THE CORRECTION FACTOR IN ARTIN TYPE PROBLEMS

MILAD FAKHARI
Master of Science, University of Western Ontario, 2019
Bachelor of Science, Shahid Beheshti University, 2017

A thesis submitted
in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in

MATHEMATICS

Department of Mathematics and Computer Science
University of Lethbridge
LETHBRIDGE, ALBERTA, CANADA

THE CORRECTION FACTOR IN ARTIN TYPE PROBLEMS

MILAD FAKHARI

Date of Defence: August 6, 2021

Dr. A. Akbary Thesis Supervisor	Professor	Ph.D.
Dr. H. Kharaghani Thesis Examination Committee Member	Professor	Ph.D.
Dr. A. Fiori Thesis Examination Committee Member	Associate Professor	Ph.D.
Dr. J. Sheriff Chair, Thesis Examination Committee	Assistant Professor	Ph.D.

Abstract

In 1927, Emil Artin conjectured a product expression for the density of primes p for which a given non-zero integer a is a primitive root modulo p. The conjectured density was proved in 1967 by Hooley under the assumption of the Generalized Riemann Hypothesis. In 2014, Lenstra, Moree, and Stevenhagen introduced a method involving character sums to deduce the formula for the product in the density for Artin's conjecture. The method applies in similar problems such as the density of primes of cyclic reduction for Serre curves. In this thesis, we introduce a generalization of this method which yields product expressions for a large family of problems that can be stated by summations involving the orders of certain finite groups. As a consequence, the product expressions of some Artin type problems, such as the Titchmarsh Divisor Problem in Kummer families for primes in a given arithmetic progression, are computed here.

Acknowledgments

I would like to thank my esteemed supervisor, Dr. Amir Akbary for his invaluable advice, continuous support, and patience. I would also like to thank all the members in my Defence Committee, Dr. Hadi Kharaghani, Dr. Andrew Fiori, and Dr. John Sheriff for their time and valuable comments. I am deeply and heartily indebted to Azar for her sustained patience and support. Finally, I wish to express my sincere thanks to my mother, Zahra, and my sister, Reyhane for their endless support and kindness.

Contents

Chapter 1

Introduction

1.1 Artin Type Problems

The study of primes p for which the decimal expansion of $1/p$ has the longest period was initiated by Gauss. The period of the decimal expansion of $1/p$ exists and has an upper bound $p-1$. The largest period occurs if and only if 10 has order $p-1$ mod p. This means 10 is a primitive root modulo p. Therefore it is natural to ask for which prime p a given integer a is a primitive root modulo p, or whether there are infinitely primes p for which a is a primitive root modulo p.

In 1927, Emil Artin proposed a conjecture for the density of primes p for which a given integer a is a primitive root modulo p. Let a be a non-zero integer that is not ± 1. We can show that the integer a is a primitive root modulo prime p for $p \nmid 2a$ if and only if p does not split completely in $K_q = \mathbb{Q}(\zeta_q, \sqrt[q]{a})$ for all primes $q \mid p-1$, where the *Kummer field* K_q is the splitting field of $x^q - a$ over $\mathbb{Q}$ (see [26, Page 384]). The initial version of Artin's conjecture states that for a given integer a, not 0 and not ± 1, the density of primes p such that a is a primitive root modulo p is

$$A_a = \prod_{q \text{ prime}} \left(1 - \frac{1}{[K_q : \mathbb{Q}]}\right).$$

Observe that if the integer a is not a perfect power, then the conjectured density is independent of the choice of integer a. In fact, if a is not a perfect power, then $[K_q : \mathbb{Q}] = q(q-1)$

for all primes q and thus, $A_a = A$, where

$$A = \prod_{q\,\text{prime}} \left(1 - \frac{1}{q(q-1)}\right) \approx 0.3739558.$$

The constant A is named *Artin's constant*.

In 1957, computer calculations of the density for various values of a, by D. H. Lehmer and E. Lehmer revealed some discrepancies from the conjectured value A. The reason for these inconsistencies is the dependency between the splitting conditions in Kummer fields K_q's. More precisely, if D is the discriminant of K_2, then $K_2 \subset K_{|D|}$. Thus, if p does not split completely in K_2, then it does not split completely in $K_{|D|}$. Hence, the splitting of primes in K_q for $q \mid D$ is not independent of splitting of primes in K_2. To deal with these dependencies, Artin introduced a correction factor. An *entanglement correction factor* appears when $D = \text{disc}(K_2/\mathbb{Q}) \equiv 1 \pmod 4$ and hence the conjectured density is $A_a \cdot E(D)$, where

$$E(D) = 1 - \mu(|D|) \prod_{q|2D} \frac{1}{[K_q : \mathbb{Q}] - 1}.$$

Here $\mu(.)$ is the Möbius function. This way of writing of the correction factor is due to Lenstra, Moree and Stevenhagen [15]. The modified conjecture was proved by Hooley in 1967 under the assumption of the *Generalized Riemann Hypothesis* (GRH) for Kummer fields K_n's for square-free n's. More precisely, Hooley proved, under the GRH, that the density is

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{[K_n : \mathbb{Q}]}.$$

He then showed that the above sum is equal to the corrected conjectured density $A_a \cdot E(D)$.

We call a problem an *Artin type problem* if we can tackle it by Hooley's method introduced in [10]. More specifically, such problems can be formulated in terms of splitting behaviour of primes in extensions of number fields. We next introduce some examples of Artin type problems.

A problem analogous to Artin's conjecture for Elliptic curves is the *cyclicity problem*.

This problem asks for an asymptotic formula for the number of primes $p \leq x$ for which the group of rational points $E_p(\mathbb{F}_p)$ of the reduction mod p of a given elliptic curve E over $\mathbb{Q}$ is cyclic. Here $\mathbb{F}_p$ denotes the finite field of p elements. Let $E[n]$ be the group of n-torsion points of E. Let $\mathbb{Q}(E[n])$ be the n-th division field associated to E. In 1976, J. P. Serre established an asymptotic formula for the cyclicity problem under the assumption of the GRH for division fields $\mathbb{Q}(E[n])$ where n is square-free. Similar to Artin's conjecture there exists a connection between the cyclicity problem and the splitting behaviour of primes in a certain family of number fields. For an elliptic curve E over $\mathbb{Q}$ which has a good reduction modulo p, we have that $E_p(\mathbb{F}_p)$ is cyclic if and only if p does not split completely in $\mathbb{Q}(E[q])$ for all primes $q \neq p$ (see [5, Lemma 2.1]). By employing this fact and following Hooley's method, Serre showed that the density of primes for which $E_p(\mathbb{F}_p)$ is cyclic is

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}(E[n]) : \mathbb{Q}]}. \tag{1.1}$$

Let $\mathbb{Q}^{\text{tor}}$ be the field obtained by adding all the coordinates of the torsion points of E to $\mathbb{Q}$. Let G be the Galois group of $\mathbb{Q}^{\text{tor}}$ over $\mathbb{Q}$. The following representation is known for an elliptic curve E

$$r\colon \operatorname{Gal}(\mathbb{Q}^{\text{tor}}/\mathbb{Q}) \to \operatorname{GL}_2(\hat{\mathbb{Z}}) = \varprojlim \operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

where $\mathbb{Q}^{\text{tor}} = \cup_{n=1}^{\infty} \mathbb{Q}(E[n])$ and $\operatorname{GL}_2(\hat{\mathbb{Z}})$ is the group of invertible matrices with entries in the profinite completion of integers $\hat{\mathbb{Z}}$ (see Section 2.5 for more explanation). An elliptic curve E is named a *Serre curve* if $[\operatorname{GL}_2(\hat{\mathbb{Z}}) : r(G)] = 2$. Let Δ be the discriminant of Weierstrass equation of E. For the family of Serre curves, the authors of [15] show that (1.1) has the product expression

$$\left(1 - \mu(|D|) \prod_{q \mid 2D} \frac{1}{[K_q : \mathbb{Q}] - 1}\right) \prod_{q \text{ prime}} \left(1 - \frac{1}{[K_q : \mathbb{Q}]}\right),$$

where $K_q = \mathbb{Q}(E[q])$ and $D = \operatorname{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{\Delta}))$.

The work of Titchmarsh on $\tau(p-a)$, the number of divisors of a shifted prime $p-a$, provides another example of an Artin type problem.

Theorem 1.1 (Titchmarsh Divisor Problem (TDP), 1931)**.** *Let a be a fixed positive integer. If we assume the GRH for Dirichlet L-functions, then*

$$\sum_{a<p\leq x} \tau(p-a) = \prod_{p\mid a}\left(1-\frac{1}{p}\right)\prod_{p\nmid a}\left(1-\frac{1}{p(p-1)}\right)x + O\left(\frac{x\log\log x}{\log x}\right), \tag{1.2}$$

as $x\to\infty$.

The assumption of the GRH in the above theorem was removed by Linnik in 1961. This theorem can be considered as the Titchmarsh Divisor Problem for family of number fields $\{\mathbb{Q}(\zeta_n) : n\geq 1\}$. In this case, the arithmetic function $\tau(p-1)$ can be related to counting of primes that split completely in cyclotomic fields. Observe that when p is an odd prime, then $p\equiv 1 \mod m$ if and only if p splits completely in $\mathbb{Q}(\zeta_m)$. The prime 2 splits completely in $\mathbb{Q}(\zeta_m)$ if and only if $m\in\{1,2\}$. Therefore for odd primes p we have

$$\tau(p-1) = \#\{m;\ p \text{ splits completely in } \mathbb{Q}(\zeta_m)\}.$$

Observe that in this case the constant in the asymptotic formula (1.2) can also be written as

$$\sum_{n=1}^{\infty}\frac{1}{[\mathbb{Q}(\zeta_n):\mathbb{Q}]}.$$

As other examples of Artin type problems, we can consider the Titchmarsh Divisor Problem for different families such as Kummer fields and division fields of a given Serre curve.

1.2 Product Expressions of the Constants in Artin Type Problems

One of the topics in studying Artin type problems is product expressions for the constants. There are advantages in finding such product expressions. For instance, they help

us in finding the conditions under which the constant becomes zero. Finding these product expressions is not straightforward, since, similar to Artin's conjecture, we should deal with the possible entanglements in the family of number fields. These entanglements lead to correction factors in Artin type problems.

In [15], Lenstra, Moree, and Stevenhagen introduced an effective method in finding product expressions in certain Artin type problems. Their method directly studies the primes that do not split completely in a family of number fields without considering the summation expressions for the constants. For Artin's conjecture they consider the family of Kummer fields and for the cyclicity problem for Serre curves they consider the family of division fields. Then, they interpret these problems using representations attached to the Galois groups of these families. Their method can be described as follows.

Assume that $K_\infty = \cup_n K_n$, where $\{K_n, n \geq 1\}$ is the family of Kummer fields. Let G be the Galois group of K_∞ over $\mathbb{Q}$. Let

$$R_\infty = \{x \in \overline{\mathbb{Q}}^\times ; x^k \in \langle a \rangle \subset \mathbb{Q}^\times \text{ for some } k \in \mathbb{Z}_{>0}\}$$

be the group of radicals that generate the field extension K_∞ of $\mathbb{Q}$. The authors of [15] construct an embedding $r : G \to A$, where $A = \mathrm{Aut}_{R_\infty \cap \mathbb{Q}^\times}(R_\infty)$ is a profinite group such that $A = \prod_p A_p$. Then, they establish the existence of a quadratic character

$$\chi : A \to \mu_2$$

such that $G \cong \ker\chi$, where μ_2 is the multiplicative group $\{\pm 1\}$. Let S be the family of "good Frobenius elements" in A corresponding to primes p that do not split completely in any K_q for primes $q \mid p-1$. Then it is shown in [14], that under the assumption of the GRH, the density of such primes becomes $\nu_A(G \cap S)/\nu_A(G)$, where ν_A is the normalized Haar

measure attached to the profinite group A. It is proved in [15, Theorem 3.3] that

$$\frac{\nu_A(G\cap S)}{\nu_A(G)} = \left(1+\frac{1}{\nu_A(S)}\int_S \chi d\nu_A\right)\frac{\nu_A(S)}{\nu_A(A)}. \tag{1.3}$$

Note that $\nu_A = \prod_p \nu_{A_p}$ and $S = \prod_p S_p$, where ν_{A_p} is the normalized Haar measure on A_p and $S_p \subset A_p$. The authors of [15] also show that $\chi = \prod_p \chi_p$ for certain characters $\chi_p : A_p \to \mu_2$. Therefore, they conclude that (1.3) has the product form

$$\frac{\nu_A(G\cap S)}{\nu_A(G)} = \left(1+\prod_p E_p\right)\prod_p \nu_{A_p}(S_p),$$

where for all except finitely many primes p, we have $E_p = 1$. Thus, the computation of the integral in (1.3) implies the product expression in Artin's conjecture. The authors of [15] applied this method effectively for several Artin type problems such as Artin's conjecture for primes in a given arithmetic progression and near primitive roots. They also extend their method to cover the cyclicity problem for Serre curves. However, their method should be adjusted to deal with prime powers in some Artin type problems such as the Titchmarsh Divisor Problem and the Titchmarsh Divisor Problem for primes in a given arithmetic progression.

The aim of this thesis is to generalize the method introduced in [15] to include the product expressions of Artin type problems involving prime powers. Observe that the character sums method introduced in [15] gives us the product expression of $\nu(G\cap S)/\nu(G)$, where S is a family of "good Frobenius elements" in A attached to the density of primes in each Artin type problem. Instead of finding the product expression of $\nu(G\cap S)/\nu(G)$, the generalization introduced in this thesis yields directly the product expression of the summations appearing in Artin type problems. This helps us to consider a larger family of Artin type problems. More specifically, we can consider the problems such as the Titchmarsh Divisor Problem which are not formulated as a density of a subset of primes. Hence, our generalization can be applied to find new explicit product formulas for some problems such as

the Titchmarsh Divisor Problem in Kummer and division fields and also the Titchmarsh Divisor Problem for primes in an arithmetic progression in Kummer fields.

1.3 This Thesis

This thesis is organized as follows. After introducing needed preliminaries in Chapter 2, in Chapter 3, we formulate and prove two main theorems as generalizations of the method described in [15]. Our generalization has this important advantage that instead of starting with a density of primes, we can consider any absolutely convergence summation

$$\sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)}, \tag{1.4}$$

where $g(n)$ is a multiplicative function and $G(n)$ is a group with the following properties.

Let $(G(n))_{n\in\mathbb{N}}$ and $(A(n))_{n\in\mathbb{N}}$ be inverse systems of finite groups. Moreover, assume that there are injective maps $r_n : G(n) \to A(n)$ for all $n \geq 1$. By taking inverse limit over n, we have an injective map $r : G = \varprojlim G(n) \to A = \varprojlim A(n)$. Further, suppose $A \cong \prod_p A_p$, where $A_p = \varprojlim A(p^i)$. Then, if a character $\chi : A \to \mu_m$ exists such that the sequence

$$1 \to G \xrightarrow{r} A \xrightarrow{\chi} \mu_m \to 1 \tag{1.5}$$

is exact, by our Theorem 3.2 and Corollary 3.3, we have a product expression over primes with a possible correction factor for summation (1.4). Here μ_m is the group of m-th roots of unity in $\overline{\mathbb{Q}}$. For finding the product expression, we first show that by the normalized Haar measure on the profinite group G, the summation (1.4) can be written as a summation of measures of measurable subsets of G. Then, by the injective homomorphism $r : G \to A$, we interpret the new summation as a summation of measurable subsets of A. Next, the property $A \cong \prod_p A_p$ together with the properties of the character χ given in (1.5) helps us to write the desired product expression for (1.4) with a possible correction factor. The following important corollary is a consequence of our Theorem 3.2 and Corollary 3.3, when $\mu_m = \mu_2$.

Corollary 3.4. *Let g be a real multiplicative arithmetic function such that*

$$\sum_{n\geq 1}\frac{|g(n)|}{\#G(n)}<\infty.$$

Let

$$\tilde{g}=\sum_{n\geq 1}g(n)1_{\ker\varphi_{A,n}}$$

be a function from A to $\overline{\mathbb{R}}=[-\infty,\ +\infty]$, where $\varphi_{A,n}:A\to A(n)$ is the projection map. Let

$$\tilde{g}_p=\sum_{k\geq 0}g(p^k)1_{\ker\varphi_{p^k}}$$

be a function from A_p to $\overline{\mathbb{R}}$, where $\varphi_{p^k}:A_p\to A(p^k)$ is the projection map, such that $\tilde{g}=\prod_p\tilde{g}_p$. Let $\chi:A\to\mu_2$ be the character given in (1.5) *and assume that $\chi=\prod_p\chi_p$. Then, if $\int_A\tilde{g}d\nu_A\neq 0$, we have*

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{g(n)}{\#G_n}&=\left(1+\frac{\int_A\tilde{g}\chi d\nu_A}{\int_A\tilde{g}d\nu_A}\right)\int_A\tilde{g}d\nu_A\\&=\left(1+\prod_p\frac{\int_{A_p}\tilde{g}_p\chi_p d\nu_{A_p}}{\int_{A_p}\tilde{g}_p d\nu_{A_p}}\right)\prod_p\int_{A_p}\tilde{g}_p d\nu_{A_p}.\end{aligned}$$

This corollary can be considered as a generalization of (1.3).

To state our next main result, we consider a more specific family of groups $\{G(n):n\geq 1\}$. Let $\{K_n:n\geq 1\}$ be a family of finite Galois extensions of $\mathbb{Q}$ with the property that K_2 contains a quadratic field K and $\zeta_n\in K_n$, where ζ_n is a primitive n-th root of unity. Suppose there exist injective homomorphisms $G(n)\to A(n)$, where $G(n)=\mathrm{Gal}(K_n/\mathbb{Q})$. If both families $\{G(n);n\geq 1\}$ and $\{A(n);n\geq 1\}$ are inverse systems of finite groups, then by taking inverse limit we have injective homomorphism $r:G=\varprojlim G(n)\to A=\varprojlim A(n)$. Suppose that $A=\prod_p A_p$, where $A_p=\varprojlim A(p^n)$. Moreover, suppose there exist different characters

$$\chi_D:A\to(\mathbb{Z}/D\mathbb{Z})^{\times}\xrightarrow{\left(\frac{D}{\cdot}\right)}\mu_2$$

and

$$\psi : A \to \mu_2$$

such that χ_D and ψ are compatible, as defined in (3.15), with the restriction maps $G \to \mathrm{Gal}(\mathbb{Q}(\zeta_{|D|})/\mathbb{Q}) \cong (\mathbb{Z}/D\mathbb{Z})^\times$ and $G \to \mathrm{Gal}(K/\mathbb{Q})$ respectively, where $D = \mathrm{disc}_{\mathbb{Q}} K$. Then, we can construct a character $\chi : A \to \mu_2$ such that $r(G) \subset \ker\chi$. In Theorem 3.5, we explicitly construct such character χ. The computations in Theorem 3.5 for character χ helps us to find the possible correction factor in Corollary 3.4 explicitly. As a consequence of this theorem and Corollary 3.4, we have the following result.

Corollary 3.6. *Let A and G be as above. Assume that $[A : r(G)] = 2$. Let g be a real multiplicative arithmetic function such that*

$$\sum_{n\geq 1} \frac{|g(n)|}{\#G(n)} < \infty.$$

Assume that

$$\tilde{g} = \prod_p \tilde{g}_p = \prod_p \sum_{k\geq 0} g(p^k) 1_{\ker \varphi_{p^k}}$$

is a function from A to $\overline{\mathbb{R}}$, where $\tilde{g}_p$ is a function from A_p to $\overline{\mathbb{R}}$ and $\varphi_{p^k} : A_p \to A(p^k)$ is the projection map. If $\zeta_4 \notin K_2$ and $\zeta_8 \notin K_4$, then

$$\sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)} = \left(1 + \prod_{p|2D} \left(\frac{\sum_{k\geq \ell} g(p^k)/\#A(p^k)}{1+\sum_{k\geq 1} g(p^k)/\#A(p^k)}\right)\right) \prod_p \left(1 + \sum_{k\geq 1} \frac{g(p^k)}{\#A(p^k)}\right),$$

where in the product on primes dividing $2D$, we have $\ell = 1$ for odd primes and for prime 2 we have $\ell = 1$ if D is odd, $\ell = 2$ if $4 \parallel D$, and $\ell = 3$ if $8 \parallel D$.

Note that by Corollary 3.6, we can find the product expression for problems involving prime powers such as the Titchmarsh Divisor Problem. Moreover, in the summation (1.4), instead of $\mu(n)$ or 1, we can consider any multiplicative function $g(n)$ and any family of Galois groups that satisfies conditions of Corollary 3.6.

In Chapter 4, we describe needed properties of two families of fields namely *Kummer fields* and division fields of *Serre curves* for applying the above corollaries. Let a be an integer such that $|a|$ is not a perfect power. For $n \geq 1$, the Kummer field $K_n = \mathbb{Q}(\zeta_n, \sqrt[n]{a})$ is the splitting field of $x^n - a$ over $\mathbb{Q}$. We will show that the inverse limit of the Galois groups $G(n)$ of $K_n/\mathbb{Q}$ is embedded in a profinite group $A = \varprojlim A(n)$, where $A(n) = \left(\begin{smallmatrix} 1 & 0 \\ b & d \end{smallmatrix}\right)$, with $b \in \mathbb{Z}/n\mathbb{Z}$ and $d \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then, we will observe that A satisfies the conditions needed in Corollary 3.6. Thus, by showing $[A : G] = 2$, and employing Corollary 3.6, we derive

$$\sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)} = \left(1 + \prod_{p|2D} \frac{\sum_{k\geq \ell} g(p^k)/p^{2k-1}(p-1)}{1+\sum_{k\geq 1} g(p^k)/p^{2k-1}(p-1)}\right) \prod_p \left(1 + \sum_{k\geq 1} \frac{g(p^k)}{p^{2k-1}(p-1)}\right), \tag{1.6}$$

where in the product on primes dividing $2D$, we have $\ell = 1$ for odd primes and for prime 2 we have $\ell = 1$ if D is odd, $\ell = 2$ if $4 \parallel D$, and $\ell = 3$ if $8 \parallel D$. Using similar ideas, we also find a general product formula for the sum in the left-hand side of (1.6) for the family of division fields of a Serre curve. In addition, at the end of Chapter 4, we prove necessary and sufficient conditions under which the important property $[A : G] = 2$ holds.

In Chapter 5, we generalize Theorem 3.2. This generalization helps us to put more conditions on the set of primes which we consider. As an application, in Section 5.2, we find the explicit product of the Titchmarsh Divisor Problem for primes in a given arithmetic progression for the family of Kummer fields.

There are many directions that one can consider in extending the ideas and methods described in this thesis. We briefly outline some of these possibilities in the final concluding chapter of the thesis.

Chapter 2

Preliminaries

2.1 Topological Groups

In this section, we briefly introduce topological groups. Moreover, we will present the Haar measure and its properties on topological groups.

Definition 2.1. We say a group G is a *topological group* if it is equipped with a topology such that the maps

$$\begin{array}{ll} G \times G \to G & \\ (g_1, g_2) \mapsto g_1 g_2 & \end{array} \quad \text{and} \quad \begin{array}{l} G \to G \\ g \mapsto g^{-1} \end{array}$$

are continuous.

Similarly, one can define *topological rings* and *topological fields*. The following are some examples of topological groups.

Example 2.2. (i) The Euclidean n-space $\mathbb{R}^n$ with the usual topology, coming from the Euclidean norm, forms a topological group under addition.

(ii) If R is a topological ring, then the group of $n \times n$ invertible matrices with entries from R, denoted by $\mathrm{GL}_n(R)$, forms a topological group. This topology is implied by the subspace topology as a subset of the $n \times n$ matrices $\mathrm{Mat}_n(R) \cong R^{n^2}$.

Next, we describe some properties of subgroups of topological groups.

Lemma 2.3. *Let G be a topological group. The following assertions hold.*

(i) A subgroup H of G is open (closed) if and only if the cosets gH are open (closed) for all $g \in G$.

(ii) Every open subgroup of G is closed.

(iii) Every closed subgroup of finite index in G is open.

(iv) If G is compact, then a subgroup H is open if and only if it is closed and has finite index in G.

Proof. (i) For an element g in a topological group G, the maps $g' \mapsto g \cdot g'$ and $g' \mapsto g' \cdot g$ are continuous. Note that $g' \mapsto g \cdot g'$ has a continuous inverse $g' \mapsto g^{-1} \cdot g'$. Thus, it is an open map. Therefore, if H is open, then cosets of H are open. A similar argument shows that if H is closed, then its cosets are closed.

(ii) Let H be an open subgroup of G. The group G is the union of cosets of H. On the other hand, by part (i), each coset is open. Since H is the complement of a union of these cosets, H is closed.

(iii) If H is closed and of finite index in G, its complement $G\backslash H$ is the finite union of some left cosets gH's. Since each gH is closed, then H is open.

(iv) Let H be an open subgroup. Hence, by part (i), any coset of H is open. Thus, if G is compact, then H has finite index, since the collection of H and its cosets is an open cover for G. Therefore, parts (ii) and (iii) imply the desired result. □

By a homomorphism of topological groups we mean a continuous group homomorphism. Similarly, an isomorphism of topological groups is a group isomorphism which is also a homeomorphism of topological spaces.

We call a Borel measure μ on a topological space X *regular* if for every measurable set A, we have

$$\mu(A) = \sup\{\mu(B); B \subset A, B \text{ is compact and measurable}\}.$$

Finally, we introduce the Haar measure on topological groups.

Definition 2.4. A regular Borel measure μ on a topological group G is named *Haar measure*

if it is translation invariant (i.e., $\mu(gA) = \mu(A)$ for any $g \in G$ and for any measurable subset A).

It is known that any locally compact topological group admits a unique Haar measure up to multiplication by a constant (see [4, Section 9.2]).

In the next section, we will define a specific family of topological groups, named profinite groups.

2.2 Profinite Groups

In this section, we introduce profinite groups which are special example of topological groups. The ring of p-adic integers may be considered as a motivation for this concept. Furthermore, the topology on profinite groups attached to Galois groups helps us to obtain the fundamental theorem of Galois theory for the infinite Galois extensions. At the end of this section, we introduce a probability measure on profinite groups. In Chapter 3, we will use this measure to construct and prove our main theorem.

In order to define profinite groups, we need first to introduce inverse systems. An inverse system is a collection of objects indexed by a directed partially ordered set.

Definition 2.5. A nonempty set I equipped with a partial order relation $\leq$ is named a *directed partially ordered set* (a directed *poset* for short) if every pair of its elements has an upper bound.

We next define the concept of an inverse system of a collection of groups.

Definition 2.6. An *inverse system of groups* is a collection of groups $(G_i)_I$, where I is a directed poset, together with a collection of *transition maps* f_{ij} for any pair (i, j) with $i \leq j$. The maps $f_{ij} : G_j \to G_i$ are group homomorphisms such that $f_{ii} = \mathrm{id}_{G_i}$ and $f_{ij} \circ f_{jk} = f_{ik}$ for all $i, j, k \in I$ with $i \leq j \leq k$.

We continue with some examples of inverse systems.

Example 2.7. (i) Consider the directed poset $(\mathbb{Z}, \leq)$ such that $n \leq m$ if and only if $n \mid m$. Then the natural projections

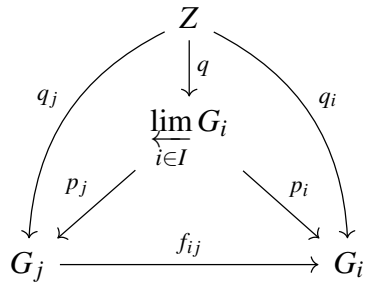
$$f_{nm} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

are well-defined transitions maps when $n \mid m$. Hence $(\mathbb{Z}/m\mathbb{Z}, f_{nm})_{\mathbb{Z}}$ is an inverse system.

(ii) Consider the collection of finite Galois extensions L over a fixed field K. This collection is a directed poset by inclusion. Note that if L and L' are two finite extensions of K, then the compositum of L and L' is a finite extension of K. The set of such L's equipped with the restriction maps $\mathrm{Gal}(L/K) \to \mathrm{Gal}(L'/K)$ for $L' \subset L$ forms an inverse system.

We next define the inverse systems as a categorical concept. Then we will introduce an explicit description of them in Lemma 2.11.

Definition 2.8. The *inverse limit* of the inverse system $((G_i)_{i\in I}, (f_{ij})_{\substack{i,j\in I \\ i\leq j}})$ is a group $\varprojlim_{i\in I} G_i$ together with projection maps $p_i : \varprojlim_{i\in I} G_i \to G_i$ such that $f_{ij} \circ p_j = p_i$ and that satisfy the following universal property: Suppose Z is a group with projection maps $q_i : Z \to G_i$ for $i \in I$ such that $f_{ij} \circ q_j = q_i$ for any $i \leq j$. Then there exists a map $q : Z \to \varprojlim_{i\in I} G_i$ such that the diagram



commutes.

We will drop the index of inverse limit when the directed poset is specified from the context.

Definition 2.9. A group which is isomorphic to an inverse limit of an inverse system of finite groups is called a *profinite group*.

One may define the *profinite ring* in a similar way by starting with an inverse system of finite rings.

Example 2.10. (i) The inverse limit of the inverse system $(\mathbb{Z}/m\mathbb{Z}, f_{nm})$ of rings defined in Example 2.7 (i) is a profinite ring denoted by $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$.

(ii) The inverse limit $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is a profinite ring and $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$. Moreover any element $\alpha \in \mathbb{Z}_p$ has a unique p-adic expansion

$$\sum_{i=0}^{\infty} a_i p^i,$$

with $0 \leq a_i \leq p-1$.

(iii) The multiplicative groups of $\hat{\mathbb{Z}}$ and $\mathbb{Z}_p$, denoted by $\hat{\mathbb{Z}}^\times$ and $\mathbb{Z}_p^\times$ respectively, are profinite groups. Moreover, $\hat{\mathbb{Z}}^\times \cong \prod_p \mathbb{Z}_p^\times$. We note that $\alpha = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p^\times$ if and only if $p \nmid a_0$.

(iv) Any Galois group $\mathrm{Gal}(L/K)$ is a profinite group. More precisely, $\mathrm{Gal}(L/K)$ is the inverse limit of $\mathrm{Gal}(E/K)$ over the finite intermediate fields E ordered by inclusion.

As a consequence of the universal property of the inverse limit, for an inverse system of groups G_i there exists a unique inverse limit up to isomorphism. An explicit description of an inverse limit of $(G_i, f_{ij})_{i,j\in I}$ is given by the next lemma.

Lemma 2.11. *Let $(G_i, f_{ij})_{i,j\in I}$ be an inverse system of groups. Then*

$$\varprojlim G_i \cong \{(g_i)_{i\in I} \in \prod_{i\in I} G_i;\ f_{ij}(g_j) = g_i \ \textit{for all}\ i \leq j\}.$$

Proof. We note that the candidate set on the right side of the above equation, which we show by S, is a subgroup of the direct product of G_i's since f_{ij}'s are group homomorphisms. Consider the projection map p_i from S to G_i. Hence $f_{ij} \circ p_j = p_i$ for all $i \leq j$. Thus, it remains to show that the universal property of Definition 2.8 holds. Let Z be another group with maps $q_i : Z \to G_i$ such that $f_{ij} \circ q_j = q_i$ whenever $i \leq j$. Then the map $q : Z \to \prod G_i$ defined by $q(z) = (q_i(z))_{i\in I}$ yields the desired map in the universal property. □

Next we show that profinite groups are equipped with a compact topology. Each finite group G_i (or ring) can be equipped with the discrete topology. Hence we may consider $\prod G_i$ with the product topology as a topological group. By Lemma 2.11, we consider $\varprojlim G_i$ as a subset of $\prod G_i$. Thus the product topology on $\prod G_i$ yields a subspace topology for the profinite group $\varprojlim G_i$ as a subspace of $\prod G_i$. Hence, $\varprojlim G_i$ with this topology is a topological group. Moreover, the maps f_{ij} and p_i are continuous. Note that p_i's are restrictions of the projection maps of the product topology, and f_{ij}'s are maps between finite discrete topological groups.

Next, we introduce the profinite group attached to a Galois extension. Let L be an arbitrary Galois extension of K. Hence L is the union of finite Galois extensions M of K contained in L. We know that $\mathrm{Gal}(L/K) \cong \varprojlim \mathrm{Gal}(M/K)$ where the limit is taken over the collection of intermediate fields

$$\mathcal{M} = \{M \subset L : M/K \text{ is a finite Galois extension}\}.$$

Therefore $\mathrm{Gal}(L/K)$ is equipped with a topology through the profinite topology on $\varprojlim \mathrm{Gal}(M/K)$. We name this topology *Krull topology*.

The discrete topology for each G_i is compact since G_i is finite. Hence the product topology on $\prod_i G_i$ is compact. On the other hand, if $(g_i)_i \in (\prod G_i) \setminus \varprojlim G_i$ then for some $i \leq j$ we have $f_{ij}(g_j) \neq g_i$. Hence the open subgroup $\mathcal{U} = \{(g'_i)_i \in \prod G_i;\ g'_i = g_i \text{ for } i \leq j\}$ contains $(g_i)_i$, and $\mathcal{U} \cap \varprojlim G_i = \emptyset$. Thus, the subspace $\varprojlim G_i$ is closed in $\prod_i G_i$. Therefore $\varprojlim G_i$ is a compact topological group. This prove the compactness part of the following general proposition about the topology of any profinite group.

Proposition 2.12. *([17, Theorem 1.1.12]) A topological group G is profinite if and only if G is Hausdorff, compact, and totally disconnected.*

We next introduce the abelianization of a profinite group G which is denoted by G^{ab}.

Definition 2.13. Let G be a profinite group. The *commutator subgroup* of G is the closure

of

$$\langle [x,y] \; ; \; x,y \in G \rangle$$

in G, where $[x,y] = x^{-1}y^{-1}xy$ is the *commutator* of x and y. We denote the commutator of G by G'.

We can see that for a closed normal subgroup N of G, the quotient group G/N is abelian if and only if N contains G'. Therefore, we define *abelianization* of G to be $G^{ab} = G/G'$.

Finally, we introduce a probability measure in profinite groups.

A profinite group is endowed with a two sided invariant Haar measure (see [9, Proposition 18.2.1]). This measure is implied by the Haar measure on locally compact groups as described at the end of Section 2.1. Since G is compact, the Haar measure on G is finite (see [4, Proposition 9.3.3]). Hence, we can consider the normalized Haar measure ν_G on the profinite group G, i.e., a measure ν_G with $\nu_G(G) = 1$. This gives a probability measure on a profinite group.

We have the following lemmas regarding the probability measure ν_G on a profinite group G.

Lemma 2.14. *If H is a closed subgroup of a profinite group G, then $\nu_G(H) = 1/[G:H]$.*

Proof. If $[G:H] = n$ then G is the union of n disjoint cosets g_iH $(1 \leq i \leq n)$ of H. Hence,

$$1 = \nu_G(G) = \sum_{i=1}^{n} \nu_G(g_iH) = n \cdot \nu_G(H),$$

which is the desired result. If H has infinite index, then it is contained in the intersection of a decreasing sequence of open subgroup $H_1 > H_2 > \dots$ (see [9, Lemma 1.2.3]). Thus,

$$0 \leq \nu_G(H) \leq \lim_{i \to \infty} 1/[G:H_i] = 0.$$

Therefore, $\nu_G(H) = 0 = 1/[G:H]$. □

Consider the product of measurable spaces G and G'. A product measure $\nu_G \times \nu_{G'}$ on $G \times G'$ is defined by

$$(\nu_G \times \nu_{G'})(H \times H') = \nu_G(H)\nu_{G'}(H'),$$

for all measurable subsets $H \subset G$ and $H \subset G'$.

We have the following property of the normalized Haar measure of products of profinite groups.

Lemma 2.15. *([9, Proposition 18.4.2]) The normalized Haar measure on the direct product $G \times G'$ of profinite groups G and G' coincides with $\nu_G \times \nu_{G'}$.*

We also need to define the direct limit of a direct system of groups. We first introduce a direct system of groups.

Definition 2.16. Let I be a directed partially ordered set. Let $(G_i)_{i\in I}$ be a family of groups together with homomorphisms $f_{ij} : G_i \to G_j$ for all $i \leq j \in I$. We name this family a directed system over I, if $f_{ii} = \mathrm{id}_{G_i}$ and $f_{ik} = f_{jk} \circ f_{ij}$ for all $i \leq j \leq k \in I$.

Note that if $i \leq j$, then in an inverse system the maps f_{ij} are defined from G_j to G_i and in a directed system the maps f_{ij} are defined from G_i to G_j.

Example 2.17. The family of additive groups $(\frac{1}{n}\mathbb{Z})/\mathbb{Z}$ with homomorphisms $f_{nm} : (\frac{1}{n}\mathbb{Z})/\mathbb{Z} \to (\frac{1}{m}\mathbb{Z})/\mathbb{Z}$ for all $n \mid m$ which sends $a + \mathbb{Z}$ to $\frac{a}{c} + \mathbb{Z}$, where $m = cn$. Hence, this family is a direct system.

Finally, we define the direct limit of a direct system of groups.

Definition 2.18. The direct limit of a directed system of groups $(G_i)_{i\in I}$ is the disjoint union of G_i's modulo an equivalence relation $\sim$, denoted

$$\varinjlim_i G_i = \left(\bigsqcup_i G_i \right) / \sim,$$

where $g_i \sim g_j$, for $g_i \in G_i$ and $g_j \in G_j$, if and only if there is $k \in I$ with $i, j \leq k$ such that $f_{ik}(g_i) = f_{jk}(g_j)$.

As an example, we have $\varinjlim(\frac{1}{n}\mathbb{Z}/\mathbb{Z}) \cong \mathbb{Q}/\mathbb{Z}$.

2.3 Characters

In this section, we introduce characters of a group G. Specifically, we consider the quadratic Dirichlet character associated to the Kronecker symbol χ_D, where D is a fundamental discriminant.

Definition 2.19. A *multiplicative character* on a group G is a group homomorphism

$$\chi : G \to \mathbb{C}^\times.$$

If the group G is a topological group, we shall require χ to be a continuous homomorphism. A character $\chi : G \to \mu_2$ is named *a quadratic character*, where μ_2 is the multiplicative group $\{\pm 1\}$.

Next, we introduce some basic facts about Dirichlet characters.

Definition 2.20. For $k \in \mathbb{Z}$, consider a multiplicative homomorphism

$$\chi : (\mathbb{Z}/k\mathbb{Z})^\times \to \mathbb{C}^\times.$$

We extend this map on $\mathbb{Z}$ by defining $\chi(n) = 0$, when $\gcd(k,n) \neq 1$. A *Dirichlet character* mod k is the extended homomorphism

$$\chi : \mathbb{Z} \to \mathbb{C}^\times.$$

The *conductor* of a Dirichlet character χ mod k is the smallest integer $f \mid k$, such that there is a Dirichlet character χ' mod f for which $\chi(n) = \chi'(n)$ for $(n,k) = 1$. We denote the conductor of χ by f_χ. A character is also named even if $\chi(-1) = 1$ and odd otherwise.

Example 2.21. Let χ be the character mod 8 such that $\chi(x) = 1$ for $x \in \{1,5\}$, and $\chi(x) = -1$ for $x \in \{3,7\}$. We have $\chi(x+4) = \chi(x)$. Since 4 is the smallest n such that χ can be

defined mod n then $f_\chi = 4$. Furthermore, since $\chi(-1) = -1$, the character χ is odd. Also χ is a quadratic character since it maps to $\mu_2 = \{\pm 1\}$.

Next, we introduce the Kronecker symbol which is an important example of a Dirichlet character. To define this character first we need to define the Legendre symbol.

Definition 2.22. The Legendre symbol $\left(\frac{a}{p}\right)$ for odd primes p is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a nonzero solution,} \\ -1 & \text{if } x^2 \equiv a \pmod{p} \text{ has no solutions.} \end{cases}$$

For odd primes p and q, we have the relation

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

known as *the law of quadratic reciprocity* (see [16, Thorem I.8.6]). Next, we extend the definition of the Legendre symbol.

Definition 2.23. Set $\left(\frac{a}{0}\right) = 0$, $\left(\frac{a}{1}\right) = 1$, $\left(\frac{a}{-1}\right) = \text{sign}(a)$, and

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } 2 \mid a, \\ 1 & \text{if } a \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } a \equiv \pm 3 \pmod{8}. \end{cases}$$

For integer $b = \text{sign}(b) p_1^{e_1} \dots p_k^{e_k}$, the *Kronecker symbol* $\left(\frac{a}{b}\right)$ is defined by

$$\left(\frac{a}{b}\right) = \left(\frac{a}{\text{sign}(b)}\right)\left(\frac{a}{p_1}\right)^{e_1} \dots \left(\frac{a}{p_k}\right)^{e_k}.$$

Let D be a fundamental discriminant. Then, it is known that the Kronecker symbol $\left(\frac{D}{\cdot}\right)$ is a Dirichlet character mod $|D|$ (see [7, Chapter 5]). We denote this Dirichlet character by

χ_D. By using the law of quadratic reciprocity, we can show that the Kronecker symbol corresponding to a fundamental discriminant D is the product of Legendre symbols of primes $p \mid D$ and a Dirichlet character mod 8.

Proposition 2.24. *Let D be a fundamental discriminant. If $D = \pm 2^{\ell} p_1 \dots p_k$ with $\ell \in \{0, 2, 3\}$, then, for any integer a, we have*

$$\chi_D(a) = \left(\frac{D}{a}\right) = \chi_{D,2}(a) \prod_{i=1}^{k} \left(\frac{a}{p_i}\right),$$

where $\left(\frac{a}{p_i}\right)$ is the Legendre symbol and $\chi_{D,2}$ is one of the four Dirichlet characters mod 8. More precisely, if D is odd, then $\chi_{D,2} = 1$, if $4 \parallel D$, then $\chi_{D,2} = \left(\frac{-4}{\cdot}\right)$ is the unique Dirichlet character mod 8 of conductor 4, and if $8 \parallel D$, then $\chi_{D,2} = \left(\frac{\pm 8}{\cdot}\right)$ is one of the two Dirichlet characters mod 8 of conductor 8. More precisely, for the case $8 \parallel D$, if $D > 0$ and the number of $1 \le i \le k$ with $p_i \equiv 3 \pmod 4$ is even, or $D < 0$ and the number of $1 \le i \le k$ with $p_i \equiv 3 \pmod 4$ is odd, then $\chi_{D,2} = \left(\frac{8}{\cdot}\right)$. Otherwise, we have $\chi_{D,2} = \left(\frac{-8}{\cdot}\right)$.

Proof. See [7, Chapter 5]. □

2.4 Artin Symbol

In this section, we define the Artin symbol associated to a prime ideal in a Galois extension of a number field. Then, we will see the relation between the Artin and Kronecker symbols which is one of the most important tools for us in Chapter 3.

We denote the ring of integers of a number field K (a finite extension of $\mathbb{Q}$) by O_K. Let L/K be an extension of number fields. Let $\mathfrak{p}$ be a prime ideal of O_K. Then, $\mathfrak{p}O_L$ (the ideal generated by $\mathfrak{p}$ in O_L) is an ideal of O_L. Since O_L is a Dedekind domain, $\mathfrak{p}O_L$ has a prime factorization

$$\mathfrak{p}O_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$$

in O_L, where $\mathfrak{P}_i$'s are the distinct primes of O_L containing $\mathfrak{p}$. We say $\mathfrak{p}$ is unramified in L if

$e_i = 1$ for $1 \leq i \leq g$. Otherwise, we say $\mathfrak{p}$ ramifies in L. If L/K is a Galois extensions, then the e_i's are all equal (see [12, Corollary I.7.2]) and we name $e_{L,\mathfrak{p}} = e_i$ (for $1 \leq i \leq g$) the *ramification index* of $\mathfrak{p}$. For a fixed prime $\mathfrak{P}$ of O_L lying over $\mathfrak{p}$, the subgroup

$$D_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K);\ \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

of $\mathrm{Gal}(L/K)$ is named the *decomposition group* of $\mathfrak{P}$. Let $\tilde{G}$ be the Galois group of the residue field extension $(O_L/\mathfrak{P})/(O_K/\mathfrak{p})$. We define the natural map $\sigma \mapsto \tilde{\sigma}$ from $D_{\mathfrak{P}}$ to $\tilde{G}$, where $\tilde{\sigma}(\alpha + \mathfrak{P}) = \sigma(\alpha) + \mathfrak{P}$ for $\alpha \in O_L$. It can be shown that this map is a surjective homomorphism. We denote the kernel of this homomorphism by

$$I_{\mathfrak{P}} = \{\sigma \in D_{\mathfrak{P}};\ \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P} \text{ for all } \alpha \in O_L\}$$

and we call it the *inertia group* of $\mathfrak{P}$. It is known that $|I_{\mathfrak{P}}| = e_{L,\mathfrak{p}}$ (see [6, Proposition 5.10]). Therefore, if $\mathfrak{p}$ is unramified in L, then we have $D_{\mathfrak{P}} \cong \tilde{G}$. On the other hand, since $\tilde{G}$ is the Galois group of an extension of finite fields, then $\tilde{G}$ is a cyclic group generated by the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{P}} : x \mapsto x^q$, where $q = |O_K/\mathfrak{p}|$.

Definition 2.25. Let $\mathfrak{p}$ be unramified in L. Let $\sigma \in D_{\mathfrak{P}}$ be the unique element that maps to the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{P}}$ through the isomorphism $D_{\mathfrak{P}} \xrightarrow{\sim} \tilde{G}$. The element σ is named *Artin symbol* of $\mathfrak{P}$ in the extension L/K, and is denoted by $\left(\frac{L/K}{\mathfrak{P}}\right)$.

If L/K is an abelian extension, then the Artin symbol of $\mathfrak{P}'s$ are the same for all prime $\mathfrak{P}'s$ above $\mathfrak{p}$, i.e., all primes $\mathfrak{P}$ in factorization of $\mathfrak{p}$ into prime ideals in O_L (see [6, Corollary 5.21]). In this case, we denote the Artin symbol of any $\mathfrak{P}$ above $\mathfrak{p}$ by $\left(\frac{L/K}{\mathfrak{p}}\right)$.

Let L/K be an abelian extension of number fields. We generalize the Artin symbol to any fractional ideal $\mathfrak{a} = \prod_i \mathfrak{p}_i^{r_i} \subset O_K$, coprime to ramified primes of L/K, multiplicatively by

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_i \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}.$$

Example 2.26 (Cyclotomic extensions)**.** Let $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ be the cyclotomic extension obtained by adjoining a primitive n-th root of unity ζ_n to $\mathbb{Q}$. Then, an element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is correspond to the Artin symbol $\left(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{a}\right)$, where $\sigma(\zeta_n) = \zeta_n^a$ with $\gcd(a,n) = 1$ (see [12, Example, Page 199])

Next, we observe that the Artin symbol of a quadratic extension $K/\mathbb{Q}$ coincides with the Kronecker symbol of the discriminant of $K/\mathbb{Q}$.

Proposition 2.27. *Let $\mathbb{Q}(\sqrt{a})$ be a quadratic field of discriminant $D_{\mathbb{Q}(\sqrt{a})}$. The prime p in $\mathbb{Z}$ ramifies in $\mathbb{Q}(\sqrt{a})$ if and only if $p \mid D_{\mathbb{Q}(\sqrt{a})}$. For primes p that are unramified in $\mathbb{Q}(\sqrt{a})$, we have*

$$\left(\frac{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}{p}\right)(\sqrt{a}) = \left(\frac{D_{\mathbb{Q}(\sqrt{a})}}{p}\right)\sqrt{a}.$$

Proof. For a proof see [6, Proposition 5.16 and Corollary 5.17]. □

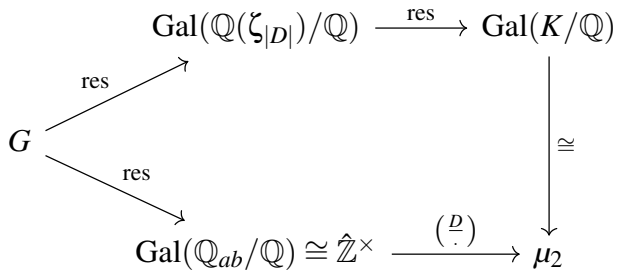
We next describe an application of Proposition 2.27 which will be used in Chapter 3.

Let $\{K_n : n \geq 1\}$ be a family of finite Galois extensions of $\mathbb{Q}$ with the property that $\zeta_n \in K_n$, where ζ_n is a primitive n-th root of unity. Let $K_n \subset K_m$ if $n \mid m$. Hence, we have restriction maps $\mathrm{res}_{nm} : G(m) \to G(n)$ for all $n \mid m$. Thus, the family $(G(n) = \mathrm{Gal}(K_n/\mathbb{Q}), \mathrm{res}_{nm})$ is an inverse system of finite groups with respect to division order, i.e., $n \leq m$ if and only if $n \mid m$. Assume that K_2 contains a quadratic field K of discriminant D. There are restriction homomorphisms

$$G \xrightarrow{\text{res}} \mathrm{Gal}(\mathbb{Q}_{ab}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^\times \qquad \text{and} \qquad G \xrightarrow{\text{res}} \mathrm{Gal}(\mathbb{Q}(\zeta_{|D|})/\mathbb{Q}),$$

where $\mathbb{Q}_{ab} = \bigcup_{n>2} \mathbb{Q}(\zeta_n)$ is the maximal abelian extension of $\mathbb{Q}$. Considering Example 2.26, we have the following proposition which plays a crucial rule in Theorem 3.5 in the next chapter.

Proposition 2.28. *With the notations described above, the diagram*



is a commutative diagram, where $\left(\frac{D}{\cdot}\right)$ *is the Kronecker symbol mod D.*

Proof. The diagram is commutative because of Proposition 2.27 and the fact that the restriction map $\mathrm{Gal}(\mathbb{Q}(\zeta_{|D|})/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$ sends $\left(\frac{\mathbb{Q}(\zeta_{|D|})/\mathbb{Q}}{a}\right)$ to $\left(\frac{K/\mathbb{Q}}{a}\right)$ (see [13, Property A2, Page 198]). □

2.5 Elliptic Curves

In this section, we will introduce division fields associated to an elliptic curve. The Galois group attached to the family of division fields of an elliptic curve forms a profinite group. We will describe the representation of this profinite group on the p-torsion points of the elliptic curve. At the end, we introduce the family of Serre curves. We begin with the definition of an elliptic curve.

Definition 2.29. An *elliptic curve E* defined over $\mathbb{Q}$ is a non-singular curve which is defined by an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1,\ a_2,\ a_3,\ a_4,\ a_6 \in \mathbb{Q}$ with a point O at infinity.

Let E be an elliptic curve defined over $\mathbb{Q}$. The *discriminant* of E is a polynomial in the a_i which is non-zero if and only if E is non-singular. The set of points of the elliptic curve E with rational coordinates forms an abelian group, in which $O = (0,1,0)$ (in projective coordinates) is the identity element. We denote the subgroup of all n-torsion points of E

with coordinates in $\overline{\mathbb{Q}}$ by $E[n]$. We assume that E is given by a global minimal Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, where $a_i \in \mathbb{Z}$ (see [24, Section VIII.8]). For a prime $p \nmid \Delta$, the *reduction modulo p* of the elliptic curve E is the elliptic curve E_p given by

$$E_p : y^2 + \overline{a}_1xy + \overline{a}_3y = x^3 + \overline{a}_2x^2 + \overline{a}_4x + \overline{a}_6,$$

where $\overline{a}_i$ denotes a_i modulo p. We say E is *cyclic* modulo p if the group of points of E_p with coordinates in $\mathbb{F}_p$ (the finite field of p elements) is cyclic.

Definition 2.30. The extension field $\mathbb{Q}(E[n])$ over $\mathbb{Q}$ which is generated by the x and y-coordinates of all points in $E[n]$ is named the *n-division field* of E.

Recall that the set of n-torsion points $E[n]$ forms a subgroup of the group of points of E. The following assertion describes the structure of this subgroup.

Lemma 2.31. *If E is an elliptic curve over $\mathbb{Q}$, for any integer $n \geq 2$, we have*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Proof. See [24, Corollary III.6.4b]. □

We can show that the n-division fields of E over $\mathbb{Q}$ are Galois extensions (see [25, Proposition 6.5]). We introduce representations for the Galois groups attached to such extensions. Each $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ acts on $E[n]$ and thus yields an automorphism on $E[n]$. By fixing two generators of $E[n]$, we can correspond a matrix in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ for each σ. This yields a representation of $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ to $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Note that for $n = \prod_{p^e \| n} p^e$, we have

$$|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})| = \prod_{p^e \| n} p^{4e-3}(p^2-1)(p-1). \tag{2.1}$$

Theorem 2.32. *Let E be an elliptic curve over $\mathbb{Q}$ and let $n \geq 2$. Then the map*

$$r_n : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

described above is an injective homomorphism.

Proof. See [25, Theorem 6.7] for a proof. □

By taking the inverse limit on r_n in Theorem 2.32 over all positive integer n, we have the injective homomorphism

$$r\colon\ \mathrm{Gal}(\mathbb{Q}^{\mathrm{tor}}/\mathbb{Q}) \to \mathrm{GL}_2(\hat{\mathbb{Z}}) = \varprojlim \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}), \tag{2.2}$$

where $\mathbb{Q}^{\mathrm{tor}} = \cup_{n=1}^{\infty} \mathbb{Q}(E[n])$. It can be shown that this representation is never surjective. An elliptic curve is called *non-CM* if its ring of endomorphisms is isomorphic to integers $\mathbb{Z}$. In [23], Serre shows that for a non-CM elliptic curve E, the image of r has finite index in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

Definition 2.33. An elliptic curve E defined over $\mathbb{Q}$ is called a *Serre curve* if $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : r(\mathrm{Gal}(\mathbb{Q}^{\mathrm{tor}}/\mathbb{Q}))] = 2$.

It is proved in [11] that almost all elliptic curves over $\mathbb{Q}$ are Serre curves.

Chapter 3

The Main Theorems

Throughout this section, let $(G(n))_{n\in\mathbb{N}}$ and $(A(n))_{n\in\mathbb{N}}$ be inverse systems of finite groups. Moreover, assume that there is an injective map $r_n : G(n) \to A(n)$ for all $n \geq 1$. This yields an injective map $r : G \to A$ by taking inverse limit over n. Further, suppose $A \cong \prod_p A_p$, where $A_p = \varprojlim A(p^i)$.

3.1 The First Main Theorem

In the following, we introduce the expected value of a measurable function.

Definition 3.1. Let $\mathcal{M}$ be a σ-algebra on a set M and let ν be a measure on $(M, \mathcal{M})$. Let $f : M \to \overline{\mathbb{R}}$ be any ν-measurable function where $\overline{\mathbb{R}} = [-\infty, +\infty]$ is the extended real line. For $N \in \mathcal{M}$, we define the expected value of f over N by

$$E_N(f) = \frac{\int_M f \cdot 1_N d\nu}{\int_M 1_N d\nu},$$

where

$$1_N(\alpha) = \begin{cases} 1 & \text{if } \alpha \in N, \\ 0 & \text{otherwise,} \end{cases}$$

is the characteristic function of N.

Let A be the profinite group defined in the beginning of this chapter. Note that since A is a profinite group, it is equipped by a probability measure ν_A, which is introduced at the end of Section 2.2. Let χ be a character of A. Considering a measurable function $f : A \to \overline{\mathbb{R}}$, we

denote the expected value of f over $\ker\chi$ by $E_\chi(f)$, i.e.,

$$E_\chi(f) = \frac{\int_A f.1_{\ker\chi} d\nu_A}{\int_A 1_{\ker\chi} d\nu_A}.$$

Let μ_m be the multiplicative group of the complex m-th roots of unity equipped with the discrete topology.

The following theorem is the first main theorem of this thesis.

Theorem 3.2. *Let $(G(n))_{n\in\mathbb{N}}$, $(A(n))_{n\in\mathbb{N}}$, $(r_n)_{n\in\mathbb{N}}$, G, A, and r be as the beginning of this chapter. Suppose there exists an exact sequence*

$$1 \to G \xrightarrow{r} A \xrightarrow{\chi} \mu_m \to 1 \tag{3.1}$$

of continuous homomorphisms. Let g be a real arithmetic function such that

$$\sum_{n\geq 1} \frac{|g(n)|}{\#G(n)} < \infty.$$

Consider the natural projections $\varphi_{A,n} : A \to A(n)$ and assume that

$$\tilde{g} = \sum_{n\geq 1} g(n) 1_{\ker\varphi_{A,n}} \tag{3.2}$$

defines a function from A to $\overline{\mathbb{R}}$. Then,

$$\sum_{n\geq 1} \frac{g(n)}{\#G(n)} = E_\chi(\tilde{g}) = \sum_{i=0}^{m-1} \int_A \tilde{g}\chi^i d\nu_A.$$

Moreover, if $\int_A \tilde{g} d\nu_A \neq 0$, then

$$\sum_{n\geq 1} \frac{g(n)}{\#G(n)} = \left(1 + \frac{\sum_{i=1}^{m-1} \int_A \tilde{g}\chi^i d\nu_A}{\int_A \tilde{g} d\nu_A}\right) \int_A \tilde{g} d\nu_A.$$

Proof. We start by writing the summation

$$\sum_{n\geq 1}\frac{g(n)}{\#G(n)}$$

in terms of measures of certain measurable subgroups of G. For this purpose, let $\Phi_n : G \to G(n)$ be the projection map for each $n \geq 1$. Then, $G/\ker\Phi_n \cong G(n)$ and $[G : \ker\Phi_n] = \#G(n)$. Hence, by Lemma 2.14, $\nu_G(\ker\Phi_n) = 1/\#G(n)$, where ν_G is the normalized Haar measure on G. Thus,

$$\sum_{n\geq 1}\frac{g(n)}{\#G_n} = \sum_{n\geq 1} g(n)\nu_G(\ker\Phi_n). \tag{3.3}$$

Observe that the number of cosets of the set $A/r(\ker\Phi_n)$ divided by the number of cosets of the group $G/\ker\Phi_n \cong r(G)/r(\ker\Phi_n)$ is equal to $|A/r(G)|$. Hence, by Lemma 2.14, we have

$$\nu_G(\ker\Phi_n) = \frac{\nu_A(r(\ker\Phi_n))}{\nu_A(r(G))}, \tag{3.4}$$

where ν_A is the normalized Haar measure on A (note that $r(G)$ is closed in A and $r(\ker\Phi_n)$ is closed in $r(G)$ and thus it is closed subgroup of A). Hence, by (3.4), we have

$$\begin{aligned}\sum_{n\geq 1} g(n)\nu_G(\ker\Phi_n) &= \sum_{n\geq 1} g(n)\frac{\nu_A(r(\ker\Phi_n))}{\nu_A(\ker\chi)}\\ &= \frac{1}{\nu_A(\ker\chi)}\sum_{n\geq 1} g(n)\nu_A(r(\ker\Phi_n)).\end{aligned} \tag{3.5}$$

Next, we show that $r(\ker\Phi_n) = \ker(\varphi_{A,n})\cap\ker\chi$, where $\varphi_{A,n} : A \to A(n)$ is the projection map for $n \geq 1$. We denote the identity of a group H by e_H. To prove this claim, we note that the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{\Phi_n} & G(n) \\ \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle r_n} \\ A & \xrightarrow{\varphi_{A,n}} & A(n) \end{array} \tag{3.6}$$

If $\sigma \in \ker\Phi_n$, then $r_n(\Phi_n(\sigma)) = r_n(e_{G(n)}) = e_{A(n)}$. Hence, by commutative diagram (3.6),

we have $r(\sigma) \in \ker(\varphi_{A,n})$. Moreover, by the exact sequence (3.1), we have $r(\sigma) \in r(G) = \ker\chi$. Therefore, $r(\ker\Phi_n) \subset \ker(\varphi_{A,n}) \cap \ker\chi$. On the other hand, if $\alpha \in \ker(\varphi_{A,n}) \cap \ker\chi \subset \ker\chi = r(G)$, then there exists a $\sigma \in G$ such that $r(\sigma) = \alpha$. Moreover, $r(\sigma) \in \ker(\varphi_{A,n})$ means $\varphi_{A,n}(r(\sigma)) = e_{A(n)}$. Hence, $r_n(\Phi_n(\sigma)) = e_{A(n)}$ since (3.6) is commutative. Thus, $\sigma \in \ker\Phi_n$ since r_n is injective. This shows that $\ker(\varphi_{A,n}) \cap \ker\chi \subset r(\ker\Phi_n)$. Therefore,

$$r(\ker\Phi_n) = \ker(\varphi_{A,n}) \cap \ker\chi. \tag{3.7}$$

By (3.7), we have

$$\begin{aligned}
\sum_{n\geq 1} g(n)\nu_A(r(\ker\Phi_n)) &= \sum_{n\geq 1} g(n)\nu_A(\ker\varphi_{A,n} \cap \ker\chi) \\
&= \sum_{n\geq 1} g(n) \int_A 1_{\ker\varphi_{A,n}\cap\ker\chi} d\nu_A \\
&= \sum_{n\geq 1} g(n) \int_A 1_{\ker\varphi_{A,n}} 1_{\ker\chi} d\nu_A \\
&= \int_A \left(\sum_{n\geq 1} g(n) 1_{\ker\varphi_{A,n}} \right) 1_{\ker\chi} d\nu_A.
\end{aligned} \tag{3.8}$$

We note that the last equality holds because of the following fact. Observe that

$$\left| \sum_{n=1}^{m} g(n) 1_{\ker\varphi_{A,n}\cap\ker\chi} \right| \leq \sum_{n\geq 1} |g(n)| 1_{\ker\varphi_{A,n}\cap\ker\chi}.$$

By the assumption $\sum_{n\geq 1} |g(n)|/\#G(n)$ converges. Hence, $\sum_{k\geq 1} |g(n)| 1_{\ker\varphi_{A,n}\cap\ker\chi}$ is integrable. Thus, by the Lebesgue's dominated convergence theorem (see [19, Chapter 11, 16]), we can interchange the sum and the integrals to get

$$\sum_{n\geq 1} g(n) \int_A 1_{\ker\varphi_n\cap\ker\chi} d\nu_A = \int_A \sum_{n\geq 1} g(n) 1_{\ker\varphi_{A,n}\cap\ker\chi} d\nu_A.$$

Now from (3.3), (3.5), and (3.8), we have

$$\begin{aligned}\sum_{n\geq 1}\frac{g(n)}{\#G(n)} &= \frac{\int_A \tilde{g}\,1_{\ker\chi}d\nu_A}{\int_A 1_{\ker\chi}d\nu_A}\\ &= E_\chi(\tilde{g}).\end{aligned} \tag{3.9}$$

Note that the character χ in (3.1) induces the character $\chi' : A/r(G) \xrightarrow{\sim} \mu_m$ by $\chi'(\overline{\alpha}) = \chi(\alpha)$. More precisely χ is the lift of χ' to A. Thus, χ' sends a generator of $A/r(G)$ to a generator of μ_m. Hence, χ' is a generator of the group of characters of $A/r(G)$ denoted by $\widehat{A/r(G)}$.

For $\overline{\alpha} \in A/r(G)$, by [21, Chapter VI, Proposition 4], we have

$$\sum_{\varepsilon\in\widehat{A/G}} \varepsilon(\overline{\alpha}) = \sum_{i=0}^{m-1}(\chi')^i(\overline{\alpha}) = \begin{cases} m & \text{if } \overline{\alpha}=1,\\ 0 & \text{if } \overline{\alpha}\neq 1.\end{cases}$$

Therefore, since $\overline{\alpha}=1$ means $\alpha\in\ker\chi$, we have

$$\sum_{i=0}^{m-1}\chi^i(\alpha) = \begin{cases} m & \text{if } \alpha\in\ker\chi,\\ 0 & \text{if } \alpha\notin\ker\chi.\end{cases}$$

This implies $\sum_{i=0}^{m-1}\chi^i(\alpha) = m\cdot 1_{\ker\chi}(\alpha)$. Thus,

$$E_\chi(\tilde{g}) = \frac{\int_A \tilde{g}\,1_{\ker\chi}\,d\nu_A}{\int_A 1_{\ker\chi}\,d\nu_A} = \frac{\int_A \tilde{g}\sum_1^m\chi^i d\nu_A}{n\int_A 1_{\ker\chi}d\nu_A}. \tag{3.10}$$

Furthermore, by (3.1), we have $[A:\ker\chi] = [A:r(G)] = m$. Hence, $\nu_A(\ker\chi) = 1/m$. Thus, by (3.10),

$$E_\chi(\tilde{g}) = \int_A \tilde{g}\sum_{i=0}^{m-1}\chi^i d\nu_A. \tag{3.11}$$

The desired result holds by considering (3.9) and (3.11). □

Next we consider the special case that $A\cong\prod_p A_p$ and $\chi=\prod_p\chi_p$, where $A_p = \varprojlim A(p^i)$

and χ_p's ($\chi_p : A_p \to \mu_m$) are characters of A_p's. Then, by Lemma 2.15, we have $\nu_A = \prod_p \nu_{A_p}$, since ν_{A_p}'s are probability measures. The following corollary considers this special case of Theorem 3.2.

Corollary 3.3. *In Theorem 3.2, suppose that g is a real multiplicative arithmetic function. In addition, assume that $A \cong \prod_p A_p$, where $A_p = \varprojlim A(p^i)$, and $\chi = \prod_p \chi_p$, where $\chi_p : A_p \to \mu_m$ is a character of A_p. Let*

$$\tilde{g}_p = \sum_{k \geq 0} g(p^k) 1_{\ker \varphi_{p^k}} \tag{3.12}$$

be a function from A_p to $\overline{\mathbb{R}}$, where $\varphi_{p^k} : A_p \to A(p^k)$ is the projection map, such that $\tilde{g} = \prod_p \tilde{g}_p$. If $\int_A \tilde{g} d\nu_A \neq 0$, then

$$\sum_{n=1}^{\infty} \frac{g(n)}{\#G_n} = \left(1 + \sum_{i=1}^{m-1} \prod_p \frac{\int_{A_p} \tilde{g}_p \chi_p^i d\nu_{A_p}}{\int_{A_p} \tilde{g}_p d\nu_{A_p}}\right) \prod_p \int_{A_p} \tilde{g}_p d\nu_{A_p}.$$

Proof. By Theorem 3.2, we have

$$\sum_{n \geq 1} \frac{g(n)}{\#G(n)} = \sum_{i=0}^{m-1} \int_A \tilde{g} \chi^i d\nu_A. \tag{3.13}$$

Since $g(n)$ is multiplicative, $A \cong \prod_p A_p$, $\nu_A = \prod_p \nu_{A_p}$, $\chi = \prod_p \chi_p$, and $\tilde{g} = \prod_p \tilde{g}_p$, then, from (3.13), we have

$$\sum_{n \geq 1} \frac{g(n)}{\#G(n)} = \sum_{i=0}^{m-1} \prod_p \int_{A_p} \tilde{g}_p \chi_p^i d\nu_{A_p}.$$

Thus, the desired result holds since $\int_A \tilde{g} d\nu_A = \prod_p \int_{A_p} \tilde{g}_p d\nu_{A_p} \neq 0$. □

Next, we consider the case that $[A : r(G)] = 2$ which plays a crucial role in the Artin type problems we consider in this thesis.

Corollary 3.4. *In Corollary 3.3, if $[A : r(G)] = 2$, then*

$$\sum_{n=1}^{\infty} \frac{g(n)}{\#G_n} = \left(1 + \prod_p \frac{\int_{A_p} \tilde{g}_p \chi_p d\nu_{A_p}}{\int_{A_p} \tilde{g}_p d\nu_{A_p}}\right) \prod_p \int_{A_p} \tilde{g}_p d\nu_{A_p}.$$

3.2 The Second Main Theorem

In this section, we introduce a family of Galois groups for which we apply the results of Section 3.1. We fix the following notations and conditions throughout this section.

Let $\{K_n : n \geq 1\}$ be a family of finite Galois extensions of $\mathbb{Q}$ with the property that $\zeta_n \in K_n$, where ζ_n is a primitive n-th root of unity. Suppose that $K_n \subset K_m$ if $n \mid m$. Let $\mathrm{res}_{nm} : G(m) \to G(n)$ be restriction maps for $n \mid m$. Thus, the family $(G(n) = \mathrm{Gal}(K_n/\mathbb{Q}), \mathrm{res}_{nm})$ is an inverse system of finite groups with respect to division order, i.e., $n \leq m$ if and only if $n \mid m$. Assume that K_2 contains a quadratic field K. Let $(A(n), f_{nm})$ be an inverse system of finite groups with respect to division order. Assume that for any $n \geq 1$, there exists an injective homomorphism

$$r_n : \mathrm{Gal}(K_n/\mathbb{Q}) \to A(n)$$

such that the diagram

$$\begin{array}{ccc} G(m) & \xrightarrow{\mathrm{res}_{nm}} & G(n) \\ \downarrow{\scriptstyle r_m} & & \downarrow{\scriptstyle r_n} \\ A(m) & \xrightarrow{f_{nm}} & A(n) \end{array}$$

commutes. Hence, we have an injective homomorphism of profinite groups

$$r : G = \varprojlim \mathrm{Gal}(K_n/\mathbb{Q}) \to A = \varprojlim A(n).$$

Note that since $\mathbb{Q}(\zeta_n) \subset K_n$ (for all $n \geq 1$) and $K \subset K_2$, then the restriction maps $G \to \mathrm{Gal}(\mathbb{Q}_{ab}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^\times$ and $G \to \mathrm{Gal}(K/\mathbb{Q})$ are well-defined (Recall that $\mathbb{Q}_{ab}$ is the maximal abelian extension of $\mathbb{Q}$). In addition, assume that there are profinite homomorphisms

$$A \xrightarrow{\gamma} \hat{\mathbb{Z}}^\times \qquad \text{and} \qquad A \xrightarrow{\psi} \mu_2 \tag{3.14}$$

such that γ is induced by taking the inverse limit of maps $\gamma_n : A(n) \to (\mathbb{Z}/n\mathbb{Z})^\times$ and the

diagrams

$$\begin{array}{ccc} G & \longrightarrow & \mathrm{Gal}(\mathbb{Q}_{ab}/\mathbb{Q}) \\ {\scriptstyle r}\downarrow & & \downarrow{\scriptstyle \cong} \\ A & \xrightarrow{\gamma} & \hat{\mathbb{Z}}^{\times} \end{array} \qquad \text{and} \qquad \begin{array}{ccc} G & \longrightarrow & \mathrm{Gal}(K/\mathbb{Q}) \\ {\scriptstyle r}\downarrow & & \downarrow{\scriptstyle \simeq} \\ A & \xrightarrow{\psi} & \mu_2 \\ & \searrow \quad \nearrow & \\ & A(2) & \end{array} \tag{3.15}$$

commute, where $A \to A(2)$ is the projection map. Note that γ and ψ are surjective since the restriction maps $G \to \mathrm{Gal}(\mathbb{Q}_{ab}/\mathbb{Q})$ and $G \to \mathrm{Gal}(K/\mathbb{Q})$ are surjective. Moreover, let $A = \prod_p A_p$, where $A_p = \varprojlim A(p^n)$.

In the next theorem, we construct a quadratic character on A and we show how this character helps us to study the index $[A : r(G)]$.

Theorem 3.5. *With the above notations and assumptions, there exists a non-trivial quadratic character $\chi : A \to \mu_2$ for which the following statements hold:*

(i) $r(G) \subset \ker\chi$.

(ii) The character $\chi = \prod_p \chi_p$, where each χ_p is a certain quadratic character of A_p described in the proof.

In addition, let $\varphi_{p^k} : A_p \to A(p^k)$ be the projection map, and D be the discriminant of the quadratic field K. Then, the following assertions are true:

(iii) For odd primes $p \nmid D$, $\chi_p = 1_{A_p}$.

(iv) If $p \mid D$ and p is odd, then $\chi_p \neq 1_{A_p}$ and $\chi_p\big|_{\ker\varphi_{p^k}} = 1_{\ker\varphi_{p^k}}$ for all $k \geq 1$.

(v) If D is odd, then $\chi_2 \neq 1_{A_2}$ and $\chi_2|_{\ker\varphi_{2^k}} = 1_{\ker\varphi_{2^k}}$ for all $k \geq 1$.

(vi) If $4 \parallel D$ and $\zeta_4 = i \notin K_2$, then $\chi_2 \neq 1_{A_2}$, $\chi_2|_{\ker\varphi_2} \neq 1_{\ker\varphi_2}$, and $\chi_2|_{\ker\varphi_{2^k}} = 1_{\ker\varphi_{2^k}}$ for all $k \geq 2$.

(vii) If $8 \parallel D$ and $\zeta_8 \notin K_4$, then $\chi_2 \neq 1_{A_2}$, $\chi_2|_{\ker\varphi_{2^k}} \neq 1_{\ker\varphi_{2^k}}$ for $k = 1, 2$, and $\chi_2|_{\ker\varphi_{2^k}} = 1_{\ker\varphi_{2^k}}$ for all $k \geq 3$.

Proof. We start by describing the construction of the quadratic character χ. Let γ be as defined in (3.14). Consider the sequence of continuous homomorphisms

$$A \xrightarrow{\gamma} \hat{\mathbb{Z}}^\times \xrightarrow{\text{proj}} (\mathbb{Z}/D\mathbb{Z})^\times \xrightarrow{\left(\frac{D}{\cdot}\right)} \mu_2,$$

where the second map is projection and the last map is the Kronecker symbol mod $D(=\text{disc}_{\mathbb{Q}}(K))$. Hence, the composition of the lift of the Kronecker symbol mod D to $\hat{\mathbb{Z}}^\times$ with γ gives the quadratic character

$$\chi_D : A \to \mu_2.$$

On the other hand, let

$$\psi : A \to A(2) \to \mu_2$$

be the character on A defined in (3.14).

Define the character $\chi = \chi_D \cdot \psi$. We claim that the character χ is non-trivial. If $\chi_D = \psi$ on A, then χ_D splits via $A(2)$ as ψ does. Moreover, since χ_D factors via $\hat{\mathbb{Z}}^\times$ then each component $A(n)$ factors via $(\mathbb{Z}/n\mathbb{Z})^\times$. Thus, we have the commutative diagram:

$$\begin{array}{ccc} A & \xrightarrow{\chi_D} & \mu_2 \\ & \searrow \quad \nearrow & \uparrow \\ & A(2) \xrightarrow{\gamma_2} (\mathbb{Z}/2\mathbb{Z})^\times \cong \{1\} & \end{array} \tag{3.16}$$

Therefore, since the above diagram is commutative, χ_D is the trivial character on A. On the other hand, χ_D is the composition of the lift of the Kronecker symbol and γ. Since γ is surjective (see the left diagram in (3.15)), then χ_D is surjective. This is a contradiction with the claim $\chi_D = \psi$. Therefore, the characters χ_D and ψ are not the same on A. Thus, $\chi = \chi_D \cdot \psi$ is non-trivial on A.

We now prove the other assertions.

(i) By Proposition 2.28, we know that the characters χ_D and ψ are the same on $r(G)$. Thus, $\chi = \chi_D \cdot \psi$ is trivial on $r(G)$, i.e., $r(G) \subset \ker\chi$.

(ii) Next we show that $\chi = \prod_p \chi_p$ for certain quadratic characters χ_p of A_p. The character χ_D is the lift of the Kronecker symbol $\left(\frac{D}{\cdot}\right)$ to A via

$$A \xrightarrow{\gamma} \hat{\mathbb{Z}}^\times \xrightarrow{\text{proj}} (\mathbb{Z}/D\mathbb{Z})^\times.$$

Note that D is a fundamental discriminant. Thus, $D = \pm 2^\ell p_1 \dots p_k$, where p_i's are odd primes and $\ell \in \{0, 2, 3\}$. Hence, $\chi_D = \prod_{p|D} \chi_{D,p}$, where $\chi_{D,p}$ is the Legendre symbol modulo p for odd p, and for D even, $\chi_{D,2}$ is one of the non-trivial Dirichlet characters mod 8 (see Proposition 2.24). On the other hand, since ψ factors via $A(2)$, then it factors via A_2. Let $\psi_2 : A_2 \to \mu_2$ be the corresponding homomorphism obtained from factorization of ψ via A_2. Let $\chi_p = \chi_{D,p}$ for odd primes $p \mid D$ and for prime 2 let $\chi_2 = \chi_{D,2} \cdot \psi_2$ if $2 \mid D$ and $\chi_2 = \psi_2$ if $2 \nmid D$. For odd primes $p \nmid D$, let $\chi_p = 1$. Therefore, we have the decomposition $\chi = \prod_p \chi_p$. This complete the proof of (ii).

Next we describe the action of χ_p on A_p for all p. First of all note that $\ker \varphi_{p^k} \subset \ker \varphi_{p^t}$ for all primes p and for any $k \geq t$. Thus, if a character is trivial on $\ker \varphi_{p^t}$, then it is trivial on $\ker \varphi_{p^k}$ for any $k \geq t$. We now consider assertions (iii)-(vii).

(iii) If p is odd and $p \nmid D$, then χ_p is trivial. Thus, the desired result holds.

(iv) For odd primes $p \mid D$, the character χ_p is the Legendre symbol mod p. Since the map $\gamma_p : A_p \to \mathbb{Z}_p^\times$ is surjective as $\gamma : \prod_p A_p \cong A \to \hat{\mathbb{Z}}^\times \cong \prod_p \mathbb{Z}_p^\times$ is surjective, then χ_p is non-trivial on A_p. Moreover, χ_p is trivial on $\ker \varphi_p$, since we can factor $A_p \to (\mathbb{Z}/p\mathbb{Z})^\times$ via $A(p)$, i.e., the diagram

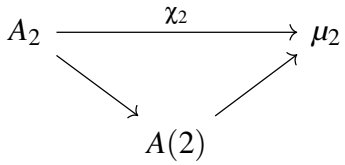
$$\begin{array}{ccc} A_p & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ & {\scriptstyle \varphi_p} \searrow \quad \nearrow & \\ & A(p) & \end{array}$$

commutes, where $A_p \to (\mathbb{Z}/p\mathbb{Z})^\times$ is the composition of γ_p with the projective map $\mathbb{Z}_p^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$. Hence, elements of $\ker \varphi_p$ maps to $1 \bmod p$.

Next consider $p = 2$. Since $\chi_D \neq \psi$ on $A(2)$, then $\chi_2 = \chi_{D,2} \cdot \psi_2$ is not trivial on A_2. Moreover, since ψ_2 factors via $A(2)$, the character ψ_2 is trivial on $\ker \varphi_2$. Hence, the char-

acter χ_2 is the same as $\chi_{D,2}$ on $\ker\varphi_{2^k}$ for $k \geq 1$.

(v) If D is odd, then $\chi_2 = \psi_2$. Hence, the character χ_2 factors via $A(2)$, i.e.,



The factorization comes from commutative diagram 3.15 corresponding to ψ. Thus, it is non-trivial on A_2 and trivial on $\ker\varphi_2$.

(vi) If $4 \parallel D$, then $\chi_{D,2}$ is the lift of the unique non-trivial Dirichlet character mod 8 of conductor 4. In the following, we describe the action of this character on $\ker\varphi_{p^k}$. In this case, since the conductor of $\chi_{D,2}$ is 4, for $k > 1$, we have the following map

$$\chi_{D,2}\colon A_2 \xrightarrow{\varphi_{2^k}} A(2^k) \to (\mathbb{Z}/2^k\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times \xrightarrow{\left(\frac{-4}{\cdot}\right)} \mu_2,$$

where $A(2^k) \to (\mathbb{Z}/2^k\mathbb{Z})^\times$ is the map corresponding to component 2^k of $\gamma_2 : A_2 \to \mathbb{Z}_2^\times$, and $(\mathbb{Z}/2^k\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$ is the natural map coming from reducing to modulo 4. Hence, for $\alpha \in \ker\varphi_{2^k}$, we have $\varphi_{2^k}(\alpha) = 1$ if $k > 1$. Thus, χ_2 is trivial on $\ker\varphi_{2^k}$ for $k > 1$. For the case $k = 1$, let $(\beta_i)_i \in G$ be such that $\beta_4 : \zeta_4 \mapsto \zeta_4^3$. If $(\beta_i)_i$ maps to α via $G \to A \to A_2$, then $\chi_{D,2}(\alpha) = \left(\frac{-4}{3}\right) = -1$. On the other hand, since $\beta_4 : \zeta_4 \mapsto \zeta_4^3$ and $\zeta_4 \notin K_2$, we have $\beta_2 = \beta_4\big|_{K_2} = \mathrm{id}_{K_2}$. Hence, $r_2(\beta_2) = 1_{A(2)}$. Thus, $\alpha \in \ker\varphi_2$. Thus, $\chi_{D,2}$ is non-trivial on $\ker\varphi_2$. Therefore, if $4 \parallel D$, the character χ_2 is non-trivial on A_2 and $\ker\varphi_2$, and trivial on $\ker\varphi_{2^k}$ for $k > 1$.

(vii) If $8 \parallel D$, then $\chi_{D,2}$ is the lift of one of the two characters modulo 8 of conductor 8. Similar to part (vi), if $8 \parallel D$, we observe that $\chi_{D,2}$ is trivial on φ_{2^k} for $k > 2$ since $\chi_{D,2}$ factors via $(\mathbb{Z}/8\mathbb{Z})^\times$ and we have

$$\chi_{D,2}\colon A_2 \xrightarrow{\varphi_{2^k}} A(2^k) \to (\mathbb{Z}/2^k\mathbb{Z})^\times \to (\mathbb{Z}/8\mathbb{Z})^\times \xrightarrow{\left(\frac{\pm 8}{\cdot}\right)} \mu_2,$$

for $k > 2$, where $A(2^k) \to (\mathbb{Z}/2^k\mathbb{Z})^\times$ is the map corresponding to component 2^k of $\gamma_2 : A_2 \to \mathbb{Z}_2^\times$, and $(\mathbb{Z}/2^k\mathbb{Z})^\times \to (\mathbb{Z}/8\mathbb{Z})^\times$ is the natural map coming from reducing to modulo 8. For the case $k = 2$, an argument similar to the one given in the proof of (vi) works for element $(\beta_i)_i \in G$ such that $\beta_8 : \zeta_8 \mapsto \zeta_8^5$ in $G(8)$. Thus, if $(\beta_i)_i$ maps to α via $G \to A \to A_2$, then $\chi_{D,2}(\alpha) = \left(\frac{\pm 8}{5}\right) = -1$. On the other hand, since $\zeta_8 \notin K_4$, we have $\beta_4 = \mathrm{id}_{K_4}$ and hence $r_4(\beta_4) = 1_{A(4)}$. Thus, since $\alpha \in \ker\varphi_4$, we have $\chi_{D,2}$ is non-trivial on $\ker\varphi_4$. Since $\ker\chi_4 \subset \ker\chi_2$, we have $\chi_{D,2}$ is non-trivial on $\ker\varphi_2$. Therefore, if $8 \parallel D$, the character χ_2 is non-trivial on A_2, $\ker\varphi_2$ and $\ker\varphi_4$, and it is trivial on $\ker\varphi_{2^k}$ for $k > 2$. □

Next, we have the following corollary which unifies the product forms of several Artin type problems, such as Cyclicity problem and the Titchmarsh Divisor Problem.

Corollary 3.6. *Let A and G be as described in the beginning of this section. Assume that $[A : r(G)] = 2$. Let g be a real multiplicative arithmetic function such that*

$$\sum_{n\geq 1} \frac{|g(n)|}{\#G(n)} < \infty.$$

Assume that (3.2) *defines a function $\tilde{g}$ from A to $\overline{\mathbb{R}}$. Let $\tilde{g}_p$ defined in* (3.12) *be the function from A_p to $\overline{\mathbb{R}}$ such that $\tilde{g} = \prod_p \tilde{g}_p$. Then, if $\zeta_4 \notin K_2$, $\zeta_8 \notin K_4$, and $\int_A \tilde{g} d\nu_A \neq 0$, we have*

$$\sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)} = \left(1 + \prod_{p|2D} \frac{\sum_{k\geq \ell} g(p^k)/\#A(p^k)}{1 + \sum_{k\geq 1} g(p^k)/\#A(p^k)}\right) \prod_p \left(1 + \sum_{k\geq 1} \frac{g(p^k)}{\#A(p^k)}\right),$$

where in the product on primes dividing $2D$, we have $\ell = 1$ for odd primes and for prime 2 we have $\ell = 1$ if D is odd, $\ell = 2$ if $4 \parallel D$, and $\ell = 3$ if $8 \parallel D$.

Proof. By Theorem 3.5, there exists a non-trivial character $\chi : A \to \mu_2$, where $\chi = \prod_p \chi_p$, such that $r(G) \subset \ker\chi$. Hence, since $[A : r(G)] = [A : \ker\chi] = 2$, we have $r(G) = \ker\chi$. Thus, the sequence

$$1 \to G \xrightarrow{r} A \xrightarrow{\chi} \mu_2 \to 1 \tag{3.17}$$

is exact. Therefore, by Corollary 3.4,

$$\sum_{n=1}^{\infty}\frac{g(n)}{\#G_n}=\left(\prod_p\int_{A_p}\tilde{g}_p d\nu_{A_p}\right)\left(1+\prod_p\frac{\int_{A_p}\tilde{g}_p\chi_p d\nu_{A_p}}{\int_{A_p}\tilde{g}_p d\nu_{A_p}}\right). \tag{3.18}$$

Recall that by Lemma 2.14, we have $\nu_{A_p}(\ker\varphi_{p^k})=1/\#A(p^k)$. Observe that

$$\begin{aligned}\int_{A_p}\tilde{g}_p d\nu_{A_p}&=\int_{A_p}\left(1_{A_p}+\sum_{k\geq 1}g(p^k)1_{\ker\varphi_{p^k}}\right)d\nu_{A_p}\\&=\nu_{A_p}(A_p)+\sum_{k\geq 1}g(p^k)\nu_{A_p}(\ker\varphi_{p^k})\\&=1+\sum_{k\geq 1}\frac{g(p^k)}{\#A(p^k)}.\end{aligned} \tag{3.19}$$

Next, by part (iii) of Theorem 3.5, for $p\nmid 2D$, the character χ_p is trivial on A_p. Hence,

$$\prod_p\frac{\int_{A_p}\tilde{g}_p\chi_p d\nu_{A_p}}{\int_{A_p}\tilde{g}_p d\nu_{A_p}}=\prod_{p\mid 2D}\frac{\int_{A_p}\tilde{g}_p\chi_p d\nu_{A_p}}{\int_{A_p}\tilde{g}_p d\nu_{A_p}}. \tag{3.20}$$

In addition, by part (iv) of Theorem 3.5, for odd primes $p\mid D$,

$$\begin{aligned}\int_{A_p}\tilde{g}_p\chi_p d\nu_{A_p}&=\int_{A_p}\left(1_{A_p}\chi_p+g(p)1_{\ker\varphi_p}\chi_p+\cdots+g(p^k)1_{\ker\varphi_{p^k}}\chi_p+\ldots\right)d\nu_{A_p}\\&=0+\sum_{k\geq 1}g(p^k)\nu_{A_p}(\ker\varphi_{p^k})\\&=\sum_{k\geq 1}\frac{g(p^k)}{\#A(p^k)}.\end{aligned} \tag{3.21}$$

For prime 2, by parts (v), (vi), and (vii) of Theorem 3.5,

$$\begin{aligned}\int_{A_2}\tilde{g}_2\chi_2 d\nu_{A_2}&=\int_{A_2}\left(1_{A_2}\chi_p+g(2)1_{\ker\varphi_2}\chi_2+\cdots+g(2^k)1_{\ker\varphi_{2^k}}\chi_2+\ldots\right)d\nu_{A_2}\\&=0+\sum_{k\geq \ell}g(2^k)\nu_{A_2}(\ker\varphi_{2^k})\\&=\sum_{k\geq \ell}\frac{g(2^k)}{\#A(2^k)},\end{aligned} \tag{3.22}$$

where $\ell = 2$ if $4 \parallel D$, $\ell = 3$ if $8 \parallel D$, and $\ell = 1$ otherwise.

Therefore, (3.18), (3.19), (3.20), (3.21) and (3.22) imply

$$\sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)} = \left(1 + \prod_{p|2D} \frac{\sum_{k\geq \ell} g(p^k)/\#A(p^k)}{1+\sum_{k\geq 1} g(p^k)/\#A(p^k)}\right) \prod_{p} \left(1 + \sum_{k\geq 1} \frac{g(p^k)}{\#A(p^k)}\right),$$

where in the product on primes dividing $2D$, we have $\ell = 1$ for odd primes and for prime 2 we have $\ell = 1$ if D is odd, $\ell = 2$ if $4 \parallel D$, and $\ell = 3$ if $8 \parallel D$. □

Chapter 4

Examples and Results

4.1 Kummer Fields

In this section, for $n \geq 1$, the field K_n is the splitting field of $x^n - a$ over $\mathbb{Q}$, where $|a|$ is not a perfect power. We will show that the inverse limit of the Galois groups of $K_n/\mathbb{Q}$ is embedded in a profinite group A, where A satisfies the conditions described at the beginning of Section 3.2.

Let $G(n)$ be the Galois group of $K_n = \mathbb{Q}(\zeta_n, \sqrt[n]{a})$ over $\mathbb{Q}$. Let $a^{1/n}$ be a fixed root of $x^n - a = 0$. Then each $\sigma \in G(n)$ is determined uniquely by its action on $a^{1/n}$ and a primitive root of unity ζ_n. For such σ, we have $\sigma(a^{1/n}) = \zeta_n^b a^{1/n}$ and $\sigma(\zeta_n) = \zeta_n^d$, where $b \in \mathbb{Z}/n\mathbb{Z}$ and $d \in (\mathbb{Z}/n\mathbb{Z})^\times$. Therefore, each $\sigma \in G(n)$ is determined by a pair (b,d), with $b \in \mathbb{Z}/n\mathbb{Z}$ and $d \in (\mathbb{Z}/n\mathbb{Z})^\times$. Thus, there exists an injective homomorphism

$$r_n : G(n) \to A(n), \tag{4.1}$$

where $A(n)$ is the group of matrices of the form $\left(\begin{smallmatrix} 1 & 0 \\ b & d \end{smallmatrix}\right)$ with multiplication, where $b \in \mathbb{Z}/n\mathbb{Z}$ and $d \in (\mathbb{Z}/n\mathbb{Z})^\times$ (see [13, Chapter VI, Section 9, Example 2] for details). Taking the inverse limit on both sides of (4.1), we have an injective homomorphism of profinite groups

$$r : G \to A, \tag{4.2}$$

where

$$A = \left\{ \begin{pmatrix} 1 & 0 \\ b & d \end{pmatrix} ; \, b \in \hat{\mathbb{Z}} \text{ and } d \in \hat{\mathbb{Z}}^{\times} \right\}. \tag{4.3}$$

Note that $A \cong \prod_p A_p$. On the other hand, $G = \mathrm{Gal}(K_\infty/\mathbb{Q})$, where $K_\infty = \cup_{n\geq 1} K_n$. Let $\mu_m(L)$ be the group of all m-th roots of unity in L. Note that K_∞ contains the group $\mu_\infty = \cup_{n\geq 1}\mu_m(\overline{\mathbb{Q}})$ of all roots of unity in $\overline{\mathbb{Q}}$.

Therefore, A and G satisfy conditions of Theorem 3.5. Let the map γ, introduced in (3.14), be the determinant map $A \xrightarrow{\det} \hat{\mathbb{Z}}^{\times}$ and $\psi : A \to A(2) \cong \mu_2$ be the projection map. Consider the surjective map $\det : A \to \hat{\mathbb{Z}}^{\times}$. Let H be

$$H = \ker(\det) = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} ; \, b \in \hat{\mathbb{Z}} \right\}. \tag{4.4}$$

Thus, the sequence

$$1 \to H \xrightarrow{i} A \xrightarrow{\det} \hat{\mathbb{Z}}^{\times} \to 1 \tag{4.5}$$

is exact, where i is the inclusion map.

Next note that since $\mathbb{Q}_{ab}$ is the maximal abelian extension over $\mathbb{Q}$, the exact sequence

$$1 \to \mathrm{Gal}(K_\infty/\mathbb{Q}_{ab}) \to G \to \mathrm{Gal}(\mathbb{Q}_{ab}/\mathbb{Q}) \to 1$$

shows that $\mathrm{Gal}(K_\infty/\mathbb{Q}_{ab}) = G'$, where G' is the commutator of G. Note that $r(G') \subset A' \subset H$. Hence, r maps G' to H, i.e., we have the homomorphism $\eta = r\big|_{G'} : G' \to H$. Hence, the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G' & \xrightarrow{i_1} & G & \xrightarrow{\mathrm{res}} & \mathrm{Gal}(\mathbb{Q}_{ab}/\mathbb{Q}) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle \simeq} & & \\ 1 & \longrightarrow & H & \xrightarrow{i_2} & A & \xrightarrow{\det} & \hat{\mathbb{Z}}^{\times} & \longrightarrow & 1, \end{array} \tag{4.6}$$

commutes, where i_1 and i_2 are inclusions.

We claim that $[A : r(G)] = 2$. The next three lemmas summarize some facts used in [15]

that will help us in achieving this goal.

Lemma 4.1. *Consider the group* $\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Z}},\mu_\infty)$ *of all homomorphisms from* $a^{\mathbb{Q}}/a^{\mathbb{Z}}$ *to* μ_∞*, where groups* $a^{\mathbb{Q}}=\{a^q;q\in\mathbb{Q}\}$ *and* $a^{\mathbb{Z}}=\{a^z;z\in\mathbb{Z}\}$ *are considered with multiplication. Then* $\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Z}},\mu_\infty)\cong H$*, where* H *is defined in* (4.4)*.*

Proof. Let $\hat{\mu}=\varprojlim\mu_m$. Then, $H\cong\hat{\mu}$. The multiplicative group $a^{\mathbb{Q}}/a^{\mathbb{Z}}$ is isomorphic to the additive group $\mathbb{Q}/\mathbb{Z}$. Hence, $\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Z}},\ \mu_\infty)\cong\mathrm{Hom}(\mathbb{Q}/\mathbb{Z},\ \mu_\infty)$. Thus, since $\varinjlim_n(\frac{1}{n}\mathbb{Z}/\mathbb{Z})=\mathbb{Q}/\mathbb{Z}$, we have $\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Z}},\ \mu_\infty)\cong\mathrm{Hom}(\varinjlim_n(\frac{1}{n}\mathbb{Z}/\mathbb{Z}),\ \mu_\infty)$. On the other hand,

$$\mathrm{Hom}(\varinjlim_n(\tfrac{1}{n}\mathbb{Z}/\mathbb{Z}),\ \mu_\infty)=\varprojlim_n\mathrm{Hom}(\tfrac{1}{n}\mathbb{Z}/\mathbb{Z},\ \mu_\infty)\cong\hat{\mu}$$

(see [18, Proposition 5.26]). Therefore, $H\cong\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Z}},\ \mu_\infty)$. □

Next we consider the injective homomorphism

$$\begin{aligned}\delta : G'=\mathrm{Gal}(K_\infty/\mathbb{Q}_{ab})&\to\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Z}},\ \mu_\infty)\\ \sigma&\mapsto[a^x\mapsto\sigma(a^x)/a^x].\end{aligned}$$

Note that this map is injective since if σ maps to identity, then $\sigma(a^x)=a^x$ fo all $x\in\mathbb{Q}$. Hence, σ is the identity in $\mathrm{Gal}(K_\infty/\mathbb{Q}_{ab})$.

The next lemma provides a description of the image of this injective hopmomorphism.

Lemma 4.2. *The image of*

$$\delta : G'\to\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Z}},\ \mu_\infty)$$

is $\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Q}}\cap\mathbb{Q}_{ab}^{\times},\ \mu_\infty)$.

Proof. For the proof, see [15, Page 494]. □

Note that the composition of δ with the isomorphism $H\cong\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Z}},\ \mu_\infty)$ proved in Lemma 4.1 is the same as $\eta=r\big|_{G'}:G'\to H$.

To understand the intersection $a^{\mathbb{Q}} \cap \mathbb{Q}_{ab}^{\times}$ in Lemma 4.2, we need to know when the splitting field of $x^n - a$ is abelian over $\mathbb{Q}$. The next lemma gives us the answer.

Lemma 4.3 ([20], Theorem 2)**.** *Let $k \geq 1$ be not divisible by the characteristic of field L. The splitting field of $x^k - a$ over L is abelian if and only if $a^{\#\mu_k(L)}$ is a k-th power in L, where $\#\mu_k(L)$ is the number of k-th roots of unity contained in L.*

We are ready to prove our claim regarding $[A : r(G)]$.

Theorem 4.4. *With G and A as defined at the beginning of this section, we have*

$$[A : r(G)] = 2.$$

Proof. First, we show that $\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Q}} \cap \mathbb{Q}_{ab}^{\times}, \mu_\infty)$ has index 2 in $\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Z}}, \mu_\infty)$. To determine the intersection $a^{\mathbb{Q}} \cap \mathbb{Q}_{ab}^{\times}$, we show that $k = 2$ is the largest integer such that the splitting field of $x^k - a$ is abelian over $\mathbb{Q}$. By Lemma 4.3, such a splitting field is abelian over $\mathbb{Q}$ if and only if $a^{\#\mu_k(\mathbb{Q})}$ is a k-th power in $\mathbb{Q}$. This means $a^{\#\mu_k(\mathbb{Q})} = b^k$ for some $b \in \mathbb{Q}$. Since a is not a perfect power and $\#\mu_k(\mathbb{Q}) \leq k$, we conclude that $k = \#\mu_k(\mathbb{Q}) = 2$. Therefore, $a^{\mathbb{Q}} \cap \mathbb{Q}_{ab}^{\times} = a^{\frac{1}{2}\mathbb{Z}}$. Hence, $a^{\mathbb{Q}}/a^{\frac{1}{2}\mathbb{Z}} \cong (a^{\mathbb{Q}}/a^{\mathbb{Z}})/\langle a^{\frac{1}{2}} \bmod a^{\mathbb{Z}} \rangle$, where $\langle a^{\frac{1}{2}} \bmod a^{\mathbb{Z}} \rangle$ is the unique subgroup of order 2 of $a^{\mathbb{Q}}/a^{\mathbb{Z}}$. Thus, $\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Q}} \cap \mathbb{Q}_{ab}^{\times}, \mu_\infty)$ is of index 2 in $\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Z}}, \mu_\infty)$. Equivalently, by Lemma 4.2, the image of $\mathrm{Gal}(K_\infty/\mathbb{Q}_{ab})$ in $\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Z}}, \mu_\infty)$ has index 2 in $\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Z}}, \mu_\infty)$. Hence, the image of G' in $\mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Z}}, \mu_\infty)$ has index 2, then by Lemma 4.1, the image of G' under the map

$$G' \xrightarrow{\delta} \mathrm{Hom}(a^{\mathbb{Q}}/a^{\mathbb{Z}}, \mu_\infty) \xrightarrow{\cong} H$$

has index 2 in H. Note that this map is the same as η. Therefore, $[H : \eta(G')] = 2$. Thus, since the diagram (4.6) is commutative, we have $[A : r(G)] = 2$. □

Our next goal is to describe a quadratic character of A, which will play an essential role in computing the correction factors in Artin type problems for Kummer fields.

As described at the beginning of this section, let the map γ be the determinant map $A \xrightarrow{\det} \hat{\mathbb{Z}}^\times$ and $\psi : A \to A(2) \cong \mu_2$ be the projection map. Note that $A(2) \cong \mathrm{Gal}(K_2/\mathbb{Q})$. Corresponding to γ, consider the quadratic character χ_D described in the proof of Theorem 3.5 with $K = K_2$. Thus, $\chi_D : A \to \mu_2$ is the quadratic character which is the lift of the Kronecker symbol attached to $D = \mathrm{disc}_{\mathbb{Q}}(K_2)$. Hence, we have the exact sequence

$$1 \to G \xrightarrow{r} A \xrightarrow{\chi} \mu_2 \to 1, \tag{4.7}$$

where $\chi = \chi_D \cdot \psi$. This is true since, by Theorem 3.5(i), the character χ is non-trivial on A with $r(G) \subset \ker\chi$, and by Theorem 4.4, $[A : r(G)] = 2$.

We are ready to present a general formula for

$$\sum_{n\geq 1}^{\infty} \frac{g(n)}{\#G(n)},$$

where $G(n) = \mathrm{Gal}(\mathbb{Q}(\sqrt[n]{a}, \zeta_n)/\mathbb{Q})$. Let g be a real multiplicative arithmetic function such that

$$\sum_{n\geq 1}^{\infty} \frac{|g(n)|}{\#G(n)} < \infty.$$

Let

$$\tilde{g} = \sum_{n\geq 1} g(n) 1_{\ker\varphi_{A,n}}$$

be a function from A to $\overline{\mathbb{R}}$, where $\varphi_{A,n} : A \to A(n)$ is the projection map such that $\tilde{g} = \prod_p \tilde{g}_p$. Let

$$\tilde{g}_p = \sum_{k\geq 0} g(p^k) 1_{\ker\varphi_{p^k}}$$

be a function from A_p to $\overline{\mathbb{R}}$, where $\varphi_{p^k} : A_p \to A(p^k)$ is the projection map. Let $\chi : A \to \mu_2$ be the character given in (1.5) and assume that $\chi = \prod_p \chi_p$. Then, if $\int_A \tilde{g} \neq 0$, by Corollary 3.6 and

$$\#A(p^k) = p^k\phi(p^k) = p^{2k-1}(p-1),$$

where ϕ denotes the Euler phi function,

$$\sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)} = \left(1 + \prod_{p|2D} \frac{\sum_{k\geq \ell} g(p^k)/p^{2k-1}(p-1)}{1+\sum_{k\geq 1} g(p^k)/p^{2k-1}(p-1)}\right) \prod_{p} \left(1 + \sum_{k\geq 1} \frac{g(p^k)}{p^{2k-1}(p-1)}\right), \tag{4.8}$$

where in the product on primes dividing $2D$, we have $\ell = 1$ for odd primes and for prime 2 we have $\ell = 1$ if D is odd, $\ell = 2$ if $4 \parallel D$, and $\ell = 3$ if $8 \parallel D$.

Note that the conditions appearing in parts (vi) and (vii) of Theorem 3.5 are not needed for the family of Kummer fields. In this case, the profinite group A is the group of matrices given in (4.3). Hence, for part (vi), considering $\alpha \in A$ such that α maps to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \overline{3} \end{smallmatrix}\right)$ via projection to $A(4)$, then α is in $\ker\varphi_2$. On the other hand, we have $\chi_2(\alpha) = \chi_{D,2}(\overline{3}) = -1$. Thus, χ_2 is non-trivial on $\ker\varphi_2$. Therefore, the assertions of part (vi) of Theorem 3.5 hold for χ_2. Similarly, for part (vii), let α map to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \overline{5} \end{smallmatrix}\right)$ via projection to $A(8)$. Then, α is in $\ker\varphi_2$ and $\ker\varphi_4$. On the other hand, $\chi_2(\alpha) = \chi_{D,2}(\overline{5}) = -1$. Therefore, χ_2 is non-trivial on $\ker\varphi_2$ and $\ker\varphi_4$. Hence, in the case of the family of Kummer fields the assertions in part (vii) hold automatically.

We next employ (4.8) to compute the correction factor in some Artin type problems.

4.1.1 The Classical Artin Problem

In this section, we apply (4.8) to the Artin's primitive root conjecture. The following result is proved in [10].

Corollary 4.5 (Artin's Primitive Root Density)**.** *Let a be an integer for which $|a|$ is not a perfect power. Let δ be the density of primes q for which a is a primitive root modulo q. Let D be the discriminant of $\mathbb{Q}(\sqrt{a})$. Then, under the Generalized Riemann Hypothesis (GRH) for $\mathbb{Q}(\zeta_n, \sqrt[n]{a})$, n square-free, if $D \equiv 1 \pmod 4$,*

$$\delta = \left(1 + \prod_{p|2D} \frac{-1}{p(p-1)-1}\right) \prod_{p} \left(1 - \frac{1}{p(p-1)}\right)$$

and

$$\delta = \prod_p \left(1 - \frac{1}{p(p-1)}\right)$$

otherwise.

Proof. It is known that the integer a is a primitive root modulo $q \nmid 2a$ if and only if for all primes $p \mid q-1$, the prime q does not split completely in K_p, the splitting field of $x^p - a$ (see [26, Page 384]). By the main result of [10], we have, under the GRH, that the density δ is finite and is given by

$$\delta = \sum_{n=1}^{\infty} \frac{\mu(n)}{[K_n : \mathbb{Q}]}, \tag{4.9}$$

where $K_n = \mathbb{Q}(\zeta_n, \sqrt[n]{a})$ and $\mu(n)$ is the Möbius function. By (4.8), we have

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{[K_n : \mathbb{Q}]} = \left(1 + \prod_{p|2D} \frac{\sum_{k\geq \ell} \mu(p^k)/p^{2k-1}(p-1)}{1+\sum_{k\geq 1} \mu(p^k)/p^{2k-1}(p-1)}\right) \prod_p \left(1 + \sum_{k\geq 1} \frac{\mu(p^k)}{p^{2k-1}(p-1)}\right), \tag{4.10}$$

where $\ell = 1$ for odd primes. For prime 2, we have $\ell = 1$ if D is odd, $\ell = 2$ if $4 \parallel D$, and $\ell = 3$ if $8 \parallel D$.

If $D \equiv 1 \pmod 4$, then $\ell = 1$ for all $p \mid 2D$. Hence, in this case

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{\mu(n)}{[K_n : \mathbb{Q}]} &= \left(1 + \prod_{p|2D} \frac{\sum_{k\geq 1} \mu(p^k)/p^{2k-1}(p-1)}{1+\sum_{k\geq 1} \mu(p^k)/p^{2k-1}(p-1)}\right) \prod_p \left(1 + \sum_{k\geq 1} \frac{\mu(p^k)}{p^{2k-1}(p-1)}\right) \\ &= \left(1 + \prod_{p|2D} \frac{\mu(p)/p^{2-1}(p-1)}{1+\mu(p)/p^{2-1}(p-1)}\right) \prod_p \left(1 + \frac{\mu(p)}{p^{2-1}(p-1)}\right), \end{aligned} \tag{4.11}$$

which is the desired result. On the other hand, if D is even then for prime 2, we have $\ell > 1$. Hence, the first parentheses in (4.11) become 1 since $\mu(2^k) = 0$. This completes the proof. □

4.1.2 Titchmarsh Divisor Problem (Kummer Case)

Consider a family of Galois extensions $\mathcal{F} = \{F_m/\mathbb{Q};\ m \in \mathbb{N}\}$. Let D_m be a union of conjugacy classes of $\mathrm{Gal}(F_m/\mathbb{Q})$. Define

$$\tau_{\mathcal{F}}(p) = \#\left\{m \in \mathbb{N};\ p \text{ is unramified in } F_m/\mathbb{Q} \text{ and the Artin symbol } \left(\frac{F_m/\mathbb{Q}}{p}\right) \subset D_m\right\}.$$

Recall that the Titchmarsh divisor problem concerns the behaviour of $\sum_{p\le x}\tau_{\mathcal{F}}(p)$ as $x \to \infty$.

For the family of Kummer fields, the following theorem is proved in [8, Theorem 1.6].

Theorem 4.6 (Felix-Murty)**.** *Let $\mathcal{F}$ be the family of Kummer fields*

$$\{K_n = \mathbb{Q}(\zeta_n, a^{1/n});\ n \ge 1\}.$$

Then under the GRH for the Dedekind zeta function of $\mathbb{Q}(\zeta_n, \sqrt[n]{a})/\mathbb{Q}$ for $n \ge 1$, we have

$$\sum_{p\le x}\tau_{\mathcal{F}}(p) \sim \left(\sum_{n\ge 1}\frac{1}{[K_n:\mathbb{Q}]}\right)\cdot \mathrm{li}(x) \tag{4.12}$$

as $x \to \infty$, where $\mathrm{li}(x) = \int_2^x \frac{1}{\log t}dt$.

Note that unlike Artin's conjecture, instead of $\mu(n)$, we have 1 in the numerator of the summands of the infinite sum in (4.12). Thus, integers that are not square free make contributions to the constant in (4.12).

We next give the product form of the summation $\sum_{n\ge 1}\frac{1}{[K_n:\mathbb{Q}]}$. The following corollary is a new result derived from the methods presented in this thesis.

Corollary 4.7. *Let a be an integer such that $|a|$ is not a perfect power. Let*

$$\{K_n = \mathbb{Q}(\zeta_n, a^{1/n}),\ n \ge 1\}$$

be the family of Kummer fields. We have

$$\sum_{n\geq 1}\frac{1}{[K_n:\mathbb{Q}]}=\left(1+c_0\prod_{p|2D}\frac{p}{(p-1)(p^2-1)+p}\right)\prod_p\left(1+\frac{p}{(p-1)(p^2-1)}\right), \quad (4.13)$$

where $c_0\in\{1,1/4,1/16\}$. *More precisely,* $c_0=1$ *if* D *is odd,* $c_0=1/4$ *if* $4\,||\,D$, *and* $c_0=1/16$ *if* $8\,||\,D$.

Proof. By (4.8),

$$\sum_{n=1}^{\infty}\frac{1}{[K_n:\mathbb{Q}]}=\left(1+\prod_{p|2D}\frac{\sum_{k\geq\ell}1/p^{2k-1}(p-1)}{1+\sum_{k\geq 1}1/p^{2k-1}(p-1)}\right)\prod_p\left(1+\sum_{k\geq 1}\frac{1}{p^{2k-1}(p-1)}\right),$$

where in the product on the primes dividing $2D$, we have $\ell=1$ for odd primes and for prime 2, $\ell=1$ if D is odd, $\ell=2$ if $4\parallel D$, and $\ell=3$ if $8\parallel D$.

Note that

$$\frac{\sum_{k\geq 1}1/p^{2k-1}(p-1)}{1+\sum_{k\geq 1}1/p^{2k-1}(p-1)}=\frac{p}{(p-1)(p^2-1)+p}$$

and we have

$$\sum_{k\geq\ell}\frac{1}{2^{2k-1}(2-1)}=c_0\cdot\sum_{k\geq 1}\frac{1}{2^{2k-1}(2-1)},$$

where $c_0=1$ if $\ell=1$, $c_0=1/4$ if $\ell=2$, and $c_0=1/16$ if $\ell=3$. Therefore, the desired result holds. □

4.2 Serre Curves

Let E be an elliptic curve over $\mathbb{Q}$ given by a Weierstrass equation

$$y^2=x^3+ax+b,$$

where $a, b \in \mathbb{Q}$. Let Δ be the discriminant of x^3+ax+b. Let $K_n = \mathbb{Q}(E[n])$ be the n-division field of E. By taking the inverse limit of the natural injective maps

$$r_n : \mathrm{Gal}(K_n/\mathbb{Q}) \to \mathrm{Aut}(E[n]) \cong A(n) = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

over all $n \geq 1$ given in Theorem 2.32, we have an injective profinite homomorphism

$$r\colon\ G = \mathrm{Gal}(K_\infty/\mathbb{Q}) \to \mathrm{Aut}(E[\infty]) \cong A = \mathrm{GL}_2(\hat{\mathbb{Z}}).$$

As a consequence of the Chinese Remainder Theorem, we note that $A = \mathrm{GL}_2(\hat{\mathbb{Z}}) \cong \prod_p A_p$, where $A_p = \mathrm{GL}_2(\mathbb{Z}_p)$. For $K = \mathbb{Q}(\sqrt{\Delta})$, we have that $K \subset K_2 = \mathbb{Q}(E[2])$ since

$$\Delta = ((x_1-x_2)(x_1-x_3)(x_2-x_3))^2, \tag{4.14}$$

where x_1, x_2, and x_3 are roots of x^3+ax+b and thus, they are the x-coordinate of the points of order 2 of E. Moreover, by the Weil pairing we have that $\zeta_n \in K_n$ (see [24, Corollary III.8.1.1]). Thus, we have the following commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G' & \xrightarrow{i_1} & G & \xrightarrow{\text{rest}} & \mathrm{Gal}(\mathbb{Q}_{ab}/\mathbb{Q}) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow r & & \downarrow \simeq & & \\ 1 & \longrightarrow & \mathrm{SL}_2(\hat{\mathbb{Z}}) & \xrightarrow{i_2} & A = \mathrm{GL}_2(\hat{\mathbb{Z}}) & \xrightarrow{\det} & \hat{\mathbb{Z}}^\times & \longrightarrow & 1, \end{array} \tag{4.15}$$

where i_1 and i_2 are inclusion maps, $G' = \mathrm{Gal}(K_\infty/\mathbb{Q}_{ab})$ is the commutator of G, and $\mathrm{SL}_2(\hat{\mathbb{Z}}) = \ker(\det)$ is the subgroup of matrices in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ with determinant 1.

In anticipation of applying Theorem 3.2, let γ be the determinant map $\det : A \to \hat{\mathbb{Z}}^\times$ and

$$\chi_D : A \xrightarrow{\gamma} \hat{\mathbb{Z}}^\times \xrightarrow{\left(\frac{D}{\cdot}\right)} \mu_2$$

be the composition of γ with the lift of the Kronecker symbol attached to D to $\hat{\mathbb{Z}}^\times$. We also

note that $A(2) = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$, where S_3 is the symmetric group on three letters. Let

$$\psi : A \to A(2) \cong S_3 \xrightarrow{\text{sign}} \mu_2$$

be the composition of the projection map with the signature character on S_3. By (4.14), the signature map for $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is the same as $\frac{\sigma(\sqrt{\Delta})}{\sqrt{\Delta}}$. Thus, the diagram attached to ψ in (3.15) commutes. Therefore, by Theorem 3.2, we have $r(G) \subset \ker\chi$, where $\chi = \chi_D \cdot \psi$ is a non-trivial character on A. This construction of character χ was described by J. P. Serre in [23].

Recall that we name E a *Serre curve* if $r(G) = \ker\chi$. The condition $r(G) = \ker\chi$ is equivalent to $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : r(G)] = 2$ since $r(G) \subset \ker\chi$. Thus, for Serre curve E, the sequence

$$1 \longrightarrow G \xrightarrow{r} A \xrightarrow{\chi} \mu_2 \longrightarrow 1 \tag{4.16}$$

is an exact sequence. Therefore, we can conclude the result of Corollary 3.6 for sums involving the size of $G(n) = \mathrm{Gal}(K_n/\mathbb{Q})$. More precisely, let g be a real multiplicative arithmetic function such that

$$\sum_{n\geq 1} \frac{|g(n)|}{\#G(n)} < \infty.$$

Let

$$\tilde{g} = \sum_{n\geq 1} g(n) 1_{\ker\varphi_{A,n}}$$

be a function from A to $\overline{\mathbb{R}}$, where $\varphi_{A,n} : A \to A(n)$ is the projection map, such that $\tilde{g} = \prod_p \tilde{g}_p$. Let

$$\tilde{g}_p = \sum_{k\geq 0} g(p^k) 1_{\ker\varphi_{p^k}}$$

be a function from A_p to $\overline{\mathbb{R}}$, where $\varphi_{p^k} : A_p \to A(p^k)$ is the projection map. Let $\chi : A \to \mu_2$ be the character given in (1.5) and assume that $\chi = \prod_p \chi_p$. Therefore, if $\int_A \tilde{g} \neq 0$, by Corollary

3.6, we have

$$\sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)}$$
$$= \left(1 + \prod_{p|2D} \frac{\sum_{k\geq \ell} g(p^k)/p^{4k-3}(p^2-1)(p-1)}{1+\sum_{k\geq 1} g(p^k)/p^{4k-3}(p^2-1)(p-1)}\right) \prod_p \left(1 + \sum_{k\geq 1} \frac{g(p^k)}{p^{4k-3}(p^2-1)(p-1)}\right), \tag{4.17}$$

where in the product on primes dividing $2D$, we have $\ell = 1$ for odd primes and for prime 2 we have $\ell = 1$ if D is odd, $\ell = 2$ if $4 \parallel D$, and $\ell = 3$ if $8 \parallel D$. Here, we used (2.1) that states $\#A(p^k) = p^{4k-3}(p^2-1)(p-1)$.

Note that the conditions $\zeta_4 \notin K_2$ and $\zeta_8 \notin K_4$ are not needed here since the profinite group A is $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Hence, similar to the case of Kummer family using an argument identical to the one described after formula (4.8), the desired results hold automatically without conditions $\zeta_4 \in K_2$ and $\zeta_8 \in K_4$.

4.2.1 The Cyclicity Problem (Serre Curve Case)

In this section, we study the density of primes q for which a given Serre curve E is cyclic modulo q (Cyclicity Problem). It is known that the reduction of E is cyclic modulo q if and only if the prime q does not split completely in division fields $K_p = \mathbb{Q}(E[p])$, for any prime p less than q (see [5, Lemma 2.1]). We derive the following as a combination of Serre's cyclicity result and our formula (4.17) for $g(n) = \mu(n)$.

Corollary 4.8 (Cyclic Reduction of Serre Curves)**.** *Let E be a Serre curve with discriminant Δ. Let δ be the density of primes q for which E is cyclic modulo q. Let D be the discriminant of $\mathbb{Q}(\sqrt{\Delta})$. Then, under the GRH for the Dedekind zeta function of $\mathbb{Q}(E[n])/\mathbb{Q}$ for each n, if D is odd,*

$$\delta = \left(1 + \prod_{p|2D} \frac{-1}{(p^2-1)(p^2-p)-1}\right) \prod_p \left(1 - \frac{1}{(p^2-1)(p^2-p)}\right),$$

and

$$\delta = \prod_p \left(1 - \frac{1}{(p^2-1)(p^2-p)}\right)$$

otherwise.

Proof. Under the assumption of the GRH for the Dedekind zeta function of $\mathbb{Q}(E[n])/\mathbb{Q}$ for square-free n, in [22], Serre proved that the density in the Cyclicity Problem is

$$\delta = \sum_{n=1}^{\infty} \frac{\mu(n)}{[K_n : \mathbb{Q}]}.$$

Hence, by (4.17), we have

$$\begin{aligned} &\sum_{n=1}^{\infty} \frac{\mu(n)}{\#G(n)} \\ &= \left(1 + \prod_{p|2D} \frac{\sum_{k\geq \ell} \mu(p^k)/p^{4k-3}(p^2-1)(p-1)}{1+\sum_{k\geq 1} \mu(p^k)/p^{4k-3}(p^2-1)(p-1)}\right) \prod_p \left(1 + \sum_{k\geq 1} \frac{\mu(p^k)}{p^{4k-3}(p^2-1)(p-1)}\right), \end{aligned} \tag{4.18}$$

where in the product on primes dividing $2D$, we have $\ell = 1$ for odd primes and for prime 2 we have $\ell = 1$ if D is odd, $\ell = 2$ if $4 \parallel D$, and $\ell = 3$ if $8 \parallel D$.

If $D \equiv 1 \bmod 4$, then $\ell = 1$ for all $p \mid 2D$. Hence, in this case

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{\#G(n)} = \left(1 + \prod_{p|2D} \frac{\mu(p)/p^{4-3}(p^2-1)(p-1)}{1+\mu(p)/p^{4-3}(p^2-1)(p-1)}\right) \prod_p \left(1 + \frac{\mu(p)}{p^{4-3}(p^2-1)(p-1)}\right),$$

which is the desired result for odd D. On the other hand, if D is even then for prime 2 in (4.18), we have $\ell > 1$. Hence, the first parentheses in the right-hand side of the identity (4.18) becomes 1. This completes the proof. □

4.2.2 The Titchmarsh Divisor Problem (Serre Curve Case)

In this section, we study the elliptic curve analogue of the Titchmarsh Divisor Problem studied in Section 4.1.2. Let $\mathcal{F}$ be the family of fields $\{K_n = \mathbb{Q}(E[n]), n \geq 1\}$, where E is a

Serre curve. Let $\tau_{\mathcal{F}}(p)$ be as described in Section 4.1.2. The following result was proven in [1, Theorem 1.2].

Theorem 4.9 (Akbary-Ghioca)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. Then under the GRH for the Dedekind zeta function of $\mathbb{Q}(E[n])/\mathbb{Q}$ for each $n \geq 1$, we have*

$$\sum_{p \leq x} \tau_{\mathcal{F}}(p) = \left(\sum_{n=1}^{\infty} \frac{1}{[\mathbb{Q}(E[n]) : \mathbb{Q}]} \right) \cdot \mathrm{li}(x) + O\left(x^{5/6} (\log x)^{2/3} \right).$$

An application of (4.17) with $g(n) = 1$ provides the following result regarding the constant in the asymptotic formula of Theorem 4.9.

Corollary 4.10. *For the family of fields $\{K_n = \mathbb{Q}(E[n]), n \geq 1\}$, where E is a Serre curve, we have*

$$\begin{aligned} &\sum_{n=1}^{\infty} \frac{1}{[\mathbb{Q}(E[n]) : \mathbb{Q}]} \\ &= \left(1 + \prod_{p \mid 2D} \frac{\sum_{k \geq \ell} 1/p^{4k-3}(p^2-1)(p-1)}{1 + \sum_{k \geq 1} 1/p^{4k-3}(p^2-1)(p-1)} \right) \prod_{p} \left(1 + \sum_{k \geq 1} \frac{1}{p^{4k-3}(p^2-1)(p-1)} \right), \end{aligned}$$

where in the product on primes dividing $2D$, we have $\ell = 1$ for odd primes and for prime 2 we have $\ell = 1$ if D is odd, $\ell = 2$ if $4 \parallel D$, and $\ell = 3$ if $8 \parallel D$.

Proof. By Theorem 4.9 and (4.17), where $g(n) = 1$, the result holds. □

The above corollary is proved in [2, Theorem 5] by another method.

4.3 Remarks on the Condition $[A : r(G)] = 2$

It is evident that the condition $[A : r(G)] = 2$ in Corollary 3.6 plays a crucial rule in our computation of the constants in the Artin type problems. This condition holds in Serre curves as part of the definition of a Serre curve. The proof of this condition for the Kummer family was one of our major tasks in Section 4.1. We end this chapter by stating necessary

and sufficient assertions for which the condition $[A : r(G)] = 2$ in Corollary 3.6 holds. Recall that, we denote the commutator of a group G by G'.

Proposition 4.11. *Let A and G be the profinite groups described in the beginning of Section 3.2 with injective homomorphism $r : G \to A$. Let $\chi = \prod_p \chi_p : A \to \mu_2$ be the quadratic character defined in Theorem 3.5. If $A^{ab} \cong \hat{\mathbb{Z}}^\times \times \mu_2$, where $A^{ab} = A/A'$ is the abelianization of A, then $[A : r(G)] = 2$ if and only if $G' \cong A'$.*

Proof. Observe that G/G' is the Galois group of maximal the abelian extension over $\mathbb{Q}$ which is contained in $K_\infty = \cup_{n\geq 1} K_n$. Thus, since $\mathbb{Q}_{ab}$ is contained in K_∞, we have $G/G' = \mathrm{Gal}(\mathbb{Q}_{ab}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^\times$.

Assume $[A : r(G)] = 2$. Hence, $[A/A' : r(G)/r(G')] = [\hat{\mathbb{Z}}^\times \times \mu_2 : \hat{\mathbb{Z}}^\times] = [A : r(G)]$. Thus, since r is injective and $r(G') \subset A'$, we have $G' \cong A'$.

Conversely, if $G' \cong A'$, we get

$$A/r(G') \cong A/A' \cong \hat{\mathbb{Z}}^\times \times \mu_2.$$

Therefore, since $r(G)/r(G') \cong G/G' \cong \hat{\mathbb{Z}}^\times$, we have $[A/r(G') : r(G)/r(G')] = 2$. Thus, $[A : r(G)] = 2$. □

For the family of Kummer fields in Section 4.1, we are able to prove that one of the conditions of Proposition 4.11 holds.

Proposition 4.12. *With the above notation, we have $A^{ab} \cong \hat{\mathbb{Z}}^\times \times \mu_2$.*

Proof. Consider the surjective map $\det : A \to \hat{\mathbb{Z}}^\times$. Let H be

$$H = \ker(\det) = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} ; \, b \in \hat{\mathbb{Z}} \right\}.$$

Thus, the sequence

$$1 \to H \xrightarrow{i} A \xrightarrow{\det} \hat{\mathbb{Z}}^\times \to 1 \tag{4.19}$$

is exact, where i is the inclusion map. Since $A/H \cong \hat{\mathbb{Z}}^\times$ is abelian, we have $A' \subset H$, where A' is the commutator of A.

Next, we find the index of A' in H. Observe that if $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ b & d \end{smallmatrix}\right)$ and $\beta = \left(\begin{smallmatrix} 1 & 0 \\ b' & d' \end{smallmatrix}\right)$ are in A, then

$$\alpha\beta\alpha^{-1}\beta^{-1} = \begin{pmatrix} 1 & 0 \\ b(1-d') + b'(1-d) & 1 \end{pmatrix}. \tag{4.20}$$

Hence,

$$A' = \left\{ \begin{pmatrix} 1 & 0 \\ \sum_k b_k(1-d_k) & 1 \end{pmatrix};\ b_k \in \hat{\mathbb{Z}} \text{ and } d_k \in \hat{\mathbb{Z}}^\times \right\}.$$

We claim that

$$A' = \left\{ \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \in H;\ c = (c_i) \in \hat{\mathbb{Z}} \text{ and } c_2 = 0 \in \mathbb{Z}/2\mathbb{Z} \right\}.$$

First, we show $A' \subset \{\left(\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix}\right) \in H;\ c = (c_i) \in \hat{\mathbb{Z}} \text{ and } c_2 = 0\}$. If $c = (c_i) \in \hat{\mathbb{Z}}$ has the form $\sum_k b_k(1-d_k)$ with $b_k \in \hat{\mathbb{Z}}$ and $d_k \in \hat{\mathbb{Z}}^\times$, then $c_2 = 0$ since $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$. Thus, $A' \subset \{\left(\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix}\right) \in H;\ c = (c_i) \in \hat{\mathbb{Z}} \text{ and } c_2 = 0\}$. On the other hand, if i is odd, then we can consider $c_i = \frac{c_i}{2}(1-(-1))$, since both -1 and 2 are invertible in $\mathbb{Z}/i\mathbb{Z}$. If $i \neq 2$ is even, then we have $c_i = 2c_i' = c_i'(1-(-1))$ for some $c_i' \in \mathbb{Z}/i\mathbb{Z}$ and $-1 \in (\mathbb{Z}/i\mathbb{Z})^\times$. Therefore, $\{\left(\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix}\right) \in H;\ c = (c_i) \in \hat{\mathbb{Z}} \text{ and } c_2 = 0\} \subset A'$. Thus, we showed that

$$A' = \left\{ \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \in H;\ c = (c_i) \in \hat{\mathbb{Z}} \text{ and } c_2 = 0 \in \mathbb{Z}/2\mathbb{Z} \right\}.$$

From description of H and A' we conclude that $H/A' \cong \mu_2$. Hence, (4.5) implies

$$A^{ab} = A/A' \cong A/H \times H/A' \cong \hat{\mathbb{Z}}^\times \times \mu_2.$$

Note that $A' \trianglelefteq H \trianglelefteq A$ and thus $A/A' \cong A/H \times H/A'$. □

We note that in view of Propositions 4.11 and 4.12 for the family of Kummer fields, if we can prove in a straightforward way that $A' \cong G'$, then we have another proof of the important fact $[A : r(G)] = 2$ for the Kummer family. In addition, we observe that the assertion $[A : r(G)] = 2$ for the Kummer family implies that $A' \cong G'$. This is true since $G' \subset A'$ and by the commutative diagram (4.6) and the proof of Proposition 4.12, we have $[H : A'] = [H : G'] = 2$. Therefore for the Kummer family the condition $[A : r(G)] = 2$ is equivalent to $G' \cong A'$.

We finally provide a characterization of Serre curves using the idea described in this section.

Proposition 4.13. *Let E be an elliptic curve defined over $\mathbb{Q}$. With notation of diagram* (4.15)*, we have that E is a Serre curve if and only if $G' \cong A'$.*

Proof. First of all we note that $A^{ab} \cong \hat{\mathbb{Z}}^\times \times \mu_2$. This is true since in [27, Lemma 4.11], Zywina proves that the commutator $\mathrm{GL}_2'(\hat{\mathbb{Z}})$ has index 2 inside $\mathrm{SL}_2(\hat{\mathbb{Z}})$. More precisely, he shows that $[\mathrm{SL}_2(\mathbb{Z}_2) : \mathrm{GL}_2'(\mathbb{Z}_2)] = 2$ and $\mathrm{SL}_2(\mathbb{Z}_p) = \mathrm{GL}_2'(\mathbb{Z}_p)$ for odd primes. Hence, considering the second row of the commutative diagram (4.15), we have $\mathrm{GL}_2(\hat{\mathbb{Z}})/\mathrm{GL}_2'(\hat{\mathbb{Z}}) \cong \hat{\mathbb{Z}}^\times \times \mu_2$. Thus, $A^{ab} = \hat{\mathbb{Z}}^\times \times \mu_2$.

Now by Proposition 4.11, the desired result holds. □

Chapter 5

Generalizations and Results

In this section, we generalize the idea of using the maps $\varphi_{A,n} : A \to A(n)$ in Theorem 3.2. Let $B = \varprojlim B(n)$ be a profinite group together with a homomorphism from A to B. Let $B \cong \prod_p B_p$, where $B_p = \varprojlim B(p^k)$. We consider the homomorphisms $\varphi_{A,n} : A \to B(n)$ for $n \geq 1$. Then we have the following assertion that generalizes parts of Theorem 3.2 and Corollary 3.4.

Theorem 5.1. *Let $A = \varprojlim A(n)$ and $B = \varprojlim B(n)$ be as described above. Let g be an arithmetic function. Let $\chi : A \to \mu_m$ be a surjective continuous homomorphism. For a fixed subset $H \subset B$, let $\varphi_{A,n}^{-1}(H(n))$ be the inverse image of $H(n)$ via $\varphi_{A,n}$, where $H(n)$ is the projection of H in $B(n)$. Suppose*

$$\sum_{n\geq 1} |g(n)| \nu_A(\varphi_{A,n}^{-1}(H(n)) \cap \ker\chi) < \infty,$$

and $\tilde{g} = \sum_{n\geq 1} g(n) 1_{\varphi_{A,n}^{-1}(H(n))}$ defines a function from A to $\overline{\mathbb{R}}$. Then

$$\frac{1}{\nu_A(\ker\chi)} \sum_{n\geq 1} g(n)\nu_A(\varphi_{A,n}^{-1}(H(n)) \cap \ker\chi) = \sum_{i=0}^{m-1} \int_A \tilde{g}\chi^i d\nu_A.$$

Furthermore, if g is real multiplicative, $A \cong \prod_p A_p$, $\chi = \prod_p \chi_p$, $\tilde{g} = \prod_p \tilde{g}_p$, $[A : \ker\chi] = 2$, and $\int_A \tilde{g} d\nu_A \neq 0$, then

$$\frac{1}{\nu_A(\ker\chi)} \sum_{n\geq 1} g(n)\nu_A(\varphi_{A,n}^{-1}(H(n)) \cap \ker\chi) = \left(\prod_p \int_{A_p} \tilde{g}_p d\nu_{A_p}\right)\left(1 + \prod_p \frac{\int_{A_p} \tilde{g}_p\chi_p d\nu_{A_p}}{\int_{A_p} \tilde{g}_p d\nu_{A_p}}\right).$$

Here, we assume that $\tilde{g}_p = \sum_{k\geq 0} g(p^k) 1_{\varphi_{p^k}^{-1}(H(p^k))}$ *defines a function from* A_p *to* $\overline{\mathbb{R}}$*, where the functions* $\varphi_{p^k} : A_p \to B(p^k)$ *are projections.*

Proof. The proof follows steps indicated in the proofs of Theorem 3.2 and Corollary 3.3. We have, by an application of dominant convergence theorem,

$$\frac{1}{\nu_A(\ker\chi)} \sum_{n\geq 1} g(n)\nu_A(\varphi_{A,n}^{-1}(H(n)\cap \ker\chi) = \frac{\int_A \tilde{g} 1_{\ker\chi} d\nu_A}{\int_A 1_{\ker\chi} d\nu_A}.$$

Now using the character relations described in the proof of Theorem 3.2, we get

$$\frac{\int_A \tilde{g} 1_{\ker\chi} d\nu_A}{\int_A 1_{\ker\chi} d\nu_A} = E_\chi(\tilde{g}) = \sum_{i=1}^{m-1} \int_A \tilde{g}\chi^i d\nu_A.$$

The rest of the proof is similar to the proof of Corollary 3.3, which uses the multiplicativity of g, $A \cong \prod_p A_p$, $\nu_A = \prod_p \nu_{A_p}$, $\chi = \prod_p \chi_p$, $\tilde{g} = \prod_p \tilde{g}_p$, and $[A : \ker\chi] = 2$. □

5.1 The Generalized Artin Problem

Artin's conjecture predicts the density of primes p such that p does not split completely in any K_q for all primes $q < p$. In another words, this is the density of primes p such that $\left(\frac{K_q/\mathbb{Q}}{p}\right) \neq \mathrm{id}$ for any prime $q < p$.

We have the following theorem related to the density in a generalization of Artin's conjecture.

Theorem 5.2. *For a fixed integer* a *where* $|a|$ *is not a perfect power, let*

$$\{K_n = \mathbb{Q}(\sqrt[n]{a}, \zeta_n), n \geq 1\}$$

be the family of Kummer fields with Galois groups $G(n)$ *over* $\mathbb{Q}$*. Let* $D = \mathrm{disc}_{\mathbb{Q}}(K_2)$*. Let* $G = \varprojlim G(n)$ *and let* C *be a conjugacy class in* G*. Let* $C(n)$ *be the image of* C *under*

projection (restriction map) $\Phi_n : G \to G(n)$. *Assume that*

$$\sum_{n\geq 1} \frac{\mu^2(n)\#C(n)}{[K_n:\mathbb{Q}]} < \infty.$$

Then, we have

$$\begin{aligned}\sum_{n\geq 1} \frac{\mu(n)\#C(n)}{[K_n:\mathbb{Q}]} &= \left(1-\mu(D)\prod_{p|2D}\frac{\#C(p)}{[K_p:\mathbb{Q}]-\#C(p)}\right)\prod_p\left(1-\frac{\#C(p)}{[K_p:\mathbb{Q}]}\right)\\ &= \left(1-\mu(D)\prod_{p|2D}\frac{\#C(p)}{p^2-p-\#C(p)}\right)\prod_p\left(1-\frac{\#C(p)}{p^2-p}\right).\end{aligned}$$

Proof. We first show that

$$\nu_G(\Phi_n^{-1}(C(n))) = \frac{\#C(n)}{\#G(n)}. \tag{5.1}$$

Since ν_G is translation invariant, we have

$$\nu_G(a\ker\Phi_n) = \nu_G(\ker\Phi) = \frac{1}{\#G(n)}.$$

Note that $G = \cup_{i=1}^m (a_i \ker\Phi_n)$, where $G(n) = \{\Phi_n(a_1),\dots,\Phi_n(a_m)\}$. Hence,

$$\nu_G(\Phi_n^{-1}(C(n))) = \nu_G(\cup_{i=1}^k b_i\ker\Phi_n) = \sum_{i=1}^k \frac{1}{\#G(n)} = \frac{k}{\#G(n)},$$

where $k = \#C(n)$.

By (3.4), we have $\nu_G(\ker\Phi_n) = \nu_A(r(\ker\Phi_n))/\nu_A(r(G))$. Hence,

$$\begin{aligned}\nu_G(\Phi_n^{-1}(C(n))) &= \sum_1^k \nu_G(\ker\Phi_n)\\ &= \sum_1^k \frac{\nu_A(r(\ker\Phi_n))}{\nu_A(r(G))}\\ &= \frac{\nu_A(r(\cup_1^k b_i\ker\Phi_n))}{\nu_A(\ker\chi)}\\ &= \frac{\nu_A(r(\Phi^{-1}(C(n))))}{\nu_A(\ker\chi)}.\end{aligned} \tag{5.2}$$

Let $H = r(C)$ and $H(n)$ be the image of H under the projection map $\varphi_{A,n} : A \to A(n)$. We claim that

$$r(\Phi_n^{-1}(C(n))) = \varphi_{A,n}^{-1}(H(n)) \cap \ker\chi. \tag{5.3}$$

To prove the claim, note that we have the commutative diagram:

$$\begin{array}{ccc} G & \xrightarrow{\Phi_n} & G(n) \\ \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle r_n} \\ A & \xrightarrow{\varphi_{A,n}} & A(n) \end{array} \tag{5.4}$$

Note that $r(C) = H$ and so $r_n(C(n)) = H(n)$. Let $\alpha \in r(\Phi_n^{-1}(C(n)))$. Hence, $\alpha \in \ker\chi$ and there exists $\sigma \in \Phi_n^{-1}(C(n))$ such that $r(\sigma) = \alpha$. Thus, $\Phi_n(\sigma) \in C(n)$. Hence, $r_n(\Phi_n(\sigma)) \in H(n)$. On the other hand by commutative diagram (5.4), $\varphi_{A,n}(\alpha) \in H(n)$. Thus, $\alpha \in \varphi_{A,n}^{-1}(H(n))$. Therefore, $r(\Phi_n^{-1}(C(n))) \subset \varphi_{A,n}^{-1}(H(n)) \cap \ker\chi$. On the other hand, let $\alpha \in \varphi_n^{-1}(H(n)) \cap \ker\chi$. Hence, there exists $\sigma \in G$ such that $r(\sigma) = \alpha$. Since $r(\sigma) \in \varphi_{A,n}^{-1}(H(n))$, we have $\varphi_{A,n}(r(\sigma)) \in H(n)$. Note that $r_n(C(n)) = H(n)$. Thus, since r_n is injective and the diagram commutes, we have $\Phi_n(\sigma) \in C(n)$. Therefore, $\sigma \in \Phi_n^{-1}(C(n))$. This proves the claim.

Now by (5.1), (5.2), and (5.3), we have

$$\sum_{n\geq 1} \frac{\mu(n)\#C(n)}{\#G(n)} = \frac{1}{\nu_A(\ker\chi)} \sum_{n\geq 1} \mu(n)\nu_A(\varphi_{A,n}^{-1}(H(n)) \cap \ker\chi).$$

Thus, by Theorem 5.1 for $B = A$ and $H = r(C)$, we have

$$\sum_{n\geq 1} \frac{\mu(n)\#C(n)}{\#G(n)} = \left(\prod_p \int_{A_p} \tilde{g}_p d\nu_{A_p}\right)\left(1 + \prod_p \frac{\int_{A_p} \tilde{g}_p \chi_p d\nu_{A_p}}{\int_{A_p} \tilde{g}_p d\nu_{A_p}}\right), \tag{5.5}$$

where $\tilde{g}_p = (1_{A_p} + \sum_{k\geq 1} \mu(p^k) 1_{\varphi_{p^k}^{-1}(H(p^k))}) = (1_{A_p} - 1_{\varphi_p^{-1}(H(p))})$. By an argument similar to the proof of (5.1), we have

$$\nu_A(\varphi_p^{-1}(H(p))) = \frac{\#H(p)}{\#A(p)}.$$

Note that $r_n(C(n)) = H(n)$ and r_n is injective, thus $\#H(p) = \#C(p)$. Therefore, the computation of the integrals is (5.5) implies the result. □

Similarly, we can consider the following generalization of the Cyclicity Problem for Serre curves.

Let C be a conjugacy class in $G = \mathrm{Gal}(\mathbb{Q}(E^{\mathrm{tor}})/\mathbb{Q})$, where E is a Serre curve. Let $C(n)$ be the image of C under the projection (restriction map) $\Phi_n : G \to G(n)$. Assume that

$$\sum_{n\geq 1} \frac{\mu^2(n)\#C(n)}{[K_n : \mathbb{Q}]} < \infty.$$

Then, we have

$$\sum_{n\geq 1} \frac{\mu(n)\#C(n)}{[K_n : \mathbb{Q}]} = \left(1 - \mu(D) \prod_{p|2D} \frac{\#C(p)}{[K_p : \mathbb{Q}] - \#C(p)}\right) \prod_{p} \left(1 - \frac{\#C(p)}{[K_p : \mathbb{Q}]}\right),$$

where $[K_p : \mathbb{Q}] = p(p^2-1)(p-1)$.

5.2 Artin Type Problems in Kummer Family for Primes in Arithmetic Progressions

In this section, we consider extensions of the results of Section 4.1 to the case of primes in a given arithmetic progression. The definitions of the notations that are not defined here are as Section 4.1.

Let $f > 1$ be a fixed positive integer and ℓ be a positive integer coprime to f. We let $\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})$ be the automorphism sending ζ_f to ζ_f^ℓ. For integer $n \geq 1$, let

$$c_\ell(n) = \begin{cases} 1 & \sigma_\ell\big|_{K_n \cap \mathbb{Q}(\zeta_f)} = \mathrm{id}_{K_n \cap \mathbb{Q}(\zeta_f)}, \\ 0 & \text{otherwise.} \end{cases} \tag{5.6}$$

We are interested in finding a product formula for the summation

$$\sum_{n\geq 1} \frac{g(n)\cdot c_\ell(n)}{[K_n(\zeta_f):\mathbb{Q}]}, \tag{5.7}$$

where g is a real multiplicative function. As we will see, such sums appear naturally when we study some Artin type problems for primes in arithmetic progressions.

In order to study the above sum, for any $n \geq 1$, we consider the homomorphisms

$$\Phi_n : G \to G(n) \times \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})$$

such that Φ_n maps $\sigma \in G$ to the pair of its projection in $G(n)$ and its restriction on $\mathbb{Q}(\zeta_f)$ via its projection on $G(f)$. We note that the homomorphism Φ_n factors via $\mathrm{Gal}(K_n(\zeta_f)/\mathbb{Q})$, i.e., the diagram

$$\begin{array}{ccc} G & \xrightarrow{\quad\Phi_n\quad} & G(n)\times \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q}) \\ & {\scriptstyle\tau_1}\searrow \quad \nearrow{\scriptstyle\tau_2} & \\ & \mathrm{Gal}(K_n(\zeta_f)/\mathbb{Q}) & \end{array}$$

commutes. Here τ_1 is the composition of the projection map to $G(nf)$ with the restriction to $\mathrm{Gal}(K_n(\zeta_f)/\mathbb{Q})$, and τ_2 is the restriction map on each of its components. Hence, $\Phi_n = \tau_2 \circ \tau_1$ and $\Phi_n^{-1}(\mathrm{id}_{G(n)}, \sigma_\ell) = \tau_1^{-1} \circ \tau_2^{-1}(\mathrm{id}_{G(n)}, \sigma_\ell)$. By [14, Section 2], if $\sigma_\ell\big|_{K_n\cap\mathbb{Q}(\zeta_f)} = \mathrm{id}$, then we have $\tau_2^{-1}(\mathrm{id}_{G(n)}, \sigma_\ell) = \{\sigma\}$ for a unique $\sigma \in \mathrm{Gal}(K_n(\zeta_f)/\mathbb{Q})$. Thus,

$$\nu_G(\Phi_n^{-1}(\mathrm{id}_{G(n)}, \sigma_\ell)) = \nu_G(\tau_1^{-1}(\sigma)) = \nu_G(g \ker \tau_1) = \nu_G(\ker \tau_1) \tag{5.8}$$

for some $g \in G$ such that $\tau_1(g) = \sigma$. Therefore, by Theorem 2.14, we have

$$\nu_G(\Phi_n^{-1}(\mathrm{id}_{G(n)}, \sigma_\ell)) = \begin{cases} \frac{1}{[K_n(\zeta_f):\mathbb{Q}]} & \sigma_\ell\big|_{K_n\cap\mathbb{Q}(\zeta_f)} = \mathrm{id}, \\ 0 & \text{otherwise.} \end{cases}$$

Hence, the summation in (5.7) is equal to

$$\sum_{n\geq 1} g(n)\nu_G(\Phi_n^{-1}(\mathrm{id}_{G(n)},\sigma_\ell)). \tag{5.9}$$

Let $A=\{\left(\begin{smallmatrix}1 & 0\\ b & d\end{smallmatrix}\right); b\in\hat{\mathbb{Z}} \text{ and } d\in\hat{\mathbb{Z}}^\times\}$ be the profinite group described in Section 4.1. We claim that

$$\nu_G(\Phi_n^{-1}(\mathrm{id}_{G(n)},\sigma_\ell)) = \frac{\nu_A(r(\Phi_n^{-1}(\mathrm{id}_{G(n)},\sigma_\ell)))}{\nu_A(r(G))}. \tag{5.10}$$

To prove the claim note that if $\sigma_\ell\big|_{K_n\cap\mathbb{Q}(\zeta_f)}\neq \mathrm{id}$, then both sides are equal to zero. Hence, let $\sigma_\ell\big|_{K_n\cap\mathbb{Q}(\zeta_f)}=\mathrm{id}$. In this case, by (5.8), we have $\nu_G(\Phi_n^{-1}(\mathrm{id}_{G(n)},\sigma_\ell))=\nu_G(\ker\tau_1)$ and $\nu_A(r(\Phi_n^{-1}(\mathrm{id}_{G(n)},\sigma_\ell)))=\nu_A(r(g\ker\tau_1))=\nu_A(r(g)r(\ker\tau_1))$, where $\tau_1(g)=\sigma$. Since ν_A is translation invariant, then the claimed identity is equivalent to

$$\nu_G(\ker\tau_1)=\frac{\nu_A(r(\ker\tau_1))}{\nu_A(r(G))}.$$

This identity holds since the left-hand side is $1/[G:\ker\tau_1]$ and the right-hand side is $(1/2[r(G):r(\ker\tau_1)])/1/2$. This proves the desired identity (5.10).

For each n, next define the homomorphism

$$\varphi_{A,n}: A\to A(n)\times(\hat{\mathbb{Z}}/f\hat{\mathbb{Z}})^\times,$$

where $A\to A(n)$ is the projection map and $A\to(\hat{\mathbb{Z}}/f\hat{\mathbb{Z}})^\times$ is the composition of det with the projection map $\hat{\mathbb{Z}}^\times\to(\hat{\mathbb{Z}}/f\hat{\mathbb{Z}})^\times$. Consider the subset $H(n)=\{(I_{2\times 2}(\mathbb{Z}/n\mathbb{Z}),\bar{\ell})\}\subset A(n)\times(\hat{\mathbb{Z}}/f\hat{\mathbb{Z}})^\times$, where $I_{2\times 2}(\mathbb{Z}/n\mathbb{Z})$ is the identity matrix and $\bar{\ell}$ is the image of ℓ in $(\hat{\mathbb{Z}}/f\hat{\mathbb{Z}})^\times$. We claim that

$$r(\Phi_n^{-1}(\mathrm{id}_{G(n)},\sigma_\ell))=\varphi_{A,n}^{-1}(H(n))\cap\ker\chi. \tag{5.11}$$

To prove the claimed identity, let $\sigma\in\Phi_n^{-1}(\mathrm{id}_{G(n)},\sigma_\ell)$. Hence, $r(\sigma)\in\ker\chi=r(G)$. Also, as

σ maps to $\mathrm{id}_{G(n)}$, the first component of $\varphi_{A,n}(r(\sigma))$ becomes $I_{2\times 2}(\mathbb{Z}/n\mathbb{Z})$ since the diagram

$$\begin{array}{ccc} G & \longrightarrow & G(n) \\ \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle r_n} \\ A & \longrightarrow & A(n) \end{array}$$

commutes. Note that σ_ℓ maps to $\overline{\ell}$ via the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q}) \cong (\hat{\mathbb{Z}}/f\hat{\mathbb{Z}})^\times$. Hence, the second component of $\varphi_{A,n}(r(\sigma))$ is $\overline{\ell}$ since the diagram

$$\begin{array}{ccc} G & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q}) \\ \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle \simeq} \\ A & \longrightarrow & (\hat{\mathbb{Z}}/f\hat{\mathbb{Z}})^\times \end{array}$$

commutes. Thus, $r(\Phi_n^{-1}(\mathrm{id}_{G(n)}, \sigma_\ell)) \subset \varphi_{A,n}^{-1}(H(n)) \cap \ker\chi$.

Next let $\alpha \in \varphi_{A,n}^{-1}(H(n)) \cap \ker\chi$. Then, since $\alpha \in \ker\chi$, there exists $\sigma \in G$ such that $r(\sigma) = \alpha$. By the above commutative diagram, since $r(\sigma) = \alpha \in \varphi_{A,n}^{-1}((I_{2\times 2}(\mathbb{Z}/n\mathbb{Z}), \overline{\ell}))$, the first component of $\Phi_n(\sigma)$ is $\mathrm{id}_{G(n)}$ as r_n is injective. The second component is σ_ℓ since we have $\mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q}) \cong (\hat{\mathbb{Z}}/f\hat{\mathbb{Z}})^\times$. Thus, $\varphi_{A,n}^{-1}(H(n)) \cap \ker\chi \subset r(\Phi_n^{-1}(\mathrm{id}_{G(n)}, \sigma_\ell))$. This proves the claimed identity (5.11).

Now, by (5.10) and (5.11), we have

$$\sum_{n\geq 1} g(n)\nu_G(\Phi_n^{-1}(\mathrm{id}_{G(n)}, \sigma_\ell)) = \frac{1}{\nu_A(r(G))} \sum_{n\geq 1} g(n)\nu_A(\varphi_{A,n}^{-1}(H(n)) \cap \ker\chi).$$

Note that $A \cong \prod_p A_p$ and $\nu_A = \prod_p \nu_{A_p}$. Suppose

$$\sum_{n\geq 1} |g(n)|\nu_A(\varphi_{A,n}^{-1}(H(n)) \cap \ker\chi) < \infty.$$

Let

$$\varphi_{p^k} : A_p \to A(p^k) \times (\mathbb{Z}_p/f\mathbb{Z}_p)^\times,$$

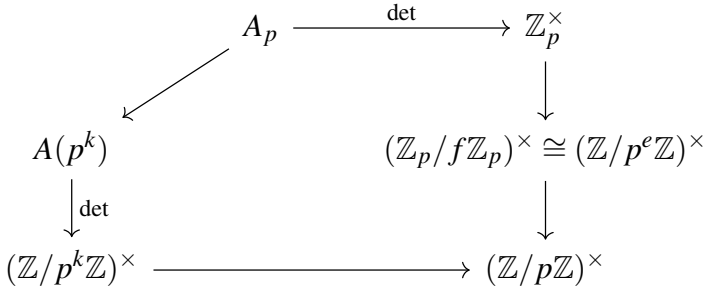
where the first component is the projection and the second component is the composition of the determinant with the map sending to modulo f. Let $\tilde{g}$ and $\tilde{g}_p$ be as defined in Theorem 5.1. Thus, if $\int_A \tilde{g} d\nu_A \neq 0$, then by applying Theorem 5.1 for $B = A \times (\hat{\mathbb{Z}}/f\hat{\mathbb{Z}})^\times$, $H = \{(I_{2\times 2}(\hat{\mathbb{Z}}), \overline{\ell})\}$, and $H(n) = \{(I_{2\times 2}(\mathbb{Z}/n\mathbb{Z}), \overline{\ell})\}$, we have

$$\sum_{n\geq 1} g(n)\nu_G(\Phi_n^{-1}(\mathrm{id}_{G(n)}, \sigma_\ell)) = \left(\prod_p \int_{A_p} \tilde{g}_p d\nu_{A_p}\right)\left(1 + \prod_p \frac{\int_{A_p} \tilde{g}_p \chi_p d\nu_{A_p}}{\int_{A_p} \tilde{g}_p d\nu_{A_p}}\right). \tag{5.12}$$

In order to evaluate the above integral, we first need to find the measure $\nu_{A_p}(\varphi_{p^k}^{-1}(H(p^k)))$ for all $k \geq 0$. We consider cases.

Case (a): If $p \nmid f$, then $(\mathbb{Z}_p/f\mathbb{Z}_p)^\times \cong \{1\}$. Hence, in this case $\varphi_{p^k} : A_p \to A(p^k) \times \{1\} \cong A(p^k)$. Thus, by Theorem 2.14, $\nu_{A_p}(\varphi_{p^k}^{-1}(H(p^k))) = 1/\#A(p^k)$.

Case (b): If $p^e \parallel f$ and $\ell \not\equiv 1 \bmod p$, then for $\alpha \in \varphi_{p^k}^{-1}(H(p^k))$ with $k > 0$, the commutative diagram



sends α to $1 \bmod p$ and at the same time sends α to $\ell \not\equiv 1 \bmod p$ which is a contradiction. Thus, we have $\nu_{A_p}(\varphi_{p^k}^{-1}(H(p^k))) = 0$ if $k > 0$. For $k = 0$, we have

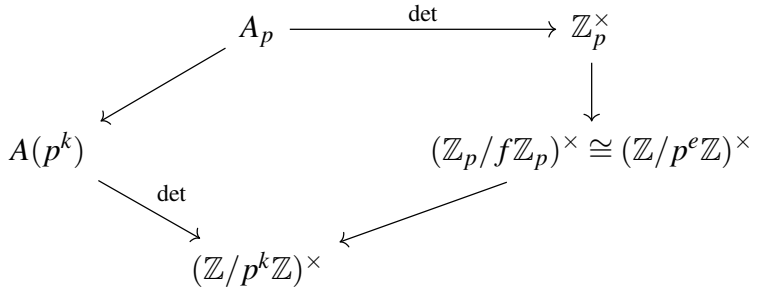
$$\varphi_{p^0} : A_p \to A(p^0) \times (\mathbb{Z}_p/f\mathbb{Z}_p)^\times \cong \{1\} \times (\mathbb{Z}/p^e\mathbb{Z})^\times.$$

Hence, we only need to check the condition on $(\mathbb{Z}_p/f\mathbb{Z}_p)^\times$. Thus, in this case

$$\nu_{A_p}(\varphi_{p^0}^{-1}(H(p^0))) = \nu_{A_p}(\ell' \ker(A_p \to (\mathbb{Z}/p^e\mathbb{Z})^\times)) = \nu_{A_p}(\ker(A_p \to (\mathbb{Z}/p^e\mathbb{Z})^\times)) = 1/\phi(p^e),$$

where ℓ' is a preimage of ℓ via $A_p \to (\mathbb{Z}/p^e\mathbb{Z})^\times$.

Case (c): If $p^e \parallel f$ and $p^t \parallel \ell - 1$, then we have several cases which we study here. If $0 \leq k \leq \min(e,t)$, then we have the following commutative diagram:

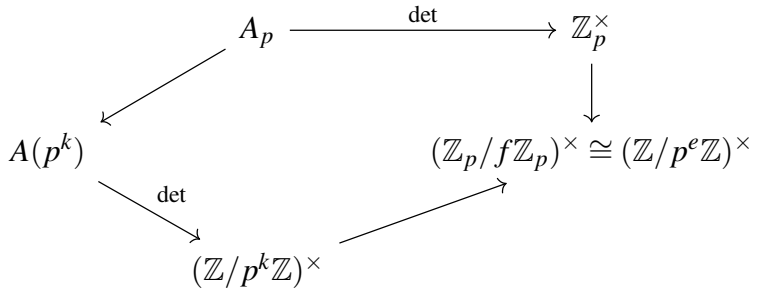


Hence, if $0 \leq k \leq \min(e,t)$, then

$$\nu_{A_p}(\varphi_{p^k}^{-1}(H(p^k))) = \frac{\phi(p^k)}{\phi(p^e)\#A(p^k)}.$$

Note that ν_{A_p} is a probability measure. Thus, using the conditional probability for $\alpha \in A_p$ that maps to $I_{2\times 2}(\mathbb{Z}/p^k\mathbb{Z})$ and $\ell \bmod (\mathbb{Z}/p^e\mathbb{Z})^\times$, we get $\nu_{A_p}(\varphi_{p^k}^{-1}(H(p^k))) = 1/p^{e-k}\#A(p^k)$ which is the same as the above formula. More precisely, assume that the condition on ℓ in $(\mathbb{Z}/p^e\mathbb{Z})^\times$ is given. Hence, we need matrices of the form $\left(\begin{smallmatrix} 1 & 0 \\ x & \ell \end{smallmatrix}\right)$ such that $x \equiv 0 \pmod{p^k}$ to satisfy the identity condition on $A(p^k)$. Thus, the probability of the identity condition on $A(p^k)$ given the condition on ℓ in $(\mathbb{Z}/p^e\mathbb{Z})^\times$ is $1/p^k$.

If $e \leq t$ and $e < k$, then we have the commutative diagram:



Hence, if $\alpha \in A_p$ maps to $I_{2\times 2}(\mathbb{Z}/p^k\mathbb{Z})$, then it maps to $\ell \equiv 1 \bmod p^e$ by the above commu-

tative diagram. Thus, if $e \leq t$ and $e < k$, then

$$\nu_{A_p}(\varphi_{p^k}^{-1}(H(p^k))) = \frac{1}{\#A(p^k)}.$$

For two remaining cases, i.e., $t < k \leq e$ and $t < e < k$, the conditions are not compatible on $(\mathbb{Z}/p^k\mathbb{Z})^\times$. Hence, for the other cases, we have $\nu_{A_p}(\varphi_{p^k}^{-1}(H(p^k))) = 0$.

Using the above information on $\nu_{A_p}(\varphi_{p^k}^{-1}(H(p^k)))$, we conclude that if $p \nmid f$, then

$$\begin{aligned}\int_{A_p} \sum_{k\geq 0} g(p^k) 1_{\varphi_{p^k}^{-1}(H(p^k))} &= \sum_{k\geq 0} g(p^k)\nu_{A_p}(\varphi_{p^k}^{-1}(H(p^k))) \\ &= 1 + \sum_{k\geq 1} \frac{g(p^k)}{\#A(p^k)}.\end{aligned} \tag{5.13}$$

If $p^e \parallel f$ and $p \nmid \ell - 1$, then

$$\begin{aligned}\int_{A_p} \sum_{k\geq 0} g(p^k) 1_{\varphi_{p^k}^{-1}(H(p^k))} &= \sum_{k\geq 0} g(p^k)\nu_{A_p}(\varphi_{p^k}^{-1}(H(p^k))) \\ &= \frac{1}{\phi(p^e)}.\end{aligned} \tag{5.14}$$

If $p^e \parallel f$ and $p^t \parallel \ell - 1$ with $1 \leq e \leq t$, then

$$\begin{aligned}\int_{A_p} \sum_{k\geq 0} g(p^k) 1_{\varphi_{p^k}^{-1}(H(p^k))} &= \sum_{k\geq 0} g(p^k)\nu_{A_p}(\varphi_{p^k}^{-1}(H(p^k))) \\ &= \sum_{k=0}^{e} \frac{g(p^k)\phi(p^k)}{\phi(p^e)\#A(p^k)} + \sum_{k>e} \frac{g(p^k)}{\#A(p^k)}.\end{aligned} \tag{5.15}$$

If $p^e \parallel f$ and $p^t \parallel \ell - 1$ with $1 \leq t < e$, then

$$\begin{aligned}\int_{A_p} \sum_{k\geq 0} g(p^k) 1_{\varphi_{p^k}^{-1}(H(p^k))} &= \sum_{k\geq 0} g(p^k)\nu_{A_p}(\varphi_{p^k}^{-1}(H(p^k))) \\ &= \sum_{k=0}^{t} \frac{g(p^k)\phi(p^k)}{\phi(p^e)\#A(p^k)}.\end{aligned} \tag{5.16}$$

We now summarize the above observations. For $p \mid f$, letting e to be the largest exponent

of p dividing f and for $p \mid \gcd(f, \ell-1)$, letting t to be the largest exponent of p dividing $\ell-1$, we get, by (5.13), (5.14), (5.15), and (5.16),

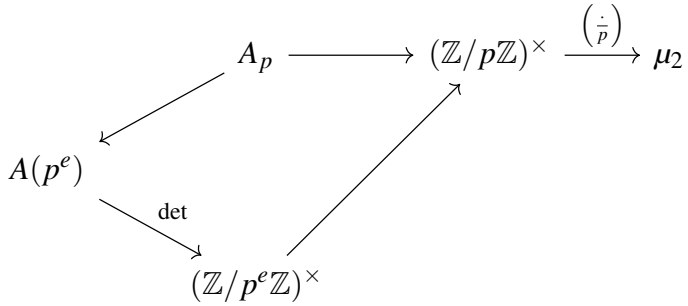
$$\begin{aligned}&\prod_p \int_{A_p} \tilde{g}_p d\nu_{A_p} \\ &= \prod_{p \nmid f} \left(1 + \sum_{k \geq 1} \frac{g(p^k)}{\#A(p^k)}\right) \prod_{p \mid \gcd(f, \ell-1)} \left(\sum_{k=0}^{\min(t,e)} \frac{g(p^k)\phi(p^k)}{\phi(p^e)\#A(p^k)} + r \sum_{k>e} \frac{g(p^k)}{\#A(p^k)}\right) \prod_{\substack{p \mid f \\ p \nmid \ell-1}} \frac{1}{\phi(p^e)},\end{aligned} \tag{5.17}$$

where $r = 1$ if $e \leq t$ and $r = 0$ otherwise.

Next, we need to study the correction factor

$$1 + \prod_p \frac{\int_{A_p} \tilde{g}_p \chi_p d\nu_{A_p}}{\int_{A_p} \tilde{g}_p d\nu_{A_p}}.$$

Recall that D is the discriminant of K. If $p \nmid 2D$, then by Theorem 3.5.(iii), χ_p is trivial, and $\frac{\int_{A_p} \tilde{g}_p \chi_p d\nu_{A_p}}{\int_{A_p} \tilde{g}_p d\nu_{A_p}}$ becomes one. Hence, we need to find $\int_{A_p} \tilde{g}_p \chi_p d\nu_{A_p}$ for each prime $p \mid 2D$. We note that if $\varphi_{p^k}^{-1}(H(p^k))$ is empty, then $1_{\varphi_{p^k}^{-1}(H(p^k))} \chi_p = 0$. Moreover, elements of $\varphi_{p^k}^{-1}(H(p^k))$ map to $\ell \bmod f$ via $A_p \to (\mathbb{Z}_p/f\mathbb{Z}_p)^\times \cong (\mathbb{Z}/p^e\mathbb{Z})^\times$. Thus, for odd p, χ_p is the constant map $\left(\frac{\ell}{p}\right)$ on $\varphi_{p^k}^{-1}(H(p^k))$ since the diagram



(5.18)

commutes for odd prime p.

Let $p \mid 2D$. We consider cases.

Case (1): If $p \nmid f$, then $(\mathbb{Z}_p/f\mathbb{Z}_p)^\times \cong \{1\}$ is trivial. Hence, similar to Corollary 3.6, we

have

$$\int_{A_p} \tilde{g}_p \chi_p d\nu_{A_p} = \sum_{k \geq c} \frac{g(p^k)}{\#A(p^k)}, \tag{5.19}$$

where $c = 1$ if p is odd and for prime 2, we have $c = 1$ if D is odd, $c = 2$ if $4 \parallel D$, and $c = 3$ if $8 \parallel D$.

Case (2): If $p \mid f$ and $p \nmid \ell - 1$, then p is odd since f and ℓ are coprime. Hence, by (5.14) and (5.18), we have

$$\begin{aligned} \int_{A_p} \tilde{g}_p \chi_p d\nu_{A_p} &= \int_{A_p} \left(\sum_{k \geq 0} g(p^k) 1_{\varphi_{p^k}^{-1}(H(p^k))} \right) \chi_p d\nu_{A_p} \\ &= \int_{A_p} 1_{\varphi_1^{-1}(H(1))} \chi_p d\nu_{A_p} \\ &= \left(\frac{\ell}{p} \right) \frac{1}{\phi(p^e)}. \end{aligned} \tag{5.20}$$

Case (3): If p is odd, $p^e \parallel f$, and $p^t \parallel \ell - 1$, then by (5.15), (5.16), and (5.18), we have

$$\int_{A_p} \tilde{g}_p \chi_p = \left(\frac{\ell}{p} \right) \left(\sum_{k \geq 0}^{\min(t,e)} \frac{g(p^k)\phi(p^k)}{\phi(p^e)\#A(p^k)} + r \sum_{k \geq e} \frac{g(p^k)}{\#A(p^k)} \right), \tag{5.21}$$

where $r = 1$ if $e \leq t$ and $r = 0$ otherwise.

Case (4): Let $2^e \parallel f$ and $2^t \parallel \ell - 1$. If D is odd then $\chi_2 = \psi_2$ and for any $k \geq 1$ the diagram

$$\begin{array}{ccc} A_2 & \xrightarrow{\chi_2 = \psi_2} & A(2) \cong \mu_2 \\ \downarrow & \nearrow & \\ A(2^k) & & \end{array}$$

commutes. Hence, χ_2 is trivial on $1_{\varphi_{2^k}^{-1}(H(2^k))}$ for $k \geq 1$. For $k = 0$, we have $\varphi_1 : A_2 \to \{1\} \times (\mathbb{Z}/2^e\mathbb{Z})^\times$. If $e = 1$, then $\varphi_1^{-1}(H(1)) = A_2$. Hence, χ_2 is non-trivial on $\varphi_{2^0}^{-1}(H(2^0))$.

If $e \geq 2$, then the diagram

$$\begin{array}{ccc} A_2 & \xrightarrow{\det} & (\mathbb{Z}_2)^\times \\ \downarrow & & \downarrow \\ A(2^e) & \longrightarrow & (\mathbb{Z}_2/f\mathbb{Z}_2)^\times \cong (\mathbb{Z}/2^e\mathbb{Z})^\times \\ \downarrow & & \\ A(2) \cong \mu_2 & & \end{array}$$

commutes. Note that both $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \overline{\ell} \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 1 & \overline{\ell} \end{smallmatrix}\right)$ map to $\overline{\ell}$. Thus, χ_2 is non-trivial on $\varphi_{2^0}^{-1}(H(2^0))$. Hence, in Case (4), if D is odd, by (5.15) and (5.16), we have

$$\begin{aligned} \int_{A_2} \tilde{g}_2 \chi_2 d\nu_{A_2} &= \sum_{k\geq 1} g(2^k) \nu_{A_2}(\varphi_{2^k}^{-1}(H(2^k))) \\ &= \sum_{k=1}^{\min(e,t)} \frac{g(2^k)\phi(2^k)}{\phi(2^e)\#A(2^k)} + r \sum_{k>e} \frac{g(2^k)}{\#A(2^k)}, \end{aligned} \tag{5.22}$$

where $r = 1$ if $e \leq t$ and $r = 0$ otherwise.

If $4 \parallel D$ and $e \geq 2$, then $\chi_2 = \psi_2 \cdot \chi_{D,2}$, where $\chi_{D,2}$ is the non-trivial character mod 8 of conductor 4. Thus, similar to the previous case, χ_2 is non-trivial on $\varphi_{2^0}^{-1}(H(2^0))$. Moreover, for $k \geq 1$, similar to (5.18), we have the commutative diagram:

$$\begin{array}{ccccc} & & A_2 & \longrightarrow & (\mathbb{Z}/4\mathbb{Z})^\times \xrightarrow{\left(\frac{-4}{\cdot}\right)} \mu_2 \\ & \swarrow & & & \\ A(2^e) & & & \nearrow & \\ & \searrow^{\det} & & & \\ & & (\mathbb{Z}/2^e\mathbb{Z})^\times & & \end{array}$$

Hence, χ_2 is the constant map $\left(\frac{-4}{\ell}\right)$ on $\varphi_{2^k}^{-1}(H(2^k))$ for $k \geq 1$. Thus, by (5.15) and (5.16), we have

$$\int_{A_2} \tilde{g}_2 \chi_2 = \left(\frac{-4}{\ell}\right) \left(\sum_{k\geq 1}^{\min(t,e)} \frac{g(2^k)\phi(2^k)}{\phi(2^e)\#A(2^k)} + r \sum_{k\geq e} \frac{g(2^k)}{\#A(2^k)} \right), \tag{5.23}$$

where $r = 1$ if $e \leq t$ and $r = 0$ otherwise. If $e = 1$, then $(\mathbb{Z}_2/f\mathbb{Z}_2)^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times$. Hence,

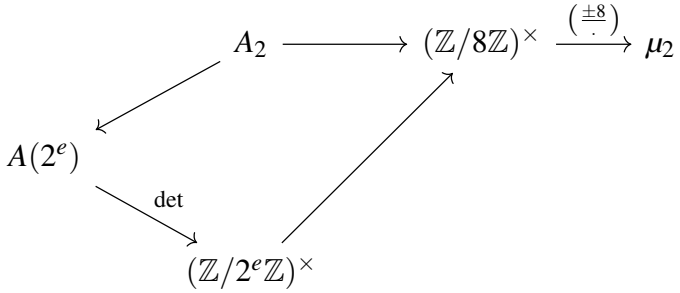
$\varphi_{2^k}^{-1}(H(2^k)) = \ker(A_2 \to A(2^k))$. Thus,

$$\begin{aligned}\int_{A_2} \tilde{g}_2\chi_2 d\nu_{A_2} &= \int_{A_2} \left(\sum_{k\geq 0} g(2^k) 1_{\varphi_{2^k}^{-1}(H(2^k))}\right)\chi_2 d\nu_{A_2} \\ &= \int_{A_2} \left(\sum_{k\geq 0} g(2^k) 1_{\ker(A_2\to A(2^k))}\right)\chi_2 d\nu_{A_2}.\end{aligned}$$

Therefore, by the proof of Corollary 3.6, similar to Case (1), we have

$$\int_{A_2} \tilde{g}_2\chi_2 d\nu_{A_2} = \sum_{k\geq 2} \frac{g(2^k)}{\#A(2^k)}. \tag{5.24}$$

If $8 \parallel D$ and $e \geq 3$, then similar to (5.18), we have the commutative diagram:



Hence, χ_2 is the constant map $\left(\frac{\pm 8}{\ell}\right)$ on $\varphi_{2^k}^{-1}(H(2^k))$ for $k \geq 1$. Moreover, for $k = 0$, χ_2 is non-trivial on $\varphi_{2^0}^{-1}(H(2^0))$. Thus, by (5.15) and (5.16), we have

$$\int_{A_2} \tilde{g}_2\chi_2 = \left(\frac{\pm 8}{\ell}\right)\left(\sum_{k\geq 1}^{\min(t,e)} \frac{g(2^k)\phi(2^k)}{\phi(2^e)\#A(2^k)} + r\sum_{k\geq e} \frac{g(2^k)}{\#A(2^k)}\right), \tag{5.25}$$

where $r = 1$ if $e \leq t$ and $r = 0$ otherwise. If $e = 1$, similar to the case $4 \parallel D$ and $e = 1$, we have

$$\int_{A_2} \tilde{g}_2\chi_2 d\nu_{A_2} = \sum_{k\geq 3} \frac{g(2^k)}{\#A(2^k)}. \tag{5.26}$$

Finally, if $e = 2$, we will show that χ_2 is non-trivial on $\varphi_{2^k}^{-1}(H(2^k))$ for $k = 0, 1, 2$, and it is trivial on $\varphi_{2^k}^{-1}(H(2^k))$ otherwise. Let $k = 0$. If $\ell \equiv 1 \pmod 4$, then both $\left(\begin{smallmatrix} 1 & 0 \\ b & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ b & 5 \end{smallmatrix}\right)$ in $A(8)$ map to $\overline{\ell}$ which shows χ_2 is non-trivial. Similarly, if $\ell \equiv 3 \pmod 4$, then both

$\left(\begin{smallmatrix}1 & 0\\ b & 3\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 0\\ b & 7\end{smallmatrix}\right)$ in $A(8)$ map to $\overline{\ell}$ which shows χ_2 is non-trivial. Thus, χ_2 is non-trivial on $\varphi_{2^0}^{-1}(H(2^0))$. For $k=1$, the same matrices as above with $b=0$ show that χ_2 is non-trivial on $\varphi_2^{-1}(H(2))$. For $k=2$, the same matrices as above with $b=0$ show that χ_2 is non-trivial on $\varphi_4^{-1}(H(4))$ if $\overline{\ell}=1$. Since $A_2 \to (\mathbb{Z}/4\mathbb{Z})^\times$ factors via $A(4)$, if $\overline{\ell}\neq 1$, then $\varphi_4^{-1}(H(4))$ becomes empty.

For $k\geq 3$, if $t=1$, then $\varphi_{2^k}^{-1}(H(2^k))$ is empty. Since if $\alpha \in \varphi_{2^k}^{-1}(H(2^k))$, then by the commutative diagram

$$\begin{array}{ccc} & A_2 & \\ \swarrow & & \searrow \\ A(2^k) & \longrightarrow & (\mathbb{Z}/4\mathbb{Z})^\times \end{array}$$

α maps to 1 (mod 4) which is a contradiction with $t=1$. Otherwise the identity condition on $A(2^k)$ implies the condition on $\overline{\ell}$ in $(\mathbb{Z}/4\mathbb{Z})^\times$. Thus, χ_2 is trivial on $\Phi_{2^k}^{-1}(H(2^k)) = \ker(A_2 \to A(2^k))$. Therefore, in the case that $8 \parallel D$ and $e=2$, if $t>1$, then

$$\int_{A_2} \tilde{g}_2 \chi_2 d\nu_{A_2} = \sum_{k\geq 3} \frac{g(2^k)}{\#A(2^k)}, \tag{5.27}$$

and $\int_{A_2} \tilde{g}_2\chi_2 d\nu_{A_2} = 0$ otherwise.

We now summarize the above observations. For $p \mid f$, letting e to be the largest exponent of p dividing f and for $p \mid \gcd(f, \ell-1)$, letting t to be the largest exponent of p dividing $\ell-1$, we get, by (5.19), (5.20), (5.21), (5.22), (5.23), (5.24), (5.25), (5.26), and (5.27),

$$\prod_{p\mid 2D} \int_{A_p} \tilde{g}_p \chi_p = \prod_{\substack{p\mid 2D \\ p\nmid f}} \left(\sum_{k\geq 1} \frac{g(p^k)}{\#A(p^k)} \right) \prod_{\substack{p\mid 2D \\ p\mid f,\, p\nmid \ell-1}} \left(\left(\frac{\ell}{p}\right) \frac{1}{\phi(p^e)} \right) \prod_{\substack{p\mid 2D \\ p\mid \gcd(f,\ell-1)}} C_p, \tag{5.28}$$

where for odd primes p, we have

$$C_p = \left(\frac{\ell}{p}\right) \left(\sum_{k=0}^{\min(t,e)} \frac{g(p^k)\phi(p^k)}{\phi(p^e)\#A(p^k)} + r \sum_{k>e} \frac{g(p^k)}{\#A(p^k)} \right),$$

where $r=1$ if $e\leq t$ and $r=0$ otherwise. For prime 2, we have the following cases by

applications of Case (4):

Case (i): If D is odd, then

$$C_2 = \sum_{k=1}^{\min(t,e)} \frac{g(2^k)\phi(2^k)}{\phi(2^e)\#A(2^k)} + r\sum_{k>e} \frac{g(2^k)}{\#A(2^k)},$$

where $r = 1$ if $e \leq t$ and $r = 0$ otherwise.

Case (ii): If $4 \parallel D$ and $e \geq 2$, then

$$C_2 = \left(\frac{-4}{\ell}\right)\left(\sum_{k=1}^{\min(t,e)} \frac{g(2^k)\phi(2^k)}{\phi(2^e)\#A(p^k)} + r\sum_{k>e} \frac{g(2^k)}{\#A(2^k)}\right),$$

where $r = 1$ if $e \leq t$ and $r = 0$ otherwise.

Case (iii): If $4 \parallel D$ and $e = 1$, then

$$C_2 = \sum_{k\geq 2} \frac{g(2^k)}{\#A(2^k)}.$$

Case (iv): If $8 \parallel D$ and $e \geq 3$, then

$$C_2 = \left(\frac{\pm 8}{\ell}\right)\left(\sum_{k=1}^{\min(t,e)} \frac{g(2^k)\phi(2^k)}{\phi(2^e)\#A(p^k)} + r\sum_{k>e} \frac{g(2^k)}{\#A(2^k)}\right),$$

where $r = 1$ if $e \leq t$ and $r = 0$ otherwise.

Case (v): If $8 \parallel D$ and $e = 1$, then

$$C_2 = \sum_{k\geq 3} \frac{g(2^k)}{\#A(2^k)}.$$

Case (vi): If $8 \parallel D$, $e = 2$, and $t > 1$, then

$$C_2 = \sum_{k\geq 3} \frac{g(2^k)}{\#A(2^k)}.$$

Case (vii): If $8 \parallel D$, $e = 2$, and $t = 1$, then

$$C_2 = 0.$$

We summarize the above results in the following theorem.

Theorem 5.3. *Under the notations and assumptions of this section we have*

$$\sum_{n\geq 1} \frac{g(n)\cdot c_\ell(n)}{[K_n(\zeta_f):\mathbb{Q}]} = A\cdot(1+E),$$

where

$$A = \prod_{p\nmid f}\left(1+\sum_{k\geq 1}\frac{g(p^k)}{\#A(p^k)}\right)\prod_{p\mid \gcd(f,\ell-1)}\left(\sum_{k=0}^{\min(t,e)}\frac{g(p^k)}{\phi(p^e)p^k}+r\sum_{k>e}\frac{g(p^k)}{\#A(p^k)}\right)\prod_{\substack{p\mid f\\ p\nmid \ell-1}}\frac{1}{\phi(p^e)}$$

with $r = 1$ if $e \leq t$ and $r = 0$ otherwise, and

$$E = \prod_{\substack{p\mid 2D\\ p\nmid f}}\left(\frac{\sum_{k\geq 1} g(p^k)/\#A(p^k)}{1+\sum_{k\geq 1} g(p^k)/\#A(p^k)}\right)\prod_{\substack{p\mid 2D\\ p\mid f}} E_p,$$

where

$$E_p = \left(\frac{\ell}{p}\right)$$

if p is odd, and for E_2 we have the following cases:

Case (i): If D is odd, then

$$E_2 = \frac{\sum_{k=1}^{\min(t,e)}\frac{g(2^k)}{\phi(2^e)2^k}+r\sum_{k>e}\frac{g(2^k)}{\#A(2^k)}}{\sum_{k=0}^{\min(t,e)}\frac{g(2^k)}{\phi(2^e)2^k}+r\sum_{k>e}\frac{g(2^k)}{\#A(2^k)}},$$

where $r = 1$ if $e \leq t$ and $r = 0$ otherwise.

Case (ii): If $4 \parallel D$ *and* $e \geq 2$*, then*

$$E_2 = \left(\frac{-4}{\ell}\right)\left(\frac{\sum_{k=1}^{\min(t,e)} \frac{g(2^k)}{\phi(2^e)2^k} + r\sum_{k>e} \frac{g(2^k)}{\#A(2^k)}}{\sum_{k=0}^{\min(t,e)} \frac{g(2^k)}{\phi(2^e)2^k} + r\sum_{k>e} \frac{g(2^k)}{\#A(2^k)}}\right),$$

where $r = 1$ *if* $e \leq t$ *and* $r = 0$ *otherwise.*

Case (iii): If $4 \parallel D$ *and* $e = 1$*, then*

$$E_2 = \frac{\sum_{k\geq 2} \frac{g(2^k)}{\#A(p^k)}}{\sum_{k=0}^{\min(t,e)} \frac{g(2^k)}{\phi(2^e)2^k} + r\sum_{k>e} \frac{g(2^k)}{\#A(2^k)}},$$

where $r = 1$ *if* $e \leq t$ *and* $r = 0$ *otherwise.*

Case (iv): If $8 \parallel D$ *and* $e \geq 3$*, then*

$$E_2 = \left(\frac{\pm 8}{\ell}\right)\left(\frac{\sum_{k=1}^{\min(t,e)} \frac{g(2^k)}{\phi(2^e)2^k} + r\sum_{k>e} \frac{g(2^k)}{\#A(2^k)}}{\sum_{k=0}^{\min(t,e)} \frac{g(2^k)}{\phi(2^e)2^k} + r\sum_{k>e} \frac{g(2^k)}{\#A(2^k)}}\right),$$

where $r = 1$ *if* $e \leq t$ *and* $r = 0$ *otherwise.*

Case (v): If $8 \parallel D$ *and* $e = 1$*, then*

$$E_2 = \frac{\sum_{k\geq 3} \frac{g(2^k)}{\#A(p^k)}}{\sum_{k=0}^{\min(t,e)} \frac{g(2^k)}{\phi(2^e)2^k} + r\sum_{k>e} \frac{g(2^k)}{\#A(2^k)}},$$

where $r = 1$ *if* $e \leq t$ *and* $r = 0$ *otherwise.*

Case (vi): If $8 \parallel D$*,* $e = 2$*, and* $t > 1$*, then*

$$E_2 = \frac{\sum_{k\geq 3} \frac{g(2^k)}{\#A(p^k)}}{\sum_{k=0}^{\min(t,e)} \frac{g(2^k)}{\phi(2^e)2^k} + r\sum_{k>e} \frac{g(2^k)}{\#A(2^k)}},$$

where $r = 1$ *if* $e \leq t$ *and* $r = 0$ *otherwise.*

Case (vii): If $8 \parallel D$, $e = 2$, *and* $t = 1$, *then*

$$E_2 = 0.$$

Proof. By (5.9), (5.12), (5.17) and (5.28), the desired result holds. □

Recall the arithmetic function $\tau_{\mathcal{F}}(p)$ associated to a family $\mathcal{F}$ of Galois extensions of $\mathbb{Q}$ as defined at the beginning of Section 4.1.2. Following the method of Hooley and its extension by Felix and Murty to the Titchmarsh Divisor Problem for Kummer fields, we expect to establish for Kummer family $\mathcal{F}$, under the assumption of GRH, that

$$\sum_{\substack{p \le x \\ p \equiv \ell \pmod{f}}} \tau_{\mathcal{F}}(p) \sim \left(\sum_{n=1}^{\infty} \frac{c_\ell(n)}{[K_n(\zeta_f) : \mathbb{Q}]} \right) \mathrm{li}(x),$$

as $x \to \infty$, where $c_\ell(n)$ is defined in (5.6). The following corollary of Theorem 5.3 provides a product expression for this expected density.

Corollary 5.4. *Assume the notations of Theorem 5.3. Recall that* $r = 1$ *if* $e \le t$ *and* $r = 0$, *otherwise. We have*

$$\sum_{n \ge 1} \frac{c_\ell(n)}{[K_n(\zeta_f) : \mathbb{Q}]} = A \cdot (1 + E),$$

where

$$A = \prod_{p \nmid f} \left(1 + \sum_{k \ge 1} \frac{1}{\#A(p^k)} \right) \prod_{p \mid \gcd(f, \ell - 1)} \left(\sum_{k=0}^{\min(t,e)} \frac{1}{\phi(p^e) p^k} + r \sum_{k > e} \frac{1}{\#A(p^k)} \right) \prod_{\substack{p \mid f \\ p \nmid \ell - 1}} \frac{1}{\phi(p^e)}$$

and

$$E = \prod_{\substack{p \mid 2D \\ p \nmid f}} \left(\frac{\sum_{k \ge 1} 1/\#A(p^k)}{1 + \sum_{k \ge 1} 1/\#A(p^k)} \right) \prod_{\substack{p \mid 2D \\ p \mid f}} E_p,$$

where

$$E_p = \left(\frac{\ell}{p} \right)$$

if p is odd, and E_2 is the same as the value of E_2 in Theorem 5.3 for $g(n) = 1$.

Chapter 6

Future Works

In this chapter, we outline a few directions for future research in topics related to this thesis.

In Chapter 4, for the Kummer fields, we fixed an integer a for which $|a|$ was not a perfect power. We can eliminate this restriction on a by considering the profinite group A introduced in [15, Section 2]. In order to extend our results to all integers a ($\neq 0, \pm 1$), we need to deal with the case that $-a$ is a perfect square. Following [15], we name this case as the *twisted case*. In the twisted case, the quadratic field K associated to the character χ is not a subset of K_2. We can modify our Theorem 3.5 by considering the condition $K \subset K_{2^m}$ for an integer $m \geq 1$ instead of $K \subset K_2$. We are optimistic that with such modification, we will be able to extend our results of Section 4.1 to integers a ($\neq 0, \pm 1$).

In Chapter 5, we computed the product expression of the Titchmarsh Divisor Problem for primes in an arithmetic progression for the Kummer family. For family of division fields attached to a Serre curve the product expression of the cyclicity problem for primes in an arithmetic progression is computed in [3, Proposition 2.6.3]. To obtain an analog of Theorem 5.3 for Serre curves we need to know which roots of unity are in each division field $\mathbb{Q}(E[n])$.

Finally, we can also consider Artin type problems related to near primitive roots, higher rank primitive roots, simultaneous cyclicity of several Serre curves, etc. We can investigate the possibility of applications of our general theorems in finding product expressions of asymptotic constants in such problems.

Bibliography

[1] Amir Akbary and Dragos Ghioca. A geometric variant of Titchmarsh divisor problem. *Int. J. Number Theory*, 8(1):53–69, 2012.

[2] Renee Bell, Clifford Blakestad, Alina Carmen Cojocaru, Alexander Cowan, Nathan Jones, Vlad Matei, Geoffrey Smith, and Isabel Vogt. Constants in Titchmarsh divisor problems for elliptic curves. *Res. Number Theory*, 6(1):Paper No. 1, 24, 2020.

[3] Julio Brau Avila. *Galois representations of elliptic curves and abelian entanglements*. PhD thesis, Leiden University, 2015.

[4] Donald L. Cohn. *Measure theory*. Birkhäuser Advanced Texts: Basler Lehrbücher. [Birkhäuser Advanced Texts: Basel Textbooks]. Birkhäuser/Springer, New York, second edition, 2013.

[5] Alina Carmen Cojocaru and M. Ram Murty. Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem. *Math. Ann.*, 330(3):601–625, 2004.

[6] David A. Cox. *Primes of the form x^2+ny^2*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[7] Harold Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[8] Adam Tyler Felix and M. Ram Murty. A problem of Fomenko's related to Artin's conjecture. *Int. J. Number Theory*, 8(7):1687–1723, 2012.

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

[10] Christopher Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.

[11] Nathan Jones. Almost all elliptic curves are Serre curves. *Trans. Amer. Math. Soc.*, 362(3):1547–1570, 2010.

[12] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[13] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[14] H. W. Lenstra, Jr. On Artin's conjecture and Euclid's algorithm in global fields. *Invent. Math.*, 42:201–224, 1977.

[15] H. W. Lenstra, Jr., P. Stevenhagen, and P. Moree. Character sums for primitive root densities. *Math. Proc. Cambridge Philos. Soc.*, 157(3):489–511, 2014.

[16] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[17] Luis Ribes and Pavel Zalesskii. *Profinite groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 2010.

[18] Joseph J. Rotman. *An introduction to homological algebra*. Universitext. Springer, New York, second edition, 2009.

[19] H. L. Royden. *Real analysis*. Macmillan Publishing Company, New York, third edition, 1988.

[20] A. Schinzel. Abelian binomials, power residues and exponential congruences. *Acta Arith.*, 32(3):245–274, 1977.

[21] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[22] Jean-Pierre Serre. Résumé des cours de lánnée scolaire 1977-1978. *Annuaire du Collège de France*, 1978, 67–70, in Collected Papers, volume III, Springer-Verlag, 1985.

[23] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[24] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[25] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer, Cham, second edition, 2015.

[26] Peter Stevenhagen. The correction factor in Artin's primitive root conjecture. volume 15, pages 383–391. 2003. Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[27] David Zywina. Possible indices for the Galois image of elliptic curves over $\mathbb{Q}$. Preprint, 1–24, arXiv:1508.07663, 2015.