university of groningen

faculty of science and engineering

Is there a fake function field analogue of the Ankeny-Artin-Chowla conjecture?

Master Project Mathematics

September 2024

Student: J. Pruim

First supervisor: Prof. dr. Steffen Müller

Second supervisor: Prof. dr. Jaap Top

Abstract

Let $D \equiv 1 \mod 4$ be a prime. Then the Ankeny-Artin-Chowla conjecture claims that for the smallest $a, b \in \mathbb{N}$ that satisfy $a^2 - Db^2 = \pm 4$, we have that $D \nmid b$. Inspired by a similar notion in the case of number fields, we describe fake real quadratic orders in function fields and use these to formulate an analogue of the Ankeny-Artin-Chowla conjecture. We find that this analogue is false in general. We provide horizontal asymptotics when the constant field is finite, which are largely inspired by unpublished work of Florian Hess, Renate Scheidler and Michael John Jacobson. We also find conditions under which the analogue holds and we observe what happens when changing the fake real quadratic order in natural ways.

Word of Thanks

I wish to thank my supervisors Steffen Müller and Jaap Top for their help, motivation and patience. I furthermore wish to thank Florian Hess for helping me discover how I could mimic some of the ideas in [11] in a number field setting towards a function field setting in my Thesis. Additionally I thank him for the proof of an important step in my proof of Theorem 7.4.5, which he provided in [9].

Contents

1 Introduction

Let $D > 0$ be a prime number that is congruent to 1 modulo 4 and let $K = \mathbb{Q}(\sqrt{D})$. Then the ring of integers $\mathcal{O}_K$ can be calculated to be $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. According to Dirichlet's unit theorem, the unit group $\mathcal{O}_K^\times$ then has rank 1, meaning $\mathcal{O}_K^\times = \mathrm{Tor}(\mathcal{O}_K^\times) \times \epsilon^{\mathbb{Z}}$ for some $\epsilon \in \mathcal{O}_K^\times \setminus \mathrm{Tor}(\mathcal{O}_K^\times)$. Write $\epsilon = \frac{a+b\sqrt{D}}{2}$ for some $a, b \in \mathbb{Z}$ such that $a \equiv b \mod 2$.

In 1952, Ankeny, Artin and Chowla conjectured that $D \nmid b$. This hypothesis is refered to as the Ankeny-Artin-Chowla conjecture. Up to this day, a counterexample has not been found and van der Poorten, te Riele and Williams verified the conjecture for all $D < 2 \cdot 10^{11}$ that are congruent to 1 modulo 4.

Consequently, researchers have started analyzing various analogous criteria to the Ankeny-Artin-Chowla conjecture. Firstly, Louis J. Mordell wondered if this would be the case if D is congruent to 3 modulo 4. (In which case $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$.) In 2024, Andreas Reinhart answered this by finding that $D = 39028039587479$ gives a counterexample.

Secondly, Henri Cohen suggested that by considering the fundamental unit of a so called fake real quadratic order, an analogy can be made, to which he found counterexamples. This fake real quadratic order is obtained by extending a real quadratic order by the inverse of a prime ideal.

Thirdly, Jing Yu and Jiu-Kang Yu have shown that the natural function field analogue of the Ankeny-Artin-Chowla conjecture holds. This analogue states that given a field k and a squarefree $f \in k[x]$, assuming $\mathcal{O}_K^\times = k[x, \sqrt{f}]^\times$ is not torsion, its fundamental unit $a + b\sqrt{f}$ for $a, b \in k[x]$ satisfies $f \nmid b$.

In this project we propose yet another analogy using fake real quadratic orders in a function field setting, which combines the ideas of Henri Cohen and Jing Yu and Jiu-Kang Yu. Let k be perfect of characteristic $\ell \neq 2$. To every squarefree $f \in k[x]$ and irreducible $p \in k[x]$, there corresponds a fake real quadratic order, for which we ask if the fundamental unit $a + b\sqrt{f}$ satisfies $f \nmid b$. We refer to this property as the f.f. fake Ankeny-Artin-Chowla property. We find many counterexamples to this property, but also found a criterion under which it always holds. Next to this, we calculate the proportion of counterexamples when fixing f and varying p. This proportion is related to the Ray Class Group, which is discussed in Subsection 2.3. We furthermore compare related fake real quadratic orders, constructed by extending the constant field or by reducing a quadratic order over $\mathbb{Q}$ to a quadratic order over $\mathbb{F}_\ell$ for some appropriate prime ℓ.

In Section 2, we provide some preliminary material. After that, in Section 3, we discuss the construction that is also used to make fake real quadratic orders. In Section 4, I discuss the original Ankeny-Artin-Chowla conjecture and Mordell's variant on it. Subsequently in Section 5, we go over the analogy by Henry Cohen. We study the (real) function field analogue in Section 6. The main section is Section 7, which is about the analogous fake function field situation we are proposing. In Section 8, we give a conclusion and summary, additionally we pose some open questions.

2 Preliminaries

In this thesis, we assume that the reader is familiar with the basics of commutative algebra, algebraic geometry and algebraic number theory. Recommended material for this is found in [3], [7], [24]. Next to this, there is some additional preliminary theory that I will give in this section. We start off with a few definitions. Then in Subsection 2.1, we give the basics of hyperelliptic curves and (their) Jacobians. In Subsection 2.2, we describe the group $(R[\sqrt{D}]/D)^\times$ for a Unique Factorisation Domain R and a squarefree element $D \in R$. Lastly in Subsection 2.3, we go over the theory on Ray Class Groups and Class Field Theory.

Definition 2.0.1. For any commutative ring A with 1 and ideal $I \leq A$ of finite index, we define $N(I) := N_A(I) := \#(A/I)$.

Definition 2.0.2. For any finite extension of fields L/K and any $\alpha \in L$, we define $N(\alpha) := N_{L/K}(\alpha)$ to be the determinant of the K-linear map $L \to L$ given as sending any $\beta \in L$ to $\alpha\beta$.

The above definitions have been taken from [24, pages 41-42].

Definition 2.0.3. For a field k, we write $\overline{k}$ for the algebraic closure of k.

Proposition 2.0.4. *Let k be a field of characteristic ℓ. The following are equivalent.*

1. *Every irreducible polynomial over k has no multiple roots in $\overline{k}$.*
2. *Every irreducible polynomial over k has a non-zero formal derivative.*
3. *Every irreducible polynomial over k is separable.*
4. *Every finite extension of k is separable.*
5. *Every algebraic extension of k is separable.*
6. *Either $\ell = 0$ or every element of k is an ℓ-th power*
7. *Either $\ell = 0$ or the Frobenius map $x \to x^\ell$ is an automorphism of k.*
8. *Any separable closure of k is isomorphic to any algebraic closure of k.*

We call k perfect if these statements hold.

Examples of perfect fields are fields of characteristic 0, algebraically closed fields, finite fields and algebraic extensions of perfect fields. An example of an imperfect field is $k(x)$, where k is a field of characteristic $\ell > 0$ and x is transcendental over k. This is because x is not an ℓ-th power in $k(x)$. See [4, page 10].

Definition 2.0.5. Let G be a finite abelian group and let ℓ be a prime number. We define the ℓ-rank of G to be the dimension of $G/\ell G$ viewed as a $\mathbb{F}_\ell$-vector space.

Note that if G is a finite abelian group, we can find an isomorphism $G \to \prod_{i=1}^{n}(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$ for some $p_1, \ldots, p_n \in \mathbb{N}_{\geq 0}$ and $r_1, \ldots, r_n \in \mathbb{N}_{\geq 0}$, where the p_i are primes. Then we see that $G/\ell G \cong (\mathbb{Z}/\ell\mathbb{Z})^{\#\{i \leq n : p_i = \ell\}}$ the ℓ-rank of G is given as $\#\{i \leq n : p_i = \ell\}$. From here, it is not too hard to see that the ℓ-rank is the maximal number of linearly independent elements of G of order ℓ, where we view G as a $\mathbb{Z}$-module. See [20].

2.1 Hyperelliptic curves and Jacobians

The main reference in this subsection is given in [25].

Definition 2.1.1 (Weighted projective plane)**.** Let k be a field. For $(d_1, d_2, d_3) \in \mathbb{Z}^3$, we define $\mathbb{P}^2_{(d_1,d_2,d_3)}$ to be the geometric object such that $\mathbb{P}^2_{(d_1,d_2,d_3)}(k) := (k^3 \setminus \{0\})/\sim$, where $(\chi, \eta, \zeta) \sim (\chi', \eta', \zeta')$ if $\exists \lambda \in \overline{k}$ s.t. $(\chi', \eta', \zeta') = (\lambda^{d_1}\chi', \lambda^{d_2}\eta', \lambda^{d_3}\zeta')$. We denote $(\chi : \eta : \zeta)$ for the equivalence class of $(\chi, \eta, \zeta) \in k^3 \setminus \{0\}$. The coordinate ring of $\mathbb{P}^2_{(d_1,d_2,d_3)}$ is $k[x, y, z]$ with grading such that x has degree d_1, y has degree d_2 and z has degree d_3. In this way, it turns out that we can view $\mathbb{P}^2_{(d_1,d_2,d_3)}$ as a projective variety in the usual sense. We also denote $\mathbb{P}^2_g := \mathbb{P}^2_{(1,g+1,1)}$.

Definition 2.1.2. Let $g \in \mathbb{N}_{\geq 0}$. Notice that we can inject $\mathbb{A}^2(k)$ into $\mathbb{P}^2_g(k)$ in at least two ways: $(\chi, \eta) \to (\chi : \eta : 1)$ and $(\chi, \eta) \to (1 : \chi : \eta)$. We will call the images of these two injections the standard affine patches of $\mathbb{P}^2_g$. The union of the images of these two injections is $\mathbb{P}^2_g(k) \setminus \{(0 : 1 : 0)\}$.

For $g > 0$, the weighted projective plane $\mathbb{P}^2_g$ is smooth everywhere except at $(0 : 1 : 0)$, so every smooth point lies on one of the standard affine patches.

Definition 2.1.3 (Hyperelliptic curve)**.** Let $g \in \mathbb{N}$. Let k be a field with characteristic unequal to 2. A hyperelliptic curve of genus g over k is the subvariety of $\mathbb{P}^2_g$ defined by an equation of the form $y^2 = F(x, z)$ where $F \in k[x, z]$ is homogeneous of degree $2g + 2$ and squarefree in $\overline{k}[x, z]$. We call the affine curves $y^2 = F(x, 1)$ and $y^2 = F(1, z)$ its standard affine patches.

The term hyperelliptic curve often excludes elliptic curves and genus 0 curves in literature, however for our purposes, we make a different convention. If $g > 0$, note that that $(0 : 1 : 0)$ is not a point on the curve and so since F is squarefree in $\overline{k}[x, z]$, we see this implies that hyperelliptic curves are smooth. For $g = 0$, the point $(0 : 1 : 0)$ is not even singular in $\mathbb{P}^2_g = \mathbb{P}^2$, so also those hyperelliptic curves are smooth. Furthermore, because F is squarefree in $k[x, z]$, we have that hyperelliptic curves are geometrically irreducible.

Definition 2.1.4. An *algebraic group* G over a field k is a variety such that $G(k)$ is a group, the group law extends to a morpism $G \times G \to G$ and inversion extends to a morphism $G \to G$.

Definition 2.1.5. An *abelian variety* is an algebraic group which is projective.

Elliptic curves are the most famous examples of abelian varieties. Unfortunately for $g > 1$, an hyperelliptic curve is no longer an abelian variety. However, we can still consider a related abelian variety called the Jacobian.

Theorem 2.1.6 (Jacobian)**.** *For any smooth projective geometrically irreducible curve C of genus g over a field k, there exists an abelian variety J over k of dimension g, unique up to isomorphism over k s.t. $J(L) \cong Pic^0_C(L)$ for all*

fields $k \subseteq L \subseteq \overline{k}$. We call J the Jacobian of C. Here $Pic_C^0(L)$ is the subgroup of the divisor class group consisting of the elements with degree 0.

Proof. A sketch of the proof can be found in [12, pages 136-138]. □

The special thing about hyperelliptic curves where $F(x,1)$ is of odd degree is that there is actually an algorithm for computing within the Jacobian, which I skip over for now. It can be found in [5, pages 95-101].

Corollary 2.1.7. *For C as in Theorem 2.1.6 over a finite field k, the Picard group $Pic_C^0(k)$ is finite.*

Definition 2.1.8. Let ℓ be a prime and let $C : y^2 = F(x,z)$ be a hyperelliptic curve over $\mathbb{Q}_\ell$. We can without loss of generality assume $F \in \mathbb{Z}_\ell[x,z]$. Then we define a new curve $\tilde{C} : y^2 = \overline{F}(x,z)$ over $\mathbb{F}_\ell$ (subvariety of $\mathbb{P}^2_{\mathbb{F}_\ell,g}$), we call this the reduction of C modulo ℓ.

If C is defined over $\mathbb{Q}$, then we just copy this terminology by viewing it as a curve over $\mathbb{Q}_\ell$. We call ℓ a prime of good reduction if $\overline{F}$ if $\overline{C}$ is smooth (which is equivalent to $\overline{F}$ being squarefree for $\ell \neq 2$) and a prime of bad reduction otherwise.

Assume that C has some k-rational point P_0 and let $i : C \to J$ be the function that sends any P to $[P - P_0]$. It extends to a morphism of varieties, which is injective if $g > 0$. Also for C over $\mathbb{Q}_p$ and a prime ℓ, there is a map $C(\mathbb{Q}_\ell) \to \tilde{C}(\mathbb{F}_\ell)$. Note that any element of $C(\mathbb{Q}_\ell)$ can be written as $(\chi : \eta : \zeta)$ with $\chi, \eta, \zeta \in \mathbb{Z}_\ell$ where ℓ does not divide all χ, η, ζ. Then this map sends this to $(\overline{\chi} : \overline{\eta} : \overline{\zeta})$. One can check that this is well-defined. This map can be restricted to a map $C(\mathbb{Q}) \to \tilde{C}(\mathbb{F}_\ell)$.

Lemma 2.1.9. *Let C be a hyperelliptic curve over $\mathbb{Q}$. Then there is a commutative square*

$$\begin{array}{ccc} C(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}) \\ \downarrow & & \downarrow \\ \tilde{C}(\mathbb{F}_\ell) & \longrightarrow & \tilde{J}(\mathbb{F}_\ell). \end{array}$$

for any prime ℓ of good reduction. Here the map $J(\mathbb{Q}) \to \tilde{J}(\mathbb{F}_\ell)$ is induced by $C(\overline{\mathbb{Q}}) \to \tilde{C}(\overline{\mathbb{F}_\ell})$, through divisors. The same is true when replacing each $\mathbb{Q}$ by $\mathbb{Q}_\ell$.

There is also a generalization, extending $\mathbb{Q}$ to a number field k. Let $\mathcal{O}_k$ be its ring of integers and let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_k$. Let $\tilde{C}$ be the curve obtained by reducing equations modulo $\mathfrak{q}$. Then there is a reduction map $C(k) \to \tilde{C}(\mathcal{O}_K/\mathfrak{q})$ that sends a $(\chi : \eta : \zeta)$ with $\chi, \eta, \zeta \in \mathcal{O}_k$, not all in $\mathfrak{q}$, to $(\overline{\chi} : \overline{\eta} : \overline{\zeta})$. Again, we leave checking it is well-defined as an exercise to the reader.

Theorem 2.1.10. *Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_k$ such that $\tilde{C}$ is smooth. Then there is a natural injective group homomorphism $J(k)_{tors} \to \tilde{J}(\mathcal{O}_k/\mathfrak{q})$ induced by the map $C(\overline{k}) \to \tilde{C}(\overline{\mathcal{O}_k/\mathfrak{q}})$. Here $J(k)_{tors}$ is the torsion subgroup of $J(k)$.*

Proof. The proof can be found in [12, Theorem C.1.4 and Theorem C.2.6]. □

Corollary 2.1.11. *Let ℓ be a prime of good reduction. Then there is a natural injection $J(\mathbb{Q})_{tors} \to \tilde{J}(\mathbb{F}_\ell)$. The same holds when replacing $\mathbb{Q}_\ell$ by $\mathbb{Q}$.*

Proof. Apply Theorem 2.1.10 to $k = \mathbb{Q}$. □

2.2 Describing the residue unit group $(R[\sqrt{D}]/D)^\times$

Let R be a Unique Factorisation Domain and let $D \in R$ be squarefree; meaning the factorisation of D has no multiple factors. We wish to describe the residue unit group $(R[\sqrt{D}]/D)^\times$.

Lemma 2.2.1. *There is an injective group homomorphism $R/D \to (R[\sqrt{D}]/D)^\times$, given by sending $\overline{r} \in R/D$ to $1 + \overline{r}\sqrt{D}$. As a consequence, there is a subgroup $A \subseteq (R[\sqrt{D}]/D)^\times$ that is isomorphic to the additive group of R/D.*

Proof. We construct a group homomorphism $R \to (R[\sqrt{D}]/D)^\times$ by sending $r \in R$ to $\overline{1 + r\sqrt{D}}$. This is a group homomorphism because

$$\overline{(1 + r_1\sqrt{D})(1 + r_2\sqrt{D})} = \overline{1 + (r_1 + r_2)\sqrt{D} + r_1 r_2 D} = \overline{1 + (r_1 + r_2)\sqrt{D}}$$

for any $r_1, r_2 \in D$. Now this group homomorphism clearly has kernel $D \cdot R$, so an injection $R/D \to (R[\sqrt{D}]/D)^\times$ is induced. □

There is also the natural ring homomorphism $R \to R[\sqrt{D}]/D$, which has kernel $D \cdot R$. Therefore, there is an injective ring morphism $R/D \to R[\sqrt{D}]/D$. So it also induces the injective group homomorphism $(R/D)^\times \to (R[\sqrt{D}]/D)^\times$. Let B denote its image. We notice that $B \cong (R/D)^\times \cong \prod_i (R/D_i)^\times$ where $D = \prod_i D_i$ is the decomposition of D into irreducibles.

Proposition 2.2.2. *We have $(R[\sqrt{D}]/D)^\times = A \times B \cong (R/D) \times (R/D)^\times$.*

Proof. It is clear that $A \cap B = (1)$, since it consists of all elements $a + b\sqrt{D}$ such that $a = 1$ and $b = 0$. Let $\overline{r + s\sqrt{D}} \in (R[\sqrt{D}]/D)^\times$ be arbitrary. Then $\overline{(r + s\sqrt{D})(r - s\sqrt{D})} = \overline{r}^2$. This shows $\overline{r} \in (R/D)^\times$. So we can write $\overline{r + s\sqrt{D}} = \overline{r}(1 + \overline{sr^{-1}}\sqrt{D})$ and so $\overline{r + s\sqrt{D}} \in A \times B$. □

Example 2.2.3. *Let $R = \mathbb{Z}$. Then $(\mathbb{Z}[\sqrt{D}]/D)^\times \cong (\mathbb{Z}/D\mathbb{Z}) \times (\mathbb{Z}/D\mathbb{Z})^\times$ for $D \in \mathbb{Z}$ squarefree, according to Proposition 2.2.2.*

We can also note the following:

Proposition 2.2.4. *Let $R[\sqrt{D}] \subseteq S \subseteq Frac(R[\sqrt{D}])$ be an intermediate ring satisfying $S \cap \frac{1}{D}R[\sqrt{D}] = R[\sqrt{D}]$. Then $S/D \cong R[\sqrt{D}]/D$ as rings. Therefore, their unit groups are isomorphic as well.*

Proof. It suffices to show that the map $R[\sqrt{D}] \to S \to S/D$ has kernel $D \cdot R[\sqrt{D}]$. The kernel can be described as $R[\sqrt{D}] \cap D \cdot S$. Then this fact follows directly by our assumption. □

Remark 2.2.5. This subsection is a generalization of ideas used in [11], in which the relevant example is $S = \mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{D})$ is an imaginary quadratic number field with $D < -2$.

2.3 Ray Class Groups and Class Field Theory

The main source of this subsection is [10].

Let K be a global field, meaning it is either a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_q(x)$, where q is a prime power and x is transcendental over $\mathbb{F}_q$.

Definition 2.3.1. We call a (formal) finite product of places $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})}$ a *modulus* if $v_{\mathfrak{p}}(\mathfrak{p}) \geq 0$ for all places $\mathfrak{p}$ and furthermore

1. If K is a number field, then $v_{\mathfrak{p}}(\mathfrak{m}) \leq 1$ for all real infinite places $\mathfrak{p}$ and $v_{\mathfrak{p}}(\mathfrak{m}) = 0$ for all complex infinite places $\mathfrak{p}$.
2. If K is a function field, then $v_{\mathfrak{p}}(\mathfrak{m}) = 0$ for all infinite places $\mathfrak{p}$.

Definition 2.3.2. Let $a \in K^\times$, $n \geq 0$ and $\mathfrak{p}$ a place of K. We say $a \equiv^* 1 \mod \mathfrak{p}^n$ if

1. $v_{\mathfrak{p}}(a-1) \geq n$ for $\mathfrak{p}$ a finite place.
2. $\sigma(a) \geq 0$ for $\mathfrak{p}$ a real infinite place with corresponding real embedding $\sigma : K \to \mathbb{R}$, if K is a number field.

Definition 2.3.3. Let $a \in K^\times$ and $\mathfrak{m}$ a modulus. We say $a \equiv^* 1 \mod \mathfrak{m}$ if $a \equiv^* 1 \mod \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})}$ for all places $\mathfrak{p}$ dividing $\mathfrak{p}$.

If K is a function field with constant field k, we let $\mathcal{O}_K$ be the integral closure of $k[t]$ in K. In the number field case, we just let $\mathcal{O}_K$ be the ring of integers as usual.

Proposition 2.3.4. *Let $\mathfrak{m}_0$ be the finite part of $\mathfrak{m}$. Then*

$$\mathfrak{I}_{\mathfrak{m}} := \{I \text{ fractional ideal of } K : v_{\mathfrak{p}}(I) = 0 \ (\forall \mathfrak{p} | \mathfrak{m}_0)\}$$

is a subgroup of the group of fractional ideals and

$$\mathcal{P}_{\mathfrak{m}} := \{\alpha \cdot \mathcal{O}_K : \alpha \in K^\times, \alpha \equiv^* 1 \mod \mathfrak{m}\}$$

is a subgroup of $\mathfrak{I}_{\mathfrak{m}}$.

Proof. For any $I, J \in \mathfrak{I}_{\mathfrak{m}}$, we have $v_{\mathfrak{p}}(IJ^{-1}) = v_{\mathfrak{p}}(I) - v_{\mathfrak{p}}(J) = 0 - 0 = 0$ for all $\mathfrak{p}|\mathfrak{m}_0$. Hence $IJ^{-1} \in \mathcal{I}_{\mathfrak{m}}$. This shows $\mathfrak{I}_{\mathfrak{m}}$ is a subgroup of the group of fractional ideals.

Let $\alpha, \beta \in K^\times$ satisfy $\alpha, \beta \equiv^* 1 \mod \mathfrak{m}$. Then for any finite place $\mathfrak{p}$ we have

$$\begin{aligned} v_\mathfrak{p}(\alpha\beta^{-1} - 1) &= v_\mathfrak{p}((\alpha - 1)(\beta^{-1} + 1)) + (\beta^{-1} - 1) + (1 - \alpha)) \\ &\geq \min\{v_\mathfrak{p}(\alpha - 1) + v_\mathfrak{p}(\beta^{-1} + 1), v_\mathfrak{p}(\beta^{-1} - 1), v_\mathfrak{p}(1 - \alpha)\} \\ &\geq \min\{v_\mathfrak{p}(\mathfrak{m}), v_\mathfrak{p}(\mathfrak{m}), v_\mathfrak{p}(\mathfrak{m})\} = v_\mathfrak{p}(\mathfrak{m}). \end{aligned}$$

Here, we used that $v_\mathfrak{p}(\beta^{-1} + 1) \geq \min\{v_\mathfrak{p}(\beta^{-1} - 1), v_\mathfrak{p}(2)\} \geq \min\{v_\mathfrak{p}(\mathfrak{m}), 0\} \geq 0$ if the characteristic of K is unequal to 2 and $v_\mathfrak{p}(\beta^{-1} + 1) = v_\mathfrak{p}(\beta^{-1} - 1) \geq v_\mathfrak{p}(\mathfrak{m}) \geq 0$ if this characteristic equals 2.

Also $\sigma(\alpha\beta^{-1}) = \sigma(\alpha)\sigma(\beta)^{-1} \geq 0$ for real embeddings σ in case K is a number field, so we see that $\alpha\beta^{-1} \equiv^* 1 \mod \mathfrak{m}$. This has shown that $\mathcal{P}_\mathfrak{m}$ is a subgroup of the group of fractional ideals.

Furthermore we need to show that $v_\mathfrak{p}(\alpha \cdot \mathcal{O}_K) = 0$ for all $\mathfrak{p}|\mathfrak{m}_0$. Well, we observe that $\alpha \cdot \mathcal{O}_K, (\alpha - 1) \cdot \mathcal{O}_K$ are coprime ideals, for their sum contains $\alpha - (\alpha - 1) = 1$. Therefore, $\mathfrak{p}$ does not divide both ideals and by assumption, it divides $(\alpha - 1) \cdot \mathcal{O}_K$ at least $v_\mathfrak{p}(\mathfrak{m}) \geq 1$ times. This shows $\mathfrak{p}$ does not divide $\alpha \cdot \mathcal{O}_K$. □

Definition 2.3.5. We define

$$\mathrm{Cl}^0_\mathfrak{m}(K) := \mathfrak{I}_\mathfrak{m}/\mathcal{P}_\mathfrak{m}.$$

For the above definition, note that the relevant subgroup is actually a subgroup. We have the following result:

Theorem 2.3.6. *Let $\mathfrak{m}$ be a modulus with trivial infinite part $\mathfrak{m}_\infty$. If K is a number field, then there is an exact sequence*

$$1 \longrightarrow \{\pm 1\} \longrightarrow (\mathcal{O}_K/\mathfrak{m})^\times \longrightarrow Cl^0_\mathfrak{m}(K) \longrightarrow Cl^0(K) \longrightarrow 1.$$

If K is a function field with constant field k, then there is an exact sequence

$$1 \longrightarrow k^\times \longrightarrow (\mathcal{O}_K/\mathfrak{m})^\times \longrightarrow Cl^0_\mathfrak{m}(K) \longrightarrow Cl^0(K) \longrightarrow 1.$$

Proof. All maps are constructed in the natural way; but before we check exactness, we first check whether they are well-defined. The map $(\mathcal{O}_K/\mathfrak{m})^\times \to \mathrm{Cl}^0_\mathfrak{m}(K)$ is constructed as sending $\overline{\alpha} \in (\mathcal{O}_K/\mathfrak{m})^\times$ to $[\alpha \cdot \mathcal{O}_K]_\mathfrak{m}$. Suppose $\alpha, \beta \in \mathcal{O}_K$ and assume that $\overline{\alpha} = \overline{\beta} \in (\mathcal{O}_K/\mathfrak{m})^\times$. It follows that $\alpha\beta^{-1} \equiv^* 1 \mod \mathfrak{m}$, hence $[\alpha \cdot \mathcal{O}_K]_\mathfrak{m} = [\beta \cdot \mathcal{O}_K]_\mathfrak{m}$.

The map $\mathrm{Cl}^0_\mathfrak{m}(K) \to \mathrm{Cl}^0(K)$ is defined as sending $[I]_\mathfrak{m}$ to $[I]$. Let us show that this map is well-defined. Suppose fractional ideals I, J satisfy $[I]_\mathfrak{m} = [J]_\mathfrak{m}$. Then $IJ^{-1} = a \cdot \mathcal{O}_K$ for some $a \equiv^* 1 \mod \mathfrak{m}$. In particular, IJ^{-1} is principal, so $[I] = [J]$.

Now we will show that this sequence is exact. It is clear that $\{\pm 1\} \to (\mathcal{O}_K/\mathfrak{m})^\times$ or $k^\times \to (\mathcal{O}_K/\mathfrak{m})^\times$ respectively is injective. Surjectivity of $\mathrm{Cl}^0_\mathfrak{m}(K) \to \mathrm{Cl}^0(K)$ comes from the fact that each ideal is equivalent to an ideal coprime to

$\mathfrak{m}$, which is implied by the approximation theorem. (See also [24, page 27]) Also note that the sequence is exact at $\mathrm{Cl}^0_{\mathfrak{m}}(K)$. □

Let $E|K$ be a finite abelian field extension and let $\mathfrak{p}$ be a non-zero prime ideal of K. Then we claim there is a unique $\sigma \in \mathrm{Gal}(E|K)$ that induces the Frobenius morphism $\mathcal{O}_E/\mathfrak{P} \to \mathcal{O}_E/\mathfrak{P}$ for all prime ideals $\mathfrak{P}$ of $\mathcal{O}_E$ above $\mathfrak{p}$. This fact induces a mapping $\mathrm{Spec}(\mathcal{O}_K) \setminus \{0\} \to \mathrm{Gal}(E|K)$. By unique factorisation of prime ideals in $\mathcal{O}_K$, this induces a group homomorphism $I_K \to \mathrm{Gal}(E|K)$, where I_K is the set of fractional ideals of K, hence also when restricting to the ideals coprime to a modulus $\mathfrak{m}$.

Definition 2.3.7. We say $\mathfrak{m}$ is a modulus of $E|K$ if under the group homomorphism $I_K \to \mathrm{Gal}(E|K)$ described above, all principal ideals coprime to $\mathfrak{m}$ are mapped to the identity map.

In this case, there is an induced group homomorphism $\mathrm{Cl}^0_{\mathfrak{m}}(K) \to \mathrm{Gal}(E|K)$, which we call the Artin map. Fact: the Artin map is always surjective by [10, Theorem 3.3].

Theorem 2.3.8. *Let $\mathfrak{m}$ be a modulus. Then for every subgroup H of $Cl^0_{\mathfrak{m}}(K)$ there exists a unique field $E|K$ s.t. $\mathfrak{m}$ is a modulus of $E|K$ and H is the kernel of the surjective Artin map $Cl^0_{\mathfrak{m}}(K) \to Gal(E|K)$. We call E the ray class field corresponding to $\mathfrak{m}$.*

Theorem 2.3.9 (Chebatorev Density Theorem, [14])**.** *Let X be a subset of $Gal(E|K)$. The density of primes of $\mathcal{O}_K$ that correspond under the Artin map to an element of X is equal to $\frac{\#X}{\#Gal(E|K)}$.*

3 Extending Dedekind domains by inverses of prime ideals

In this section, we will study the ring obtained by extending a Dedekind domain by inverses of prime ideals. This construction is essential for defining and understanding so called fake real quadratic orders.

3.1 Inverting a single prime ideal

Let A be a Dedekind domain with field of fractions K. Then recall that any non-zero fractional ideal can be inverted.

Definition 3.1.1. Let $\mathfrak{p}$ be a non-zero prime ideal. We let $A[\mathfrak{p}^{-1}] := \bigcup_{i=0}^{\infty} \mathfrak{p}^{-i}$.

Lemma 3.1.2. *The elements of $A[\mathfrak{p}^{-1}]$ are precisely the elements of K that have non-negative valuation at every prime ideal except $\mathfrak{p}$.*

Proof. Suppose $x \in K$ has $v_{\mathfrak{q}}(x) \geq 0$ for all $\mathfrak{q} \neq \mathfrak{p}$. Consider the ideal xA, let its prime factorisation be $\mathfrak{p}^{v_{\mathfrak{p}}(x)} \prod_{\mathfrak{q}} \mathfrak{q}^{v_{\mathfrak{q}}(x)}$. Then we see that therefore $xA \subset \mathfrak{p}^{v_{\mathfrak{p}}(x)} \subseteq A[\mathfrak{p}^{-1}]$. □

Corollary 3.1.3. *The set $A[\mathfrak{p}^{-1}]$ is a subring of K.*

Proof. If $x, y \in K^{\times}$ have non-negative valuation at a prime ideal $\mathfrak{q} \neq \mathfrak{p}$, then $v_{\mathfrak{q}}(xy) = v_{\mathfrak{q}}(x) + v_{\mathfrak{q}}(y) \geq 0$ and $v_{\mathfrak{q}}(x \pm y) \geq \min\{v_{\mathfrak{q}}(x), v_{\mathfrak{q}}(y)\} \geq 0$. Furthermore, $v_{\mathfrak{q}}(1) = 0 \geq 0$. □

If A is a discrete valuation ring, then $A[\mathfrak{p}^{-1}] = K$, so let us from now on assume A is not a Discrete Valuation Ring. In this subsection, we prove that $A[\mathfrak{p}^{-1}]$ is a Dedekind domain and we describe its unit group and ideal class group.

Lemma 3.1.4. *The map $\{$integral ideals of A coprime to $\mathfrak{p}\} \to \{$integral ideals of $A[\mathfrak{p}^{-1}]\}$ given by $\mathfrak{a} \to \mathfrak{a}A[\mathfrak{p}^{-1}]$ is an order-preserving bijection.*

Proof. It is clear that it is order-preserving, let me now show that it is bijective. Suppose $\mathfrak{a}_1 A[\mathfrak{p}^{-1}] = \mathfrak{a}_2 A[\mathfrak{p}^{-1}]$. Then the set of elements of non-negative valuation at $\mathfrak{p}$ is $\mathfrak{a}_1 = \mathfrak{a}_2$, showing injectivity. Now let $\mathfrak{b}$ be an ideal of $A[\mathfrak{p}^{-1}]$. Then we claim that $\mathfrak{b} = (\mathfrak{b} \cap A)A[\mathfrak{p}^{-1}]$. To see one inclusion, let $x \in \mathfrak{b}$ be arbitrary. Then there is a k s.t. $x \in \mathfrak{p}^{-k}$. So $x\mathfrak{p}^k \subseteq \mathfrak{p}^{-k}\mathfrak{p}^k = A$. Also, clearly $x\mathfrak{p}^k \subseteq \mathfrak{b}$, because $x \in \mathfrak{b}$. So $x\mathfrak{p}^k \subseteq \mathfrak{b} \cap A$ and hence $x \in \mathfrak{p}^{-k}(\mathfrak{b} \cap A) \subseteq (\mathfrak{b} \cap A)A[\mathfrak{p}^{-1}]$. The other inclusion is clear.

Since this is order preserving and A is Noetherian by being a Dedekind domain, this also implies that $A[\mathfrak{p}^{-1}]$ is Noetherian. □

Corollary 3.1.5. *In particular, this shows that $A[\mathfrak{p}^{-1}]$ is Noetherian.*

Lemma 3.1.6. *For any integral ideal $\mathfrak{a}$ of A coprime to $\mathfrak{p}$, we have $A/\mathfrak{a} \cong A[\mathfrak{p}^{-1}]/\mathfrak{a}A[\mathfrak{p}^{-1}]$. In particular, the bijection given in Lemma 3.1.4 sends prime ideals to prime ideals and maximal ideals to maximal ideals.*

Proof. Let φ be the composition $A \to A[\mathfrak{p}^{-1}] \to A[\mathfrak{p}^{-1}]/\mathfrak{a}A[\mathfrak{p}^{-1}]$. First off, I wish to show that it is surjective. Let $x \in A[\mathfrak{p}^{-1}]$ be arbitrary. Let $k = v_{\mathfrak{p}}(x)$. Because $\mathfrak{a}$ is coprime to $\mathfrak{p}^k$, there exist some $a \in \mathfrak{a}$ and $u \in \mathfrak{p}^k$ s.t. $a + u = 1$. Hence $ax + ux = x$ and since $ax \in \mathfrak{a}A[\mathfrak{p}^{-1}]$, we have $\overline{x} = \overline{ux}$ in $A[\mathfrak{p}^{-1}]/\mathfrak{a}A[\mathfrak{p}^{-1}]$. Note that $v_{\mathfrak{p}}(ux) = 0$, so $ux \in A$.

Now note that $\ker(\varphi) = A \cap \mathfrak{a}A[\mathfrak{p}^{-1}]$, which by the bijection in Lemma 3.1.4 is equal to $\mathfrak{a}$. So this shows $A/\mathfrak{a} \cong A[\mathfrak{p}^{-1}]/\mathfrak{a}A[\mathfrak{p}^{-1}]$. □

Corollary 3.1.7. *$A[\mathfrak{p}^{-1}]$ is a domain of Krull dimension 1.*

Proof. Indeed every non-zero prime ideal is maximal, and since there are at least two non-zero prime ideals of A (because otherwise A is a Discrete Valuation Ring), there is at least one non-zero prime ideal of A coprime to $\mathfrak{p}$, which shows that $A[\mathfrak{p}^{-1}]$ has at least one non-zero prime ideal. □

Theorem 3.1.8. *$A[\mathfrak{p}^{-1}]$ is a Dedekind domain.*

Proof. Let $\mathfrak{b}$ be a non-zero proper ideal of $A[\mathfrak{p}^{-1}]$. Then by the bijection, we can write $\mathfrak{b} = \mathfrak{a}A[\mathfrak{p}^{-1}]$ for $\mathfrak{a} = \mathfrak{b} \cap A$. Now since $\mathfrak{a}$ is an ideal in the Dedekind domain A, we can write a prime decomposition $\mathfrak{q}_1 \cdots \mathfrak{q}_r$. (The primes are not necessarily distinct) Now the ideals $\mathfrak{q}_i A[\mathfrak{p}^{-1}]$ are found to be prime ideals of $A[\mathfrak{p}^{-1}]$. Then we observe that $\prod_i \mathfrak{q}_i A[\mathfrak{p}^{-1}]$ and $\mathfrak{a}A[\mathfrak{p}^{-1}] = (\prod_i \mathfrak{q}_i)A[\mathfrak{p}^{-1}]$ are equal because their intersection with A is both $\prod_i \mathfrak{q}_i = \mathfrak{a}$. So $\prod_i \mathfrak{q}_i A[\mathfrak{p}^{-1}]$ is a factorisation into prime ideals of $\mathfrak{b}$. □

Example 3.1.9. *There are two main examples for which we wish to apply this construction, in which case we call it a fake real quadratic order. The first example is where $A = \mathcal{O}_K$ with $K|\mathbb{Q}$ a number field. Specifically we will study K imaginary quadratic. The second example is where $A = \mathcal{O}_K$ is the integral closure of $k[x]$ inside a finite extension $K|k(x)$, which is a function field over k. Geometrically, this is $\mathcal{O}_X$ where X is an affine patch of the smooth geometrically irreducible curve corresponding to K.*

Remark 3.1.10. A scheme-theoretic interpretation of this construction can be given as follows: Start with a smooth curve with at least two points. In other words, we start with $\mathrm{Spec}(A)$ with A a Dedekind domain which is not a Discrete Valuation Ring. Let $[\mathfrak{p}] \in \mathrm{Spec}(A)$ be a closed point. Then we note that the topological spaces $\mathrm{Spec}(A[\mathfrak{p}^{-1}])$ and $X := \mathrm{Spec}(A) \setminus \{[\mathfrak{p}]\}$ are homeomorphic, using the order-preserving bijection in Lemma 3.1.4. Let $X \to \mathrm{Spec}(A[\mathfrak{p}^{-1}])$ be given by a ring homomorphism $A[\mathfrak{p}^{-1}] \to \mathcal{O}_X(X)$, which can be constructed through the family of injections $A[\mathfrak{p}^{-1}] \to A[\frac{1}{f}]$ for $f \in \mathfrak{p}$. This induces a morphism of schemes, which turns out to be an isomorphism and so we discover that the open subscheme $X \subseteq \mathrm{Spec}(A)$ is an affine smooth curve. (We skip the details)

Now not only is $A[\mathfrak{p}^{-1}]$ a Dedekind domain, but we can use information about A to gain information about $A[\mathfrak{p}^{-1}]$. To be precise, we can determine the group of units and the ideal class group.

Definition 3.1.11. We write $o(\mathfrak{p})$ for the order of the prime ideal $\mathfrak{p}$ in $\mathrm{Cl}(A)$.

Theorem 3.1.12. *If $[\mathfrak{p}]$ is of finite order in $Cl(A)$, then $A[\mathfrak{p}^{-1}]^\times = A^\times \times \epsilon^{\mathbb{Z}}$ where $\epsilon \in A$ is such that $\epsilon A = \mathfrak{p}^{o(\mathfrak{p})}$ and $o(\mathfrak{p})$ is the order of $[\mathfrak{p}]$ in $Cl(A)$. Otherwise $A[\mathfrak{p}^{-1}]^\times = A^\times$.*

Proof. First assume $[\mathfrak{p}]$ is a torsion element in the class group. Let $\gamma \in A[\mathfrak{p}^{-1}]^\times$ be arbitrary. Then for all non-zero $\mathfrak{q} \in \mathrm{Spec}(A)$ distinct from $\mathfrak{p}$ we have $v_\mathfrak{q}(\gamma), v_\mathfrak{q}(1/\gamma) \geq 0$, showing $v_\mathfrak{q}(\gamma) = 0$. This shows that $\gamma A = \mathfrak{p}^k$ for some $k \in \mathbb{Z}$. By definition of $o(\mathfrak{p})$, this means $o(\mathfrak{p})|k$. Then

$$\gamma A = (\mathfrak{p}^{o(\mathfrak{p})})^{k/o(\mathfrak{p})} = (\epsilon A)^{k/o(\mathfrak{p})} = \epsilon^{k/o(\mathfrak{p})} A.$$

So γ is of the form $\nu\epsilon^{k/o(\mathfrak{p})}$ with $\nu \in A^\times$. This has shown that $A[\mathfrak{p}^{-1}]^\times \subseteq A^\times \times \epsilon^\mathbb{Z}$. The other inclusion is shown by the fact that $v_\mathfrak{q}(\epsilon) = v_\mathfrak{q}(\mathfrak{p}^{o(\mathfrak{p})}) = 0$ for all $\mathfrak{q} \in \mathrm{Spec}(A)$ distinct from $\mathfrak{p}$.

If $[\mathfrak{p}]$ is not torsion, then in our proof we have $k = 0$, showing $\gamma \in A^\times$. □

Remark 3.1.13. Note that ϵ is unique up to multiplication by elements in $A^\times$.

Theorem 3.1.14. *$Cl(A[\mathfrak{p}^{-1}]) \cong Cl(A)/\langle[\mathfrak{p}]\rangle$.*

Proof. The bijection in Lemma 3.1.4 can be used to induce a group homomorphism $\phi : \mathrm{Cl}(A) \to \mathrm{Cl}(A[\mathfrak{p}^{-1}])$. (It is easy to see that this is well-defined.) In other words $[\mathfrak{a}]$ is sent to $[\mathfrak{a}A[\mathfrak{p}^{-1}]]$. This new function is also surjective by the map in Lemma 3.1.4 being surjective. Now suppose that $[\mathfrak{a}A[\mathfrak{p}^{-1}]] = [0]$ for some $\mathfrak{a}$. Without loss of generality, assume it is integral. Then $\mathfrak{a}A[\mathfrak{p}^{-1}] = xA[\mathfrak{p}^{-1}]$ for some $x \in A[\mathfrak{p}^{-1}]$. Then $\mathfrak{a}A[\mathfrak{p}^{-1}] = (x\mathfrak{p}^k)A[\mathfrak{p}^{-1}]$ for all $k \in \mathbb{Z}$. Take $k = -v_\mathfrak{p}(x)$ and observe that $x\mathfrak{p}^{-v_\mathfrak{p}(x)}$ is coprime to $\mathfrak{p}$, because its valuation equals 0. Therefore by the bijection in Lemma 3.1.4, we see that $\mathfrak{a} = x\mathfrak{p}^{-v_\mathfrak{p}(x)}$. So $[\mathfrak{a}] = [\mathfrak{p}]^{-v_\mathfrak{p}(x)}$. This shows $\ker(\phi) \subseteq \langle[\mathfrak{p}]\rangle$. The other inclusion is clear, so $\ker(\phi) = \langle[\mathfrak{p}]\rangle$. This proves the result. □

Remark 3.1.15. The results in this subsection are a generalization of the case where $A = \mathcal{O}_K$ for K an imaginary quadratic number field, which has been done by Henri Cohen in [6] and worked out in more detail by Micheal Oh in [19].

3.2 Inverting multiple prime ideals

Let the Dedekind domain A have at least $n+1$ non-zero prime ideals, and let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ be a finite set of non-zero primes of Dedekind domain A. Then one can invert prime ideals one at a time, since at each step you start off with a Dedekind domain and prime ideals not yet inverted are always sent to prime ideals. The ring one ends up with is hence a Dedekind domain. Then the order in which one does this doesn't matter.

Proposition 3.2.1. *Let $A_0 := A$ and $A_{i+1} := A_i[(\mathfrak{p}_{i+1}A_i)^{-1}]$ for all $i = 0, \ldots, n-1$. The ring A_n does not change after reordering $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Denote $A[\mathfrak{p}_1^{-1}, \ldots, \mathfrak{p}_n^{-1}] = A[S^{-1}] := A_n$.*

Proof. This ring is also equal to $\{a \in K^\times : v_\mathfrak{q}(a) \geq 0 \ (\forall \mathfrak{q} \notin S)\} \cup \{0\}$. □

We notice that $A[S^{-1}]^\times/A^\times \cong \mathbb{Z}^m$, where m is the number of primes in S of finite order in $\mathrm{Cl}(A)$. Also $\mathrm{Cl}(A[S^{-1}]) \cong \mathrm{Cl}(A)/\langle S\rangle$. Observe that therefore $A[S^{-1}]$ is a Principal Ideal Domain if and only if S generates all of $\mathrm{Cl}(A)$.

One could also ask if an infinite set of non-zero prime ideals could be inverted. Assume A has infinitely many non-zero prime ideals. Let S be an infinite set of non-zero prime ideals (not all of them) and again define $A[S^{-1}] = \{a \in K^\times : v_\mathfrak{q}(a) \geq 0 \ (\forall \mathfrak{q} \notin S)\} \cup \{0\}$. We can again see this is a subring of K, by looking at properties of valuations.

Proposition 3.2.2. *Assume S is countably infinite. Then*

$$A[S^{-1}] = \bigcup_{T \subseteq S : T \text{ finite}} A[T^{-1}].$$

Proof. One inclusion is clear and for the other, you need the observation that each element of $K^\times$ only has non-zero valuation at finitely many primes. □

Remark 3.2.3. In the case where A is the ring of integers of a number field, one can recognize $A[S^{-1}]$ as the ring of S-integers. A nice resource is found in [18, page 71-72].

4 Real quadratic orders in a number field setting

Let $K|\mathbb{Q}$ be a quadratic number field, then $K = \mathbb{Q}(\sqrt{D})$ for some squarefree $D \in \mathbb{Z}$. If $D < 0$, we call K imaginary and if $D > 0$, we call K real.

Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic number field. Then by Dirichlet's unit theorem, the rank of $\mathcal{O}_K^\times$ equals 1. We shall be mostly interested in the case where D is prime.

4.1 $D \equiv 1 \mod 4$

Let us for now assume $D \equiv 1 \mod 4$, then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. We denote $a+b\sqrt{D}$ for a fundamental unit with $a, b \in \frac{1}{2}\mathbb{Z}$. In 1952, Nesmith Ankeny, Emil Artin and Sarvadaman Chowla conjectured the following:

Conjecture 4.1.1 (Ankeny, Artin, Chowla, [1])**.** *If $D \equiv 1 \mod 4$ is prime, then $D \nmid b$.*

The motivation behind conjecturing this is that implies a certain class number formula holds in terms of the fundamental unit, since they proved in 1962 in [2] the following:

Theorem 4.1.2. *Let $D \equiv 1 \mod 4$ be prime and let h be the class number of K. Then $hb \equiv aB_{\frac{D-1}{2}} \mod D$, where B_n is the n-th Bernoulli number.*

And a year earlier, they showed that $h < D$ in this context in [1], leading to:

Corollary 4.1.3. *If the Ankeny-Artin-Chowla conjecture holds, then h is the unique representative of $\frac{a}{b}B_{\frac{D-1}{2}} \mod D$ in $\{0, \ldots, D-1\}$.*

What they were unaware of, is that Kiselev already proved these results in [13] in 1948. Also note that Theorem 4.1.2 implies that an equivalent condition for the Ankeny-Artin-Chowla conjecture in this case ($D \equiv 1 \mod 4$ and prime) is that $B_{\frac{D-1}{2}} \not\equiv 0 \mod D$.

The Ankeny-Artin-Chowla conjecture has been verified to hold for all such $D < 2 \cdot 10^{11}$ by van der Poorten, te Riele and Williams in [26]. It seems therefore reasonable to believe that it holds. However, if one assumes that $b \mod D$ behaves randomly, then the expected value for number of counterexamples for $5 \leq D \leq n$ is approximately $N(5, n) := \frac{1}{2}(\log(\log(n)) - \log(\log(5)))$. So we have $N(5, 2 \cdot 10^{11}) \approx 1.39$. In this sense, it is not as special that a counterexample hasn't occured. Also, $N(5, n)$ grows very slowly as n increases. For instance, to obtain an expected value of 3, we need $n > 8.05 \cdot 10^{175}$, which means by the prime number theorem, we roughly need to check at least $1.98 \cdot 10^{173}$ many prime numbers. See [26, page 1312].

4.2 $D \equiv 3 \mod 4$

Now we shall assume $D \equiv 3 \mod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$. Let $a + b\sqrt{D}$ with $a, b \in \mathbb{Z}$ be the fundamental unit. Louis Joel Mordell proved the following:

Theorem 4.2.1 (Mordell, [17]). *We have $D \nmid b$ if and only if $D \nmid E_{(D-1)/2}$, where E_n is the n-th Euler number.*

Based on this, he proposed an analogue of the Ankeny-Artin-Chowla conjecture:

Conjecture 4.2.2 (Mordell). *We have $D \nmid b$.*

Letting go of the assumption that D is prime, small counterexamples were already found by Andreas Reinhart in [21, Remark 5.5]. However very recently, he has actually found a counterexample for Mordell's conjecture with $D = 39028039587479$, which is prime [22].

Two analoguous rings have been analysed with a corresponding analogue to the Ankeny-Artin-Chowla conjecture for a comparison, namely the fake real quadratics in number fields and the real quadratics in function fields. In this thesis, I delve into another analogue situation, the fake real quadratics in function fields.

5 Fake real quadratic orders in a number field setting

Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary number field, with $D < -2$ squarefree. Let $\omega = \begin{cases} \frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \mod 4 \\ \sqrt{D} & \text{if } D \not\equiv 1 \mod 4 \end{cases}$, so that $\mathcal{O}_K = \mathbb{Z}[\omega]$. Take any non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, above a prime p.

Definition 5.0.1. For a non-zero prime ideal $\mathfrak{p}$ of finite order $o(\mathfrak{p})$ in $\mathrm{Cl}(\mathcal{O}_K)$, we call $\mathcal{O}_K[\mathfrak{p}^{-1}]$ a *fake real quadratic order*.

Note that $\mathcal{O}_K^\times$ is torsion by Dirichlet's unit theorem. Therefore by Theorem 3.1.12, we have that $\mathcal{O}_K[\mathfrak{p}^{-1}]^\times \cong \mathcal{O}_K^\times \times \epsilon^{\mathbb{Z}}$ is the decomposition into the torsion and torsion-free part. Now one can ask if for $\epsilon = \frac{a+b\sqrt{D}}{2}$ with $a, b \in \mathbb{Z}$ we have that $D|b$. (We have $a, b \in \mathbb{Z}$ if $D \not\equiv 1 \mod 4$)

Definition 5.0.2. We say the fake real quadratic order satisfies the *n.f. fake Ankeny-Artin-Chowla property* if $D \nmid b$.

Remark 5.0.3. This definition involves a choice of ϵ and therefore it may depend on this choice whether the n.f. fake Ankeny-Artin-Chowla property holds. In case $|D| \geq 5$ however, we have $\mathcal{O}_K^\times = \{\pm 1\}$ and hence the fundamental unit is unique up to multiplication by ± 1 by applying Remark 3.1.13. Hence in this case, the n.f. fake Ankeny-Artin-Chowla property is independent of the choice of ϵ.

Recall from number theory that we call p inert if $p \cdot \mathcal{O}_K$ is a prime ideal and otherwise $p \cdot \mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ (since K is quadratic), we say p splits in $\mathcal{O}_K$. Here $\bar{\mathfrak{p}}$ denotes the image of $\mathfrak{p}$ under the conjugation that sends $\sqrt{D}$ to $-\sqrt{D}$. Before we start, we first consider the case $p|D$. We observe that $p|D$ splits, with $p \cdot \mathcal{O}_K = \mathfrak{p}^2$.

If D is prime, then $p = D$ and so $\mathfrak{p} = (\sqrt{D})$, hence the fundamental unit is $\sqrt{D}$ and $o(\mathfrak{p}) = 1$. Otherwise the fundamental unit is p with $o(\mathfrak{p}) = 2$. (This is true no matter what $D \mod 4$ is)

Assumption 5.0.4. *From now on, we will assume $p \nmid D$.*

In [6], Henri Cohen gives counterexamples to the n.f. fake Ankeny-Artin-Chowla property such as for $p = 7$ and $D = -3$, where a fundamental unit can be given as $\frac{-1+3\sqrt{-3}}{2}$. This example perhaps does not seem as satisfying, since $(\frac{-1+\sqrt{-3}}{2})(\frac{1-\sqrt{-3}}{2}) = 2 + \sqrt{-3}$ is an equally valid fundamental unit which satisfies the property. Therefore, Richard Micheal Oh proposes in [19, page 37] another counterexample that does not come with such an issue, by looking at $|D| \geq 5$. That way, the only units in $\mathcal{O}_K$ are ± 1. Take $p = 347$ and $D = -7$, here the only fundamental units that can be taken are $\pm(2 + 7\sqrt{-7})$.

Hongyan Wang conjectured in [27, page 46] that fixing D, the proportion of counterexamples among those with $p \leq N$ splitting goes to $\frac{1}{|D|}$ as $N \to \infty$. Florian Hess, Renate Scheidler and Micheal John Jacobson proved this conjecture in [11]. Applying Proposition 2.2.4 and Proposition 2.2.2 is a key element of the proof, which inspired the proof of Theorem 7.4.5.

Now we will discuss some conditions I found under which the property does hold.

Proposition 5.0.5. *If p splits and $p \nmid D$, then $4N(\frac{a+b\sqrt{D}}{2}) = a^2 - Db^2 = 4c \cdot p^{o(\mathfrak{p})}$, for some $c \in \mathcal{O}_K^\times$.*

Proof. We can write the ideal $(p)^{o(\mathfrak{p})}$ as $\mathfrak{p}^{o(\mathfrak{p})}\overline{\mathfrak{p}}^{o(\mathfrak{p})} = (\frac{a+b\sqrt{D}}{2})(\frac{a-b\sqrt{D}}{2}) = (N(\frac{a+b\sqrt{D}}{2}))$, so $p^{o(\mathfrak{p})}$ and $N(\frac{a+b\sqrt{D}}{2})$ are equal up to multiplication in $\mathcal{O}_K^\times$. □

Corollary 5.0.6. *If p splits and $p \nmid D$, then $|D| < 4p^{o(\mathfrak{p})}$ if $D \equiv 1 \mod 4$ and $|D| < p^{o(\mathfrak{p})}$ if $D \not\equiv 1 \mod 4$.*

Proof. Since p splits, we have $b \neq 0$, and so $b^2 \geq 1$. Because $p \nmid D$, we have $a \neq 0$ and so $a^2 \geq 1$. Therefore,

$$4p^{o(\mathfrak{p})} = |4cp^{o(\mathfrak{p})}| = |a^2 - Db^2| \geq 1 + |D| > |D|.$$

In case $D \not\equiv 1 \mod 4$, we can do even better. We then get $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$ and so a, b are both even. Therefore, $a^2, b^2 \geq 4$ and so

$$4p^{o(\mathfrak{p})} = |4cp^{o(\mathfrak{p})}| = |a^2 - Db^2| \geq 4 + |4D| > 4|D|.$$

□

Proposition 5.0.7. *If $p \nmid D$ splits and $|D| > \begin{cases} \sqrt[3]{4} \cdot p^{o(\mathfrak{p})/3} & \text{if } D \equiv 1 \mod 4 \\ p^{o(\mathfrak{p})/3} & \text{if } D \not\equiv 1 \mod 4 \end{cases}$, then the n.f. fake Ankeny-Artin-Chowla property holds.*

Proof. Taking the cube of both sides of the inequality, we get $|D|^3 > 4p^{o(\mathfrak{p})} \geq |Db^2|$ if $D \equiv 1 \mod 4$ and $4|D|^3 > 4p^{o(\mathfrak{p})} \geq |Db^2|$ elsewise. From these we can conclude that $|D| > |b| \in \mathbb{Z}$ if $D \equiv 1 \mod 4$ and $2|D| > |b|$ otherwise. In the first case, it is clear to see that the n.f. fake Ankeny-Artin-Chowla property holds. In the second case, observe that b is even and so $|D| > |\frac{b}{2}|$ shows that D does not divide $\frac{b}{2}$ and hence also not b. □

6 Real quadratic orders in a function field setting

The main goal of this subsection is to give a proof of a function field analogue of the Ankeny-Artin-Chowla conjecture, found in [28].

Let k be a perfect field of characteristic $\ell \neq 2$ (some statements may also hold for more general k) and let $K|k(x)$ be a finite extension. We denote $\mathcal{O}_K$ for the integral closure of $k[x]$ in K, in analogy with a ring of integers in the number field setting. Note that $\mathcal{O}_K$ is a Dedekind domain by construction.

From now on, let's look at the quadratic case, so $K \cong k(x)[y]/(y^2 + h(x)y - f(x))$ for some $h, f \in k[x]$. Now because the characteristic doesn't equal 2, we can complete the square and therefore without loss of generality we have $K \cong k(x)[y]/(y^2 - f(x))$. Then $\mathcal{O}_K = k[x, \sqrt{f(x)}]$. We can also assume f squarefree. If f is constant, then K is a constant extension, which we aren't interested in, so let us assume f to be non-constant. Then K is the function field of a hyperelliptic curve C/k which has an affine patch given by $y^2 = f(x)$. So picking an affine patch given by $y^2 = f(x)$, we let $K = k(x, \sqrt{f(x)})$ and so $\mathcal{O}_K = k[x, \sqrt{f(x)}]$. We shall both use the language of the function field K and of this corresponding hyperelliptic curve C. We call $\mathcal{O}_K$ a maximal quadratic order, but we will often just say quadratic order. The most important situation is $k = \mathbb{F}_q = \mathbb{F}_{\ell^r}$ in this section, so that K becomes global.

In this function field setting, we shall also talk about a real and fake real quadratic order, and in both the real and fake real quadratic case, there will be a fundamental unit $\epsilon = a + b\sqrt{f}$, where we will study the hypothesis $f \nmid b$. In the real case, we will call this the *f.f. Ankeny-Artin-Chowla property*. In the fake real case, we will call this the *f.f. fake Ankeny-Artin-Chowla property*. We treat the real case in this section and the fake real case in the next section.

We call $\mathcal{O}_K$ real if $\deg(f) = 2g + 2$, where g is the genus of the corresponding curve C. The name comes from the following fact, which resembles the number field scenario:

Proposition 6.0.1. *Let $\mathcal{O}_K = k[x, \sqrt{f(x)}]$ be real with corresponding curve C. Let $\infty_+, \infty_- \in C(\overline{k})$ be the two points at infinity. Then*

$$\mathcal{O}_K^\times = \begin{cases} k^\times \times \epsilon^{\mathbb{Z}} & \text{if } \infty_+, \infty_- \in C(k) \text{ and } [\infty_+ - \infty_-] \in J(k)_{tors} \\ k^\times & \text{otherwise} \end{cases},$$

for some $\epsilon \in \mathcal{O}_K^\times \setminus k^\times$.

Proof. First let us assume the conditions of the first case. Then $\operatorname{div}(\epsilon) = m(\infty_+ - \infty_-)$ for some $\epsilon \in K$, where m is the order of $[\infty_+ - \infty_-]$ in the divisor class group $\mathrm{Cl}_k(C)$. Here J is the Jacobian of C, recall its definition given in Theorem 2.1.6. Since ϵ has no affine poles, it is in $\mathcal{O}_K$. This shows that $\epsilon \in \mathcal{O}_K^\times$, because its inverse also has no affine poles, but at the same time it isn't in $k^\times$ since $\operatorname{div}(\epsilon) \neq 0$. This shows that $\mathcal{O}_K^\times \supseteq k^\times \times \epsilon^{\mathbb{Z}}$.

Now let $\eta \in \mathcal{O}_K^\times$ be arbitrary. Then it has no affine poles and neither does η^{-1}, so it has neither affine poles nor affine zeros. Hence $\operatorname{div}(\eta) = n_+\infty_+ + n_-\infty_-$ for some $n_+, n_- \in \mathbb{Z}$. Since principal divisors are of degree 0, we have $n := n_+ = -n_-$, so $\operatorname{div}(\eta) = n(\infty_+ - \infty_-)$. Hence $m|n$, since m is the order of $[\infty_+ - \infty-]$. So $\operatorname{div}(\frac{\eta}{\epsilon^{n/m}}) = 0$ and therefore $\frac{\eta}{\epsilon^{n/m}} \in k^\times$, which shows $\eta \in k^\times \times \epsilon^{\mathbb{Z}}$.

Now let us suppose $\infty_+, \infty_- \notin C(k)$ or $[\infty_+ - \infty_-]$ is of infinite order in the divisor class group $\mathrm{Cl}_k(C)$. In both cases, $\infty_+ - \infty_-$ is not a k-rational divisor of finite order in $J(k)$. Let $\eta \in \mathcal{O}_K^\times$, then it has neither affine poles nor affine zeros, so because $\operatorname{div}(\eta)$ is of degree 0, it is a multiple of $\infty_+ - \infty_-$. We assumed that $\infty_+ - \infty_-$ is not a k-rational divisor of finite order, so this means $\operatorname{div}(\eta) = 0$, hence $\eta \in k^\times$. Since $k \subseteq \mathcal{O}_K$, we have $k^\times \subseteq \mathcal{O}_K^\times$. □

Now look at $k = \mathbb{F}_q$. We observe that $J(\mathbb{F}_q)$ is finite, which simplifies Proposition 6.0.1 a little. In case the leading coefficient of f is square, the points at infinity are $\mathbb{F}_q$-rational, so then $\mathcal{O}_K^\times = \mathbb{F}_q^\times \times \epsilon^{\mathbb{Z}}$ for some $\epsilon \in \mathcal{O}_K^\times \setminus \mathbb{F}_q^\times$. If the leading coefficient of f is non-square, then $\mathcal{O}_K^\times = \mathbb{F}_q^\times$.

Definition 6.0.2. Assume we are in the first case of Proposition 6.0.1 and denote $\epsilon = a + b\sqrt{f}$ for $a, b \in k[t]$. We say the *f.f. Ankeny-Artin-Chowla property* is satisfied if $f \nmid b$.

Note that this definition is independent of the choice of ϵ. The f.f. Ankeny-Artin-Chowla property has been proven to always hold by Jing Yu and Jiu-Kang Yu. Before we give the proof, first we need to introduce the Mason-Stothers Theorem, which is analogous to and precedes the abc-conjecture as posed in [16].

Theorem 6.0.3 (Mason-Stothers, 1984 [15])**.** *Let $a, b, c \in k[x]$ satisfy the following conditions:*

1. $a + b = c$
2. $\gcd(a, b, c) = 1$
3. $(a', b', c') \neq (0, 0, 0)$.

Then $\max\{\deg(a), \deg(b), \deg(c)\} \leq \deg(rad(abc)) - 1$*, where rad(abc) is the product of the distinct monic irreducible factors of abc.*

Theorem 6.0.4 (Yu-Yu, 1998 [28])**.** *Let $u = c + d\sqrt{f} \in \mathcal{O}_K^\times$ be non-constant. Suppose u as a morphism $C \to \mathbb{A}_k^1$ is seperable. (This is equivalent to $k(u)$ being a seperable extension of $k(x)$) Then* $\deg(\gcd(f, d)) \leq g$.

Proof. Since u is a unit, we have that $N(u) = c^2 - fd^2 \in k[x]^\times = k^\times$. Let us write $d = \gcd(f, d)\tilde{d}$ for some $\tilde{d} \in k[x]$. Note that the separability assumption gives that u is not a ℓ-th power, hence $c^2, -fd^2, N(u)$ are not all ℓ-th powers, in case $\ell = 0$. So we are allowed to apply the Mason-Stothers Theorem to $c^2, -fd^2, N(u)$. Then we get

$$\deg(d^2 f) \leq \deg(\mathrm{rad}(N(u)c^2 f d^2)) - 1 = \deg(\mathrm{rad}(cf\tilde{d})) - 1 \leq \deg(c) + \deg(f) + \deg(\tilde{d}) - 1.$$

From this we see that

$$2\deg(d) + \deg(\gcd(f, d)) \leq \deg(c) + \deg(d) - 1,$$

hence

$$2\deg(\gcd(f,d)) \leq 2\deg(c) - 2\deg(d) - 2 = \deg(f) - 2 = 2g.$$

This proves the result. □

Remark 6.0.5. Jing Yu and Jiu-Kang Yu also gave a geometric proof involving algebraic differentials in [28]. Furthermore in the same paper, they proved something analogous for the case where the characteristic ℓ equals 2.

Corollary 6.0.6 (Yu-Yu, 1998 [28])**.** *Assume that* $\infty_+, \infty_- \in C(k)$ *and* $[\infty_+ - \infty_-] \in J(k)_{tors}$*. Then the f.f. Ankeny-Artin-Chowla property holds.*

Proof. Let u in Theorem 6.0.4 be a fundamental unit ϵ. Then we notice that u is separable, otherwise $k(u) \subseteq k(t, \sqrt{f})^\ell$, hence u is an ℓ-th power; which contradicts ϵ being a fundamental unit. Therefore, $\deg(\gcd(f,d)) \leq g < 2g+1 = \deg(f)$, so $f \nmid \gcd(f,d)$ and hence $f \nmid d$. □

7 Fake real quadratic orders in a function field setting

This is the main section of the thesis. Its goal is to study the behaviour of the property analogous to the Ankeny-Artin-Chowla conjecture, using fake real quadratic orders in a function field setting. We start off with an introduction in Subsection 7.1, explaining the analogy we are considering. In Subsection 7.2, we specifically assume that the genus of curve C is 0, which allows for an equivalent condition to the f.f. fake Ankeny-Artin-Chowla property. Then in Subsection 7.3, we give a few results that imply that the f.f. fake Ankeny-Artin-Chowla property holds, under certain conditions. After that, Subsection 7.4 revolves around Theorem 7.4.5, which for the case the constant field is finite, calculates the proportion of counterexamples when fixing the parameter f and varying parameter p. (This p is yet to be introduced.) In Subsection 7.5, we show in Proposition 7.5.3 that in case the parameters behave nicely under extending the constant field, doing so does not affect whether the Ankeny-Artin-Chowla conjecture holds. Next up, Subsection 7.6's main result is Theorem 7.6.5, which compares fake real quadratic orders over $\mathbb{Q}(x)$ to corresponding reductions over $\mathbb{F}_\ell(x)$ for primes $\ell > 2$. In Subsection 7.7, we generalize Subsection 7.6 by considering number fields and their ring of integers modulo a prime ideal. In Subsection 7.8, we see that we can apply the ideas of Subsection 7.6 to say something about the fake n.f. scenario. Finally, in Subsection 7.9, we roughly sketch how to consider an analogy for the case where the characteristic is 2.

7.1 Introduction

We call $\mathcal{O}_K$ imaginary if f is of odd degree $2g+1$. Let $a \in k^\times$ be the leading coefficient of f. Then we observe that the affine curves $y^2 = f(x)$ and $y^2 = a^{2g} f(\frac{x}{a})$ are isomorphic and $a^{2g} f(\frac{x}{a})$ is monic, so we can focus on f monic. Again the name "imaginary" comes from the number field setting, because of the following fact:

Proposition 7.1.1. *If $\mathcal{O}_K$ is imaginary, then $\mathcal{O}_K^\times = k^\times$.*

Proof. It is clear that $k^\times \subseteq \mathcal{O}_K^\times$, so we must show these are the only units.

Function Field proof: Suppose $a + b\sqrt{f} \in \mathcal{O}_K^\times$. Then $N(a + b\sqrt{f}) = a^2 - fb^2 \in k^\times$. This is impossible if $a = 0$, since f has positive degree. Suppose $b \neq 0$. Then a^2, fb^2 are respectively of even and odd degree, so their leading terms don't cancel out. This means that $\deg(a^2 - fb^2) \geq \deg(fb^2) \geq 1$, which contradicts it being in $k^\times$. This shows $b = 0$, so $a^2 \in k^\times$, so $a \in k^\times$.

Geometric proof: Suppose $a + b\sqrt{f} \in \mathcal{O}_K^\times$. Then it has neither affine zeros nor affine poles, so it can only have non-zero valuation at the unique point at infinity. However $\operatorname{div}(a + b\sqrt{f})$, being principal, has degree 0, so $\operatorname{div}(a + b\sqrt{f}) = 0 \cdot \infty = 0$, which is equivalent to $a + b\sqrt{f} \in k^\times$. □

In this section, let $\mathcal{O}_K$ be imaginary.

Definition 7.1.2. For a non-zero prime ideal $\mathfrak{p}$ of finite order $o(\mathfrak{p})$ in $\mathrm{Cl}(\mathcal{O}_K)$, we call $\mathcal{O}_K[\mathfrak{p}^{-1}]$ a *fake real quadratic order*.

This name comes from the observation that we also have $\mathcal{O}_K[\mathfrak{p}^{-1}]^\times = k^\times \times \epsilon^{\mathbb{Z}}$, for $\epsilon \in \mathcal{O}_K$ such that $\epsilon\mathcal{O}_K = \mathfrak{p}^{o(\mathfrak{p})}$, by Theorem 3.1.12 and in the case that k is finite, this means $\mathcal{O}_K[\mathfrak{p}^{-1}]^\times$ is of rank 1 and ϵ is a generator of it modulo its torsion. We shall call this $\epsilon = a + b\sqrt{f}$ the fundamental unit.

Note that if k is infinite, then $\mathcal{O}_K[\mathfrak{p}^{-1}]^\times$ has rank greater than 1. However even for infinite k, it makes sense to call ϵ a fundamental unit. Namely, let's view $\mathcal{O}_K[\mathfrak{p}^{-1}]$ as a ring extension of $k[x]$, hence view $\mathcal{O}_K[\mathfrak{p}^{-1}]^\times$ as a group extension of $(k[x])^\times = k^\times$. Then ϵ can be seen as a generator of $\mathcal{O}_K[\mathfrak{p}^{-1}]^\times/(k[x])^\times$ modulo its torsion. In the fake real number field setting, this is also how we can view the fundamental unit; since there $\mathcal{O}_K[\mathfrak{p}^{-1}]$ is a ring extension of $\mathbb{Z}$ and hence we view $\mathcal{O}_K[\mathfrak{p}^{-1}]^\times$ as a group extension of $\mathbb{Z}^\times = \{\pm 1\}$.

Next up, we find that there are two ways in which prime ideals of $\mathcal{O}_K$ can occur.

Proposition 7.1.3. *Let $\alpha \in \overline{k}$ with minimal polynomial $p \in k[x]$. If $(\alpha, s(\alpha))$ is a $k(\alpha)$-rational point on the curve C with $s \in k[x]$, then the prime factorisation of $p \cdot \mathcal{O}_K$ is given as $(p, s - \sqrt{f})(p, s + \sqrt{f})$. If there is no $k(\alpha)$-rational point on the hyperelliptic curve of the form (α, y), then $p \cdot \mathcal{O}_K$ is prime already.*

Proof. First we shall assume that a $k(\alpha)$-rational point $(\alpha, s(\alpha))$ on the hyperelliptic curve exists. In order to prove that $(p, s - \sqrt{f})$ and $(p, s + \sqrt{f})$ are prime, it suffices to show that they are the kernel of ring morphisms that map to domains. Let us construct two ring morphisms $k[x, y] \to k[\alpha]$ with kernel containing $y^2 - f(x)$ in order to get two morphisms $k[x, \sqrt{f(x)}] \to k[\alpha]$. These can be given as sending $g \in k[x, y]$ to $g(\alpha, \pm s(\alpha))$. This has kernel $(p(x), s(x) \mp y)$ respectively which contains $y^2 - f(x) \equiv (y - s(x))(y + s(x)) \mod p$. These morphisms $k[x, \sqrt{f(x)}] \to k[\alpha]$ have kernel $(p, s \pm \sqrt{f})$ respectively, which shows that this ideal in $\mathcal{O}_K$ is prime because $k[\alpha]$ is a domain.

Now let me multiply these two ideals:

$$(p, s + \sqrt{f})(p, s - \sqrt{f}) = (p^2, ps, p\sqrt{f}, s^2 - f).$$

Assuming p, f are coprime, this ideal is equal to (p) as it contains p^2 and pf.

From now on, assume there is no $k(\alpha)$-rational point $(\alpha, s(\alpha))$ on the hyperelliptic curve. Then we can recognize $p \cdot \mathcal{O}_K$ as the kernel of $k[x, \sqrt{f(x)}] \to k[\alpha, t]/(t^2 - f(\alpha))$ induced by $k[x, y] \to k[\alpha, t]/(t^2 - f(\alpha))$ given as sending p to $p(\alpha, t) \mod (t^2 - f(\alpha))$, which has a kernel generated by $y^2 - f(x)$. Since $t^2 - f(\alpha)$ is irreducible over $k[\alpha]$ by assumption, we have that $k[\alpha, t]/(t^2 - f(\alpha))$ is a domain, this shows $p \cdot \mathcal{O}_K$ is a prime ideal. □

Corollary 7.1.4. *Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$, let $p \in k[x]$ be the unique monic irreducible generator of $\mathfrak{p} \cap k[x]$, let $\alpha \in \overline{k}$ be a root of p. Then*

- *$\mathfrak{p} = p \cdot \mathcal{O}_K$ if and only if $f(\alpha)$ is non-square in $k(\alpha)$, if and only if there is no affine point in $C(\mathbb{F}_q(\alpha))$ with x-coordinate α.*
- *Otherwise $\mathfrak{p} = (p, s - \sqrt{f})$ for some $s \in k[x]$ such that $(\alpha, s(\alpha)) \in C(k(\alpha))$.*

Definition 7.1.5. We say a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is *inert* in the first case of Corollary 7.1.4 and we say it is *split* in the second case of Corollary 7.1.4.

All of this can be translated to the language of divisors. Namely, let $P = (\alpha, \beta) \in C(\overline{k})$ and let p be the minimal polynomial of $\alpha \in \overline{k}$. Then if $\beta \in k(\alpha)$, we have that

$$\operatorname{div}(p) + 2\deg(p)\infty = \Big(\sum_{\sigma(P):\sigma\in \mathrm{Gal}(\overline{k}/k)} \sigma(P)\Big) + \Big(\sum_{\sigma(P):\sigma\in \mathrm{Gal}(\overline{k}/k)} \sigma(\iota(P))\Big)$$

is the sum of two k-rational prime divisors. Here, $\iota : C \to C$ is the morphism such that a point $(x_0, y_0) \in C(k)$ is sent to $(x_0, -y_0)$. If $\beta \notin k(\alpha)$, then $\operatorname{div}(p) + 2\deg(p)\infty$ is a prime divisor itself. Additionally these are the only types of k-rational prime divisors.

If p is inert, then $o(\mathfrak{p}) = 1$ and so the fundamental unit of $A[\mathfrak{p}^{-1}]$ is p. This is hence a less interesting case.

Assumption 7.1.6. *From now on, we will focus on the case where p splits.*

Let $\sigma \in \mathrm{Gal}(K|k(x))$ be defined as $\sigma(c + d\sqrt{f}) := c - d\sqrt{f}$ for all $c, d \in k(x)$. We also denote σ by a bar.

Lemma 7.1.7. *The induced ideal $\overline{\mathfrak{p}}$, which is the image of $\mathfrak{p}$ under σ, is also above p. Moreover, we have $\mathcal{O}_K[\mathfrak{p}^{-1}] \cong \mathcal{O}_K[\overline{\mathfrak{p}}^{-1}]$, the isomorphism being σ.*

Proof. We notice that $\overline{\mathfrak{p}} = (p, s + \sqrt{f})$ if $\mathfrak{p} = (p, s - \sqrt{f})$ for some $s \in k[x]$. Therefore,

$$\mathfrak{p}^{-1} = (\mathfrak{p}\overline{\mathfrak{p}}(\overline{\mathfrak{p}})^{-1})^{-1} = (p \cdot \mathcal{O}_K)^{-1}\overline{\mathfrak{p}}$$

is generated by 1 as a $k[x]$-module and $\frac{s+\sqrt{f}}{p}$. Similarly $\overline{\mathfrak{p}}^{-1}$ is generated by 1 and $\frac{s-\sqrt{f}}{p}$ as a $k[x]$-module. So

$$\mathcal{O}_K[\mathfrak{p}^{-1}] = \mathcal{O}_K[\frac{s + \sqrt{f}}{p}]$$

and

$$\mathcal{O}_K[\overline{\mathfrak{p}}^{-1}] = \mathcal{O}_K[\frac{s - \sqrt{f}}{p}].$$

□

The geometric view of this proof is that σ corresponds to the automorphism $\iota : C \to C$, and that removing an affine point P from C gives an affine patch isomorphic to the affine patch attained by removing $\iota(P)$.

Corollary 7.1.8. *For each squarefree $f \in k[x]$ and irreducible $p \in k[x]$, there is a unique fake real quadratic order (up to isomorphism) corresponding to it.*

Definition 7.1.9. We say that the *f.f. fake Ankeny-Artin-Chowla property* is satisfied if $f \nmid b$.

Notice that due to Remark 3.1.13, this definition is independent of the choice of ϵ. What we will be interested in from now on, is to study when and how often the f.f. fake Ankeny-Artin-Chowla property holds. Before we do that, let's first develop methods to actually compute the fundamental unit.

Proposition 7.1.10. *Let D be the k-rational divisor of degree 0 corresponding to $\mathfrak{p}$. Then $\mathcal{L}(-o(\mathfrak{p})D)$ is 1-dimensional and equal to $Span_k(a+b\sqrt{f})$ where $a+b\sqrt{f}$ is a fundamental unit for $\mathcal{O}_K[\mathfrak{p}^{-1}]$.*

Proof. Let $\nu \in \mathcal{O}_K$ be arbitrary. Then $\nu \in \mathcal{L}(-o(\mathfrak{p})D)$ if and only if $\mathrm{div}(\nu) - o(\mathfrak{p})D$ is effective and of degree 0. That is if and only if $\mathrm{div}(\nu) - o(\mathfrak{p})D = 0$, if and only if $\mathrm{div}(\nu) = o(\mathfrak{p})D$. Translating this to ideal language, $\nu \in \mathcal{L}(-o(\mathfrak{p})D)$ if and only if $\nu\mathcal{O}_K = \mathfrak{p}^{o(\mathfrak{p})}$, if and only if ν is a fundamental unit for $\mathcal{O}_K[\mathfrak{p}^{-1}]$. Fundamental units are unique up to multiplication by an element of $\mathcal{O}_K^\times = k^\times$. □

Since the algebraic software package Magma has an implemented algorithm for computing Riemann-Roch spaces based off the work of Florian Hess in [8], this gives us a way to compute a fundamental unit.

7.2 A characterisation for genus 0

Let us first investigate the genus 0 case, as it turns out to be simpler. We are dealing then with $\mathcal{O}_K = k[x, \sqrt{x+a}]$ for some $a \in k$ or equivalently the curve $y^2 = x + a$. Through a coordinate change, we can assume we are dealing with the curve $y^2 = x$ or equivalently $\mathcal{O}_K = k[x, \sqrt{x}] = k[\sqrt{x}] \cong k[t]$. The following proposition gives an easy way to find out if the f.f. fake Ankeny-Artin-Chowla property holds, as well as a method to construct examples or counterexamplese.

Proposition 7.2.1. *Let $p \in k[x]$ be irreducible and splitting over $k[\sqrt{x}]$. Then we can factor $p(t^2) = c(t)\cdot(-1)^{\deg(p)}c(-t)$ in $k[t]$. Conversely, for every $c \in k[t]$ irreducible and not even (meaning $c(-t) \neq c(t)$.), we can find $p \in k[x]$ irreducible and splitting over $k[\sqrt{x}]$ such that $p(t^2) = c(t)\cdot(-1)^{\deg(p)}c(-t)$ in $k[t]$.*

Furthermore, the f.f. fake Ankeny-Artin-Chowla property holds for p if and only if $c'(0) \neq 0$.

Proof. The first statement is simply translating Proposition 7.1.3 and Corollary 7.1.4 to polynomials, since $\mathcal{O}_K$ is a Principal Ideal Domain. So $c(\sqrt{x})$ is the generator of one of the prime ideals above p and also hence the fundamental unit. Let us write $c = \sum_i^{\deg(c)} c_i t^i$, then we can write $c(\sqrt{x}) = (\sum_{1\leq 2j\leq \deg(c)} c_{2j}x^j) + (\sum_{1\leq 2l+1\leq \deg(c)} c_{2l+1}x^l)\sqrt{x}$. Then the f.f. fake Ankeny-Artin-Chowla property holds if and only if x doesn't divide $\sum_{1\leq 2l+1\leq \deg(c)} c_{2l+1}x^l$, if and only if $c'(0) = c_1 \neq 0$. □

Example 7.2.2. *Let us take $p = x - 1 \in k[x]$. Then $p(t^2) = t^2 - 1 = (t-1)(t+1)$. Thus we have $c(t) = t - 1$ and so $c'(0) = 1$. The corresponding fake real quadratic order is $\mathcal{O}_K[\frac{1}{\sqrt{x}-1}]$, which satisfies the Ankeny-Artin-Chowla conjecture.*

Example 7.2.3. *Let's now do the converse for $k = \mathbb{F}_3$ and take c such that $c'(0) = 0$ to construct a counterexample, so let us take $c(t) = t^3+t^2-1 \in \mathbb{F}_3[t]$. Then $p(t^2) = (t^3+t^2-1)(t^3-t^2+1) = t^6-t^4-t^2-1$. So $p(x) = x^3-x^2-x-1$. We have found that the fake real quadratic order corresponding to $p(x) = x^3 - x^2 - x - 1$ is $\mathcal{O}_K[\frac{1}{x\sqrt{x}+x-1}]$ and does not satisfy the Ankeny-Artin-Chowla conjecture.*

Corollary 7.2.4. *Let $g = 0$. For all finite fields $k = \mathbb{F}_q$, there exist examples of p splitting such that the f.f. fake Ankeny-Artin-Chowla property holds, and examples such that it doesn't hold.*

Proof. One can use $c(t) = t$ to construct an example such that it holds. The corresponding fake real quadratic order is $\mathcal{O}_K[\frac{1}{\sqrt{x}}]$ where $p(x) = x$.

Note that the function $\mathbb{F}_q \to \mathbb{F}_q$ given as $\chi \to \chi^3 - \chi^2$ is not an injection (since $\chi = 0, 1$ get mapped to the same), hence also not a surjection. Therefore, there is some $\eta \in \mathbb{F}_q$ which is not in its image, let $c(t) = t^3 - t^2 - \eta$. By construction, c has no roots and hence is irreducible because $\deg(c) \leq 3$. So we can use $c(t)$ to construct a counterexample since $c'(0) = 0$. The corresponding fake real quadratic order is $\mathcal{O}_K[\frac{1}{x\sqrt{x}-x-\eta}]$ with $p(x) = x^3 - (x + \eta)^2$. □

Corollary 7.2.5. *Let $g = 0$. Then the f.f. fake Ankeny-Artin-Chowla property holds for p splitting such that $\deg(p) \leq 2$.*

Proof. First note $\deg(c) = \deg(p) \leq 2$. Then the requirement that c is not even shows c requires a linear non-zero term, hence $c'(0) \neq 0$. □

7.3 Positive results

In this subsection we give some results that provide sufficient conditions to the f.f. fake Ankeny-Artin-Chowla property. First however, there is some simple scenario that we wish to get rid of.

Proposition 7.3.1. *Let $p|f$. If f is irreducible, then the f.f. fake Ankeny-Artin-Chowla property holds. If f is reducible, then the f.f. fake Ankeny-Artin-Chowla property does not hold.*

Proof. For f irreducible and $p = f$, we have $\mathfrak{p} = \sqrt{f} \cdot \mathcal{O}_K$ already principal, so $\sqrt{f}$ is a fundamental unit. For f reducible and $p|f$, we have $\mathfrak{p} = \overline{\mathfrak{p}} = (p, \sqrt{f})$, so $\mathfrak{p}^2 = \mathfrak{p}\overline{\mathfrak{p}} = p \cdot \mathcal{O}_K$, so p is the fundamental unit. □

Now before we start having some more significant results, we start off with a useful fact about the fundamental unit.

Proposition 7.3.2. *If $\epsilon = a + b\sqrt{f}$ is a fundamental unit of a fake real quadratic order $\mathcal{O}_K[\mathfrak{p}^{-1}]$ with $\mathfrak{p}$ above $p \in k[x]$ splitting and $p \nmid f$, then $N(a + b\sqrt{f}) = a^2 - fb^2 = c \cdot p^{o(\mathfrak{p})}$ for some $c \in k^\times$.*

Moreover, if $a^2 - fb^2 = c \cdot p^m$ for some $a, b \in k[x]$, $m \in \mathbb{N}$ and $c \in k^\times$, then $o(\mathfrak{p})|m$ and either $a + b\sqrt{f}$ or $a - b\sqrt{f}$ is equal to $\epsilon^{\frac{m}{o(\mathfrak{p})}}$.

Proof. We have an equality of ideals:

$$(a^2 - fb^2) = (a + b\sqrt{f})(a - b\sqrt{f}) = \mathfrak{p}^{o(\mathfrak{p})}\overline{\mathfrak{p}}^{o(\mathfrak{p})} = (p)^{o(\mathfrak{p})} = (p^{o(\mathfrak{p})}).$$

Therefore $a^2 - fb^2, p^{o(\mathfrak{p})}$ generate the same ideal, so they differ multiplicatively by an element in $\mathcal{O}_K^\times = k^\times$.

If $a^2 - fb^2 = c \cdot p^m$, then there is an equality of ideals $(a + b\sqrt{f})(a - b\sqrt{f}) = (p)^k = \mathfrak{p}^k\overline{\mathfrak{p}}^k$. Since $p \nmid f$, we have that p is not a unit in $\mathcal{O}_K[\mathfrak{p}^{-1}]$ and so $p \nmid (a + b\sqrt{f})$. Therefore by unique factorisation of prime ideals, we have $\mathfrak{p}^m = (a + b\sqrt{f})$ or $\mathfrak{p}^m = (a - b\sqrt{f})$. Then it follows from this that $o(\mathfrak{p})|m$ and $a + b\sqrt{f} = \epsilon^{\frac{m}{o(\mathfrak{p})}}$. □

Corollary 7.3.3. *If $p \nmid f$ is splitting in $\mathcal{O}_K$, then $o(\mathfrak{p}) \deg(p) \geq \deg(f) = 2g + 1$.*

Proof. Observe that $b \neq 0$, since otherwise either $p|f$ or p is inert. Then the Corollary follows from comparison of degrees in the equation of Proposition 7.3.2. □

Doing another simple comparison of degrees allows us to give a sufficient condition for the f.f. fake Ankeny-Artin-Chowla property.

Proposition 7.3.4. *Let $p \in k[x]$ be irreducible, coprime to f and splitting over $\mathcal{O}_K$. Then if*

$$o(\mathfrak{p}) \deg(p) < 3 \deg(f) = 6g + 3,$$

the f.f. fake Ankeny-Artin-Chowla property holds.

Proof. Since a^2 has even degree and fb^2 has odd degree, their leading terms don't cancel out. Therefore

$$\deg(fb^2) \leq \deg(a^2 - fb^2) = \deg(p^{o(\mathfrak{p})}) = o(\mathfrak{p}) \deg(p) < 3 \deg(f).$$

Therefore $\deg(b) < \frac{1}{2}(2 \deg(f)) = \deg(f)$. So either $f \not| b$ or $b = 0$. If $b = 0$ however, then p is the fundamental unit, so $\mathfrak{p}^{o(\mathfrak{p})} = \mathfrak{p}\overline{\mathfrak{p}}$ and so by unique prime ideal factorisation $o(\mathfrak{p}) = 2$ and $\mathfrak{p} = \overline{\mathfrak{p}}$. That means that $\mathfrak{p}$ corresponds to a Weierstrass point, hence p divides f, which we assumed not to be the case. □

Now we will give a result independent of $o(\mathfrak{p})$.

Theorem 7.3.5. *Let p be irreducible, coprime to f and splitting over $\mathcal{O}_K$. Assume $\deg(p) \leq g + 1$. Then the f.f. fake Ankeny-Artin-Chowla property holds.*

Proof. Let us apply the Mason-Stothers theorem to the equation $a^2 - fb^2 = c \cdot p^{o(\mathfrak{p})}$. We notice that $\gcd(a, f) = 1$, otherwise $a^2 - fb^2$ wouldn't be coprime to f, which $c \cdot p^{o(\mathfrak{p})}$ is. Also, a, b are coprime, since otherwise $a + b\sqrt{f}$ wouldn't be fundamental. This together with not all derivatives being zero, would allow us to use the Mason-Stothers theorem.

Suppose that all derivatives are zero. If the characteristic ℓ equals 0, then this would mean p is constant, which is a contradiction. Now treat the case $\ell > 2$. Then a^2, fb^2 are ℓ-th powers. The first gives that a is an ℓ-th power, so let $a = \tilde{a}^\ell$ for some $\tilde{a} \in k[x]$. For the second, let $k \in \mathbb{N}$ the amount of times f divides b. Then we observe that $1 + 2k \equiv 0 \mod \ell$. In other words, $k = \frac{\ell-1}{2} + m\ell$ for some $m \in \mathbb{N}$. Furthermore, notice that $b^2 f^{-2k} = (fb^2) f^{-2k-1}$ is an ℓ-th power, hence also bf^{-k}. It follows that $b = f^k \tilde{b}^\ell$ for some $\tilde{b} \in k[t]$. Therefore, we can write

$$fb^2 = f^{1+2k}\tilde{b}^{2\ell} = f^{1+(\ell-1)+2m\ell}\tilde{b}^{2\ell} = f^{(2m+1)\ell}\tilde{b}^{2\ell}.$$

In other words, $b\sqrt{f} = \tilde{b}^{\ell} f^{(m+\frac{1}{2})\ell}$. Now one can notice that $(\tilde{a} + \tilde{b} f^m \sqrt{f})^{\ell} = a + b\sqrt{f}$. This is a contradiction with the assumption that $a + b\sqrt{f}$ is a fundamental unit.

So not all derivatives are zero and we are allowed to use the Mason-Stothers theorem. Let us for a contradiction assume the f.f. fake Ankeny-Artin-Chowla property doesn't hold. Let $b = fd$ for some $d \in k[x]$. The equation then becomes $a^2 - f^3 d^2 = c \cdot p^{o(\mathfrak{p})}$. The Mason-Stothers theorem gives

$$2\deg(a) \leq \deg(a) + \deg(f) + \deg(d) + \deg(p) - 1,$$

from which we see

$$\deg(a) + \deg(p) - 1 \leq \deg(f) + \deg(d) + 2\deg(p) - 2. \tag{1}$$

It also gives us

$$3\deg(f) + 2\deg(d) \leq \deg(a) + \deg(f) + \deg(d) + \deg(p) - 1,$$

which implies

$$2\deg(f) + \deg(d) \leq \deg(a) + \deg(p) - 1. \tag{2}$$

Combining inequalities (1) and (2), we obtain

$$2\deg(f) + \deg(d) \leq \deg(f) + \deg(d) + 2\deg(p) - 2.$$

Therefore, $\deg(f) \leq 2\deg(p) - 2$. So $2\deg(p) \geq 2 + \deg(f) = 2g + 3$. That implies $\deg(p) > g + 1$. This contradicts our assumption that $\deg(p) \leq g + 1$, so our assumption that the fake f.f. Ankeny-Artin-Chowla property doesn't hold, is false. □

Corollary 7.3.6. *Let $p \nmid f$ be splitting such that $\deg(p) \leq 2$. Then the f.f. fake Ankeny-Artin-Chowla property holds.*

Proof. If $g \geq 1$, this follows from Theorem 7.3.5. If $g = 0$, then this follows from Corollary 7.2.5. □

Corollary 7.3.7. *Let k be such that $[\overline{k} : k] \leq 2$. Then the f.f. fake Ankeny-Artin-Chowla property holds for $p \nmid f$ splitting.*

Proof. This follows from the fact that in this case, all irreducible polynomials have degree at most 2. □

Corollary 7.3.8. *Let k be algebraically closed or let $k = \mathbb{R}$. Then the f.f. fake Ankeny-Artin-Chowla property holds for $p \nmid f$ splitting.*

Corollary 7.3.9. *Let k be finite and fix $p \in k[x]$ irreducible. Then for all but finitely many $f \in k[x]$ squarefree among those such that p is splitting, the f.f. fake Ankeny-Artin-Chowla property is satisfied.*

7.4 Horizontal asymptotics for $k = \mathbb{F}_q$

We will now study horizontal asymptotics of the f.f. fake Ankeny-Artin-Chowla property in the global case, so in the case $k = \mathbb{F}_q = \mathbb{F}_{\ell^r}$. Before we restrict to such k, we first describe $(\mathcal{O}_K/f)^\times = A \times B$ (see Subsection 2.2) where $A \cong k[x]/f$ and $B \cong (k[x]/f)^\times$ for general perfect k, to give another characterization of the f.f. fake Ankeny-Artin-Chowla property.

Lemma 7.4.1. *Assume $p \nmid f$. The image of the fundamental unit ϵ under $\mathcal{O}_K \to \mathcal{O}_K/f$ is in $(\mathcal{O}_K/f)^\times$. Moreover, the f.f. fake Ankeny-Artin-Chowla property holds if and only if the image of ϵ is not in B.*

Proof. Observe that $\epsilon\bar{\epsilon} = c \cdot p^{o(\mathfrak{p})}$ is a unit in $\mathcal{O}_K/f$, as its inverse is $h \in k[x]$ such that $cp^{o(\mathfrak{p})}h \equiv 1 \mod f$, which exists because p doesn't divide f. □

We see that A is torsion-free for characteristic $\ell = 0$ and that every non-trivial element of A is of order ℓ if $\ell > 2$. In other words, if $\ell = 0$, then A can be viewed as a $\mathbb{Q}$-vector space and if $\ell > 2$, then $\mathcal{O}_K/(f)$ can be viewed as an $\mathbb{F}_\ell$-vector space.

Lemma 7.4.2. *If $\ell > 2$, (the torsion of) B is coprime to ℓ.*

Proof. If not, then there is an element in B of order ℓ. This can be represented by a $b \in k[x]$ coprime to f. Then $b^\ell \equiv 1 \mod f$. So also $b^\ell \equiv 1 \mod f_i$ for each irreducible factor $f_i | f$. Now since k is perfect and $k[x]/(f_i)$ is a finite extension for all $f_i | f$, we have $k[x]/(f_i)$ perfect. Therefore, we have $b \equiv 1 \mod f$. So this element is trivial, which contradicts it being of order ℓ. □

Corollary 7.4.3. *For $\ell > 0$, the ℓ-part of $(\mathcal{O}_K/f)^\times$ is A.*

Corollary 7.4.4. *Let $c + d\sqrt{f} := \epsilon^m$ for some $m \in \mathbb{Z}$.*

- *If $\ell = 0$, then $f|d$ if and only if $f|b$.*
- *If $\ell > 2$ and $\ell \nmid m$, then $f|d$ if and only if $f|b$.*

Proof. If $\ell = 0$, then this follows from A being torsion-free. If $\ell > 2$, then it follows from A being an ℓ-group. □

Now assume $k = \mathbb{F}_q = \mathbb{F}_{\ell^r}$ is finite. Then the following theorem holds, which is inspired by the work of Florian Hess, Renate Scheidler and Micheal J. Jacobson in [11], which is the number field analogue.

Theorem 7.4.5. *Fix f and vary p. Let G be the ℓ-part of $Cl_f^0(K)$. Then the proportion of p irreducible, splitting, with $\deg(p) = n$ such that the fake f.f. Ankeny-Artin-Chowla property does not hold, approaches $\frac{1}{\#G}$ as $n \to \infty$.*

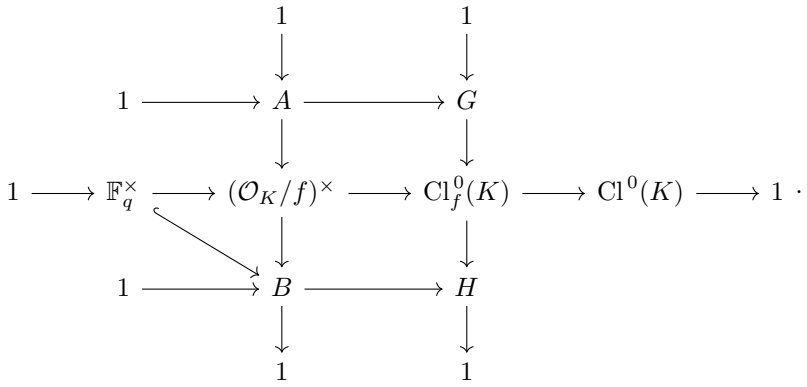
Proof. Before we start, note that all but finitely many irreducible $p \in \mathbb{F}_q[t]$ are coprime to f, so we can focus on those.

We look at the exact sequence

$$1 \to \mathbb{F}_q^\times \to (\mathcal{O}_K/f)^\times \to \mathrm{Cl}_f^0(K) \to \mathrm{Cl}^0(K) \to 1. \tag{3}$$

Then $\mathcal{O}_K[\mathfrak{p}^{-1}]$ gives a counterexample if and only if $[\mathfrak{p}]_f^{o(\mathfrak{p})} = [\epsilon \cdot \mathcal{O}_K]_f^{o(\mathfrak{p})}$ is in the image of B, i.e. has trivial A-part.

We decompose $\mathrm{Cl}_f^0(K) \cong G \times H$, where G is the ℓ-part and H is the part coprime to ℓ. (This can be done due to the fundamental theorem of finitely generated abelian groups.) Then we see that A injects into G. The following diagram gives an overview of the relations between the groups studied so far, where all horizontal and vertical sequences are exact:



We claim that in general $[I]_f^{o(I)}$ is in the image of B if and only if $[I]_f \in H$.

'If': $[I]_f$ has G-part 0 and A injects into G, so $[I]_f^{o(I)}$ has A-part 0.

'Only if': If $\ell \nmid o(I)$, then $[I]_f \in H$ simply because G is a ℓ-group.
It remains to consider the case that $\ell | o(I)$, let's show that this case doesn't occur. If it did, then the G-component $[J]_f$ of $[I^{o(I)/\ell}]_f$ has order $o(J) = \ell$ in $\mathrm{Cl}^0(K)$ (because H is primary to ℓ) and hence satisfies $[J]_f^{o(J)} = [0]$ (It has A-part 0 by assumption and B-part 0 by construction). So it is an element of $G[\ell]$, which is not induced by a member of $A[\ell]$. Hence $A[\ell] \ncong G[\ell]$. Now while finishing the final state of this master's project, Florian Hess sent me a proof [9] of the following:

Fact. *The ℓ-rank of $Cl_f(K)$ is equal to $r \deg(f)$.*

As a consequence, $(\mathcal{O}_K/f \cdot \mathcal{O}_K)^\times$ and $\mathrm{Cl}_f^0(K)$ are finite abelian groups of the same ℓ-rank and A, G are the corresponding ℓ-parts. So this means $A[\ell] \cong G[\ell]$. This is a contradiction, so the case that $\ell | o(I)$ cannot occur.

Therefore the cases where the f.f. fake Ankeny-Artin-Chowla property doesn't hold are those where $[\mathfrak{p}]_f \in H$. Now let E be the class field corresponding to H. In other words, there is a surjective Artin map $A_{E|K} : \mathrm{Cl}_f(K) \to \mathrm{Gal}(E|K)$ which has kernel H, in other words $G \cong \mathrm{Cl}_f(K)/H \cong \mathrm{Gal}(E|K)$.

So by Lemma 7.4.1, this means that cases where the fake f.f. Ankeny-Artin-Chowla property doesn't hold are those where the image of $[\mathfrak{p}]_f$ in $\mathrm{Gal}(E|K)$ is trivial.

According to Theorem 2.3.9 for function fields, we have

$$\#\{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K) : \deg(p) = n \text{ and } (\mathfrak{p}, E|K) = 1\} = \frac{1}{\#\mathrm{Gal}(E|K)} \frac{q^n}{n} + o\left(\frac{q^{n/2}}{n}\right) \sim \frac{1}{\#G} \frac{q^n}{n}.$$

We also have

$$\#\{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K) : \deg(p) = n\} \sim \frac{q^n}{n}.$$

These two facts combine to imply

$$\lim_{n\to\infty} \frac{\#\{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K) : \deg(p) = n \text{ and } f|b\}}{\#\{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K) : \deg(p) = n\}} = \lim_{n\to\infty} \frac{\#\{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K) : \deg(p) = n \text{ and } (\mathfrak{p}, E|K) = 1\}}{\#\{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K) : \deg(p) = n\}} = \frac{1}{\#G}.$$

□

Remark 7.4.6. An analogous proof shows that Theorem 7.4.5 also holds when replacing the condition $\deg(p) = n$ with the condition $\deg(p) \leq n$.

Remark 7.4.7. I checked this condition that the ℓ-rank of $\mathrm{Cl}_f^0(K)$ is equal to $r\deg(f)$ before I received the proof of Florian Hess in [9]. I have verified using Magma that the ℓ-rank of $\mathrm{Cl}_f^0(K)$ equals $r\deg(f)$ for

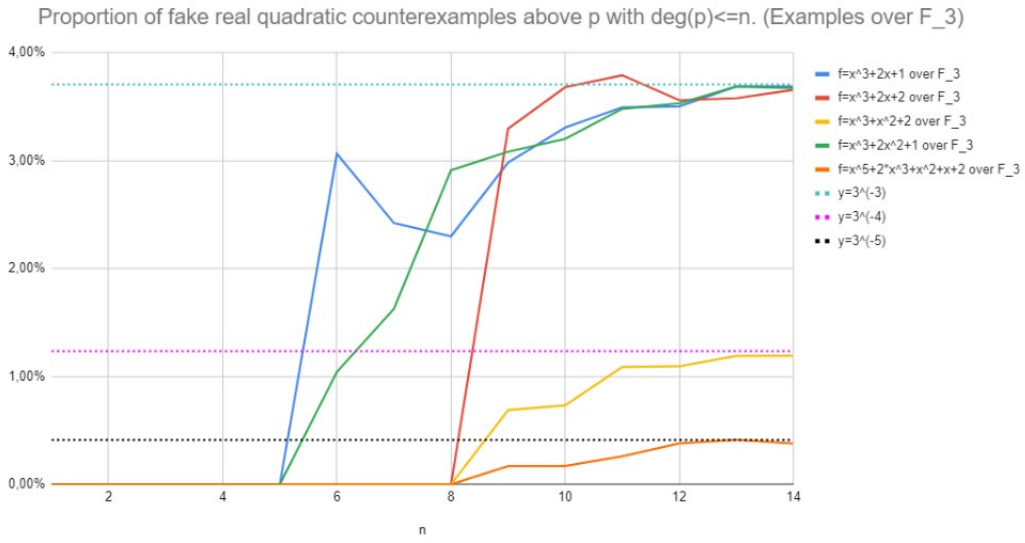
$$\begin{cases} g \leq 5 & \text{if } q = 3 \\ g \leq 3 & \text{if } q \leq 7 \\ g \leq 2 & \text{if } q \leq 25 \text{ or } q = 29, 31, 37 \\ g \leq 1 & \text{if } q \leq 47 \end{cases}.$$

In the number field analogue in [11] on which this theorem and proof are based, there is no additional condition like this required and the proportion is also independent of the ray class group, although the proof makes use of the ray class group.

Corollary 7.4.8. *We fix f and vary p. Assume $\ell \nmid \#Cl_f^0(K)$. Then the proportion of p irreducible, splitting, with $\deg(p) = n$ (or $\deg(p) \leq n$), such that the f.f. fake Ankeny-Artin-Chowla property does not hold, approaches $\frac{1}{q^{\deg(f)}}$ as $n \to \infty$.*

Proof. Observe that the ℓ-rank of $\mathrm{Cl}_f^0(K)$ is $r\deg(f)$, so we may use Theorem 7.4.5. In this case, we note that the cokernel of injection $A \to G$ is trivial, so $G \cong A$. In particular, the ℓ-rank of $\mathrm{Cl}_f^0(K)$ is equal to the ℓ-rank of A, which is $r\deg(f)$. Now apply Theorem 7.4.5 together with the observation that $\#G = \#A = q^{\deg(f)}$ to get the result. □

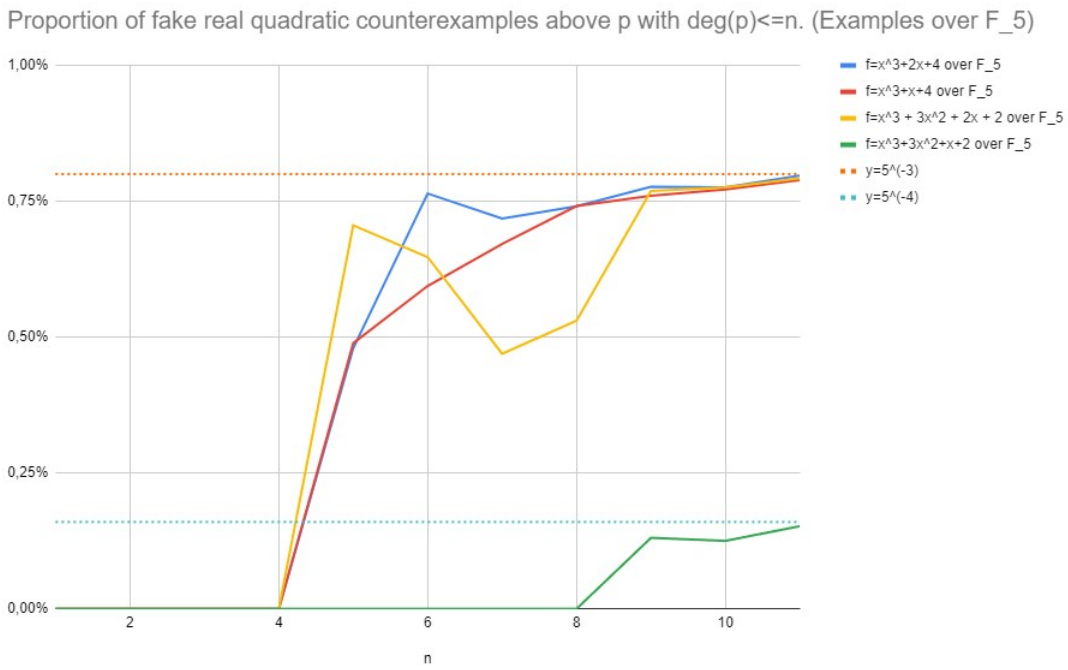
Given below is some numerical data showing how this proportion converges. I took $k = \mathbb{F}_3, \mathbb{F}_5$ for a low computation time, since the amount of examples needed to be checked is roughly $\mathcal{O}(q^n)$. A graph showing convergence behaviour is given, as well as a table checking we can apply Theorem 7.4.5 and what therefore the expected proportion is.



f	$G \cong$	3-rank of G	$r\deg(f)$	Expected proportion $1/\#G$
x^3+2x+1	$(\mathbb{Z}/3\mathbb{Z})^3$	3	3	3^{-3}
x^3+2x+2	$(\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})^2$	3	3	3^{-4}
x^3+x^2+2	$(\mathbb{Z}/3\mathbb{Z})^3$	3	3	3^{-3}
x^3+2x^2+1	$(\mathbb{Z}/3\mathbb{Z})^3$	3	3	3^{-3}
$x^5+2x^3+x^2+x+2$	$(\mathbb{Z}/3\mathbb{Z})^5$	5	5	3^{-5}

Table 1: Examples over $\mathbb{F}_3$

On the next page, there are some other examples with $k = \mathbb{F}_5$.



f	Representation of G	5-rank of G	$r\deg(f)$	Expected proportion $1/\#G$
x^3+2x+4	$(\mathbb{Z}/5\mathbb{Z})^3$	3	3	5^{-3}
x^3+x+4	$(\mathbb{Z}/5\mathbb{Z})^3$	3	3	5^{-3}
x^3+3x^2+2x+2	$(\mathbb{Z}/5\mathbb{Z})^3$	3	3	5^{-3}
x^3+3x^2+2x+2	$(\mathbb{Z}/5\mathbb{Z})^3$	3	3	5^{-3}
x^3+3x^2+x+2	$(\mathbb{Z}/25\mathbb{Z})\times(\mathbb{Z}/5\mathbb{Z})^2$	3	3	5^{-4}

Table 2: Examples over $\mathbb{F}_5$

7.5 Constant field extensions

A question that one might ask is; is satisfying the f.f. fake Ankeny-Artin-Chowla property independent of the constant field? To be precise, let us start off with a fake real quadratic order over $k(x)$ determined by $f, p \in k[x]$, p irreducible and f squarefree. Additionally assume p is irreducible in $l[x]$ for some perfect field l extending k. Then there is a canonical fake real quadratic order over $l(x)$ corresponding to f, p. Does the f.f. fake Ankeny-Artin-Chowla property hold over $k(x)$ if and only if it holds over $l(x)$? Before we answer this, let us compare the corresponding residue rings. Recall from Subsection 2.2 that $(\mathcal{O}_K/f)^\times = A \times B$ where $A \cong k[x]/f$ and $B \cong (k[x]/f)^\times$. We put k, l in subscripts of any variables to indicate we are working over $k(x), l(x)$ respectively.

Lemma 7.5.1. *There is a commutative diagram of injective group homomorphisms:*

$$\begin{array}{ccccc} A_k & \hookrightarrow & (\mathcal{O}_{K_k}/f)^\times & \hookleftarrow & B_k \\ \downarrow & & \downarrow & & \downarrow \\ A_l & \hookrightarrow & (\mathcal{O}_{K_l}/f)^\times & \hookleftarrow & B_l \end{array}$$

Proof. The ring morphism $\mathcal{O}_{K_k} \to \mathcal{O}_{K_l} \to \mathcal{O}_{K_l}/f$ induced by $K_k \to K_l$ has kernel $f \cdot \mathcal{O}_{K_k}$. Therefore, there is an injective ring homomorphism $\mathcal{O}_{K_k}/f \to \mathcal{O}_{K_l}/f$ and so also an injective group homomorphism $(\mathcal{O}_{K_k}/f)^\times \to (\mathcal{O}_{K_l}/f)^\times$.

The ring morphism $k[x] \to l[x] \to l[x]/f$ has kernel $f \cdot k[x]$, so there is an injective ring homomorphism $k[x]/f \to l[x]/f$. So there is also an injective group homomorphism on the additive groups, giving the injective group homomorphism $A_k \to A_l$. It also means there is an injective group homomorphism of the unit groups $B_k \to B_l$.

Here is a proof that the left square is commutative: take an element of A_k, it is of the form $d \mod f \cdot l[x]$ for some $d \in k[x]$. Its image in A_l is also given as $d \mod f \cdot l[x]$, but this time around, this is modular arithmetic in $l[x]$. So the image of that would be given as $1 + d\sqrt{f}$. And this is the same result that one gets if one first maps to $(\mathcal{O}_{K_k}/f)^\times$ and then to $(\mathcal{O}_{K_l}/f)^\times$.

Proving that the second square is commutative works very similarly. □

Lemma 7.5.2. *We have that ϵ_k is a positive power of ϵ_l modulo $l^\times$.*

Proof. We note that $\mathfrak{p}_k$ is the pre-image of $\mathfrak{p}_l$ under the injective ring morphism $\mathcal{O}_{K_k} \to \mathcal{O}_{K_l}$. Therefore, $\mathfrak{p}_k^{-1}$ is the pre-image of $\mathfrak{p}_l^{-1}$ under $\mathcal{O}_{K_k} \to \mathcal{O}_{K_l}$. Hence $\mathfrak{p}_k^{-1} \subseteq \mathfrak{p}_l^{-1}$ and so there is an injective ring homomorphism $\mathcal{O}_{K_k}[\mathfrak{p}_k^{-1}] \to \mathcal{O}_{K_l}[\mathfrak{p}_l^{-1}]$. Therefore, there is also an injective group homomorphism $k^\times \times \epsilon_k^{\mathbb{Z}} \to l^\times \times \epsilon_l^{\mathbb{Z}}$. In particular, $\epsilon_k \in (l^\times \times \epsilon_l^{\mathbb{Z}}) \cap \mathcal{O}_{K_k}$ is a positive power of ϵ_l up to multiplication in $l^\times$. □

Proposition 7.5.3. *Let $f, p \in k[x]$ be such that f is squarefree in $k[x]$ and p is irreducible in $l[x]$. Then the f.f. fake Ankeny-Artin-Chowla property holds for the pair (f, p) over $k(x)$ if and only if it holds for the pair (f, p) over $l(x)$.*

Proof. By Lemma 7.4.1, the f.f. fake Ankeny-Artin-Chowla property is satisfied if and only if the image of fundamental unit under $\mathcal{O}_K \to \mathcal{O}_K/f \cdot \mathcal{O}_K$ is in B. So the fake f.f. Ankeny-Artin-Chowla property is satisfied over $k(x), l(x)$if and only if $\overline{\epsilon_k} \in B_k$, $\overline{\epsilon_l} \in B_l$ respectively. Let $m \in \mathbb{N}$ be such that $\epsilon_k \epsilon_l^{-m} \in l^\times$.

If $\ell = 0$, then the A_k-part of $\overline{\epsilon_k}$ is 0 if and only if the A_l-part of $\overline{\epsilon_l}^{-m}$ is 0, if and only if A_l-part of $\overline{\epsilon_l}$ is 0, because A_l is torsion-free. So this is clear.

If $\ell > 2$ and $\ell \nmid m$, then the A_k-part of $\overline{\epsilon_k}$ is 0 if and only if the A_l-part of $\overline{\epsilon_l}^{-m}$ is 0, if and only if the A_l-part of $\overline{\epsilon}_l$ is 0. This is because all elements of A_l except the identity are of order ℓ.

Now assume $\ell | m$. Then ϵ_l^m is an ℓ-th power. So write $\epsilon_l^m = (c + d\sqrt{f})^\ell = c^\ell + d^\ell f^{\frac{\ell-1}{2}}\sqrt{f}$ for some $c, d \in l[x]$. Hence c^ℓ is in $c^\ell \cdot k[t]$. Let χ be the leading coefficient of c, then $(\chi^{-1}c)^\ell$ is monic, hence in $k[x]$ by this logic. Writing $c = \sum c_i x^i$, we have hence $\chi^{-\ell} c_i^\ell \in k$ for all i. Since both k and l are perfect, we have that the frobenius $k \to k$ and $l \to l$ are automorphisms of k, l respectively. Therefore the pre-image of k under Frobenius $l \to l$ is k. This implies $\chi^{-1} c_i \in k$ for all i. Therefore, $\chi^{-1} c \in k[x]$. So c is in $l^\times \cdot k[x]$. And without loss of generality, we can assume d monic hence by similar logic, d is in $k[x]$. However that implies $\chi^\ell \in k^\times$, since $\chi^{-\ell}\epsilon_l^m \in \mathcal{O}_{K_k}$. So $\chi \in k^\times$ (again since k, l are perfect) and hence $c + d\sqrt{f} \in \mathcal{O}_{K_k}$, which is a contradiction. So $\ell \nmid m$ and we are done. □

What if p is not irreducible in $l[x]$, but we just look at all the fake real quadratic orders over $l(x)$ such that the prime is above p? Then it turns out that whether the f.f. fake Ankeny-Artin-Chowla property is satisfied can change. A simple example is when one takes l to be the splitting field of f. Then in the $l(x)$-situation, the f.f. fake Ankeny-Artin-Chowla property always holds according to Corollary 7.3.6 because the new p is linear, while the fake f.f. Ankeny-Artin-Chowla property doesn't necessarily hold in the $k(x)$-situation.

7.6 Comparing $k = \mathbb{Q}, \mathbb{Q}_\ell$ with $k = \mathbb{F}_\ell$

Let $K = \mathbb{Q}(t, \sqrt{f(x)})$, we can without loss of generality assume $f \in \mathbb{Z}[x]$ monic. Let $p \in \mathbb{Z}[x]$ be monic irreducible and let $a + b\sqrt{f}$ be a fundamental unit of $\mathcal{O}_K$, where $a, b \in \mathbb{Z}[x]$ and $\gcd_i(a_i) = \gcd_i(b_i) = 1$.

Definition 7.6.1. We say that a prime ℓ is of *extra good reduction* with respect to the fake real quadratic order $\mathcal{O}_K[\mathfrak{p}^{-1}]$ if ℓ is of good reduction for the corresponding curve C and $p \mod \ell$ is irreducible. We write $\overline{\mathcal{O}_K[\mathfrak{p}^{-1}]}$ or $\mathcal{O}_K[\mathfrak{p}^{-1}] \mod \ell$ for the fake real quadratic order corresponding to $\overline{f}, \overline{p}$.

How can one find out how many primes of extra good reduction there are? The following lemma answers that.

Lemma 7.6.2. *Let L be the splitting field of p, let $n = \deg(p)$. Then if $Gal(L/\mathbb{Q})$ as a subgroup of S_n contains n-cycles, the proportion of ℓ such that $p \mod \ell$ is irreducible is $\frac{\#\{n-cycles\ in\ Gal(L/\mathbb{Q})\}}{\#Gal(L/\mathbb{Q})}$, hence then there are infinitely many such ℓ. Otherwise, there are no primes of extra good reduction.*

Proof. There are only finitely many ℓ for which $f \mod \ell$ isn't squarefree, these are the primes of good reduction of the hyperelliptic curve C. Therefore, we can focus on the condition that $p \mod \ell$ is irreducible. Each element of $\mathrm{Gal}(L/\mathbb{Q})$ can be given by a permutation of the roots of p and vice versa. This is the way in which we view $\mathrm{Gal}(L/\mathbb{Q})$ as a subgroup of S_n. Let $\overline{p} = \prod_{i=1}^r \overline{p_i}$ for some $r \in \mathbb{N}$, $\overline{p_1}, \ldots, \overline{p_r} \in \mathbb{F}_\ell[x]$. (not necessarily distinct.) Then the corresponding permutation is the product of cycles where each $\overline{p_i}$ corresponds with a $\deg(\overline{p_i})$-cycle. Therefore, $\overline{p}$ is irreducible if and only if the corresponding permutation is an n-cycle. Then Theorem 2.3.9 implies the result. See also [23]. □

Remark 7.6.3. We note that in this case, p splitting implies $\overline{p}$ splitting. The reverse is not true however. Take for example $\ell = 5$, $p = x + 1$ and $f = x$. Then $\overline{p}$ is split in $\mathbb{F}_5[x, \overline{f}]$ since the corresponding points are $(-1, \pm 2)$. (Due to Proposition 7.1.3.) In contrast, p is not split in $\mathbb{Q}[x, f]$, since -1 is not a square in $\mathbb{Q}$.

Lemma 7.6.4. *Let $\epsilon_{\mathbb{Q}} = a + b\sqrt{f}$ be a fundamental unit of $\mathcal{O}_K[\mathfrak{p}^{-1}]$ and let ℓ be a prime of extra good reduction. Then $\overline{a} + \overline{b}\sqrt{\overline{f}}$ is a fundamental unit of $\mathcal{O}_K[\mathfrak{p}^{-1}] \mod \ell$.*

Proof. We have $a^2 - fb^2 = c \cdot p^{o(\mathfrak{p})}$ for some $c \in \mathbb{Q}^\times \cap \mathbb{Z}$ according to Proposition 7.3.2. Without loss of generality, $c = \pm 1$. Then we reduce the fundamental unit modulo a prime of good reduction ℓ and so we get an equation $\overline{a}^2 - \overline{f}\overline{b}^2 = \pm\overline{p}^{o(\mathfrak{p})}$. Since $J(\mathbb{Q})_{\text{tors}} \to \tilde{J}(\mathbb{F}_\ell)$ is an injective group homomorphism where J is the Jacobian of C according to Theorem 2.1.10, we have $o(\mathfrak{p})$ is the order of the corresponding reduced prime ideal in $\overline{\mathcal{O}_K[\mathfrak{p}^{-1}]}$. Therefore by Proposition 7.3.2, $\overline{a} + \overline{b}\sqrt{\overline{f}} = \overline{\epsilon_{\mathbb{Q}}}$ is a fundamental unit of $\mathcal{O}_K[\mathfrak{p}^{-1}] \mod \ell$. □

Theorem 7.6.5. *Assume that there exists a prime ℓ such that $p \mod \ell$ is irreducible. Then the following are equivalent.*

1. *The f.f. fake Ankeny-Artin-Chowla property holds for $\mathcal{O}_K[\mathfrak{p}^{-1}]$. (over $\mathbb{Q}(x)$)*
2. *For all but finitely many primes ℓ of extra good reduction, the fake f.f. Ankeny-Artin-Chowla property holds for $\mathcal{O}_K[\mathfrak{p}^{-1}] \mod \ell$.*
3. *For some prime ℓ of extra good reduction, the f.f. fake Ankeny-Artin-Chowla property holds for $\mathcal{O}_K[\mathfrak{p}^{-1}] \mod \ell$.*

Proof. (1) $\implies$ (2): Let $b = cf + d$ for some $c, d \in \mathbb{Z}[x]$ such that $\deg(d) < \deg(f)$. Then $d \neq 0$, since we assumed the f.f. fake Ankeny-Artin-Chowla property to hold over $\mathbb{Q}(x)$. So there are only finitely many (integral) primes ℓ that divide d, in which case $b \equiv cf \mod \ell$ and hence the fake f.f. Ankeny-Artin-Chowla property does not hold. For all other ℓ, $d \not\equiv 0 \mod \ell$, so the f.f. fake Ankeny-Artin-Chowla property holds.

(2) $\implies$ (3): Follows from Lemma 7.6.2.

(3) $\implies$ (1): We note that $(f \mod \ell) \nmid (b \mod \ell)$ implies $f \nmid b$ and then apply Lemma 7.6.5. □

We can also rephrase this in terms of when the f.f. fake Ankeny-Artin-Chowla property is not satisfied. (This is hence not new information, but can give helpful insight.)

Corollary 7.6.6. *Assume that there exists a prime ℓ such that $p \mod \ell$ is irreducible. The following are equivalent.*

1. *The f.f. fake Ankeny-Artin-Chowla property does not hold for $\mathcal{O}_K[\mathfrak{p}^{-1}]$. (over $\mathbb{Q}(x)$)*
2. *For infinitely many primes ℓ of extra good reduction, the f.f. Ankeny-Artin-Chowla property does not hold for $\mathcal{O}_K[\mathfrak{p}^{-1}] \mod \ell$. (over $\mathbb{F}_\ell(x)$)*
3. *For all primes ℓ of extra good reduction, the f.f. fake Ankeny-Artin-Chowla property does not hold for $\mathcal{O}_K[\mathfrak{p}^{-1}] \mod \ell$. (over $\mathbb{F}_\ell(x)$)*

Example 7.6.7. *It is however not the case that the f.f. fake Ankeny-Artin-Chowla property holding over $\mathbb{Q}(x)$ implies it holds over $\mathbb{F}_\ell(x)$ for all ℓ of extra good reduction. Let m be an integer divisible by 3. Then we let*

$$f = x^3 - x - 1,$$
$$p = (x^3 - x - 1)(x^3 - x + m - 1)^2 - (-x^3 + x^2 + x + 1)^2.$$

Observe that f is squarefree since it is squarefree modulo 3 and p is irreducible since it is irreducible modulo 3. In this case, a fundamental unit is

$$\epsilon = (-x^3 + x^2 + x + 1) + (x^3 - x + m - 1)\sqrt{x^3 - x - 1}$$

by Proposition 7.3.2, since its norm is $-p$. Then the f.f. fake Ankeny-Artin-Chowla property by construction is true over $\mathbb{Q}(x)$. It does not hold over $\mathbb{F}_\ell(x)$ for all primes ℓ of extra good reduction that divide m, since then $\overline{m} = \overline{0}$. Also, it holds over $\mathbb{F}_\ell(x)$ for all primes ℓ of extra good reduction coprime to m, since then $\overline{m} \neq \overline{0}$.

Taking $m = 0$ gives that the f.f. fake Ankeny-Artin-Chowla property does not hold for $\mathbb{Q}(x)$ and hence not for all $\mathbb{F}_\ell(x)$ where ℓ is of extra good reduction, by Corollary 7.6.6.

We can also take $m = \pm 1$, letting go of the requirement that $3|m$. Magma ensures us that p is still irreducible and the fundamental unit is still the same. Then this gives that the f.f. fake Ankeny-Artin-Chowla property holds over $\mathbb{Q}(x)$ and hence also over $\mathbb{F}_\ell(x)$ for all primes ℓ of extra good reduction, since $\overline{m} = \overline{\pm 1} \neq \overline{0}$.

Example 7.6.8. *The $m = 0$ case is an example of a more general phenomenon; Let us have a case over $\mathbb{F}_\ell(x)$ where the fake f.f. Ankeny-Artin-Chowla property does not hold and the prime ideal is principal. Write $\overline{b} = \overline{df}$ for some $\overline{d} \in \mathbb{F}_\ell[x]$. Then we take some lifts a, d, f of $\overline{a}, \overline{d}, \overline{f}$. Furthermore let $p := \pm(a^2 - f^3 d^2)$ such that p is a lift of $\overline{p}$. We are garantueed f, p are squarefree and irreducible just like before. Then $a + df\sqrt{f}$ is a fundamental unit corresponding to (f, p) again by Proposition 7.3.2, so it is a counterexample over $\mathbb{Q}(x)$.*

Here is a table of constructed principal counterexamples over $\mathbb{Q}(x)$ in this way:

Genus	f	p	a	b
0	x	$x^3 - 4$	2	x
1	$x^3 - x - 1$	$fb^2 - a^2$	$x^3 - x^2 - x - 1$	$x^3 - x - 1$
2	$x^5 - x^2 + x + 1$	$fb^2 - a^2$	$x^3 + x^2$	$x^5 - x^2 + x + 1$
3	$x^7 + x^2 - 1$	$fb^2 - a^2$	$x^9 + x^7 + x^6 + x^5 + x^3 + x^2 + x - 1$	$x^7 + x^2 - 1$
4	$x^9 - x^3 - x^2 + x + 1$	$fb^2 - a^2$	$x^{12} + x^{10} - x^9 + x^7 - x^4 + x^3 + x$	$x^9 - x^3 - x^2 + x + 1$

Example 7.6.9. *Another way to view finding counterexamples where the prime ideal is principal is by looking at the norm equation. Fix $a, b \in k(x)$ and try to find solutions to $a^2 - f^3 d^2 = p$ where $f \in k(x)$ is squarefree and $p \in k(x)$*

and $b = fd$ for some $d \in k[x]$. Take $k = \mathbb{Q}$. There is a lot of room for attempts here, but a simple case would be to consider $f = x^3 - 2$ and $b = 1$ for instance. Vary a and see if you can make $a(x)^2 - (x^3-2)^3$ irreducible. We can immediately see that for instance taking $a(x) = x$ gives a counterexample. This is analogous to what is done for finding counterexamples to the n.f. fake Ankeny-Artin-Chowla property, as mentioned in [11].

We can also compare the cases $k = \mathbb{Q}_\ell$ and $k = \mathbb{F}_\ell$ by reducing. We need to be careful: we assume ℓ is of extra good reduction in the analogous sense. Again we have that the order of the prime ideal doesn't change when reducing; so again we have $\epsilon_{\mathbb{F}_\ell} = \overline{\epsilon_{\mathbb{Q}_\ell}}$. We write $\mathcal{O}_K[\mathfrak{p}^{-1}] \mod \ell$ again for the reduction of the relevant fake real quadratic modulo ℓ.

Proposition 7.6.10. *Let $f, p \in \mathbb{Z}_\ell[x]$ be such that f monic squarefree and let $K = \mathbb{Q}_\ell(x, \sqrt{f(x)})$. Let p monic irreducible splitting in $\mathcal{O}_K$ and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ above p. Assume that ℓ is of extra good reduction. Then the f.f. fake Ankeny-Artin-Chowla property holds for $\mathcal{O}_K[\mathfrak{p}^{-1}]$ if it holds for $\mathcal{O}_K[\mathfrak{p}^{-1}] \mod \ell$.*

Proof. Follows from $\overline{f} \nmid \overline{b}$ implying $f \nmid b$. □

7.7 Comparing k a number field with $k = \mathbb{F}_q$

This subsection aims to generalize the previous subsection. Let k be a number field, $\mathcal{O}_k$ the ring of integers. Let $y^2 = f(x)$ be (an affine patch of) a hyperelliptic curve over k; without loss of generality we let $f \in \mathcal{O}_k[x]$. Assume that f is monic. Let $p \in \mathcal{O}_k[x]$ be irreducible and let $\mathcal{O}_K[\mathfrak{p}^{-1}]$ be the fake real quadratic order corresponding to f, p. Now reduce this modulo a prime ideal $\mathfrak{q}$ of $\mathcal{O}_k$ above some integral prime $\ell > 2$. When is this possible? Note that $\mathcal{O}_k/\mathfrak{q} \cong \mathbb{F}_q$, where $q = \ell^r$ for some $r \in \mathbb{N}$. So it makes sense to reduce f to $\mathbb{F}_q[t]$, we want the reduction to be squarefree. The same goes for $p \in k[x]$ monic irreducible, we want the reduction to be irreducible.

Definition 7.7.1. We say that $\mathfrak{q}$ is of extra good reduction if $f \mod \mathfrak{q}$ is squarefree and $p \mod \mathfrak{q}$ is irreducible. We denote $\overline{\mathcal{O}_K[\mathfrak{p}^{-1}]} = \mathcal{O}_K[\mathfrak{p}^{-1}] \mod \mathfrak{q}$ for the fake real quadratic order corresponding to $f \mod \mathfrak{q}, p \mod \mathfrak{q}$.

Lemma 7.7.2. *Let l be the splitting field of $\mathfrak{q}$, let $n = \deg(\mathfrak{q})$. Then if $Gal(L|k)$ as a subgroup of S_n contains n-cycles, the proportion of $\mathfrak{q}$ such that $p \mod \mathfrak{q}$ is irreducible is $\frac{\#\{n-cycles\ in\ Gal(L|k)\}}{\#Gal(L|k)}$, hence in this case, there are infinitely many. Otherwise, there are no primes of extra good reduction.*

Proof. There are only finitely many $\mathfrak{q}$ for which $f \mod \mathfrak{q}$ is not squarefree. This is because these $\mathfrak{q}$ are precisely the factors of $\mathrm{disc}(f) \cdot \mathcal{O}_k$, of which there are only finitely many. The rest of the proof is analogous to the proof of Lemma 7.6.2. □

Lemma 7.7.3. *Let $\epsilon_k = a + b\sqrt{f}$ be a fundamental unit of $\mathcal{O}_K[\mathfrak{p}^{-1}]$. Then $\overline{\epsilon_k} = \overline{a} + \overline{b}\sqrt{\overline{f}}$ is a fundamental unit of $\mathcal{O}_K[\mathfrak{p}^{-1}] \mod \mathfrak{q}$.*

Proof. The proof is analogous to the proof of Lemma 7.6.5. □

Theorem 7.7.4. *Let $f, p \in \mathcal{O}_k[x]$ be such that f is monic squarefree and p is monic irreducible splitting. Assume that there exists a prime ideal $\mathfrak{q}$ of extra good reduction. The following are equivalent.*

1. *The f.f. fake Ankeny-Artin-Chowla property holds for $\mathcal{O}_K[\mathfrak{p}^{-1}]$ (over $k(x)$)*
2. *For all but finitely many $\mathfrak{q}$ of extra good reduction, the f.f. fake Ankeny-Artin-Chowla property holds for $\mathcal{O}_K[\mathfrak{p}^{-1}]$ mod $\mathfrak{q}$.*
3. *For some $\mathfrak{q}$ of extra good reduction, the f.f. fake Ankeny-Artin-Chowla property holds for $\mathcal{O}_K[\mathfrak{p}^{-1}]$ mod $\mathfrak{q}$.*

Proof. (1) $\implies$ (2): Let $\epsilon_k = a + b\sqrt{f}$. Now apply division by remainder to get $b = cf + d$ for some $c, d \in \mathcal{O}_k[x]$. Then there are only finitely many prime ideals $\mathfrak{q}$ dividing d. Therefore there are also finitely many $\mathfrak{q}$ of extra good reduction such that this holds.

(2) $\implies$ (3): This follows from the fact that there are infinitely many prime ideals of extra good reduction by Lemma 7.7.2.

(3) $\implies$ (1): We have that $\overline{f} \nmid \overline{b}$ implies $f \nmid b$ and then we apply Lemma 7.7.3 □

And again we can make a reformulation.

Corollary 7.7.5. *Let $f, p \in \mathcal{O}_k[x]$ be such that f is monic squarefree and p is monic irreducible splitting. Assume that there exists a prime ideal $\mathfrak{q}$ of extra good reduction. The following are equivalent.*

1. *The f.f. fake Ankeny-Artin-Chowla property doesn't hold for (f, p) (over $k(x)$)*
2. *For infinitely many $\mathfrak{q}$ of extra good reduction, the f.f. fake Ankeny-Artin-Chowla property doesn't hold for $(\overline{f}, \overline{p})$ (over $\mathbb{F}_q(x)$ with $\mathbb{F}_q \cong \mathcal{O}_k/\mathfrak{q}$)*
3. *For all $\mathfrak{q}$ of extra good reduction, the f.f. fake Ankeny-Artin-Chowla property doesn't hold for $(\overline{f}, \overline{p})$ (over $\mathbb{F}_q(x)$ with $\mathbb{F}_q \cong \mathcal{O}_K/\mathfrak{q}$)*

Example 7.7.6. *Here's a (non-trivial) principal example for $k = \mathbb{Q}(i)$ where the f.f. fake Ankeny-Artin-Chowla property doesn't hold; let $f = x^3 - x - 1$, $p = f^3 - (-2ix^4 + (2 + 2i)x^2 + (-8 - 8i)x + (-1 + i))^2$. We obtained this example by lifting from $\mathbb{F}_9$, where one can lift a generator of $\mathbb{F}_9$ to $-1 + i$.*

7.8 An application to the number field setting

Let $\mathcal{O}_K[\mathfrak{p}^{-1}]$ be a fake real quadratic order over $\mathbb{Q}(x)$ corresponding to $f, p \in \mathbb{Z}[x]$ such that f is monic squarefree and p is monic, irreducible and splitting in $\mathcal{O}_K$. Let $a + b\sqrt{f}$ be the fundamental unit, so that $a^2 - fb^2 = \pm p^{o(\mathfrak{p})}$. Now we apply the following trick: plug in $x_0 \in \mathbb{Z}$ such that $|p(x_0)|$ is prime and that $f(x_0)$ is negative and squarefree. Then since $a(x_0)^2 - f(x_0)b(x_0)^2 = p(x_0)^{o(\mathfrak{p})}$, this induces the unit $a(x_0) + b(x_0)\sqrt{f(x_0)}$ in the fake real quadratic order in the number field setting, with discriminant $D = f(x_0)$ and above the prime $|p(x_0)|$. We notice that if $o(\mathfrak{p}) = 1$, then this necessarily gives the fundamental unit. Therefore in this case, a (fake real principal) counterexample to the f.f. fake Ankeny-Artin-Chowla property over $\mathbb{Q}(x)$ induces a (fake real principal) counterexample over $\mathbb{Q}$. Considering the Subsection 7.6, we hence see that we can move a (fake real principal) counterexample over $\mathbb{F}_\ell(x)$ to a (fake real

principal) counterexample over $\mathbb{Q}$.

This method works, but not for the $p(x_0)$ that have been confirmed to have no counterexamples for $-D < p(x_0)$. This is because D is negative, thus the equation $a(x_0)^2 - Db(x_0)^2 = p(x_0)^{o(\mathfrak{p})}$ implies $-D < p(x_0)^{o(\mathfrak{p})}$.

Example 7.8.1. *An example of this manoeuvre is given as follows: Take the genus* 0 *counterexample* $f = x$, $p = x^3 - 4$, *plug in* $x_0 = -3$. *Then we get* $D = f(-3) = -3$ *and prime* $|p(x_0)| = |-31| = 31$. *This is one of the counterexamples found by Micheal Oh in [19, Appendix D].*

We obtain another example when plugging in $x_0 = -19$, *we then get* $D = f(-19) = -19$ *and* $|p(x_0)| = |-6863| = 6863$. *This example is not in [19, Appendix D].*

We note that similar strategies have already been applied, as mentioned in [11].

7.9 Characteristic 2

Up to now, we have been assuming that $\ell := \mathrm{char}(k) \neq 2$. In this subsection, let us study the case that $\ell = 2$.

Let $K|k(x)$ be a quadratic extension, then any primitive element $\alpha(x)$ has minimal polynomial $y^2 + h(x)y + f(x)$ for some $h, f \in k[x]$. My first claim is that as long as the corresponding curve is smooth, we have that $\mathcal{O}_K$, which we again define to be the integral closure of $k[x]$ in K, is given as $k[x, \alpha(x)]$. Additionally, $\deg(f)$ is either $2g+1$ or $2g+2$ and $\deg(h) \leq g+1$. Lastly we notice that for $\deg(f) = 2g+1$, i.e. odd, we have $\mathcal{O}_K^\times = k^\times$, since there is one point at infinity. So when we consider the fake real quadratic order $\mathcal{O}_K[\mathfrak{p}^{-1}]$ for a $\mathfrak{p}$ such that $o(\mathfrak{p}) < \infty$, we again have $\mathcal{O}_K[\mathfrak{p}^{-1}]^\times = k^\times \times \epsilon^{\mathbb{Z}}$, where ϵ generates $\mathfrak{p}^{o(\mathfrak{p})}$. Since ϵ is not of the form $a + b\sqrt{f}$ anymore, but rather $a + b\alpha$, it may not make sense anymore to ask whether f divides b.

In order to fairly compare, we have to explain why in the $\ell \neq 2$ case, the condition $f \nmid b$ is inherent to the $k[t]$-algebra $\mathcal{O}_K$ rather than to the specific generator $\sqrt{f}$. One way we can do that, is to argue that f, b are invariants of the $k[t]$-algebra $\mathcal{O}_K$ up to unit multiplication. Let $1, c + d\sqrt{f}$ be generators of $\mathcal{O}_K$ viewed as a $k[x]$-algebra. Then $\mathcal{O}_K$ is also generated by $1, d\sqrt{f}$, which shows that $d \in k^\times$. In this sense, we can write

$$\epsilon = a + b\sqrt{f} = (a - bd^{-1}c) + bd^{-1}(c + d\sqrt{f}) = \tilde{a} + \tilde{b}(c + d\sqrt{f})$$

In this sense, we notice $\tilde{b}$ is only a unit multiple away from b. Additionally, the discriminant of the minimal polynomial of $c + d\sqrt{f}$ is a unit multiple away from f. This can be seen by completing the square.

Now go back to the characteristic 2 situation, where $\epsilon = a + b\alpha$. I wish to argue that $h \nmid b$ is the natural question to ask. Note that h^2 is the discriminant of the polynomial $y^2 + h(x)y + f(x)$. Again observe that if $\mathcal{O}_K$ is generated by $1, c + d\alpha$, then it is generated by $1, d\alpha$ and therefore $d \in k^\times$. One can check that $x^2 + (dh)x + (c^2 + cdh + d^2x) \in k[x]$ is the minimal polynomial of $c + d\sqrt{f}$, and therefore its discriminant is d^2h^2, which is a unit away from h^2. From

this point of view, it is logical to argue that $h^2 \not| b$ is the right criterion to consider. However, it would make sense to consider whether $h_i \nmid b$ instead for all irreducible factors $h_i | h$, since in the original Ankeny-Artin-Chowla conjecture we look modulo something irreducible/prime. Let us assume h is squarefree for simplicity, then we can also look modulo h. This approach is also similar to the approach given in [28] for the real quadratic case.

We again have the exact sequence

$$1 \to k^\times \to (\mathcal{O}_K/h)^\times \to \mathrm{Cl}_h^0(K) \to \mathrm{Cl}^0(K) \to 1,$$

and we can identify through this sequence the elements of $\mathrm{Cl}_h^0(K)$ corresponding to counterexamples. Notice that $\mathcal{O}_K/h \cong k[x,\sqrt{f}]/h$, where $\alpha \mod h$ is sent to $\sqrt{f} \mod h$. Given specific f, h, one computes $(k[x,\sqrt{f}]/h)^\times$ and which elements are in the subgroup induced by $(k[x]/h)^\times$. Since h is squarefree, $(k[x]/h)^\times \cong \prod_i (k[x]/h_i)^\times$ is hence of odd size. Now notice that all squares of $(k[x,\sqrt{f}]/h)^\times$ are induced by $(k[x]/h)^\times$, for if we take $c + d\sqrt{f} \mod h$ and square it, we obtain $c^2 + fd^2$. This shows that this subgroup is of index 2 and so, we deduce that $(k[x,\sqrt{f}]/h)^\times \cong (k[x]/h)^\times \times \mathbb{Z}/2\mathbb{Z}$. (Because $(k[x]/h)^\times$ is coprime to 2) In a similar way as in Theorem 7.4.5, we discover that if the 2-rank of $\mathrm{Cl}_h^0(K)$ is $r\deg(h)$, then the proportion of counterexamples is $\frac{1}{\#G}$, where G is the 2-part of $\mathrm{Cl}_h^0(K)$.

Here is an example. Take $k = \mathbb{F}_2$, $f = x^3 + x^2 + 1$, $h = x$. Then it turns out that $Cl_h^0(K) \cong \mathbb{Z}/4\mathbb{Z}$. Hence its 2-part is also $\mathbb{Z}/4\mathbb{Z}$. So we expect that the proportion approaches $\frac{1}{4}$ and it does, considering for $\deg(p) \leq 18$ we have a proportion of around 0.249 or 24,9%, which I checked numerically.

The fundamental unit also has a norm equation corresponding to it, namely

$$a^2 + abh + b^2 f \in k^\times p^{o(\mathfrak{p})}.$$

It would be nice if using this norm equation we would be able to find a condition under which $h \nmid b$ is true, but it is not as obvious as the $\ell \neq 2$ case. In conclusion, the $\ell = 2$ case is similar, but can make things more complicated.

8 Conclusion and open questions

In this thesis, we have been looking at a few analogues of the Ankeny-Artin-Chowla conjecture, out of which the f.f. fake analogue is the one that is introduced in this Thesis. We have seen Mordell's conjecture and the n.f. fake and f.f. fake variants do not hold in general. On the other hand, the f.f. real variant does hold.

We zoomed in on the f.f. fake variant to study the behaviour of the f.f. fake Ankeny-Artin-Chowla property when varying various parameters. We have also seen that there is some interplay between different types of fake real quadratic orders. First off, one can extend the constant field in an appropriate way and whether the f.f. fake Ankeny-Artin-Chowla property holds is not affected. Next to this, a f.f. fake real quadratic order with $k = \mathbb{Q}$ induces f.f. fake real quadratic orders with $k = \mathbb{F}_q$ and also induces n.f. fake real quadratic orders. If the Ankeny-Artin-Chowla property is not satisfied in the f.f. fake scenario with $k = \mathbb{Q}$, then it is also not satisfied in the f.f. fake scenario with $k = \mathbb{F}_q$, and also in the n.f. fake scenario if the prime ideal is principal.

Here are some open questions regarding the f.f. fake Ankeny-Artin-Chowla property:

1. We know that for each genus, there are counterexamples to the f.f. fake Ankeny-Artin-Chowla property with $k = \mathbb{Q}$ where the prime ideal is principal. Are there also counterexamples where the prime ideal is not principal? If so, how does one find them (efficiently) if possible?

   Notice that a counterexample over $k = \mathbb{Q}$ also induces a counterexample over any field k of characteristic 0 that doesn't contain the roots of p. Therefore, answering this open question for $\mathbb{Q}$ automatically answers it for any such k.

2. Given $p \in k[x]$ irreducible, can we determine if there exists f squarefree coprime to p such that the Ankeny-Artin-Chowla conjecture doesn't hold for (f, p)? We already saw in Corollary 7.3.9 that for finite k, we can check this in finite time.

   However now the question arises: how does the answer relate to $\deg(p)$? We know for $\deg(p) \leq 2$ that the f.f. fake Ankeny-Artin-Chowla property always holds by Corollary 7.3.6.

3. Given any field k (perfect of char. $\ell \neq 2$) can we decide if there are counterexamples? If $[\overline{k} : k] \leq 2$, then the f.f. fake Ankeny-Artin-Chowla property always holds by Corollary 7.3.7.

4. Suppose K is real (i.e. f is of even degree) and $\infty_+ - \infty_-$ is not a k-rational divisor of finite order in $\mathrm{Cl}_k(C)$. Then $\mathcal{O}_K^\times$ is finite by Proposition 6.0.1 and so we can consider $\mathcal{O}_K[\mathfrak{p}^{-1}]$ for a prime ideal of finite order, there is again a fundamental unit $\epsilon = a + b\sqrt{f}$. One could study whether $f \nmid b$ always holds in this setting and whether the results for the f.f. fake case can be carried over.

5. For $\ell = 2$, does there exist a positive result; affirming the f.f. fake Ankeny-Artin-Chowla property under some

conditions? Perhaps one could manipulate the norm equation $a^2 + abh + b^2 f \in k^\times p^{o(\mathfrak{p})}$ again using the Mason-Stothers theorem.

9 Magma implementations

The following Magma codes are also found in a Github respository.

The following Magma code computes the fundamental unit for fake real quadratics over $k(t)$ for $\mathrm{char}(k) \neq 2$, checks the f.f. fake Ankeny-Artin-Chowla property and provides additional information.

```
    function AAC_check(F,f,p)
// (Given the exact constant field F) This checks if the pair (f,p) satisfies the f.f. fake AAC property and outputs that as a boolean value.
// Moreover, outputs a,b s.t. the Fundamental Unit is given as a+b*sqrt(f). Also the order of the prime ideal in the ideal class group is computed.
        if not(IsIrreducible(p)) then
                error("p must be irreducible");
        end if;
        R<t>:=PolynomialRing(F);
        C:=HyperellipticCurve(f);
        J:=Jacobian(C);
        K<x,y>:=FunctionField(C);
        O:=CoordinateRing(C);
        S:=Zeros(C,Evaluate(p,x));
        D:=S[1];
        P:=Points(C)[1];
        Pplace:=Place(P);
        D1:=-D+Degree(D)*Pplace;
        pt:=JacobianPoint(J,D1);
        m:=Order(pt);
        AFF<Y>,toAlgFF := AlgorithmicFunctionField(K);
        V,phi := RiemannRochSpace(FunctionFieldDivisor(m*E1));
        bas := Basis(V);
        gamma := phi(bas[1]);
        toCrvFF := Inverse(toAlgFF);
        yAlgFF := toAlgFF(y);
        b := Eltseq(gamma)[2];
        quotient, remainder := Quotrem(R!b,R!f);
        AAC_true := not (remainder eq 0);
        return AAC_true, Eltseq(gamma)[1], Eltseq(gamma)[2],m;
```

```
end function;
```

The following function computes the groups in the ray exact sequence.

```
function ClassFieldGroups(C)
    // Given a hyperelliptic curve C: y^2=f(x) over a finite field, this outputs
       (O_K/<f>)^x, Cl_f(K), Cl(K), with K=k(C).
    f:=HyperellipticPolynomials(C);
    S:=Zeros(C,f);
    tuples:=[];
    for i in [1..#S] do
            tuples:=Append(tuples,<S[i],2>);
    end for;
    E:=Divisor(tuples);
    E:=FunctionFieldDivisor(E);
    J:=Jacobian(C);
    A:=RayResidueRing(E);
    B:=TorsionSubgroup(RayClassGroup(E));
    F:=AbelianGroup(J);
    return A,B,F;
end function;
```

References

[1] Nesmith Cornett Ankeny, Emil Artin, and Sarvadaman Chowla. The class-number of real quadratic number fields. *Annals of Mathematics*, pages 479–493, 1952.

[2] Nesmith Cornett Ankeny and Sarvadaman Chowla. A further note on the class number of real quadratic fields. *Acta Arithmetica*, 3(7):271–272, 1961/1962.

[3] Michael Francis Atiyah and Ian Grant MacDonald. *Introduction to commutative algebra.* Addison-Wesley-Longman, 1969.

[4] Julio Rafael Bastida. *Field Extensions and Galois Theory.* Cambridge University Press, 1984.

[5] David Geoffrey Cantor. Computing in the Jacobian of a Hyperelliptic Curve. *Mathematics of Computation*, 48(177), January 1987.

[6] Henri Cohen. Fake real quadratic orders. Unpublished manuscript, 2013.

[7] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, 1977.

[8] Florian Hess. Computing Riemann–Roch spaces in algebraic function fields and related topics. *Journal of Symbolic Computation*, pages 425–445, 2002.

[9] Florian Hess. Personal communication, 23-09-2024.

[10] Florian Hess and Maike Massierer. Tame class field theory for global function fields. *Journal of Number Theory*, 162, 2013.

[11] Florian Hess, Renate Scheidler, and Michael John Jacobson. Unpublished manuscript. 2024.

[12] Marc Hindry and Joseph Hillel Silverman. *Diophantine Geometry: An Introduction.* Graduate Texts in Mathematics. Springer New York, 2013.

[13] A. A. Kiselev. An expression for the number of classes of ideals of real quadratic fields by means of Bernoulli numbers. In *Doklady Akad. Nauk SSSR (NS)*, volume 61, pages 777–779, 1948.

[14] Michiel Kosters. A short proof of a Chebotarev density theorem for function fields. *Mathematical Communications*, 22, 2014.

[15] Richard Clive Mason. *Diophantine Equations over Function Fields.* Cambridge University Press, Cambridge, UK, 2008.

[16] David William Masser. Open problems. In W. W. L. Chen, editor, *Proceedings of the Symposium on Analytic Number Theory*, London, 1985. Imperial College.

[17] Louis Joel Mordell. On a Pellian equation conjecture (ii). *Journal of the London Mathematical Society*, s1-36(1):282–288, 1961.

[18] Jürgen Neukirch. *Algebraic Number Theory*. Springer Verlag, 1999.

[19] Richard Michael Oh. Fake real quadratic orders. Master's thesis, University of South Carolina - Columbia, 2014.

[20] Richard Pinch. P-rank, 2020. Available at http://encyclopediaofmath.org/index.php?title=P-rank&oldid=51117.

[21] Andreas Reinhart. On orders in quadratic number fields with unusual sets of distances, 2023.

[22] Andreas Reinhart. A counterexample to the Pellian equation conjecture of Mordell. *Acta Arithmetica*, 215:85–95, 2024.

[23] David Speyer. Factoring polynomials and the Frobenius, 2007. Available at https://sbseminar.wordpress.com/2007/08/24/factoring-polynomials-and-the-frobenius/.

[24] Peter Stevenhagen. Number rings (lecture notes), 2020. Available at https://websites.math.leidenuniv.nl/algebra/ant.pdf.

[25] Michael Stoll. Arithmetic of hyperelliptic curves. Lecture notes. University of Bayreuth, 2014. Available at https://www.mathe2.uni-bayreuth.de/stoll/teaching/ArithHypKurven-SS2014/Skript-ArithHypCurves-pub-screen.pdf.

[26] Alfred Jacobus van der Poorten, Hermanus Johannes Joseph Te Riele, and Hugh Cowie Williams. Computer Verification of the Ankeny-Artin-Chowla Conjecture for all primes less than 100 000 000 000. *Mathematics of Computation*, 70(235):1311–1328, 2001.

[27] Hongyan Wang. Numerical tests of two conjectures in fake real quadratic orders. Master's thesis, University of Calgary, 2017.

[28] Jing Yu and Jiu-Kang Yu. A note on a geometric analogue of Ankeny-Artin-Chowla's conjecture. *Contemporary Mathematics*, 1998.