Universiteit
Leiden
The Netherlands

Radicals in arithmetic

Palenstijn, W.J.

Citation
Palenstijn, W. J. (2014, May 22). *Radicals in arithmetic*. Retrieved from https://hdl.handle.net/1887/25833

Version:	Corrected Publisher's Version
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/25833

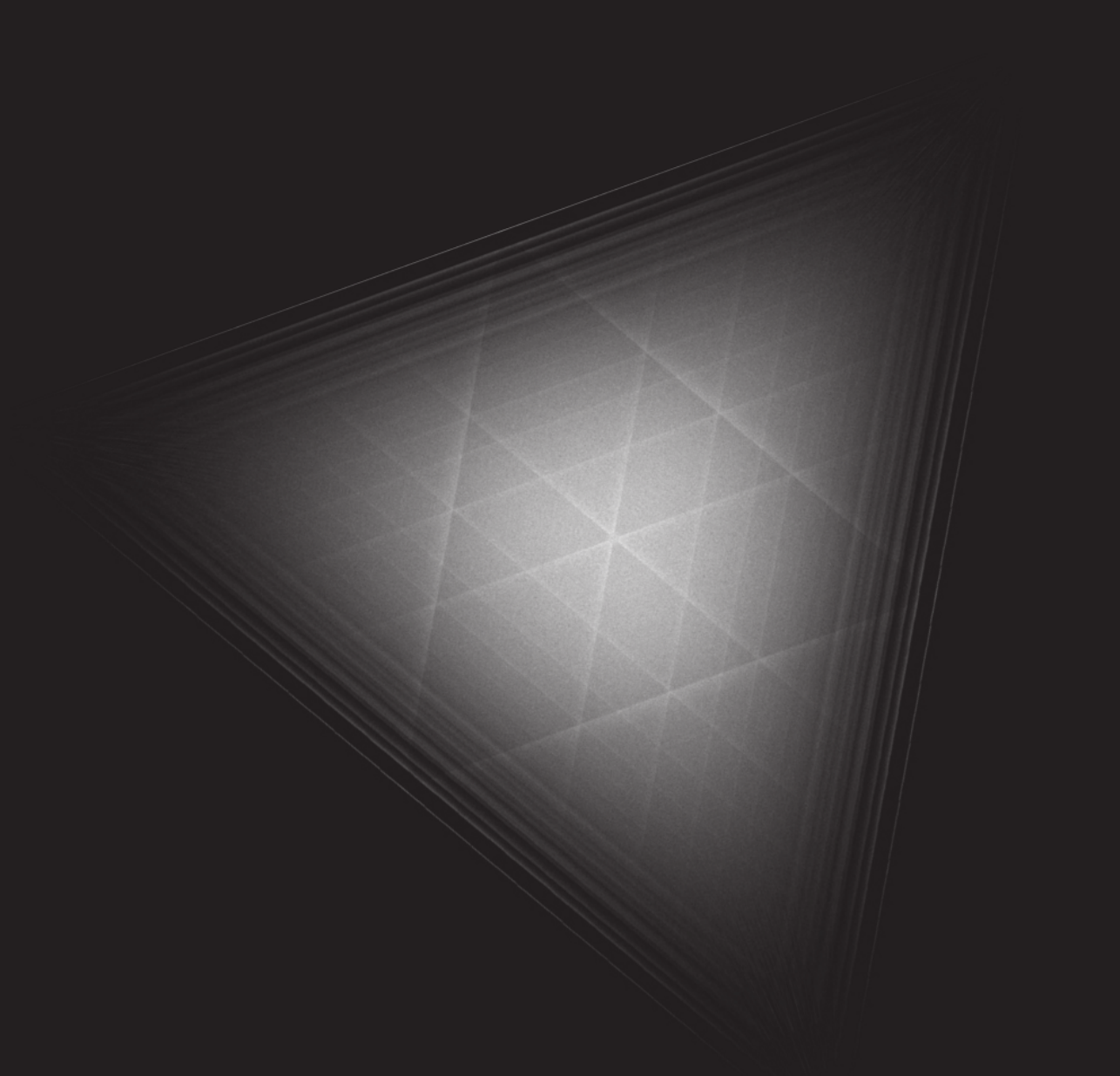
Note: To cite this publication please use the final published version (if applicable).

Cover Page

Universiteit Leiden

The handle http://hdl.handle.net/1887/25833 holds various files of this Leiden University dissertation

Author: Palenstijn, Willem Jan
Title: Radicals in Arithmetic
Issue Date: 2014-05-22



Radicals in Arithmetic

Willem Jan Palenstijn

Radicals in Arithmetic

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op donderdag 22 mei 2014
klokke 15:00 uur

door

Willem Jan Palenstijn

geboren te Leiden
in 1980

Promotiecommissie:

Promotor:	Prof. dr. P. Stevenhagen
Copromotor:	Dr. B. de Smit
Overige leden:	Prof. dr. K.J. Batenburg
	Prof. dr. H.W. Lenstra, Jr.
	Dr. P. Moree
	Prof. dr. R. Tijdeman
	Prof. dr. J. Top

Radicals in Arithmetic

Copyright © Willem Jan Palenstijn, Leiden, 2014.

Printed by Ridderprint, Ridderkerk.

The research in this thesis has been financially supported by the Netherlands Organisation for Scientific Research (NWO), project 613.000.317, entitled Radicals in Arithmetic.

Contents

Preface **7**

1 Primitive roots in number fields **11**
1.1 Introduction 11
1.2 Entanglement 14
1.3 Computing the entanglement groups 19
1.4 Proof of main results 20
1.5 Explicit densities 23

2 Radical extensions of abelian groups **25**
2.1 Introduction 25
2.2 Maximal radical extensions 26
2.3 Galois radical extensions 28
2.4 Kummer theory of radical extensions 31
2.5 Abelian radical extensions and Schinzel's theorem 36
2.6 The entanglement group 39

3 The absolute entanglement group **45**
3.1 Introduction 45
3.2 Preliminaries 46
3.3 Main results 47
3.4 Positive characteristic 50

4 Computing radical field degrees **53**
4.1 Introduction 53
4.2 Coprime bases 54
4.3 Entanglement 55
4.4 Field degrees 59

5 Near-primitive roots and higher rank **63**
5.1 Introduction 63
5.2 Proof of main theorems 64
5.3 Explicit density computations 69

6 Artin for rank one tori **77**
6.1 Introduction 77
6.2 Preliminaries 79
6.3 Proof of main theorems 81
6.4 Explicit density computations 83

7 Enumerating ABC triples **93**
7.1 Introduction 93
7.2 Bounds 94
7.3 Enumeration algorithm 96
7.4 Implementation details 99
7.5 Data 101

Bibliography **109**

Samenvatting **113**

Curriculum vitae **117**

Preface

This manuscript consists of two parts. In the first part, comprising Chapters 1 to 6, we build a theory for *entangled radicals*, and apply this to generalizations of Artin's primitive root conjecture. In the second part, consisting of Chapter 7, we give an algorithm for enumerating so-called *ABC triples* and report results from the ABC@home project, a volunteer computing project that has enumerated all ABC triples up to 10^{18}.

Artin's primitive root conjecture, first stated in 1927 and adapted in the 1950s, concerns the density of prime numbers q for which a fixed integer $x \neq 0$ generates the cyclic group $\mathbf{F}_q^*$. Artin conjectured that this density exists and is equal to a constant A times a rational correction factor depending on x that can be given explicitly [2], with A defined as

$$A = \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right) \approx 0.3739558\ldots$$

In 1967 this conjecture was proved by Hooley [16] assuming the Generalized Riemann Hypothesis.

The algebraic number theory argument behind the conjecture, which we give in its entirety in Chapter 1, revolves around the degrees of splitting fields K_p of the polynomials $X^p - x$ and their composita. These degrees are reflected in the expression $p(p-1)$ in the constant above.

If we for the moment assume that x is not a perfect power, the mentioned correction factor is necessary to compensate for the fact that the fields K_p are not always linearly disjoint. For $x = 3$ the fields K_p *are* all linearly disjoint, and in this case the correction factor is 1. However, for $x = 5$, the splitting field of $X^2 - 5$ is contained in the splitting field of $X^5 - 5$ since we have $\mathbf{Q}(\sqrt{5}) \subset \mathbf{Q}(\zeta_5)$.

These unexpected additive relations determine the value of the correction factor. In 2003, H.W. Lenstra, P. Moree and P. Stevenhagen [31] gave an interpretation of this factor which served as the basis for the treatment in the present manuscript.

Roots of polynomials of the form $X^n - a$ are called *radicals*, and following H.W. Lenstra [19], we shall refer to these unexpected additive relations as *entanglement* between radicals.

In Chapter 1, Theorem 1.5, we give a **generalization of Artin's primitive root conjecture to number fields**. We give the density as a similar product of a

constant independent of x, times an explicit rational correction factor. Chapter 1 is self-contained, and, besides containing the generalization of Artin's conjecture, acts as a prelude to the more general theory of entangled radicals covered in Chapter 2.

Let K be a field, $\bar{K}$ an algebraic closure of K, and $B \supset K^*$ a multiplicative group of radicals in $\bar{K}^*$ over K, i.e., elements of $\bar{K}^*$ of which a power is in K^*. Let us also assume that $K(B)$ is a Galois extension of K. Then determining the entanglement is a key ingredient for the computation of the field degree $[K(B) : K]$ and the Galois group $\mathrm{Gal}(K(B)/K)$. The strictly multiplicative structure of B is much more straightforward. In particular, the index of K^* in B and the structure of the automorphism group $\mathrm{Aut}_{K^*}(B)$ of automorphisms of B that are the identity on K^* are much simpler to analyze. This is also apparent in the context of Artin's conjecture: if we define $B_p = \langle \mathbf{Q}^*, \zeta_p, \sqrt[p]{x} \rangle$ for primes p, and B as the group generated by all B_p, then the structure of $\mathrm{Aut}_{\mathbf{Q}^*}(B)$ is independent of x (again assuming for the moment that x is not a perfect power), and in fact we have natural isomorphisms

$$\mathrm{Aut}_{\mathbf{Q}^*}(B) \cong \prod_{p \text{ prime}} \mathrm{Aut}_{\mathbf{Q}^*}(B_p) \cong \prod_{p \text{ prime}} (\mathbf{Z}/p\mathbf{Z}) \rtimes (\mathbf{Z}/p\mathbf{Z})^*.$$

Chapter 2 takes one further step back, and covers the setting of any group (in applications usually a Galois group) acting on a group B of radicals. Groups of radicals over a field have the property that all finite subgroups (i.e., those consisting of roots of unity) are cyclic. This property is sufficient for the automorphism group of the torsion subgroup of B to be abelian, and it turns out to be an essential part of the theory. In fact, this property is not only sufficient, but also necessary for the torsion subgroup of B to have an abelian automorphism group. (See Dixon [12], exercise 3.12 for this result due to G.A. Miller.)

Let B therefore be an abelian group of which all finite subgroups are cyclic, and let G be a profinite group acting continuously on B, where we give B the discrete topology. We write B^G for the subgroup of B consisting of the invariants under the action of G, and assume that B/B^G is torsion. This extension $B^G \subset B$ is what we shall call a Galois radical group extension (Definition 2.7). The condition of B/B^G being torsion encodes that the elements of B are radicals over B^G.

One of the main results of this thesis (Theorem 2.25) is that in this generality, **the image of G in $\mathrm{Aut}(B)$ is a normal subgroup of $\mathrm{Aut}_{B^G}(B)$ and $E = \mathrm{Aut}_{B^G}(B)/\mathrm{im}(G)$ is abelian**. We call E the *entanglement group* of the action of G on B.

This result builds on analogues of Kummer theory, Schinzel's theorem, and other theorems traditionally used to describe radical field extensions, which we state and prove in Chapter 2.

A case of special interest is the entanglement group of the maximal radical extension of a field. We call this the **absolute entanglement group**, and compute it in Chapter 3 based on the theory of Chapter 2. The characteristic 0 case of these results has been announced in the lecture notes for a series of Colloquium Lectures by H.W. Lenstra [19] at the AMS Annual Meeting in 2006.

In Chapter 4 we explicitly compute entanglement groups over $\mathbf{Q}$, and apply that

to **compute field degrees of radical field extensions of Q**. We use the expressions for the entanglement group derived in Chapter 2 to construct a polynomial time algorithm to compute these degrees, up to an evaluation of Euler's totient function φ.

In Chapter 5 we then return to Artin's conjecture. Many variants of Artin's conjecture have been described and studied in the literature (see, e.g., [18, 20, 22, 24]). In many of these generalizations, the theory from Chapter 1 can no longer directly be used, since that only considered roots of square-free order. In Chapter 5 we apply the more general theory of Chapters 2 and 4 to a number of generalizations of Artin's conjecture over number fields.

Specifically, we look at so-called **near-primitive roots**, where we consider the density of primes $\mathfrak{q}$ of a number field K where a fixed $x \in K^*$ generates a subgroup of $(\mathcal{O}_K/\mathfrak{q})^*$ of index dividing a given integer t. For the case $K = \mathbf{Q}$, this has been treated by P. Moree [23] building on a result by Wagstaff [35]. Another extension we study is that of **higher rank analogues of Artin's conjecture**, where we take multiple non-zero elements $x_1, \ldots, x_k$ and consider the set of primes $\mathfrak{q}$ of K for which $\bar{x}_1, \ldots \bar{x}_k$ together generate $(\mathcal{O}_K/\mathfrak{q})^*$. Over the rationals, this is covered by P. Moree and P. Stevenhagen [24].

Due to the generality of the results of Chapter 2, we can also apply them outside of the setting of radicals in unit groups of (number) fields. The setting we turn to in Chapter 6 is that of tori. A torus is an algebraic group closely related to the multiplicative group $\mathbf{G}_{\mathrm{m}}$, which we considered in Chapters 1 and 5. To satisfy the requirement that finite subgroups are cyclic, we specifically restrict to **rank one tori over number fields**. A point on such a torus can be reduced at almost all primes, and as a consequence there is an analogue of Artin primitive root densities in this setting, studied for tori over $\mathbf{Q}$ by Chen [7]. We show that our theory of entangled radicals also applies to this setting, and use it to obtain a generalization of Artin's conjecture to rank one tori over number fields.

The final chapter of this manuscript covers an entirely different topic, and is independent of the first six chapters — except for the central role the word radical plays in both parts. Here, the *radical* of a positive integer is defined to be the product of its prime divisors, without multiplicity. An *ABC triple* is a triple (a, b, c) of coprime positive integers satisfying $a + b = c$ and $a \leq b$, and for which the radical of abc is smaller than c. For example, the smallest such triples are $1 + 8 = 9$ and $5 + 27 = 32$. In this chapter, we give bounds for the number of ABC triples, describe an **algorithm for enumerating all ABC triples** below a given bound, and report results from ABC@home, **a distributed volunteer computing project** that has enumerated all ABC triples with $c < 10^{18}$.

Chapter 1

Artin's primitive root conjecture for number fields

1.1 Introduction

The unit group of a finite field of n elements is a cyclic group, and it has $\varphi(n-1)$ choices of generator. For example, the finite field $\mathbf{F}_{11}$ of 11 elements has $\varphi(10) = 4$ elements that each generate its unit group. To see if an element x is a generator of $\mathbf{F}_{11}^*$, we could check that x isn't a square or a fifth power, 2 and 5 being the prime divisors of 10, the order of $\mathbf{F}_{11}^*$. We find that the residue classes of 2, 6, 7 and 8 are the four generators of $\mathbf{F}_{11}^*$. We call the integers in these residue classes primitive roots modulo 11. More generally, we call a rational number x a *primitive root* modulo a prime q if q does not divide the denominator of x and x mod q generates $\mathbf{F}_q^*$.

Instead of determining which integers generate the unit group of a given finite field $\mathbf{F}_q$, we can reverse the question and ask modulo which (or how many) primes q a fixed integer (or rational number) is a primitive root. For example, 2 is not only a primitive root modulo 11, but also modulo 3, 5, 13, 19, 29, 37 and numerous other primes.

Question 1.1. *If x is a non-zero rational number, for how many primes q not dividing the numerator and denominator of x is the unit group of $\mathbf{F}_q$ generated by x mod q?*

Only in the simple case when x is -1 or a square, where the answer is finite, can this question be easily answered. In 1927, Emil Artin conjectured that there should be an infinite number of primes q modulo which $x = 2$ is a primitive root, and even that the set of such q should have a natural density. In the 1950s he adapted his conjecture for general $x \in \mathbf{Q}^*$, and this *Artin's primitive root conjecture* was proved by Hooley in 1967 under the assumption of the Generalized Riemann Hypothesis.

In this chapter, we will find a similar answer to the following analogue of the previous Question 1.1 in arbitrary number fields.

Question 1.2. *If K is a number field with $x \in K^*$, for how many primes $\mathfrak{q}$ of the ring of integers $\mathcal{O}_K$ of K with $\operatorname{ord}_{\mathfrak{q}}(x) = 0$ is $(\mathcal{O}_K/\mathfrak{q})^*$ generated by $x \bmod \mathfrak{q}$?*

Let us first turn back to the heuristic argument Artin used to derive his conjectural answer to Question 1.1. Since x is a primitive root modulo q exactly when $\operatorname{ord}_q(x) = 0$ and the index $[\mathbf{F}_q^* : \langle \bar{x} \rangle]$ is 1, one may determine for each prime p the set of primes q for which p divides $[\mathbf{F}_q^* : \langle \bar{x} \rangle]$, and remove these infinitely many sets from the set of all primes to see which primes q are left.

If p is a prime that divides the index $[\mathbf{F}_q^* : \langle \bar{x} \rangle]$, then p divides the group order $\#\mathbf{F}_q^*$, and $x \bmod q$ is an element of the index p subgroup of p-th powers in $\mathbf{F}_q^*$. In this case, $x \bmod q$ is the p-th power of p distinct elements of $\mathbf{F}_q^*$, so the polynomial $X^p - x$ splits completely into distinct linear factors modulo q.

Conversely, if $X^p - x$ splits completely into distinct linear factors modulo q, then x is a p-th power in $\mathbf{F}_q^*$ and has distinct p-th roots. So, $\mathbf{F}_q$ contains a primitive p-th root of unity, and p divides $[\mathbf{F}_q^* : \langle \bar{x} \rangle]$.

We conclude that for prime numbers p and q, we have

$$p \mid [\mathbf{F}_q^* : \langle \bar{x} \rangle] \iff X^p - x \text{ splits completely into distinct linear factors modulo } q.$$

In other words, the set of primes q modulo which x is a primitive root consists of those q (coprime to the numerator and denominator of x) that do not split completely in any of the splitting fields K_p of $X^p - x$, with $p \neq q$ prime.

The Frobenius density theorem (or alternatively the stronger Chebotarëv density theorem; see [32]) tells us that the set of primes q that split completely in K_p has a natural density of $\frac{1}{[K_p:\mathbf{Q}]}$. If x is not a p-th power, this is equal to $\frac{1}{p(p-1)}$.

Artin's heuristic argument now continues: at each prime p, the condition that p does not divide the index $[\mathbf{F}_q^* : \langle \bar{x} \rangle]$ excludes a fraction of $\frac{1}{[K_p:\mathbf{Q}]}$ of all primes q. Since for $x = 2$ the fields K_p are linearly disjoint over $\mathbf{Q}$ (embedding all K_p in a common algebraic closure $\bar{\mathbf{Q}}$), these conditions are independent, and it is reasonable to assume the set of primes modulo which 2 is a primitive root should have density

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right) \approx 0.3739558\ldots, \tag{1.3}$$

a value that is now known as Artin's constant.

When computers became sufficiently powerful in the 1950s to verify this density empirically, Derrick and Emma Lehmer computed for a few small integers x the number of primes $q < 20\,000$ modulo which x is a primitive root. For $x = 2$, the data matched Artin's conjectured density well. For $x = -3$ and $x = 5$ however, the observed densities were notably higher.

When Artin saw this, he realized that for general x, the conditions at the various primes p are not always independent. To see why, consider $x = 5$ and look at the splitting fields K_p of $X^p - 5$ over $\mathbf{Q}$ for primes p. We have $K_2 = \mathbf{Q}(\sqrt{5})$ and

$K_5 = \mathbf{Q}(\zeta_5, \sqrt[5]{5})$ where ζ_5 is a primitive fifth root of unity. In this case we see that K_2 is *contained* in K_5 because we have $\pm\sqrt{5} = \zeta_5 + \zeta_5^{-1} - \zeta_5^2 - \zeta_5^{-2}$ (The sign depends on the choice of ζ_5.) and therefore $\mathbf{Q}(\sqrt{5})$ is a subfield of $\mathbf{Q}(\zeta_5)$. Somewhat informally, we say that $\sqrt{5}$ and ζ_5 are *entangled radicals*.

If q is a prime that splits completely in K_5, then it also splits completely in the subfield K_2. In other words, the primes q that the condition at $p = 5$ means to exclude, have already all been excluded by the condition at $p = 2$. So, the factor $1 - \frac{1}{5(5-1)}$ in the infinite product must be omitted, and the density of primes modulo which 5 is a primitive root should be $\frac{20}{19}$ times Artin's constant.

It can be shown that in the case of Question 1.1, where the ground field is $\mathbf{Q}$, the only dependency between the splitting fields occurs when the discriminant d of K_2 is odd, in which case $K_2 = \mathbf{Q}(\sqrt{x})$ is contained in $\mathbf{Q}(\zeta_d)$ and thus also in K_d, the compositum of all K_p with $p \mid d$. Lang and Tate gave the necessary correction factor that results from this in 1965 in their preface to Artin's collected works [2]. To prove this corrected conjecture, one needs to show that imposing countably many splitting conditions does indeed give rise to a product density as in (1.3). If one uses the Generalized Riemann Hypothesis to bound the error terms in Frobenius' density theorem, this can be done in the way given by Hooley [16]. To date, there is no unconditional proof.

We now turn to Question 1.2 over a general number field K.

Just as for $K = \mathbf{Q}$, we need to describe the set of primes $\mathfrak{q}$ that do not split completely in any of the splitting fields K_p of $X^p - x$ over K. Imposing the splitting condition in *finitely many* K_p amounts to prescribing the splitting behaviour in the compositum K_n of these K_p (inside a fixed algebraic closure $\bar{K}$), where n is the product of the primes p considered.

More precisely, a prime $\mathfrak{q}$ does not split completely in any of the extensions $K \subset K_p$ with $p \mid n$ if and only if the Frobenius class $\mathrm{Frob}_\mathfrak{q}$ in $G_n = \mathrm{Gal}(K_n/K)$ is non-trivial when restricted to any of the subfields $K_p \subset K_n$. So, by the Chebotarëv density theorem the set of primes $\mathfrak{q}$ that do not split completely in any extension $K \subset K_p$ with $p \mid n$ has a density equal to the ratio $\#S_n/\#G_n$ with

$$S_n = \{\sigma \in G_n : \sigma\,|_{K_p} \neq \mathrm{id} \text{ for all } p \mid n\}.$$

Letting n in the ratio $\#S_n/\#G_n$ tend to the product of all primes then gives a conjectured density of primes $\mathfrak{q}$ modulo which x is a primitive root. Generalizing Hooley's work, Cooke and Weinberger showed in [9] that this conjectured density is the correct density when the Riemann Hypothesis holds for all fields K_n.

In the number field case, there are two complications: the group $\mathrm{Gal}(K_p/K)$ can be significantly harder to compute than for $K = \mathbf{Q}$. Moreover, as we have already seen over $\mathbf{Q}$, the Galois group $G_n = \mathrm{Gal}(K_n/K)$ can be a strict subgroup of the product $\prod_{p|n} \mathrm{Gal}(K_p/K)$, complicating the computation of this density. In the general case, $\mathrm{Gal}(K_n/K)$ can differ from the product of $\mathrm{Gal}(K_p/K)$ in many more ways than over $\mathbf{Q}$.

The fields K_n are "radical extensions" of K generated by all n-th roots of x. For such extensions, the Galois group G_n is a subgroup of the automorphism group of

the *multiplicative group* generated by these roots.

To make this precise, adjoin all n-th roots of x (in $\bar{K}$) to the multiplicative group K^*, resulting in the abelian group $B_n = \langle K^*, \zeta_n, \sqrt[n]{x} \rangle \subset \bar{K}^*$. The group extension $K^* \subset B_n$ is a much simpler structure than the field extension $K \subset K_n$. For example, adjoining a fifth root of unity to the abelian group $\mathbf{Q}^*$ does not also give a square root of 5.

We consider $G_n = \mathrm{Gal}(K_n/K)$ as a subgroup of the group $A_n = \mathrm{Aut}_{K^*}(B_n)$ of group automorphisms of B_n that are the identity on K^*. This larger automorphism group is much easier to compute than G_n itself. For one thing, unlike the Galois group, the group A_n does always factor as $\prod_{p|n} A_p$ (see Lemma 1.12).

Even though we ignored the additive structure of the fields involved, the difference between the Galois groups G_n and the groups A_n is actually quite modest, as reflected by the following theorem, proved in Section 1.4.

Theorem 1.4. *For all n, the Galois group G_n is a normal subgroup of A_n with finite, abelian quotient. There is a group $E = E_{K,x}$ such that for all n divisible by all of a finite set of critical primes, the quotient A_n/G_n equals E.*

This limit group E covers two things. For an individual prime p, the group G_p may be smaller than A_p, although Theorem 1.4 implies this only occurs for a finite number of primes. Additionally, E encodes the interdependencies between the local conditions at all primes p. The entanglement group E admits an explicit description that we derive in Section 1.3, and the set of critical primes in the theorem is given in Section 1.4. For example, when $K = \mathbf{Q}$, this set is empty unless the discriminant d of K_2 is odd, in which case it consists of the primes dividing $2d$.

The correction factor we need for the density statement has a transparent description in terms of the finitely many characters $\chi : E \to \mathbf{C}^*$ that "cut out" the Galois group G_n of K_n/K from the automorphism group A_n.

Theorem 1.5. *If the Generalized Riemann Hypothesis holds, the density of primes $\mathfrak{q}$ of K for which $(\mathcal{O}_K/\mathfrak{q})^*$ is generated by $x \bmod \mathfrak{q}$ exists and it is equal to*

$$C_{K,x} \cdot \prod_{p \text{ prime}} (1 - \frac{1}{\#A_p}), \text{ with } C_{K,x} = \sum_{\chi \in E^\vee} \prod_{\substack{p \text{ prime} \\ \chi(A_p) \neq 1}} \frac{-1}{\#A_p - 1}.$$

The proof of this theorem occupies most of the rest of this chapter. Afterwards, in Section 1.5 we give an explicit method to compute the rational correction factor $C_{K,x}$ with Lemma 1.13, and conclude with several examples.

1.2 Entanglement

In this section we will take a step back from the number theoretic view point of the previous section, and study the Galois group of normal, separable field extensions generated by radicals.

Formally, if $K \subset M$ is any field extension, we call a subgroup $B \subset M^*$ a *radical group* over K if B contains K^* and the quotient group B/K^* is torsion. This last condition means that every element of B has a power that is contained in K^*, or in other words, B consists of radicals over K. The field extension $K(B)$ of K is then called a *radical extension*.

The extensions $K \subset K_n$ from the previous section are examples of radical extensions, with $B_n = \langle K^*, \zeta_n, \sqrt[n]{x} \rangle$ as their generating radical groups. Here ζ_n denotes a primitive n-th root of unity in a fixed algebraic closure $\bar{K}$. We write $\mu_n \subset \bar{K}^*$ for the group of all n-th roots of unity of $\bar{K}$.

We will only consider radical groups B satisfying

$$\forall x \in B : \exists n \in \mathbf{Z}_{>0} : \operatorname{char} K \nmid n, x^n \in K^* \text{ and } \mu_n \subset B,$$

and call such groups *Galois* radical groups. The field extension $K(B)/K$ generated by such a group of radicals is separable due to the condition $\operatorname{char} K \nmid n$, and normal since we require B to contain sufficiently many roots of unity, so $K(B)/K$ is a Galois field extension.

Since any field automorphism of $K(B)$ is defined by its action on B, we can consider $\operatorname{Gal}(K(B)/K)$ as a subgroup of the group $\operatorname{Aut}_{K^*}(B)$ of group automorphisms of B that are the identity on K^*, also known as K^*-*automorphisms*.

The K^*-automorphism group genuinely depends on the generating radical group, and not just on the radical field extension it generates. For example, the radical group $B = \langle \mathbf{Q}^*, \zeta_5 \rangle$ over $\mathbf{Q}$ has $\mathbf{Q}^*$-automorphism group equal to the Galois group $\operatorname{Gal}(\mathbf{Q}(\zeta_5)/\mathbf{Q}) \cong (\mathbf{Z}/5\mathbf{Z})^*$. However, $B' = \langle \mathbf{Q}^*, \zeta_5, \sqrt{5} \rangle$, which generates the same field as B, has a $\mathbf{Q}^*$-automorphism group isomorphic to $\operatorname{Aut}_{\mathbf{Q}^*}(B) \times \operatorname{Aut}_{\mathbf{Q}^*}(\langle \mathbf{Q}^*, \sqrt{5} \rangle) \cong (\mathbf{Z}/5\mathbf{Z})^* \times C_2$. In this case, the Galois group $\operatorname{Gal}(\mathbf{Q}(B')/\mathbf{Q})$ is a normal subgroup of index 2 in $\operatorname{Aut}_{\mathbf{Q}^*}(B')$.

In two important cases, the K^*-automorphism group is equal to the Galois group of the generated field extension.

The first case is that of cyclotomic extensions of $\mathbf{Q}$. If μ is a multiplicative group of roots of unity of $\bar{\mathbf{Q}}$, the radical group $B = \langle \mathbf{Q}^*, \mu \rangle$ has $\mathbf{Q}^*$-automorphism group naturally isomorphic to $\operatorname{Aut}(\mu)$, since any automorphism of μ induces a $\mathbf{Q}^*$-automorphism of B. Any automorphism of μ also induces a field automorphism of $\mathbf{Q}(\mu)$, so here we find that $\operatorname{Gal}(\mathbf{Q}(B)/\mathbf{Q})$ is equal to $\operatorname{Aut}_{\mathbf{Q}^*}(B)$.

The second important case is the case of Kummer extensions. We call $x \in \bar{K}^*$ a *Kummer radical* over K if x^w is an element of K^* for some w with $\mu_w \subset K$. Radical extensions generated by Kummer radicals are called *Kummer extensions*. For instance, all Kummer extensions of $\mathbf{Q}$ are of the form $\mathbf{Q}(\sqrt{W})$ where we adjoin all square roots of elements of some set $W \subset \mathbf{Q}^*$.

For a group $B \subset \bar{K}^*$ of Kummer radicals, any K^*-automorphism σ of B multiplies each radical in B with a root of unity of K, and this fully determines σ. Writing μ_K for the set of roots of unity of K, the following therefore defines an

injective homomorphism:

$$\begin{array}{rcl} \omega : \mathrm{Aut}_{K^*}(B) & \longrightarrow & \mathrm{Hom}(B/K^*, \mu_K) \\ \sigma & \longmapsto & \left(x \mapsto \dfrac{\sigma(x)}{x} \right). \end{array}$$

Kummer theory (see, e.g., [17], §VI.8) tells us the following composed map is an isomorphism:

$$\mathrm{Gal}(K(B)/K) \xrightarrow{\mathrm{res}} \mathrm{Aut}_{K^*}(B) \xrightarrow{\omega} \mathrm{Hom}(B/K^*, \mu_K).$$

We find that the natural restriction $\mathrm{Gal}(K(B)/K) \to \mathrm{Aut}_{K^*}(B)$ is an isomorphism.

The remainder of this section is devoted to proving the following main structure theorem.

Theorem 1.6. *If B is a Galois radical group over a field K, then the Galois group $\mathrm{Gal}(K(B)/K)$ is a normal subgroup of $\mathrm{Aut}_{K^*}(B)$ with an abelian quotient.*

We write $E(B)$ for this quotient group, and call it the *entanglement group* of B over K.

In both the cyclotomic case and the Kummer case, the automorphism group is abelian. Restricting to the maximal abelian subextension B_{ab} is the main ingredient of the proof of this theorem, and we can characterise B_{ab} for an arbitrary radical extension using the following theorem of Schinzel. We state this theorem and prove two lemmas before proceeding with the proof of Theorem 1.6.

Theorem 1.7. *Let F be a field, $a \in F$, and n a positive integer not divisible by $\mathrm{char}\, K$. Let w be the number of n-th roots of unity in F. Then, a splitting field of $X^n - a$ is abelian over F if and only if there exists $b \in F$ with $a^w = b^n$.*

Proof. See [28], or alternatively, Corollary 2.21 in the next chapter. □

Lemma 1.8. *If $C \subset D$ are two radical groups over K that are both Galois, any K^*-automorphism of C can be extended to an automorphism of D.*

Proof. Let $\varphi \in \mathrm{Aut}_{K^*}(C)$ be a K^*-automorphism of C. It follows from Zorn's lemma that the set of subgroups of D with an injective homomorphism to D that extends φ has a maximal element M with an injection $\psi : M \to D$.

To show that M is in fact equal to D, assume it is not, and take $x \in D \setminus M$. We will extend ψ to an injection $\langle M, x \rangle \to D$.

First of all, if x is a p-th root of unity, then $\langle M, x \rangle$ equals $M \oplus \mu_p$ and we can extend ψ with the identity on μ_p. This contradicts the fact that M is maximal, so M contains all torsion of D of prime order.

Otherwise, take the minimal $k \in \mathbf{Z}_{>1}$ such that $x^k \in M$ and the minimal $n \in \mathbf{Z}_{>1}$ such that $x^n \in K^*$. The injection ψ maps x^k to ζx^k for some $\zeta \in D$ with $\zeta^{n/k} = 1$. Since D is Galois, there exists $\xi \in D$ with $\xi^n = 1$ and $\xi^k = \zeta$. We can now define the injection $\psi' : \langle x \rangle \to D$ by $x \mapsto \xi x$. Since $\psi'(x^k)$ then equals $\psi(x^k)$, the injections ψ and ψ' are compatible on the intersection of M and $\langle x \rangle$.

The group $\langle M, x\rangle \subset D$ can be written as a fibered sum (or push-out):

$$\langle M, x\rangle \cong M \oplus_{\langle x^k\rangle} \langle x\rangle.$$

The pair of injections $\psi : M \to D$ and $\psi' : \langle x\rangle \to D$ together with the universal property of this push-out now defines a homomorphism $\chi : \langle M, x\rangle \to D$ that extends φ.

We claim that χ is injective. Since χ multiplies all elements by torsion elements, the kernel of χ is torsion. However, all elements ζ of D of prime order are contained in M, so we have $\chi(\zeta) = \psi(\zeta) \neq 1$. The kernel of χ is therefore trivial, so χ is an injective homomorphism $\langle M, x\rangle \to D$. This contradicts the maximality of M, so M is equal to D.

The injection $\psi : M \to D$ is now necessarily an automorphism, since for any $n > 0$ and $x \in D$ it permutes the finitely many n-th roots of x. □

Let B be a Galois radical extension over K. We will write B_{tors} for the subgroup of torsion elements of B.

Lemma 1.9. *Let x be an element of B and n the minimal positive integer such that $x^n \in K^*$. Then the following are equivalent:*

1. $\exists w \in \mathbf{Z}_{>0} : x^w \in B_{\text{tors}}K^*$ and $\mu_w \subset K^*$;
2. $\text{Aut}_{K^*}(\langle K^*, \zeta_n, x\rangle)$ *is abelian;*
3. $\text{Gal}(K(\zeta_n, x)/K)$ *is abelian.*

Proof.

(1) ⇒ (2). If $x^w \in B_{\text{tors}}K^*$ for a positive integer w with $\mu_w \subset K^*$, then $\langle K^*, \zeta_n, x\rangle$ is a subset of $B' = \mu_{\bar{K}}\sqrt[w]{K^*}$. Since any K^*-automorphism of B' sends roots of unity to roots of unity and w-th roots of elements of K^* to w-th roots of elements of K^*, there are restriction maps $\text{Aut}_{K^*}(B') \to \text{Aut}(\mu_{\bar{K}})$ and $\text{Aut}_{K^*}(B') \to \text{Aut}_{K^*}(\sqrt[w]{K^*})$. This implies there is an injective homomorphism from $\text{Aut}_{K^*}(B')$ to $\text{Aut}(\mu_{\bar{K}}) \times \text{Aut}_{K^*}(\sqrt[w]{K^*})$, which, as we saw, is abelian. Finally, by Lemma 1.8, the restriction map from $\text{Aut}_{K^*}(B')$ to $\text{Aut}_{K^*}(\langle K^*, \zeta_n, x\rangle)$ is surjective, and therefore the latter is also abelian.

(2) ⇒ (3). This is trivial since $\text{Gal}(K(\zeta_n, x)/K)$ can be considered a subgroup of $\text{Aut}_{K^*}(\langle K^*, \zeta_n, x\rangle)$.

(3) ⇒ (1). Since $K(\zeta_n, x)$ is a splitting field of $X^n - x^n$ over K, by Schinzel's Theorem 1.7 there is an element $b \in K$ with $x^{nw} = b^n$ if we take w to be the number of n-th roots of unity in K. Then we have $x^w \in \mu_n b$, proving the lemma. □

We are now ready to prove Theorem 1.6. The group of radicals

$$B_{\text{ab}} = \{x \in B : \exists w : x^w \in B_{\text{tors}}K^* \text{ and } \mu_w \subset K^*\},$$

consisting of the elements of B satisfying the conditions from Lemma 1.9, has an abelian group of K^*-automorphisms $\text{Aut}_{K^*}(B_{\text{ab}})$. Since B_{ab} contains all roots of unity in B, any K^*-automorphism of B maps B_{ab} into itself. So, there is a well-defined restriction map $\text{Aut}_{K^*}(B) \to \text{Aut}_{K^*}(B_{\text{ab}})$ with kernel $\text{Aut}_{B_{\text{ab}}}(B)$, which is surjective by Lemma 1.8.

Thus, we get the following exact sequence.

$$0 \to \mathrm{Aut}_{B_{\mathrm{ab}}}(B) \to \mathrm{Aut}_{K^*}(B) \xrightarrow{\mathrm{res}} \mathrm{Aut}_{K^*}(B_{\mathrm{ab}}) \to 0.$$

This sequence is the K^*-automorphism equivalent of the exact sequence of Galois groups of the tower of extensions $K \subset K(B_{\mathrm{ab}}) \subset K(B)$. Combining the two gives the following diagram, where the rows are exact and the vertical arrows are injective. Since the only maps involved are natural injections and restrictions, the squares are both commutative.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Gal}(K(B)/K(B_{\mathrm{ab}})) & \longrightarrow & \mathrm{Gal}(K(B)/K) & \xrightarrow{\pi} & \mathrm{Gal}(K(B_{\mathrm{ab}})/K) & \longrightarrow & 0 \\
 & & \downarrow f & & \downarrow g & & \downarrow h & & \\
0 & \longrightarrow & \mathrm{Aut}_{B_{\mathrm{ab}}}(B) & \longrightarrow & \mathrm{Aut}_{K^*}(B) & \xrightarrow{\pi'} & \mathrm{Aut}_{K^*}(B_{\mathrm{ab}}) & \longrightarrow & 0
\end{array}$$

We can now finish the proof of Theorem 1.6. On the left side of the diagram, the radical extension $K(B)/K(B_{\mathrm{ab}})$ is a Kummer extension since B_{ab} contains all roots of unity of B. Therefore, the image of the Galois group $\mathrm{Gal}(K(B)/K(B_{\mathrm{ab}}))$ under f is the image of the restriction map

$$\mathrm{Aut}_{K(B_{\mathrm{ab}})^*}(K(B_{\mathrm{ab}})^*B) \to \mathrm{Aut}_{B \cap K(B_{\mathrm{ab}})^*}(B).$$

We claim that this restriction is a surjection. To see this, choose any automorphism $\sigma \in \mathrm{Aut}_{B \cap K(B_{\mathrm{ab}})^*}(B)$. We have that $K(B_{\mathrm{ab}})^*B$ is the following fibered sum:

$$K(B_{\mathrm{ab}})^*B = K(B_{\mathrm{ab}})^* \oplus_{(B \cap K(B_{\mathrm{ab}})^*)} B.$$

The automorphism σ induces an injective homomorphism $\varphi_\sigma : B \to K(B_{\mathrm{ab}})^*B$. By the universal property of the fibered sum, the injection φ_σ together with the inclusion $K(B_{\mathrm{ab}})^* \subset K(B_{\mathrm{ab}})^*B$ induces an automorphism of $K(B_{\mathrm{ab}})^*B$ that is the identity on $K(B_{\mathrm{ab}})^*$ and that extends σ. This proves the claim.

Because $K(B_{\mathrm{ab}})$ is abelian over K, the intersection $B \cap K(B_{\mathrm{ab}})^*$ is contained in B_{ab} by Lemma 1.9. Of course, B_{ab} is also contained in $B \cap K(B_{\mathrm{ab}})^*$, so we have $B_{\mathrm{ab}} = B \cap K(B_{\mathrm{ab}})^*$ and we conclude that f is an isomorphism.

On the right side of the diagram, $\mathrm{Aut}_{K^*}(B_{\mathrm{ab}})$ is abelian, so π' maps the commutator subgroup H of $\mathrm{Aut}_{K^*}(B)$ to 1, so H is contained in $\mathrm{Aut}_{B_{\mathrm{ab}}}(B)$. Since f is a surjection, this implies H is in fact contained in the image of $\mathrm{Gal}(K(B)/K)$. From this we can directly conclude that the image of $\mathrm{Gal}(K(B)/K)$ is a normal subgroup of $\mathrm{Aut}_{K^*}(B)$ with an abelian cokernel, which concludes the proof of Theorem 1.6.

1.3 Computing the entanglement groups

Let B again be a Galois radical group over a field K. In the previous section, we have seen that the entanglement group of B over K is equal to the entanglement group $E(B_{\mathrm{ab}})$ of the subgroup B_{ab} of B. As mentioned in the proof of Lemma 1.9, this group B_{ab} is a subgroup of the group generated by all Kummer radicals and all roots of unity in $\bar{K}$. If B_{ab} is *itself* generated by Kummer radicals and roots of unity and if the characteristic of K is 0, there is an explicit way to describe $E(B_{\mathrm{ab}})$ as a Galois group, which we give in this section.

All the Galois radical groups that play a role for the results of this chapter are of this form, but this is not the case in general. As an example, let α be a fourth root of -4 in $\bar{\mathbf{Q}}$ and consider the radical extension $\langle \mathbf{Q}^*, \alpha \rangle$ over $\mathbf{Q}$. This is a Galois radical extension since $\frac{1}{2}\alpha^2$ is a primitive 4th root of unity. Its automorphism group is of order 4 and abelian, but $\langle \mathbf{Q}^*, \alpha \rangle$ is not generated over $\mathbf{Q}^*$ by a Kummer radical or a root of unity. We will see in Chapter 5 how to handle this case.

For radical groups over fields of non-zero characteristic we refer to the more general treatment in Chapter 2 and Chapter 3, and in particular Section 3.4.

Now suppose that K is of characteristic 0 and that $B_{\mathrm{ab}} = \mu W$ is a group generated by a group of roots of unity μ and a group of Kummer radicals $W \supset K^*$. Since the Galois group $\mathrm{Gal}(K(\mu W)/K)$ is the kernel of the homomorphism $\mathrm{Aut}(\mu W) \to E(\mu W)$, the image of a group automorphism σ in $E(\mu W)$ determines whether or not σ is the restriction of a field automorphism.

In the examples in the previous section, we saw that any K^*-automorphism of W can be uniquely extended to a field automorphism of $K(W)$, and any automorphism of μ can be uniquely extended to a field automorphism of $\mathbf{Q}(\mu)$. To determine if a given element $\sigma \in \mathrm{Aut}(\mu W)$ is the restriction of an element of $\mathrm{Gal}(K(\mu W)/K)$, it therefore makes sense to compare the obtained field automorphisms of $K(W)$ and $\mathbf{Q}(\mu)$, and see if they are compatible.

To this end, we define the homomorphisms φ_1 and φ_2 as follows.

$$\begin{array}{rcl} \varphi_1 : \mathrm{Aut}_{K^*}(\mu W) & \xrightarrow{\text{res}} & \mathrm{Aut}_{K^*}(W) \xrightarrow{\sim} \mathrm{Gal}(K(W)/K) \\ \varphi_2 : \mathrm{Aut}_{K^*}(\mu W) & \xrightarrow{\text{res}} & \mathrm{Aut}_{\mu \cap K^*}(\mu) \xrightarrow{\sim} \mathrm{Gal}(\mathbf{Q}(\mu)/\mathbf{Q}(\mu \cap K^*)) \end{array}$$

Finally, we write $K_0 = K(W) \cap \mathbf{Q}(\mu)$. This is an abelian Galois field extension of $\mathbf{Q}$ since $\mathbf{Q}(\mu)/\mathbf{Q}$ is abelian. We then define φ as the difference of φ_1 and φ_2:

$$\begin{array}{rcl} \varphi : \mathrm{Aut}_{K^*}(\mu W) & \longrightarrow & \mathrm{Gal}(K_0/\mathbf{Q}) \\ \sigma & \longmapsto & \varphi_1(\sigma)|_{K_0} \cdot \varphi_2(\sigma)|_{K_0}^{-1}. \end{array}$$

Because $\mathbf{Q}(\mu)$ is abelian over $\mathbf{Q}$, the subextension $K_0/\mathbf{Q}$ is also abelian, so φ is a group homomorphism. Furthermore, for $\sigma \in \mathrm{Aut}_{K^*}(\mu W)$, both $\varphi_1(\sigma)|_{(\mu \cap W)}$ and $\varphi_2(\sigma)|_{(\mu \cap W)}$ are equal to $\sigma|_{(\mu \cap W)}$. Because φ is the difference of the two, $\varphi(\sigma)$ restricts to the identity on $\mu \cap W$. We see that the image of φ is in fact contained in $\mathrm{Gal}(K_0/\mathbf{Q}(W \cap \mu))$.

Theorem 1.10. *The homomorphism φ induces an isomorphism*

$$\psi : E(\mu W) \xrightarrow{\sim} \mathrm{Gal}(K_0/\mathbf{Q}(W \cap \mu)).$$

Proof. For ψ to be well-defined and injective, we show that the kernel of φ equals $\mathrm{Gal}(K(\mu W)/K)$.

We can write $\mathrm{Aut}_{K^*}(\mu W)$ as a fibered product:

$$\mathrm{Aut}_{K^*}(\mu W) \cong \mathrm{Aut}_{\mu \cap K^*}(\mu) \times_{\mathrm{Aut}_{\mu \cap K^*}(\mu \cap W)} \mathrm{Aut}_{K^*}(W).$$

The two factors are naturally isomorphic to $\mathrm{Gal}(\mathbf{Q}(\mu)/\mathbf{Q}(\mu \cap K^*))$ respectively $\mathrm{Gal}(K(W)/K)$. Using this structure, an element of $\mathrm{Aut}_{K^*}(\mu W)$ can be uniquely represented by a pair (σ, τ) with $\sigma \in \mathrm{Gal}(\mathbf{Q}(\mu)/\mathbf{Q}(\mu \cap K^*))$ and $\tau \in \mathrm{Gal}(K(W)/K)$. By construction of φ, the pair (σ, τ) is in the kernel of φ if and only if $\sigma|_{K_0}$ equals $\tau|_{K_0}$.

We now observe that $\mathrm{Gal}(K(\mu W)/K)$ admits the following fibered product structure:

$$\mathrm{Gal}(K(\mu W)/K) \cong \mathrm{Gal}(K(W)/K) \times_{\mathrm{Gal}(K(W) \cap K(\mu)/K)} \mathrm{Gal}(K(\mu)/K)$$

Composing this with the restriction $\mathrm{Gal}(K(\mu)/K) \xrightarrow{\sim} \mathrm{Gal}(\mathbf{Q}(\mu)/K \cap \mathbf{Q}(\mu))$ results in an isomorphism

$$\mathrm{Gal}(K(\mu W)/K) \xrightarrow{\sim} \mathrm{Gal}(K(W)/K) \times_{\mathrm{Gal}(K_0/\mathbf{Q}(\mu) \cap K)} \mathrm{Gal}(\mathbf{Q}(\mu)/\mathbf{Q}(\mu) \cap K)$$

Therefore, we see that the pair (σ, τ) extends to an automorphism of the field $\mathrm{Gal}(K(\mu W)/K)$ if and only if $\sigma|_{K_0}$ equals $\tau|_{K_0}$. This implies that the Galois group $\mathrm{Gal}(K(\mu W)/K)$ is precisely the kernel of φ and therefore that ψ is well-defined and injective.

For the surjectivity of ψ, we show that $\psi(\mathrm{Aut}_W(\mu W))$ already gives the full image $\mathrm{Gal}(K_0/\mathbf{Q}(W \cap \mu))$. Note that $\varphi_1(\mathrm{Aut}_W(\mu W))$ is trivial, so we only need to follow $\mathrm{Aut}_W(\mu W)$ through the composite map φ_2. The restriction map $\mathrm{Aut}_W(\mu W) \to \mathrm{Aut}_{(W \cap \mu)}(\mu)$ is surjective because μW is the fibered sum of μ and W over $\mu \cap W$, using the same argument as in the proof of Theorem 1.6. Its image in $\mathrm{Gal}(\mathbf{Q}(\mu)/\mathbf{Q})$ then equals $\mathrm{Gal}(\mathbf{Q}(\mu)/\mathbf{Q}(W \cap \mu))$. So, $\varphi_2(\mathrm{Aut}_W(\mu W))$ is equal to the Galois group $\mathrm{Gal}(\mathbf{Q}(\mu)/\mathbf{Q}(\mu \cap W))$.

Finally, we see that ψ is surjective since the restriction $\varphi_2(\mathrm{Aut}_W(\mu W))|_{K_0}$ equals $\mathrm{Gal}(K_0/\mathbf{Q}(W \cap \mu))$. □

1.4 Proof of main results

In this section we tie together the results from the previous two sections to prove Theorem 1.4 and the main theorem of this chapter, Theorem 1.5.

Let K be a number field, and $x \in K$ non-zero. As described in the introduction, a main ingredient of our computation of the density of primes $\mathfrak{q}$ of K for which $(\mathcal{O}_K/\mathfrak{q})^*$ is generated by x mod $\mathfrak{q}$, is determining for squarefree positive integers n the entanglement groups of the Galois radical groups $B_n = \langle K^*, \zeta_n, \sqrt[n]{x} \rangle$ over K.

We will prove Theorem 1.4 by directly proving the following more explicit variant.

Theorem 1.11. *Let w be the product of all primes p with $\zeta_p \in K$, and W the group of radicals $\langle K^*, \sqrt[w]{x}\rangle$. Let K_0 be the maximal subfield of $K(W)$ that is abelian over $\mathbf{Q}$, tamely ramified, and unramified at all primes $p \mid w$. Let n be a positive squarefree integer divisible by w and by all primes ramified in K_0, and write $r = n/w$. Then with $\mu = \mu_r$, the map defined in Theorem 1.10 induces an isomorphism from $E(B_n)$ to the finite abelian group $E = \mathrm{Gal}(K_0/\mathbf{Q})$.*

Proof. First, we show that we can apply Theorem 1.10 to compute the entanglement group $E(B_n) = E(B_{n,\mathrm{ab}})$. We will show that $B_{n,\mathrm{ab}}$ equals $\mu_r W$.

Since n is squarefree, $B_{\mathrm{tors}}K^*$ equals $\mu_r K^*$. If y is an element of $B_{n,\mathrm{ab}}$, then we have $y^w \in B_{\mathrm{tors}}K^* = \mu_r K^*$. Since w and r are coprime, this makes y the product of an element of μ_r and a w-th root of an element of K^*.

Theorem 1.10 then gives us an explicit isomorphism from $E(\mu_r W)$ to the Galois group $\mathrm{Gal}(K(W)\cap\mathbf{Q}(\mu_r)/\mathbf{Q}(\mu_r \cap W))$. Note that since r and w are coprime, $W \cap \mu_r$ is trivial, so we find an isomorphism

$$E(B_n) \xrightarrow{\sim} \mathrm{Gal}(K(W) \cap \mathbf{Q}(\mu_r)/\mathbf{Q}).$$

Since for a prime p, the field $\mathbf{Q}(\mu_p)$ is only (tamely) ramified at p, the field K_0 defined in this theorem is equal to $K(W) \cap \mathbf{Q}(\hat{\mu})$ where $\hat{\mu}$ is the group generated by primitive p-th roots of unity for all $p \nmid w$. We see that because n is divisible by w and by all primes ramified in $K_0/\mathbf{Q}$, we have $K(W) \cap \mathbf{Q}(\hat{\mu}) = K(W) \cap \mathbf{Q}(\mu_r)$, so $E(B_n)$ is isomorphic to $\mathrm{Gal}(K_0/\mathbf{Q})$.

Since $K(W)$ has finite degree over $\mathbf{Q}$, so does the subfield K_0, and we conclude that the limit entanglement group $E = \mathrm{Gal}(K_0/\mathbf{Q})$ is finite. □

Theorem 1.4 is now a direct corollary of Theorem 1.6 and Theorem 1.11. To derive the explicit formula for the density, we need one last ingredient.

Lemma 1.12. *For every squarefree positive integer n, there is a natural isomorphism*

$$\mathrm{Aut}_{K^*}(B_n) \cong \prod_{p \mid n \text{ prime}} \mathrm{Aut}_{K^*}(B_p).$$

Proof. Let n be a squarefree positive integer. Since B_p is a Galois radical group, there is a natural restriction map from $A_n = \mathrm{Aut}_{K^*}(B_n)$ to $A_p = \mathrm{Aut}_{K^*}(B_p)$ for every prime $p \mid n$. Since B_n is generated by all B_p with $p \mid n$, the combined map $\varphi : A_n \to \prod A_p$ is an injection.

The restriction maps $A_n \to A_p$ are surjective by Lemma 1.8. To see that the map to $\prod A_p$ is also surjective, let $(\sigma_p)_p$ be an element of $\prod A_p$. We construct $\sigma \in A_n$ with $\varphi(\sigma) = (\sigma_p)_p$ as follows: define $\sigma : B_n \to B_n$ by $\prod b_p \mapsto \prod \sigma_p(b_p)$ (with $b_p \in B_p$). Since every element of B_n can be uniquely written as $\prod b_p$ (up to multiplication with elements of K^*), the map σ is a well-defined homomorphism. It is invertible because its inverse is given by applying the same procedure to $(\sigma_p^{-1})_p$. We see that σ is contained in A_n and $\varphi(\sigma)$ is indeed $(\sigma_p)_p$. □

This factorization of A_n into a product of A_p for $p \mid n$ now allows us to prove the main density theorem.

Proof of Theorem 1.5. Recall that the density (under GRH, as described in the introduction) is given by the limit of $\#S_n/\#G_n$ when we let n tend to all primes. Let n therefore be a squarefree positive integer that is large enough for $E(B_n)$ to equal the (finite) entanglement group $E = \mathrm{Gal}(K_0/\mathbf{Q})$, as defined by Theorem 1.11.

Also recall the definition of S_n:

$$S_n = \{\sigma \in G_n : \text{ for all } p \mid n : \sigma\,|_{K_p} \neq \mathrm{id}\}.$$

As an analogue of S_n inside the K^*-automorphism group A_n, define

$$T_n = \{\sigma \in A_n : \text{ for all } p \mid n : \sigma\,|_{B_p} \neq \mathrm{id}\}.$$

We then have $S_n = T_n \cap G_n$ inside A_n. Also, under the natural isomorphism of A_n with $\prod A_p$, the subset T_n is mapped to $\prod A_p \setminus \{1\}$. Now we rewrite $\#S_n/\#G_n$ as follows, using the characteristic function 1_{G_n} of G_n inside A_n.

$$\delta_n = \frac{\#S_n}{\#G_n} = \frac{\#(T_n \cap G_n)}{\#G_n} = \frac{\sum_{s \in T_n} 1_{G_n}(s)}{\#G_n}$$

Exploiting the fact that E is abelian, we can rewrite 1_{G_n}.

$$\delta_n = \frac{1}{\#G_n \#E} \sum_{s \in T_n} \sum_{\chi \in E^\vee} \chi(s)$$

Under the natural isomorphism of A_n with $\prod A_p$, the subset T_n is mapped to the product $\prod A_p \setminus \{1\} = \prod T_p$.

$$\begin{aligned}\delta_n &= \frac{1}{\#A_n} \sum_{\chi \in E^\vee} \prod_{p \mid n} \sum_{s_p \in T_p} \chi(s_p) = \frac{1}{\#A_n} \sum_{\chi \in E^\vee} \prod_{p \mid n} \left(-1 + \sum_{s_p \in A_p} \chi(s_p) \right) \\ &= \frac{\#T_n}{\#A_n} \sum_{\chi \in E^\vee} \prod_{p \mid n} \frac{1}{\#T_p} \left(-1 + \sum_{s_p \in A_p} \chi(s_p) \right)\end{aligned}$$

Because $\sum_{s_p \in A_p} \chi(s_p)$ equals $\#A_p$ if $\chi(A_p)$ is trivial, and 0 otherwise, we get:

$$\begin{aligned}\delta_n &= \frac{\#T_n}{\#A_n} \sum_{\chi \in E^\vee} \prod_{\substack{p \text{ prime} \\ \chi(A_p) \neq 1}} \frac{-1}{\#A_p - 1} \\ &= \prod_{p \mid n} \left(1 - \frac{1}{\#A_p}\right) \sum_{\chi \in E^\vee} \prod_{\substack{p \text{ prime} \\ \chi(A_p) \neq 1}} \frac{-1}{\#A_p - 1} \\ &= C_{K,x} \prod_{p \mid n} \left(1 - \frac{1}{\#A_p}\right)\end{aligned}$$

Taking the limit of n to infinity now gives the desired formula. □

1.5 Explicit densities

Computing the correction factor $C_{K,x}$ explicitly requires determining for each character $\chi \in E^\vee$ for which primes p the image $\chi(A_p)$ is non-trivial. We call a character χ *bad* at p in this case. We start this section with an explicit criterion for determining at which primes characters are bad.

Lemma 1.13. *A character $\chi \in E^\vee$ is bad at a prime p if and only if one of the following two conditions holds:*

1. *χ is ramified at p, or*
2. *$\zeta_p \in K$ and $x \notin K^{*p}$ and the restriction to K_0 of the K-automorphism of $K(\sqrt[w]{x})$ given by $\sqrt[w]{x} \mapsto \zeta_p \sqrt[w]{x}$ is not in the kernel of χ.*

Proof. Let n be large enough for $E(B_n)$ to be isomorphic to E. Recall that the isomorphism $\varphi : A_n/G_n \xrightarrow{\sim} \mathrm{Gal}(K_0/\mathbf{Q})$ is given by $\varphi(\sigma) = \varphi_1(\sigma)\varphi_2(\sigma)^{-1}$ as defined in Section 1.3.

First, let p be a prime. We claim that at least one of $\varphi_1(A_p)$ and $\varphi_2(A_p)$ is trivial. If this is not the case, then both $\mathrm{Aut}_{K^*}(B_p \cap W)$ and $\mathrm{Aut}_{\mu \cap K^*}(B_p \cap \mu_n)$ are non-trivial. This first condition implies that B_p/K^* has a non-trivial element of order dividing w, and the second that B_p/K^* has an element of order not dividing w. This contradicts the fact that B_p/K^* has prime exponent p.

Now let χ be an element of $E^\vee$.

Assume that $\varphi_1(A_p)$ is non-trivial. Then $\varphi_2(A_p)$ is trivial, and χ is bad precisely if $\varphi_1(A_p)\,|_{K_0} = \mathrm{Gal}(K(W) \cap \mathbf{Q}(\mu_p)/\mathbf{Q})$ is not contained in the kernel of χ. This in turn is equivalent to the first condition from this lemma.

Alternatively, assume that $\varphi_2(A_p)$ is non-trivial. In that case, p divides w and $\varphi_1(A_p)$ is trivial. Since K contains ζ_p, the image $\varphi_2(A_p)\,|_{K_0}$ is trivial if x is a p-th power in K. Otherwise, it is generated by the automorphism $\sqrt[w]{x} \mapsto \zeta_p \sqrt[w]{x}$. We see that in this case, χ is bad precisely if the second condition from the lemma holds. □

We start by comparing our results with the known (under GRH) densities in the classical case over $\mathbf{Q}$.

Consider $x = 2$. Since $\mathbf{Q}$ only contains 2 roots of unity, we have $w = 2$. Using Theorem 1.11, we see that the limit entanglement group E is $\mathrm{Gal}(K_0/\mathbf{Q})$ for K_0 the maximal subfield of $\mathbf{Q}(\sqrt{2})$ that is abelian over $\mathbf{Q}$, tamely ramified, and unramified at 2. Since $\mathbf{Q}(\sqrt{2})$ is ramified at 2, K_0 equals $\mathbf{Q}$, and E is trivial, so the correction factor $C_{\mathbf{Q},2}$ is 1. This results in a density of

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right) \approx 0.373955\ldots,$$

as expected.

Next, we consider $K = \mathbf{Q}$ and $x = 5$. In this case $K_0 = \mathbf{Q}(\sqrt{5})$ and $E = \mathrm{Gal}(K_0/\mathbf{Q})$ is a group of order two. The non-trivial character in $E^\vee$ is only ramified at 5, so it is bad at 5 and potentially at primes dividing $w = 2$. Since $K_0 = K(\sqrt{5})$,

the automorphism sending $\sqrt{5}$ to $-\sqrt{5}$ is clearly not in the kernel of χ, so χ is indeed bad at 2.

We find $a_2 = 2$ and $a_5 = 20$, so we have $C_{\mathbf{Q},5} = 1 + \frac{1}{19} = \frac{20}{19}$. This leads to a conjectured density of $\frac{20}{19}$ times Artin's constant, as was also observed by the Lehmers.

As an example where K is larger than the rationals, consider the case $K = \mathbf{Q}(\sqrt{-7})$ and $x = 21$. Since K doesn't contain any new roots of unity, w equals 2 as before. The field $K(\sqrt[w]{x}) = \mathbf{Q}(\sqrt{-3}, \sqrt{-7})$ is now abelian and only (tamely) ramified above 3 and 7, so $K_0 = \mathbf{Q}(\sqrt{-3}, \sqrt{-7})$. We now need to determine at which primes the four characters in $\mathrm{Gal}(K_0/\mathbf{Q})^\vee$ are bad. We write $\mathrm{Gal}(K_0/\mathbf{Q})^\vee = \{\mathrm{id}, \chi_{-3}, \chi_{-7}, \chi_{21}\}$ where χ_t is such that $\mathbf{Q}(\sqrt{t})$ is the invariant field of $\ker \chi_t$. This yields the following table, where the minus signs indicate at which primes the characters are bad.

	2	3	7
1	+	+	+
χ_{-3}	−	−	+
χ_{-7}	+	+	−
χ_{21}	−	−	−

Since $a_2 = 2$, $a_3 = 6$ and $a_7 = 42$, we find $C_{K,x} = 1 + \frac{1}{5} - \frac{1}{41} - \frac{1}{5 \cdot 41} = \frac{48}{41}$.

To verify this empirically, the following table lists approximations to the density computed with Sage [30]. For each N in the table, it lists the fraction of primes $\mathfrak{q}$ with norm smaller than N for which $\bar{x} = \overline{21}$ is a primitive root modulo $\mathfrak{q}$.

N	density
10^5	0.443679...
10^6	0.436286...
10^7	0.437864...
10^8	0.437940...
10^9	0.437870...
10^{10}	0.437818...
conjectured	0.437801...

The conjectured density matches the observed approximations well.

Chapter 2

Radical extensions of abelian groups

2.1 Introduction

In the previous chapter, we used radical extensions of abelian groups to gain insight into Galois groups. In this chapter we will build on this idea to set up a theory for automorphisms of such radical group extensions, free from the context of fields. We will derive analogues of a number of results familiar from Galois theory, including basic properties of restrictions and extensions of automorphisms, and also a translation of Kummer theory and Schinzel's theorem for the classification of abelian radical extensions.

As we hinted at in the preface, a key property that we require of our groups of radicals is that all finite subgroups are cyclic. This means that for any prime p, there are no two linearly independent p-torsion elements, and it implies that the automorphism group of the torsion subgroup is abelian.

Specifically, let B be an abelian group of which every finite subgroup is cyclic. We say that an abelian group $C \supset B$ is a *radical extension* of B if the quotient C/B is torsion and all finite subgroups of C are again cyclic. The cardinality of C/B is the *degree* of the extension, and if the degree of the extension is finite, we say that the extension itself is finite.

In Section 2.2 we will define the concept of a maximal radical extension of B, and give its universal properties.

In Chapter 1, we studied the action of the absolute Galois group of a field on a group of radicals. Taking the role of that Galois group in this chapter is an arbitrary profinite group with a continuous action on B, where we give B the discrete topology. Write B^G for the invariants of B under the action of G. In Section 2.3 we will look at extensions of the form $B^G \subset B$ where B/B^G is torsion, which we will call Galois radical extensions of abelian groups.

In Section 2.4 we will then give an analogue of Kummer extensions of fields,

and in Section 2.5 we will show that a Galois radical extension $B^G \subset B$ has a maximal abelian sub-extension B_{ab}. This group B_{ab} has the defining properties that $\mathrm{Aut}_{B^G}(B_{\mathrm{ab}})$ is abelian and that for every sub-extension C with $\mathrm{Aut}_{B^G}(C)$ abelian, we have that B_{ab} contains C. The main ingredient in the definition and construction of B_{ab} will be a generalization of Schinzel's Theorem 1.7.

The main theorem of this chapter is Theorem 2.25 in section 2.6, which is a generalization of Theorem 1.6 to the setting of this chapter. It states that if G is a subgroup of $\mathrm{Aut}(B)$ such that $B^G \subset B$ is a radical extension, then G is a normal subgroup of $\mathrm{Aut}_{B^G}(B)$, and $\mathrm{Aut}_{B^G}(B)/G$ is abelian. We call this quotient $\mathrm{Aut}_{B^G}(B)$ the *entanglement group* of B with the action of G.

We conclude the chapter with a number of results giving more explicit expressions for the entanglement group. These will form the basis for the results of Chapters 3 to 6.

2.2 Maximal radical extensions

In this section we will define the maximal radical extension of an abelian group B of which all finite subgroups are cyclic, and prove its universal property.

We start with a definition. If $B \subset C$ and $B \subset D$ are two radical extensions of B, then a homomorphism from C to D is a *B-homomorphism* if it is the identity on B. A B-homomorphism that is a bijection is a *B-isomorphism*.

Theorem 2.1. *Let B be an abelian group of which every finite subgroup is cyclic. Then there is a group $\bar{B}$ that has the following properties.*

1. *The group $\bar{B}$ is a radical extension of B.*
2. *For every radical extension C of B, there is an injective B-homomorphism $C \to \bar{B}$.*

Up to a not necessarily unique B-isomorphism, there is exactly one group $\bar{B}$ with these two properties. Furthermore, given this group $\bar{B}$, if $\bar{B} \subset F$ is a radical extension, then F equals $\bar{B}$.

Definition 2.2. Let B be an abelian group of which every finite subgroup is cyclic. We call the group $\bar{B}$ given by Theorem 2.1 the *maximal radical extension* of B.

Before proving this theorem by constructing $\bar{B}$, we first recall the concept of an *essential extension* (see e.g., [13], definition A3.10): an abelian group C is an essential extension of a group $B \subset C$ if every non-zero subgroup of C has a non-zero intersection with B.

Proposition 2.3. *Let B be an abelian group of which all finite subgroups are cyclic. If $B \subset C$ is an essential extension, it is a radical extension.*

Proof. Let $x \neq 0$ be an element of C. Then $\langle x \rangle$ has a non-trivial intersection with B, so a multiple of x is contained in B. Therefore, C/B is torsion. It remains to be

shown that all finite subgroups of C are cyclic, or equivalently, that for every prime p there is at most one subgroup $H \subset C$ of order p.

Suppose p is a prime and H_1 and H_2 are two subgroups of C of order p. Because $B \subset C$ is essential, $H_1 \cap B$ is non-trivial and therefore equal to H_1. The same holds for H_2, so $H_2 \cap B$ equals H_2. All finite subgroups of B are cyclic, so B has a unique subgroup of order p, equal to H_1 and H_2. □

Theorem 2.4. *Let B be an abelian group of which all finite subgroups are cyclic. Then there exists a divisible abelian group E that is an essential extension of B. This group E is unique up to a not necessarily unique B-isomorphism and it has two universal properties: for any essential extension C of B, there is an injective B-homomorphism from C into E, and for any divisible abelian group F containing B, there is an injective B-homomorphism from E into F.*

Proof. See [13], §A3.4, Corollary A3.9 and Proposition A3.10. □

Since a divisible abelian group is the same as an injective $\mathbf{Z}$-module, the group E given by this theorem is called the *injective hull* of B (following [13], section A3.4).

We will use the existence of maximal essential extensions to show the existence of a maximal radical extension $\bar{B}$ of an abelian group B of which all finite subgroups are cyclic. We start by considering torsion subgroups of prime order.

If for a prime q the subgroup $B[q]$ of q-torsion of B is trivial, the direct sum $B \oplus \mathbf{Z}/q\mathbf{Z}$ is a radical extension of B, but not an essential extension. We therefore first define

$$B' = B \oplus \bigoplus_{\substack{q \text{ prime} \\ B[q]=0}} \mathbf{Z}/q\mathbf{Z}.$$

Next, we define $\bar{B}$ to be the injective hull of B'. We can now prove that the group $\bar{B}$ thus constructed satisfies the properties of Theorem 2.1.

Proof of Theorem 2.1. (1). The extension $B \subset B'$ is a radical extension by construction, and $B' \subset \bar{B}$ is an essential extension by definition and therefore also radical by Proposition 2.3. A radical extension of a radical extension of B is again radical over B, so $\bar{B}$ is a radical extension of B.

(2). Define the group $C' \supset C$ as follows:

$$C' = C \oplus \bigoplus_{\substack{q \text{ prime} \\ C[q]=0}} \mathbf{Z}/q\mathbf{Z}.$$

We will construct an injective B-homomorphism $C' \to \bar{B}$, which implies the existence of an injective B-homomorphism $C \to \bar{B}$.

The group C' contains B', and we claim $B' \subset C'$ is an essential extension. Let x be any element of C' C, and pick $n \in \mathbf{Z}_{>0}$ minimal such that nx is in B. We have $x \notin B$, so $n > 1$. If nx is 0, take any prime $p \mid n$, and we then have $\frac{n}{p}x \in C'[p] \setminus \{0\} = B'[p] \setminus \{0\}$. Otherwise, if nx is not 0, then $nx \in B \setminus \{0\} \subset B' \setminus \{0\}$.

We conclude that $B' \subset C'$ is an essential extension, so by Theorem 2.4 there is an injective D-homomorphism $C' \to \bar{B}$.

Next, we show that every group X that has properties 1 and 2 has no non-trivial radical extensions. Let X be such a group, and suppose $X \subset F$ is a radical extension. Let f be any element of F, and $n \in \mathbf{Z}_{>0}$ such that $nf \in B$. By property 2, there is a B-injection $\varphi : F \to X$. We have $n\varphi(f) = \varphi(nf) = nf$, so $n(\varphi(f) - f)$ equals 0, and $\varphi(f) - f$ is an n-torsion element of F. Because F and X both have the property that their finite subgroups are cyclic, they share a unique subgroup of order n, so we see $\varphi(f) - f \in F[n] = X[n] \subset X$. We conclude that f is an element of X, so F equals X.

We conclude the proof of Theorem 2.1 by showing unicity. If there are two extensions $B \subset X$ and $B \subset Y$ both satisfying the properties from the theorem, then there is a B-injection $\varphi : X \to Y$ (by property 1 of X and 2 of Y). The image $\varphi(X)$ clearly also satisfies these properties, and $\varphi(X) \subset Y$ is a radical extension, so $\varphi(X)$ equals Y (since $\varphi(X)$ has no non-trivial radical extensions) and φ is a B-isomorphism. □

2.3 Galois radical extensions

Since we aim to study Galois groups of fields using similar structures for radical group extensions, in this section we will explore analogous concepts. We will look at some of the different properties characterizing Galois field extensions and what these lead to in our current setting, such as the ground field being the invariant subfield of some automorphism group, or all embeddings into a fixed algebraic closure having the same image.

Lemma 2.5. *Let C be an abelian group with all finite subgroups of C cyclic. Let $G \subset \mathrm{Aut}(C)$ be a subgroup, and write C^G for the G-invariants of C. Then the following three properties are equivalent.*

1. *$C^G \subset C$ is a radical extension, i.e., C/C^G is torsion;*
2. *$I_G \cdot C$ is torsion, where I_G is the augmentation ideal $\langle 1 - \sigma : \sigma \in G \rangle \subset \mathbf{Z}[G]$;*
3. *G acts trivially on C/C_{tors}.*

We start the proof of this lemma with a small proposition about the augmentation ideal.

Proposition 2.6. *Let C and G be as above, and let x be an element of C and $\bar{x}$ its image in C/C^G. If $I_G \cdot x$ or $\langle \bar{x} \rangle$ is finite, then $I_G \cdot x$ and $\bar{x}$ are cyclic of the same order.*

Proof. For any positive integer n we have $nI_G \cdot x = I_G \cdot nx$, so $nI_G \cdot x$ is 0 if and only if nx is invariant under G. The proposition immediately follows from this observation and the fact that all finite subgroups of C are cyclic. □

Proof of Lemma 2.5. (1) $\Leftrightarrow$ (2): This follows directly from the proposition.

(2) $\Leftrightarrow$ (3): Both statements are equivalent to G only shifting elements of C by torsion elements of C. □

These properties lead to the following definition.

Definition 2.7. A *Galois radical extension* is a radical extension $B \subset C$ such that there is a subgroup $G \subset \mathrm{Aut}(C)$ with $B = C^G$.

Note that despite the name we have given these Galois extensions, there is in general no one to one correspondence between subgroups of the radical group and subgroups of its automorphism group. Most extensions generated by elements of prime order do not have this property, for example: if we take $C = \mathbf{Z}/p\mathbf{Z}$ for a prime $p > 3$, and $G = \mathrm{Aut}(C) = (\mathbf{Z}/p\mathbf{Z})^*$, then C^G is $\{1\}$ and C/C^G is a Galois radical extension. It has no subextensions other than C and C^G, but G does have non-trivial subgroups.

This also implies that there are possibly multiple choices for the group G from the definition.

Galois radical extensions do share a number of properties with Galois field extensions, some of which are given by the following theorem. Other parallels are explored in the next two sections.

Theorem 2.8. *Let $B \subset C$ be a Galois radical extension, and choose a fixed maximal radical extension $\bar{B}$ of B. Then the following three statements hold.*

1. *For every $x \in C$ there is an integer $n > 0$ such that we have $nx \in B$ and C contains an element of order n;*
2. *All injective B-homomorphisms $C \to \bar{B}$ have the same image;*
3. *$B[2]$ equals $C[2]$.*

Proof. (1.) Let $B \subset C$ be a Galois radical extension, write $G = \mathrm{Aut}_B(C)$, and let x be any element of C. Let k be the order of $\bar{x} \in C/B$, which is well-defined because C/B is torsion. Consider the group $Z = I_G \cdot x \subset C$. Since C/B is torsion, Proposition 2.6 implies Z is finite. Because Z is finite, it is cyclic (by assumption on C). Let z be a generator of Z, and write n for the order of z and Z. Then, again by the proposition, nx is invariant under G and therefore an element of B. This means n satisfies the requirements of the statement.

(2.) We will proceed from statement 1. Suppose φ_1 and φ_2 are two injective B-homomorphisms from C to $\bar{B}$. Let $y = \varphi_1(x)$ be an element of the image of φ_1. It suffices to show y is in the image of φ_2.

Since $B \subset C$ satisfies statement 1, there is a positive integer n such that nx is in B and C contains an element z of order n. The image $\varphi_2(z)$ in $\bar{B}$ also has order n because φ_2 is an injection. Because φ_1 and φ_2 are the identity on B, we find $n\varphi_1(x) = n\varphi_2(x) \in B \subset \bar{B}$, which implies that $\varphi_1(x)$ equals $\varphi_2(x) + z'$ for some element z' of order dividing n. Using that all finite subgroups of $\bar{B}$ are cyclic, we conclude that z' is a multiple of $\varphi_2(z)$, so $y = \varphi_1(x)$ is in the image of φ_2.

(3.) If C contains an element of order 2, that element is unique and therefore invariant under all automorphisms of C and contained in C^G. □

Theorem 2.9. *If $B \subset C$ is a radical extension with $B[2]$ equal to $C[2]$ that satisfies statement 1 or statement 2 from Theorem 2.8, then it is a Galois radical extension.*

Proof. Since the proof of Theorem 2.8 shows that statement 1 implies statement 2, we only need to show the following statement:

If $B[2]$ equals $C[2]$ and all injective B-homomorphisms $C \to \bar{B}$ have the same image, then $B \subset C$ is a Galois radical extension.

To prove this, it suffices to show that $\mathrm{Aut}_B(C)$, the group of automorphisms of C that are the identity on B, does not have a set of invariants larger than B.

Suppose x is an element of $C \setminus B$ of order $p > 1$ in the quotient C/B. We will show there is an automorphism $\sigma \in \mathrm{Aut}_B(C)$ with $\sigma x \neq x$. Since every such x has a multiple of prime order, we can assume that p is prime without loss of generality.

We start by looking at the sub-extension $D = \langle B, x\rangle = B \oplus_{\langle px\rangle} \langle x\rangle$ and classifying the B-homomorphisms $D \to \bar{B}$.

Not all of these homomorphisms are necessarily injections. Suppose y is an element of the kernel of $\varphi \in \mathrm{Hom}_B(D, \bar{B})$. Then py is an element of B and also $\varphi(py) = p\varphi(y) = 0$. However, φ is a B-homomorphism, so φ restricted to B is injective. We see that py is 0 and y is p-torsion. We conclude that if there is no p-torsion in the kernel of φ, then φ is an injection.

If B contains an element of order p, there will clearly be no p-torsion in the kernel of any B-homomorphism (since the p-torsion is a cyclic group by assumption).

If B does not contain an element of order p, but D does, then B has index p in both $B + D[p]$ and in D, so $B + D[p]$ equals D. Then by the same reasoning as above, $\#\mathrm{Hom}_B(D, \bar{B}) = \#\mathrm{Hom}_B(B + D[p], \bar{B})$ equals p, and clearly exactly one of these homomorphisms is not an injection: the homomorphism sending all elements of order p to 0.

Note that for $p = 2$ we cannot be in the latter case, since we have assumed $B[2] = C[2] = D[2]$. This means that we have (at least) two different injections ψ_1 and ψ_2 of D to $\bar{B}$. These are uniquely defined by the image of x, so $\psi_1(x) \neq \psi_2(x)$.

Because $B \subset D$ is a radical extension, the maximal radical extension $\bar{B}$ of B is also a maximal radical extension of D. Its universal property implies ψ_1 and ψ_2 can be extended to injections $\tilde{\psi}_1$, $\tilde{\psi}_2$ from C to $\bar{B}$.

We have assumed that all such injections have the same image, so $\tilde{\psi}_2$ is invertible on the image of $\tilde{\psi}_1$, and $\sigma = \tilde{\psi}_2^{-1}\tilde{\psi}_1$ gives the desired automorphism of C with $\sigma(x) \neq x$. □

Example 2.10.

Statements 1 and 2 from Theorem 2.8 are equivalent if the extra condition $B[2] = C[2]$ (i.e., statement 3) is satisfied, as the above theorems and proofs show. The necessity of this condition $B[2] = C[2]$ is illustrated by the following example where B satisfies statement 2, but not statements 1 and 3 from Theorem 2.8.

Let X be the group $(\mathbf{Q}/\mathbf{Z}) \times \mathbf{Q}$, and define C to be the subgroup generated by $x = (\frac{1}{4}, \frac{1}{2})$ and $(0, 1)$. Let B be the (infinite cyclic) subgroup of C generated by $(0, 1)$. Then $\bar{B}$ equals X.

We have that C/B is cyclic of order 4, but C has no element of order 4. We will show that all injective B-homomorphisms $\varphi : C \to \bar{B}$ have the same image.

Let φ be any injective B-homomorphism $C \to \bar{B}$. Then $4\varphi(x)$ equals $(0, 2)$, so we find

$$\varphi(x) \in \left\{(\tfrac{1}{4}, \tfrac{1}{2}), (\tfrac{1}{2}, \tfrac{1}{2}), (\tfrac{3}{4}, \tfrac{1}{2}), (0, \tfrac{1}{2})\right\}.$$

If we have $\varphi(x) \in \{(\frac{1}{2}, \frac{1}{2}), (0, \frac{1}{2})\}$, then we obtain $\varphi(2x) = 2\varphi(x) = (0, 1) = \varphi((0, 1))$ which contradicts the fact that φ is an injection. We conclude $\varphi(x) \in \{(\frac{1}{4}, \frac{1}{2}), (\frac{3}{4}, \frac{1}{2})\}$.

Since we have $(\frac{1}{4}, \frac{1}{2}) = (0, 1) - (\frac{3}{4}, \frac{1}{2})$ with $(0, 1) \in B$, this implies that $\varphi(C)$ equals C, independent of the choice of φ.

In many cases in this thesis, the base group B is the unit group of a field K. If $K \subset L$ is a field extension and C is a subgroup of L^*, then $K^*[2] = C[2]$ holds, so one of the conditions of Theorem 2.9 is automatically satisfied.

If K has characteristic zero, then $\bar{K}^*$ is a divisible abelian group containing non-trivial p-torsion for every prime p. It follows from Theorem 2.1 that the maximal radical extension $\bar{B}$ of B can then be considered a subgroup of $\bar{K}^*$, with a natural action of the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$. With this action, $K^* \subset \bar{B}$ is a Galois radical extension.

Also, if we start from a Galois field extension $K \subset L$, and take $C \subset L^*$ to be the elements of L^* of which a power is in K, then C is a Galois radical group extension of K^* since C is closed under the action of $\mathrm{Gal}(L/K)$ and $K^* \subset C$ is the subgroup of invariants of the action.

Remark 2.11. If K has positive characteristic p, it is no longer true that the maximal radical extension of K^* can be considered a subgroup of $\bar{K}^*$, because $\bar{K}^*$ does not contain non-trivial p-torsion. We can adjust the definition of radical extensions to require that all finite subgroups are cyclic of order coprime to p, and likewise exclude p-torsion and extensions of degree divisible by p from the maximal radical extension. While we will not go into details, the resulting maximal radical extension will then again have the required universal properties for this restricted class of extensions, and also a natural action from the absolute Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ of K.

2.4 Kummer theory of radical extensions

If $B \subset C$ is a radical extension, an automorphism of C that is the identity on B is called a B-automorphism, and we denote the group of such automorphisms by $\mathrm{Aut}_B(C)$.

Suppose that $B \subset C \subset D$ is a tower of abelian groups such that C and D are both radical groups over B, and C is a Galois radical group over B. By Theorem 2.8,

for every x in C there is a positive integer n such that $y = nx$ is in B and C has an element of order n. Any $\sigma \in \mathrm{Aut}_B(D)$ leaves y invariant, so $\sigma(x) - x$ is an n-torsion element of B, and therefore in C. So, we see that every B-automorphism of D maps C into itself. Therefore there is a well-defined restriction map $\mathrm{Aut}_B(D) \to \mathrm{Aut}_B(C)$.

As we already saw in a special case in Lemma 1.8, if D is also Galois over B, this restriction map is a surjection. This is true in general.

Theorem 2.12. *If $B \subset C \subset D$ is a tower of abelian groups such that C and D are both Galois radical groups over B, there is a natural exact sequence of groups*

$$0 \to \mathrm{Aut}_C(D) \to \mathrm{Aut}_B(D) \xrightarrow{\text{res}} \mathrm{Aut}_B(C) \to 0.$$

Proof. Since the proof of Lemma 1.8 doesn't use the fact that the abelian groups in question are radical groups over (the unit group of) a field specifically, the proof of that lemma applies to the present theorem unchanged. □

If C is a Galois radical extension of B, then C is the injective limit (and union) of all finite Galois radical extensions $D \subset C$ over B. This makes $\mathrm{Aut}_B(C)$ a *profinite* group, and the exact sequence given in Theorem 2.12 is an exact sequence of profinite groups.

Theorem 2.13. *Let $B \subset F$ be a radical extension of abelian groups, and C and D two subgroups of F such that $B \subset C$ and $B \subset D$ are Galois radical extensions. Then $C \cap D$ and $C + D$ are also Galois radical extensions of B and there is a natural isomorphism of profinite groups*

$$\mathrm{Aut}_B(C + D) \xrightarrow{\sim} \mathrm{Aut}_B(C) \times_{\mathrm{Aut}_B(C \cap D)} \mathrm{Aut}_B(D).$$

Proof. Since C and D are both Galois, they satisfy statements 2 and 3 from Theorem 2.8. These two statements directly transfer to $C \cap D$ and $C + D$, so by Theorem 2.9, these two groups are also Galois over B. For the second part of the theorem, we use Theorem 2.12, which gives us two restriction maps from $\mathrm{Aut}_B(C + D)$ to $\mathrm{Aut}_B(C)$ resp. $\mathrm{Aut}_B(D)$ that combine into a natural homomorphism

$$\mathrm{Aut}_B(C + D) \xrightarrow{\sim} \mathrm{Aut}_B(C) \times_{\mathrm{Aut}_B(C \cap D)} \mathrm{Aut}_B(D).$$

It is an isomorphism since an explicit inverse exists:

$$(f, g) \mapsto (c + d \mapsto f(c) + g(d)),$$

This is a well-defined map because (f, g) is in the fibered product.

□

In the general setting of a radical extension $B \subset C$ we call an element $x \in C$ a *Kummer radical* if there is a positive integer w such that wx is in B and B contains an element of order w. Generalizing the concept as it was introduced in Chapter 1, we call a radical extension generated by Kummer radicals a *Kummer radical extension*.

Every element of a Kummer radical extension is a Kummer radical, so all subextensions of a Kummer radical extension are also Kummer radical extensions. Note that by Theorem 2.9 Kummer radical extensions are Galois radical extensions.

Theorem 2.14. *Let G be a profinite group and B be an (additively written) abelian group with the discrete topology and a continuous G-action given by $f : G \to \mathrm{Aut}(B)$. Assume that all finite subgroups of B are cyclic, and that B is a Kummer radical extension of B^G. Then the image of f is $\mathrm{Aut}_{B^G}(B)$ and $\mathrm{Aut}_{B^G}(B)$ is abelian.*

We begin the proof of this theorem with the familiar Kummer pairing, for which we largely follow Lang [17], §VI.8.

Lemma 2.15. *Let $C \subset D$ be a Kummer radical extension of finite degree. Then $\mathrm{Aut}_C(D)$ is an abelian group and there is a bilinear map*

$$\begin{array}{rcl} \mathrm{Aut}_C(D) \times D & \longrightarrow & C_{\mathrm{tors}} \\ (\sigma, x) & \longmapsto & \sigma(x) - x. \end{array}$$

The kernel on the left is 1 and the kernel on the right is C.

Proof. Let x be an element of D and w a corresponding positive integer with $wx \in C$ and $\#C[w] = w$. For any element $\sigma \in \mathrm{Aut}_C(D)$ we then find $\sigma(x) - x \in D[w] \subset C_{\mathrm{tors}}$, so the map given is well-defined.

Now fix an element $x \in D$ and let $\sigma, \tau \in \mathrm{Aut}_C(D)$ be two automorphisms. Note that because σ leaves the elements of C invariant, we have the identity

$$\sigma(\tau(x) - x) = \tau(x) - x.$$

This directly implies that $\sigma\tau(x)$ equals $\tau(x)+\sigma(x)-x$. From this we see $\sigma\tau(x)-x = (\tau(x) - x) + (\sigma(x) - x)$, so the map $\mathrm{Aut}_C(D) \to C_{\mathrm{tors}}$ we get from the pairing with a fixed x is a group homomorphism.

Now define $D' = \langle C, x \rangle$. This is also a Kummer extension of C, so by the same reasoning as above, the following map defines a group homomorphism.

$$\begin{array}{rcl} \mathrm{Aut}_C(C') & \longrightarrow & C_{\mathrm{tors}} \\ \sigma & \longmapsto & \sigma(x) - x. \end{array}$$

It is injective, since if an automorphism in $\mathrm{Aut}_C(C')$ leaves x invariant, it is the identity. We see that $\mathrm{Aut}_C(C')$ is abelian. If we combine this using Theorem 2.13 for a finite set of generators of D, we see that $\mathrm{Aut}_C(D)$ is abelian.

We continue by fixing $\sigma \in \mathrm{Aut}_C(D)$ and taking $x, y \in D$. Then we can derive $\sigma(x+y)-(x+y) = \sigma(x)+\sigma(y)-(x+y) = (\sigma(x)-x))+(\sigma(y)-y)$. This means that the map $D \to C_{\mathrm{tors}}$ from the pairing with a fixed σ is also a group homomorphism, and the map $\mathrm{Aut}_C(D) \times D \to C_{\mathrm{tors}}$ is indeed bilinear.

For the kernel on the left, let $\sigma \in \mathrm{Aut}_C(D)$ be such that for all $x \in D$ we have $\sigma(x) - x = 0$. Then clearly σ is the identity.

On the right, let x be an element of D. Then by definition x is in the kernel on the right if and only if for all $\sigma \in \mathrm{Aut}_C(D)$ we have $\sigma(x) - x = 0$. This is equivalent with x being invariant under $\mathrm{Aut}_C(D)$. Since $C \subset D$ is a Galois radical extension, the invariants of $\mathrm{Aut}_C(D)$ are exactly C. We conclude that the kernel on the right is C. □

Corollary 2.16. *Let $C \subset D$ be a Kummer radical extension of finite degree. Then the automorphism group $\mathrm{Aut}_C(D)$ is abelian of order $\#(D/C)$.*

Proof. We can invoke duality (specifically, Theorem 9.2 in Chapter 1 of [17]) to see that the following map induced by the pairing is a group isomorphism.

$$\begin{array}{rcl} \mathrm{Aut}_C(D) & \xrightarrow{\sim} & \mathrm{Hom}(D/C, C_{\mathrm{tors}}) \\ \sigma & \longmapsto & (x \mapsto \sigma(x) - x) \end{array}$$

This directly shows that $\mathrm{Aut}_C(D)$ is an abelian group of order $\#(D/C)$. □

Proof of Theorem 2.14. Abusing notation, we will write $\sigma(x)$ for $f(\sigma)(x)$, for $\sigma \in G$ and $x \in B$.

We start by proving the theorem in the case that G is finite. The lemma shows that $G/\ker f$ is abelian, and a similar construction to the one in the lemma gives a bilinear map of abelian groups

$$\begin{array}{rcl} (G/\ker f) \times B & \longrightarrow & B^G_{\mathrm{tors}} \\ (\sigma, x) & \longmapsto & \sigma(x) - x. \end{array}$$

The kernel on the left is 1 since we have already divided by $\ker f$. The kernel on the right is B^G by definition.

Since B^G_{tors} is finite and cyclic, by duality the following map is an isomorphism.

$$\begin{array}{rcl} G/\ker f & \longrightarrow & \mathrm{Hom}(B/B^G, B^G_{\mathrm{tors}}) \\ \sigma & \longmapsto & (x \mapsto \sigma(x) - x) \end{array}$$

Using duality as in the proof of Corollary 2.16 now proves the theorem in the finite case.

In the general profinite case, note that B is the union of all C with $B^G \subset C \subset B$ and $B^G \subset C$ a finite Galois radical extension. This implies that $\mathrm{Aut}_{B^G}(B)$ is the projective limit of $\mathrm{Aut}_{B^G}(C)$, and in particular we give it the corresponding profinite topology.

For every C with $B^G \subset C \subset B$, the induced map $\varphi_C : G \to \mathrm{Aut}_{B^G}(C)$ is surjective and it factors via $G/\ker(\varphi_C)$, which is finite since $\mathrm{Aut}_{B^G}(C)$ is finite. That means the finite case of the present theorem applies to the action $G/\ker(\varphi_C) \to \mathrm{Aut}_{B^G}(C)$.

As G maps surjectively to each $\mathrm{Aut}_{B^G}(C)$, the image of G is dense in $\mathrm{Aut}_{B^G}(B)$.

The group G is profinite and therefore compact, and its image under the continuous map to $\mathrm{Aut}_{B^G}(B)$ is therefore also compact. Since $\mathrm{Aut}_{B^G}(B)$ is Hausdorff because it is also profinite, this compact image is closed. We have already shown it is dense, so it is equal to the full group, proving that $f : G \to \mathrm{Aut}_{B^G}(B)$ is surjective. Since additionally $\mathrm{Aut}_{B^G}(B)$ is the projective limit of the abelian groups $\mathrm{Aut}_{B^G}(C)$, it is itself abelian.

This concludes the proof of Theorem 2.14.

□

To compute an automorphism group of a Galois radical extension of abelian groups $B \subset C$, it is often useful to consider the tower $B \subset B + C_{\text{tors}} \subset C$. By Theorem 2.12 there is an exact sequence

$$0 \to \text{Aut}_{(B+C_{\text{tors}})}(C) \to \text{Aut}_B(C) \xrightarrow{\text{res}} \text{Aut}_B(B + C_{\text{tors}}) \to 0.$$

Since the restriction map $\text{Aut}_B(B + C_{\text{tors}}) \to \text{Aut}_{B_{\text{tors}}}(C_{\text{tors}})$ is an isomorphism, we in fact have an exact sequence

$$0 \to \text{Aut}_{(B+C_{\text{tors}})}(C) \to \text{Aut}_B(C) \xrightarrow{\text{res}} \text{Aut}_{B_{\text{tors}}}(C_{\text{tors}}) \to 0. \tag{2.17}$$

This sequence does not necessarily split, as illustrated by the following example.

Example 2.18.

Let C be the abelian group $\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}$ and B the subgroup generated by $(4, 0)$ and $(1, 2)$. Note that this is a radical extension since $8C$ is a subgroup of B. The torsion of C is of order 8, so $\text{Aut}(C_{\text{tors}})$ is isomorphic to V_4. Since B_{tors} is of order 2 and C has only one element of order 2 (as required), every automorphism of C_{tors} automatically leaves the elements of B_{tors} invariant. We find that $\text{Aut}_{B_{\text{tors}}}(C_{\text{tors}}) \cong V_4$.

For the step from $B + C_{\text{tors}}$ to C, we see that C is generated by $(0, 1)$ as an extension of $B + C_{\text{tors}}$, and that $2 \cdot (0, 1)$ is in $B + C_{\text{tors}}$. We conclude that $\text{Aut}_{B+C_{\text{tors}}}(C)$ is of order 2.

Finally, consider the isomorphism σ of C sending $(1, 0)$ to $(3, 0)$ and $(0, 1)$ to $(3, 1)$. This leaves the elements of B invariant since it satisfies $\sigma(4, 0) = (4, 0)$ and $\sigma(1, 2) = (1, 2)$. Its order is 4 because $\sigma(0, 1) = (3, 1)$, and $\sigma^2(0, 1) = (4, 1)$. This means the exact sequence does not split.

Using the exact sequence 2.17, we can count the number of automorphisms of a Galois radical extension of finite degree.

Theorem 2.19. *If $B \subset C$ is a Galois radical extension of finite degree, then the order of the automorphism group $\text{Aut}_B(C)$ equals*

$$\#(C/B) \prod_{\substack{p \text{ prime} \\ C[p] \neq B[p]}} \frac{p-1}{p}.$$

Proof. The automorphism group $\text{Aut}_{(B+C_{\text{tors}})}(C)$ on the left side of (2.17) corresponds to a Kummer extension, so the cardinality of the automorphism group is equal to $\#C/(B + C_{\text{tors}})$.

On the right side of (2.17), the automorphism group $\text{Aut}_{B_{\text{tors}}}(C_{\text{tors}})$ is a subgroup of $\text{Aut}(C_{\text{tors}})$. If we write $n = \#C_{\text{tors}}$ and $w = \#B_{\text{tors}}$, we see that $\text{Aut}(C_{\text{tors}})$ is canonically isomorphic to $(\mathbf{Z}/n\mathbf{Z})^*$. Under that isomorphism, $\text{Aut}_{B_{\text{tors}}}(C_{\text{tors}})$ corresponds to the subgroup of elements that are 1 modulo w, of which there are

exactly $\varphi(n)/\varphi(w)$. So, the order of $\mathrm{Aut}_{B_{\mathrm{tors}}}(C_{\mathrm{tors}})$ is equal to

$$\frac{n}{w}\prod_{\substack{p \text{ prime}\\ p|n}}\frac{p-1}{p}\prod_{\substack{p \text{ prime}\\ p|w}}\frac{p}{p-1}=\#(C_{\mathrm{tors}}/B_{\mathrm{tors}})\prod_{\substack{p \text{ prime}\\ C[p]\neq B[p]}}\frac{p-1}{p}.$$

Multiplying the orders on the left and right sides of the exact sequence 2.17 concludes the proof of the theorem. □

2.5 Abelian radical extensions and Schinzel's theorem

Let G be a profinite group and B be an abelian group with the discrete topology and a continuous G-action. In this section we will give an explicit criterion for when the image of G in $\mathrm{Aut}(B)$ is abelian, as a generalization of Schinzel's Theorem 1.7. We will then use it to identify the maximal abelian sub-extension of a Galois radical extension.

Theorem 2.20. *Let G be a profinite group and B be an (additively written) discrete abelian group with a continuous G-action given by $f : G \to \mathrm{Aut}(B)$. Assume B/B^G is a Galois radical extension.*

Then, the image of f is abelian if and only if the following holds:

$$\forall x \in B : \exists w \in \mathbf{Z}_{>0} : wx \in B_{\mathrm{tors}} + B^G \text{ and } B^G \text{ has an element of order } w.$$

Proof. First assume that the image of f is abelian. Let x be an element of B. We will explicitly give an integer w that satisfies the condition from the theorem.

Let $I \subset \mathbf{Z}[G]$ again be the augmentation ideal, and denote Ix by T. The group T is finite and cyclic by Proposition 2.6. Let τ be a generator and n its order.

The $\mathbf{Z}[G]$-module T has an annihilator $J \subset \mathbf{Z}[G]$, which is a two-sided ideal. As J is also the annihilator of τ, this gives an isomorphism of $\mathbf{Z}[G]$-modules

$$\mathbf{Z}[G]/J \cong_{\mathbf{Z}[G]} T = \langle\tau\rangle,$$

and since T is cyclic of order n, a unique isomorphism of rings

$$\mathbf{Z}[G]/J \cong \mathbf{Z}/n\mathbf{Z}.$$

Under this isomorphism, the ideal $(I+J)/J$ corresponds to an ideal $\bar{I}$ in $\mathbf{Z}/n\mathbf{Z}$. Now define $w \mid n$ by $\bar{I} = w\mathbf{Z}/n\mathbf{Z}$.

Then the w-torsion of the $\mathbf{Z}/n\mathbf{Z}$-module T is cyclic of order w and equal to the $(I+J)/J$-torsion of T as a $\mathbf{Z}[G]/J$-module. This is in turn equal to the I-torsion of T as a $\mathbf{Z}[G]$-module, which is T^G. So $T^G \subset B^G$ contains an element of order w, and the condition that B^G contains an element of order w is satisfied.

We have defined w to be in $I+J$, so $wx \in Ix + Jx$. Since the image of G in $\mathrm{Aut}(B)$ is abelian, we have $IJx = JIx = 0$. So, the $\mathbf{Z}[G]$-module Jx is annihilated

by I and therefore contained in B^G. Moreover, Ix is contained in B_{tors}, so we conclude $wx \in B_{\text{tors}} + B^G$ holds, as required. This proves the first implication.

For the converse, assume that for every $x \in B$ there exists $w \in \mathbf{Z}_{>0}$ such that wx is in $B_{\text{tors}} + B^G$ and B^G has an element of order w.

The group B is a radical group over B^G, so there is a maximal B^G-radical extension $\bar{B}$. Since all elements of a Kummer radical extension are Kummer radicals, the subgroup of $\bar{B}$ consisting of all Kummer radicals is the maximal Kummer radical extension of B. We call this $\bar{B}_{\text{Kum}}$:

$$\bar{B}_{\text{Kum}} = \{x \in \bar{B} : \exists w \in \mathbf{Z}_{>0} : wx \in B^G \text{ and } B^G \text{ has an element of order } w\},$$

Then from the assumption, it follows that B is a subset of $C = \bar{B}_{\text{Kum}} + \bar{B}_{\text{tors}}$. Since both $\bar{B}_{\text{Kum}}$ and $B^G + \bar{B}_{\text{tors}}$ are Galois radical groups over B^G (by Theorem 2.9), the automorphism group $\text{Aut}_{B^G}(C)$ is a subgroup of the product $\text{Aut}_{B^G}(\bar{B}_{\text{Kum}}) \times \text{Aut}_{B^G}(B^G + \bar{B}_{\text{tors}})$ due to Theorem 2.13. The extension $B^G \subset B^G + \bar{B}_{\text{tors}}$ is generated by torsion elements so $\text{Aut}_{B^G}(B^G + \bar{B}_{\text{tors}})$ is abelian, and $\text{Aut}_{B^G}(\bar{B}_{\text{Kum}})$ is abelian by Theorem 2.14, so this product of automorphism groups is abelian. This implies that $\text{Aut}_{B^G}(B)$, which is a quotient of $\text{Aut}_{B^G}(C)$ by Theorem 2.12, is also abelian, proving the theorem. □

Schinzel's Theorem 1.7 is a corollary of this theorem:

Corollary 2.21 (Schinzel)**.** *Let F be a field, $a \in F$, and n a positive integer not divisible by* $\operatorname{char} K$*. Let w be the number of n-th roots of unity in F. Then, the splitting field Ω of $X^n - a$ is abelian over F if and only if there exists $b \in F$ with $a^w = b^n$.*

Proof. Define B as $\langle F^*, \zeta_n, \sqrt[n]{a} \rangle$ and apply the theorem to the natural action given by the map $\text{Gal}(\Omega/F) \to \text{Aut}(B)$. Since this action is faithful, we only need to verify that there exists $b \in F$ with $a^w = b^n$ if and only if the following condition from the theorem holds:

$$\forall x \in B : \exists w \in \mathbf{Z}_{>0} : wx \in B_{\text{tors}} + B^G \text{ and } B^G \text{ has an element of order } w.$$

Suppose there is an element $b \in F$ with $a^w = b^n$. To show that the theorem applies, it is sufficient to prove the condition for a set of generators of B over F^*, such as ζ_n and a choice of $\sqrt[n]{a}$. For the root of unity this is immediate.

For $x \in B$ with $x^n = a$, we use that we have $a^w = b^n$. This implies that $x^w = \zeta b$ for some $\zeta \in \mu_n$. Since μ_n is contained in B, this shows that x^w is in $B_{\text{tors}} B^G$.

For the other implication, suppose that the condition from the theorem holds. We will show $a^w \in F^{*n}$.

Let $x \in B$ be such that $x^n = a$. Then by assumption there is a positive integer v such that F^* has an element of order v and $x^v \in B_{\text{tors}} F^*$. Since both x^v and x^n are elements of $B_{\text{tors}} F^*$, we in fact have $x^w \in B_{\text{tors}} F^*$, since w is a multiple of $\gcd(n, v)$. So, we can choose $\zeta \in B_{\text{tors}}$ such that we have $x^w \in \zeta F^*$, and we have that ζ^n is an element of F^{*w}.

Let m be any common multiple of n and the order of ζ. Then because we have $F^*[n] = F^*[w]$, the orders of $(F^*[m])^n$ and $(F^*[m])^w$ are equal, and therefore these two subgroups of F^* are equal. Since we have $\zeta^n \in F^*[m]^w$, we then also have $\zeta^n \in F^*[m]^n \subset F^{*n}$. We now conclude that $a^w = x^{nw} \in F^{*n}$. □

Theorem 2.20 gives a condition for when a group acts in an abelian way on a radical group extension. This can also be used to characterize the maximal G-submodule B_{ab} on which a group G acts in an abelian way, shown by the following definition and accompanying theorem.

Define B_{ab} as follows:

$$B_{\mathrm{ab}} = \{x \in B : \exists w \in \mathbf{Z}_{>0} : wx \in B_{\mathrm{tors}} + B^G \text{ and } B^G \text{ has an element of order } w\}.$$

Note that this definition does not depend on the choice of G, but only on its invariants B^G.

Theorem 2.22. *Let G be a profinite group and B be a discrete abelian group with a continuous G-action. Assume that B/B^G is torsion and all finite subgroups of B are cyclic.*

1. *For a G-module C with $B^G \subset C \subset B$, the image of G in $\mathrm{Aut}(C)$ is abelian if and only if C is a subgroup of B_{ab}.*
2. *Write $[G, G]$ for the closed subgroup of G generated by the commutators of G. Then B_{ab} equals $B^{[G,G]}$.*

We will use the following proposition in the proof of this theorem.

Proposition 2.23. *Let C be a G-module with $B^G \subset C \subset B$. Then we have $C_{\mathrm{ab}} = B_{\mathrm{ab}} \cap C$.*

Proof. Since B^G equals C^G and $(B_{\mathrm{tors}} + B^G) \cap C$ equals $C_{\mathrm{tors}} + C^G$, we can derive the following expressions for C_{ab}.

$$\begin{aligned}
C_{\mathrm{ab}} &= \{x \in C : \exists w \in \mathbf{Z}_{>0} : wx \in C_{\mathrm{tors}} + C^G \text{ and} \\
&\qquad\qquad C^G \text{ has an element of order } w\} \\
&= \{x \in C : \exists w \in \mathbf{Z}_{>0} : wx \in (B_{\mathrm{tors}} + B^G) \cap C \text{ and} \\
&\qquad\qquad B^G \text{ has an element of order } w\} \\
&= C \cap \{x \in B : \exists w \in \mathbf{Z}_{>0} : wx \in B_{\mathrm{tors}} + B^G \text{ and} \\
&\qquad\qquad B^G \text{ has an element of order } w\} \\
&= B_{\mathrm{ab}} \cap C.
\end{aligned}$$

□

Proof of Theorem 2.22. Let C be a G-module with $B^G \subset C \subset B$. By Theorem 2.20, the group G acts in an abelian way on C if and only if C equals C_{ab}. Because C_{ab} is the intersection of B_{ab} and C (Prop. 2.23), the first part of the theorem follows.

Since the image of G in $\mathrm{Aut}(B_{\mathrm{ab}})$ is abelian, B_{ab} is pointwise invariant under the action of the commutator subgroup $[G,G]$, and so B_{ab} is a subgroup of $B^{[G,G]}$.

For the opposite inclusion, the abelian group $G/[G,G]$ acts on $B^{[G,G]}$ since $[G,G]$ is a normal subgroup of G. We conclude that G itself acts on $B^{[G,G]}$ in an abelian way, so by the first part of the theorem, $B^{[G,G]}$ is contained in B_{ab}. □

Corollary 2.24. *The action of G on B induces a surjection $[G,G] \to \mathrm{Aut}_{B_{\mathrm{ab}}}(B)$.*

Proof. The (closed) commutator subgroup $[G,G]$ acts on B, and the extension of radical groups B over $B^{[G,G]} = B_{\mathrm{ab}}$ is a Kummer radical extension. Therefore, by Theorem 2.14 the induced map $[G,G] \to \mathrm{Aut}_{B_{\mathrm{ab}}}(B)$ is a surjection. □

2.6 The entanglement group

As before, let G be a profinite group, and let B be a discrete (additively written) abelian group with a continuous G-action given by $f : G \to \mathrm{Aut}(B)$. Assume B/B^G is a Galois radical extension.

In this section we will prove the following main theorem.

Theorem 2.25. *With B and G as above, $f(G)$ is a normal subgroup of $\mathrm{Aut}_{B^G}(B)$ and $\mathrm{Aut}_{B^G}(B)/f(G)$ is an abelian profinite group.*

Definition 2.26. This cokernel $\mathrm{Aut}_{B^G}(B)/f(G)$ is called the *entanglement group* of B, and written $E(G,B)$, or $E(B)$ if the group G is clear from the context.

The term reflects how in the case of radical group extensions of the unit group of a field, certain multiplicatively independent radicals are *entangled* in the additive field structure. For example, the radical extensions $\mathbf{Q}^* \subset \langle \mathbf{Q}^*, \zeta_5, \sqrt{5} \rangle$ and $\mathbf{Q}^* \subset \langle \mathbf{Q}^*, \zeta_5, \sqrt{-5} \rangle$ have the same group structure and hence have isomorphic automorphism groups. However, when considering them with the natural action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, the corresponding field extensions are $\mathbf{Q}(\zeta_5, \sqrt{5})/\mathbf{Q}$ and $\mathbf{Q}(\zeta_5, \sqrt{-5})/\mathbf{Q}$. These have different degrees due to the additive relation $\sqrt{5} = \zeta_5 + \zeta_5^{-1} - \zeta_5^2 - \zeta_5^{-2}$, which has no equivalent for $\sqrt{-5}$. Informally, we say that the radicals $\sqrt{5}$ and ζ_5 are entangled. This lower degree of $\mathbf{Q}(\zeta_5, \sqrt{5})$ is reflected in a smaller image of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ in the automorphism group, and leads to an entanglement group of order 2.

The map from the automorphism group $\mathrm{Aut}_{\mathbf{Q}^*}(\langle \mathbf{Q}^*, \zeta_5, \sqrt{5} \rangle)$ to the entanglement group can be used to determine if a group automorphism extends to a field automorphism. In this example, this map checks if the action on ζ_5 and that on $\sqrt{5}$ are compatible with respect to the additive relation between the two radicals.

For the radical extension $\mathbf{Q}^* \subset \langle \mathbf{Q}^*, \zeta_5, \sqrt{-5} \rangle$, with the action of the absolute Galois group of $\mathbf{Q}$, the entanglement group is trivial.

Another example of non-trivial entanglement is the radical group extension $\mathbf{Q}^* \subset \langle \mathbf{Q}^*, \sqrt[4]{-4} \rangle$. Note that the square of $\sqrt[4]{-4}$ is $2\sqrt{-1}$, so this extension contains 4th roots of unity and is therefore a Galois radical extension. The automorphism group $\mathrm{Aut}_{\mathbf{Q}^*}(\langle \mathbf{Q}^*, \sqrt[4]{-4} \rangle)$ is non-cyclic of order 4.

On the field side, the extension $\mathbf{Q}(\sqrt[4]{-4})/\mathbf{Q}$ has degree 2, which can be seen by writing $\sqrt[4]{-4}$ as $\zeta_8\sqrt{2} = 1 + i$, with corresponding Galois group isomorphic to C_2, and an entanglement group of order 2.

Replacing $\sqrt[4]{-4}$ by $\sqrt[4]{-9}$ in this example leaves the abelian group structure unchanged, but removes the additive relation and leads to a trivial entanglement group.

We proceed with the proof of the main theorem.

Proof of Theorem 2.25. A main ingredient in the proof is restricting to the maximal subgroup $B_{\mathrm{ab}} \subset B$ for which $\mathrm{Aut}_{B^G}(B_{\mathrm{ab}})$ is abelian, as defined in the previous section.

Consider the following exact sequence of automorphism groups.

$$0 \to \mathrm{Aut}_{B_{\mathrm{ab}}}(B) \to \mathrm{Aut}_{B^G}(B) \xrightarrow{\mathrm{res}} \mathrm{Aut}_{B^G}(B_{\mathrm{ab}}) \to 0$$

For brevity, we will write N for the commutator subgroup $[G, G]$ in this proof. As we have seen, the action of G on B induces an action of G/N on B_{ab} with invariants B^G. It also induces an action of N on B with invariants B_{ab}. Adding those actions (as vertical maps) to the exact sequence above, we get the rows of the following diagram. These rows are exact, and the squares commute by definition of the vertical maps.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & N & \longrightarrow & G & \xrightarrow{\pi} & G/N & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle h} & & \\
0 & \longrightarrow & \mathrm{Aut}_{B_{\mathrm{ab}}}(B) & \longrightarrow & \mathrm{Aut}_{B^G}(B) & \xrightarrow{\pi'} & \mathrm{Aut}_{B^G}(B_{\mathrm{ab}}) & \longrightarrow & 0 \\
 & & & & & \searrow^{\varphi} & \downarrow & & \\
 & & & & & & E(B_{\mathrm{ab}}) & &
\end{array}$$

We proceed analogously to the proof of Theorem 1.6.

On the right side of the diagram, the group $\mathrm{Aut}_{B^G}(B_{\mathrm{ab}})$ is abelian by definition of B_{ab} and Theorem 2.20, so the image of h is a normal subgroup with abelian cokernel $E(B_{\mathrm{ab}})$. Let φ be the composite homomorphism from $\mathrm{Aut}_{B^G}(B)$ through $\mathrm{Aut}_{B^G}(B_{\mathrm{ab}})$ to $E(B_{\mathrm{ab}})$. We have to show that φ is surjective with kernel $f(G)$.

The image of f is contained in $\ker(\varphi)$ because of the commutativity of the right square of the diagram. To show the other inclusion, take $x \in \ker(\varphi)$. Then $\pi'(x)$ maps to 0 in $E(B_{\mathrm{ab}})$, so it is the image of h. The map π is surjective, so there is an element $y \in G$ with $h\pi(y) = \pi'(x)$. We then have $\pi' f(y) = \pi'(x)$, so $xf(y)^{-1}$ is in the kernel of π', which equals $\mathrm{Aut}_{B_{\mathrm{ab}}}(B)$. Because g is a surjection (Corollary 2.24), there is an element $z \in N \subset G$ with $g(z) = xf(y)^{-1}$. It follows that $f(zy) = x$ and $x \in f(G)$.

Surjectivity of φ follows immediately from its being composed from two surjective maps. This shows that $f(G)$ is a normal subgroup of $\mathrm{Aut}_{B^G}(B)$ with an abelian cokernel and concludes the proof of Theorem 2.25. □

If C is a G-submodule of B containing B^G, then by Theorem 2.12 the restriction map from $\mathrm{Aut}_{B^G}(B)$ to $\mathrm{Aut}_{B^G}(C)$ is a surjection, so there is a natural surjection $E(G,B) \twoheadrightarrow E(G,C)$. The proof of the theorem shows that this surjection is an isomorphism if we take $C = B_{\mathrm{ab}}$:

Corollary 2.27. *With B and G as in the theorem, $E(G, B_{\mathrm{ab}})$ is equal to $E(G,B)$.*

To derive more tangible expressions for the entanglement group, we study how $E(G,B) = E(G,B_{\mathrm{ab}})$ behaves when B_{ab} is the sum of two smaller G-modules.

Theorem 2.28. *Let B, G and B_{ab} be as before, and suppose $B_{\mathrm{ab}} = C + D$ with C, D two G-submodules of B_{ab}. Then the entanglement group $E(G,B) = E(G, C+D)$ is a part of the following short exact sequence.*

$$0 \to \mathrm{Aut}_{D\cap(B^G+C)}(D)/\mathrm{im}(G_C) \to E(G, C+D) \to E(G,C) \to 0,$$

where G_C is the kernel of the map $G \to \mathrm{Aut}(C)$ induced by the action of G on B.

Proof. We build up a diagram around the short exact sequence

$$0 \to \mathrm{Aut}_{B^G+C}(B_{\mathrm{ab}}) \to \mathrm{Aut}_{B^G}(B_{\mathrm{ab}}) \to \mathrm{Aut}_{B^G}(B^G + C) \to 0$$

and the G-action on B_{ab}.

First of all, note that we can replace G by its image in $\mathrm{Aut}_{B^G}(B_{\mathrm{ab}})$. This group is abelian, so we assume without loss of generality that G is abelian in this proof. Because C is a G-submodule of B_{ab}, there is an induced map $G \to \mathrm{Aut}_{B^G}(B^G + C)$, and this factors faithfully via G/G_C, by definition of G_C. On the left side of the sequence, the subgroup G_C acts on B_{ab} and leaves B^G and C pointwise invariant, so the image of G_C inside $\mathrm{Aut}_{B^G}(B_{\mathrm{ab}})$ ends up inside $\mathrm{Aut}_{B^G+C}(B_{\mathrm{ab}})$.

This leads to the following commutative diagram of abelian groups.

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & G_C & \longrightarrow & G & \longrightarrow & G/G_C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Aut}_{B^G+C}(B_{\mathrm{ab}}) & \longrightarrow & \mathrm{Aut}_{B^G}(B_{\mathrm{ab}}) & \longrightarrow & \mathrm{Aut}_{B^G}(B^G+C) & \longrightarrow & 0
\end{array}$$

Because D is a Galois radical extension of D^G, we have that D is a Galois radical extension over $D \cap (B^G + C)$, by statement 1 of Theorem 2.8 and Theorem 2.9. Therefore, there is a well-defined restriction homomorphism

$$\mathrm{Aut}_{B^G+C}(B_{\mathrm{ab}}) \xrightarrow{\sim} \mathrm{Aut}_{D\cap(B^G+C)}(D).$$

By the fibered sum structure $B_{\mathrm{ab}} = (B^G+C) \oplus_{D\cap(B^G+C)} D$, and the same reasoning as in the proof of Theorem 2.13, this restriction map is an isomorphism.

The cokernel of f is then given by $\mathrm{Aut}_{D\cap(B^G+C)}(D)/\mathrm{im}(G_C)$. The cokernels of the middle and right vertical maps are $E(G, B_{\mathrm{ab}})$ and $E(G, C)$ respectively, by definition. The snake lemma then gives us the desired sequence:

$$\begin{array}{ccccccccc}
 & & & & & & 0 & \longrightarrow & \cdots \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & G_C & \longrightarrow & G & \longrightarrow & G/G_C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Aut}_{B^G+C}(B_{\mathrm{ab}}) & \longrightarrow & \mathrm{Aut}_{B^G}(B_{\mathrm{ab}}) & \longrightarrow & \mathrm{Aut}_{B^G}(B^G+C) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & \mathrm{Aut}_{D\cap(B^G+C)}(D)/\mathrm{im}(G_C) & \longrightarrow & E(G, B_{\mathrm{ab}}) & \longrightarrow & E(G, C) & \longrightarrow & 0
\end{array}$$

□

Corollary 2.29. *Let B, G and B_{ab} be as in the theorem, and again suppose we have $B_{\mathrm{ab}} = C + D$ with C, D two G-submodules of B_{ab}. Define G_C to be the kernel of the induced map $G \to \mathrm{Aut}(C)$.*

If we have $E(G, C) = 1$, then there is an isomorphism

$$E(G, B) \xrightarrow{\sim} \mathrm{Aut}_{D\cap(B^G+C)}(D)/\mathrm{im}(G_C)$$

that, for each $\sigma \in \mathrm{Aut}_{B^G}(B)$ and $g \in G$ with $\sigma|_C = g|_C$, sends $\bar{\sigma} \in E(G, B)$ to $\sigma|_D(g|_D)^{-1}$.

Proof. Note that the existence of an isomorphism follows directly from the theorem since $E(G, C)$ is trivial. To get the explicit expression for the isomorphism, consider an element $\sigma \in \mathrm{Aut}_{B^G}(B)$. We proceed by diagram chasing in the diagram from the proof of the theorem. Since $E(G, C)$ is trivial, the vertical map $G/G_C \to \mathrm{Aut}_{B^G}(B^G + C)$ on the right side is a surjection, which implies there exists $g \in G$ satisfying $g|_C = \sigma|_C$. By multiplying σ with the inverse of g, we get $\tau = \sigma g^{-1} \in \mathrm{Aut}_{B^G}(B_{\mathrm{ab}})$ which acts as the identity on C by construction. This implies that τ is an element of the subgroup $\mathrm{Aut}_{B^G+C}(B_{\mathrm{ab}})$, on the left side of the diagram, and by mapping it down to $\mathrm{Aut}_{D\cap(B^G+C)}(D)/\mathrm{im}(G_C)$ we find the unique residue class there that maps to $\bar{\tau} \in E(B_{\mathrm{ab}})$, by commutativity. Because τ and σ differ by an element of G, we see that $\bar{\tau} = \bar{\sigma} \in E(B_{\mathrm{ab}})$, concluding the proof of this corollary. □

In the case that D is a Kummer radical extension of B^G, we can simplify the quotient we obtained here. First of all, since in that case D contains B^G, we can rewrite $D \cap (B^G + C)$ to the more symmetric $B^G + (C \cap D)$. Then, it follows from Theorem 2.14 (applied on G_C acting on W) that the image of G_C in $\mathrm{Aut}(D)$ is

$\mathrm{Aut}_{W^{G_C}}(W)$, and the following natural restriction map of the quotient is therefore an isomorphism:

$$\mathrm{Aut}_{B^G+(C\cap D)}(D)/\mathrm{im}(G_C) \xrightarrow{\sim} \mathrm{Aut}_{B^G+(C\cap D)}(D^{G_C}). \tag{2.30}$$

Going one step further, we can conclude the following if additionally there is no cyclotomic entanglement. This is a generalization of Theorem 1.10.

Corollary 2.31. *Let B, G and B_{ab} be as in the theorem, and suppose we have $B_{\mathrm{ab}} = \mu + W$ with μ a subgroup of B_{tors} and $W \subset B$ a Kummer radical extension of B^G. Define G_μ as the kernel of the restriction map $G \to \mathrm{Aut}(\mu)$.*

If we have $E(G, \mu) = 1$, then there is an isomorphism

$$E(G, B) \xrightarrow{\sim} \mathrm{Aut}_{B^G+(\mu\cap W)}(W^{G_\mu})$$

that, for each $\sigma \in \mathrm{Aut}_{B^G}(B)$ and $g \in G$ with $\sigma|_\mu = g|_\mu$, sends $\bar{\sigma} \in E(G, B)$ to $\sigma|_{W^{G_\mu}}(g|_{W^{G_\mu}})^{-1}$.

Proof. We start from the previous corollary (2.29), take $C = \mu$ and $D = W$ and apply Equation 2.30. □

This description of the entanglement group assumes that B_{ab} can be generated by roots of unity and Kummer roots. This condition is often fulfilled, in particular in the case of maximal radical extension which we study in Chapter 3, but we shall encounter situations where this is not the case later. In those cases, it is possible to extend B and B_{ab} with extra roots of unity to handle this. We describe this approach in Propositions 4.9 and 5.6.

Chapter 3

The absolute entanglement group

3.1 Introduction

Let K be a field, and choose a fixed separable closure K^{sep}. Define $\sqrt[\infty]{K^*} \subset K^{\mathrm{sep}*}$ as the group of all radicals over K^* inside $K^{\mathrm{sep}*}$. The entanglement group of $\sqrt[\infty]{K^*}$ with the action of the absolute Galois group G of K is of particular interest. We refer to this entanglement group as the *absolute entanglement group* of K, and write $E_{\mathrm{abs}}(K)$. Recall from Theorem 2.25 and Definition 2.26 that we have the following exact sequence that defines $E_{\mathrm{abs}}(K)$:

$$G \to \mathrm{Aut}_{K^*}(\sqrt[\infty]{K^*}) \to E_{\mathrm{abs}}(K) \to 1.$$

If K has characteristic 0, this maximal radical extension $\sqrt[\infty]{K^*}$ coincides with the group $\overline{K^*}$ defined in section 2.2. For characteristic $p > 0$, the same is true if we make the adjustments mentioned in Remark 2.11.

If $B \subset \sqrt[\infty]{K^*}$ is any Galois radical extension of K^*, then the restriction map from $\mathrm{Aut}_{K^*}(\sqrt[\infty]{K^*})$ to $\mathrm{Aut}_{K^*}(B)$ induces a surjection $E_{\mathrm{abs}}(K) \to E(B)$, so every entanglement group over K^* is a quotient of $E_{\mathrm{abs}}(K)$.

Before stating the main results of this chapter in Section 3.3, we first cover preliminaries on $\hat{\mathbf{Z}}$-ideals and Steinitz numbers in Section 3.2. The proofs of the main results are in Section 3.3 and Section 3.4, with the latter section treating the case of positive characteristic.

The result for characteristic zero was already announced in the lecture notes for Colloquium Lectures by H.W. Lenstra on Entangled Radicals [19] at the AMS Annual Meeting in 2006.

3.2 Preliminaries

In order to state the main results of this chapter, we first introduce some concepts related to the profinite groups concerned.

We define Z to be the endomorphism ring $\mathrm{End}(\mu)$ of the group μ of roots of unity of K^{sep}. The automorphism group $\mathrm{Aut}(\mu)$ is then equal to Z^*. Note that if K has characteristic 0, then Z is isomorphic to $\hat{\mathbf{Z}} \cong \prod_l \mathbf{Z}_l$, and if K has characteristic $p > 0$, then it is isomorphic to $\prod_{l \neq p} \mathbf{Z}_l$.

A convenient way to describe closed $\hat{\mathbf{Z}}$-ideals (and Z-ideals) is given by *Steinitz numbers*.

By unique factorization a positive integer can be uniquely written as a product $\prod_l l^{n(l)}$, where l ranges over the prime numbers, and $n(l)$ is a non-negative integer that is zero at all but finitely many l.

A Steinitz number is a formal expression of the form $\prod_l l^{n(l)}$, where $n(l)$ is an element of $\mathbf{Z}_{\geq 0} \cup \{\infty\}$ and l again ranges over the primes. Here infinitely many $n(l)$ may be non-zero. Steinitz numbers form a multiplicative monoid, containing the positive integers.

Given a Steinitz number n and an (additively written) profinite abelian group A, we define the $\hat{\mathbf{Z}}$-submodule nA of A by

$$nA = \bigcap_{\substack{m \mid n \\ m \in \mathbf{Z}_{\geq 1}}} mA.$$

Using that A is a product of pro-l-groups, one sees that nA equals $(n\hat{\mathbf{Z}})A$. If A is a profinite ring, then nA is in fact a closed A-ideal. For multiplicatively written A, we write A^n instead of nA.

One can check that this gives rise to an isomorphism between the monoid of Steinitz numbers and the monoid of closed $\hat{\mathbf{Z}}$-ideals given by $n \mapsto n\hat{\mathbf{Z}}$. If I is a closed $\hat{\mathbf{Z}}$-ideal, then I is equal to $n\hat{\mathbf{Z}}$ for the Steinitz number $n = \prod_l l^{n(l)}$ defined by

$$n(l) = \sup\{k \in \mathbf{Z}_{\geq 0} : I \subset l^k \hat{\mathbf{Z}}\}.$$

Let us write

$$\mathcal{S} = \{\text{Steinitz numbers } n = \prod_l l^{n(l)} \text{ with } n(p) = 0 \text{ if } p = \mathrm{char}(K) > 0\}.$$

We obtain a bijection

$$\mathcal{S} \longrightarrow \{\text{closed } Z\text{-ideals}\}$$

that sends n to nZ.

For a positive integer m, we write $\mu_m \subset \bar{K}^*$ for the m-th roots of unity in $\bar{K}$. If n is a Steinitz number in $\mathcal{S}$, we define μ_n as the union of all finite subgroups μ_m for $m \in \mathbf{Z}_{\geq 1}$ with $m \mid n$. Every subgroup of μ is of this form for a unique $n \in \mathcal{S}$, and the annihilator $\mathrm{Ann}_Z(\mu_n)$ of μ_n in Z is equal to nZ.

3.3 Main results

We use the notation of μ, Z, $\mathcal{S}$ from the previous section. The absolute Galois group G of K acts on μ, and we define Γ to be the image of G in Z^* of this action:

$$\Gamma = \operatorname{im}\left[\operatorname{Gal}(K^{\mathrm{sep}}/K) \longrightarrow \operatorname{Aut}(\mu) = Z^*\right] \subset Z^*.$$

Also define W as

$$W = \{x \in \sqrt[\infty]{K^*} : \exists w \in \mathbf{Z}_{>0} : x^w \in K^* \text{ and } K^* \text{ contains an element of order } w\},$$

the "Kummer part" of $\sqrt[\infty]{K^*}$ over K^*.

Finally, we define $w \in \mathcal{S}$ to be the Steinitz number for which wZ is the closure of the Z-ideal generated by $\{1-\gamma : \gamma \in \Gamma\}$. If n is a positive integer not divisible by the characteristic of K, then we have the equivalences

$$n \mid w \Leftrightarrow \forall \gamma \in \Gamma : \gamma \equiv 1 \bmod n \Leftrightarrow \mu_n \subset \mu \cap K.$$

From this we conclude that $\mu \cap K$ equals μ_w.

Theorem 3.1. *There is an isomorphism*

$$E_{\mathrm{abs}}(K) \xrightarrow{\sim} \left(Z^* \cap (1+w^2Z)\right)/\Gamma^w,$$

that, for each $\sigma \in \operatorname{Aut}_{K^*}(\sqrt[\infty]{K^*})$ and $g \in G$ with $g|_W = \sigma|_W$, sends $\bar{\sigma} \in E_{\mathrm{abs}}(K)$ to $\sigma|_\mu (g|_\mu)^{-1}$.

In characteristic $p > 0$ there is in fact an alternative easier description of $E_{\mathrm{abs}}(K)$ since all entanglement turns out to be visible on the roots of unity.

Proposition 3.2. *If K is of characteristic $p > 0$, the natural restriction map $E_{\mathrm{abs}}(K) \to E(\mu)$ is an isomorphism.*

Corollary 3.3. *Suppose K has characteristic $p > 0$. Define the Steinitz number a by*

$$\forall m \in \mathbf{Z}_{\geq 1} : \; m \mid a \Leftrightarrow \mathbf{F}_{p^m} \subset K.$$

Then the restriction map $\operatorname{Aut}(\sqrt[\infty]{K^*}) \to \operatorname{Aut}(\mu)$ induces an isomorphism of the absolute entanglement group of K to

$$\left(Z^* \cap (1+wZ)\right)/p^{a\hat{\mathbf{Z}}},$$

where p is considered as an element of the $\hat{\mathbf{Z}}$-module Z^*.

The Steinitz number a defined in this Corollary satisfies that for positive integers m we have $m \mid a \Leftrightarrow p^m - 1 \mid w$, so the Steinitz numbers w and a uniquely determine each other.

Example 3.4.

We compute the absolute entanglement group of $\mathbf{Q}$ as an illustration of Theorem 3.1.

We are in characteristic zero, so Z simply equals $\hat{\mathbf{Z}}$. Also, since $\mathbf{Q}$ has exactly two roots of unity, w is the integer 2. The restriction map of $\mathrm{Gal}(\mathbf{Q}(\mu)/\mathbf{Q})$ to $\mathrm{Aut}(\mu)$ is an isomorphism, so the image Γ of the action of the absolute Galois group of $\mathbf{Q}$ in $\mathrm{Aut}(\mu) \cong \hat{\mathbf{Z}}^*$ is the full group $\hat{\mathbf{Z}}^*$.

We now turn to the expression from Theorem 3.1 for the absolute entanglement group of $\mathbf{Q}$.

$$E_{\mathrm{abs}}(\mathbf{Q}) \cong \left(Z^* \cap (1 + w^2 Z)\right) / \Gamma^w$$

Rewriting this with the observations made above, we obtain the following.

$$E_{\mathrm{abs}}(\mathbf{Q}) \cong \left(\hat{\mathbf{Z}}^* \cap (1 + 4\hat{\mathbf{Z}})\right) \Big/ (\hat{\mathbf{Z}}^*)^2$$

Using the fact that we can identify $\hat{\mathbf{Z}}^*$ with $\prod_p \mathbf{Z}_p^*$, we see that $\hat{\mathbf{Z}}^* \cap (1+4\hat{\mathbf{Z}})$ corresponds to $(1+4\mathbf{Z}_2) \times \prod_{p \text{ odd}} \mathbf{Z}_p^*$, since 4 is invertible in Z_p^* for odd primes p. Also, $(\hat{\mathbf{Z}}^*)^2$ corresponds to $(1 + 8\mathbf{Z}_2) \times \prod_{p \text{ odd}} (\mathbf{Z}_p^*)^2$.

At the prime 2, the quotient $(1 + 4\mathbf{Z}_2)/(1 + 8\mathbf{Z}_2)$ is isomorphic to $\mathbf{Z}/2\mathbf{Z}$, and at odd primes p, the quotient $\mathbf{Z}_p^*/(\mathbf{Z}_p^*)^2$ is also isomorphic to $\mathbf{Z}/2\mathbf{Z}$. If we write $\mathcal{P}$ for the set of primes, we conclude that the absolute entanglement group of $\mathbf{Q}$ is isomorphic to

$$E = \{\pm 1\}^{\mathcal{P}}.$$

An explicit map from $A = \mathrm{Aut}_{\mathbf{Q}^*}(\sqrt[\infty]{\mathbf{Q}^*})$ to E can also be derived from the theorem.

We start with some notation. For $a \in \hat{\mathbf{Z}}^*$ and p a prime number, we let $(\frac{a}{p}) \in \{\pm 1\}$ be the Kronecker symbol. Recall that for odd p we have $(\frac{a}{p}) = 1$ if and only if a is a square mod p, and $(\frac{a}{2}) = 1$ if and only if $k \equiv \pm 1 \bmod 8$.

Then, for a prime p, write $p^* = (\frac{-1}{p})p$. Finally, given $\sigma \in A$, define $a_\sigma \in \hat{\mathbf{Z}}^*$ as the image of $\sigma|_\mu$ under the isomorphism $\mathrm{Aut}(\mu) \cong \hat{\mathbf{Z}}^*$. Note that for $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ and p prime, we have $(\frac{a_\sigma}{p}) = 1 \Leftrightarrow \sigma(\sqrt{p^*}) = \sqrt{p^*}$.

The homomorphism from A to E is then given by

$$\begin{array}{ccc} A & \longrightarrow & \{\pm 1\}^{\mathcal{P}} = E \\ \sigma & \longmapsto & \left(p \mapsto \dfrac{\sigma(\sqrt{p^*})}{\sqrt{p^*}} \cdot \left(\dfrac{a_\sigma}{p}\right)\right) \end{array}$$

In the remainder of this section we will prove Theorem 3.1. The other two results on positive characteristic are the topic of Section 3.4.

Proof of Theorem 3.1. The absolute entanglement group E_{abs} is equal to the entanglement group $E(B_{\mathrm{ab}})$ of the maximal abelian part B_{ab} of $B = \sqrt[\infty]{K^*}$ by Corollary 2.27.

To determine this entanglement group we proceed via Corollary 2.29.

Recall the definition of B_{ab}, transformed into the typical multiplicative notation for K^*:

$$B_{\mathrm{ab}} = \{x \in B : \exists w \in \mathbf{Z}_{>0} : x^w \in B_{\mathrm{tors}} \cdot B^G \text{ and } B^G \text{ has an element of order } w\}.$$

In our situation the abelian group B_{tors} is divisible by integers coprime to the characteristic p, so we have $B_{\mathrm{ab}} = \mu \cdot W$.

The Kummer part W has no entanglement as $E(W)$ is trivial by Theorem 2.14, so with $D = \mu$ and $C = W$ we can invoke Corollary 2.29 to get an expression for the entanglement group $E(B_{\mathrm{ab}})$ and corresponding map from $\mathrm{Aut}_{K^*}(\sqrt[\infty]{K^*})$.

We get the isomorphism

$$\varphi : E_{\mathrm{abs}} \xrightarrow{\sim} \mathrm{Aut}_{\mu \cap W}(\mu)/\mathrm{im}(G_W), \tag{3.5}$$

where G_W is the kernel of the map $G \to \mathrm{Aut}(W)$ induced by the action of G. Still according to Corollary 2.29, for any $\bar{\sigma} \in E(B_{\mathrm{ab}})$ with $\sigma \in \mathrm{Aut}(B)$, there exists $g \in G$ such that $\sigma|_W = g|_W$, and $\varphi(\bar{\sigma})$ is given by $\sigma|_\mu (g|_\mu)^{-1}$.

To reach the expression from the present Theorem, we will use the following proposition.

Proposition 3.6. *The ideal wZ is the annihilator in Z of $\mu \cap K$, and $w^2 Z$ is the annihilator in Z of $\mu \cap W$.*

Proof. Since $\mu \cap W$ equals μ_w, we find that $\mathrm{Ann}_Z(\mu \cap K)$ equals wZ.

Next, we remark that because the action of G is continuous, annihilators are closed Z-ideals and are therefore given by Steinitz numbers, and a Steinitz number is uniquely defined by the set of positive integers dividing it.

For the second statement, it suffices to show that $\mu \cap W$ equals μ_{w^2}, or equivalently, that for every positive integer n, the finite group μ_n is contained in $\mu \cap W$ if and only if n divides w^2.

Suppose $\mu \cap W$ contains an element of order n. Then there exists m such that we have $x^m \in \mu \cap K$ and $\mu_m \subset K$. This implies that n divides wm and m divides w, so n divides w^2.

Conversely, if n divides w^2, then there is a positive integer $m \mid n$ such that $m \mid w$ and $\frac{n}{m} \mid w$, which is easy to see per prime. Then any element x of order dividing n satisfies $x^m \in \mu \cap K$ and $\mu_m \subset K$, so x is in $\mu \cap W$. □

A direct corollary of this proposition is that if the number of roots of unity $\#(\mu \cap K)$ in K is finite, then w is the integer $\#(\mu \cap K)$.

We now continue with the proof of the main Theorem 3.1.

Since $w^2 Z$ is the annihilator in Z of $\mu \cap W$, the elements of Z^* that are 1 mod $w^2 Z$ are exactly those that fix $\mu \cap W$ pointwise. Therefore $Z^* \cap (1 + w^2 Z)$ is equal to $\mathrm{Aut}_{\mu \cap W}(\mu)$.

Recall that G_W is the kernel of the map $G \to \mathrm{Aut}(W)$ induced by the Galois action, i.e., the subgroup of G corresponding to the maximal Kummer extension of K in K^{sep}. This subgroup G_W is the intersection of all subgroups of G corresponding

to Kummer extensions of finite exponent, which are given by G^n with n ranging over the positive integers dividing the Steinitz number w.

We conclude that G_W is equal to G^w. Since the image of G in $\mathrm{Aut}(\mu)$ is defined to be Γ, the image of G_W in Aut_μ is given by Γ^w.

The expression from this theorem now immediately follows from the map 3.5. □

3.4 Positive characteristic

We continue with the proofs of Proposition 3.2 and Corollary 3.3, for the case where the characteristic p of K is positive.

Proof of Proposition 3.2. Applying the combination of Theorem 2.28 and Equation 2.30 to $C = \mu$ and $D = W$, we can observe that the absolute entanglement group fits into the following short exact sequence:

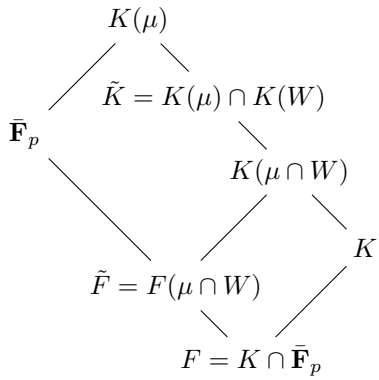
$$1 \to \mathrm{Aut}_{B^G(\mu \cap W)}(W^{G_\mu}) \to E_{\mathrm{abs}} \to E(\mu) \to 1 \tag{3.7}$$

Both W^{G_μ} and $B^G(\mu \cap W)$ are Kummer radical extensions of B^G. We claim these two groups are in fact equal. By Kummer duality there is a natural bijection between Kummer radical extensions of B^G and Kummer field extensions of K, so we can proceed by verifying they are both equal to the group of radicals of the same Kummer (field) extension of K.

We first look at W^{G_μ}. The kernel G_μ of the map $G \to \mathrm{Aut}(\mu)$ is the Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K(\mu))$, so W^{G_μ} equals $W \cap K(\mu)$. Now consider the Kummer extension $K(W) \cap K(\mu)$ over K. Its radical group is given by $(K(W) \cap K(\mu))^* \cap W = W \cap K(\mu)^* = W^{G_\mu}$, so we conclude by Kummer duality that $K(W^{G_\mu}) = K(W) \cap K(\mu)$.

Next we turn to $B^G(\mu \cap W)$. This group generates the field $K(B^G(\mu \cap W)) = K(\mu \cap W)$.

We will now prove that the fields $K(\mu \cap W)$ and $K(W) \cap K(\mu)$ are one and the same. To see this, we take the intersection with $\bar{\mathbf{F}}_p$.



Since $\bar{\mathbf{F}}_p$ equals $\mu \cup \{0\}$, the maximal Kummer extension $\tilde{F}$ of F inside $\bar{\mathbf{F}}_p$ is generated by roots of unity. Since all roots of unity of K are contained in $F = K \cap \bar{\mathbf{F}}_p$, this implies that $\tilde{F} = F(\mu \cap W)$. The maximal Kummer extension of K inside $K(\mu)$ is given by $\tilde{K} = K(\mu) \cap K(W)$.

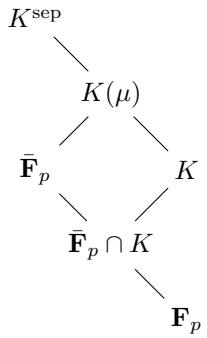
Because the roots of unity of K are exactly the roots of unity of F, the maximal Kummer extension of K inside $K(\mu)$ corresponds with the maximal Kummer extension of F inside $F(\mu) = \bar{\mathbf{F}}_p$ when taking intersections with $\bar{\mathbf{F}}_p$. We get the identity $\tilde{F} = \tilde{K} \cap \bar{\mathbf{F}}_p$, or, $F(\mu \cap W) = \tilde{K} \cap \bar{\mathbf{F}}_p$. We conclude that $\tilde{K}$ equals $K(\mu \cap W)$, as desired.

Combining these results leads to the fact that the group $\mathrm{Aut}_{B^G(\mu \cap W)}(W^{G_\mu})$ is trivial, and E_{abs} is equal to $E(\mu)$ according to the sequence 3.7. □

Proof of Corollary 3.3. It follows from Proposition 3.2 that the restriction map of $\mathrm{Aut}_{K^*}(\sqrt[\infty]{K^*})$ to $\mathrm{Aut}(\mu)$ induces an isomorphism of E_{abs} to $\mathrm{Aut}_{\mu \cap K}(\mu)/\Gamma$.

Since wZ is the annihilator of $(\mu \cap K)$, the elements of Z^* that fix $\mu \cap K$ pointwise are exactly those that are 1 mod wZ. Therefore $Z^* \cap (1 + wZ)$ is equal to $\mathrm{Aut}_{\mu \cap K}(\mu)$.

To conclude, recall that Γ is defined as the image of the restriction homomorphism $\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}(\mu)$. Since $\bar{\mathbf{F}}_p$ equals $\mu \cup \{0\}$, this map factors via the Galois group $\mathrm{Gal}(\bar{\mathbf{F}}_p \cap K(\mu)/\bar{\mathbf{F}}_p \cap K) = \mathrm{Gal}(\bar{\mathbf{F}}_p/\bar{\mathbf{F}}_p \cap K)$.



The group $\mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$ is pro-cyclic, and is generated by Frob_p. It has $H = \mathrm{Gal}(\bar{\mathbf{F}}_p/\bar{\mathbf{F}}_p \cap K)$ as a subgroup. Because $\bar{\mathbf{F}}_p \cap K$ is the union of its finite subfields, we have

$$H = \bigcap_{\substack{\mathbf{F}_{p^m} \subset K \\ m \in \mathbf{Z}_{\geq 1}}} \mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_{p^m}).$$

Recall that we defined the Steinitz number $a \in \mathcal{S}$ by

$$\forall m \in \mathbf{Z}_{\geq 1} : \ m \mid a \Leftrightarrow \mathbf{F}_{p^m} \subset K.$$

Since $\mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_{p^m})$ is generated by $(\mathrm{Frob}_p)^m$, we can then conclude that H is generated by $(\mathrm{Frob}_p)^{a\hat{\mathbf{Z}}}$ and Γ by $p^{a\hat{\mathbf{Z}}}$. □

Chapter 4

Computing radical field degrees

4.1 Introduction

One application of entanglement as we defined it in the previous chapter is computing degrees of radical field extensions of the rationals, e.g., the degree of the field $\mathbf{Q}(\zeta_{12}, \sqrt[6]{6}, \sqrt[4]{-9})$ over $\mathbf{Q}$.

Radical expressions like $\mathbf{Q}(\sqrt[16]{-4})$ do not define a unique field: there are multiple choices for roots, and the fields they generate may not be equal. If we add sufficiently many roots of unity, then the generated field *is* uniquely defined, since all choices for each root differ by a root of unity. In this chapter we assume that our radical fields contain enough roots of unity, as made precise in the following Question.

Question 4.1. *Let $c_1, \ldots, c_k$ be non-zero integers, and $a_1, \ldots, a_k$ be integers greater than 1. How do we efficiently compute the degree over $\mathbf{Q}$ of*

$$K = \mathbf{Q}(\mu_{a_1}, \sqrt[a_1]{c_1}, \ldots, \mu_{a_k}, \sqrt[a_k]{c_k})?$$

Unfortunately, this question is (very likely) difficult to answer. Suppose we take only a single root, $\sqrt[d]{2}$, with d the product of two large — and unknown — primes p and q. Then K is $\mathbf{Q}(\mu_d, \sqrt[d]{2})$ with degree $d\varphi(d)$. Then obtaining the value of $d\varphi(d) = d(p-1)(q-1) = d(d+1-(p+q))$ allows us to easily solve p and q from the equations $p+q = d+1-\varphi(d)$ and $pq = d$. Answering Question 4.1 would therefore let us factor d, which is presumed to be hard.

We will instead give an algorithm answering a modified question:

Theorem 4.2. *There is a polynomial time algorithm that given non-zero integers $c_1, \ldots, c_k$, and $a_1, \ldots, a_k$ integers greater than 1, computes the degree of K over $\mathbf{Q}(\mu_d)$, where d is the least common multiple of $a_1, \ldots a_k$, and K is defined as*

$$K = \mathbf{Q}(\mu_{a_1}, \sqrt[a_1]{c_1}, \ldots, \mu_{a_k}, \sqrt[a_k]{c_k}).$$

This algorithm will be stated (proving the theorem) in Section 4.4, combining results from Sections 4.2 and 4.3.

Following Chapter 2, the basic ingredients will consist of computing an index of abelian groups, and the order of an entanglement group.

To this end, define the (Galois) radical extension B of $\mathbf{Q}^*$ as follows:

$$B = \langle \mathbf{Q}^*, \mu_d, \sqrt[a_i]{c_i} : i \in \{1, \ldots, k\} \rangle \subset \bar{\mathbf{Q}}^*.$$

Let $E(B)$ be the entanglement group of B with the action of the absolute Galois group G of $\mathbf{Q}$, as defined by Definition 2.26. In Section 4.4 we will prove and use the following proposition.

Proposition 4.3. *With notation as above, the following equality holds:*

$$[K : \mathbf{Q}(\mu_d)] = \frac{[B : \mathbf{Q}^* \mu_d]}{\#E(B)}$$

The next two sections cover the computation of the factors in this fraction.

4.2 Coprime bases

We start by computing the index $[B : \mathbf{Q}^* \mu_d]$ of abelian groups. This is essentially a matter of $\mathbf{Z}$-linear algebra computation, once we have identified a basis to work with. Factoring all involved numbers into primes would suffice, but is computationally prohibitive. A suitable basis is provided by the following theorem due to D.J. Bernstein.

Theorem 4.4. *(D.J. Bernstein, [3, 4]) There is an algorithm with (up to* log *factors) linear run time that given a finite set $X \subset \mathbf{Z}_{>0}$, computes a set $\mathcal{P} \subset \mathbf{Z}_{>1}$ of pairwise coprime positive integers, none of which are perfect powers, as well as a factorization of each element of X as a product of elements of $\mathcal{P}$.*

We call a set $\mathcal{P}$ that satisfies these properties a *reduced coprime basis* for X. In this chapter, we take $\mathcal{P}$ to be the reduced coprime basis of the set consisting of 2, d, all a_i and all c_i. Define M to be the abelian group

$$M = \langle \mathbf{Q}^*, \zeta_{2d}, \sqrt[d]{p} : p \in \mathcal{P} \rangle / \mathbf{Q}^*.$$

Lemma 4.5. *Let d, $\mathcal{P}$ and M be as above. Then the abelian group M is a free (multiplicative) $\mathbf{Z}/d\mathbf{Z}$-module with basis $\{\zeta_{2d}, \sqrt[d]{p} : p \in \mathcal{P}\}$.*

Proof. The $\mathbf{Z}$-module M has exponent d, so it is a $\mathbf{Z}/d\mathbf{Z}$-module, and the set $\{\zeta_{2d}, \sqrt[d]{p} : p \in \mathcal{P}\}$ is clearly a generating set.

To show they form a basis, suppose a linear combination $\zeta_{2d}^{e_\zeta} \prod_{p \in \mathcal{P}} (\sqrt[d]{p})^{e_p} = x$ is an element of $\mathbf{Q}^*$. Taking the dth power, we find $\prod_{p \in \mathcal{P}} p^{e_p}$ equals $(-1)^{e_\zeta} x^d$.

Since the right-hand side is plus or minus a d-th power, the order of all prime factors of the right-hand side is a multiple of d. Since all $p \in \mathcal{P}$ are pairwise coprime and no perfect powers, this implies the exponents e_p are multiples of d too.

We obtain that $\prod_{p\in\mathcal{P}}(\sqrt[d]{p})^{e_p}$ is an element of $\mathbf{Q}$, so $\zeta_{2d}^{e_\zeta}$ is also in $\mathbf{Q}$, from which we see that e_ζ is also a multiple of d. This shows that the set $\{\zeta_{2d}, \sqrt[d]{p} : p \in \mathcal{P}\}$ is $\mathbf{Z}/d\mathbf{Z}$-linearly independent. □

Determining the index $[B : \mathbf{Q}^*\mu_d]$ can be conveniently done via M if every $|c_i|$ can be factored over $\mathcal{P}$. Specifically, define $s_i \in \{0, 1\}$ and $a_{p,i} \in \mathbf{Z}$ such that $c_i = (-1)^{s_i} \prod_{p\in\mathcal{P}} p^{e_{p,i}}$.

Let $\psi : M \longrightarrow (\mathbf{Z}/d\mathbf{Z})^{1+\#\mathcal{P}}$ be the $\mathbf{Z}/d\mathbf{Z}$-module isomorphism that sends $m \in M$ to its sequence of coordinates on the basis given by the lemma.

The coordinate vectors of the generators of $B/\mathbf{Q}^*$ are given by:

$$\begin{aligned} \psi(\zeta_d) &= (2, (0)_{p\in\mathcal{P}}) \\ \psi(\sqrt[a_i]{c_i}) &= \left(\frac{s_i d}{a_i}, \left(\frac{e_{p,i} d}{a_i}\right)_{p\in\mathcal{P}}\right) \end{aligned} \tag{4.6}$$

Theorem 4.7. *Let $\mathcal{P}$, M and ψ be as above. Then we have*

$$[B : \mathbf{Q}^*\mu_d] = \frac{(2, d)\#\psi(B/\mathbf{Q}^*)}{d}.$$

Proof. This follows from the existence of the isomorphism from Lemma 4.5. The index $[B : \mathbf{Q}^*\mu_d]$ is equal to $[B : \mathbf{Q}^*]/[\mathbf{Q}^*\mu_d : \mathbf{Q}^*]$. The index in the denominator only depends on d, and equals d if d is odd, and $d/2$ if d is even. □

Since we have explicitly written $B/\mathbf{Q}^*$ on a basis of M, we can now compute the index efficiently, using for example the methods from [8].

4.3 Entanglement

For computing the size of the entanglement group $E(B)$, we recall that $E(B)$ is equal to $E(B_{\text{ab}})$ (Corollary 2.27), where B_{ab} is defined as

$$B_{\text{ab}} = \{x \in B : \exists w \in \mathbf{Z}_{>0} : x^w \in B_{\text{tors}}B^G \text{ and } B^G \text{ has an element of order } w\}.$$

Since $B^G = \mathbf{Q}^*$ has exactly two roots of unity, $w = 2$ suffices and this definition reduces to

$$B_{\text{ab}} = \{x \in B : x^2 \in B_{\text{tors}}\mathbf{Q}^*\}. \tag{4.8}$$

If d is odd, then for all $x \in B_{\text{ab}}$, both x^2 and x^d are contained in $B_{\text{tors}}\mathbf{Q}^*$, so B_{ab} is in fact equal to $\mathbf{Q}^*B_{\text{tors}}$. This has no entanglement since every automorphism of $\mathbf{Q}^*B_{\text{tors}}$ over $\mathbf{Q}^*$ extends uniquely to a field automorphism in $\text{Gal}(\mathbf{Q}(B_{\text{tors}})/\mathbf{Q})$.

In the rest of this section, we will therefore assume that d is even.

We turn to Corollary 2.31, which gives an explicit description in the case where B_{ab} is of the form μW where μ consists of roots of unity and W is Kummer. The

group B_{ab} cannot always be written in this form, but as we shall see, that is always possible if we slightly enlarge B by adding the $2d$-th roots of unity:

$$B' = \mu_{2d}B = \langle \mathbf{Q}^*, \mu_{2d}, \sqrt[a_i]{c_i} : i \in \{1, \ldots, k\} \rangle \subset \bar{\mathbf{Q}}^*.$$

Since $B'/\mathbf{Q}^*$ has exponent d, the torsion subgroup of B' is contained in μ_{2d} and therefore equal to it. We can now compute B'_{ab}.

Proposition 4.9. *With B' defined as above, B'_{ab} is equal to $\mu_{2d}(\sqrt{\mathbf{Q}^*} \cap B')$, with $\sqrt{\mathbf{Q}^*} = \{x \in \bar{\mathbf{Q}}^* : x^2 \in \mathbf{Q}\}$.*

Proof. Analogously to Equation 4.8, we have

$$B'_{\mathrm{ab}} = \{x \in B' : x^2 \in B'_{\mathrm{tors}}\mathbf{Q}^*\} = \{x \in B' : x^2 \in \mu_{2d}\mathbf{Q}^*\}.$$

It is clear that $\mu_{2d}(\sqrt{\mathbf{Q}^*} \cap B')$ is contained in B'_{ab}. For the opposite inclusion, suppose that x is an element of B'_{ab}. Then we have $x \in B'$ and $x^2 \in \mathbf{Q}^*\mu_{2d}$. Then x^2 can be written as $x^2 = \zeta b$ with $b \in \mathbf{Q}^*$ and $\zeta \in \mu_{2d}$. Taking d-th powers, we get $\zeta^d = \frac{x^{2d}}{b^d} \in (\mathbf{Q}^*)^2$ because d is even. Since ζ^d is now in $(\mathbf{Q}^*)^2$ and in μ_2, we can conclude that ζ^d is 1, so ζ is a d-th root of unity. Since now $x^2 \in \mu_d\mathbf{Q}^*$, we find that $x \in \mu_{2d}\sqrt{\mathbf{Q}^*}$. This proves the claim. □

Following the notation from Corollary 2.31, we will now write $\mu = \mu_{2d}$ and $W = \sqrt{\mathbf{Q}^*} \cap B'$ so that $B'_{\mathrm{ab}} = \mu W$.

Note that Corollary 2.31 allows an amount of freedom in how to distribute elements that are both roots of unity and Kummer roots. In the definition of μ and W above, we have chosen to add these roots of unity to both μ and W.

Proposition 4.10. *With $G_\mu = \ker(G \to \mathrm{Aut}(\mu))$, we have*

$$\begin{aligned} E(\mu) &= 1, \text{ and} \\ E(B') &\cong \mathrm{Aut}_{\mathbf{Q}^* \cdot \langle i \rangle}(W^{G_\mu}). \end{aligned}$$

Proof. Each group automorphism of $\mathrm{Aut}(\mu)$ can be uniquely extended to a field automorphism in $\mathrm{Gal}(\mathbf{Q}(\mu)/\mathbf{Q})$, so $\mathrm{Gal}(\mathbf{Q}(\mu)/\mathbf{Q}) \cong \mathrm{Aut}(\mu)$ and $E(\mu)$ is trivial.

Because of that, Corollary 2.31 leads to

$$E(B') \cong \mathrm{Aut}_{W^G \cdot (\mu \cap W)}(W^{G_\mu}).$$

Since W^G is $\mathbf{Q}^*$ and $\mu \cap W$ is $\langle i \rangle$, the statement follows. □

Using this expression, we can find the order of $E(B')$ by a computation inside $M[2]$, where M (and $\mathcal{P}$) are the objects defined in the previous section. To determine W^{G_μ} we need to look at how G_μ acts on W.

Lemma 4.11. *For a positive integer k that can be factored over $\mathcal{P}$, the intersection $M_k = (\mathbf{Q}(\mu_k)^*/\mathbf{Q}^*) \cap M[2]$ has $\mathbf{F}_2$-basis*

$$\mathcal{B} = \{\sqrt{-1} \text{ if } 4 \mid k\} \cup \{\sqrt{p^*} : p \in \mathcal{P} \text{ with } p^* \mid k\},$$

where $2^* = 8$ and $p^* = \pm p \equiv 1 \bmod 4$ for odd $p \in \mathcal{P}$.

Proof. First of all, note that elements of the reduced coprime basis $\mathcal{P}$ are by definition either 2 or odd, so p^* is properly defined for all $p \in \mathcal{P}$.

For primes q it is well-known that $\sqrt{q^*}$ is an element of $\mathbf{Q}(\mu_{|q^*|})$. On odd integers, both reduction mod 4 and taking square roots (up to the sign of the root) are strictly multiplicative, so for $p = 2$ as well as for p odd, $\sqrt{p^*}$ is an element of $\mathbf{Q}(\mu_{|p^*|})$. Also, $\sqrt{-1}$ is in $\mathbf{Q}(\mu_4)$, so $\mathcal{B}$ is contained in M_k. Since elements of $\mathcal{P}$ are coprime, $\mathcal{B}$ is also $\mathbf{F}_2$-linearly independent.

To see that $\mathcal{B}$ generates M_k, consider an element $\sqrt{x} \in M_k$. We can choose the representative in such a way that x is a product of distinct elements of $\mathcal{P} \cup \{-1\}$. Choose an element $p \in \mathcal{P}$ that divides x, and suppose that p^* does not divide k. Let $l \mid p$ then be a prime number with $\mathrm{ord}_l(p)$ odd. (Such a prime l exists because p is not a perfect power.) Then $\mathbf{Q}(\sqrt{x})$ is ramified at l, while $\mathbf{Q}(\mu_k)$ is not, so $\sqrt{x}$ is not an element of M_k, leading to a contradiction. This shows that $\sqrt{x}$ or $\sqrt{-x}$ (or both) are in $\langle \mathcal{B} \rangle$.

If we have $4 \mid k$, then both $\sqrt{x}$ and $\sqrt{-x}$ are elements of $\langle \mathcal{B} \rangle$, and we are done. If on the other hand we have $4 \nmid k$, then only one of $\sqrt{x}$ and $\sqrt{-x}$ is in M_k, and therefore we conclude $\sqrt{x} \in \langle \mathcal{B} \rangle$. □

Proposition 4.12. *We have* $W^{G_\mu} = W \cap \mathbf{Q}(\mu_{2d})$ *and* $W^{G_\mu}/\mathbf{Q}^* = (W/\mathbf{Q}^*) \cap M_{2d}$.

Proof. By definition, G_μ is the kernel of the map $G \to \mathrm{Aut}(\mu)$, so in this setting it is $\mathrm{Gal}(\mathbf{Q}(B)/\mathbf{Q}(\mu_{2d}))$. The subgroup of W invariant under G_μ is then $W \cap \mathbf{Q}(\mu_{2d})$.

Since $W/\mathbf{Q}^*$ is contained in $M[2]$, we find $(W/\mathbf{Q}^*) \cap \mathbf{Q}(\mu_{2d})/\mathbf{Q}^* = (W/\mathbf{Q}^*) \cap ((\mathbf{Q}(\mu_{2d})/\mathbf{Q}^*) \cap M[2]) = (W/\mathbf{Q}^*) \cap M_{2d}$. □

For the actual explicit computations, we start by taking the intersection of $B'/\mathbf{Q}^*$ and $M[2]$ inside M to get a basis for the $\mathbf{F}_2$-module $(B'/\mathbf{Q}^*) \cap M[2] = ((B'/\mathbf{Q}^*) \cap (\sqrt{\mathbf{Q}^*}/\mathbf{Q}^*)) \cap M[2] = W/\mathbf{Q}^*$. Since we then have an explicit basis for $W/\mathbf{Q}^*$ and M_{2d} inside $M[2]$, we can now compute the order of their intersection, and then also that of $E(B')$.

Theorem 4.13. *The order of the entanglement group of* B' *is given by*

$$\#E(B') = \frac{1}{2}\#\mathrm{Hom}(W^{G_\mu}/\mathbf{Q}^*, \mu_2) = \frac{1}{2}\#(W^{G_\mu}/\mathbf{Q}^*).$$

Proof. Since $\langle \mathbf{Q}^*, \sqrt{\mathcal{P}}, i \rangle$ is a Kummer extension over $\mathbf{Q}^*$, there is an isomorphism $\mathrm{Aut}_{\mathbf{Q}^*}(\langle \mathbf{Q}^*, \sqrt{\mathcal{P}}, i \rangle) \to \mathrm{Hom}(\langle \mathbf{Q}^*, \sqrt{\mathcal{P}}, i \rangle/\mathbf{Q}^*, C_2) = M[2]^\vee$.

This isomorphism induces the three isomorphisms $\mathrm{Aut}_{\mathbf{Q}^*}(W) \cong (W/\mathbf{Q}^*)^\vee$, and $\mathrm{Aut}_{\mathbf{Q}^*}(W^{G_\mu}) \cong (W^{G_\mu}/\mathbf{Q}^*)^\vee$, and $\mathrm{Aut}_{\mathbf{Q}^* \cdot \langle i \rangle}(W^{G_\mu}) \cong (W^{G_\mu}/(\mathbf{Q}^* \cdot \langle i \rangle))^\vee$.

The order of this last dual is half the order of $(W^{G_\mu}/\mathbf{Q}^*)^\vee$, due to the added subgroup $\langle i \rangle$. Proposition 4.10 then gives the desired equality. □

To compute $\#E(B)$, we need to determine if the step from B to B' introduced extra entanglement. The following theorem gives a sufficient and necessary condition for this.

Theorem 4.14. *We have*

$$\#E(B) = \#E(B') \cdot \begin{cases} \frac{1}{2} & \text{if } \mu_{2d} \not\subset B \text{ and } (W^{G_\mu} \cap B)/\mathbf{Q}^* \neq (W/\mathbf{Q}^*) \cap M_d \\ 1 & \text{otherwise.} \end{cases}$$

Proof. If B equals B', we are of course done. So, assume that ζ_{2d} is not in B. Then we have $[B' : B] = 2$ and the kernel of the natural restriction map $\mathrm{Aut}_{\mathbf{Q}^*}(B') \twoheadrightarrow \mathrm{Aut}_{\mathbf{Q}^*}(B)$ equals $\mathrm{Aut}_B(B')$ and therefore contains exactly one non-trivial automorphism σ. The induced surjection $E(B') \twoheadrightarrow E(B)$ has a kernel generated by the image of σ, and it has order at most 2.

We can determine the order of this kernel by checking if σ maps to 1 in $E(B')$. There is no entanglement in extensions generated by roots of unity over $\mathbf{Q}$ (by Proposition 4.10), so we can use Corollary 2.31 for this.

In this corollary we have seen that the entanglement group $E(B')$ is isomorphic to $\mathrm{Aut}_{W^G(\mu \cap W)}(W^{G_\mu})$ and that the corresponding homomorphism from $\mathrm{Aut}_{\mathbf{Q}^*}(B')$ to $\mathrm{Aut}_{W^G(\mu \cap W)}(W^{G_\mu})$ sends σ to $\sigma|_{W^{G_\mu}}(g|_{W^{G_\mu}})^{-1}$ for any $g \in G$ with $\sigma|_\mu = g|_\mu$. To check if σ maps to 1 in $E(B)$ we can therefore check if g and σ have the same restriction to W^{G_μ}.

Since σ has order 2, and $g|_\mu = \sigma|_\mu$, the restriction $g|_{W^{G_\mu}}$ has order at most 2. We then have for all $x \in W^{G_\mu}$ that $gx, \sigma x \in \{\pm 1\}x$. Therefore, the automorphisms $\sigma|_{W^{G_\mu}}$ and $g|_{W^{G_\mu}}$ are equal if and only if they have the same groups of invariants.

The automorphism $\sigma|_{W^{G_\mu}}$ has group of invariants $W^{G_\mu} \cap B$, since we have $B = (B')^{\langle \sigma \rangle}$.

Since we have $g|_\mu = \sigma|_\mu$, the invariant field $\mathbf{Q}(\mu_{2d})^{\langle g \rangle}$ equals $\mathbf{Q}(\mu_d)$. The restriction $g|_{W^{G_\mu}}$ therefore has group of invariants $\mathbf{Q}(\mu_d) \cap W^{G_\mu} = \mathbf{Q}(\mu_d)^* \cap W$.

The image of σ in $E(B)$ therefore equals 1, if and only if the two submodules $(W^{G_\mu} \cap B)/\mathbf{Q}^*$ and $(W/\mathbf{Q}^*) \cap M_d$ of $M[2]$ are equal. The image of σ in $E(B)$ has order 2 otherwise. □

Combining the previous two theorems directly gives the following result for the order of $E(B)$.

Corollary 4.15. *The order of the entanglement group of B is given by*

$$\#E(B) = \#(W^{G_\mu}/\mathbf{Q}^*) \cdot \begin{cases} \frac{1}{4} & \text{if } \mu_{2d} \not\subset B \text{ and } (W^{G_\mu} \cap B)/\mathbf{Q}^* \neq (W/\mathbf{Q}^*) \cap M_d \\ \frac{1}{2} & \text{otherwise.} \end{cases}$$

Since we have already determined explicit bases for all modules in the condition of this corollary, computing the order of $E(B)$ from $\#(W^{G_\mu}/\mathbf{Q}^*)$ is a straightforward $\mathbf{F}_2$-linear algebra computation.

4.4 Field degrees

We will complete the proof of Theorem 4.2 in this section.

We recall the definition of the radical extension B of $\mathbf{Q}^*$:

$$B = \langle \mathbf{Q}^*, \mu_d, \sqrt[a_i]{c_i} : i \in \{1, \ldots, k\} \rangle.$$

Proof of proposition 4.3. Since B is a Galois radical group over $\mathbf{Q}^*$ by construction, Theorem 2.25 shows that B — with the Galois action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ — has an entanglement group $E(B)$. Recall that in this case, $E(B)$ is the cokernel of the natural embedding of $\mathrm{Gal}(\mathbf{Q}(B)/\mathbf{Q})$ into $\mathrm{Aut}_{\mathbf{Q}^*}(B)$.

We find

$$[\mathbf{Q}(B) : \mathbf{Q}(\mu_d)] = \frac{[\mathbf{Q}(B) : \mathbf{Q}]}{\varphi(d)} = \frac{\#\mathrm{Aut}_{\mathbf{Q}^*}(B)}{\varphi(d)\#E(B)}.$$

Using Theorem 2.19 we conclude

$$\begin{aligned}[\mathbf{Q}(B) : \mathbf{Q}(\mu_d)] &= \frac{[B : \mathbf{Q}^*]}{\varphi(d)\#E(B)} \prod_{\substack{p \text{ prime} \\ B[p] \neq \mathbf{Q}^*[p]}} \frac{p-1}{p} \\ &= \frac{[B : \mathbf{Q}^*\mu_d] \cdot [\mathbf{Q}^*\mu_d : \mathbf{Q}^*]}{(d/2) \cdot \#E(B)} = \frac{[B : \mathbf{Q}^*\mu_d]}{\#E(B)}.\end{aligned}$$

□

Proof of Theorem 4.2. The previous two sections show how to compute the quantities $[B : \mathbf{Q}^*\mu_d]$ and $\#E(B)$ in this fraction in the required time. Combining these statements yields Algorithm 4.16 to compute $[\mathbf{Q}(B) : \mathbf{Q}(\mu_d)]$.

This algorithm runs in time polynomial in the input. The computation and factoring over the co-prime basis is polynomial time due to Theorem 4.4. Computing the intersections and equality inside $M[2]$ is basic linear algebra over $\mathbf{F}_2$ with matrix sizes linear in the input size.

Finally, evaluating the expression from Theorem 4.7 involves computing an order of a $\mathbf{Z}/d\mathbf{Z}$-module D, where the generators of D are written on a basis of the free $\mathbf{Z}/d\mathbf{Z}$-module M of rank, say, r. The computation of this order can be performed by dividing d^r by the index of $((d\mathbf{Z})^r + D)$ inside $\mathbf{Z}^r$. Since both the number of generators of D and the size of each coefficient are linear in the size of the input, this index can be computed in polynomial time, using for example the methods from [8]. □

Algorithm 4.16.

1. Determine a coprime base $\mathcal{P}$ for the set consisting of 2, all a_i, and all c_i and factor all these numbers over $\mathcal{P}$.
2. Compute $d = \operatorname{lcm}\{a_i\}$ using this factorization.
3. Define the $\mathbf{Z}/d\mathbf{Z}$-module M as in Lemma 4.5.
4. Use Equation 4.6 and Theorem 4.7 to compute $[B : \mathbf{Q}^*\mu_d]$.
5. If d is odd, then $\#E(B) = 1$. Proceed with step 10.
6. Use Lemma 4.11 to find $\mathbf{F}_2$-bases of M_d and M_{2d} inside $M[2]$.
7. Use Proposition 4.12 to find $W^{G_\mu}/\mathbf{Q}^*$ by computing $(W/\mathbf{Q}^*) \cap M_{2d}$ inside $M[2]$.
8. Compute the intersections $(W^{G_\mu} \cap B)/\mathbf{Q}^*$ and $(W/\mathbf{Q}^*) \cap M_d$ inside $M[2]$.
9. Use Corollary 4.15 to compute $\#E(B)$.
10. Finally, use Proposition 4.3 to compute $[\mathbf{Q}(B) : \mathbf{Q}(\mu_d)]$.

Example 4.17.

Consider $K = \mathbf{Q}(\mu_{12}, \sqrt[6]{6}, \sqrt[4]{-9})$, or, equivalently

$$K = \mathbf{Q}\left(\mu_{12},\ \sqrt[12]{6^2},\ \sqrt[12]{-3^6}\right).$$

Using the notation from throughout this chapter, we get $d = 12$ and

$$B = \left\langle \mathbf{Q}^*, \mu_{12},\ \sqrt[12]{6^2},\ \sqrt[12]{-3^6} \right\rangle.$$

The coprime base for the numbers involved necessarily consists of actual primes in this case: $\mathcal{P} = \{2, 3\}$. This means that the free $\mathbf{Z}/d\mathbf{Z}$-module M is given by

$$M = \left\langle \mathbf{Q}^*, \mu_{24},\ \sqrt[12]{2},\ \sqrt[12]{3} \right\rangle \Big/ \mathbf{Q}^*.$$

Inside this module, we compute the index $[B : \mu_{12}\mathbf{Q}^*]$. On the (ordered) basis $(\zeta_{24},\ \sqrt[12]{2},\ \sqrt[12]{3})$, the submodule $\mu_{12}\mathbf{Q}^*$ is generated by $\langle(2,0,0)\rangle$ and B by $\langle(2,0,0),(0,2,2),(1,0,6)\rangle$. Adding $3 \cdot (0,2,2)$ to $(1,0,6)$ results in a basis for B in triangular form:

$$B = \langle(2,0,0),(1,6,0),(0,2,2)\rangle.$$

From this we see that $[B : \mu_{12}\mathbf{Q}^*]$ equals $(12/6) \cdot (12/2) = 12$.

We continue with the entanglement group computation, starting with $E(B')$ for $B' = \langle B, \mu_{24} \rangle$. This takes place in the 2-torsion of M:

$$M[2] = \left\langle \sqrt{-1}, \sqrt{2}, \sqrt{3} \right\rangle.$$

Since $\sqrt{-1}$, $\sqrt{2}$ and $\sqrt{3}$ are all contained in $\mathbf{Q}(\mu_{24})$, the intersection $M_{24} = M[2] \cap (\mathbf{Q}(\mu_{24})^*/\mathbf{Q}^*)$ actually equals $M[2]$. The three roots $\sqrt{-1}$, $\sqrt{2}$ and $\sqrt{3}$ are also all contained in B', so $W^{G_\mu}/\mathbf{Q}^* = M_{24} \cap (W/\mathbf{Q}^*) = M_{24} \cap B'$ also equals $M[2]$.

As an aside, according to Theorem 4.13 the order of $E(B')$ is half that of $W^{G_\mu}/\mathbf{Q}^*$, so we have $\#E(B') = 4$. To compute the size of $E(B)$ from this, we need to determine if $(W^{G_\mu} \cap B)/\mathbf{Q}^*$ equals $(W/\mathbf{Q}^*) \cap M_{12}$. Since $\sqrt{3}$ is not in B, it is not in the former module, while it is in the latter, so they are not equal, and $\#E(B) = 8 \cdot \frac{1}{4} = 2$.

This leads us to the conclusion

$$\left[\mathbf{Q}\left(\mu_{12}, \sqrt[6]{6}, \sqrt[4]{-9}\right) : \mathbf{Q}\right] = \varphi(12) \cdot \frac{12}{2} = 24.$$

Chapter 5

Near-primitive roots and higher rank

5.1 Introduction

In this chapter we generalize the results from Chapter 1 to a broader setting.

Let K be a number field, and let $V \subset K^*$ be a finitely generated subgroup with $\mathrm{rank}(V/V_{\mathrm{tors}}) \geq 1$ and t a positive integer. We consider the set $M = M(K, V, t)$ of primes $\mathfrak{q}$ of K satisfying:

- $\mathrm{ord}_{\mathfrak{q}}(v) = 0$ for all $v \in V$, and
- $[(\mathcal{O}_K/\mathfrak{q})^* : \bar{V}] \mid t$.

This is a special case of the broader context considered by H.W. Lenstra [18]. If we take V to be generated by a single element, this element is called a *near-primitive root* modulo the primes $\mathfrak{q}$ satisfying the conditions. Over the rationals, these densities have previously been computed; see Wagstaff [35] and Moree [23].

If on the other hand we take $t = 1$, but V generated by multiple elements, this leads to higher rank analogues of Artin's conjecture. For $K = \mathbf{Q}$, this topic has been treated by Cangelmi and Pappalardi [6], and is covered in a way very similar to the approach in this chapter by Moree and Stevenhagen [24].

The work of Cooke and Weinberger [9] shows that the set $M(K, V, t)$ has a natural density under the appropriate generalized Riemann hypotheses.

First of all, note that the set of primes $\mathfrak{q}$ not satisfying the first condition is finite, since V is finitely generated. After all, it is sufficient to check this condition for a set of generators of V.

Following the same strategy as in Chapter 1, we will see that the second condition can also be translated to splitting conditions on radical extension fields of K.

Specifically, for a (rational) prime p, let $e(p)$ be the smallest positive integer such that $p^{e(p)}$ does not divide t, and define the radical extensions

$$K^* \subset B_p = \langle K^*, \mu_{p^{e(p)}}, \sqrt[p^{e(p)}]{V} \rangle.$$

Here $\sqrt[p^{e(p)}]{V}$ denotes the group of all elements x in a fixed algebraic closure $\bar{K}$ of K that satisfy $x^{p^{e(p)}} \in V$. Let B be the abelian group generated by all B_p, and let $E = E(B)$ be its entanglement group with respect to the action of the absolute Galois group of K.

Theorem 5.1. *The entanglement group $E = E(B)$ of B is finite.*

As $A = \mathrm{Aut}_{K^*}(B)$ is naturally isomorphic to the product of all $A_p = \mathrm{Aut}_{K^*}(B_p)$ and E is finite, only a finite number of A_p have a non-trivial image in E. This ensures that the (a priori infinite) product in the correction factor formula below is in fact a finite product.

Theorem 5.2. *Assuming GRH, the set $M(K, V, t)$ has a natural density equal to*

$$C(K, V, t) \cdot \prod_{p \text{ prime}} \left(1 - \frac{1}{\#A_p}\right),$$

where $C(K, V, t)$ is a rational correction factor given by

$$C(K, V, t) = \sum_{\chi \in E^\vee} \prod_{\substack{p \text{ prime} \\ \chi(A_p) \neq 1}} \frac{-1}{\#A_p - 1}.$$

We prove these two main theorems in the following section.

In this generality, the results from Chapter 1 no longer suffice to give explicit expressions for E and $\chi(A_p)$. In the remainder of the chapter we will address these issues, using the theory from Chapters 2 and 4.

5.2 Proof of main theorems

In this section we will prove Theorems 5.1 and 5.2. As in the introduction, let K be a number field, $V \subset K^*$ a finitely generated subgroup with $\mathrm{rank}(V/V_{\mathrm{tors}}) \geq 1$ and t a positive integer. We will consider the set $M = M(K, V, t)$ of primes $\mathfrak{q}$ of K satisfying:

- $\mathrm{ord}_{\mathfrak{q}}(v) = 0$ for all $v \in V$, and
- $[(\mathcal{O}_K/\mathfrak{q})^* : \bar{V}] \mid t$.

First of all, note that the set of primes $\mathfrak{q}$ not satisfying the first condition is finite, since V is finitely generated and it is sufficient to check this condition for a

set of generators of V. We will therefore only consider primes $\mathfrak{q}$ satisfying the first condition in the remainder of this section.

For the second condition, let $e(p)$ be the smallest positive integer such that $p^{e(p)}$ does not divide t. Then for a given prime $\mathfrak{q}$ of K, the index $[(\mathcal{O}_K/\mathfrak{q})^* : \bar{V}]$ divides t if and only if for all (rational) primes p the power $p^{e(p)}$ does not divide the index.

For a given prime p with $\mathfrak{q} \nmid p$, we have

$$p^{e(p)} \mid [(\mathcal{O}_K/\mathfrak{q})^* : \bar{V}]$$

if and only if

$$p^{e(p)} \mid (N\mathfrak{q} - 1) \text{ and all elements of } \bar{V} \text{ are } p^{e(p)}\text{-th powers in } \mathcal{O}_K/\mathfrak{q}$$

if and only if

$$\mathfrak{q} \text{ splits completely in } K \subset K(\zeta_{p^{e(p)}}, \sqrt[p^{e(p)}]{V}).$$

We conclude that, up to a finite number, the set of primes $M(K, V, t)$ we are interested in is the set of primes $\mathfrak{q}$ of K that do not split completely in any of the extensions $K \subset K_p = K(\zeta_{p^{e(p)}}, \sqrt[p^{e(p)}]{V})$ with $\mathfrak{q} \nmid p$.

As in Chapter 1, for each individual rational prime p the density of primes satisfying this condition has a simple expression given by the Chebotarëv density theorem:

$$1 - \frac{1}{[K_p : K]}.$$

Moreover, we can again combine these conditions at finitely many different primes p by looking at the splitting behaviour in the compositum.

If we take n to be a product of primes to consider, we define K_n to be the compositum of the fields K_p for the p dividing n. Also, we define G_n to be the Galois group $\mathrm{Gal}(K_n/K)$, and S_n as

$$S_n = \{\sigma \in G_n : \sigma \mid_{K_p} \neq \mathrm{id} \text{ for all } p \mid n\}.$$

Chebotarëv implies that the set of primes $\mathfrak{q}$ of K that do not split completely in any of the p dividing n has a density equal to the ratio $\#S_n/\#G_n$.

The results of Cooke and Weinberger [9] also apply in this generality, and show that if we assume the Generalized Riemann Hypothesis (GRH) for the fields K_n, the primes in M have a natural density of

$$\lim_{n\to\infty} \frac{\#S_n}{\#G_n}.$$

In this limit the positive integers n are ordered by divisibility.

We will compute these quotients using the tools of radical group extensions and entanglement developed in the previous chapters. To that end, recall from the introduction in this chapter the definition of the radical extensions $K^* \subset B_p$:

$$B_p = \left\langle K^*, \mu_{p^{e(p)}}, \sqrt[p^{e(p)}]{V} \right\rangle.$$

Also, as before, for a positive integer n, we write B_n for the abelian group generated by all B_p for primes $p \mid n$, and B for the abelian group generated by *all* B_p.

A key ingredient in the derivation of the conjectured Artin densities in this chapter is the finiteness of the entanglement group of B with the action of the absolute Galois group of K, which is provided by Theorem 5.1 and which we prove here.

Proof of Theorem 5.1. Recall from Chapter 2 that $E(B)$ equals $E(B_{\mathrm{ab}})$, so it suffices to show that $E(B_{\mathrm{ab}})$ is finite.

Write w for the number of roots of unity in K, and define the integer n as the product of all primes p satisfying

$$p \mid w\Delta_{K/\mathbf{Q}}.$$

We aim to separate the n-part from the non-n-part of B_{ab}, which we will make precise below. To this end, note that B_{ab}/K^* is torsion, so it is the direct sum of its p-parts, for which we write $(B_{\mathrm{ab}})_p/K^*$. For a prime p, this subgroup $(B_{\mathrm{ab}})_p$ consists of the radicals in B_{ab} of p-power order mod K^*. In our current setting, those correspond exactly to the elements of B_{ab} that are also in B_p. Furthermore, by Proposition 2.23 we see that $B_p \cap B_{\mathrm{ab}}$ equals $(B_p)_{\mathrm{ab}}$. We conclude that

$$B_{\mathrm{ab}}/K^* = \bigoplus_{p \text{ prime}} (B_p)_{\mathrm{ab}}/K^*.$$

For any prime p, the group $(B_p)_{\mathrm{ab}}$ as defined in Section 2.5 is given by

$$(B_p)_{\mathrm{ab}} = \{x \in B_p : x^w \in \mu_{p^{e(p)}}K^*\}.$$

If p is a prime not dividing w, then we have that for any $x \in (B_p)_{\mathrm{ab}}$, the order of $\bar{x}$ in B_p/K^* is coprime with w. Therefore $x^w \in \mu_{p^{e(p)}}K^*$ is equivalent to $x \in \mu_{p^{e(p)}}K^*$. We obtain that

$$p \nmid w \Rightarrow (B_p)_{\mathrm{ab}} = \mu_{p^{e(p)}}K^*. \tag{5.3}$$

Now write $C_n = (B_n)_{\mathrm{ab}}$ and, since primes not dividing n in particular do not divide w, define C_n' as

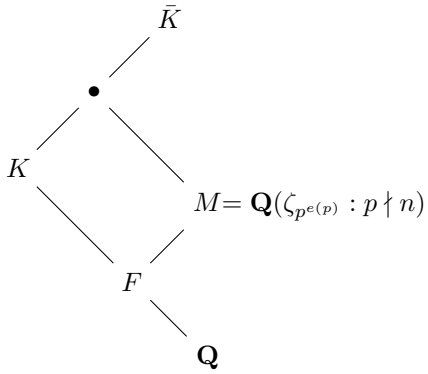
$$C_n' = \langle K^*, \zeta_{p^{e(p)}} : p \nmid n\rangle.$$

This allows us to decompose B_{ab} as a fibered sum over K^*

$$B_{\mathrm{ab}} = C_n \oplus_{K^*} C_n',$$

and $\mathrm{Aut}_{K^*}(B_{\mathrm{ab}})$ as

$$\mathrm{Aut}_{K^*}(B_{\mathrm{ab}}) = \mathrm{Aut}_{K^*}(C_n) \times \mathrm{Aut}_{K^*}(C_n'). \tag{5.4}$$



We write $M = \mathbf{Q}(\zeta_{p^{e(p)}} : p \nmid n)$. Consider the following restriction map:

$$\varphi : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Gal}(M/\mathbf{Q}).$$

The invariant field F of the image of φ is given by the intersection $K \cap M$. The extension $F/\mathbf{Q}$ is then unramified at primes $p \nmid n$ since $K/\mathbf{Q}$ is unramified there. Also, $F/\mathbf{Q}$ is unramified at primes $p \mid n$ since $M/\mathbf{Q}$ is unramified there. We conclude that $F/\mathbf{Q}$ is unramified at all primes, so F is equal to $\mathbf{Q}$.

Therefore $\mathrm{Gal}(\bar{K}/K)$ maps surjectively to the Galois group of M over $\mathbf{Q}$, which is in turn naturally isomorphic to $\mathrm{Aut}_{K^*}(C_n')$.

Furthermore, the factor $\mathrm{Aut}_{K^*}(C_n)$ of $\mathrm{Aut}_{K^*}(B_{\mathrm{ab}})$ is finite, so the image of $\mathrm{Gal}(\bar{K}/K)$ in $\mathrm{Aut}_{K^*}(B_{\mathrm{ab}})$ is of finite index. □

Since $E(B)$ is finite, we know there is an integer n such that $E(B)$ equals $E(B_n)$. In fact, with some extra work we can extend the strategy followed in the above proof to give an explicit sufficient condition for such n. While it is not strictly necessary for Theorem 5.2, we already give the proof here since it builds directly on the previous arguments.

Theorem 5.5. *Again write w for the number of roots of unity in K, and let n be a positive integer divisible by all primes p satisfying*

$$p \mid w\Delta_{K((B_w)_{\mathrm{ab}})/\mathbf{Q}}.$$

Then the natural map $E(B) \to E(B_n)$ is an isomorphism.

Proof. Define C_n and C_n' analogously to how they were defined in the proof of Theorem 5.1 above: $C_n = (B_n)_{\mathrm{ab}}$ and

$$C_n' = \langle K^*, \zeta_{p^{e(p)}} : p \nmid n \rangle.$$

Because of Equation 5.3, we can see that

$$K(C_n) = K((B_n)_{\mathrm{ab}}) = K((B_w)_{\mathrm{ab}}, \zeta_{p^{e(p)}} : p \mid n) = K((B_w)_{\mathrm{ab}}) \cdot \mathbf{Q}(\zeta_{p^{e(p)}} : p \mid n).$$

All rational primes ramifying in $K((B_w)_{\mathrm{ab}})/\mathbf{Q}$ divide n by definition of n, and all rational primes ramifying in $\mathbf{Q}(\zeta_{p^{e(p)}} : p \mid n)/\mathbf{Q}$ also divide n. We conclude that $K(C_n)/\mathbf{Q}$ is unramified outside of the primes dividing n.

For brevity, define $M = \mathbf{Q}(\zeta_{p^{e(p)}} : p \nmid n)$. Proceeding entirely analogously to the reasoning in the proof of Theorem 5.1, the intersection $K(C_n) \cap M$ is now equal to $\mathbf{Q}$, and one can deduce from this that $\mathrm{Gal}(K(B_{\mathrm{ab}})/K(C_n))$ maps surjectively to the Galois group of M over $\mathbf{Q}$. This group is in turn naturally isomorphic to $\mathrm{Aut}_{K^*}(C_n')$.

We complete the proof assisted by the following diagram of abelian groups with exact rows and columns, where the first center vertical map is provided by Equation 5.4.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Gal}(K(B_{\mathrm{ab}})/K(C_n)) & \longrightarrow & \mathrm{Gal}(K(B_{\mathrm{ab}})/K) & \longrightarrow & \mathrm{Gal}(K(C_n)/K) & \longrightarrow & 0 \\
 & & \downarrow f & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Aut}_{K^*}(C_n') & \longrightarrow & \mathrm{Aut}_{K^*}(C_n) \times \mathrm{Aut}_{K^*}(C_n') & \longrightarrow & \mathrm{Aut}_{K^*}(C_n) & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & E(B_{\mathrm{ab}}) & \longrightarrow & E(C_n) & \longrightarrow & 0
\end{array}$$

Since the map $f : \mathrm{Gal}(K(B_{\mathrm{ab}})/K(C_n)) \to \mathrm{Aut}_{K^*}(C_n')$ is a surjection, the map from $E(B_{\mathrm{ab}}) \to E(C_n)$ is injective. It is also surjective, and since C_n is defined as $(B_n)_{\mathrm{ab}}$, this gives the equality claimed by the present Theorem. □

Now that we know the entanglement group is finite, we can proceed with the derivation of the conjectured density formula given by Theorem 5.2.

Proof of Theorem 5.2. The computation of the density with the correction factor in the form of a character sum can now continue as in Chapter 1.

Recall from the start of this section that we want to compute the limit

$$\lim_{n \to \infty} \frac{\#S_n}{\#G_n}.$$

To express this in terms of $A_n = \mathrm{Aut}_{K^*}(B_n)$ rather than in the Galois groups G_n, define T_n as follows.

$$T_n = \{\sigma \in A_n : \sigma|_{B_p} \neq \mathrm{id} \text{ for all } p \mid n\}.$$

This gives the equality $S_n = T_n \cap G_n$ inside A_n.

Now assume that n is an integer large enough to have $E = E(B) = E(B_n)$. (Refer to Theorem 5.5 for an explicit sufficient condition for this.) Then, because E is an abelian group, the characteristic function 1_{G_n} of G_n inside A_n is given by

$$1_{G_n}(s) = \frac{1}{\#E} \sum_{\chi \in E^\vee} \chi(s).$$

We apply this as follows.

$$\begin{aligned}\frac{\#S_n}{\#G_n} &= \frac{\#(T_n \cap G_n)}{\#G_n} = \frac{1}{\#E\#G_n}\sum_{s\in T_n} 1_{G_n}(s) \\ &= \frac{1}{\#A_n}\sum_{s\in T_n}\sum_{\chi\in E^\vee}\chi(s)\end{aligned}$$

We swap the order of the summations, and continue using the multiplicative structure of T_n.

$$\frac{\#S_n}{\#G_n} = \frac{\#T_n}{\#A_n}\sum_{\chi\in E^\vee}\prod_{p|n}\frac{1}{\#T_p}\sum_{s\in T_p}\chi(s)$$

Since for all χ we have $\chi(1)=1$, we can change the inner sum to run over all of A_p.

$$\frac{\#S_n}{\#G_n} = \frac{\#T_n}{\#A_n}\sum_{\chi\in E^\vee}\prod_{p|n}\frac{1}{\#A_p-1}\left(-1+\sum_{s\in A_p}\chi(s)\right)$$

If $\chi(A_p)$ is not trivial, then $\sum_{s\in A_p}\chi(s)$ equals 0. Otherwise, it equals $\#A_p$.

$$\begin{aligned}\frac{\#S_n}{\#G_n} &= \frac{\#T_n}{\#A_n}\sum_{\chi\in E^\vee}\prod_{\substack{p \text{ prime}\\ \chi(A_p)\neq 1}}\frac{-1}{\#A_p-1} \\ &= C(K,V,t)\prod_{p|n}\left(1-\frac{1}{\#A_p}\right)\end{aligned}$$

Since $C(K,V,t)$ does not depend on n, taking the limit of n to infinity gives the desired expression. □

5.3 Explicit density computations

In section 1.3 the exponent of the radical groups in question is squarefree, and we have used that to decompose B_{ab} as μW with μ a group of roots of unity and W a group of Kummer roots of elements of K. In the more general context of the present chapter, B_{ab} cannot be written in this way, but we can extend B with extra roots of unity to enable this. In Proposition 4.9 we saw how to do this over $\mathbf{Q}$, and the following Proposition gives the generalization for arbitrary number fields.

Proposition 5.6. *Let $C \subset D$ be a Galois radical extension such that D/C is of finite exponent dividing n. Let w be the order of $C[n]$, the n-torsion subgroup of C. If the order of $D[nw]$ equals nw, then D_{ab} can be decomposed as $D_{\mathrm{ab}} = \mu W$ with $\mu = D_{\mathrm{tors}}$ and $W = \{x \in D : x^w \in C\}$.*

Proof. We first recall the definition of D_{ab} from Section 2.5, adapted to the context of the proposition.

$$D_{\mathrm{ab}} = \{x \in D : x^w \in D_{\mathrm{tors}}C\}.$$

The inclusion $\mu W \subset D_{\mathrm{ab}}$ is clear, so we proceed with the opposite inclusion.

Suppose x is an element of D_{ab}, so we have $x^w \in \zeta C$ for an element $\zeta \in D_{\mathrm{tors}}$. We aim to show that we have $x \in \mu W$, or, equivalently, $x^w \in D^w_{\mathrm{tors}}C$. Since we know $x^n \in C$, we see $\zeta^{n/w} \in x^n C \subset C$, and we have $\zeta^{n/w} \in C_{\mathrm{tors}}$.

Now consider the quotient map $\pi : D_{\mathrm{tors}} \to D_{\mathrm{tors}}/C_{\mathrm{tors}}$. The restriction $\pi|_{D[n]}$ has kernel $C[n] = C[w]$ of order w, by definition of w and since all finite subgroups of D (and C) are cyclic. Since $D[n]$ has order n, the image $\pi(D[n])$ in $D_{\mathrm{tors}}/C_{\mathrm{tors}}$ is of order n/w and therefore equal to $(D_{\mathrm{tors}}/C_{\mathrm{tors}})[\frac{n}{w}]$.

Because we have $\zeta \in D_{\mathrm{tors}}$ and $\zeta^{n/w} \in C_{\mathrm{tors}}$, we see that ζC_{tors} is in $\pi(D[n])$, so we have $\zeta \in D[n]C_{\mathrm{tors}}$. Finally, since $\#D[nw] = nw$, we have that $D[n] = D[nw]^w \subset D^w_{\mathrm{tors}}$, and therefore $\zeta \in D^w_{\mathrm{tors}}C$. We now conclude that $x^w \in \zeta C \subset D^w_{\mathrm{tors}}C$, and therefore $x \in \mu W$. □

For a prime p, define $e'(p)$ and B'_p as

$$p^{e'(p)} = p^{e(p)} \cdot \#K^*[p^{e(p)}];$$
$$B'_p = \mu_{p^{e'(p)}} B_p = \left\langle K^*, \mu_{p^{e'(p)}}, \sqrt[p^{e(p)}]{V} \right\rangle.$$

For positive integers n, analogously to the definitions of B_n and K_n, we define the group B'_n as the group generated by all B'_p for $p \mid n$ and the field K'_n as $K(B'_n)$. The radical extensions $K^* \subset B'_n$ now satisfy the conditions of Proposition 5.6 by construction.

Example 5.7.

The following is a typical example in which B_{ab} is not generated by roots of unity and Kummer roots, but B'_{ab} is. Let l be a rational prime, and let ζ_l be a primitive l-th root of unity in a fixed algebraic closure $\bar{\mathbf{Q}}$. Consider the case $K = \mathbf{Q}(\zeta_l)$, $V = \langle 2^l \zeta_l \rangle$, $t = l$.

Then we see that B_l is given by

$$B_l = \left\langle K^*, \zeta_{l^2}, \sqrt[l^2]{2^l \zeta_l} \right\rangle.$$

If we choose elements $\sqrt[l]{2}$ and ζ_{l^3} inside $\bar{K}$, then B_l contains an element $x = \zeta_{l^3}\sqrt[l]{2}$. This element x is contained in B_{ab}, since x^l is contained in $\mu_{l^2}K^*$. Since $\sqrt[l]{2}$ is itself a Kummer root, but ζ_{l^3} cannot be written as a Kummer root times a root of unity inside B_l, we can conclude that x cannot be written in this way, and B_{ab} cannot be decomposed as a subgroup of roots of unity and a subgroup of Kummer roots.

The situation changes when we extend B_l to B'_l as above:

$$B'_l = \left\langle K^*, \zeta_{l^3}, \sqrt[l^2]{2^l \zeta_l} \right\rangle.$$

While x is also an element of B'_{ab}, in this case we clearly do obtain x as a product of a Kummer root $\sqrt[l]{2}$ times a root of unity ζ_{l^3} inside B'_l.

Finally define B' as the group generated by all B'_p, and $E' = E(B')$ as its entanglement group. Besides deriving E from E', and then evaluating the correction factor formula from Theorem 5.2, it is also possible to directly compute the correction factor from E'.

To this end, consider the automorphism group $\mathrm{Aut}_B(B')$. Since B' is generated by a single root of unity that is a Kummer radical over B, the group $\mathrm{Aut}_B(B')$ is cyclic. Let σ be its generator. If we then write $A'_p = \mathrm{Aut}_{K^*}(B'_p)$, the following theorem gives an expression for the correction factor.

Theorem 5.8. *The correction factor $C(K, V, t)$ defined in Theorem 5.2 is equal to*

$$\sum_{\substack{\chi \in E'^{\vee} \\ \chi(\bar{\sigma})=1}} \prod_{\substack{p \text{ prime} \\ \chi(A'_p)\neq 1}} \frac{-1}{\#A_p - 1}.$$

Proof. The equivalence of this formula and the one from Theorem 5.2 follows directly from these two claims:

1. $E^{\vee}$ is equal to $\{\chi \in E'^{\vee} : \chi(\bar{\sigma}) = 1\}$;
2. For $\chi \in E^{\vee} \subset E'^{\vee}$ we have $\chi(A'_p) = 1 \Leftrightarrow \chi(A_p) = 1$.

We prove them in order. For the first claim, note that the kernel of the restriction map $\mathrm{Aut}_{K^*}(B') \to \mathrm{Aut}_{K^*}(B)$ is generated by σ. This implies that the kernel of the induced (surjective) map $E(B') \to E(B)$ is generated by $\bar{\sigma}$. Identifying $E(B)$ with $E(B')/\langle\bar{\sigma}\rangle$ then shows that $E^{\vee}$ consists of the characters in $E'^{\vee}$ that are trivial on $\langle\bar{\sigma}\rangle$, as claimed.

For the second claim, let χ be a character of E, where we again consider $E^{\vee}$ as a subgroup of $E'^{\vee}$. Recall that we can factor A' as $\prod_p A'_p$ and A as $\prod_p A_p$. This leads to the following commutative diagram.

$$\begin{array}{ccccc} A'_p & \twoheadrightarrow & A_p & & \\ \downarrow & & \downarrow & & \\ A' & \twoheadrightarrow & A & \xrightarrow[\chi]{} & \mathbf{C}^* \end{array}$$

The group of interest $\chi(A'_p)$ is the image of the composition

$$A'_p \hookrightarrow A' \twoheadrightarrow A \xrightarrow{\chi} \mathbf{C}^*.$$

As the commutativity of the diagram shows, this composed map factors via A_p, so we see that $\chi(A_p) = 1 \Rightarrow \chi(A'_p) = 1$. The opposite implication is trivial, proving the second claim. □

Example 5.9.

We illustrate this theorem, and the methods in this chapter in general, by computing an Artin density (assuming GRH).

Take $K = \mathbf{Q}(\zeta_3)$, and $x = 8\zeta_3$, and $V = \langle x \rangle$, and $t = 3$. In Example 5.7 we saw that we need to enlarge B with extra roots of unity in this case. Proposition 5.6 implies that adding 4th and 27th roots of unity is sufficient, but in this case only adding 27th roots already suffices, as we shall see.

Define B'_p for primes p as

$$B'_p = \langle K^*, \zeta_p, \sqrt[p]{x} \rangle \text{ if } p \neq 3, \text{ and}$$

$$B'_3 = \langle K^*, \zeta_{27}, \sqrt[9]{x} \rangle = \langle K^*, \zeta_{27}, \sqrt[3]{2} \rangle.$$

By Theorem 5.5, only the primes 2 and 3 affect entanglement, and $E(B') = E(B'_6) = E((B'_6)_{\mathrm{ab}})$. In fact, B'_6 is itself equal to $(B'_6)_{\mathrm{ab}}$ since it is generated by roots of unity and Kummer roots.

We have that

$$B'_2 = \langle K^*, \zeta_2, \sqrt[2]{8\zeta_3} \rangle = \langle K^*, \zeta_3\sqrt{2} \rangle; \text{ and}$$

$$B'_6 = \langle K^*, \zeta_{27}, \sqrt[3]{2}, \sqrt{2} \rangle.$$

We now take $\mu = \mu_{27}$ and $W = \langle K^*, \sqrt[6]{2} \rangle$. We then obtain $B'_6 = \mu W$. Defining G_W to be the absolute Galois group of $K(W) = K(\sqrt[6]{2})$, the expression for the entanglement group we obtain from Corollary 2.31, with $C = W$ and $D = \mu$, is

$$E' = \mathrm{Aut}_{\mu \cap W}(\mu)/\mathrm{im}(G_W).$$

Since we have $\mu \cap W = \mu_3$ and $K(W) \cap \mathbf{Q}(\mu)$ equals $\mathbf{Q}(\mu_3)$, we see that E' is trivial.

For all primes $p \neq 3$, we have $\#A_p = p(p-1)$. For $p = 3$ on the other hand, we get $\#A_3 = 9$.

Assuming GRH, we then arrive at a density of

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{\#A_p}\right) = \frac{16}{15} \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right).$$

Example 5.10.

In the previous example, we took the case from Example 5.7 with $l = 3$. In this example we take $l = 2$, so we get $K = \mathbf{Q}$, and $x = -4$, and $V = \langle x \rangle$, and $t = 2$.

As before, we need to add extra roots of unity: in this case 8th roots.

Define B'_p for primes p as

$$B'_p = \langle K^*, \zeta_p, \sqrt[p]{x} \rangle \text{ if } p \neq 2, \text{ and}$$

$$B'_2 = \langle K^*, \zeta_8, \sqrt[4]{x} \rangle = \langle K^*, \zeta_8, \sqrt{2} \rangle.$$

By Theorem 5.5, only the prime 2 affects entanglement, and $E(B') = E(B'_2) = E((B'_2)_{\mathrm{ab}})$. If we define $\mu = \mu_8$ and $W = \langle \mathbf{Q}^*, \sqrt{2} \rangle$, then B'_2 equals μW, so $(B'_2)_{\mathrm{ab}}$ equals B'_2.

Define G_W to be the absolute Galois group of $K(W) = \mathbf{Q}(\sqrt{2})$. We then again get the following expression for $E(B')$ from Corollary 2.31, again with $C = W$ and $D = \mu$.

$$E' = \mathrm{Aut}_{\mu \cap W}(\mu)/\mathrm{im}(G_W).$$

We have $\mu \cap W = \{\pm 1\}$ and $K(W) \cap \mathbf{Q}(\mu)$ equals $\mathbf{Q}(\sqrt{2})$, so the image of G_W in $\mathrm{Aut}(\mu) = \mathrm{Aut}(\mu_8)$ equals $\langle \zeta_8 \mapsto \zeta_8^{-1} \rangle$.

So E' is an entanglement group of order 2. Let χ be the non-trivial character in $E'^{\vee}$.

To compute the correction factor, we use Theorem 5.8. First, take σ to be the generator of $\mathrm{Aut}_B(B')$, which sends ζ_8 to ζ_8^5. Then the image of σ in E' is not trivial, since it is not in the image of G_W.

Since $E(B') = E(B'_2)$, we see that A'_2 can only map surjectively to E', so $\chi(A'_2)$ is not trivial.

Since $\#A'_2$ equals 4, this gives a correction factor of

$$1 + \frac{-1}{3} = \frac{2}{3}.$$

For all odd primes, we have $\#A_p = p(p-1)$, so, assuming GRH, we then obtain the density

$$\frac{2}{3} \prod_{p \text{ prime}} \left(1 - \frac{1}{\#A_p}\right) = \frac{2}{3} \cdot \frac{3}{2} \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right) = \text{Artin's constant}.$$

We conclude this chapter with two remarks on different generalizations of Artin densities.

One possible generalization is adding a congruence condition to the primes $\mathfrak{q}$ considered. (See Moree [21], for $K = \mathbf{Q}$.) This can be translated to a condition on $\mathrm{Frob}_{\mathfrak{q}}$ in a ray class field F over K. One can in fact handle such Frobenius conditions for an arbitrary Galois extension F of K, cf. Lenstra [18]. If we extend the radical group B considered with extra radicals to include the radical part of F, we get extra

conditions on $\mathrm{Frob}_{\mathfrak{q}}$ inside the automorphism groups A_n, which in turn lead to a smaller T_n.

The resulting density does not necessarily permit a character sum formula using the methods described in this chapter, since the smaller group T_n does not necessarily factor as a product $\prod_{p|n} T_p$. Also, if F is itself not generated by radicals, then the restriction of the map $\mathrm{Gal}(F/K) \to \mathrm{Gal}(F \cap K(B)/K)$ to a set $C \subset \mathrm{Gal}(F/K)$ closed under conjugation will not in general have fibers of the same size, which will require extra administration.

For $K = \mathbf{Q}$ and a congruence condition modulo n, the ray class field F is in fact equal to $\mathbf{Q}(\zeta_n)$. In this case, the two difficulties described above do not occur, and we are able to get a character sum formula for the density. For details, we refer to [20].

In this chapter we have considered the set $M = M(K, x, t)$ of primes $\mathfrak{q}$ of K for which an element $x \in K^*$ generates a subgroup of $(\mathcal{O}_K/\mathfrak{q})^*$ of index dividing t. Moree [23] considers the set of primes $M' = M'(\mathbf{Q}, x, t)$ where this index is *equal* to t. The density of M' can be derived from $M(K, x, t')$ for all $t' \mid t$ using Möbius inversion, but there is a more direct way to use the theory from this chapter to compute it, which is also described in detail for a related method by Lenstra, Moree and Stevenhagen [20].

For a prime p, we define $C_p = \langle K^*, \zeta_{p^{e(p)}}, \sqrt[p^{e(p)}]{V} \rangle$ and also the subgroup $C'_p = \langle K^*, \zeta_{p^{e(p)-1}}, \sqrt[p^{e(p)-1}]{V} \rangle \subset C_p$. For a positive integer n we define from these the groups C_n and C'_n generated by C_p respectively C'_p for all $p \mid n$. Define the automorphism groups $A_n = \mathrm{Aut}_{K^*}(C_n)$ and $A'_n = \mathrm{Aut}_{C'_n}(C_n) \subset A_n$. Also let G_n be the Galois group $\mathrm{Gal}(K(C_n)/K)$ and E_n the entanglement group of C_n with the action of G_n. Theorem 5.1 applies to this situation, and implies there is a limit entanglement group E such that if n is divisible by all of a finite set of critical primes, E_n is equal to E.

Theorem 5.11. *Assuming GRH, the set $M'(K, V, t)$ has a natural density equal to*

$$C'(K, V, t) \cdot \prod_{p \text{ prime}} \left(1 - \frac{1}{\#A_p}\right),$$

where $C'(K, V, t)$ is a rational correction factor given explicitly by

$$C'(K, V, t) = \left(\prod_{p|t} \frac{\#A'_p - 1}{\#A_p - 1}\right) \left(\sum_{\chi \in E^\vee} \prod_{\substack{p \text{ prime} \\ \chi(A'_p) \neq 1}} \frac{-1}{\#A'_p - 1}\right).$$

Proof. Using the notation from this chapter, the main difference with Theorem 5.2 is that for a prime p, the set S_p of allowed Frobenius elements at p will no longer be $G_p \setminus \{1\}$. The condition that led to this at p for index dividing t was:

$$\mathfrak{q} \text{ does not split completely in } K \subset K(\zeta_{p^{e(p)}}, \sqrt[p^{e(p)}]{V}).$$

In the case where we are interested in index *equal* to t, this becomes:

$$\begin{gathered}\mathfrak{q} \text{ does not split completely in } K \subset K(\zeta_{p^{e(p)}}, \sqrt[p^{e(p)}]{V}), \text{ and} \\ \mathfrak{q} \textit{ does} \text{ split completely in } K \subset K(\zeta_{p^{e(p)-1}}, \sqrt[p^{e(p)-1}]{V}).\end{gathered}$$

Using C_p and C'_p as defined above the Theorem, this leads to the condition at p that $\mathrm{Frob}_{\mathfrak{q}}$ in $\mathrm{Gal}(K(C_p)/K)$ is an element of the subset $\mathrm{Gal}(K(C_p)/K(C'_p)) \setminus \{1\}$. Translating this to the context of automorphisms of abelian groups, this gives us:

$$\frac{\#(\mathrm{Gal}(K(C_p)/K(C'_p)) \setminus \{1\})}{\#\mathrm{Gal}(K(C_p)/K)} = \frac{\#((\mathrm{Aut}_{C'_p}(C_p) \setminus \{1\}) \cap \mathrm{Gal}(K(C_p)/K))}{\#\mathrm{Gal}(K(C_p)/K)}.$$

From this expression one can derive a character sum formula for the density, analogously to the approach followed in the proof of Theorem 5.2 in Section 5.2. To this end, recall $A'_p = \mathrm{Aut}_{C'_p}(C_p)$ and define

$$T_n = \{\sigma \in A_n : \sigma|_{B_p} \in A'_p \setminus \{1\} \text{ for all primes } p \mid n\}.$$

We then get the following computation, if we assume all primes dividing t also to divide n.

$$\begin{aligned}\frac{\#(T_n \cap G_n)}{\#G_n} &= \frac{1}{\#E\#G_n} \sum_{s \in T_n} 1_{G_n}(s) = \frac{1}{\#A_n} \sum_{s \in T_n} \sum_{\chi \in E^\vee} \chi(s) \\ &= \frac{\#T_n}{\#A_n} \sum_{\chi \in E^\vee} \prod_{p \mid n} \frac{1}{\#T_p} \sum_{s \in T_p} \chi(s)\end{aligned}$$

Since for all χ we have $\chi(1) = 1$, we can change the inner sum to run over all of A'_p.

$$\frac{\#(T_n \cap G_n)}{\#G_n} = \frac{\#T_n}{\#A_n} \sum_{\chi \in E^\vee} \prod_{p \mid n} \frac{1}{\#A'_p - 1} \left(-1 + \sum_{s \in A'_p} \chi(s) \right)$$

If $\chi(A'_p)$ is not trivial, then $\sum_{s \in A'_p} \chi(s)$ equals 0. Otherwise, it equals $\#A'_p$.

$$\begin{aligned}\frac{\#(T_n \cap G_n)}{\#G_n} &= \frac{\#T_n}{\#A_n} \sum_{\chi \in E^\vee} \prod_{\substack{p \text{ prime} \\ \chi(A'_p) \neq 1}} \frac{-1}{\#A'_p - 1} \\ &= \left(\prod_{p \mid n} \left(1 - \frac{1}{\#A_p} \right) \right) \left(\prod_{p \mid t} \frac{\#A'_p - 1}{\#A_p - 1} \right) \left(\sum_{\chi \in E^\vee} \prod_{\substack{p \text{ prime} \\ \chi(A'_p) \neq 1}} \frac{-1}{\#A'_p - 1} \right)\end{aligned}$$

Only the first product now depends on n, and taking the limit of n to infinity then gives the density of $M'(K, V, t)$, assuming GRH. We conclude that with the correction factor $C'(K, V, t)$ defined in the Theorem, we get the desired expression for the density. □

Chapter 6

Artin's primitive root conjecture for rank one tori

6.1 Introduction

The theory we set up in Chapter 2 is applicable in a wider setting than that of radicals over fields which we have studied so far. In this chapter, we use it for *division points* of rank one tori. After briefly introducing the concept of a torus, we state analogues of Artin's primitive root density question and a conjectured density theorem for rank one tori over number fields. For tori defined over $\mathbf{Q}$, these densities have previously been computed by Chen [7].

An *algebraic group* is an algebraic variety with a group operation. A well-known example is the algebraic group called $\mathbf{G}_{\mathrm{m}}$, defined as an affine variety by the equation

$$xy = 1$$

and the group law

$$(x, y)(x', y') = (xx', yy').$$

For any commutative ring R, the map $(x, y) \mapsto x$ gives an isomorphism of the group $\mathbf{G}_{\mathrm{m}}(R)$ to the unit group R^* of R.

Definition 6.1. A *torus* over a field K is an algebraic group that is isomorphic to $\mathbf{G}_{\mathrm{m}}^r$ over K^{sep} for some positive integer r. This integer r is called the *rank* of the torus.

If an algebraic group G over K is isomorphic to $\mathbf{G}_{\mathrm{m}}^r$ for $r \in \mathbf{Z}_{>0}$ over a field $L \supset K$, then we say G is *split* over L.

If T is a torus of rank r defined over a number field K, the group of *division points* of such a torus is given by

$$\{P \in T(K^{\mathrm{sep}}) : \exists n \in \mathbf{Z}_{>0} : P^n \in T(K)\}.$$

The torsion subgroup of this group is isomorphic to $(\mathbf{Q}/\mathbf{Z})^r$. To satisfy our condition on radical group extensions that all finite subgroups are cyclic, we therefore restrict to tori of rank 1. If K has characteristic 0, the group of division points is then isomorphic to the maximal radical extension of $T(K)$ as defined by Theorem 2.1. For characteristic $p > 0$ this holds if we make the adjustments mentioned in Remark 2.11.

We shall later show that all tori of rank one over a field K can be described as follows. If $f = X^2 + aX + b$ is a separable monic quadratic polynomial over K, let α be the zero X of f in the quadratic K-algebra $L = K[X]/(f)$.

We can then define an algebraic group T with equation and group law given by

$$x^2 + axy + by^2 = 1;$$

$$(x, y)(x', y') = (xx' - yy'b, xy' + x'y + yy'a).$$

The map sending a point $(x, y) \in T(K)$ to $(x - y\alpha) \in L$ gives a group isomorphism between $T(K)$ and the kernel of the norm map $N_K^L : L^* \to K^*$. In particular, if f factors as a product of two linear polynomials, then T is isomorphic to $\mathbf{G}_\mathrm{m}$ over K. If on the other hand f is irreducible, then T is split over the quadratic extension field L defined by f.

From here on, let T be the rank one torus defined over a number field K by the quadratic polynomial f.

Define S to be the set of primes of K that occur in the denominators of the coefficients of f or in the discriminant of f. Then we say that T has *good reduction* at all primes outside of S, in the following sense. For a prime $\mathfrak{q} \notin S$, the torus T is defined over the local ring $\mathcal{O}_{K,\mathfrak{q}}$, given by

$$\mathcal{O}_{K,\mathfrak{q}} = \{x \in K : \mathrm{ord}_\mathfrak{q}(x) \geq 0\}.$$

There is then a reduction map which gives a group homomorphism:

$$T(\mathcal{O}_{K,\mathfrak{q}}) \to T(\mathcal{O}_K/\mathfrak{q}).$$

Since $\mathfrak{q}$ does not divide the discriminant of f, the equation f taken modulo $\mathfrak{q}$ defines a torus $\bar{T}$ over $\mathcal{O}_K/\mathfrak{q}$. The group $T(\mathcal{O}_K/\mathfrak{q}) = \bar{T}(\mathcal{O}_K/\mathfrak{q})$ is then a subgroup of the unit group of its (finite) splitting field, and is therefore cyclic.

Also, for a point P of $T(K)$, we have that for almost all primes $\mathfrak{q}$ the point P is in $T(\mathcal{O}_{K,\mathfrak{q}})$ and the reduction $\bar{P} \in T(\mathcal{O}_K/\mathfrak{q})$ is well-defined. Because of these properties, there is an analogue of Artin's primitive root density question for rank one tori.

Question 6.2. *If P is a point of $T(K)$, for how many primes $\mathfrak{q}$ of $\mathcal{O}_K$ is the group $T(\mathcal{O}_K/\mathfrak{q})$ generated by $\bar{P}$?*

If T is $\mathbf{G}_\mathrm{m}$ and $K = \mathbf{Q}$, this is exactly the original question Artin asked. In this chapter we will work in greater generality, analogously to Chapter 5. With K a number field and T a rank one torus defined over K, let V be a finitely generated subgroup of $T(K)$ that is not contained in $T(K)_\mathrm{tors}$, and let t be a positive integer.

We will look at the set $M = M(T, V, t)$ of primes $\mathfrak{q}$ of K satisfying:

- $v \in T(\mathcal{O}_{K,\mathfrak{q}})$ for all $v \in V$; and
- $[T(\mathcal{O}_K/\mathfrak{q}) : \bar{V}] \mid k$.

We again reduce this to an expression about automorphism groups of radical group extensions and their entanglement. Choose a fixed algebraic closure $\bar{K}$ of K. As in the previous chapter, for a rational prime p, let $e(p)$ be the smallest positive integer such that $p^{e(p)}$ does not divide t, and define the radical group extensions

$$T(K) \subset B_p = \left\langle T(K), \{z \in T(\bar{K}) : z^{p^{e(p)}} \in V\} \right\rangle.$$

We also define $A_p = \mathrm{Aut}_{T(K)}(B_p)$, and B as the subgroup of $T(\bar{K})$ generated by all B_p. The absolute Galois group G_K of K acts on $T(\bar{K})$ as described above, and this action induces a map G_K to $A = \mathrm{Aut}_{T(K)}(B)$ with as cokernel the abelian entanglement group $E = E(B)$.

In the present setting, we get the same two main theorems as in Chapter 5.

Theorem 6.3. *The entanglement group $E(B)$ of B is finite.*

Theorem 6.4. *Assuming GRH, the set $M(T, V, t)$ has a natural density equal to*

$$C(T, V, t) \cdot \prod_{p \text{ prime}} \left(1 - \frac{1}{\#A_p}\right),$$

where $C(T, V, t)$ is a rational correction factor given by

$$C(T, V, t) = \sum_{\chi \in E^\vee} \prod_{\substack{p \text{ prime} \\ \chi(A_p) \neq 1}} \frac{-1}{\#A_p - 1}.$$

We prove these results in Section 6.3. In the remainder of the chapter, we give results to make the necessary computations explicit, and illustrate this with a number of examples in Section 6.4.

6.2 Preliminaries

Let K be a field. One can show (see e.g., Borel [5], §8) that there is a covariant equivalence of categories

$$\{\text{rank } r \text{ tori over } K\}$$
$$\longleftrightarrow$$
$$\{\text{rank } r \text{ free abelian groups with continuous } \mathrm{Gal}(K^{\mathrm{sep}}/K)\text{-action}\}.$$

Following the notation from [5], this maps a torus T to $X_*(T) = \mathrm{Mor}(\mathbf{G}_{\mathrm{m}}, T)$.

We also have the following Galois module isomorphism.

$$\begin{array}{rcl} \bar{K}^* \otimes_{\mathbf{Z}} X_*(T) & \xrightarrow{\sim} & T(\bar{K}) \\ z \otimes f & \longmapsto & f(z). \end{array}$$

Here the Galois group acts on both factors on the left separately. In particular, a rank one torus T over K corresponds to the infinite cyclic group with an action of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$, and we choose a fixed generator τ. If the Galois action on τ is trivial, then T is isomorphic to the torus $\mathbf{G}_{\mathrm{m}}$ over K.

If the action is not trivial, then there is a field L of degree 2 over K such that the action factors via the quotient $\mathrm{Gal}(L/K)$ of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ because $\mathrm{Aut}(\mathbf{Z})$ equals $\{\pm 1\}$. In this case, T is not split over K, but it is split over L, and more generally over all fields containing L. Let σ be an element of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. The Galois action on τ is then explicitly given by

$$\sigma(\tau) = \begin{cases} \tau & \text{if } \sigma|_L = \mathrm{id}; \text{ and} \\ -\tau & \text{if } \sigma|_L \neq \mathrm{id}. \end{cases}$$

We can use the morphism $\tau \in \mathrm{Mor}(\mathbf{G}_{\mathrm{m}}, T)$ to twist the Galois action on $\bar{K}^*$. If z is an element of $\bar{K}^*$, then, using the Galois module isomorphism above, $z \otimes \tau$ gives a point on the torus. Since $\bar{K}^*$ is a multiplicatively written module, we write $z^\tau = z \otimes \tau$. Because τ is a generator of $X_*(T) = \mathrm{Mor}(\mathbf{G}_{\mathrm{m}}, T)$, we then also have $\bar{K}^{*\tau} = \bar{K}^* \otimes_{\mathbf{Z}} X_*(T)$, with an induced isomorphism of Galois modules:

$$\begin{array}{rcl} \bar{K}^{*\tau} & \xrightarrow{\sim} & T(\bar{K}) \\ z^\tau & \longmapsto & \tau(z) \end{array}$$

In this chapter, we will view this as an identification, and consider z^τ as a point of $T(\bar{K})$. This notation allows us to conveniently write the action of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ on $T(\bar{K})$ as

$$\sigma(z^\tau) = \sigma(z)^{\sigma(\tau)},$$

where $\sigma(z)$ is the usual Galois action on $\bar{K}$.

Note that the map $z \mapsto z^\tau$ gives a bijection of $\bar{K}^* \to T(\bar{K})$, but this does not respect the Galois action of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$.

In characteristic 0, each non-split rank one torus over K is isomorphic to a torus T_d defined by the norm equation of $K(\sqrt{d})/K$,

$$T_d : x^2 - dy^2 = 1,$$

with multiplication of two points (x, y) and (x', y') defined by

$$(x, y)(x', y') = (xx' + dyy', xy' + x'y).$$

For one of the two choices of generator $\tau \in X_*(T)$, the Galois module isomorphism with $\bar{K}^{*\tau}$ is then given as

$$\begin{array}{rcl} T_d(\bar{K}) & \xrightarrow{\sim} & \bar{K}^{*\tau} \\ (x,y) & \longmapsto & (x - y\sqrt{d})^\tau. \end{array}$$

Sending (x,y) to $(x+y\sqrt{d})^\tau$ would correspond with the other choice of generator of $X_*(T)$.

Non-split rank one tori differ from the $\mathbf{G}_\mathrm{m}$ case in a number of interesting ways relevant to the topic of this thesis. For example, the torus T_{-1} defined by $x^2+y^2=1$ and splitting field $\mathbf{Q}(i)$ has rational 4-torsion. Similarly, the torus T_{-3} given by $x^2+3y^2=1$ has splitting field $\mathbf{Q}(\sqrt{-3}) = \mathbf{Q}(\zeta_3)$ and has rational 6-torsion. This means radical group extensions over these tori can have greater entanglement groups than similar examples over $\mathbf{G}_\mathrm{m}$, as we shall see in the examples in this chapter.

Another significant way in which they can differ from $\mathbf{G}_\mathrm{m}$ is that for negative d, the group of division points of $T_d(\mathbf{R})$ is divisible and contains non-trivial p-torsion for all primes p, so the maximal radical extension of $T_d(\mathbf{Q})$ in this case is contained in $T_d(\mathbf{R})$.

We conclude this section with remarks on notation. Let G_K be the absolute Galois group of K, and M a G_K-module. Then we can adjoin the Galois module M to K by defining $K(M)$ as the invariant field of the kernel of the action $G_K \to \mathrm{Aut}(M)$.

If M is a G_K-submodule of $\bar{K}^*$, then $K(M)$ is the field extension of K generated by M.

If M is a G_K-submodule of $T(\bar{K})$, or equivalently a Galois radical extension of $T(K)$ inside $T(\bar{K})$, then $K(M)$ is the field extension of K generated by the coordinates of the elements of M.

We have seen that if C is a Galois submodule of $\bar{K}^*$, then C^τ can be considered a Galois submodule of $T(\bar{K})$. For example, if μ is the group of all roots of unity of $\bar{K}^*$, then μ^τ is naturally isomorphic to $T(\bar{K})_\mathrm{tors}$ as a Galois module.

Note that the field extension $K(\mu^\tau)$ obtained by adjoining the Galois module μ^τ is in general not the same as the field extension $K(\mu)$ obtained by adjoining μ to K. Consider for example the torus T_{-1} defined by $x^2+y^2=1$ over $\mathbf{Q}$, and μ the roots of unity of $\bar{\mathbf{Q}}^*$. Then the coordinates of μ^τ are real, and one can in fact show that for T_{-1} the field $\mathbf{Q}(\mu^\tau)$ is equal to $\mathbf{Q}(\mu) \cap \mathbf{R}$.

6.3 Proof of main theorems

In this section we will prove Theorems 6.3 and 6.4. The main ingredient for the correction factor being a rational number is that the entanglement group $E(B)$ of B as defined in Section 6.1 is finite.

We show this by proving the analogue of Theorem 5.5. As before, if n is a positive integer, we write B_n for the abelian group generated by all B_p for $p \mid n$.

Theorem 6.5. *Write w for the number of torsion points in $T(K)$ and let L be the splitting field of T. Define the integer n as the product of all primes p satisfying*

$$p \mid w\Delta_{L((B_w)_{\mathrm{ab}})/\mathbf{Q}}.$$

Then the natural map $E(B) \to E(B_n)$ is an isomorphism.

Proof. Before we start, note that if T is split over K, then this theorem reduces to Theorem 5.5, so we assume that T is not split over K.

We now mirror the proofs of Theorem 5.1 and Theorem 5.5. Specifically, define C_n and C_n' as follows.

$$\begin{aligned} C_n &= (B_n)_{\mathrm{ab}} \text{ and} \\ C_n' &= \left\langle T(K), \mu_{p^{e(p)}}^{\tau} : p \nmid n \right\rangle. \end{aligned}$$

By the same reasoning as for Theorem 5.1, we can decompose B_{ab} and $\mathrm{Aut}_{T(K)}(B_{\mathrm{ab}})$.

$$B_{\mathrm{ab}} = C_n \oplus_{T(K)} C_n'$$

$$\mathrm{Aut}_{T(K)}(B_{\mathrm{ab}}) = \mathrm{Aut}_{T(K)}(C_n) \times \mathrm{Aut}_{T(K)}(C_n').$$

Apart from different notation, Equation 5.3 holds in this setting since its proof is purely group theoretic. Translated, it reads

$$p \nmid w \Rightarrow (B_p)_{\mathrm{ab}} = \mu_{p^{e(p)}}^{\tau} T(K).$$

Because $L(\mu_{p^{e(p)}}^{\tau})$ equals $L(\zeta_{p^{e(p)}})$, we can deduce from the previous statement that we have:

$$L(C_n) = L((B_n)_{\mathrm{ab}}) = L((B_w)_{\mathrm{ab}}, \zeta_{p^{e(p)}} : p \mid n) = L((B_w)_{\mathrm{ab}}) \cdot \mathbf{Q}(\zeta_{p^{e(p)}} : p \mid n).$$

Now following exactly the reasoning from the proof of Theorem 5.5, we arrive at the statement that $\mathrm{Gal}(L(B_{\mathrm{ab}})/L(C_n))$ maps surjectively to the Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^{e(p)}} : p \nmid n)/\mathbf{Q})$, which is naturally isomorphic to $\mathrm{Aut}(\langle \mu_{p^{e(p)}} : p \nmid n \rangle)$.

Since $L(C_n)$ contains L, the action of the absolute Galois group $G_{L(C_n)}$ of $L(C_n)$ on $\mu_{p^{e(p)}}^{\tau}$ is the regular Galois action on $\mu_{p^{e(p)}}$, so the Galois action on the torus induces a surjection $G_{L(C_n)} \twoheadrightarrow \mathrm{Aut}_{T(K)}(C_n')$.

Since the larger Galois group $G_{K(C_n)}$ also acts on $T(C_n')$, we have a surjection $G_{K(C_n)} \twoheadrightarrow \mathrm{Aut}_{T(K)}(C_n')$. This factors via $\mathrm{Gal}(K(B_{\mathrm{ab}})/K(C_n))$ since the absolute Galois group of $K(B_{\mathrm{ab}})$ acts as the identity on $C_n' \subset B_{\mathrm{ab}}$.

The proof now concludes exactly as the proof of Theorem 5.5. □

Proof of Theorem 6.4. Recall that for a rational prime p, we defined $e(p)$ to be the smallest positive integer such that $p^{e(p)}$ does not divide t.

Now let $\mathfrak{q}$ be a prime of K for which T has good reduction and for which V is contained in $\mathcal{O}_{K,q}$. These conditions only exclude a finite number of primes as we saw in the introduction, so this does not affect the density. For such a prime, $T(\mathcal{O}_K/\mathfrak{q})$ is well-defined and V can be mapped to $T(\mathcal{O}_K/\mathfrak{q})$.

The index $[T(\mathcal{O}_K/\mathfrak{q}) : \bar{V}]$ now divides t if and only if for all primes p, the index is not divisible by $p^{e(p)}$. Choose a rational prime p with $\mathfrak{q} \nmid p$, and write $e = e(p)$ for brevity.

We saw in the introduction that $T(\mathcal{O}_K/\mathfrak{q})$ is cyclic, so we find that

$$p^e \mid [T(\mathcal{O}_K/\mathfrak{q}) : \bar{V}]$$

if and only if

$$p^e \mid \#T(\mathcal{O}_K/\mathfrak{q}) \text{ and } \bar{V} \subset T(\mathcal{O}_K/\mathfrak{q})^{p^e}$$

if and only if

$$\#T(\mathcal{O}_K/\mathfrak{q}) \text{ has an element of order } p^e \text{ and } \bar{V} \subset T(\mathcal{O}_K/\mathfrak{q})^{p^e}.$$

This is in turn equivalent with

$$\mathfrak{q} \text{ splits completely in } K \subset K(\mu_{p^e}^{\tau}, \sqrt[p^e]{V}) = K_p.$$

If we write $G_n = \mathrm{Gal}(K_p/K)$ and $S_n = G_n \setminus \{1\}$, then our condition for $\mathfrak{q}$ at p is that the Frobenius of $\mathfrak{q}$ in K_p/K is in S_n.

This describes the condition for $\mathfrak{q}$ we have at the single prime p. To combine this for multiple primes, let n be a positive integer, and define the field K_n as the compositum of the fields K_p for $p \mid n$. Let G_n be $\mathrm{Gal}(K_n/K)$ and define S_n as

$$S_n = \{\sigma \in G_n : \sigma \mid_{K_p} \neq \mathrm{id} \text{ for all } p \mid n\}.$$

Assuming the Generalized Riemann Hypothesis, the work of Murty [25] provides the analytic number theory argument that the set of primes $\mathfrak{q}$ satisfying the condition at every prime has a density, and that the density is equal to the limit

$$\lim_{n\to\infty} \frac{\#S_n}{\#G_n}.$$

The derivation of the formula for the density we give in Theorem 6.4, including its correction factor as a character sum now proceeds entirely as in the proof of Theorem 5.2. □

6.4 Explicit density computations

In this section we show how to explicitly compute Artin densities, and in particular the entanglement groups involved.

Let T be a non-split rank one torus over a number field K, and let L be its splitting field, so L/K is a quadratic extension. Let $B \supset T(K)$ be a Galois radical group extension, and B_{ab} its maximal abelian subextension.

By using the strategy from Section 5.3 if necessary, we may assume that to compute Artin densities, we can take B_{ab} of the form $\mu^{\tau}W$, where μ^{τ} is a group of torsion division points of $T(\bar{K})$, and W is a set of Kummer roots of $T(\bar{K})$ with $T(K) \subset W$.

Corollary 2.29 (with $C = W$ and $D = \mu^\tau$) gives us an isomorphism

$$E(\mu^\tau W) \xrightarrow{\sim} \mathrm{Aut}_{\mu^\tau \cap W}(\mu^\tau)/\mathrm{im}(G_W).$$

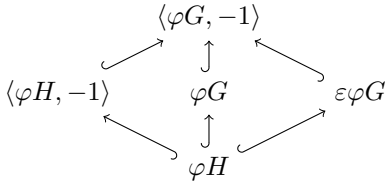
Here G_W is the kernel of the action of the absolute Galois group G_K of K on W. We will come back to the exact map later, and start by considering the image of G_W in $\mathrm{Aut}(\mu^\tau)$. To aid in determining this, we start with a group theoretic technical proposition.

Proposition 6.6. *Let G be a group acting on an abelian group M via the map $\varphi : G \to \mathrm{Aut}(M)$. Let $\varepsilon : G \to \{\pm 1\}$ be a surjective group homomorphism, and define H to be the kernel of ε. Define the group homomorphism $\varepsilon\varphi$ as follows.*

$$\begin{array}{rcl} \varepsilon\varphi : G & \longrightarrow & \mathrm{Aut}(M) \\ g & \longmapsto & \varepsilon(g)\varphi(g) \end{array}$$

Then the following statements characterize $\varepsilon\varphi G$.

- *If $-1 \in \varphi H$, then $\varepsilon\varphi G = \varphi G$.*
- *If $-1 \in \varphi G \setminus \varphi H$, then $\varepsilon\varphi G = \varphi H$.*
- *If $-1 \notin \varphi G = \varphi H$, then $\varepsilon\varphi G = \langle \varphi G, -1 \rangle$.*
- *If $-1 \notin \varphi G \neq \varphi H$, then $\varepsilon\varphi G$, and φG and $\langle \varphi H, -1 \rangle$ are the three distinct index 2 subgroups of $\langle \varphi G, -1 \rangle$ containing φH.*



Proof. First of all, note that exactly one of the four statements applies to any given situation.

We write G as the disjoint union of H and $G \setminus H$, so $\varepsilon\varphi G = \varepsilon\varphi H \cup \varepsilon\varphi(G \setminus H)$. Because we have $\varepsilon H = 1$, we get $\varepsilon\varphi H = \varphi H$. We turn to $\varepsilon\varphi(G \setminus H)$.

Suppose that we have $-1 \in \varphi H$. Then there is an element $c \in H$ with $\varphi(c) = -1$. We see that $\varepsilon\varphi(G \setminus H) = \varphi c(G \setminus H) = \varphi(G \setminus H)$. In this case, we get $\varepsilon\varphi G = \varphi G$.

Next, suppose that $-1 \notin \varphi H$, but $-1 \in \varphi G$. Then there is an element $c \in (G \setminus H)$ with $\varphi(c) = -1$. We then have that $G \setminus H = cH$, so $\varepsilon\varphi(G \setminus H) = \varepsilon\varphi cH = -1 \cdot -1 \cdot \varphi H = \varphi H$. We get $\varepsilon\varphi G = \varphi H$.

For the final two statements, assume $-1 \notin \varphi G$, and pick an element $\sigma \in (G \setminus H)$. Then we get $\varepsilon\varphi(G \setminus H) = \varepsilon\varphi(\sigma H) = (-\varphi(\sigma))\varphi(H)$.

If we then additionally have $\varphi G = \varphi H$, then we continue with $(-\varphi(\sigma))\varphi(H) = -\varphi(\sigma)\varphi(G) = -\varphi(G)$, and we get $\varepsilon\varphi G = \varphi G \cup -\varphi G = \langle \varphi G, -1 \rangle$.

Finally, if $-1 \notin \varphi G \neq \varphi H$, then φG and $\langle \varphi H, -1 \rangle$ contain φH with index 2. Since $\varphi(\sigma)$ and -1 commute in M, they are both contained in $\langle \varphi G, -1 \rangle$ with index 2, and there is a third distinct index 2 subgroup, which we claim is $\varepsilon\varphi G$, as shown in the diagram above.

To see this, note that $\varphi G = \varphi H \cup \varphi(\sigma)\varphi H$, and $\langle \varphi H, -1 \rangle = \varphi H \cup -\varphi H$. The third subgroup is $\varphi H \cup -\varphi(\sigma)\varphi H$, which is exactly how we had rewritten $\varepsilon\varphi G$. □

We use this proposition to determine the image of G_W in $\mathrm{Aut}(\mu^\tau)$ induced by the Galois action on μ^τ. To use the proposition in explicit examples, we first describe how we can apply it to the context of the torus T, taking $G = G_W$ acting on $M = \mu^\tau$.

Let $K(W)$ be the field obtained by adjoining the coordinates of the points in W to K. Then G_W is the absolute Galois group of $K(W)$. Recall that L is the splitting field of the torus T, so it is a quadratic field extension of K. Let H be the absolute Galois group of $L(W)$. It is a subgroup of index 2 of G_W. Let ε be the unique map $G_W \to \{\pm 1\}$ with kernel H.

We will now use Proposition 6.6 for the action of G_W on $\mu \subset \bar{K}$ compared to that of G_W on $\mu^\tau \subset T(\bar{K})$. The former is the regular Galois action, which we shall denote by $\varphi : G_W \to \mathrm{Aut}(\mu)$, while the latter is the Galois action on points of the torus, which is then given by $\varepsilon\varphi : G_W \to \mathrm{Aut}(\mu^\tau)$.

We now identify $\mathrm{Aut}(\mu)$ and $\mathrm{Aut}(\mu^\tau)$. Note that the induced diagram is *not* commutative:

$$\begin{array}{ccc} G_W & \xrightarrow{\varphi} & \mathrm{Aut}(\mu) \\ & \searrow^{\varepsilon\varphi} & \downarrow \mathrm{id} \\ & & \mathrm{Aut}(\mu^\tau) \end{array}$$

We can then use Proposition 6.6 to explicitly obtain the Galois action $\varepsilon\varphi$ of G_W on $\mu^\tau = T(\bar{K})_{\mathrm{tors}}$ in terms of the regular Galois action φ on the roots of unity μ of $\bar{K}$.

In this situation, since $-1 \in \mathrm{Aut}(\mu)$ corresponds to complex conjugation in $\mathrm{Gal}(\mathbf{Q}^{\mathrm{ab}}/\mathbf{Q})$, the condition $-1 \in \varphi G$ is equivalent to $K(W) \cap \mathbf{Q}^{\mathrm{ab}} \subset \mathbf{R}$. The condition $-1 \in \varphi H$ is similarly equivalent to $L(W) \cap \mathbf{Q}^{\mathrm{ab}} \subset \mathbf{R}$. Also, the condition $\varphi G = \varphi H$ is equivalent to $K \cap \mathbf{Q}^{\mathrm{ab}} = L \cap \mathbf{Q}^{\mathrm{ab}}$.

Example 6.7.

As a first example, we will compute the entanglement group of the maximal cyclotomic extension of a torus. Specifically, let T be a rank one torus over a number field K with splitting field L, and let μ be the roots of unity in $\bar{K}$. Then μ^τ is naturally isomorphic as a Galois module to $T(\bar{K})_{\mathrm{tors}}$. We will determine $E(\mu^\tau)$ with the action of the absolute Galois group G_K of K.

In this example, we are only adjoining torsion points, so take $W = T(K)$. Using the terminology from above, we get $G_W = G_K$ and $H = G_L$.

Let w be the number of roots of unity in K. We take the expression for the entanglement group from the beginning of this section, and adapt it for the current example:

$$E(\mu^\tau) \xrightarrow{\sim} \mathrm{Aut}_{\mu^\tau \cap T(K)}(\mu^\tau)/\varphi(G_W).$$

If we identify $\mathrm{Aut}(\mu^\tau)$ with $\hat{\mathbf{Z}}^*$, the automorphism group $\mathrm{Aut}_{\mu^\tau \cap T(K)}(\mu^\tau)$ in this expression is identified with $(\hat{\mathbf{Z}}^* \cap (1 + w\hat{\mathbf{Z}}))$.

Next, write Γ_K for φG_K and Γ_L for φG_L. The proposition then leads to the following four cases.

If $L \cap \mathbf{Q}^{\mathrm{ab}}$ is real, then $\varepsilon\varphi G_K = \varphi G_K = \Gamma_K$, and we obtain

$$E(\mu^\tau) = \left(\hat{\mathbf{Z}}^* \cap (1 + w\hat{\mathbf{Z}})\right) \Big/ \Gamma_K.$$

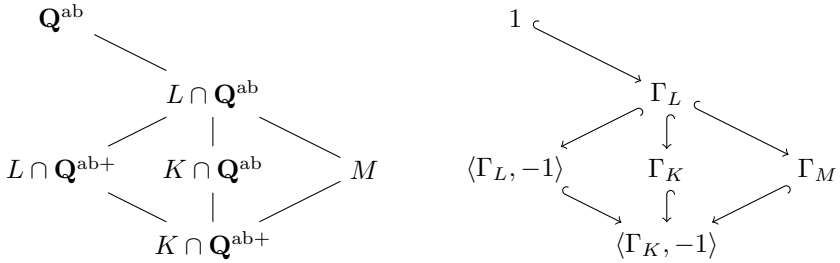
If $L \cap \mathbf{Q}^{\mathrm{ab}}$ is not real, but $K \cap \mathbf{Q}^{\mathrm{ab}}$ is real, then $\varepsilon\varphi G_K = \varphi G_L = \Gamma_L$, and we get

$$E(\mu^\tau) = \left(\hat{\mathbf{Z}}^* \cap (1 + w\hat{\mathbf{Z}})\right) \Big/ \Gamma_L.$$

If $K \cap \mathbf{Q}^{\mathrm{ab}}$ is not real, and $K \cap \mathbf{Q}^{\mathrm{ab}} = L \cap \mathbf{Q}^{\mathrm{ab}}$, then $\varepsilon\varphi G_K = \langle \varphi G_K, -1 \rangle$, and we obtain

$$E(\mu^\tau) = \left(\hat{\mathbf{Z}}^* \cap (1 + w\hat{\mathbf{Z}})\right) \Big/ \langle \Gamma_K, -1 \rangle.$$

Finally, suppose $K \cap \mathbf{Q}^{\mathrm{ab}}$ is not real and $K \cap \mathbf{Q}^{\mathrm{ab}} \neq L \cap \mathbf{Q}^{\mathrm{ab}}$. Write $\mathbf{Q}^{\mathrm{ab}+}$ for $\mathbf{Q}^{\mathrm{ab}} \cap \mathbf{R}$. Then $\mathrm{Gal}(L \cap \mathbf{Q}^{\mathrm{ab}}/K \cap \mathbf{Q}^{\mathrm{ab}+})$ is isomorphic to V_4 as depicted in the diagram on the left below. The field M is the third distinct field between $K \cap \mathbf{Q}^{\mathrm{ab}+}$ and $L \cap \mathbf{Q}^{\mathrm{ab}}$. The figure on the right shows the Galois groups of $\mathbf{Q}^{\mathrm{ab}}$ over the fields on the left.



If we write Γ_M for the image of the absolute Galois group of M to $\mathrm{Aut}(\mu)$, we then get

$$E(\mu^\tau) = \left(\hat{\mathbf{Z}}^* \cap (1 + w\hat{\mathbf{Z}})\right) \Big/ \Gamma_M.$$

We conclude this chapter by computing a number of Artin densities.

Example 6.8.

Let T be the torus defined by $x^2 + 3y^2 = 1$ over $K = \mathbf{Q}$. Its splitting field is $L = \mathbf{Q}(\zeta_3)$, and $T(\mathbf{Q})$ contains non-trivial 2-torsion and 3-torsion points so w equals 6.

We take $t = 1$ in this example, and let the subgroup $V \subset T(\mathbf{Q})$ be generated by a single point x with affine coordinates $(\frac{13}{14}, \frac{3}{14})$ that as an element of L is written by

$$x^\tau = \frac{13 + 3\sqrt{-3}}{14}.$$

For the right choice of $\pi \in \mathcal{O}_L$, we have $\pi\bar{\pi} = 7$ and $x = -\pi/\bar{\pi}$.

The radical extension we work in is

$$T(\mathbf{Q}) \subset B = \langle T(\mathbf{Q}), \mu_p^\tau, \sqrt[p]{x^\tau} : p \text{ prime} \rangle.$$

For entanglement, only the primes 2, 3 and 7 matter (Theorem 6.5), and so $E(B) = E(B_{\mathrm{ab}}) = E(\mu_{21}^\tau W)$ where W is the subset of B_{ab} given by

$$W = \langle T(\mathbf{Q}), \sqrt[6]{x^\tau} \rangle.$$

When adjoining the Kummer square and cube division points of x^τ to L, we get

$$L(\sqrt{x^\tau}) = \mathbf{Q}(\zeta_3, \sqrt{-7});$$
$$L(\sqrt[3]{x^\tau}) = \mathbf{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1}); \text{ and}$$
$$L(\sqrt[6]{x^\tau}) = \mathbf{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1}, \sqrt{-7}) = \mathbf{Q}(\zeta_{21}).$$

These fields are extensions of degree two over the subfields obtained when we adjoin these division points to $K = \mathbf{Q}$. These subfields are additionally real because $T(\mathbf{R})$ contains p-torsion for every prime p and is divisible, and the maximal radical extension of $T(\mathbf{Q})$ is therefore contained in $T(\mathbf{R})$.

$$K(\sqrt{x^\tau}) = \mathbf{Q}(\sqrt{21});$$
$$K(\sqrt[3]{x^\tau}) = \mathbf{Q}(\zeta_7 + \zeta_7^{-1}) \cap \mathbf{R} = \mathbf{Q}(\zeta_7) \cap \mathbf{R} = \mathbf{Q}(\zeta_7)^+; \text{ and}$$
$$K(\sqrt[6]{x^\tau}) = \mathbf{Q}(\zeta_{21}) \cap \mathbf{R} = \mathbf{Q}(\zeta_{21})^+.$$

From the expression for the entanglement group $E(\mu_{21}^\tau W)$ from the start of this section, we see that it is isomorphic to

$$\mathrm{Aut}_{\mu_3}(\mu_{21})/\mathrm{im}(G_W).$$

Using the reasoning from Proposition 6.6 and Example 6.7, we can compute $\mathrm{im}(G_W)$. Using the notation from the proposition, take G to be the absolute Galois group of $K(W)$ and H the subgroup of index 2 with invariant field $L(W)$, and let φ be the natural Galois action of G on $\hat{\mu} = \bar{K}^*_{\mathrm{tors}}$. Since $K(W) \subset \mathbf{Q}^{\mathrm{ab}}$ is real and $L(W) \subset \mathbf{Q}^{\mathrm{ab}}$ is not real, the proposition states that

$\varepsilon\varphi G_W$ is isomorphic to $\mathrm{Gal}(\mathbf{Q}^{\mathrm{ab}}/L(W)) = \Gamma_{L(W)}$. When restricting that result from $\mathrm{Aut}(\hat{\mu})$ to $\mathrm{Aut}_{\mu_3}(\mu_{21})$, the image of $\Gamma_{L(W)}$ is trivial since $L(W) = \mathbf{Q}(\zeta_{21})$, so the entanglement group is isomorphic to

$$E = \mathrm{Aut}_{\mu_3}(\mu_{21}).$$

This is a cyclic group of order 6.

Recall the definition of A_p for rational primes p, with $t = 1$ and $V = \langle x \rangle$:

$$A_p = \mathrm{Aut}_{T(K)}\left(\langle T(K), \mu_p^\tau, \sqrt[p]{x^\tau}\rangle\right).$$

To compute the correction factor in the density formula, we need to compute the image of A_p in E, for $p = 2, 3, 7$.

We start with A_2. This is a group of order 2, generated by the automorphism sending $\sqrt{x^\tau}$ to $-\sqrt{x^\tau}$. We extend this to an automorphism σ of B with the identity on A_p with $p \neq 2$. This automorphism in particular fixes the elements of $\mu_7^\tau \subset B_{\mathrm{ab}}$. We shift it with a Galois element $g \in G_{\mathbf{Q}}$ with $g|_W = \sigma|_W$. Since $K(\sqrt{x^\tau}) = \mathbf{Q}(\sqrt{21})$, we see that we can choose the automorphism g acting on $L(W) = \mathbf{Q}(\zeta_{21})$ as follows.

$$\begin{aligned} g: \quad & \zeta_7 \mapsto \zeta_7^{-1} \\ & \zeta_3 \mapsto \zeta_3. \end{aligned}$$

By Corollary 2.31, the image of A_2 in E is generated by $(\sigma g^{-1})|_{\mu_{21}^\tau}$. This is

$$\langle \zeta_7^\tau \mapsto \zeta_7^{-\tau} \rangle \subset \mathrm{Aut}_{\mu_3}(\mu_{21}) = E.$$

So the image of A_2 is the unique subgroup of order 2 in E.

Next is A_3 of order 3, generated by the automorphism sending $\sqrt[3]{x^\tau}$ to $\zeta_3^\tau \sqrt[3]{x^\tau}$. We also extend this to an automorphism σ of B with the identity on A_p with $p \neq 3$. As with A_2 above, σ leaves the elements of $\mu_7^\tau \subset B_{\mathrm{ab}}$ invariant. We shift this too with a Galois element $g \in G_{\mathbf{Q}}$ with $g|_W = \sigma|_W$. Because we have $K(\sqrt[3]{x^\tau}) = \mathbf{Q}(\zeta_7)^+$, we see that, for the right choice of ζ_3^τ and ζ_7, we can pick g to act on $L(W) = \mathbf{Q}(\zeta_{21})$ as

$$\begin{aligned} g: \quad & \zeta_7 \mapsto \zeta_7^2 \\ & \zeta_3 \mapsto \zeta_3. \end{aligned}$$

Again by Corollary 2.31, the image of A_3 in E is generated by $(\sigma g^{-1})|_{\mu_{21}^\tau}$. This is now

$$\langle \zeta_7^\tau \mapsto \zeta_7^{2\tau} \rangle \subset \mathrm{Aut}_{\mu_3}(\mu_{21}) = E.$$

So the image of A_3 is the unique subgroup of order 3 in E.

We continue with A_7. The action of this automorphism group on $\sqrt[7]{x^\tau}$ has no effect on its image in the entanglement group, so we need only consider the image of

$$A_7' = \mathrm{Aut}_{T(K)}\left(\langle T(K), \mu_7^\tau \rangle\right).$$

We extend a generator of this cyclic group of order 6 to an automorphism σ of B with the identity on A_p with $p \neq 7$. Since $\langle T(K), \mu_7^\tau \rangle \cap W$ equals $T(K)$, we see that σ acts as the identity on W, so the image of A_7' in E is generated by $\sigma|_{\mu_{21}^\tau}$, which implies that the map from A_7' to E is in fact an isomorphism, and A_7 maps surjectively to E.

Since E is cyclic of order 6, its dual $E^\vee$ is also cyclic of order 6. Let χ be a generator. From the images of A_p we have determined above, we can now directly determine for which powers χ^k of χ and for which primes we have $\chi^k(A_p) = 1$, indicated by the symbol $+$ in the table below, and for which we have $\chi^k(A_p) \neq 1$, indicated by the symbol $-$. That information will then let us evaluate the density correction factor.

	2	3	7
1	+	+	+
χ	−	−	−
χ^2	+	−	−
χ^3	−	+	−
χ^4	+	−	−
χ^5	−	−	−

With $\#A_2 = 2$, and $\#A_3 = 3$ and $\#A_7 = 42$, this results in the following correction factor, using the formula from Theorem 6.4.

$$C(T, V, t) = 1 - \frac{1}{2 \cdot 41} + \frac{1}{2 \cdot 41} + \frac{1}{41} - \frac{1}{2 \cdot 41} + \frac{1}{2 \cdot 41} = \frac{42}{41}.$$

For almost all primes p we have that $\#A_p = p(p-1)$, with as the only exception $\#A_3 = 3$. Assuming GRH, this gives a density of

$$\frac{42}{41} \cdot \prod_{p \text{ prime}} \left(1 - \frac{1}{\#A_p}\right) = \frac{42}{41} \cdot \frac{4}{5} \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right).$$

The amount of cancellation in the correction factor formula is due to the *almost* multiplicative structure of this particular table. If we were to replace the $+$ symbol in the top-right corner by a $-$ symbol, then we would be able to factor the formula for the changed correction factor C^- as follows, if we define $E_2^\vee = \{1, \chi^2, \chi^4\}$ and $E_3^\vee = \{1, \chi^3\}$.

$$C^- = \frac{-1}{\#A_7 - 1} \left(\sum_{\psi \in E_2^\vee} \prod_{\substack{p=2 \\ \psi(A_p) \neq 1}} \frac{-1}{\#A_p - 1} \right) \left(\sum_{\psi \in E_3^\vee} \prod_{\substack{p=3 \\ \psi(A_p) \neq 1}} \frac{-1}{\#A_p - 1} \right)$$

Since in fact *both* the factor for $p = 2$ and that for $p = 3$ are 0, we get $C^- = 0$. The actual correction factor C is therefore the difference between just the contribution of the top row with a $+$ symbol in the top-right in C and the contribution of the top row with a $-$ symbol in C^-. This leads, as expected, to $1 - \frac{-1}{41} = \frac{42}{41}$.

Example 6.9.

Finally, we consider an example with $t \neq 1$.

Let T again be the torus defined by $x^2+3y^2 = 1$ over $K = \mathbf{Q}$, with splitting field $L = \mathbf{Q}(\zeta_3)$ and $w = 6$.

We now take $t = 2$, and let the subgroup $V \subset T(\mathbf{Q})$ be generated by a single point $x^\tau \in T(\mathbf{Q})$, this time given with sign opposite to the previous example:

$$x^\tau = -\frac{13 + 3\sqrt{-3}}{14}.$$

So, if we choose $\pi \in \mathcal{O}_L$ right, we have $\pi\bar{\pi} = 7$ and $x = \pi/\bar{\pi}$.

In this example, the radical extensions B_p are given by

$$B_2 = \langle T(\mathbf{Q}), \mu_4^\tau, \sqrt[4]{x^\tau} \rangle; \text{ and}$$

$$B_p = \langle T(\mathbf{Q}), \mu_p^\tau, \sqrt[p]{x^\tau} \rangle \text{ for } p \text{ an odd prime.}$$

The primes that affect entanglement are again only 2, 3 and 7. We have $E(B) = E(B_{\mathrm{ab}}) = E((B_{42})_{\mathrm{ab}})$. Since x has valuation 1 at the prime π of L, we see that $(\sqrt[4]{x^\tau})^2$ is not a root of unity times an element of K^*. By the definition of B_{ab}, this implies the 4th root of x^τ is not an element of B_{ab}. So, we do not need to adjoin extra torsion division points to write $(B_{42})_{\mathrm{ab}}$ as a product of torsion division points and Kummer roots. Specifically, if we define $W = \langle T(K), \sqrt[6]{x^\tau} \rangle$, we have $(B_{42})_{\mathrm{ab}} = \mu_{84}^\tau W$.

Adjoining the Kummer square and cube division points of x^τ to L and K we get

$$L(\sqrt{x^\tau}) = \mathbf{Q}(\zeta_3, \sqrt{7});$$

$$L(\sqrt[3]{x^\tau}) = \mathbf{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1}); \text{ and}$$

$$L(\sqrt[6]{x^\tau}) = \mathbf{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1}, \sqrt{7}).$$

$$K(\sqrt{x^\tau}) = \mathbf{Q}(\sqrt{7});$$

$$K(\sqrt[3]{x^\tau}) = \mathbf{Q}(\zeta_7)^+; \text{ and}$$

$$K(\sqrt[6]{x^\tau}) = \mathbf{Q}(\sqrt{7}, \zeta_7 + \zeta_7^{-1}).$$

Note that as in the previous example, adjoining these points to L gives quadratic extensions of the real fields obtained by adjoining these points to K.

The entanglement group $E = E(\mu_{84}^\tau W)$ is now isomorphic to

$$\mathrm{Aut}_{\mu_3}(\mu_{84})/\mathrm{im}(G_W).$$

Using the same conclusion drawn from Proposition 6.6 in the last example, we see that the image of G_W is given by $\mathrm{Gal}(\mathbf{Q}^{\mathrm{ab}}/L(W)) = \Gamma_{L(W)}$, restricted to μ_{84}. Because $\mathbf{Q}(\mu_{84})$ is a quadratic extension of $L(W)$, the image of G_W is

a group of order 2 and E is again an abelian group of order 6. The automorphism τ of $\mathbf{Q}(\mu_{84})$ that has $L(W)$ as its invariant field is given by

$$\begin{aligned} \tau : \quad \zeta_7 &\mapsto \zeta_7^{-1} \\ \zeta_3 &\mapsto \zeta_3 \\ \zeta_4 &\mapsto \zeta_4^{-1}. \end{aligned}$$

To compute the correction factor in the density formula, we need to compute the image of A_p in E, for $p = 2, 3, 7$.

The group A_2 now has order 8, but since E has a unique subgroup of order 2, the computation of the image of A_2 in the previous example almost identically applies here. That computation shows that the image of A_2 has order at least 2, which suffices to show that it has order exactly 2.

The computation for the group A_3 of order 3 proceeds exactly the same as in the last example, and we obtain that A_3 is the unique subgroup of order 3 in E.

For A_7 we again only need to consider the image of

$$A_7' = \mathrm{Aut}_{T(K)} \left(\langle T(K), \mu_7^\tau \rangle \right).$$

We extend a generator of this cyclic group of order 6 to an automorphism σ of B with the identity on A_p with $p \neq 7$. Since $\langle T(K), \mu_7^\tau \rangle \cap W$ equals $T(K)$, we see that σ acts as the identity on W, so the image of A_7' in E is generated by $\sigma|_{\mu_{84}^\tau}$. Since the unique subgroup of $\mathrm{Aut}(\mu_{84})$ maps injectively to E, the image of A_7 is at least order 3. Therefore consider σ^3. This acts on μ_{84} as follows:

$$\begin{aligned} \sigma^3 : \quad \zeta_7 &\mapsto \zeta_7^{-1} \\ \zeta_3 &\mapsto \zeta_3 \\ \zeta_4 &\mapsto \zeta_4 \end{aligned}$$

This is not contained in the image of G_W which we explicitly computed above, and the map from A_7 to E is therefore surjective.

This leads to the following table.

	2	3	7
1	+	+	+
χ	−	−	−
χ^2	+	−	−
χ^3	−	+	−
χ^4	+	−	−
χ^5	−	−	−

Because of the same cancellation as in the previous example, the correction factor is again

$$C(T, V, t) = \frac{42}{41}.$$

For almost all primes p we have that $\#A_p = p(p-1)$, with as the only exception $\#A_2 = 8$ and $\#A_3 = 2$. Assuming GRH, this gives a density of

$$\frac{42}{41} \cdot \prod_{p \text{ prime}} \left(1 - \frac{1}{\#A_p}\right) = \frac{42}{41} \cdot \frac{7}{4} \cdot \frac{4}{5} \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right).$$

Chapter 7

Enumerating ABC triples

7.1 Introduction

The *radical* $\mathrm{rad}(n)$ of a positive integer n is defined to be the product of the prime numbers dividing n. We say that positive integers a, b, c form an *ABC triple* if they satisfy the following conditions:

- $a + b = c$;
- $a \leq b$;
- $\gcd(a, b, c) = 1$, and
- $\mathrm{rad}(abc) < c$

The two smallest examples of ABC triples are $1 + 8 = 9$ and $5 + 27 = 32$, with radicals $2 \cdot 3 = 6$ and $2 \cdot 3 \cdot 5 = 30$ respectively. There are in fact infinitely many ABC triples. For example, for every positive integer n, the sum $1 + (64^n - 1) = 2^{6n}$ defines an ABC triple since 9 divides $(64^n - 1)$ and we have $\mathrm{rad}((64^n - 1)2^{6n}) \leq \frac{2}{3}(64^n - 1) \leq 2^{6n}$.

The *quality* $q(a, b, c)$ of an ABC triple is defined as

$$q(a, b, c) = \frac{\log(c)}{\log(\mathrm{rad}(abc))}.$$

By the fourth condition for ABC triples, this quality is always greater than 1.

The famous *ABC conjecture* [33] proposed by Masser and Oesterlé in 1985 states that the limsup of the quality of all ABC triples is equal to 1.

Over the years, it has become popular to search for triples with high quality [26, 29]. The current record is held by the triple $2 + 3^{10} \cdot 109 = 23^5$ with quality approximately 1.630, found by Eric Reyssat in 1987.

In this chapter, we report results of the project *ABC@home*, a distributed computing project built on the BOINC platform [1], for which many people worldwide contributed computing resources to enumerate *all* ABC triples with $c < 10^{18}$.

In Section 7.2 we derive an upper bound for the number of such ABC triples, and in Section 7.3 we give the algorithm used by *ABC@home* to perform the enumeration. After that, in Section 7.4 we describe a number of algorithmic implementation details to accelerate the process, and finally Section 7.5 contains an overview of the produced data.

Related efforts have previously been made. In 1993, Elkies and Kanapka used a similar, but unpublished, algorithm to enumerate all ABC triples below 2^{32} with quality above 1.2. Their results are no longer available from their original location, but are mirrored at `http://www.abcathome.com/Elkies1993/`.

In 2007, Jeroen Demeyer computed all ABC triples with $c \leq 2^{67} \approx 1.4 \cdot 10^{20}$ and quality at least 1.4 (see [11]). His results have been incorporated into the tables of known ABC triples with quality at least 1.4 maintained by Nitaj [26] and de Smit [29].

7.2 Bounds

In this section we derive an upper bound for the number of ABC triples.

Theorem 7.1. *For every $\varepsilon > 0$, the number of ABC triples $a + b = c$ with $c < N$ is $O(N^{2/3+\varepsilon})$.*

The main ingredient of the proof is the following theorem.

Theorem 7.2. *Let α be a real number with $0 < \alpha \leq 1$. Then for every $\varepsilon > 0$, the number $X(N, \alpha)$ of positive integers $x < N$ with $\operatorname{rad}(x) < N^\alpha$ is $O(N^{\alpha+\varepsilon})$.*

Proof. This is Theorem 12 from section II.1 in [34]

□

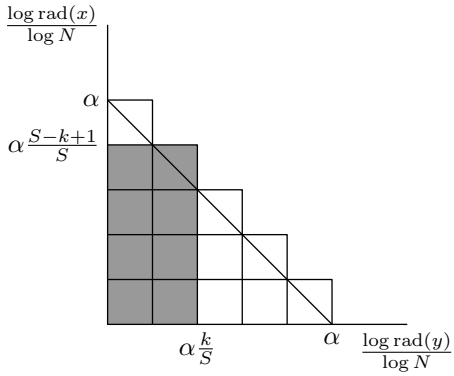
Corollary 7.3. *Let α be a real number with $0 < \alpha \leq 1$. Then for every $\varepsilon > 0$, the number $Y(N, \alpha)$ of pairs of coprime positive integers $x, y < N$ with $\operatorname{rad}(xy) < N^\alpha$ is $O(N^{\alpha+\varepsilon})$.*

Proof. Let $\varepsilon > 0$ be an arbitrary positive real number.

Let S be a positive integer, and k an integer with $0 < k \leq S$. Define the set R_k to be

$$R_k = \Big\{ x, y \in \mathbf{Z}_{\geq 1} : \quad \begin{array}{l} x, y < N; \\ x,\ y \text{ coprime}; \\ \operatorname{rad}(x) < N^{\alpha \frac{S-k+1}{S}}; \\ \operatorname{rad}(y) < N^{\alpha \frac{k}{S}} \end{array} \Big\}.$$

In $\log \operatorname{rad}(x)$, $\log \operatorname{rad}(y)$ space, we can depict R_k as the following rectangle.



By using Theorem 7.2 twice, for x and y separately, we can for every $\delta > 0$ bound the order of R_k from above by

$$\#R_k = O(N^{\alpha\frac{S-k+1}{S}+\delta} N^{\alpha\frac{k}{S}+\delta}) = O(N^{\alpha+\frac{1}{S}+2\delta}).$$

Since the union $\bigcup_{0<k\leq S} R_k$ covers the set we are counting in this Corollary, we find $Y(N,\alpha) \leq S \cdot \#R_k = O(N^{\alpha+\frac{1}{S}+2\delta})$.

This holds for every $\delta > 0$ and S, so we can choose them such that $\frac{1}{S} + 2\delta < \varepsilon$ to complete the proof. □

It is often convenient to sort the integers in an ABC triple by radical rather than by size. We use the following notation for that purpose.

Definition 7.4. If $a + b = c$ is a triple of positive integers, let (x, y, z) be a permutation of (a, b, c) such that

$$\mathrm{rad}(x) \leq \mathrm{rad}(y) \leq \mathrm{rad}(z).$$

We then define $x(a,b,c) = x$, $y(a,b,c) = y$ and $z(a,b,c) = z$.

Proof of Theorem 7.1. Let $a + b = c$ be an ABC triple with $c < N$. For brevity, we write $x = x(a,b,c)$, $y = y(a,b,c)$ and $z = z(a,b,c)$.

We have $\mathrm{rad}(xy) < \mathrm{rad}(xz) < \mathrm{rad}(yz)$, so we can derive

$$\begin{aligned} \mathrm{rad}(xy)^3 &< \mathrm{rad}(xy)\mathrm{rad}(xz)\mathrm{rad}(yz) \\ &= \mathrm{rad}(xyz)^2 < c^2 < N^2. \end{aligned}$$

We conclude $\mathrm{rad}(xy) < N^{2/3}$.

Given any two coprime positive integers x, y, there are at most 2 ABC triples $(\{x, y, x+y\},\ \{x, y, |x-y|\})$ that could correspond to this pair x, y, so we get an upper bound

$$\#\{\text{ABC triples } a+b=c<N\} \leq 2\#\{x, y \in \mathbf{Z}_{\geq 1} : x, y < N \text{ and } \mathrm{rad}(xy) < N^{2/3}\}.$$

The theorem now immediately follows from Corollary 7.3. □

Lower bound

The following theorem by Sander Dahmen provides an asymptotic lower bound for the number of ABC triples. It builds on earlier results and methods from van Frankenhuysen [14] and Stewart and Tijdeman [33].

Theorem 7.5 (S. Dahmen, [10])**.** *For every $\varepsilon > 0$ and N large enough, the number of ABC triples $a + b = c$ with $c < N$ is at least* $\exp((\log N)^{1/2-\varepsilon})$.

7.3 Enumeration algorithm

Here we describe the main enumeration algorithm used in the ABC@home project.

The speed of the algorithm we give below is not asymptotically optimal. One could instead enumerate every potential triple and execute a sub-exponential time factoring algorithm such as the Quadratic Sieve, or heuristically the General Number Field Sieve [27], to obtain a run time of $O(N^{2/3+\varepsilon})$ as a consequence of Theorem 7.1.

However, in the search range that is currently feasible, the integers to be considered are small enough that they can be factored much more efficiently using different methods. The algorithm from this section does this using a combination of sieving small factors in blocks of numbers simultaneously, and basic trial division.

Proposition 7.6. *For positive integers a and b, the following algorithm enumerates all squarefree integers x satisfying $a \leq x < b$ in factored form.*

Algorithm 7.7.

1. Create a list of integers $r(n)$ for $a \leq n < b$, initialized to $r(n) = 1$.
2. Create a list of sets $P(n)$ for $a \leq n < b$, initialized to $P(n) = \emptyset$.
3. Loop over all primes p with $p^2 < b$:
   (a) For all $n \equiv 0 \bmod p$ and $a \leq n < b$:
      i. Multiply $r(n)$ with p.
      ii. Add p to $P(n)$.
   (b) For all $n \equiv 0 \bmod p^2$ and $a \leq n < b$:
      i. Set $r(n) = 0$.
4. Loop over all n with $a \leq n < b$ and $r(n) \neq 0$:
   (a) If $r(n) \neq n$, add $n/r(n)$ to $P(n)$.
   (b) Return the squarefree integer $r(n)$ with its prime factors $P(n)$.

Proof. If an integer $n < b$ is not squarefree, there is a prime p such that $p^2 \mid n$. Since we then have $p^2 \leq n < b$, we set $r(n)$ to 0 in step 3b. Conversely, if $r(n)$ is 0, it can only have been set to 0 in this step, so n is divisible by the square of a prime. We conclude that this algorithm indeed returns all squarefree integers between a and b.

Finally, note that $r(n)$ divides n, so the quantity $q = n/r(n)$ added to the set $P(n)$ in step 4a is an integer. In fact, q is prime since it has no prime divisors p with $p^2 \leq n/r(n) \leq n < b$. This implies that $P(n)$ indeed contains exactly the prime divisors of $n = r(n) = \mathrm{rad}(n)$. □

Before we give the algorithm used to enumerate ABC triples, we first state and prove a number of elementary propositions that provide limits for steps in the algorithm.

Proposition 7.8. *Let n be a positive integer not divisible by primes p with $p^3 \leq n$. Then n is either the square of a prime or squarefree.*

Proof. Suppose that n is not squarefree and let q be a prime divisor of n with $\mathrm{ord}_q(n) \geq 2$. Because we have $q^3 > n$, we then find that $n/q^2 < n^{1/3}$, so $n/q^2 = 1$ and n is the square of a prime. □

Proposition 7.9. *Let $n > 1$ be an integer not divisible by primes $p < P$. Then n is either a prime power or we have $\mathrm{rad}(n) > P^2$.*

Proof. If n has only one prime divisor, it is a prime power. Otherwise, since n is not 1, the radical of n has at least two prime divisors p and q, with $p \geq P$ and $q > P$, the product of which is greater than P^2. □

Theorem 7.10. *Given integers N, m_x, M_x, m_y, M_y, and squarefree positive integers t, g with $g \mid t$, Algorithm 7.11 lists exactly all ABC triples $a + b = c$ satisfying*

- $c < N$;
- $\gcd(x, t) = g$;
- $m_x \leq \mathrm{rad}(x) < M_x$; *and*
- $m_y \leq \mathrm{rad}(y) < M_y$,

where $x = x(a, b, c)$ and $y = y(a, b, c)$.

Algorithm 7.11.

1. Pre-compute the list of prime numbers below $N^{1/3}$.
2. Generate list L_x of square-free integers r with $\gcd(r, t) = g$ in $[m_x, M_x)$ in factored form.
3. Generate list L_y of square-free integers coprime with g in $[m_y, M_y)$ in factored form.
4. Generate list X of positive integers $< N$ with radical in L_x.
5. Generate list Y of positive integers $< N$ with radical in L_y.
6. Sort X and Y by size.

7. Partition X into subsets $(X_1, \ldots)$ and Y into subsets $(Y_1, \ldots)$.

8. Loop over pairs of sets (X_i, Y_j):

   (a) Generate rectangular table with $r(x, y)$ and $s(x, y)$ for $x \in X_i$, $y \in Y_j$.

   (b) Initialize $r(x, y) = 1$ (partial radical found so far) and $u(x, y) = x + y$ (unfactored part).

   (c) Loop over all primes p up to a given sieve bound:

      i. Sort elements of X_i into their residue classes mod p.

      ii. Loop over $y \in Y_j$:

         A. Find all elements $x \in X_i$ such that $p \mid x + y$, using the pre-sorted list mod p.

         B. Divide all factors p from $u(x, y)$.

         C. Multiply $r(x, y)$ with p.

   (d) Loop over all elements $x + y$ in the table

      i. If x and y are not coprime, skip this triple.

      ii. If $r(x, y) > c/\mathrm{rad}(xy)$, skip this triple.

      iii. Perform trial division by consecutive primes p, updating $r(x, y)$ and $u(x, y)$ as above, until one of the following occurs.

      iv. If $p^3 > u(x, y)$, test if $u(x, y)$ is a square and use Prop. 7.8.

      v. If $p^2 \cdot r(x, y) > c/\mathrm{rad}(xy)$, test if $u(x, y)$ is a prime power and use Prop. 7.9.

      vi. In either case, if $\mathrm{rad}(xyz) > c$ skip this triple. If $\mathrm{rad}(x) < \mathrm{rad}(y) < \mathrm{rad}(z)$ return this triple. Otherwise, skip it.

   (e) Repeat the above for a table of elements $|x - y|$ for $x \in X_i$, $y \in Y_j$.

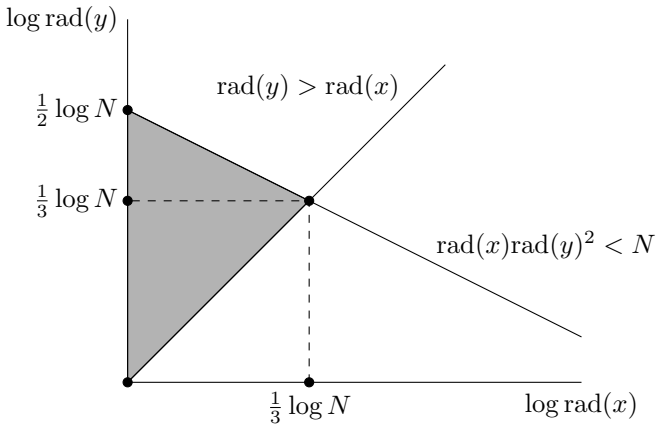
Proof. From the block structure of the algorithm it is clear that all potential triples with radicals of x and y in the right range are considered. Propositions 7.8 and 7.9 then ensure that the right ones are returned.

The remaining point of attention is verifying that the list of pre-computed primes in step 1 is long enough. For listing the squarefree integers using Algorithm 7.7 a list of primes up to the square root of the upper bound of the interval is sufficient. Since the radicals of x and y are at most $N^{1/3}$ and $N^{1/2}$, respectively, we primes up to $N^{1/4}$ suffice for this step.

The trial division loop only needs to loop over primes up to $N^{1/3}$ since the loop terminates at the latest when $u(x, y)$ is not divisible by any primes p with $p^3 \leq u(x, y) < N$ according to Proposition 7.8. □

We use this algorithm to enumerate *all* ABC triples with $c < N$.

The range of possible values for pairs $(\mathrm{rad}(x), \mathrm{rad}(y))$ is determined by the inequalities $\mathrm{rad}(x) < \mathrm{rad}(y)$ and $\mathrm{rad}(x)\mathrm{rad}(y)^2 < N$:



We have covered this triangle by rectangles, and have distributed the resulting work units over participating clients using the BOINC framework.

7.4 Implementation details

In this section we describe a number of implementation details that have a significant impact on performance.

Small prime pre-selection

Algorithm 7.11 processes a block with a prescribed value for $\gcd(x, t)$. This allows us to ensure $\gcd(x, y)$ will not contain primes dividing t, which makes the number of discarded potential triples due to a common factor in x and y significantly smaller. In practice, we take $t = 2 \cdot 3 \cdot 5 \cdot 7 = 210$. Adding more primes produced no significant extra speed-up.

Pre-sorting

In step 6 of Algorithm 7.11, we sort X and Y by size prior to dividing them into smaller sets. After doing this, some sub-blocks $X_i \times Y_j$ will only contain integers so small that they can only lead to triples with c smaller than the radicals considered in this work unit. We can discard these sub-blocks early.

Division strength reduction

In the sieving stage of the enumeration algorithm, we compute the remainders of a large number of integers modulo a relatively small set of primes. We have implemented an approach described in [15].

Theorem 7.12 (Granlund, Montgomery, [15])**.** *Suppose m, p, k are non-negative integers such that $p \neq 0$ and*

$$2^{M+k} \leq mp \leq 2^{M+k} + 2^k.$$

Then $\lfloor n/p \rfloor = \lfloor mn/2^{M+k} \rfloor$ for every integer n with $0 \leq n < 2^M$.

We have pre-computed such integers m and k for every prime $p < 10^6$ with $M = 64$. This allows us to replace an integer division by p by a multiplication with m followed by an integer division by a power of two.

A remainder operation of n divided by p can then be performed by computing $n - p\lfloor n/p \rfloor$.

Divisibility testing

In the trial division stage, we test divisibility of a large number of integers by a relatively small number of primes.

Proposition 7.13. *Let $p < 2^M$ be an odd prime number. Let q satisfy $0 < q < 2^M$ and $pq \equiv 1 \bmod 2^M$. Then for every integer n with $0 \leq n < 2^M$ we have*

$$p \mid n \iff nq \bmod 2^M < \left\lfloor \frac{2^M}{p} \right\rfloor.$$

Here $nq \bmod 2^M$ is the unique non-negative integer smaller than 2^M that is congruent to $nq \bmod 2^M$.

Proof. Multiplication by p gives a permutation of $\mathbf{Z}/2^M\mathbf{Z}$ and maps the integers between 0 and $\lfloor 2^M/p \rfloor$ to the multiples of p between 0 and 2^M. Multiplication by q gives the inverse permutation, so the proposition follows. □

By precomputing q and $\lfloor 2^M/p \rfloor$ for all primes $p < 10^6$ and $M = 64$, we can implement divisibility tests by p as a 64-bit multiplication and a comparison.

Delayed bound checking

The tests 8.d.iv and 8.d.v in the inner loop that check if we can stop processing the current potential triple are relatively expensive. Instead of performing these tests after every prime p, we process 16 primes before every test. This empirically proved a good trade-off between not testing too many primes, and not testing the bounds too often.

To accommodate this, we have to make the list of pre-computed primes 15 elements longer than just the primes up to $N^{1/3}$.

Prime power testing

In step 8.d.v we have to test if a number is a prime power. Due to the delayed bound checking described before, we have already tested divisibility by (at least) the first 16 primes, so we need only consider powers of primes at least 57. Since 57^{11} is greater than 10^{18}, we additionally only need check up to 10th powers.

We perform tests for squares and cubes by first checking if the number is a square or cube, respectively, modulo 63, and if so, doing a binary search through the possible range of roots. These two tests check for any squares and cubes, not just prime powers.

After repeatedly taking 2nd and 3rd roots, we check if the remaining integer is a 5th or 7th power of a prime by table lookup in the precomputed set of 902 such prime powers.

7.5 Data

As part of the ABC@home project a large number of volunteers have executed the algorithm described in the previous sections. The entire search space for the enumeration algorithm has been split up into a large number of so-called *workunits*. Each of these workunits has been sent to multiple clients to ensure their outputs match.

Since many workunits are expected to contain no triples, this output check is not yet sufficiently strong to ensure the clients have properly and completely searched their section of the search space. To that end, the clients report not only the triples they found in their section of the search space, but also a number of internal statistics and counters. This is possible since the algorithms are fully deterministic and platform independent.

The search has resulted in a total of 14 482 065 ABC-triples below 10^{18}. In this section we show a number of tables and graphs highlighting parts of these data. The full dataset is available for download from the website at:

`http://www.abcathome.com/data/`

The first figure (Figure 7.14) shows the number of triples below each power of ten up to 10^{18}. Figure 7.15 shows the number of triples of a given size graphically, and additionally shows how many of these triples have quality larger than $1.1, \ldots, 1.5$.

The next tables show a selection of data on how often specific values of a, b and c occur in the set of found triples. Figure 7.16 does this for a set of small values of a. Figures 7.17, 7.18, 7.19 show the most common values for a, b and c for $c < 10^{14}$, and $c < 10^{16}$ and $c < 10^{18}$, respectively.

The next two tables switch to triples avoiding certain primes. Specifically, Figure 7.20 gives the number of triples below 10^{18} where $\mathrm{rad}(abc)$ is coprime to a selection of small integers. Next, Figure 7.21 gives (indirectly) for each integer p the smallest triple which is not divisible by any odd primes up to and including p.

Figure 7.22 concludes the set of tables with a list of all seven pairs of triples found with identical quality.

Cover illustration

The image on the cover, which is reproduced on the opposite page, illustrates the distribution of $\mathrm{rad}(abc)$ over $\mathrm{rad}(a)$, $\mathrm{rad}(b)$ and $\mathrm{rad}(c)$. More precisely, let S be the set of triples x, y, z of (not necessarily positive) coprime integers satisfying $x + y = z > 0$ and $\mathrm{rad}(|xyz|) < \max(|x|, |y|, |z|)$.

Note that if we would restrict to positive integers here, we would get regular ABC triples. As it is defined, the set S has 6-fold symmetry: given $(x, y, z) \in S$, every permutation of $\{|x|, |y|, |z|\}$ leads to exactly one triple in S by choosing proper signs.

If (x, y, z) is a triple in S, define $r = \mathrm{rad}(|xyz|)$. Then because x, y, z are coprime, we have $\mathrm{rad}(|x|)\mathrm{rad}(|y|)\mathrm{rad}(z) = r$ and therefore

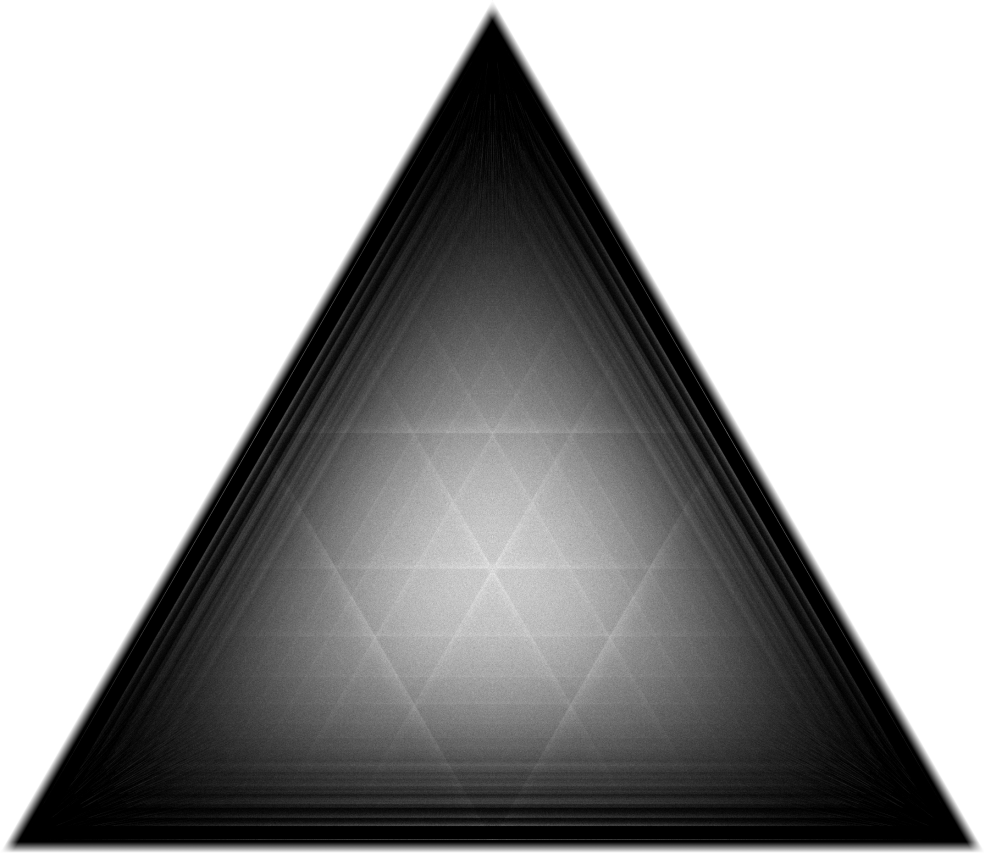
$$\frac{\log \mathrm{rad}(|x|)}{\log(r)} + \frac{\log \mathrm{rad}(|y|)}{\log(r)} + \frac{\log \mathrm{rad}(z)}{\log(r)} = 1.$$

If we take an equilateral triangle T with sides $\frac{2}{3}\sqrt{3}$, and P any point inside T, then the sum of the distances of P to the three sides of T equals 1, and these distances uniquely define P. We can therefore interpret the three fractions $\frac{\log \mathrm{rad}(|x|)}{\log(r)}$, $\frac{\log \mathrm{rad}(|y|)}{\log(r)}$, $\frac{\log \mathrm{rad}(z)}{\log(r)}$ as coordinates in T.

If the radical of a triple is almost entirely concentrated in a single integer, the triple lies near a corner of T. If on the other hand the radical is distributed evenly among the three integers, the triple will lie near the center of T. The image now displays the distribution over T of triples in S with $z < 10^{18}$.

Acknowledgements

The author would like to thank Jeroen Demeyer for useful discussions and suggestions on the performance of algorithms for enumerating ABC triples, Alexander Petric, Joppe Bos and Alyssa Milburn for assisting with verifying and debugging the implementation, Hendrik Verhoek and Alyssa Milburn for setting up and maintaining the infrastructure for the project, and all volunteers for contributing.



n	#
1	1
2	6
3	31
4	120
5	418
6	1 268
7	3 499
8	8 987
9	22 316
10	51 677
11	116 978
12	252 856
13	528 275
14	1 075 319
15	2 131 671
16	4 119 410
17	7 801 334
18	14 482 065

Figure 7.14: Number of triples below 10^n.

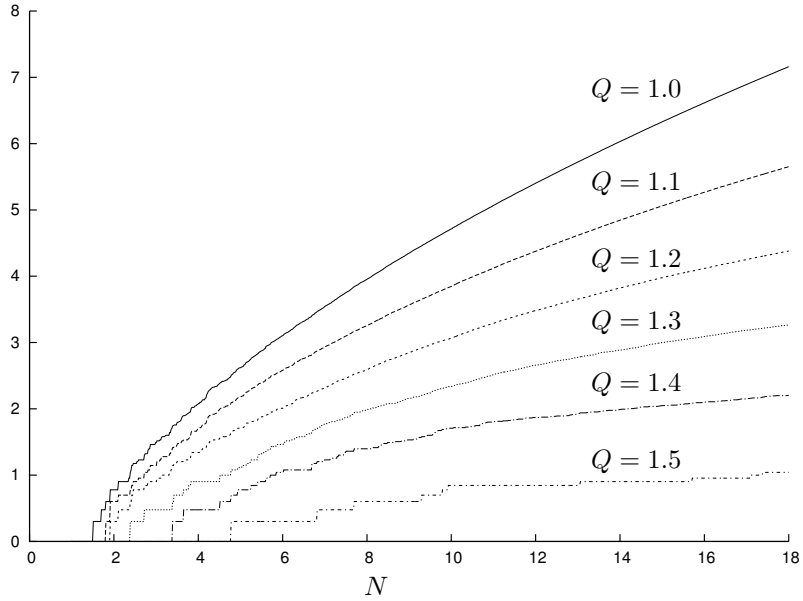


Figure 7.15: $^{10}\log \#\{\text{triples with } c < 10^N, \text{quality} > Q\}$

a	#	a	#
1	45 603	15	222
2	1 965	16	2 026
3	2 936	17	2 347
4	1 967	18	119
5	3 288	19	2 141
6	117	20	132
7	3 233	25	3 696
8	1 849	27	2 875
9	3 044	30	8
10	143	32	2 065
11	2 929	64	2 006
12	98	125	3 435
13	2 655	128	1 894
14	127	256	2 175

Figure 7.16: Number of triples below 10^{18} with given a.

a	$^{10}\log a$	#	b	$^{10}\log b$	#	c	$^{10}\log c$	#
1	0.0	9255	7^{16}	13.5	817	5^{20}	14.0	1236
5^4	2.8	866	5^{19}	13.3	753	7^{16}	13.5	1095
5^8	5.6	864	3^{29}	13.8	714	13^{12}	13.4	821
5^6	4.2	862	11^{13}	13.5	693	3^{28}	13.4	801
5^{12}	8.4	851	5^{20}	14.0	662	5^{18}	12.6	791
7^4	3.4	846	13^{12}	13.4	619	3^{29}	13.8	704
7^6	5.1	825	3^{28}	13.4	606	11^{12}	12.5	650
5^2	1.4	819	5^{18}	12.6	570	11^{13}	13.5	637
7^2	1.7	812	7^{15}	12.7	570	7^{15}	12.7	623
5^9	6.3	800	17^{11}	13.5	535	5^{19}	13.3	611
5^{10}	7.0	795	3^{27}	12.9	510	2^{46}	13.8	586
7^3	2.5	794	2^{45}	13.5	463	3^{27}	12.9	550
7^8	6.8	789	23^{10}	13.6	463	2^{44}	13.2	543
5^3	2.1	757	3^{26}	12.4	445	23^{10}	13.6	532
7^5	4.2	750	2^{46}	13.8	438	17^{11}	13.5	497

Figure 7.17: Most frequent values of a, b, c among triples with $c < 10^{14}$

a	$^{10}\log a$	#	b	$^{10}\log b$	#	c	$^{10}\log c$	#
1	0.0	21025	5^{22}	15.4	1716	7^{18}	15.2	2046
5^{8}	5.6	1930	3^{33}	15.7	1598	5^{22}	15.4	1837
5^{6}	4.2	1916	11^{15}	15.6	1591	11^{15}	15.6	1811
5^{12}	8.4	1885	7^{18}	15.2	1587	13^{14}	15.6	1656
5^{4}	2.8	1874	13^{14}	15.6	1380	3^{32}	15.3	1628
7^{6}	5.1	1869	3^{32}	15.3	1352	3^{33}	15.7	1606
7^{4}	3.4	1860	5^{21}	14.7	1262	19^{12}	15.3	1476
7^{8}	6.8	1849	7^{17}	14.4	1103	5^{21}	14.7	1409
7^{12}	10.1	1810	11^{14}	14.6	1083	2^{53}	16.0	1326
5^{2}	1.4	1802	3^{31}	14.8	1069	17^{13}	16.0	1304
7^{2}	1.7	1733	2^{52}	15.7	1056	17^{12}	14.8	1252
5^{9}	6.3	1731	5^{20}	14.0	1039	5^{20}	14.0	1236
5^{10}	7.0	1710	19^{12}	15.3	1038	3^{30}	14.3	1182
7^{3}	2.5	1698	3^{30}	14.3	974	11^{14}	14.6	1149
7^{10}	8.5	1684	13^{13}	14.5	912	2^{52}	15.7	1148

Figure 7.18: Most frequent values of a, b, c among triples with $c < 10^{16}$

a	$^{10}\log a$	#	b	$^{10}\log b$	#	c	$^{10}\log c$	#
1	0.0	45603	7^{21}	17.7	3731	5^{24}	16.8	4104
5^{6}	4.2	3999	5^{25}	17.5	3448	7^{21}	17.7	4075
5^{12}	8.4	3995	11^{17}	17.7	3340	13^{16}	17.8	3830
7^{12}	10.1	3973	13^{16}	17.8	3006	7^{20}	16.9	3566
5^{8}	5.6	3969	5^{24}	16.8	2960	3^{36}	17.2	3399
7^{6}	5.1	3946	3^{37}	17.7	2950	5^{25}	17.5	3287
7^{8}	6.8	3919	7^{20}	16.9	2927	11^{17}	17.7	3154
5^{4}	2.8	3914	3^{36}	17.2	2741	19^{14}	17.9	2987
7^{4}	3.4	3873	11^{16}	16.7	2381	3^{37}	17.7	2870
5^{2}	1.4	3696	19^{14}	17.9	2293	11^{16}	16.7	2838
7^{10}	8.5	3661	17^{14}	17.2	2245	17^{14}	17.2	2654
7^{2}	1.7	3636	3^{35}	16.7	2194	31^{12}	17.9	2518
5^{10}	7.0	3586	2^{59}	17.8	2187	13^{15}	16.7	2391
5^{15}	10.5	3560	13^{15}	16.7	2177	2^{59}	17.8	2390
5^{16}	11.2	3538	5^{23}	16.1	2163	29^{12}	17.5	2369

Figure 7.19: Most frequent values of a, b, c among triples with $c < 10^{18}$

n	#
2	0
3	756 946
5	2 523 717
7	4 194 390
11	6 804 914
13	7 769 311
15	126 233
17	9 207 072
19	9 744 974
21	208 359
23	10 586 016
35	702 418
55	1 152 234
$3 \cdot 5 \cdot 7$	33 105
$3 \cdot 5 \cdot 11$	56 056
$3 \cdot 5 \cdot 7 \cdot 11$	14 314
$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	6 913

Figure 7.20: Number of triples below 10^{18} with rad(abc) coprime to n.

p	triple	quality
3	$4 + 121 = 125$	1.0271
5	$169 + 343 = 512$	1.1987
7	$128 + 4913 = 5041$	1.0945
17	$751 + 130321 = 131072$	1.1486
19	$2048 + 705233 = 707281$	1.0237
29	$263 + 3442688 = 3442951$	1.0037
41	$271 + 38272753 = 38273024$	1.0642
73	$137 + 46268279 = 46268416$	1.0165
137	$8192 + 26171619209 = 26171627401$	1.0044
601	$3539721569 + 562949953421312 = 562953493142881$	1.0895
4871	none with $c < 10^{18}$	

Figure 7.21: Smallest triples with rad(abc) not divisible by any odd primes $\leq p$.

$$
\begin{aligned}
128 + 3645 &= \\
648 + 3125 &= 3773 \\
\mathrm{rad}(abc) &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310
\end{aligned}
$$

$$
\begin{aligned}
27 + 12005 &= \\
125 + 11907 &= 12032 \\
\mathrm{rad}(abc) &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 47 = 9870
\end{aligned}
$$

$$
\begin{aligned}
637 + 52488 &= \\
2704 + 50421 &= 53125 \\
\mathrm{rad}(abc) &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 = 46410
\end{aligned}
$$

$$
\begin{aligned}
729 + 212960 &= \\
81920 + 131769 &= 213689 \\
\mathrm{rad}(abc) &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 89 = 205590
\end{aligned}
$$

$$
\begin{aligned}
8281 + 218700 &= \\
32500 + 194481 &= 226981 \\
\mathrm{rad}(abc) &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 61 = 166530
\end{aligned}
$$

$$
\begin{aligned}
254800 + 23882769 &= \\
2843100 + 21294469 &= 24137569 \\
\mathrm{rad}(abc) &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 181 = 8400210
\end{aligned}
$$

$$
\begin{aligned}
4645188 + 113348636875 &= \\
20095029775 + 93258252288 &= 113353282063 \\
\mathrm{rad}(abc) &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 47 \cdot 53 \cdot 59 \cdot 61 = 32005439130
\end{aligned}
$$

Figure 7.22: Pairs of ABC triples below 10^{18} with the same quality.

Bibliography

[1] D.P. Anderson, *BOINC: A system for public-resource computing and storage*, Proceedings of the 5th IEEE/ACM International Workshop on Grid Computing (2004), 4–10.

[2] E. Artin, *Collected papers*, S. Lang and J.T. Tate (eds.), Addison-Wesley, 1965.

[3] D.J. Bernstein, *Detecting perfect powers in essentially linear time*, Mathematics of Computation **67** (1998), no. 223, 1253–1284.

[4] D.J. Bernstein, *Factoring into coprimes in essentially linear time*, Journal of Algorithms **54** (2005), no. 1, 1–30.

[5] A. Borel, *Linear algebraic groups*, Graduate Texts in Mathematics, vol. 126, Springer Verlag, 1991.

[6] L. Cangelmi and F. Pappalardi, *On the r-rank Artin conjecture, II*, Journal of Number Theory **75** (1999), no. 1, 120–132.

[7] Y.-M.J. Chen, *On primitive roots of one-dimensional tori*, Journal of Number Theory **93** (2002), 23–33.

[8] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer Verlag, 1993.

[9] G. Cooke and P.J. Weinberger, *On the construction of division chains in algebraic number rings, with applications to* SL_2, Communications in Algebra **3** (1975), 481–524.

[10] S.R. Dahmen, *Lower bounds for numbers of ABC-hits*, Journal of Number Theory **128** (2008), no. 6, 1864–1873.

[11] J. Demeyer, *Enumerating ABC triples*, Presented at 25th Journées Arithmétiques, Edinburgh, 2007.

[12] J.D. Dixon, *Problems in group theory*, Dover Publications (New York), 1973.

[13] D. Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer Verlag, 1995.

[14] M. van Frankenhuysen, *A lower bound in the abc conjecture*, Journal of Number Theory **82** (2000), no. 1, 91–95.

[15] T. Granlund and P.L. Montgomery, *Division by invariant integers using multiplication*, ACM SIGPLAN Notices **29** (1994), no. 6, 61–72.

[16] C. Hooley, *On Artin's conjecture*, Journal für die reine und angewandte Mathematik **225** (1967), 209–220.

[17] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer Verlag, 2002.

[18] H.W. Lenstra, Jr., *On Artin's conjecture and Euclid's algorithm in global fields*, Inventiones Mathematicae **42** (1977), 201–224.

[19] H.W. Lenstra, Jr., *Entangled radicals*, Lecture notes of Colloquium Lectures, 112th Annual Meeting of the American Mathematical Society, 2006, `http://www.math.leidenuniv.nl/~hwl/papers/rad.pdf`.

[20] H.W. Lenstra, Jr., P. Moree, and P. Stevenhagen, *Character sums for primitive root densities*, arXiv preprint (2013), arXiv:1112.4816v2.

[21] P. Moree, *On primes in arithmetic progression having a prescribed primitive root*, Journal of Number Theory **78** (1999), no. 1, 85–98.

[22] P. Moree, *Artin's primitive root conjecture — A survey*, Integers **12** (2012), no. 6, 1305–1416.

[23] P. Moree, *Near-primitive roots*, Functiones et Approximatio Commentarii Mathematici **48** (2013), no. 1, 133–145.

[24] P. Moree and P. Stevenhagen, *Computing higher rank primitive root densities*, Acta Arithmetica **163** (2014), no. 1, 15–32.

[25] M. Ram Murty, *On Artin's conjecture*, Journal of Number Theory **16** (1983), no. 2, 147–168.

[26] A. Nitaj, *The ABC conjecture home page*, `http://www.math.unicaen.fr/~nitaj/abc.html`.

[27] C. Pomerance, *A tale of two sieves*, Notices of the AMS **43** (1996), no. 12, 1473–1485.

[28] A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arithmetica **32** (1977), 245–274.

[29] B. de Smit, *ABC triples*, `http://www.math.leidenuniv.nl/~desmit/abc`.

[30] W.A. Stein et al., *Sage Mathematics Software (Version 5.11)*, The Sage Development Team, 2013, `http://www.sagemath.org/`.

[31] P. Stevenhagen, *The correction factor in Artin's primitive root conjecture*, Journal de Théorie des Nombres de Bordeaux **15** (2003), 383–391.

[32] P. Stevenhagen and H.W. Lenstra, Jr., *Chebotarëv and his density theorem*, Mathematical Intelligencer **18** (1996), 26–37.

[33] C.L. Stewart and R. Tijdeman, *On the Oesterlé-Masser conjecture*, Monatshefte für Mathematik **102** (1986), no. 3, 251–257.

[34] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge University Press, 1995.

[35] S.S. Wagstaff, Jr., *Pseudoprimes and a generalization of Artin's conjecture*, Acta Arithmetica **41** (1982), 141–150.

Samenvatting

Dit proefschrift bestaat uit twee onafhankelijke delen. In het eerste deel, dat de Hoofdstukken 1 tot en met 6 beslaat, bouwen we een theorie op om *verstrengelde radicaaluitbreidingen* te beschrijven. Deze theorie gebruiken we om generalisaties te geven van een vermoeden van Artin over *primitieve wortels*.

Het tweede deel bestaat uit Hoofdstuk 7. In dit hoofdstuk beschrijven we het algoritme om alle zogeheten *ABC-drietallen* onder een gegeven grens te bepalen dat gebruikt is door het gedistribueerde online rekenproject ABC@home.

Om het vermoeden van Artin over primitieve wortels te begrijpen kijken we eerst naar de machten van 2. Dit is een snel groeiende rij:

$$2^1 = 2, 2^2 = 2 \times 2 = 4, 2^3 = 2 \times 2 \times 2 = 8, 2^4 = 16, 2^5 = 32, \text{enz.}$$

Als we de resten bij deling door het priemgetal 5 nemen van deze rij, dan raken we in een lus: 2, 4, 3 (8 geeft rest 3), 1 (16 geeft rest 1), 2, 4, 3, 1, enz. We zien dat we, op 0 na, alle mogelijke resten bij deling door 5 krijgen als macht van 2.

Als we hetzelfde doen met het priemgetal 7 in plaats van 5, is dit niet meer het geval. De machten van 2 geven wel nog steeds een lus, 2, 4, 1 (8 geeft rest 1), 2, 4, 1, enz., maar deze lus bevat niet meer alle mogelijke resten op 0 na. In het bijzonder zal een macht van 2 nooit rest 3, 5 of 6 hebben bij deling door 7.

Rekenen met resten na deling door 5 (of 7) noemen we rekenen *modulo* 5 (of 7). Omdat de machten van 2 modulo 5 alle resten op 0 na geven, heet 2 een *primitieve wortel* modulo 5. Zoals we gezien hebben is 2 juist geen primitieve wortel modulo 7, maar bijvoorbeeld 3 wel. We krijgen daarvoor de lus 3, $3^2 = 9$ geeft 2, $3^3 = 27$ geeft 6, en dan verder 4, 5, 1, 3, enz.

Als q een priemgetal groter dan 3 is, zijn er altijd meerdere primitieve wortels modulo q tussen 1 en q. Zo zijn modulo 5 de getallen 2 en 3 primitieve wortels, en modulo 7 hebben we 3 en 5.

Zij $x \neq 0$ een geheel getal. In 1927 formuleerde Artin een vermoeden over hoeveel priemgetallen q er zijn waarvoor x een primitieve wortel is modulo q.

Deze hoeveelheid is uitgedrukt als een zogeheten dichtheid van priemgetallen. We kijken voor een getal N welke fractie van de priemgetallen onder de N deze eigenschap heeft. Als we N dan onbeperkt laten groeien, is het mogelijk dat deze

fractie convergeert naar een getal d tussen 0 en 1. In die situatie zeggen we dat deze verzameling priemgetallen *dichtheid* d heeft.

De redenering achter het vermoeden van Artin is als volgt. Voor het gemak nemen we hier aan dat het gehele getal x geen macht is. Als x geen veelvoud van q is, dan vormen de machten van x modulo q altijd een lus waarvan de lengte een deler van $q-1$ is. Als we deze lengte l noemen, dan heet het quotient $\frac{q-1}{l}$ de *index* van de lus. Het getal x is nu een primitieve wortel modulo q dan en slechts dan als de index 1 is.

Een positief geheel getal is 1 precies als het geen priemdelers heeft. We kunnen dus zien of x een primitieve wortel is door voor elk priemgetal p te controleren of p een deler is van de index.

Laat p nu een priemgetal zijn. Artin heeft een getaltheoretisch argument gegeven om te bepalen voor hoeveel priemgetallen q, het priemgetal p geen deler is van deze index. Deze redenering staat in zijn geheel in Hoofdstuk 1 van dit proefschrift, en de kern van dit argument rust op het begrijpen van de structuur van de p-demachtswortels van x, zowel modulo q als binnen de complexe getallen. Het resultaat ervan is dat de dichtheid van de priemgetallen q waarvoor p geen deler van de index is, gelijk is aan

$$1 - \frac{1}{p(p-1)}.$$

Als we aannemen dat al deze voorwaarden onafhankelijk zijn van elkaar en we daarom al deze dichtheden met elkaar vermenigvuldigen, krijgen we het vermoeden dat de dichtheid van de priemgetallen q waarvoor x een primitieve wortel modulo q is, gelijk is aan het oneindige product

$$\prod_{p \text{ priem}} 1 - \frac{1}{p(p-1)} = \left(1 - \frac{1}{2 \cdot 1}\right)\left(1 - \frac{1}{3 \cdot 2}\right)\left(1 - \frac{1}{5 \cdot 4}\right) \cdots \approx 0,3739558\ldots$$

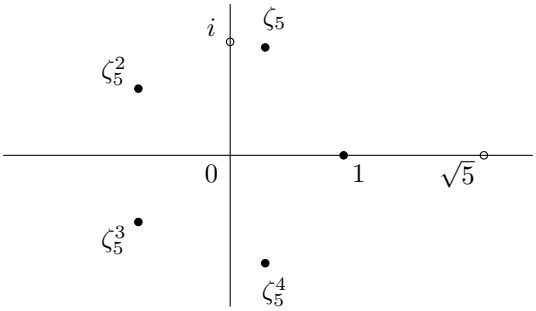
In de jaren '50 hebben Derrick en Emma Lehmer dit eerste vermoeden met een computer gecontroleerd voor de priemgetallen tot 20 000. Voor $x = 2$ bleek dit numerieke experiment goed overeen te komen met de formule hierboven, maar voor $x = 5$ leek de werkelijke dichtheid groter te zijn.

Artin realiseerde zich hierop dat voor $x = 5$ de voorwaarde voor $p = 2$ en $p = 5$ niet onafhankelijk zijn van elkaar. Dit komt door een onverwachte relatie tussen 2-demachtswortels van 5 en 5-demachtswortels van 1 binnen de complexe getallen. Binnen de reële getallen is er slechts een enkele 5-demachtswortel van 1 (namelijk 1 zelf), maar binnen de complexe getallen zijn het er 5, gegeven door

$$1, e^{2\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5}, e^{8\pi i/5}.$$

We schrijven vaak $\zeta_5 = e^{2\pi i/5}$. Met die notatie zijn de 5-demachtswortels van 1 gegeven door $1, \zeta_5, \zeta_5^2, \zeta_5^3$ en ζ_5^4.

Grafisch vormen deze 5 punten de hoekpunten van een regelmatige vijfhoek op de eenheidscirkel.



Het blijkt dat de wortel van 5 te schrijven is in termen van ζ_5:

$$\sqrt{5} = (\zeta_5 + \zeta_5^4) - (\zeta_5^2 + \zeta_5^3).$$

Immers, het is na te rekenen dat het kwadraat van de formule aan de rechterkant gelijk is aan 5. Een dergelijke onverwachte relatie tussen wortels (of radicalen) noemen we *verstrengeling van radicalen*.

Deze relaties zorgen voor een correctiefactor voor de dichtheid van priemgetallen $q \neq 5$ waarvoor 5 een primitieve wortel modulo q is. Dit door Artin aangepaste vermoeden is in 1967 bewezen door Hooley, onder de aanname van de zogeheten Gegeneraliseerde Riemann-Hypothese (GRH). Dit is een nog onbewezen diepe getaltheoretische hypothese die gevolgen heeft voor de nauwkeurigheid waarmee we de verdeling van de priemgetallen kunnen beschrijven. Hij wordt in het bewijs van het vermoeden van Artin gebruikt om het combineren van de oneindig veel condities bij priemgetallen p mogelijk te maken.

In Hoofdstuk 1 geven we een **generalisatie van het vermoeden van Artin naar getallenlichamen**. Onder aanname van GRH heeft de dichtheid in deze generalisatie dezelfde vorm van een oneindig product maal een rationale correctiefactor. Dit hoofdstuk vormt een opzichzelfstaand geheel.

In Hoofdstuk 2 bouwen we een theorie voor verstrengelde wortels op, los van getallenlichamen. De eenhedengroep van een lichaam heeft de eigenschap dat elke eindige ondergroep cyclisch is. Dit blijkt een essentiële eigenschap voor de theorie in dit proefschift. Laat daarom B een abelse groep zijn waarvan alle eindige ondergroepen cyclisch zijn, en G een pro-eindige groep die werkt op B. We schrijven B^G voor de ondergroep van B die invariant is onder de actie van G. Als B/B^G torsie is, dan noemen we B een Galois-radicaaluitbreiding van B^G. In Hoofdstuk 2 beschrijven we een aantal eigenschappen hiervan die sterk lijken op Galoistheorie van lichamen. Eén van de hoofdresultaten uit Hoofdstuk 2 is dat **het beeld van G in $\mathrm{Aut}_{B^G}(B)$ een normale ondergroep is, met een abels quotient** $\mathrm{Aut}_{B^G}(B)/\mathrm{im}(G)$. We noemen dit quotient de *verstrengelingsgroep* van de werking van G op B.

In Hoofdstuk 3 kijken we naar de verstrengelingsgroep van de maximale radicaaluitbreiding van de eenhedengroep van een lichaam K, met de werking van de absolute Galoisgroep van K. Deze noemen we de **absolute verstrengelingsgroep**.

In Hoofdstuk 4 beschrijven we expliciet verstrengelingsgroepen over $\mathbf{Q}$, en gebruiken dit om een algoritme te geven voor het berekenen van **de lichaamsgraad van radicaaluitbreidingen van Q**.

In Hoofdstuk 5 geven we een verdere generalisatie van het vermoeden van Artin over primitieve wortels. We kijken hier naar **bijna-primitieve wortels**, die niet noodzakelijk de gehele eenhedengroep van de maximale orde van een getallenlichaam modolo een priem voortbrengen, maar een ondergroep waarvan de index een gegeven geheel getal t deelt. Een andere generalisatie die we in dit hoofdstuk beschouwen is die van **hogere rang**, waar we een eindige verzameling $x_1, \ldots, x_k$ van niet-0 elementen van een lichaam K nemen, en de dichtheid bepalen van de priemen $\mathfrak{q}$ van K, met voor alle x_i de eigenschap $\mathrm{ord}_{\mathfrak{q}}(x_i) = 0$, waarvoor $x_1, \ldots, x_k$ samen $(\mathcal{O}_K/\mathfrak{q})^*$ voortbrengen.

De algemeenheid van de theorie uit Hoofdstuk 2 stelt ons in staat om in Hoofdstuk 6 ook een generalisatie van het vermoeden van Artin voor **tori van rang 1 over getallenlichamen** te geven. Dit zijn algebraïsche groepen die sterk lijken op de multiplicatieve groep $\mathbf{G}_{\mathrm{m}}$, waarover we in Hoofdstuk 1 en 5 gewerkt hebben. De eis dat een torus T over een lichaam K rang 1 heeft, zorgt er precies voor dat eindige ondergroepen van de groep van punten $T(K)$ cyclisch zijn, waardoor de theorie uit Hoofdstuk 2 van toepassing is.

Het tweede deel van dit proefschrift bestaat uit Hoofdstuk 7. In dit hoofdstuk beschrijven we een algoritme dat we gebruikt hebben in het gedistribueerde online rekenproject ABC@home om alle zogeheten *ABC-drietallen* te vinden kleiner dan 10^{18}. Een ABC-drietal is een drietal positieve gehele getallen (a, b, c) dat voldoet aan de volgende voorwaarden:

- $a + b = c$;
- $a \leq b$;
- a, b en c hebben geen gemeenschappelijke priemdelers, en
- het product van de priemdelers van abc is kleiner dan c.

Het product van de priemdelers van een positief geheel getal n noemen we het *radicaal* van n, en we schrijven dit als $\mathrm{rad}(n)$. De *kwaliteit* van een ABC-drietal wordt gegeven door het volgende quotient:

$$q = \frac{\log(c)}{\log(\mathrm{rad}(abc))}.$$

Deze ABC-drietallen vormen een centrale rol in het *ABC-vermoeden*, dat een uitspraak doet over het limietgedrag van de kwaliteit van ABC-drietallen. Het algoritme dat we beschrijven in dit hoofdstuk is in het kader van het ABC@home-project gebruikt met de hulp van vele vrijwilligers wereldwijd om alle ABC-drietallen kleiner dan 10^{18} te vinden. In Sectie 7.5 sluiten we dit proefschrift af met een aantal observaties over de 14 482 065 gevonden drietallen.

Curriculum vitae

Willem Jan Palenstijn is geboren op 9 juni 1980 te Leiden, en heeft daar in 1998 het VWO-diploma behaald aan het Stedelijk Gymnasium Leiden.

Direct aansluitend is hij aan de Universiteit Leiden begonnen aan de opleidingen Wiskunde en Informatica, en heeft hij in 1999 van beide de propedeuse afgerond. Tijdens het vervolg van de studie Wiskunde heeft hij ook nog een groot aantal Informatica-vakken gevolgd. Onder begeleiding van dr. Bart de Smit heeft hij een afstudeerscriptie *Galois Action on Division Points* geschreven, en is daarmee in 2004 cum laude afgestudeerd. In dat jaar is hij ook aan zijn promotieonderzoek op het Mathematisch Instituut van de Universiteit Leiden begonnen onder begeleiding van prof. dr. Peter Stevenhagen en dr. Bart de Smit.

Over de resultaten hiervan heeft hij tijdens zijn promotietraject voordrachten gegeven op congressen in de Verenigde Staten, Italië, Groot Brittannië, Frankrijk en Duitsland. Naast dit onderzoek heeft hij werkcollege's voor zowel bachelor- als master-vakken gegeven, en voor de Stichting Vierkant voor Wiskunde als vrijwilliger zomerkampen voor middelbare scholieren begeleid.

Van 2009 tot en met april 2014 heeft hij als wetenschappelijk programmeur bij het iMinds-Visielab van de Universiteit Antwerpen in België gewerkt aan algoritmen voor tomografische reconstructie van CT- en MRI-beelden.

Dit proefschrift heeft hij begin 2014 afgerond.