On Number Fields with Unit Group of a Prescribed Reduction

Kyle Wu

Mentor: Dr. Alexander Petrov

PRIMES-USA

Abstract

We investigate the attainability of various subgroups of $\mathbb{F}_{p^n}^\times$ as images of the unit group of a number field under reduction modulo an inert prime. We prove several results about possible images under reduction when fixing a finite field $\mathbb{F}_{p^n}$ and varying the number field K of degree n in which p is inert. Using the finite field norm, we fully describe the maximal image for general n and obtain a complete description of the possible images in the quadratic case. We also consider the analogous problem for unit groups of non-maximal orders of a quadratic number field, where the number field is fixed and the order is varied. Similarly, we consider the analogous problem for S-unit groups of localizations of the ring of integers, where the number field is fixed and the choice of localization is varied.

Keywords: unit group, prime ideal, reduction map, fundamental units, non-maximal orders, S-unit group

Contents

1 Introduction

The unit group of the ring of integers of a number field has been an important subject of study in algebraic number theory. Dirichlet's Unit Theorem ([Conb]) describes the unit group as a product of a finite $\mathbb{Z}$-module of specified degree and a cyclic group of roots of unity. However, it does not give an explicit description of a system of fundamental units for the unit group, and so determining a system of fundamental units has been a problem of interest in algebraic number theory.

We consider the problem of controlling the image of the group of units under reduction modulo a prime ideal. Specifically, we consider the possible images of $\mathcal{O}_K^\times$ in the map $\phi_p : \mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_{p^n}$, where p and n are fixed and K is varied. Our problem is related to Artin's conjecture in its focus on the multiplicative group generated by the reduction of an element. Artin's primitive root conjecture states that an integer that is neither square nor -1 is a primitive root modulo infinitely many primes. A natural generalization for Artin's conjecture for number fields asks when a nonzero element α of the ring of integers of a number field K is a generator of the group $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^\times$ for infinitely many prime ideals $\mathfrak{p}$. Sections 6.1.1 and 9.7 of [Mor12] explain several other variants of the conjecture for number fields and the progress that has been made on them. Kitaoka, Ishikawa, Chen, and Yu ([IK98], [CKY00], [Kit06], [Kit07]) have also considered the size of the image of the unit group when reduced modulo a prime ideal, especially in the case of a real quadratic field. Our problem is a natural "converse" of this problem, starting with a given prime p and constructing a number field K such that p is inert in K and the group of units of K has a given image when reduced modulo p.

In a number field K of degree n, we will denote the ring of integers of K by $\mathcal{O}_K$ and the group of units by $\mathcal{O}_K^\times$. Supposing that a rational prime p is inert in K, we find that the quotient $\mathcal{O}_K/p\mathcal{O}_K$ is isomorphic to the finite field $\mathbb{F}_{p^n}$. Making use of the structure of $\mathbb{F}_{p^n}^\times$, we note that the finite field norm agrees with the the field norm $N_{K/\mathbb{Q}}$ modulo p, so that all units must reduce modulo p to an element with finite field norm ± 1. This gives restrictions on the the image of the unit group, and leads to a general conjecture on the attainability of various subgroups of $\mathbb{F}_{p^n}$ as the image of the reduction of the unit group of a number field. We define the subgroup

$$U_{\mathbb{F}_{p^n}^\times} = \{x \in \mathbb{F}_{p^n} : N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(x) = \pm 1\} \tag{1}$$

of $\mathbb{F}_{p^n}^\times$, and by the argument sketched we demonstrate that the image of the group of units must lie in this group. This leads to the conjecture that all subgroups of $U_{\mathbb{F}_{p^n}^\times}$ can be realized as the reduction of the group of units of some number field. More formally, we have the following:

Conjecture 1.1. *Let p be a prime, n be a positive integer, and G be a subgroup of $U_{\mathbb{F}_{p^n}^\times}$ containing -1. Then there exists a number field K of degree n in which p is inert and such that the reduction of $\mathcal{O}_K^\times$ modulo p is exactly the subgroup G of $\mathbb{F}_{p^n}$.*

We first show the more specific case that the maximal subgroup, the entirety of $U_{\mathbb{F}_{p^n}^\times}$, is always attainable. That is, the following theorem holds:

Theorem 3.3. *For a fixed rational prime p and positive integer n, there exist infinitely many number fields K of degree n for which p is inert in K and the reduction of the unit group modulo $p\mathcal{O}_K$ attains the maximal image $U_{\mathbb{F}_{p^n}^\times}$.*

This can be shown by constructing a number field containing a unit that reduces to a generator of the subgroup $U_{\mathbb{F}_{p^n}^\times}$. This result does not require much control over the group of units, as there are no further constraints on the unit that we construct a number field to contain; it does not need to be a fundamental unit.

We then give some bounds on the reduction of the unit group modulo a non inert prime, using the methods developed to describe the possible images of the unit group when reduced modulo a single inert prime. Specifically, we assume p is unramified and splits as $\mathfrak{p}_1\mathfrak{p}_2, \ldots, \mathfrak{p}_k$ for prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$. Then, we relate the modulo p reduction of $N_{K/\mathbb{Q}}(\alpha)$ with the finite field norms of the reduction of α modulo each $\mathfrak{p}_i$. This gives Theorem 4.4, a bound on the size of the image of the group of units analogous to the bound given in Lemma 2.2.

We also show that, in the case of a real quadratic number field, every subgroup of $U_{\mathbb{F}_{p^2}}$ is realizable as the image of the group of units, given that it contains -1:

Theorem 5.5. *For a fixed odd prime p and subgroup G of $U_{\mathbb{F}_{p^n}^\times}$ containing -1, there exists a real quadratic field $K = \mathbb{Q}(\sqrt{m})$ in which p is inert and the group of units of K reduces modulo $p\mathcal{O}_K$ to exactly G.*

This result requires a more careful choice of number field, since a unit we construct it to contain may not necessarily be fundamental. To prove this theorem, we correspond units α that are not fundamental units of $\mathbb{Q}(\alpha)$ with values of the Dickson polynomials. We then show that the sequence of Dickson polynomials approximate an infinite exponential sequence and thus have density 0, guaranteeing a choice of α reducing to a desired generator of a subgroup of $U_{\mathbb{F}_{p^n}^\times}$ that is a fundamental unit in $\mathbb{Q}(\alpha)$.

As a consequence of this result, all even divisors d of $2(1+p)$ are realizable as the size of the reduction of the group of units of some number field K modulo $p\mathcal{O}_K$, where p is inert in K.

It is also interesting to consider the problem in non-maximal orders $\mathcal{O} \subsetneq \mathcal{O}_K$. The unit group of the order $\mathcal{O}^\times$ is a subset of $\mathcal{O}_K^\times$ so it may have a different image in $\mathcal{O}/p\mathcal{O}$. We consider the problem of fixing a number field K and choosing an order $\mathcal{O}$ in which the image of the reduction of $\mathcal{O}^\times$ modulo $p\mathcal{O}$ gives a specific image. For this question to be well defined, we describe conditions for p to be "inert" so that $\mathcal{O}/p\mathcal{O} \cong \mathbb{F}_{p^n}$. In the quadratic case, we have a complete characterization of the possible images:

Theorem 6.6. *Let K be a real quadratic number field with ring of integers $\mathcal{O}_K$, and let p be a prime which is inert in K. Let $U \subseteq U_{\mathbb{F}_{p^2}}$ be the image of the group of units when reduced modulo $p\mathcal{O}_K$. Then for a given subgroup $G \subseteq U$ containing -1, there exists an order $\mathcal{O} \subseteq \mathcal{O}_K$ such that p remains inert in $\mathcal{O}$ and the group of units of $\mathcal{O}$ has image G under reduction modulo $p\mathcal{O}$.*

Alternatively, we generalize the question to S-units, considering the reduction of the unit group of the localized ring $\mathcal{O}_K^S$. The problem then becomes one of enlarging the unit group. That is, if its image was previously some $G \subseteq U_{\mathbb{F}_{p^n}^\times}$, we consider enlarging it to some U for $G \subseteq U \subseteq \mathbb{F}_{p^n}^\times$. Here, there is no longer a restriction on whether U must lie in $G \subseteq U_{\mathbb{F}_{p^n}^\times}$ since it need not have norm 1. We approach the problem by localizing to a prime with a given reduction modulo p so that it generates our desired subgroup, and apply class field theory to construct such a prime. In the general case, we have the following theorem:

Theorem 7.6. *Let p be an odd rational prime inert in a number field K. Suppose that $U \subseteq (\mathcal{O}_K/p\mathcal{O}_K)^\times$ is the image of $\mathcal{O}_K^\times$ under reduction modulo $p\mathcal{O}_K$ and G is a subgroup satisfying*

$U \subseteq G \subseteq (\mathcal{O}_K/p\mathcal{O}_K)^\times$. Then there exists a prime $q \in \mathcal{O}_K$ such that if $S = \{q\mathcal{O}_K\}$ the image of $(\mathcal{O}_K^S)^\times$ under reduction modulo $p\mathcal{O}_K^S$ is G.

We also consider the real cubic case. Since the unit group has rank two in this case, it is much harder to control the exact image of the unit group because must produce number fields in which we have control over both fundamental units. We focus on Minkowski units, or units in cyclic extensions $K/\mathbb{Q}$ such that the unit and its conjugate generate $\mathcal{O}_K^\times$. The existence of Minkowski units in cyclic cubic fields is proven in Theorem 3.28 of [Nar04]. We use Minkowski units to restrict the image of the group of units under reduction, since Galois conjugates of elements of $\mathbb{F}_{p^n}$ are powers of the original element due to the Frobenius automorphism, making the problem once again a matter of controlling the reduction of one unit. We prove a sufficient condition for a root of a polynomial to be a Minkowski unit (Theorem 8.1) and expect that this condition is satisfied enough to resolve Conjecture 1.1 in the case of real cubic fields. When considering the construction of a field with a given Minkowski unit, we refer to other papers on the construction of number fields satisfying given properties, including Shanks [Sha74] and Balady [Bal16].

2 Background

Let K be a number field of degree n with ring of integers $\mathcal{O}_K$ and unit group $\mathcal{O}_K^\times$. Furthermore, let p be a rational prime inert in K and let $\phi_p : \mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K$ denote the reduction map on $\mathcal{O}_K$ sending an element to its residue class in $\mathcal{O}_K/p\mathcal{O}_K$.

We first consider the multiplicative structure of $\mathcal{O}_K/p\mathcal{O}_K$. It is well-known that $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_{p^n}$, where n is the degree of K, and furthermore we have that the multiplicative group of $\mathbb{F}_{p^n}$ is cyclic. Thus, using the finite field norm $N_{\mathbb{F}_{p^n}/\mathbb{F}_p}$ we define a subgroup $U_{\mathbb{F}_{p^n}^\times}$ as in Equation 1 containing all elements of norm ±1. Due to the structure of $\mathbb{F}_{p^n}$, this subgroup is cyclic and has order equal to the number of solutions to

$$N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(x) = x^{1+p+\cdots+p^{n-1}} = \pm 1,$$

which is precisely $2(1 + p + \cdots + p^{n-1})$.

Remark 2.1. In order to begin to consider the image of the group of units $\mathcal{O}_K^\times$ under reduction by ϕ_p, we must first make a choice of isomorphism between $\mathcal{O}_K/p\mathcal{O}_K$ and $\mathbb{F}_{p^n}$. However, since $\mathbb{F}_{p^n}^\times$ is cyclic, automorphisms on it preserve subgroups and thus the subgroup $\phi_p(\mathcal{O}_K^\times) \subset \mathbb{F}_{p^n}^\times$ does not depend on a choice of isomorphism $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_{p^n}$.

We now relate $\mathcal{O}_K^\times$ with $U_{\mathbb{F}_{p^n}^\times}$. We first describe a relationship between the field norm $N_{K/\mathbb{Q}}$ and the finite field norm on $\mathcal{O}_K/p\mathcal{O}_K$. This allows us to characterize the possible images of the unit group under reduction modulo $p\mathcal{O}_K$ in terms of $U_{\mathbb{F}_{p^n}^\times}$:

Lemma 2.2. *The image of $\mathcal{O}_K^\times$ under ϕ_p is equal to a subgroup of $U_{\mathbb{F}_{p^n}^\times}$ containing -1.*

Proof. We first show that for $\alpha \in \mathcal{O}_K$, we have

$$\phi_p(N_{K/\mathbb{Q}}(\alpha)) = N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\phi_p(\alpha)).$$

Consider a $\mathbb{F}_p$-basis $1, \overline{\alpha_1}, \ldots, \overline{\alpha_{n-1}}$ of $\mathbb{F}_{p^n}$. Let $1, \alpha_1, \ldots, \alpha_{n-1}$ be some choice of elements of $\mathcal{O}_K$ whose reductions are $1, \overline{\alpha_1}, \ldots, \overline{\alpha_{n-1}}$ respectively. Observe that these elements are $\mathbb{Z}$-linearly independent because if they were not then we could take a $\mathbb{Z}$-linear combination of them that is 0 in $\mathcal{O}_K$ and divide factors of p from the coefficients until one of them is nonzero modulo p. Then, the resulting linear combination has reduction equivalent to 0 in $\mathbb{F}_{p^n}$ but not all coefficients equivalent to 0 in $\mathbb{F}_p$, contradicting the assumption that $1, \overline{\alpha_1}, \dots, \overline{\alpha_{n-1}}$ formed a basis in $\mathbb{F}_{p^n}$. Since they are all elements of $\mathcal{O}_K$, it follows that they form a basis of K.

Now, consider the matrix $M_{\phi_p(\alpha)}$ over K representing multiplication by $\phi_p(\alpha)$ as a linear map from $\mathbb{F}_{p^n}$ to itself with basis $1, \overline{\alpha_1}, \dots, \overline{\alpha_{n-1}}$. Additionally, consider the matrix M_α over $\mathbb{Q}$ representing multiplication by α as a linear map from K to itself with basis $1, \alpha_1, \dots, \alpha_{n-1}$. Since the basis used in $M_{\phi_p(\alpha)}$ is the reduction of the basis used in M_α and it represents a reduction of the multiplication map of M_α, we see that the entries of $M_{\phi_p(\alpha)}$ are the reductions of the entries of M_α. By treating the determinant as a polynomial in the entries of the matrix, we observe that $\det(M_{\phi_p(\alpha)}) = \phi_p(\det(M_\alpha))$.

By Theorem 67 in [Rot98], the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois. Thus, by Theorem 5.1 in [Conc], the determinant of the matrix representing multiplication by α in the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is equal to the product of the Galois conjugates of α, or $\alpha^{1+p+\dots+p^{n-1}} = N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha)$.

Thus, $\det(M_{\phi_p(\alpha)}) = N_{L/\mathbb{F}_p}(\phi_p(\alpha))$ and by the definition of norm $\det(M_\alpha) = N_{K/\mathbb{Q}}(\alpha)$ so it follows that $\phi_p(N_{K/\mathbb{Q}}(\alpha)) = N_{L/\mathbb{F}_p}(\phi_p(\alpha))$.

Our desired result follows, as we have that the image of $\mathcal{O}_K^\times$ under ϕ_p is a subgroup of $U_{\mathbb{F}_{p^n}^\times}$, and it must contain -1 since $-1 \in \mathcal{O}_K$ is a unit. □

Corollary 2.3. *The size of the image of the unit group under ϕ_p is an even divisor of $2(1 + p + \dots + p^{n-1})$.*

Having established a necessary condition for the possible images of $\mathcal{O}_K^\times$ under ϕ_p, it remains to determine which images are obtainable. Fixing a prime p and degree n, we will consider whether there exists a number field K whose unit group reduces to a given subgroup of $U_{\mathbb{F}_{p^n}^\times}$.

The following will be helpful in our analysis of the the possible images of the unit group:

Theorem 2.4 (Dirichlet's Unit Theorem)**.** *Suppose a number field K has r_1 real embeddings and $2r_2$ complex embeddings. Then $\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r_1+r_2-1}$, where μ_K is a finite cyclic torsion group of roots of unity.*

Thus, one may describe the reduction of the unit group of K by considering only the reductions of its $r_1 + r_2 - 1$ generators. This will be a useful tool in our analysis of the possible non-maximal images.

3 Maximal Image of the Unit Group

The first case we will consider is how to construct a number field whose group of units attains the maximal image $U_{\mathbb{F}_{p^n}^\times}$ when reduced modulo p. To do so, we will consider constructing K by adjoining an element whose reduction maps to a generator of $U_{\mathbb{F}_{p^n}^\times}$. First, we prove a lemma to ensure the inertness of p in K:

Lemma 3.1. *For a number field $K = \mathbb{Q}(\alpha)$ and rational prime p, if α has minimal polynomial f of degree n which is irreducible in $\mathbb{F}_p[x]$, then p is inert in K.*

Proof. By the Dedekind-Kummer Theorem, from the irreducibility of f in $\mathbb{F}_p[x]$ it suffices to show that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. By Lemma 3.32 in [Jar14] this is equivalent to the discriminant of the integral basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ not being divisible by p. Considering the discriminant as a Vandermonde determinant, we have that it is equal to $\prod_{i<j}(\sigma_i(\alpha) - \sigma_j(\alpha))^2$ where each σ_i is a distinct embedding of K into a fixed extension of $\mathbb{Q}$. Since all finite fields are perfect, f is separable in $\mathbb{F}_p[x]$ so by its irreducibility it follows that f has no double roots in $\mathbb{F}_{p^n}$. Thus, $(\sigma_i(\alpha) - \sigma_j(\alpha))^2$ is nonzero in $\mathbb{F}_{p^n}$ so the product is nonzero modulo p. Therefore, the discriminant is not divisible by p and p is inert in K. □

Theorem 3.2. *For a fixed rational prime p and positive integer n, there exists a number field K of degree n in which p is inert and such that the image of its unit group $\mathcal{O}_K^\times$ under the reduction map ϕ_p is exactly $U_{\mathbb{F}^\times_{p^n}}$.*

Proof. Since $\mathbb{F}^\times_{p^n}$ is cyclic, it has a generator g. If p is odd, then we may write $U_{\mathbb{F}^\times_{p^n}}$, a cyclic subgroup of $\mathbb{F}^\times_{p^n}$ of order $2(1+p+\cdots+p^{n-1}) = \frac{p^n-1}{(p-1)/2}$, as the subgroup generated by the element $u = g^{(p-1)/2}$. If $p = 2$, we note that $U_{\mathbb{F}^\times_{p^n}} = \{x \in \mathbb{F}_{p^n} : N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(x) = 1\} = \mathbb{F}^\times_{p^n}$, so we may simply set $u = g$. In either case, by the fact that u generates a group of order more than p^{n-1}, we have that the minimal polynomial f of u has degree n. We also have that f is monic and has constant coefficient $(-1)^{n+1}$. Now, consider an arbitrary polynomial $\widetilde{f} \in \mathbb{Z}[x]$ which is monic, has constant coefficient $(-1)^{n+1}$, and whose reduction modulo p is equal to f. Then $\widetilde{f}$ is irreducible by the irreducibility of f in $\mathbb{F}_p[x]$ and thus we may let K be the extension $\mathbb{Q}(\alpha)$ where α is an arbitrary root of f. Then we claim K satisfies the desired property.

To show this claim, we first observe that by Lemma 3.1 we have that the irreducibility of f in $\mathbb{F}_p[x]$ implies that p is inert in K. Now, we see that α is a unit in K since its minimal polynomial has a constant coefficient $(-1)^{n+1}$. Additionally, $\phi_p(\alpha)$ generates $U_{\mathbb{F}^\times_{p^n}}$ because it is a conjugate of u so it generates the same subgroup, as discussed in Remark 2.1. Thus, we have exhibited a number field K of degree n for which p is inert and the image of the unit group $\mathcal{O}_K^\times$ under ϕ_p contains $U_{\mathbb{F}^\times_{p^n}}$. By Lemma 2.2 the reduction of the unit group of K is also contained in $U_{\mathbb{F}^\times_{p^n}}$, so it must be exactly $U_{\mathbb{F}^\times_{p^n}}$. □

Note that due to the freedom in constructing a polynomial $\widetilde{f}$ in Theorem 3.2, we may extend the result to give a number field such that the group of units achieves the maximal image of $U_{\mathbb{F}^\times_{p^n}}$ when reduced modulo multiple different primes p separately.

Theorem 3.3. *For any k distinct rational primes $p_1, \ldots, p_k$ and positive integer n, there exists a number field K for which every p_i is inert in K and the reduction of the unit group modulo each $\langle p_i \rangle$ is exactly $U_{\mathbb{F}_{p_i^n}}$.*

Proof. Let g_i denote the generator of $\mathbb{F}^\times_{p_i^n}$, and then define $u_i = g_i^{(p_i-1)/2}$ if p_i is odd and $u_i = g_i$ otherwise. Define $f_i \in \mathbb{F}_{p_i}[x]$ as the minimal polynomial of u_i. Then by Chinese Remainder Theorem we may construct $\widetilde{f}$ to be a monic integer polynomial of degree n and constant coefficient $(-1)^{n-1}$ such that it reduces to f_i modulo each p_i. This is possible because the p_i's are distinct, and thus for each x^t coefficient of $\widetilde{f}$ for $1 \leq t \leq n-1$ the Chinese Remainder Theorem states that there exists a residue class modulo $p_1 p_2 \ldots p_k$ equivalent to that x^t coefficient modulo each p_i. Then, following the rest of the proof for Theorem 3.2 for each p_i we see that $\widetilde{f}$ is irreducible and if it has a root α then $K = \mathbb{Q}(\alpha)$ has degree n. Furthermore, we see that each p_i is inert in K. We also find that α is a unit in K and also reduces under each ϕ_{p_i} to a conjugate of u_i which generates each $U_{\mathbb{F}_{p_i^n}}$. □

4 The Image Modulo Non-Inert Primes

Using the same tools as in the inert prime case, we place some bounds on the image of the unit group of K when reduced modulo a prime p not inert in K.

Theorem 4.1. *Let K be a number field of degree n with r_1 real embeddings, $2r_2$ complex embeddings, and finite torsion subgroup μ_K. Let p be a rational prime which is unramified in K and splits as $\mathfrak{p}_1 \dots \mathfrak{p}_k$ where the prime ideal $\mathfrak{p}_i$ has inertial degree e_i. Then the size of the image of the reduction of the group of units modulo p is at most $|\mu_K| \cdot \operatorname{lcm}(p^{e_1}-1, \dots, p^{e_k}-1)^{r_1+r_2-1}$.*

Proof. First, note that by the Chinese Remainder Theorem we have

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{p}_1 \times \cdots \times \mathcal{O}_K/\mathfrak{p}_k \cong \mathbb{F}_{p^{e_1}} \times \cdots \times \mathbb{F}_{p^{e_k}}$$

as an isomorphism between rings. Thus, considering their multiplicative groups, we have

$$(\mathcal{O}_K/p\mathcal{O}_K)^\times \cong \mathbb{F}_{p^{e_1}}^\times \times \cdots \times \mathbb{F}_{p^{e_k}}^\times \cong \mathbb{Z}/(p^{e_1}-1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(p^{e_k}-1)\mathbb{Z}.$$

Thus every element of $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ has order dividing $\operatorname{lcm}(p^{e_1}-1, \dots, p^{e_k}-1)$. Thus, each of the r_1+r_2-1 fundamental units has order $\operatorname{lcm}(p^{e_1}-1, \dots, p^{e_k}-1)$ and since in addition to μ_K they generate all units, the image of the group of units has maximum size $|\mu_K| \cdot \operatorname{lcm}(p^{e_1}-1, \dots, p^{e_k}-1)^{r_1+r_2-1}$. □

Corollary 4.2. *If p splits completely in K, then the size of the reduction of the group of units modulo p is at most $2(p-1)^{r_1+r_2-1}$, since in this case $\operatorname{lcm}(p^{e_1}-1, \dots, p^{e_k}-1) = \operatorname{lcm}(p-1, \dots, p-1) = p-1$.*

We also prove a result relating the field norm of an element $\alpha \in \mathcal{O}_K$ with the finite field norms of its reductions modulo $\mathcal{O}_K/\mathfrak{p}_i$ for each prime ideal $\mathfrak{p}_i$ in the splitting of p when p is unramified.

Lemma 4.3. *Let K be a number field of degree n and let p be a rational prime which is unramified in K which splits as $\mathfrak{p}_1 \dots \mathfrak{p}_k$, where each $\mathfrak{p}_i$ has inertial degree e_i. Let $\phi_i : \mathcal{O}_K \to \mathbb{F}_{p^{e_i}}$ denote the reduction map modulo $\mathfrak{p}_i$ and let $\phi_p : \mathcal{O}_K \to \mathbb{F}_p$ denote the reduction map modulo p. Then for a given element $\alpha \in K$ we have that*

$$\phi_p(N_{K/\mathbb{Q}}(\alpha)) = \prod_{i=1}^{k} N_{\mathbb{F}_{p^{e_i}}/\mathbb{F}_p}(\phi_i(\alpha)).$$

Proof. We may consider residue classes of $\mathfrak{p}_1 \dots \mathfrak{p}_k$ as elements of $F = \mathbb{F}_{p^{e_1}} \times \cdots \times \mathbb{F}_{p^{e_k}}$, an n-dimensional vector space over $\mathbb{F}_p$. Then, viewing F as a direct sum of k independent subspaces we may take a standard basis $\mathfrak{B}$ of F in which e_i of the basis vectors have nonzero projection to $\mathbb{F}_{p^{e_i}}$ for each $1 \le i \le k$. If we let $\widetilde{\mathfrak{B}}$ be a set of elements of K whose reduction modulo p is $\mathfrak{B}$, we find that this must be a basis of K because if we could write 0 as a nontrivial $\mathbb{Q}$-linear combination of elements of $\widetilde{\mathfrak{B}}$ then by scaling up to get a $\mathbb{Z}$-linear combination and dividing by powers of p until one of the coefficients is not a multiple of p, we find that the reduction of this linear combination is a nontrivial linear combination of elements of $\mathfrak{B}$ that equals 0, which would contradict the fact that $\mathfrak{B}$ is a basis.

Now, considering F and K as n-dimensional vector spaces over $\mathbb{F}_p$ and $\mathbb{Q}$ with bases $\mathfrak{B}$ and $\widetilde{\mathfrak{B}}$ respectively, we see that multiplication by α in F and in K are both linear maps. Thus, we may describe the map over F as an $n \times n$ matrix M_α with entries in $\mathbb{F}_p$, and the map over K as an $n \times n$ matrix $\widetilde{M_\alpha}$ with entries in $\mathbb{Q}$. Now, since the basis used in M_α is the reduction of the basis used in

$\widetilde{M_\alpha}$ and it represents a reduction of the multiplication map of $\widetilde{M_\alpha}$, we see that the entries of M_α are the reductions of the entries of $\widetilde{M_\alpha}$. Thus, we have that $\phi_p(N_{K/\mathbb{Q}}(\alpha)) = \phi_p(\det \widetilde{M_\alpha}) = \det M_\alpha$.

Now, it suffices to show that $\det M_\alpha = \prod_{i=1}^k N_{\mathbb{F}_{p^{e_i}}/\mathbb{F}_p}(\phi_i(\alpha))$. To see this, first observe that since each e_i in $\mathfrak{B}$ was picked to be a basis element of the independent subspace $\mathbb{F}_{p^{e_i}}$, a linear map on F with basis $\mathfrak{B}$ can be split up into the direct sum of linear maps on each $\mathbb{F}_{p^{e_i}}$ so the matrix M_α can be split up into the direct sum of the multiplication by α matrices over each $\mathbb{F}_{p^{e_i}}$. The determinant of the multiplication by α matrix over $\mathbb{F}_{p^{e_i}}$ has determinant $N_{\mathbb{F}_{p^{e_i}}/\mathbb{F}_p}(\phi_i(\alpha))$ and the determinant of a direct sum of matrices is equal to the product of their determinants, so we have the relationship between the norms

$$\phi_p(N_{K/\mathbb{Q}}(\alpha)) = \det M_\alpha = \prod_{i=1}^k N_{\mathbb{F}_{p^{e_i}}/\mathbb{F}_p}(\phi_i(\alpha)).$$

□

Using this property of the norm, we find that a result analogous to Lemma 2.2 holds:

Theorem 4.4. *Let K be a number field of degree n and let p be a rational prime unramified in K which splits as $\mathfrak{p}_1 \dots \mathfrak{p}_k$, where each $\mathfrak{p}_i$ has inertial degree e_i. Then the size of the reduction of the group of units modulo p is at most $\frac{2}{p-1}\prod_{i=1}^k (p^{e_i}-1)$.*

Proof. By the Chinese Remainder Theorem, we have $\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{p}_1 \times \cdots \times \mathcal{O}_K/\mathfrak{p}_k \cong \mathbb{F}_{p^{e_1}} \times \cdots \times \mathbb{F}_{p^{e_k}}$, so an element of $\mathcal{O}_K/p\mathcal{O}_K$ is uniquely determined by its residue classes modulo each $\mathfrak{p}_i$. Let $\phi_i : \mathcal{O}_K \to \mathbb{F}_{p^{e_i}}$ denote the reduction map modulo $\mathfrak{p}_i$. Then, consider any of the $\prod_{i=1}^{k-1}(p^{e_i}-1)$ choices of residue classes modulo each $\mathfrak{p}_i$ from $i = 1$ to $k-1$. Then any element α which satisfies each of these equivalences and is a unit must have

$$\prod_{i=1}^k N_{\mathbb{F}_{p^{e_i}}/\mathbb{F}_p}(\phi_i(\alpha)) \equiv \pm 1 \pmod p$$

by Theorem 4.3. Thus,

$$N_{\mathbb{F}_{p^{e_k}}/\mathbb{F}_p}(\phi_k(\alpha)) \equiv \pm \left(\prod_{i=1}^{k-1} N_{\mathbb{F}_{p^{e_i}}/\mathbb{F}_p}(\phi_i(\alpha)) \right)^{-1}$$

so the other residue classes determine two possibilities for the norm of $\phi_k(\alpha)$ for a unit α.

Now, note that for each $\alpha \in \mathbb{F}_p^\times$ the equation $N_{\mathbb{F}_{p^{e_k}}/\mathbb{F}_p}(x) = \alpha$ or $x^{1+p+\cdots+p^{e_k-1}} = \alpha$ has at most $1 + \cdots + p^{e_k-1}$ roots in $\mathbb{F}_{p^{e_k}}$. Additionally, every one of the $p^{e_k} - 1 = (p-1)(1 + p + \cdots + p^{e_k-1})$ elements of $\mathbb{F}_{p^{e_k}}^\times$ has a norm that is equal to one of the $p-1$ elements of $\mathbb{F}_p$. Thus, the preimages of all the elements of $\mathbb{F}_p^\times$ under the norm map $N_{\mathbb{F}_{p^{e_k}}/\mathbb{F}_p} : \mathbb{F}_{p^{e_k}}^\times \to \mathbb{F}_p^\times$ have the same size $1 + p + \cdots + p^{e_k-1}$.

It follows that the first $k-1$ residue classes of an element $\alpha \in K$ determine 2 possible values for $N_{\mathbb{F}_{p^{e_k}}/\mathbb{F}_p}(\phi_k(\alpha))$ so that α lies in one of $\frac{2}{p-1}(p^{e_k}-1)$ possible residue classes modulo $\mathfrak{p}_k$. Thus, there are $\frac{2}{p-1}\prod_{i=1}^k(p^{e_i}-1)$ possible k-tuples of residue classes modulo each $\mathfrak{p}_i$ for a unit, so this is the maximum on the size of the image of the group of units under the reduction map. □

Remark 4.5. This bound is sometimes larger than the one given in Theorem 4.1 and sometimes smaller, depending on the different inertial degrees of the ideals that p splits into.

5 Real Quadratic Fields

We now consider the case where $n = 2$. We also restrict our focus to real quadratic fields, as Dirichlet's Unit Theorem gives that the rank of the unit group is 0 in a complex quadratic field and 1 in a real quadratic field. We will use a similar lifting argument to construct $K = \mathbb{Q}(\alpha)$ for α a generator of a given subgroup of $U_{\mathbb{F}_{p^2}^\times}$ containing -1, but more work will need to be done to ensure this unit is fundamental.

We first focus on minimal polynomials of the form $x^2 - ax + 1$ and $x^2 - ax - 1$, and determine when one of them has a root $\alpha = \beta^k$ for β a root of another polynomial of that form and k an integer greater than 1. The polynomials $x^2 - ax \pm 1$ for which no such β exist are precisely the ones for which α is a fundamental unit in $\mathbb{Q}(\alpha)$. To characterize exactly the set of a for which the root of $x^2 - ax \pm 1$ for which no such β exists, we use a polynomial series in order to relate polynomials whose roots are powers of each other.

Definition 5.1. For a real number b, we define the sequence of polynomials $P_{b,0}, P_{b,1}, \ldots$ recursively with $P_{b,0}(x) = 2$, $P_{b,1}(x) = x$, and $P_{b,n+1}(x) = xP_{b,n}(x) - bP_{b,n-1}(x)$.

This sequence is also called the sequence of Dickson polynomials $D_n(x, b)$, where $P_{b,n}(x) = D_n(x, b)$. More on Dickson polynomials can be found in Section 9.6 of [MP13].

Lemma 5.2. *If α is a root of the polynomial $x^2 - ax + b$ where $b \neq 0$, then α^k is a root of $x^2 - P_{b,k}(a)x + b^k$ for all nonnegative integers k.*

Proof. We see that by Vieta's formulas $a = \alpha + \frac{b}{\alpha}$ so by Identity 7.8 from [LN87], $P_{b,k}(a) = \alpha^k + \frac{b^k}{\alpha^k}$. Additionally, $\alpha^k \cdot \frac{b^k}{\alpha^k} = b^k$ so by Vieta's formulas α^k and $\frac{b^k}{\alpha^k}$ are roots of $x^2 - P_{b,k}(a)x + b^k$.

For the sake of completeness, we provide a full proof by induction on k. For $k = 0, 1$ we have $\alpha^0 = 1$ is a root of $x^2 - 2x + 1$ and α^1 is a root of $x^2 - ax + b$. Now, assume that α^k is a root of $x^2 - P_{b,k}(a)x + b^k$ for all $k \leq n$. Then α is a root of $x^2 - ax + b$, α^n is a root of $x^2 - P_{b,n}(a)x + b^n$, and α^{n-1} is a root of $x^2 - P_{b,n-1}(a)x + b^{n-1}$. Equivalently, α is a root of the polynomials $x^2 - ax + b$, $x^{2n} - P_{b,n}(a)x + b^n$, and $x^{2(n-1)} - P_{b,n-1}x^{n-1} + b^{n-1}$ so it is a root of

$$(x^2 + b)(x^{2n} - P_{b,n}(a)x^n + b^n) + P_{b,n}(a)x^n(x^2 - ax + b) - bx^2(x^{2(n-1)} - P_{b,n-1}(a)x^{n-1} + b^{n-1})$$

which simplifies to

$$x^{2n+2} - (aP_{b,n}(a) - bP_{b,n-1}(a))x^{n+1} + b^{n+1} = x^{2n+2} - P_{b,n+1}(a) + b^{n+1},$$

so α^{n+1} is a root of $x^2 - P_{b,n+1}(a)x + b^{n+1}$ and our induction is complete. □

Now, we have characterized all a for which the root of $x^2 - ax \pm 1$ is a power of the root of another quadratic polynomial $x^2 - a'x \pm 1$ by giving a sequence of polynomials such that this property holds when a is attained as a value of one of the polynomials. We will show that the natural density of such values is 0.

Lemma 5.3. *Let $\mathcal{S}_1$ denote the set of all integers a greater than 2 for which a root α of $x^2 - ax + 1$ is not a fundamental unit in the real quadratic number field $\mathbb{Q}(\alpha)$. Similarly, let $\mathcal{S}_2$ denote the set of all integers a greater than 2 for which a root α of $x^2 - ax - 1$ is not a fundamental unit in the number field $\mathbb{Q}(\alpha)$. Then the natural density of both $\mathcal{S}_1$ and $\mathcal{S}_2$ in the integers is 0.*

Proof. Our proof will show that the values the Dickson polynomials take on over the integers has density 0. To show this, we will make use of multiple properties specific to the Dickson polynomials, and this result does not hold for general sequences of polynomials with increasing degree; see Remark 5.4.

We first consider the natural density of $\mathcal{S}_2$. If a root α of $x^2 - ax - 1$ is not a fundamental unit in the number field, then we must have that α can be written as β^k for some unit β and integer $k > 1$. Then, if we let β be a root of $x^2 - bx - 1$, it follows from Lemma 5.2 that $a = P_{-1,k}(b)$. Thus, in order for a to be in S_2 it must be of the form $P_{-1,k}(b)$ for some integer b and positive integer $k > 1$.

We may further reduce the problem using the fact that every coefficient in $P_{-1,k}$ is positive and that $P_{-1,k}$ is either an even polynomial or an odd polynomial. Thus, if b is negative and $P_{-1,k}$ is odd then $P_{-1,k}(b)$ is negative and if $P_{-1,k}$ is even then $P_{-1,k}(b) = P_{-1,k}(-b)$. Thus, it suffices to show that the set

$$\mathcal{S}_2' = \mathbb{N} \cap \left(\bigcup_{b \in \mathbb{Z}} \{P_{-1,k}(b) : k \geq 2\} \right) = \mathbb{N} \cap \left(\bigcup_{b \in \mathbb{N}_0} \{P_{-1,k}(b) : k \geq 2\} \right)$$

has natural density 0.

To show this, we first note that the sequence $P_{-1,2}(0), P_{-1,3}(0), \dots$ alternates between 0 and 2. We also have that, up to a finite number of cases, the sequence $P_{-1,0}(1), P_{-1,1}(1), \dots$ is greater than geometric with ratio $3/2$. To see this, we recognize the sequence as Lucas' sequence with closed form $\varphi^k + (1-\varphi)^k$ for $\varphi = \frac{1+\sqrt{5}}{2} > 3/2$, and furthermore the $(1-\varphi)^k$ term has absolute value strictly less than 1 for $k \geq 1$. Now, we also have that the sequence $P_{-1,2}(b), P_{-1,3}(b), \dots$ is greater than geometric with common ratio b. This is because $P_{-1,n+1}(b) = bP_{-1,n}(b) + P_{-1,n-1}(b) > bP_{-1,n}(b)$.

To show $\mathcal{S}_2'$ has density 0, we may consider the cardinality of the intersection $\mathcal{S}_2' \cap \{1, 2, \dots n^2\}$ for each positive integer n. From the fact that $P_{-1,k}(b)$ increases as k increases, we see that for a fixed b we have that $P_{-1,k}(b)$ attains its minimum at $k = 2$, when $P_{-1,k}(b) = b^2 + 2$. Thus, in order for $\{P_{-1,k}(b) : k \geq 2\}$ to intersect $\{1, 2, \dots n^2\}$ at all, we need, $b^2 + 2 \leq n^2$ or $b < n$. Then, for each such b, we have that since $P_{-1,k}(b)$ is greater than geometric with common ratio b, its intersection with $\{1, 2, \dots n^2\}$ has size at most $\log_b(n^2)$. Thus, for some positive integer c,

$$\begin{aligned}
\frac{1}{n^2} \left| \mathcal{S}_2' \cap \{1, 2, \dots, n^2\} \right| &\leq \frac{1}{n^2} \left(c + \sum_{b=1}^{\infty} \left| \{P_{-1,k}(b) : k \geq 2\} \cap \{1, 2, \dots, n^2\} \right| \right) \\
&= \frac{1}{n^2} \left(c + \log_{3/2}(n^2) + \sum_{b=2}^{n-1} \left| \{P_{-1,k}(b) : k \geq 2\} \cap \{1, 2, \dots, n^2\} \right| \right) \\
&\leq \frac{1}{n^2} \left(c + \log_{3/2}(n^2) + \sum_{b=2}^{n-1} \log_b(n^2) \right) \\
&\leq \frac{1}{n^2} \left(c + 2(n-1) \log_{3/2}(n) \right) \\
&\leq \frac{1}{n^2} (c + 2n \log_{3/2}(n)) \\
&\leq \frac{c + 6 \log n}{n}
\end{aligned}$$

which approaches 0 as n grows large. So $\mathcal{S}_2'$ also has natural density 0 so $\mathcal{S}_2$ does, as desired.

We now deal with the density of $\mathcal{S}_1$. Similarly to in the first case, note that a root α of $x^2 - ax + 1$

not being a fundamental unit is equivalent to it being written as β^k for some other unit β, which has a minimal polynomial of the form $x^2 - bx \pm 1$ for integer b. There are a finite number of cases where $\mathbb{Q}(\alpha)$ is not a totally real quadratic field, which occurs when $a \leq 2$. Thus, by Lemma 5.2, up to a finite number of cases, we have that a being in $\mathcal{S}$ is equivalent to a being written in the form $P_{1,k}(b)$ for some integer $k \geq 2$ and $b \in \mathbb{Z}$ or as $P_{-1,k}(b)$ for some even $k \geq 2$ and $b \in \mathbb{Z}$. Also, by the density of $\mathcal{S}_2'$, the set of cases where $a = P_{-1,k}(b)$ has natural density 0. Thus, it only suffices to consider the natural density of the set

$$\mathcal{S}_1' = \mathbb{N} \cap \left(\bigcup_{b \in \mathbb{Z}} \{P_{1,k}(b) : k \geq 2\} \right).$$

Now, observe that when $|b| \leq 2$, we have that $\{P_{1,k}(b) : k \geq 2\}$ is a subset of $\{-2, -1, 0, 1, 2\}$. To show this, note that if $|b| \leq 2$ then the root of $x^2 - bx + 1$ is a root of unity so any kth power of the root is also either 0 or a root of unity. Thus, the polynomial $x^2 - P_{1,k}(b)x + 1$ always has roots that are roots of unity and it follows that $|P_{1,k}(b)| \leq 2$ as well.

Now, for $|b| > 2$, we will prove inductively that the sequence $|P_{1,2}(b)|, |P_{1,3}(b)|, \ldots$ is strictly increasing and is greater than geometric with common ratio $|b| - 1$. For our base case, we note that $|P_{1,2}(b)| = |b^2 - 2|$ and $|P_{1,1}(b)| = |b^3 - 3b| \leq |b|(|b^2 - 2| - 1) \leq (|b| - 1)|b^2 - 2|$ since $|b| - 1 < |b^2 - 2|$ from the fact that $|b| > 2$, so this case works. Then, assuming $|P_{1,n-1}(b)| < |P_{1,n}(b)|$, we see that

$$|P_{1,n+1}(b)| = |bP_{1,n}(b) - P_{1,n-1}(b)| \geq \Big| |bP_{1,n}(b)| - |P_{1,n-1}(b)| \Big| \geq (|b| - 1)|P_{1,n}(b)|.$$

Thus, our induction is done.

To show $\mathcal{S}_1'$ has density 0, we may consider the cardinality of the intersection $\mathcal{S}_1' \cap \{1, 2, \ldots n^2\}$ for each positive integer n. From the fact that $|P_{1,k}(b)|$ increases as k increases, we see that for a fixed b we have that $|P_{1,k}(b)|$ attains its minimum at $k = 2$, when $P_{1,k}(b) = b^2 - 2$. Thus, in order for $\{P_{1,k}(b) : k \geq 2\}$ to intersect $\{1, 2, \ldots n^2\}$ at all, we need, $b^2 - 2 \leq n^2$, which can be rewritten as $b \leq n$. Then, for each such b, we have that since $|P_{1,k}(b)|$ is greater than geometric with common ratio $|b| - 1$, its intersection with $\{1, 2, \ldots n^2\}$ has size at most $\log_{|b|-1}(n^2)$. Thus

$$\begin{aligned}
\frac{1}{n^2} \left| \mathcal{S}_1' \cap \{1, 2, \ldots, n^2\} \right| &\leq \frac{1}{n^2} \left(5 + \sum_{b \in \mathbb{Z}, |b| > 2} \left| \{P_{1,k}(b) : k \geq 2\} \cap \{1, 2, \ldots, n^2\} \right| \right) \\
&= \frac{1}{n^2} \left(5 + \sum_{b \in \mathbb{Z}, 2 < |b| \leq n} \left| \{P_{1,k}(b) : k \geq 2\} \cap \{1, 2, \ldots, n^2\} \right| \right) \\
&\leq \frac{1}{n^2} \left(5 + \sum_{b \in \mathbb{Z}, 2 < |b| \leq n} \log_{|b|-1}(n^2) \right) \\
&= \frac{1}{n^2} \left(5 + 4 \sum_{b=2}^{n-1} \log_b(n) \right) \\
&\leq \frac{1}{n^2} (5 + 4(n-2) \log_2(n)) \\
&\leq \frac{4n \log_2(n)}{n^2} \\
&\leq \frac{4}{\log 2} \cdot \frac{\log n}{n}
\end{aligned}$$

which approaches 0 as n grows large. Thus, $\mathcal{S}_1'$ has natural density 0 so $\mathcal{S}_1$ has natural density 0. □

Remark 5.4. Note that the density argument used in this result on the family of polynomials $P_{b,k}$ for $b = \pm 1$ is not true of general families of integer polynomials with increasing degrees. In fact, we may take an example as simple as $x^2+1, x^3+2, x^4+3, \ldots$ to see that the natural density of the values attained by the polynomials can be 1. The families considered here are special in a sense due to the fact that $P_{b,n}(x)$ for $b = \pm 1$ only takes on a finite number of values for small x and is on the order of x^n for large x. Thus, the values attained by $P_{b,n}(x)$ are roughly in correspondence with the perfect powers, which have natural density 0.

Having shown that polynomials of the form $x^2 - ax \pm 1$ "almost always" have a root α such that α is a fundamental unit in $K = \mathbb{Q}(\alpha)$, we now consider when p is inert in K. This is not immediate because in the case where we want the image of the unit group to have size 2 or 4, we need α to reduce to an element of $\mathbb{F}_p$ under ϕ_p, implying that the corresponding $x^2 - ax \pm 1$ is reducible in $\mathbb{F}_p[x]$. Thus, we give the following criteria, leveraging the fact that $\mathcal{O}_K$ need not be equal to $\mathbb{Z}[\alpha]$:

Lemma 5.5. *Fix a prime $p \geq 3$. Then the following quadratic polynomials f have a root α for which p is inert in $\mathbb{Q}(\alpha)$:*

(i) $x^2 - (mp^{2k}+2)x + 1$ *for positive integer k and m congruent to a quadratic nonresidue modulo p.*

(ii) $x^2 - (2mp^2 + 2q) - 1$ *when* $p \equiv 1 \pmod 4$, *where m is congruent to a quadratic nonresidue modulo p and q is an integer satisfying* $q^2 \equiv -1 \pmod{p^3}$.

(iii) $x^2 - ax + 1$, *where the reduction of the quadratic modulo p is irreducible in* $\mathbb{F}_p[x]$.

Additionally, for (ii), we have that such a residue class $\pmod{p^3}$ *corresponding to q exists.*

Proof. For (i), we have by the quadratic formula that

$$\alpha = \frac{mp^{2k} + 2 \pm \sqrt{(mp^{2k}+2)^2 - 4}}{2},$$

so $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{(mp^{2k}+2)^2-4})$ and thus if $\sqrt{(mp^{2k}+2)^2-4} = b\sqrt{d}$ for squarefree d and integer b, then $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$. By Section 5.9 of [Jar14] it suffices to show d is a quadratic nonresidue modulo p. Then observe that

$$b\sqrt{d} = \sqrt{(mp^{2k}+2)^2 - 4} = \sqrt{m^2p^{4k} + 4mp^{2k}} = p^k\sqrt{m^2p^{2k} + 4m}$$

so $\frac{b}{p^k} = \sqrt{\frac{m^2p^{2k}+4m}{d}}$ is an integer so $\frac{m^2p^{2k}+4m}{d} \equiv \frac{4m}{d}$ is a quadratic residue modulo p. From the fact that m is a quadratic nonresidue, it follows that d is also a nonresidue. Thus, p is inert in $\mathbb{Q}(\alpha)$ in this case.

For (ii), we first show that a residue class corresponding to such a q exists given $p \equiv 1 \pmod 4$. Observe that there exists a generator g of $(\mathbb{Z}/p^3\mathbb{Z})^\times$ which has order $p^3 - p^2$ and that $p^3 - p^2 \equiv 0 \pmod 4$. Thus, we may take any q in the residue class equivalent to $g^{(p^3-p^2)/4}$ modulo p, as it will have order 4 and thus satisfies $q^2 \equiv -1 \pmod{p^3}$. Now, to show that p is inert in $\mathbb{Q}(\alpha)$, we see that by the quadratic formula

$$\alpha = \frac{2mp^2 + 2q \pm \sqrt{(2mp^2+2q)^2+4}}{2},$$

so $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{(2mp+2q)^2+4})$ and thus if $\sqrt{(2mp+2q)^2+4} = b\sqrt{d}$ for squarefree d and integer b, then $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$. Again, it suffices to show d is a quadratic nonresidue modulo p. Assume for the sake of contradiction it were a quadratic residue modulo p. Then observe that

$$b\sqrt{d} = \sqrt{(2mp^2+2q)^2+4} = 2\sqrt{m^2p^4 + 2mp^2q + q^2 + 1} = 2p\sqrt{m^2p^2 + 2mq + (q^2+1)/p^2}$$

so $\frac{b}{2p} = \sqrt{\frac{m^2p^2+2mq+(q^2+1)/p^2}{d}}$ is an integer so $\frac{m^2p^2+2mq+(q^2+1)/p^2}{d} \equiv \frac{2mq}{d}$ is a quadratic residue modulo p. By similar reasoning to the previous case, it suffices to show that $2q$ is equivalent to a quadratic residue modulo p.

To see this, we will consider p modulo 8 and make use of quadratic reciprocity, which states that 2 is a quadratic residue modulo an odd prime p if and only if $p \equiv \pm 1 \pmod 8$. If $p \equiv 1 \pmod 8$ then $q \equiv g^{(p^3-p^2)/4} \equiv (g^{(p^3-p^2)/8})^2 \pmod p$ is a quadratic residue and by quadratic reciprocity 2 is a quadratic residue as well so $2q$ is. If $p \equiv 7 \pmod 8$ then $(p^3-p^2)/4$ is odd so $q \equiv g^{(p^3-p^2)/4} \pmod p$ is a quadratic nonresidue and by quadratic reciprocity 2 is also a quadratic nonresidue so $2q$ is a quadratic residue. We conclude that d is a quadratic nonresidue, so p is inert in K.

For (iii), we have by Lemma 3.1 that p is inert in $\mathbb{Q}(\alpha)$. □

Theorem 5.6. *For any odd prime p and subgroup G of $U_{\mathbb{F}_{p^2}}$ containing -1, there exists a real quadratic number field K in which p is inert and the image of the group of units of K under ϕ_p is exactly G.*

Proof. We first treat the case where G is a subgroup of $\mathbb{F}_p^\times$. Letting g be a generator of $\mathbb{F}_{p^2}^\times$, we see that G lies in $\mathbb{F}_p^\times$ if and only if its order divides $p-1$. However, it also has order dividing $2(p+1)$, and it must also have an even number of elements. Thus, we find that the only possibilities are when the order of G is 2 or when $p \equiv 1 \pmod 4$ and the order of G is 4.

When G has size 2, consider the set of a for which $a = mp^{2k} + 2$ for k an integer and m congruent to a quadratic nonresidue modulo p. Then since the set of such a has positive natural density greater than $1/p^2$, we have by Lemma 5.3 that there exists some such a for which the root α of $x^2 - ax + 1$ is a fundamental unit in $\mathbb{Q}(\alpha)$. Then take K to be $\mathbb{Q}(\alpha)$. To show this works for this case, we first note that by part (i) of Lemma 5.5 p is inert in $\mathbb{Q}(\alpha)$. Now, by construction we have that α is a fundamental unit in $\mathbb{Q}(\alpha)$ so every other unit is of the form $\pm\alpha^k$ for $k \in \mathbb{Z}$. Finally, note that the reduction of α under ϕ_p is a root of $x^2 - ax + 1$ which is equivalent to $x^2 - 2x + 1$, so α reduces to 1 in $\mathbb{F}_{p^2}$. Thus, every element in the unit group reduces to ± 1 under ϕ_p so the image of $\mathcal{O}_K^\times$ under ϕ_p has order 2.

For $s = 4$ and $p \equiv 1 \pmod 4$, we have by part (ii) of Lemma 5.5 that there exists an integer q for which $q^2 \equiv -1 \pmod p$. Also, we have that for this q and any m equivalent to a quadratic nonresidue modulo p, p is inert in $\mathbb{Q}(\alpha)$ for α a root of $x^2 - ax - 1$ when $a = 2mp^2 + 2q - 1$. Since the set of such a has positive natural density greater than $1/p^2$, we have by Lemma 5.3 that some such a has the property that α is a fundamental unit in $\mathbb{Q}(\alpha)$, and we may take $K = \mathbb{Q}(\alpha)$ for this value of a. Thus, every element of $\mathcal{O}_K^\times$ is of the form $\pm\alpha^k$ for $k \in \mathbb{Z}$. Let the reduction of α modulo p be $\overline{\alpha}$. Then $\overline{\alpha}$ is a root of the reduction of $x^2 - ax - 1$ modulo p, which is equivalent to

$x^2 - 2q - 1 = (x - q)^2$. Thus, $\overline{\alpha} = q$ and the order of $\overline{\alpha}$ is 4. Thus, the reduction of the group of units has size 4 in this case.

Now, we consider when G is not a subgroup of $\mathbb{F}_p^\times$. Then consider a generator g_s of G. Since g_s is not in $\mathbb{F}_p$, its minimal polynomial is of the form $x^2 - \overline{a}x + 1$ or $x^2 - \overline{a}x - 1$ for some $\overline{a} \in \mathbb{F}_p$. Then, consider the set of a whose reductions modulo p map to $\overline{a}$. Since the set of such a has positive natural density equal to $\frac{1}{p}$, we have by Lemma 5.3 that there exists some such a for which the root α of $x^2 - ax + 1$ or $x^2 - ax - 1$ is a fundamental unit in $\mathbb{Q}(\alpha)$. Then take K to be $\mathbb{Q}(\alpha)$. To show this works, we first note that p is inert in $\mathbb{Q}(\alpha)$ by part (iii) of Lemma 3.1. We also have that the image of α under ϕ_p is a root of $x^2 - \overline{a}x + 1$ in $\mathbb{F}_{p^2}$ so it is g_s or g_s^{-1}, both of which give that the reduction of the unit group is exactly the group generated by g_s which is G.

Thus, for every subgroup of $U_{\mathbb{F}_{p^2}}$, we have exhibited a number field whose group of units has the desired image when reduced under ϕ_p. □

Example 5.7. We may construct a real quadratic number field K in which the prime $p = 23$ is inert and whose unit group has size exactly 8 when reduced modulo p. We first find a polynomial in $\mathbb{F}_p[x]$ of the form $x^2 - ax + 1$ whose roots in $\mathbb{F}_{p^2}$ have order 8. This can be done by factoring the 8th cyclotomic polynomial in $\mathbb{F}_p[x]$ as $\Phi_8(x) = x^4 + 1 = (x^2 - 5x + 1)(x^2 - 18x + 1)$ and choosing a to be equivalent to $5 \pmod{p}$. Then we may lift a to be 5 and notice that by part (iii) of Lemma 5.5, p is inert in $K = \mathbb{Q}(\alpha)$. We also see that the element α has a minimal polynomial that reduces modulo p to the minimal polynomial of an element of order 8 in $U_{\mathbb{F}_{p^2}}$. Thus, the image of the reduction of the group of units has size exactly 8. Finally, we have that $5 \notin \mathcal{S}_1$ so that α is a fundamental unit in $\mathcal{O}_K$. Thus, the reduction of the group of units of $\mathcal{O}_K$ is exactly the subgroup of size 8 in $U_{\mathbb{F}_{p^2}}$.

Example 5.8. We may construct a real quadratic number field K in which the prime $p = 5$ is inert and where the reduction of the group of units of $\mathcal{O}_K$ modulo $p\mathcal{O}_K$ has size exactly 2 (i. e., is the subgroup $\{\pm 1\}$ of $U_{\mathbb{F}_{p^2}}$). Using the process given in part (i) of Lemma 5.5, we first consider the number field $K = \mathbb{Q}(\alpha)$ where α is a root of the polynomial $x^2 - (2 \cdot p^2 + 2)x + 1 = x^2 - 52x + 1$. In this number field, p is inert and we also have that the reduction of the minimal polynomial of α is $x^2 - 2x + 1$, thus the reduction of α must be 1. However, we actually have that $52 \in S_1$, as $52 = P_{1,3}(4)$. In other words, we see that $\alpha^{1/3}$ is a root of $x^2 - 4x + 1$, so α is not a fundamental unit of K, and instead $\alpha^{1/3}$ is. Thus, this number field does not work. If we instead try letting α be a root of $x^2 - (3 \cdot p^2 + 2)x + 1 = x^2 - 77x + 1$, we see again that p is inert in K and that the reduction of the minimal polynomial of α is $x^2 - 2x + 1$ so α must reduce to 1. A short computation shows that $77 \notin S_1$ so in this case α is a fundamental unit of K. Thus, we see that for this choice of K the reduction of the group of units of $\mathcal{O}_K$ modulo $p\mathcal{O}_K$ is exactly the set $\{\pm 1\}$ with size exactly 2.

6 Non-Maximal Orders

It is also interesting to consider the same question for the unit group of a non-maximal ideal. Fixing a prime p and number field K in which p is inert, we will consider varying a choice of order $\mathcal{O} \subseteq \mathcal{O}_K$ to determine possible images of the unit group when reduced modulo $p\mathcal{O}$.

In order to formulate the problem, we first define what it means for a prime p inert in K to remain inert in an order $\mathcal{O} \subseteq \mathcal{O}_K$.

Definition 6.1. We will say that a rational prime p which is inert in a number field K remains inert in an order $\mathcal{O} \subseteq \mathcal{O}_K$ if the ideal $p\mathcal{O}$ is a prime ideal of $\mathcal{O}$.

For the purposes of describing when p remains inert, we prove the following equivalence:

Lemma 6.2. *Let p be a rational prime and K be a number field of degree n in which p is inert. Let $\mathcal{O} \subseteq \mathcal{O}_K$ be an order of K. Then the following statements are equivalent:*

(1) The prime p remains inert in $\mathcal{O}$, i.e. $p\mathcal{O}$ is a prime ideal.

(2) The quotient $\mathcal{O}/p\mathcal{O}$ is isomorphic to $\mathbb{F}_{p^n}$.

(3) The conductor ideal $\mathfrak{c}$ of $\mathcal{O}$ satisfies $\mathfrak{c} + p\mathcal{O} = \mathcal{O}$, i.e. is relatively prime to $p\mathcal{O}$.

Proof. We first show that (1) $\implies$ (2). Considering $\mathcal{O}$ as a finitely generated $\mathbb{Z}$-module of rank n, we may choose an additive basis $\mathfrak{B}$ of $\mathcal{O}$ that has size n. Then, in the representation of any element of $\mathcal{O}$ a reduction of each of the coefficients modulo p gives an isomorphism between $\mathcal{O}/p\mathcal{O}$ and $(\mathbb{Z}/p\mathbb{Z})^n$. Since $p\mathcal{O}$ is a prime ideal, it follows that $\mathcal{O}/p\mathcal{O}$ is an integral domain of finite size p^n, so it is isomorphic to $\mathbb{F}_{p^n}$.

We also have that (2) $\implies$ (1) because the quotient $\mathcal{O}/p\mathcal{O}$ being a field implies that $p\mathcal{O}$ is a maximal $\mathcal{O}$-ideal, and thus it is a prime $\mathcal{O}$-ideal. Thus, (1) is equivalent to (2).

To show that (2) $\implies$ (3), we assume for the sake of contradiction that $\mathfrak{c} + p\mathcal{O} = \mathfrak{a} \neq \mathcal{O}$ but $\mathcal{O}/p\mathcal{O} \cong \mathbb{F}_{p^n}$. It follows that $p\mathcal{O} \subseteq \mathfrak{a}$. However, from the fact that $\mathcal{O}/p\mathcal{O}$ is a field we see that $p\mathcal{O}$ is maximal. Thus, $p\mathcal{O} \subseteq \mathfrak{a} \neq \mathcal{O}$ implies that $\mathfrak{a} = p\mathcal{O}$, and thus $\mathfrak{c} \subseteq p\mathcal{O}$. Taking an element $\alpha \in \mathfrak{c}$ we find that $\alpha\mathcal{O}_K$ is an $\mathcal{O}$-ideal. Furthermore, since $\frac{\alpha}{p} \notin \mathfrak{c}$ by the minimality of $\nu_p(\alpha)$, we find that $\frac{\alpha}{p}\mathcal{O}_K$ is not an $\mathcal{O}$-ideal so $\alpha\mathcal{O}_K \not\subseteq p\mathcal{O}$. However, the ideal product $\alpha\mathcal{O}_K \cdot \alpha\mathcal{O}_K = \alpha^2\mathcal{O}_K \subseteq p\mathcal{O}$ since $\alpha\mathcal{O}_K$ is an $\mathcal{O}$-ideal and $\alpha \in p\mathcal{O}$. Thus the ideal $p\mathcal{O}_K$ is not prime, a contradiction.

We have that (3) $\implies$ (2) from statement (2) in Theorem 3.8 of [Cona]. Thus, all three statements are equivalent. □

We now pose the question:

Question 6.3. *Let K be a number field of degree n with ring of integers $\mathcal{O}_K$ and let p be a prime which is inert in K. Let $U \subseteq U_{\mathbb{F}_{p^2}}$ be the image of the group of units when reduced modulo $p\mathcal{O}_K$. For a given subgroup $G \subseteq U$ containing -1, does there exist an order $\mathcal{O} \subseteq \mathcal{O}_K$ such that p remains inert in $\mathcal{O}$ and the group of units $\mathcal{O}$ has image G under the reduction map $\phi'_p : \mathcal{O} \to \mathcal{O}/p\mathcal{O}$?*

Lemma 6.4. *For number field K of degree n and prime p inert in K, let ε be an element of $\mathcal{O}_K$. If $\phi_p(\varepsilon)$ is a generator of $\mathbb{F}_{p^n}$, then p remains inert in the order $\mathbb{Z}[\varepsilon]$.*

Proof. Let ε have minimal polynomial $f(x)$ and let $\overline{f}(x) \in \mathbb{F}_p[x]$ denote the reduction of $f(x)$ modulo p. Then we have

$$\mathcal{O}/p\mathcal{O} = \mathbb{Z}[\varepsilon]/p \cong (\mathbb{Z}[x]/f(x))/p \cong \mathbb{Z}[x]/(f(x), p) \cong (\mathbb{Z}[x]/p)/f(x) \cong \mathbb{F}_p[x]/f(x).$$

In the case where $\phi_p(\varepsilon)$ is a generator of $\mathbb{F}_{p^n}$, we have that $\overline{f}(x)$ has degree n so $\mathcal{O}/p\mathcal{O} \cong \mathbb{F}_p[x]/\overline{f}(x) \cong \mathbb{F}_{p^n}$ so by Lemma 6.2 we get that p remains inert in $\mathcal{O}$. □

Lemma 6.5. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic number field for squarefree d and let p be an odd rational prime inert in K. Let $\varepsilon = a + b\sqrt{d}$ be an element of $\mathcal{O}_K^\times$, where $2a, 2b \in \mathbb{Z}$. Furthermore assume that $\varepsilon > 1$, $\varepsilon \neq \frac{3+\sqrt{5}}{2}$, and $p^{\nu_p(b)} < \sqrt{b}$. If $b' = bp^{-\nu_p(b)}$, then the order $\mathcal{O} = \mathbb{Z}[b'\sqrt{d}]$ has p remaining inert and ε as a fundamental unit.*

Proof. Note that $\gcd(b', p) = 1$. Then observe that the conductor of $\mathcal{O}$ is $2b'\mathcal{O}$ in the case where $d \equiv 1 \pmod 4$ and $b'\mathcal{O}$ otherwise. Thus, by Lemma 6.2 we see that p remains inert since the conductor of $\mathcal{O}$ is coprime with $p\mathcal{O}$.

We now show that ε is fundamental in $\mathcal{O}$. Using the discriminant formula for a power basis gives that $\mathrm{Disc}(\mathcal{O}) = (2b'\sqrt{d})^2 = 4b'^2 d$. By Eq. (1.1) of [JLW95], we find that the regulator R satisfies

$$\begin{aligned} R &\geq \log\left(\frac{1}{2}(\sqrt{\mathrm{Disc}(\mathcal{O})} + \sqrt{\mathrm{Disc}(\mathcal{O}) - 4})\right) \\ &\geq \log(\sqrt{\mathrm{Disc}(\mathcal{O}) - 4}) \\ &= \frac{1}{2}\log(4b'^2 d - 4). \end{aligned}$$

Thus, to show that ε is a fundamental unit, it suffices to show that

$$\log \varepsilon < 2R = \log(4b'^2 d - 4).$$

Note that since $\varepsilon > 1$, it follows that the conjugate of ε is equal to $a - b\sqrt{d} = \frac{1}{\varepsilon} < 1$. Thus, it suffices to show

$$4b'^2 d - 4 > \varepsilon = 2b\sqrt{d} + (a - b\sqrt{d}) > 2b\sqrt{d}.$$

From the fact that $p^{\nu_p(b)} < \sqrt{b}$, we have that $b' = b/p^{\nu_p(b)} > \sqrt{b}$. Thus $4b'^2 d - 4 > 4bd - 4$ so it suffices to show $4bd - 4 > 2b\sqrt{d}$ or $2b(2d - \sqrt{d}) > 4$ which holds in the case where $b \geq 1$ since $d \geq 2$. In the case where $b = \frac{1}{2}$, we find that we need $d \equiv 1 \pmod 4$ so we can only have the case $d = 5$ corresponding to $\varepsilon = \frac{3+\sqrt{5}}{2}$. Thus, we are done. □

Lemma 6.6. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic number field for squarefree d and let p be an odd rational prime inert in K. For an element ε in $\mathcal{O}_K$, write $\varepsilon = a + b\sqrt{d}$ for $2a, 2b \in \mathbb{Z}$ and write $\varepsilon^p = a_1 + b_1\sqrt{d}$ for $2a_1, 2b_1 \in \mathbb{Z}$. If $p \nmid a$ and $p \mid b$, then $\nu_p(b_1) = \nu_p(b) + 1$.*

Proof. Let $\varepsilon = a + b\sqrt{d}$ for $2a, 2b \in \mathbb{Z}$. Observe that, by the binomial theorem,

$$\varepsilon^p = (a + b\sqrt{d})^p = a^p + a^{p-1}b\sqrt{d}\binom{p}{1} + a^{p-2}(b\sqrt{d})^2\binom{p}{2} + a^{p-3}(b\sqrt{d})^3\binom{p}{3} + \cdots + (b\sqrt{d})^p.$$

Extracting the $\sqrt{d}$ component, we find that it is equal to the sum of the terms with odd $b\sqrt{d}$ exponent:

$$a^{p-1}b\sqrt{d}\binom{p}{1} + a^{p-3}b^3 d\sqrt{d}\binom{p}{3} + \cdots + b^p d^{(p-1)/2}\sqrt{d}.$$

Note that the p-adic valuation of the $\sqrt{d}$-coefficient of each term in the sum strictly increases due to the fact that the kth coefficient has p-adic valuation

$$\nu_p\left(a^{p-k}b^k d^{(k-1)/2}\binom{p}{k}\right) = (p-k)\nu_p(a) + k\nu_p(b) + \frac{k-1}{2}\nu_p(d) + \nu_p\left(\binom{p}{k}\right) = k\nu_p(b) + 1,$$

and the last term has p-adic valuation $p\nu_p(b)$ which is larger than the rest. It follows from the non-Archimedean property of p-adic valuation that

$$\nu_p(b_1) = \nu_p\left(a^{p-1}b\binom{p}{1} + a^{p-3}b^3 d\binom{p}{3} + \cdots + b^p d^{(p-1)/2}\right) = \nu_p\left(a^{p-1}b\binom{p}{1}\right) = \nu_p(b) + 1.$$

Thus, we are done. □

Theorem 6.7. *Let K be a real quadratic number field with ring of integers $\mathcal{O}_K$, and let p be a rational prime which is inert in K. Let $U \subseteq U_{\mathbb{F}_{p^2}}$ be the image of the group of units when reduced modulo $p\mathcal{O}_K$. Then for a given subgroup $G \subseteq U$ containing -1, there exists an order $\mathcal{O} \subseteq \mathcal{O}_K$ such that p remains inert in $\mathcal{O}$ and the group of units $\mathcal{O}$ has image G under the reduction map $\phi'_p : \mathcal{O} \to \mathcal{O}/p\mathcal{O}$.*

Proof. Let $K = \mathbb{Q}(\sqrt{d})$ for squarefree d, and let $\bar{\varepsilon} \in \mathcal{O}_K/p\mathcal{O}_K$ denote a generator of G. We consider cases, depending on whether $\bar{\varepsilon}$ is an element of $\mathbb{F}_p \subset \mathcal{O}_K/p\mathcal{O}_K$ (note that this embedding of $\mathbb{F}_p$ is canonical).

We first consider the case where $\bar{\varepsilon}$ is not sent to an element of $\mathbb{F}_p$. Since the image of $\mathcal{O}_K^\times$ under reduction modulo p has an image U of which G is a subgroup, we may lift $\bar{\varepsilon}$ to an element ε of $\mathcal{O}_K^\times$ satisfying $\phi_p(\varepsilon) = \bar{\varepsilon}$. We may also assume that $\varepsilon \neq (3+\sqrt{5})/2$ by raising it to the power of p^2 if necessary, as $\phi_p(\varepsilon) = \phi_p(\varepsilon^{p^2})$ due to the Frobenius endomorphism. Considering $\mathcal{O} = \mathbb{Z}[\varepsilon]$, we have by Lemma 6.4 that p remains inert in $\mathcal{O}$.

Now, by Theorem 3.8 of [Cona] it follows that there is a natural ring isomorphism $\mathcal{O}/p\mathcal{O} \cong \mathcal{O}_K/p\mathcal{O}_K$ given by inclusion. Thus this isomorphism sends $\phi'_p(\varepsilon)$ to $\phi_p(\varepsilon)$ so they have the same multiplicative order. Thus, the subgroup of $\mathcal{O}/p\mathcal{O}$ generated by $\phi'_p(\varepsilon)$ has the same size as the subgroup of $\mathcal{O}_K/p\mathcal{O}_K$ generated by $\phi_p(\varepsilon)$, which is G. Thus, it suffices to show that $\mathcal{O}^\times$ is generated by ε. Since $\varepsilon \neq (3+\sqrt{5})/2$, we have by Theorem 1 in [Ste08] that ε is a fundamental unit of $\mathcal{O}$, so we are done in this case. (Note that this can also be obtained by a similar argument to 6.5.)

We now consider if the generator $\bar{\varepsilon}$ of G is an element of $\mathbb{F}_p$. Since the image of $\mathcal{O}_K^\times$ under reduction modulo p has an image U of which G is a subgroup, we may lift $\bar{\varepsilon}$ to an element ε of $\mathcal{O}_K^\times$ satisfying $\phi_p(\varepsilon) = \bar{\varepsilon}$. We may also assume that $\varepsilon \neq (3+\sqrt{5})/2$ by raising it to the power of p if necessary, as $\phi_p(\varepsilon) = \phi_p(\varepsilon^p)$ due to the Frobenius endomorphism. We may also negate it and take its multiplicative inverse if necessary so that $\varepsilon > 1$ so that we may write $\varepsilon = a + b\sqrt{d}$ for $2a, 2b \in \mathbb{N}$. In order to apply Lemma 6.5 we wish to find a power of ε with the same reduction such that the p-adic valuation of the $\sqrt{d}$ coefficient is sufficiently small.

From the fact that $\phi_p(\varepsilon) \in \mathbb{F}_p$ we have that $p \mid b$ and from the fact that $\phi_p(\varepsilon)$ has finite multiplicative order in $\mathbb{F}_{p^2}^\times$, we find that $\phi_p(\varepsilon) \neq 0$ so $p \nmid a$. Thus, applying Lemma 6.6 we see that if $\varepsilon^p = a_1 + b_1\sqrt{d}$ for $2a_1, 2b_1 \in \mathbb{N}$, then $\nu_p(b_1) = \nu_p(b) + 1$. Repeating this process by defining $\varepsilon_k = \varepsilon^{p^k} = a_k + b_k\sqrt{d}$ for $2a_k, 2b_k \in \mathbb{N}$, we find that $p \nmid a_k$ and $p \mid b_k$ since ε^{p^k} reduces to the same nonzero element under ϕ_p by the Frobenius endomorphism. Thus $\nu_p(b_{k+1}) = \nu_p(b_k) + 1$ so $\nu_p(b_k) = \nu_p(b) + k$. For each one, we see that $a_k - b_k\sqrt{d} = \varepsilon^{-k}$ satisfying $0 < \varepsilon^{-k} < 1$ so $\varepsilon_k = 2b_k + (a_k - b_k)$ satisfies $2b_k < \varepsilon_k < 2b_k + 1$. This gives

$$p^{\nu_p(b_k)} = p^{\nu_p(b)+k} < 2bp^k < p^k\varepsilon \text{ and } \sqrt{b_k} > \sqrt{\varepsilon_k/2} = \sqrt{\varepsilon^{p^k}/2}.$$

Thus, in order to have $p^{\nu_p(b_k)} < \sqrt{b_k}$ it suffices to have $p^k\varepsilon < \sqrt{\varepsilon^{p^k}/2}$. Taking the logarithm of both sides it suffices to have $k\log p + \log\varepsilon < \frac{1}{2}(p^k\log\varepsilon - \log 2)$. Since the exponential term grows faster than the linear term, there exists sufficiently large k for which this holds. Taking such a k, we find that we may apply Lemma 6.5 to ε_k to find an order $\mathcal{O}$ in which p is inert and ε_k is fundamental. By a similar argument to the first case, $\phi_p(\varepsilon_k)$ has the same multiplicative order as $\phi'_p(\varepsilon_k)$ so they generate the same subgroup G. Thus, the image of $\mathcal{O}^\times$ under ϕ'_p is G. □

We conjecture that a similar result holds in a number field of arbitrary degree, provided that the unit group is infinite:

Conjecture 6.8. *Let K be a number field of degree n, and let p be a rational prime which is inert in K. Let $U \subseteq U_{\mathbb{F}_{p^n}}$ be the image of the group of units when reduced modulo $p\mathcal{O}_K$. Then for a given subgroup $G \subseteq U$ containing -1, there exists an order $\mathcal{O}$ of K such that p remains inert in $\mathcal{O}$ and the group of units $\mathcal{O}$ has image G under the reduction map $\phi'_p : \mathcal{O} \to \mathcal{O}/p\mathcal{O}$.*

7 S-Unit Group Reduction

The S-unit group is another generalization of the unit group for which many similar results hold. We use the definition given in page 70 of [NS13]. For a number field K and a finite set S of prime ideals of K, the ring of S-integers is the subring of K defined by $\mathcal{O}_K^S = \{\frac{\alpha}{\beta} : \alpha, \beta \in \mathcal{O}_K, \beta \notin \mathfrak{p} \text{ for all } \mathfrak{p} \notin S\}$. The group of S-units $(\mathcal{O}_K^S)^\times$ is defined to be the set of invertible elements in $\mathcal{O}_K^S$. We now describe what it means for a prime p inert in K to remain inert in $\mathcal{O}_K^S$.

Definition 7.1. We will say that a rational prime p which is inert in a number field K remains inert in the S-integers $\mathcal{O}_K^S$ when the ideal $p\mathcal{O}_K^S$ is prime.

Equivalently, by Proposition 11.1 in Chapter 1 of [NS13], a rational prime p inert in K remains inert in $\mathcal{O}_K^S$ if $p \notin S$.

Lemma 7.2. *When a rational prime p is inert in K and remains inert in $\mathcal{O}_K^S$, the reduction map $\phi_p : \mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K$ extends uniquely to a reduction map*

$$\phi_p^S : \mathcal{O}_K^S \to \mathcal{O}_K/p\mathcal{O}_K.$$

Furthermore, we derive from ϕ_p^S an induced map

$$\Phi : \mathcal{O}_K^S/p\mathcal{O}_K^S \to \mathcal{O}_K/p\mathcal{O}_K$$

which is an isomorphism.

Proof. Since every element of $\mathcal{O}_K^S$ may be written as α/β where $\mathfrak{p} \nmid \beta$ for all $\mathfrak{p} \notin S$, we may extend the reduction map by setting $\phi_p^S(\alpha/\beta) = \phi_p(\alpha)/\phi_p(\beta)$. Since p remains inert in $\mathcal{O}_K^S$, we have that $p \notin S$ so $p \nmid \beta$ implying $\phi_p(\beta) \neq 0$, allowing this extension to be defined. We see that the kernel of this extended reduction map is exactly

$$\{\alpha/\beta : \alpha, \beta \in \mathcal{O}_K, \mathfrak{p} \nmid \beta \text{ for all } \mathfrak{p} \notin S, p \mid \alpha\} = p\mathcal{O}_K^S$$

so the map induces an injective homomorphism $\Phi : \mathcal{O}_K^S/p\mathcal{O}_K^S \to \mathcal{O}_K/p\mathcal{O}_K$. This homomorphism is also surjective from the fact that $\mathcal{O}_K \subset \mathcal{O}_K^S$ and ϕ_p is surjective. Thus, Φ is an isomorphism. □

It follows that $\mathcal{O}_K^S/p\mathcal{O}_K^S \cong \mathbb{F}_{p^n}$. We consider the question:

Question 7.3. *Let p be an odd rational prime inert in a number field K. Suppose that $U \subseteq (\mathcal{O}_K/p\mathcal{O}_K)^\times$ is the image of $\mathcal{O}_K^\times$ under reduction modulo $p\mathcal{O}_K$. Then, for any subgroup G satisfying $U \subseteq G \subseteq (\mathcal{O}_K/p\mathcal{O}_K)^\times$, does there exist a prime $q \in \mathcal{O}_K$ such that if $S = \{q\mathcal{O}_K\}$ the image of $(\mathcal{O}_K^S)^\times$ under reduction modulo $p\mathcal{O}_K^S$ is G?*

Lemma 7.4. *For a real quadratic number field $K = \mathbb{Q}(\sqrt{d})$, odd rational prime p which is inert in K, and nonzero residue $a \in \mathbb{Z}/p\mathbb{Z}$, there exists a rational prime q which is inert in K and equivalent to a modulo p.*

It suffices to find a prime q such that $\left(\frac{d}{q}\right) = -1$ and $q \equiv a \pmod{p}$. The first condition can be rewritten as an equivalence modulo $4d$ by quadratic reciprocity. From the fact that p is odd and inert in K, we have that $(4d, a) = 1$. Thus, we simply wish to find a prime q which satisfies a congruence condition modulo $4dp$, which exists by Dirichlet's theorem on primes in arithmetic progressions (Theorem 2.2 in [Mil20]).

□

Then, in the case where K is a quadratic number field of choice and q must be rational, we have the following result:

Theorem 7.5. *Let p be an odd rational prime, and let G be a subgroup of $\mathbb{F}_{p^2}^\times$ of even index. Then there exists a quadratic number field K and rational prime $q \neq p$ such that p and q are inert in K and setting $S = \{q\mathcal{O}_K\}$ the image of $(\mathcal{O}_K^S)^\times$ under reduction modulo $p\mathcal{O}_K^S$ is G.*

Proof. Consider the subgroups

$$T = G \cap \mathbb{F}_p^\times \text{ and } U = G \cap U_{\mathbb{F}_{p^2}^\times}.$$

We wish to show that G is equal to the subgroup G' of $\mathbb{F}_{p^2}^\times$ generated by T and U. It is clear that $G' \subseteq G$ since its generators lie in G. Now, for an element $g \in G$, note that since the index of G is even the element $g^{p/2}$ can be defined such that $(g^{p/2})^2 = g^p$. Then we find that $(g^{p/2})^{p+1} = N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(g^{p/2}) \in T$ and $(g^{p/2})^{p-1}$ satisfies $N_{\mathbb{F}_{p^2}/\mathbb{F}_p}((g^{p/2})^{p-1}) = (g^{p/2})^{p^2-1} = 1$ so $(g^{p/2})^{p-1} \in U$. Thus, $g = g^{p^2} = (g^{p/2})^{p+1}(g^{p/2})^{p-1}$ so g is generated by T and U. We conclude that $G' = G$.

By Theorem 5.6 there exists a real quadratic number field K in which p is inert and the image of $\mathcal{O}_K^\times$ under reduction modulo $p\mathcal{O}_K$ is exactly U. Also, by Lemma 7.4 there exists a rational prime q inert in K such that $q \equiv t \pmod{p}$, where t denotes a generator of T. Then, we may consider the S-unit group of $p\mathcal{O}_K^S$, where $S = \{q\mathcal{O}_K\}$. By the exactness at $\bigoplus_{\mathfrak{p} \notin S} K^\times/\mathcal{O}_\mathfrak{p}^\times$ in Theorem 11.6 of [NS13], we have that $(\mathcal{O}_K^S)^\times$ is generated by $\mathcal{O}_K^\times$ and q. Thus, the reduction of $(\mathcal{O}_K^S)^\times$ is generated by U and t, so it is equal to $G' = G$.

□

We now prove an analogue of Dirichlet's theorem on primes in arithmetic progressions for number fields:

Theorem 7.6. *Let p be an odd prime inert in a number field K of degree n. Let $U \subsetneq (\mathcal{O}_K/p\mathcal{O}_K)^\times$ be the image of $\mathcal{O}_K^\times$ under reduction modulo $p\mathcal{O}_K$. Then for a given element $\alpha \in (\mathcal{O}_K/p\mathcal{O}_K)^\times$, there exists a (not necessarily rational) prime q in K such that the reduction of q modulo $p\mathcal{O}_K$ lies in αU.*

Proof. We provide a proof based on [Cha]. Set $\mathfrak{m}_0 = p\mathcal{O}_K$, $\mathfrak{m}_\infty = 1$, and $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ and consider the ray class group with modulus $\mathfrak{m}$, which we denote by $C_\mathfrak{m}$. By Takagi's existence theorem (Theorem 0.5 in [Mil20] there exists a class field $K_\mathfrak{m}$ corresponding to the trivial subgroup of $C_\mathfrak{m}$ such that

$$\mathrm{Gal}(K_m/K) \cong C_\mathfrak{m} = \frac{\bigoplus_{\nu \nmid p} \mathbb{Z}}{K_{\mathfrak{m},1}}.$$

Lifting α to an arbitrary element $\widetilde{\alpha} \in \mathcal{O}_K$, we may let $[\alpha] = [(\widetilde{\alpha})] \in C_{\mathfrak{m}}$. This is well defined because if $\widetilde{\alpha}$ and $\widetilde{\alpha}'$ are liftings of α then $\nu_p(\frac{\widetilde{\alpha}}{\widetilde{\alpha}'} - 1) = \nu_p(\widetilde{\alpha} - \widetilde{\alpha}') - \nu_p(\widetilde{\alpha}) \geq 1 = \nu_p(\mathfrak{m})$ so $\frac{\widetilde{\alpha}}{\widetilde{\alpha}'} \in K_{\mathfrak{m},1}$.

By the Chebotarev Density Theorem (Theorem 7.4 in [Mil20]), since $C_{\mathfrak{m}}$ is abelian there exists a positive density of prime ideals $\mathfrak{q} \subset \mathcal{O}_K$ such that $(\mathfrak{q}, K_{\mathfrak{m}}/K) = \theta([\alpha])$. By Artin reciprocity (Theorem 0.8 in [Mil20]) and the fact that $(\mathfrak{q}, K_{\mathfrak{m}}/K) = \theta([\mathfrak{q}])$, we have $[\mathfrak{q}] = [\alpha]$. We conclude that $(\mathfrak{q}) = (\widetilde{\alpha}\beta)$ for $\beta \in K_{\mathfrak{m},1}$. Thus, $\mathfrak{q}$ is principal and may be written as $\mathfrak{q} = (q)$ for some prime $q \in \mathcal{O}_K$. It follows that $q = \widetilde{\alpha}\beta\varepsilon$ for $\varepsilon \in \mathcal{O}_K^\times$, so reducing both sides modulo p we have that $\phi_p(q) \in \alpha U$. □

Using this, we are able to answer our original question:

Theorem 7.7. *Let p be an odd rational prime inert in a number field K. Suppose that $U \subseteq (\mathcal{O}_K/p\mathcal{O}_K)^\times$ is the image of $\mathcal{O}_K^\times$ under reduction modulo $p\mathcal{O}_K$ and G is a subgroup satisfying $U \subseteq G \subseteq (\mathcal{O}_K/p\mathcal{O}_K)^\times$. Then there exists a prime $q \in \mathcal{O}_K$ such that if $S = \{q\mathcal{O}_K\}$ the image of $(\mathcal{O}_K^S)^\times$ under reduction modulo $p\mathcal{O}_K^S$ is G.*

Proof. Let $\alpha \in (\mathcal{O}_K/p\mathcal{O}_K)^\times$ be a generator of G. By Theorem 7.6 there exists a prime element $q \in \mathcal{O}_K$ satisfying $\phi_p(q) \in \alpha U$. We will show that such a q works. Setting $S = \{q\mathcal{O}_K\}$ we find that by the exactness at $\bigoplus_{\mathfrak{p}\notin S} K^\times/\mathcal{O}_{\mathfrak{p}}^\times$ in Theorem 11.6 of [NS13] that $(\mathcal{O}_K^S)^\times$ is generated by $\mathcal{O}_K^\times$ and q. Thus, the reduction of $(\mathcal{O}_K^S)^\times$ is generated by U and an element of αU, so it is equal to G. □

8 Cubic Fields

When considering totally real cubic fields, the problem of obtaining all subgroups of $U_{\mathbb{F}_{p^3}}$ becomes more complex due to the unit group having rank 2. We prove a theorem that suggests that this should be possible, by focusing on constructing number fields in which a unit of our choice becomes a Minkowski unit. Here, by Minkowski unit we mean a unit that forms a system of fundamental units with its conjugate. This property would be helpful because the conjugates of an element α of $\mathbb{F}_{p^n}$ are of the form α^{p^k} due to the Frobenius endomorphism. Thus, any subgroup of $\mathbb{F}_{p^3}$ generated by the reduction of a Minkowski unit of a number field K automatically contains the reduction of all of its conjugates. Therefore it contains the reduction of the system of fundamental units so it contains the reduction of the entire unit group.

In terms of constructing number fields to have Minkowski units with a given minimal polynomial, we have the following result on when the roots of a polynomial of the form $P(x) = x^3 + ax^2 + bx + 1$ are Minkowski units, subject to an assumption that they generate a Galois field and whose discriminant is not too far from $\mathrm{Disc}(P)$:

Theorem 8.1. *For a fixed positive integer D and constant $\varepsilon > 0$, there exists a constant $C = C(D, \varepsilon)$ such that the following holds. Assume integers a and b satisfy $|a|^{2-\varepsilon} > |b| > |a| + 2 > C$ and the number field K with defining polynomial $P(x) = x^3 + ax^2 + bx + 1$ is Galois. Furthermore assume $\mathbb{Z}[\alpha]$ for α a root of P has index $d < D$ inside $\mathcal{O}_K$. Then any two roots of P form a system of fundamental units for $\mathcal{O}_K$.*

Proof. First note that since $|b| > |a| + 2$ we have that either $P(1) = 2 + a + b$ or $P(-1) = a - b$ is negative. It follows by the Intermediate Value Theorem that P has a root between -1 and 1, we will call this root u. Then let the other two roots be s_1 and s_2. We see that at least one of $|s_1|, |s_2|$ is greater than 1 because the product $s_1 s_2 u$ is equal to -1. Furthermore, note that $|s_1|, |s_2| > 1$

because if one had absolute value less than 1, P would have two roots in the interval $[-1,1]$ so $P(1)$ and $P(-1)$ would be the same sign, but this is not possible from the fact that $P(1) = 2 + a + b$, $P(-1) = a - b$, and $|b| > |a| + 2$.

Since P has constant coefficient 1, each of u, s_1, and s_2 are units in $\mathcal{O}_K$. Since any choice of two roots from u, s_1, and s_2 form a system of units that generate the third one, it suffices to show that s_1 and s_2 form a system of fundamental units.

A result from Cusick [Cus84] states that the regulator R of K satisfies $R \geq \frac{1}{16}\log^2(\mathrm{Disc}(K)/4)$. Now, observe that $\mathrm{Disc}(K) = \frac{1}{d^2}\mathrm{Disc}(\mathbb{Z}[\alpha])$ by Proposition 3.22 from [Jar14]. It follows that

$$\mathrm{Disc}(K) = \frac{1}{d^2}\mathrm{Disc}(P) = \frac{1}{d^2}(-27 - 4a^3 + 18ab + a^2b^2 - 4b^3).$$

From the fact that $a^2 \gg |b| > |a| + 2$ this is greater than $\frac{1}{d^2}a^2b^2$ which is greater than $\frac{1}{d^2}b^3$ for sufficiently large a and b. Thus, we have that

$$R \geq \frac{1}{16}\log^2(\mathrm{Disc}(P)/4) \geq \frac{1}{16}\log^2\left(\frac{b^3}{d^2}\right) \geq \frac{1}{16}\log^2\left(\frac{b^3}{D^2}\right).$$

Since D is fixed, for sufficiently large b relative to D this is greater than $(1-\varepsilon_1)\cdot\frac{1}{16}\log^2(b^3) = (1-\varepsilon_1)\cdot\frac{9}{16}\log^2 b$ for any fixed $\varepsilon_1 > 0$, so that $R \geq (1-\varepsilon_1)\frac{9}{16}\log^2 b$.

At the same time, we have that the regulator R' of the system of fundamental units formed by r_1 and r_2 is

$$R' = \begin{vmatrix} \log|s_1| & \log|s_2| \\ \log|s_2| & \log|u| \end{vmatrix} = \begin{vmatrix} \log|s_1| & \log|s_2| \\ \log|s_2| & -\log|s_1s_2| \end{vmatrix} = \log^2|s_1| + \log|s_1|\log|s_2| + \log^2|s_2|.$$

Now, since $|s_1|, |s_2| > 1$, we have $\log|s_1|\log|s_2| \geq 0$ so

$$R' = \log^2|s_1| + \log|s_1|\log|s_2| + \log^2|s_2| \leq \log^2|s_1| + 2\log|s_1|\log|s_2| + \log^2|s_2| = \log^2|s_1s_2|.$$

We also have that $b = s_1s_2 + s_1u + s_2u = s_1s_2 + \frac{1}{s_2} + \frac{1}{s_1}$ so s_1s_2 is within 2 of b. Thus, for sufficiently large b we may approximate $R' \leq (1-\varepsilon_1)\log^2 b$ using the same sufficiently small $\varepsilon_1 > 0$. Setting ε_1 to be a constant such as 0.01, we may choose $C(D,\varepsilon)$ such that all of the "sufficiently large" conditions on a and b hold. For this value of $C(D,\varepsilon)$, we conclude that $R' \leq (1-\varepsilon_1)\log^2 b < \frac{16}{9}R < 2R$ by taking $\varepsilon_1 < 0.01$. Since $\frac{R'}{R}$ is the index of the units generated by s_1 and s_2 over the group of units in $\mathcal{O}_K$, it follows that $\frac{R'}{R}$ is a positive integer which is less than 2 so it must be 1, implying that s_1 and s_2 form a system of fundamental units. □

Due to this result, it suffices to consider the following: Let $f \in \mathbb{F}_p[x]$ be the minimal polynomial of a given generator of a subgroup G of $U_{\mathbb{F}_{p^3}}$. Then there exists a Galois field K defined by the polynomial $\widetilde{f}$ reducing to f modulo p such that f has large coefficients with respect to $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, where α denotes a root of $\widetilde{f}$.

9 Future directions

For the totally real cubic case, considering the problem for orders would also be interesting. For Theorem 8.1, the conditions may be be satisfied more often in specific orders. After constructing a polynomial of the form $x^3 + ax^2 + bx + 1$ with roots r_1 and r_2 which defines a number field K, it may be helpful to consider the unit group of the order $\mathbb{Z}[r_1, r_2]$ rather than the unit group of $\mathcal{O}_K$. This is because we expect $[\mathcal{O}_K : \mathbb{Z}[r_1]] > [\mathbb{Z}[r_1, r_2] : \mathbb{Z}[r_1]]$, loosening the conditions on a and b.

Additionally, in order to prove the totally real cubic case from Theorem 8.1, it becomes important to consider possible ways to construct families of Galois fields, which have been studied by Shanks [Sha74] in his consideration of cubic fields defined by polynomials of the form $x^3 - ax^2 - (a+3)x - 1$. Such fields are always Galois, but it is not always true that the minimal polynomial of a generator of a subgroup of $U_{\mathbb{F}_{p^3}}$ will be of such a form. Thus, we turn to Balady [Bal16], who gives a method of generating families of cubic fields and a result on these families similar to Theorem 8.1, conditional on the squarefreeness of a specific quantity. In combination with Poonen's work on squarefree values of multivalued polynomials ([Poo03]), it may be possible to use Balady's general families of polynomials to prove the cubic case.

Acknowledgments

I would like to thank my PRIMES mentor Alexander Petrov for his advice, patience, and guidance throughout this research project. I also thank the PRIMES-USA program for giving me the opportunity to conduct research on this topic.

References

[Bal16] Steve Balady. "Families of cyclic cubic fields". In: *Journal of Number Theory* 167 (Oct. 2016), pp. 394–406. DOI: 10.1016/j.jnt.2016.03.011.

[Cha] Robin Chapman. *Dirichlet's theorem for number fields.* MathOverflow. Posted by user https://mathoverflow.net/users/4213/robin-chapman. eprint: https://mathoverflow.net/q/29194.

[CKY00] Yen-Mei J. Chen, Yoshiyuki Kitaoka, and Jing Yu. "Distribution of units of real quadratic number fields". In: *Nagoya Mathematical Journal* 158 (2000), pp. 167–184. DOI: 10.1017/S0027763000007364.

[Cona] Keith Conrad. URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf.

[Conb] Keith Conrad. *Dirichlet's Unit Theorem.* URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/unittheorem.pdf.

[Conc] Keith Conrad. *Trace and Norm, II.* URL: https://kconrad.math.uconn.edu/blurbs/galoistheory/tracenorm2.pdf.

[Cus84] T. W. Cusick. "Lower bounds for regulators". In: *Number Theory Noordwijkerhout 1983.* Ed. by Hendrik Jager. Berlin, Heidelberg: Springer Berlin Heidelberg, 1984, pp. 63–73. ISBN: 978-3-540-38906-4.

[IK98] Masaru Ishikawa and Yoshiyuki Kitaoka. "On the distribution of units modulo prime ideals in real quadratic fields". In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 1998.494 (Jan. 1998), pp. 65–72. DOI: 10.1515/crll.1998.011.

[Jar14] Frazer Jarvis. *Algebraic Number Theory.* Springer International Publishing, 2014.

[JLW95] Michael J. Jacobson, Richard F. Lukes, and Hugh C. Williams. "An investigation of bounds for the regulator of Quadratic Fields". In: *Experimental Mathematics* 4.3 (Jan. 1995), pp. 211–225. DOI: 10.1080/10586458.1995.10504322.

[Kit06] Yoshiyuki Kitaoka. "Distribution of units of a cubic abelian field modulo prime numbers". In: *Journal of the Mathematical Society of Japan* 58.2 (Apr. 2006). DOI: 10.2969/jmsj/1149166789.

[Kit07] Yoshiyuki Kitaoka. "Distribution of units of an algebraic number field modulo an ideal". In: *Number Theory* (July 2007), pp. 39–96. DOI: 10.1142/9789812770134_0003.

[LN87] Rudolf Lidl and Harald Niederreiter. *Finite fields.* Cambridge Univ. Press, 1987.

[Mil20] J.S. Milne. *Class Field Theory (v4.03).* Available at www.jmilne.org/math/. 2020.

[Mor12] Pieter Moree. *Artin's primitive root conjecture -a survey -.* 2012. arXiv: math/0412262 [math.NT]. URL: https://arxiv.org/abs/math/0412262.

[MP13] Gary L. Mullen and Daniel Panario. *Handbook of Finite Fields.* CRC Press, 2013.

[Nar04] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers.* Springer, 2004.

[NS13] Jürge Neukirch and Norbert Schappacher. *Algebraic number theory.* 1st ed. Springer Berlin, 2013.

[Poo03] Bjorn Poonen. “Squarefree values of multivariable polynomials”. In: *Duke Mathematical Journal* 118.2 (June 2003). ISSN: 0012-7094. DOI: 10.1215/s0012-7094-03-11826-8. URL: http://dx.doi.org/10.1215/S0012-7094-03-11826-8.

[Rot98] Joseph Rotman. *Galois Theory*. 2nd edition. Springer-Verlag New York, 1998.

[Sha74] Daniel Shanks. “The simplest cubic fields”. In: *Mathematics of Computation* 28.128 (Oct. 1974), p. 1137. DOI: 10.2307/2005372.

[Ste08] Louboutin Stephane. “The fundamental unit of some quadratic, cubic or quartic orders”. In: *J. Ramanujan Math. Soc.* 23 (Jan. 2008), pp. 191–210.