm{ord}_Q(\pi_{Q_0}) = 0$ for $Q \in M^\infty \setminus \{Q_0\}$ (it may be computed by solving an instance of the Chinese Remainder Problem). Let κ_0 be the residue field of Q_0 and let $\omega = d(\pi_{Q_0})$. For any integer ℓ, we write $\lceil \ell \rceil_0$ for the smallest power of $|\kappa_0|$ larger or equal to ℓ. That is, $\lceil \ell \rceil_0 = |\kappa_0|^{\lceil \log(\ell)/\log(|\kappa_0|) \rceil}$.

We present Algorithm 4 which, given a basis of $H^0(\iota(\omega)^{-1}L^\vee)$ of size s and a linear form represented in this basis by a row vector $\varphi \in F^s$, outputs a vector $v \in k^n$ such that the infinite répartition vector v_∞ satisfies $\theta_\omega(\cdot, v_\infty) = \varphi$.

Input: A matrix pair $g = (\mathfrak{a}, g_{fi}, g_\infty)$ over X
Input: A matrix $M = (m_{i,j}) \in M_{n,s}(k)$ whose columns are a F-basis of $H^0(\iota(\omega)^{-1}L^\vee)$
Input: A row vector $\varphi \in M_{1,s}(F)$ representing a linear form on $H^0(\iota(\omega)^{-1}L^\vee)$ written in the basis given by M
Output: $a \in k^n$ such that the linear form represented by f is $\theta_\omega(\cdot, a_\infty)$

1 For $i \in [r]$ and $Q \in X_\infty$, set $v_i^Q = \min_{j \in [s]} \left(\mathrm{ord}_Q(m_{i,j})\right)$;
2 Compute the matrix $N_{Q_0,\ell}$ (see Lemma 5.2.19) for increasing values of ℓ until it has rank s;
3 Let $x = \begin{pmatrix} x_1 & \dots & x_{n\ell} \end{pmatrix} \in M_{1,n\ell}(\kappa_0)$ such that $\mathrm{Tr}_{\kappa_0/F}(xN_{Q_0,\ell}) = \varphi$;
4 Let $\widetilde{x} = \begin{pmatrix} \widetilde{x}_1 & \dots & \widetilde{x}_{r\ell} \end{pmatrix} \in M_{1,n\ell}(\mathcal{O}_{Q_0})$ be a lift of x in $M_{1,n\ell}(\mathcal{O}_{Q_0})$ such that $\mathrm{ord}_Q(\widetilde{x}_i) \geq 1$ for all $i \in [r\ell]$ and $Q \in M^\infty \setminus \{Q_0\}$;
5 Let $\pi \in k$ such that $\lceil \ell \rceil_0 \mathrm{ord}_Q(\pi) \geq \max_{i \in [r]} -v_i^Q$ for all $Q \in X_\infty \setminus \{Q_0\}$ and $\mathrm{ord}_{Q_0}(\pi - 1) \geq 1$;
6 **return** $\left(\pi^{\lceil \ell \rceil_0} \pi_{Q_0}^{-v_i^{Q_0}-1} \sum_{j=0}^{\ell-1} \pi_{Q_0}^{-j} \widetilde{x}_{(i-1)\ell+j+1}^{\lceil \ell \rceil_0} \right)_{1 \leq i \leq r}$

Algorithm 4: Representing elements of $H^1(L)$

Theorem 5.2.20. *Algorithm 4 is correct and terminates after a polynomial amount of arithmetic operations in F.*

Proof. First, observe that Algorithm 4 terminates in polynomial time: each line of the algorithm corresponds either to linear algebra over F or to a task discussed in Section 2.2.

We prove that the output of the algorithm is correct. Set $c = (c_1, \ldots, c_n)$ as the coordinates of the output and $\begin{pmatrix}\varphi_1 & \ldots & \varphi_s\end{pmatrix} = \varphi$. If M_j is the vector given as the j-th column of M, we claim that $\theta_\omega(M_j, c_\infty) = \varphi_j$.

Now, $\theta_\omega(M_j, c_\infty) = \sum_{i=1}^{n} \sum_{Q \in X_\infty} \operatorname{res}_{\pi_Q}(m_{i,j} c_i \omega)$. And the result will follow from the identity $xN_{Q_0,\ell} = \varphi$ if we prove that for $i \in [r]$ and j *ins*, setting

$$\mu_{ij} = \left(\pi^{\lceil \ell \rceil_0} \pi_{Q_0}^{-v_i^{Q_0}-1} \left(\sum_{\alpha=0}^{\ell-1} \pi_{Q_0}^{-\alpha} \widetilde{x}_{(i-1)\ell+\alpha+1}^{\lceil \ell \rceil_0} \right) m_{i,j} \omega \right),$$

we have

$$\mu_{ij}^{(-1)} = \sum_{\alpha=0}^{\ell-1} x_{(i-1)\ell+\alpha+1} m_{i,j}^{(-v_i^{Q_0}+\alpha)}$$

and $\operatorname{ord}_Q(\mu_{ij}) \geq 0$ for $Q \in M^\infty \setminus \{Q_0\}$ where, for any $a \in k$ and integer n, $a^{(n)}$ is the coefficient of degree n in the expansion of a as a formal series in variable π_{Q_0}. We fix $i \in [r]$ and $j \in [s]$.

Let $Q \in M^\infty \setminus \{Q_0\}$. By construction, $\operatorname{ord}_Q(\pi^{\lceil \ell \rceil_0}) \geq \max(-v_i^Q)$ and it follows readily that $\operatorname{ord}_Q(\mu_{ij}) \geq 0$ since $\operatorname{ord}_Q(\pi_{Q_0}) = 0$ and $\widetilde{x}_m \in \mathcal{O}_Q$ for all $m \in [rn]$.

Now, we have the following:

$$\pi^{\lceil \ell \rceil_0} = 1 + O(\pi_{Q_0}^\ell)$$

and

$$\widetilde{x}_i^{\lceil \ell \rceil_0} = x_i + O(\pi_{Q_0}^\ell).$$

Then, we get

$$\mu_{i,j} = \left(\sum_{\alpha=0}^{\ell-1} x_{(i-1)\ell+\alpha+1} m_{i,j}^{(-v_i^{Q_0}+\alpha)} \right) \pi_{Q_0}^{-1} + O(1).$$

□

Corollary 5.2.21. *There exists a polynomial algorithm which, given matrix pairs g' and g'', as well as a row vector φ representing a F-linear form over*

$$H^0\left(\iota(\omega)^{-1} \mathcal{H}om(g', g'')\right),$$

returns the corresponding extension of $\mathrm{LP}(g'')$ *by* $\mathrm{LP}(g')$.

Proof. Let n', n'' be the respective ranks of g' and g''. Using Algorithm 4, one may compute $\kappa \in k^{n' \times n''}$ such that the infinite répartition matrix κ represents the element of $H^1\left(\mathcal{H}om(R(g''), R(g'))\right) = \mathrm{Ext}^1\left(R(g''), R(g')\right)$ corresponding to φ.

Then, adapting Theorem 5.1.19, the corresponding extension is given by the matrix pair $(\mathfrak{a}, g_{fi}, g_\infty)$ with

$$\mathfrak{b} = (\mathfrak{a}'_1, \ldots, \mathfrak{a}'_n, \mathfrak{a}''_1, \ldots, \mathfrak{a}''_{n'}),$$

$$g_{fi} = \begin{pmatrix} g'_{fi} & (0) \\ (0) & g''_{fi} \end{pmatrix},$$

and

$$g_\infty = \begin{pmatrix} g'_\infty & -\kappa g''_\infty \\ (0) & g''_\infty \end{pmatrix}.$$

□

Example 5.2.22. Let L be again as in Examples 5.2.8, 5.2.13 and 5.2.18 Since $\deg(L) = 1$, we get $H^1(L) = 0$. Instead, we compute $H^1(L^\vee)$. We let $\omega = d\pi$. Since the field k has genus 1, the differential ω has a principal divisor. It is the divisor of $\frac{x^2+3}{x^2}$, and we may represent $\iota(\omega)^{-1}$ by the following matrix pair of size 1:

$$\left(\mathcal{O}_{fi}, \frac{x^2}{x^2+3}, 1\right).$$

Now, $H^1(L^\vee) = H^0(\iota(\omega)^{-1}L)$. Applying Algorithm 3, we compute a basis for the F-vector space $H^0(\iota(\omega)^{-1}L)$. We find that it has dimension 1 and is generated by

$$v := \begin{pmatrix} \frac{x^4}{x^4+5} \\ 0 \end{pmatrix}.$$

Since k has only one place at infinity and $[H^0(\iota(\omega)^{-1}L)) : F] = 1$, applying Algorithm 4 is straightorward: as $\frac{x^4}{x^4+5} = 1 + O(\pi^8)$,

$$\mathrm{res}_\infty\left(v, \begin{pmatrix} \pi^{-1} \\ 0 \end{pmatrix}\right) = 1.$$

Then, the element of $H^1(L^\vee)$ dual to v is represented by the infinite répartition vector $\begin{pmatrix} \pi_\infty^{-1} \\ 0 \end{pmatrix}$.

5.2.4 Computing isomorphisms between lattice pairs

We want to decide whether two lattice pairs are isomorphic and, if they are, find an isomorphism. We first give a probabilistic algorithm of the Monte-Carlo type for this task when the field F is large enough and a deterministic algorithm for a weakening of the problem (the lattice pairs are assumed indecomposable) when F is any finite field. Then, a general solution will be given in Section 5.2.5.

Theorem 5.2.23. *Let L, L' be lattice pairs such that*

$$[\mathrm{End}(L) : F] = [\mathrm{Hom}(L, L') : F] = [\mathrm{Hom}(L', L) : F].$$

Let s be the dimension of these spaces and we assume that $|F| > s$. There is a polynomial Monte-Carlo algorithm which outputs an isomorphism $\varphi\colon L \to L'$ if it exists, with probability at least $1 - s/|S|$, where S is a subset of F in which we can sample random elements.

Proof. First, observe that we may compute $\mathrm{End}(L), \mathrm{End}(L')$ and $\mathrm{Hom}(L, L')$ by applying Corollary 5.2.16 to the lattice pairs $L^\vee \otimes L$, $L^\vee \otimes L'$ and $(L')^\vee \otimes L$. Their elements are represented as matrices in $M_n(k)$ (n the rank of L and L'), and the matrix product gives a bilinear map from $\mathrm{Hom}(L, L') \times \mathrm{Hom}(L', L)$ to $\mathrm{End}(L)$. This, together with a fixed choice of bases of $\mathrm{Hom}(L', L)$ and $\mathrm{End}(L)$ gives a map $\alpha\colon \mathrm{Hom}(L, L') \to M_s(F)$. Observe that $f \in \mathrm{Hom}(L, L')$ is an isomorphism if and only if $\alpha(f)$ is an invertible matrix. That is, if and only if $\det(\alpha(f)) = 0$.

Now, setting $f = \sum_{i=1}^{s} a_i m_i$, where (m_i) is a basis of $\mathrm{Hom}(L, L')$, we see that $\det(\alpha(f))$ is a homogeneous polynomial of degree s in the a_i. By the Schwartz-Zippel lemma, if $S \subset F$ is a subset of size at least $s + 1$, the probability that a uniform random element of $\bigoplus_{j=1}^{s} Sm_j$ is an isomorphism is at least $1 - s/|S|$. Therefore, sampling a random element of $\mathrm{Hom}(L, L')$ is a valid algorithm. □

When F is a finite field, the approach of Theorem 5.2.23 does not work if s is too large, as the Schwartz-Zippel lemma fails. For now, we only give an algorithm for the case that L is an indecomposable lattice pair. This algorithm will be used as a subroutine in Algorithm 6, which will then be used to compute isomorphisms in the general case (see Corollary 5.2.30).

Lemma 5.2.24. *Assume that F is a finite field. Then Algorithm 5 is correct and runs in polynomial time.*

Input: Matrix pairs g and g' of rank n such that $\mathrm{LP}(g)$ is indecomposable

Output: A matrix $T \in M_n(k)$ giving an isomorphism from $\mathrm{LP}(g)$ to $\mathrm{LP}(g')$ if $\mathrm{LP}(g) \simeq \mathrm{LP}(g')$, and $\perp$ otherwise

Compute structure constants for the F-algebra $A = \mathrm{End}(\mathrm{LP}(g \oplus g'))$;

Compute sub-algebras S and R such that $A = S \oplus R$, S is semi-simple, and R is the Jacobson radical of A;

if *S is not simple* **then**

  return $\perp$

end

Compute $s \in \mathbb{N}$, a finite extension F'/F, and an isomorphism $\varphi\colon S \simeq M_s(F')$;

if $s \neq 2$ **then**

  return $\perp$;

end

Compute $P \in GL_{2s}(F')$ such that $P\varphi(\mathrm{Id}_{\mathrm{LP}(g)})P^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $P\varphi(Id_{\mathrm{LP}(g')})P^{-1} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$;

return $\varphi^{-1}\left(P^{-1}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}P\right)$

Algorithm 5: Computing isomorphisms between quasi-indecomposable lattice pairs over finite fields

Proof. We first discuss the algorithm line by line, proving that the task may be executed in polynomial time.

Line 1: A basis of $\mathrm{End}(\mathrm{LP}(g \oplus g'))$ may be computed using Corollary 5.2.16. Then, the structure constants may be computed using Lemma 5.2.19.

Line 2: The Jacobson radical of A may be computed using Item 1 of Proposition 3.1.7 and a basis of S may be computed using Item 2.

Line 3: Checking that S is simple can be done by checking if the centre of S is a field. See Item 6 of Proposition 3.1.5

Line 6: This may be done using Item 4 of Proposition 3.1.7. Note that since a finite field has a trivial Brauer group, a simple F-algebra is always of the form $M_{n_i}(F')$, where F' is a finite extension of F, and F' is then the centre of this algebra.

Line 10: Observe that the matrices $\varphi(Id_{\mathrm{LP}(g)})$ and $\varphi(Id_{\mathrm{LP}(g')})$ are two orthogonal idempotents of rank 1 which sum to I_2. They can be simultaneously diagonalised as demanded by computing generators of their respective images.

We now prove that the algorithm is correct. First, since $\mathrm{LP}(g)$ is indecomposable, by Proposition 5.1.26 we have $D(\mathrm{LP}(g) \oplus \mathrm{LP}(g')) \simeq M_2(F')$ for some finite extension F'/F if and only if $\mathrm{LP}(g') \simeq \mathrm{LP}(g)$. Hence, our two tests do detect correctly whether $\mathrm{LP}(g) \simeq \mathrm{LP}(g')$.

Assume that $\mathrm{LP}(g) \simeq \mathrm{LP}(g')$. Then, after conjugating by matrix P as in Line 10, φ gives an isomorphism from S to the straightforward representation of $D(\mathrm{LP}(g) \oplus \mathrm{LP}(g'))$. Then, the matrix we return corresponds to an isomorphism from $\mathrm{LP}(g)$ to $\mathrm{LP}(g')$. □

5.2.5 Algorithms for homomorphisms of lattice pairs

This section presents algorithms related to homomorphisms of lattice pairs. All the algorithms we present rely on the computation of a pseudo-Hermite normal form of matrices with coefficients in $\mathcal{O}_{fi}$ and $\mathcal{O}_\infty$. They are, therefore, only polynomial-time if Conjecture 2.2.12 is assumed.

We first give algorithms to compute kernels and images of homomorphisms of lattice pairs. Since a lattice pair is normally composed of $\mathcal{O}_{fi}$ and $\mathcal{O}_\infty$-submodules of k^n of full rank, we are not able to give a set-theoretical definition

of subobjects, such as kernels and images. Instead, we turn to a more categorical approach:

Definition 5.2.25. *Let L, L' be lattice pairs of respective ranks n and n', and consider a homomorphism $f\colon k^n \to k^{n'}$ from L to L' (that is, $f(L_{fi}) \subset L'_{fi}$ and $f(L_\infty) \subset L'_\infty$).*

1. *An image of f is a pair (I, ι), where I is a lattice pair of rank $n_i = \operatorname{rank}(f)$ and $\iota\colon k^{n_i} \to k^{n'}$ is an injective linear map such that $\iota(I_{fi}) = f(L_{fi})$ and $\iota(I_\infty) = f(L_\infty)$.*

2. *A kernel of f is a pair (κ, ι) such that κ is a lattice pair of rank $n_\kappa = n - \operatorname{rank}(f)$ and $\iota\colon k^{n_\kappa} \to n^r$ is an injective linear map such that $\iota(\kappa_{fi}) = \operatorname{Ker} f \cap L_{fi}$ and $\iota(\kappa_\infty) = \operatorname{Ker} f \cap L_\infty$.*

We observe that our definitions match the definitions of kernels and images in the Abelian category of lattice pairs and that kernels and images are unique up to isomorphism. To compute such images and kernels, we adopt a similar strategy: compute the set-theoretical kernel and image and then use Theorem 5.2.26 below to compute a kernel and image as defined in Definition 5.2.25.

Theorem 5.2.26. *Let L be a lattice pair of rank n, let S_{fi} be a submodule of L_{fi} of rank $m \leq n$ and let S_∞ be a submodule of L_∞ also of rank m. We further assume that $kS_{fi} = kS_\infty$. Then we may compute in polynomial time a lattice pair L' of rank m and a map $f\colon L' \to L$ such that $f(L'_{fi}) = S_{fi}$ and $f(L'_\infty) = S_\infty$.*

Proof. Assume that the modules S_{fi} and S_∞ are respectively given as the images of a pseudo-matrix $(\mathfrak{a}, C_{fi})$ of size $n \times m$ and of a matrix C_∞ of the same size. Then, a matrix pair $(\mathfrak{b}, g_{fi}, g_\infty)$ of size m and a matrix $C \in M_{n,m}(k)$ will be a solution to the problem if

$$\mathfrak{b} = \mathfrak{a},$$

$$C_{fi} = Cg_{fi},$$

and

$$C_\infty = Cg_\infty.$$

We set $g_\infty = I_n$, so the problem becomes

$$C_{fi} = C_\infty g_{fi}.$$

However, since the matrices C_{fi} and C_∞ both have rank m and have equal images (as k-linear maps), there exists a matrix $g_{fi} \in GL_m(k)$ such that $C_{fi} = C_\infty g_{fi}$ and it may be computed in polynomial time by solving a system of linear equations. □

Corollary 5.2.27. *Given an oracle for Problem 2.2.11, there is an algorithm which computes the image of a homomorphism of lattice pairs in polynomial time.*

Proof. Let L, L' be lattice pairs of respective ranks n and n' and let $g = (\mathfrak{a}, g_{fi}, g_\infty)$ be a matrix pair representing L. Let $f\colon L \to L'$ be a homomorphism represented by a matrix $C \in M_{n',n}(k)$. Now, $f(L_{fi})$ is the image of the pseudo-matrix $(\mathfrak{a}, Cg_{fi})$ and $f(L_\infty)$ is $Cg_\infty \mathcal{O}_\infty^n$. By Proposition 2.2.10 (2), a pseudo-matrix of full rank spanning $f(L_{fi})$ and a matrix of full rank spanning $f(L_\infty)$ may be computed in polynomial time from the Hermite normal forms of pseudo-matrix $(\mathfrak{a}, Cg_{fi})$ over $\mathcal{O}_{fi}$ and matrix Cg_∞ over $\mathcal{O}_\infty$. Then, an image of f may be computed using Theorem 5.2.26. □

Corollary 5.2.28. *Given an oracle for Problem 2.2.11, there is an algorithm which computes the kernel of a homomorphism of lattice pairs in polynomial time.*

Proof. The proof is similar to that of Corollary 5.2.27. □

Finally, we may compute a splitting of a lattice pair.

Theorem 5.2.29. *Given an oracle for Problem 2.2.11, Algorithm 6 gives a correct output in polynomial time.*

Proof. First, we prove that every step of the algorithm makes sense and may be done in polynomial time.

Lines 1 to 4 and 6: This was already discussed in the proof of Lemma 5.2.24.

Line 8: can be done using Corollary 5.2.27.

Line 9: may be done using Algorithm 5.

Finally, the number t of loop iterations is bounded by r, the rank of g.

Now, we prove that the output of Algorithm 6 is correct. First, we prove that $L \coloneqq \mathrm{LP}(g)$ is indeed isomorphic to $\bigoplus \mathrm{LP}(g_{i1})^{n_i}$. By Proposition 5.1.26,

$$\mathrm{End}(L) = \bigoplus M_{n_i}(D(\mathrm{End}(L_i))) \oplus J(\mathrm{End}(L)),$$

Input: A matrix pair g of rank n

Output: Matrix pairs $g_1, \ldots, g_s$, integers $n_1, \ldots, n_s$ and a matrix $C \in M_n(k)$ such that the $\mathrm{LP}(g_i)$ are indecomposable lattice pairs and C gives an isomorphism $\bigoplus_{i=1}^{s} \mathrm{LP}(g_i)_i^n \simeq \mathrm{LP}(g)$

Compute structure constants for the F-algebra $A = \mathrm{End}(\mathrm{LP}(g))$;
Compute a Wedderburn-Malcev complement $D(A)$;
Compute simple algebras $(S_i)_{i\in[t]}$ such that $D(A) \simeq \bigoplus_{i\in[t]} S_i$;
Compute the projection maps $p_i \colon D(A) \to S_i$;
for $i \in [t]$ **do**
    Compute $n_i \in \mathbb{N}$, a finite extension F_i of F and an isomorphism $\varphi_i \colon S_i \to M_{n_i}(F_i)$;
    Set $e_{ij} = (\varphi_i \circ p_i)^{-1}(\mathrm{Diag}(0, \ldots, 1, 0, \ldots, 0))$, with the nonzero coefficient in j-th position, for $j \in [n_i]$;
    Compute images (g_{ij}, A_{ij}) of the endomorphisms e_{ij} of $\mathrm{LP}(g)$;
    Compute isomorphisms $B_{ij} \colon \mathrm{LP}(g_{i1}) \to \mathrm{LP}(g_{ij})$;
end
Compute the matrix C defined as the horizontal joint of the matrices $A_{ij}B_{ij}$ as $i \in [t]$ and $j \in [n_i]$ are enumerated in lexicographic order;
return $((g_1, \ldots, g_s), (n_1, \ldots, n_s), C)$

Algorithm 6: Splitting a lattice pair

the S_i are the $M_{n_i}(D(\mathrm{End}(L_i))) \simeq M_{n_i}(F_i)$ (up to reordering) and up to an automorphism of L, the elements e_{ij} are the projections on a factor L_i of L. An image of e_{ij} is a vector bundle $\widetilde{L}_{ij}$ isomorphic with L_i. It follows that $L \simeq \bigoplus \mathrm{LP}(g_{i0})^{n_i}$.

Then, it is easy to see that by construction, T gives an isomorphism as desired. □

Corollary 5.2.30. *If F is finite and given an oracle for Problem 2.2.11, there is an algorithm for deciding whether lattice pairs are isomorphic and, if so, computing an isomorphism.*

Proof. We may compute splittings for L and L' using Algorithm 6. Then, it is only a matter of checking that their indecomposable components are isomorphic (up to reordering) and appear with equal power. This condition may be checked by repeated use of Algorithm 5. □

5.3 Applications

5.3.1 Maximal orders and the explicit isomorphism problem

As discussed in Section 1.2, the methods of [46] admit a geometric interpretation. For F a finite field, let $k = F(X)$ and let $X = \mathbb{P}^1_F$. Maximal orders in a K-algebra A isomorphic to $M_d(K)$ for some $d \in \mathbb{N}$ represent sheaves of endomorphisms of a vector bundle over X. Since every vector bundle over X splits into a direct sum of line bundles, one may easily find an endomorphism of rank one. Here, we discuss this interpretation in detail and provide some explicit examples.

In general, let k be a global function field and let B be a K-algebra of dimension $n \in \mathbb{N}$. We fix a basis $(e_1, \ldots, e_n)$ of B, so that B is identified with K^n as a vector space. We let $\pi_B \colon K^n \times K^n \to K^n$ be the bilinear map corresponding to the multiplication on B via its identification with K^n. This bilinear map extends naturally to R^n by computing products pointwise.

We now give several equivalent definitions of orders, which rely on the equivalent categories from Definition 5.1.1.

Definition 5.3.1.

- *An $\mathcal{O}_X$-order of B is a coherent $\mathcal{O}_X$-algebra O such that its generic stalk O_η is isomorphic to B as a K-algebra.*
- *An* $\mathcal{O}_R$-order *of B is an $\mathcal{O}_R$-lattice of rank n which is stable by application of π_B.*

- *An* order pair *of B is a lattice pair O of rank n, where both O_{fi} and O_∞ are stable by π_B.*

In all cases, an order is said to be maximal if it is not contained in a strictly larger order.

Proposition 5.3.2. *Let $B = M_d(K)$ for some $d \in \mathbb{N}$, and let O be a maximal order pair in B. Then there exists a lattice pair L of rank d such that $O = \mathcal{E}nd(L)$.*

Proof. By [33, Theorem 11.3.17], as $\mathcal{O}_{fi}$ and $\mathcal{O}_\infty$ are both noetherian and integrally closed integral domains, there exist an $\mathcal{O}_{fi}$-lattice L_{fi} and an $\mathcal{O}_\infty$-lattice L_∞, both of rank d, such that $O_{fi} = \mathrm{End}_{\mathcal{O}_{fi}}(L_{fi})$ and $O_\infty = \mathrm{End}_{\mathcal{O}_\infty}(L_\infty)$. The lattice pair $L = (L_{fi}, L_\infty)$ is as required. □

Now, the pivotal argument in [46] is the point (ii) of its Theorem 21, which states that if k is a rational function field and O is as in Proposition 5.3.2, then $O_{fi} \cap O_\infty$ contains a rank one idempotent of B. As we shall argue, this is a direct consequence of the following result, often attributed to Grothendieck in the case that the base field is the field of complex numbers, and proved in [43] for a general base field.

Lemma 5.3.3. *Let F be a field, and let $X = \mathbb{P}^1_F$. Let E be a vector bundle over X of rank $n \in \mathbb{N}$. Then there is an isomorphism*

$$E \simeq \bigoplus_{i=1}^{r} L_i^{n_i},$$

where the L_i are pairwise non-isomorphic line bundles over X, and the n_i are positive integers such that $n_1 + \ldots + n_r = n$.

we may then prove the following restatement of [46, Theorem 21]

Proposition 5.3.4. *Assume that $k = F(X)$. If O and B are as in Proposition 5.3.2, then $H^0(O)$ is a F-algebra which contains some $e \in B$ (under the identificaton of B and K^{d^2} discussed above) which is idempotent of rank one.*

Proof. By Proposition 5.3.2, there exists a lattice pair L of rank d such that $O = \mathcal{E}nd(L)$, and in particular, $H^0(O) = \mathrm{End}(L)$ is a k-algebra. By a combination of Lemma 5.3.3 and Theorem 5.1.2, we have

$$L \simeq \bigoplus_{i=1}^{r} L_i^{n_i},$$

where the L_i are pairwise non-isomorphic lattice pairs of rank 1, and the n_i are positive integers which sum up to d. By Proposition 5.1.26, it follows that we have the following splitting of k-algebras

$$H^0(O) = \mathrm{End}(L) \simeq J \oplus \bigoplus M_{n_i}(k),$$

where J is the Jacobson radical of $H^0(O)$. Then, $e = \mathrm{Diag}(1, 0, \ldots, 0) \in M_{n_1}(k) \subset H^0(L)$ is the projection of L onto a sublattice pair of rank 1, and therefore corresponds to an idempotent of rank 1 in B. □

Remark 5.3.5. In this subsection, we recover the result from [46] on $F[X]$ lattices by applying a structural theorem on vector bundles over $\mathbb{P}^1_F$. A converse argument was published in [77], where a lattice-based proof of the splitting theorem for vector bundles is given.

5.3.2 Vector bundles on an elliptic curve

In [5], Atiyah systematically described the category of vector bundles on an elliptic curve over an algebraically closed field F. Let X be such an elliptic curve with function field k, and let $E(r, d)$ be the set of isomorphism classes of indecomposable $\mathcal{O}_R$-lattices of rank r and degree d over k. In what follows, we give a succinct summary of his construction, rephrased in our setting of $\mathcal{O}_R$-lattices, and then we give an explicit construction using lattice pairs.

Definition 5.3.6. *Let L be an A_R-lattice, let $s = [H^0(L) : F]$ and let ω be a differential of K. Observe that, by Proposition 5.1.18 and Serre duality,*

$$\mathrm{Ext}^1(L, R(\iota(\omega)^{-1})^s) = H^1(L^\vee \otimes R(\iota(\omega)^{-1})^s) \simeq H^0(A_R^s \otimes L)^\vee = H^0(L^s)^\vee.$$

Upon fixing a basis of $H^0(L)$, this extension group identifies with $\mathrm{End}_F(H^0(L))$. We define the Atiyah extension *of L as the extension*

$$0 \to R(\iota(\omega^{-s})) \to L' \to L \to 0$$

given by the identity automorphism of $H^0(L)$.

Proposition 5.3.7. *Let $r \in \mathbb{N}$. Then there exists a unique $F_r \in E(r, 0)$ such that $[H^0(X, F_r) : F] = 1$. For $L \in E(r, 0) \setminus \{F_r\}$, $[H^0(L) : F] = 0$.*

We let $\mathrm{Pic}^0(k)$ be the group of isomorphism class of $\mathcal{O}_R$-lattices of rank 1. We note that if k has a unique infinite places O of degree 1 with uniformiser π, the elements of $\mathrm{Pic}^0(k)$ are uniquely represented by $\mathcal{O}_R$ and the $\mathrm{LP}(\mathfrak{p}, 1, \pi^{-1})$, where $\mathfrak{p}$ varies over the prime ideals of $\mathcal{O}_{fi}$.

Proposition 5.3.8. *Let $r \in \mathbb{N}$ and $d \in \mathbb{Z}$. Fix a rank one $\mathcal{O}_R$-lattice L_1 of degree* 1.

- *F_1 is represented by $\mathcal{O}_R$.*
- *F_r is the Atiyah extension of F_{r-1}.*
- *The map $L \mapsto F_r \otimes L$ gives a bijection $\mathrm{Pic}^0(k) \to E(r, 0)$.*
- *Assume that $d > 0$, the Atiyah extension gives a bijection $E(r, d) \to E(r + d, d)$.*
- *The map $E \mapsto E \otimes L$ gives a bijection $E(r, d) \to E(r, d + r)$.*
- *The map $E \mapsto E^\vee$ gives a bijection $E(r, d) \to E(r, -d)$.*

Put together, these facts give explicit bijections $\mathrm{Pic}^0(X) \to E(r, d)$ for all $r \in \mathbb{N}$, $d \in \mathbb{Z}$. Furthermore, the works [3, 90] showed that these constructions are also valid on an arbitrary perfect field k if $E(r, d)$ now means the set of isomorphism classes of absolutely indecomposable vector bundles. Since an indecomposable vector bundle is always the trace of an absolutely indecomposable vector bundle defined over some finite extension of k, this yields an algorithm for constructing any indecomposable lattice pair over an elliptic curve over a perfect field.

We also note that a generalisation to curves of genus 1 with no rational points was given in [68].

Example 5.3.9. In this example we consider the fields $F = \mathbb{F}_7$ and $k = F(x, y)/(y^2 - x^3 - x)$. We construct the image of the line bundle $\mathcal{L}(\mathfrak{p} - \infty)$ in $E(3, 2)$, where $\mathfrak{p}$ is the divisor of the prime ideal $\langle x, y \rangle$ of $\mathcal{O}_{fi}$ and ∞ is the divisor of the unique prime ideal of $\mathcal{O}_\infty$. First, we set

$$L_0 = \mathrm{LP}(\mathfrak{p}^{-1}, 1, \pi).$$

Following the construction of the map $\mathrm{Pic}^0(X) \to E(3, 2)$, we must first tensor the lattice pair L_0 twice by a fixed lattice pair of degree 1. The result is a lattice pair lying in $E(1, 2)$. We shall then take its Atiyah extension to get an element of $E(3, 2)$.

We compute the tensor product $L_1 = L_0 \otimes L_\infty^{\otimes 2}$, where L_∞ represents the line bundle of degree 1 $\mathcal{L}(\infty)$. We get

$$L_1 = \mathrm{LP}(\mathfrak{p}^{-1}, 1, \pi^{-1}).$$

Since $\deg(L_1) = 2$ and k has genus 1, it follows by the Riemann-Roch theorem that $[H^0(L_1) : k] = 2$. Applying Algorithm 3, we find that a basis for $H^0(L_1)$ is $(1, x\pi)$.

Now, we let $\omega = d\pi$, and recall that this differential's divisor is the principal divisor corresponding to $h := \frac{x^2+3}{x^2}$, and so the corresponding lattice pair is

$$L_\omega = \mathrm{LP}\left((h), 1, 1\right).$$

We must now compute a répartition vector representing the element of $H^1(L_1^\vee \otimes L_\omega^s)$ corresponding to the identity automorphism of $H^0(L_1)$ as discussed in Definition 5.3.6. This H^1 group is the dual of the vector space $H^0(L_1 \otimes L_t^s)$ by Serre duality, where L_t is the trivial lattice pair:

$$L_t = \mathrm{LP}(A_{fi}, 1, 1).$$

Now, it is quite clear that a basis of $H^0(L_1 \otimes L_t^s)$ is $((1,0), (x\pi, 0), (0,1), (0, x\pi))$. The space $H^0(L_1 \otimes L_t^s)$ is identified with $\mathrm{End}_F(H^0(L_1))$ by mapping a vector (a, b) to the k-linear map sending 1 to a and $x\pi$ to b. Thus, we shall find a vector $(\alpha, \beta) \in K^2$ such that

$$\begin{cases} \mathrm{res}_\infty(\alpha_\infty) = \mathrm{res}_\infty(x\pi\beta_\infty) = 1 \\ \mathrm{res}_\infty(x\pi\alpha_\infty) = \mathrm{res}_\infty(\beta_\infty) = 0. \end{cases} \tag{5.2}$$

Observe that $x\pi = \pi^{-1} + O(\pi^3)$, so we may set $\alpha = \pi^{-1}$ and $\beta = 1$. We have shown that the Atiyah extension of L_1 is represented in $H^1(L_1^\vee \otimes L_\omega^s)$ by the répartition vector $\kappa = (\pi_\infty^{-1}, 1_\infty)$. By Theorem 5.1.19, it follows that the Atiyah extension of L_1 is the lattice pair

$$L = \mathrm{LP}\left(((h), (h), \mathfrak{p}^{-1}), I_3, \begin{pmatrix} 1 & 0 & -\pi^{-2} \\ 0 & 1 & -\pi^{-1} \\ 0 & 0 & \pi^{-1} \end{pmatrix}\right).$$

The determinant of L is

$$\det(L) = \mathrm{LP}\left(h^2\mathfrak{p}^{-1}, 1, \pi^{-1}\right).$$

Now, the divisor of ı has degree 1 and the finite part of the divisor of h has degree 0, so we find that $\deg(L) = 2$ as expected. By [5, Theorem 6], we should have

$$\det(L) \simeq L_1,$$

and indeed one observes readily that division by h^2 is such an isomorphism.

We will now check that the lattice pair L is indeed absolutely indecomposable. By Proposition 5.1.27, we need to check that $D(L) = \mathbb{F}_7$. In fact, since the rank and degree of L are coprime, we expect $\mathrm{End}(L) = \mathbb{F}_7$ by [65, Corollary 2.5]. We first compute $\mathcal{E}nd(L, L) = L^\vee \otimes L$. Using the formulas from Definition 5.2.5, we find:

$$\mathcal{E}nd(L) = \mathrm{LP}(\mathfrak{a}, I_3, g_\infty),$$

with

$$\mathfrak{a} = (A_{fi}, A_{fi}, (h\mathfrak{p})^{-1}, A_{fi}, A_{fi}, (h\mathfrak{p}^{-1}), h\mathfrak{p}, h\mathfrak{p}, A_{fi})$$

and

$$g_\infty = \left(\begin{pmatrix} 1 & 0 & -\pi^{-2} \\ 0 & 1 & -\pi^{-1} \\ 0 & 0 & \pi^{-1} \end{pmatrix}^t\right)^{-1} \otimes \begin{pmatrix} 1 & 0 & -\pi^{-2} \\ 0 & 1 & -\pi^{-1} \\ 0 & 0 & \pi^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & \frac{-x^3}{x^2+1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & \frac{-xy}{x^2+1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{xy}{x^2+1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & \frac{-x^3}{x^2+1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \frac{-xy}{x^2+1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{xy}{x^2+1} & 0 & 0 & 0 \\ \frac{xy}{x^2+1} & 0 & \frac{-x^4y}{(x^2+1)^2} & 1 & 0 & \frac{-x^3}{x^2+1} & \frac{y}{x^2} & 0 & \frac{-xy}{x^2+1} \\ 0 & \frac{xy}{x^2+1} & \frac{-x^3}{x^2+1} & 0 & 1 & \frac{-xy}{x^2+1} & 0 & \frac{y}{x^2} & -1 \\ 0 & 0 & \frac{x^3}{x^2+1} & 0 & 0 & \frac{xy}{x^2+1} & 0 & 0 & 1 \end{pmatrix}$$

Using the algorithm from Corollary 5.2.16, we may compute $\mathrm{End}(L) = H^0(\mathcal{E}nd(L))$ and find a 1 dimensional $\mathbb{F}_7$-vector space, whose basis element identifies with the identity matrix under our usual identification $K^9 \simeq M_3(K)$. So, we indeed have $\mathrm{End}(L) = \mathbb{F}_7$.

5.3.3 Algebraic geometry codes

In [76], Savin introduced a generalisation of algebraic geometry codes to vector bundles of arbitrary rank. His construction is optimal when performed over so-called *weakly-stable* vector bundle, and this motivated a line of work constructing weakly-stable vector bundles on projective curves over finite fields [6, 62]. Independently, Weng gave a similar construction [94] based on his adelic setting for vector bundles and introduced the notion of D-balanced vector bundle,

where D is an effective divisor. As in Section 5.3.2, we rephrase known definitions and results in terms of $\mathcal{O}_R$-lattices and give an explicit example as a lattice pair.

For what follows, we assume that k is a global function field with constant field F.

Definition 5.3.10. *Let L be an $\mathcal{O}_R$-lattice. The* slope *of L is defined as*

$$\mu(L) \coloneqq \frac{\deg(L)}{\operatorname{rank}(L)}.$$

Definition 5.3.11. *An $\mathcal{O}_R$-lattice L is said to be* weakly-stable *if for all rank 1 $\mathcal{O}_R$-sublattices L' of L,*

$$\mu(L') \leq \mu(L).$$

Definition 5.3.12. *Let D be an effective divisor of k, and let L be an $\mathcal{O}_R$-lattice. Then L is D-*balanced *if $L_P = \mathcal{O}_P$ for P in* $\operatorname{Supp}(D)$.

Proposition 5.3.13 ([76])**.** *Let $n, d \in \mathbb{N}$. Let α, β be the quotient and the remainder of the Euclidean division of d by n. Let L'_1, L'_2 be rank 1 $\mathcal{O}_R$-lattices of degree α and let L' be a rank 1 $\mathcal{O}_R$-lattice of degree $\alpha + 1$. Consider the following construction:*

1. *$L_1 \coloneqq L'_1$.*
2. *for $2 \leq i \leq n - \beta + 1$, L_i is a non-trivial extension of L'_2 by L_{i-1}.*
3. *for $n - \beta + 2 \leq i \leq n$, L_i is a non-trivial extension of L' by L_{i-1}.*

Then, L_n is a weakly-stable $\mathcal{O}_R$-lattice of rank n and degree d. If D is an effective divisor with support in M^{fi} such that L', L'_1 and L'_2 are D-balanced. Then, if the successive extensions are constructed using the algorithm from Corollary 5.2.21, the lattice L_n is D-balanced.

Example 5.3.14. We let $F = \mathbb{F}_{101}$, $k = F(x, y)/(y^2 - x^5 - 1)$ and construct a weakly-stable vector bundle of rank 3 and degree 10 over k. We also set $\omega = d\pi$.

First, we set $\pi = \frac{y}{x^3}$, a local uniformiser of ∞, the unique infinite place of k. We also define $\mathfrak{p}_1 = \langle x, y + 1\rangle$ and $\mathfrak{p}_2 = \langle x, y - 1\rangle$, two prime ideals of $\mathcal{O}_{fi}$. We will build our vector bundle from the following line bundles:

$$L = \mathrm{LP}(\mathcal{O}_{fi}, 1, \pi^{-4}),$$

$$L_1 = \mathrm{LP}(\mathfrak{p}_1^{-3}, 1, 1),$$

and

$$L_2 = \mathrm{LP}(\mathfrak{p}_7{}^{-3}, 1, 1).$$

We first set $E_1 = L_1$ and compute a non-trivial extension E_2 of L_2 by E_1. We compute a basis of $H^0(\iota(\omega)^{-1}E_1^\vee \otimes L_2)$. This space has dimension 1 and is generated by

$$a = \frac{-2x^2}{x^5+6}(y+1).$$

Computing the formal series expansion of a with respect to π, we find

$$a = -2\pi + O(\pi^6).$$

Therefore, the non-trivial linear form on $H^0(\iota(\omega)^{-1}E_1^\vee \otimes L_2)$ sending a to 1 is represented by the infinite répartition b_∞, where

$$b = \frac{-1}{2\pi^2}.$$

We may, therefore, set

$$E_2 = \mathrm{LP}\left((\mathfrak{p}_1^{-3}, \mathfrak{p}_2^{-3}), I_2, \begin{pmatrix} 1 & \frac{1}{2\pi^2} \\ 0 & 1 \end{pmatrix}\right).$$

Our vector bundle E_3 will then be constructed as a nontrivial extension of L by E_2. Again, we compute a basis of $H^0(\iota(\omega)^{-1}E_2^\vee \otimes L)$ and find:

$$\left(\begin{pmatrix} 0 \\ \frac{x^7}{x^5+6} \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{x^4}{x^5+6}y - \frac{x^4}{x^5+6} \end{pmatrix}, \begin{pmatrix} \frac{x^7}{x^5+6} \\ \frac{-x^8}{2(x^5+6)} \end{pmatrix} \begin{pmatrix} \frac{x^4}{x^5+6}y + \frac{x^4}{x^5+6} \\ \frac{-x^5}{2(x^5+6)}y + \frac{x^5}{2(x^5+6)} \end{pmatrix}\right).$$

We let f_1, f_2, f_3 and f_4 be these columns.

We shall find a vector $v \in k^2$ such that $\theta_\omega(\cdot, v_\infty)$ corresponds to the linear form $\begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}$ with respect to the dual of the basis given above. That is, we must find v_1 and v_2 in k such that for all $1 \leq i \leq 4$,

$$\mathrm{res}_\infty\left(\sum_{j=1}^{2} f_{ij}v_j\right) = \begin{cases} 1 \text{ if } i = 1, \\ 0 \text{ otherwise.} \end{cases} \tag{5.3}$$

Following Algorithm 4, we compute $v_1 = -4$ and $v_2 = -6$. We compute the power series expansion of the coefficients of the f_i, starting at degree -4 on the first row and degree -6 on the second row. We get:

$$f_1 = \begin{pmatrix} 0 \\ \pi^{-4} + O(\pi^{-2}) \end{pmatrix},$$

$$f_2 = \begin{pmatrix} 0 \\ \pi^{-3} + O(\pi^{-2}) \end{pmatrix},$$

$$f_3 = \begin{pmatrix} \pi^{-4} + O(1) \\ \frac{-1}{2}\pi^{-6} + O(\pi^{-2}) \end{pmatrix},$$

and

$$f_4 = \begin{pmatrix} \pi^{-3} + O(1) \\ \frac{-1}{2}\pi^{-5} + O(\pi^{-2}) \end{pmatrix}.$$

Therefore, we must solve the linear system

$$R \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{-1}{2} & 0 \\ 0 & 0 & 0 & \frac{-1}{2} \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}.$$

An obvious solution is $R = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$. Bringing things together, we set $v_1 = 0$ and $v_2 = \pi^3$ and Equation (5.3) is satisfied. Finally, we may set

$$E_3 = \mathrm{LP}\left((\mathfrak{p}_1^{-3}, \mathfrak{p}_2^{-3}, \mathcal{O}_{fi}), I_3, \begin{pmatrix} 1 & \frac{1}{2\pi^2} & 0 \\ 0 & 1 & \frac{-1}{\pi} \\ 0 & 0 & \frac{1}{\pi^4} \end{pmatrix} \right).$$

Conclusions

In this thesis, we have constructed a presentation for central simple algebras based on Amitsur cohomology that allows for efficient computation. We have used this presentation to exhibit a polynomial quantum algorithm under GRH, which solves the explicit isomorphism problem. We have also constructed a representation for vector bundles over normal projective curves as well as algorithms for several natural tasks.

This latter construction relates to the explicit isomorphism problem by the method outlined in Section 5.3.1. With this tool now available, we intend in further research to leverage known results on the structure of vector bundles over curves of positive genus to provide algorithms for the explicit isomorphism problem for global function fields of positive genus. Another perspective for further work is the development of polynomial algorithms for computing Hermite normal forms of pseudo-matrices over the ring $\mathcal{O}_{fi}$ of a global function field.

Also in perspective are the possibilities offered by the computational practicality of our presentation of central simple algebras as Amitsur algebras. There is a polynomial reduction from the Amitsur version of the explicit isomorphism problem to the general explicit isomorphism problem, and there is no known efficient classical algorithm for this latter problem over global fields other than $F(X)$. These facts suggest that the explicit isomorphism problem may be used as a hard problem in cryptography (see [53] for an identification scheme based on a similar problem). The problem of finding a preimage of a coboundary through the group homomorphism $\partial^1 \colon C^1_{Am}(k, K) \to B^2_{Am}(k, K)$ reduces directly to the explicit isomorphism problem, with elements of the codomain encoding an instance of the problem and elements of the domain encoding witnesses to a solution. This setting may prove fruitful for the construction of cryptographic primitives and protocols.

Bibliography

[1] Adamson, I. T. Cohomology theory for non-normal subgroups and non-normal fields. *Proc. Glasgow Math. Assoc. 2* (1954), 66–76. https://doi.org/10.1017/S2040618500033050.

[2] Amitsur, S. A. Simple algebras and cohomology groups of arbitrary fields. *Trans. Amer. Math. Soc. 90* (1959), 73–112. https://doi.org/10.2307/1993268.

[3] Arason, J. K., Elman, R., and Jacob, B. On indecomposable vector bundles. *Comm. Algebra 20*, 5 (1992), 1323–1351. https://doi.org/10.1080/00927879208824407.

[4] Atiyah, M. On the Krull-Schmidt theorem with application to sheaves. *Bull. Soc. Math. France 84* (1956), 307–317. http://www.numdam.org/item?id=BSMF_1956__84__307_0.

[5] Atiyah, M. F. Vector bundles over an elliptic curve. *Proc. London Math. Soc. (3) 7* (1957), 414–452. https://doi.org/10.1112/plms/s3-7.1.414.

[6] Ballico, E. Vector bundles on curves over $\mathbb{F}_q$ and algebraic codes. *Finite Fields Appl. 14*, 4 (2008), 1101–1107. https://doi.org/10.1016/j.ffa.2008.07.003.

[7] Biasse, J.-F., and Fieker, C. Subexponential class group and unit group computation in large degree number fields. *LMS J. Comput. Math. 17* (2014), 385–403. https://doi.org/10.1112/S1461157014000345.

[8] Biasse, J.-F., Fieker, C., and Hofmann, T. On the computation of the HNF of a module over the ring of integers of a number field. *J. Symbolic Comput. 80* (2017), 581–615. https://doi.org/10.1016/j.jsc.2016.07.027.

[9] Biasse, J.-F., and Song, F. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms* (2016), ACM, New York, pp. 893–902. https://doi.org/10.1137/1.9781611974331.ch64.

[10] Bosma, W., Cannon, J., Fieker, C., and Stell, A., Eds. *Handbook of Magma functions (Version 2.13)*. 2023.

[11] Bourbaki, N. *Algebra II. Chapters 4–7*, english ed. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 2003. https://doi.org/10.1007/978-3-642-61698-3.

[12] Bremner, M. R. How to compute the Wedderburn decomposition of a finite-dimensional associative algebra. *Groups Complex. Cryptol. 3*, 1 (2011), 47–66. https://doi.org/10.1515/GCC.2011.003.

[13] Cassels, J. W. S., and Fröhlich, A., Eds. *Algebraic number theory* (1967), Academic Press, London; Thompson Book Co., Inc., Washington, DC.

[14] Chase, S. U., and Rosenberg, A. Amitsur cohomology and the brauer group. In *Galois theory and cohomology of commutative rings*, vol. 1 of *Memoirs of the Americam Mathematical Society*. American Mathematical Society, 1965, pp. 20–65.

[15] Cohen, H. *A course in computational algebraic number theory*, vol. 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993. https://doi.org/10.1007/978-3-662-02945-9.

[16] Cohen, H. Hermite and Smith normal form algorithms over Dedekind domains. *Math. Comp. 65*, 216 (1996), 1681–1699. https://doi.org/10.1090/S0025-5718-96-00766-1.

[17] Cohen, H. *Advanced topics in computational number theory*, vol. 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. https://doi.org/10.1007/978-1-4419-8489-0.

[18] Colliot-Thélène, J.-L., and Skorobogatov, A. N. *The Brauer-Grothendieck Group*. Springer Cham, 2021. https://doi.org/10.1007/978-3-030-74248-5.

[19] Cremona, J., Fisher, T., O'Neil, C., Simon, D., and Stoll, M. Explicit n-descent on elliptic curves, i. algebra. *J. Reine Angew. Math. 2008*, 615 (2008), 121–155. https://doi.org/10.1515/CRELLE.2008.012.

[20] Cremona, J., Fisher, T., O'Neil, C., Simon, D., and Stoll, M. Explicit n-descent on elliptic curves, ii. geometry. *J. Reine Angew. Math. 2009*, 632 (2009), 63–84. https://doi.org/10.1515/CRELLE.2009.050.

[21] Cremona, J., and Rusin, D. Efficient solution of rational conics. *Math. Comp. 72*, 243 (2003), 1417–1441. https://doi.org/10.1090/S0025-5718-02-01480-1.

[22] Cremona, J. E., Fisher, T. A., O'Neil, C., Simon, D., and Stoll, M. Explicit n-descent on elliptic curves III. Algorithms. *Math. Comp. 84*, 292 (2015), 895–922. https://doi.org/10.1090/S0025-5718-2014-02858-5.

[23] Csahók, T., Kutas, P., Montessinos, M., and Zábrádi, G. Explicit isomorphisms of quaternion algebras over quadratic global fields. *Research in Number Theory 8*, 4 (2022), 77. https://doi.org/10.1007/s40993-022-00380-3.

[24] De Graaf, W. A., Harrison, M., Pílniková, J., and Schicho, J. A Lie algebra method for rational parametrization of severi–brauer surfaces. *J. Algebra 303*, 2 (2006), 514–529. https://doi.org/10.1016/j.jalgebra.2005.06.022.

[25] de Graaf, W. A., and Ivanyos, G. Finding splitting elements and maximal tori in matrix algebras. In *Interactions between ring theory and representations of algebras (Murcia)*, vol. 210 of *Lecture Notes in Pure and Appl. Math.* Dekker, New York, 2000, pp. 95–105. https://dspace.library.uu.nl/handle/1874/1616.

[26] de Graaf, W. A., Ivanyos, G., Küronya, A., and Rónyai, L. Computing Levi decompositions in Lie algebras. *Appl. Algebra Engrg. Comm. Comput. 8*, 4 (1997), 291–303. https://doi.org/10.1007/s002000050066.

[27] Decker, W., and Eisenbud, D. Sheaf algorithms using the exterior algebra. In *Computations in algebraic geometry with Macaulay 2*, vol. 8 of

Algorithms Comput. Math. Springer, Berlin, 2002, pp. 215–249. https://doi.org/10.1007/978-3-662-04851-1_9.

[28] Eberhard, S. The characteristic polynomial of a random matrix. *Combinatorica 42*, 4 (2022), 491–527. https://doi.org/10.1007/s00493-020-4657-0.

[29] Fieker, C. Minimizing representations over number fields. II. Computations in the Brauer group. *J. Algebra 322*, 3 (2009), 752–765. https://doi.org/10.1016/j.jalgebra.2009.05.009.

[30] Fisher, T. Explicit 5-descent on elliptic curves. *Open Book Ser. 1*, 1 (2013), 395–411. https://doi.org/10.2140/obs.2013.1.395.

[31] Fisher, T. Higher descents on an elliptic curve with a rational 2-torsion point. *Math. Comp. 86*, 307 (2017), 2493–2518. https://doi.org/10.1090/mcom/3163.

[32] Fisher, T., and Newton, R. Computing the cassels-tate pairing on the 3-selmer group of an elliptic curve. *Int. J. Number Theory 10*, 07 (2014), 1881–1907. https://doi.org/10.1142/S1793042114500602.

[33] Ford, T. J. *Separable algebras*, vol. 183 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017. https://doi.org/10.1090/gsm/183.

[34] Friedrichs, C. *Berechnung von Maximalordnungen über Dedekindringen*. PhD thesis, Technische Universität Berlin, 2000. http://www.math.tu-berlin.de/~kant/publications/diss/diss_fried.pdf.gz.

[35] Garg, A., Gupta, N., Kayal, N., and Saha, C. Determinant Equivalence Test over Finite Fields and over Q. In *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)* (Dagstuhl, Germany, 2019), C. Baier, I. Chatzigiannakis, P. Flocchini, and S. Leonardi, Eds., vol. 132 of *Leibniz International Proceedings in Informatics (LIPIcs)*, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, pp. 62:1–62:15. https://doi.org/10.4230/LIPIcs.ICALP.2019.62.

[36] Gille, P., and Szamuely, T. *Central simple algebras and Galois cohomology*, second ed., vol. 165 of *Cambridge Studies in Advanced*

Mathematics. Cambridge University Press, Cambridge, 2017. https://doi.org/10.1017/CBO9780511607219.

[37] Gómez-Torrecillas, J., Kutas, P., Lobillo, F. J., and Navarro, G. Primitive idempotents in central simple algebras over fq (t) with an application to coding theory. *Finite Fields Appl. 77* (2022), 101935. https://doi.org/10.1016/j.ffa.2021.101935.

[38] Görtz, U., and Wedhorn, T. *Algebraic geometry I. Schemes—with examples and exercises*, second ed. Springer Studium Mathematik—Master. Springer Spektrum, Wiesbaden, [2020] ©2020. https://doi.org/10.1007/978-3-658-30733-2.

[39] Guàrdia, J., Montes, J., and Nart, E. Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields. *J. Théor. Nombres Bordeaux 23*, 3 (2011), 667–696. https://doi.org/10.5802/jtnb.782.

[40] Guàrdia, J., Montes, J., and Nart, E. A new computational approach to ideal theory in number fields. *Found. Comput. Math. 13*, 5 (2013), 729–762. https://doi.org/10.1007/s10208-012-9137-5.

[41] Gupta, S., Sarkar, S., Storjohann, A., and Valeriote, J. Triangular x-basis decompositions and derandomization of linear algebra algorithms over $K[x]$. *J. Symbolic Comput. 47*, 4 (2012), 422–453. https://doi.org/10.1016/j.jsc.2011.09.006.

[42] Hartshorne, R. *Algebraic geometry*, vol. No. 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1977. https://doi.org/10.1007/978-1-4757-3849-0.

[43] Hazewinkel, M., and Martin, C. F. A short elementary proof of Grothendieck's theorem on algebraic vectorbundles over the projective line. *J. Pure Appl. Algebra 25*, 2 (1982), 207–211. https://doi.org/10.1016/0022-4049(82)90037-8.

[44] Hess, F. An algorithm for computing Weierstrass points. In *Algorithmic number theory (Sydney, 2002)*, vol. 2369 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 2002, pp. 357–371. https://doi.org/10.1007/3-540-45455-1_29.

[45] Hess, F. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comput. 33*, 4 (2002), 425–445. https://doi.org/10.1006/jsco.2001.0513.

[46] Ivanyos, G., Kutas, P., and Rónyai, L. Computing explicit isomorphisms with full matrix algebras over $\mathbb{F}_q(x)$. *Found. Comput. Math. 18*, 2 (2018), 381–397. https://doi.org/10.1007/s10208-017-9343-2.

[47] Ivanyos, G., Lelkes, A. D., and Rónyai, L. Improved algorithms for splitting full matrix algebras. *JP J. Algebra Number Theory Appl. 28*, 2 (2013), 141–156. http://www.pphmj.com/abstract/7461.htm.

[48] Ivanyos, G., and Rónyai, L. Finding maximal orders in semisimple algebras over **Q**. *Comput. Complexity 3*, 3 (1993), 245–261. https://doi.org/10.1007/BF01271370.

[49] Ivanyos, G., Rónyai, L., and Schicho, J. Splitting full matrix algebras over algebraic number fields. *J. Algebra 354* (2012), 211–223. https://doi.org/10.1016/j.jalgebra.2012.01.008.

[50] Jacobson, N. Brauer factor sets, Noether factor sets, and crossed products. In *Emmy Noether in Bryn Mawr (Bryn Mawr, Pa., 1982)*. Springer, New York-Berlin, 1983, pp. 1–20. https://doi.org/10.1007/978-1-4612-5547-5_1.

[51] Jacobson, N. *Finite-dimensional division algebras over fields*. Springer-Verlag, Berlin, 1996. https://doi.org/10.1007/978-3-642-02429-0.

[52] Kailath, T. *Linear systems*. Prentice-Hall Information and System Sciences Series. Prentice-Hall, Inc., Englewood Cliffs, NJ, 1980.

[53] Kiss, S. Z., and Kutas, P. An identification system based on the explicit isomorphism problem. *Appl. Algebra Engrg. Comm. Comput. 34*, 6 (2023), 913–930. https://doi.org/10.1007/s00200-021-00529-0.

[54] Kutas, P. Splitting quaternion algebras over quadratic number fields. *J. Symbolic Comput. 94* (2019), 173–182. https://doi.org/10.1016/j.jsc.2018.08.002.

[55] Kutas, P., and Montessinos, M. Efficient computations in central simple algebras using amitsur cohomology. *J. Algebra 665* (2025), 255–281. https://doi.org/10.1016/j.jalgebra.2024.10.045.

[56] Le Potier, J. *Lectures on vector bundles*, vol. 54 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997. Translated by A. Maciocia.

[57] Lenstra, Jr., H. W., and Silverberg, A. Algorithms for commutative algebras over the rational numbers. *Found. Comput. Math. 18*, 1 (2018), 159–180. https://doi.org/10.1007/s10208-016-9336-6.

[58] McConnell, J. C. Division algebras—beyond the quaternions. *Amer. Math. Monthly 105*, 2 (1998), 154–162. https://doi.org/10.2307/2589646.

[59] Méndez Omaña, J., and Pohst, M. E. Factoring polynomials over global fields. II. *J. Symbolic Comput. 40*, 6 (2005), 1325–1339. https://doi.org/10.1016/j.jsc.2005.03.003.

[60] Montessinos, M. Algebraic algorithms for vector bundles over curves. Journal of Algebra and Its Applications (to appear), 2024. http://doi.org/10.1142/S0219498826500210.

[61] Motsak, O. *Graded commutative algebra and related structures in Singular with applications*. PhD thesis, Technische Universität Kaiserslautern, 2011. https://nbn-resolving.de/urn:nbn:de:hbz:386-kluedo-26479.

[62] Nakashima, T. AG codes from vector bundles. *Des. Codes Cryptogr. 57*, 1 (2010), 107–115. https://doi.org/10.1007/s10623-009-9354-3.

[63] Neukirch, J. *Algebraic number theory*, vol. 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. https://doi.org/10.1007/978-3-662-03983-0.

[64] Newman, M. *Integral matrices*, vol. Vol. 45 of *Pure and Applied Mathematics*. Academic Press, New York-London, 1972.

[65] Oda, T. Vector bundles on an elliptic curve. *Nagoya Math. J. 43* (1971), 41–72. http://projecteuclid.org/euclid.nmj/1118798365.

[66] Pílniková, J. Trivializing a central simple algebra of degree 4 over the rational numbers. *J. Symbolic Comput. 42*, 6 (2007), 579–586. https://doi.org/10.1016/j.jsc.2007.01.001.

[67] Preu, T. Effective lifting of 2-cocycles for Galois cohomology. *Cent. Eur. J. Math. 11*, 12 (2013), 2138–2149. https://doi.org/10.2478/s11533-013-0319-4.

[68] Pumplün, S. Vector bundles and symmetric bilinear forms over curves of genus one and arbitrary index. *Math. Z. 246*, 3 (2004), 563–602. https://doi.org/10.1007/s00209-003-0589-9.

[69] Reiner, I. *Maximal orders*, vol. 28 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, With a foreword by M. J. Taylor.

[70] Rónyai, L. Computing the structure of finite algebras. *J. Symbolic Comput. 9*, 3 (1990), 355–373. https://doi.org/10.1016/S0747-7171(08)80017-X.

[71] Rónyai, L. Algorithmic properties of maximal orders in simple algebras over $\mathbf{Q}$. *Comput. Complexity 2*, 3 (1992), 225–243. https://doi.org/10.1007/BF01272075.

[72] Rosen, M. *Number theory in function fields*, vol. 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002. https://doi.org/10.1007/978-1-4757-6046-0.

[73] Rosenberg, A., and Zelinsky, D. On Amitsur's complex. *Trans. Amer. Math. Soc. 97* (1960), 327–356. https://doi.org/10.2307/1993305.

[74] Saltman, D. J. *Lectures on division algebras*, vol. 94 of *CBMS Regional Conference Series in Mathematics*. American Mathematical Society, Providence, RI; on behalf of Conference Board of the Mathematical Sciences, Washington, DC, 1999. https://doi.org/10.1090/cbms/094.

[75] Sarkar, S., and Storjohann, A. Normalization of row reduced matrices. In *ISSAC 2011—Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation* (2011), ACM, New York, pp. 297–303. https://doi.org/10.1145/1993886.1993931.

[76] Savin, V. Algebraic-geometric codes from vector bundles and their decoding. https://arxiv.org/abs/0803.1096v1, 2008. Preprint, 5 pages.

[77] Schoemann, C., and Wiedmann, S. Another proof of Grothendieck's theorem on the splitting of vector bundles on the projective line. *Arch. Math. (Basel) 110*, 6 (2018), 573–580. https://doi.org/10.1007/s00013-018-1158-0.

[78] Serre, J.-P. Faisceaux algébriques cohérents. *Ann. of Math. (2) 61* (1955), 197–278. https://doi.org/10.2307/1969915.

[79] Serre, J.-P. *Algebraic groups and class fields*, vol. 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988. Translated from the French.

[80] Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*. IEEE Comput. Soc. Press, Los Alamitos, CA, 1994, pp. 124–134. https://doi.org/10.1109/SFCS.1994.365700.

[81] Silverman, J. H. *The arithmetic of elliptic curves*, second ed., vol. 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, 2009. https://doi.org/10.1007/978-0-387-09494-6.

[82] Simon, D. Solving norm equations in relative number fields using S-units. *Math. Comp. 71*, 239 (2002), 1287–1305. https://doi.org/10.1090/S0025-5718-02-01309-1.

[83] Smith, G. G. Computing global extension modules. *Journal of Symbolic Computation 29*, 4 (2000), 729–746. https://doi.org/10.1006/jsco.1999.0399.

[84] Stichtenoth, H. *Algebraic function fields and codes*, second ed., vol. 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 2009. https://doi.org/10.1007/978-3-540-76878-4.

[85] Storjohann, A., and Labahn, G. Asymptotically fast computation of hermite normal forms of integer matrices. In *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation* (New York, NY, USA, 1996), ISSAC '96, Association for Computing Machinery, p. 259–266. https://doi.org/10.1145/236869.237083.

[86] Sugahara, K. Adelic riemann-roch theorem on curve. Master's thesis, Kyushu University, 2012.

[87] Tate, J. Residues of differentials on curves. *Ann. Sci. École Norm. Sup. (4) 1* (1968), 149–159. http://www.numdam.org/item?id=ASENS_1968_4_1_1_149_0.

[88] The PARI Group. *PARI/GP version 2.15.4*. Univ. Bordeaux, 2023. available from http://pari.math.u-bordeaux.fr/.

[89] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.3)*, 2024. https://www.sagemath.org.

[90] Tillmann, A. *Unzerlegbare Vektorbündel über algebraischen Kurven*. PhD thesis, FernUniversität, Hagen, 1983.

[91] Voight, J. *Quaternion algebras*, vol. 288 of *Graduate Texts in Mathematics*. Springer, Cham, 2021. https://doi.org/10.1007/978-3-030-56694-4.

[92] Weil, A. *Basic number theory*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. Reprint of the second (1973) edition.

[93] Weng, L. Adelic extension classes, atiyah bundles and non-commutative codes. https://arxiv.org/abs/1809.00791v1, 2018. Preprint, 25 pages.

[94] Weng, L. Codes and stability. https://arxiv.org/abs/1806.04319v1, 2018. Preprint, 24 pages.

[95] Weng, L. *Zeta functions of reductive groups and their zeros*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2018. https://doi.org/10.1142/10723.

[96] Yan, J. *Computing the Cassels-Tate Pairing for Jacobian Varieties of Genus Two Curves*. PhD thesis, Apollo - University of Cambridge Repository, 2021. https://doi.org/10.17863/CAM.72729.

Santrauka (Summary in Lithuanian)

Tyrimo objektas

Disertacijoje yra nagrinėjama išreikštinio izomorfizmo problema ir susijusios algoritminės problemos.

Problema A (išreikštinio izomorfizmo problema)**.** *Duotam kūnui k ir k-algebrai A, izomorfiškai matricinei algebrai $M_d(k)$ su tam tikru $d \in \mathbb{N}$, apskaičiuoti izomorfizmą $\varphi : A \to M_d(k)$.*

Išreikštinio izomorfizmo problema paprastai nagrinėjama tam tikrame kūne arba kūnų klasėje. Mūsų atveju daugiausia dėmesio skiriame aiškaus izomorfizmo problemos sprendimui globaliuose kūnuose, t. y., skaičių kūnams ir globaliesiems funkcijų kūnams, kurie yra racionaliųjų funkcijų kūno $F(X)$, kur F yra baigtinis kūnas, baigtiniai plėtiniai.

Kadangi nustatėme, kad vektorių grižtės apimančios normaliąsias projekcines kreives yra svarbūs objektai tiriant išreikštinio izomorfizmo problemą funkcijų kūnams, taip pat nagrinėjame tokių vektorių grižčių algoritminę teoriją.

Aktualumas

Išreikštinio izomorfizmo problemą galima laikyti natūralia problema algoritminėje įvaizdžių teorijoje. Turint k-algebrą A, galima norėti aprašyti jos struktūrą: apskaičiuoti Jakobsono radikalą $J(A)$ ir algebros A puspaprastę dalį bei išskaidymą kaip paprastųjų k-algebrų sumą, kurios pačios yra izomorfiškos tam tikrai $M_n(D)$, kur D yra k-algebra su dalyba. Apskritai sunkiausia šiame uždavinyje yra rasti izomorfizmą $A \to M_n(D)$, kai algebra A yra paprastoji.

Bendrasis šios problemos sprendimo receptas yra toks: nustatyti D Brauerio klasę virš jos centro K/k, rasti struktūros konstantas algebrai $M_d(D^{\mathrm{op}})$ ir tada apskaičiuoti aiškų izomorfizmą $A \otimes M_d(D^{\mathrm{op}}) \simeq M_{d^2}(K)$ [23, 37, 49].

Išreikštinio izomorfizmo problemos taikymai neapsiriboja vien tik asociatyviųjų algebrų algoritmine teorija. Aritmetinėje geometrijoje problema yra svarbi trivializuojant obstrukcines algebras apskaičiuojant nusileidimą virš elipsinių kreivių [22] ir skaičiuojant Cassels-Tate porynius [32, 96]. Problema taip pat susijusi su Severi-Brauer paviršių parametrizavimu [24]. Naujausi darbai algebrino sudėtingumo teorijoje redukavo determinanto lygiavertiškumo testą iki išreikštinio izomorfizmo problemos [35]. Galiausiai, išreikštinio izomorfizmo problema virš racionalių funkcijų kūno $F(X)$ (čia F baigtinis) taip pat yra aktuali ir klaidas taisantiems kodams [37].

Baigtinio bazinio kūno atveju, išreikštinio izomorfizmo uždavinio polinominio laiko algoritmą pasiūlė Ronyai [70].

Išreikštinio izomorfizmo problemos atvejai $\mathbb{Q}$-algebroms pirmiausiai buvo nagrinėjami mažoms d reikšmėms. Kai $d = 2$, problema susiveda į racionalaus taško radimą projekciniame kūgyje [91, 5.5.4 teorema], kuri išspręsta, pavyzdžiui, straipsnyje [21]. Atvejis $d = 3$ yra nagrinėjamas straipsnyje [24], kuriame buvo pasiūlytas subeksponentinis algoritmas, duodant ciklinę išraišką ir sprendžiant kubinę normos lygtį. Atvejis $d = 4$ nagrinėjamas [66], suvedant problemą į kvaternionų algebrų virš $\mathbb{Q}$ ir kvadratinių skaičių kūnų atvejį ir sprendžiant kvadratinę normos lygtį.

Straipsnyje [22] buvo pateiktas ir ištirtas algoritmas, skirtas daugiausia atvejams $d = 3$ ir $d = 5$. Vėliau jis buvo apibendrintas [47, 49] iki K-algebros, izomorfiškos algebrai $M_d(K)$, kur d yra natūralusis skaičius, o K yra skaičių kūnas. Pastarojo algoritmo sudėtingumas yra polinominis įvesties algebros struktūrinių konstantų dydžiui, bet eksponentiškai priklauso nuo d, kūno K laipsnio ir diskriminanto dydžio.

2018 m. G. Ivanyos ir kt. [46] pristatė polinominio laiko algoritmą išreikštinio izomorfizmo problemai kūnui $F(X)$, kur F yra baigtinis kūnas.

Fiksuoto d ir varijuojamojo bazinio kūno atveju darbuose [31, 54] nepriklausomai pateiktas algoritmas algebrai, izomorfinei $M_2(K)$, kur K yra kvadratinis skaičių kūnas. Šio algoritmo sudėtingumas polinomiškai auga kūno K diskriminanto atžvilgiu.

Nors straipsnio [46] metodai yra grynai algebriniai, 5.3.1 sekcijoje teigiame, kad pagrindinis teorinis rezultatas, kuriuo paremtas algoritmas, gali būti natūraliai interpretuojamas kaip garsioji Grotendiko teorema apie vektorių

grižčių strukturą virš projekcinės tiesės. Kadangi Grotendiko teorema negalioja aukštesnio rūšio funkcijų kūnams, metodas, išvystytas straipsnyje [46], nėra tiesiogiai apibendrinamas tokiems kūnams. Tačiau mūsų šio metodo geometrinė interpretacija rodo, kad pažangą galima pasiekti pasinaudojus ankstesniais rezultatais apie vektorių grižčių strukturą, apimančią normaliąsias projekcines kreives, turinčias aukštesnį rūšį. Tai leidžia manyti, kad tikslinga sukurti algoritminę teoriją vektorių grižtiems virš normaliųjų projekcinų kreivių išreikšti, naudojant gardelių poras.

Tikslai

Disertacijos tikslas - pristatyti naujus metodus, skirtus išreikštnio izomorfizmo problemai globaliuose kūnuose spręsti. Skaičių kūnuose siekiame pateikti naują kohomologinį centrinių paprastųjų algebrų aprašą, tinkamą praktiniams skaičiavimams, ir ištirti tokio įrankio poveikį, sprendžiant išreikštinio izomorfizmo problemą skaičių kūnuose. Funkcijų kūnuose siekiame sukurti algoritminę vektorių grižčių teoriją, paremtą gardelių virš maksimalių eilių teorija.

Pagrindiniai rezultatai

Kūnui k ir etalinei k-algebrai K apibrėžiame grupę $Z^2_{Am}(k,K) \subset (K^{\otimes 3})^\times$, pogrupį $B^2_{Am}(k,K)$ ir nagrinėjame faktorgrupę

$$H^2_{Am}(k,K) = Z^2_{Am}(k,K)/B^2_{Am}(k,K).$$

Tada apibrėžiame Amitsuro algebrą $A(K,c)$, skirtą $c \in Z^2_{Am}(k,K)$, kurios pagrindinė k-vektorinė erdvė yra $K^{\otimes 2}$, ir įrodome sekantį klasifikacijos rezultatą:

Teorema B. *Tegu k yra kūnas, o K - etalinė k-algebra, kurios dimensija d. Tegul $c \in K^{\otimes 3}$. Tada $A(K,c)$ yra centrinė paprastoji k-algebra tada ir tik tada, kai $c \in Z^2_{Am}(k,K)$. Šiuo atveju $A(K,c)$ yra laipsnio k ir joje K yra viena maksimalių iš jos komutativiųjų poalgebrų ir, atvirkščiai, jei A yra centrinė paprastoji k-algebra, kurioje K yra maksimalus komutatyvusis poalgebris, tai egzistuoja $c \in Z^2_{Am}(k,K)$ toks, kad algebra $A(K,c)$ yra izomorfiška algebrai A.*

Taip gaunamas izomorfizmas $H^2_{Am}(k,K) \simeq \mathrm{Br}(K/k)$ su algebros K santykine Brauerio grupe virš k.

Parinkime polinomą tokį $\chi \in k[X]$, kad egzistuotu izomorfizmas $K \simeq k[X]/(\chi(X))$. Nagrinėjame algebras $K_1 = k[X,Y]/(\chi(X), \chi(Y))$ ir $K_2 = k[X,Y,Z]/(\chi(X), \chi(Y), \chi(Z))$. Pastebėkime, kad algebra K_n (čia $n = 1$ arba $n = 2$) yra natūraliai izomorfiška algebrai $K^{\otimes(n+1)}$, o jos elementai gali būti pateikti apskaičiavimo būdu kaip polinomų liekanų klasės. Įrodome Amitsuro algebrų algoritminius rezultatus:

Teorema C. *Sutapatindami grupės $Z^2_{Am}(k,K)$ elementus su jų vaizdais algebroje K_2 ir sutapatindami algebrą $A(K,c)$ su algebra K_1 kaip k-vektorinę erdvę, gauname šiuos rezultatus:*

1. *Egzistuoja polinominis algoritmas, kuris, su $\chi, c \in Z^2_{Am}(k,K)$ ir α bei β algebroje $A(K,c)$, apskaičiuoja sandaugą $\alpha\beta$;*

2. *Egzistuoja tikimybinis polinominis algoritmas, kuris, duotai centrinei paprastąjai k-algebrai A, apskaičiuoja maksimalų komutatyvųjų poalgebrį $K \subset A$, polinomą χ tokį, kad $K \simeq k[X]/(\chi(X))$, $c \in Z^2_{Am}(k,K)$ ir k-algebros izomorfizmą iš k-algebros A į k-algebrą $A(K,c)$.*

Taikydami Amitsuro algebrų konstrukciją, įrodome sekantį rezultatą:

Teorema D. *Jei yra teisinga apibendrintoji Rymano hipotezė, tai Algoritmas 2 yra polinominis kvantinis algoritmas, sprendžiantis išreikštino izomofrizmo problemą skaičių kūnuose.*

Tegul X yra normalioji projekcinė kreivė virš baigtinio kūno F ir tegul k yra jos funkcijų kūnas. Tegul $\mathcal{O}_{fi}$ ir $\mathcal{O}_\infty$ yra atitinkamai $F[X]$ ir $F(X)_\infty = \{R \in k(X) : \deg R \leq 0\}$ sveikieji uždariniai kūne k. Gardelės pora, kurios rangas ant kūno k yra n, yra duomenys projektinio $\mathcal{O}_{fi}$-pomodulio L_{fi} iš erdvės k^n ir laisvojo $\mathcal{O}_\infty$ pomodulio L_∞ iš erdvės k^n, tokie, kad $kL_{fi} = kL_\infty = k^n$. Įrodysime tokią teoremą:

Teorema E. *Vektorių grižčių apimančių kreivę X kategorija yra ekvivalenti kūno k gardelių porų kategorijai.*

Pateikiame funkcijų kūno k gardelių porų skaičiavimo reiškimą. Tegul LP yra funktorius iš vektorių grižčių apimančių kreivės X kategorijos į aukščiau aptartą gardelių porų kategoriją. Tada gauname keletą algoritminių rezultatų. Jei nenurodyta kitaip, sekančioje teoremoje E ir E' yra vektorių grižtės apimančios kreivę X.

Teorema F. *1. Egzistuoja polinominis algoritmas, kuris, duotai gardelių porai* $\mathrm{LP}(E)$*, apskaičiuoja* $\mathrm{LP}(\det(E))$.

2. *Egzistuoja polinominis algoritmas, kuris, duotai gardelių porai* $\mathrm{LP}(E)$*, apskaičiuoja* $\deg(E)$.

3. *Egzistuoja polinominis algoritmas, kuris, duotoms gardelių poroms* $\mathrm{LP}(E)$ *ir* $\mathrm{LP}(E')$*, apskaičiuoja* $\mathrm{LP}(E \otimes E')$.

4. *Egzistuoja polinominis algoritmas, kuris, duotoms gardelių poroms* $\mathrm{LP}(E)$ *ir* $\mathrm{LP}(E')$*, apskaičiuoja* $\mathrm{LP}(E \oplus E')$.

5. *Egzistuoja polinominis algoritmas, kuris, duotai gardelių porai* $\mathrm{LP}(E)$*, apskaičiuoja* $\mathrm{LP}(E^\vee)$.

6. *Egzistuoja polinominis algoritmas, kuris, duotoms gardelių poroms* $\mathrm{LP}(E)$ *ir* $\mathrm{LP}(E')$*, apskaičiuoja* $\mathrm{LP}(\mathcal{H}om(E, E'))$.

7. *Jei* $f\colon Y \to X$ *yra normaliųjų projekcinių kreivių morfizmas, tai egzistuoja polinominis algoritmas, kuris, esant duotam* $\mathrm{LP}(E)$*, kai* E *yra vektorių grįžtė apimančia kreivę* Y*, apskaičiuoja* $\mathrm{LP}(f_*(E))$.

8. *Jei* f *ir* Y *yra kaip aukščiau, tai egzistuoja polinominis algoritmas, kuris, duotai garedlių porai* $\mathrm{LP}(E)$*, kai* E *yra vektorių grįžtė apimančia kreivę* X*, apskaičiuoja gardelių porą* $\mathrm{LP}(f^*(E))$ *kreivės* Y *funkcijų kūnui.*

9. *Egzistuoja polinominis algoritmas, kuris, duotai gardelių porai* $\mathrm{LP}(E)$*, apskaičiuoja erdvės* $H^0(X, E)$ *bazę.*

10. *Egzistuoja polinominis algoritmas, kuris, duotai gardelių porai* $\mathrm{LP}(E)$*, apskaičiuoja erdvės* $H^1(X, E)$ *bazę.*

11. *Egzistuoja polinominis algoritmas, kuris, duotoms gardelių poroms* $\mathrm{LP}(E)$ *ir* $\mathrm{LP}(E')$*, ir* $\xi \in H^1(X, \mathcal{H}om(E, E'))$*, apskaičiuoja* $\mathrm{LP}(E'')$*, kur* E'' *yra* E *plėtinys pagal* E'*, atitinkantis* ξ.

12. *Egzistuoja polinominis algoritmas, kuris, su duotu orakulu*[1]*, apskaičiuojančiu Hermito normaliąsias formas pseudomatricoms virš* $\mathcal{O}_{fi}$*, gardelių poras* $\mathrm{LP}(E)$ *ir* $\mathrm{LP}(E')$ *bei matricą, vaizduojančią* $\mathrm{LP}(f)$*, homomorfizmui* $f\colon E \to E'$*, apskaičiuoja* $\mathrm{LP}(\mathrm{Ker}(f))$.

[1] idealus algoritmas, greitai išsprendžiantis specifinį uždavinį

13. *Egzistuoja polinominis algoritmas, kuris, su duotu orakulu, apskaičiuojančių Hermito normaliąsias formas pseudomatricoms virš $\mathcal{O}_{fi}$, ir duotoms gardelių poroms* $\mathrm{LP}(E)$ *ir* $\mathrm{LP}(E')$ *bei matricai, vaizduojančiai* $\mathrm{LP}(f)$*, homomorfizmui* $f\colon E \to E'$*, apskaičiuoja* $\mathrm{LP}(\mathrm{Im}(f))$.

14. *Egzistuoja polinominis algoritmas, kuris, su duotu orakulu, apskaičiuojančiu Hermito normaliąsias formas pseudomatricoms virš $\mathcal{O}_{fi}$, ir duotai gardelių porai* $\mathrm{LP}(E)$*, apskaičiuoja gardelių poras* $\mathrm{LP}(E_1), \ldots, \mathrm{LP}(E_r)$*, kad vektorių grižtės* $E_1, \ldots, E_r$ *yra neskaidžios, bei izomorfismą iš gardelių poros* $\mathrm{LP}(E)$ *į gardelių porą* $\mathrm{LP}(E_1 \oplus \ldots \oplus (E_r))$.

15. *Egzistuoja polinominis algoritmas, kuris, su duotu orakulu, apskaičiuojančiu Hermito normaliąsias formas pseudomarticoms virš $\mathcal{O}_{fi}$, ir duotoms dvi gardelių poroms* $\mathrm{LP}(E)$ *ir* $\mathrm{LP}(E')$*, nustato, ar* E *ir* E' *yra izomorfiniai, ir, jei taip, apskaičiuoja izomorfizmą* $\mathrm{LP}(f)$.

Visi aptarti algoritmai gardelių poroms buvo realizuoti kaip Sagemath [89] paketas[2].

Metodai

Straipsnyje [55] Teorema B įrodoma parodant, kad mūsų Amitsur algebrų konstrukcija yra ekvivalenti Brauerio algebrų konstrukcijai, ir toliau pasinaudojant ankstesniais rezultatais Brauerio algebroms [51, 2 sk]. Šiame darbe vietoj to pateikiame tiesioginį įrodymą, kaip siūloma straipsnio [55] pastaboje 3.8.

Tegu k yra globalus kūnas, R yra etalinė k-algebra ir S yra R-algebra, kuri yra etalinė kaip k-algebra ir laisva kaip R-modulis. Tegu $S^{\otimes n}$ yra n-lypė tenzorių sandauga $S \otimes_R \ldots \otimes_R S$. Priminsime Amitsuro komplekso apibrėžimą. Kai $n \in \mathbb{Z}_{\geq 0}$ ir $i \in [n+1]_0$, apibrėžiame R-algebros homomorfizmą

$$\begin{array}{rccc} \varepsilon_i^n\colon & S^{\otimes n+1} & \to & S^{\otimes n+2} \\ & a_0 \otimes \ldots \otimes a_n & \mapsto & a_0 \ldots a_{i-1} \otimes 1 \otimes a_i \otimes \ldots \otimes a_n \end{array}$$

ir grupės homomorfizmą

$$\begin{array}{rccc} \partial_{Am}^n\colon & (S^{\otimes n+1})^\times & \to & (S^{\otimes n+2})^\times \\ & x & \mapsto & \prod_{i \in [n+1]_0} \varepsilon_i^n(x)^{-1^i}. \end{array}$$

[2] `https://git.disroot.org/montessiel/vector-bundles-sagemath`

R-algebros S Amitsuro kompleksas yra tokia grupių homomorfizmų seka:

$$S^\times \xrightarrow{\partial^0_{Am}} (S^{\otimes 2})^\times \xrightarrow{\partial^1_{Am}} (S^{\otimes 3})^\times \xrightarrow{\partial^2_{Am}} \dots$$

Su $n \in \mathbb{Z}_{\geq 0}$ galime nustatyti $Z^n_{Am}(R,S) = \operatorname{Ker} \partial^n_{Am}$, o jei $n \geq 1$, $B^n_{Am}(R,S) = \operatorname{Im} \partial^{n-1}_{Am}$. Jei $c \in S^{\otimes 3}$, Amitsuro algebra $A(S,c)$ apibrėžiama kaip R-modulis $S^{\otimes 2}$ su sandauga

$$xy = \operatorname{Tr}^1_1(\varepsilon^1_2(x)c\varepsilon^1_0(y)), \tag{i}$$

kur Tr^1_1 yra pėdsako atvaizdis $S^{\otimes 3} \to S^{\otimes 2}$, kur $S^{\otimes 3}$ laikomas $S^{\otimes 2}$-algebra per homomorfizmą $\varepsilon^1_1 \colon S^{\otimes 2} \to S^{\otimes 3}$.

Įvairūs Teoremos B teiginiai įrodomi išsamiais algebriniais skaičiavimais, tačiau pagrindinis argumentas grindžiamas izomorfizmų seka, atsirandančia išplečiant skaliarus į S. Tai yra, bet kuriai R-algebrai A leidžiame, kad A_S būtų S-algebra $A \otimes_R S$. Tuomet parodome, kad

$$A(S,c)_S \simeq A(S_S, c \otimes 1) \simeq \operatorname{End}_S(S_S).$$

Daugelis rezultatų apie R-algebrą $A(S,c)$ išplaukia iš S-algebros $\operatorname{End}_S(S_S)$.

Teorema C įrodymas susideda iš dviejų dalių. Algoritmo, skirto Amitsur algebrų sandaugoms apskaičiuoti, egzistavimas tiesiogiai išplaukia iš formulės (i) ir iš to, kad

$$\operatorname{Tr}^1_1(a_0 \otimes a_1 \otimes a_2) = \operatorname{Tr}_{S/R}(a_1)a_0 \otimes a_2.$$

Norint gauti tam tikros centrinės paprastosios algebros išraiškią per Amitsuro algebrą, remiamės dviem faktais:

1. Jei A yra centrinė paprastoji k-algebra, elementai $u \in A$, tokie, kad $K = k[u]$ yra maksimalus algebros A komutatyvusis poalgebris, ir $v \in A$, tokie, kad $A = KvK$, gali būti efektyviai apskaičiuoti.

2. Kai u, K ir v apibrėžti kaip aukščiau, gauname izomorfizmą $K^{\otimes 2} \simeq A$, atvaizduojantį $a_0 \otimes a_1$ į $a_0 v a_1$. Norint rasti $c \in K^{\otimes 3}$, kad algebros A sandauga atitiktų formulę (i), užtenka išspręsti tiesinių lygčių sistemą.

Teoremos D įrodymas remiasi polinominio kvantinio algoritmo, skirto skaičiuoti S-vienetų grupes skaičių kūne, egzistavimu [9]. Įrodome teoremą, apibendrinančią straipsnio [29] 7 teoremą mūsų Amitsuro kohomologijos nustatymui. Tai yra, įrodome, kad jei $c \in B^2_{Am}(k,K)$, tai egzistuoja tam tikros aibės $S^{(1)}, S^{(2)}$ atitinkamų vietų iš $K^{\otimes 2}$ ir $K^{\otimes 3}$ tokių, kad c yra algebros $K^{\otimes 3}$ $S^{(2)}$-vienetų grupėje, o pirmavaizdis a pagal ∂^1_{Am} yra algebros $K^{\otimes 2}$

$S^{(1)}$-vienetų grupėje. Kadangi tokios vienetų grupės yra baigtai generuojamos abelinės grupės, atvaizdį ∂^1_{Am}, kai jis yra ribotas, galima laikyti tiesiniu atvaizdžiu tarp $\mathbb{Z}$-modulių, o pirmavaizdį galima apskaičiuoti naudojant esamus tiesinės algebros virš $\mathbb{Z}$ algoritmus. Pažymime, kad priklausomybė nuo apidenbrintosios Rymano hipotezės atsiranda dėl to, kad $S^{(n)}$ turi apimti visas vietas, esančias virš K vietų aibės, kuri generuoja jo klasės grupę. Apibentrintoji Rymano hipotezė duoda polinominį viršutinį rėžį skaičių kūno, taigi ir etalinės algebros virš skaičių kūno, klasės grupės generatorių aibės minimalaus dydžio apribojimą.

Mūsų pateiktas [29, 7 teorema] apibendrinimo įrodymas atitinka Fiekerio įrodymo struktūrą, tačiau dėl bendresnių sąlygų susiduriame su naujais sunkumais. Pagrindinė pirminio įrodymo lema, [29, 9 lema], yra išnykimo teorema apie kūnų daliklių grupių H^1 grupes. Tai yra Hilberto 90 teoremos apie H^1 grupės trivialumą kūno daugiamačiai grupei apibendrinimas. Mūsų atveju turime dirbti ne tik su skaičių kūnais, bet ir su etalinėmis algebromis virš skaičių kūnų. Todėl turime įvesti etalinės algebros vietų ir daliklių apibrėžimus ir įrodyti kai kuriuos pagrindinius rezultatus, kurių nepavyko rasti literatūroje.

Teoremą E nesunku gauti iš apibrėžimų. Gardelių poras patogu vaizduoti skaičiavimo būdu, nes tokios yra $\mathcal{O}_{fi}$ ir $\mathcal{O}_\infty$-gardelės. Iš tiesų, $\mathcal{O}_{fi}$ yra Dedekindo sritis, todėl $\mathcal{O}_{fi}$-gardelė yra formos $\mathfrak{a}_1 x_1 \oplus \ldots \oplus \mathfrak{a}_n x_n$, kur $\mathfrak{a}_i$ yra trupmeniniai $\mathcal{O}_{fi}$-idealai kūne k, o x_i sudaro erdvės k^n bazę. Tokią gardelę galima pavaizduoti matricos $GL_n(k)$ ir dalinių frakcinių $\mathcal{O}_{fi}$-idealų rinkinio $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ duomenimis. Kadangi žiedas $\mathcal{O}_\infty$ yra pagrindinių idealų sritis, $\mathcal{O}_\infty$-gardelė turi bazę ir gali būti pavaizduota matrica $GL_n(k)$.

Keletas algoritmų, pateiktų teoremoje F, tiesiogiai išplaukia iš apibrėžimų. Kai kuriems kitiems reikia sudėtingesnių metodų, kurie aptariami toliau. Toliau gardelės poros L atveju atitinkama $\mathcal{O}_{fi}$-gardelė žymima L_{fi}, o atitinkama $\mathcal{O}_\infty$-gardelė žymima L_∞.

- Teiginyje 9 apskaičiuojame gardelės poros L H^0 grupę. Tai Rymano-Rocho problemos funkcijų kūnų dalikliams apibendrinimas. Mūsų metodas remiasi Popovo redukuotos matricos formos skaičiavimu virš $F(X)$ ir yra straipsnio [45] metodo apibendrinimas. Pažymime, kad šis metodas taip pat naudojamas straipsnyje [46] maksimalių eilių porai $F(X)$-algebroje, kuri yra atskiras gardelės poros atvejis. Įrodome, kad $H^0(L) = L_{fi} \cap L_\infty$, tinklelių sankirtą apskaičiuojame naudodami Popovo redukuotą pagrindą L_{fi} pagrindo L_∞ atžvilgiu. Popovo redukuotasis pagrindas yra analogiškas ortogonaliojo $\mathbb{Z}$-modulio pagrindui ir leidžia paprastai

apskaičiuoti $L_{fi} \cap L_\infty$ kaip mažų gardelės L_{fi} elementų aibę.

- Teiginyje 10 pirmos kohomologinės grupės $H^1(L)$, priklausančiai rango n gardelių porai L, skaičiavimas sukelia daugiau sunkumų. Pritaikius straipsnio [94] metodą, gardelės poros H^1 grupė apibrėžiama kaip F-vektorinė erdvė $R_k^n/(L' + k^n)$, kur R_k yra kūno k reparticijų žiedas, o L' yra tam tikra gardelė, esanti erdvėje R_k^n ir apibrėžta gardelių pora L. Dėl to kyla keletas sunkumų: žiedo R_k elementai yra begaliniai kūno k elementų rinkiniai, todėl paprastai jų negalima pateikti apskaičiavimo būdu. Taip pat nėra akivaizdaus būdo patikrinti, ar išreiškiami erdvės R_k^n elementai yra toje pačioje ekvivalentumo klasėje, arba sukurti pilną likinių sistemą. Akivaizdžiausias būdas apeiti šiuos sunkumus yra remtis Sero dualumu, kuris duoda izomorfizmą tarp grupės $H^1(L)$ ir dualios F-vektorinės erdvės, priklausančios erdvei $H^0(L'')$, kur L'' yra gardelių pora, apibrėžta L. Nors to pakanka, kad apskaičiuotume erdvės $H^1(L)$ F-dimensiją, mums reikia, kad erdvės $H^1(L)$ elementai būtų išreikšti kaip reparticijų vektorių liekanų klasės, tam kad galėtume apskaičiuoti gardelių porų plėtinius (žr. teiginį 11). Tam pasiekti, mes linearizuojame išreikštinę Sero dualumo formulę, apribodami ją erdvės R_k^n poaibiu, kuris yra baigtinės dimensijos F-vektorinė erdvė. Tuomet galime efektyvai apskaičiuoti elementų, priklausančių H erdvės dualiai erdvei, pirmvaizdžius ir gauti elementų, priklausančių kiekvienai $H^1(L)$ ekvivalentumo klasei, skaičiavimo reiškimą.

- Tegul ξ yra vektorių grižčių plėtinys apimantis kreivę X, kurį pateikia tikslioji seka

$$0 \to G \to E \to F \to 0.$$

  Tiesoginį gyvatės lemos taikymą komutatyviai diagramai, sudarytai naudojant vektorių grižčių $\mathcal{H}om(F, G)$, $\mathcal{H}om(F, E)$ ir $\mathcal{H}om(F, F)$ glebiąsias rezoliucijas, galime susieti su plėtiniu ξ grupės $H^1(\mathcal{H}om(F, G))$ elementu, kurio aprašas kaip adelinių vektorių liekanų klasės pats savaime duoda išreikštinį $\mathrm{LP}(E)$ aprašą.

- Homomorfizmų branduolių ir atvaizdžių skaičiavimas yra tiesoginis rezultatų apie Hermito normaliąją formą taikymas.

- Vektorių grižčių, taigi ir gardelių porų kategorija, yra Krulo-Šmito kategorija [4]. Iš čia išplaukia, kad tai, kaip gardelių pora suskyla kaip neskaidžiųjų objektų tiesoginė suma, visiškai priklauso nuo jos

endomorfizmų algebros struktūros. Iš tikrųjų, tegu A yra F-endomorfizmų algebros gardelių poros L puspaprastė faktor-algebra. Turime izomorfizmą

$$A \simeq M_{n_1}(D_1) \oplus \ldots \oplus M_{n_s}(D_s),$$

kur D_i yra F-algebros su dalyba. Tada L turi tokį skaldymo modelį:

$$L \simeq L_1^{n_1} \oplus \ldots \oplus L_s^{n_s},$$

kur L_i yra neskaidi, o D_i yra gardelių poros L_i endomorfizmo algebros puspaprastas santykis. Todėl gardelių poros skaldymo apskaičiavimas susiveda į jo endomorfizmo algebros skaičiavimo uždavinį, jo puspaprastės faktor-algebros centrinių idempotentų skaičiavimo uždavinį, ir po to šių idenpotentinių endomorfizmų vaizdų skaičiavimą. Endomorfizmo algebra yra gardelių porų homomorfizmų erdvė H^0, todėl ji yra apskaičiuojama pritaikant Teiginius 6 ir 9 iš Teoremos F. Algebros struktūros virš baigtinio kūno skaičiavimas yra nagrinėjamas straipsnyje [70]. Galiausiai, galime apskaičiuoti endomorfizmų vaizdus, remiantis Teiginiu 13 iš Teoremos F.

- Kai bazinis kūnas F yra pakankamai didelis (t. y. didesnis nei L rangas), izomorfizmą tarp gardelių porų galima rasti imant atsitiktinius homomorfizmus. Atlikus pakankamai bandymų, izomorfizmas yra randamas, arba yra labai didelė tikimybė, kad dvi gardelių poros nėra izomorfinės. Kai bazinis kūnas yra mažas, apskaičiuojant abiejų įvesties gardelės porų skaidymo schemą, problema susiveda į izomorfizmų tarp neskaidžių objektų skaičiavimą. Tai savo ruožtu atliekama apskaičiuojant jų tiesioginės sumos endomorfizmų algebros struktūrą. Iš tiesų, jei abi gardelės poros yra izomorfinės, tai endomorfizmo algebros puspaprastas santykis turės formą $M_2(D)$, kur D yra F-algebra su dalyba, o morfizmas, atitinkantis $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, yra izomorfizmas. Kita vertus, jei gardelių poros nėra izomorfinės, endomorfizmo algebros puspaprastas santykis bus formos $D_1 \oplus D_2$, o D_i F-algebros su dalyba.

Naujumas

Mūsų pristatomos Amitsuro algebros yra naujos, nors centrinių paprastųjų algebrų ir Azumajos algebrų išraiškos naudojant Amitsuro (arba etalinę) kohomologiją jau yra žinomi [2, 14, 18, 73]. Mūsų konstrukcija išsiskiria tuo, kad

bendrumą aukojame dėl praktiškumo: daugyba Amitsuro algebroje yra tiesoginės formulės su apibrėžiančiu Amitsuro kociklu rezultatas. Šia Amitsuro algebros išraiška apibendrina esamus ciklinių ir kryžminių sandaugų išraiškus ir iš tikrųjų yra ekvivalentus Brauerio algebros išraiškai [55]. Mūsų išraiškas tenkina Teoremą C, tačiau cikliniai ir kryžminių sandaugų išraiškai tenkina tik pirmąjį teoremos teiginį. Tam tikros centrinės paprastosios algebros ciklinei (arba kryžminio sandaugų) išraiškai apskaičiuoti reikia žinoti maksimalų komutatyvųjį poalgebrį, kuris yra bazinio kūno ciklinis plėtinys (arba Galua plėtinys). Kiek mums žinoma, nėra efektyvaus algoritmo tokiam poalgebriui apskaičiuoti.

Kita vertus, nors teoriškai Brauerio išraiškos konstravimui reikia žinoti tik bet kurį maksimalų komutatyvųjį poalgebrį, Brauerio algebros ir Brauerio faktoraibės yra išreiškiamos šio poalgebrio normalaus skiliojo kūno elementais. Aritmetinės statistikos rezultatai rodo, kad su didele tikimybe laipsnio d matricinės algebros atsitiktinis maksimalus komutatyvusis poalgebris yra bazinio kūno plėtinys su Galois grupe $\mathfrak{S}_d$ [28]. Toks plėtinys normaliame skiliame kūne yra meskaičiuotinas, nes tokio kūno laipsnis yra $d!$. Taigi, tai kad abu Teoremos C teiginiai galioja, yra nauja mūsų Amitsuro algebros konstrukcijos savybė.

Teorema D iš esmės yra straipsnių [29, 82] rezultatų apibendrinimas iki Amitsuro kohomologijos. Nors mūsų naudojamas įrodymo metodas yra analogiškas [29, 7 teoremos] įrodymui, mūsų prielaidos sukelia papildomus sunkumus. Iš tiesų, tai reikalauja etalinių algebrų divizorių virš globalių laukų teorijos ir jų skaidymo elgsenos. Nors mūsų įrodomi ir naudojami rezultatai, be abejo, labai prieinami specialistams, literatūroje nepavyko aptikti nuorodos į juos, taigi jie gali būti įdomūs patys savaime.

Kiek mums žinoma, literatūroje nėra sąlyginio polinominio kvantinio algoritmo, skirto išreikštinio izomorfizmo problemai skaičių laukuose spręsti. Žinomi klasikiniai algoritmai arba yra orientuoti į ribotas problemos versijas (apribojant bazinį lauką arba algebros laipsnį), arba turi eksponentinį sudėtingumą pagal kai kuriuos parametrus. Todėl mūsų algoritmas yra pirmasis polinominis kvantinis algoritmas, sprendžiantis išrekštinio izomorfizmo problemą skaičių laukuose esant teisingai apibendrintai Rymano hipotezei.

Vektorių grižčių virš projekcinių kreivių skaičiavimai yra nagrinėjami kaip atskiri skaičiavimų su koherentinais pluoštais virš projekcinių schemų atvejai, kai algoritmai, naudojantys Gröbnerio bazes, išplaukia iš koherentinų pluoštų kaip graduotų modulių Sero aprašymo [78]. Tai, pavyzdžiui, yra Sagemath

ir Magma [10, 89] atvejis. Buvo sukurta ir daugiau efektyvių metodų tokių pluoštų kohomologinių grupių skaičiavimui, žr., pavyzdžiui, [27, 61, 83].

Mūsų metodas yra siauresnis, tačiau leidžia taikyti labiau specializuotus algoritmus ir reiškimus . Mūsų žiniomis, metodas, išreiškiantis skaičiavimo būdu vektorių grižtes kaip gardelių poras, yra naujas. Mūsų vektorių grižčių reiškimas kaip gardelės virš integralinių pertvarų žiedo yra artimas nepublikuoto Vengo darbo apie taip vadinamąsias adeliškas vektorių grižtes idėjoms [93]. 0-nės kohomologijos grupių skaičiavimas yra žinomų metodų, skirtų Rymano-Rocho erdvėms [45] ir eilių sankirtoms [46] skaičiuoti, apibendrinimas. Mūsų metodas, skirtas išreikštiniam Sero dualumo izomorfizmų skaičiavimui, taip pat yra naujas.

Išvada

Šioje disertacijoje mes pristatome centrinių paprastųjų algebrų išraišką, pagrįstą Amitsuro kohomologija, kurios vienas iš rezultatų yra efektyvus skaičiavimas. Jei yra teisinga apibendrintoji Rymano hipotezė, šią išraišką panaudojome polinominiam kvantiniam algoritmui, kuris išsprendžia išreikštinio izomorfizmo problemą. Taip pat pristatome vektorių grįžčių virš normaliųjų projekcinių kreivių skaičavimo išraišką ir algoritmus, kurie sprendžia daugelį natūralių uždavinių.

Pastaroji konstrukcija susijusi su išreikštinio izomorfizmo problema pagal metodą, aprašytą 5.3.1 sekcijoje. Turėdami šią priemonę, tolimesniuose tyrimuose ketiname pasinaudoti žinomais rezultatais apie vektorių grįžčių struktūrą virš kreivių, turinčių teigamą rūšį, tam kad pateiktume išreikštinio izomorfizmo uždavinio algoritmus globaliųjų funkcijų laukams. Kita tolimesnio darbo perspektyva - polinominių algoritmų, skirtų Hermito normaliosioms formoms pseudomatricoms virš globalaus funkcijų lauko žiedo $\mathcal{O}_{fi}$ skaičiuoti, paieškos.

Amitsuro algebros turi potencialo tolimesniems tyrimams. Amitsuro išreikštinio izomorfizmo uždavinio versiją galima polinomiškai suvesti į bendrąjį aiškaus izomorfizmo uždavinį, o pastarajam uždaviniui spręsti nėra žinomo efektyvaus klasikinio algoritmo globaliuose laukuose, išskyrus $F(X)$. Šie faktai rodo, kad išreikštinio izomorfizmo uždavinys gali būti naudojamas kaip sunkus kriptografijos uždavinys (žr. [53], kuriame pateikta panašiu uždaviniu pagrįsta identifikavimo schema). Problema, kaip surasti kokraščio pirmavaizdį per grupės homomorfizmą $\partial^1 \colon C^1_{Am}(k, K) \to B^2_{Am}(k, K)$, tiesiogiai redukuojama į išreikštinio izomorfizmo problemą, kai grupės $B^2_{Am}(k, K)$ elementai

koduoja problemos atvejį, o grupės $C^1_{Am}(k, K)$ elementai koduoja sprendimo liudininkus. Ši idėja gali būti naudinga kuriant kriptografinius protokolus.

Aprobacija

Autoriaus pristatymai

1. Finding Nontrivial Zeros of Quadratic Forms over Rational Function Fields of Characteristic 2. International Symposium on Symbolic and Algebraic Computation, Lilio universitetas, Prancūzija, 2022 liepos mėn.

2. The Explicit Isomorphism Problem. Arithmetic Geometry Seminar, Bairoito universitetas, Vokietija, 2023 sausio mėn.

3. The Splitting Problem in Central Simple Algebras. 19th Atelier PARI/GP 2024, Liono ENS, Prancūzija, 2024 sausio mėn.

Bendraautorių pristatymai

1. Explicit Isomorphisms of Quaternion Algebras over Quadratic Global Fields. Algorithmic Number Theory Symposium XV. Bristolio universitetas, Jungtinė Karalystė, 2022 liepos mėn. Péterio Kuto prezentacija.

Kiti tarptautiniai renginiai, kuriuose dalyvavo autorius

1. Isogeny-based Cryptography School. Virtuali erdvė, 2021 liepos mėn.

2. Isogeny-based Cryptography Workshop. Birmingemo universitetas, Jungtinė Karalyste, 2022 kovo mėn.

3. Park City Mathematics Institute Graduate Summer School: Number Theory Informed by Computation. Park Sitis, Juta, JAV, 2022 leipos mėn.

Publikacijos

Doktorantūros studijų metu autorius paskelbė šiuos straipsnius:

1. Tímea Csahók, Péter Kutas, Mickaël Montessinos and Gergely Zábrádi. Finding Nontrivial Zeros of Quadratic Forms over Rational Function

Fields of Characteristic 2. ISSAC '22—Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation, 235–244. https://doi.org/10.1145/3476446.3535485

2. Tímea Csahók, Péter Kutas, Mickaël Montessinos and Gergely Zábrádi. Explicit isomorphisms of quaternion algebras over quadratic global fields. Research in Number Theory 8, 4 (2022), 77, 24 p. https://doi.org/10.1007/s40993-022-00380-3

3. Mickaël Montessinos. Algebraic algorithms for vector bundles over curves. Journal of Algebra and its Applications, 2024. https://doi.org/10.1142/S0219498826500210

4. Péter Kutas, Mickaël Montessinos. Efficient computations in central simple algebras using Amitsur cohomology. Journal of Algebra 665 (2025), 255-281. https://doi.org/10.1016/j.jalgebra.2024.10.045

Trumpai apie autorių

Gimimo data ir vieta

1993 m. gruodžio 10 d., Nogent-le-Rotrou, Prancūzija.

Išsilavinimas

- 2011 m. Barthelemy de Laffemas gimnazija, Valansas, Prancūzija. Vidurinis išsilavinimas.
- 2014 m. La Martinière Monplaisir, Lionas, Prancūzija. Parengiamoji klasė.
- 2015 m. Liono ENS, Lionas, Prancūzija. Matematikos bakalauro laipsnis.
- 2017 m. Liono ENS, Lionas, Prancūzija. Išplėstinės matematikos magistro laipsnis. Aritmetinės geometrijos specialybė.

Darbo patirtis

- Matematikos korepetitorius, La Martinière Monplaisir parengiamoji klasė, 2015-2017.

- Matematikos mokytojas, St Anne d'Auray gimnazija, 2019-2020.
- Jaunesnysis asistentas, Vilniaus universitetas, Matematikos ir informatikos fakultetas (nuo 2023).

Publications by the author

1. Tímea Csahók, Péter Kutas, Mickaël Montessinos and Gergely Zábrádi. Finding Nontrivial Zeros of Quadratic Forms over Rational Function Fields of Characteristic 2. ISSAC '22—Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation, 235–244. https://doi.org/10.1145/3476446.3535485

2. Tímea Csahók, Péter Kutas, Mickaël Montessinos and Gergely Zábrádi. Explicit isomorphisms of quaternion algebras over quadratic global fields. Research in Number Theory 8, 4 (2022), 77, 24 p. https://doi.org/10.1007/s40993-022-00380-3

3. Mickaël Montessinos. Algebraic algorithms for vector bundles over curves, Journal of Algebra and its Applications, 2024. https://doi.org/10.1142/S0219498826500210

4. Péter Kutas, Mickaël Montessinos. Efficient computations in central simple algebras using Amitsur cohomology. Journal of Algebra 665 (2025), 255-281. https://doi.org/10.1016/j.jalgebra.2024.10.045

NOTES

NOTES

NOTES

Vilniaus universiteto leidykla
Saulėtekio al. 9, III rūmai, LT-10222 Vilnius
El. p. info@leidykla.vu.lt, www.leidykla.vu.lt
bookshop.vu.lt, journald.vu.lt
Tiražas 20 egz.