Kummer theory for number fields

Antonella Perucca

j.w. Bryan Advocaat, Chi Wa (Clifford) Chan, Christophe Debry, Fritz Hörmann, Olli Järviniemi, Antigona Pajaziti, Flavio Perissinotto, Pietro Sgobba, Sebastiano Tronto

Table of contents

Introduction

Kummer theory

Let K be a field, and n a positive integer. Suppose that

- n is coprime to $\mathrm{char}(K)$
- $\zeta_n \in K$.

Fundamental Theorem

For an extension of K, the following are equivalent:

- being abelian with exponent dividing n
- being generated by n-th roots of elements of K.

Such extensions are called **Kummer extensions**.

They correspond to the subgroups of $K^\times / K^{\times n}$.

The correspondence (for finite extensions) also gives:

Galois group $\simeq$ Group of "radicals-to-be" .

Example: Cyclic Galois group $\leftrightarrow$ Just one radical

Let $K = \mathbb{Q}(\zeta_{3^4})$ and consider the extension $K(5^{1/3^4})/K$.

- The subfields are

$$K \qquad K(5^{1/3}) \qquad K(5^{1/3^2}) \qquad K(5^{1/3^3}) \qquad K(5^{1/3^4})$$

- The group

$$\langle 5, K^{\times 3^4} \rangle \bmod K^{\times 3^4}$$

  is cyclic of order 3^4 [because 5 is not a third power in $K^\times$].

- The subfields correspond to the subgroups of order

$$1 \qquad 3 \qquad 3^2 \qquad 3^3 \qquad 3^4$$

- The 3^4-th radicals-to-be are

$$5^{3^4} \qquad 5^{3^3} \qquad 5^{3^2} \qquad 5^3 \qquad 5$$

Problem

Consider a finitely generated subgroup G of $K^\times$.

Kummer extension

If $\zeta_n \in K$,

$$[K(\sqrt[n]{G}) : K] = \# G/K^{\times n}$$

$$\mathrm{Gal}(K(\sqrt[n]{G})/K) \simeq G/K^{\times n}$$

Cyclotomic-Kummer extension

If $\mathrm{char}(K) \nmid n$,

$$[K(\sqrt[n]{G}) : K(\zeta_n)] = \# G/K(\zeta_n)^{\times n} = \cdots$$

$$\mathrm{Gal}(K(\sqrt[n]{G})/K(\zeta_n)) \simeq G/K(\zeta_n)^{\times n} \simeq \cdots$$

Motivation

From now on, K is a number field.

Cyclotomic-Kummer extensions

- Studying them is a natural question of algebraic number theory.
- They appear when counting reductions with specific properties (on the order or index of the reductions of algebraic numbers).

Artin's Primitive Root Conjecture

Under GRH, the primes $\mathfrak{p}$ of K for which $(G \bmod \mathfrak{p}) = k_{\mathfrak{p}}^{\times}$ have density

$$\sum_{n \geq 1} \frac{\mu(n)}{[K(\sqrt[n]{G}) : K]}$$

Divisibility parameters

References

This section is based on my works

with Christophe Debry, *Reductions of algebraic integers*, Journal of Number Theory (2016).

with Pietro Sgobba and Sebastiano Tronto, *Addendum to: Reductions of algebraic integers*, Journal of Number Theory (2020).

Parameters for ℓ-divisibility over K

Let $\alpha \in K^\times$, not a root of unity.
Fix some prime number ℓ.

Divisibility parameters (over K)

Integers (d, h), where

$$\alpha = \beta^{\ell^d} \zeta_{\ell^h}$$

with $\beta \in K^\times$ and d maximal.

Example

2-divisibility parameters for $-81 \in \mathbb{Q}$ are $(2, 1)$ because

$$-81 = 3^{2^2} \cdot \underbrace{(-1)}_{2^1}$$

Parameters for ℓ-divisibility over K

Let $G < K^\times$ be finitely generated and torsion-free. Write

$$G = \langle \alpha_1, \dots, \alpha_r \rangle$$
$$\alpha_i = \beta_i^{\ell^{d_i}} \zeta_{\ell^{h_i}}$$

Parameters

⚠ The parameters (d_i, h_i) depend on the basis.

☺ We can use any basis that "shows all divisibility", namely for which

$$\sum_{i=1}^{r} d_i \qquad \text{is maximal}$$

Example

3-divisibility parameters for $\langle 12, 18 \rangle \in \mathbb{Q}$ are $(1, 0); (0, 0)$ because

$$\langle 12, 18 \rangle = \langle 6^3, 18 \rangle$$

Good ℓ-basis over K

$$G = \langle \alpha_1, \ldots, \alpha_r \rangle$$

$$\alpha_i = \beta_i^{\ell^{d_i}} \zeta_{\ell^{h_i}}$$

- $\sum d_i$ is maximal if and only if $\beta_1, \ldots, \beta_r$ are strongly ℓ-independent
- Testing for independence allows us (if not independent) to replace a generator and get a basis that shows more divisibility. This is an explicit finite procedure to construct a good ℓ-basis.

Strongly ℓ-independent

$$\prod_{i=1}^{r} \alpha_i^{x_i} \in \langle K^{\times \ell}, \mu_K \rangle \qquad \Rightarrow \qquad \forall i \quad \ell \mid x_i$$

Independence versus indivisibility

Strongly ℓ-independent

$$\prod_{i=1}^{r} \alpha_i^{x_i} \in \langle K^{\times \ell}, \mu_K \rangle \qquad \Rightarrow \qquad \forall i \quad \ell \mid x_i$$

For $r > 1$, this is more than "each α_i strongly ℓ-indivisible".

Strongly ℓ-indivisible

$$\alpha^x \in \langle K^{\times \ell}, \mu_K \rangle \qquad \Rightarrow \qquad \ell \mid x$$

Example

Over $\mathbb{Q}$: 12 and 3 are not $\pm\square$, so they are each strongly 2-indivisible.
However, they are not strongly 2-independent because $12 \cdot 3 = 6^2$.

The non-unicity of the divisibility parameters

The d-parameters are unique up to reordering.
The associated h-parameters are not unique.

Dilemma

We will present a parametric formula that also depends on the h-parameters, but we say that they are not unique. Do we have to worry?

Intermezzo

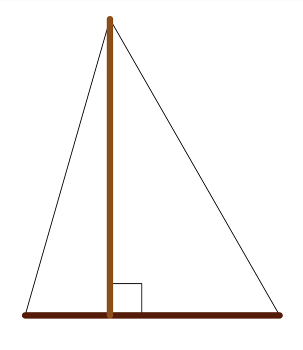

Figure : Area $=$ Basis x Height / 2

The non-unicity of the divisibility parameters

The d-parameters are unique up to reordering.
The associated h-parameters are not unique.

Theorem

We could make the h-parameters unique, by imposing the following conditions (which mean that, whenever possible, we must set the h-parameters to 0):

- For every $1 \leqslant i \leqslant r$ we have $h_i = 0$ or $h_i > z - d_i$.
- If $1 \leqslant i < j \leqslant r$ and $h_i, h_j > 0$ hold, then we have $h_i > h_j$ and $d_i + h_i < d_j + h_j$.
- If $1 \leqslant i < j \leqslant r$ and $d_i = d_j$ hold, then $h_j = 0$.

Parameters over $K(\zeta_4)$, for $\ell = 2$ and $\zeta_4 \notin K$

To study $K(\sqrt[2^n]{G})$ for $n \geq 2$, we need divisibility parameters over $K(\zeta_4)$.

Example

Over $\mathbb{Q}$: 2 has parameters $(0,0)$ because $2 \neq \pm\square$.
Over $\mathbb{Q}(\zeta_4)$: 2 has parameters $(1,2)$ because $2/\zeta_4 = \square$.

Theorem

In K there is at most one element that causes trouble, namely

$$\zeta_{2^s} + \zeta_{2^s} + 2$$

where $s \geq 2$ is maximal such that $K \cap \mathbb{Q}(\zeta_{2^\infty}) = \mathbb{Q}(\zeta_{2^s} + \zeta_{2^s})$.

The d-parameters over $K(\zeta_4)$ are the same over K up to one parameter that could increase by 1. The h-parameters can change and we have an explicit case distinction.

Key result: Schinzel's Theorem (rephrased)

Schinzel's Theorem on Abelian radical extensions

If α is strongly ℓ-indivisible, $K(\zeta_{\ell^n}, \sqrt[\ell^n]{\alpha})$ is abelian only if $\zeta_{\ell^n} \in K$.

Idea (for ℓ^n): Cyclotomic-Kummer extensions are non-abelian unless they are cyclotomic or Kummer.

Important consequence

If ℓ is odd, or if $\zeta_4 \in K$, the divisibility parameters over K are the same as the divisibility parameters over $K(\zeta_{\ell^n})$.

Cyclotomic-Kummer extensions

Main Result for ℓ^n extensions (in layman's terms)

Let K be a number fields, ℓ a prime number, $G < K^\times$ finitely generated and torsion-free. Consider the cyclotomic-Kummer extensions

$$K(\sqrt[\ell^n]{G})$$

We want to pin down the Kummer extensions $K(\sqrt[\ell^n]{G})/K(\zeta_{\ell^n})$.

USE THE DIVISIBILITY PARAMETERS OVER K
(in fact, over $K(\zeta_4)$ for $\ell = 2$ and $n > 1$)

- You have everything you need.
- Divisibility parameters to rule them all.

The degree of $K(\sqrt[\ell^n]{G})/K(\zeta_{\ell^n})$

Theorem [Debry and P., Journal of Number Theory 2016]

- For ℓ odd or $\zeta_4 \in K$, the degree of $K(\sqrt[\ell^n]{G})/K(\zeta_{\ell^n})$ is ℓ to the power

  $$\sum_i \max(n-d_i,0) \quad + \quad \max(\max_i(h_i+\min(n,d_i)-n'),0)$$

  where $n' = \max(n, v_\ell \# \mu_{K(\zeta_\ell)})$.

- For $\ell = 2$, $\zeta_4 \notin K$, $n \geq 2$: we use divisibility parameters over $K(\zeta_4)$.

The Galois group of $K(\sqrt[\ell^n]{G})/K(\zeta_{\ell^n})$

Work in progress:

[Advocaat, Chan, Pajaziti, Perissinotto and P., 2023]

The Galois group of $K(\sqrt[\ell^n]{G})/K(\zeta_{\ell^n})$ has a group structure that is determined by the divisibility parameters. There is an explicit formula.

Further results

The degree of $K(\sqrt[n]{G})/K(\zeta_n)$

Example

$\zeta_2 \in \mathbb{Q}$, $\sqrt{5} \in \mathbb{Q}(\zeta_5)$

Theorem

There is some constant C such that, to compute the *failure of maximality* for the degree of $K(\sqrt[n]{G})/K(\zeta_n)$, we may replace n by $\gcd(n, C)$.

Computability of all degrees

$\mathbb{Q}$ (Tronto's GitHub); Multiquadratic fields; Quartic cyclic fields; Number fields without quadratic subfields.

Compute generators for the Kummer extensions of K inside $K(\zeta_\infty)$.

References: Many papers j.w. Hörmann, Perissinotto, Sgobba, Tronto.

The degree of $K(\zeta_N, \sqrt[n]{G})$

Procedure

- Compute the degree of $K(\zeta_{\ell^E}, \sqrt[\ell^e]{G})$ for all ℓ and $E \geq e$.
- Compute $K(\zeta_{\ell^E}, \sqrt[\ell^e]{G}) \cap K(\zeta_\infty)$ for $\zeta_{\ell^e} \in K$.

One can compute finitely many elements whose radicals generate all Kummer extensions of K inside $K(\zeta_\infty)$. Then it suffices to check whether equivalent radicals are contained in G.

Entanglement groups

Introduced by H.W. Lenstra, developed by W.J. Palenstijn.

Theorem [P. Sgobba Tronto, Manuscripta Math. 2021]

The degree of $K(\sqrt[n]{G})$ over K is

$$\frac{\#\langle K^\times, \sqrt[n]{G}\rangle / K^\times}{\# E_n} \cdot \prod_{p \mid n, \zeta_p \notin K} \frac{p-1}{p}$$

where E_n is the finite abelian group

$$\frac{\mathrm{Aut}_{K^\times}\langle K^\times, \sqrt[n]{G}\rangle}{\mathrm{Gal}(K(\sqrt[n]{G})/K)}$$

There is a constant C such that

$$\# E_n = \# E_{\gcd(n,C)}$$

Maximality of Kummer extensions

Example

For every $\alpha \in \mathbb{Q}^\times$, we have $\sqrt{\alpha} \in \mathbb{Q}(\zeta_\infty)$.

Theorem [Järviniemi P., Research in Number Theory 2022]

If $K \neq \mathbb{Q}$, then there exists a sequence $(\alpha_i)_{i \in \mathbb{Z}_{>0}}$ with $\alpha_i \in K^\times$ for all $i > 0$ which are algebraic integers and not units, whose norms $N(\alpha_i)$ are pairwise coprime, and such that for all positive integers r, n we have

$$[K(\zeta_\infty, \alpha_1^{1/n}, \ldots, \alpha_r^{1/n}) : K(\zeta_\infty)] = n^r \,.$$

Thank you!