C. M. Barendrecht

Primitive roots in number fields

Bachelor thesis

August 2, 2018

Thesis supervisor: prof.dr. P. Stevenhagen

Universiteit Leiden
Mathematisch Instituut

Contents

1 The rational Artin conjecture **4**
1.1 Conditions 4
1.2 The splitting of prime ideals 5
1.3 The problem reformulated 7
1.4 The density of primitive roots in $\mathbb{Q}$ 8

2 The Artin conjecture for number fields **10**
2.1 Formulating the conjecture for number fields 10
2.2 The Frobenius element 12
2.3 Applications of the Frobenius element 14

3 The density of primitive roots in number fields **18**
3.1 The main theorem 18
3.2 Proof of the main theorem 20
3.3 Applications of the main theorem 23

References **24**

Introduction

Let $a \in \mathbb{Z}\backslash\{0\}$ be a non-zero integer, and let $p \nmid a$ be a prime number. Since a is coprime to p, its residue modulo p is a unit in the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The unit group $\mathbb{F}_p^*$ is a cyclic group of order $p-1$. Naturally, the question rises, when the residue of a is a generator of $\mathbb{F}_p^*$. If it is, a is said to be a *primitive root modulo p*.

Example. It is a commonly known fact that a real number $x \in \mathbb{R}$ is a rational number if and only if its decimal expansion is ultimately periodic; given the decimal expansion $x = \sum_{n=-d}^{\infty} a_n \cdot 10^{-n}$ of x, there exist integers $k, n_0 \in \mathbb{Z}_{\geq 0}$ such that $a_n = a_{n+k}$ for all $n > n_0$. If $p \neq 2, 5$ is a prime number, there exist minimal $k, m \in \mathbb{Z}_{>0}$ such that $\frac{1}{p} = \sum_{i=1}^{\infty} m \cdot 10^{-ki}$. Here, k denotes the period of the decimal expansion of $\frac{1}{p}$. This series is a geometric series, hence, $\frac{1}{p} = \frac{m}{10^k - 1}$. It follows that k is the minimal integer for which $10^k = 1 \mod p$, which is precisely the order of 10 in the unit group $\mathbb{F}_p^*$. Thus, 10 is a primitive root modulo p if and only if the period of the decimal expansion of $\frac{1}{p}$ has length $p-1$.

In 1927, Emil Artin conjectured that the collection of prime numbers p for which a given integer a is a primitive root modulo p, denoted by $P(a)$, possesses a density in the collection of prime numbers. This natural density of $P(a)$ is given by

$$\delta_a = \lim_{n \to \infty} \frac{\#\{p \in P(a) \mid p \leq n\}}{\#\{p \text{ prime } \mid p \leq n\}}.$$

Artin discovered that a being a primitive root modulo p, is determined by the splitting behaviour of the prime ideal $(p) \subset \mathbb{Z}$ in the splitting field $F_l = \Omega_{\mathbb{Q}}^{X^l - a} = \mathbb{Q}(\zeta_l, \sqrt[l]{a})$, where l is a prime number dividing $p-1$. He conjectured the following [7]:

Artin conjecture. *Let $a \in \mathbb{Z}\backslash\{0\}$ be a non-zero integer, not equal to ± 1, that is not a perfect power. Then there are infinitely many prime numbers p for which a is primitive root modulo p. Moreover, the collection of these primes $P(a)$ posessess a density inside the collection of all prime numbers. This density is independent of a and is given by*

$$\delta_a = \prod_{l \ prime} \left(1 - \frac{1}{l(l-1)}\right) \approx 0.37396.$$

It is important to note that the number $l(l-1)$ is in fact the degree of the field extension $F_l/\mathbb{Q}$. Moreover, if we replace the condition that a is an integer with the condition that a is a rational number, we obtain the following generalization: Let $a \in \mathbb{Q}^*$ be a rational number, not equal to ± 1, then $P(a)$ possesses a natural density δ_a in the collection of prime numbers, given by:

$$\delta_a = \prod_{l \text{ prime}} \left(1 - \frac{1}{[F_l : \mathbb{Q}]}\right). \tag{1}$$

In 1957, numerical calculations made by Derrick and Emma Lehmer gave unexpected results [7]. They sent their results to Artin, who explained why the density δ_5, should be approximately 5% higher than the conjectural value of 0.37396. In 1967, Christopher Hooley proved a restated theorem, under assumption of the Generalized Riemann Hypothesis [2].

In 1977, Hendrik W. Lenstra proved several generalizations of the conjecture, also under assumption of the Generalized Riemann Hypothesis [3]. One of these generalizations is given by

replacing the field $\mathbb{Q}$ with an arbitrary number field K. This thesis is dedicated to proving this generalization with minimal prior knowledge of algebraic number theory. Also an explicit formula will be given for the corresponding density δ_a, which relates this density to the density of primes which split completely in a given finite field extension F_n/K, where $F_n = K(\zeta_n, \sqrt[n]{a})$.

1 The rational Artin conjecture

Before the Artin conjecture be formulated in arbitrary number fields, we will first consider the field $K = \mathbb{Q}$, and a non-zero rational number $a \in \mathbb{Q}^*$. In this chapter, the concept of ideal factorisation and the splitting of prime ideals in number fields will be introduced. Moreover, an equivalence will be proved between the property of a being a primitive root modulo a prime p and the splitting behaviour of the ideal (p) in the fields $F_l = \mathbb{Q}(\zeta_l, \sqrt[l]{a})$, where $l \mid p-1$ is a prime number. Finally, several results with respect to the density δ_a will be stated.

1.1 Conditions

Let $a \in \mathbb{Q}^*$ be a non-zero rational number. The rational numbers allow unique prime factorisation. Hence, a can be written uniquely as $a = \frac{b}{c}$, where b and c are two coprime integers, with $c > 0$. Let p be a prime number such that $\mathrm{ord}_p(b) = \mathrm{ord}_p(c) = 0$. The residues of b and c modulo p are units in $\mathbb{F}_p$, since p is coprime to b and c. The residue of a modulo p is therefore defined as $\bar{c}^{-1}\bar{b}$ and is a unit in $\mathbb{F}_p$ as well. The residue of a modulo p is denoted by a, and the order of p in a is defined as $\mathrm{ord}_p(a) = \mathrm{ord}_p(b) - \mathrm{ord}_p(c)$. We wish to classify the conditions for which a is a primitive root modulo p. The condition that a generates $\mathbb{F}_p^*$ is equivalent to the condition that the group $\langle a \rangle$ has index 1 in $\mathbb{F}_p^*$:

$$\langle a \rangle = \mathbb{F}_p^* \Leftrightarrow [\mathbb{F}_p^* : \langle a \rangle] = 1$$

Hence, a is *not* a primitive root modulo p if and only if there exists a prime number l such that $l \mid [\mathbb{F}_p^* : \langle a \rangle]$. The index of a subgroup of a finite group is always a divisor of the group order. For any odd prime number p, the group order of $\mathbb{F}_p^*$ is divisible by 2. This observation allows us to impose several restrictions on a. This is illustrated in the following example.

Example 1.1. Let $a \in \mathbb{Q}^*$ be a perfect square, and let p be a prime number with $\mathrm{ord}_p(a) = 0$. Then a is a primitive root modulo p, if and only if $p = 2$. Let $p \neq 2$ be an odd prime number. Since $\mathbb{F}_p^*$ is a cyclic group of finite order $p-1$, the collection of squares, $\mathbb{F}_p^{*2}$, is a subgroup of index 2. It follows from the multiplicativity of the index that $2 \mid [\mathbb{F}_p^* : \langle a \rangle]$, and hence a is not a primitive root modulo p. The other implication is trivial.
Furthermore, the integer -1 is an element of order 2 in $\mathbb{Q}^*$. Hence, if $p \neq 2$ is an odd prime number, then the equality $\langle -1 \rangle = \{1, -1\}$ holds. It follows that -1 is a primitive root modulo p if and only if $p \in \{2, 3\}$.

Example 1.1 is in fact a direct result from the following lemma, which relates the divisibility of the index $[\mathbb{F}_p^* : \langle a \rangle]$ to the splitting behaviour of certain polynomials in $\mathbb{F}_p[X]$:

Lemma 1.2. *Let $a \in \mathbb{Q}^*$ be a rational number and $p, l \in \mathbb{Z}$ be two distinct prime numbers, such that $\mathrm{ord}_p(a) = 0$. Then the following are equivalent:*

(1) $l \mid [\mathbb{F}_p^* : \langle a \rangle]$.

(2) $l \mid \#\mathbb{F}_p^*$ and $a \equiv y^l \mod p$ for certain $y \in \mathbb{F}_p^*$.

(3) $\mathbb{F}_p^*$ contains an element of order l and $a \equiv y^l \mod p$ for certain $y \in \mathbb{F}_p^*$.

(4) The polynomial $X^l - a$ splits in l distinct factors in $\mathbb{F}_p[X]$.

Proof. The proof of the equivalence of (1) and (2) relies on the fact that the unit group $\mathbb{F}_p^*$ is a cyclic group of finite order. Since it is, all subgroups of $\mathbb{F}_p^*$ are cyclic, and for every $d \mid \#\mathbb{F}_p^*$, there exists a unique subgroup $H_d \subset \mathbb{F}_p^*$ of index d, given by $H_d = \mathbb{F}_p^{*d} = \{x^d \mid x \in \mathbb{F}_p^*\}$. Moreover, for every $m \mid \#\mathbb{F}_p^*$ and $d \mid m$, there is a natural inclusion $H_m \subset H_d \subset \mathbb{F}_p^*$. Hence if $l \mid [\mathbb{F}_p^* : \langle a \rangle]$ we naturally have that $l \mid \mathbb{F}_p^*$, and by the above we have that the group $\langle a \rangle$ is contained in the subgroup H_l of index l. Thus there exists an $y \in \mathbb{F}_p^*$ such that $a \equiv y^l \mod p$. To proof the converse we note that since $l \mid F_p^*$, and $a \equiv y^l \mod p$ for certain $y \in \mathbb{F}_p^*$, the inclusion $\langle a \rangle \subset \mathbb{F}_p^{*l}$ holds. This inclusion now gives us that $l \mid [\mathbb{F}_p^* : \langle a \rangle]$. This proves the equivalence of (1) and (2).

The theorem of Cauchy states that for every prime number $l \mid \#\mathbb{F}_p^*$ there exists an element $\zeta \in \mathbb{F}_p^*$ of order l. Moreover, the order of every element in a finite group is a divisor of the group order. This proves the equivalence of (2) and (3).

(3) $\Rightarrow$ (4): Since $\mathbb{F}_p$ is a field, the polynomial $X^l - a$ has at most l distinct roots in $\mathbb{F}_p$. Since $\mathbb{F}_p^*$ contains an element ζ of order l, the polynomial $X^l - a$ splits into l distinct linear factors as $X^l - a = \prod_{k=1}^{l}(X - \zeta^k y)$ in $\mathbb{F}_p[X]$. To show that these factors are distinct, it suffices to show that $X^l - a$ has no common roots with its derivative. Since $\frac{d}{dX}(X^l - a) = lX^{l-1}$ has 0 as only root, we can conclude that all the roots of $X^l - a$ are distinct.

(4) $\Rightarrow$ (3): Clearly, there exists an $y \in \mathbb{F}_p^*$ such that $a \equiv y^l \mod p$. The map $\varphi : \mathbb{F}_p^* \to \mathbb{F}_p^*, x \mapsto x^l$ is a homomorphism of groups. From the first isomorphism theorem, it follows that all cosets of $\ker(\varphi)$ have the same cardinality. The polynomial $X^l - a$ splits in l distinct factors in $\mathbb{F}_p[X]$. Hence, all cosets have size l. Therefore, the kernel of φ is a subgroup of $\mathbb{F}_p^*$ of order l. This proves the final implication. □

It follows directly from Lemma 1.2 that a is a primitive root modulo p, if and only if there exists no prime number $l \mid \mathbb{F}_p^*$, for which the polynomial $f_l = X^l - a \in \mathbb{F}_p[X]$ splits completely in $\mathbb{F}_p[X]$. Condition (4) is equivalent to the condition that the splitting field $\Omega_{\mathbb{F}_p}^{X^l-a}$ of f_l has degree 1 over $\mathbb{F}_p$. The splitting field of f_l over $\mathbb{F}_p$, is strongly related to the splitting field of f_l over $\mathbb{Q}$. In order to fully comprehend this relation, several objects have to be introduced.

1.2 The splitting of prime ideals

In order to examine the splitting behaviour of $X^l - a$ in $\mathbb{F}_p[X]$ more closely, several objects have to be introduced.

Definition 1.3. Let K be a number field. The integral closure of $\mathbb{Z}$ in K is called the *ring of integers of K*. It is denoted by $\mathcal{O}_K$, and is given by

$$\mathcal{O}_K = \{\alpha \in K \mid \text{ there exists a monic polynomial } f \in \mathbb{Z}[X] \text{ such that } f(\alpha) = 0\}.$$

The ring of integers $\mathcal{O}_K$ of a number field K satisfies several useful properties. These properties are listed in the following proposition.

Proposition 1.4. *Let K be a number field of degree n over $\mathbb{Q}$. The ring of integers $\mathcal{O}_K$ of K satisfies the following properties.*

1. *The ring of integers is a Dedekind domain: Every non-zero ideal $I \subset \mathcal{O}_K$ can be decomposed uniquely as*
$$I = \prod_{I \subset \mathfrak{p}} \mathfrak{p}^{e_\mathfrak{p}},$$
where $\mathfrak{p}$ denote distinct prime ideals and $e_\mathfrak{p} \geq 1$ is an integer.

2. *K has an integral basis: There exist $\omega_1, ..., \omega_n \in \mathcal{O}_K$ such that*
$$\mathcal{O}_K = \bigoplus_{i=1}^{n} \mathbb{Z} \cdot \omega_i, \qquad K = \mathrm{Frac}(\mathcal{O}_K) = \bigoplus_{i=1}^{n} \mathbb{Q} \cdot \omega_i.$$
Every element $x \in K$ can be written as $x = \frac{\alpha}{\beta}$, with $\alpha, \beta \in \mathcal{O}_K$, and $\beta \neq 0$.

These properties are certainly not trivial. The proof of the proposition will not be given in this article however. For this we refer to [6]. The collection of non-zero prime ideals of $\mathcal{O}_K$ is denoted by $\mathcal{P}_K$. Throughout this article, a prime $\mathfrak{p}$ of K refers to an element of $\mathcal{P}_K$. A prime $\mathfrak{p}$ is said to divide an ideal I, if the inclusion $I \subset \mathfrak{p}$ holds.

Every non-zero rational number $q \in \mathbb{Q}^*$, permits a unique prime decomposition $q = \prod_{p \in \mathcal{P}_\mathbb{Q}} p^{n_p}$, with $n_p \in \mathbb{Z}$. Proposition 1.4 allows a similar decomposition in general number fields. It falls beyond the scope of this thesis to formally define this. However, for $x \in K^*$, we can define the collection of prime ideals of $\mathcal{O}_K$ that divide x. By Proposition 1.4, there exist algebraic integers $\alpha, \beta \in \mathcal{O}_K \backslash \{0\}$, such that $x = \frac{\alpha}{\beta}$. As the ideals generated by α and β allow a unique factorisation, the *divisor set* $D_K(x)$ of x in K is defined as:
$$D_K(x) = \{\mathfrak{p} \in \mathcal{P}_K : \mathrm{ord}_\mathfrak{p}(\alpha) - \mathrm{ord}_\mathfrak{p}(\beta) \neq 0\}.$$
The divisor set $D_K(x)$ of an algebraic number in a number field K is always a finite set.

Let p be a prime number. Since $\mathcal{O}_K$ is a Dedekind domain, the ideal $p\mathcal{O}_K$ can be decomposed uniquely as
$$p\mathcal{O}_K = \prod_{\mathfrak{p} | p\mathcal{O}_K} \mathfrak{p}^{e(\mathfrak{p}/p)}. \tag{2}$$
The prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ in this decomposition are called the primes *extending* p or the extensions of p in K. The index $e(\mathfrak{p}/p)$ is called the ramification index of $\mathfrak{p}$ in K. Note that $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ containing (p). Hence, $\mathfrak{p} \cap \mathbb{Z} = (p)$ and therefore this index is depends only on the prime $\mathfrak{p}$. If there exists a prime $\mathfrak{p} \in \mathcal{P}_K$ with $e(\mathfrak{p}/p) > 1$, then p is *ramified* in K. The prime numbers that ramify in K are precisely those prime numbers that divide the absolute discriminant of K. This statement is given without proof.

Lemma 1.5. *Let $K/\mathbb{Q}$ be a field extension of degree n. Let $G = \{\sigma_1, ..., \sigma_n\}$ denote the collection of embeddings of K into $\mathbb{C}$. Let $\{\omega_1, ..., \omega_n\}$ be any integral basis of K. A prime number p is ramified in K if and only if p divides the absolute discriminant Δ_K of K, given by $\Delta_K = (\det(\sigma_i(\omega_j))_{i,j})^2$. Moreover, if $f \in \mathbb{Z}[X]$ is an irreducible polynomial, and $K = \Omega^f_\mathbb{Q}$ is its splitting field over $\mathbb{Q}$, then $D_\mathbb{Q}(\Delta_K) \subset D_\mathbb{Q}(\Delta(f))$.*

Since $\Delta_K \in \mathbb{Z}\backslash\{0\}$, there are at most finitely many prime numbers l that ramify in K. Let $a \in \mathbb{Q}^*$ be a rational number, let l be a prime number, and let $p \in \mathcal{P}_\mathbb{Q}$ be a prime ideal of $\mathbb{Q}$. It follows that if p ramifies in F_l, then $p \in D_\mathbb{Q}(l) \cup D_\mathbb{Q}(a)$.

Let K be a number field of degree n over $\mathbb{Q}$, and let p be a prime number. From the Chinese remainder theorem, it follows that

$$\mathcal{O}_K \big/ p\mathcal{O}_K \cong \prod_{\mathfrak{p}|p\mathcal{O}_K} \mathcal{O}_K \big/ \mathfrak{p}^{e(\mathfrak{p}/p)}. \tag{3}$$

Since the ideals $\mathfrak{p}$ are prime ideals in a number ring, the rings $k_\mathfrak{p} = \mathcal{O}_K \big/ \mathfrak{p}$ are finite fields of characteristic p. The field $k_\mathfrak{p}$ is called the *residue class field* of $\mathfrak{p}$. The degree of the field extension $k_\mathfrak{p}/\mathbb{F}_p$ is called the *residue class degree* and is denoted by $f(\mathfrak{p}/p)$. From Proposition 1.4, it follows that

$$\mathcal{O}_{K+} \big/ p\mathcal{O}_{K+} = \bigoplus_{i=1}^{n} \mathbb{Z} \cdot \omega_i \big/ p\mathbb{Z} \cdot \omega_i \cong (\mathbb{Z}/p\mathbb{Z})^n \tag{4}$$

From equation (3) we obtaint the equality $|\mathcal{O}_K \big/ p\mathcal{O}_K| = \prod_{\mathfrak{p}|p} p^{e(\mathfrak{p}/p)f(\mathfrak{p}/p)}$. On the other hand, we have by equality (4) that $|\mathcal{O}_K \big/ p\mathcal{O}_K| = p^n$, hence we conclude that

$$p^n = \prod_{\mathfrak{p}|p}^{k} p^{e(\mathfrak{p}/p)f(\mathfrak{p}/p)} = p^{\sum_{\mathfrak{p}|p} e(\mathfrak{p}/p)f(\mathfrak{p}/p)}.$$

And therefore,

$$[K : \mathbb{Q}] = \sum_{\mathfrak{p}|p} e(\mathfrak{p}/p)f(\mathfrak{p}/p). \tag{5}$$

This gives rise to the definition of the splitting of prime ideals in number fields; let $K/\mathbb{Q}$ be a field extension of degree n with corresponding ring of integers $\mathcal{O}_K$. A prime ideal (p) is said to *split completely* in K if (p) has n distinct extensions in $\mathcal{O}_K$. Naturally, if p splits completely in $\mathcal{O}_K$, then $f(\mathfrak{p}/p) = 1$ for all primes $\mathfrak{p}$ of K extending p. Hence, $k_\mathfrak{p} = \mathbb{F}_p$ for all primes of K extending p. The prime p is said to be *totally ramified* in K, if there exists a prime $\mathfrak{p}$ of K extending p, with $e(\mathfrak{p}/p) = n$.

Example 1.6. Let l be a prime number. We will show that l is totally ramified in the extension $\mathbb{Q}(\zeta_l)/\mathbb{Q}$. It is a commonly known fact that is the ring of integers of $\mathbb{Q}(\zeta_l)$ is given by $\mathbb{Z}[\zeta_l]$. Let $\tau : \mathbb{Z}[\zeta_l] \to \overline{\mathbb{F}_l}$ be a homomorphism. τ is determined uniquely by its action on ζ_l, and since τ is a homomorphism, $\tau(\zeta_l)$ must be a root of the l-th cyclic polynomial $\Phi_l(X)$ modulo l. This polynomial splits as $\Phi_l(X) = (X-1)^{l-1}$ over $\mathbb{F}_l$, hence $\tau(\zeta_l) = 1$. Consequently, we have that $\mathrm{Im}(\tau) = \mathbb{F}_l$, and by the first isomorphism theorem $\mathfrak{p} = \ker \tau$ is a prime ideal of $\mathbb{Q}(\zeta_l)$, extending l. In particular, this is the only prime of $\mathbb{Q}(\zeta_l)$ extending l. It follows from equation (5) that $e(\mathfrak{p}/l) = l - 1$, and hence l is totally ramified in $\mathbb{Q}(\zeta_l)$. Finally, since $\Delta(\Phi_l(X)) = \pm l^{l-2}$, we note that l is the only prime that ramifies in $\mathbb{Q}(\zeta_l)$.

1.3 The problem reformulated

Lemma 1.2 shows that the property of being a primitive root modulo p is closely related to the splitting behaviour of f_l in $\mathbb{F}_p[X]$. The splitting behaviour of the polynomial f_l is closely related to the splitting behaviour of the ideal $(p) \subset \mathcal{O}_{F_l}$. This relation is formalized in the following theorem.

Theorem 1.7. *Let $a \in \mathbb{Q}^*$ be a rational number, let l be a prime number and let F_l denote the splitting field of $f_l = X^l - a \in \mathbb{Q}[X]$. Let $(p) \in \mathcal{P}_{\mathbb{Q}} \backslash (D_{\mathbb{Q}}(l) \cup D_{\mathbb{Q}}(a))$ be a prime of $\mathbb{Q}$ such that $\mathrm{ord}_p(a) = 0$, and $\mathrm{ord}_p(l) = 0$. The following are equivalent.*

(1) The polynomial f_l splits completely in $\mathbb{F}_p[X]$.

(2) The ideal (p) splits completely in $\mathcal{O}_{F_l}$.

Proof. In order to show that (p) splits completely in $\mathcal{O}_{F_l}$, we need to show that (p) has $[F_l : \mathbb{Q}]$ extensions in F_l. The polynomial f_l is irreducible in $\mathbb{Q}[X]$ if and only if it has no rational roots [5]. Hence, we assume without loss of generality, that $[F_l : \mathbb{Q}] = l(l-1)$. The ring $\mathcal{O}_{F_l}$ contains the subring $R = \mathbb{Z}[\zeta_l, \sqrt[l]{a}]$. Consider the collection $\mathcal{C}$ of surjective homomorphisms $\tau : R \to \mathbb{F}_p$. It follows from the first isomorphism theorem that $\ker(\tau)$ must be a prime ideal of R, for all $\tau \in \mathcal{C}$. Moreover, since $\mathbb{F}_p$ is a field, a homomorphism $\tau : R \to \mathbb{F}_p$ is surjective, if and only if τ is non-trivial. Hence, if $\mathcal{C}$ is non-empty, then there are exactly $l(l-1)$ homomorphisms in $\mathcal{C}$, since there are $l-1$ distinct images of ζ_l, and exactly l distinct images of $\sqrt[l]{a}$. Every $\tau \in \mathcal{C}$ corresponds to a unique prime ideal $\mathfrak{p}_\tau$ extending p. Hence, there are $l(l-1)$ prime ideals $\mathfrak{p}$ of R that extend (p). None of these prime ideals are ramified in $\mathcal{O}_{F_l}$, and since there are at most $[F_l : \mathbb{Q}] = l(l-1)$ primes of $\mathcal{O}_{F_l}$ extending p, each prime $\mathfrak{p}$ of R can be extended uniquely to a prime $\mathfrak{q}$ of $\mathcal{O}_{F_l}$. Hence, (p) splits completely in F_l if $\mathcal{C}$ is non-empty, and $\mathcal{C}$ is non-empty if and only if the polynomial f_l splits completely in $\mathbb{F}_p[X]$, by Lemma 1.2.

On the other hand, if the prime (p) splits completely in $\mathcal{O}_{F_l}$, it follows from equality (5) that $\mathcal{O}_{F_l}/p\mathcal{O}_{F_l} \cong (\mathbb{F}_p)^{l(l-1)}$. Therefore, there exists a non-trivial homomorphism $\tau : \mathcal{O}_{F_l} \to \mathbb{F}_p$, and since $\tau|_R$ is a non-trivial homomorphism from R to $\mathbb{F}_p$, it follows that $\mathcal{C} \neq \emptyset$. □

Theorem 1.7 gives the first concrete result with respect to the Artin conjecture:

Corollary 1.7.1. *Let $a \in \mathbb{Q}^*$ be a non-zero rational number, and let $p \notin D_{\mathbb{Q}}(a)$ be a prime number. Then a is a primitive root modulo p if and only if for all $l \mid p-1$, the ideal p does not split completely in F_l.*

1.4 The density of primitive roots in $\mathbb{Q}$

Corollary 1.7.1 offers an alternative proof for Example 1.1, using field extensions. Let $a \in \mathbb{Q}^*$ be a perfect square, and let p be an odd prime number coprime to a. Since a is a perfect square in $\mathbb{Q}^*$, the extension $F_2/\mathbb{Q}$ is trivial. And since p has exactly 1 extension in $\mathbb{Q}$, the ideal (p) splits completely in F_2. We conclude that a is not a primitive root modulo p, unless $p = 2$.

In fact, this alternative proof of Example 1.1, gives rise to a general statement with respect to the density δ_a of the collection $P(a)$ of primes p for which a is a primitive root modulo p, in the collection of all rational primes:

Corollary 1.7.2. *Let $a \in \mathbb{Q}^*$ be a non-zero rational number. If there exists a prime number l, for which the field extension $F_l/\mathbb{Q}$ is trivial, then $\delta_a = 0$.*

This corollary is in fact equivalent with Example 1.1, since $\zeta_1 = 1$, and $\zeta_2 = -1$ are the only roots of unity contained in $\mathbb{Z}$. In arbitrary number fields, this is less trivial however. We conclude this chapter by stating a correction of the Artin conjecture, under assumption of the Generalized Riemann Hypothesis [2].

Theorem 1.8 (C. Hooley, 1967)**.** *Let $a \in \mathbb{Z}\backslash\{\pm 1\}$ be an integer that is not a perfect square. Let h denote the largest integer for which a is a perfect h-th power. Let a_1 denote the square-free part of a. Let $C(h)$ be given by:*

$$C(h) = \prod_{\substack{l \text{ prime}, \\ l|h}} \left(1 - \frac{1}{l-1}\right) \prod_{\substack{l \text{ prime}, \\ l\nmid h}} \left(1 - \frac{1}{l(l-1)}\right).$$

Assume that the Generalized Riemann Hypothesis holds. If $a_1 \not\equiv 1 \mod 4$, then $\delta_a = C(h)$, while if $a_1 \equiv 1 \mod 4$, we have:

$$\delta_a = C(h)\left(1 - \mu(|a_1|) \cdot \prod_{\substack{l|h, \\ l|a_1}} \frac{1}{l-2} \prod_{\substack{l\nmid h, \\ l|a_1}} \frac{1}{l^2-l-1}\right),$$

where μ denotes the Möbius counting function.

A simple calculation shows that for $a = 5$, we have:

$$\delta_5 = C(1) \cdot \left(1 - 1 \cdot \frac{1}{5^2-5-1}\right) = C(1) \cdot \left(1 - \frac{1}{19}\right) = \frac{20}{19} \prod_{l \text{ prime}} \left(1 - \frac{1}{l(l-1)}\right).$$

Hence for $a = 5$, the density δ_5 is approximately 5% greater than the Artin constant, which is the numerical deviation that Derrick and Emma Lehmer estimated in 1957 [7]. Not only does Hooley's theorem give a method to explicitly calculate the density δ_a of a given integer a, it also precisely states the conditions under which the density δ_a vanishes:

Corollary 1.8.1. *Assume the Generalized Riemann Hypothesis holds. Let $a \in \mathbb{Q}^*\backslash\{\pm 1\}$ be a rational unit. The density δ_a vanishes if and only if a is a perfect square in $\mathbb{Q}^*$.*

Proof. We note that the proof of Hooley's theorem does not require a to be an integer, it still holds if a is replaced by a rational number that is not a root of unity. Assume that a is not a perfect square. Since $2 \nmid h$, it follows that $C(h) > 0$. Hence if $a \neq 1 \mod 4$, then $\delta_a > 0$. Note that the correction factor when $a \equiv 1 \mod 4$ as described in Hooley's theorem never vanishes. It follows that $\delta_a > 0$. The other implication is given by Corollary 1.7.2. □

2 The Artin conjecture for number fields

In this chapter the Artin conjecture will be formulated for arbitrary number fields K, and a non-trivial example of a number field K and algebraic number $a \in K^*$, for which the density δ_a vanishes, will be examined. Further, the Frobenius element and Frobenius symbol of unramified primes in Galois extensions will be defined. We will classify primes of K, by their respective Frobenius symbol in the fields $F_n = K(\zeta_n, \sqrt[n]{a})$. We will show that the primes $\mathfrak{p}$ of K, not contained in the divisor set of a or $2\Delta_K$, for which a is not a primitive root modulo $\mathfrak{p}$, are those primes for which there exists a prime number $l \mid \#k_\mathfrak{p}^*$, such that the Frobenius symbol in F_l is trivial. This chapter is concluded by proving a lemma regarding the vanishing of the density δ_a.

2.1 Formulating the conjecture for number fields

All proofs in chapter 1 can be generalized to arbitrary number field extensions L/K, by replacing $\mathbb{Z}$ with the ring of integers $\mathcal{O}_K$ and the prime number p with general prime ideals $\mathfrak{p} \in \mathcal{P}_K$. Since the residue class fields $k_\mathfrak{p}$ are finite fields, the collection $\mathcal{P}_K$ can be provided with the natural ordering induced by the cardinality of the residue class fields; let $A \subset \mathcal{P}_K$ be a subset of $\mathcal{P}_K$, the natural density of A in $\mathcal{P}_K$ is defined as:

$$\delta = \lim_{n\to\infty} \frac{\{\mathfrak{p} \in A \mid \#k_\mathfrak{p} \leq n\}}{\{\mathfrak{p} \in \mathcal{P}_K \mid \#k_\mathfrak{p} \leq n\}},$$

whenever this limit exists. This allows us to formalize the Artin conjecture over general number fields K.

Generalized Artin conjecture. *Let K be a number field with ring of integers $\mathcal{O}_K$. Let $a \in K^*\backslash\mu_K$ be a unit of K. Let $P(a) \subset \mathcal{P}_K\backslash D_K(a)$ denote the set of all prime ideals $\mathfrak{p} \subset \mathcal{O}_K$, for which a is a primitive root modulo $\mathfrak{p}$. Then $P(a)$ possesses a natural density δ_a in $\mathcal{P}_K$.*

Under assumption of the Generalized Riemann Hypothesis, it was shown in section 1.4 that when $K = \mathbb{Q}$, $\delta_a = 0$ if and only if $a \in \mathbb{Q}^{*2} \cup \{\pm 1\}$. In general number fields however, this need not be the case. This is illustrated in the following examples.

Example 2.1. The results from Example 1.1 can be generalized to arbitrary number fields K. Let K be a number field with ring of integers $\mathcal{O}_K$ and let $\zeta \in \mu_K$ be a primitive n-th root of unity. Let $\mathfrak{p} \in \mathcal{P}_K\backslash D_K(n)$ be a prime of K that is not contained in the divisor set of n. Note that $\mathrm{char}(k_\mathfrak{p}) \nmid n$, and since the polynomial $X^n - 1$ splits completely in $K[X]$, it splits completely in $k_\mathfrak{p}$ as well. We therefore conclude that $n \mid k_\mathfrak{p}^*$, and since ζ has order n in $k_\mathfrak{p}^*$, it will only be a primitive root modulo $\mathfrak{p}$ if $\#k_\mathfrak{p}^* = n$. This holds for only finitely many primes $\mathfrak{p}$. In general, if K contains a primitive n-th root of unity and $a \in K^{*n}$, then the polynomial $X^n - a$ splits completely in $K[X]$, and therefore splits completely over all but finitely many residue class fields $k_\mathfrak{p}$.

From Example 2.1, we conclude that if $\zeta_n \in K$, and $a \in K^{*n}$, then $\delta_a = 0$. In general the density δ_a vanishes if there exists a square-free integer n, such that the polynomial $X^n - a$ is reducible in $K[X]$. A less trivial example is given when considering the field $\mathbb{Q}(\sqrt{5})$:

Example 2.2. Consider the number field $K = \mathbb{Q}(\sqrt{5})$, with corresponding ring of integers $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. Let $x \in K^*\backslash\mu_K$, be a fixed algebraic number to be determined later, and let

$a = x^{15}$. Let $\mathfrak{p} \in \mathcal{P}_K \backslash D_K(a)$ be a prime of K that is not contained in the divisor set of a. Analogous to Lemma 1.2, it can be concluded that $3 \mid [k_\mathfrak{p}^* : \langle a \rangle] \Leftrightarrow X^3 - 1 \in k_\mathfrak{p}[X]$ splits in distinct factors, and there exists a $y \in K$ such that $a \equiv y^3 \mod \mathfrak{p}$. The second statement holds trivially since $a = x^{15}$. Hence, it suffices to show that the polynomial $X^3 - 1$ splits completely in distinct factors in $k_\mathfrak{p}[X]$. If $\text{char}(k_\mathfrak{p}) \neq 3$, this holds if and only if $X^2 + X + 1$ splits completely in $k_\mathfrak{p}[X]$ and since there are only finitely many primes extending 3, there are only finitely many primes $\mathfrak{p}$ for which $\text{char}(k_\mathfrak{p}) = 3$. Note that by the quadratic formula, the roots of this polynomial are given by $y = \frac{-1 \pm \sqrt{-3}}{2}$.
Hence, if $\text{char}(k_\mathfrak{p}) \neq 2, 3$, the following can be concluded:

$$3 \mid [k_\mathfrak{p}^* : \langle a \rangle] \text{ if and only if } -3 \text{ is a square in } k_\mathfrak{p}.$$

The same deductive strategy can be used to determine the conditions for which $5 \mid [k_\mathfrak{p}^* : \langle a \rangle]$. Assume that $\text{char}(k_\mathfrak{p}) \neq 5$. Since $a = (x^3)^5 \mod \mathfrak{p}$, it can be concluded that $5 \mid [k_\mathfrak{p}^* : \langle a \rangle]$ if and only if $X^5 - 1$ splits completely in $k_\mathfrak{p}[X]$. This is equivalent with the statement that the splitting field $\Omega_{k_\mathfrak{p}}^{X^5-1}$ has degree one over $k_\mathfrak{p}$. In order to examine this condition more closely, we note that the extension $\Omega_\mathbb{Q}^{X^5-1}/\mathbb{Q}$ is cyclic of degree 4. Therefore, $\Omega_\mathbb{Q}^{X^5-1}$ has a subfield L of degree 2 over $\mathbb{Q}$, given by $L = \mathbb{Q}(\sqrt{5}) = K$. Hence, the extension $\Omega_K^{X^5-1}/K$ has degree 2 and is given by a polynomial $f = X^2 - \tau X + c \in K[X]$. Since K is a real number field, we note that $\text{Gal}(\mathbb{Q}(\zeta_5)/K) = \{id, \sigma\}$, where σ is given by complex conjugation. It follows that $f_K^{\zeta_5}$ is given by $f = (X - \zeta_5)(X - \sigma(\zeta_5)) = X^2 - (\zeta_5 + \overline{\zeta_5})X + \zeta_5\overline{\zeta_5}$. We note that $\overline{\zeta_5} = \zeta_5^{-1}$ and thus $f_K^{\zeta_5} = X^2 - \tau X + 1$, where $\tau = \zeta_5 + \zeta_5^{-1} = \frac{-1+\sqrt{5}}{2}$.
Assume that $\text{ord}_\mathfrak{p}(\tau) = 0$. From the above it can be concluded that $X^5 - 1$ splits completely in $k_\mathfrak{p}[X]$ if and only if $X^2 - \tau X + 1$ splits completely in $k_\mathfrak{p}[X]$. By the quadratic formula, the roots of $X^2 - \tau X + 1$ are given by $y = \frac{\tau \pm \sqrt{\tau^2 - 4}}{2}$. Thus, if $\text{char}(k_\mathfrak{p}) \neq 2, 5$ and $\text{ord}_\mathfrak{p}(\tau) = 0$, the following can be concluded:

$$5 \mid [k_\mathfrak{p}^* : \langle a \rangle] \text{ if and only if } \tau^2 - 4 \text{ is a square in } k_\mathfrak{p}.$$

Now let $x = -3(\tau^2 - 4)$. Assume that $\text{char}(k_\mathfrak{p}) \neq 2$. Since the polynomial $X^2 - 1$ splits in distinct factors in $k_\mathfrak{p}[X]$, it follows that $2 \mid [k_\mathfrak{p}^* : \langle a \rangle]$ if and only if there exists a $y \in K$ such that $a \equiv y^2 \mod \mathfrak{p}$.

Assume that $\text{char}(k_\mathfrak{p}) \neq 2, 3, 5$ and assume $\text{ord}_\mathfrak{p}(x) = \text{ord}_\mathfrak{p}(\tau) = 0$. Assume that $[k_\mathfrak{p}^* : \langle a \rangle] = 1$. Since $3, 5 \nmid [k_\mathfrak{p}^* : \langle a \rangle]$ it follows that $-3 \notin k_\mathfrak{p}^{*2}$ and $\tau^2 - 4 \notin k_\mathfrak{p}^{*2}$. We note that $k_\mathfrak{p}^*$ is a cyclic group and therefore, the product of two non-squares *is* a square. It follows that $-3(\tau^2 - 4) = x \in k_\mathfrak{p}^{*2}$. We conclude that there exists a $y \in K$ such that $a \equiv y^2 \mod \mathfrak{p}$. And thus, $2 \mid [k_\mathfrak{p}^* : \langle a \rangle]$. This gives a contradiction. Hence, a is not a primitive root modulo $\mathfrak{p}$ for all but finitely many primes $\mathfrak{q}$.

In both example 1.1, and 2.1, there exists a prime number l, such that for all but finitely many primes $\mathfrak{p}$, the index $[k_\mathfrak{p}^* : \langle a \rangle]$ is divisible by l. In Example 2.2 this is not the case. For every prime $\mathfrak{p}$ of K, the index $[k_\mathfrak{p}^* : \langle a \rangle]$ is divisible by either $2, 3$ or 5, however for each of these individual prime numbers there are infinitely many primes of K for which the index $[k_\mathfrak{p}^* : \langle a \rangle]$ is not divisible by K. In Example 2.2, there exists no prime number l, such that the extension F_l/K is trivial, however the density δ_a still vanishes. This example shows that Corollary 1.7.2 does not generalize directly to arbitrary number fields K.

The result of Example 2.2 is not just a coincidence. In fact, the field K and the element x were chosen in such a way that the fields F_2, F_3 and F_5 all have degree 2 over K, whereas the

compositum $F_{30} = F_2 \cdot F_3 \cdot F_5$ is of degree 4 over K instead of 8. Due to this dependence of fields, every prime $\mathfrak{p}$ of K splits completely in either F_2, F_3 or F_5. In order to fully comprehend this, several concepts have to be introduced.

2.2 The Frobenius element

There appear to be no restrictions, other than the restriction imposed by equality (5), on the splitting behaviour of a prime $\mathfrak{p} \in \mathcal{P}_K$ in $\mathcal{O}_L$. However, if L/K is a Galois extension, there exists a strong relation between the primes of L extending $\mathfrak{p}$. This is shown in the following theorem.

Theorem 2.3. *Let L/K be a Galois extension of number fields with Galois group G, and let $\mathfrak{p} \in \mathcal{P}_K$ be a prime of K. Then the following statements hold:*

1. *The group G acts transitively on the collection $D_L(\mathfrak{p})$ of primes in L extending $\mathfrak{p}$.*
2. *All residue class fields of the extensions $\mathfrak{q}$ of $\mathfrak{p}$ in L are isomorphic.*
3. *The residue class degree $f_\mathfrak{p} = f(\mathfrak{q}/\mathfrak{p})$ and the ramification index $e(\mathfrak{q}/\mathfrak{p})$ depend only on $\mathfrak{p}$.*
4. *If $g_\mathfrak{p}$ denotes the number of extensions of $\mathfrak{p}$ in L, the following equality holds:*

$$e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p} = [L : K].$$

Proof. Let $\sigma \in G$ be an automorphism of L that acts trivially on K. Let $x \in \mathcal{O}_L$ be an algebraic integer with minimum polynomial $f^x_{\mathcal{O}_K}$. Since σ is an automorphism that acts trivially on $\mathcal{O}_K$, we have that $\sigma(x)$ is a root of $f^x_{\mathcal{O}_K}$ and is therefore contained in $\mathcal{O}_L$. Let $\mathfrak{q}$ be a prime of L extending $\mathfrak{p}$. Let $z = xy \in \sigma\mathfrak{q}$ be given. Naturally, we have that $\sigma^{-1}(xy) = \sigma^{-1}(x)\sigma^{-1}(y) \in \mathfrak{q}$. Since $\mathfrak{q}$ is a prime ideal, it follows that either $\sigma^{-1}(x) \in \mathfrak{q}$ or $\sigma^{-1}(y) \in \mathfrak{q}$ holds, and hence either $x \in \sigma\mathfrak{q}$ or $y \in \sigma\mathfrak{q}$ holds. We conclude that $\sigma\mathfrak{q}$ is a prime of L extending $\mathfrak{p}$.

Assume that $\mathfrak{q}$ and $\mathfrak{q}'$ are two primes of L extending $\mathfrak{q}$ that are in different G-orbits. By applying the Chinese remainder theorem on $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$, we find that there exists an $x \in \mathfrak{q}$ that is not contained in $\sigma\mathfrak{q}'$, for all $\sigma \in G$. The minimum polynomial of x over $\mathcal{O}_K$ divides the polynomial $f = \prod_{\sigma \in G}(X - \sigma(x)) \in \mathcal{O}_K[X]$. It follows that $a_0 = \prod_{\sigma \in G} \sigma(x) \in \mathcal{O}_K$. Moreover, we have that $a_0 \notin \mathfrak{q}'$. It follows that $a_0 \in \mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p} = \mathfrak{q}' \cap \mathcal{O}_K$. This gives a contradiction. Hence, G acts transitively on $D_L(\mathfrak{p})$.

Let $\mathfrak{q}$ and $\mathfrak{q}'$ be two distinct primes of L extending $\mathfrak{p}$. By Theorem 2.3.1, there exists an automorphism $\sigma \in G$ such that $\sigma\mathfrak{q} = \mathfrak{q}'$. The map $\bar{\sigma} : k_\mathfrak{q} \to k_{\mathfrak{q}'},\ x \mod \mathfrak{q} \mapsto \sigma(x) \mod \mathfrak{q}'$, is therefore a well-defined homomorphism. Its inverse is given by $\bar{\sigma}^{-1} : k_{\mathfrak{q}'} \to k_\mathfrak{q},\ x \mod \mathfrak{q}' \mapsto \sigma^{-1}(x) \mod \mathfrak{q}$. Therefore, $\bar{\sigma}$ is an isomorphism. This proves the second statement. The third and fourth statement are a direct result from the second statement and equation (5). □

Let L/K be a Galois extension of number fields with Galois group G, and let $\mathfrak{p} \in \mathcal{P}_K$ be a prime of K that is unramified in L. Theorem 2.3 shows that G acts transitively on the collection of primes extending $\mathfrak{p}$. Hence, let $\mathfrak{q} \in D_L(\mathfrak{p})$ be a prime of L extending $\mathfrak{p}$. Then $\mathfrak{q}$ has a stabilizer group $G_{\mathfrak{q}/\mathfrak{p}}$ in G. This group is called the *decomposition group* of $\mathfrak{q}$ over $\mathfrak{p}$. Since every automorphism $\sigma \in G_{\mathfrak{q}/\mathfrak{p}}$ acts trivially on $\mathfrak{q}$, the reduction map $r : G_{\mathfrak{q}/\mathfrak{p}} \to \mathrm{Gal}(k_\mathfrak{q}/k_\mathfrak{p})$ is well-defined. In fact, there is a strong relation between the decomposition group $G_{\mathfrak{q}/\mathfrak{p}}$ and the Galois group of

$k_\mathfrak{q}$ over $k_\mathfrak{p}$:

Lemma 2.4. *Let L/K be a Galois extension of number fields with Galois group G. Let $\mathfrak{p}$ be a prime of K that is unramified in L, and let $\mathfrak{q}$ be a prime of L extending $\mathfrak{p}$. Let $G_{\mathfrak{q}/\mathfrak{p}}$ denote the decomposition group of $\mathfrak{q}$ in G. Then the map*

$$r_\mathfrak{q} : G_{\mathfrak{q}/\mathfrak{p}} \to \mathrm{Gal}(k_\mathfrak{q}/k_\mathfrak{p}),$$
$$(\sigma : x \mapsto \sigma(x)) \mapsto (\overline{\sigma} : x \mod \mathfrak{q} \mapsto \sigma(x) \mod \mathfrak{q}),$$

is a well-defined isomorphism of groups.

Proof. Let $\sigma, \tau \in G_{\mathfrak{q}/\mathfrak{p}}$, and $x \in \mathfrak{q}$ be given. Since $\sigma(x) \in \mathfrak{q}$, the automorphism $r_\mathfrak{q}(\sigma)$ is well-defined. And since $r_\mathfrak{q}(\sigma\tau) = r_\mathfrak{q}(\sigma)r_\mathfrak{q}(\tau)$, the map $r_\mathfrak{q}$ is a well-defined homomorphism. Since G acts transitively on the set $D_L(\mathfrak{p})$ of primes extending $\mathfrak{p}$, there is a bijective correspondence between set $G/G_{\mathfrak{q}/\mathfrak{p}}$ and $D_L(\mathfrak{p})$. It therefore follows that $\#G_{\mathfrak{q}/\mathfrak{p}} = f_\mathfrak{p} = \#\mathrm{Gal}(k_\mathfrak{q}/k_\mathfrak{p})$. It therefore suffices to show that $r_\mathfrak{q}$ is surjective, in order to complete the proof.

There exists an $\overline{\alpha} \in k_\mathfrak{q}^*$, such that $k_\mathfrak{q} = k_\mathfrak{p}(\overline{\alpha})$. Since every $\overline{\sigma} \in \mathrm{Im}(r_\mathfrak{q})$ is determined by its action on $\overline{\alpha}$, it suffices that $\mathrm{Im}(r_\mathfrak{q})$ acts transitively on the conjugates $\overline{\beta}$ of $\overline{\alpha}$ in $k_\mathfrak{q}$. By the Chinese remainder theorem, there exists an $\alpha \in \mathcal{O}_L$, such that $\alpha \equiv \overline{\alpha} \mod \mathfrak{q}$, and $\alpha \in \mathfrak{q}'$ for all primes $\mathfrak{q}' \neq \mathfrak{q}$ of L extending $\mathfrak{p}$. Let $\sigma \in G\backslash G_{\mathfrak{q}/\mathfrak{p}}$ be an automorphism of L. Since G acts transitively on the collection of primes extending $\mathfrak{p}$ there exists a prime $\mathfrak{q}'$ extending $\mathfrak{p}$, such that $\sigma\mathfrak{q}' = \mathfrak{q}$. Since $\alpha \in \mathfrak{q}'$, it follows that $\sigma(\alpha) \in \mathfrak{q}$ for all $\sigma \in G\backslash G_{\mathfrak{q}/\mathfrak{p}}$. The characteristic polynomial of α in $K[X]$ is given by $f = \prod_{\sigma\in G}(X - \sigma(\alpha)) = \prod_{\sigma\in G_{\mathfrak{q}/\mathfrak{p}}}(X - \sigma(\alpha)) \prod_{\sigma\in G\backslash G_{\mathfrak{q}/\mathfrak{p}}}(X - \sigma(\alpha))$. Its reduction modulo $\mathfrak{q}$ is therefore given by $\overline{f} = X^{(\#G - f_\mathfrak{p})} \prod_{\sigma\in G_{\mathfrak{q}/\mathfrak{p}}}(X - \overline{\sigma}(\overline{\alpha}))$. The minimum polynomial of α is a divisor of its characteristic polynomial. Hence, the minimum polynomial of $\overline{\alpha}$ in $k_\mathfrak{p}[X]$ is an irreducible polynomial of degree $f_\mathfrak{p}$ that divides $\prod_{\sigma\in G_{\mathfrak{q}/\mathfrak{p}}}(X - \overline{\sigma}(\overline{\alpha}))$. It follows that this polynomial is the minimum polynomial of α over $k_\mathfrak{p}$, and that $\mathrm{Im}(r_\mathfrak{q})$ acts transitively on the collection of conjugates of $\overline{\alpha}$. □

Since $\mathrm{Gal}(k_\mathfrak{q}/k_\mathfrak{p})$ is a cyclic group generated by $\mathrm{Frob}_\mathfrak{q} : x \mapsto x^{\#k_\mathfrak{p}}$, it follows from Lemma 2.4 that $G_{\mathfrak{q}/\mathfrak{p}}$ is a cyclic group as well. Therefore, there exists an automorphism $\sigma \in G_{\mathfrak{q}/\mathfrak{p}}$ such that $r_\mathfrak{q}(\sigma) = \mathrm{Frob}_\mathfrak{q}$. This automorphism is called the *Frobenius element* of $\mathfrak{q}$ over $\mathfrak{p}$ and is denoted by $\mathrm{Fr}_\mathfrak{q}$. The Frobenius element has various useful properties:

Proposition 2.5. *Let $K \subset L \subset M$ be a tower of number field extensions such that L/K, and M/K are Galois. Let $\mathfrak{p}$ be a prime of K that is unramified in M. Let $\mathfrak{q}$ be a prime of M extending $\mathfrak{p}$. Then $\mathfrak{q}' = \mathfrak{q} \cap \mathcal{O}_L$ is a prime of L extending $\mathfrak{p}$, and $Fr_\mathfrak{q}|_L = Fr_{\mathfrak{q}'}$.*

Proof. It is a trivial exercise to show that $\mathfrak{q}'$ is a prime of L, extending $\mathfrak{p}$. We note that $k_\mathfrak{p} \subset k_{\mathfrak{q}'} \subset k_\mathfrak{q}$ is a tower of finite Galois extensions. Since the Frobenius element $\mathrm{Fr}_\mathfrak{q}$ acts on $k_\mathfrak{q}$ by $x \mapsto x^{\#k_\mathfrak{p}}$, and $k_{\mathfrak{q}'} \subset k_\mathfrak{q}$, it has the same action on $k_{\mathfrak{q}'}$. Hence, the Frobenius automorphism of $k_{\mathfrak{q}'}$ over $k_\mathfrak{p}$ is given by $\mathrm{Frob}_{\mathfrak{q}'}(x) = \mathrm{Fr}_\mathfrak{q}(x) \mod \mathfrak{q}'$. On the other hand, it is given by $\mathrm{Frob}_{\mathfrak{q}'}(x) = \mathrm{Fr}_{\mathfrak{q}'}(x) \mod \mathfrak{q}'$. Since M/L is Galois, we have that $\mathrm{Gal}(L/K) = \mathrm{Gal}(M/K)|_L$. In particular we have that $G_{\mathfrak{q}'/\mathfrak{p}} = G_{\mathfrak{q}/\mathfrak{p}}|_L$, and hence $\mathrm{Fr}_\mathfrak{q}|_L \in G_{\mathfrak{q}'/\mathfrak{p}}$. It follows from the uniqueness of the Frobenius element that $\mathrm{Fr}_\mathfrak{q}|_L = \mathrm{Fr}_{\mathfrak{q}'}$. □

2.3 Applications of the Frobenius element

Let L/K be a Galois extension of number fields, and let $\mathfrak{p} \in \mathcal{P}_K$ be a prime of K that is unramified in L. If $\mathfrak{q}$ and $\mathfrak{q}'$ are two primes of L extending $\mathfrak{p}$, then there exists a $\sigma \in \mathrm{Gal}(L/K)$ such that $\mathfrak{q}' = \sigma\mathfrak{q}$. Consequently, we have that $G_{\mathfrak{q}'/\mathfrak{p}} = \sigma^{-1} G_{\mathfrak{q}/\mathfrak{p}} \sigma$. Since these primes are isomorphic, we conclude that the Frobenius element $\mathrm{Fr}_{\mathfrak{q}'}$ of $\mathfrak{q}'$ over $\mathfrak{p}$ is given by $\mathrm{Fr}_{\mathfrak{q}'} = \sigma \mathrm{Fr}_{\mathfrak{q}} \sigma^{-1}$. This gives rise to the definition of the *Frobenius symbol*:

Definition 2.6. Let L/K be a Galois extension of number fields, and let $\mathfrak{p} \in \mathcal{P}_K$ be a prime of K that is unramified in L. The *Frobenius symbol* $(\mathfrak{p}, L/K)$ of $\mathfrak{p}$ in L, is the union of all Frobenius elements lying above $\mathfrak{p}$ in L:

$$(\mathfrak{p}, L/K) = \bigcup_{\mathfrak{q}|\mathfrak{p}} \{\mathrm{Fr}_{\mathfrak{q}}\}.$$

In particular, the Frobenius symbol is a conjugacy class.

Theorem 2.3 and Lemma 2.4, allow us to identify the splitting behaviour of a prime in a number field, with the order of the elements in its corresponding Frobenius symbol:

Lemma 2.7. *Let L/K be a Galois extension of number fields, and let $\mathfrak{p}$ be a prime of K that is unramified in L. Then,* $\mathrm{ord}(\sigma) = f_{\mathfrak{p}}$*, for all* $\sigma \in (\mathfrak{p}, L/K)$.

Proof. Since the Frobenius symbol is a conjugacy class all automorphisms in the Frobenius symbol have the same order. Let $\sigma \in (\mathfrak{p}, L/K)$ be given. There exists a prime $\mathfrak{q} \in \mathcal{P}_L$ extending $\mathfrak{p}$ with $\sigma = \mathrm{Fr}_{\mathfrak{q}}$. By Lemma 2.4 the decomposition group $G_{\mathfrak{q}/\mathfrak{p}}$ is cyclic of order $f_{\mathfrak{p}}$. Hence, $\mathrm{ord}(\sigma) = f_{\mathfrak{p}}$. □

Lemma 2.7 has a direct result in the case that $\mathfrak{p}$ splits completely:

Corollary 2.7.1. *Let L/K be a Galois extension of number fields, and let $\mathfrak{p}$ be a prime of K that is unramified in L. The following are equivalent:*

(1) The prime $\mathfrak{p}$ splits completely in L.

(2) The Frobenius symbol $(\mathfrak{p}, L/K)$ of $\mathfrak{p}$ in L, is the collection of the trivial element, $(\mathfrak{p}, L/K) = \{\mathrm{id}_L\}$.

(3) There exists a prime $\mathfrak{q}$ in L extending $\mathfrak{p}$, for which the corresponding Frobenius element $\mathrm{Fr}_{\mathfrak{q}}$ is the trivial automorphism.

Proof. A prime $\mathfrak{p}$ splits completely in L, if and only if $f_{\mathfrak{p}} = 1$, and the only element of order 1 is the trivial element. □

We wish to relate the property of a being a primitive root modulo a prime $\mathfrak{p}$, to the Frobenius symbol of $\mathfrak{p}$ in the splitting fields F_l. However, there exists primes of K for which a is a primitive root, but still have a trivial Frobenius symbol in certain fields F_l.

Example 2.8. Consider the field $K = \mathbb{Q}(\zeta_3)$, and let $a = 10$. Let $\mathfrak{p} = (\zeta_3 - 1)$ be the prime extending 3. Since 3 is totally ramified in K, it follows that $k_{\mathfrak{p}} = \mathbb{F}_3$. Since $10 \equiv 1 \mod 9$, it can be shown that the prime $\mathfrak{p}$ splits completely in $F_3 = \sqrt[3]{10}$. However, 3 can never divide the indexe $[k_{\mathfrak{p}}^* : \langle 10 \rangle]$, since $\# k_{\mathfrak{p}}^* = 2$. This gives a contradiction.

Fortunately, there are at most finitely many primes for which this may occur, hence this will have no effect on the density δ_a. The following lemma restates the conditions.

Lemma 2.9. *Let K be a number field and let $\mathfrak{p}$ be a prime of K not contained in the divisor set of a or $2\Delta_K$, and let l be a prime number. Then,*

$$l \mid [k_\mathfrak{p}^* : \langle a \rangle] \text{ if and only if } \mathfrak{p} \text{ splits completely in } F_l.$$

Proof. The proof of Lemma 2.9 relies on the same argument as Theorem 1.7.
Let $\mathfrak{p} \notin D_K(a) \cup D_K(2\Delta_K)$ be a prime of K and let l be a prime number. Consider the ring $R = \mathcal{O}_K[\zeta_l, \sqrt[l]{a}]$, and the collection $\mathcal{C}$ of homomorphisms $\tau : R \to k_\mathfrak{p}$, with the condition that $x \mapsto x \mod \mathfrak{p}$ for $x \in \mathcal{O}_K$. Analogous to Theorem 1.7, every map $\tau \in \mathcal{C}$ corresponds to a unique prime $\mathfrak{q} \in D_{F_l}(\mathfrak{p})$ extending $\mathfrak{p}$. Hence, $\mathfrak{p}$ splits completely in F_l if, and only if $\#\mathcal{C} = [F_l : K]$.

Assume that $l \mid [k_\mathfrak{p}^* : \langle a \rangle]$. Then $k_\mathfrak{p}^*$ contains an element ζ of order l, and a is contained in the unique subgroup of l-th powers $k_\mathfrak{p}^{*l}$. Since $k_\mathfrak{p}^*$ contains $l-1$ elements of order l, there are precisely $[K(\zeta_l) : K]$ embeddings of ζ_l in $k_\mathfrak{p}$. And since $X^l - a$ has one root in $k_\mathfrak{p}^*$, all of its roots are contained in $k_\mathfrak{p}^*$, and hence there are $[F_l : K(\zeta_l)]$ distinct embeddings of $\sqrt[l]{a}$ in $k_\mathfrak{p}$. It follows that $\#\mathcal{C} = [F_l : K]$.

For the converse, we note that since $K(\zeta_l)/K$ is a totally ramified extension of degree $l - 1 > 1$ for $l \nmid 2\Delta_K$, a prime $\mathfrak{q}$ that splits completely in F_l/K can never divide l. Therefore, $\mathfrak{p}$ does not divide l, and hence the polynomial $X^l - 1$ is seperable in $k_\mathfrak{p}[X]$. And since there exists a homomorphism $\tau : R \to k_\mathfrak{p}$, the group $k_\mathfrak{p}^*$ contains an element of order l. Since $\mathfrak{p} \notin D_K(a)$, we have that $a \in k_\mathfrak{p}^*$, and hence $\tau(\sqrt[l]{a}) \in k_\mathfrak{p}^*$. It follows that $l \mid [k_\mathfrak{p}^* : \langle a \rangle]$.

□

Lemma 2.9 shows that a is not a primitive root modulo a prime $\mathfrak{p} \notin D_K(a) \cup D_K(2\Delta_K)$, if and only if there exists a prime number l, such that $\mathfrak{p}$ splits completely in the field $F_l = K(\zeta_l, \sqrt[l]{a})$. By Corollary 2.7.1, this occurs if and only if the Frobenius symbol $(\mathfrak{p}, L/K)$ is the collection of the identity automorphism. Combining these observations, it can be proven δ_a vanishes, if it satisfies a certain condition.

Lemma 2.10. *Let $a \in K^* \backslash \mu_K$ be a non-zero algebraic number. If there exists a square-free integer $n \in \mathbb{Z}_{>0}$, with the property that:*

$$\mathrm{Gal}(F_n/K) = \bigcup_{l \mid n} \mathrm{Gal}(F_n/F_l),$$

then there are at most finitely many primes $\mathfrak{p}$ of K for which a is a primitive root modulo $\mathfrak{p}$.

Proof. Let $n \in \mathbb{Z}_{>0}$ be a square-free integer and assume $\mathrm{Gal}(F_n/K) = \bigcup_{l|n} \mathrm{Gal}(F_n/F_l)$. Let $\mathfrak{p} \in \mathcal{P}_K \backslash (D_K(a) \cup D_K(2\Delta_K)$ be a prime of K, that is not contained in the divisor set of a or $2\Delta_K$. From Lemma 2.9 and Corollary 2.7.1, it follows that a is not a primitive root modulo $\mathfrak{p}$ if and only if there exists a prime number l such that $(\mathfrak{p}, F_l/K) = \{\mathrm{id}_{F_l}\}$. Let $\sigma \in (\mathfrak{p}, F_n/K) \subset \mathrm{Gal}(F_n/K)$, per assumption there exists a prime number $l \mid n$, such that $\sigma|_{F_l} = \mathrm{id}_{F_l}$. From Proposition 2.5 it follows that $(\mathfrak{p}, F_l/K) = (\mathfrak{p}, F_n/K)|_{F_l}$. Since $\mathrm{id}_{F_l} \in (\mathfrak{p}, F_l/K)$, it follows that $(\mathfrak{p}, F_l/K) = \{\mathrm{id}_{F_l}\}$. Hence, a is not a primitive root modulo $\mathfrak{p}$. □

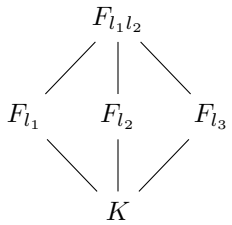
Given a square-free integer n, one might wonder whether there exists a field K and an algebraic number $a \in K^*$ such that $\mathrm{Gal}(F_n/K) = \bigcup_{l|n} \mathrm{Gal}(F_n/F_l)$. In fact, if we exclude the pairs (K, a) for which there exists a prime number l such that $F_l = K$, we can show that the smallest square-free integer n, for which there exists a pair (K, a) satisfying Lemma 2.10, is the integer $n = 30$. This is illustrated in the following examples.

Example 2.11. Let n be a square-free integer and assume that the equality $\mathrm{Gal}(F_n/K) = \bigcup_{l|n} \mathrm{Gal}(F_n/F_l)$ holds.
If n is the product of one prime number, we have that $n = l$. Hence $\mathrm{Gal}(F_n/K) = \mathrm{Gal}(F_n/F_l) = \{\mathrm{id}_{F_l}\}$. It follows that $F_l = K$, hence this is the trivial example where $a \in K^{*l}$ and $\zeta_l \in K$.

If n is the product of two prime numbers, then $\mathrm{Gal}(F_n/K)$ is the union of two subgroups. Since no group is the union of two proper subgroups, it follows that there exists a prime number $l \mid n$ such that $\mathrm{Gal}(F_n/F_l) = \mathrm{Gal}(F_n/K)$. Hence we arrive at the trivial example $F_l = K$.

Hence, the first non-trivial example is given when n is the product of three prime numbers.

Example 2.12. Let $n = l_1 l_2 l_3$ be the product of three prime numbers. We wish to construct a field K and an algebraic number $a \in K^*$, such that the equality $\mathrm{Gal}(F_n/K) = \cup_{l|n}\mathrm{Gal}(F_n/F_l)$ holds. From the above, we conclude that there exists an automorphism $\sigma \in \mathrm{Gal}(F_{l_1 l_2}/K)$, with the property that $\sigma \notin \mathrm{Gal}(F_{l_1 l_2}/F_{l_1}) \cup \mathrm{Gal}(F_{l_1 l_2}/F_{l_2})$. If F_{l_3} is not contained in $F_{l_1 l_2}$, then this automorphism can be extended to an automorphism $\tilde{\sigma} \in \mathrm{Gal}(F_n/K)$ such that $\tilde{\sigma} \notin \mathrm{Gal}(F_n/F_{l_3})$. Since its not contained in the Galois groups of F_n/F_{l_1} or F_n/F_{l_2} either, we arrive at a contradiction. We therefore must have that $F_{l_3} \subset F_{l_1 l_2}$. We are looking for prime numbers l_1, l_2 and l_3, such that if a prime does not $\mathfrak{p}$ split completely in F_{l_1} and F_{l_2}, then it must split completely in F_{l_3}. We have the following diagram.



This diagram has great similarities with the diagram of the Klein four-group. In fact, it follows directly from Lemma 2.10, that δ_a vanishes if $\mathrm{Gal}(F_n/K)$ is isomorphic to the Klein four-group. Hence, the question rises if this diagram can be realized as a V_4-diagram.

To this end, we let $n = l_1 l_2 l_3$ be the product of three distinct odd prime numbers. All extensions F_l/K must be of degree 2 over K. If $a \notin K^{*l}$, then $K(\sqrt[l]{a})/K$ is an extension of degree $l > 2$. Hence we choose $\in K^{*l_1 l_2 l_3}$. It follows that $F_n = K(\zeta_{l_1 l_2 l_3}$, and the Galois group $\mathrm{Gal}(F_n/K)$ must be a subgroup of $(\mathbb{Z}/l_1\mathbb{Z})^* \times (\mathbb{Z}/l_2\mathbb{Z})^* \times (\mathbb{Z}/l_3\mathbb{Z})^*$, which is the Galois group of $\mathbb{Q}(\zeta_{l_1 l_2 l_3})/\mathbb{Q}$. Since F_{l_i}/K must have degree 2 for all i, we conclude that $\mathrm{Gal}(F_{l_1 l_2 l_3}/K)$ must be contained in the subgroup $C_2 \times C_2 \times C_2$ of $(\mathbb{Z}/l_1\mathbb{Z})^* \times (\mathbb{Z}/l_2\mathbb{Z})^* \times (\mathbb{Z}/l_3\mathbb{Z})^*$, which exists since the prime numbers are odd. In particular, we are looking for the subgroup H, where each $\sigma \in H$, has the property that if $\sigma|_{F_{l_1}} = -1$, and $\sigma|_{F_{l_2}} = -1$, then we must have that $\sigma|_{F_{l_3}} = 1$. We note that this group H is precisely the group given by

$$H = \{(g_1, g_2, g_3) \in (\mathbb{Z}/l_1\mathbb{Z})^* \times (\mathbb{Z}/l_2\mathbb{Z})^* \times (\mathbb{Z}/l_3\mathbb{Z})^* \mid g_i = \pm 1,\ g_1 g_2 g_3 = 1\}.$$

This group is indeed isomorphic to the Klein four-group and has the property that F_{l_1}, F_{l_2} and

F_{l_3} all have degree 2 over the field $K = \mathbb{Q}(\zeta_{l_1 l_2 l_3})^H$. Hence we arrive at a non-trivial example where the density δ_a vanishes. Moreover, if L is any number field such that $l_1, l_2, l_3 \nmid \Delta_L$, then the extensions $\mathbb{Q}(\zeta_{l_1 l_2 l_3})/\mathbb{Q}$ and $L(\zeta_{l_1 l_2 l_3})/L$, have the same Galois group. Hence, other example where the Galois group $\mathrm{Gal}(F_{l_1 l_2 l_3}/K)$ is isomorphic to the Klein four-group are given when $\mathbb{Q}$ is replaced by such a field L.

A similar construction exists when $l_3 = 2$, in this case we let $a \in K^{*l_1 l_2}$. Again, we choose the field K such that F_{l_1} and F_{l_2} are quadratic extensions. Since they are quadratic, there exist algebraic numbers α and β, such that $F_{l_1} = K(\alpha)$, $F_{l_2} = K(\beta)$, and we have that $\alpha^2, \beta^2 \in K$. Hence, if we let $a = (\alpha\beta)^{l_1 l_2}$, then the field F_2 is given by $F_2 = K(\alpha\beta)$. Since $\alpha\beta \notin K$, this is a subfield of $F_{l_1 l_2}$ of degree 2, and the Galois group of $F_{2 l_1 l_2}$ is isomporhic to the Klein four-group.

3 The density of primitive roots in number fields

In this chapter two explicit expressions for the density δ_a corresponding an algebraic number $a \in K^*\backslash\mu_K$ will be conjectured. Using the Chebotarëv Density Theorem [4], the theorem of George Cooke and Peter Weinberger [1], and the theorem of Hendrik W. Lenstra [3], a conditional proof for these expressions is given, under the assumption of the Generalized Riemann Hypothesis. To this end, the concept of linear disjointness of number fields is introduced. This chapter is concluded by proving two corollaries of the main theorem, stating that the density δ_a vanishes if and only if a certain square-free integer $n(a, K)$ satisfies Lemma 2.10, where $n(a, K)$ is an integer depending only on a and K.

3.1 The main theorem

Theorem 3.1. *Let K be a number field and let $a \in K^*\backslash\mu_K$ be a non-zero algebraic number. Let $\mathcal{P}_K$ denote the collection of prime ideals of $\mathcal{O}_K$, and let $P(a) \subset \mathcal{P}_K$ denote the collection of primes $\mathfrak{p}$ of K for which a is a primitive root in $k_\mathfrak{p}$. Under assumption of the Generalized Riemann Hypothesis, $P(a)$ possesses a natural density δ_a in $\mathcal{P}_K$. Moreover, there exists a square-free integer $d \in \mathbb{Z}$, such that the density is given by*

$$\delta_a = \sum_{n|d} \frac{\mu(n)}{[F_n : K]} \cdot \prod_{\substack{l \text{ prime,} \\ l \nmid d}} \left(1 - \frac{1}{l(l-1)}\right). \tag{6}$$

Here, $\mu(n)$ denotes the Möbius counting function.

In order to prove the theorem, we first determine for every prime number l, the primes $\mathfrak{p}$ of K, for which the index $[k_\mathfrak{p}^* : \langle a \rangle]$ is divisible by l. As shown in section 2.3, for $\mathfrak{p} \notin D_K(a) \cup D_K(2\Delta_K)$, this occurs if and only if $\mathfrak{p}$ splits completely in F_l. In section 2.2, it was shown that this occurs if and only if the Frobenius symbol $(\mathfrak{p}, F_l/K)$ of $\mathfrak{p}$ in F_l is the trivial element. By Proposition 2.5, this can be generalized to arbitrary, square-free $n \in \mathbb{N}$. Let $n \in \mathbb{N}$ be a square-free integer, and let $\sigma \in \mathrm{Gal}(F_n/K)$ be an automorphism. Let $\mathfrak{p} \notin D_K(a) \cup D_K(2\Delta_K)$ be a prime of K such that $\sigma \in (\mathfrak{p}, F_n/K)$. If there there exists a prime number $l \mid n$, for which the restriction $\sigma|_{F_l} = \mathrm{id}_{F_l}$ holds, then a is not a primitive root modulo $\mathfrak{p}$. Hence if a is a primitive root modulo $\mathfrak{p}$, then σ must act non-trivially on all subfields F_l. Hence we define the collection

$$C_n = \{\sigma \in \mathrm{Gal}(F_n/K) : \sigma|_{F_l} \neq \mathrm{id}_{F_l}, \text{ for all } l \mid n\}.$$

If the Frobenius symbol $(\mathfrak{p}, F_n/K)$ of a prime $\mathfrak{p}$ is not contained in C_n, then a is not a primitive root modulo $\mathfrak{p}$. This proves fruitful in combination with the Chebotarëv Density Theorem, which states the following [4]:

Theorem 3.2 (N. Chebotarëv, 1926)**.** *Let L/K be a finite Galois extension of number fields. Let $C \subset G = \mathrm{Gal}(L/K)$ be a conjugacy class of $\mathrm{Gal}(L/K)$. The collection*

$$\{\mathfrak{p} \in \mathcal{P}_K \mid \mathfrak{p} \text{ is unramified in } L \text{ and } (\mathfrak{p}, L/K) \subset C\}$$

has density $\frac{\#C}{\#G}$ in $\mathcal{P}_K$.

Since C_n is a conjugacy class, it can be concluded from this theorem that the collection M_n of primes $\mathfrak{p}$ of K, that do not split completely in any subfield F_l of F_n, has density $\delta_{a,n} = \frac{\#C_n}{[F_n:K]}$

in $\mathcal{P}_K$. If $m \in \mathbb{N}$ is a divisor of n, then the splitting field F_m is a subfield of F_n. Every $\sigma \in C_m$ has $[F_n : F_m]$ extensions in $\mathrm{Gal}(F_m/K)$. From the injectivity of the inclusion map $i : C_n \to C_m \times \mathrm{Gal}(F_n/F_m)$, it is therefore concluded that $\#C_n \leq \#C_m \cdot [F_n : F_m]$. The following inequality therefore holds:

$$\delta_{a,n} = \frac{\#C_n}{[F_n : K]} \leq \frac{\#C_m \cdot [F_n : F_m]}{[F_n : F_m] \cdot [F_m : F_l]} = \delta_{a,m}.$$

Let $\mathfrak{P}$ denote the collection of products of increasing prime numbers,

$$\mathfrak{P} = \left\{ \prod_{p \leq n} p \;\middle|\; n \in \mathbb{N},\ p \text{ prime} \right\},$$

that is totally ordered by divisibility. Then, by the monotone convergence theorem, we conclude that the limit

$$\lim_{i \in \mathfrak{P}} \delta_{a,i}$$

exists. Naively, one might conclude from the above that this limit is δ_a. Proving this is rather non-trivial however. In 1975, George Cooke and Peter Weinberger proved that this equality does hold under assumption of the General Riemann Hypothesis [1].

Theorem 3.3 (G. Cooke, P. Weinberger, 1975)**.** *Under assumption of the Generalized Riemann Hypothesis, we have that*

$$\delta_a = \lim_{i \in \mathfrak{P}} \delta_{a,i}.$$

In order to give an explicit expression for the density, it therefore suffices to find an explicit value for $\#C_n$. This can be given using the principle of inclusion-exclusion:

Proposition 3.4. *Let $n \in \mathbb{N}$ be a square-free integer. The density $\delta_{a,n}$ is given by*

$$\delta_{a,n} = \sum_{d|n} \frac{\mu(d)}{[F_d : K]}.$$

Proof. Let $\sigma \in \mathrm{Gal}(F_n/K)$ be given. We note that $\sigma \notin C_n$ if and only if there exists a square-free integer $d \mid n$ for which $\sigma|_{F_d} = \mathrm{id}_{F_d}$. In particular, for $d \mid n$, define

$$D_d = \{\sigma \in \mathrm{Gal}(F_n/K) : \sigma|_{F_l} = \mathrm{id}_{F_l},\ \text{for all } l \mid d\}.$$

Then $C_n = \mathrm{Gal}(F_n/K) \setminus \left(\bigcup_{l|n} D_l \right)$. By the principle of inclusion and exclusion, $\#C_n$ is given by

$$\#C_n = \sum_{d|n} \mu(d) \# D_d.$$

Since $D_d = \{\sigma \in \mathrm{Gal}(F_n/K) : \sigma|_{F_l} = \mathrm{id}_{F_l},\ \text{for all } l \mid d\} = \mathrm{Gal}(F_n/F_d)$, we conclude that

$$\delta_{a,n} = \frac{\#C_n}{[F_n : K]} = \sum_{d|n} \frac{\mu(d) \cdot [F_n : F_d]}{[F_n : K]} = \sum_{d|n} \frac{\mu(d)}{[F_d : K]}.$$

□

By taking the limit $n \in \mathfrak{P}$ in Proposition 3.4, we obtain

$$\lim_{n\in\mathfrak{P}} \delta_{a,n} = \lim_{n\in\mathfrak{P}} \sum_{d|n} \frac{\mu(d)}{[F_d : K]} = \sum_{n=1}^{\infty} \frac{\mu(n)}{[F_n : K]}. \tag{7}$$

Under assumption of the Generalized Riemann Hypothesis, this limit is equal to the density δ_a.

3.2 Proof of the main theorem

When comparing Theorem 3.1 with Artin's original conjecture (1) for square-free $a \in \mathbb{Q}^*$, it can easily be seen that the equations differ by replacing the finite product $\prod_{l|d} \left(1 - (l^2 - l)^{-1}\right)$ with the inclusion-exclusion sum

$$\epsilon = \sum_{n|d} \frac{\mu(n)}{[F_n : K]}.$$

Here d is a square-free integer, depending only on the choice of K and $a \in K^*$. In the previous section it was concluded that ϵ is in fact the density of primes $\mathfrak{p} \in \mathcal{P}_K$, that do not split completely in any subfield $F_l \subset F_d$. For almost all prime numbers l, the density of primes that do not split completely in F_l is given by $\delta_{a,l} = [F_l : K]^{-1} = (l^2 - l)^{-1}$. Artin's original conjecture proved incorrect, since it did not take the 'linear dependence' of the splitting fields into account. As shown in Example 2.2, for the given field K and algebraic number a, a prime $\mathfrak{p}$ of K will split completely in either F_2, F_3 or F_5. This is due to the fact that these fields are not linearly disjoint over K. In order to formalize this, the concept of linear disjointness is introduced:

Definition 3.5. Let K be a number field. Let $S = \{L_i\}_{i\in I}$ be a collection of number fields that are Galois over K. Let $L = \prod_{i\in I} L_i$ denote the compositum of these fields. The collection S is *linearly disjoint over* K, if the natural injection

$$\begin{aligned} \iota : \mathrm{Gal}(L/K) &\to \prod_{i\in I} \mathrm{Gal}(L_i/K), \\ \sigma &\mapsto (\sigma|_{L_i})_{i\in I} \end{aligned}$$

is surjective.

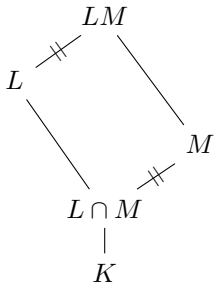
This definition is equivalent with the condition that ι is a well-defined isomorphism of groups. If I is a finite collection, this definition is also equivalent with the condition that

$$[L : K] = \prod_{i\in I} [L_i : K]. \tag{8}$$

In particular, two fields L and M are linearly disjoint over K if and only if they have intersection K. This is illustrated in the following example.

Example 3.6. Let L/K and M/K be two finite Galois extensions of K. We will show that the fields L and M are linearly disjoint over K, if and only if they satisfy the equality, $L \cap M = K$. To this end, we will show that there is a natural isomorphism $\varphi : \mathrm{Gal}(LM/L) \xrightarrow{\sim} \mathrm{Gal}(M/M \cap L)$, given by the restriction $\sigma \mapsto \sigma|_M$. Since M is a Galois extension, this map is well-defined. Let $\sigma \in \mathrm{Gal}(LM/L)$ be given and assume that $\sigma|_M = \mathrm{id}_M$. Since $\sigma|_L = \mathrm{id}_L$, it follows that $\sigma = \mathrm{id}_{LM}$. Hence, φ is injective. Let $\tau \in \mathrm{Gal}(M/M \cap L)$ be given. Since an automorphism $\tilde{\tau} \in \mathrm{Gal}(LM/L \cap M)$ is defined by its action on the fields M and L, we can define the automorphism

$\tilde{\tau}$, by $\tilde{\tau}(x) = \tau(x)$ for all $x \in M$ and $\tilde{\tau}(x) = x$, whenever $x \in L$. Since $\tau|_{L\cap M} = \mathrm{id}_{L\cap M}$, this automorphism is well-defined, and contained in $\mathrm{Gal}(LM/L)$. Moreover, it satisfies that $\tilde{\tau}|_M = \tau(x)$. Hence, φ is surjective. This is illustrated in the following diagram.



We therefore have a natural isomorphism

$$\begin{aligned} \mathrm{Gal}(LM/K) &\xrightarrow{\sim} \mathrm{Gal}(M/L\cap M) \times \mathrm{Gal}(L/K), \\ \sigma &\mapsto (\sigma|_M, \sigma|_L). \end{aligned} \tag{9}$$

It follows directly from equation (8), and the definition of linear disjointness that, L and M are linearly disjoint over K if and only if the $L \cap M = K$ holds.

It is important to note that this alternative definition of linear disjointness does not generalize when S is a collection of cardinality greater than 2; the fields F_2, F_3 and F_5 as described in Example 2.2 are pairwise linearly disjoint over $\mathbb{Q}(\sqrt{5})$. The collection $\{F_2, F_3, F_5\}$ is not linearly disjoint however, as the map ι is not surjective.

Let d, m be two square-free integers such that the fields F_d and F_m are linearly disjoint. Then the image of C_{dm} under the restriction map ι as defined in Definition 3.5 is the direct product of C_d and C_m. We therefore obtain the equality

$$\delta_{a,dm} = \frac{\#C_{dm}}{[F_{dm} : K]} = \frac{\#C_d \cdot \#C_l}{[F_d : K][F_m : K]} = \delta_{a,d} \cdot \delta_{a,m}.$$

If the collection $\{F_l \mid l \text{ prime}\}$ is linearly disjoint over $\mathbb{Q}$, then equality (1) would hold. For example, if $a = 2$, and d is a square-free integer we obtain the equality

$$\delta_{2,d} = \prod_{\substack{l \text{ prime}, \\ l|d}} \delta_{2,l} = \prod_{\substack{l \text{ prime}, \\ l|d}} \left(1 - \frac{1}{[F_l : \mathbb{Q}]}\right).$$

This is not the case if $a \equiv 1 \mod 4$ however. Galois theory shows that if p is an odd prime number, then the field $\mathbb{Q}(\zeta_p)$ has a subfield L of degree 2 given by $L = \mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{(p-1)/2}p$. [5, p. 54]. Hence, if $p \equiv 1 \mod 4$, we have that $p^* = p$ and therefore, $L = F_2$. It follows that $F_{2p} = F_p$ and hence the fields F_p and F_2 are not linearly disjoint. In order to prove Theorem 3.1 in arbitrary number fields K, we need to determine a finite collection I of prime numbers, such that the collection $\{F_l\}_{l\notin I} \cup \{\prod_{p\in I} F_p\}$ is linearly disjoint over K. Over $\mathbb{Q}$, such a collection is given by $I = \{2\} \cup D_{\mathbb{Q}}(a)$. the only eligble primes are the primes 2 and the prime numbers l for which $\mathrm{ord}_l(a) \neq 0$.
For a number field K, a similar collection exists. In 1977, Hendrik W. Lenstra, analyzed the conditions for which the field F_l is linearly disjoint of all fields F_d, where d is a square-free integer coprime to d, [3]. This is summarized in the following theorem.

Theorem 3.7 (H. W. Lenstra, 1977)**.** *Let l be a prime number satisfying the following conditions:*

1. *l does not divide $2 \cdot \Delta_K$,*
2. *there exists no $x \in K^*$ such that $a = x^l$,*
3. *the divisor sets $D_K(l)$ and $D_K(a)$ are disjoint.*

Further, let $d \in \mathbb{Z}$ be a square-free integer, coprime to l. Then the fields F_l and F_d are linearly disjoint over K. Moreover, the field extension F_l/K has degree $l(l-1)$.

Proof. Let l be a prime number satisfying all the listed conditions. It follows from the first condition that the l-th cyclotomic polynomial $\Phi_l(X)$ is irreducible in $K[X]$. We therefore have that $[K(\zeta_l) : K] = l - 1$. From the second condition, it follows that the polynomial $X^l - a$ is irreducible in $K(\zeta_l)[X]$, [5, p. 72]. We conclude that $[F_l : K] = l(l-1)$.

Let $d \in \mathbb{Z}_{>0}$ be a square-free integer coprime to l. In order to prove that F_l and F_d are linearly disjoint over K, it suffices to show that $[F_{dl} : F_d] = l(l-1)$. The extension $K(\zeta_l)/K$ is totally ramified of degree $l - 1 > 1$. The only primes that ramify in F_d are the primes contained in the union $D_K(a) \cup D_K(d)$. Since l is coprime to d, and the intersection $D_K(a) \cap D_K(l) = \emptyset$ is empty, the extension F_d/K is unramified over l. Hence, it follows that $K(\zeta_l) \cap F_d = K$, and therefore the equality $[F_d(\zeta_l) : F_d] = (l-1)$ holds. F_d is a Galois extension, hence if $\sqrt[l]{a} \in F_d$, then $\zeta_l \in F_d$. We conclude that $\sqrt[l]{a} \notin F_d$. Since l is a prime number, it therefore follows from the second condition that the polynomial $X^l - a$ is irreducible in $F_d(\zeta_l)[X]$ as well. We conclude that $[F_d(\zeta_l, \sqrt[l]{a}) : F_d(\zeta_l)] = l$, and hence the fields F_d and F_l are linearly disjoint over K. □

There are only finitely many prime numbers l that violate a condition of Theorem 3.7. Let d denote the product of these primes. For all other primes p coprime to d, we have that the fields F_d and F_p are linearly disjoint over K. This observation allows us to prove Theorem 3.1.

Proof of Theorem 3.1. Let K be a number field and let $a \in K^* \backslash \mu_K$ be a non-zero algebraic number that is not a root of unity. Let $g \in \mathbb{N}$ denote the largest integer for which the polynomial $X^g - a$ has a root in K. For all primes $\mathfrak{p}_i \in D_K(a)$ in the divisor set of a, let $p_i = \mathrm{char}(k_{\mathfrak{p}_i})$ denote the characteristic of the residue class field $k_{\mathfrak{p}_i}$, and let $P = \prod_i p_i$ be the product of all these prime numbers. Finally, let d be the square-free integer given by $d = \mathrm{rad}(2\Delta_K g P) \in \mathbb{Z}$, where rad denotes the radical function.

Let l be a prime number that is coprime to d. By Theorem 3.7, the fields F_d and F_l are linearly disjoint over K. Let $\iota : \mathrm{Gal}(F_{dl}/K) \mapsto \mathrm{Gal}(F_d/K) \times \mathrm{Gal}(F_l/K)$ be the restriction map as given in Definition 3.5. From the equality $\iota(C_{dl}) = C_d \times C_l$, it follows that $\#C_{dl} = \#C_d \cdot \#C_l$, and therefore the equality

$$\delta_{a,dl} = \frac{\#C_{dl}}{[F_{dl} : K]} = \frac{\#C_d \cdot \#C_l}{[F_d : K][F_l : K]} \tag{10}$$

holds. Since l is a prime number, the equality $\#C_l = [F_l : K] - 1$ holds. Therefore, equation (10) reduces to

$$\delta_{a,dl} = \frac{\#C_d}{[F_d : K]} \left(\frac{[F_l : K] - 1}{[F_l : K]} \right) = \delta_{a,d} \cdot \left(1 - \frac{1}{[F_l : K]} \right). \tag{11}$$

Let $m \in \mathfrak{P}$ be a product of prime numbers, such that $d \mid m$. By repeating the given argument we obtain

$$\delta_{a,m} = \delta_{a,d} \prod_{\substack{l \text{ prime}, \\ l \mid m/d}} \left(1 - \frac{1}{[F_l : K]}\right).$$

For all $l \nmid d$, we have that $[F_l : K] = l(l-1)$ by Theorem 3.7. Theorem 3.3 finally gives

$$\delta_a = \sum_{n \mid d} \frac{\mu(n)}{[F_n : K]} \cdot \prod_{\substack{l \text{ prime}, \\ l \nmid d}} \left(1 - \frac{1}{l(l-1)}\right).$$

□

3.3 Applications of the main theorem

We will conclude this thesis by proving several corollaries of the main theorem.

Corollary 3.1.1. *Let K be a number field and $a \in K^* \backslash \mu_K$ be a non-zero algebraic number that is not a root of unity. Then the following are equivalent:*

1. $\delta_a = 0$.
2. *There exists a square-free $n \in \mathbb{Z}_{>0}$, for which the equality $\mathrm{Gal}(F_n/K) = \bigcup_{l \mid n} \mathrm{Gal}(F_n/F_l)$ holds.*

Proof. If $\delta_a = 0$, then it follows from Theorem 3.1, that there exists a square-free integer $n \in \mathbb{Z}$ for which $\delta_{a,n} = 0$, and since $\delta_{a,n} = \frac{\#C_n}{[F_n:K]}$, we conclude that

$$\{\sigma \in \mathrm{Gal}(F_n/K) : \sigma|_{F_l} \neq \mathrm{id}_{F_l}, \text{ for all } l \mid n\} = \emptyset.$$

Hence, for all $\sigma \in \mathrm{Gal}(F_n/K)$ there exists a prime number $l \mid n$ for which $\sigma|_{F_l} = \mathrm{id}_{F_l}$, hence $\sigma \in \mathrm{Gal}(F_n/F_l)$. We conclude that $\mathrm{Gal}(F_n/K) = \bigcup_{l \mid n} \mathrm{Gal}(F_n/F_l)$. The other implication was proven in Lemma 2.10. □

Corollary 3.1.2. *Let K be a number field, and let $a \in K^* \backslash \mu_K$ be an algebraic number that is not a perfect power. Then δ_a does not vanish.*

Proof. Let K be a number field, let $a \in K^*$ be an algebraic integer that is not a perfect power. We will show using induction on $\mathfrak{P}$, that $C_n \neq \emptyset$ for all $n \in \mathfrak{P}$.

We note that $C_2 \neq \emptyset$, hence the statement holds for $n = 2$. Let $n \in \mathfrak{P}$ be given and assume that $C_n \neq \emptyset$. Let l be the smallest prime number that does not divide n. We note that the degree $[F_n : K]$ is a divisor of $\prod_{p \mid n} [F_p : \mathbb{Q}] = \prod_{p \mid n} p(p-1)$, where p ranges over all prime numbers dividing n. Since $a \notin K^{*l}$, we have that $l \mid [F_l : K]$, and since $l \nmid n$, we conclude that $l \nmid [F_n : K]$, and therefore $l \mid [F_l : F_l \cap F_n]$. From Example 3.6, we conclude that there is a natural isomorphism:

$$\begin{aligned} \mathrm{Gal}(F_{nl}/F_n \cap F_l) &\xrightarrow{\sim} \mathrm{Gal}(F_l/F_n \cap F_l) \times \mathrm{Gal}(F_n/F_n \cap F_l), \\ \sigma &\mapsto (\sigma|_{F_l}, \sigma|_{F_n}). \end{aligned}$$

Hence, there exists an automorphism $\sigma \in \mathrm{Gal}(F_{nl}/F_n \cap F_l)$ of order l, such that $\sigma|_{F_l} \neq \mathrm{id}_{F_l}$, and $\sigma|_{F_n} = \mathrm{id}_{F_n}$. This automorphism can be extended to an automorphism $\tilde{\sigma} \in \mathrm{Gal}(F_{nl}/K)$. By the induction hypothesis, there exists a $\tau \in C_n$, which can be extended to an automorphism $\tilde{\tau} \in \mathrm{Gal}(F_{nl}/K)$, with order coprime to l. The composition $\phi = \tilde{\sigma}\tilde{\tau}$, is an automorphism of F_{nl}, for which the restriction $\phi|_{F_n} = \tau$ holds. Since the order of $\tilde{\tau}$ and $\tilde{\sigma}$ are coprime, it follows that $\phi|_{F_l} \neq \mathrm{id}_{F_l}$. Hence, this automorphism acts non-trivially on all subfields $F_d \subset F_l$ and on F_l. It therefore acts non-trivially on all subfields $F_d \subset F_{nl}$. We conclude that $\phi \in C_{nl}$. It follows that $C_n \neq \emptyset$, for all $n \in \mathfrak{P}$.

To finalize the proof, we note that by the proof of Theorem 3.1, there exists an $m \in \mathfrak{P}$, such that $\delta_a = \delta_{a,m} \cdot \prod_{l \nmid m}(1 - (l^2 - l)^{-1})$, and by the Chebotarëv Density theorem, it follows that $\delta_{a.m} \neq 0$. □

References

[1] George Cooke and Peter J. Weinberger. *On the construction of division chains in algebraic number rings,with applications to SL2*. In: *Communications in Algebra* 3.6 (1975), pp. 481–524. DOI: 10.1080/00927877508822057.

[2] Christopher Hooley. *On Artin's conjecture*. In: *Journal für die reine und angewandte Mathematik* 225 (1967), pp. 209–220.

[3] H. W. Lenstra. *On Artin's Conjecture and Euclid's Algorithm in Global Fields*. In: *Inventiones mathematicae* 42 (1977), pp. 201–224.

[4] H. W. Lenstra & Peter Stevenhagen. *Chebotarëv and his density theorem*. In: *The Mathematical Intelligencer* 18.2 (1996).

[5] Peter Stevenhagen. *Algebra 3*. 2012. URL: websites.math.leidenuniv.nl/algebra/.

[6] Peter Stevenhagen. *Number Rings*. Oct. 13, 2017. URL: websites.math.leidenuniv.nl/algebra/.

[7] Peter Stevenhagen. *The correction factor in Artin's primitive root conjecture*. In: *Journal de Theorie des Nombres de Bordeaux* (2003).