The Support Problem

Ana Lukić

Contents

Introduction

The support problem is the following question, asked by Pál Erdös:

> *Let x and y be positive integers with the property that for all positive integers n the set of prime numbers dividing $x^n - 1$ is equal to the set of prime numbers dividing $y^n - 1$. Is then $x = y$?*

The name support refers to $\mathrm{Supp}(m)$ which is the support of a positive integer m. This is the set of primes dividing m. One can thus also say that Erdös asked whether

$$[\forall n \in \mathbb{Z}_{>0}\ \mathrm{Supp}(x^n - 1) = \mathrm{Supp}(y^n - 1)] \iff x = y$$

Capi Corrales-Rodrigáñez and René Schoof [1] gave the answer to this question by proving the following theorem:

Theorem 0.1 *Let F be a number field and let $x, y \in F^*$. If for almost all prime ideals $\wp$ of the ring of integers of F and for all positive integers n one has*

$$y^n \equiv 1 (mod\ \wp) \ \ whenever\ \ x^n \equiv 1 (mod\ \wp)$$

then y is a power of x.

In the above, for almost all means for all but for a finite set. We will not give the proof of this theorem here, but it is this theorem and its proof which are the main inspiration for this paper. Our main goal is to answer the following questions:

1) Can we enlarge the set of primes for which the condition of the theorem does not hold?

2) Does the condition need to hold for every positive integer n?

As a result we will prove the following theorem

Theorem 0.2 *Let F be a number field and let $x, y \in F^*$. If for all prime numbers l and for all positive integers n, one has that for almost all primes $\wp$ of F which are completely split in $F(\zeta_{l^n})$, the following holds:*

$$y^{\frac{N(\wp)-1}{l^n}} \equiv 1 (mod\ \wp) \ whenever\ \ x^{\frac{N(\wp)-1}{l^n}} \equiv 1 (mod\ \wp)$$

then y is a power of x. For almost all here means for all but for a set of density at most $\frac{l-2}{2 \cdot l^{3n}}$.

We refer to this theorem as the main theorem of our paper, because it is mostly related to the original problem.

The density used here, and throughout this paper, is not the Dirichlet density. If we were to use Dirichlet density we would have a problem since we can't know for sure that it exists for a given set of primes. The density we use here will be defined in chapter 1. It is a density very similar to Dirichlet density, with a nice property that it always exists.

We also notice that the statements of theorem 0.1 and theorem 0.2 are actually "if and only if" statements. That is if there is an integer a such that $y = x^a$ then $x^n \equiv 1 (mod\ \wp) \Rightarrow x^{an} \equiv 1 (mod\ \wp) \Rightarrow y^n \equiv 1 (mod\ \wp)$ holds for all integers n and all primes $\wp$.

We will also prove the following generalization of our main theorem

Theorem 0.3 *Let F be a number field, with $\mathbb{Z}_F$ its ring of integers, and let $x, y \in F^*$. Let l be a prime number and m and m' two positive integers. Then the implication:*

$$\textit{order of } x^{\frac{N(\wp)-1}{l^n}} \textit{ in } (\mathbb{Z}_F/\wp)^* \textit{ is } l^m \implies \textit{order of } y^{\frac{N(\wp)-1}{l^n}} \textit{ in } (\mathbb{Z}_F/\wp)^* \textit{ is } l^{m'}$$

is true for all positive integers n and for almost all primes $\wp$ of $\mathbb{Z}_F$ which are completely split in $F(\zeta_{l^n})$, if and only if either x is a root of unity of order not divisible by l^m, or there are integers a and $b > 0$ with $gcd(l, ab) = 1$, such that $y^{l^{m'-1}b} = x^{l^{m-1}a}$. Almost all here means all but a set of density at most $\frac{l-2}{l^{3n}}$

We also want to refer to an article written by A. Schinzel [2] where, amongst several theorems, he also proves the following generalization of theorem 0.1

Theorem 0.4 *Let Φ_n denote the n-th cyclotomic polynomial, and let k and l be two positive integers, where l does not have any square factors. Let F be a number field, and let $x, y \in F^*$, where x is not a root of unity. Then the implication*

$$\wp \mid \Phi_k(x^n) \implies \wp \mid \Phi_l(y^n)$$

is true for all integers $n > 0$ and all but a finite number of primes $\wp$ of F, if and only if $l \mid k$ and $y = x^{\frac{k\lambda}{l}}$ with $gcd(\lambda, l) = 1$.

Notice that $\wp \mid \Phi_k(x^n)$ is the same as to say that the order of x^n in $\mathbb{Z}_F/\wp$ is k, provided that k is not contained in the prime ideal $\wp$. However the differences between these two theorems are more interesting to observe. In terms of theorem 0.4, k and l are allowed to be composite numbers, we are allowing only the prime powers. On the other hand, in theorem 0.4 l must divide k and can not have square factors, and in theorem 0.3 we allow $m' > 1$ and we are not assuming that $m' \leq m$. Not to mention that the condition and the conclusion of the two theorems are slightly different. The reason for this is, of course, that the methods used to prove these two theorems are different. But we do not want to discuss these differences, we want to prove our theorems.

Beside the basic knowledge of algebra, Galois theory and number theory, the reader needs to have some knowledge of algebraic number theory. However, in appendix we summarize the machinery needed for the proofs of our theorems.

As for the notation, if F is a field, then F^* denotes its multiplicative group of units and $\mathbb{Z}_F$ the ring of integers of F. A nonzero prime ideal of $\mathbb{Z}_F$ will often, simply, be called a prime of F. Furthermore ζ_q denotes a primitive q-th root of unity and μ_q the group of q-th roots of unity. As usual we let $i = \zeta_4$.

Chapter 1

Some Tools

This chapter contains the preliminaries needed for our theorems. In the first section we talk about the density and in the second section we prove three lemmas.

1.1 Density

As we already mentioned in the introduction we do not want to be bothered by whether the density of a certain set of primes exists or not. We need a density which exists for any given set of primes. Now the Dirichlet density, denoted by δ, is defined as a limit and therefore doesn't always exist. Hence we must define a new density. For S, a set of primes of a number field we let:

$$\Delta(S) = \limsup_{s \to 1+} \frac{\sum_{\wp \in S} \frac{1}{N(\wp^s)}}{\log(\frac{1}{s-1})}$$

This is the density which we will use. We call it the **sup-density**. Some of the properties of the Dirichlet density also hold for the sup-density, but some don't. For example we do have that $0 \leq \Delta(S) \leq 1$, but if T and S are two disjoint sets we do not necessarily have $\Delta(S \cup T) = \Delta(S) + \Delta(T)$. Notice that if the Dirichlet density of a set S exists then $\delta(S) = \Delta(S)$.

We would like to be able to use the Chebotarev density theorem, but we can not because this theorem states something about the Dirichlet density. Fortunately we can "adapt" this theorem to our density:

Theorem 1.1 ***(Chebotarev*).*** *Let K/k be abelian with Galois group G, and let S be a set of primes of k. Let $G_S = \{\sigma \in G | \ \exists \wp \in S \text{ with } \sigma = (\wp, K/k)\}$. Then*

$$\Delta(S) \leq \frac{|G_S|}{|G|}$$

Proof We extend S to a set of primes for which the Dirichlet density exists and then use the Chebotarev density theorem. Define $S' = \{\wp| \ \exists \sigma \in G_S \text{ with } \sigma = (\wp, K/k)\}$. Then by Chebotarev density theorem $\delta(S')$ exists and is equal to $\frac{|G_S|}{|G|}$, hence $\Delta(S') = \delta(S') = \frac{|G_S|}{|G|}$. We also have the following inequality:

$$\Delta(S) = \limsup_{s \to 1+} \frac{\sum_{\wp \in S} \frac{1}{N(\wp^s)}}{\log(\frac{1}{s-1})} \leq \limsup_{s \to 1+} \frac{\sum_{\wp \in S'} \frac{1}{N(\wp^s)}}{\log(\frac{1}{s-1})} = \Delta(S')$$

which proofs the theorem. □

In the proofs of our theorems we will also use the following lemma

Lemma 1.1 *Let K/k be Galois of degree n. Let T be a set of primes of k and T' the set of primes of K which are above the primes of T. Then*

$$\Delta(T') \leq n \cdot \Delta(T)$$

Proof Per definition we have

$$\Delta(T') = \limsup_{s \to 1+} \frac{\sum_{q \in T'} \frac{1}{N(q^s)}}{\log(\frac{1}{s-1})}$$

Furthermore, for every prime $\wp$ in T there are at most n different primes in T' lying above $\wp$. Also, for every prime q lying above $\wp$ we have $N(q) = N(\wp)^{f(q/\wp)}$, hence $1/N(q^s) \leq 1/N(\wp^s)$. It follows that

$$\Delta(T') \leq n \cdot \limsup_{s \to 1+} \frac{\sum_{\wp \in T} \frac{1}{N(\wp^s)}}{\log(\frac{1}{s-1})} = n \cdot \Delta(T)$$

In particular, if all of the primes in T are completely split into the primes of T' then for each prime in T there are exactly n primes in T' and $f(q/\wp) = 1$ so that $\Delta(T') = n \cdot \Delta(T)$. □

Of course, if Dirichlet density of T and T' exists then the same is true for δ. Notice also that if all of the primes of T are completely split in K and we know that $\delta(T)$ exists, then $\delta(T')$ also exists and it is equal to $n \cdot \delta(T)$.

1.2 Lemmas

In this section we prove three lemmas which we will need to use in the proofs of our theorems. They might seem irrelevant at this moment, and if so one can postpone reading them until they are needed in the proofs.

Lemma 1.2 *Let F be a number field and let q be a power of a prime number l. If $l = 2$, assume that $i \in F$. Then $G_q = Gal(F(\zeta_q)/F)$ is cyclic. Furthermore, let σ denote a generator of G_q and let $N_q : F(\zeta_q)^* \longrightarrow F^*$ denote the norm map. Then the following holds:*

(i) For $\zeta \in \mu_q$ we have that $N_q(\zeta) = 1$ if and only if $\zeta = \sigma(\xi)/\xi$ for some $\xi \in \mu_q$.

(ii) The natural map $F^*/F^{*q} \longrightarrow F(\zeta_q)^*/F(\zeta_q)^{*q}$ is injective.

Proof First we prove that the Galois group G_q is cyclic. From the Galois theorem of cyclotomic extensions we know that G_q is isomorphic to a subgroup H of $(\mathbb{Z}/q\mathbb{Z})^*$. Now if q is odd then $(\mathbb{Z}/q\mathbb{Z})^*$ is cyclic and thus H must be cyclic. If $q = 2^n$ then we need to make some effort since $(\mathbb{Z}/2^n\mathbb{Z})^*$ isn't cyclic. We claim that, in this case H is contained in $\{x \in (\mathbb{Z}/2^n\mathbb{Z})^* | \ x \equiv 1 (\text{mod } 4)\}$, where n is an integer which we can take larger then 2. To see this we need to look at the effect of $\sigma \in G_q$ on $i = \zeta_4$. Since we assumed that $i \in F$ we know that we must have $\sigma(i) = i$. On the other hand if we write i as $\zeta_{2^n}^{2^{n-2}}$ then $\sigma(\zeta_{2^n}^{2^{n-2}}) = \zeta_{2^n}^{2^{n-2} \cdot s} = i^s$ for some $s \in (\mathbb{Z}/2^n\mathbb{Z})^*$. It follows that $s \equiv 1(\text{mod } 4)$. We leave it as an exercise to the reader to show that the order of $\bar{5}$ in $(\mathbb{Z}/2^n\mathbb{Z})^*$ is 2^{n-2} and that therefore $\langle \bar{5} \rangle = \{x \in (\mathbb{Z}/2^n\mathbb{Z})^* | \ x \equiv 1(\text{mod } 4)\}$ is cyclic.

(i) Let a be the image of σ in H, and let d be the order of H. Define $Z = \{x \in \mathbb{Z}/q\mathbb{Z} | \ (1 + a + \cdots + a^{d-1})x \equiv 0\}$ and $B = \{(1 - a)x | \ x \in \mathbb{Z}/q\mathbb{Z}\}$. Then it is clear that $B \subset Z$. Furthermore the homomorphism $\psi : Z \to \{\zeta \in \mu_q | \ N_q(\zeta) = 1\}$ given by $\psi(x) = \zeta_q^x$ induces an isomorphism

$$\psi : Z/B \longrightarrow \{\zeta \in \mu_q | \ N_q(\zeta) = 1\}/\{\sigma(\zeta)/\zeta | \ \sigma \in G_q\}$$

It is now sufficient to show that $Z = B$. We already know that $B \subset Z$. For the other inclusion we distinguish two cases:

1) There is a prime p, different from l, with $p \mid d$. Let $b = a^{d/p}$. Then $b^p \equiv 1(\text{mod } l)$ but $b \not\equiv 1(\text{mod } l)$. Therefore $(1 - b)$ is a unit in $\mathbb{Z}/q\mathbb{Z}$. Since $1 - b = (1 - a)(1 + a + \cdots + a^{-1+d/p})$, we see that $(1 - a)$ is also a unit in $\mathbb{Z}/q\mathbb{Z}$. But then $B = \mathbb{Z}/q\mathbb{Z}$ and thus $Z \subset B$.

2) The order of H is a power of l, i.e., d is a power of l. Lift a to $\mathbb{Z}$. Let $s = \text{ord}_l(q)$ and $t = \text{ord}_l(a - 1)$, where $\text{ord}_p(N)$ denotes the order of p at N, i.e., the number of factors p in N. We know that $l^s \mid (a^d - 1)$. Let A denote the group generated by a in $\mathbb{Z}/lq\mathbb{Z}$. Suppose that $l^{s+1} \mid (a^d - 1)$. Then the order of A in $\mathbb{Z}/lq\mathbb{Z}$ is also d. This implies that the map $\tau : A \to H$, which is the reduction modulo l^s, is injective. But the map $\rho : (\mathbb{Z}/l^{s+1}\mathbb{Z})^* \to (\mathbb{Z}/l^s\mathbb{Z})^*$ is not injective and the kernel of ρ, which is therefore not trivial, is contained in every subgroup of $\mathbb{Z}/l^{s+1}\mathbb{Z}$, of order divisible by l. Therefore it is also contained in A and hence $\tau = \rho|_A$ can not be injective. We conclude that

$\mathrm{ord}_l(a^d-1)=s$. Then $\mathrm{ord}_l(1+a+\cdots+a^d)=\mathrm{ord}_l(a^d-1)-\mathrm{ord}_l(a-1)=s-t$. This means that if $z\in Z$ then $\mathrm{ord}_l(z)\geq t$. But since $\mathrm{ord}_l(1-a)=t$, we see that $\mathrm{ord}_l((1-a)x)\geq t$, $\forall x\in\mathbb{Z}/q\mathbb{Z}$. Therefore $z\in B$, and thus $Z\subset B$.

(ii) Suppose that $t\in F^*$ is equal to s^q for some $s\in F(\zeta_q)$. Then $\sigma(s)^q=\sigma(s^q)=\sigma(t)=t=s^q$ so that $(\frac{\sigma(s)}{s})^q=1$, therefore $\frac{\sigma(s)}{s}$ is a q-th root of unity. Furthermore $N_q(\frac{\sigma(s)}{s})=\frac{\sigma^2(s)\cdots\sigma^{d+1}(s)}{\sigma(s)\cdots\sigma^d(s)}=1$. Part (i) now implies that $\frac{\sigma(s)}{s}=\frac{\sigma(\xi)}{\xi}$ for some $\xi\in\mu_q$. It follows that $\sigma(\frac{s}{\xi})=\frac{\sigma(s)}{\sigma(\xi)}=\frac{s}{\xi}$ and therefore $s\xi^{-1}\in F$. Since $t=s^q=(s\xi^{-1})^q$, the lemma follows. $\square$

Lemma 1.3 *Let F be a number field and let $x\in F^*$. Let q be a power of a prime number l. Let $\wp$ be a prime ideal of $\mathbb{Z}_F$, with $\wp\nmid l$, and $\wp\nmid x$ nor $\wp\nmid x^{-1}$. Then the following three statements are equivalent:*

(i) $\wp$ is completely split in $F_x=F(\zeta_q,\sqrt[q]{x})$

(ii) $N(\wp)\equiv 1(\mathrm{mod}\, q)$ and x is an q-th power in $\mathbb{Z}_F/\wp$

(iii) $x^{(N(\wp)-1)/q}\equiv 1\ (\mathrm{mod}\ \wp)$.

Proof

"(i)$\Rightarrow$ (ii)": Suppose that $\wp$ is completely split in F_x. Then $\wp$ must be completely split in $F(\zeta_q)$ which implies that the Frobenius automorphism of $\wp$ in $F(\zeta_q)/F$ is 1 i.e. $\sigma_\wp=(\wp,F(\zeta_q)/F)=1$.

Let p be the prime number contained in $\wp$ and $f=f(\wp/p)$ the residue class degree. Consider the following lattice of fields:

$$\begin{tikzcd}[column sep=small] & F(\zeta_q) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\zeta_q) \arrow[dr, dash] & & F \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

Then from the properties of the Artin symbol we know that: $(\wp,F(\zeta_q)/F)|_{\mathbb{Q}(\zeta_q)}=(p,\mathbb{Q}(\zeta_q)/\mathbb{Q})^f=\sigma_p^f$. But $\sigma_p^f=1 \iff \sigma_p^f(\zeta_q)=\zeta_q \iff \zeta_q^{p^f}=\zeta_q \iff p^f\equiv 1(\mathrm{mod}\ q)$. Notice that the necessary condition for the Artin symbol property, that p is unramified in $\mathbb{Q}(\zeta_q)$, would not be satisfied if $\wp\mid l$. Since l is the only prime that ramifies in $\mathbb{Q}(\zeta_q)$ it is sufficient that we exclude only $\wp$ dividing l.

It remains to prove that x is a q-th power in $\mathbb{Z}_F/\wp$. Let γ be a prime of $F(\zeta_q, \sqrt[q]{x})$ lying above $\wp$. Since $\wp$ is completely split in this field we have the following isomorphism between the residue class fields:

$$\mathbb{Z}_{F(\zeta_q,\, \sqrt[q]{x})}/\gamma \simeq \mathbb{Z}_F/\wp$$

Since we assumed that $\wp \nmid x$, we know that $\gamma \nmid x$, so that $x \not\equiv 0$ in $\mathbb{Z}_{F(\zeta_q,\, \sqrt[q]{x})}/\gamma$. Now x is obviously a q-th power in $\mathbb{Z}_{F(\zeta_q,\, \sqrt[q]{x})}/\gamma$ since we can write $x = (\sqrt[q]{x})^q$. The isomorphism from above then implies that x is a q-th power in $\mathbb{Z}_F/\wp$.

"(ii) $\Rightarrow$ (i)": Assume that $N(\wp) = p^f \equiv 1(\text{mod } q)$ and that x is a q-th power in $\mathbb{Z}_F/\wp$. We consider the following diagram:

$$\begin{array}{ccc}
F(\zeta_q, \sqrt[q]{x}) & & \gamma \\
\Big| & & \\
F(\zeta_q) & & \beta \\
\Big| & & \\
F & & \wp
\end{array}$$

where $\gamma \mid \beta$ and $\beta \mid \wp$. We have already seen that $p^f \equiv 1(\text{mod } q)$ if and only if $\wp$ is completely split in $F(\zeta_q)$. Therefore we know that $\wp$ is completely split in $F(\zeta_q)$ which gives us the isomorphism between the residue class fields:

$$\mathbb{Z}_{F(\zeta_q)}/\beta \simeq \mathbb{Z}_F/\wp$$

Next let $\hat{q}$ be the degree of the extension $F(\zeta_q, \sqrt[q]{x})/F(\zeta_q)$, where $\hat{q} \mid q$. Then $F(\zeta_q, \sqrt[q]{x}) = F(\zeta_q)[X]/(X^{\hat{q}} - x^{\hat{q}/q})$ [see theorem A.2]. Now x being an q-th power in $\mathbb{Z}_F/\wp$ implies that $X^q - x \equiv 0(\text{mod } \wp)$ has a solution in $\mathbb{Z}_F$, and we denote it with $x^{1/q}$. Then $x^{1/q}$ is also a solution for $X^{\hat{q}} - x^{\hat{q}/q} \equiv 0(\text{mod } \wp)$, hence $X^{\hat{q}} - x^{\hat{q}/q} \equiv 0(\text{mod } \wp)$ has a solution in $\mathbb{Z}_F$. The isomorphism from above now implies that $X^{\hat{q}} - x^{\hat{q}/q} \equiv 0(\text{mod } \beta)$ has a solution in $\mathbb{Z}_{F(\zeta_q)}$. The polynomial $f(X) = X^{\hat{q}} - x^{\hat{q}/q}$ is the monic minimal polynomial of $F(\zeta_q, \sqrt[q]{x})/F(\zeta_q)$, which is separable modulo β, hence the fact that $X^{\hat{q}} - x^{\hat{q}/q} \equiv 0(\text{mod } \beta)$ has a solution in $\mathbb{Z}_{F(\zeta_q)}$ implies that β is completely split in $F(\zeta_q, \sqrt[q]{x})$ [see proposition A.1]. Since we already know that $\wp$ splits completely in $F(\zeta_q)$ we can conclude that $\wp$ is completely split in $F(\zeta_q, \sqrt[q]{x})$.

"(ii) $\Rightarrow$ (iii)": We first notice that the equation in (iii) has meaning if and only if $\frac{p^f-1}{q} \in \mathbb{Z}$, that is if and only if $p^f \equiv 1(\text{mod } q)$. Now if x is a q-th power in $\mathbb{Z}_F/\wp$ then $x^{1/q} \in \mathbb{Z}_F/\wp$. We also know that $\alpha^{(p^f-1)} \equiv 1 \ (\text{mod } \wp)\ \forall \alpha \in \mathbb{Z}_F/\wp$ (because $\mathbb{Z}_F/\wp \cong \mathbb{F}_{p^f}$). It follows that $x^{(p^f-1)/q} \equiv 1 \ (\text{mod } \wp)$.

"(iii) $\Rightarrow$ (ii)": Suppose that $x^{(p^f-1)/q} \equiv 1 \pmod{\wp}$. The multiplicative group $(\mathbb{Z}_F/\wp)^*$ is isomorphic to $(\mathbb{F}_{p^f})^*$, and is thus cyclic. Therefore we can write $x \equiv \alpha^m (\text{mod } \wp)$, where $\langle\alpha\rangle = (\mathbb{Z}_F/\wp)^*$, and m an integer. Then $x^{(p^f-1)/q} \equiv \alpha^{m(p^f-1)/q} \equiv 1$ and because the order of α in the group $(\mathbb{Z}_F/\wp)^*$ is $p^f - 1$ we must have that $\frac{m}{q} \in \mathbb{Z}$ or equivalently that q divides m. Therefore x is a q-th power in $\mathbb{Z}_F/\wp$. $\square$

Lemma 1.4 *Let F be a number field and let p be a prime number. If $p = 2$, assume that $i \in F$. For each positive integer n we define $W_n = F^* \cap F(\zeta_{p^n})^{*p^n}$. Then the following holds:*

(i) $W_1 \supset W_2 \supset W_3 \supset ...$

(ii) $\cap_{n\geq 1} W_n = \{x \in F^* |$ order of x is finite and relatively prime to $p\}$

Proof (i) Let $a \in F^*$ and suppose that $a \in F(\zeta_{p^n})^{*p^n}$. Hence $a = b^{p^n}$ for some $b \in F(\zeta_{p^n})$. From lemma 1.2 we then know that there is a $\xi \in \mu_{p^n}$ such that $b \cdot \xi^{-1} \in F$ and $a = b^{p^n} = (b \cdot \xi^{-1})^{p^n}$. It follows that $a \in F^{*p^n}$, hence $W_n = F^{*p^n}$. It is now obvious that $W_{n+1} \subset W_n$.

(ii) Suppose that $a \in \cap_{n\geq 1} W_n$. Then, as we have seen above, a is trivial in $F(\zeta_{p^n})^*/F(\zeta_{p^n})^{*p^n}$ for all $n \geq 1$. By lemma 1.2 it follows that a is trivial in F^*/F^{*p^n} for all $n \geq 1$.

Next, let S be the set of primes F dividing a or a^{-1}, and let U_S denote the multiplicative group of S-units that is $U_S = \{\alpha \in F^* : |\alpha|_\wp = 1 \ \forall \wp \notin S\} = \{\alpha \in F^* : \wp|\alpha \text{ or } \wp|\alpha^{-1} \text{ then } \wp \in S\}$. Notice that $a \in U_S$. We claim that a is trivial in $U_S/U_S^{p^n}$ for all n. Consider the following inclusion diagram:

$$\begin{array}{ccc} F^{*p^n} & \subset & F^* \\ \cup & & \cup \\ U_S^{p^n} & \subset & U_S \end{array}$$

First we show that $U_S^{p^n} = U_S \cap F^{*p^n}$. Well it is obvious that $U_S^{p^n} \subset U_S \cap F^{*p^n}$. For the other inclusion take $t \in U_S \cap F^{*p^n}$. Then, since $t \in F^{*p^n}$, t is a p^n-th power of some non-zero element of F^*, say $t = r^{p^n}$. But $t \in U_S$ thus $|t|_\wp = |r^{p^n}|_\wp = |r|_\wp^{p^n} = 1 \ \forall \wp \notin S \implies |r|_\wp = 1 \ \forall \wp \notin S$ which means that $r \in U_S$ and thus $t = r^{p^n} \in U_S^{p^n}$. Now, $F^{*p^n} U_S / F^{*p^n}$ is a subgroup of F^*/F^{*p^n} and is isomorphic to $U_S/U_S^{p^n}$. Since a is trivial in F^*/F^{*p^n} and $a \in U_S$ we can conclude that a is trivial in $U_S/U_S^{p^n}$. This is true for all $n \geq 1$ so that $a \in \cap_{n\geq 1} U_S^{p^n}$. Since U_S is multiplicative group and finitely generated, we know from the Dirichlet Unit theorem [see appendix] that: $U_S \cong \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}^s$, for some positive integers k and s; here $\mathbb{Z}/k\mathbb{Z}$ is isomorphic to the group of roots of unity of F. It follows that

$$\begin{aligned} \cap_n U_S^{p^n} &\cong \cap_n p^n(\mathbb{Z}/k\mathbb{Z}) \times \underbrace{\cap_n p^n\mathbb{Z} \times ... \times \cap_n p^n\mathbb{Z}}_{s\,times} \\ &\cong \cap_n p^n(\mathbb{Z}/k\mathbb{Z}) \times 1_{U_S} \end{aligned}$$

Therefore a is in the torsion of $\cap_{n\geq 1} U_S^{p^n}$, hence a is a root of unity. Since the order of $p^n(\mathbb{Z}/k\mathbb{Z})$ is equal to $\frac{k}{\gcd(k,p^n)}$, we see that the order of a is relatively prime to p. $\square$

Chapter 2

Theorems

In this chapter we will prove theorems mentioned in the introduction. In the first section we prove our main theorem, and in section 2 we prove the generalization of it.

In the following we let $S_{K/k}$ denote the set of primes of a number field k, which are completely split in the finite extension K of k.

2.1 The Main Theorem

Theorem 2.1 *Let F be a number field and let $x, y \in F^*$. If for all prime numbers l and for all positive integers n, one has that for almost all primes $\wp$ of $S_{F(\zeta_{l^n})/F}$ the following holds:*

$$y^{\frac{N(\wp)-1}{l^n}} \equiv 1 (mod\, \wp) \text{ whenever } x^{\frac{N(\wp)-1}{l^n}} \equiv 1 (mod\, \wp)$$

then y is a power of x. For almost all here means for all but for a set of sup-density at most $\frac{l-2}{[F(i,\zeta_{l^n}, \sqrt[l^n]{x}, \sqrt[l^n]{y}):F]}$.

In the proof we deal with two extensions of F, namely $F(\zeta_{l^n}, \sqrt[l^n]{x})$ and $F(\zeta_{l^n}, \sqrt[l^n]{y})$. Sometimes we will denote these fields simply with F_x and F_y. We also write $F_{x,y}$ for the composite of F_x and F_y. Basically the proof is done in three steps. In the first step we use lemma 1.3 and a density argument to show that $F(\zeta_{l^n}, \sqrt[l^n]{y}) \subset F(\zeta_{l^n}, \sqrt[l^n]{x})$. In the second step the Kummer theory is used to conclude that $y = x^d$ in $F(\zeta_{l^n})^*/F(\zeta_{l^n})^{*l^n}$. From lemma 1.2 it then follows that $y = x^d$ in F^*/F^{*l^n}. In the last step we complete the proof.

Proof We first assume that $i \in F$. We do this because we will need to use lemma 1.2. Of course, after proving the theorem for this case we will show that there is no loss of generality due to this assumption, proving the theorem for any number field F. For each $q = l^n$ define T_q to be the set of primes of $S_{F(\zeta_q)/F}$ for which the condition of the theorem does not hold. Also, we define $\tilde{T}_q$ as the set of primes of F containing the infinite primes, those that occur in the factorization of x and y and the primes of the set T_q. Since the set $\tilde{T}_q - T_q$ is finite, it has density 0. Therefore the density of $\tilde{T}_q$ equals the density of T_q and by the assumption of the theorem it is less than $\frac{l-2}{[F(i,\zeta_q,\sqrt[q]{x},\sqrt[q]{y}):F]} = \frac{l-2}{[F(\zeta_q,\sqrt[q]{x},\sqrt[q]{y}):F]}$. The last equality follows from the fact that we assumed $i \in F$.

STEP 1. Let $\wp \in S_{F(\zeta_q)/F}$ with $\wp \notin \tilde{T}_q$; notice that $\wp \nmid x$, $\wp \nmid y$ and $\wp \nmid l$. We consider the following lattice of fields:

$$\begin{tikzcd}
 & F(\zeta_q,\sqrt[q]{x},\sqrt[q]{y}) \arrow[dl, dash] \arrow[dr, dash] & \\
F(\zeta_q,\sqrt[q]{x}) \arrow[dr, dash] & & F(\zeta_q,\sqrt[q]{y}) \arrow[dl, dash] \\
 & F(\zeta_q) \arrow[d, dash] & \\
 & F \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Lemma 1.3 now implies that

$$x^{\frac{N(\wp)-1}{q}} \equiv 1(\bmod \wp) \iff \wp \text{ is completely split in } F(\zeta_q,\sqrt[q]{x})$$

Let β be a prime of $F(\zeta_q)$ lying above $\wp$. Then since we know that $\wp$ is completely split in $F(\zeta_q)$, we have the following equivalences: $\wp$ is completely split in $F_x \iff \beta$ is completely split in $F(\zeta_q,\sqrt[q]{x}) \iff (\beta, F(\zeta_q,\sqrt[q]{x})/F(\zeta_q)) = 1 \iff \mathrm{Frob}_\beta^{F_{x,y}/F(\zeta_q)} \in H_x = \mathrm{Gal}(F_{x,y}/F_x)$. The same is true for the field F_y and the group $H_y = \mathrm{Gal}(F_{x,y}/F_y)$. This way the condition of the theorem becomes equivalent to the following

$$\mathrm{Frob}_\beta \in H_x \implies \mathrm{Frob}_\beta \in H_y \tag{2.1}$$

Now if H_x is trivial then (2.1) isn't very useful, but then we already know that $F_{x,y} = F_x$, hence $F_y \subset F_x$. Suppose now that H_x is not empty, and let q_x denote its order, which is a power of the prime number l. We also need to know for which primes β the implication in (2.1) holds. For this matter, let $\tilde{T}'_q$ be the set of primes of $F(\zeta_q)$ lying above the primes of $\tilde{T}_q$, and let S denote the set of primes of $F(\zeta_q)$ lying above the primes of $S_{F(\zeta_q)/F}$. Then (2.1) holds for all $\beta \in S$ with $\beta \notin \tilde{T}'_q$. Furthermore with Chebotarev Density Theorem we know that

$\Delta(S_{F(\zeta_q)/F}) = \delta(S_{F(\zeta_q)/F}) = \frac{1}{[F(\zeta_q):F]}$. Lemma 1.1 then implies that $\Delta(S) = 1$. The same lemma also implies that $\Delta(\tilde{T}'_q) \leq [F(\zeta_q) : F] \cdot \Delta(\tilde{T}'_q) \leq \frac{l-2}{[F_{x,y}:F(\zeta_q)]}$. We conclude that (2.1) holds for all primes β of $F(\zeta_q)$ except for a set of sup-density at most $\frac{l-2}{[F_{x,y}:F(\zeta_q)]}$. Theorem 1.1 now implies that 2.1 does not hold for at most $l-2$ different $\mathrm{Frob}_\beta \in G = \mathrm{Gal}(F_{x,y}/F(\zeta_q))$. Now even if all of these Frob_β's are in H_x then there are still at least $q_x - (l-2)$ different elements in H_x for which (2.1) does hold. Let ϕ denote the Euler function, then $q_x - (l-2) \geq q_x - (\phi(q_x) - 1)$. Therefore at least $q_x - \phi(q_x) + 1$ elements of H_x are also in H_y. Hence at least one of these elements is a generator of H_x. Therefore $H_x \subset H_y$, and thus

$$F(\zeta_q, \sqrt[q]{y}) \subset F(\zeta_q, \sqrt[q]{x}) \tag{2.2}$$

STEP 2. Let $W_x = \langle F(\zeta_q)^{*q}, x\rangle$ and $W_y = \langle F(\zeta_q)^{*q}, y\rangle$. With the Kummer theory and (2.2) it follows that $W_y \subset W_x$. Therefore $\langle y\rangle = W_y/F(\zeta_q)^{*q} \subset W_x/F(\zeta_q)^{*q} = \langle x\rangle$, i.e. $y = x^d$ in $W_x/F(\zeta_q)^{*q}$, for some integer d. Since $W_x \subset F(\zeta_q)^*$ and thus $W_x/F(\zeta_q)^{*q} \subset F(\zeta_q)^*/F(\zeta_q)^{*q}$ we see that $y = x^d$ in $F(\zeta_q)^*/F(\zeta_q)^{*q}$. From lemma 1.2 it then follows that $y = x^d$ in F^*/F^{*q}.

STEP 3. In the last step of the proof we again need to define a set of primes of F. Here it is sufficient to define T as the set of those primes which occur in the factorization of x and y. Let U_T denote the multiplicative group of T-units that is $U_T = \{\alpha \in F^* : \ |\alpha|_\wp = 1 \ \forall \wp \ \notin T\} = \{\alpha \in F^* : \ \wp \mid \alpha \text{ or } \wp \mid \alpha^{-1} \text{ then } \wp \in T\}$. Notice that $x, y \in U_T$.

We want to show that $y = x^d$ in U_T/U_T^q. Consider the following inclusion diagram:

$$\begin{array}{ccc} F^{*q} & \subset & F^* \\ \cup & & \cup \\ U_T^q & \subset & U_T \end{array}$$

In the proof of lemma 1.4 we have seen that $U_T^q = U_T \cap F^{*q}$. Furthermore $F^{*q}U_T/F^{*q}$ is a subgroup of F^*/F^{*q} which is isomorphic to U_T/U_T^q. Since we have showed that $y = x^d$ in F^*/F^{*q} and because $x, y \in U_T$ we can conclude that $y = x^d$ in U_T/U_T^q.

Next we define $A = U_T/\langle x\rangle$. Then

$$\begin{aligned} A/A^q &= (U_T/\langle x\rangle)/(U_T^q/(U_T^q \cap \langle x\rangle)) \\ &\cong (U_T/\langle x\rangle)/(\langle U_T^q, x\rangle/\langle x\rangle) \\ &\cong U_T/\langle U_T^q, x\rangle \\ &\cong (U_T/U_T^q)/(\langle U_T^q, x\rangle/U_T^q) \\ &= (U_T/U_T^q)/\langle \bar{x}\rangle \end{aligned}$$

where $\bar{x} \equiv x (\mathrm{mod}\ U_T^q)$. This gives us an isomorphism: $\psi : (U_T/U_T^q)/\langle \bar{x}\rangle \longrightarrow A/A^q$. Since $y = x^d$ in U_T/U_T^q, and thus is trivial in $(U_T/U_T^q)/\langle \bar{x}\rangle$, it's image by ψ is in A^q. This is true for all prime powers q so that the image of y in A is in $\cap_q A^q$.

It remains to show that $\cap_q A^q$ is trivial. Well, A is a multiplicative group and since T is finite, A is finitely generated. Therefore A is isomorphic to a direct product of cyclic groups: $A \cong \mathbb{Z}/k_1\mathbb{Z} \times \cdots \times \mathbb{Z}/k_r\mathbb{Z} \times \mathbb{Z}^s$. We see that:

$$\cap_q A^q \cong \cap_q q(\mathbb{Z}/k_1\mathbb{Z}) \times \cdots \times \cap_q q(\mathbb{Z}/k_r\mathbb{Z}) \times \underbrace{\cap_q q\mathbb{Z} \times \ldots \times \cap_q q\mathbb{Z}}_{s\ times} = 0$$

Since the image of y in A was in $\cap_q A^q$ we see that y is trivial in A i.e. $y = x^d$ for some $d \in \mathbb{Z}$. This proves the theorem for a field F with $i \in F$.

Let us now look at a number field F with $i \notin F$. Let $x, y \in F^*$ and let T_q be the set of primes of F for which the condition of the theorem does not hold. We still assume that the density of T_q is at most $\frac{l-2}{[F_{x,y}(i):F]}$. Let T_q' be the set of primes of $F(i)$ for which the condition of the theorem does not hold. We claim that T_q' is exactly the set of primes lying above the primes of T_q. To prove this we show that for a prime $\wp$ of $S_{F(\zeta_q)/F}$ the condition

$$y^{\frac{N(\wp)-1}{q}} \equiv 1 (\text{mod } \wp) \text{ whenever } x^{\frac{N(\wp)-1}{q}} \equiv 1 (\text{mod } \wp)$$

holds if and only if the condition

$$y^{\frac{N(\beta)-1}{q}} \equiv 1 (\text{mod } \beta) \text{ whenever } x^{\frac{N(\beta)-1}{q}} \equiv 1 (\text{mod } \beta)$$

holds for every prime $\beta \in F(i)$ lying above $\wp$. It is sufficient to show that for $a = x, y$ we have

$$a^{\frac{N(\wp)-1}{q}} \equiv 1 (\text{mod } \wp) \iff a^{\frac{N(\beta)-1}{q}} \equiv 1 (\text{mod } \beta) \qquad (2.3)$$

First we notice that since $\beta \mid \wp$ the diagram bellow commutes

$$\begin{array}{ccc} \mathbb{Z}_{F(i)} & \to & \mathbb{Z}_{F(i)}/\beta \\ \uparrow & & \uparrow \\ \mathbb{Z}_F & \to & \mathbb{Z}_F/\wp \end{array}$$

which implies that $a^n \equiv 1 (\text{mod } \wp) \iff a^n \equiv 1 (\text{mod } \beta)$, for all $n \in \mathbb{Z}_{>0}$.

We now need to separate two cases:
1) <u>q is a power of 2</u>: Notice that leaving $q = 2$ out does not change the intersection $\cap_q A^q$. We can therefore take $q \geq 4$ so that $F(i) \subset F(\zeta_q)$ and since $\wp$ is completely split in $F(\zeta_q)$, $\wp$ is completely split in $F(i)$. Hence $N(\beta) = N(\wp)$ and (2.3) follows.

2) <u>q is power of an odd prime</u>: Now if $N(\beta) = N(\wp)$ we are done. Otherwise, $N(\beta) = N(\wp)^2$ and we consider the following lattice of fields:

$$
\begin{tikzcd}
\mathcal{P} \in & & F(i,\zeta_q,\sqrt[q]{x}) \arrow[dl, dash] \arrow[dr, dash] & & \\
\gamma \in & F(\zeta_q,\sqrt[q]{x}) \arrow[d, dash] & & F(i,\zeta_q) \arrow[d, dash] & \\
\delta \in & F(\zeta_q) \arrow[dr, dash] & & F(i) \arrow[dl, dash] & \ni \beta \\
& & F & &
\end{tikzcd}
$$

Let $\mathcal{P}$, γ and δ be the primes of $F(i,\zeta_q,\sqrt[q]{x}), F(\zeta_q,\sqrt[q]{x})$ and $F(\zeta_q)$ respectively, such that $\mathcal{P} \mid \gamma \mid \delta \mid \wp$. Then

$$
\begin{aligned}
f(\mathcal{P}/\wp) &= f(\mathcal{P}/\gamma)f(\gamma/\wp) = f(\mathcal{P}/\gamma)f(\gamma/\delta) \\
&= f(\mathcal{P}/\beta)f(\beta/\wp) = 2\cdot f(\mathcal{P}/\beta)
\end{aligned}
$$

Suppose that $a^{\frac{N(\wp)-1}{q}} \equiv 1 (\mathrm{mod}\ \wp)$. Then by lemma 1.3 $\wp$ is completely split in $F(\zeta_q,\sqrt[q]{x})$. It follows that $f(\gamma/\wp)=1$, and thus $f(\mathcal{P}/\gamma) = 2\cdot f(\mathcal{P}/\beta)$. Since $f(\mathcal{P}/\gamma)$ is at most 2 it follows that $f(\mathcal{P}/\beta)=1$, i.e. β is completely split in $F(i,\zeta_q,\sqrt[q]{x})$. Hence, by lemma 1.3, $a^{\frac{N(\beta)-1}{q}} \equiv 1 (\mathrm{mod}\ \beta)$.
Now suppose that $a^{\frac{N(\beta)-1}{q}} \equiv 1 (\mathrm{mod}\ \beta)$, thus β is completely split in $F(i,\zeta_q,\sqrt[q]{x})$. Then $f(\mathcal{P}/\wp) = f(\mathcal{P}/\gamma)f(\gamma/\delta) = 2$. Now $f(\gamma/\delta)$ can not be equal to 2 because $[F(\zeta_q,\sqrt[q]{x}) : F(\zeta_q)]$ is odd. Therefore $f(\mathcal{P}/\gamma)=2$ and $f(\gamma/\delta)=1$. Hence $\wp$ is completely split in $F(\zeta_q,\sqrt[q]{x})$ and thus $a^{\frac{N(\wp)-1}{q}} \equiv 1 (\mathrm{mod}\ \wp)$. This proves our claim.

Furthermore, by lemma 1.1 it follows that $\Delta(T'_q) \le 2\cdot\Delta(T_q) = \frac{l-2}{[F_{x,y}(i):F(i)]}$. We can now use theorem 2.1 for $x,y\in F(i)$ to conclude that y is a power of x in $F(i)$. Since $x,y\in F$ then certainly y is a power of x in F. This completes the proof of our theorem. $\square$

2.2 A Generalization

In this section we prove the following theorem, which is a generalization of our main theorem

Theorem 2.2 *Let F be a number field and let $x, y \in F^*$. Let l be a prime number and m and m' two integers. Then the implication:*

$$\text{order of } x^{\frac{N(\wp)-1}{l^n}} \text{ in } (\mathbb{Z}_F/\wp)^* \text{ is } l^m \implies \text{order of } y^{\frac{N(\wp)-1}{l^n}} \text{ in } (\mathbb{Z}_F/\wp)^* \text{ is } l^{m'}$$

holds for all positive integers n and for almost all primes $\wp \in S_{F(\zeta_{l^n})/F}$, if and only if either x is a root of unity of order not divisible by l^m, or there are integers a and $b > 0$ with $gcd(l, ab) = 1$, such that $y^{l^{m'-1}b} = x^{l^{m-1}a}$. Almost all here means all but a set of sup-density at most $\frac{l-2}{[F(\zeta_{l^n}, \sqrt[l^n]{x^{l^{m-1}}}, \sqrt[l^n]{y^{l^{m'-1}}}):F]}$

Basically the proof is done in the same manner as the previous one, and we will occasionally refer to it. Some steps will require a bit more effort. We will now need more than just two extensions of F. Namely, we will consider the following extensions: $F_x = F(\zeta_{l^n}, \sqrt[l^n]{x^{l^{m-1}}})$, $F_y = F(\zeta_{l^n}, \sqrt[l^n]{y^{l^{m'-1}}})$, $F_{x^l} = F(\zeta_{l^n}, \sqrt[l^n]{x^{l^m}})$ and $F_{y^l} = F(\zeta_{l^n}, \sqrt[l^n]{y^{l^{m'}}})$. Again we let $F_{x,y}$ denote the composite of F_x and F_y.

Proof "$\Leftarrow$" If x is a root of unity, say $x = \zeta_w$, with $l^m \nmid w$ then the order of $x^{\frac{N(\wp)-1}{l^n}}$ in $(\mathbb{Z}_F/\wp)^*$ is never l^m, hence the implication of the theorem always holds. Otherwise, if $y^{bl^{m'-1}} = x^{al^{m-1}}$ for some integers a and b with $\gcd(l, ab) = 1$ then: the order of $x^{\frac{N(\wp)-1}{l^n}}$ in $(\mathbb{Z}_F/\wp)^*$ is l^m $\iff$ the order of $x^{l^{m-1}\frac{N(\wp)-1}{l^n}}$ in $(\mathbb{Z}_F/\wp)^*$ is $l \implies$ the order of $x^{l^{m-1}a\frac{N(\wp)-1}{l^n}}$ in $(\mathbb{Z}_F/\wp)^*$ is l, where the last implication holds because $l \nmid a$. But $x^{l^{m-1}a\frac{N(\wp)-1}{l^n}} = y^{l^{m'-1}b\frac{N(\wp)-1}{l^n}}$, hence the order of $y^{l^{m'-1}b\frac{N(\wp)-1}{l^n}}$ in $(\mathbb{Z}_F/\wp)^*$ is l which again implies that the order of $y^{l^{m'-1}\frac{N(\wp)-1}{l^n}}$ in $(\mathbb{Z}_F/\wp)^*$ is l. But then the order of $y^{\frac{N(\wp)-1}{l^n}}$ in $(\mathbb{Z}_F/\wp)^*$ is $l^{m'}$.

"$\Rightarrow$" As before we will need to use lemma 1.2, therefore for $l = 2$ we assume that $i \in F$. After proving the theorem for this case we will of course show that theorem also holds for a field which does not contain i. For each n we define T_n to be the set of primes of $S_{F(\zeta_{l^n})/F}$ for which the condition of the theorem does not hold. Also we define $\tilde{T}_n$ as the set of primes of F containing the infinite primes, those that divide x or y, and the primes of the set T_n. As before we see that the density of $\tilde{T}_n$ equals the density of T_n and by the assumption of the theorem it is less than $\frac{l-2}{[F_{x,y}:F]}$.

STEP 1. Let $\wp \in S_{F(\zeta_{l^n})/F}$ with $\wp \notin T_n$, hence $\wp \nmid x$, $\wp \nmid x^{-1}$, $\wp \nmid y$, $\wp \nmid y^{-1}$ and $\wp \nmid l$. We consider the following lattice of fields:

$$\begin{tikzcd}[column sep=small]
 & F(\zeta_{l^n},\, \sqrt[l^n]{x^{l^{m-1}}},\, \sqrt[l^n]{y^{l^{m'-1}}}) \arrow[dl, dash] \arrow[dr, dash] & & \\
F(\zeta_{l^n},\, \sqrt[l^n]{x^{l^{m-1}}}) \arrow[d, dash] & & F(\zeta_{l^n},\, \sqrt[l^n]{y^{l^{m'-1}}}) \arrow[d, dash] & \\
F(\zeta_{l^n},\, \sqrt[l^n]{x^{l^{m}}}) \arrow[dr, dash] & & F(\zeta_{l^n},\, \sqrt[l^n]{y^{l^{m'}}}) \arrow[dl, dash] & \\
 & F(\zeta_{l^n}) \arrow[d, dash] & & \\
 & F \arrow[d, dash] & & \ni \wp \\
 & \mathbb{Q} & & \ni p
\end{tikzcd}$$

We first notice that for all integers $r > 0$ we have

$$\text{order of } x^r \text{ in } (\mathbb{Z}_F/\wp)^* \text{ is } l^m \iff x^{rl^m} \equiv 1 (\bmod\ \wp) \text{ and } x^{rl^{m-1}} \not\equiv 1 (\bmod\ \wp)$$

Using this and lemma 1.3 we see that:

$$\text{order of } x^{\frac{N(\wp)-1}{l^n}} \text{ in } (\mathbb{Z}_F/\wp)^* \text{ is } l^m \iff \begin{array}{l} \wp \text{ is completely split in } F(\zeta_{l^n},\, \sqrt[l^n]{x^{l^m}}) \text{ and} \\ \wp \text{ is not completely split in } F(\zeta_{l^n},\, \sqrt[l^n]{x^{l^{m-1}}}) \end{array}$$

Next let β be a prime in $F(\zeta_{l^n})$ which is above $\wp$, and let $H_x = \mathrm{Gal}(F_{x,y}/F_{x^l})$ and $H'_x = \mathrm{Gal}(F_{x,y}/F_x)$. Then, since $\wp$ is completely split in $F(\zeta_{l^n})$, we have the following equivalences:

$$\begin{array}{c}
\wp \text{ is completely split in } F(\zeta_{l^n},\, \sqrt[l^n]{x^{l^m}}) \text{ and} \\
\wp \text{ is not completely split in } F(\zeta_{l^n},\, \sqrt[l^n]{x^{l^{m-1}}}) \\
\Updownarrow \\
\beta \text{ is completely split in } F(\zeta_{l^n},\, \sqrt[l^n]{x^{l^m}}) \text{ and} \\
\beta \text{ is not completely split in } F(\zeta_{l^n},\, \sqrt[l^n]{x^{l^{m-1}}}) \\
\Updownarrow \\
(\beta, F(\zeta_{l^n},\, \sqrt[l^n]{x^{l^m}})/F(\zeta_{l^n})) = 1 \\
\text{and } (\beta, F(\zeta_{l^n},\, \sqrt[l^n]{x^{l^{m-1}}})/F(\zeta_{l^n})) \neq 1 \\
\Updownarrow \\
\mathrm{Frob}_\beta^{F_{x,y}/F(\zeta_{l^n})} \in H_x \text{ and} \\
\mathrm{Frob}_\beta^{F_{x,y}/F(\zeta_{l^n})} \notin H'_x
\end{array}$$

The same equivalences are true for the fields F_y and F_{y^l}, and the groups $H_y = \mathrm{Gal}(F_{x,y}/F_{y^l})$ and $H_y' = \mathrm{Gal}(F_{x,y}/F_y)$. We see that the condition in the theorem is equivalent to the following:

$$\mathrm{Frob}_\beta \in H_x \backslash H_x' \Longrightarrow \mathrm{Frob}_\beta \in H_y \backslash H_y' \tag{2.4}$$

Now it can happen that $H_x \backslash H_x'$ is empty for all integers n. If this is the case then we can not deduce much from (2.4). But we then have $F(\zeta_{l^n}, \sqrt[l^n]{x^{l^m}}) = F(\zeta_{l^n}, \sqrt[l^n]{x^{l^{m-1}}})$ for all n. When $F(\zeta_{l^n}, \sqrt[l^n]{x^{l^m}}) = F(\zeta_{l^n}, \sqrt[l^n]{x^{l^{m-1}}})$, then since F_x and F_{x^l} are cyclic extensions of $F(\zeta_{l^n})$, we know from Kummer theory [see appendix] that these extensions are of the same degree if and only if they are trivial. Hence $F(\zeta_{l^n}, \sqrt[l^n]{x^{l^{m-1}}}) = F(\zeta_{l^n})$, so that $x^{l^{m-1}} \in F(\zeta_{l^n})^{*l^n}$. This is true for all n so that $x^{l^{m-1}} \in \cap_{n \geq 1} F(\zeta_{l^n})^{l^n}$, and by lemma 1.4 it then follows that $x^{l^{m-1}} \in \mu_k$ with $\gcd(k,l) = 1$. Therefore x is a root of unity of order not divisible by l^m. This gives us one case of "$\Rightarrow$".

Furthermore if $H_y \backslash H_y'$ is empty for all n and (2.4) is true, then $H_x \backslash H_x'$ must be empty for all n. But then both $x^{l^{m-1}}$ and $y^{l^{m'-1}}$ are roots of unity of order not divisible by l, say $x^{l^{m-1}} = \zeta_a$ and $y^{l^{m'-1}} = \zeta_b$ with $\gcd(l, ab) = 1$. Then obviously $x^{l^{m-1}a} = 1 = y^{l^{m'-1}b}$.

We now assume that both $H_x \backslash H_x'$ and $H_y \backslash H_y'$ are not always empty. Let N be the smallest integer for which both $H_x \backslash H_x'$ and $H_y \backslash H_y'$ are not empty, thus $[F(\zeta_{l^N}, \sqrt[l^N]{x^{l^{m-1}}}) : F(\zeta_{l^N}, \sqrt[l^N]{x^{l^m}})] = [F(\zeta_{l^N}, \sqrt[l^N]{y^{l^{m'-1}}}) : F(\zeta_{l^N}, \sqrt[l^N]{y^{l^{m'}}})] = l$. Then $x^{l^{m-1}}$ and $y^{l^{m'-1}}$ are not (l^N)-th powers in $F(\zeta_{l^N})$. Lemma 1.4 now implies that for all $n > N$, $x^{l^{m-1}}$ and $y^{l^{m'-1}}$ are not (l^n)-th powers in $F(\zeta_{l^n})$. Therefore for all $n \geq N$ we have that $[F(\zeta_{l^n}, \sqrt[l^n]{x^{l^{m-1}}}) : F(\zeta_{l^n}, \sqrt[l^n]{x^{l^m}})] = [F(\zeta_{l^n}, \sqrt[l^n]{y^{l^{m'-1}}}) : F(\zeta_{l^n}, \sqrt[l^n]{y^{l^{m'}}})] = l$, and $H_x \backslash H_x'$ and $H_y \backslash H_y'$ are not empty.

From now on we consider only $n \geq N$. Let $\tilde{T}_n'$ be the set of primes in $F(\zeta_{l^n})$ which are above the primes of $\tilde{T}_n$. Then (2.4) is true for all primes β which are completely split in the extension $F(\zeta_q)/F$ and are not in $\tilde{T}_n'$. Just as in the proof of the previous theorem we can deduce that the sup-density of the set of primes of $F(\zeta)$, for which (2.4) does not hold, is equal to the sup-density of the set $\tilde{T}_n'$. Lemma 1.1 implies that $\Delta(\tilde{T}_n') \leq [F(\zeta_{l^n}) : F] \cdot \Delta(\tilde{T}_n) \leq \frac{l-2}{[F_{xy} : F(\zeta_{l^n})]}$. Theorem 1.1 now tells us that (2.4) does not hold for at most $(l-2)$ different $\mathrm{Frob}_\beta \in G = \mathrm{Gal}(F_{xy}/F(\zeta_q))$. In other words,

$$H_x \backslash H_x' \subset H_y \backslash H_y' \cup S \text{ with } |S| \leq l-2 \tag{2.5}$$

If we let $q_x = |H_x'|$ and $q_y = |H_y'|$, then $|H_x \backslash H_x'| = q_x(l-1)$ and $|H_y \backslash H_y'| = q_y(l-1)$. The inclusion in (2.5) then implies that $q_x \leq q_y$. We now need to separate two cases, namely H_x is cyclic or not.

1) Let H_x be cyclic. Then every element of H_x/H_x' is a generator of H_x. From

(2.5) we know that at least one of these generators is in $H_y/H_y' \subset H_y$. It follows that $H_x \subset H_y$ and thus $H_x' = H_x^l \subset H_y^l = H_y'$. Hence $F_y \subset F_x$.

2) Suppose now that H_x is not cyclic, and that $q_y \neq 1$. Then $H_y = \langle \sigma_y, \tau_y \rangle$, $H_y' = \langle \sigma_y \rangle$, $H_x = \langle \sigma_x, \tau_x \rangle$ and $H_x' = \langle \sigma_x \rangle$. Here

$$\begin{array}{ll} \sigma_y : \sqrt[l^n]{x^{l^{m-1}}} \to \zeta_{q_y} \sqrt[l^n]{x^{l^{m-1}}} & \text{and} \quad \sigma_y \quad \text{is identity on} \quad \sqrt[l^n]{y^{l^{m'-1}}} \\ \tau_y : \sqrt[l^n]{y^{l^{m'}}} \to \zeta_l \sqrt[l^n]{y^{l^{m'}}} & \text{and } \tau_y^l = id \\ \sigma_x : \sqrt[l^n]{y^{l^{m'-1}}} \to \zeta_{q_x} \sqrt[l^n]{y^{l^{m'-1}}} & \text{and} \quad \sigma_x \quad \text{is identity on} \quad \sqrt[l^n]{x^{l^{m-1}}} \\ \tau_x : \sqrt[l^n]{x^{l^m}} \to \zeta_l \sqrt[l^n]{x^{l^m}} & \text{and } \tau_x^l = id \end{array}$$

Now $\tau_x = \tau_y$ or $\tau_x = \sigma_y^{q_y/l}\sigma_x^{q_x/l}$ or $\tau_x = \sigma_y^{q_y/l}$ depending on whether τ_x is identity on $\sqrt[l^n]{y^{l^{m'-1}}}$ or not, and whether τ_y is identity on $\sqrt[l^n]{x^{l^{m-1}}}$ or not. In the first case we thus have $\tau_x = \tau_y = \tau$, hence by (2.5), there is an integer $j \in \{1, ..., q_y\}$ such that $\tau\sigma_x = \tau\sigma_y^j$. But we know that for all j, $\sigma_x \neq \sigma_y^j$, hence we can not have $\tau_x = \tau_y$. In the other two cases we have $H_x = \langle \sigma_x, \sigma_y^{q_y/l} \rangle$. This implies that $X = \{(\sigma_y^{q_y/l})^i | \; i = 1...(l-1)\} \subset H_x \backslash H_x'$. Since X has $l-1$ elements, (2.5) now tells us that at least one of the elements of X must lie in $H_y \backslash H_y'$. But $X \subset \langle \sigma_y \rangle = H_y'$, hence we have reached a contradiction. Therefore $q_y = 1$ and since $q_x \leq q_y$ we see that $q_x = q_y = 1$. Hence $F_x = F_y$. In both cases we can conclude that

$$F(\zeta_q, \sqrt[q]{y^{l^{m'-1}}}) \subset F(\zeta_q, \sqrt[q]{x^{l^{m-1}}}) \tag{2.6}$$

STEP 2. We write $\hat{x} = x^{l^{m-1}}$ and $\hat{y} = y^{l^{m'-1}}$. Define $W_{\hat{x}} = \langle F(\zeta_{l^n})^{*l^n}, \hat{x} \rangle$ and $W_{\hat{y}} = \langle F(\zeta_{l^n})^{*l^n}, \hat{y} \rangle$. With the Kummer theory and (2.6) it follows that $W_{\hat{y}} \subset W_{\hat{x}}$. Therefore $\langle \hat{y} \rangle = W_{\hat{y}}/F(\zeta_{l^n})^{*l^n} \subset W_{\hat{x}}/F(\zeta_{l^n})^{*l^n} = \langle \hat{x} \rangle$, i.e., $\hat{y} = \hat{x}^d$ in $W_{\hat{x}}/F(\zeta_{l^n})^{*l^n}$, for some integer d. Since $W_{\hat{x}} \subset F(\zeta_{l^n})^*$ and thus $W_{\hat{x}}/F(\zeta_{l^n})^{*l^n} \subset F(\zeta_{l^n})^*/F(\zeta_{l^n})^{*l^n}$ we see that $y^{l^{m'-1}} = x^{l^{m-1}d}$ in $F(\zeta_{l^n})^*/F(\zeta_{l^n})^{*l^n}$. From lemma 1.2 it then follows that $y^{l^{m'-1}} = x^{l^{m-1}d}$ in F^*/F^{*l^n}.

STEP 3. From the previous step we know that $\hat{y} = \hat{x}^d$ in F^*/F^{*l^n} for some integer d. We define the set T to be the set of those primes which divide $\hat{x}$ or $\hat{y}$. We let U_T be the multiplicative group of T-units and define $A = U_T/\langle \hat{x} \rangle$. Then following the same argument as in the proof of the main theorem we deduce that $\hat{y} = \hat{x}^d$ in $U_T/U_T^{l^n}$ and we have the following isomorphism:

$$\psi : (U_T/U_T^{l^n})/\langle \bar{\hat{x}} \rangle \longrightarrow A/A^{l^n}$$

Since $\hat{y} = \hat{x}^d$ in $U_T/U_T^{l^n}$, and thus is trivial in $(U_T/U_T^{l^n})/\langle \bar{\hat{x}} \rangle$, it's image by ψ is in A^{l^n}. This is true for all $n \geq N$, so that the image of $\hat{y}$ in A is in $\cap_{n \geq N} A^{l^n}$.

Now again we have:

$$\begin{aligned}\cap_{n\geq N}A^{l^n} &\cong \cap_{n\geq N}l^n(\mathbb{Z}/k_1\mathbb{Z})\times\cdots\times\cap_{n\geq N}l^n(\mathbb{Z}/k_r\mathbb{Z})\times\underbrace{\cap_{l^n}l^n\mathbb{Z}\times\ldots\times\cap_{l^n}l^n\mathbb{Z}}_{s\ times}\\ &\cong \cap_{n\geq N}l^n(\mathbb{Z}/k_1\mathbb{Z})\times\cdots\times\cap_{n\geq N}l^n(\mathbb{Z}/k_r\mathbb{Z})\times 0\end{aligned}$$

so that the image of $\hat{y}$ in A is in the torsion of $\cap_{n\geq N}A^{l^n}$, i.e., $\psi(\hat{y})^b=\psi(y^{l^{m'-1}b})=1_A$ for some $b\in\mathbb{N}\implies y^{l^{m'-1}b}\in\langle\hat{x}\rangle=\langle x^{l^{m-1}}\rangle$. Since the order of $l^n(\mathbb{Z}/k_i\mathbb{Z})$ is equal to $\frac{k_i}{\gcd(k_i,l^n)}$, we see that b is not divisible by l. We conclude that:

$$y^{l^{m'-1}b}=x^{l^{m-1}a}\text{ for some }a,b\in\mathbb{Z},\text{ with }b>0\text{ and }l\nmid b$$

To show that $l\nmid a$ we will go back to the condition of the theorem. The assumption we made that $H_x\backslash H'_x$ isn't always empty implies that there is an integer $n\geq m$ and a prime $\wp\in S_{F(\zeta_{l^n})/F}$ for which the order of $x^{\frac{N(\wp)-1}{l^n}}$ in $(\mathbb{Z}_F/\wp)^*$ is l^m. By the condition of the theorem we also have that the order of $y^{\frac{N(\wp)-1}{l^n}}$ in $(\mathbb{Z}_F/\wp)^*$ is $l^{m'}$. But then the order of $y^{l^{m'-1}b\frac{N(\wp)-1}{l^n}}$ in $(\mathbb{Z}_F/\wp)^*$ is l and it is equal to the order of $x^{l^{m-1}a\frac{N(\wp)-1}{l^n}}$, hence a can not be divisible by l.

Let us now look at the case when $l=2$ and $i\notin F$. For each $q=2^n$ let T_q be the set of primes of F for which the condition of the theorem does not hold. We still assume that the density of T_q is at most $\frac{l-2}{[F_{x,y}:F]}$. Also, let T'_q be the set of primes of $F(i)$ for which the condition of the theorem does not hold. We claim that T'_q is exactly the set of primes lying above the primes of T'_q. To prove this we need to show that for a $\wp\in S_{F(\zeta_q)/F}$ the condition

$$\text{order of }x^{\frac{N(\wp)-1}{q}}\text{ in }(\mathbb{Z}_F/\wp)^*\text{ is }l^m\implies\text{order of }y^{\frac{N(\wp)-1}{q}}\text{ in }(\mathbb{Z}_F/\wp)^*\text{ is }l^{m'}$$

holds if and and only if

$$\text{order of }x^{\frac{N(\beta)-1}{q}}\text{ in }(\mathbb{Z}_{F(i)}/\beta)^*\text{ is }l^m\implies\text{order of }y^{\frac{N(\beta)-1}{q}}\text{ in }(\mathbb{Z}_{F(i)}/\beta)^*\text{ is }l^{m'}$$

holds for every prime $\beta\in F(i)$ lying above $\wp$. In the previous section we have already seen that for $a=x,y$ and for $q=l^n$ we have

$$a^{\frac{N(\wp)-1}{q}}\equiv 1(\text{mod }\wp)\iff a^{\frac{N(\beta)-1}{q}}\equiv 1(\text{mod }\beta)$$

for all $\beta\mid\wp$. Then for $M\leq n$

$$\left(\begin{array}{c}a^{\frac{N(\wp)-1}{q}l^M}\equiv 1(\text{mod }\wp)\text{ and}\\ a^{\frac{N(\wp)-1}{q}l^{M-1}}\not\equiv 1(\text{mod }\wp)\end{array}\right)\iff\left(\begin{array}{c}a^{\frac{N(\beta)-1}{q}l^M}\equiv 1(\text{mod }\beta)\text{ and}\\ a^{\frac{N(\beta)-1}{q}l^{M-1}}\not\equiv 1(\text{mod }\beta)\end{array}\right)$$

or equivalently

$$\text{order of }a^{\frac{N(\wp)-1}{q}}\text{ in }(\mathbb{Z}_F/\wp)^*\text{ is }l^M\iff\text{order of }a^{\frac{N(\beta)-1}{q}}\text{ in }(\mathbb{Z}_{F(i)}/\beta)^*\text{ is }l^M$$

holds for all $\beta \mid \wp$. This proves our claim.

Next, just as in the previous proof we notice that the intersection $\cap_n A^{2^n}$ does not change if we leave $n = 2$ out. We then have that $i \in F(\zeta_q)$ and by lemma 1.1 it follows that

$$\Delta(T_q') \leq \frac{l-2}{[F_{x,y} : F(i)]}$$

We can now use theorem 2.2 to conclude that $y^{l^{m'-1}b} = x^{l^{m-1}a}$ in $F(i)$, for some $a, b \in \mathbb{Z}$, with $b > 0$ and $l \nmid ab$. Since $x, y \in F^*$ it follows that $y^{l^{m'-1}b} = x^{l^{m-1}a}$ in F. $\square$

Appendix A

Appendix

In this appendix, we summarize the basic terms and theorems needed for this paper. We are not going to give any proofs, but one can find these, and much more, for example in [3] and [4].

A.1 Prime Ideals in Number Fields

Let k be a number field and K a finite extension of k. Let $\wp$ be a prime of k and β a prime of K. We say that β **lies above** $\wp$, or that $\wp$ is contained in β, if $\beta \cap \mathbb{Z}_k = \wp$. If this is the case we write $\beta \mid \wp$ and we have a commutative diagram

$$\begin{array}{ccc} \mathbb{Z}_K & \to & \mathbb{Z}_K/\beta \\ \uparrow & & \uparrow \\ \mathbb{Z}_k & \to & \mathbb{Z}_k/\wp \end{array}$$

The fields $\mathbb{Z}_k/\wp$ and $\mathbb{Z}_K/\beta$ are finite and are called the **residue class fields**. With $f(\beta/\wp)$ we denote the degree of the residue class field extension $\mathbb{Z}_K/\beta$ over $\mathbb{Z}_k/\wp$ and call it the **residue class degree**. We define $N_k^K(\beta)$, the norm of β over k, to be $\wp^{f(\beta/\wp)}$.

Furthermore $\wp\mathbb{Z}_K$ is an ideal of $\mathbb{Z}_K$ and has a factorization

$$\wp\mathbb{Z}_K = \beta_1^{e_1(\beta_1/\wp)} \cdots \beta_r^{e_r(\beta_r/\wp)} \quad (e_i \geq 1)$$

into primes of $\mathbb{Z}_K$. A prime β of $\mathbb{Z}_K$ occurs in the factorization of $\wp$ if and only if it lies above $\wp$. Each $e_i(\beta_i/\wp)$ is called the **ramification index** of β_i over $\wp$. We also have the following basic relation between the ramification index and the residue class degree

$$[K : k] = \sum_{\beta \mid \wp} e(\beta/\wp) f(\beta/\wp)$$

Also if $k \subset K \subset E$ is a tower of finite extensions, and $\wp$, β and q are primes of

k, K and E respectively, such that $q \mid \beta \mid \wp$, then

$$e(q/\wp) = e(q/\beta)e(\beta/\wp)$$
$$f(q/\wp) = f(q/\beta)f(\beta/\wp)$$

Furthermore we say that $\wp$ is **completely split** in K if there are exactly $[K : k]$ different primes of K lying above $\wp$. This is the case if and only if $e(\beta/\wp) = f(\beta/\wp) = 1$ for all $\beta \mid \wp$. A prime is **ramified** in K if any of the ramification indices $e_i(\beta_i/\wp)$ is greater than 1. It can be proved that only a finite number of primes of k ramify in K. If a prime $\wp$ of k is neither split nor ramified in K then it is said to be inert in K. In this case there is only one prime β of K lying above $\wp$ and $e(\beta/\wp) = 1$ and $f(\beta/\wp) = [K : k]$.

When the extension K/k is Galois, and all the extensions we deal with are, then all the $e_i's$ are equal to the same number e and all the $f_i's$ are equal to the same number f.

We now want to define the Frobenius automorphism and the Artin symbol. Before doing so we need to know little more about when a prime is ramified in an extension. Now all the extensions we deal with in this paper are made by adjoining a primitive q-th root of unity to a number field k and/or adjoining a q-th root of an element $a \in k^*$, where q is a power of a prime number. It is now sufficient to know that if a prime $\wp$ of k does not divide q or a, then it is unramified in $k(\zeta_q, \sqrt[q]{a})$. Also the only prime ramified in $k(\zeta_q)$ is the prime dividing q.

Let now k be a number field and K/k a Galois extension with group G. Let $\wp$ be a prime of k unramified in K, and let β be a prime of K lying above $\wp$. The **decomposition group** of β is defined by

$$D_\beta = \{\sigma \in G \mid \sigma(\beta) = \beta\}$$

To each $\sigma \in D_\beta$ we can associate an automorphism $\bar{\sigma}$ of $\mathbb{Z}_K/\beta$ over $\mathbb{Z}_k/\wp$. Let $\tilde{G}$ denote the Galois group of $\mathbb{Z}_K/\beta$ over $\mathbb{Z}_k/\wp$. Then the map $\sigma \mapsto \bar{\sigma}$ induces a isomorphism between D_β and $\tilde{G}$ (if $\wp$ is ramified then we only have a surjective homomorphism). By the theory of finite fields we know that $\tilde{G}$ is cyclic with canonical generator given by the Frobenius automorphism $x \mapsto x^{N(\wp)}$. Hence there is a unique element of D_β which maps to this generator (if $\wp$ is ramified then this is not a unique element but a coset in G_β). This element of D_β is called the **Frobenius automorphism** of β and is denoted by $(\beta, K/k)$ or just $\mathrm{Frob}_\beta = \mathrm{Frob}_\beta^{K/k}$. It has the following property

$$\mathrm{Frob}_\beta(\alpha) \equiv \alpha^{N(\wp)} (mod\ \beta), \quad \forall \alpha \in \mathbb{Z}_K$$

Also, a prime $\wp$ is completely split in K if and only if for all $\beta \mid \wp$ we have $(\beta, K/k) = 1$.

When K/k is abelian and $\wp$ is unramified in K then $(\beta, K/k)$ is the same for all $\beta \mid \wp$. We then denote this element with $(\wp, K/k)$ and call it the **Artin symbol** of $\wp$ in G.

Let now E/k be a finite extension, not necessarily Galois, so that we have the following lattice of fields

$$\begin{tikzcd} & KE \arrow[dl, dash] \arrow[dr, dash] & \\ K \arrow[dr, dash] & & E \arrow[dl, dash] \\ & k & \end{tikzcd}$$

Here K/k is still assumed abelian. Let $\wp$ be a prime of k unramified in K and let q be a prime of E lying above $\wp$. Then

$$\mathrm{res}_K(q, KE/k) = (\wp, K/k)^{f(q/\wp)}$$

To conclude the subject of splitting we state a part of a proposition [4, proposition 5.11].

Proposition A.1 *Let $k \subset K$ be a Galois extension, where $K = k(\alpha)$ for some $\alpha \in \mathbb{Z}_K$. Let $f(x)$ be the monic minimal polynomial of α over k, so that $f(x) \in \mathbb{Z}_k[x]$. If $\wp$ is a prime of k and $f(x)$ is separable modulo $\wp$, then $\wp$ splits completely in K if and only if $f(x) \equiv 0 (mod\ \wp)$ has a solution in $\mathbb{Z}_k$.*

So far we were talking about the prime ideals of the ring of integers of a number field k. These primes are sometimes called the finite primes to distinguish them from the **infinite primes**. An infinite prime is determined by the embedding of k into $\mathbb{C}$. A real infinite prime is an embedding $\sigma : k \to \mathbb{R}$, and a complex infinite prime is a pair of embeddings $\sigma, \bar{\sigma} : k \to \mathbb{C}$. Furthermore, given an extension K/k, an infinite prime σ of k is ramified in K if σ is real but it has an extension to K which is complex.

Another thing we must mention is the Dirichlet Unit Theorem. Without going to deep into the subject of this theorem it will be sufficient to define U_S, the set of **S-units**. Let S be a finite set of primes of a number field k. Then $U_S = \{\alpha \in k^* : |\alpha|_\wp = 1 \, \forall \wp \notin S\} = \{\alpha \in k^* : \wp \mid \alpha \text{ or } \wp \mid \alpha^{-1} \text{ then } \wp \in S\}$. We will not actually need the unit theorem but the following corollary of it.

Corollary A.1 ***(Unit Theorem)*** *Let k be a number field and S a finite set of primes of k. Then U_S modulo the group of roots of unity in k is a finitely generated, free abelian group.*

A.2 Density

Definition A.1 *Let S be a set of primes of a number field K. The Dirichlet density of S (if it exists) is defined to be*

$$\delta(S) = \lim_{s \to 1+} \frac{\sum_{\wp \in S} \frac{1}{N(\wp^s)}}{\log(\frac{1}{s-1})}$$

Some basic properties of the Dirichlet density are:

1. If $\delta(S)$ exists then $0 \leq \delta(S) \leq 1$
2. If S is finite then $\delta(S) = 0$
3. If S and T are disjoint and $\delta(S)$ and $\delta(T)$ exist, then $\delta(S \cup T) = \delta(S) + \delta(T)$

Theorem A.1 ***(Chebotarev)****. Let K/k be Galois with Galois group G. Let $\sigma \in G$. Let $[K : k] = N$, and let c be the number of elements in the conjugacy class of σ in G. Then those primes $\wp$ of k which are unramified in K and for which there exists $\beta \mid \wp$ such that*

$$\sigma = (\beta, K/k)$$

have a density, and this density is equal to c/N.

A.3 Kummer Theory

For a positive integer n we let ζ_n denote a primitive n-th root of unity and μ_n the group generated by ζ_n. We begin with a field K and assume that $\zeta_n \in K$ for some integer n prime to the characteristic of K.

Let $a \in K^*$. Now the symbol $\sqrt[n]{a}$ (or $a^{1/n}$) is not well defined but we will use it to denote any root of $X^n - a$. Since the n-th roots of unity are in K the extension $K(\sqrt[n]{a})$ of K is the same no matter which root of $X^n - a$ we take.

Let W be a subgroup of K^* containing K^{*n} (the n-th powers of non-zero elements of K). Let $K(W^{1/n})$ denote the composite of all the fields $K(a^{1/n})$ for which $a \in W$. One can check that the extension $K(W^{1/n})/K$ is Galois and abelian of exponent n (exponent n means that the Galois group, $G_W = \mathrm{Gal}(K(W^{1/n})/K)$, is annihilated by n i.e. $\sigma^n = 1 \ \forall \sigma \in G_W$).

We have the following diagram:

$$\begin{tikzcd}
\bar{K} \arrow[d, dash] \\
K(W^{1/n}) \arrow[d, dash, "G_W"] \\
K
\end{tikzcd}$$

The Kummer theorem states that the map $W \mapsto K(W^{1/n})$ gives a bijection between of the set of subgroups of K^* containing K^{*n} and the abelian extensions of K of exponent n.
Furthermore $K(W^{1/n})/K$ is finite if and only if $(W : K^{*n})$ is finite (in particular we then have $[K(W^{1/n}) : K] = (W : K^{*n})$). In this case we have an isomorphism:

$$\theta : W/K^{*n} \longrightarrow \mathrm{Hom}(G_W, \mu_n)$$

given by $\theta(w) = \phi_w$ where $\phi_w(\sigma) = \frac{\sigma(\sqrt[n]{w})}{\sqrt[n]{w}}$

In the proof of our theorems we will actually need only the first statement, that is the existence of the bijection between the set $\{W \mid K^{*n} \subset W \subset K^*\}$ and the set of abelian extensions of K of exponent n.

We will also use the following special case of Kummer Theory, concerning the determination of the cyclic extensions [3, chapter IV, §6]:

Theorem A.2 *Let k be a field. Let n be a positive integer prime to the characteristic of k, and assume that there is a primitive n-th root of unity in k.*
(i) Let K be a cyclic extension of k of degree n. Then there exists $\alpha \in K$ such that $K = k(\alpha)$, and α satisfies an equation $X^n - a = 0$ for some $a \in k$.
(ii) Conversely, let $a \in k$, and let α be a root of $X^n - a = 0$. Then $k(\alpha)$ is cyclic over k of degree n/d, where d is the greatest divisor of n for which a is a d-th power in k.

Bibliography

[1] Capi Corrales-Rodrigáñez and René Schoof, *The Support Problem and its Elliptic Analogue*, Journal of Number Theory 64, (1988), 276-290

[2] A. Schinzel, *Une caractérisation arithmétique de suites récurrentes linéaires*, J. reine angew. Math. 494 (1998), 73-84

[3] Serge Lang, *Algebraic Number Theory*, Springer-Verlag

[4] David A. Cox, *Primes of the Form $x^2 + ny^2$*, Wiley-Interscience