PhD-FSTM-2025-008
Faculty of Science, Technology and Medicine

Faculty of Science

DISSERTATION

Defence held on 5 February 2025 in Leiden

to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG

EN MATHÉMATIQUES

AND

DOCTOR AAN DE UNIVERSITEIT LEIDEN

by

Flavio PERISSINOTTO
Born on 9 June 1995 in (Italy)

On the degree of Kummer extensions for commutative algebraic groups

Dissertation defence committee

Prof. Dr Antonella PERUCCA, Supervisor
Associate professor in Mathematics, UNIVERSITÉ DU LUXEMBOURG / Esch-sur-Alzette / Luxembourg

Prof. Peter STEVENHAGEN, Co-Supervisor
UNIVERSITEIT LEIDEN / Leiden / Netherlands

Prof. Gabor WIESE, Chair
Full professor in Mathematics, UNIVERSITÉ DU LUXEMBOURG / Esch-sur-Alzette / Luxembourg

Prof. Dr Davide LOMBARDO, Vice-Chair
Professor, UNIVERSITÀ DI PISA / Italy

Dr Peter BRUIN, Member
Assist. Professor, UNIVERSITEIT LEIDEN / The Netherlands

Prof. Dr René SCHOOF, Member
Professor, UNIVERSITÀ DI ROMA TOR VERGATA / Italy

ON THE DEGREE OF KUMMER EXTENSIONS FOR COMMUTATIVE ALGEBRAIC GROUPS

Proefschrift

ter verkrijging van
de graad van doctor aan de Universiteit Leiden,
op gezag van rector magnificus prof. dr. ir. H. Bijl,
volgens besluit van het college voor promoties
te verdedigen op woensdag 5 februari 2025
klokke 10.00 uur

door

Flavio Perissinotto
geboren te Motta di Livenza, Italië
in 1995

Promotor:

Prof.dr. P. Stevenhagen

Copromotor:

Dr. A. Perucca (University of Luxembourg)

Promotiecommissie:

Prof.dr.ir. G.L.A. Derks

Prof.dr. M. Fiocco

Prof.dr. F. Pappalardi (Università Roma Tre)

Prof.dr. R.J. Schoof (Università Roma Tor Vergata)

Dr. P. Moree (Max Planck Institut für Mathematik, Bonn)

Research financially supported by the University of Luxembourg through the Luxembourg National Research Fund (PRIDE17/1224660/GPS) and by the University of Leiden.

Contents

Introduction

Let K be a field for which we fix an algebraic closure $\overline{K}$ and let A be a commutative connected algebraic group over K. Let G be a finitely generated subgroup of $A(K)$. For a positive integer n, we may consider the n-torsion field $K(A[n])$ and the field $K(\frac{1}{n}G)$, which is the minimal field extension of K over which all elements $\beta \in A(\overline{K})$ such that $n\beta \in G$ are defined. The extension $K(\frac{1}{n}G)/K(A[n])$ is a Galois extension called *Kummer extension*, and the aim of this thesis is to study its degree for specific choices of K and A. The following cases will be considered: in Chapter 2, A is the multiplicative group and K is a multiquadratic or a quartic cyclic number field; in Chapter 3, A is any product of one-dimensional algebraic tori over a number field K; in Chapter 4, A is the multiplicative group and K is a finite extension of $\mathbb{Q}_p$ for a prime p; in Chapter 5, A is an abelian variety and K is a number field. Each of these four chapters is the content of a research paper, whose main results involve explicit computations or effective bounds for the degree of Kummer extensions.

If $A = \mathbb{G}_m$ is the multiplicative group, and if n is coprime to the characteristic of K, we are dealing with classical Kummer theory (see for example [Lan02, Sec.VI.8] and [Bir67]), which was first developed by Ernst Kummer in the 19th century in his celebrated work on Fermat's Last Theorem. If K is a field containing the n-th roots of unity for some positive integer n, the main result of Kummer theory (see Theorem 1.0.1) characterizes the abelian extensions of exponent dividing n. These extensions are called Kummer extensions and, if their degree is finite, they are of the form $K(\sqrt[n]{G})/K$ for some finitely generated subgroup G of $K^\times$.

Kummer extensions of number fields, and in particular their degree, have found important applications more recently in the study of certain density problems. Let K be a number field, let $\alpha \in K^\times$ and fix some prime number ℓ. Consider the set of primes $\wp$ of K for which the reduction of α modulo $\wp$ is well-defined and has multiplicative order coprime to ℓ (or more generally the order has a prescribed ℓ-valuation). This set admits natural density, and this density can be expressed in terms of the degrees of cyclotomic-Kummer extensions $K(\zeta_n, \sqrt[n]{\alpha})/K$, where n is some power of ℓ. This problem was first studied in the sixties by Hasse in [Has65, Has66] and recently explicit fomulas for

the density, also in the more general case of reductions of a subgroup G of $K^\times$, were given by Perucca, Debry and Sgobba in their papers [DP16] and [PS19]. This motivated Perucca to delve into the computation of degrees of Kummer extensions for number fields in a more general setting, namely for any extension $K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)$ where n, N are positive integers such that $n \mid N$. Perucca, Sgobba, Tronto and Hörmann proved that these degrees can be explicitly computed at once for all n, N in [PST21], and developed algorithms in the case $K = \mathbb{Q}$ in [PST20] and in the case K is a quadratic number field in [HPST21], whose outputs are formulas for the degrees with a finite case distinctions. In Chapter 2 we extend this result to multiquadratic or quartic cyclic number fields, hence proving the following:

Theorem 1. *Let K be either a multiquadratic or a quartic cyclic number field. Let G be a finitely generated subgroup of $K^\times$. Then there exists an explicit finite procedure to compute at once the degrees*

$$[K(\zeta_N, \sqrt[n]{G}) : K(\zeta_N)]$$

for all positive integers n, N such that n divides N.

One of the latest results on Kummer extensions for number fields [ACP+25] went beyond the study of their degrees with the computation of the size of each cyclic component of the Galois group of $K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)$ for all n, N with n dividing N. Motivated by the results on number field, we extended the problem of the computation of the degree of Kummer extensions also to other fields. If K is a finite field, then such computation is straightforward (see [PP24a]). If K is a p-adic field, namely a finite extension of $\mathbb{Q}_p$, formulas for the degrees can be given explicitly, using similar techniques as the ones used for number fields but with some substantial differences that come from structure of the multiplicative group of p-adic fields. This is the content of Chapter 4, where we prove the following:

Theorem 2. *Let p be a prime and let K be a finite extension of $\mathbb{Q}_p$. Let G be a finitely generated subgroup of $K^\times$ and let n, N be two positive integers such that $n \mid N$. Then there exists an explicit finite procedure to compute the degree $[K(\zeta_N, \sqrt[n]{G}) : K(\zeta_N)]$.*

Unlike number fields, if K is either a p-adic field or a finite field, it is not possible to compute at once all degrees for every n, N such that n divides N, unless we assume the knowledge of the multiplicative order of p in $(\mathbb{Z}/M\mathbb{Z})^\times$ for every integer M coprime to p. In this environment, it is also natural to compare local and global results. We compare Kummer extensions of number fields with the corresponding Kummer extensions of p-adic fields obtained by completion with respect to some non-zero prime ideal of their ring of integers in Chapter 4. We show that there is a positive density of primes of the number field such that the degree of the local Kummer extension is the same as the global one.

For any connected commutative algebraic group A over a number field K we may consider density problems akin to the ones for the multiplicative group. Namely, fix an element $\alpha \in A(K)$ and a prime ℓ. Consider the set of primes $\wp$ of K for which the

reduction of α modulo $\wp$ is well-defined and has order coprime to ℓ. We may investigate whether such set admits a natural density, and, if that is the case, we may want to compute such density. If b is the first Betti number of A, it can be shown that such density exists for every prime ℓ if the integer

$$f_N := \frac{N^b}{[K(\frac{1}{N}\alpha) : K(A[N])]},$$

which we call the *Kummer failure of maximality* for the degree of the Kummer extension, is bounded independently of N. If this condition is satisfied, Lombardo and Perucca [LP21] gave a non explicit formula for the density.

If $A = T$ is an algebraic torus, Bertrand [Ber88], following the work of Ribet [Rib79], proved that f_N is bounded independently of N. The density problem was studied by Perucca in the case T is one-dimensional, giving closed formulas for the density (see [Per17]). As for the multiplicative group, also in this case the density can be expressed in terms of degrees of Kummer extensions where N is a power of a prime ℓ, and Perucca provided explicit formulas for the degrees of such extensions. In Chapter 3 we take this a step further, proving the following two statements:

Theorem 3. *Let T be a finite product of one-dimensional tori defined over a number field K, and fix a finitely generated subgroup G of $T(K)$. If n, N are positive integers such that n divides N, then there is an explicit finite procedure to determine whether T is split over $K(T[N], \frac{1}{n}G)$ and to compute the degree of this field over K and over $K(T[N])$.*

Theorem 4. *Let T be a finite product of one-dimensional tori whose splitting field is a multiquadratic number field K, and fix a finitely generated subgroup G of $T(K)$. There exists an explicit finite procedure to compute at once the degree of $K(T[N], \frac{1}{n}G)/K(T[N])$, for all n, N positive integers such that n divides N.*

Let now A be an abelian variety over a number field K. As mentioned before, the primes $\wp$ of K for which the reductions of elements of $A(K)$ modulo $\wp$ have order coprime to a given prime ℓ admit a natural density if the failure of maximality f_N is uniformely bounded with respect to N. This problem (together with the one already mentioned for algebraic tori) was first studied by Ribet [Rib79], who proved the uniform boundedness of f_N as $N = \ell$ ranges over the prime numbers. He showed that the Kummer failure is trivial for all primes ℓ large enough, assuming a list of 'axioms' which were later proved by Faltings [Fal83] and Serre [Ser86]. The existence of a uniform bound for f_N as N ranges over all positive integers was proven by Bertrand [Ber88]. Hindry [Hin88] later gave a streamlined proof. In the case of elliptic curves, effective bounds for the Kummer failure are known. The work of Javan Peykar [Jav21] deals with CM elliptic curves, while the work of Tronto and Lombardo [LT22] handles the case of non-CM elliptic curves. In both cases, the effective bound is obtained by exploiting certain properties of the endomorphism ring. In his recent paper [Tro23a], Tronto refined these results, setting the foundations for possible similar results for other commutative connected algebraic groups. More precisely, he proves that, under certain conditions on the

endomorphism ring and the geometric torsion of the algebraic group (which are satisfied for elliptic curves), the Kummer failure can be bounded in terms of three independent parameters. In Chapter 5 we show that these three parameters exist for every abelian variety A over a number field and can be effectively bounded in terms of basic invariants of A/K, if A has complex multiplication over $\overline{K}$. We also show how to take care of the assumptions on the endomorphism ring and on the geometric torsion of the algebraic group of A. Ultimately, we are able to obtain bounds that only depend on the abelian variety A, on the field K, and on the divisibility of the point α (respectively, of the subgroup G of $A(K)$) for which we consider the Kummer extension.

One of the results of Chapter 5 is therefore the following:

Theorem 5. *Consider an abelian variety A defined over a number field K and with complex multiplication over $\overline{K}$. Let G be a finitely generated subgroup of $A(K)$. Suppose a set of generators of G is linearly independent over $\mathrm{End}_K(A)$ and is given in terms of a $\mathbb{Z}$-basis for $A(K)/A(K)_{\mathrm{tors}}$. There exists an effective upper bound for f_N, uniform in N and depending only on K, A and G.*

In his work on exponential Diophantine equations in the seventies, Schinzel investigated Galois groups of field extensions obtained by adjoining radicals. One of his results ([Sch77, Theorem 2], see Theorem 1.0.3), which is known as *Schinzel's theorem on radical extensions*, characterizes abelian radical extensions of a field and is an important asset in the study of Kummer extensions of fields. In Chapter 5 we look into possible analogues of Schinzel's theorem in the setting of abelian varieties. This problem lead us to the following, which generalizes a similar result for abelian varieties over $\overline{K}$ contained in a recent paper of Le Fourn, Lombardo and Zywina [LLZ23]:

Theorem 6. *Let A be an abelian variety over a number field K. The following are equivalent:*

(i) The extension $K(A[n])/K$ is abelian for every positive integer n.

(ii) The variety A is K-isogenous to a product of simple abelian varieties with CM over K.

Finally, Chapter 1 introduces Kummer theory, providing results ranging from standard theorems in the field to more advanced ones which are preparatory for the following chapters of this thesis. In particular, we will define for any field K and any prime ℓ the ℓ-adic and ℓ-adelic failures of maximality of the degree of a Kummer extension and, if K is a number field, we will define the parameters of ℓ-divisibility of a subgroup G of $K^\times$. These notions will be essential for Chapters 2, 3 and 4. Moreover, for any connected commutative algebraic group A over a number field K, we define the adelic torsion representation and the adelic Kummer representation, and we recall the theorem by Tronto which is the starting point of Chapter 5.

Samenvatting

Zij K een lichaam, $\overline{K}$ een vast gekozen algebraïsche afsluiting van K, en A een commutatieve samenhangende algebraïsche groep over K. Zij G een eindig voortgebrachte ondergroep van $A(K)$. Gegeven een positief geheel getal n, kunnen we het n-torsie lichaam $K(A[n])$ en het lichaam $K(\frac{1}{n}G)$ beschouwen, waar $K(\frac{1}{n}G)$ het minimale lichaam is waarover alle elementen $\beta \in A(\overline{K})$ zodat $n\beta \in G$ gedefiniëerd zijn. De uitbreiding $K(\frac{1}{n}G)/K(A[n])$ is dan een speciale Galoisuitbreiding, genaamd Kummeruitbreiding, en het doel van dit proefschrift is de graad van deze uitbreiding te bestuderen voor specifieke keuzes van K en A. We zullen de volgende gevallen beschouwen: in Hoofdstuk 2 is A een multiplicatieve groep en K een multikwadratisch of een vierdegraads cyclisch getallenlichaam; in Hoofdstuk 3 is A een product van één-dimensionale algebraïsche tori over een getallenlichaam K; in Hoofdstuk 4 is A een multiplicatieve groep en K een eindige uitbreiding van $\mathbb{Q}_p$ voor een priemgetal p; in Hoofdstuk 5 is A een abelse variëteit en K een getallenlichaam. Elke van deze vier hoofdstukken is de inhoud van een artikel waarvan de hoofdresultaten betrekking hebben op expliciete berekeningen of effectieve grenzen voor de graden van Kummer uitbreidingen.

Als $A = \mathbb{G}_m$ de multiplicatieve groep is, en als n en de karakteristiek van K onderling ondeelbaar zijn, dan hebben we te maken met de klassieke Kummertheorie (zie bijvoorbeeld [Lan02, Sec.VI.8] en [Bir67]), die als eerste ontwikkeld werd door Ernst Kummer in de 19de eeuw in zijn befaamde onderzoek naar de laatste stelling van Fermat. Als K een lichaam is dat de $n$de eenheidswortels bevat, voor een geheel getal n, dan karakteriseert het belangrijkste resultaat van de Kummertheorie (zie Stelling 1.0.1) alle abelse uitbreidingen met een exponent die n deelt. Deze uitbreidingen worden Kummeruitbreidingen genoemd en, als hun graad eindig is, zijn ze van de vorm $K(\sqrt[n]{G})/K$, waar G een eindig voortgebrachte ondergroep is van $K^\times$.

Kummeruitbreidingen van getallenlichamen, en in het bijzonder hun graden, hebben recent belangrijke toepassingen gevonden in de studie van bepaalde dichtheidsproblemen. Zij K een getallenlichaam, $\alpha \in K^\times$ en ℓ een priemgetal. Beschouw de verzameling van de priemgetallen $\wp$ van K waarvoor geldt dat de reductie van α modulo $\wp$ welgedefiniëerd is en een multiplicatieve orde heeft die onderling ondeelbaar is met ℓ (of, algemener, een

orde heeft met een vooraf vastgelegde ℓ- valuatie). Deze verzameling heeft een natuurlijke dichtheid en deze dichtheid kan worden uitgedrukt in de graden van de cyclotomische Kummer uitbreidingen $K(\zeta_n, \sqrt[n]{\alpha})/K$, waar n een macht is van ℓ. Dit probleem werd als eerste bestudeerd in de jaren 60 door Hasse in [Has65, Has66], en recenter zijn expliciete formules voor de dichtheid, ook in het algemenere geval van reducties van een ondergroep G van $K^\times$, gegeven door Perucca, Debry en Sgobba in hun artikelen [DP16] en [PS19]. Dit was de motivatie voor Perucca om dieper in de berekeningen van graden van Kummer uitbreidingen van getallenlichamen te duiken in algemenere situaties, namelijk voor elke uitbreiding $K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)$, waar n, N positieve gehele getallen zijn met $n \mid N$. Perucca, Sgobba, Tronto en Hörmann hebben bewezen in [PST21] dat het mogelijk is om deze graden voor alle n, N in één keer expliciet te berekenen, en ze hebben een algoritme ontwikkeld in het geval $K = \mathbb{Q}$ (zie [PST20]) en in het geval dat K een kwadratisch getallenlichaam is (zie [HPST21]), waarvan de output formules voor de graden zijn, met eindig veel gevalsonderscheidingen. In Hoofdstuk 2 breiden we dit resultaat uit naar multikwadratische en vierdegraadse cyclische getallenlichamen, en bewijzen we het volgende:

Theorem 1. *Zij K of een multikwadratisch of een vierdegraads cyclisch getallenlichaam. Zij G een eindig voortgebrachte ondergroep van $K^\times$. Dan bestaat er een expliciete, eindige procedure om, tegelijk, alle graden*

$$[K(\zeta_N, \sqrt[n]{G}) : K(\zeta_N)]$$

te berekenen, voor alle positieve gehele getallen n, N zodat N deelbaar is door n.

Een van de meest recente resultaten m.b.t. Kummeruitbreidingen van getallenlichamen (zie [ACP+25]) gaat een stapje verder dan de studie van de graden door niet alleen de graad te berekenen, maar ook de precieze grootte van elke cyclische component van de Galoisgroep van $K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)$ voor alle n, N waarvoor N deelbaar is door n. Met de resultaten voor getallenlichamen als motivatie, breiden we het probleem om de graden van Kummeruitbreidingen te berekenen uit naar andere lichamen. Als K een eindig lichaam is, dan is zo'n berekening vanzelfsprekend (zie [PP24a]). Als K een p-adisch lichaam is, d.w.z. een eindige uitbreiding van $\mathbb{Q}_p$, dan kunnen formules voor de graden expliciet gegeven worden door gebruik te maken van soortgelijke technieken als bij getallenlichamen, met een aantal aanzienlijke verschillen, die voortkomen uit de structuur van de multiplicatieve groep van p-adische lichamen. Dit is de inhoud van Hoofdstuk 4, waar we het volgende bewijzen:

Theorem 2. *Zij p een priemgetal, en K een eindige uitbreiding van $\mathbb{Q}_p$. Zij G een eindig voortgebrachte ondergroep van $K^\times$ en n, N twee positieve gehele getallen zodat $n \mid N$. Dan bestaat er een eindige procedure om de graad $[K(\zeta_N, \sqrt[n]{G}) : K(\zeta_N)]$ te berekenen.*

In tegenstelling tot getallenlichamen, als K of een p-adisch lichaam of een eindig lichaam is, is het niet mogelijk om alle graden voor alle n, N, zodat n niet N deelt, in één keer te berekenen, behalve als we aannemen dat de multiplicatieve orde van p

in $(\mathbb{Z}/M\mathbb{Z})^\times$ bekend is voor alle gehele getallen M die onderling ondeelbaar zijn met p. Het is een logische vervolgstap om dan de lokale en globale resultaten te vergelijken. We vergelijken, in Hoofdstuk 4, Kummeruitbreidingen van getallenlichamen met de corresponderende Kummer uitbreidingen van p-adische lichamen die verkregen worden door vervollediging met betrekking tot een (niet-nul) priemideaal in de ring van de gehele getallen. We laten zien dat er een positieve dichtheid van priemgetallen in het getallen lichaam is, zodat de graad van de lokale Kummer uitbreiding hetzelfde is als die van de globale uitbreiding.

Voor elke samenhangende commutatieve algebraïsche groep A over een getallenlichaam K kunnen we een dichtheidsprobleem beschouwen van dezelfde aard als dat voor multiplicatieve groepen. Namelijk, neem een element $\alpha \in A(K)$ en een priemgetal ℓ. Beschouw de verzameling van de priemgetallen $\wp$ in K zodat de reductie van α modulo $\wp$ welgedefiniëerd is en zodat zijn orde onderling ondeelbaar is met ℓ. Men kan zich dan afvragen of zo'n verzameling een natuurlijke dichtheid heeft, en, zo ja, of we die kunnen berekenen. Als b het eerste Betti getal is van A, dan kan worden aangetoond dat zo'n dichtheid bestaat voor elk priemgetal ℓ zolang het gehele getal

$$f_N := \frac{N^b}{[K(\frac{1}{N}\alpha) : K(A[N])]},$$

dat we het *Kummer falen van maximaliteit* noemen, begrensd is, onafhankelijk van N. Onder deze voorwaarde, hebben Lombardo en Perucca [LP21] een niet-expliciete formule voor de dichtheid gegeven.

In het geval dat $A = T$ een algebraïsche torus is, heeft Bertrand [Ber88], als vervolgwerk op Ribet [Rib79], bewezen dat f_N begrensd is, onafhankelijk van N. Dit dichtheidsprobleem is bestudeerd door Perucca in het geval dat T ééndimensionaal is, en Perucca heeft expliciete formules gegeven voor de dichtheid (zie [Per17]). Net zoals voor de multiplicatieve groep, kan ook in dit geval de dichtheid uitgedrukt worden in de graden van Kummeruitbreidingen, waar N een macht is van een priemgetal ℓ, en Perucca heeft expliciete formules voor de graden van dit soort uitbreidingen gegeven. In Hoofdstuk 3 gaan we nog een stapje verder, door de volgende twee beweringen te bewijzen:

Theorem 3. *Zij T een eindig product van eendimensionale tori, gedefinieerd over een getallenlichaam K, en neem een eindig voortgebrachte ondergroep G van $T(K)$. Als n, N twee gehele positieve getallen zijn zodat N deelbaar is door n, dan is er een eindige, expliciete procedure om te bepalen of T gesplitst is over $K(T[N], \frac{1}{n}G)$ en om de graad te berekenen van dit lichaam over zowel K als over $K(T[N])$.*

Theorem 4. *Zij T een eindig product van eendimensionale tori waarvoor het splijtlichaam een multikwadratisch getallenlichaam K is, en neem een eindig voortgebrachte ondergroep G van $T(K)$. Er bestaat een eindige, expliciete procedure om, in één keer, alle graden $K(T[N], \frac{1}{n}G)/K(T[N])$ te berekenen, voor alle n, N positieve gehele getallen zodat N deelbaar is door n.*

Zij nu A een abelse variëteit over een getallenlichaam K. Zoals eerder vermeld heeft de verzameling de priemgetallen $\wp$ van K waarvoor de reductie van de elementen van $A(K)$ modulo $\wp$ een orde heeft onderling ondeelbaar met een gegeven priemgetal ℓ een natuurlijke dichtheid als het falen van maximaliteit f_N uniform begrensd is met betrekking tot N. Dit probleem (samen met het reeds genoemde probleem voor algebraïsche tori) is als eerste bestudeerd door Ribet [Rib79], die bewees dat de f_N uniform begrensd is als $N = \ell$ over alle priemgetallen loopt. Hij liet zien dat het Kummerfalen triviaal is voor alle voldoend grote priemgetallen ℓ, onder de aanname van een aantal "axioma's" die later bewezen werden door Faltings [Fal83] en Serre [Ser86]. Het bestaan van een uniforme grens van f_N wanneer N over alle gehele getallen loopt is bewezen door Bertrand [Ber88]. Hindry [Hin88] heeft later een gestroomlijnd bewijs gegeven. In het geval van elliptische krommen zijn effectieve grenzen voor het Kummerfalen bekend. Het werk van Javan Peykar [Jav21] betreft CM elliptische krommen, en het werk van Tronto en Lombardo [LT22] betreft het geval van niet-CM elliptische krommen. In beide gevallen is de effectieve grens verkregen door bepaalde eigenschappen van de endomorfismenring uit te buiten. In een recent artikel [Tro23a] verfijnt Tronto zijn resultaten, en weet hij de fundamenten te leggen voor mogelijke soortgelijke resultaten voor andere commutatieve samenhangende algebraïsche groepen. Preciezer, hij bewijst dat, onder bepaalde voorwaarden voor de endomorfismenring en de geometrische torsie van de algebraïsche groep (beide voorwaarden zijn vervuld in het geval van elliptische krommen), het Kummerfalen begrensd kan worden in termen van drie onafhankelijke parameters. In Hoofdstuk 5 laten we zien dat deze drie parameters bestaan voor elke abelse variëteit A over een getallenlichaam en dat deze effectief begrensd kunnen worden in termen van basisinvarianten van A/K, als A complexe vermenigvuldiging over $\overline{K}$ heeft. Uiteindelijk verkrijgen we grenzen die alleen afhangen van de abelse variëteit A, het lichaam K, en de deelbaarheid van het punt α (respectievelijk, van de ondergroep G van $A(K)$) waarvoor we de Kummer uitbreiding beschouwen.

Een van de resultaten van Hoofdstuk 5 is dan ook het volgende:

Theorem 5. *Beschouw een abelse variëteit A gedefiniëerd over een getallenlichaam K met complexe vermenigvuldiging over $\overline{K}$. Zij G een eindig voortgebrachte ondergroep van $A(K)$. Neem aan dat een verzameling van voortbrengers van G lineair onafhankelijk is over $\mathrm{End}_K(A)$ en gegeven is in termen van een $\mathbb{Z}$-basis voor $A(K)/A(K)_{\mathrm{tors}}$. Er bestaat dan een effectieve bovengrens voor f_N, uniform in N en alleen afhankelijk van K, A en G.*

In zijn werk over exponentiële Diophantische vergelijkingen in de jaren zeventig onderzocht Schinzel Galoisgroepen van lichaamsuitbreidingen verkregen door wortels toe te voegen. Een van zijn resultaten ([Sch77, Theorem 2], zie Stelling 1.0.3), karakteriseert abelse radicaaluitbreidingen van een lichaam en is onmisbaar in de studie van Kummer uitbreidingen. In Hoofdstuk 5 kijken we naar mogelijke analogieën van de stelling van Schinzel in de context van abelse variëteiten. Dit probleem leidt ons tot de volgende stelling, die een resultaat voor abelse variëteiten over $\overline{K}$ in een recent artikel van Le Fourn, Lombardo en Zywina [LLZ23] generaliseert:

Theorem 6. *Zij A een abelse variëteit over een getallenlichaam K. De volgende beweringen zijn dan equivalent:*

(i) De uitbreiding $K(A[n])/K$ is abels voor elk positief geheel getal n.

(ii) De variëteit A is K-isogeen met een product van simpele abelse variëteiten met complexe vermenigvuldiging over K.

Tenslotte wordt in Hoofdstuk 1 Kummertheorie geïntroduceerd, met resultaten variërend van de standaardstellingen in dit gebied, tot meer geavanceerde stellingen die voorbereiden op de andere hoofdstukken in dit proefschrift. In het bijzonder, zullen we voor elk lichaam K en elk priemgetal ℓ het ℓ-adische en ℓ-adelische falen van maximaliteit van de graad van een Kummer uitbreiding definiëren. Ook zullen we, als K een getallenlichaam is, de parameters van ℓ-deelbaarheid van een ondergroep G van $K^\times$ definiëren. Deze begrippen zullen onmisbaar zijn voor de hoofdstukken 2, 3 en 4. Bovendien definiëren we voor elke samenhangende commutatieve algebraïsche groep A over een getallenlichaam K de adelische torsierepresentatie en de adelische Kummerrepresentatie, en brengen we de stelling van Tronto in herinnering die het uitgangspunt vormt van hoofdstuk 5.

CHAPTER 1

Basic notions of Kummer theory

Let K be a field and fix an algebraic closure $\overline{K}$ of K. Fix a positive integer n coprime to the characteristic of K and let a be an element in $K^\times$. We denote by ζ_n a fixed root of unity of order n in $\overline{K}$ (in general the choice does not matter, but when we write ζ_n and ζ_{nt} we sometimes choose $\zeta_n = \zeta_{nt}^t$). If K contains the n-th roots of unity, then the extension $K(\sqrt[n]{a})/K$ obtained adjoining the n-th roots of a is clearly a Galois extension as $K(\sqrt[n]{a})$ is the splitting field of $x^n - a$ and is cyclic of order dividing n. Kummer theory states that, if $\zeta_n \in K$, every cyclic extension of K of order dividing n is the splitting field of $x^n - a$ for some element $a \in K^\times$.

More generally, the following holds (see [Lan02, Sec. VI.8]):

Theorem 1.0.1. *Let K be a field and n a positive integer coprime to $\mathrm{char}(K)$. Suppose that K contains the n-th roots of unity. Then for an extension L/K the following are equivalent:*

(i) L/K is abelian with exponent dividing n

(ii) $L = K(\sqrt[n]{G})$ for some subgroup $(K^\times)^n \subseteq G \subseteq K^\times$

Moreover, if L/K satisfies the equivalent conditions, the bilinear map

$$\begin{aligned} \mathrm{Gal}\left(L/K\right) \times G/(K^\times)^n &\to \mu_n \\ (\sigma, a) &\mapsto \frac{\sigma(\alpha)}{\alpha} \end{aligned} \tag{1.1}$$

is a perfect pairing, where α is any choice of n-th root of a. This pairing exhibits a Pontryagin duality between $\mathrm{Gal}(L/K)$ as profinite group and the group $G/(K^\times)^n$ endowed with the discrete topology.

We define any extension satisfying the equivalent conditions of Theorem 1.0.1 a *Kummer extension*.

Remark 1.0.2. If a Kummer extension L/K is finite, then the subgroup G of $K^\times$ such that $L = K(\sqrt[n]{G})$ is finitely generated. In this situation, the fact that (1.1) is a perfect pairing leads to the following group isomorphism:

$$\mathrm{Gal}\left(L/K\right) \cong {G(K^\times)^n}/{(K^\times)^n}$$

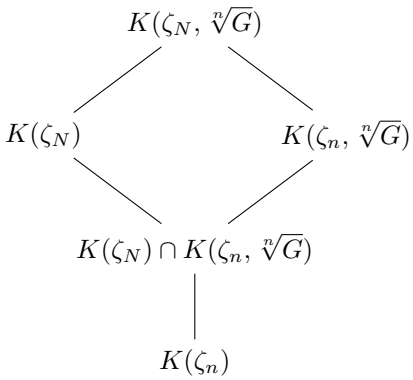
If K does not contain the n-th roots of unity, then the extension L/K where L is the splitting field of $x^n - a$ for some element $a \in K^\times$ is in general not an abelian extension. Indeed, $L = K(\zeta_n, \sqrt[n]{a})$ is abelian over $K(\zeta_n)$, but its Galois group is a subgroup of $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$. In this situation, the following result by Schinzel characterises the abelian extensions:

Theorem 1.0.3 ([Sch77, Theorem 2])**.** *Let K be a field and n a positive integer coprime to $\mathrm{char}(K)$. Let $a \in K^\times$. The Galois group of the splitting field of $x^n - a$ is abelian if and only if there exists an element $b \in K^\times$ such that $a^w = b^n$ where w is the largest divisor of n such that K contains the w-th roots of unity.*

In general, for any field K, any pair of positive integers n, N with n dividing N and any finitely generated subgroup G of $K^\times$ we may want to study Kummer extensions of the form

$$K(\zeta_N, \sqrt[n]{G})/K(\zeta_N). \tag{1.2}$$

Notice first that, if the group G is generated by r elements, the Galois group of such Kummer extension is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^r$ and hence its degree divides n^r. It is useful then to look at the following diagram of field extensions:



It follows that, given the prime decomposition $n = \prod \ell^m$, we have:

$$\begin{aligned} \mathrm{Gal}\left(\frac{K(\zeta_N, \sqrt[n]{G})}{K(\zeta_N)}\right) &\cong \mathrm{Gal}\left(\frac{K(\zeta_n, \sqrt[n]{G})}{K(\zeta_N) \cap K(\zeta_n, \sqrt[n]{G})}\right) \\ &\cong \prod_{\ell | n} \mathrm{Gal}\left(\frac{K(\zeta_{\ell^m}, \sqrt[\ell^m]{G})}{K(\zeta_N) \cap K(\zeta_{\ell^m}, \sqrt[\ell^m]{G})}\right) \end{aligned} \tag{1.3}$$

where the last isomorphism is simply the decomposition of the Galois group into its maximal ℓ-subgroups. If we want to only study the degree of the extension, it is useful to consider the integer

$$f_{N,n} := \frac{n^r}{[K(\zeta_N, \sqrt[n]{G}) : K(\zeta_N)]}$$

which we call the *failure of maximality* for the degree of the Kummer extension. Using the same decomposition of (1.3), we can write:

$$f_{N,n} = \prod_{\ell | n} f_{\ell^m, \ell^m} \cdot B(N, \ell^m) \tag{1.4}$$

where

$$B(N, \ell^m) = [K(\zeta_N) \cap K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) : K(\zeta_{\ell^m})].$$

We call the *ℓ-adic failure* the integer f_{ℓ^m, ℓ^m} and we call the *ℓ-adelic failure* the integer $B(N, \ell^m)$, which measures the so-called entanglement between the Kummer extension and the cyclotomic extension. Clearly, both f_{ℓ^m, ℓ^m} and $B(N, \ell^m)$ are powers of ℓ.

1.1 Kummer theory for number fields

Let now K be a number field. We fix here some notation that will be used throughout the thesis. We denote by μ_K the subgroup of $K^\times$ consisting of the roots of unity. For a positive integer n, we denote by μ_n the group of n-th roots of unity in $\overline{K}$. We also write $\mu_\infty = \cup_n \mu_n$ and, if ℓ is a prime number, $\mu_{\ell^\infty} = \cup_m \mu_{\ell^m}$. If N is a non-zero integer and ℓ is a prime number, then we write $v_\ell(N)$ for the ℓ-adic valuation. If $\alpha \in K^\times$ and $\wp$ is a prime of K (by which we mean a non-zero prime ideal of the ring of integers of K), then $v_\wp(\alpha)$ is the $\wp$-adic valuation of the fractional ideal generated by α.

In this section we describe the divisibility properties of elements in $K^\times$ and more in general of finitely generated subgroups of $K^\times$ in terms of the divisibility parameters. If G is a finitely generated subgroup of $K^\times$, knowledge of its divisibility parameters allows us to compute at once all the degrees of Kummer extensions $K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)$ for all integers $n \mid N$ and the structure of their Galois groups (namely, the size of all cyclic components), see Theorem 1.1.10.

Let $a \in K^\times$. The natural notion of divisibility consists in checking whether a is a n-th power in K for some positive integer n but, for the purpose of Kummer theory, it is useful to consider divisibility up to roots of unity in K. Fix a prime ℓ. If a is such that ζa is not an ℓ-th power in K for any $\zeta \in \mu_K \cap \mu_{\ell^\infty}$, we say that a is *strongly ℓ-indivisible*.

Proposition 1.1.1 ([DP16, Proposition 9]). *Let $a \in K^\times$ be strongly ℓ-indivisible and suppose ℓ is odd or $\zeta_4 \in K$. For any non-negative integer m, the element a is strongly ℓ-indivisible in $K(\zeta_{\ell^m})$.*

Any element $a \in K^\times$ can be written as $a = \zeta_{\ell^h} b^{\ell^d}$ for some non-negative integers h and d, where ζ_{ℓ^h} is a root of unity of order ℓ^h and b is a strongly ℓ-indivisible element in $K^\times$. The integers d and h are called the *parameters for ℓ-divisibility* of the element a. Notice that h is uniquely determined if we impose the restriction that either $h = 0$ or $h > \max(0, v_\ell(\#\mu_K) - d)$.

Consider now finitely many elements $a_1, \cdots, a_r \in K^\times$. We say that $a_1, \cdots, a_r$ are *strongly ℓ-independent* if the element $a_1^{e_1} \cdots a_r^{e_r}$ is strongly ℓ-indivisible whenever $e_1, \cdots, e_r$ are integers not all divisible by ℓ. Let G be a finitely generated and torsion free subgroup of $K^\times$ of rank r. The following result lets us choose a basis of G through which we define the parameters for ℓ-divisibility for the group.

Theorem 1.1.2 ([DP16, Theorem 14]). *There is a basis $\{b_1, \cdots, b_r\}$ of G such that $b_i = B_i^{\ell^{d_i}} \zeta_i$ holds for some strongly ℓ-independent elements $B_1, \cdots, B_r$ of $K^\times$, for some non-negative integers $d_1, \cdots, d_r$ and for some roots of unity $\zeta_i \in \mu_K$ of order ℓ^{h_i}.*

For a basis of G as in Theorem 1.1.2, we say that the tuple of non-negative integers

$$(d_1, \cdots, d_r; h_1, \cdots, h_r)$$

represents the *parameters for ℓ-divisibility for the group G*. In particular, $d_1, \cdots, d_r$ are the d-parameters for ℓ-divisibility, and $h_1, \cdots, h_r$ are the h-parameters for ℓ-divisibility. The d-parameters are unique up to reordering, while the h-parameters are in general not unique, but can be made unique with additional restrictions (see [DP16, Appendix A.2]). Moreover, for almost all primes ℓ, all parameters of ℓ-divisibility for the group G can be taken to be 0, as consequence of the following result:

Theorem 1.1.3 ([PS19, Theorem 2.7]). *There exists a basis of G whose elements are strongly ℓ-independent for all but finitely many primes ℓ.*

The following results allows us to compute the degree and the structure of the Galois group $K(\zeta_{\ell^m}, \sqrt[\ell^m]{G})/K(\zeta_{\ell^m})$ (and hence the ℓ-adic failure f_{ℓ^m,ℓ^m}) for all positive integers m at once:

Theorem 1.1.4 ([DP16, Theorem 18]). *Suppose that ℓ is odd or $\zeta_4 \in K$. Let $t \geqslant 1$ be the largest integer such that $K(\zeta_\ell) = K(\zeta_{\ell^t})$. Let M, m be positive integers with $M \geqslant \max(t, m)$. Then we have*

$$v_\ell([K(\zeta_{\ell^M}, \sqrt[\ell^m]{G}) : K(\zeta_{\ell^M})]) = \max(0, \max_i(h_i - \delta_i + m - M)) + \delta_1 + \cdots + \delta_r$$

where $(d_1, \cdots, d_r; h_1, \cdots, h_r)$ are parameter for ℓ-divisibility of G in K and $\delta_i := \max(m - d_i, 0)$.

Theorem 1.1.5 ([ACP+25, Theorem 6 and Remark 12]). *Suppose that ℓ is odd or $\zeta_4 \in K$. Let $t \geqslant 1$ be the largest integer such that $K(\zeta_\ell) = K(\zeta_{\ell^t})$. Let M, m be positive integers with $M \geqslant \max(t, m)$. There exists an algorithm to compute the structure of the Galois group of the Kummer extension $K(\zeta_{\ell^M}, \sqrt[\ell^m]{G})/K(\zeta_{\ell^M})$. This structure only depends on the parameters for ℓ-divisibility of G over K, and the integers m and $\max(M, t)$. Moreover, we need to apply the algorithm above only finitely many times to compute the structure of the Galois group of $K(\zeta_{\ell^m}, \sqrt[\ell^m]{G})/K(\zeta_{\ell^m})$ at once for all $m \geqslant 1$.*

To extend Theorem 1.1.4 and Theorem 1.1.5 to the remaining case where $\ell = 2$ and $\zeta_4 \notin K$, we can investigate $K(\zeta_{2^M}, \sqrt[2^m]{G})/K(\zeta_{2^M})$ by replacing the field K by $K(\zeta_4)$. The only case left is when $M = m = 1$, for which we easily conclude thanks to the following lemma and the fact that $K(\sqrt{G})/K$ has exponent 2.

Lemma 1.1.6 ([DP16, Lemma 19]). *We have $[K(\sqrt{G}) : K] = e[K(\zeta_4, \sqrt{G}) : K(\zeta_4)]$ where $e = 2$ if G contains minus a square in $K^\times$ and $e = 1$ otherwise.*

Consider now, for a prime ℓ and positive integers m, N such that $\ell^m \mid N$, extensions of the form

$$(K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) \cap K(\zeta_N))/K(\zeta_{\ell^m}) \tag{1.5}$$

and their degree, which we called the ℓ-adic failure and we denoted by $B(N, \ell^m)$. This extension is a finite Kummer extension over $K(\zeta_{\ell^m})$, and therefore by Remark 1.0.2 there exists a subgroup H_{N,ℓ^m} of G such that:

$$K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) \cap K(\zeta_N) = K(\zeta_{\ell^m}, \sqrt[\ell^m]{H_{N,\ell^m}}). \tag{1.6}$$

Remark 1.1.7. By Theorem 1.0.3 we have

$$K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) \cap K(\zeta_N) = K(\zeta_{\ell^m})$$

for all primes ℓ such that $\ell \nmid \#\mu_K$, as the field $K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) \cap K(\zeta_N)$ is an abelian extension of K, obtained as the splitting field over K of a finite family of polynomials of the form $x^{\ell^m} - g$.

For the finitely many primes dividing $\#\mu_K$ we may use the following:

Theorem 1.1.8 ([PST21, Proposition 3.2 and Lemma 3.4]). *There exists a computable integer N_0 depending on ℓ, K and G such that, for every $m \geqslant t_0 := v_\ell(N_0)$ and $N \geqslant 1$ with $\ell^m \mid N$, we have*

$$K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) \cap K(\zeta_N) = (K(\zeta_{\ell^{t_0}}, \sqrt[\ell^{t_0}]{G}) \cap K(\zeta_{\gcd(N,N_0)}))(\zeta_{\ell^m})$$

and hence

$$B(N, \ell^m) = B(\gcd(N, N_0), \ell^{t_0}) \quad \textit{and} \quad H_{N,\ell^m} = H_{N_0,\ell^{t_0}}.$$

The following Proposition allows us to explicitly determine the groups H_{N,ℓ^m}:

Proposition 1.1.9. *Let $t = v_\ell(\#\mu_K)$, and let $\alpha \in K^\times$. For a prime ℓ, write $\alpha = \zeta_{\ell^h}\beta^{\ell^d}$, where $\beta \in K^\times$ is strongly ℓ-indivisible, d and h are the parameters for ℓ divisibility of α and either $h = 0$ or $t - d < h \leqslant t$. We define s to be the non-negative integer such that $\sqrt[\ell^s]{\beta} \in K(\mu_\infty)$ and $\sqrt[\ell^{s+1}]{\beta} \notin K(\mu_\infty)$. Then, for every positive integer m the following holds:*

$$K(\zeta_{\ell^m}, \sqrt[\ell^m]{\alpha}) \cap K(\mu_\infty) = \begin{cases} K(\zeta_{\ell^{m+h}}), & \text{if } 1 \leqslant m \leqslant d; \\ K(\zeta_{\ell^m}, \zeta_{\ell^{m+h}}\sqrt[\ell^{m-d}]{\beta}), & \text{if } d < m < d+s; \\ K(\zeta_{\ell^{h+d+s}}\sqrt[\ell^s]{\beta}), & \text{if } d+s \leqslant m < h+d+s; \\ K(\zeta_{\ell^m}, \sqrt[\ell^s]{\beta}), & \text{if } m \geqslant h+d+s. \end{cases}$$

Proof. If $m \leqslant d$, the statement is clear as $K(\sqrt[\ell^m]{\alpha}) = K(\zeta_{\ell^{m+h}})$. If $d < m < d+s$, then:

$$K(\zeta_{\ell^m}, \sqrt[\ell^m]{\alpha}) = K(\zeta_{\ell^m}, \zeta_{\ell^{m+h}}\sqrt[\ell^{m-d}]{\beta})$$

is contained in $K(\mu_\infty)$ as $m - d < s$. If $m \geqslant d+s$, then

$$K(\zeta_{\ell^m}, \sqrt[\ell^m]{\alpha}) = K\left(\zeta_{\ell^m}, \sqrt[\ell^{m-d-s}]{\zeta_{\ell^{h+d+s}}\sqrt[\ell^s]{\beta}}\right)$$

The element $\zeta_{\ell^{h+d+s}}\sqrt[\ell^s]{\beta}$ is contained in $K(\mu_\infty)$, but $\zeta_{\ell^{h+d+s+1}}\sqrt[\ell^{s+1}]{\beta}$ is not, as $\sqrt[\ell^{s+1}]{\beta} \notin K(\mu_\infty)$. This implies that $K(\zeta_{\ell^m}, \sqrt[\ell^m]{\alpha}) \cap K(\mu_\infty)$ is generated over $K(\zeta_m)$ by $\zeta_{\ell^{h+d+s}}\sqrt[\ell^s]{\beta}$.

□

Theorem 1.1.8 implies that, for the primes $\ell \mid \#\mu_K$, we are able compute the ℓ-adelic failure $B(N, \ell^m)$ and the structure of the Galois group of the extension 1.5 for all pairs (m, N) such that $\ell^m \mid N$ by computing them only for the finitely many pairs (m, N) with $m \leqslant t_0$ and $N \mid N_0$. To compute the group structure of the Galois group of the extension for a pair (m, N) we apply Theorem 1.1.5 with the group H_{N,ℓ^m} using the identity (1.6). We can therefore conclude:

Theorem 1.1.10. *Let K be a number field and let G be a finitely generated and torsion free subgroup of $K^\times$. Then the structure of the Galois group (and in particular of the degree) of the Kummer extension $K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)$ can be computed for all positive integers n, N with $n \mid N$ at once.*

Proof. If G has rank r, Theorem 1.1.3 implies that $f_{\ell^m,\ell^m} = \ell^{mr}$ for almost all primes ℓ. The computation of the degree is then an easy consequence of formula (1.4), Theorem 1.1.4 and Theorem 1.1.8. The structure of the Galois group can be determined applying Theorem 1.1.5 to the extensions:

$$\frac{K(\zeta_{\ell^m}, \sqrt[\ell^m]{G})}{K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) \cap K(\zeta_N)} = \frac{K(\zeta_{\ell^m}, \sqrt[\ell^m]{G})}{K(\zeta_{\ell^m}, \sqrt[\ell^m]{H_{N,\ell^m}})}$$

using the parameters for ℓ-divisibility of G over the field $K(\zeta_{\ell^m}, \sqrt[\ell^m]{H_{N,\ell^m}})$. For almost all primes ℓ, Theorem 1.1.3 and [ACP+25, Remark 13] imply that such group is

isomorphic to $(\mathbb{Z}/\ell^m\mathbb{Z})^r$. Using Theorem 1.1.8 for the remaining primes, we may then reduce to finitely many computations. □

The computation of $f_{N,n}$ can be made very explicit when K is $\mathbb{Q}$ or a quadratic number field (see [PST20] and [HPST21]). More specifically, algorithms can be described to compute $f_{N,n}$ for all n, N with $n \mid N$ at once, where the output is an explicit formula with a finite case distinction. The algorithm for $K = \mathbb{Q}$ was implemented in SageMath (see [Tro19])

1.2 Kummer theory for algebraic groups

Let A be a connected commutative algebraic group over a number field K, and let $\alpha \in A(K)$. Fix an algebraic closure $\overline{K}$ of K. For a positive integer N we denote by $[N]$ the multiplication by N endomorphism of A and by $A[N]$ the subgroup of N-torsion points of $A(\overline{K})$, which is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^b$, where b is the first Betti number of A. We denote by $K(A[N])$ the smallest extension of K on which the N-th torsion points are defined, and by $K(\frac{1}{N}\alpha)$ the smallest extension of K on which all points $\beta \in A(\overline{K})$ such that $N\beta = \alpha$ are defined. Clearly, $K(A[N]) \subseteq K(\frac{1}{N}\alpha)$. The analogue of Kummer extensions defined in the setting of fields at the beginning of this chapter are then field extensions of the form

$$K\left(\frac{1}{N}\alpha\right)/K(A[N]). \tag{1.7}$$

To study such extensions, we rely on Galois representations. We recall the construction of torsion and Kummer representations attached to A/K and α (see for example [LP21] and [LT22]).

For every integer N, we fix a basis $\{t_1^N, \cdots, t_b^N\}$ of $A[N]$ such that $Nt_i^M = t_i^{M/N}$ whenever $N \mid M$. Similarly, we fix a set of points $\{\beta^N\}_{N\in\mathbb{Z}_{>0}} \subseteq A(\overline{K})$ such that $\beta^1 = \alpha$ and $N\beta^M = \beta^{M/N}$ whenever $N \mid M$.

We denote by τ_N the *N-torsion representation*:

$$\tau_N : G_K \to \mathrm{Aut}(A[N])$$

given by the natural $\mathbb{Z}/N\mathbb{Z}$-linear Galois action of G_K on $A[N]$. Since we fixed a basis for $A[N]$, the Galois group of $K(A[N])/K$ can be identified with the image of τ_N, and hence with a subgroup of $\mathrm{GL}_b(\mathbb{Z}/N\mathbb{Z})$.

We denote by κ_N the *N-Kummer representation*:

$$\begin{aligned}\kappa_N : G_{K(A[N])} &\to A[N]\\ \sigma &\mapsto \sigma(\beta^N) - \beta^N.\end{aligned}$$

Notice that this definition does not depend on the choice of β^N, as σ is the identity on $K(A[N])$. Again, the Galois group of $K(\frac{1}{N}\alpha)/K(A[N])$ can be identified with the image of κ_N, and hence with a subgroup of $(\mathbb{Z}/N\mathbb{Z})^b$. It is then clear that the degree of the

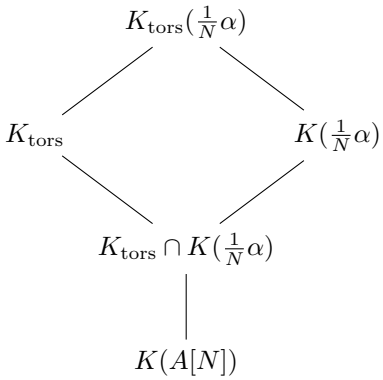
extension (1.7) is bounded by N^b, and hence we may define the *failure of maximality* for the degree of the extension as the integer

$$f_N := \frac{N^b}{\#\operatorname{Im}(\kappa_N)}.$$

We define the adelic Tate module of A, denoted by $T(A)$, as the projective limit over N of the groups $A[N]$, which is isomorphic to $\hat{\mathbb{Z}}^b$. We denote by K_{tors} the compositum of all $K(A[N])$ and by K_{kum} the compositum of all $K(\frac{1}{N}\alpha)$. By taking the inverse limit over N for τ_N and κ_N, we obtain the *adelic torsion representation* $\tau_\infty : G_K \to \operatorname{Aut}(T(A))$ and the *adelic Kummer representation* $\kappa_\infty : G_{K_{\mathrm{tors}}} \to T(A)$.

We can therefore identify the Galois group of the extension K_{tors}/K with $\operatorname{Im}(\tau_\infty)$ and hence with a subgroup of $\mathrm{GL}_b(\hat{\mathbb{Z}})$, and the Galois group of the extension $K_{\mathrm{kum}}/K_{\mathrm{tors}}$ with $\operatorname{Im}(\kappa_\infty)$ and hence with a subgroup of $\hat{\mathbb{Z}}^b$.

Remark 1.2.1 ([LT22, Remark 2.6])**.** The following diagram shows that the Galois group of $K_{\mathrm{tors}}(\frac{1}{N}\alpha)/K_{\mathrm{tors}}$ is isomorphic to the Galois group of $K(\frac{1}{N}\alpha)/K_{\mathrm{tors}} \cap K(\frac{1}{N}\alpha)$, and hence is a subgroup of $\operatorname{Im}(\kappa_N)$.



We have therefore that

$$f_N \Big| \frac{N^b}{\#\operatorname{Gal}\left(K_{\mathrm{tors}}(\frac{1}{N}\alpha)/K_{\mathrm{tors}}\right)}$$

and, if $\operatorname{Im}(\kappa_\infty)$ is an open subgroup of $T(A)$,

$$f_N \mid [T(A) : \operatorname{Im}(\kappa_\infty)]$$

Theorem 1.2.2 ([Ber88, Theorem 1])**.** *Let A be the product of an abelian variety by a torus. Assume that $\alpha \in A(K)$ is such that the set of its multiples $\mathbb{Z}\alpha$ is Zariski dense in A. Then $\operatorname{Im}(\kappa_\infty)$ is open in $T(A)$, and hence f_N is uniformly bounded in N.*

With the extra condition for the $\operatorname{End}_K(A)$-module of geometric torsion points $A(\overline{K})_{\mathrm{tors}}$ to be injective, the following theorem gives a criterion to decide whether $\operatorname{Im}(\kappa_\infty)$ is an open subgroup of $T(A)$, and if this is the case gives a bound for its index.

Theorem 1.2.3 ([Tro23a, Theorem 5.4])**.** *Let A be a connected commutative algebraic group over a number field K. Let $\alpha \in A(K)$ be such that $\mathbb{Z}\alpha$ is Zariski dense in A and let $\Gamma := \{\beta \in A(\overline{K}) \mid \exists n \in \mathbb{Z}_{\geqslant 1} : n\beta \in \langle\alpha\rangle\}$. Assume that $A(\overline{K})_{\mathrm{tors}}$ is an injective $\mathrm{End}_K(A)$-module. Suppose that there exist positive integers d, n, m such that:*

1. *$d(\Gamma \cap A(K)) \subseteq \langle\alpha\rangle + A(K)_{\mathrm{tors}}$;*
2. *$n \cdot H^1(\mathrm{Im}(\tau_\infty), A(\overline{K})_{\mathrm{tors}}) = 0$;*
3. *the subring of $\mathrm{End}(A(\overline{K})_{\mathrm{tors}})$ generated by $\mathrm{Im}(\tau_\infty)$ contains $m \cdot \mathrm{End}(A(\overline{K})_{\mathrm{tors}})$.*

Then $\mathrm{Im}(\kappa_\infty)$ contains $(dnm \cdot \hat{\mathbb{Z}})^b$.

Theorem 1.2.3 can be applied in the case A is an elliptic curve. In this case, explicit values of d, n, m can be found, and hence the bound is explicit:

Corollary 1.2.4 ([Tro23a, Theorem 5.11])**.** *Let A be an elliptic curve over a number field K and let $\alpha \in A(K)$ is given in terms of a basis of $A(K)/A(K)_{\mathrm{tors}}$. Then there exists an effectively computable positive constant c such that the index of $\mathrm{Im}(\kappa_\infty)$ in $T(A)$ divides c. In particular, f_N divides c for any integer N.*

CHAPTER 2

Kummer theory for multiquadratic or quartic cyclic number fields

This chapter is based on the joint work with Antonella Perucca [PP22], and its main focus is to investigate Kummer theory for a multiquadratic or quartic cyclic number field K (to ease notation we always consider quadratic number fields to be multiquadratic) and to prove the following theorem:

Theorem 2.0.1. *Let K be either a multiquadratic or a quartic cyclic number field. Let G be a finitely generated subgroup of $K^\times$. Then there exists an explicit finite procedure to compute at once the degrees*

$$[K(\zeta_N, \sqrt[n]{G}) : K(\zeta_N)]$$

for all positive integers n, N such that n divides N.

To achieve this we fully describe the procedure mentioned in the statement, and we prove various results that classify the intersection between the Kummer extensions and the cyclotomic extensions of K. Since our results can be applied to study further number theoretical questions, we give here an overview.

We investigate the cyclic Kummer extensions of K that are abelian over $\mathbb{Q}$ or, equivalently, that are contained in a cyclotomic extension of K (for K multiquadratic, see Sections 2.4–2.5; for K quartic cyclic, see Section 2.6). In Theorem 2.2.1 we classify the

intersection of $K(\zeta_{\ell^m}, \sqrt[\ell^m]{\alpha})$ with the cyclotomic extensions of K where $\alpha \in K^\times$ and ℓ^m is any prime power. Lemma 2.3.1 and Lemma 2.6.1 (for multiquadratic and quartic cyclic number fields respectively) allow us to determine those positive integers x such that $K(\zeta_x)$ contains $\sqrt{\pm 2}$ or some given root of unity with order a power of 2.

For certain multiquadratic number fields, Lemmas 2.3.4 and 2.3.6 (see also Lemma 2.8.4 for $\mathbb{Q}(\zeta_5)$) allow us to classify all cyclic Kummer extensions of degree 4 and 8 which are contained in a cyclotomic extension of K. See also Lemma 2.3.2 to determine whether a Kummer extension is Galois over $\mathbb{Q}$.

For multiquadratic number fields, we investigate in Theorem 2.4.1 the quadratic extensions of K, more precisely which positive integers x are such that $K(\zeta_x)$ contains these extensions. In Theorems 2.5.1 and 2.5.2 we deal with the same problem for the cyclic extensions of K of degree 4 (if $\zeta_4 \in K$) and of degree 8 (if $\zeta_8 \in K$).

For quartic cyclic number fields we may check whether a quadratic extension is abelian over $\mathbb{Q}$ thanks to Lemma 2.6.2. Then in Theorems 2.6.3 and 2.6.5 we determine those positive integers x such that $K(\zeta_x)$ contains such an extension. See also Lemma 2.6.6.

Finally, Propositions 2.4.2, 2.4.3, 2.5.3 (for multiquadratic number fields) and Propositions 2.6.4, 2.6.7 (for quartic cyclic number fields) allow us to compute the positive integers x for which $K(\zeta_x)$ contains elements of the form $\zeta_{2^n}\sqrt{\beta}$, $\zeta_{2^n}\sqrt[4]{\beta}$, $\zeta_{2^n}\sqrt[8]{\beta}$ with $\beta \in K^\times$. See also Propositions 2.8.1, 2.8.3 which are related to the prime numbers 3 and 5 instead.

To prove Theorem 2.0.1, by [HPST21, Section 8] we may replace G by one element $\alpha \in K^\times$ which is not a root of unity, and we consider the Kummer extension

$$K(\zeta_N, \sqrt[n]{\alpha})/K(\zeta_N) \tag{2.1}$$

for all positive integers n, N such that n divides N. Recall by Chapter 1 that, instead of computing the degree of these extensions, we can focus on computing the *failure of maximality* $f_{N,n}$ for the degree of the Kummer extension. If $n = \prod \ell^m$ is the prime decomposition of n, we have

$$f_{N,n} := \frac{n}{[K(\zeta_N, \sqrt[n]{\alpha}) : K(\zeta_N)]} = \prod_{\ell \mid n} f_{\ell^m,\ell^m} \cdot B(N, \ell^m)$$

where f_{ℓ^m,ℓ^m} is the *ℓ-adic failure* and $B(N, \ell^m)$ is the *ℓ-adelic failure*, namely:

$$B(N, \ell^m) := \left[K(\zeta_{\ell^m}, \sqrt[\ell^m]{\alpha}) \cap K(\zeta_N) : K(\zeta_{\ell^m})\right].$$

By Theorem 1.1.4 we can compute at once, with explicit formulas, all ℓ-adic failures f_{ℓ^m,ℓ^m} where ℓ is a prime number and $m \geqslant 1$, so we only need to provide formulas for the ℓ-adelic failure $B(N, \ell^m)$.

As mentioned in Chapter 1, [PST20] and [HPST21] describe a finite procedure for the computation of the ℓ-adelic failure over $\mathbb{Q}$ and over quadratic number fields. Now we consider number fields which are either multiquadratic or quartic cyclic, and we provide

an explicit finite procedure to compute the ℓ-adelic failure $B(N, \ell^m)$ for all prime numbers ℓ, all $m \geqslant 1$, and for all $N \geqslant 1$ such that ℓ^m divides N, see Sections 2.7 and 2.8. By Remark 1.1.7 we have $B(N, \ell^m) = 1$ if $\zeta_\ell \notin K$. Thus for all considered number fields we investigate the 2-adelic failure; if K is multiquadratic and $\zeta_3 \in K$, then we also study the 3-adelic failure; for the quartic field $\mathbb{Q}(\zeta_5)$ we also study the 5-adelic failure.

Finally, we have the following:

Remark 2.0.2. Theorem 2.0.1 also holds for all number fields that have no quadratic subfields (in particular, it holds for all number fields of odd degree).

Indeed, the above discussion is still valid hence it suffices to study the 2-adelic failure, see Section 2.7.

2.1 Preliminaries

Squarefree numbers, multiples, and divisors can be negative integers. The same holds for the *squarefree part* of a non-zero integer (i.e. the squarefree integer that multiplied by the given integer is a square) and for the *odd squarefree part* (i.e. the odd squarefree integer which multiplied by a power of 2 is the squarefree part). When we say that an integer is *minimal*, then we always mean that it is minimal w.r.t. divisibility.

Let K be a number field. If the extension $K/\mathbb{Q}$ is abelian, we define the *conductor* c_K of K to be the minimal positive integer n such that $K \subseteq \mathbb{Q}(\zeta_n)$.

Lemma 2.1.1. *Consider a number field Q and two finite abelian extensions K/Q and K'/Q which are linearly disjoint. A quadratic subextension of KK'/Q which is not contained in K or K' is of the form $Q(\sqrt{dd'})$ for some $d, d' \in Q$ such that $\sqrt{d} \in K \setminus Q$ and $\sqrt{d'} \in K' \setminus Q$.*

Proof. If L is a quadratic subextension of KK'/Q which is not contained in K or K', then it suffices to prove that it is contained in $L_K L_{K'}$, where $L_K \subseteq K$ and $L_{K'} \subseteq K'$ are quadratic over Q. Consider the quadratic character

$$\chi : \mathrm{Gal}(KK'/Q) \to \{\pm 1\}$$

corresponding to L: composing χ with the natural embedding

$$\mathrm{Gal}(K/Q) \hookrightarrow \mathrm{Gal}(K/Q) \times \mathrm{Gal}(K'/Q) \cong \mathrm{Gal}(KK'/Q)$$

we get a character $\chi_K : \mathrm{Gal}(K/Q) \to \{\pm 1\}$. Since $L \not\subseteq K$, the character χ_K is quadratic and corresponds to a quadratic subextension L_K/Q. We similarly define $\chi_{K'}$ and $L_{K'}$. The kernel of χ is contained in the product of the kernels of χ_K and $\chi_{K'}$, and we conclude because this product corresponds to $L_K L_{K'}$. Indeed, it is the largest subgroup of $\mathrm{Gal}(KK'/Q)$ whose restriction to $\mathrm{Gal}(K/Q)$ (respectively, $\mathrm{Gal}(K'/Q)$) is contained in the kernel of χ_K (respectively, $\chi_{K'}$). □

Remark 2.1.2. Let F be the largest multiquadratic subextension of $\mathbb{Q}(\zeta_M)$, where $M \geqslant 3$. By Lemma 2.1.1, F is generated by the elements $\sqrt{\pm p}$, where $p \mid M$ is a prime such that $\pm p \equiv 1 \bmod 4$, and by ζ_4 (if $4 \mid M$), and by $\sqrt{2}$ (if $8 \mid M$). Moreover, if K is a multiquadratic number field, then KF is the largest multiquadratic subextension of $K(\zeta_M)$.

Remark 2.1.3. Let $K = \mathbb{Q}(\sqrt{d_1}, \dots \sqrt{d_r})$ for some squarefree integers $d_1, \dots, d_r$. For a non-empty subset I of $\{1, \dots, r\}$ we call d_I the squarefree part of $\prod_{i \in I} d_i$. By applying Lemma 2.1.1 the squarefree integers in $K^{\times 2}$ are the integers d_I.

Lemma 2.1.4 ([HS00, Lemma C.17 and its proof])**.** *Let K be a number field and let n be a positive integer such that $\zeta_n \in K^\times$. Let $\alpha \in K^\times$ and let $\wp$ be a prime of K.*

1. *If $v_\wp(\alpha)$ is not divisible by n, then $\wp$ ramifies in $K(\sqrt[n]{\alpha})$.*
2. *If $v_\wp(\alpha)$ is divisible by n and the prime integer below $\wp$ is coprime to n, then $\wp$ does not ramify in $K(\sqrt[n]{\alpha})$.*

Quartic cyclic number fields

A quartic cyclic number field (i.e. an abelian extension of $\mathbb{Q}$ with Galois group $\mathbb{Z}/4\mathbb{Z}$) is either a totally real or a CM field, and the quadratic subextension is totally real: for a CM quartic field embedded in $\mathbb{C}$, the quadratic subextension is the field fixed by the complex conjugation. The roots of unity contained in a quartic cyclic number field are μ_{10} for $\mathbb{Q}(\zeta_5)$, and μ_2 otherwise. In particular, for $\mathbb{Q}(\zeta_5)$ we have to study only the 2-adelic failure and the 5-adelic failure, and for the other quartic cyclic number fields only the 2-adelic failure.

Remark 2.1.5 ([HHR+87, Theorem 1 and the following lines, Theorem 3])**.** Let D be a squarefree positive integer. A quartic cyclic number field containing $\sqrt{D}$ is of the form

$$\mathbb{Q}\Big(\sqrt{A(D + B\sqrt{D})}\Big) = \mathbb{Q}\Big(\sqrt{A(D - B\sqrt{D})}\Big)$$

where A is an odd squarefree integer coprime to D and B is a positive integer such that $D - B^2$ is a square (the integers A and B exist unique). In particular, D and B cannot be both even, and (by the Sum of two squares theorem) D is not divisible by prime numbers congruent to 3 modulo 4. The conductor of the quartic cyclic number field is

$$\begin{cases} 8\,|A|\,D & \text{if } 2 \nmid B \\ 4\,|A|\,D & \text{if } A + B \equiv 3 \bmod 4 \\ |A|\,D & \text{if } A + B \equiv 1 \bmod 4\,. \end{cases}$$

In particular, A is the product of the odd prime numbers coprime to D that ramify in the quartic cyclic number field.

Let C be the positive integer such that $D = B^2 + C^2$, and notice that precisely one among the integers D, B, C is even. We define

$$\gamma = A(D + B\sqrt{D}) \qquad \text{and} \qquad \gamma' = A(D + C\sqrt{D})\,.$$

Remark 2.1.6. Suppose that $2 \mid C$. Then we have $\mathbb{Q}(\sqrt{\gamma}, \sqrt{2}) = \mathbb{Q}(\sqrt{\gamma'}, \sqrt{2})$ because we can write

$$2\frac{\gamma'}{\gamma} = \Big(\frac{(C-B) - \sqrt{D}}{B}\Big)^2\,. \tag{2.2}$$

Moreover, the conductor of $\mathbb{Q}(\sqrt{\gamma})$ is $8\,|A|\,D$, so we have $\mathbb{Q}(\zeta_{|A|D}, \sqrt{\gamma}) = \mathbb{Q}(\zeta_{|A|D}, \sqrt{\pm 2})$ and hence $\sqrt{\pm\gamma'} \in \mathbb{Q}(\zeta_{|A|D})$ for one choice of the sign.

2.2 Intersection between cyclotomic extensions and Kummer extensions

Theorem 2.2.1. *Let K be a number field, and let ℓ be a prime number. We assume that $t \in \{1,2,3\}$, where $t = v_\ell(\sharp(\mu_{\ell^\infty} \cap K))$. Let $\alpha \in K^\times \setminus \mu_\infty$, and write $\alpha = \zeta_{\ell^h}\beta^{\ell^d}$, where $\beta \in K^\times$ is strongly ℓ-indivisible, $d \geqslant 0$, and $h = 0$ or $t - d < h \leqslant t$. For $n \geqslant 1$ we describe the field*

$$K(\zeta_{\ell^n},\, \sqrt[\ell^n]{\alpha}) \cap K(\mu_\infty)\,.$$

1. *If $1 \leqslant n \leqslant d$, then it is $K(\zeta_{\ell^{n+h}})$.*

2. *If $\sqrt[\ell]{\beta} \notin K(\mu_\infty)$, then it is*

$$\begin{cases} K(\zeta_{\ell^{n+2}}) & \text{if } n = d+1,\ h = 3 \\ K(\zeta_{\ell^{n+1}}) & \text{if } n = d+1,\ h = 2 \text{ or } n = d+2,\ h = 3 \\ K(\zeta_{\ell^n}) & \text{if } n \geqslant d+h\,. \end{cases}$$

3. *If $\sqrt[\ell]{\beta} \in K(\mu_\infty)$ and $\sqrt[\ell^2]{\beta} \notin K(\mu_\infty)$, then it is*

$$\begin{cases} K(\zeta_{\ell^n}, \zeta_{\ell^{n+h}}\sqrt[\ell]{\beta}) & \text{if } n = d+1 \\ K(\zeta_{\ell^{n+2}}\sqrt[\ell]{\beta}) & \text{if } n = d+2,\ h = 3 \\ K(\zeta_{\ell^{n+1}}\sqrt[\ell]{\beta}) & \text{if } n = d+2,\ h = 2 \text{ or } n = d+3,\ h = 3 \\ K(\zeta_{\ell^n}, \sqrt[\ell]{\beta}) & \text{if } n \geqslant d+1+h\,. \end{cases}$$

4. *If $\sqrt[\ell^2]{\beta} \in K(\mu_\infty)$ and $\sqrt[\ell^3]{\beta} \notin K(\mu_\infty)$ (which implies $t \in \{2,3\}$), then it is*

$$\begin{cases} K(\zeta_{\ell^n}, \zeta_{\ell^{n+h}}\sqrt[\ell]{\beta}) & \text{if } n = d+1 \\ K(\zeta_{\ell^n}, \zeta_{\ell^{n+h}}\sqrt[\ell^2]{\beta}) & \text{if } n = d+2 \\ K(\zeta_{\ell^{n+2}}\sqrt[\ell^2]{\beta}) & \text{if } n = d+3,\ h = 3 \\ K(\zeta_{\ell^n}, \zeta_{\ell^{n+1}}\sqrt[\ell^2]{\beta}) & \text{if } n = d+3,\ h = 2 \text{ or } n = d+4,\ h = 3 \\ K(\zeta_{\ell^n}, \sqrt[\ell^2]{\beta}) & \text{if } n \geqslant d+2+h\,. \end{cases}$$

5. If $\sqrt[\ell^3]{\beta} \in K(\mu_\infty)$ *(which implies* $t = 3$*), then it is*

$$\begin{cases} K(\zeta_{\ell^n}, \zeta_{\ell^{n+h}}\sqrt[\ell]{\beta}) & \text{if } n = d+1 \\ K(\zeta_{\ell^n}, \zeta_{\ell^{n+h}}\sqrt[\ell^2]{\beta}) & \text{if } n = d+2 \\ K(\zeta_{\ell^n}, \zeta_{\ell^{n+h}}\sqrt[\ell^3]{\beta}) & \text{if } n = d+3 \\ K(\zeta_{\ell^n}, \zeta_{\ell^{n+2}}\sqrt[\ell^3]{\beta}) & \text{if } n = d+4,\ h = 3 \\ K(\zeta_{\ell^n}, \zeta_{\ell^{n+1}}\sqrt[\ell^3]{\beta}) & \text{if } n = d+4,\ h = 2 \text{ or } n = d+5,\ h = 3 \\ K(\zeta_{\ell^n}, \sqrt[\ell^3]{\beta}) & \text{if } n \geqslant d+3+h\,. \end{cases}$$

If $1 < r \leqslant h$*, then by* $\zeta_{\ell^{n+r}}$ *we mean here any* ℓ^{n+r-h}*-th root of* ζ_{ℓ^h}*.*

In the above formulas, the extension $K(\zeta_{\ell^n}, \sqrt[\ell^n]{\alpha}) \cap K(\mu_\infty)/K(\zeta_{\ell^n})$ is generated by an element of the form $\zeta_{\ell^{n+x}}\sqrt[\ell]{\beta}$ only when $n + x \geqslant t + 2$, of the form $\zeta_{\ell^{n+x}}\sqrt[\ell^2]{\beta}$ only when $n + x \geqslant t + 3$ (and $t \in \{2, 3\}$) and of the form $\zeta_{\ell^{n+x}}\sqrt[\ell^3]{\beta}$ only when $n + x \geqslant 7$ (and $t = 3$).

Proof. This is just an application of Proposition 1.1.9 in our situation.

□

2.3 Cyclotomic extensions of multiquadratic number fields

Let K be a multiquadratic number field.

Lemma 2.3.1. *Let* $K = \mathbb{Q}(\sqrt{d_1}, \ldots \sqrt{d_r})$ *for some squarefree integers* $d_1, \ldots, d_r$*. For a non-empty subset* I *of* $\{1, \ldots, r\}$ *we call* d_I *the squarefree part of* $\prod_{i\in I} d_i$*. If* $x \geqslant 1$*, then the following are necessary and sufficient conditions for the elements* ζ_{2^n} *for any* $n \geqslant 2$ *and for* $\sqrt{\pm 2}$ *to be in* $K(\zeta_x)$*:*

Element in $K(\zeta_x)$	*Equivalent condition*
ζ_{2^n} $(n \geqslant 4)$	$2^n \mid x$
ζ_8	$\zeta_4, \sqrt{2} \in K(\zeta_x)$
ζ_4	$4 \mid x$*, or* $d_I \equiv 3 \bmod 4$ *and* $d_I \mid x$ *for some* I
$\sqrt{\pm 2}$	$8 \mid x$*, or* $4 \mid x$ *and* $2 \mid d_I$ *and* $d_I \mid 2x$ *for some* I*, or* $d_I \mid 2x$ *and* $d_I \equiv \pm 2 \bmod 8$ *for some* I*.*

Proof. The assertion for ζ_{2^n} follows from the fact that $16 \nmid c_K$, and the assertion for ζ_8 is clear. It is straight-forward to prove that all given conditions are sufficient. We now apply Remarks 2.1.2–2.1.3. If $\zeta_4 \in K(\zeta_x)$ and $4 \nmid x$, then there is some squarefree $m \mid x$ such that $m \equiv 1 \bmod 4$ and $-md_I \in \mathbb{Q}^{\times 2}$ hence we have $d_I = -m$ for some I. If $\sqrt{\pm 2} \in K(\zeta_x)$ and $8 \nmid x$, then there is some odd squarefree $m \mid x$ (such that $m \equiv 1 \bmod 4$, if $2 \nmid x$) such that $\pm 2md_I \in \mathbb{Q}^{\times 2}$ hence we have $d_I = \pm 2m$ for some I. □

The following result allows us in certain cases to conclude directly that a Kummer extension of K is not contained in any cyclotomic extension of K:

Lemma 2.3.2. *If $\alpha \in K^\times$ and $0 \leqslant s \leqslant v_2(\#(\mu_{2^\infty} \cap K))$, then the following properties are equivalent:*
• *The extension $K(\sqrt[2^s]{\alpha})/\mathbb{Q}$ is Galois.*
• *For every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ we have $K(\sqrt[2^s]{\alpha}) = K(\sqrt[2^s]{\sigma(\alpha)})$.*
• *For every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ there is some odd integer x such that $\alpha \cdot \sigma(\alpha)^x \in K^{\times 2^s}$.*
In the last two properties we could restrict to any set of generators for $\mathrm{Gal}(K/\mathbb{Q})$.

Proof. Up to replacing α with a root which is in $K^\times$ and choosing a smaller s, we may suppose that $[K(\sqrt[2^s]{\alpha}) : K] = 2^s$. The second and third property are equivalent by Kummer theory. The number fields $K(\sqrt[2^s]{\alpha})$ and $K(\sqrt[2^s]{\sigma(\alpha)})$ have the same degree, so the equality means that $\tilde{\sigma}(\sqrt[2^s]{\alpha}) \in K(\sqrt[2^s]{\alpha})$, where $\tilde{\sigma} : K(\sqrt[2^s]{\alpha}) \to \bar{K}$ is any field homomorphism extending σ. This shows that the first two properties are equivalent. We are left to show that the second property holds for all $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ if it holds for a set of generators. We write τ as a product of generators, and we proceed by induction on the number of factors. The assertion is clear if there is only one factor, so let $\tau = \sigma\sigma'$, where σ is a generator and the induction hypothesis holds for σ'. We know that $K(\sqrt[2^s]{\alpha}) = K(\sqrt[2^s]{\sigma'(\alpha)})$, and we conclude because $\tilde{\sigma}(\sqrt[2^s]{\alpha})$ is in this field, and $\tilde{\sigma}(\sqrt[2^s]{\sigma'(\alpha)})$ is a 2^s-th root of $\tau(\alpha)$. □

Definition 2.3.3. Let p be a prime number such that $p \equiv 1 \bmod 4$. If $p \equiv 5 \bmod 8$, then let $\beta_p \in \mathbb{Q}(\zeta_4)$ be such that $\mathbb{Q}(\zeta_4, \sqrt[4]{\beta_p})$ is the quartic subextension of $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$; if $p \equiv 1 \bmod 8$, then let $\beta_p \in \mathbb{Q}(\zeta_4, \sqrt{p})$ be such that $\mathbb{Q}(\zeta_4, \sqrt{p}, \sqrt[4]{\beta_p})$ is the subextension of degree 8 of $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$. To determine these elements one can apply the procedure presented in [HPST22, Section 4].

Lemma 2.3.4. *Suppose that $\zeta_4 \in K$, and let N be a positive integer such that $\sqrt{p} \in K$ for every odd prime $p \mid N$. Any cyclic subextension of $K(\zeta_N)/K$ of degree 4 equals $K(\sqrt[4]{g})$ for some $g \in K^\times \setminus K^{\times 2}$ of the form*

$$g = \zeta_{2^e} \prod_{p \equiv 5 \bmod 8} \beta_p^{e_p} \prod_{q \equiv 1 \bmod 8} \beta_q^{e_q}$$

such that p, q are odd prime divisors of N and the integers $e \in \{0, 1, 2, 3\}$, $e_p \in \{0, 2\}$, and $e_q \in \{0, 1, 2\}$ satisfy the following conditions:

$$\begin{aligned} &e \neq 1, \text{ if } \zeta_8 \in K; \\ &e \neq 3, \text{ if } \zeta_8 \notin K \text{ or } 32 \nmid N; \\ &e = 0, \text{ if } 8 \nmid N \text{ or if } \zeta_8 \in K \text{ and } 16 \nmid N; \\ &e = 3 \text{ or } e_q = 1 \text{ for some } q\,. \end{aligned}$$

Different choices for the exponents give rise to distinct extensions. If $x \geqslant 1$, then we have $\sqrt[4]{g} \in K(\zeta_x)$ if and only if we have $v_2(x) \geqslant e + 2$ for $e \neq 0$ and $p \mid x$ for all primes $p \equiv 1 \bmod 4$ such that $e_p \neq 0$.

Proof. The given conditions on x are clearly sufficient to ensure $\sqrt[4]{g} \in K(\zeta_x)$. They are also necessary, as can be seen by adding the fourth roots of all but one of the elements ζ_{2^e}

(if $e \neq 0$) and $\beta_p^{e_p}$ (if $e_p \neq 0$). This line of reasoning also shows that different choices for the exponents give rise to distinct extensions, and that $K(\sqrt[4]{g})/K$ has degree 4.

We have $\sqrt[4]{g} \in L$, where L is the field corresponding to the largest quotient of exponent 4 of $\mathrm{Gal}(K(\zeta_N)/K)$. We can factor $\mathrm{Gal}(L/K)$ as the product of the largest quotient of exponent 4 of $\mathrm{Gal}(K(\zeta_{2^{v_2(N)}})/K)$ and, for every odd prime $p \mid N$, the quotient of order 2 (respectively, 4) of $\mathrm{Gal}(K(\zeta_p)/K)$ if $p \equiv 5 \bmod 8$ (respectively, $p \equiv 1 \bmod 8$), calling L_2 and L_p the corresponding fields. Notice that the fourth roots of ζ_{2^e} (respectively, $\beta_p^{e_p}$) generate a cyclic subextension of L_2/K (respectively, L_p/K) of degree dividing 4, and of degree dividing 2 if $p \equiv 5 \mod 8$. By taking products of these roots, we get an extension of K of degree 4 unless all roots generate extensions of degree at most 2, so we may conclude with a counting argument as in the proof of [HPST21, Theorem 11]. □

Definition 2.3.5. Let p be a prime number. If $p \equiv 5 \bmod 8$, then let $\eta_p \in \mathbb{Q}(\zeta_4)$ be such that $\mathbb{Q}(\zeta_4, \sqrt[4]{\eta_p})$ is the quartic subextension of $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$. If $p \equiv 9 \bmod 16$, then let $\eta_p \in \mathbb{Q}(\zeta_4, \sqrt{p})$ be such that $\mathbb{Q}(\zeta_4, \sqrt{p}, \sqrt[4]{\eta_p})$ is the subextension of degree 8 of $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$ (alternatively, one could work with $\eta_p' \in \mathbb{Q}(\zeta_8)$ such that $\mathbb{Q}(\zeta_8, \sqrt[8]{\eta_p'})$ is the subextension of degree 8 of $\mathbb{Q}(\zeta_{8p})/\mathbb{Q}(\zeta_8)$). If $p \equiv 1 \bmod 16$, then let $\eta_p \in \mathbb{Q}(\zeta_8, \sqrt{p})$ be such that $\mathbb{Q}(\zeta_8, \sqrt{p}, \sqrt[8]{\eta_p})$ is the subextension of degree 16 of $\mathbb{Q}(\zeta_{8p})/\mathbb{Q}(\zeta_8)$. To determine these elements one can apply the procedure presented in [HPST22, Section 4].

Lemma 2.3.6. *Suppose that $\zeta_8 \in K$, and let N be a positive integer such that $\sqrt{p} \in K$ for every odd prime $p \mid N$. Any cyclic subextension of $K(\zeta_N)/K$ of degree 8 equals $K(\sqrt[8]{g})$ for some $g \in K^\times \setminus K^{\times 2}$ of the form*

$$g = \zeta_{2^e} \prod_{p \equiv 5 \bmod 8} \eta_p^{e_p} \prod_{q \equiv 9 \bmod 16} \eta_q^{e_q} \prod_{r \equiv 1 \bmod 16} \eta_r^{e_r}$$

such that p, q, r are odd prime divisors of N and the integers $e \in \{0,1,2,3\}$, $e_p \in \{0,4\}$, $e_q \in \{0,2\}$, and $e_r \in \{0,1,2,4\}$ satisfy the following conditions:

$$\begin{aligned} &e = 0, \text{ if } 16 \nmid N; \\ &e \leqslant 1, \text{ if } 32 \nmid N; \\ &e \neq 3, \text{ if } 64 \nmid N; \\ &e = 3 \text{ or } e_r = 1 \text{ for some } r\,. \end{aligned}$$

Different choices for the exponents give rise to distinct extensions. If $x \geqslant 1$, then we have $\sqrt[8]{g} \in K(\zeta_x)$ if and only if we have $v_2(x) \geqslant e+3$ for $e \neq 0$ and $p \mid x$ for all primes $p \equiv 1 \bmod 4$ such that $e_p \neq 0$.

Proof. The proof is analogous to the one of Lemma 2.3.4. □

2.4 Quadratic extensions of multiquadratic number fields

Let K be a multiquadratic number field, and write $K = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_r})$ for some squarefree integers $d_1, \dots, d_r$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r$. An extension of K of degree 2 is of the form $K(\sqrt{\alpha})$ for some $\alpha \in K^\times \setminus K^{\times 2}$, and we fix such an α. The extension $K(\sqrt{\alpha})/\mathbb{Q}$ is abelian if and only if $K(\sqrt{\alpha}) \subseteq \mathbb{Q}(\mu_\infty)$, and in this case the Galois group $\mathrm{Gal}(K(\sqrt{\alpha})/\mathbb{Q})$ is isomorphic to either

$$(\mathbb{Z}/2\mathbb{Z})^{r+1} \qquad \text{or} \qquad (\mathbb{Z}/2\mathbb{Z})^{r-1} \times \mathbb{Z}/4\mathbb{Z}\,.$$

In the first case $K(\sqrt{\alpha})$ is multiquadratic and hence $K(\sqrt{\alpha}) = K(\sqrt{m})$ for some squarefree integer m (thus, $\alpha/m \in K^{\times 2}$). We can find m or conclude that no such m exists by checking finitely many possibilities because the odd prime divisors of m ramify in $K(\sqrt{\alpha})$.

In the second case we have $K(\sqrt{\alpha}) = K(\sqrt{\gamma})$ for some $\gamma \in K^\times$ such that $\mathbb{Q}(\sqrt{\gamma})$ is quartic cyclic (thus, $\alpha/\gamma \in K^{\times 2}$). We let $\gamma, \gamma', A, B, C, D$ be as in Section 2.1. We can find γ or conclude that no such γ exists by checking finitely many possibilities (since $\mathbb{Q}(\sqrt{D}) \subseteq K$, there are only finitely many possibilities for D and hence for B; the prime divisors of A ramify in $K(\sqrt{\alpha})$). Notice that the odd primes ramifying in $K(\sqrt{\alpha})$ are those ramifying in K and those that lie below a prime of K ramifying in $K(\sqrt{\alpha})$ (these can be found with Lemma 2.1.4).

Theorem 2.4.1. *We keep the above notation, and we suppose that $K(\sqrt{\alpha})/\mathbb{Q}$ is abelian. The minimal integers $x \geqslant 1$ such that $\sqrt{\alpha} \in K(\zeta_x)$ form a non-empty, finite, and computable set. For any $x \geqslant 1$ we have $\sqrt{\alpha} \in K(\zeta_x)$ if and only if one of the following holds:*

1. *We have $K(\sqrt{\alpha}) = K(\sqrt{m})$ and $\sqrt{m \prod_{j \in J} d_j} \in \mathbb{Q}(\zeta_x)$ for some $J \subseteq \{1, \dots, r\}$.*
2. *We have $K(\sqrt{\alpha}) = K(\sqrt{\gamma})$ and x is a multiple of*

$$\begin{cases} w8D & \text{for some } w \text{ such that } \sqrt{A} \in K(\zeta_{w8D}) \quad \text{if } 2 \mid D \\ wD & \text{for some } w \text{ such that } \sqrt{\pm A} \in K(\zeta_{wD}) \quad \text{if } 1 + B \equiv \pm 1 \bmod 4 \\ wD & \text{for some } w \text{ such that } \sqrt{\pm 2A} \in K(\zeta_{wD}) \quad \text{if } 1 + C \equiv \pm 1 \bmod 4\,. \end{cases}$$

We can take w minimal, so that it belongs to a finite computable set.

Proof. Case (1) is a consequence of Lemma 2.1.1 because we can focus on the maximal multiquadratic subextension of $\mathbb{Q}(\zeta_x)$ and because it is immediate to determine the conductor of each field $\mathbb{Q}(\sqrt{m \prod d_j})$. Now we deal with Case (2) (recall that precisely one among B, C, D is even). If $p \mid D$ is prime, then let C_p be the quartic cyclic subextension of $\mathbb{Q}(\zeta_p)$, or $\mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$ for $p = 2$; if $q \nmid D$ is an odd prime ramifying in $K(\sqrt{\alpha})$, then consider the quadratic subextension C'_q of $\mathbb{Q}(\zeta_q)$. So $K(\sqrt{\gamma})$ is contained in

$$L := \mathbb{Q}(\zeta_8) \prod_q C'_q \prod_p C_p\,.$$

We claim that $K(\sqrt{\gamma}) \not\subseteq L'$, where L' is obtained from L by replacing some C_p by a quadratic subextension. This implies that $D \mid x$, and that $16 \mid x$ if $2 \mid D$. In the three subcases of (2) the field $K(\zeta_x)$ contains $\sqrt{\gamma/A}$, $\sqrt{\pm\gamma/A}$, and $\sqrt{\pm\gamma'/A}$ respectively. So we are left to determine the minimal x such that $K(\zeta_x)$ contains $\sqrt{A}$, $\sqrt{\pm A}$ and $\sqrt{\pm 2A}$ respectively, and we conclude by Case (1).

To prove the claim, let $G := \mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/4\mathbb{Z})^s \times (\mathbb{Z}/2\mathbb{Z})^t$ for some integers s, t. We may choose $g_1, \ldots, g_s$ which generate the cyclic factors of order 4 and are such that $g_1 g_i$ fixes $\sqrt{D}$. Without loss of generality we have

$$G' := \mathrm{Gal}(L'/\mathbb{Q}) = G/ < g_1^2 > \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})^{s-1} \times (\mathbb{Z}/2\mathbb{Z})^t .$$

If $\sqrt{\gamma} \in L'$, then there are subgroups $G'_2 < G'_1 < G'$ such that $G'/G'_2 \cong \mathbb{Z}/4\mathbb{Z}$ and $G'/G'_1 \cong \mathbb{Z}/2\mathbb{Z}$. This is impossible because we have $G'_1 = (\mathbb{Z}/4\mathbb{Z})^{s-1} \times (\mathbb{Z}/2\mathbb{Z})^t$ (as generators for $(\mathbb{Z}/4\mathbb{Z})^{s-1}$ we can take the class of $g_1 g_i$ for $i \neq 1$). □

Proposition 2.4.2. *If $\beta \in K^\times \setminus K^{\times 2}$ is such that $K(\sqrt{\beta})$ is multiquadratic, then the set S consisting of the squarefree integers b such that $K(\sqrt{b}) = K(\sqrt{\beta})$ is non-empty, finite, and computable. For $x \geqslant 1$, the following are necessary and sufficient conditions for the elements $\sqrt{\beta}$ and $\zeta_{2^e}\sqrt{\beta}$ for any $e \geqslant 3$ to be in $K(\zeta_x)$:*

Element in $K(\zeta_x)$	*Equivalent condition*
$\sqrt{\beta}$	$\sqrt{b} \in \mathbb{Q}(\zeta_x)$ *for some* $b \in S$
$\zeta_{2^e}\sqrt{\beta}$ *($e \geqslant 4$)*	$2^e \mid x$ *and* $b \mid x$ *for some* $b \in S$
$\zeta_8\sqrt{\beta}$	$\zeta_8 \in K(\zeta_x)$ *and* $b \mid x$ *for some odd* $b \in S$, *or* $\sqrt{2}, \sqrt{-2} \notin K$ *and* $\zeta_4 \in K(\zeta_x)$ *and* $b \mid 2x$ *for some even* $b \in S$.

Proof. There is a squarefree integer m such that $K(\sqrt{\beta}) = K(\sqrt{m})$, thus S consists of the squarefree part of the integers mz, where z is a subproduct of $d_1 \cdots d_r$. The assertion on $\sqrt{\beta}$ then follows from Theorem 2.4.1 (1). Consider $b \in S$. If $8 \mid x$, then the condition $b \mid x$ is equivalent to $\sqrt{b} \in \mathbb{Q}(\zeta_x)$, and in general it is a necessary condition. If $\sqrt{2}$ and ζ_4 are in $K(\zeta_x)$, or if $\zeta_4 \in K(\zeta_x)$ and b is odd, then $b \mid x$ is sufficient for $\sqrt{b} \in K(\zeta_x)$. The given conditions for $\zeta_{2^e}\sqrt{\beta}$ and $\zeta_8\sqrt{\beta}$ are then sufficient (for the last one, we have $\sqrt{2b} \in K(\zeta_x)$ and we conclude because $\sqrt{2}/\zeta_8 \in \mathbb{Q}(\zeta_4)$). The given condition for $\zeta_{2^e}\sqrt{\beta}$ is necessary because we must have $2^e \mid x$ (if $v_2(y) < e$, then 2^e does not divide the conductor of $K(\sqrt{\beta}, \zeta_y)$).

Now suppose that $\zeta_8\sqrt{\beta} \in K(\zeta_x)$ and hence $\zeta_4 \in K(\zeta_x)$. If $\zeta_8 \in K(\zeta_x)$, then we conclude for b odd. If b is even and $\sqrt{2}$ or $\sqrt{-2}$ are in K, then we can reduce to the case b odd and $\zeta_8 \in K(\zeta_x)$. Now suppose that $\sqrt{2}, \sqrt{-2} \notin K$. Since for all $b \in S$ we have $\sqrt{b} \in K(\zeta_{\mathrm{lcm}(8,x)})$, by Lemma 2.1.1 we deduce that $\sqrt{b} \in \mathbb{Q}(\zeta_{\mathrm{lcm}(8,x)})$ for some $b \in S$ and hence $b \mid 2x$. If b is odd, then $\sqrt{\beta}$ and hence ζ_8 would be in $K(\zeta_x)$. □

Notice that in the following result the sets S, S_4 and S_8 exist and they are non-empty, finite, and computable by Lemma 2.3.1 and Theorem 2.4.1.

Proposition 2.4.3. *If $\beta \in K^\times \setminus K^{\times 2}$ is such that $K(\sqrt{\beta})$ is contains a quartic cyclic number field, then consider the finite non-empty computable set S of minimal positive integers y such that $\sqrt{\beta} \in K(\zeta_y)$, and similarly define S_4 by requiring $\zeta_4 \in K(\zeta_y)$ and S_8 by requiring $\zeta_8 \in K(\zeta_y)$. Let y' denote the odd part of y. For any fixed $e \geqslant 3$, the integers $x \geqslant 1$ such that $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$ are those satisfying at least one of the following conditions:*
- $2^e \mid x$ *and* $y \mid x$ *for some* $y \in S$*;*
- *if* $e = 3$, $\operatorname{lcm}(s, y) \mid x$ *for some* $s \in S_8$ *and for some* $y \in S$*;*
- *if* $e = 4$, $v_2(y) = 4$ *(thus,* $\zeta_8 \in K$*),* $y' \mid x$ *for some* $y \in S$*;*
- *if* $e = 3$ *and* $\sqrt{2}, \sqrt{-2} \notin K$, $v_2(y) = 3$, $\operatorname{lcm}(s, y') \mid x$ *for some* $s \in S_4$ *and for some* $y \in S$.

Proof. By minimality, for every $y \in S$ we have: $v_2(y) \in \{0, 2, 3, 4\}$; $v_2(y) = 4$ implies $\zeta_8 \in K$; $v_2(y) = 3$ implies $\sqrt{2}, \sqrt{-2} \notin K$; $v_2(y) = 2$ implies $\zeta_4 \notin K$.

If $x \geqslant 1$ is such that $\zeta_{2^e}\sqrt{\beta}$ (and hence also $\zeta_{2^{e-1}}$) is in $K(\zeta_x)$, then we have $\sqrt{\beta} \in K(\zeta_{\operatorname{lcm}(2^e,x)})$ and in particular $y' \mid x$ for some $y \in S$. If $\zeta_{2^e} \in K(\zeta_x)$, then we have $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$ if and only if $\sqrt{\beta} \in K(\zeta_x)$ (this leads to the first two conditions in the statement). If $\zeta_{2^e} \notin K(\zeta_x)$, then we can have $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$ only if $\sqrt{\beta} \notin K(\zeta_x)$. Now suppose that $\zeta_{2^e}, \sqrt{\beta} \notin K(\zeta_x)$: we claim that $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$ holds if and only if $\zeta_{2^{e-1}} \in K(\zeta_x)$, $y' \mid x$ for some $y \in S$, and $v_2(y) = e$ (this leads to the last two conditions in the statement).

To prove the converse implication in the claim, consider that $K(\zeta_x, \zeta_{2^e}) = K(\zeta_x, \sqrt{\beta})$ because both fields have degree 2 over $K(\zeta_x)$ and the former contains the latter, thus $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$. We now prove the direct implication, namely that $v_2(y) = e$: if $v_2(y) < e$, then we would deduce $\sqrt{\beta} \in K(\zeta_x)$; if $v_2(y) > e$ (which holds for either none or all $y \in S$), then (since $v_2(x) < e$) we would have $\sqrt{\beta} \notin K(\zeta_{\operatorname{lcm}(2^e,x)})$, contradicting $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$. □

2.5 Cyclic extensions of degree 4 or 8 of multiquadratic number fields

Let K be a multiquadratic number field containing ζ_4, and let $\operatorname{Gal}(K/\mathbb{Q})$ be isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ for some $r \geqslant 1$. If L/K is an extension which is cyclic of degree 4 and it is contained in $K(\mu_\infty)$, then $L/\mathbb{Q}$ is abelian and we have $L = K(\sqrt[4]{\alpha})$ for some $\alpha \in K^\times \setminus K^{\times 2}$. Moreover, $\operatorname{Gal}(L/\mathbb{Q})$ is isomorphic to either

$$(\mathbb{Z}/2\mathbb{Z})^r \times \mathbb{Z}/4\mathbb{Z} \qquad \text{or} \qquad (\mathbb{Z}/2\mathbb{Z})^{r-1} \times \mathbb{Z}/8\mathbb{Z}$$

because it has a cyclic subgroup of order 4 and it is not $(\mathbb{Z}/2\mathbb{Z})^{r-2} \times (\mathbb{Z}/4\mathbb{Z})^2$, as $\operatorname{Gal}(K/\mathbb{Q})$ is obtained by quotienting a cyclic subgroup of order 4. We now fix $\alpha \in K^\times \setminus K^{\times 2}$, so that $K(\sqrt[4]{\alpha})/K$ is cyclic of degree 4.

Theorem 2.5.1. *It is possible to check whether $K(\sqrt[4]{\alpha})/\mathbb{Q}$ is abelian with an explicit finite procedure, and in this case there are finitely many computable minimal integers $x \geqslant 1$ such that $\sqrt[4]{\alpha} \in K(\zeta_x)$.*

Proof. The extension $K(\sqrt[4]{\alpha})/\mathbb{Q}$ is abelian of exponent 4 if and only if $K(\sqrt[4]{\alpha}) = K(\sqrt{\gamma})$, where $\mathbb{Q}(\sqrt{\gamma})$ is quartic cyclic (we keep the notation of Section 2.1). If γ exists, then it belongs to a finite computable set, as seen at the beginning of Section 2.4 (there are only finitely many possibilities for D because $K(\sqrt{D}) = K(\sqrt{\alpha})$, and we may work with this multiquadratic number field). Those integers x as requested can be found with Theorem 2.4.1 (first we make sure that $\sqrt{D} \in K(\zeta_x)$, and then we apply the result to $K(\sqrt{D})$).

Let M be the product of all odd prime numbers ramifying in $K(\sqrt[4]{\alpha})$ (the primes of K ramifying in $K(\sqrt[4]{\alpha})$ can be found with Lemma 2.1.4). If $K(\sqrt[4]{\alpha})/\mathbb{Q}$ is abelian (and hence it has exponent dividing 8), then $\sqrt[4]{\alpha} \in K(\zeta_{32M})$ (and $\sqrt[4]{\alpha} \in K(\zeta_{16M})$ if $\zeta_8 \notin K$). To determine whether it is abelian of exponent 8, let F be the extension of K obtained by adding $\sqrt{p}$ for all odd primes $p \mid M$. It is equivalent that $F(\sqrt[4]{\alpha})/\mathbb{Q}$ is abelian of exponent 8, and this is the case if and only if $\alpha/g \in F^{\times 4}$ for some g as in Lemma 2.3.4 (notice that the set of possible g is finite and computable).

By Lemma 2.3.4 we can also determine the minimal integer $y \geqslant 1$ such that $\sqrt[4]{\alpha} \in F(\zeta_y)$. Let $y = y_0 2^v$, where y_0 is the odd part of y, and consider the largest multiquadratic subfield of $K(\zeta_{y_0})$, which we call K'. If $0 < e \leqslant 3$ is as in Lemma 2.3.4, then we have $e + 2 = v \leqslant 4$ if $\zeta_8 \notin K$ and hence $\zeta_{2^e} \in K$. So we have $g \in K'$. Since $F/\mathbb{Q}$ has exponent 2 and $\sqrt[4]{\alpha/g} \in F$, we must have $\sqrt{\alpha/g} \in K'$ and hence by Proposition 2.4.2 we are able to find those finitely many minimal Y (requiring $y_0 \mid Y$) such that $\sqrt[4]{\alpha/g}$, respectively $\zeta_{2^{e+2}}\sqrt[4]{\alpha/g}$ if $e > 0$, is in $K'(\zeta_Y) = K(\zeta_Y)$. These Y are minimal with the property that $y_0 \mid Y$ and $\sqrt[4]{\alpha} \in K(\zeta_Y)$ because, writing $g = \zeta_{2^e} g_0$, we have $\sqrt[4]{g_0} \in K(\zeta_{y_0})$. □

Now we suppose that $\zeta_8 \in K$, and we study the extensions L/K which are cyclic of degree 8. We have $L = K(\sqrt[8]{\alpha})$ for some $\alpha \in K^\times \setminus K^{\times 2}$, so we fix α as such. If $K(\sqrt[8]{\alpha})/\mathbb{Q}$ is abelian, then its Galois group is isomorphic to either

$$(\mathbb{Z}/2\mathbb{Z})^r \times \mathbb{Z}/8\mathbb{Z} \qquad \text{or} \qquad (\mathbb{Z}/2\mathbb{Z})^{r-1} \times \mathbb{Z}/16\mathbb{Z}$$

because there is a cyclic subgroup of order 8, and $\mathrm{Gal}(K/\mathbb{Q})$ is a quotient by a cyclic group of order 8.

Theorem 2.5.2. *It is possible to check whether $K(\sqrt[8]{\alpha})/\mathbb{Q}$ is abelian with an explicit finite procedure, and in this case there are finitely many computable minimal integers $x \geqslant 1$ such that $\sqrt[8]{\alpha} \in K(\zeta_x)$.*

Proof. Let $\alpha' = \sqrt{\alpha}$. The extension $K(\sqrt[8]{\alpha})/\mathbb{Q}$ is abelian of exponent 8 only if $K(\alpha')$ is multiquadratic. In this case we have $K(\sqrt[8]{\alpha}) = K(\alpha', \sqrt[4]{\alpha'})$, so we can apply Theorem 2.5.1 to find all x such that $\sqrt[8]{\alpha} \in K(\alpha', \zeta_x)$, and then Theorem 2.4.1 (1) to select those x such that $\alpha' \in K(\zeta_x)$.

Let M, F be as in the proof of Theorem 2.5.1. The extension $K(\sqrt[8]{\alpha})/\mathbb{Q}$ is abelian only if $\sqrt[8]{\alpha} \in K(\zeta_{64M})$. It is abelian of exponent 16 if and only if the same holds for $F(\sqrt[8]{\alpha})/\mathbb{Q}$, equivalently there is some $g \in F$ as in Lemma 2.3.6 such that $\alpha/g \in F^{\times 8}$

(the set of possible g is finite and computable). By Lemma 2.3.6 we can find the minimal $y \geqslant 1$ such that $\sqrt[8]{\alpha} \in F(\zeta_y)$. Consider the largest multiquadratic subfield of $K(\zeta_y)$ or equivalently of $F(\zeta_y)$, which we call K'. As in the proof of Theorem 2.5.1, we have $g \in K'$ and $\sqrt[4]{\alpha/g} \in K'$. By Proposition 2.4.2 we may then find the finitely many minimal $Y \geqslant 1$ with $y \mid Y$ such that $\sqrt[8]{\alpha/g} \in K'(\zeta_Y) = K(\zeta_Y)$. These are the minimal $Y \geqslant 1$ such that $y \mid Y$ and $\sqrt[8]{\alpha} \in K(\zeta_Y)$ because $\sqrt[8]{g} \in K(\zeta_y)$. □

Proposition 2.5.3. *Let $\beta \in K^\times \setminus K^{\times 2}$.*

1. *Suppose that $\zeta_4 \in K$ (here we do not require $\zeta_8 \in K$) and that $K(\sqrt[4]{\beta})/\mathbb{Q}$ is abelian. Let $e \geqslant 6$, or $e = 5$ and $\zeta_8 \notin K$. We have $\zeta_{2^e}\sqrt[4]{\beta} \in K(\zeta_x)$ for some $x \geqslant 1$ if and only if $\mathrm{lcm}(2^e, y) \mid x$ for some $y \geqslant 1$ such that $\sqrt[4]{\beta} \in K(\zeta_y)$.*

2. *Suppose that $\zeta_8 \in K$ and that $K(\sqrt[8]{\beta})/\mathbb{Q}$ is abelian. Let $e \geqslant 7$. We have $\zeta_{2^e}\sqrt[8]{\beta} \in K(\zeta_x)$ for some $x \geqslant 1$ if and only if $\mathrm{lcm}(2^e, y) \mid x$ for some $y \geqslant 1$ such that $\sqrt[8]{\beta} \in K(\zeta_y)$.*

In particular, the minimal integers $x \geqslant 1$ as above are, in both cases, a finite computable set.

Proof. The minimal integers y as in the statement are a non-empty finite computable set S by Theorems 2.5.1 and 2.5.2. Moreover, the condition $\mathrm{lcm}(2^e, y) \mid x$ for some $y \in S$ is clearly sufficient. To prove that it is necessary, we apply Lemma 2.3.1. For (1), since $\sqrt[4]{\beta} \in K(\zeta_{\mathrm{lcm}(2^e,x)})$, the odd part of some $y \in S$ divides x and we are left to prove $2^e \mid x$. If $e \geqslant 6$, then $\zeta_{2^{e-1}} \in K(\zeta_x)$ and hence $2^{e-1} \mid x$. Thus $y \mid x$ hence $\zeta_{2^e} \in K(\zeta_x)$ and we conclude. If $e = 5$ and $\zeta_8 \notin K$, then for every odd $z \geqslant 1$ we have $\zeta_{32}\sqrt[4]{\beta} \notin K(\zeta_{16z})$ (this field contains $\sqrt[4]{\beta}$ but not ζ_{32}) and we conclude. For (2), since $\zeta_{2^{e-1}}\sqrt[4]{\beta} \in K(\zeta_x)$ we get $2^{e-1} \mid x$ by (1), and we similarly conclude. □

2.6 Extensions of a quartic cyclic number field

In this section $K = \mathbb{Q}(\sqrt{\gamma})$ is a quartic cyclic number field, and we keep the notation of Section 2.1.

Lemma 2.6.1. *For $x \geqslant 1$, the following are necessary and sufficient conditions for the elements ζ_{2^n} for any $n \geqslant 2$ and for $\sqrt{2}$ and $\sqrt{-2}$ to be in $K(\zeta_x)$:*

Element in $K(\zeta_x)$	*Equivalent condition*
ζ_{2^n} *($n \geqslant 5$)*	$2^n \mid x$
ζ_{16}	$16 \mid x$, *or* $2 \mid D$, $4AD \mid x$
ζ_8	$8 \mid x$, *or* $2 \mid D$, $2D \mid x$, *or* $2 \mid C$, $4AD \mid x$
ζ_4	$4 \mid x$, *or* $AD \mid x$, $A + B \equiv 3 \bmod 4$
$\sqrt{2}$	$\zeta_8 \in K(\zeta_x)$, *or* $2 \mid D$, $D \mid 2x$, *or* $AD \mid x$, $A + C \equiv 1 \bmod 4$
$\sqrt{-2}$	$\zeta_8 \in K(\zeta_x)$, *or* $AD \mid x$, $A + C \equiv 3 \bmod 4$.

Proof. We may suppose without loss of generality that x is odd or $4 \mid x$ (notice that in the conditions in the statement each congruence implies that D is odd). We set $\eta = 2+\sqrt{2}$ and $\gamma_0 = \gamma/A$, and we call c_K the conductor of K. The assertion for ζ_{2^n} is clear because $32 \nmid c_K$.

The element ζ_{16}: Suppose that $\zeta_{16} \in K(\zeta_x)$ and $16 \nmid x$, which implies $16 \mid c_K$ and hence $2 \mid D$. Thus $\sqrt{\eta} \in K(\zeta_x) \setminus \mathbb{Q}(\zeta_x)$. We claim that $\sqrt{D} \in \mathbb{Q}(\zeta_x)$ or equivalently $4D \mid x$. If not, then by Lemma 2.1.1 we have $\sqrt{\eta D} \in \mathbb{Q}(\zeta_x)$ thus $(D/2) \mid x$ and $\eta \in \mathbb{Q}(\zeta_x)$, which gives $8 \mid x$ and hence $4D \mid x$, contradiction. The conductor of $\mathbb{Q}(\sqrt{\gamma_0})$ is $8D$, so both $\sqrt{\gamma}$ and $\sqrt{\gamma_0}$ generate $K(\zeta_x)$ over $\mathbb{Q}(\zeta_x)$. Thus $\sqrt{A} \in \mathbb{Q}(\zeta_x)$ and hence $A \mid x$. For the other implication: if $2 \mid D$, $4AD \mid x$, and $16 \nmid x$, then we have $\mathbb{Q}(\zeta_x) \subsetneq K(\zeta_x) \subseteq \mathbb{Q}(\zeta_x, \zeta_{16})$ so we conclude because $\zeta_8 \in \mathbb{Q}(\zeta_x)$.

The element ζ_8: Suppose that $\zeta_8 \in K(\zeta_x)$ and $8 \nmid x$, which implies $8 \mid c_K$ and hence either $2 \mid D$ or $2 \mid C$. If $\sqrt{D} \notin \mathbb{Q}(\zeta_x)$, then by Lemma 2.1.1 we have $\sqrt{2D} \in \mathbb{Q}(\zeta_x)$, which implies $2 \mid D$ and $(D/2) \mid x$. We have $K(\zeta_x) = \mathbb{Q}(\zeta_x, \sqrt{2})$ and hence $\zeta_4 \in \mathbb{Q}(\zeta_x)$, so $2D \mid x$. Now suppose $\sqrt{D} \in \mathbb{Q}(\zeta_x)$: if D is even, then $4D \mid x$; if D is odd, then $\sqrt{2} \in K(\zeta_x)$ implies $2 \mid x$ hence $4D \mid x$. To prove $A \mid x$, or equivalently $\sqrt{A} \in \mathbb{Q}(\zeta_x)$, consider that $\sqrt{\gamma}, \sqrt{\gamma_0}$ are both in $K(\zeta_x) \setminus \mathbb{Q}(\zeta_x)$ because $8 \mid c_K$ and the conductor of $\mathbb{Q}(\sqrt{\gamma_0})$ is $8D$. For the other implication: if $8 \nmid x$, $2 \mid D$, and $2D \mid x$, then we have $\zeta_4 \in \mathbb{Q}(\zeta_x)$, and we also have $\sqrt{2} \in K(\zeta_x)$ because both $\sqrt{D}$ and $\sqrt{D/2}$ are in this field; if $8 \nmid x$, $2 \mid C$, and $4AD \mid x$, then $\zeta_4 \in \mathbb{Q}(\zeta_x)$ and we conclude because $K(\zeta_x)$ is contained in $\mathbb{Q}(\zeta_x, \zeta_8)$ but not in $\mathbb{Q}(\zeta_x)$.

The element ζ_4: Suppose that $\zeta_4 \in K(\zeta_x)$ and that x is odd, hence $4 \mid c_K$. We cannot have $8 \mid c_K$, else $K(\zeta_{|A|Dx})/\mathbb{Q}(\zeta_{|A|Dx})$ would not be cyclic as it would be generated by ζ_8. So $c_K = 4|A|D$ and hence $A+B \equiv 3 \bmod 4$, thus D is odd and hence it is congruent to $1 \bmod 4$. Since $K(\zeta_x)/\mathbb{Q}(\zeta_x)$ is cyclic and $K(\zeta_x)$ contains $\sqrt{D}$ and ζ_4, we must have $\sqrt{D} \in \mathbb{Q}(\zeta_x)$, thus $K(\zeta_x) = \mathbb{Q}(\zeta_{4x})$ and hence $AD \mid x$. For the other implication: if $4 \nmid x$ and $AD \mid x$ and $A + B \equiv 3 \bmod 4$, then we conclude because $K(\zeta_{|A|D}) \subseteq K(\zeta_x)$ is contained in $\mathbb{Q}(\zeta_{4|A|D})$ but not in $\mathbb{Q}(\zeta_{|A|D})$.

The elements $\sqrt{\pm 2}$: Suppose that $\sqrt{\pm 2} \in K(\zeta_x)$ and $\zeta_8 \notin K(\zeta_x)$, so $\zeta_4 \notin K(\zeta_x)$ and x is odd. Since $8 \mid c_K$, we have either $2 \mid D$ or $2 \mid C$. If $\sqrt{D} \in \mathbb{Q}(\zeta_x)$, then $2 \nmid D$ and $D \mid x$. If $\sqrt{D} \notin \mathbb{Q}(\zeta_x)$, then $\sqrt{\pm 2D} \in \mathbb{Q}(\zeta_x)$ by Lemma 2.1.1 and so the odd part of D divides x. Now we may suppose that $2 \nmid BD$ and $D \mid x$, which imply $\sqrt{D} \in \mathbb{Q}(\zeta_x)$ and hence $K(\zeta_x) = \mathbb{Q}(\zeta_x, \sqrt{\pm 2})$. In particular, we have $A \mid x$. From Remark 2.1.6 we deduce that $\sqrt{\pm\gamma'} \in \mathbb{Q}(\zeta_x)$. With the plus sign, the conductor of $\mathbb{Q}(\sqrt{\gamma'})$ is odd, else the conductor is four times an odd number. We conclude that $A + C \equiv \pm 1 \bmod 4$. For the other implication: if $2 \mid D$ and $D \mid 2x$ (recalling that all odd prime divisors of D are congruent to $1 \bmod 4$), then $K(\zeta_x)$ contains $\sqrt{D}$ and $\sqrt{D/2}$; if $AD \mid x$ and $A + C \equiv \pm 1 \bmod 4$, then $\sqrt{\gamma} \in K(\zeta_x)$ and $\sqrt{\pm\gamma'} \in \mathbb{Q}(\zeta_{|A|D}) \subset K(\zeta_x)$, so $K(\zeta_x)$ contains $\sqrt{\pm 2}$ by Remark 2.1.6. □

Fix $\alpha \in K^\times \setminus K^{\times 2}$. If $K(\sqrt{\alpha})$ is contained in $K(\mu_\infty)$, then it is an abelian extension of $\mathbb{Q}$ of degree 8. Its Galois group over $\mathbb{Q}$ has a cyclic quotient of order 4, so it is

isomorphic either to

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad \text{or} \qquad \mathbb{Z}/8\mathbb{Z}\,.$$

Lemma 2.6.2. *The extension $K(\sqrt{\alpha})/\mathbb{Q}$ is abelian if and only if it is Galois if and only if we have $\alpha \cdot \sigma(\alpha) \in K^{\times 2}$, where σ is some generator for* $\mathrm{Gal}(K/\mathbb{Q})$.

Proof. If $K(\sqrt{\alpha})/\mathbb{Q}$ is Galois, then it is abelian because its Galois group has order 8 and it has a quotient isomorphic to $\mathbb{Z}/4\mathbb{Z}$. For the second equivalence we may reason as in the proof of [HPST21, Lemma 4], where we consider $\alpha \cdot \sigma(\alpha)$ instead of $N_{K/\mathbb{Q}}(\alpha)$. □

The extension $K(\sqrt{\alpha})/\mathbb{Q}$ is abelian and not cyclic only if there is some squarefree integer m such that $K(\sqrt{\alpha}) = K(\sqrt{m})$ and hence $\alpha/m \in K^{\times 2}$. To determine if m exists and to find it, it suffices to check finitely many possibilities because the odd primes dividing m ramify in $K(\sqrt{\alpha})$ (these can be found with [HPST21, Lemma 2] and by considering the conductor of K).

Theorem 2.6.3. *We keep the above notation and the one from Section 2.1. If $K(\sqrt{\alpha}) = K(\sqrt{m})$, then for $x \geqslant 1$ we have $\sqrt{\alpha} \in K(\zeta_x)$ if and only if x is a multiple of at least one of the following numbers:*
- *the conductor of $\mathbb{Q}(\sqrt{m})$;*
- *the conductor of $\mathbb{Q}(\sqrt{Dm})$;*
- *$8D$ times the conductor of $\mathbb{Q}(\sqrt{Am})$;*
- *D times the conductor of $\mathbb{Q}(\sqrt{\pm Am})$, if $A + B \equiv \pm 1 \bmod 4$;*
- *D times the conductor of $\mathbb{Q}(\sqrt{\pm 2Am})$, if $A + C \equiv \pm 1 \bmod 4$.*

Proof. Since $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{mD})$ are the quadratic subextensions of $K(\sqrt{\alpha})$ not contained in K, the first two given conditions are sufficient. The other conditions are also sufficient because $\mathbb{Q}(\zeta_x)$ respectively contains the square roots of $D + B\sqrt{D}$, of $\pm(D + B\sqrt{D})$ and of $\pm 2(D + B\sqrt{D})$ by Remark 2.1.5 and (2.2), so it contains $\sqrt{A}$,$\sqrt{\pm A}$ and $\sqrt{\pm 2A}$.

Now suppose that $\sqrt{\alpha} \in K(\zeta_x)$. If $K \subseteq \mathbb{Q}(\zeta_x)$ or $K \cap \mathbb{Q}(\zeta_x) = \mathbb{Q}$, then by Lemma 2.1.1 $\sqrt{m}$ or $\sqrt{Dm}$ is in $\mathbb{Q}(\zeta_x)$ and we have the first or second condition. Now suppose that $\sqrt{D} \in \mathbb{Q}(\zeta_x)$ and $K \not\subseteq \mathbb{Q}(\zeta_x)$, and in particular we have $D \mid x$, and $4D \mid x$ if $2 \mid D$.

If $A + B \equiv \pm 1 \bmod 4$, then $\sqrt{\pm(D + B\sqrt{D})} \in \mathbb{Q}(\zeta_x)$ and hence $K(\zeta_x) = \mathbb{Q}(\zeta_x, \sqrt{\pm A})$. Thus, by Lemma 2.1.1 $\sqrt{m}$ or $\sqrt{\pm Am}$ is in $\mathbb{Q}(\zeta_x)$ and we have the first or fourth condition. If $8D \mid x$, then we may reason analogously because $\sqrt{D + B\sqrt{D}} \in \mathbb{Q}(\zeta_x)$.

If $2 \mid D$ (thus $4D \mid x$) and $8D \nmid x$, then we have $K(\zeta_x) = \mathbb{Q}(\zeta_x, \sqrt{A(2 + \sqrt{2})})$ because $\sqrt{2 + \sqrt{2}}$ and $\sqrt{D + B\sqrt{D}}$ generate the same extension over $\mathbb{Q}(\zeta_{4D})$. By Lemma 2.1.1 and since $\sqrt{2} \in \mathbb{Q}(\zeta_x)$ all quadratic subextensions of $K(\zeta_x)$ are contained in $\mathbb{Q}(\zeta_x)$, so we have the first condition.

If $A + C \equiv \pm 1 \bmod 4$, then we have $\sqrt{\pm 2(D + B\sqrt{D})} \in \mathbb{Q}(\zeta_x)$ by (2.2). So $K(\zeta_x) = \mathbb{Q}(\zeta_x, \sqrt{\pm 2A})$ and hence $\sqrt{m}$ or $\sqrt{\pm 2Am}$ is in $\mathbb{Q}(\zeta_x)$ and we conclude. □

Proposition 2.6.4. *Let $\beta \in K^\times$ be such that $K(\sqrt{\beta})/\mathbb{Q}$ is abelian and not cyclic, and let $e \geqslant 3$. An integer $x \geqslant 1$ such that $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$ is the multiple of at least one of the following numbers:*
• $\mathrm{lcm}(2^e, y)$, *for $e \geqslant 5$, where y is such that $\sqrt{\beta} \in K(\zeta_y)$;*
• $\mathrm{lcm}(w, y)$, *if $e = 4$, where w is such that $\zeta_{2^e} \in K(\zeta_w)$ and y is such that $\sqrt{\beta} \in K(\zeta_y)$;*
• $\mathrm{lcm}(4, z)$, *if $e = 3$, where z is such that $\sqrt{2\beta} \in K(\zeta_z)$;*
• $\mathrm{lcm}(AD, z)$, *if $e = 3$ and $A + B \equiv 3 \bmod 4$, where z is such that $\sqrt{2\beta} \in K(\zeta_z)$.*
The minimal integers x form a non-empty finite computable set.

Proof. We can find all minimal w, y, z by applying Lemmas 2.6.1 and Theorem 2.6.3.

Write $K(\sqrt{\beta}) = K(\sqrt{m})$ for some squarefree integer m as seen before Theorem 2.6.3. So we need to describe those x such that $\zeta_{2^e}\sqrt{m} \in K(\zeta_x)$. Notice that $\zeta_{2^e}\sqrt{m} \in K(\zeta_x)$ implies $\zeta_{2^{e-1}} \in K(\zeta_x)$. For $e \geqslant 4$ (considering Lemma 2.6.1 for $e \geqslant 5$) it suffices to prove that both ζ_{2^e} and $\sqrt{m}$ are in $K(\zeta_x)$. This is the case because, if $K(\zeta_x, \sqrt{m})$ and $K(\zeta_x, \zeta_{2^e})$ are non-trivial over $K(\zeta_x)$, then they cannot be equal as the former field has more quadratic subextensions than the latter by Lemma 2.1.1. If $e = 3$, then $\zeta_4 \in K(\zeta_x)$ and hence $\sqrt{2\beta} \in K(\zeta_x)$ so we conclude by Lemma 2.6.1. □

Theorem 2.6.5. *Let c_K be the conductor of K (call c'_K its odd part and v_K its 2-adic valuation). Let $\mathcal{P}$ be a prime of K over 2. If $K(\sqrt{\alpha})/\mathbb{Q}$ is cyclic of degree 8, then there exists unique a minimal integer $x \geqslant 1$ such that $\sqrt{\alpha} \in K(\zeta_x)$. The odd part of x is a multiple of c'_K and it is the product of all odd primes whose primes of K above them ramify in $K(\sqrt{\alpha})$. Moreover, $v_2(x)$ is given by*

$$\begin{cases} 5 & \text{if } v_K = 4 \\ 4 & \text{if } v_K = 3 \\ 3 & \text{if } v_K = 2 \text{ and } \mathcal{P} \text{ ramifies in } K(\sqrt{\alpha}), \\ & \quad \text{or } v_K = 0 \text{ and } \mathcal{P} \text{ ramifies in } K(\sqrt{\alpha}),\ K(\sqrt{-\alpha}) \\ 2 & \text{if } v_K = 0 \text{ and } \mathcal{P} \text{ does not ramify in } K(\sqrt{-\alpha}) \\ 0 & \text{if } v_K = 0, 2 \text{ and } \mathcal{P} \text{ does not ramify in } K(\sqrt{\alpha})\,. \end{cases}$$

Proof. Let x be minimal such that $\sqrt{\alpha} \in K(\zeta_x)$: its odd part x' is squarefree, $1 \neq v_2(x) \leqslant 5$, all prime divisors of x ramify in $K(\sqrt{\alpha})$. Recall that the primes ramifying in K are those dividing c_K, and notice that, if $p \nmid c_K$ is a prime ramifying in $K(\sqrt{\alpha})$, then $p \mid x$.

To show $c'_K \mid x'$ it suffices to prove $c'_K \mid y$, where $y \geqslant 1$ is such that $\sqrt{\alpha} \in K(\zeta_4, \zeta_y)$. Notice that $K(\zeta_4, \sqrt{\alpha})/\mathbb{Q}(\sqrt{D}, \zeta_4)$ is a cyclic Kummer extension of degree 4 with intermediate extension $K(\zeta_4)$. Thus the extension $K(\zeta_4, \zeta_y)/\mathbb{Q}(\sqrt{D}, \zeta_4, \zeta_y)$ is trivial as it has degree at most 2 and hence the base field contains $K(\zeta_4)$. We deduce that A and the odd part of D divide y because if $p \mid AD$ is an odd prime, then $\mathbb{Q}(\zeta_{16|A|D/p}) \neq K(\zeta_{16|A|D/p}) \subseteq \mathbb{Q}(\zeta_{16|A|D})$. We may reason analogously to prove that $v_K \leqslant v_2(x)$ holds if $v_K \geqslant 3$.

Since $K(\sqrt{\alpha}, \zeta_{c_K})/\mathbb{Q}(\zeta_{c_K})$ has degree at most 2, we have $v_2(x) \leqslant \max(3, v_K + 1)$. If $v_K = 3, 4$, then we know $v_2(x) \in \{v_K, v_K + 1\}$, so we conclude by the minimality

of x because $K(\zeta_{2^{v_K}x'}) = K(\zeta_{2^{v_K-1}x'})$. If $v_K = 2$, then $K(\sqrt{\alpha}, \zeta_{x'})$ is either $\mathbb{Q}(\zeta_{4x'})$ or $\mathbb{Q}(\zeta_{8x'})$. In the latter case $\mathcal{P}$ ramifies in $K(\sqrt{\alpha})$, while in the former case it does not because $K(\sqrt{\alpha}, \zeta_{x'}) = K(\zeta_{x'})$. If $v_K = 0$, then 2 does not ramify in K: if $\mathcal{P}$ does not ramify in $K(\sqrt{\alpha})$, then $v_2(x) = 0$; else $v_2(x) \in \{2, 3\}$, and it equals 2 if and only if $\mathcal{P}$ does not ramify in $K(\sqrt{-\alpha})$. Notice that there is an explicit finite procedure to check whether the primes of K lying over 2 ramify in $K(\sqrt{\alpha})$, see [Coh93, Algorithm 6.2.9]. □

Lemma 2.6.6. *If A has some prime divisor congruent to $3 \bmod 4$, then $K(\sqrt{\alpha})/\mathbb{Q}$ is not cyclic. If $K(\sqrt{\alpha})/\mathbb{Q}$ is abelian, then it is cyclic if and only if all prime ideals of K above the odd prime divisors of AD ramify in $K(\sqrt{\alpha})$ (we can apply Lemma 2.1.4 to check this condition).*

Proof. If $K(\sqrt{\alpha})/\mathbb{Q}$ is cyclic, then $\sqrt{\alpha} \notin K(\zeta_4)$ and we have $\sqrt{\alpha} \in K(\zeta_{16|A|Dw})$ for some odd squarefree integer $w \geqslant 1$ coprime to AD. So $K(\zeta_4, \sqrt{\alpha})/\mathbb{Q}(\sqrt{D}, \zeta_4)$ is cyclic of degree 4 and $K \not\subseteq \mathbb{Q}(\sqrt{D}, \zeta_4, \zeta_x)$ if $A \nmid x$. Thus, if $p \mid A$ is prime, then

$$K(\zeta_{16|A|Dw/p}, \sqrt{\alpha})/\mathbb{Q}(\zeta_{16|A|Dw/p})$$

is a subextension of $\mathbb{Q}(\zeta_{16|A|Dw})/\mathbb{Q}(\zeta_{16|A|Dw/p})$ of degree 4, which implies $p \equiv 1 \bmod 4$.

In the second assertion, the prime divisors of AD divide the conductor of K hence the ramification condition is necessary by Theorem 2.6.5. It is also sufficient because if $K(\sqrt{\alpha})/\mathbb{Q}$ is abelian and not cyclic, then by Theorem 2.6.3 (the first two cases) there is some $x \geqslant 1$ such that $\sqrt{\alpha} \in K(\zeta_x)$ and $D \nmid 2x$.

□

Proposition 2.6.7. *Let $\beta \in K^\times$ be such that $K(\sqrt{\beta})/\mathbb{Q}$ is cyclic of degree 8, and let $e \geqslant 3$. Let y vary in the set of integers such that $\sqrt{\beta} \in K(\zeta_y)$, and denote by y' the odd part of y. Those integers $x \geqslant 1$ such that $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$ are the multiples of at least one of the following numbers:*
- $\operatorname{lcm}(2^e, y)$;
- *$4y'$, if $e = v_2(y) = 5$;*
- $\operatorname{lcm}(w, y')$, *if $e = v_2(y) = 4$ or if $e = 3$ and $v_2(y) < 3$, where w is such that $\zeta_8 \in K(\zeta_w)$;*
- $\operatorname{lcm}(z, y')$, *if $e = v_2(y) = 3$, where z is such that $\zeta_4 \in K(\zeta_z)$.*

The minimal x are a non-empty finite computable set.

Proof. We can find all minimal w and z with Lemma 2.6.1 and y with Theorem 2.6.5. If $x \geqslant 1$ is such that $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$, then we have $\zeta_{2^{e-1}} \in K(\zeta_x)$ and $\sqrt{\beta} \in K(\zeta_{\operatorname{lcm}(2^e,x)})$, and in particular $y' \mid x$ for some y.

Unless ζ_{2^e} and $\sqrt{\beta}$ are both in $K(\zeta_x)$, we have $\zeta_{2^e} \notin K(\zeta_x)$ and $\sqrt{\beta} \notin K(\zeta_x)$ so, as in the proof of Proposition 2.4.3, $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$ holds if and only if $\zeta_{2^{e-1}} \in K(\zeta_x)$, $y' \mid x$ for some y as above, and $v_2(y) = e$.

Suppose that ζ_{2^e} and $\sqrt{\beta}$ are both in $K(\zeta_x)$. If $e > 3$ or if $e = 3$ and $v_2(y) \geqslant 3$, then the first condition is necessary and sufficient. Now let $e = 3$ and $v_2(y) < 3$. Then the third condition is sufficient because $K(\zeta_{\mathrm{lcm}(w,y')}) = K(\zeta_{\mathrm{lcm}(w,4y')})$ and it is necessary because $\zeta_8 \in K(\zeta_x)$.

Now suppose that neither ζ_{2^e} nor $\sqrt{\beta}$ are in $K(\zeta_x)$, and let $e = v_2(y)$ and $y' \mid x$. We only have to ensure $\zeta_{2^{e-1}} \in K(\zeta_x)$. If $e = 3$ or $e = 4$, then clearly the last condition or respectively the third condition applies. Finally let $e = v_2(y) = 5$, which implies $2 \mid D$ and that (recalling from Theorem 2.6.5 that $AD \mid 2y$) we have $K(\zeta_{4y'}) = \mathbb{Q}(\zeta_{4y'}, \sqrt{\delta}) = \mathbb{Q}(\zeta_{16y'})$, where $\delta = 2 + \sqrt{2}$, while clearly $\zeta_{16} \notin K(\zeta_{y'})$. □

2.7 The 2-adelic failure

The 2-adelic failure for quartic cyclic number fields

Let K be a quartic cyclic number field and let $m, N \geqslant 1$ be such that $2^m \mid N$. Without loss of generality let $\alpha \in K^\times$ be not a root of unity. We write $F = K(\zeta_{2^m}, \sqrt[2^m]{\alpha}) \cap K(\mu_\infty)$ and we compute the 2-adelic failure

$$B(N, 2^m) = [F \cap K(\zeta_N) : K(\zeta_{2^m})] .$$

We can write $\alpha = \pm\beta^{2^d}$, where $d \geqslant 0$ and $\beta \in K^\times$ is strongly 2-indivisible. By Theorem 2.2.1 we can determine F, and we have

$$B(N, 2^m) = \begin{cases} 2 & \text{if } F = K(\zeta_{2^{m+1}}) \text{ and } \zeta_{2^{m+1}} \in K(\zeta_N), \\ & \text{or if } F = K(\zeta_{2^m}, \sqrt{\beta}) \text{ and } \sqrt{\beta} \in K(\zeta_N), \\ & \text{or if } m \geqslant 2,\ F = K(\zeta_{2^{m+1}}\sqrt{\beta}), \text{ and } \zeta_{2^{m+1}}\sqrt{\beta} \in K(\zeta_N) \\ 1 & \text{otherwise} \end{cases}$$

so we may conclude by applying the results of Section 2.6 to determine whether the given elements are in $K(\zeta_N)$.

Example 2.7.1. Let $K = \mathbb{Q}(\sqrt{3(5+2\sqrt{5})})$, and let $\alpha = 21$ or $\alpha = -21^4$. Consider all $m, N \geqslant 1$ such that $2^m \mid N$, and recall that $B(N, 2^m) \in \{1, 2\}$. If $\alpha = 21$, then $B(N, 2^m) = 2$ if and only if $2^m \cdot 21 \mid N$ or $2^{\max(2,m)} \cdot 35 \mid N$. If $\alpha = -21^4$, then $B(N, 2^m) = 2$ if and only if we are in the following cases: $m \leqslant 2$ and $2^{m+1} \mid N$; $m = 3$ and $16 \cdot 21 \mid N$ or $16 \cdot 35 \mid N$; $m \geqslant 4$ and $2^m \cdot 21 \mid N$ or $2^m \cdot 35 \mid N$.

Indeed, Theorem 2.2.1 gives $K(\zeta_{2^m}, \sqrt[2^m]{21}) \cap K(\mu_\infty) = K(\zeta_{2^m}, \sqrt{21})$ and

$$K(\zeta_{2^m}, \sqrt[2^m]{-21^4}) \cap K(\mu_\infty) = \begin{cases} K(\zeta_{2^{m+1}}) & \text{if } m \leqslant 2 \\ K(\zeta_{2^{m+1}}\sqrt{21}) & \text{if } m = 3 \\ K(\zeta_{2^m}, \sqrt{21}) & \text{if } m \geqslant 4 . \end{cases}$$

Moreover, by Lemma 2.6.1 for $m \geqslant 2$ we have $\zeta_{2^m} \in K(\zeta_N)$ if and only if $2^m \mid N$; by Theorem 2.6.3 we have $\sqrt{21} \in K(\zeta_N)$ if and only if $21 \mid N$ or $4 \cdot 35 \mid N$; by Proposition 2.6.4 for $m \geqslant 3$ we have $\zeta_{2^m}\sqrt{21} \in K(\zeta_N)$ if and only if $2^m \cdot 21 \mid N$ or $2^m \cdot 35 \mid N$ (by Theorem 2.6.3 we have $\sqrt{42} \in K(\zeta_N)$ if and only if $8 \cdot 21 \mid N$ or $8 \cdot 35 \mid N$).

Example 2.7.2. Let $K = \mathbb{Q}(\sqrt{\gamma})$, where $\gamma = 5(17 + \sqrt{17})$, so the conductor of K is $8 \cdot 85$. Let $\alpha = -\beta^8$, where $\beta = 12\sqrt{\gamma} + 78\gamma + 7\gamma\sqrt{\gamma}$. Consider all $m, N \geqslant 1$ such that $2^m \mid N$, and recall that $B(N, 2^m) \in \{1, 2\}$. We prove that $B(N, 2^m) = 2$ if and only if we are in the following cases: $m = 2$, and $8 \mid N$ or $4 \cdot 85 \mid N$; $m = 3$ and $16 \mid N$; $m = 4$ and $32 \cdot 85 \mid N$; $m \geqslant 5$ and $2^m \cdot 85 \mid N$.

With [The21] we can check that $\beta \in K^\times$ is strongly 2-indivisible, and that $\beta \cdot \sigma(\beta) \in K^{\times 2}$, where σ is a generator of $\mathrm{Gal}(K/\mathbb{Q})$. By Lemma 2.6.2 $K(\sqrt{\beta})/\mathbb{Q}$ is then abelian, so Theorem 2.2.1 gives

$$K(\zeta_{2^m}, \sqrt[2^m]{\alpha}) \cap K(\mu_\infty) = \begin{cases} K(\zeta_{2^{m+1}}) & \text{if } m \leqslant 3 \\ K(\zeta_{2^{m+1}}\sqrt{\beta}) & \text{if } m = 4 \\ K(\zeta_{2^m}, \sqrt{\beta}) & \text{if } m \geqslant 5\,. \end{cases}$$

By [The21], working with the ring of integers of K, the prime ideals dividing (β) with an odd exponent lie over $2, 5, 17$. Then by Lemma 2.6.6 the Galois group of $K(\sqrt{\beta})/\mathbb{Q}$ is $\mathbb{Z}/8\mathbb{Z}$ and hence by applying Theorem 2.6.5 we have $\sqrt{\beta} \in K(\zeta_x)$ if and only if $16 \cdot 85 \mid x$.

By Lemma 2.6.1 for $m \neq 1, 3$ we have $\zeta_{2^m} \in K(\zeta_x)$ if and only if $2^m \mid x$, while $\zeta_8 \in K(\zeta_x)$ if and only if $8 \mid x$ or $4 \cdot 85 \mid x$. By Proposition 2.6.7 we have $\zeta_{2^m}\sqrt{\beta} \in K(\zeta_x)$ if and only if $m \geqslant 5$ and $2^m \cdot 85 \mid x$, or $m = 4$ and $4 \cdot 85 \mid x$, or $m = 3$ and $16 \cdot 85 \mid x$.

The 2-adelic failure for multiquadratic number fields

Let K be a multiquadratic number field and let $m, N \geqslant 1$ be such that $2^m \mid N$. Without loss of generality let $\alpha \in K^\times$ be not a root of unity. We write $F = K(\zeta_{2^m}, \sqrt[2^m]{\alpha}) \cap K(\mu_\infty)$ and we compute the 2-adelic failure

$$B(N, 2^m) = [F \cap K(\zeta_N) : K(\zeta_{2^m})]\,.$$

We can write $\alpha = \zeta_{2^h}\beta^{2^d}$, where $\zeta_{2^h} \in K$ (thus $h \leqslant 3$), $d \geqslant 0$, and $\beta \in K^\times$ is strongly 2-indivisible. We can find F by applying Theorem 2.2.1, and then we can find the degrees $B(N, 2^m)$ by applying the results in Sections 2.4–2.5 to the generator of F over $K(\zeta_{2^m})$ indicated by Theorem 2.2.1 (and to the generators of the subextensions of F over $K(\zeta_{2^m})$, which are 2-powers of the given generator).

Example 2.7.3. Let $K = \mathbb{Q}(\zeta_4, \sqrt{5}, \sqrt{21})$ and $\alpha = \zeta_4\beta^8$, where $\beta = 3(5 + 2\sqrt{5}) \in K^\times$ is strongly 2-indivisible. We prove that for all $m, N \geqslant 1$ such that $2^m \mid N$ we have

$$B(N, 2^m) = \begin{cases} 4 & \text{if } m = 2, 3 \text{ and } 2^{m+2} \mid N, \text{ or} \\ & \text{if } m = 4 \text{ and } 2^6 \cdot 15 \mid N \text{ or } 2^6 \cdot 35 \mid N \\ 2 & \text{if } m = 1 \text{ and } 2^3 \mid N, \text{ or} \\ & \text{if } m = 2, 3 \text{ and } v_2(N) = m + 1, \text{ or} \\ & \text{if } m = 4 \text{ and } 2^5 \mid N,\ 2^6 \cdot 15 \nmid N,\ 2^6 \cdot 35 \nmid N, \text{ or} \\ & \text{if } m = 5 \text{ and } 2^6 \cdot 15 \mid N \text{ or } 2^6 \cdot 35 \mid N, \text{ or} \\ & \text{if } m \geqslant 6 \text{ and } 2^m \cdot 15 \mid N \text{ or } 2^m \cdot 35 \mid N \\ 1 & \text{otherwise}\,. \end{cases}$$

Since $\mathbb{Q}(\sqrt{\beta})$ is quartic cyclic, the Galois group of $K(\sqrt{\beta})/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$. We have $\sqrt[4]{\beta} \notin K(\mu_\infty) = \mathbb{Q}(\sqrt{\beta}, \mu_\infty)$ by Lemma 2.6.2 because $\sqrt{\beta \cdot 3(5-2\sqrt{5})} = 3\sqrt{5} \notin \mathbb{Q}(\sqrt{\beta})^{\times 2}$. By Theorem 2.4.1 we have $\sqrt{\beta} \in K(\zeta_N)$ if and only if $15 \mid N$ or $35 \mid N$.

For $M \geqslant 3$, $\zeta_{2^M} \in K(\zeta_N)$ implies $2^M \mid N$ by Lemma 2.3.1, so by Proposition 2.4.3 we have $\zeta_{2^M}\sqrt{\beta} \in K(\zeta_N)$ if and only if $2^M \cdot 15 \mid N$ or $2^M \cdot 35 \mid N$. We may conclude because Theorem 2.2.1 gives

$$K(\zeta_{2^m}, \sqrt[2^m]{\alpha}) \cap K(\mu_\infty) = \begin{cases} K(\zeta_{2^{m+2}}) & \text{if } m \leqslant 3 \\ K(\zeta_{2^6}\sqrt{\beta}) & \text{if } m = 4, 5 \\ K(\zeta_{2^m}, \sqrt{\beta}) & \text{if } m \geqslant 6\,. \end{cases}$$

Example 2.7.4. Let $K = \mathbb{Q}(\zeta_4, \sqrt{17})$ and let $\alpha = 8(13\sqrt{17}+51)(4\zeta_4-1)$. With [The21] we can check that $K(\sqrt[4]{\alpha})$ is the subextension of degree 8 of $\mathbb{Q}(\zeta_{4\cdot 17})/\mathbb{Q}(\zeta_4)$, and then by Lemma 2.3.4 that $K(\sqrt[4]{\alpha}) \subseteq K(\zeta_N)$ holds if and only if $17 \mid N$. Since $K(\sqrt{\alpha})$ is the quartic subextension of $\mathbb{Q}(\zeta_{4\cdot 17})/\mathbb{Q}(\zeta_4)$, we also have that $\sqrt{\alpha} \in K(\zeta_N)$ holds if and only if $17 \mid N$. We can apply Theorem 2.2.1 to get, for $m \geqslant 1$ and $2^m \mid N$:

$$B(N, 2^m) = \begin{cases} 4 & \text{if } m \geqslant 2 \text{ and } 17 \mid N \\ 2 & \text{if } m = 1 \text{ and } 17 \mid N \\ 1 & \text{otherwise}\,. \end{cases}$$

Number fields without quadratic subfields

Let K be a number field without quadratic subfields, i.e. such that the maximal subextension of K which is Galois over $\mathbb{Q}$ has odd degree. In particular $K \cap \mathbb{Q}(\mu_\infty)$ has odd degree, and $K \cap \mu_\infty = \{\pm 1\}$. So for K we only need to study the 2-adelic failure: if $\alpha \in K^\times \setminus \{\pm 1\}$, then we write $F = K(\zeta_{2^m}, \sqrt[2^m]{\alpha}) \cap K(\mu_\infty)$ and we compute the 2-adelic failure

$$B(N, 2^m) = [F \cap K(\zeta_N) : K(\zeta_{2^m})]$$

for all $N, m \geqslant 1$ such that $2^m \mid N$. We can write $\alpha = \pm\beta^{2^d}$ where $d \geqslant 0$ and $\beta \in K^\times$ is such that $\pm\beta \notin K^{\times 2}$. Notice that $\sqrt[4]{\beta} \notin K(\mu_\infty)$ by Schinzel's Theorem on abelian radical extensions (see [Sch77, Theorem 2]). We can apply Theorem 2.2.1 to compute F, and we have

$$B(N, 2^m) = \begin{cases} 2 & \text{if } F = K(\zeta_{2^{m+1}}) \text{ and } \zeta_{2^{m+1}} \in K(\zeta_N), \\ & \text{or if } F = K(\zeta_{2^m}, \sqrt{\beta}) \text{ and } \sqrt{\beta} \in K(\zeta_N), \\ & \text{or if } m \geqslant 2,\ F = K(\zeta_{2^{m+1}}\sqrt{\beta}), \text{ and } \zeta_{2^{m+1}}\sqrt{\beta} \in K(\zeta_N) \\ 1 & \text{otherwise}\,. \end{cases}.$$

To determine whether the given elements are in $K(\zeta_N)$, we can apply the following Proposition.

Proposition 2.7.5. *There is a finite procedure to determine whether $\sqrt{\beta} \in K(\mu_\infty)$. In this case there exists unique a minimal integer $x \geqslant 1$ such that $\sqrt{\beta} \in K(\zeta_x)$. Moreover, if*

$e \geqslant 3$, then there exists unique a minimal integer $y_e \geqslant 1$ such that $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_{y_e})$. We have $y_e = \mathrm{lcm}(2^e, x)$ unless $e = v_2(x) = 3$, where we have $y_e = x/2$. We can determine x (and hence y_e) with a finite procedure.

Proof. We have $\sqrt{\beta} \in K(\mu_\infty)$ if and only if there is some squarefree integer m (it is unique) such that $K(\sqrt{\beta}) = K(\sqrt{m})$, which means $\beta m \in K^{\times 2}$. In this case, since $K \cap \mathbb{Q}(\mu_\infty)$ has odd degree over $\mathbb{Q}$, we have that x is the unique conductor of $\mathbb{Q}(\sqrt{m})$, and y_e is the unique conductor of $\mathbb{Q}(\zeta_{2^e}\sqrt{m})$. To check if m exists and, if so, to determine it, it suffices to find a finite set to which m belongs: an odd prime divisors of m is such that there is some prime $\mathfrak{p}$ of K above it which ramifies in $K(\sqrt{\beta})$, so the $\mathfrak{p}$-adic valuation of the fractional ideal (β) is odd (see [HPST21, Lemma 2]). □

Example 2.7.6. Consider the number field $K = \mathbb{Q}(T)$, where T is a root of $X^4+8X+12$. By [Cona, Remark 4.16] K has no quadratic subfields because the Galois group of $K/\mathbb{Q}$ is isomorphic to A_4. Let $\alpha = 2T + 3 = -(T^2/2)^2$, so with the above notation we have $\beta = T^2/2$ and $d = 1$. Since $K(\sqrt{\beta}) = K(\sqrt{2})$, we have $\sqrt{\beta} \in K(\zeta_x)$ if and only if $8 \mid x$. By Theorem 2.2.1 (where $t = 1$ and $h = 1$) and by Proposition 2.7.5 we deduce that for $m, N \geqslant 1$ and $2^m \mid N$ we have

$$B(N, 2^m) = \begin{cases} 2 & \text{if } m = 1 \text{ and } 4 \mid N \\ 1 & \text{otherwise}. \end{cases}$$

2.8 The ℓ-adelic failure for ℓ odd

The 3-adelic falilure for multiquadratic number fields containing ζ_3

Let K be a multiquadratic number field containing ζ_3, and let $m, N \geqslant 1$ be such that $3^m \mid N$. If $\alpha \in K^\times$, then we set $F = K(\zeta_{3^m}, \sqrt[3^m]{\alpha}) \cap K(\mu_\infty)$ and we compute the 3-adelic failure

$$B(N, 3^m) = [F \cap K(\zeta_N) : K(\zeta_{3^m})].$$

This computation is evident if α is a root of unity, so we exclude this case and we write $\alpha = \beta^{3^d}$ with $d \geqslant 0$ or $\alpha = \zeta_3\beta^{3^d}$ with $d \geqslant 1$, where $\beta \in K^\times$ is strongly 3-indivisible. We can apply Theorem 2.2.1 to compute F, and we have

$$B(N, 3^m) = \begin{cases} 3 & \text{if } F = K(\zeta_{3^{m+1}}) \text{ and } 3^{m+1} \mid N, \\ & \text{or if } F = K(\zeta_{3^m}, \sqrt[3]{\beta}) \text{ and } \sqrt[3]{\beta} \in K(\zeta_N), \\ & \text{or if } m \geqslant 2,\ F = K(\zeta_{3^{m+1}}\sqrt[3]{\beta}), \text{ and } \zeta_{3^{m+1}}\sqrt[3]{\beta} \in K(\zeta_N) \\ 1 & \text{otherwise}. \end{cases}$$

To determine whether the given elements are in $K(\zeta_N)$ we can apply the following result:

Proposition 2.8.1. *We can check whether $K(\sqrt[3]{\beta})/\mathbb{Q}$ is abelian with an explicit finite procedure. In this case, if $e \geqslant 0$, then there is precisely one minimal integer $x \geqslant 1$ such that $\zeta_{3^e}\sqrt[3]{\beta} \in K(\zeta_x)$, and x is computable. If $e \geqslant 3$, then $x = \mathrm{lcm}(3^e, y)$, where y is the minimal integer such that $\sqrt[3]{\beta} \in K(\zeta_y)$, which is computable.*

Proof. Since $K(\sqrt[3]{\beta})/K$ has degree 3, we have $K(\sqrt[3]{\beta}) = KL$ for some number field L such that $L/\mathbb{Q}(\zeta_3)$ is an extension of degree 3. Moreover, we have

$$K(\sqrt[3]{\beta}) \subseteq K(\zeta_x) \quad \Leftrightarrow \quad L \subseteq \mathbb{Q}(\zeta_3, \zeta_x)\,.$$

Thus to check if $K(\sqrt[3]{\beta})/\mathbb{Q}$ is abelian it suffices to check whether $\beta/g \in K^{\times 3}$ for any of the finitely many elements g as in [HPST21, Theorem 9], where we take N to be the product of 3 and all primes congruent to 1 modulo 3 that ramify in $K(\sqrt[3]{\beta})$ (which can be found with [HPST21, Lemma 2]). The same result provides the minimal $y \geqslant 1$ such that $\sqrt[3]{g}$, or equivalently $\sqrt[3]{\beta}$, is in $K(\zeta_y)$.

For $e = 1$ we may reduce to the case $e = 0$ because $\zeta_3 \in K$, and the same holds for $e = 2$ because we may replace β with $\zeta_3\beta$. Finally, if $e \geqslant 3$ and $\zeta_{3^e}\sqrt[3]{\beta} \in K(\zeta_x)$, then we need $3^e \mid x$. Else $K(\zeta_x, \zeta_{3^e}) = K(\zeta_x, \sqrt[3]{\beta})$ would be impossible because the latter field does not contain ζ_{3^e}. □

Example 2.8.2. Let K be a multiquadratic number field containing ζ_3. Then the element $\alpha = \frac{21\sqrt{-3}-7}{2}$ is such that $\sqrt[3]{\alpha}$ generates the cubic subextension of $\mathbb{Q}(\zeta_{21})/\mathbb{Q}(\zeta_3)$. Thus, 7 is the minimal integer $z \geqslant 1$ such that $\sqrt[3]{\alpha} \in \mathbb{Q}(\zeta_{3z})$. For $m \geqslant 1$ and $3^m \mid N$ we have:

$$[K(\zeta_{3^m},\ \sqrt[3^m]{\alpha}) \cap K(\zeta_N) : K(\zeta_{3^m})] = \begin{cases} 3 & \text{if } 7 \mid N \\ 1 & \text{otherwise}\,. \end{cases}$$

The 5-adelic failure for $\mathbb{Q}(\zeta_5)$

Let $K = \mathbb{Q}(\zeta_5)$, and let $m, N \geqslant 1$ with $5^m \mid N$. If $\alpha \in K^\times$, then we set

$$F = K(\zeta_{5^m},\ \sqrt[5^m]{\alpha}) \cap K(\mu_\infty)$$

and compute the 5-adelic failure

$$B(N, 5^m) = [F \cap K(\zeta_N) : K(\zeta_{5^m})]\,.$$

We proceed as in the previous subsection: without loss of generality α is not a root of unity, and we associate to it some $\beta \in K^\times$ which is strongly 5-indivisible. We can apply Theorem 2.2.1 to compute F, and we have

$$B(N, 5^m) = \begin{cases} 5 & \text{if } F = K(\zeta_{5^{m+1}}) \text{ and } 5^{m+1} \mid N, \\ & \text{or if } F = K(\zeta_{5^m}, \sqrt[5]{\beta}) \text{ and } \sqrt[5]{\beta} \in K(\zeta_N), \\ & \text{or if } m \geqslant 2,\ F = K(\zeta_{5^{m+1}}\sqrt[5]{\beta}), \text{ and } \zeta_{5^{m+1}}\sqrt[5]{\beta} \in K(\zeta_N) \\ 1 & \text{otherwise}\,. \end{cases}$$

To determine whether the given elements are in $K(\zeta_N)$ we can apply the following result:

Proposition 2.8.3. *We can check whether $K(\sqrt[5]{\beta})/\mathbb{Q}$ is abelian with an explicit finite procedure. In this case, if $e \geqslant 0$, then there is precisely one minimal $x \geqslant 1$ such that $\zeta_{5^e}\sqrt[5]{\beta} \in K(\zeta_x)$, and x is computable. If $e \geqslant 3$, then $x = \operatorname{lcm}(5^e, y)$, where y is the minimal integer such that $\sqrt[5]{\beta} \in K(\zeta_y)$, which is computable.*

Proof. The statement is analogous to Proposition 2.8.1, thus we can prove analogously the last assertion and we may reduce to the case $e = 0$. So, let $e = 0$. Since x is minimal, then we have $x \mid 25t$, where t is either 1 or it is a squarefree product of prime numbers congruent to 1 modulo 5, and we may take t to be the product of the prime numbers $p \neq 5$ ramifying in $K(\sqrt[5]{\alpha})$. We may find these p with Lemma 2.1.4, and having $p \not\equiv 0, 1 \bmod 5$ for some p ramifying in $K(\sqrt[5]{\beta})$ already implies that $K(\sqrt[5]{\beta})/\mathbb{Q}$ is not abelian. Then to check if $K(\sqrt[5]{\beta})/\mathbb{Q}$ is abelian it suffices to check whether $\beta/g \in K^{\times 5}$ for some of the finitely many elements g as in Lemma 2.8.4 (where $N = 5t$). We conclude because we know the minimal integer x such that $\sqrt[5]{g} \in K(\zeta_x)$. □

Lemma 2.8.4. *Let $N = \prod_{i=1}^{r} p_i$, where the p_i's are distinct prime numbers such that $p_i = 5$ or $p_i \equiv 1 \pmod 5$. Set $\beta_5 = \zeta_5$, and for $p_i \neq 5$ let $\beta_{p_i} \in K^\times$ be such that $K(\sqrt[5]{\beta_i})$ is the subextension of $K(\zeta_{p_i})/K$ of degree 5 (to find β_i see [HPST22, Section 4]).*

The extension $\mathbb{Q}(\zeta_{5N})/K$ has $(5^r - 1)/4$ subextensions of degree 5. They are of the form $K(\sqrt[5]{g})$, where

$$g = \prod_{\emptyset \neq I \subseteq \{1,\dots,r\}} \beta_{p_i}^{e_i}, \qquad e_i \in \{1, 2, 3, 4\}.$$

Moreover, for every $x \geqslant 1$ we have $K(\sqrt[5]{g}) \subseteq \mathbb{Q}(\zeta_{5x})$ if and only if $p_i \mid x$ for every $i \in I$.

Proof. The field $K(\sqrt[5]{g})$ is contained in $\mathbb{Q}(\zeta_{5x})$ if $p_i \mid x$ for every $i \in I$ by definition of the β_i's. Conversely, if $K(\sqrt[5]{g}) \subseteq \mathbb{Q}(\zeta_{5x})$, then $p_i \mid x$ because $\sqrt[5]{\beta_i} \in \mathbb{Q}(\zeta_{5x})$. In particular, $K(\sqrt[5]{g})/K$ has degree 5.

There are $5^r - 1$ elements g as in the statement, and they generate $(5^r - 1)/4$ distinct extensions (because $K(\sqrt[5]{g_1}) = K(\sqrt[5]{g_2})$ holds if and only if $g_1 \cdot g_2^e \in K^{\times 5}$ for some $e \in \{1, 2, 3, 4\}$).

We conclude by proving that $\mathbb{Q}(\zeta_{5N})/K$ has $(5^r - 1)/4$ subextensions of degree 5. Its Galois group G is such that $G/G^5 \simeq (\mathbb{F}_5)^r$. Thus counting the kernels of the surjective group homomorphisms $G \to \mathbb{F}_5$ amounts to counting the kernels of the surjective linear maps $(\mathbb{F}_5)^r \to \mathbb{F}_5$. These are precisely the vector subspaces of $(\mathbb{F}_5)^r$ of codimension 1: by orthogonality w.r.t. the standard scalar product (after having fixed a basis) they correspond to the vector subspaces of dimension 1 and we conclude. □

Example 2.8.5. Let $K = \mathbb{Q}(\zeta_5)$ and let $\alpha = \zeta_5\beta^5$, where $\beta = 11(15\zeta_5^3 + 35\zeta_5^2 + 25\zeta_5 + 41)$. We can check with [The21] that $\sqrt[5]{\beta}$ generates the subextension of $\mathbb{Q}(\zeta_{55})/\mathbb{Q}(\zeta_5)$ of degree 5. Thus 11 is the minimal integer $z \geqslant 1$ such that $\sqrt[5]{\beta} \in \mathbb{Q}(\zeta_{5z})$. We then have, for $m \geqslant 1$ and $5^m \mid N$:

$$[K(\zeta_{5^m}, \sqrt[5^m]{\alpha}) \cap K(\zeta_N) : K(\zeta_{5^m})] = \begin{cases} 5 & \text{if } m = 1 \text{ and } 5^2 \mid N, \text{ or} \\ & \text{if } m = 2 \text{ and } 5^3 \cdot 11 \mid N, \text{ or} \\ & \text{if } m \geqslant 3 \text{ and } 11 \mid N \\ 1 & \text{otherwise}. \end{cases}$$

CHAPTER 3

Kummer theory for products of one-dimensional tori

This Chapter is based on the joint work with Antonella Perucca [PP23], and its main focus is to investigate Kummer theory for products of one-dimensional tori defined over number fields. Our main result is the following:

Theorem 3.0.1. *Let T be a finite product of one-dimensional tori defined over a number field K, and fix a finitely generated subgroup G of $T(K)$. If n, N are positive integers such that n divides N, then there is an explicit finite procedure to determine whether T is split over $K(T[N], \frac{1}{n}G)$ and to compute the degree of this field over K and over $K(T[N])$.*

To prove this theorem we fully describe the procedure mentioned in the statement, see Section 3.2 for the case of a single one-dimensional torus and Section 3.3 for the general case. Then in Section 3.4 we prove the following result:

Theorem 3.0.2. *Let T be a finite product of one-dimensional tori defined over $\mathbb{Q}$, and fix a finitely generated subgroup G of $T(\mathbb{Q})$. There exists an explicit finite procedure to compute at once the degree of all extensions $\mathbb{Q}(T[N], \frac{1}{n}G)/\mathbb{Q}(T[N])$, for all n, N positive integers such that n divides N.*

The above result is stated over $\mathbb{Q}$ for simplicity, however one may generalize it to those number fields such that the analogous computations are feasible. For example, by Theorem 2.0.1 we have the following:

Remark 3.0.3. In Theorem 3.0.1 we may compute at once the degree of the torsion-Kummer extensions for all n and N if the splitting field of T is multiquadratic.

Finally, in Section 3.5 we present various examples of computations of the degree of torsion-Kummer extensions. Notice that the results about one-dimensional tori from Sections 3.1 and 3.2 may be used to study further arithmetic problems.

The challenge is to study Kummer theory for all tori, and in this Chapter settle a first important case in higher-dimension.

3.1 Torsion fields of one-dimensional tori

Fix a number field K and some algebraic closure $\bar{K}$. Let T be a non-split one-dimensional torus over K with splitting field L, and call $T(K)$ the group of K-points. Every such torus is defined by the equation $x^2 - dy^2 = 1$ for some $d \in K^\times$ which is not a square and its splitting field is $L = K(\sqrt{d})$, see for example [Vos98, §4.9]. Over L the above equation becomes $(x + \sqrt{d}y)(x - \sqrt{d}y) = 1$ thus for every field $L \subseteq F \subseteq \bar{K}$ the map

$$T(F) \hookrightarrow F^\times \qquad (x, y) \mapsto x + \sqrt{d}y \tag{3.1}$$

is a bijection (the image of $T(K)$ consists of the elements of $L^\times$ whose L/K-norm is 1). The multiplication of $\bar{K}^\times$ induces a group law for T, namely we have

$$(x_1, y_1) * (x_2, y_2) = (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1)\,. \tag{3.2}$$

For every positive integer N we let $\zeta_N \in \bar{K}$ be a root of unity of order N and write $\mu_N = \langle \zeta_N \rangle$. Moreover, we call $T[N] \subset T(\bar{K})$ the group of points of order dividing N. By (3.1) we have the following group isomorphism:

$$\mu_N \to T[N] \qquad \zeta \mapsto \Big(\frac{\zeta + \zeta^{-1}}{2}, \frac{\zeta - \zeta^{-1}}{2\sqrt{d}} \Big)\,. \tag{3.3}$$

We set $\mathbb{Q}_N := \mathbb{Q}(\zeta_N)$ and call $\mathbb{Q}_N^+$ the largest totally real subfield of $\mathbb{Q}_N$. Moreover, we use the notation $K_N := K(\zeta_N)$ and $K_N^+ := K \cdot \mathbb{Q}_N^+$. We call $K(T[N])$ the smallest extension of K over which the points of $T[N]$ are defined. We write K_{2^∞}, K_∞ for the union of the fields K_{2^m}, K_N and we similarly define $K(T[2^\infty])$ and $K(T[\infty])$. We clearly have $K(T[1]) = K(T[2]) = K$. If N is odd, then we have $K(T[2N]) = K(T[N])$ hence to study the torsion fields we may suppose that either N is odd or $4 \mid N$.

Proposition 3.1.1. *Let $N, M \geqslant 3$ with $M \mid N$. Then we have*

$$K(T[N]) = K_N^+ \Big(\frac{\zeta_M - \zeta_M^{-1}}{\sqrt{d}} \Big) = K_N^+ \cdot K(T[M])\,. \tag{3.4}$$

In particular, $K(T[N])$ is at most quadratic over K_N^+ and we have $L(T[N]) = L_N$. Thus $L \subseteq K(T[N])$ holds if and only if $L \subseteq K_N^+$ or $K_N^+ = K_N$ (for example, it holds if $\zeta_4 \in K$).

Proof. By (3.3) we get $K(T[M]) = K_M^+(\frac{\zeta_M - \zeta_M^{-1}}{\sqrt{d}})$ and this implies the second equality in (3.4). We conclude the proof of (3.4) because $(\zeta_N - \zeta_N^{-1})/(\zeta_M - \zeta_M^{-1})$ is a real number contained in $\mathbb{Q}_N$. If $L \not\subseteq K_N^+$, then $L \subseteq K(T[N])$ holds if and only if $\sqrt{d}$ and $\frac{\zeta_N - \zeta_N^{-1}}{\sqrt{d}}$ generate the same quadratic extension over K_N^+, that means $\zeta_N - \zeta_N^{-1} \in K_N^+$ and hence $K_N^+ = K_N$. □

Remark 3.1.2. If $4 \mid N$, then by (3.4) we have

$$K(T[N]) = K_N^+(\sqrt{-d})\,. \tag{3.5}$$

Moreover, if N is odd and w is its squarefree part, then $L \subseteq K(T[N])$ holds if and only if $L \subseteq K(T[w])$ because by (3.4) the degree of $K(T[N])/K(T[w])$ is odd.

Theorem 3.1.3. *Suppose that $\zeta_4 \notin K$ and $4 \mid N$, and write $N = wt2^e$, where wt is odd and w is the squarefree part of wt. Let $r \geqslant 2$ be the largest integer such that $\mathbb{Q}_{2^r}^+ \subseteq K$. If $e \leqslant r$, then $L \subseteq K(T[N])$ holds if and only if $L \subseteq K_{4w}^+$ or $\zeta_4 \in K_{4w}^+$. If $e \geqslant r+1$, then $L \subseteq K(T[N])$ holds if and only if $L \subseteq K(T[w2^{r+1}])$ if and only if $L \subseteq K_{w2^{r+1}}^+$ or $\zeta_4 \in K_{w2^{r+1}}^+$.*

Proof. We make repeated use of (3.5), and by Remark 3.1.2 we may assume $t = 1$. Notice that we have $\mathbb{Q}_{w2^e}^+ = \mathbb{Q}_{4w}^+ \cdot \mathbb{Q}_{2^e}^+$. If $e \leqslant r$ then $K(T[N]) = K_{4w}^+(\sqrt{-d}) \cdot \mathbb{Q}_{2^e}^+ = K_{4w}^+(\sqrt{-d})$. Therefore if $L \subseteq K_{4w}^+$ or $\zeta_4 \in K_{4w}^+$, then $L \subseteq K(T[N])$, while if $\sqrt{d}, \zeta_4 \notin K_{4w}^+$, then $K_{4w}^+(\sqrt{d}) \neq K_{4w}^+(\sqrt{-d})$ hence $L \not\subseteq K(T[N])$. Now let $e \geqslant r+1$. Notice that if $L \subseteq K_{w2^{r+1}}^+$ or $\zeta_4 \in K_{w2^{r+1}}^+$, then $L \subseteq K(T[w2^{r+1}])$, while if $\sqrt{d}, \zeta_4 \notin K_{w2^{r+1}}^+$, then $K_{w2^{r+1}}^+(\sqrt{d}) \neq K_{w2^{r+1}}^+(\sqrt{-d})$ hence $L \not\subseteq K(T[w2^{r+1}])$. To conclude, suppose that $L \not\subseteq K(T[w2^{r+1}])$ and hence $K \cap \mathbb{Q}_{2^\infty} = \mathbb{Q}_{2^r}^+$. Let $K' = K_{4w}^+(\sqrt{-d})$, so we have $K' \cap \mathbb{Q}_{2^\infty} \subseteq \mathbb{Q}_{2^\infty}^+$ because $\zeta_4, \zeta_{2^{r+1}} - \zeta_{2^{r+1}}^{-1} \notin K'$ and $K' \cap \mathbb{Q}_{2^\infty}$ is at most a quadratic extension of $\mathbb{Q}_{2^r}^+$. Therefore $K' \cdot \mathbb{Q}_{2^\infty}^+ \cap \mathbb{Q}_{2^\infty} = \mathbb{Q}_{2^\infty}^+$ and, as $\zeta_4 \in L \cdot K'$, we deduce that $L \not\subseteq K(T[w2^\infty]) = K' \cdot \mathbb{Q}_{2^\infty}^+$.

□

3.2 Kummer theory for a non-split one-dimensional torus

Let T be a non-split one-dimensional torus defined over a number field K, and call L the splitting field. Let G be a finitely generated and torsion-free subgroup of $T(K)$. For all positive integers N, n with $n \mid N$, consider the torsion-Kummer extension $K(T[N], \frac{1}{n}G)$ which is obtained by adding to $K(T[N])$ the coordinates of all points $P \in T(\bar{K})$ such that $nP \in G$. We present an explicit finite procedure to compute the degree of the extension $K(T[N], \frac{1}{n}G)/K$. Notice that for $n = 1$ we are computing the degree of $K(T[N])/K$, thus we can also determine the degree of $K(T[N], \frac{1}{n}G)$ over $K(T[N])$. Also notice that we could remove the assumption that G is torsion-free because, if the torsion subgroup of G has order t, then we can reduce to the torsion-free case replacing N by $\mathrm{lcm}(N, nt)$. We call $G' \subset L^\times$ the image of G under (3.1).

Remark 3.2.1. We have

$$\left[K\Big(T[N],\frac{1}{n}G\Big):K\right]=\begin{cases}2[L(\zeta_N,\sqrt[n]{G'}):L] & \text{if } L\subseteq K(T[N],\frac{1}{n}G)\\ [L(\zeta_N,\sqrt[n]{G'}):L] & \text{otherwise}.\end{cases}$$

Thus we may reduce to the multiplicative group (and do the computations thanks to [DP16]) provided that we can determine whether $L\subseteq K(T[N],\frac{1}{n}G)$. We may suppose that n is a power of 2 because, if n is odd, then the degree of $K(T[N],\frac{1}{n}G)/K(T[N])$ is odd.

We are left to investigate the following question:

Question 3.2.2. *Given $N\geqslant 1$ and $m\geqslant 0$ with $2^m\mid N$, do we have $L\subseteq K(T[N],\frac{1}{2^m}G)$?*

Notice that we could easily investigate Question 3.2.2 also if G is not torsion-free, reducing to the torsion-free case by replacing N.

Theorem 3.2.3 ([Per17, Lemmas 3.3 and 3.4])**.** *We have $L\subseteq K\big(\frac{1}{2}G\big)$ if and only if there is some $P\in G$ such that $L\subseteq K\big(\frac{1}{2}P\big)$. This means, identifying P with its image $P'\in L^\times$ by* (3.1)*, that $\sqrt{P'}\in L$ and $N_{L/K}(\sqrt{P'})\neq 1$. If a basis of G is given and P exists, then we may take P to be a sum of a subset of basis elements.*

Consider $K':=K(T[4])=K(\sqrt{-d})$ and suppose w.l.o.g. that $\zeta_4\notin K'$. We call $L'=L(\zeta_4)$. We let $s\geqslant 2$ be the largest integer satisfying $\mathbb{Q}_{2^s}^+\subseteq K'$. For $s\geqslant 3$, we call $\mathbb{Q}_{2^s}^-$ the subextension of $\mathbb{Q}_{2^s}$ of relative degree 2 which is neither $\mathbb{Q}_{2^s}^+$ nor $\mathbb{Q}_{2^{s-1}}$. By [Per17, Theorem 2.3] we know that $K(T[2^s])=K'$ and we have either $K'\cap\mathbb{Q}_{2^\infty}=\mathbb{Q}_{2^{s+1}}^-$ and $L'=K'_{2^{s+1}}=K(T[2^{s+1}])$, or $K'\cap\mathbb{Q}_{2^\infty}=\mathbb{Q}_{2^s}^+$ and $L'=K'_{2^s}\not\subseteq K(T[2^\infty])$.

Consider a $\mathbb{Z}$-basis $P_1,\dots,P_r$ for G and its image under (3.1). Up to replacing this basis of G' in a computable way, see [DP16, Theorem 14], we may suppose that it is of the form $\xi_i a_i^{2^{\delta_i}}$, where the a_i's are strongly 2-independent elements of $(L')^\times$, the δ_i's are non-negative integers and the ξ_i's are roots of unity in L' of order 2^{h_i} for some non-negative integer h_i such that $h_i=0$ or $\zeta_{2^{h_i+\delta_i}}\notin L'$. If $\zeta_4\notin K'$, then we have $N_{L'/K'}(a_i)\in\{\pm 1\}$ by [Per17, proof of Lemma 3.8].

Theorem 3.2.4 ([Per17, Theorems 3.9 and 3.10])**.** *With the above notation, suppose that $\zeta_4\notin K'$. Consider the property $L'\subseteq K'(T[2^v],\frac{1}{2^m}G)$ for non-negative integers $v\geqslant m$.*

1. *If $L'=K'_{2^{s+1}}=K(T[2^{s+1}])$, then the property holds if and only if $v\geqslant s+1$ or*

$$\min(\{s+1\}\cup\{s+1-h_i:i\in I\}\cup\{\delta_j:j\in J\})\leqslant m$$

   where I consists of the indices satisfying $h_i\neq 0$ and J of the indices satisfying $h_j=0$ and $N_{L'/K'}(a_j)=-1$.

2. *If $L'=K'_{2^s}\not\subseteq K(T[2^\infty])$, then the property holds if and only if there is some $j\in J$ such that $\delta_j\leqslant m$ and*

$$h_j + \delta_j \leqslant \max(\{v\} \cup \{h_i + \min(m, \delta_i) : i \notin J\} \cup \{h_i + \min(m, \delta_i - 1) : i \in J\})$$

where J is the set of indices j satisfying $N_{L'/K'}(a_j) = -1$.
Thus $L \subseteq K(T[2^\infty], \frac{1}{2^\infty}G)$ holds if and only if $J \neq \emptyset$.

We conclude this section by answering Question 3.2.2. By (3.5), if $\zeta_4 \in K'$ and $L \not\subseteq K(T[N])$, then $4 \nmid N$ hence $L \subseteq K\big(T[N], \frac{1}{2^m}G\big)$ holds if and only if $m = 1$ and there exists P as in Theorem 3.2.3 with base field $K(T[N])$. Now assume $\zeta_4 \notin K'$: by Theorem 3.2.4 we may determine whether $L \subseteq K(T[2^v], \frac{1}{2^m}G)$ holds for any integer $v \geqslant \max(2, m)$, as this is equivalent to $L' \subseteq K'(T[2^v], \frac{1}{2^m}G)$.

Suppose that $4 \mid N$, and write $N = wt2^v$, where wt is odd and with squarefree part w. By Remark 3.1.2 we reduce to the case $t = 1$. If $L \subseteq K(T[4w])$, then we are done. Else, we replace K by $K(T[4w]) = K^+_{4w}(\sqrt{-d})$ and, since again $\zeta_4 \notin K$, we have reduced to the known case where N is a power of 2.

Finally suppose that $4 \nmid N$ hence $m \in \{0, 1\}$. By Proposition 3.1.1 we can determine whether $L \subseteq K(T[N])$. If not, then we consider the largest subfield $F \subseteq K(T[N])$ whose Galois group over K has exponent dividing 2, and we investigate whether $L \subseteq F(\frac{1}{2}G)$ with Theorem 3.2.3.

3.3 Kummer theory for a product of one-dimensional tori

Let $T = \prod_{i=1}^r T_i$ be a finite product of one-dimensional tori defined over a number field K, and let $L_i = K(\sqrt{d_i})$ be the splitting field of T_i.

Remark 3.3.1. For $N = 1, 2$ we have $K(T[N]) = K$, while for $N \geqslant 3$ by Proposition 3.1.1 we have

$$K(T[N]) = K^+_N\Big(\sqrt{d_1d_2}, \ldots, \sqrt{d_1d_r}, \frac{\zeta_N - \zeta_N^{-1}}{\sqrt{d_1}}\Big). \tag{3.6}$$

We may thus compute the degree of $K(T[N])/K$ (this is an extension of K^+_N obtained by adding square roots). Moreover, all T_i are isomorphic over $K(T[N])$ because they are either all split over $K(T[N])$ or none is, and they are all split over $K(T[N], \sqrt{d_1})$.

We fix a finitely generated subgroup G of $T(K)$ and consider the group G_i consisting of the coordinates in T_i of the points in G.

Remark 3.3.2. For $N \geqslant 1$ the extension $K(T[N], \frac{1}{2}G)/K(T[N])$ is generated by square-roots of elements of $K(T[N])$. Indeed, if $P = (x, y) \in G_i \backslash T_i[2]$, then by [Per17, Lemma 3.1] we have $K(\frac{1}{2}P) = K(\sqrt{2(x + 1)})$.

Proof of Theorem 3.0.1. Avoiding trivial cases we may suppose that either $N \geqslant 3$ or $N = n = 2$. By Remark 3.3.3 we reduce to the case in which all G_i are torsion-free.

We then reduce to the case where the T_i's are pairwise not K-isomorphic (up to replacing G). Indeed, having a point in the power of a torus amounts to having a group of points on the torus, so we may suppose that $T_i \neq T_j$ for $i \neq j$. Moreover, if w.l.o.g. T_1 and T_2 are K-isomorphic, then we may replace T_2 by T_1 because, if $H_1 \subset T_1(K)$ and H_2 denotes its isomorphic image in T_2, then we have

$$K\Big(T_1[N], \frac{1}{n}H_1\Big) = K\Big(T_2[N], \frac{1}{n}H_2\Big).$$

For the case $N = n = 2$ see Remark 3.3.2, while for $N \geqslant 3$ we reduce to a single one-dimensional torus over $K(T[N])$ by Remark 3.3.1, and then we refer to Section 3.2. □

Remark 3.3.3. If G_i has a torsion group of order t_i, then we may reduce to the case where G is torsion-free provided that we work over the torsion field

$$K\Big(T_1[\mathrm{lcm}(N, nt_1)], \dots, T_r[\mathrm{lcm}(N, nt_r)]\Big). \tag{3.7}$$

For $N \geqslant 3$ this field is

$$K^+_{\mathrm{lcm}(N, nt_1, \dots, nt_r)}\Big(\sqrt{d_1d_2}, \dots, \sqrt{d_1d_r}, \frac{\zeta_N - \zeta_N^{-1}}{\sqrt{d_1}}\Big)$$

while for $N = n = 2$ it is

$$K^+_{\mathrm{lcm}(2t_1, \dots, 2t_r)}\Big(\frac{\zeta_{t_1} - \zeta_{t_1}^{-1}}{\sqrt{d_1}}, \dots, \frac{\zeta_{t_r} - \zeta_{t_r}^{-1}}{\sqrt{d_r}}\Big),$$

so the degree of this torsion field is computable, similarly to Remark 3.3.1.

Remark 3.3.4. For every i, let n_i be a positive integer dividing N, and call n their least common multiple. Then the compositum of the fields $K(T_i[N], \frac{1}{n_i}G_i)$ equals $K(T[N], \frac{1}{n}G')$, where G' is any finitely generated subgroup of $T(K)$ whose points have coordinates in T_i that form the group $G'_i = \frac{n}{n_i}G_i$.

3.4 Products of one-dimensional tori defined over $\mathbb{Q}$

This section is devoted to the proof of Theorem 3.0.2. We write $T = \prod_{i=1}^r T_i$, where T_i is given by the equation $x^2 - d_iy^2 = 1$ for some squarefree $d_i \in \mathbb{Q}$. By Theorem 3.0.1 we can deal with finitely many pairs (N, n) so we may suppose $N \geqslant 3$ and we apply Remark 3.3.1 to work with T_1 over $\mathbb{Q}(T[N])$.

Remark 3.4.1. We may compute at once the degree of $\mathbb{Q}(T[N])$ for all $N \geqslant 1$, where w.l.o.g. N is odd or $4 \mid N$. Indeed, by (3.6) we have

$$\mathbb{Q}(T[N]) = \mathbb{Q}^+_N\Big(\sqrt{-d_1}, \dots, \sqrt{-d_r}\Big) \tag{3.8}$$

if $4 \mid N$ since $(\zeta_N - \zeta_N^{-1}) \cdot \sqrt{-1} \in \mathbb{Q}^+_N$, and

$$\mathbb{Q}(T[N]) = \mathbb{Q}^+_N\Big(\sqrt{-pd_1}, \dots, \sqrt{-pd_r}\Big) \tag{3.9}$$

if N is odd and it has some prime divisor $p \equiv 3 \bmod 4$, since $(\zeta_N - \zeta_N^{-1}) \cdot \sqrt{-p} \in \mathbb{Q}_N^+$. Else, we have

$$[\mathbb{Q}(T[N]) : \mathbb{Q}_N^+] = 2[\mathbb{Q}_N^+(\sqrt{d_1 d_2}, \dots, \sqrt{d_1 d_r}) : \mathbb{Q}_N^+]. \tag{3.10}$$

Indeed, in this last case the field $\mathbb{Q}_N^+(\frac{\zeta_N - \zeta_N^{-1}}{\sqrt{d_1}})$ has degree 2 over the field $\mathbb{Q}_N^+$ and their exponents over $\mathbb{Q}$ differ by a factor 2. Thus the former field is not contained in a compositum of the latter with a multiquadratic field. We conclude by Lemma 3.4.2.

Lemma 3.4.2. *If $c, c_1, \dots, c_n$ are rational numbers, then there is an explicit finite procedure to compute at once the degree of $\mathbb{Q}_N^+(\sqrt{c_1}, \dots, \sqrt{c_n})/\mathbb{Q}_N^+$ for all $N \geqslant 1$ and to determine those $N \geqslant 1$ such that $\sqrt{c} \in \mathbb{Q}_N^+(\sqrt{c_1}, \dots, \sqrt{c_n})$.*

Proof. The second assertion follows from the first (applied to $c_1, \dots, c_n$ and $c, c_1, \dots, c_n$ respectively). For the first assertion suppose w.l.o.g. that the degree of $\mathbb{Q}(\sqrt{c_1}, \dots, \sqrt{c_n})$ is 2^n. Then we may compute the requested degree for all N as

$$\frac{2^n}{\#\left\{ I \subseteq \{1, \dots, n\} \ : \ \prod_{i \in I} \sqrt{c_i} \in \mathbb{Q}_N^+ \right\}}. \tag{3.11}$$

Given a squarefree positive integer z, it is a standard fact (see for example [Was97, Ch. 2]) that $\sqrt{z} \in \mathbb{Q}_N$ if and only if $m_z \mid N$, where $m_z = z$ if $z \equiv 1 \pmod 4$ and $m_z = 4z$ otherwise. Therefore we can compute the denominator of (3.11) at once for all N. □

We work now over the base field $K = \mathbb{Q}(\sqrt{d_1 d_2}, \dots, \sqrt{d_1 d_r})$. As each T_i is split over $L = K(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_n})$, the torus T over the field K is isomorphic to T_1^r and has splitting field L. The image of the group G under this isomorphism is generated by points of the form

$$\left(x_j, \frac{y_j \sqrt{d_j}}{\sqrt{d_1}} \right) \qquad \text{where} \quad (x_j, y_j) \in T_j(\mathbb{Q}) \quad \text{for some } j \in \{1, \dots, r\}.$$

We may suppose that the image of G is torsion free up to replacing N by $\operatorname{lcm}(N, nt)$, where t is the order of its torsion subgroup (notice that $t \mid 24$ because L is multiquadratic). Calling G' the image of this group in $L_N^\times$, by Theorem 2.0.1 we may compute the degree of all extensions $L_N(\sqrt[n]{G'})/L_N$ at once.

Notice that $K(T_1[N]) = \mathbb{Q}(T[N])$ for $N \geqslant 3$. By the above discussion and by Remark 3.2.1, to conclude the proof of Theorem 3.0.2 it suffices to answer Question 3.2.2 for T_1 over the field K for every N and m at once.

We first determine those $N \geqslant 3$ such that $\sqrt{d_1} \in \mathbb{Q}(T[N])$, where without loss of generality N is odd or $4 \mid N$. By Remark 3.4.1 the suitable N are those for which d_1 is the squarefree part of:

- a subproduct of $(-d_1) \cdots (-d_r)$ times a positive divisor of N (respectively, an odd positive divisor of N) if $8 \mid N$ (respectively, if $4 \mid N$ but $8 \nmid N$);

- a subproduct of $(-pd_1)\cdots(-pd_r)$ times a positive divisor of N congruent to $1 \bmod 4$, if N is odd and $p \mid N$ holds for some prime number $p \equiv 3 \bmod 4$;
- a subproduct of $(d_1d_2)\cdots(d_1d_r)$ times a positive divisor of N, if all primes $p \mid N$ are such that $p \equiv 1 \bmod 4$.

We now determine those $N \geqslant 3$ such that $\sqrt{d_1} \in \mathbb{Q}(T[N], \frac{1}{2}G)$, where w.l.o.g. N is odd or $4 \mid N$. By Remark 3.3.2, this field is the extension of $\mathbb{Q}(T[N])$ obtained by adding, for every generator (a_h, b_h) of G, the element $\sqrt{2(a_h+1)}$. Recall that $a_h \in \mathbb{Q}$, so by Remark 3.4.1 we can apply Lemma 3.4.2 to find the suitable N. Notice that, if all prime divisors of N are congruent to $1 \bmod 4$, then the condition is

$$\sqrt{d_1} \in \mathbb{Q}_N^+\Big(\sqrt{d_1d_2}, \ldots, \sqrt{d_1d_r}, \sqrt{2(a_h+1)}\Big).$$

Finally, suppose that $m \geqslant 2$ hence $4 \mid N$. We first determine whether $\sqrt{d_1} \in \mathbb{Q}(T[N])$, and we reduce to the case $\sqrt{d_1} \notin \mathbb{Q}(T[N])$. If $8 \mid N$, then we also have $\sqrt{d_1} \notin \mathbb{Q}(T[2^\infty N])$, as for every positive integer t the maximal field of exponent 2 over $\mathbb{Q}$ contained in $\mathbb{Q}(T[2^tN])$ is the same. If $8 \nmid N$, then $\sqrt{d_1} \in \mathbb{Q}(T[2^\infty N])$ is equivalent to $\sqrt{d_1} \in \mathbb{Q}(T[2N])$ (because $8 \mid 2N$) and hence to $\mathbb{Q}(\sqrt{d_1}, T[N]) = \mathbb{Q}(T[2N])$, so we can determine by Lemma 3.4.2 which N satisfy this condition.

Consider the multiquadratic field $L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_r})$ and its extensions L_N. We apply Lemma 3.4.3 over L to find, for all N such that $4 \mid N$, appropriate generators for the subgroup of $L^\times$ corresponding to G (we use below the notation of the lemma). Lemma 3.4.3 provides a finite partition of the integers N for which the divisibility parameters of the group G' in L_N stay the same in each subset of the partition. Therefore we need to apply Theorem 3.2.4 over $\mathbb{Q}(T[N])$ only for finitely many N.

Consider the case $\sqrt{d_1} \in \mathbb{Q}(T[2N])$ and hence $8 \nmid N$ and $m = 2$. We can apply Theorem 3.2.4 (1) to T_1 over $\mathbb{Q}(T[N])$, noticing that $s = 2$ because $\sqrt{d_1} \notin \mathbb{Q}(T[N])$. Thus $\sqrt{d_1} \in \mathbb{Q}(T[N], \frac{1}{4}G)$ holds if and only if

$$\min(\{3\} \cup \{3 - h_i : i \in I\} \cup \{\delta_j : j \in J\}) \leqslant 2\,. \tag{3.12}$$

Now consider the remaining case $\sqrt{d_1} \notin \mathbb{Q}(T[2^\infty N])$. Recall that the 2-adic valuation v of N is at least m. Applying Theorem 3.2.4 (2) to T_1 over $\mathbb{Q}(T[N])$ we have $\sqrt{d_1} \in \mathbb{Q}(T[N], \frac{1}{2^m}G)$ if and only if $J \neq \emptyset$ and (v, m) satisfies, for some $j \in J$, the two conditions $\delta_j \leqslant m$ and

$$\begin{aligned} h_j + \delta_j \leqslant \max(\{v\} &\cup \{h_i + \min(m, \delta_i) : i \notin J\} \\ &\cup \{h_i + \min(m, \delta_i - 1) : i \in J\}). \end{aligned}$$

If $m \geqslant \max\{\delta_j\}$, then the second condition does not depend on m and we only need to check it for $v < \max\{h_j + \delta_j\}$. If m is small and fixed, then for each j we check the first condition, and then we check the second condition for $v < h_j + \delta_j$. This leaves only finitely many pairs (v, m) to be checked.

This concludes the investigation of Question 3.2.2 and also the proof of Theorem 3.0.2.

Lemma 3.4.3. *Let L be a multiquadratic number field, and let H be a torsion-free subgroup of $L^\times$. We may compute at once, for all $N \geqslant 1$ such that $4 \mid N$, a $\mathbb{Z}$-basis of H whose elements are of the form $\xi_i a_i^{2^{\delta_i}}$, where $\xi_i \in \mu_8$, $\delta_i \geqslant 0$, and where the elements $a_i \in L_N^\times$ are strongly 2-independent. Moreover, we may suppose that the order of ξ_i equals 2^{h_i} where $h_i = 0$ or $\zeta_{2^{h_i+\delta_i}} \notin L_N$. There is a finite partition of the integers N such that ξ_i, δ_i, a_i are the same for all N in each subset of the partition.*

Proof. As $4 \mid N$, we may suppose w.l.o.g. that $\zeta_4 \in L$. Notice that, up to refining the partition in the end, the condition on the parameters h_i can be easily dealt with: if $\zeta_{2^{h_i+\delta_i}} \in L_N$, then we can change a_i by a root of unity to ensure $h_i = 0$. It suffices to determine ξ_i, δ_i, a_i for N odd because these objects are the same for $2^m N$ (strongly 2-independent elements in L_N are still strongly 2-independent in $L_{2^m N}$ by [DP16, Proposition 9]).

By [DP16, Theorem 14] we may determine the requested basis for $N = 1$, calling $A_1, \dots, A_r$ the involved strongly 2-independent elements. Consider the finite set S consisting of the 2^a-th roots of

$$\zeta_{2^b} \prod_I A_i^{2^{c_i}} \tag{3.13}$$

where $I \subseteq \{1, \dots, r\}$ and a, b, c_i are non-negative integers such that $b \in \{0, 1, 2, 3\}$ and a and c_i satisfy the following restrictions:

- $a \leqslant 3$ and $c_i < a$ for all i, if $b = 0$;
- $a + b \leqslant 6$ and $0 < a - c_i \leqslant 3$ for all i, if $b \neq 0$.

We define a partition of the integers N such that the elements belonging to the same subset of the partition have the same intersection $S \cap L_N$ (we can determine this intersection for all N as seen in Sections 2.4 and 2.5). Notice that $\zeta_{16} \notin L_N$ and that no product $\prod_{i \in J} A_i$ for any non-empty $J \subseteq \{1, \dots, r\}$ has a 16-th root in L_∞ by Theorem 1.0.3. Thus if for some element of the form (3.13) we have $a - c_i > 3$ for some $i \in I$, then its 2^a-th root is not in L_∞. Moreover, if $c_i \geqslant a$ for some i, we can reduce to the product over $I \setminus \{i\}$. If $b = 0$, then increasing a and all c_i by the same amount does not change $S \cap L_N$. If $b \neq 0$, the root of (3.13) is equal to

$$\zeta_{2^{a+b}} \prod_I \sqrt[2^{a-c_i}]{A_i}.$$

If this element belongs to L_N for some N, then $L_N(\prod_I \sqrt[2^{a-c_i}]{A_i}) = L_N(\zeta_{2^{a+b}})$ is an extension of degree at most $2^{\max_i(a-c_i)}$ of L_N, hence $a + b \leqslant 3 + \max_i(a - c_i) \leqslant 6$. Therefore we can lift the restrictions above without changing the defined partition.

In each subset of the partition we may use the same ξ_i, δ_i, a_i, thus we only need to apply [DP16, Theorem 14] over L_N for finitely many N. Indeed, the algorithm from [DP16, Theorem 14] only involves elements of $S \cap L_N$, and it applies with exactly the same steps for N, N' satisfying $S \cap L_N = S \cap L_{N'}$, leading to the same a_i and the same parameters δ_i and h_i. □

3.5 Examples

Example 3.5.1. Consider the torus T over $\mathbb{Q}$ given by $x^2 + 5y^2 = 1$. The splitting field $L = \mathbb{Q}(\sqrt{-5})$ is not contained in

$$\mathbb{Q}(T[5]) = \mathbb{Q}_5^+\left(\frac{\zeta_5 - \zeta_5^{-1}}{\sqrt{-5}}\right) = \mathbb{Q}\left(\sqrt{5}, \sqrt{\frac{5+\sqrt{5}}{8}}\right).$$

The point $P = (\frac{1}{9}, \frac{4}{9})$ corresponds to $P' = -(\frac{2-\sqrt{-5}}{3})^2 \in L^\times$. Since $\sqrt{P'} \notin L$, Theorem 3.2.3 implies $L \not\subseteq \mathbb{Q}(T[10], \frac{1}{2}P)$ hence by Remark 3.2.1 the degree of $\mathbb{Q}(T[10], \frac{1}{2}P)$ is 4. Alternatively, one may compute that $\mathbb{Q}(T[10])$ has degree 4 and notice by Remark 3.3.2 that $\mathbb{Q}(T[10], \frac{1}{2}P) = \mathbb{Q}(T[10], \frac{2}{3}\sqrt{5}) = \mathbb{Q}(T[10])$.

Example 3.5.2. Let $K = \mathbb{Q}_4$ and consider the torus $x^2 - 2y^2 = 1$ over K whose splitting field is $L = \mathbb{Q}_8$. The point $P = (3, 2)$ corresponds to $P' = (1+\sqrt{2})^2$ and we have $\sqrt{P'} \in L$ and $N_{L/K}(1+\sqrt{2}) = -1$ so by Theorem 3.2.3 we get $L \subseteq K(\frac{1}{2}P)$. The point $Q = (\frac{9}{7}, \frac{4}{7})$ corresponds to $Q' = \frac{9+4\sqrt{2}}{7}$ and we have $\sqrt{Q'} \notin \mathbb{Q}(\sqrt{2})$ because $63 + 28\sqrt{2}$ is not a square in $\mathbb{Z}[\sqrt{2}]$, so by Theorem 3.2.3 we get $L \not\subseteq K(\frac{1}{2}Q)$.

In the following examples we consider a torus $T = T_1 \times T_2$ over a number field K, where for $i = 1, 2$ the torus T_i is defined by $x^2 - d_i y^2 = 1$ for some $d_i \in K$. For $N \geqslant 3$ by (3.6) we have

$$K(T[N]) = K(T_1[N], \sqrt{d_1 d_2}).$$

Example 3.5.3. If $d_1 = 5$, $d_2 = 13$, and $K = \mathbb{Q}$, then by Remark 3.3.1 the tori T_1 and T_2 are isomorphic and not split over $F = \mathbb{Q}(T[8]) = \mathbb{Q}_8^+(\sqrt{-5}, \sqrt{-13})$. We call L the splitting field of T over F. To study $\mathbb{Q}(T[8], \frac{1}{8}P)$ for the point $P = ((\frac{2207}{2}, \frac{987}{2}); (\frac{497}{81}, \frac{136}{81}))$ in $T(\mathbb{Q})$ we replace P by the group $H \subset T_1(F)$ generated by $P_1 = (\frac{2207}{2}, \frac{987}{2})$ and $P_2 = (\frac{497}{81}, \frac{136\sqrt{13}}{81\sqrt{5}})$. We check with Theorem 3.2.4 that T_1 is split over $F(\frac{1}{8}H)$. We have $\zeta_4 \notin F(T_1[2^\infty])$, and the points P_1, P_2 correspond to a_1^{16}, a_2^4, where $a_1 = \frac{1+\sqrt{5}}{2}$, $a_2 = \frac{2+\sqrt{13}}{3}$ are strongly 2-independent over $F(\sqrt{5})$, and $N_{L/F}(a_1) = N_{L/F}(a_2) = -1$: we conclude because $\delta_2 = 2 \leqslant 3$, $\delta_1 = 4$, and $h_1 = h_2 = 0$, so that $h_2 + \delta_2 \leqslant h_1 + \min(3, \delta_1 - 1)$.

Example 3.5.4. Let $d_1 = 3$, $d_2 = 7$, $K = \mathbb{Q}$, and consider the point $P = ((7, 4); (\frac{4}{3}, \frac{1}{3}))$ in $T(\mathbb{Q})$. We have $F = \mathbb{Q}(T[6]) = \mathbb{Q}(\sqrt{-1}, \sqrt{21})$ and $F(\frac{1}{2}P) = F(\sqrt{2})$ by Remark 3.3.2. The degree of $F(\frac{1}{3}P)/F$ is the same as that of $L(\sqrt[3]{H})/L$, where $L = F(\sqrt{3})$ and H is generated by $a = 7 + 4\sqrt{3}$ and $b = (4 + \sqrt{7})/3$. The degree is 9 because a, b, ab, ab^2 are not cubes in $L^\times$. We conclude that $\mathbb{Q}(T[6], \frac{1}{6}P)$ is a number field of degree 72.

Example 3.5.5. Let $d_1 = -2$, $d_2 = -3$, $K = \mathbb{Q}$, and consider $P = ((-\frac{7}{9}, \frac{4}{9}); (\frac{11}{13}, \frac{4}{13}))$ in $T(\mathbb{Q})$. By Remark 3.3.1 we have $\mathbb{Q}(T[98]) = \mathbb{Q}_{49}^+(\sqrt{14}, \sqrt{6})$ hence by Remark 3.3.2 we get $\mathbb{Q}(T[98], \frac{1}{2}P) = \mathbb{Q}_{49}^+(\sqrt{14}, \sqrt{6}, \sqrt{13/3})$, which is a number field of degree 168.

Finally, we give two examples where we apply the procedure seen in Section 3.4.

Example 3.5.6. Consider the torus T over $\mathbb{Q}$ defined by $x^2 - 3y^2 = 1$ with splitting field $L = \mathbb{Q}(\sqrt{3})$, and the point $P = (7, 4)$. We determine those N, n such that $L \subseteq \mathbb{Q}(T[N], \frac{1}{n}P)$, with $n \mid N$ and w.l.o.g. $n = 2^m$. Notice first that $L \subseteq \mathbb{Q}(T[N])$ holds if and only if $12 \mid N$. Therefore for $m = 0, 1$ the suitable N are the multiples of 12, as $\mathbb{Q}(T[N]) = \mathbb{Q}(T[N], \frac{1}{2}P)$. If $m \geqslant 2$, we show that the suitable N are the multiples of 12 or of 8. Suppose in fact that $L \not\subseteq \mathbb{Q}(T[N])$ i.e. $12 \nmid N$. The point P corresponds to a^2, where $a = 2 + \sqrt{3} \in L^\times$ is strongly 2-independent in L. If $8 \mid N$, then $a = (\frac{1+\sqrt{3}}{\sqrt{2}})^2 \in L_N$ is the square of an element with norm -1 over $\mathbb{Q}(T[N])$, while a is not a fourth power in L_N for any N by Theorem 1.0.3 because $\zeta_4 \notin L$ and $\sqrt{a} \notin L_4$. As seen in Section 3.4, we must have $L \not\subseteq \mathbb{Q}(T[2^\infty N])$ hence we apply Theorem 3.2.4 (2): if $8 \nmid N$, then $J = \emptyset$ and hence $L \not\subseteq \mathbb{Q}(T[N], \frac{1}{4}P)$; if $8 \mid N$, then m and the 2-adic valuation v of N satisfy the given conditions hence $L \subseteq \mathbb{Q}(T[N], \frac{1}{2^m}P)$.

Example 3.5.7. Consider the torus $T = T_1 \times T_2$ over $\mathbb{Q}$, where T_1 is defined by $x^2 - 2y^2 = 1$ and T_2 by $x^2 - 3y^2 = 1$. Also consider the point $P = ((\frac{9}{7}, \frac{4}{7}); (7, 4))$ in $T(\mathbb{Q})$. By Remark 3.3.1 we replace P by the group $H \subset T_1(\mathbb{Q}(\sqrt{6}))$ generated by $P_1 = (\frac{9}{7}, \frac{4}{7})$ and $P_2 = (7, 2\sqrt{6})$. We thus determine the positive integers N, n with $n \mid N$ and w.l.o.g. $n = 2^m$ such that the splitting field $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is contained in $\mathbb{Q}(T[N], \frac{1}{n}H)$. Clearly $\sqrt{2} \in \mathbb{Q}(T[N])$ holds if and only if $8 \mid N$ or $12 \mid N$, and we have $\sqrt{2} \in \mathbb{Q}(T[N], \frac{1}{2}H) = \mathbb{Q}(T[N], \sqrt{14})$ if and only if $8 \mid N$ or $12 \mid N$ or $28 \mid N$. Now suppose $m \geqslant 2$ and $\sqrt{2} \notin \mathbb{Q}(T[N], \frac{1}{2}H)$. Hence we only need to consider $m = 2$ and N divisible by 4 and not by $8, 12, 28$. The point P_1 corresponds to some $a \in L^\times$ that is not plus or minus a square, and that is a square in L_N if and only if $\sqrt{7} \in L_N$ (i.e. $28 \mid N$ or $21 \mid N$), as $\frac{9}{7} + \frac{4\sqrt{2}}{7} = \frac{(2\sqrt{2}+1)^2}{7}$. The point P_2 corresponds to b^4 for $b = \frac{\sqrt{2}}{2} + \frac{\sqrt{6}}{2} \in L^\times$ that is not a square in $L_N^\times$ by Theorem 1.0.3 because $\zeta_4 \notin \mathbb{Q}(\sqrt{3})$, $b^2 \in \mathbb{Q}(\sqrt{3})$ and $b \notin \mathbb{Q}(\zeta_4, \sqrt{3})$. Moreover, $ab \in L_N^\times$ is not a square, else (for some possibly larger N) a and ab but not b would be squares. Since $\sqrt{2} \in \mathbb{Q}(T[2N]) \setminus \mathbb{Q}(T[N])$ we only need to check (3.12), which is not satisfied as $I = J = \emptyset$, so we find no further suitable N. We conclude that $L \subseteq \mathbb{Q}(T[N], \frac{1}{n}G)$ holds if and only if $8 \mid N$, or $12 \mid N$, or we have $2 \mid n$ and $28 \mid N$.

CHAPTER 4

Kummer theory for p-adic fields

This Chapter is joint work with Antonella Perucca [PP24b], and its main focus is on the development of Kummer theory for the *p-adic fields* (namely, the finite extensions of the field of p-adic numbers $\mathbb{Q}_p$).

We fix some p-adic field K and a finitely generated subgroup G of $K^\times$. For all positive integers N, n such that $n \mid N$ we consider the Kummer extension

$$K(\zeta_N, \sqrt[n]{G})/K(\zeta_N).$$

and we aim at computing their degrees with a finite procedure, for all N, n at once. Given the prime factorization $n = \prod_{\ell|n} \ell^m$, by Kummer theory (see Chapter 1) the degree of the Kummer extension above is the product of the degrees

$$[K(\zeta_N, \sqrt[\ell^m]{G}) : K(\zeta_N)] = \frac{[K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) : K(\zeta_{\ell^m})]}{[K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) \cap K(\zeta_N) : K(\zeta_{\ell^m})]}. \tag{4.1}$$

To compute the numerator in (4.1), we show more generally how to compute

$$[K(\zeta_{\ell^M}, \sqrt[\ell^m]{G}) : K(\zeta_{\ell^M})]$$

for all positive integers $M \geqslant m$, see Section 4.2. We rely on the method for number fields, adapting it to the specificities of p-adic fields (the case $\ell = p$ requires a different definition of the divisibility parameters).

As for the denominator in (4.1), we show more generally how to compute the degree

$$[K(\zeta_n, \sqrt[n]{G}) \cap K(\zeta_N) : K(\zeta_n)]$$

for all positive integers N, n such that $n \mid N$, see Section 4.4. These degrees measure the *entanglement* between Kummer extensions and cyclotomic extensions, which is described explicitly in Section 4.3 (see Theorem 4.3.2).

Finally, in Section 4.5 we compare Kummer extensions of number fields to the corresponding Kummer extensions of p-adic fields obtained by completion (completing number fields with respect to the non-zero prime ideals of their ring of integers). We prove in particular (see Theorem 4.5.5) that there is a positive density of primes of the number field such that the local Kummer degree is the same as the global Kummer degree.

4.1 Preliminaries on p-adic fields

A very valuable introduction to the theory of p-adic fields is [Ser86]. We fix an algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, and some p-adic field $K \subseteq \bar{\mathbb{Q}}_p$. We write $[K : \mathbb{Q}_p] = ef$, where e is the ramification index and f is the degree of the maximal unramified subextension of $K/\mathbb{Q}_p$. The residue field of K is the finite field $\mathbb{F}_{p^f}$. Let $\mathcal{O}_K$ be the ring of integers of K, and let $\pi \in \mathcal{O}_K$ be a uniformizer. We call v_K the valuation on K extending the normalized valuation on $\mathbb{Q}_p$ and such that $v_K(\pi) = 1/e$.

Cyclotomic extensions of $\mathbb{Q}_p$. For every positive integer n we denote by ζ_n a root of unity in $\bar{\mathbb{Q}}_p$ of order n, and by μ_n the group of roots of unity of order dividing n. We write μ_∞ for the group of all roots of unity inside $\bar{\mathbb{Q}}_p$. Remark that for every positive integer n the cyclotomic extension $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ is abelian.
Supposing $p \nmid n$, this cyclotomic extension is unramified at p and it is cyclic because its Galois group is isomorphic to the one of $\mathbb{F}_p(\zeta_n)/\mathbb{F}_p$. In particular, for every positive integer z there exists n coprime to p such that z is the degree of $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$.
For every positive integer k the cyclotomic extension $\mathbb{Q}_p(\zeta_{p^k})/\mathbb{Q}_p$ has degree $\varphi(p^k)$ and it is totally ramified at p. If $p \neq 2$, then it is cyclic, while for every $k \geqslant 2$ the Galois group of $\mathbb{Q}_2(\zeta_{2^k})/\mathbb{Q}_2$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$. Moreover, if n is coprime to p, then we have $\mathbb{Q}_p(\zeta_n) \cap \mathbb{Q}_p(\zeta_{p^k}) = \mathbb{Q}_p$. Thus for every positive integer N we know the structure of the Galois group of $\mathbb{Q}_p(\zeta_N)/\mathbb{Q}_p$. In particular, for $p \neq 2$ (respectively, $p = 2$), this group can be generated by 2 (respectively, 3) elements.
Considering the supernatural numbers p^∞ and $p_0^\infty := \prod_{\ell \text{ prime}, \ell \neq p} \ell^\infty$, the cyclotomic fields $\mathbb{Q}_p(\zeta_{p^\infty})$ and $\mathbb{Q}_p(\zeta_{p_0^\infty})$ are then linearly disjoint over $\mathbb{Q}_p$.

Roots of unity and the unit group. Define $\mu_K := \mu_\infty \cap K$ and $\tau := \#(\mu_K)$, and for any prime ℓ write $\tau_\ell := \ell^{v_\ell(\tau)}$. For every $\ell \neq p$ we have $v_\ell(\tau) = v_\ell(p^f - 1)$ hence $(p^f - 1) \mid \tau$. Moreover, $\mathbb{Q}_p(\zeta_{\tau_p}) \subseteq K$ implies that $\varphi(\tau_p) \mid e$. Notice that τ is even because $\mathbb{Z} \subseteq K$. We also define $d_p := [K(\zeta_p) : K]$, noticing that $d_p \mid (p-1)$ and that $d_p = 1$ if $p \mid \tau$. The unit group of $\mathcal{O}_K$ is the group

$$\mathcal{O}_K^\times \cong \mu_{p^f-1} \times (1 + \pi\mathcal{O}_K) \cong \mu_K \times \mathbb{Z}_p^{ef} \tag{4.2}$$

where $\mathbb{Z}_p^{ef}$ is an additive group and the second isomorphism is induced by the p-adic logarithm (see for example [Rob00, Chapter 5 §4.5]). For any prime number $\ell \neq p$ we consider the projection map

$$\mathrm{Proj}_\ell : \mathcal{O}_K^\times \to \mu_{\tau_\ell}$$

induced by (4.2) and by the projection $\mu_K \to \mu_{\tau_\ell}$. Since $\mu_{\tau_\ell} \subseteq \mu_{p^f-1}$, for every $\alpha \in \mathcal{O}_K^\times$ the ℓ-adic valuation of the order of $\mathrm{Proj}_\ell(\alpha)$, which we call $h_\ell(\alpha)$, is the same as the ℓ-adic valuation of the order of $(\alpha \bmod \pi) \in \mathbb{F}_{p^f}^\times$. We clearly have $h_\ell(\alpha) \leqslant v_\ell(\tau)$. Notice that for almost all ℓ, and in particular if $\ell \nmid \tau$, we have $h_\ell(\alpha) = 0$.

4.2 The ℓ-adic Kummer degrees

We fix a p-adic field K and a prime number ℓ. If z is a positive integer, we say that $\alpha \in K^\times$ is *ℓ^z-divisible* if α has some ℓ^z-th root in $K^\times$ (which implies $\ell^z \mid e \cdot v_K(\alpha)$). Only the elements in $\mathcal{O}_K^\times$ can be *ℓ^∞-divisible*, namely ℓ^z-divisible for every z. By (4.2) we get the following:

Remark 4.2.1. The p^∞-divisible elements are the roots of unity in K of order coprime to p, namely μ_{p^f-1}. For $\ell \neq p$, the ℓ^∞-divisible elements are those $\alpha \in \mathcal{O}_K^\times$ such that $(\alpha \bmod \pi) \in \mathbb{F}_{p^f}^\times$ has order coprime to ℓ. In general, $\alpha \in \mathcal{O}_K^\times$ equals a root of unity of order $\ell^{h_\ell(\alpha)}$ times an ℓ^∞-divisible element of $K^\times$. If $\alpha \notin \mathcal{O}_K^\times$, then $v_K(\alpha) \neq 0$ and for all ℓ not dividing $e \cdot v_K(\alpha)$ we have $\alpha\zeta \notin K^{\times \ell}$ for every $\zeta \in \mu_K$.

Remark 4.2.2. The p-adic logarithm is explicit hence we can apply the second isomorphism in (4.2) to check the p^z-th divisibility of an element in $\mathcal{O}_K^\times$. Another way to check this is with Hensel's Lemma. Indeed, $\alpha \in \mathcal{O}_K^\times$ is a p^z-th power if and only if there exists $u \in \mathcal{O}_K^\times$ such that $v_K(u^{p^z} - \alpha) > 2z/e$, see [Conb, Theorems 9.1 and 9.3]. By expanding $u = \sum_{i \geqslant 0} u_i \pi^i$ and α as power series in π (where the coefficients are zero or roots of unity in μ_{p^f-1}) we are left to check solvability for a system with finitely many polynomial equations in $\mathbb{F}_{p^f}[(u_1 \bmod \pi), \ldots, (u_{2z} \bmod \pi)]$.

We fix some finitely generated subgroup G of $K^\times$, aiming at computing the degree and the structure of the Galois group of $K(\zeta_{\ell^M}, \sqrt[\ell^m]{G})/K(\zeta_{\ell^M})$ for all positive integers $m \leqslant M$ (all at once). We call $D(\ell^M, \ell^m)$ the degree of this extension, which is a power of ℓ.

Remark 4.2.3. There can be arbitrarily large integers n such that there are elements x in $K^\times \setminus \mu_K$ satisfying $x^{\ell^n} \in G$ and $x^{\ell^{n-1}} \notin G$ (thus [DP16, Lemma 12] does not hold for p-adic fields). If $\ell \neq p$, this phenomenon is due to the ℓ^∞-divisible elements that are not roots of unity. If $\ell = p$, we may consider as an example a subgroup of $\mathcal{O}_{\mathbb{Q}_p}^\times$ (thanks to (4.2) we may work in $\mu_{\mathbb{Q}_p} \times \mathbb{Z}_p$): if G is generated by $(1,1)$ and $(1, \sum_{i=0}^\infty a_i p^i)$, where the sequence of coefficients $a_i \in \{0, \ldots, p-1\}$ is not eventually periodic, then $x := (1, \sum_{i=n}^\infty a_i p^{i-n})$ is such that $x^{p^n} \in G$ and $x^{p^{n-1}} \notin G$.

The p-adic Kummer degree.

We define *p-divisibility parameters* for G. These parameters differ from those for number fields [DP16, Section 3] but they allow to extend [DP16, Theorem 18] (and [DP16, Lemma 19] if $p = 2$ and $\zeta_4 \notin K$).

If $\log : \mathcal{O}_K^\times \to \mu_K \times \mathbb{Z}_p^{ef}$ is the isomorphism in (4.2), we also have the isomorphism

$$\begin{aligned}\phi : K^\times &\to \mu_K \times \mathbb{Z}_p^{ef} \times \mathbb{Z} \\ x &\mapsto (\log(x\pi^{-e\cdot v_K(x)}), e \cdot v_K(x)) .\end{aligned}$$

By composing ϕ with projection maps we define $\phi_0 : K^\times \to \mathbb{Z}_p^{ef} \times \mathbb{Z}$ and $\phi_p : K^\times \to \mu_{\tau_p}$. If $a \in \mathbb{Z}_p^{ef} \times \mathbb{Z}$ is not zero, we can define $v_p(a)$ as the minimum of the p-adic valuation of the non-zero entries of a.

Suppose that G is torsion-free and non trivial, and let $r > 0$ be its rank. In particular, $\phi_0(G)$ is isomorphic to G. Consider the $\mathbb{Z}_p$-module $\phi_0(G) \otimes_{\mathbb{Z}} \mathbb{Z}_p \subseteq \mathbb{Z}_p^{ef+1}$. Using the Smith normal form algorithm, we can find a basis $\gamma_1, \cdots, \gamma_s$ (where $s \leqslant \min(ef+1, r)$) such that $v_p(\gamma_1) \leqslant \cdots \leqslant v_p(\gamma_s)$ and moreover

$$v_p\left(\sum_{i=1}^{s} a_i p^{-v_p(\gamma_i)}\gamma_i\right) = 0$$

holds for all $a_i \in \{0, \cdots, p-1\}$ that are not all zero. We define the *d-parameters of p-divisibility* of G as the tuple $(d_1, \cdots, d_s)$ where $d_i := v_p(\gamma_i)$.

Let $\mathcal{B} := \{b_1, \ldots, b_r\}$ be a basis of G. We consider the matrix $M \in \mathrm{GL}_r(\mathbb{Z}_p)$ that maps $\phi_0(\mathcal{B})$ to the vectors $\gamma_1, \cdots, \gamma_s, 0, \cdots, 0$ and the matrix $M' \in \mathrm{GL}_r(\mathbb{Z}/\tau_p\mathbb{Z})$ such that $M \equiv M' \bmod \tau_p$. For all $i = 1, \ldots, r$ we define $h_i \in \mathbb{Z}_{\geqslant 0}$ as the p-adic valuation of the order of the i-th entry of

$$M' \begin{pmatrix} \phi_p(b_1) \\ \vdots \\ \phi_p(b_r) \end{pmatrix} .$$

Theorem 4.2.4. *If G is torsion-free with positive rank r, then for any positive integer n there exists a basis $g_1, \cdots, g_r$ of G such that*

$$g_i = A_i^{p^{d_i}}\xi_i \quad \textit{for } 1 \leqslant i \leqslant s \qquad \textit{and} \quad g_i \in \xi_i K^{\times p^n} \quad \textit{for } s < i \leqslant r$$

where $\xi_i \in \mu_K$ has order p^{h_i} and $A_i \in K^\times$ and the A_i's are strongly p-independent.

Proof. We let $\mathcal{B}$ and M be as above, and we suppose w.l.o.g. that $n \geqslant \max(d_s, v_p(\tau))$. Since M is invertible, we may choose $M' \in \mathrm{GL}_r(\mathbb{Z})$ such that $(M' \bmod p^n) = (M \bmod p^n)$. We let M' act on $(\mathbb{Z} \times \mathbb{Z}_p^{ef})^r$ and set $g_i' := M'(\phi_0(b_i))$. Then $g_1', \ldots, g_r'$ is a basis of $\phi_0(G)$ that satisfies $v_p(g_i') = d_i$ for $i \leqslant s$ and $v_p(g_i') \geqslant n$ otherwise. Moreover, we have

$$v_p\left(\sum_{i=1}^{s} a_i p^{-d_i} g_i'\right) = 0$$

for all $a_i \in \{0, \cdots, p-1\}$ that are not all zero. Thanks to this property, the elements $A_i := \phi^{-1}((1, p^{-d_i}g_i'))$ for $1 \leqslant i \leqslant s$ are strongly p-independent in $K^\times$. We also have $\phi^{-1}((1, g_i')) \in K^{\times p^n}$ for $s < i \leqslant r$.

Since $G \cap \mu_K = \{1\}$ there exists unique a basis $\mathcal{B}' = \{g_1, \cdots, g_r\}$ of G such that $\phi_0(\mathcal{B}') = M'\phi_0(\mathcal{B})$. The basis $\mathcal{B}'$ is as requested because we have $\phi(g_i) = (\zeta_i, g_i')$ for some root of unity ζ_i whose τ_p-part ξ_i has order p^{h_i}, as $n \geqslant v_p(\tau_p)$. □

Corollary 4.2.5. *With the above notation, suppose w.l.o.g. that $M \geqslant v_p(\tau)$ and (applying Theorem 4.2.4 with $n = m$) call $H := \langle g_1, \dots, g_s \rangle$. Let $h := \max(h_{s+1}, \cdots, h_r)$, setting $h = 0$ if $r = s$. Then we have*

$$K(\zeta_{p^M}, \sqrt[p^m]{G}) = K(\zeta_{p^{\max(M,m+h)}}, \sqrt[p^m]{H}).$$

In particular, we have

$$D(p^M, p^m) = p^{\max(M,m+h)-M}\left[K(\zeta_{p^{\max(M,m+h)}}, \sqrt[p^m]{H}) : K(\zeta_{p^{\max(M,m+h)}})\right].$$

Proof. For $i = s+1, \cdots, r$ we have $K(\zeta_{p^M}, \sqrt[p^m]{g_i}) = K(\zeta_{p^M}, \zeta_{p^{m+h_i}})$ and the statement follows. □

Remark 4.2.6. Since the given basis of H satisfies the assumptions of [DP16, Theorem 14], to compute the Kummer degree for H we may apply [DP16, Theorem 18] (and [DP16, Lemma 19] if $p = 2$ and $\zeta_4 \notin K$) to H with parameters of p-divisibility $(d_1, \cdots, d_s; h_1, \cdots, h_s)$. By inspecting those degree formulas, for all integers $n \leqslant N$ large enough we have

$$D(p^N, p^n) = D(p^n, p^n) \qquad \text{and} \qquad D(p^{n+1}, p^{n+1}) = p^s D(p^n, p^n)$$

and therefore we only need to compute finitely many degrees to determine $D(p^M, p^m)$ for all positive integers $m \leqslant M$.

Example 4.2.7. Consider the subgroup of $\mathbb{Q}_p^\times$ generated by g_1, g_2 where $\phi(g_1) = (1, 1, 0)$ and $\phi(g_2) = (1, \sum_{i=0}^{\infty} a_i p^i, 0)$, the sequence of coefficients $a_i \in \{0, \dots, p-1\}$ being not eventually periodic. Then we have $H = \langle g_1 \rangle$, $d_1 = 0$ and $h_1 = h_2 = 0$. Then for every $M \geqslant m \geqslant 1$ we have $D(p^M, p^m) = p^m$.

The ℓ-adic Kummer degree for $\ell \neq p$.

We fix some prime $\ell \neq p$. We define $d_\ell(G)$ as follows: if $G \subseteq \mathcal{O}_K^\times$, then $d_\ell(G) = \infty$; if $G \not\subseteq \mathcal{O}_K^\times$, then $d_\ell(G)$ is the minimum of $v_\ell(e \cdot v_K(\alpha))$ by varying $\alpha \in G \setminus \mathcal{O}_K^\times$.

First, we reduce to the case where 1 is the only element of G that is ℓ^∞-divisible. Denote by H the subgroup of $K^\times$ consisting of the ℓ^∞-divisible elements, and consider the subgroup GH/H of $K^\times/H$. Any class in GH/H is represented by an element of $K^\times$ of the form $\zeta\pi^D$ for some root of unity $\zeta \in \mu_K$ whose order is a power of ℓ and some non-negative integer D. Call G_ℓ the group consisting of these representatives, which is a finitely generated subgroup of $K^\times$ such that $G_\ell \cap H = \{1\}$. Moreover, remark that $K(\zeta_{\ell^n}, \sqrt[\ell^n]{G}) = K(\zeta_{\ell^n}, \sqrt[\ell^n]{G_\ell})$ and $d_\ell(G) = d_\ell(G_\ell)$.

Second, we may suppose w.l.o.g. that G_ℓ is torsion-free. Indeed, suppose that the torsion group of G_ℓ is generated by ζ_{ℓ^h} for some $h > 0$ and write $G_\ell = \langle \zeta_{\ell^h} \rangle \times G'_\ell$ for some torsion-free subgroup G'_ℓ of G_ℓ. Then we have

$$K\left(\zeta_{\ell^M}, \sqrt[\ell^m]{G_\ell}\right) = K\left(\zeta_{\max(\ell^M, \ell^{h+m})}, \sqrt[\ell^m]{G'_\ell}\right).$$

Since the unit group consists of products of roots of unity and ℓ^∞-divisible elements, we may now suppose w.l.o.g. that $G_\ell \cap \mathcal{O}_K^\times = \{1\}$. As we may clearly suppose that G_ℓ is non-trivial, we have reduced to the case where G_ℓ is cyclic, being generated by an element $\beta \notin \mathcal{O}_K^\times$ such that $v_\ell(e \cdot v_K(\beta)) = d_\ell(G)$. We can formally apply to $G_\ell = \langle\beta\rangle$ the theory presented in [DP16, Section 3], where the ℓ-divisibility parameters of G_ℓ are those of β, namely $(d_\ell(G), h_\ell(\beta))$. Supposing w.l.o.g. that $M \geqslant \max(m, v_\ell(\tau))$, [DP16, Theorem 18] gives

$$v_\ell\big(D(\ell^M, \ell^m)\big) = \max(0, h_\ell(\beta) - \delta + m - M) + \delta$$

where $\delta = \max(0, m - d_\ell(G))$.

Remark 4.2.8. Suppose that $G_\ell = \langle\beta\rangle$ is as above. We have $d_\ell(G) = 0$ for almost all primes and we have $h_\ell(\beta) = 0$ if $\tau_\ell = 0$. Therefore, for all but finitely many primes $\ell \neq p$ we have $D(\ell^M, \ell^m) = \ell^m$ for every $m \leqslant M$. In general, for $\ell \neq p$ and for all $n \leqslant N$ large enough (in particular, if $n \geqslant h_\ell(\beta) + d_\ell(G)$) we have

$$D(\ell^N, \ell^n) = D(\ell^n, \ell^n) \qquad \text{and} \qquad D(\ell^{n+1}, \ell^{n+1}) = \ell D(\ell^n, \ell^n)\,.$$

Therefore we only need to compute finitely many degrees to know $D(\ell^M, \ell^m)$ for all primes $\ell \neq p$ and for all positive integers $m \leqslant M$.

Example 4.2.9. For the group $G = \langle 35, 98\rangle$ inside $\mathbb{Q}_7^\times$ we have $D(2,2) = 2$ and $D(3,3) = 9$ because $G_2 = \langle -7\rangle$ and $G_3 = \langle \zeta_3, 7\rangle$.

4.3 Kummer extensions inside cyclotomic extensions

We consider a p-adic field K and work within an algebraic closure $\bar{\mathbb{Q}}_p$ containing K. The largest Kummer extension of K is the largest abelian extension of exponent τ, namely $K_{\mathrm{Kum}} := K(\sqrt[\tau]{a} : a \in K^\times)$. We study the *entanglement field*

$$K_{\mathrm{Ent}} := K_{\mathrm{Kum}} \cap K(\mu_\infty)\,.$$

We also define

$$K_{\mathrm{Ent},p} := K_{\mathrm{Kum}} \cap K(\mu_{p^\infty}) \qquad K_{\mathrm{Ent},p_0} := K_{\mathrm{Kum}} \cap K(\mu_{p_0^\infty})\,.$$

Lemma 4.3.1. *Suppose that $\zeta_{\ell^z} \in K$ for some prime ℓ and for some $z \geqslant 1$. Let $K(\beta)/K$ be a cyclic extension of degree ℓ^z, and let σ be a generator of its Galois group. Then $\alpha := \sum_{i=1}^{\ell^z} \zeta_{\ell^z}^i \sigma^i(\beta)$ is such that $K(\alpha) = K(\beta)$ and $\alpha^{\ell^z} \in K^\times$.*

Proof. We have $\alpha^{\ell^z} = \prod_i \zeta_{\ell^z}^{-i}\alpha = \prod_i \sigma^i(\alpha) \in K$, we have $\alpha \neq 0$ because the $\sigma^i(\beta)$'s are K-independent, and we have $K(\alpha) = K(\beta)$ because the $\sigma^i(\alpha)$'s are distinct. □

We remark that $\tau/\tau_p = p^f - 1$ and hence $\tau = p^f - 1$ if $p \nmid \tau$.

Theorem 4.3.2. *The extension K_{Ent}/K is finite and abelian of exponent τ. Moreover, we have*

$$K_{\mathrm{Ent}} = K_{\mathrm{Ent},p_0} K_{\mathrm{Ent},p} \qquad \text{and} \qquad K_{\mathrm{Ent},p_0} \cap K_{\mathrm{Ent},p} = K\,.$$

The extension $K_{\mathrm{Ent},p_0}/K$ is cyclic of degree τ, and we have $K_{\mathrm{Ent},p_0} = K(\zeta_{(p^{f\tau}-1)})$. We can write $K_{\mathrm{Ent},p_0} = K(\gamma_0)$ such that $\gamma_0^\tau \in K^\times$, setting

$$\gamma_0 := \begin{cases} \zeta_{\tau^2} & \text{if } p \nmid \tau \\ \alpha\zeta_{\tau^2/\tau_p} & \text{if } p \mid \tau\,, \end{cases}$$

where, letting q be a prime such that $v_p(\mathrm{ord}(p \bmod q)) \geqslant 2v_p(\tau) + v_p(f)$, the element α is as in Lemma 4.3.1 for the cyclic subextension of $K(\zeta_q)/K$ of degree τ_p.
Letting $r \geqslant 3$ be the greatest integer such that $(\zeta_{2^r} + \zeta_{2^r}^{-1})^2 \in K$, we have

$$K_{\mathrm{Ent},p} = \begin{cases} K(\zeta_p) = K(\sqrt[p-1]{-p}) & \text{if } p \neq 2 \text{ and } p \nmid \tau \\ K(\zeta_{2^r}) = K(\zeta_4, \zeta_{2^r} + \zeta_{2^r}^{-1}) & \text{if } p = 2 \text{ and } 4 \nmid \tau \\ K(\zeta_{\tau_p^2}) & \text{otherwise} \end{cases}$$

$$\text{and} \quad \mathrm{Gal}(K_{\mathrm{Ent},p}/K) \simeq \begin{cases} \mathbb{Z}/d_p\mathbb{Z} & \text{if } p \neq 2 \text{ and } p \nmid \tau \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p = 2 \text{ and } 4 \nmid \tau \\ \mathbb{Z}/\tau_p\mathbb{Z} & \text{otherwise}\,. \end{cases}$$

Proof. Since $K_{\mathrm{Ent},p_0}/K$ is unramified while $K_{\mathrm{Ent},p}/K$ is totally ramified, we have $K_{\mathrm{Ent},p_0} \cap K_{\mathrm{Ent},p} = K$. Clearly we have $K_{\mathrm{Ent},p_0} K_{\mathrm{Ent},p} \subseteq K_{\mathrm{Ent}}$, while the other inclusion follows from the fact that $K(\mu_\infty) = K(\zeta_{p_0^\infty}, \zeta_{p^\infty})$ and that K_{Ent,p_0}, $K_{\mathrm{Ent},p}$ are the largest Kummer subextensions of $K(\zeta_{p_0^\infty})/K$ and $K(\zeta_{p^\infty})/K$ respectively. Indeed, it suffices to show that any cyclic Kummer subextension of K_{Ent} is contained in $K_{\mathrm{Ent},p_0} K_{\mathrm{Ent},p}$, which can be done by working within a finite cyclotomic extension and decomposing the radical generating the Kummer extension.

The remaining assertions are easy to prove. First of all, $K_{\mathrm{Ent},p_0} = K(\zeta_{(p^{f\tau}-1)})$ and $K_{\mathrm{Ent},p_0}/K$ is cyclic of degree τ (this is the unique unramified extension of K of degree τ). It is clear that $\gamma_0^\tau \in K^\times$ and $K_{\mathrm{Ent},p_0} = K(\gamma_0)$ if $p \nmid \tau$, while the same assertions hold by Lemma 4.3.1 if $p \mid \tau$ (notice that the choice of q does not matter). If $2 \neq p \nmid \tau$, the largest extension of K of degree dividing τ inside $K(\zeta_{p^\infty})$ is $K(\zeta_p)$, as $(p-1) \mid \tau$ and the only subextension of $\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p$ of degree coprime to p is $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$. Similarly, the cases $p = 2$ and $p \mid \tau$ arise from the structure of the extension $\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p$. Finally, recalling e.g. from [Gou97, §5.6] that $(\zeta_p - 1)^{p-1} = -p$, we have $K(\zeta_p) = K(\sqrt[p-1]{-p})$. □

Remark 4.3.3. Define

$$\gamma := \begin{cases} \sqrt[p-1]{-p} & \text{if } p \neq 2 \text{ and } p \nmid \tau \\ \zeta_{2^r} + \zeta_{2^r}^{-1} & \text{if } p = 2 \text{ and } 4 \nmid \tau \\ \zeta_{\tau_p^2} & \text{otherwise}\,. \end{cases}$$

According to this case distinction, γ^{d_p}, γ^2, or γ^{τ_p} belongs to $K^\times$. We have $K_{\mathrm{Ent}} = K(R_K)$ where $R_K := \langle \gamma_0, \gamma \rangle$ or, if $p = 2$ and $4 \nmid \tau$, $R_K := \langle \zeta_4, \gamma_0, \gamma \rangle$. Notice that the quotient $R_K K^\times / K^\times$ is finite.

Example 4.3.4. For $p \neq 2$ we have $\mathrm{Gal}(\mathbb{Q}_{p\ \mathrm{Ent}}/\mathbb{Q}_p) \simeq (\mathbb{Z}/(p-1)\mathbb{Z})^2$ and hence

$$\mathbb{Q}_{p\ \mathrm{Ent}} = \mathbb{Q}_p(\zeta_{p(p^{p-1}-1)}) = \mathbb{Q}_p(\sqrt[p-1]{\zeta_{p-1}},\ \sqrt[p-1]{-p}) = \mathbb{Q}_p(\sqrt[p-1]{z_p},\ \sqrt[p-1]{-p})$$

for any $z_p \in \mathbb{Z}_p^\times$ whose residue in $\mathbb{F}_p^\times$ has order $p-1$, e.g. $z_3 = -1$ and $z_5 = 2$.

4.4 Computing the entanglement

Let K be a p-adic field, and fix a finitely generated subgroup G of $K^\times$. The aim of this section is computing the degrees

$$B(N,n) := [K(\zeta_n, \sqrt[n]{G}) \cap K(\zeta_N) : K(\zeta_n)]$$

adapting the method for number fields seen in Chapter 1.

Theorem 4.4.1. *For all positive integers n, N such that n divides N we have*

$$K(\zeta_n, \sqrt[n]{G}) \cap K(\zeta_N) = K(\zeta_n, H_{N,n}) \tag{4.3}$$

for some computable group $H_{N,n}$ (generated over $K^\times$ by at most two elements and possibly ζ_4) such that

$$H_{N,n}^{\gcd(n,\tau)} \subseteq K^\times \subseteq H_{N,n} \subseteq K_{\mathrm{Ent}}^\times \cap K(\zeta_N)^\times .$$

Moreover, $H_{N,n}$ belongs to a finite set independent of N, n, and we may take

$$H_{N,n} := H_n \cap K(\zeta_N) \qquad \textit{where} \qquad H_n := \sqrt[n]{GK^{\times n}} \cap K_{\mathrm{Ent}}^\times .$$

Proof. We have $H_n^{\gcd(n,\tau)} \subseteq K^\times$ (recall that K_{Ent}/K has exponent τ) and

$$K(\zeta_n, \sqrt[n]{G}) \cap K(\zeta_\infty) = K(\zeta_n, H_n) .$$

Then (4.3) holds for $H_{N,n} := H_n \cap K(\zeta_N)$. If S denotes the finite set of the subgroups of $R_K K^\times$ containing $K^\times$ (where R_K is as in Remark 4.3.3), then H_n is the largest $M \in S$ satisfying $M \subseteq \sqrt[n]{GK^{\times n}}$. We easily conclude because this condition is equivalent to $M^\tau \subseteq \sqrt[n]{G^\tau} K^{\times \tau}$ and it can be computed because R_K and G are finitely generated. □

Remark 4.4.2. Let t be the largest integer such that $K(\zeta_p) = K(\zeta_{p^t})$ if $p \neq 2$ and $K(\zeta_4) = K(\zeta_{2^t})$ if $p = 2$. We can write

$$\#\mu_{K(\zeta_N) \cap K_{\mathrm{Ent}}} = \begin{cases} p^{2v_p(\tau)-a}(p^{f\tau/b} - 1) & \text{if } p \neq 2,\ p \mid \tau \text{ or } p = 2,\ 4 \mid \tau \\ p^t(p^{f\tau/b} - 1) & \text{if } p \neq 2,\ p \nmid \tau,\ p \mid N \text{ or } p = 2,\ 4 \nmid \tau,\ 4 \mid N \\ p^{f\tau/b} - 1 & \text{if } p \neq 2,\ p \nmid \tau,\ p \nmid N \text{ or } p = 2,\ 4 \nmid \tau,\ 4 \nmid N \end{cases}$$

where $0 \leqslant a \leqslant v_p(\tau)$ depends on N only through $v_p(N)$ and $b \mid \tau$ depends on N only through the multiplicative order of p modulo $\gcd(N, p_0^\infty)$. Then we have $H_{N,n} = H_n \cap M'K^\times$, where $M' \subseteq R_K$ is, with the above case distinction: $\langle \gamma_0^b, \gamma^{p^a} \rangle$; $\langle \gamma_0^b, \gamma \rangle$ if $p \neq 2$ and $\langle \zeta_4, \gamma_0^b, \gamma \rangle$ if $p = 2$; $\langle \gamma_0^b \rangle$.

We remark that the group H_n can be computed with a finite procedure for all $n \geqslant 1$. Indeed, for every $n \mid m$ the group H_n is a subgroup of H_m. Also notice that the ℓ-part of $H_n/K^\times$ is $H_{\ell^{v_\ell(n)}}/K^\times$ and it is trivial if $\ell \nmid \tau$. For every $\ell \mid \tau$ there is some integer B_ℓ such that $H_{\ell^{B_\ell}}$ contains H_{ℓ^v} for every $v \geqslant 1$ (this integer B_ℓ can easily be computed in terms of the ℓ-divisibility parameters of G). Consequently, $H_n = H_{\gcd(n,B)}$ where $B = \prod_{\ell \mid \tau} \ell^{B_\ell}$.

Fixing n, the group $H_{N,n} \cap K(\zeta_{p^\infty})$ is determined by $v_p(N)$, and

$$H_{N,n} \cap K(\zeta_{p^\infty}) = H_{pN,n} \cap K(\zeta_{p^\infty})$$

holds if $v_p(N) \geqslant 2v_p(\tau)$. Moreover, the group $H_{N,n} \cap K(\zeta_{p_0^\infty})$ depends on N only through the multiplicative order of p modulo $N' := \gcd(N, p_0^\infty)$. Indeed, this group is determined by $\mu_{K(\zeta_{N'})} \cap H_n$ (because $K(\zeta_{N'})/K$ corresponds to an extension of finite fields), and we recall that $\mu_{K(\zeta_{N'})}$ is isomorphic to the multiplicative group of $\mathbb{F}_{p^f}(\zeta_{N'})$, whose order only depends on p^f and the multiplicative order of p modulo N'. This leads to a finite but not explicit case distinction. If one accepts it, then we have shown that $H_{N,n}$ can be determined for all N, n at once and hence all degrees $B(N, \ell^m)$ for all integers m and N such that $\ell^m \mid N$ can be computed at once. Therefore (accepting the above case distinction), thanks to the considerations in Remark 4.2.8, the degrees of the Kummer extensions $K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)$ can be determined for all $n \mid N$ at once with an explicit finite procedure.

Remark 4.4.3. We can compute at once the groups $H_{N,n}$ for all N, n that are powers of one fixed prime number ℓ. It suffices to compute H_{ℓ^z} (see the proof of Theorem 4.4.1) for every z, namely determining the largest subgroup $M \in S$ such that $M^\tau \subseteq \sqrt[\ell^z]{G^\tau} K^{\times \tau}$. Notice that $M^\tau \subseteq (\sqrt[\ell^z]{G^\tau} \cap K^\times) K^{\times \tau}$ and that we can replace G by G_ℓ as done in Section 4.2. Then we easily conclude because $\sqrt[\ell^z]{G_\ell^\tau} \cap K^\times$ is finitely generated and can be computed for all z (it does not depend on z provided that z is sufficiently large).

Example 4.4.4. We continue Example 4.2.9, showing that $[\mathbb{Q}_7(\zeta_{18}, \sqrt[6]{G}) : \mathbb{Q}_7(\zeta_{18})] = 6$ by computing $B(18, 2) = 1$ and $B(18, 3) = 3$. Notice that $[\mathbb{Q}_7(\zeta_{18}) : \mathbb{Q}_7] = 3$ hence $B(18, 2) = 1$ and $B(18, 3) \in \{1, 3\}$. To conclude, observe that $\zeta_{18} \in \mathbb{Q}_7(\sqrt[3]{G})$ because $7^6 \cdot 10^2 \in G$ and $\operatorname{ord}(10^2 \bmod 7) = 3$, thus the residue field of $\mathbb{Q}_7(\sqrt[3]{G})$ contains the 18-th roots of unity.

Example 4.4.5. For the group $\langle -1 \rangle \subseteq \mathbb{Q}_3^\times$ and for any positive integers $Z \geqslant z$, clearly $B(2^Z, 2^z)$ is 2 if $Z = z$, and it is 1 otherwise. As $R_{\mathbb{Q}_3} = \langle \zeta_4, \sqrt{-3} \rangle$, we have $H_{2^z} = \langle \zeta_4 \rangle \mathbb{Q}_3^\times$. Thus for $2^z \mid N$ we have $H_{N,2^z} \in \{H_{2^z}, \mathbb{Q}_3^\times\}$ and it is H_{2^z} if and only if $\zeta_4 \in \mathbb{Q}_3(\zeta_N)$, i.e. $4 \mid (3^{\operatorname{ord}(3 \bmod N)} - 1)$ or, equivalently, $2 \mid \operatorname{ord}(3 \bmod N)$.

We conclude by considering the structure of the Galois group of the Kummer extensions:

Remark 4.4.6. Fix some positive integers N, n such that $n \mid N$. Considering the prime decomposition of $n = \prod \ell^m$, we can write

$$\mathrm{Gal}(K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)) = \prod_{\ell \mid n} \mathrm{Gal}\left(\frac{K(\zeta_{\ell^m}, \sqrt[\ell^m]{G})}{K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) \cap K(\zeta_N)} \right). \tag{4.4}$$

By Theorem 4.4.1 we have

$$K' := K(\zeta_{\ell^m}, \sqrt[\ell^m]{G}) \cap K(\zeta_N) = K(\zeta_{\ell^m}, H_{N,\ell^m}).$$

The size of the cyclic components of the factor in (4.4) corresponding to the prime $\ell = p$ can be then computed with the method described in [ACP$^+$25, Theorem 6] with parameters of p-divisibility

$$(\infty, d_1, \cdots, d_s; h, h_1, \cdots, h_s)$$

with $h = \max(h_{s+1}, \cdots, h_r)$, where the h_i and d_i are as in Theorem 4.2.4 applied to the group G over the field K'. Consider now the factors in (4.4) for primes $\ell \neq p$. If $G \subseteq \mathcal{O}_{K'}^\times$, then each factor is cyclic as it corresponds to a cyclotomic extension. If $G \not\subseteq \mathcal{O}_{K'}^\times$, then each factor can be reduced to the product of at most two cyclic groups, again applying [ACP$^+$25, Theorem 6] with parameters of ℓ-divisibility

$$(\infty, d_\ell(G); h, h_\ell(\beta))$$

defined in Section 4.2 for the group G and over the field K'. Notice that $h = h_\ell(\beta) = 0$ if $\ell \nmid \#(\mu_{K'})$ and $d_\ell(G) = 0$ for almost all primes as seen in Remark 4.2.8. Therefore there are only finitely many primes $\ell \neq p$ for which the factor is not cyclic of order ℓ^m.

Remark 4.4.7. If we accept the case distinction to compute H_{N,ℓ^m} for all N and m at once, we can also compute for all N and n at once the group structure of the Galois group of the Kummer extension $K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)$.

4.5 Completions of Kummer extensions of number fields

In this section k is a number field and $\alpha \in k^\times$ is not a root of unity. If $\wp$ is a non-zero prime ideal of the ring of integers $\mathcal{O}_k$ over the rational prime p, we write $k_\wp$ for the corresponding completion of k and we identify k with a subset of $k_\wp$. If ℓ is a prime number and $M \geqslant m$ are positive integers, we consider the Kummer extension of number fields

$$k(\zeta_{\ell^M}, \sqrt[\ell^m]{\alpha})/k(\zeta_{\ell^M})$$

and the corresponding Kummer extension of p-adic fields

$$k_\wp(\zeta_{\ell^M}, \sqrt[\ell^m]{\alpha})/k_\wp(\zeta_{\ell^M}).$$

Let $\ell \neq p$. For almost all primes $\wp$ we have $v_\wp(\alpha) = 0$, and in this case the above extension of local fields is a cyclotomic extension, uniquely determined by $h_{\ell,\wp}(\alpha)$, namely the ℓ-adic valuation of the order of $(\alpha \bmod \wp)$. For a fixed $\wp$, we have $h_{\ell,\wp}(\alpha) = 0$ for almost all primes ℓ (as α is ℓ^∞-divisible if $\ell \nmid N(\wp) - 1 = p^f - 1$). If we fix ℓ instead, a prime $\wp$ is such that $h_{\ell,\wp}(\alpha) > 0$ if and only if ℓ divides the order of $(\alpha \bmod \wp)$ in $(\mathcal{O}_k/\wp)^\times$. There are infinitely many such $\wp$, even a set with positive density [Per15].

Remark 4.5.1. Let $\mathrm{Cl}(k)$ be the class group of k and h_k the class number. Let h, d be the ℓ-divisibility parameters of α, meaning that $\alpha = \zeta_{\ell^h}\beta^{\ell^d}$, where $\beta \in k^\times$ and d is maximal (we refer the reader to [DP16]). If $\ell \nmid h_k$, there exists a prime $\wp$ of k such that $\gcd(v_\wp(\beta), \ell) = 1$, else d would not be maximal. Consequently, the parameter $d_\wp$ of ℓ-divisibility of β in $k_\wp$ is the same as the one in k. In general, supposing that $v_\wp(\beta) \neq 0$, consider the order of $[\wp]$ in $\mathrm{Cl}(k)$ and denote by n its ℓ-adic valuation: the parameter $d_\wp$ can be any integer between d and $d + n$.

Example 4.5.2. Let $k = \mathbb{Q}(\sqrt{-5})$ and $\ell = 2$. Since $h_k = 2$, we could have $d_\wp = d + 1$. This happens for $\alpha = 2 - \sqrt{-5}$ and $\wp = (3, \sqrt{-5} + 1)$, noticing that $d = 0$ and $(\alpha) = (3, \sqrt{-5} + 1)^2$.

If ℓ is odd (respectively, $\ell = 2$) we define t as the largest integer for which $k(\zeta_\ell) = k(\zeta_{\ell^t})$ (respectively, $k(\zeta_4) = k(\zeta_{2^t})$) and, for a non-zero prime ideal $\wp$ of $\mathcal{O}_k$, we call $t_\wp$ the largest integer for which $k_\wp(\zeta_\ell) = k_\wp(\zeta_{\ell^{t_\wp}})$ (respectively, $k_\wp(\zeta_4) = k_\wp(\zeta_{2^{t_\wp}})$).

Theorem 4.5.3. *We keep the above notation, and suppose that $\ell \nmid h_k$. Consider the set P of non-zero prime ideals $\mathfrak{a} \subseteq \mathcal{O}_k$ for which $v_\ell(v_\mathfrak{a}(\alpha)) = d$. Fix some positive integers $m \leqslant M$ such that $M \geqslant \min_P t_\mathfrak{a}$. If the extension*

$$k(\zeta_{\ell^M}, \sqrt[\ell^m]{\alpha})/k(\zeta_{\ell^M})$$

is not a cyclotomic extension, there exists $\wp \in P$ such that the corresponding extension

$$k_\wp(\zeta_{\ell^M}, \sqrt[\ell^m]{\alpha})/k_\wp(\zeta_{\ell^M})$$

has the same degree and it is also not a cyclotomic extension.

Proof. Let $A := [k(\zeta_{\ell^M}, \sqrt[\ell^m]{\alpha}) : k(\zeta_{\ell^M})]$, which is a power of ℓ. Since the given extension is not cyclotomic, we must have $d < m$. Since $M \geqslant t$, by [DP16, Theorem 18] we get

$$v_\ell(A) = \begin{cases} m - (M - h) & \text{if } d \geqslant M - h \\ m - d & \text{if } d < M - h\,. \end{cases}$$

Consider a prime $\wp \in P$ for which $t_\wp$ is minimal, so $M \geqslant t_\wp$ (we have $P \neq \emptyset$ by Remark 4.5.1). The ℓ-divisibility parameters of α in $k_\wp$ are $h_\wp$ and d. We show that $A_\wp := [k_\wp(\zeta_{\ell^M}, \sqrt[\ell^m]{\alpha}) : k_\wp(\zeta_{\ell^M})]$ equals A by applying [DP16, Theorem 18] also to compute $A_\wp$. If $h_\wp = h$, then $A = A_\wp$ as all the parameters in the formula are the same. Else, we claim that $d \leqslant M - h_\wp$ and we conclude because $v_\ell(A_\wp) = m - d = v_\ell(A)$.

To prove the claim, we show that $d \leqslant t_\wp - h_\wp$ in case $h_\wp > h$ (respectively, $d \leqslant t_\wp - h$ in case $h_\wp < h$). For $h_\wp > h$, the claim holds because $\beta^{\ell^d}/\zeta \bmod \wp$ has oder coprime to ℓ for some root of unity ζ of order $\ell^{h_\wp}$ (since $h_\wp > 0$, we conclude by considering the order of $(\beta \bmod \wp)$, whose ℓ-adic valuation is at most $t_\wp$). For $h_\wp < h$ the claim holds because $\beta^{\ell^d}/\zeta_{\ell^h}^{-1}\zeta$ has order coprime to ℓ for some root of unity ζ of order $\ell^{h_\wp}$, and again the order of $(\beta \bmod \wp)$ has ℓ-adic valuation at most $\ell^{t_\wp}$. □

Theorem 4.5.4. *Fix a prime number ℓ and positive integers $m \leqslant M$. There is a positive density of primes $\wp$ of k such that*

$$[k(\zeta_{\ell^M}, \sqrt[\ell^m]{\alpha}) : k(\zeta_{\ell^M})] = [k_\wp(\zeta_{\ell^M}, \sqrt[\ell^m]{\alpha}) : k_\wp(\zeta_{\ell^M})]\,.$$

Proof. Set $\ell^{D_\ell} := [k(\zeta_{\ell^M}, \sqrt[\ell^m]{\alpha}) : k(\zeta_{\ell^M})]$. The degree of the local extension at $\wp$ divides ℓ^{D_ℓ}. So the statement is clear if $D_\ell = 0$, and we suppose that $D_\ell \geqslant 1$.

If $\ell = 2$, we suppose that $\zeta_4 \in k$ or that $M > 1$. Then, without loss of generality, we may assume that $M \geqslant t$. Consider the primes $\wp$ of k such that $v_\wp(\alpha) = 0$ and remark that $h_\wp$ is the ℓ-adic valuation of the order of $(\alpha \bmod \wp)$. The conditions $t_\wp \geqslant M$ and $h_\wp = t_\wp - (m - D_\ell)$ imply that $k_\wp(\zeta_{\ell^M}, \sqrt[\ell^m]{\alpha})/k_\wp(\zeta_{\ell^M})$ is cyclotomic of degree ℓ^{D_ℓ}. By the Chebotarev density theorem and the density results in [Per15] the primes satisfying $t_\wp = M$ and $h_\wp = t_\wp - (m - D_\ell)$ admit the density

$$\frac{1}{[k(\zeta_{\ell^M}) : k]} - \frac{1}{[k(\zeta_{\ell^{M+1}}) : k]} - \frac{1}{[k(\zeta_{\ell^M}, \sqrt[\ell^m]{\alpha^{\ell^{D_\ell - 1}}}) : k]} + \frac{1}{[k(\zeta_{\ell^{M+1}}, \sqrt[\ell^m]{\alpha^{\ell^{D_\ell - 1}}}) : k]}\,.$$

This density is positive because $\zeta_{\ell^{M+1}} \notin k(\zeta_{\ell^M})$ (as $M \geqslant t$) and $\alpha^{\ell^{D_\ell}} \notin k(\zeta_{\ell^M})$ (as $D_\ell \geqslant 1$). We are left with the case $\ell = 2$, $\zeta_4 \notin k$ and $M = 1$ hence $m = D_\ell = 1$. We may similarly consider the primes $\wp$ of k for which $4 \nmid \#\mu_{k_\wp}$ and $\sqrt{\alpha} \notin k_\wp$, which have density at least $1/4$. □

Now consider a more general Kummer extension $k(\zeta_N, \sqrt[n]{\alpha})/k(\zeta_N)$ where n and N are positive integers such that $n \mid N$. We generalize Theorem 4.5.4:

Theorem 4.5.5. *Let n, N be positive integers such that $n \mid N$. There is a positive density of primes $\wp$ of k such that*

$$[k(\zeta_N, \sqrt[n]{\alpha}) : k(\zeta_N)] = [k_\wp(\zeta_N, \sqrt[n]{\alpha}) : k_\wp(\zeta_N)]\,.$$

Proof. Let T be the greatest integer for which $k(\zeta_N) = k(\zeta_T)$. Up to replacing N, we may assume that $N = T$. For a prime $\wp$ of k, consider the prime factorization $n = \prod \ell^{m_\ell}$ and write

$$[k_\wp(\zeta_N, \sqrt[n]{\alpha}) : k_\wp(\zeta_N)] = \prod_{\ell \mid n} \frac{[k_\wp(\zeta_{\ell^{m_\ell}}, \sqrt[\ell^{m_\ell}]{\alpha}) : k_\wp(\zeta_{\ell^{m_\ell}})]}{[k_\wp(\zeta_{\ell^{m_\ell}}, \sqrt[\ell^{m_\ell}]{\alpha}) \cap k_\wp(\zeta_N) : k_\wp(\zeta_{\ell^{m_\ell}})]}\,. \tag{4.5}$$

Suppose that $\wp$ is such that $N \mid \#\mu_{k_\wp}$ and $\ell^{v_\ell(N)+1} \nmid \#\mu_{k_\wp}$ for every $\ell \mid N$. For such $\wp$ the denominators in (4.5) are 1 because we have $k_\wp(\zeta_{\ell^{m_\ell}}) = k_\wp(\zeta_N)$. We additionally

require that, for every $\ell \mid N$, the ℓ-adic local Kummer extension has degree

$$\ell^{D_\ell} := [k(\zeta_N, \sqrt[\ell^{m_\ell}]{\alpha}) : k(\zeta_N)].$$

If $D_\ell = 0$, this condition holds because the degree of the local extension divides ℓ^{D_ℓ}. If $D_\ell > 0$ and if we exclude the finitely many primes $\wp$ for which $v_\wp(\alpha) \neq 0$, the above condition means that the order of $(\alpha \bmod \wp)$ has ℓ-adic valuation $v_\ell(N) - (m_\ell - D_\ell)$, because the extension $k_\wp(\zeta_N, \sqrt[\ell^{m_\ell}]{\alpha})/k_\wp(\zeta_N)$ is cyclotomic.

We conclude by proving that there is a positive density of primes $\wp$ such that the following holds: we have $N \mid \#\mu_{k_\wp}$; for every $\ell \mid N$, we have $\ell^{v_\ell(N)+1} \nmid \#\mu_{k_\wp}$; if $D_\ell > 0$, the order of $(\alpha \bmod \wp)$ has ℓ-adic valuation $v_\ell(N) - (m_\ell - D_\ell)$. We may restrict to the positive density of primes $\wp$ that split completely in $k(\zeta_N, \sqrt[E]{\alpha})$, where

$$E := \prod_{\ell : D_\ell > 0} (m_\ell - D_\ell)\,.$$

We are left to select those primes that, for every ℓ, satisfy the following condition: they do not split in $k(\zeta_{N\ell}, \sqrt[E]{\alpha})$ and, if $D_\ell > 0$, they do not split in $k(\zeta_N, \sqrt[E\ell]{\alpha})$. Notice that these two fields have degree ℓ over $k(\zeta_N, \sqrt[E]{\alpha})$. Indeed, by the definition of D_ℓ, for every ℓ such that $D_\ell \geqslant 1$ we have that $\sqrt[\ell^{m_\ell - D_\ell}]{\alpha} \in k(\zeta_N)$ but $\sqrt[\ell^{m_\ell - D_\ell + 1}]{\alpha} \notin k(\zeta_N)$. In particular, the conditions for different primes ℓ involve field extensions that are linearly disjoint. So we are left to check that the density of primes $\wp$ satisfying the condition for one single ℓ is positive. This holds because not splitting in any of the two given extensions of degree ℓ gives density $1 - \frac{1}{\ell}$ if the two fields are the same and density $(1 - \frac{1}{\ell})(1 - \frac{1}{\ell})$ if the two fields are different hence linearly disjoint. □

Remark 4.5.6. For any number field extension $L(\gamma)/L$ and for any prime $\wp$ of L, we have $[L(\gamma) : L] \geqslant [L_\wp(\gamma) : L_\wp]$. Then Theorem 4.5.5 implies

$$[k(\zeta_N, \sqrt[n]{\alpha}) : k(\zeta_N)] = \max_{\substack{\wp \subseteq \mathcal{O}_k \\ \wp \text{ prime}}} [k_\wp(\zeta_N, \sqrt[n]{\alpha}) : k_\wp(\zeta_N)].$$

Example 4.5.7. Remark 4.5.6 does not hold for a subgroup G of $k^\times$ in place of α. For $k = \mathbb{Q}$ and $G = \langle 2, 5\rangle$, the Kummer extension $\mathbb{Q}(\zeta_9, \sqrt[3]{G})/\mathbb{Q}(\zeta_9)$ has degree 9, while for every prime p the extension $\mathbb{Q}_p(\zeta_9, \sqrt[3]{G})/\mathbb{Q}_p(\zeta_9)$ has degree strictly less than 9: the degree is at most 3 for $p \neq 3$ and it is 1 for $p = 3$. (For $p = 3$ notice that 2 and 5 are cubes in $\mathbb{Q}_3$. For $p \neq 3$ we can use the results of Section 4.2, considering G_ℓ for $\ell = 3$. Indeed, if $p \notin \{2, 3, 5\}$ then G_3 is a subgroup of $\mu_{\mathbb{Q}_p}$ hence it is cyclic, while if $p = 2, 5$ the group G_3 is torsion free and hence it is cyclic.)

CHAPTER 5

Kummer theory for abelian varieties

This Chapter is based on [Per24]. Let A be an abelian variety of dimension g defined over a number field K, for which we fix an algebraic closure $\overline{K}$. We denote by $A[N]$ the group of torsion points in $A(\overline{K})$ of order dividing N. If $P \in A(K)$, we denote by $K(\frac{1}{N}P)$ the smallest extension of K containing all points $Q \in A(\overline{K})$ such that $NQ = P$. We fix a rational point $P \in A(K)$ and assume that the set $\mathbb{Z}P$ of multiples of P is Zariski-dense in A.

Let κ_N be the Kummer representation attached to A and P. This is a representation of the absolute Galois group of $K(A[N])$ with values in $A[N] \cong (\mathbb{Z}/N\mathbb{Z})^{2g}$ whose image is isomorphic to the Galois group of the extension $K(\frac{1}{N}P)/K(A[N])$. The aim of this Chapter is to find an effective bound, independent of N, for the Kummer failure of maximality, namely the ratio

$$f_N := \frac{N^{2g}}{\#(\mathrm{Im}(\kappa_N))}.$$

Remark that we will actually tackle the more general problem where P is replaced by a finitely generated subgroup G of $A(K)$.

In the case of abelian varieties, Theorem 1.2.3 is as follows, where we denote by τ_∞ (resp. κ_∞), the adelic torsion (resp. Kummer) representation:

Theorem 5.0.1 (Tronto)**.** *Let $P \in A(K)$ be such that $\mathbb{Z}P$ is Zariski-dense in A, and let $\Gamma := \{Q \in A(\overline{K}) \mid \exists n \in \mathbb{Z}_{\geqslant 1} : nQ \in \langle P \rangle\}$. Assume that $A(\overline{K})_{\mathrm{tors}}$ is an injective $\mathrm{End}_K(A)$-module. Suppose that there exist positive integers d, n, m such that:*

1. $d(\Gamma \cap A(K)) \subseteq \langle P \rangle + A(K)_{\mathrm{tors}}$;
2. $n \cdot H^1(\mathrm{Im}(\tau_\infty), A(\overline{K})_{\mathrm{tors}}) = 0$;
3. *the subring of* $\mathrm{End}(A(\overline{K})_{\mathrm{tors}})$ *generated by* $\mathrm{Im}(\tau_\infty)$ *contains* $m \cdot \mathrm{End}(A(\overline{K})_{\mathrm{tors}})$.

Then $\mathrm{Im}(\kappa_\infty)$ *contains* $(dnm \cdot \hat{\mathbb{Z}})^{2g}$.

Consequently, we have the following result (see Remark 1.2.1):

Corollary 5.0.2. *For any positive integer N, the Kummer failure f_N divides $(dnm)^{2g}$.*

In this chapter we show that the three integers d, n, m as in Theorem 5.0.1 exist for every abelian variety A over a number field. Moreover, we prove that d and m can always be effectively bounded in terms of basic invariants of A/K, while n can be effectively bounded in the case A has CM over $\overline{K}$. We also show that the assumption on $A(\overline{K})_{\mathrm{tors}}$ is satisfied by an abelian variety A' in the same isogeny class of A and we study how the minimal admissible values of d, n, m change under isogeny. Since the degree of the isogeny $A \to A'$ can also be bounded effectively in terms of A/K, we ultimately obtain bounds that only depend on the abelian variety A, on the field K, and on the divisibility of the point P (respectively, of the subgroup G of $A(K)$) for which we consider the Kummer representation.

In this chapter we will therefore prove the following:

Theorem 5.0.3. *Consider an abelian variety A of dimension g defined over a number field K and with complex multiplication over $\overline{K}$. Let G be a finitely generated subgroup of $A(K)$. Suppose a set of generators of G is linearly independent over $\mathrm{End}_K(A)$ and is given in terms of a $\mathbb{Z}$-basis for $A(K)/A(K)_{\mathrm{tors}}$. There exists an effective upper bound for f_N, uniform in N and depending only on K, A and G.*

Our bound in Theorem 5.0.3 depends exponentially on $[K(A[3]) : K]$, on $[K : \mathbb{Q}]$ and on g, and linearly on the Faltings height $h_F(A)$ and on the 'divisibility parameter' d of the group G (see Section 5.1). Notice that $[K(A[3]) : K]$ divides $\#\,\mathrm{GL}_{2g}(\mathbb{Z}/3\mathbb{Z})$ and can therefore be bounded by 3^{4g^2}.

This chapter is almost entirely dedicated to the proof of Theorem 5.0.3. In Section 5.1 we adapt Theorem 5.0.1 to the case when we consider a group G instead of a single point P, and we provide methods to compute effectively the integer d. In Section 5.2 we prove a result (Theorem 5.2.1) which allows us to compare the cardinality of the images of torsion and Kummer representations for isogenous abelian varieties. In Section 5.3 we take care of the assumption of Theorem 5.0.1 concerning the injectivity of the module of torsion points $A(\overline{K})_{\mathrm{tors}}$ by finding an abelian variety A' isogenous to A that satisfies this condition. Theorem 5.3.3 proves the existence of such an isogeny $A \to A'$ and gives an effective bound to its degree. Sections 5.4 and 5.5 are devoted, respectively, to finding effective bounds for the integer n of Theorem 5.0.1 if A has complex multiplication (see Corollary 5.4.2) and for the integer m of the Theorem 5.0.1 for any abelian variety (see Theorem 5.5.3). Section 5.6 contains the proof of Theorem 5.0.3.

Further results in this chapter arise from the study of possible analogues of Schinzel's theorem on radical extensions [Sch77, Theorem 2] (see Theorem 1.0.3) in the setting of abelian varieties. This is the content of Section 5.7, independent of the rest of the chapter. in particular, we prove the following:

Theorem 5.0.4. *Let A be an abelian variety over a number field K. The following are equivalent:*

(i) The extension $K(A[n])/K$ is abelian for every positive integer n.

(ii) The variety A is K-isogenous to a product of simple abelian varieties with CM over K.

Preliminaries

Let A be an abelian variety defined over a number field K for which we fix an algebraic closure $\overline{K}$, and let g be its dimension. Let $R := \mathrm{End}_K(A)$ be the ring of K-endomorphisms of A. We denote by $A(K)$ the Mordell-Weil group of K-rational points of A. If N is any positive integer, we denote by $[N]$ the multiplication-by-N endomorphism of A and by $A[N]$ the subgroup of torsion points of $A(\overline{K})$ of order dividing N. We also write $K(A[N])$ for the N-th torsion field of K, obtained by adjoining to K the coordinates of the points in $A[N]$. For any prime ℓ we write $T_\ell(A) := \varprojlim_n A[\ell^n]$ for the ℓ-adic Tate module of A. Recall that $T_\ell(A)$ is a free $\mathbb{Z}_\ell$-module of rank $2g$. We write $V_\ell(A)$ for the base change of $T_\ell(A)$ to $\mathbb{Q}_\ell$ and $T(A) := \varprojlim_N A[N] = \prod_\ell T_\ell(A)$ for the adelic Tate module. For an element $e \in T_\ell(A)$, we write $e = (e^{(n)})_{n\in\mathbb{Z}_{\geqslant 1}}$ with $e^{(n)} \in A[\ell^n]$ and $\ell e^{(n)} = e^{(n-1)}$.

Let ℓ be a prime and let z be an integer or an ℓ-adic integer. We denote by $v_\ell(z)$ the ℓ-adic valuation of z, with the convention $v_\ell(0) = +\infty$.

For any field F, after fixing an algebraic closure $\overline{F}$, we denote by G_F the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$. For every positive integer N, fix a basis $\{T_1^N, T_2^N\}$ of $A[N]$ such that $NT_i^M = T_i^{M/N}$ whenever $N \mid M$.

We denote by $\tau_{A,N}$ the *N-torsion representation*

$$\tau_{A,N} : G_K \to \mathrm{Aut}(A[N])$$

given by the $\mathbb{Z}/N\mathbb{Z}$-linear action of G_K on $A[N]$. The group $A[N]$ is abstractly isomorphic to $(\mathbb{Z}/N\mathbb{Z})^{2g}$, hence we also have $\mathrm{Aut}(A[N]) \cong \mathrm{GL}_{2g}(\mathbb{Z}/N\mathbb{Z})$. The Galois group $\mathrm{Gal}(K(A[N])/K)$ can be identified with the image of $\tau_{A,N}$, and hence with a subgroup of $\mathrm{GL}_{2g}(\mathbb{Z}/N\mathbb{Z})$.

Given a point $P \in A(K)$, we denote by $K(\frac{1}{N}P)$ the smallest extension of K over which all points $Q \in A(\overline{K})$ such that $NQ = P$ are defined. In particular, $K(\frac{1}{N}P) \supseteq K(A[N])$. We denote by $\kappa_{A,N}$ the *Kummer representation*

$$\begin{aligned} \kappa_{A,N} : G_{K(A[N])} &\to A[N] \\ \sigma &\mapsto \sigma(Q) - Q, \end{aligned}$$

where $Q \in A(\overline{K})$ is such that $NQ = P$. Since we only consider the action of $G_{K(A[N])}$, it is easy to see that the map $\kappa_{A,N}$ is independent of the choice of Q. The Galois group $\mathrm{Gal}(K(\frac{1}{N}P)/K(A[N]))$ can be identified with the image of $\kappa_{A,N}$, and hence with a subgroup of $(\mathbb{Z}/N\mathbb{Z})^{2g}$. We call *Kummer failure of maximality*, denoted by f_N, the integer $N^{2g}/\#\,\mathrm{Im}(\kappa_{A,N})$.

Fix a set of points $\{Q^N\}_{N\in\mathbb{Z}_{>0}} \subseteq A(\overline{K})$ such that $Q^1 = P$ and $NQ^M = Q^{M/N}$ whenever $N \mid M$. An element $\sigma \in \mathrm{Gal}(K(\frac{1}{N}P)/K)$ can be expressed as a $(2g+1) \times (2g+1)$ matrix M_σ with entries in $\mathbb{Z}/N\mathbb{Z}$ of the form

$$M_\sigma = \left(\begin{array}{c|c} B_\sigma & t_\sigma \\ \hline 0 & 1 \end{array}\right), \tag{5.1}$$

where B_σ is the image of σ under $\tau_{A,N}$, while $t_\sigma = \sigma(Q^N) - Q^N \in \mathrm{Im}(\kappa_{A,N})$. Given two elements $\sigma, \tau \in \mathrm{Gal}(K(\frac{1}{N}P)/K)$, we have that $M_{\sigma\tau} = M_\sigma M_\tau$.

Fix a prime ℓ. By taking the inverse limit over n, the representations τ_{A,ℓ^n} and κ_{A,ℓ^n} yield the *ℓ-adic torsion representation* $\tau_{A,\ell^\infty} : G_K \to \mathrm{Aut}(T_\ell(A))$ and the *ℓ-adic Kummer representation* $\kappa_{A,\ell^\infty} : G_{K(A[\ell^\infty])} \to T_\ell(A)$. Likewise, by taking the inverse limit over all positive integers N, we get the *adelic torsion representation* $\tau_{A,\infty} : G_K \to \mathrm{Aut}(T(A))$ and the *adelic Kummer representation* $\kappa_{A,\infty} : G_{K(A(\overline{K})_{\mathrm{tors}})} \to T(A)$. If the abelian variety A is clear from the context, we drop the subscript A from the notation.

We denote by K_{tors} the smallest extension of K over which all points in $A(\overline{K})_{\mathrm{tors}}$ are defined. We let

$$\Gamma := \{Q \in A(\overline{K}) \;\big|\; \exists n \in \mathbb{Z}_{\geqslant 1} : nQ \in \langle P\rangle\}$$

and denote by K_{kum} the smallest extension of K_{tors} over which all points in Γ are defined. We call K_{tors} and K_{kum} respectively the *torsion extension* and the *Kummer extension* of K associated with A and P.

By taking the limit, with our previous identifications, in the ℓ-adic situation we have

$$\mathrm{Gal}(K(A[\ell^\infty])/K) \cong \mathrm{Im}(\tau_{\ell^\infty}) \subseteq \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$$

and

$$\mathrm{Gal}\left(K\left(\frac{1}{\ell^\infty}P\right)\Big/K(A[\ell^\infty])\right) \cong \mathrm{Im}(\kappa_{\ell^\infty}) \subseteq (\mathbb{Z}_\ell)^{2g}$$

and in the adelic case we have

$$\mathrm{Gal}(K_{\mathrm{tors}}/K) \cong \mathrm{Im}(\tau_\infty) \subseteq \mathrm{GL}_{2g}(\hat{\mathbb{Z}})$$

and

$$\mathrm{Gal}(K_{\mathrm{kum}}/K_{\mathrm{tors}}) \cong \mathrm{Im}(\kappa_\infty) \subseteq (\hat{\mathbb{Z}})^{2g}.$$

Moreover, an element $\sigma \in \mathrm{Gal}(K(\frac{1}{\ell^\infty}P)/K)$ (resp. $\sigma \in \mathrm{Gal}(K_{\mathrm{kum}}/K)$) can be identified with a matrix as in (5.1), where B_σ is the image of σ under τ_{ℓ^∞} (resp. τ_∞) and t_σ is the inverse limit over n of $\sigma(Q^{\ell^n}) - Q^{\ell^n}$ (resp. the inverse limit over N of $\sigma(Q^N) - Q^N$).

5.1 The divisibility parameter

Let G be a subgroup of $A(K)$ generated by r points that are linearly independent over $\mathrm{End}_K(A)$. For a positive integer N, let

$$\frac{1}{N}G := \{Q \in A(\overline{K}) \mid NQ \in G\} \quad \text{and} \quad \Gamma_G := \bigcup_N \frac{1}{N}G.$$

We consider the Kummer extension $K(\Gamma_G)/K_{\mathrm{tors}}$, which generalises the case considered in Theorem 5.0.1 (which corresponds to the case of rank 1). In this situation, the adelic Kummer representation we consider is

$$\begin{aligned} \kappa_N : G_{K(A[N])} &\to \mathrm{Hom}\left(\frac{1}{N}G \Big/ (G + A[N]), A[N]\right) \\ \sigma &\mapsto (Q \mapsto \sigma(Q) - Q), \end{aligned}$$

where the target space can be identified with $A[N]^r$. Indeed, if $P_1, \ldots, P_r$ are generators of G, an element in the codomain of κ_N is uniquely determined by the images of points Q_i such that $NQ_i = P_i$ (for each i such image is independent of the choice of Q_i). The image of κ_N is isomorphic to the Galois group of the Kummer extension $K(\frac{1}{N}G)/K(A[N])$, and we define the Kummer failure of maximality in this situation as $f_N = N^{2gr}/\#\,\mathrm{Im}(\kappa_N)$. Similarly, the adelic representation is

$$\kappa_\infty : G_{K_{\mathrm{tors}}} \to \mathrm{Hom}\left(\Gamma_G \Big/ (G + A(\overline{K})_{\mathrm{tors}}), A(\overline{K})_{\mathrm{tors}}\right) \cong A(\overline{K})_{\mathrm{tors}}^r.$$

Remark that, if $r = 1$, the assumption that P is linearly independent over $\mathrm{End}_K(A)$ is equivalent to requiring that $\mathbb{Z}P$ is Zariski-dense in A, and ensures that the index $[A(\overline{K})_{\mathrm{tors}} : \mathrm{Im}(\kappa_\infty)]$ is finite. Notice that Ribet in [Rib79] uses the same assumption, which is needed to generalise [Hin88, Proposition 1] to subgroups G of $A(K)$.

Theorem 5.0.1 and Corollary 5.0.2 still hold with the expected adjustments, namely:

Theorem 5.1.1. *Let G be a subgroup of $A(K)$ that is generated by r elements that are linearly independent over $\mathrm{End}_K(A)$. Assume that $A(\overline{K})_{\mathrm{tors}}$ is an injective R-module. Suppose that there exist positive integers d, n, m such that:*

1. *$d(\Gamma_G \cap A(K)) \subseteq G + A(K)_{\mathrm{tors}}$;*
2. *$n \cdot H^1(\mathrm{Im}(\tau_\infty), A(\overline{K})_{\mathrm{tors}}) = 0$;*
3. *the subring of $\mathrm{End}(A(\overline{K})_{\mathrm{tors}})$ generated by $\mathrm{Im}(\tau_\infty)$ contains $m \cdot \mathrm{End}(A(\overline{K})_{\mathrm{tors}})$.*

Then $\mathrm{Im}(\kappa_\infty)$ contains $(dnm \cdot \hat{\mathbb{Z}})^{2gr}$. In particular, for any positive integer N, the Kummer failure f_N divides $(dnm)^{2gr}$.

The smallest positive integer d that satisfies condition (1) in Theorem 5.0.1 (resp. Theorem 5.1.1) is called the *divisibility parameter* of P (resp. of G).

Lemma 5.1.2. *The divisibility parameter d exists. It is effectively computable if P (resp. a set of generators of G) is known in terms of a $\mathbb{Z}$-basis for $A(K)/A(K)_{\mathrm{tors}}$.*

Proof. We can compute d as shown in [Tro23b, Section 6.1]. Indeed, the method used for elliptic curves also applies to general abelian varieties. □

Remark 5.1.3. In order to apply Lemma 5.1.2, we only need to know the *non-zero coefficients* of the point P (resp. of the generators of the group G) with respect to some (potentially unknown) basis for $A(K)/A(K)_{\mathrm{tors}}$. Therefore, a priori, we do not need to know what the basis is, or even what the rank of the Mordell-Weil group is, to effectively compute d. Moreover, in the case a single point P is considered, the parameter of divisibility d is simply the $\gcd$ of its coefficients in any basis representation.

We may still be able to bound the parameter d effectively, through other methods. An example is the following result, which applies for example to Jacobians of curves of genus 2.

Theorem 5.1.4. *Let A be an abelian variety over a number field K. Let $P \in A(K)$, and suppose that there exist:*

1. *an algorithm that, given a point in $A(K)$, computes its canonical height (up to arbitrary numerical precision);*
2. *an algorithm that, given a positive real number α, enumerates the (finitely many) points in $A(K)$ whose canonical height is less than α.*

Then the divisibility parameter d for P can be effectively bounded.

Proof. The parameter d is the maximal integer for which there exist $Q \in A(K)$ and $T \in A(K)_{\mathrm{tors}}$ such that $P = dQ + T$. By standard properties of the canonical height $\hat{h}$, we know that $\hat{h}(P) = d^2\hat{h}(Q)$. The canonical height $\hat{h}(P)$ can be computed through algorithm 1. Consider the finite set of points

$$S = \{Q' \in A(K) \mid \hat{h}(Q') \leqslant \hat{h}(P)\}$$

which is the output of algorithm 2 applied to the real number $\hat{h}(P)$, and let $S' = S \setminus A(K)_{\mathrm{tors}}$. Then we have:

$$d \leqslant \sqrt{\hat{h}(P)\left(\min_{Q' \in S'} \hat{h}(Q')\right)^{-1}}.$$

Note that, while there are more efficient algorithms to determine the set $A(K)_{\mathrm{tors}}$, the knowledge of the set S is sufficient to determine it: indeed, $A(K)_{\mathrm{tors}}$ is contained in S, and we can test whether a point $T \in S$ is torsion by computing iT for $i = 1, \ldots, \#S$ (indeed, the order of a torsion point is at most $\#A(K)_{\mathrm{tors}}$, which in turn is at most $\#S$) □

Remark 5.1.5. Let J be the Jacobian of an algebraic curve C of genus 2 over a number field K and let $P \in J(K)$. Suppose we know the equation of the curve C and the Kummer coordinates of the point P (see [MS16, §3]). Then there exist algorithms as in Theorem 5.1.4 (see for example [MS16]). The divisibility parameter d for P can therefore be effectively bounded in this case.

Example 5.1.6. Consider the hyperelliptic curve $\mathcal{C}$ of genus 2 over $\mathbb{Q}$ given by the equation:

$$y^2 = x^6 - 6x^4 + 2x^3 + 5x^2 - 2x + 1$$

and let J be the Jacobian of $\mathcal{C}$. Consider the rational points $p_1 = (-1, -1)$ and $p_2 = (2, 1)$ of $\mathcal{C}$. Let P be the point of J corresponding to the divisor class $[p_2 - p_1]$. One can compute that $\hat{h}(P) \sim 0.669$ and that the set

$$S' = \{P' \in J(\mathbb{Q}) \mid \hat{h}(P') \leqslant \hat{h}(P), P' \notin J(\mathbb{Q})_{\mathrm{tors}}\}$$

consists of 26 points, with $\min_{S'} \hat{h}(P') \sim 0.128$. The parameter d is then bounded by $(\hat{h}(P)/\min_{S'} \hat{h}(P'))^{1/2} \sim 2.286$. Indeed, it can be checked in this case that $d = 1$.

5.2 Torsion and Kummer extensions for isogenous abelian varieties

Throughout this section, let A and A' be two isogenous abelian varieties of dimension g defined over a number field K, and let $\varphi : A \to A'$ be a fixed K-isogeny between them. Let D denote the degree of φ. We first define the tangent space $\mathcal{T}_\ell$ of the ℓ-adic torsion representation of an abelian variety. We then compare the degrees of the torsion and Kummer extensions of K associated with A and A'. To do so, we compare the images of the relevant Galois representations. In particular, we will prove the following result, consequence of Lemmas 5.2.6 and 5.2.10 and Corollary 5.2.11:

Theorem 5.2.1. *Let $\varphi : A \to A'$ be an isogeny of abelian varieties of degree D and consider a point $P \in A(K) \setminus A(K)_{\mathrm{tors}}$. For every prime ℓ and for every positive integer n we have*

$$\#\operatorname{Im}(\tau_{A',\ell^n}) \leqslant (\#\mathcal{T}_\ell)^{v_\ell(D)} \cdot \#\operatorname{Im}(\tau_{A,\ell^n})$$
$$\frac{\ell^{2gn}}{\#\operatorname{Im}(\kappa_{A',\ell^n})} \Big| \ell^{v_\ell(D)} \cdot \# \frac{T_\ell(A)}{\operatorname{Im}(\kappa_{A,\ell^\infty})}$$

and, for every positive integer N, we have

$$\frac{N^{2g}}{\#\operatorname{Im}(\kappa_{A',N})} \Big| D \cdot \# \frac{T(A)}{\operatorname{Im}(\kappa_{A,\infty})}$$

where the Kummer representations on A and A' are relative to the points P and $\varphi(P)$ respectively, and where $\mathcal{T}_\ell$ is the tangent space of τ_{A,ℓ^∞}.

There exists a K-isogeny $\psi : A' \to A$ such that $\psi \circ \varphi = [D]$. If a prime ℓ does not divide D, then $[D]$ induces an isomorphism on $T_\ell(A)$, and therefore the map $T_\ell(A) \to T_\ell(A')$ induced by φ is an isomorphism. It follows that the ℓ-adic torsion representations on A and A' are isomorphic. If $\ell \mid D$, then $[D]$ is not an isomorphism on the Tate module, but it becomes an isomorphism on $V_\ell(A)$. The two torsion representations are again isomorphic when tensored by $\mathbb{Q}_\ell$, however, in general, $\mathrm{Im}(\tau_{A,\ell^\infty})$ and $\mathrm{Im}(\tau_{A',\ell^\infty})$ are not conjugate subgroups of $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$.

The tangent space of the image of the ℓ-adic representation

Consider an abelian variety A of dimension g defined over a number field K. For a prime ℓ and a positive integer n, consider the group $\mathrm{Im}(\tau_{\ell^n})$ as a subgroup of $\mathrm{GL}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z})$. Notice that we have

$$\frac{\#\,\mathrm{Im}(\tau_{\ell^{n+1}})}{\#\,\mathrm{Im}(\tau_{\ell^n})} = \#\ker\left(\mathrm{Im}(\tau_{\ell^{n+1}}) \xrightarrow{\bmod \ell^n} \mathrm{Im}(\tau_{\ell^n})\right).$$

The projection $\mathrm{Im}(\tau_{\ell^{n+1}}) \to \mathrm{Im}(\tau_{\ell^n})$ is surjective, and we can identify its kernel with a subgroup of

$$\ker\left(\mathrm{GL}_{2g}\left(\mathbb{Z}\big/\ell^{n+1}\mathbb{Z}\right) \xrightarrow{\bmod \ell^n} \mathrm{GL}_{2g}\left(\mathbb{Z}\big/\ell^{n}\mathbb{Z}\right)\right) = \mathrm{Id} + \ell^n \mathcal{M}_{2g\times 2g}(\mathbb{F}_\ell).$$

It is easy to check that the following map is a group homomorphism:

$$\begin{aligned}\ker\left(\mathrm{Im}(\tau_{\ell^{n+1}}) \to \mathrm{Im}(\tau_{\ell^n})\right) &\to \mathcal{M}_{2g\times 2g}(\mathbb{F}_\ell)\\ (\mathrm{Id} + \ell^n S) &\mapsto S.\end{aligned}$$

We call $\mathcal{T}_\ell^{(n)}$ its image: it is an $\mathbb{F}_\ell$-vector subspace of $\mathcal{M}_{2g\times 2g}(\mathbb{F}_\ell)$.

Lemma 5.2.2 ([LP21, Proof of Lemma 9])**.** *We have $\mathcal{T}_\ell^{(n)} \subseteq \mathcal{T}_\ell^{(n+1)}$ for all integers $n \geqslant 1$.*

Since $\mathcal{T}_\ell^{(n)}$ is a subspace of $\mathcal{M}_{2g\times 2g}(\mathbb{F}_\ell)$, which is a finite dimensional vector space over $\mathbb{F}_\ell$, Lemma 5.2.2 implies that $\dim(\mathcal{T}_\ell^{(n)})$ and hence also $\mathcal{T}_\ell^{(n)}$ stabilise for n large enough. We denote such stabilised space by $\mathcal{T}_\ell$ and we call it the *tangent space* of the ℓ-adic torsion representation τ_{ℓ^∞} (see [LP21, Definition 9]). In particular, for n large enough, we have

$$\#\,\mathrm{Im}(\tau_{\ell^n}) = k \cdot \ell^{n\cdot\dim(\mathcal{T}_\ell)} \tag{5.2}$$

for some constant k which does not depend on n.

Example 5.2.3. For an elliptic curve E, the tangent space $\mathcal{T}_\ell$ can be described as follows (see [LP17, Definitions 18 and 19]):

- if E does not have CM, then $\mathcal{T}_\ell = \mathcal{M}_{2\times 2}(\mathbb{F}_\ell)$;
- if E has CM and ℓ splits in $\mathrm{End}_{\overline{K}}(E)$, then, for a suitable choice of basis, $\mathcal{T}_\ell = \mathrm{Diag}_2(\mathbb{F}_\ell)$, the subspace of diagonal matrices;

- if E has CM and $\ell > 2$ is inert in the quadratic ring $\mathrm{End}_{\overline{K}}(E)$, then, in a suitable basis,
$$\mathcal{T}_\ell = \left\{ \begin{pmatrix} x & dy \\ y & x \end{pmatrix} \mid x, y \in \mathbb{F}_\ell \right\},$$
where d is a quadratic non-residue modulo ℓ;
- more generally, if $\mathrm{End}_{\overline{K}}(E)$ is isomorphic to the quadratic ring $\mathbb{Z}[x]/(x^2 - cx - d)$, then, in a suitable basis,
$$\mathcal{T}_\ell = \left\{ \begin{pmatrix} x & dy \\ y & x + yc \end{pmatrix} \mid x, y \in \mathbb{F}_\ell \right\}.$$

Isogenies and Tate modules

Given a K-isogeny φ between the abelian varieties A and A' and a prime ℓ, there is an associated $\mathbb{Z}_\ell$-linear map on the Tate modules: if $e = (e^{(n)})_{n \in \mathbb{Z}_{\geqslant 1}}$ is a point of $T_\ell(A)$, we set $\varphi(e) = (\varphi(e^{(n)}))_{n \in \mathbb{Z}_{\geqslant 1}}$. Fix bases $v_1, \ldots, v_{2g}$ of $T_\ell(A)$ and $v'_1, \ldots, v'_{2g}$ of $T_\ell(A')$. Then $v_1 \otimes 1, \ldots, v_{2g} \otimes 1$ and $v'_1 \otimes 1, \ldots, v'_{2g} \otimes 1$ are bases for $V_\ell(A)$ and $V_\ell(A')$, respectively. We can describe $\varphi : T_\ell(A) \to T_\ell(A')$ as a matrix $M \in \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$ with ℓ-integral entries (we write this matrix with respect to the chosen bases). Notice that the multiplication by an integer N from A to itself corresponds to the matrix $N\,\mathrm{Id}$, and the isogeny ψ from A' to A such that $\psi \circ \varphi = [D]$ corresponds to the matrix DA^{-1}, which again has integer entries.

Lemma 5.2.4. *The matrix M is such that $v_\ell(\det(M)) = v_\ell(D)$.*

Proof. One may easily check that the map
$$\begin{aligned} (T_\ell(A) \otimes \mathbb{Q}_\ell)/T_\ell(A) &\to A[\ell^\infty] \\ e \otimes \ell^{-n} &\mapsto e^{(n)} \end{aligned}$$
is an isomorphism of $\mathbb{Z}_\ell$-modules. Moreover, the kernel of the action of M by multiplication on $(T_\ell(A) \otimes \mathbb{Q}_\ell)/T_\ell(A) \cong A[\ell^\infty]$ is the ℓ-part of the kernel of the isogeny φ, whose cardinality equals $\ell^{v_\ell(D)}$. As $\mathbb{Z}_\ell$ is a PID, we can write $M = P_1 S P_2$, where S is the Smith normal form of M and P_1 and P_2 are invertible matrices in $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$, so that $v_\ell(\det(M)) = v_\ell(\det(S))$. Since the matrices P_1 and P_2 are invertible, it suffices to compute the ℓ-adic valuation of the cardinality of the kernel of the action of the diagonal matrix S.

Let the diagonal entries of S be of the form $u_i \ell^{k_i}$ for $i = 1, \ldots, 2g$, where $u_i \in \mathbb{Z}_\ell^\times$ and the k_i are non-negative integers. Let
$$h = \left(\sum_{n=1}^{t_i} w_{i,n} \ell^{-n} + \mathbb{Z}_\ell \right)_{i=1,\ldots,2g}$$
be an element in $(T_\ell(A) \otimes \mathbb{Q}_\ell)/T_\ell(A) \cong (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$, where the t_i are non-negative integers and the $w_{i,n}$ are in $\{0, \cdots, \ell - 1\}$, with $w_{i,t_i} \neq 0$. Then for any element $h_0 \in$

$\mathbb{Q}_\ell^{2g}$ whose class in $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$ is h, we have $S \cdot h_0 \in \mathbb{Z}_\ell^{2g}$ if and only if $k_i \geqslant t_i$ for all i, and hence the ℓ-adic valuation of the cardinality of the kernel of φ is $\sum_{i=1}^{2g} k_i = v_\ell(\det(S))$. □

The map $\varphi \otimes 1$ is an isomorphism between $V_\ell(A)$ and $V_\ell(A')$. A K-isogeny is compatible with the Galois action of G_K, hence for every $\sigma \in G_K$ and every $v \in V_\ell(A)$ we have:

$$\sigma \cdot v = (\varphi \otimes 1)^{-1}(\sigma \cdot (\varphi \otimes 1)(v)).$$

We conclude that

$$\mathrm{Im}(\tau_{A,\ell^\infty}) = M^{-1}\,\mathrm{Im}(\tau_{A',\ell^\infty})M, \tag{5.3}$$

where $\mathrm{Im}(\tau_{A,\ell^\infty})$ is represented in the basis $v_i \otimes 1$ and $\mathrm{Im}(\tau_{A',\ell^\infty})$ is represented in the basis $v_i' \otimes 1$.

Example 5.2.5. Let E be an elliptic curve over a number field K and let $T \in E[\ell](K)$ be a point of prime order ℓ. Consider the elliptic curve $E' = E/\langle T\rangle$ and let φ be the canonical projection $\varphi : E \to E'$.

Let e_1, e_2 be a basis of $T_\ell(E)$, where $e_1^{(1)} = T$. We define a basis e_1', e_2' of $T_\ell(E')$ as follows:

1. we set $e_2' = \varphi(e_2)$. Notice that $e_2^{(1)} \notin \langle T\rangle$ since T and $e_2^{(1)}$ are linearly independent, and hence $e_2'^{(1)} \neq O$. This implies that e_2' generates a saturated submodule of $T_\ell(E')$.

2. we choose $e_1' = (e_1'^{(n)})_{n\in\mathbb{Z}_{\geqslant 1}} \in T_\ell(E')$ that completes e_2' to a basis of $T_\ell(E')$ (the existence of such an e_1' follows from the structure theory of finitely generated modules over a PID: any saturated submodule of a finitely generated, free module has a free complement).

Therefore we have $\varphi(e_2) = e_2'$ and $\varphi(e_1) = \alpha e_1' + \beta e_2'$ with $\alpha, \beta \in \mathbb{Z}_\ell$. By definition of the isogeny φ, we know that $\varphi(e_1) \equiv 0 \mod \ell$, hence $\alpha \equiv \beta \equiv 0 \mod \ell$. Now, $\alpha \not\equiv 0 \bmod \ell^2$, for otherwise we would have

$$\varphi(e_1^{(2)}) = \beta e_2'^{(2)} = v(\ell\varphi(e_2^{(2)})) = v\varphi(e_2^{(1)})$$

where $\beta \equiv v\ell \mod \ell^2$, contradicting the fact that $\ker\varphi$ is generated by $T = e_1^{(1)}$. We then have

$$\langle \begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\rangle = \langle \begin{pmatrix}\ell\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\rangle$$

as $\mathbb{Z}_\ell$-modules, hence we can choose $\alpha = \ell$ and $\beta = 0$. We conclude that, with this choice of basis, φ acts on the Tate module as multiplication by the matrix $M = \left(\begin{smallmatrix}\ell & 0\\ 0 & 1\end{smallmatrix}\right)$. In particular, it is not a bijection on the Tate modules.

Consider now $\mathrm{Im}(\tau_{E,\ell^\infty})$. Since $T \in E[\ell](K)$ and $e_1^{(1)} = T$, we have

$$\mathrm{Im}(\tau_{E,\ell^\infty}) \subseteq \left\{ \begin{pmatrix} a & b\\ c & d\end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_\ell) \;\middle|\; a \equiv 1, c \equiv 0 \bmod \ell \right\}$$

as all elements of G_K fix the point T. Applying (5.3) we get:

$$\mathrm{Im}(\tau_{E',\ell^\infty}) \subseteq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_\ell) \;\middle|\; a \equiv 1, b \equiv 0 \bmod \ell \right\}.$$

Automorphisms in $\mathrm{Im}(\tau_{E',\ell^\infty})$ do not necessarily fix a point of $E'[\ell]$, but fix the line corresponding to the second basis vector. In particular, E' admits an ℓ-isogeny over K: this is not surprising, as the isogeny having as kernel this fixed line is the dual of the map $E \to E'$ we started with.

Torsion extensions

Let $\varphi : A \to A'$ be a K-isogeny of degree D and consider $\mathrm{Im}(\tau_{A,\ell^n})$ and $\mathrm{Im}(\tau_{A',\ell^n})$. Let $\mathcal{T}_\ell$ and $\mathcal{T}'_\ell$ be the tangent spaces relative to A and A', respectively.

Lemma 5.2.6. *For every $n \geqslant 1$ we have*

$$(\#\mathcal{T}'_\ell)^{-(2g-1)v_\ell(D)} \leqslant \frac{\#\,\mathrm{Im}(\tau_{A',\ell^n})}{\#\,\mathrm{Im}(\tau_{A,\ell^n})} \leqslant (\#\mathcal{T}_\ell)^{v_\ell(D)}.$$

Proof. Let $e := v_\ell(D)$ and $D = \ell^e D'$, where D' is coprime to ℓ. We claim that $A'[\ell^n] \subseteq \varphi(A[\ell^{n+e}])$. Indeed, let $P \in A'[\ell^n]$ and let $P = \varphi(Q)$ for some $Q \in A(\overline{K})$, which exists by surjectivity of φ over $\overline{K}$. Consider an integer E such that $ED' \equiv 1 \pmod{\ell^n}$, so that $P = ED'P$ and let $Q' = ED'Q$. We have

$$0 = \ell^n P = \ell^n \varphi(Q) = \varphi(\ell^n Q).$$

Since $\ell^n Q \in \ker(\varphi)$, we have $\ell^n Q \in A[D]$ and therefore $\ell^n Q' \in A[\ell^e]$. The claim follows as $P = \varphi(Q')$ and $Q' \in A[\ell^{n+e}]$. Since φ commutes with the action of G_K, we have the inclusion

$$K(\varphi(A[\ell^{n+e}])) \subseteq K(A[\ell^{n+e}])$$

and hence $K(A'[\ell^n]) \subseteq K(A[\ell^{n+e}])$. The same reasoning, applied to the isogeny $\psi : A' \to A$ such that $\psi \circ \varphi = [D]$, implies that $K(A[\ell^n]) \subseteq K(A'[\ell^{n+(2g-1)e}])$ (recall that ψ has degree D^{2g-1}). Since $\mathrm{Im}(\tau_{A,\ell^n})$ is isomorphic to the Galois group of the torsion extension $K(A[\ell^n])/K$, we have:

$$\frac{\#\,\mathrm{Im}(\tau_{A',\ell^n})}{\#\,\mathrm{Im}(\tau_{A,\ell^n})} \leqslant \frac{\#\,\mathrm{Gal}\left(K(A[\ell^{n+e}])/K\right)}{\#\,\mathrm{Gal}\left(K(A[\ell^n])/K\right)} \xrightarrow{n\to\infty} (\#\mathcal{T}_\ell)^e$$

and

$$\frac{\#\,\mathrm{Im}(\tau_{A',\ell^n})}{\#\,\mathrm{Im}(\tau_{A,\ell^n})} \geqslant \frac{\#\,\mathrm{Gal}\left(K(A'[\ell^n])/K\right)}{\#\,\mathrm{Gal}\left(K(A'[\ell^{n+(2g-1)e}])/K\right)} \xrightarrow{n\to\infty} \frac{1}{(\#\mathcal{T}'_\ell)^{(2g-1)e}}.$$

By Lemma 5.2.2, for any positive integer t the sequence

$$(\#\,\mathrm{Gal}(K(A[\ell^{n+t}])/K(A[\ell^n])))_n$$

is increasing (and eventually constant) and the same holds for A', so this concludes the proof.

□

Corollary 5.2.7. *The tangent spaces $\mathcal{T}_\ell$ and $\mathcal{T}'_\ell$ have the same dimension.*

Proof. For n large enough, let

$$\#\operatorname{Im}(\tau_{A,\ell^n}) = k_A \ell^{n\cdot\dim(T_\ell)} \quad \text{and} \quad \#\operatorname{Im}(\tau_{A',\ell^n}) = k_{A'}\ell^{n\cdot\dim(\mathcal{T}'_\ell)}$$

for some positive constants k_A and $k_{A'}$ as in (5.2). We have that

$$(k_A/k_{A'})\ell^{n(\dim(\mathcal{T}'_\ell)-\dim(\mathcal{T}_\ell))}$$

is bounded by Lemma 5.2.6, which implies that $\dim(\mathcal{T}'_\ell) = \dim(\mathcal{T}_\ell)$. □

Remark 5.2.8. Corollary 5.2.7 can also be obtained by noticing that the $\mathbb{F}_\ell$-dimension of $\mathcal{T}_\ell$ (resp. $\mathcal{T}'_\ell$) is equal to the $\mathbb{Q}_\ell$-dimension of the identity component of the ℓ-adic monodromy group attached to A (resp. A'). Since an isogeny $A \to A'$ induces an isomorphism between the identity components of the respective ℓ-adic monodromy groups, the claim follows.

Kummer extensions

Let $\varphi : A \to A'$ be a K-isogeny of degree D. Let M be the matrix associated with φ introduced in Section 5.2. Let $P \in A(K) \setminus A(K)_{\mathrm{tors}}$ be a fixed non-torsion point. By equation (5.3) and the Galois-equivariance of φ, and using the notation (5.1), we have that

$$\begin{gathered}\operatorname{Gal}\left(K\left(\frac{1}{\ell^\infty}P\right)\Big/K\right) \xrightarrow{\sim} \operatorname{Gal}\left(K\left(\frac{1}{\ell^\infty}\varphi(P)\right)\Big/K\right)\\ \left(\begin{array}{c|c} B & t \\ \hline 0 & 1 \end{array}\right) \mapsto \left(\begin{array}{c|c} MBM^{-1} & Mt \\ \hline 0 & 1 \end{array}\right).\end{gathered}$$

Consider the ℓ-adic Kummer representations κ_{A,ℓ^∞} and κ_{A',ℓ^∞}, with respect to the points P and $\varphi(P)$ respectively. The previous formula implies

$$\operatorname{Im}(\kappa_{A',\ell^\infty}) = \varphi(\operatorname{Im}(\kappa_{A,\ell^\infty})). \tag{5.4}$$

Lemma 5.2.9. *For any prime ℓ and any positive integers n and N, we have*

$$f_{\ell^n} \mid [T_\ell(A) : \operatorname{Im}(\kappa_{\ell^\infty})]$$
$$f_N \mid [T(A) : \operatorname{Im}(\kappa_\infty)].$$

Proof. The considerations in [LT22, Remark 2.6] hold also in the case of abelian varieties. The statement follows. □

Lemma 5.2.10. *Let $\varphi : A \to A'$ be an isogeny of abelian varieties of degree D. Fix a point $P \in A(K) \setminus A(K)_{\mathrm{tors}}$ and suppose that the set $\mathbb{Z}P$ of multiples of P is Zariski-dense in A. Consider the Kummer representations κ_{A,ℓ^∞} and κ_{A',ℓ^∞} relative to (A,P) and $(A',\varphi(P))$ respectively. Then we have*

$$\#\frac{T_\ell(A')}{\mathrm{Im}(\kappa_{A',\ell^\infty})} = \ell^{v_\ell(D)} \cdot \#\frac{T_\ell(A)}{\mathrm{Im}(\kappa_{A,\ell^\infty})}$$

and

$$\#\frac{T_\ell(A')}{\kappa_{A',\ell^\infty}(\mathrm{Gal}(\overline{K}/K_{\mathrm{tors}}))} = \ell^{v_\ell(D)} \cdot \#\frac{T_\ell(A)}{\kappa_{A,\ell^\infty}(\mathrm{Gal}(\overline{K}/K_{\mathrm{tors}}))}.$$

Proof. As in Section 5.2, let M be the matrix representing the injective linear morphism $\varphi : T_\ell(A) \to T_\ell(A')$ induced by φ on the Tate modules. Recall from (5.4) that $\varphi(\mathrm{Im}(\kappa_{A,\ell^\infty})) = \mathrm{Im}(\kappa_{A',\ell^\infty})$. Let μ (resp. μ') be the Haar measure on $V_\ell(A)$ (resp. $V_\ell(A')$), normalised so that $\mu(T_\ell(A)) = 1$ (resp. $\mu'(T_\ell(A')) = 1$). Pulling back μ' along the invertible linear map $\varphi : V_\ell(A) \to V_\ell(A')$ we obtain a Haar measure on $V_\ell(A)$, which is therefore a multiple $c\,\mu$ of the Haar measure μ. To determine c, we use the change of variables formula in ℓ-adic integration:

$$c = c\int_{T_\ell(A)} d\mu = \int_{T_\ell(A)} \varphi^*(d\mu') = \int_{\varphi(T_\ell(A))} d\mu' = \mu'(\varphi(T_\ell(A))).$$

Since $T_\ell(A')$ is the disjoint union of $[T_\ell(A') : \varphi(T_\ell(A))]$ translates of $\varphi(T_\ell(A))$, we have

$$\mu'(\varphi(T_\ell(A))) = \frac{1}{[T_\ell(A') : \varphi(T_\ell(A))]} = \ell^{-v_\ell(\det(M))} = \ell^{-v_\ell(D)},$$

where the last two equalities follows from well-known facts in the theory of modules over a PID (Smith normal form) and Lemma 5.2.4. The Kummer image $\mathrm{Im}(\kappa_{A,\ell^\infty})$ is an open subgroup of $T_\ell(A)$: see for example [Hin88, Proposition 1], which implies the openness of $\mathrm{Im}(\kappa_{A,\ell^\infty})$ by passing to the inverse limit (because $\mathbb{Z}P$ is Zariski-dense in A). We can then compute, using again the change of variables formula in ℓ-adic integration:

$$\begin{aligned}\mu'(\mathrm{Im}(\kappa_{A',\ell^\infty})) &= \int_{\mathrm{Im}(\kappa_{A',\ell^\infty})} d\mu' = \int_{M(\mathrm{Im}(\kappa_{A,\ell^\infty}))} d\mu' \\ &= \int_{\mathrm{Im}(\kappa_{A,\ell^\infty})} M^*(d\mu') = c\int_{\mathrm{Im}(\kappa_{A,\ell^\infty})} d\mu = \ell^{-v_\ell(D)}\mu(\mathrm{Im}(\kappa_{A,\ell^\infty})).\end{aligned}$$

This concludes the proof of the first claimed equality, as

$$\#\frac{T_\ell A'}{\mathrm{Im}(\kappa_{A',\ell^\infty})} = \frac{1}{\mu'(\mathrm{Im}(\kappa_{A',\ell^\infty}))} \qquad \text{and} \qquad \#\frac{T_\ell A}{\mathrm{Im}(\kappa_{A,\ell^\infty})} = \frac{1}{\mu(\mathrm{Im}(\kappa_{A,\ell^\infty}))}.$$

The proof of the second equality in the statement follows, simply replacing $\mathrm{Im}\,\kappa_{A',\ell^\infty}$ with $\kappa_{A',\ell^\infty}(\mathrm{Gal}(\overline{K}/K_{\mathrm{tors}}))$ and $\mathrm{Im}\,\kappa_{A,\ell^\infty}$ with $\kappa_{A,\ell^\infty}(\mathrm{Gal}(\overline{K}/K_{\mathrm{tors}}))$. Note that the torsion fields of A and A' coincide. □

Corollary 5.2.11. *With notation and assumptions as in Lemma 5.2.10, let N be any positive integer. We have*

$$\frac{N^{2g}}{\#\operatorname{Im}(\kappa_{A',N})} \mid D \cdot \#\frac{T(A)}{\operatorname{Im}(\kappa_{A,\infty})}.$$

Proof. By Lemma 5.2.9, the left-hand side divides $[T(A') : \operatorname{Im}(\kappa_{A',\infty})]$.

We have

$$\frac{T(A')}{\operatorname{Im}(\kappa_{A',\infty})} \cong \frac{\prod_\ell T_\ell(A')}{\prod_\ell \kappa_{A',\ell^\infty}(\operatorname{Gal}(\overline{K}/K_{\mathrm{tors}}))} \cong \prod_\ell \frac{T_\ell(A')}{\kappa_{A',\ell^\infty}(\operatorname{Gal}(\overline{K}/K_{\mathrm{tors}}))}.$$

By the second part of Lemma 5.2.10 we then obtain that the order of $\frac{T(A')}{\operatorname{Im}(\kappa_{A',\infty})}$ is

$$\prod_\ell \#\frac{T_\ell(A')}{\kappa_{A',\ell^\infty}(\operatorname{Gal}(\overline{K}/K_{\mathrm{tors}}))} = \prod_\ell \ell^{v_\ell(D)} \frac{T_\ell(A)}{\kappa_{A,\ell^\infty}(\operatorname{Gal}(\overline{K}/K_{\mathrm{tors}}))} = D \cdot \#\frac{T(A)}{\operatorname{Im}\kappa_{A,\infty}}.$$

□

5.3 Injectivity of $A(\overline{K})_{\mathrm{tors}}$

Let A be an abelian variety defined over a number field K. Consider the $\operatorname{End}_K(A)$-module $A(\overline{K})_{\mathrm{tors}}$. We aim to understand when this module is injective. By [Tro23a, Remark 5.2], if $\operatorname{End}_K(A)$ is a domain which is a maximal order inside $\operatorname{End}_K(A) \otimes \mathbb{Q}$, then $A(\overline{K})_{\mathrm{tors}}$ is an injective $\operatorname{End}_K(A)$-module. Up to isogeny, we can always assume that $\operatorname{End}_K(A)$ is a maximal order in $\operatorname{End}_K(A) \otimes \mathbb{Q}$ (see [Lom16, Lemma A.3]). Our goal is then to drop the assumption that $\operatorname{End}_K(A)$ is a domain, or equivalently, that A is a simple abelian variety over K.

Up to isogeny, we can write any abelian variety A over K as $A_1^{n_1} \times \ldots \times A_r^{n_r}$ for some non-negative integers $r, n_1, \ldots, n_r$, where each A_i is K-simple and A_i is not K-isogenous to A_j for $i \neq j$. We will consider separately powers of simple abelian varieties and products of abelian varieties sharing no common factors.

Lemma 5.3.1. *If $A(\overline{K})_{\mathrm{tors}}$ is an injective $\operatorname{End}_K(A)$-module, then $A^n(\overline{K})_{\mathrm{tors}}$ is an injective $\operatorname{End}_K(A^n)$-module.*

Proof. We have $\operatorname{End}_K(A^n) = \mathcal{M}_{n\times n}(\operatorname{End}_K(A))$. Since any ring R is Morita equivalent to $\mathcal{M}_{n\times n}(R)$ (see for example [Lam99, Theorem 17.20]), we have an equivalence between the categories $\operatorname{End}_K(A)$-Mod and $\mathcal{M}_{n\times n}(\operatorname{End}_K(A))$-Mod. In particular, the module $A(\overline{K})_{\mathrm{tors}}$ in the category of $\operatorname{End}_K(A)$-modules corresponds to $A^n(\overline{K})_{\mathrm{tors}} = (A(\overline{K})_{\mathrm{tors}})^{\oplus n}$ in the category of $\mathcal{M}_{n\times n}(\operatorname{End}_K(A))$ modules through this equivalence, from which the statement follows. □

Lemma 5.3.2. *Let A and B be abelian varieties defined over K with no common factor and let $C = A \times B$. Then $C(\overline{K})_{\mathrm{tors}}$ is an injective $\operatorname{End}_K(C)$-module if and only if $A(\overline{K})_{\mathrm{tors}}$ and $B(\overline{K})_{\mathrm{tors}}$ are injective as modules over $\operatorname{End}_K(A)$ and $\operatorname{End}_K(B)$ respectively.*

Proof. We have $C(\overline{K})_{\mathrm{tors}} = A(\overline{K})_{\mathrm{tors}} \times B(\overline{K})_{\mathrm{tors}}$ and $\mathrm{End}_K(C) \cong \mathrm{End}_K(A) \times \mathrm{End}_K(B)$ as A and B have no common factor. We conclude because for two rings R_1 and R_2 the product category R_1-Mod $\times$ R_2-Mod and the category $(R_1 \times R_2)$-Mod are equivalent. □

Theorem 5.3.3. *Let A be an abelian variety defined over the field $K = K(A[3])$. There exist an isogeny $\varphi : A \to A'$ and an isogeny $\psi : A' \to A$ such that $A'(\overline{K})_{\mathrm{tors}}$ is an injective $\mathrm{End}_K(A')$-module. There exists an effective bound Ξ, depending only on A and on K, for the degree of both φ and ψ.*

Proof. Since $K = K(A[3])$, we know that $\mathrm{End}_K(A) = \mathrm{End}_{\overline{K}}(A)$ (see for instance [Eck05, Lemme 8]). By [Rém17, Théorèmes 1.1 and 1.6] there exist K-isogenies $\varphi : A \to A' \cong A_1^{n_1} \times \ldots \times A_r^{n_r}$ and $\psi : A' \to A$, where the A_i are geometrically simple abelian varieties defined over K that are pairwise not isogenous over $\overline{K}$ and such that $\mathrm{End}_K(A_i)$ is a maximal order in $\mathrm{End}_K(A_i) \otimes \mathbb{Q} = \mathrm{End}_{\overline{K}}(A_i) \otimes \mathbb{Q}$ for each i. By [Tro23a, Remark 5.2], $A_i(\overline{K})_{\mathrm{tors}}$ is an injective $\mathrm{End}_K(A_i)$-module, so we can conclude by Lemmas 5.3.1 and 5.3.2. An effective bound Ξ for the degree of φ and ψ is given in [GR23, Théorème 1.9(2)], see Remark 5.3.4 (notice that another non-effective but sharper bound is given in [GR23, Théorème 1.4]). □

Remark 5.3.4. Let A be an abelian variety of dimension g defined over a field K. The explicit value of Ξ given in [GR23] is:

$$\Xi(A) = \left((7g)^{8g^2}[K : \mathbb{Q}] \max(1, \log[K : \mathbb{Q}], h_F(A))\right)^{2g^2}$$

and it depends only on the dimension g of A, on the degree $[K : \mathbb{Q}]$ and on the Faltings height $h_F(A)$.

5.4 Torsion representations and homotheties for CM abelian varieties

In this section we consider the cohomology group $H^1(\mathrm{Im}(\tau_\infty), A(\overline{K})_{\mathrm{tors}})$ for an abelian variety A. We look for a positive integer n that is a multiple of the exponent of this cohomology group. The best tool we have to find such an integer is Sah's Lemma (see for instance [BR03, Lemma A.2]), which states that, if an element z is in the center of a group G, then $(z - \mathrm{Id})H^1(G, M) = 0$ for any G-module M, where we identify z to the endomorphism of $H^1(G, M)$ induced by it. To use Sah's Lemma in our case, we consider homotheties inside $\mathrm{Im}(\tau_\infty)$.

Serre proved that for any abelian variety A there exists an integer $c \geqslant 1$ such that the image of the torsion representation τ_∞ contains all the homotheties inside $(\hat{\mathbb{Z}}^\times)^c$ (see [Win02, Théorème 3]), but this integer c is not effective.

The following result by Eckstein [Eck05, Théorème 7] gives us an effective integer c in the case of abelian varieties with complex multiplication, therefore allowing us to provide an effective integer n to use in Theorem 5.0.1 (2) in this case.

Theorem 5.4.1 (Eckstein)**.** *Let A be an abelian variety over a number field K and with complex multiplication over $\overline{K}$. Then $\mathrm{Im}(\tau_{\ell^\infty})$ contains $(\mathbb{Z}_\ell^\times)^c \subseteq \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$, where $c = [K(A[3]) : \mathbb{Q}]$ (which divides $\#\,\mathrm{Aut}(A[3]) \cdot [K : \mathbb{Q}]$).*

Corollary 5.4.2. *Let A be an abelian variety over a number field K. There exists a positive integer n such that*

$$n \cdot H^1(\mathrm{Im}(\tau_\infty), A(\overline{K})_{\mathrm{tors}}) = 0.$$

If A has complex multiplication over $\overline{K}$, then we can effectively bound the integer n in terms of $g = \dim A$ and $[K : \mathbb{Q}]$.

Proof. Let c be a positive integer such that $\mathrm{Im}(\tau_\infty) \supseteq (\hat{\mathbb{Z}}^\times)^c$. In particular, by Theorem 5.4.1, we can choose $c = [K(A[3]) : \mathbb{Q}]$ if A has complex multiplication over $\overline{K}$. We define the element $z = (z_\ell)_\ell \in \hat{\mathbb{Z}}$ as:

$$z_\ell = \begin{cases} 1 + 2^{v_2(c)+2} & \text{if } \ell = 2 \\ 2^c & \text{otherwise} \end{cases}$$

We have $z_\ell \in (\mathbb{Z}_\ell^\times)^c$ for each ℓ, and therefore $z \in \hat{\mathbb{Z}}^{\times c} \subseteq \mathrm{Im}(\tau_\infty)$. Define

$$n := 2^{v_2(c)+2}(2^c - 1) \in \mathbb{Z}$$

and notice that $z - 1 = un$ for some unit $u \in \hat{\mathbb{Z}}^\times$. By Sah's Lemma, since z is a homothety in $\mathrm{Im}(\tau_\infty)$ and hence in the centre of $\mathrm{Im}(\tau_\infty)$, we have that $z - 1$ kills $H^1(\mathrm{Im}(\tau_\infty), M)$ for any $\mathrm{Im}(\tau_\infty)$-module M, and hence the statement follows.

□

5.5 The algebra generated by the image of the torsion representation

In this section, we consider the subring of $\mathrm{End}(A(\overline{K})_{\mathrm{tors}})$ generated by $\mathrm{Im}(\tau_\infty)$. In order to apply Theorem 5.0.1, we wish to find an integer m such that this subring contains $m \cdot \mathrm{End}(A(\overline{K})_{\mathrm{tors}})$. Notice that in the case of (non-CM) elliptic curves an effective value for such an integer m was found by bounding the so-called parameter of maximal growth μ (see [Tro23b, §6.2]), that is, an integer such that the image of τ_∞ contains all the elements of the form $\mathrm{Id} + \mu B$ where $B \in \mathrm{End}(A(\overline{K})_{\mathrm{tors}}) \cong \mathcal{M}_{2g\times 2g}(\hat{\mathbb{Z}})$.

Let $R = \mathrm{End}_K(A)$. We first consider the ℓ-adic case and look for integers m_ℓ such that the subring of $\mathrm{End}_R(T_\ell(A))$ generated by $\mathrm{Im}(\tau_{\ell^\infty})$ contains $m_\ell \cdot \mathrm{End}_R(T_\ell(A))$. We rely on the following result by Gaudron and Rémond (see [GR23, Théorème 1.5(2) and Théorème 1.9(5)]), which will also allow us to patch the various ℓ-adic results to an adelic one.

Theorem 5.5.1 (Gaudron-Rémond)**.** *There exist an integer d and an explicit constant Ξ, depending on the abelian variety A/K (see Remark 5.3.4), such that:*

$$\prod_{\ell} \mathrm{disc}(\mathbb{Z}_\ell[\mathrm{Im}(\tau_\ell)]) \mid d$$

and

$$\prod_{\ell} \mathrm{disc}(\mathbb{Z}_\ell[\mathrm{Im}(\tau_\ell)]) \leqslant \Xi^2.$$

Lemma 5.5.2. *Let ℓ be a prime and $R = \mathrm{End}_K(A)$. There exists a positive integer m_ℓ such that the subring of $\mathrm{End}_R(T_\ell A)$ generated by $\mathrm{Im}(\tau_{\ell^\infty})$ contains $m_\ell \cdot \mathrm{End}_R(T_\ell A)$. In particular one can take such an m_ℓ that satisfies $m_\ell^2 \mid \mathrm{disc}(\mathbb{Z}_\ell[\mathrm{Im}(\tau_{\ell^\infty})])$.*

Proof. Let $V_\ell A = T_\ell A \otimes \mathbb{Q}_\ell$ and consider $\mathrm{End}_{\mathrm{Im}(\tau_{\ell^\infty})}(V_\ell A)$, the endomorphisms of $V_\ell A$ that commute with the elements of $\mathrm{Im}(\tau_{\ell^\infty})$. By Faltings's theorem (see [Mil08, Chapter IV, Theorem 2.5]) we have that $\mathrm{End}_{\mathrm{Im}(\tau_{\ell^\infty})}(V_\ell A) = R \otimes \mathbb{Q}_\ell$. Therefore, the centraliser $C_{\mathrm{End}(V_\ell A)}(\mathbb{Q}_\ell[\mathrm{Im}(\tau_{\ell^\infty})])$ of $\mathbb{Q}_\ell[\mathrm{Im}(\tau_{\ell^\infty})]$ inside $\mathrm{End}(V_\ell A)$ is $R \otimes \mathbb{Q}_\ell$. Trivially, the centraliser of $R \otimes \mathbb{Q}_\ell$ inside $\mathrm{End}(V_\ell A)$ is $\mathrm{End}_{R\otimes\mathbb{Q}_\ell}(V_\ell A)$, hence by the double centraliser theorem (see for example [Mil20a, Chapter IV, Theorem 1.14]) we obtain $\mathrm{End}_{R\otimes\mathbb{Q}_\ell}(V_\ell A) = \mathbb{Q}_\ell[\mathrm{Im}(\tau_{\ell^\infty})]$. This implies that $\mathrm{rk}_{\mathbb{Z}_\ell}(\mathrm{End}_R(T_\ell A)) = \mathrm{rk}_{\mathbb{Z}_\ell}(\mathbb{Z}_\ell[\mathrm{Im}(\tau_{\ell^\infty})])$, and hence that the index $[(\mathrm{End}_R(T_\ell A)) : \mathbb{Z}_\ell[\mathrm{Im}(\tau_{\ell^\infty})]]$ is finite. This proves the existence of m_ℓ, which can be taken to be this index.

The second statement follows from the basic properties of discriminants, since we have

$$\mathrm{disc}(\mathbb{Z}_\ell[\mathrm{Im}(\tau_{\ell^\infty})]) = [(\mathrm{End}_R(T_\ell A)) : \mathbb{Z}_\ell[\mathrm{Im}(\tau_{\ell^\infty})]]^2 \cdot \mathrm{disc}(\mathrm{End}_R(T_\ell A)).$$

□

The next result can also be obtained directly from [GR23, Corollaire 13.8], but with a less sharp bound.

Theorem 5.5.3. *There exists a positive integer m such that the subring of $\mathrm{End}(A(\overline{K})_{\mathrm{tors}})$ generated by $\mathrm{Im}(\tau_\infty)$ contains $m \cdot \mathrm{End}(A(\overline{K})_{\mathrm{tors}})$. We may take m such that $m \leqslant \Xi$, where Ξ is as in Remark 5.3.4.*

Proof. If we let m_ℓ be as in Lemma 5.5.2, by Theorem 5.5.1 we have $m_\ell = 1$ for almost all ℓ. We can therefore define the integer $m = \prod_\ell m_\ell$, which is as requested because

$$\begin{aligned} m \cdot \mathrm{End}_R(TA) = m \cdot \prod_\ell \mathrm{End}_R(T_\ell A) &= \prod_\ell (m_\ell \cdot \mathrm{End}_R(T_\ell A)) \\ &\subseteq \prod_\ell \mathbb{Z}_\ell[\mathrm{Im}(\tau_{\ell^\infty})] = \hat{\mathbb{Z}}[\mathrm{Im}(\tau_\infty)] \end{aligned}$$

by Lemma 5.5.2. To justify the last equality, note that for all $\hat{\mathbb{Z}}$-modules M one has $M = \hat{\mathbb{Z}}M = (\prod_\ell \mathbb{Z}_\ell)\, M = \prod_\ell (\mathbb{Z}_\ell M)$, and it follows from the definitions that

$$\mathbb{Z}_\ell \left(\hat{\mathbb{Z}}[\mathrm{Im}(\tau_\infty)] \right) = \mathbb{Z}_\ell[\mathrm{Im}(\tau_{\ell^\infty})].$$

The last assertion follows from Theorem 5.5.1. □

5.6 An effective bound for the Kummer failure in the CM case

We are now ready to prove Theorem 5.0.3:

Theorem 5.6.1. *With the notation and the assumptions of Theorem 5.0.3, there is an abelian variety A' over K such that $A'(\overline{K})_{\mathrm{tors}}$ is an injective $\mathrm{End}_K(A')$-module and a K-isogeny $\varphi : A' \to A$ such that $\deg(\varphi)$ can be effectively bounded (the bound depending only on A and K). Moreover, we have*

$$f_N \Big| \deg(\varphi) \cdot (dnm)^{2g} \tag{5.5}$$

where d is the divisibility parameter of $G \subseteq A(K)$ and $n > 0$ is the exponent of $H^1(\mathrm{Im}(\tau_{A',\infty}), A'(\overline{K})_{\mathrm{tors}})$ and m is the smallest positive integer such that the subring of $\mathrm{End}(A'(\bar{K})_{\mathrm{tors}})$ generated by $\mathrm{Im}(\tau_{A',\infty})$ contains $m \cdot \mathrm{End}(A'(\bar{K})_{\mathrm{tors}})$. The integer d can be effectively computed and the integers n and m exist and can be effectively bounded (where the bound depends only on A and K).

Proof. Since $[K(A[3], \frac{1}{N}G) : K(A[\mathrm{lcm}(3, N)])]$ divides $[K(\frac{1}{N}G) : K(A[N])]$, the Kummer failure for A over K divides the Kummer failure for A over $K(A[3])$, and their ratio is at most $[K(A[3]) : K]$. We will then assume, without loss of generality, that $K = K(A[3])$. By Theorem 5.3.3 there exist A' and φ as in the statement. By Theorem 5.2.1 we have

$$f_N \Big| \deg(\varphi) \cdot \# \frac{T(A')}{\mathrm{Im}(\kappa_{A',\infty})}. \tag{5.6}$$

We can now apply Theorem 5.1.1 to the abelian variety A'. By Lemma 5.1.2, the divisibility parameter d of $G \subseteq A$ is effectively computable, and it is easy to check that this is also the divisibility parameter of $\varphi^{-1}(G) \subseteq A'$. By Corollary 5.4.2, n can be effectively bounded. By Theorem 5.5.3 m exists and can be effectively bounded. By (5.6) and Theorem 5.1.1 we can conclude that (5.5) holds.

By Theorem 5.3.3, $\deg \varphi$ and m are both bounded by the same constant Ξ, which only depends on A. Finally, the integer n determined in Corollary 5.4.2 depends on the primes of K for which A' has bad reduction. By [ST68, Corollary 2], these are precisely the primes of bad reduction of A. □

Corollary 5.6.2. *We have*

$$f_N \leqslant \Xi (dn_0 \Xi)^{2g} \quad \textit{and} \quad f_N \mid \Xi' (dn_0 \Xi')^{2g}$$

where n_0 is an effective constant such that $n_0 \cdot H^1(\mathrm{Im}(\tau_{A',\infty}), A'(\overline{K})_{\mathrm{tors}}) = 0$ and Ξ is as in Remark 5.3.4 and $\Xi' = e^{\psi(\Xi)}$ where ψ is the second Chebyshev function (namely, Ξ' is the least common multiple of all integers less then or equal to Ξ).

Proof. The integer n_0 exists by Corollary 5.4.2 and we may easily conclude. □

Remark 5.6.3. In Theorem 5.6.1 we may remove the assumption that A has complex multiplication over K, provided that we have an effective bound for n. Indeed, we have not assumed complex multiplication to effectively bound $\deg \varphi$, d and m.

5.7 Analogues of Schinzel's theorem on radical extensions for division fields

Schinzel's theorem on radical extensions [Sch77, Theorem 2] (see also [Len07]) gives a characterization of the abelian radical extensions of a field. For number fields, it states:

Theorem 5.7.1 (Schinzel)**.** *Let K be a number field and let n be a positive integer. For an element $a \in K$, the Galois group of the splitting field of $x^n - a$ over K is abelian if and only if there exists an element $b \in K$ such that $a^w = b^n$, where w is the largest divisor of n such that K contains the w-th roots of unity.*

Let A be an abelian variety over a number field K. In this setting, the role of an element $a \in K$ in Schinzel's theorem is played by a point $P \in A(K)$, and similarly the Galois group of the splitting field of $x^n - a$ over K corresponds to the Galois group of the extension $K(\frac{1}{n}P)/K$. Moreover, the group of torsion elements of order n over $\overline{K}$ is cyclic group μ_n of roots of unity in the setting of Schinzel's theorem and the group $A[n] \cong (\mathbb{Z}/N\mathbb{Z})^{2g}$ in our setting.

A first obstacle to the generalization of Schinzel's theorem to abelian varieties comes from the fact that any cyclotomic extension $K(\zeta_n)/K$ is abelian, but the torsion extension $K(A[n])/K$ need not be, as its Galois group is a subgroup of $\mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z})$. Since the group $\mathrm{Gal}(K(A[n])/K)$ is a quotient of $\mathrm{Gal}(K(\frac{1}{n}P)/K)$, the latter group can be abelian only when the former is. This leads to the following question, which we answer in Section 5.7:

Question 5.7.2. *When is $K(A[n])/K$ abelian for all values of n?*

A second problem arises from the fact that the torsion subgroup $A[n]$ is not cyclic, as the cyclicity of μ_n plays a vital role in the proof of Schinzel's theorem. On top of this, if $A(K)_{\mathrm{tors}}$ is not cyclic, there is no clear integer w' dividing n which plays the same role as w in the statement of Schinzel's theorem. Two candidates for w' are the largest divisor of n such that $A[w'] \subseteq A(K)$ and the integer $w' = \gcd(\exp(A(K)_{\mathrm{tors}}), n)$. We investigate the following question for both choices of w', and we show in Section 5.7 that the answer is negative in both cases:

Question 5.7.3. *Fix a positive integer n and assume $K(A[n])/K$ is abelian. Is it true that $K(\frac{1}{n}P)/K$ is abelian if and only if there exists $Q \in A(K)$ such that $w'P = nQ$?*

Finally, we consider the following question, to which we can only give a partial answer in Section 5.7:

Question 5.7.4. *Fix a positive integer n and assume $K(\frac{1}{n}P)/K$ is abelian. Can we define a proper divisor v of n such that there exists $Q \in A(K)$ with $vP = nQ$?*

Abelian torsion extensions

The aim of this section is to answer Question 5.7.2 by proving Theorem 5.0.4. We show that an abelian variety A is such that $K(A[n])$ is an abelian extension of K for every n if and only if A is K-isogenous to a product of simple abelian varieties with CM over K. Notice that thea similar result over $\overline{K}$ was already proven in [LLZ23, Lemma 8.2].

Proof of Theorem 5.0.4. The abelian variety A is K-isogenous to $A' := A_1 \times \cdots \times A_r$ where each A_i is K-simple. We clearly have that $K(A'[n]) = K(A_1[n], \dots, A_r[n])$. By the argument in the proof of Lemma 5.2.6, there exist integers $d, d' \geqslant 1$ such that $K(A'[n]) \subseteq K(A[nd])$ and $K(A[n]) \subseteq K(A'[nd'])$ for all $n \geqslant 1$. If $K(A[nd])/K$ is an abelian extension, we obtain that $K(A'[n])/K$ is abelian, and the same holds for $K(A_i[n])/K$ for all i. Similarly, if $K(A_i[nd'])$ is abelian for all i, then $K(A[n])/K$ is abelian. Thus, it suffices to prove the statement in the case A is K-simple.

We first prove (i)⇒(ii). Let g be the dimension of A and fix a prime ℓ. By taking the limit in n, since $K(A[\ell^n])/K$ is abelian, the image G_{ℓ^∞} of τ_{A,ℓ^∞} is an abelian subgroup of $\mathrm{GL}(T_\ell(A)) \cong \mathrm{GL}_{2g}(\mathbb{Z}_\ell) \subset \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$. A well-known theorem of Faltings (see [Mil08, Chapter IV, Theorem 2.5]) gives

$$\mathrm{End}_{G_{\ell^\infty}}(V_\ell(A)) \cong \mathrm{End}_{G_{\ell^\infty}}(\mathbb{Q}_\ell^{2g}) \cong \mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell. \tag{5.7}$$

By assumption, A is K-simple, so $\mathrm{End}_K(A)$ is an integral domain. By [Mil20b, Proposition 3.6], to prove that A has CM over K we aim to show that $\mathrm{End}_K(A) \otimes \mathbb{Q}$ contains a number field of degree $2g$ over $\mathbb{Q}$ (equivalently, it contains an étale $\mathbb{Q}$-algebra of degree $2g$ over $\mathbb{Q}$). By integrality of the free $\mathbb{Z}$-module $\mathrm{End}_K(A)$, it suffices to show that $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ contains a commutative semisimple $\mathbb{Q}$-subalgebra of rank $2g$.

Let $\mathcal{G}_{\ell^\infty}$ be the Zariski closure of G_{ℓ^∞}. Since G_{ℓ^∞} is abelian, the identity component $\mathcal{G}^0_{\ell^\infty}$ is an abelian affine reductive (by Faltings' results [Fal83]) algebraic group, hence a torus. In particular, all of its irreducible representations over $\overline{\mathbb{Q}_\ell}$, which is algebraically closed of characteristic 0, are 1-dimensional. The same is true for $\mathcal{G}_{\ell^\infty}$ itself since this is a commutative group of multiplicative type [Mil17, Theorem 12.30]. It follows that, as a representation of G_{ℓ^∞}, the $\overline{\mathbb{Q}}_\ell$-vector space $T_\ell \otimes \overline{\mathbb{Q}_\ell} \cong \overline{\mathbb{Q}_\ell}^{2g}$ decomposes as $\bigoplus W_i^{\oplus m_i}$, where each W_i is 1-dimensional, $\sum_i m_i = 2g$, and W_i, W_j are non-isomorphic for $i \neq j$.

Using (5.7) we obtain that $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \overline{\mathbb{Q}_\ell}$ is isomorphic to

$$\mathrm{End}_{G_{\ell^\infty}}(\overline{\mathbb{Q}_\ell}^{2g}) \cong \bigoplus_i \mathrm{End}_{G_{\ell^\infty}}\left(W_i^{\oplus m_i}\right) \cong \bigoplus_i \mathrm{Mat}_{m_i \times m_i}(\overline{\mathbb{Q}_\ell}), \tag{5.8}$$

where the last equality follows from Schur's lemma on irreducible representations.

Let $D = \mathrm{End}_K(A) \otimes \mathbb{Q}$ and let F be its center. Since A is K-simple, D is a central simple algebra over F. Let $e = [F : \mathbb{Q}]$ and $m^2 = [D : F]$. As we are working in characteristic zero, we have $em^2 \mid 2g$ (see [Mum70, §21, Theorem 2]). Moreover, the theory of central simple algebras shows that

$$D \otimes_{\mathbb{Q}} \overline{\mathbb{Q}_\ell} \cong \left(\mathrm{Mat}_{m\times m}(\overline{\mathbb{Q}_\ell})\right)^e.$$

Comparing this with (5.8), we obtain that $em = \sum_i m_i = 2g$ and hence, since $em^2 \mid 2g$, we must have $m = 1$. We conclude that $\mathrm{End}_K(A) \otimes \mathbb{Q}$ contains a field of degree $2g$ over $\mathbb{Q}$.

Now we prove (ii)⇒(i). It suffices to treat the case when n is the power of a prime number ℓ, and clearly it suffices to show that the extension $K(A[\ell^\infty])/K$ is abelian, or equivalently that $\mathrm{Im}(\tau_{\ell^\infty})$ is abelian. This is a well-known property of (simple) CM abelian varieties, see for example [ST68, Corollary 2 to Theorem 5]. □

Abelian Kummer extensions

Fix a positive integer n. Let $L_n = K(A[n])$ and suppose $\mathrm{Gal}(L_n/K)$ is abelian. Let $L_n' = K(\frac{1}{n}P)$ and $G_n = \mathrm{Gal}(L_n'/K)$. In general, as discussed in Section 5 and with the same notation, an element $\sigma \in G_n$ can be represented as a matrix:

$$M_\sigma = \left(\begin{array}{c|c} B_\sigma & t_\sigma \\ \hline 0 & 1 \end{array}\right) \in \mathcal{M}_{(2g+1)\times(2g+1)}(\mathbb{Z}/n\mathbb{Z}).$$

It is easy to check that, in general, two elements σ, τ in G_n commute if and only if

$$(B_\sigma - \mathrm{Id})t_\tau = (B_\tau - \mathrm{Id})t_\sigma.$$

We begin by answering Question 5.7.3 choosing first w' as the largest divisor of n such that $A[w'] \subseteq A(K)$, and then $w' = \gcd(\exp(A(K)_{\mathrm{tors}}, n))$.

Let w' be the largest divisor of n such that $A[w'] \subseteq A(K)$. If there exists a point $Q \in A(K)$ such that $nQ = w'P$, then G_n is abelian, since $K(\frac{1}{n}P)$ is the compositum of the two fields $K(A[n])$ and $K(\frac{1}{w'}Q)$, which are both abelian extensions of K. To see that the latter of these extensions is abelian, notice that, since $A[w'] \subseteq A(K)$, the extension $K(\frac{1}{w'}Q)$ is generated by the coordinates of any single point $R \in A(\overline{K})$ with $w'R = Q$.

However, the following example shows that the converse does not hold: if G_n is abelian, there need not exist a point $Q \in A(K)$ such that $nQ = w'P$.

Example 5.7.5. Consider the elliptic curve $E : y^2 = x^3 + 1$ over the field $K = \mathbb{Q}(\sqrt{-3})$ whose torsion subgroup is $E(K)_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. We have $w' = 2$. Let P be a torsion point of order 6 and let $n = 3$. The extension $K(\frac{1}{3}P)/K$ is abelian, but there exists no point $Q \in E(K)$ such that $3Q = 2P$, as Q would need to be a K-rational point of order 9.

Let w' be the greatest common divisor of n and $\exp(A(K)_{\mathrm{tors}})$. In this case neither of the two implications in Schinzel's theorem holds (see Examples 5.7.9 and 5.7.10), but we have the following result if $n = p$ is prime.

Lemma 5.7.6. *Let p be a prime number and suppose that $K(A[p])/K$ is an abelian extension with group H_p. The exponent of $A(K)_{\mathrm{tors}}$ annihilates $H^1(H_p, A[p])$.*

Proof. Let H_p' be the maximal subgroup of H_p of order prime to p. Since H_p is abelian, this is the direct product of the q-Sylow subgroups of H_p for $q \neq p$. In particular, the order of H_p/H_p' is a power of p. Consider the inflation-restriction sequence with respect to the normal subgroup H_p' of H_p:

$$0 \to H^1(H_p/H_p', A[p]^{H_p'}) \to H^1(H_p, A[p]) \to H^1(H_p', A[p])^{H_p/H_p'}.$$

Since $(|H_p'|, |A[p]|) = 1$, the cohomology group $H^1(H_p', A[p])$ is trivial. We now distinguish two cases:

1. If $p \mid \#A(K)_{\mathrm{tors}}$, the exponent of $A(K)_{\mathrm{tors}}$ is a multiple of p, and therefore it annihilates $H^1(H_p, A[p])$, as it annihilates $A[p]$.

2. If $p \nmid \#A(K)_{\mathrm{tors}}$, then it suffices to prove that $H^1(H_p/H_p', A[p]^{H_p'})$ is trivial. More precisely, we show that $A[p]^{H_p'}$ is trivial. If not, $A[p]^{H_p'}$ would be a non-zero vector space over $\mathbb{F}_p$. It is well-known that a p-group acting on a non-trivial vector space over $\mathbb{F}_p$ has non-zero fixed points. Applying this fact to the p-Sylow subgroup of H_p/H_p' (which is the image in H_p/H_p' of the p-Sylow subgroup of H_p) yields that $A[p]^{H_p} = A(K)[p]$ is nontrivial, contradiction.

□

Corollary 5.7.7. *Let p be a prime. If $K(\frac{1}{p}P)/K$ is abelian and $A(K)[p] = \{0\}$, then we have $P = pQ$ for some K-rational point Q.*

Proof. Let H_p be the Galois group of the extension $K(A[p])/K$ and let G_p be the Galois group of $K(\frac{1}{p}P)/K$. Consider the following inflation-restriction sequence:

$$0 \to H^1(G_p/H_p, A[p]^{H_p}) \to H^1(G_p, A[p]) \to H^1(H_p, A[p])^{G_p/H_p}.$$

The cohomology group on the left is trivial, as $A[p]^{H_p} = A(K)[p] = \{0\}$, making the map on the right injective. The integer $\exp(A(K)_{\mathrm{tors}})$ kills $H^1(H_p, A[p])^{G_p/H_p}$ by Lemma 5.7.6, hence $\exp(A(K)_{\mathrm{tors}})$ also annihilates $H^1(G_p, A[p])$. Using the following injective map coming from the exact sequence in [LT22, Lemma 4.3] when $n = p$:

$$\frac{A(K) \cap pA(K(\frac{1}{p}P))}{pA(K)} \hookrightarrow H^1(G_p, A[p]),$$

we conclude that there exists a K-rational point Q such that $P = pQ$. □

Remark 5.7.8. An analogue of Lemma 5.7.6 does not hold for composite integers. Indeed, consider the subgroup H of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ generated by the matrices

$$\begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

One easily checks that the invariants of H acting on $(\mathbb{Z}/4\mathbb{Z})^2$ are given by $(\mathbb{Z}/2\mathbb{Z})^2$, while $H^1\left(H, (\mathbb{Z}/4\mathbb{Z})^2\right)$ has exponent 4. With MAGMA, we found the following example, where H is the Galois group of $K(E[4])/K$ for the elliptic curve E over K, $K(\frac{1}{4}P)/K$ is abelian, but $w'P$ is not 4 times a K-rational point, where $w' = \gcd(4, \exp(E(K)_{tors})$.

Example 5.7.9. Consider the elliptic curve $E : y^2 = x^3 + 2x^2 - 8x$ and $P = (4, 8)$ over the field $K = \mathbb{Q}(i)$. One can check that $E(K)_{\mathrm{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^2$ and that $K(\frac{1}{4}P, E[4])/K$ is abelian, with Galois group $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$. We have $w' := \gcd(4, \exp E(K)_{\mathrm{tors}}) = 2$, but $w'P = 4Q$ does not have solutions in $E(K)$.

Example 5.7.10. Consider $n = 2$ and the abelian variety $A = E_1 \times E_2$ over $\mathbb{Q}$, where $E_1 : y^2 + y = x^3 - x$ has trivial torsion over $\mathbb{Q}$ and $E_2 : y^2 + xy = x^3 - x$ has torsion $\mathbb{Z}/2\mathbb{Z}$ over $\mathbb{Q}$. Notice that $w' := \gcd(2, \exp A(\mathbb{Q})_{\mathrm{tors}}) = 2$. Clearly, $\mathbb{Q}(E[2])/\mathbb{Q}$ is not abelian as $\mathbb{Q}(E_1[2])/\mathbb{Q} \cong S_3$. For any point $P \in A(\mathbb{Q})$, we have that $w'P = nQ$ for $Q = P$, but $\mathbb{Q}(\frac{1}{2}P, A[2])/\mathbb{Q}$ is not abelian.

We now address Question 5.7.4. Let G_n be abelian, and consider the injective homomorphism coming from the exact sequence in [LT22, Lemma 4.3]:

$$\begin{aligned} \alpha : \frac{A(K) \cap nA(L'_n)}{nA(K)} &\hookrightarrow H^1(G_n, A[n]) \\ P &\mapsto (\sigma \mapsto t_\sigma)\,. \end{aligned} \tag{5.9}$$

The group ring $\mathbb{Z}[G_n]$ acts on $A(L'_n)$ by extending the Galois action, and therefore it also acts on $H^1(G_n, A[n])$. We call H the kernel of the action of $\mathbb{Z}[G_n]$ on $H^1(G_n, A[n])$, which – by Sah's lemma (see [BR03, Lemma A.2]) and since G_n is abelian – contains the elements $(\sigma - 1)$ for $\sigma \in G_n$. If $a = \sum_g n_g g$ is an element of $\mathbb{Z}[G_n]$, we denote its trace by $||a|| = \sum_g n_g$. We define v to be the positive integer such that the ideal $v\mathbb{Z}$ is generated by the integers $||h||$ for $h \in H$. Notice that $n \cdot 1 \in H$, therefore $v \mid n$. The following Proposition gives a partial answer to Question 5.7.4: even if v divides n, we are not excluding that v may be n itself.

Proposition 5.7.11. *If G_n is abelian and v is as above, then there exists $Q \in A(K)$ such that $vP = nQ$.*

Proof. Since G_n is abelian, the map α in (5.9) is $\mathbb{Z}[G_n]$-equivariant. Indeed, we have

$$\alpha(\sigma T)(\rho) = \rho(\sigma t) - \sigma t = \sigma(\rho t) - \sigma t = \sigma\left((\alpha T)(\rho)\right)$$

for all $\sigma, \rho \in G_n$ and for all $T \in (A(K) \cap nA(L'_n))/nA(K)$, with t such that $nt = T$. Fix $h \in H$. We have

$$\alpha(hP) = h\alpha(P) = 0$$

by definition of H. Since P belongs to $A(K)$, the Galois group G_n acts trivially on it, and therefore $hP = ||h||P$. As α is injective, this implies that $||h||P \in nA(K)$, concluding the proof. $\square$

Bibliography

[ACP+25] Bryan Advocaat, Clifford Chan, Antigona Pajaziti, Flavio Perissinotto, and Antonella Perucca. Galois groups of Kummer extensions of number fields. *To appear in Publ. Math. Besançon*, 2025.

[Ber88] Daniel Bertrand. Galois representations and transcendental numbers. In *New advances in transcendence theory (Durham, 1986)*, pages 37–55. Cambridge Univ. Press, Cambridge, 1988.

[Bir67] Bryan John Birch. Cyclotomic fields and Kummer extensions. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 85–93. Academic Press, London, 1967.

[BR03] Matthew H. Baker and Kenneth A. Ribet. Galois theory and torsion points on curves. volume 15, pages 11–32. 2003. Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[Cona] Keith Conrad. Galois groups as permutation groups. Lecture notes, available at kconrad.math.uconn.edu/blurbs/galoistheory/galoisaspermgp.pdf.

[Conb] Keith Conrad. Hensel's Lemma. Lecture notes, available at kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf.

[DP16] Christophe Debry and Antonella Perucca. Reductions of algebraic integers. *J. Number Theory*, 167:259–283, 2016.

[Eck05] Carola Eckstein. *Homothéties, à chercher dans l'action de Galois sur des points de torsion*, volume 2005/7 of *Prépublication de l'Institut de Recherche Mathématique Avancée [Prepublication of the Institute of Advanced Mathematical Research]*. Université Louis Pasteur. Institut de Recherche Mathématique Avancée (IRMA), Strasbourg, 2005.

[Fal83] Gerd Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[Gou97] Fernando Q. Gouvêa. *p-adic numbers*. Universitext. Springer-Verlag, Berlin, second edition, 1997. An introduction.

[GR23] Éric Gaudron and Gaël Rémond. Nouveaux théorèmes d'isogénie. *Mém. Soc. Math. Fr. (N.S.)*, (176):vi+129, 2023.

[Has65] Helmut Hasse. über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ teilbarer bzw. unteilbarer Ordnung $\bmod p$ ist. *Math. Ann.*, 162:74–76, 1965.

[Has66] Helmut Hasse. über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung $\bmod p$ ist. *Math. Ann.*, 166:19–23, 1966.

[HHR+87] Kenneth Hardy, R. H. Hudson, D. Richman, Kenneth S. Williams, and N. M. Holtz. Calculation of the class numbers of imaginary cyclic quartic fields. *Math. Comp.*, 49(180):615–620, 1987.

[Hin88] Marc Hindry. Autour d'une conjecture de Serge Lang. *Invent. Math.*, 94(3):575–603, 1988.

[HPST21] Fritz Hörmann, Antonella Perucca, Pietro Sgobba, and Sebastiano Tronto. Explicit Kummer theory for quadratic fields. *JP J. Algebra, Number Theory Appl.*, 49(2):151–178, 2021.

[HPST22] Fritz Hörmann, Antonella Perucca, Pietro Sgobba, and Sebastiano Tronto. Explicit Kummer generators for cyclotomic extensions. *JP J. Algebra, Number Theory Appl.*, 53(1):69–84, 2022.

[HS00] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[Jav21] Abtien Javan Peykar. *Division points in arithmetic*. PhD thesis, Universiteit Leiden, 2021.

[Lam99] Tsit Yuen Lam. *Lectures on modules and rings*, volume 189 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Len07] Hendrik W. Lenstra. Commentary on H: Divisibility and congruences. *Andrzej Schinzel Selecta*, 2:901–902, 2007.

[LLZ23] Samuel Le Fourn, Davide Lombardo, and David Zywina. Torsion bounds for a fixed abelian variety and varying number field, 2023. Preprint available at arXiv:2208.02345.

[Lom16] Davide Lombardo. Explicit surjectivity of Galois representations for abelian surfaces and GL_2-varieties. *J. Algebra*, 460:26–59, 2016.

[LP17] Davide Lombardo and Antonella Perucca. The 1-eigenspace for matrices in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. *New York J. Math.*, 23:897–925, 2017.

[LP21] Davide Lombardo and Antonella Perucca. Reductions of points on algebraic groups. *J. Inst. Math. Jussieu*, 20(5):1637–1669, 2021.

[LT22] Davide Lombardo and Sebastiano Tronto. Effective Kummer theory for elliptic curves. *Int. Math. Res. Not. IMRN*, (22):17662–17712, 2022.

[Mil08] James S. Milne. Abelian varieties (v2.00). Course notes available at www.jmilne.org/math, 2008.

[Mil17] James S. Milne. *Algebraic groups*, volume 170 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017. The theory of group schemes of finite type over a field.

[Mil20a] James S. Milne. Class field theory (v4.03). Course notes available at www.jmilne.org/math, 2020.

[Mil20b] James S. Milne. Complex multiplication (v0.10). Course notes available at www.jmilne.org/math, 2020.

[MS16] Jan Steffen Müller and Michael Stoll. Canonical heights on genus-2 Jacobians. *Algebra Number Theory*, 10(10):2153–2234, 2016.

[Mum70] David Mumford. *Abelian varieties*, volume 5 of *Tata Inst. Fundam. Res., Stud. Math.* London: Oxford University Press, 1970.

[Per15] Antonella Perucca. The order of the reductions of an algebraic integer. *J. Number Theory*, 148:121–136, 2015.

[Per17] Antonella Perucca. Reductions of one-dimensional tori. *Int. J. Number Theory*, 13(6):1473–1489, 2017.

[Per24] Flavio Perissinotto. Kummer theory for abelian varieties, 2024. Preprint available on ORBilu at hdl.handle.net/10993/61819.

[PP22] Flavio Perissinotto and Antonella Perucca. Kummer theory for multiquadratic or quartic cyclic number fields. *Unif. Distrib. Theory*, 17(2):165–194, 2022.

[PP23] Flavio Perissinotto and Antonella Perucca. Kummer theory for products of one-dimensional tori. In *Publications mathématiques de Besançon. Algèbre et théorie des nombres. 2023*, volume 2023 of *Publ. Math. Besançon Algèbre Théorie Nr.*, pages 109–119. Presses Univ. Franche-Comté, Besançon, 2023.

[PP24a] Flavio Perissinotto and Antonella Perucca. Kummer extensions of finite fields, 2024. Preprint available on ORBilu at orbilu.uni.lu/handle/10993/61215.

[PP24b] Flavio Perissinotto and Antonella Perucca. Kummer theory for p-adic fields, 2024. Preprint available on ORBilu at hdl.handle.net/10993/50285.

[PS19] Antonella Perucca and Pietro Sgobba. Kummer theory for number fields and the reductions of algebraic numbers. *Int. J. Number Theory*, 15(8):1617–1633, 2019.

[PST20] Antonella Perucca, Pietro Sgobba, and Sebastiano Tronto. Explicit Kummer theory for the rational numbers. *Int. J. Number Theory*, 16(10):2213–2231, 2020.

[PST21] Antonella Perucca, Pietro Sgobba, and Sebastiano Tronto. The degree of Kummer extensions of number fields. *Int. J. Number Theory*, 17(5):1091–1110, 2021.

[Rém17] Gaël Rémond. Variétés abéliennes et ordres maximaux. *Rev. Mat. Iberoam.*, 33(4):1173–1195, 2017.

[Rib79] Kenneth A. Ribet. Kummer theory on extensions of abelian varieties by tori. *Duke Math. J.*, 46(4):745–761, 1979.

[Rob00] Alain M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[Sch77] Andrzej Schinzel. Abelian binomials, power residues and exponential congruences. *Acta Arithm.*, 32:245–274, 1977.

[Ser86] Jean-Pierre Serre. Résumé des cours de 1985-86, 1986.

[ST68] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *The Annals of Mathematics, Second Series*, 88:492–517, 1968.

[The21] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2)*, 2021. www.sagemath.org.

[Tro19] Sebastiano Tronto. Kummer degrees, 2019. GitHub repository github.com/sebastianotronto/kummer-degrees.

[Tro23a] Sebastiano Tronto. Division in modules and Kummer theory, 2023. Preprint available at arXiv:2111.14363.

[Tro23b] Sebastiano Tronto. Radical entanglement for elliptic curves, 2023. Preprint available at arXiv:2009.08298.

[Vos98] Valentin E. Voskresenskiĭ. *Algebraic groups and their birational invariants*, volume 179 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1998. Translated from the Russian manuscript by Boris Kunyavski [Boris È. Kunyavskiĭ].

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[Win02] Jean-Pierre Wintenberger. Démonstration d'une conjecture de Lang dans des cas particuliers. *J. Reine Angew. Math.*, 553:1–16, 2002.

Acknowledgments

First of all, I would like to express my gratitude to my supervisor in Luxembourg, Antonella Perucca. Thank you for your unwavering support, for always finding time for my questions and discussions, and for understanding my needs in particular when I needed time to unwind and take things slow, which greatly helped me stay motivated during the most challenging times.

Second, I would like to thank my supervisor and promotor in Leiden, Peter Stevenhagen, for your invaluable support and the insightful discussions. Thank you for helping me feel at ease, even in moments when my initial reaction would have been to stress.

I am deeply grateful to the other members of my CET. To Gabor Wiese, thank you for your dedication, your advice and also for your help in navigating all the bureaucratic requirements. To Ján Mináč, thank you for your constant positivity and heartfelt appreciation of my work.

To Davide Lombardo: thank you for your invaluable assistance in the preparation of Chapter 5, for your mentorship, for explaining even the smallest things in detail. It was a privilege to work with you.

To my reading committee – René Schoof, Francesco Pappalardi and Pieter Moree – thank you for the time and effort you dedicated to thoroughly read my thesis. Thanks as well to Peter Bruin for agreeing to be part of my defence committee and for the helpful discussions regarding Chapter 5. For their useful comments and insights during these discussions, my thanks extend also to Marco Streng and Hendrik Lenstra.

To Marta Fiocco, the secretary of my committee: thank you for the enthusiasm with which you accepted to fulfill the role and for your invaluable help at a critical moment when I needed it most.

I am profoundly grateful to all my friends among the PhDs, Postdocs and Master's students in both the department of Mathematics in Luxembourg and the Mathematical Institute in Leiden. Sharing these past four years of my life with you has been great. I could always count on you to make the best moments even more memorable and to lift me up during difficult times. You made the office and the working environment a place

where I could be myself, feel welcome and feel appreciated. There are too many of you to list you all, but rest assured I cherish every moment spent with each of you.

I would also like to thank all my other friends, old and new, scattered across the world who supported me throughout these years. Special thanks goes to Ilaria, for sharing with me the ups and downs of being a PhD student during my last six months in Leiden.

Lastly, but most importantly, I thank my family. I would not be where I am today without your love and support. To my parents, who have always believed in me, even when I did not believe in myself and who have supported me in every choice I have made. To my siblings, Filippo and Francesca, who are such an important part of who I am: I am honored to have you by my side as my paranymphs on one of the most important days of my life.

Special thanks to Bryan and Peter for their help with translations to Dutch, to Silvia for proofreading parts of the thesis and to the artist Alyssa for her work on the cover.

Curriculum Vitae

Flavio Perissinotto was born in Motta di Livenza, Italy in 1995. He earned his high school diploma from Liceo Scientifico G. Galilei in San Donà di Piave in 2014.

He began his academic journey with a Bachelor's degree at the Università degli Studi di Padova, graduating with honours in 2017 with a thesis on the congruent number problem, supervised by Prof. Matteo Longo.

He then pursued a double Master's degree under the ALGANT program, jointly at the Università degli Studi di Padova and the Universität Regensburg. His thesis on the Eichler-Selberg trace formula of modular forms was supervised by Prof. Guido Kings. He graduated *cum laude* from the Università degli Studi di Padova and with the highest grade from the Universität Regensburg in 2019.

In 2021 he began his PhD studies in a joint program at the University of Luxembourg under the supervision of Prof. Antonella Perucca and at Universiteit Leiden under the supervision of Prof. Peter Stevenhagen.

After completing his PhD, he plans to pursue a career in education.