Governing fields for hyperelliptic function fields

Joppe Stokvis *

July 8, 2025

Abstract

We study the 8-rank of class groups of hyperelliptic function fields and show that such 8-ranks are governed by splitting conditions in so-called governing fields. A similar result was proven for quadratic number fields by Stevenhagen, who used a theory of Rédei symbols and Rédei reciprocity to do so. We introduce a version of the Rédei reciprocity law for function fields and use this to show existence of governing fields.

1 Introduction

Since Gauss introduced his genus theory [Gau01], the 2-part of (narrow) class groups of quadratic number fields has been extensively studied. By the Cohen-Lenstra heuristics [CLJ84] we expect only this 2-part to have a predictable structure. To understand the structure of the 2-part, Cohn and Lagarias introduced governing fields and proved their existence for the 2- and 4-rank [CL83]. Stevenhagen gave a proof for the existence of governing fields for the 8-rank [Ste89] using class field theory. More recently, a new proof of their existence [Ste22] was given by using the Rédei symbol, which satisfies the Rédei reciprocity law. This trilinear symbol is named after the Hungarian mathematician who was the first to give a definition [Réd39]. On the existence of a governing field of the 16-rank for quadratic number fields there is only a negative answer by Koymans and Milovic [KM21], under the assumption of a short character sum conjecture.

Similarly to their number field equivalent, class groups of function fields over finite fields show the same structural behaviour in their 2-part, as was first discovered by Artin in his thesis [Art24]. Because of heuristics by Friedman and Washington [FW87] that resemble those of Cohen-Lenstra, this structural behaviour is expected to occur only in the 2-part. This motivates the introduction of governing fields for hyperelliptic function fields, which will be done in this article.

Let q be an odd prime power and consider the rational function field $\mathbb{F}_q(x)$ over the finite field with q elements. A hyperelliptic function field is a quadratic extension $K_D = \mathbb{F}_q(x, \sqrt{D})$ determined by a squarefree polynomial $D \in \mathbb{F}_q[x]$. Its ring of integers $\mathcal{O}_D$ is the algebraic closure of $\mathbb{F}_q[x]$ in K_D and we define $C(D)$ (also denoted by C) as the ideal class group of $\mathcal{O}_D$. Even though we will write $C(D)$ as a multiplicative group, we can make an identification to a vector space over $\mathbb{F}_2$. For $j \in \mathbb{Z}_{\geq 1}$ the 2^j-rank of $C(D)$ is defined as the dimension of the $\mathbb{F}_2$-vector space $C^{2^{j-1}}/C^{2^j}$.

$$r_{2^j} := \dim_{\mathbb{F}_2}\left(C^{2^{j-1}}/C^{2^j}\right) = \dim_{\mathbb{F}_2}\left(C[2^j]/C[2^{j-1}]\right). \tag{1.1}$$

Definition 1.1 (Governing fields)**.** Let q be an odd prime power and $D \in \mathbb{F}_q[x]$ squarefree. A Galois extension $\Omega_{2^j}(D)/\mathbb{F}_q(x)$ is called a *governing field for the* 2^j*-rank of* $C(DP)$ if the Frobenius conjugacy class of an unramified prime P in $\mathrm{Gal}(\Omega_{2^j}(D)/\mathbb{F}_q(x))$ completely determines the 2^k-rank for all $k \leq j$.

In order to obtain results about governing fields we will need explicit methods to determine the 2^j-rank of the class group for various j. Even though this text treats the calculations as a purely algebraic problem for function fields, we want to highlight that similar results can also be obtained through a geometrical interpretation. By relating the class group to the Jacobian of a hyperelliptic curve one obtains additional geometric structure to study the problem [Cor99, Cor01].

*Mathematical Institute, Leiden University and QuSoft, Amsterdam, j.a.stokvis@math.leidenuniv.nl

1.1 Main results

This article studies the 2^j-rank of hyperelliptic function fields for $j = 1, 2, 3$ and proves the following (see also theorem 6.4).

Theorem 1.2. *Let $D \in \mathbb{F}_q[x]$ be a squarefree polynomial. Then $\Omega_2(D)$ and $\Omega_4(D)$ exist. If not all irreducible factors of D have even degree, then $\Omega_8(D)$ exists as well.*

The main part of the proof of theorem 1.2 uses a symmetry law of the Rédei symbol $[A, B, C]$ that takes its arguments in $\mathbb{F}_q(x)^*/\mathbb{F}_q(x)^{*^2}$. Adapting the methods for number fields [Ste22], we define the Rédei symbol for function fields in definition 5.9. Its entries have to satisfy

$$\gcd(A, B, C) = 1, \text{ where not all have odd degree, and} \tag{1.2}$$

$$(A, B)_P = (A, C)_P = (B, C)_P = 1 \text{ for all primes } P, \tag{1.3}$$

where $(A, B)_P$ is the Hilbert symbol at a prime P [AT68, chapter XII]. The Rédei reciprocity law can then be stated as follows (see also theorem 5.13).

Theorem 1.3. *Let $A, B, C \in \mathbb{F}_q(x)^*/\mathbb{F}_q(x)^{*^2}$ satisfy equation (1.2) and equation (1.3). Then*

$$[A, B, C] = [B, A, C] = [A, B, C] \tag{1.4}$$

and the Rédei symbol is multiplicative in all its entries.

1.2 Outline

In section 2 we introduce some preliminary concepts and explain the general strategy on how to calculate the 2^j-rank of a class group. This is made explicit for $j = 1$ and $j = 2$ in section 3 using genus theory [Art24, Sém98, Zha87] and methods by Rédei [Réd34, Réd39, Wit07] respectively. The calculation of the 8-rank is explained in section 4. In section 5 we give a definition of Rédei symbols and prove the theorem of Rédei reciprocity. The definition is similar to the one for number fields [Ste22], but some additional care has to be taken when defining minimally ramified extensions. Rédei reciprocity will be the main tool in proving the existence of governing fields, which is done in section 6.

The theory of Rédei symbols, the reciprocity law and governing fields was originally developed for quadratic number fields. Part of the definitions and methods in this article are based on [Ste22] and adapted for function fields. The interested reader can compare the number field and function field results using the following conversion of sections:

This article	[Ste22]
section 3	sections 2, 3
section 4	sections 4, 5
section 5	sections 7, 8
section 6	section 9

Notation We always let q be an odd prime power and $k = \mathbb{F}_q(x)$ be the rational function field. Generally, $K_A = k(\sqrt{A})$ is used to denote the quadratic extension for any non-square $A \in \mathbb{F}_q[x]$. In section 5 we frequently use the extension $k(\sqrt{AB})$ with $A, B \in \mathbb{F}_q[x]$. We denote it by $K = k(\sqrt{AB})$ and use $E = K(\sqrt{A}) = K(\sqrt{B}) = k(\sqrt{A}, \sqrt{B})$ for the quartic extension. A cyclic quartic extension of K is usually denoted by F.

The 2^j-rank of a class group is defined by identifying $C^{2^j}/C^{2^{j-1}}$ as an $\mathbb{F}_2$-vector space. In this article we will always write the class group multiplicatively. Quadratic Galois groups will be represented by $\{\pm 1\}$, consistent with notation for quadratic symbols. Whenever the dimension of a vector space needs to be computed, it is assumed that an identification with $\mathbb{F}_2$ is made.

2 Preliminaries

Let q be an odd prime and denote by $k = \mathbb{F}_q(x)$ the rational function field. By a *hyperelliptic function field* we mean a quadratic extension $K_D = k(\sqrt{D})$ with $D \in \mathbb{F}_q[x]$ squarefree. The polynomial D has a decomposition into irreducible parts as $D = eP_1 \dots P_s$, where the $P_i \in \mathbb{F}_q[x]$ are distinct monic irreducible polynomials and $e \in \mathbb{F}_q^*$ is the sign of D. We may assume without loss of generality that $e = 1$ or g for some fixed generator g of $\mathbb{F}_q^*$. We denote the infinite prime of k by P_∞. The infinite primes of K_D are characterised as follows.

Lemma 2.1 ([Ros00, proposition 14.6])**.** *The infinite prime P_∞ of k*

- *splits in K_D when $\deg(D)$ is even and $e = 1$,*
- *is inert in K_D when $\deg(D)$ is even and $e = g$,*
- *ramifies in K_D when $\deg(D)$ is odd.*

We call K_D *imaginary* when P_∞ ramifies or is inert and *real* when P splits. The same distinction can also be made by the unit group, where imaginary fields have a finite unit group and real fields are of rank 1 over $\mathbb{Z}$.

Denote by $\mathcal{O}_D$ the integral closure of $\mathbb{F}_q[x]$ in K_D. The *class group* $C(D)$ (also denoted by C) is defined as the ideal class group $\mathcal{O}_D$. The 2-part of $C(D)$ is completely determined by a sequence of integers, the 2^j*-ranks* for $j \geq 1$ as defined by equation (1.1). The sequence $r_2, r_4, r_8, \dots$ is weakly decreasing and zero for large enough k. As can be seen in equation (1.1) there are two different ways of interpreting the 2^j-rank.

Firstly, we can consider the quotient $C[2^j]/C[2^{j-1}]$, which describes the ideal classes of exact order 2^j. Assuming we have a set of ideal classes generating $C[2^j]/C[2^{j-1}]$, the next rank can be calculated by checking which of these generators is the square of another ideal class. Indeed, if the class $A \in C[2^{j+1}]$ has exact order 2^{j+1} then A^2 has order 2^j. In general it is hard to check which classes are squares, which is why we will also use the other expression.

For the second expression for the 2^j-rank we use the dual group $\widehat{C} = \mathrm{Hom}(C, \mathbb{C})$. Let H/K_D be the Hilbert class field of K_D, i.e . the maximal unramified abelian extension of K_D where the infinite primes split completely [Ros87]. By the Artin map there is an isomorphism $C(D) \cong \mathrm{Gal}(H/K_D)$. For any $j \geq 0$, the subgroup $C(D)^{2^j} \leq C(D)$ corresponds to an intermediate field $H_{2^j} \subset H$ such that $C(D)^{2^j} \cong \mathrm{Gal}(H/H_{2^j})$. It holds that

$$\mathrm{Gal}(H_{2^j}/K) \cong C/C^{2^j} \text{ and } \mathrm{Gal}(H_{2^j}/H_{2^{j-1}}) \cong C^{2^j}/C^{2^{j-1}} \cong \mathbb{F}_2^{r_{2^j}}.$$

A character $\chi \in \widehat{C}[2^j]$ has a field of definition L_χ with a degree over k that divides 2^j. The kernel of χ contains C^{2^j} and L_χ will be a subfield of H_{2^j}. In particular $C^{2^j} = \cap_{\chi \in \widehat{C}[2^j]} \ker(\chi)$ and H_{2^j} is the compositum of the fields of definition of the characters $\chi \in \widehat{C}[2^j]$. The extension $H_{2^{j-1}} \subset H_{2^j}$ is Galois with a Galois group of exponent 2 and is therefore generated by r_{2^j} characters in $\widehat{C}[2^j]$ that have exact order 2^j. Similar to the first interpretation, the 2^{j+1} rank can be calculated by checking which characters in $\widehat{C}[2^j]$ are squares of ones in $\widehat{C}[2^{j+1}]$.

To find out which characters (or ideal classes) are squares of ones with higher torsion, we will need explicit expressions for the intermediate fields H_{2^j}. Writing $H_{2^j} = \prod_{i=1}^{r_{2^j}} H_{2^{j-1}}(\sqrt{A_i})$, we will explain in the next sections how to find these quadratic extensions $H_{2^{j-1}}(\sqrt{A_i})$ for $j = 1, 2, 3$.

3 Genus theory and Rédei theory

In this section we explain how to calculate the 2- and 4-rank of a hyperelliptic function field. While the results of this section are not new, we spend some time on the proof of theorem 3.1 to explicitly construct bases of $C[2]$ and $\widehat{C}[2]$ which are needed for the 8-rank and results on governing fields in sections 4 and 6.

3.1 The 2-rank

The Hilbert class field H of K_D is Galois over k with Galois group

$$\mathrm{Gal}(H/k) \cong \mathrm{Gal}(H/K_D) \rtimes \mathrm{Gal}(K_D/k) = C(D) \rtimes \langle\sigma\rangle$$

where σ acts by inversion [Pen03]. For the 2-rank we focus on the subfield H_2, which is called the *genus field* of K_D. It is the maximal subextension of H that is abelian over k and it holds that

$$\mathrm{Gal}(H_2/\mathbb{F}_q(x)) = \mathrm{Gal}(H/\mathbb{F}_q(x))^{\mathrm{ab}} = C/C^2 \rtimes \langle\sigma\rangle.$$

As the 2-rank equals the dimension of $\mathrm{Gal}(H_2/H_1) = \mathrm{Gal}(H_2/K_D)$ as an $\mathbb{F}_2$-vector space, we obtain the 2-rank by treating $\mathrm{Gal}(H_2/K_D) \subset \mathrm{Gal}(H_2/\mathbb{F}_q(x))$ as a subspace of codimension one.

The quadratic characters generating H_2 are called *genus characters*. They were first studied in the context of binary quadratic forms by Gauss (for number fields) [Gau01] and Artin (for function fields) [Art24]. A classification of the 2-rank for imaginary function fields was obtained by Artin and extended to the real case by Zhang and Sémirat. The author was unable to access [Zha87]. A proof of its results, based on the strategy explained in [Hu98, section 1] is included in the author's master's thesis [Sto24, chapter 2].

Theorem 3.1 ([Art24], [Zha87], [Sém98])**.** *Let $D = eQ_1 \dots Q_{s_1} P_1 \dots P_{s_2} \in \mathbb{F}_q[x]$ be a squarefree polynomial with the Q_i irreducible of odd degree and the P_j irreducible of even degree. Writing $s = s_1 + s_2$, the 2-rank of the class group $C(D)$ of the hyperelliptic function field K_D is given by*

- $r_2 = s - 2$ *if* $e = 1, \deg(D)$ *is even and* $s_1 > 0$,
- $r_2 = s - 1$ *if* $[\deg(D)$ *is odd*$]$ *or* $[e = 1$ *and* $s_1 = 0]$ *or* $[e = g, \deg(D)$ *is even and* $s_1 > 0]$,
- $r_2 = s$ *if* $e = g$ *and* $s_1 = 0$.

Proof (sketch). We give two methods of proving the theorem. One classifies the ideal classes in $C[2]$ while the other finds characters in $\widehat{C}[2]$.

The first way of computing the 2-rank is to find all ideal classes of $C[2]$, so-called *ambiguous ideal classes*. It can be shown that (almost) all ambiguous ideal classes can be generated by the ramified prime ideals $\mathfrak{p}_i \mid P_i$. Indeed $[\mathfrak{p}_i^2] = [(P_i)]$ is a trivial class in $C(D)$. The generators are subject to the relation $\prod_{i=1}^{s} \mathfrak{p}_i = (\sqrt{D})$, which would imply r_2 to be $s-1$. In the case that K_D is real, the 2-rank is brought down by one by the existence of a fundamental unit. It imposes an extra relation on the generators. When $s_1 = 0$, the rank is raised by one because of the existence of an extra generating ideal in $C(D)$. In this case, D can be written as $D = c(U^2 - gV^2)$ for some $c \in \mathbb{F}_q^*$ and $U, V \in \mathbb{F}_q[x]$ and the ideal $\mathfrak{A} = (V, U + \sqrt{D})$ (or swapping U and V when $c \notin \mathbb{F}_q^{*^2}$) of norm U (or V) generates an *irregular* ambiguous class in $C(D)$.

Another way of computing r_2 is to give an explicit description of the genus field of K_D as

$$H_2 = \begin{cases} \mathbb{F}_q(x)(\sqrt{e}, \sqrt{P_1}, \dots, \sqrt{P_s}) & \text{if } 2 \mid \deg(D) \text{ and } s_1 = 0, \\ \mathbb{F}_q(x)(\sqrt{e}, \sqrt{Q_1 Q_2}, \dots, \sqrt{Q_1 Q_{s_1}}, \sqrt{P_1}, \dots, \sqrt{P_{s_2}}) & \text{if } 2 \mid \deg(D) \text{ and } s_1 \neq 0, \\ \mathbb{F}_q(x)(\sqrt{eQ_1}, \dots, \sqrt{eQ_{s_1}}, \sqrt{P_1}, \dots, \sqrt{P_{s_2}}) & \text{if } 2 \nmid \deg(D). \end{cases} \tag{3.1}$$

□

The genus field mentioned in the proof is the compositum of fields of definition generated by quadratic characters

$$\chi_i : \mathrm{Gal}(H_2/k) \to \mathrm{Gal}(k(\sqrt{A_i})/k)$$

that give the Galois action on each $\sqrt{A_i}$ respectively. The A_i's correspond to the generators of the genus field in equation (3.1). When restricted to $C/C^2 = \mathrm{Gal}(H_2/K_D) \subset \mathrm{Gal}(H_2/k)$ we obtain a generating set of quadratic characters $\{\chi_1, \dots, \chi_{r_2}\} \subset \widehat{C}[2]$. The Artin map thus induces a map to $\mathrm{Gal}(H_2/K_D)$ given by

$$\begin{aligned} C(D) &\to \mathrm{Gal}(H_2/K_D) \\ [\mathfrak{p}] &\mapsto \mathrm{Art}(\mathfrak{p}, H_2/K_D) = (\chi_1(\mathfrak{p}), \dots, \chi_{r_2}(\mathfrak{p})) = \left(\left(\frac{A_i}{P}\right), \dots, \left(\frac{A_{r_2}}{P}\right)\right), \end{aligned} \tag{3.2}$$

where the latter are quadratic symbols, for example defined in [Ros00, chapter 3]. The two proofs give us a basis of ambiguous ideal classes spanning $C[2]$ and a basis of quadratic characters defining $\mathrm{Gal}(H_2/K_D)$. A quadratic character $\chi_i \in \widehat{C}[2]$ has field of definition $k(\sqrt{A_i}, \sqrt{D/A_i})$. All quadratic characters (genus characters) can be created as $\chi_{D_1} = \sum_{i \in S} \chi_i$ for any subset $S \subset \{1, \dots, r_2\}$ having field of definition $k(\sqrt{D_1}, \sqrt{D_2})$, where $D = D_1 D_2$ and $D_1 = \prod_{i \in S} A_i$. Note that $\chi_{D_1} = \chi_{D_2} \in \widehat{C}[2]$.

***Remark* 3.2.** As can be seen in equation (3.1), a splitting $D = D_1 D_2$ corresponds to a genus character χ_{D_1} only when D_2 is monic and of even degree. This is required to ensure the splitting behaviour of P_∞ is consistent in K_D and $k(\sqrt{D_1}, \sqrt{D_2})$. When D is monic, i.e. $e = 1$, the genus field may contain a trivial extension through the splitting $D = 1 \cdot D$. The corresponding character χ_e is trivial and can thus be ignored. △

3.2 The 4-rank

The following results have been introduced in [Wit07]. Consider the map

$$\varphi_4 : C[2] \to C/C^2 \tag{3.3}$$

incduced from the quotient map. An ideal class in $C[2]$ is also the square of an element in $C[4]$ if and only if it lies in $\ker(\varphi_4)$. From the two proofs of theorem 3.1 we have explicit generators for $C[2]$ and $\widehat{C}[2]$. Writing $D = eQ_1 \dots Q_{s_1} P_1 \dots P_{s_2}$ with $s = s_1 + s_2$, there exists an irregular ambiguous ideal $\mathfrak{A}$ in $C[2]$ when $s_1 = 0$. Thus the number of generators of $C[2]$ is given by

$$\delta := \begin{cases} s+1 & \text{if } \deg(D) \text{ is even and } s_1 = 0, \\ s & \text{otherwise,} \end{cases} \tag{3.4}$$

and we can define a surjection

$$\alpha : \mathbb{F}_2^\delta \twoheadrightarrow C[2], \quad e_i \mapsto \begin{cases} [\mathfrak{p}_i] & \text{if } 1 \le i \le s, \\ [\mathfrak{A}] & \text{if } i = s+1 \text{ (only when } \delta = s+1). \end{cases} \tag{3.5}$$

The first s generators are subject to one or two relations, depending on whether K_D is real or imaginary. The genus characters in $\widehat{C}[2]$ have a set of $r_2 + 1$ generators subject to one relation given by $\chi_1 = \prod_{i=1}^{r_2+1} \chi_i$. Using the inclusion map

$$\beta : C/C^2 \cong \mathrm{Gal}(H_2/K_D) \hookrightarrow \mathrm{Gal}(H_2/\mathbb{F}_q(x)) \cong \{\pm 1\}^{r_2+1} \tag{3.6}$$

we construct the so-called *Rédei map*

$$R_4 : \mathbb{F}_2^\delta \xrightarrow{\alpha} C[2] \xrightarrow{\varphi_4} C/C^2 \xrightarrow{\beta} \{\pm 1\}^{r_2+1}. \tag{3.7}$$

It follows that the 4-rank can be calculated as follows.

Theorem 3.3 ([Wit07, theorem 3.1])**.** *Let $D \in \mathbb{F}_q(x)$ be a squarefree polynomial and K_D the corresponding hyperelliptic function field. The 4-rank of the class group $C(D)$ of K_D is given by*

$$r_4 = \dim \ker(\varphi_4) = r_2 - \operatorname{rank} R_4.$$

Calculating the 4-rank means determining the rank of a $\delta \times (r_2 + 1)$-matrix R_4. The entries are quadratic symbols, which written multiplicatively are given by

$$(R_4)_{ij} = \chi_i(\mathfrak{p}_j) = \left(\frac{A_i}{P_j}\right) \text{ (whenever } P_i \text{ and } A_j \text{ are relatively prime)}, \tag{3.8}$$

where the $\mathfrak{p}_j$ are ramified primes generating $C[2]$ (and potentially one for the irregular ambiguous ideal class which is not given by equation (3.8)) and χ_i gives the Galois action on $\sqrt{A_i}$ in H_2.

4 The 8-rank

For the 8-rank of $C(D)$, we will use the same setup as for the 4-rank. Many results in this section also hold for number fields and can be found in [Ste22]. Consider the map

$$\varphi_8 : \ker(\varphi_4) = C[2] \cap C^2 \to C^2/C^4 \tag{4.1}$$

induced from the quotient map. As ideal classes of exact order 8 correspond to fourth powers in $C[2]$, the 8-rank equals the dimension of the kernel of φ_8. We can make a restriction to the Rédei map in equation (3.7) to obtain

$$R_8 : \ker(R_4) \to C^2 \cap C[2] \xrightarrow{\varphi_8} C^2/C^4 \cong \mathrm{Gal}(H_4/H_2) \cong \prod_{i=1}^{r_4} \mathrm{Gal}(H_2(\sqrt{\beta_i})/H_2) \cong \{\pm 1\}^{r_4}. \tag{4.2}$$

The first part of this map is induced from equation (3.5) and is surjective. The 8-rank can now be calculated as follows.

Theorem 4.1. *Let $D \in \mathbb{F}_q(x)$ be a squarefree polynomial and K_D the corresponding hyperelliptic function field. The* 8*-rank of the class group $C(D)$ of K_D is given by*

$$r_8 = \dim \ker(\varphi_8) = r_4 - \operatorname{rank} R_8.$$

There is no obvious choice of basis for $\ker(R_4)$ and $\mathrm{Gal}(H_4/H_2)$ as $\mathbb{F}_2$-vector spaces anymore, which makes the computation much harder. Let us try to make $\mathrm{Gal}(H_4/H_2)$ more explicit. The Hilbert subfield H_4/K_D is the compositum of the fields of definition for all characters $\psi \in \widehat{C}[4]$. The extension H_4/H_2 is generated by the characters in $\widehat{C}[4]/\widehat{C}[2]$. Such a quartic character ψ becomes a genus character when squared. Classification of squares in the group of genus characters goes as follows. A version and proof of this lemma exist also for number fields [Ste22, lemma 4.2].

Lemma 4.2. *Let K_D a hyperelliptic function field with ideal class group $C(D)$. For a non-trivial quadratic character $\chi \in \widehat{C}[2]$ with field of definition $E = k(\sqrt{D_1}, \sqrt{D_2})$, having $\chi = \psi^2 \in \widehat{C}^2$ for a quartic character ψ is equivalent to any of the following:*

1. *there exists a cyclic quartic extension $K_D \subset F$ inside H containing E,*
2. *all ambiguous ideals of K_D split completely in $K_D \subset E$,*
3. *for $i = 1, 2$ and all irreducible polynomials $P \mid D_i$ we have $\left(\frac{D/D_i}{P}\right) = 1$. When it exists, the extra irregular ambiguous ideal $\mathfrak{A}$ of norm $N(\mathfrak{A})$ satisfies $\left(\frac{D_1}{N(\alpha)}\right) = \left(\frac{D_2}{N(\alpha)}\right) = 1$.*

Proof. The character χ belonging to the splitting $D = D_1 D_2$ has E as its field of definition. Requiring $\psi = \chi^2$ for a quartic character ψ is indeed equivalent to the existence of a cyclic unramified extension $K \subset F$ of degree 4 that contains E as in (i). The extension F is contained in H_4.

The fact that $\chi = \psi^2$ is also equivalent to χ vanishing on $C[2]$. The group $C[2]$ is generated by the ramifying primes $\mathfrak{p}_i$ of K_D and the potential irregular ideal class. The fact that χ is trivial on $C[2]$ is equivalent to saying that under the Artin map all these primes are trivial. In other words, all the ramified primes (and irregular ideal) of K_D split in the extension $K \subset E$ as in item 2. Equivalently, it holds that $\left(\frac{D_i}{p}\right) = 1$ whenever $p \mid D$ and $p \nmid D_i$ as in item 3, because the ramified primes are the ones dividing D. In item 3 one has to include the condition on the irregular ideal as well. □

***Remark* 4.3.** Whenever there is no irregular ambiguous ideal, note that item 3 of lemma 4.2 is equivalent to D_1 and D_2 having a trivial Hilbert symbol for any prime P. Also note that the decompositions $D = D_1 D_2 = D_2 D_1$ are considered equal, as they generate the same quartic extension. △

Definition 4.4. A decomposition $D = D_1 D_2$ with the properties of lemma 4.2 is called a *decomposition of the second type.*

To represent R_8 as a matrix, we first choose a basis of $\ker(R_4)$ and write $[\mathfrak{m}_j] \in C^2 \cap C[2]$ for the corresponding ideals under the map α from equation (3.5). We obtain a basis of size $\dim\ker(R_4) = \dim\ker(\varphi_4) + (\delta - r_2) = r_4 + (\delta - r_2)$. These classes span $C^2 \cap C[2]$ and are subject to $(\delta - r_2)$ relations. We also choose a set $\{\psi_i\}_{i=1}^{r_4}$ of quartic characters in $\widehat{C}[4]$ that form a basis of $\widehat{C}[4]/\widehat{C}[2]$. Their fields of definition F_i are cyclic extensions of K_D of degree 4 and the quadratic extensions H_2F_i/H_2 span H_4. The intersection $F_i \cap H_2 = K_D(\sqrt{D_i})$ is a quadratic extension of K such that $D = D_i \cdot \frac{D}{D_i}$ is a decomposition of the second type with genus character $\chi_i = \psi_i^2$. The map R_8 sends a class $[\mathfrak{m}_j]$ to $R_8([\mathfrak{m}_j]) \in \mathbb{F}_2^{r_4}$, of which the i-th component is $\mathrm{Art}(\mathfrak{m}_j, H_2F_i/H_2)$. We can therefore represent R_8 by a matrix $(\eta_{ij})_{i,j} \in \mathrm{Mat}_{r_4 \times r_4 + (\delta - r_2)}(\{\pm 1\})$ with

$$\eta_{ij} = \mathrm{Art}(\mathfrak{m}_j, H_2F_i/K_D) \in \mathrm{Gal}(H_2F_i/H_2) \cong \{\pm 1\}. \tag{4.3}$$

Note that the $[\mathfrak{m}_j]$ are classes in $C[2] \cap C^2$ so that $\mathrm{Art}(\mathfrak{m}_j, H_2F_i/K_D)$ is the identity on H_2. Hence the symbol in equation (4.3) can indeed be taken in $\mathrm{Gal}(H_2F_i/H_2)$.

Each of the quartic characters ψ in our chosen basis has a field of definition F that is a quartic extension of K_D and a quadratic extension of $E = K_D(\sqrt{D_1}) = k(\sqrt{D_1}, \sqrt{D_2})$. The splitting $D = D_1D_2$ is a decomposition of the second type and E is the field of definition of the genus character $\chi_{D_1} = \psi^2$. Writing $F = E(\sqrt{\beta})$ with some $\beta \in E$, we can obtain an expression for β by the following lemma.

Lemma 4.5 ([Ste22, corollary 5.2])**.** *Let Q be a field of characteristic different from 2 and $a, b \in Q^*$ such that $a, b, ab \not\equiv 1 \pmod{{Q^*}^2}$. Then a quadratic extension $E = Q(\sqrt{a}, \sqrt{b}) \subset F$ is cyclic over $Q(\sqrt{ab})$ and dihedral of degree 8 over Q if and only if there exists a non-zero solution $(X, Y, Z) \in Q^3$ to the equation*

$$X^2 - aY^2 - bZ^2 = 0$$

such that for $\beta = X + Y\sqrt{a} \in Q(\sqrt{a})$ and $\alpha = 2(X + Z\sqrt{b}) \in Q(\sqrt{b})$ we have

$$F = E(\sqrt{\beta}) = E(\sqrt{\alpha}).$$

Any other quadratic extension of E that is dihedral over Q of degree 8 is of the form $F_t = E(\sqrt{t\beta})$ for some $t \in Q^*/\langle a, b, {Q^*}^2\rangle$, which we call a twist *of β.*

As can be seen in equation (4.3) the entry η_{ij} of R_8 depends on the choice of ideal $\mathfrak{m}_j$ and extension F_i. Because $[\mathfrak{m}_j] \in C[2]$ we can also take its conjugate (i.e. inverse) as representative, making η_{ij} only depend on $M_i = N_{K_D/\mathbb{F}_q(x)}(\mathfrak{m}_j) \in \mathbb{F}_q[x]$. By lemma 4.5 the quartic extension F_i only depends on the decomposition $D = D_1D_2$ of the second type. Writing $\eta_{ij} = \mathrm{Art}(\mathfrak{m}_j, H_2F_i/H_2) = [D_1, D_2, M_j]$, we obtain a first definition of the Rédei symbol for function fields.

Definition 4.6 (Rédei symbol, version 1)**.** Let $D = D_1D_2$ be a decomposition of the second type, F/K_D a quartic extension corresponding to item 1 in lemma 4.2, and $M \mid D$ a polynomial that is the norm of an ideal $\mathfrak{m} \in K_D$ such that $[\mathfrak{m}] \in C^2 \cap C[2]$. Then the *Rédei symbol* of D_1, D_2 and M is given by

$$[D_1, D_2, M] := \mathrm{Art}(\mathfrak{m}, H_2F/H_2) \in \{\pm 1\}. \tag{4.4}$$

***Example* 4.7.** Let us illustrate how to calculate the 2-, 4- and 8-rank in the case that $D = QP$ is the product of two primes where Q has odd degree and P has even degree. The function field $K = \mathbb{F}_q(x, \sqrt{QP})$ is imaginary and by theorem 3.1 the 2-rank equals 1. The quadratic characters generating $\widehat{C}[2]$ are χ_Q and χ_P. They are in fact equal as their product $\chi_Q\chi_P$ is the trivial character. The prime ideals generating $C[2]$ are $\mathfrak{q}$ and $\mathfrak{p}$ lying above Q and P respectively, also with the relation that $[\mathfrak{q}\mathfrak{p}]$ is the trivial class. By theorem 3.3 the 4-rank equals r_2 minus the rank of R_4. The Rédei matrix in this instance is a (2×2)-matrix of rank 0 or 1, where all the entries are equal to the same quadratic symbol $\chi_P(\mathfrak{q}) = \left(\frac{Q}{P}\right)$ as a result of quadratic reciprocity [Ros00, theorem 3.5]. Thus the 4-rank is 1 if and only if $\left(\frac{Q}{P}\right) = 1$. Note that the genus field is $H_2 = k(\sqrt{Q}, \sqrt{P})$.

Assuming that $\left(\frac{Q}{P}\right)$=1, we want to calculate the 8-rank. The only decomposition of the second type is the splitting $D_1 = Q, D_2 = P$, corresponding to the character χ_Q (which equals χ_P). A generator of $C^2 \cap C[2]$ is the ideal class $[\mathfrak{q}] = [\mathfrak{p}]$ and so the map R_8 from equation (4.2) is determined by the Rédei symbol $[Q, P, P] = \mathrm{Art}(\mathfrak{p}, H_2(\sqrt{\beta})/K_D)$. The extension $H_2(\beta)/H_2$ can be found by lemma 4.5: we know that the conic $X^2 = QY^2 + PZ^2$ has a rational solution by lemma 4.2 and we can set $\beta = X + \sqrt{Q}Y$.

The prime ideal $\mathfrak{p}$ in K_D splits in H_2/K_D as $\mathfrak{p} = \mathfrak{p}_1\mathfrak{p}_2$, where we set $\mathfrak{p}_1 = (\sqrt{P}, X - Y\sqrt{Q})$. As the extension $H_2(\beta)/K_D$ is abelian, we only have to look at the splitting behaviour of $\mathfrak{p}_1$ in $H_2(\beta)/H_2$ to compute the Artin symbol $\mathrm{Art}(\mathfrak{p}, H_2(\sqrt{\beta})/K_D)$. It follows that

$$r_8 = 1 \text{ if and only if } \beta \in H_2 \text{ is a square modulo } \mathfrak{p}_1.$$

Note that there is an isomorphism $\mathbb{F}_q[x, \sqrt{Q}, \sqrt{P}]/\mathfrak{p}_1 \cong \mathbb{F}_q[x]/(P)$ by the identification $\overline{\sqrt{Q}} \mapsto \bar{X}/\bar{Y}$. Thus β is a square modulo $\mathfrak{p}_1$ if and only if $2X$ is a square modulo P. Since P has even degree all elements in $\mathbb{F}_q^*$ are squares modulo P. Using the reciprocity law we also know that $\left(\frac{Y}{P}\right) = \left(\frac{P}{Y}\right) = \left(\frac{X^2}{Y}\right) = 1$, meaning $\bar{Y}$ is a square. Hence $\bar{\beta}$ is a square if and only if $\overline{\sqrt{Q}} = \bar{X}/\bar{Y}$ is a square in $\mathbb{F}_q[x]/(P)$. We conclude that

$$r_8 = 1 \text{ if and only if } P \text{ splits in } k(\sqrt{g}, \sqrt[4]{Q}).$$

△

5 Minimally ramified extensions and Rédei reciprocity

The matrix entries for the R_8-map in equation (4.2) are defined by constructing extensions of K_D that are completely unramified. This condition can actually be relaxed into a property we will call minimally ramified and allows for a more general definition of the Rédei symbol. This general symbol obeys a reciprocity law that can be used to show the existence of governing fields. The theory is based on the version for number fields [Ste22], which relies on methods by Rédei [Réd34] and Corsman [Cor07].

The Rédei symbol in definition 4.6 takes arguments D_1, D_2, M, where D_1 and D_2 are squarefree. When we assume there is no irregular ambiguous ideal class (which will be one of the assumptions to be able to construct governing fields in section 6), M will also be squarefree as it is the norm of a ramified prime in $C[2] \cap C^2$. The general Rédei symbol $[A, B, C]$ will therefore take its arguments in k^*/k^{*2}. Each class $\bar{A} \in k^*/k^{*2}$ contains a unique (up to multiplication by $\mathbb{F}_q^*$) squarefree element $A \in \mathbb{F}_q[x]$ which we will use to represent the class. For non-trivial squarefree polynomials $A, B \in k^*$, the extension

$$k(\sqrt{AB}) = K \subset E = k(\sqrt{A}, \sqrt{B})$$

is quadratic and unramified at all finite primes not dividing $\gcd(A, B)$, and E/k is ramified at the finite primes dividing AB and at infinity if A and/or B have odd degree. To be able to construct minimally ramified extensions, we also require A and B to have trivial quadratic Hilbert symbols $(A, B)_P = 1$ for all primes P (including the infinite prime) so that

$$X^2 - AY^2 - BZ^2 = 0 \tag{5.1}$$

has a non-trivial solution in k by the Hasse-Minkowski principle [Lam05, theorem 3.1]. For a definition of Hilbert symbols for global fields and a reciprocity law we refer to [AT68, chapter XII].

***Remark* 5.1.** Recall that the infinite prime ramifies in the quadratic extension $k(\sqrt{A})/k$ precisely when A has odd degree. This divisibility by infinity will be included in the greatest common divisor, denoted by $\gcd_\infty(\cdot, \cdot)$. For $A, B \in \mathbb{F}_q[x]$ we say that P_∞ divides $\gcd_\infty(A, B)$ if and only if A and B have odd degree. △

5.1 Minimally ramified extensions

The non-trivial solvability of equation (5.1) implies the existence of a cyclic quartic extension

$$k(\sqrt{AB}) = K \subset F = E(\sqrt{\beta}) = E(\sqrt{\alpha})$$

by lemma 4.5. In the special case that $A = B$ there is a similar result by the following lemma.

Lemma 5.2 ([Ste22, corollary 5.3]). *Let Q a field of characteristic different from 2. For $E = Q(\sqrt{a})$ with $a \not\equiv 1 \pmod{Q^{*^2}}$, a quadratic extension $E \subset F$ is cyclic over Q if and only if there exists a non-zero solution $(X,Y,Z) \in Q^3$ to*

$$X^2 - aY^2 - aZ^2 = 0$$

such that we have $F = E(\sqrt{\beta})$ for $\beta = X + Y\sqrt{a} \in Q(\sqrt{a})$ of norm $\beta\beta' \in aQ^2$. Any other such extension is of the form $F_t = E(\sqrt{t\beta})$ for some unique $t \in Q^*/\langle a, Q^{*2}\rangle$.

Suppose there exists a cyclic extension F/K coming from a solution to equation (5.1). The primes $\mathfrak{p}$ in K dividing both A and B are ramified in E/K and these $\mathfrak{p}$ will be totally ramified in F/K, because β and α have norms (up to squares in k^*) A and B respectively. This might include the infinite primes in K when A and B are both of odd degree. We cannot avoid ramification of these primes, but we will be able to find an F that allows almost no other ramification.

Definition 5.3. For non-trivial $A, B \in k^*/k^{*2}$ satisfying $(A,B)_P = 1$ for all primes P, we call the cyclic extension F/K resulting from a non-trivial solution to equation (5.1) *minimally ramified over* $E = k(\sqrt{A}, \sqrt{B})$ if it is either

1. unramified over all primes $P \nmid \gcd_\infty(A,B)$ when at least one of $\deg(A), \deg(B)$ is odd or $\gcd_\infty(A,B)$ has a finite prime of odd degree, or
2. ramified over at most one finite prime $P \nmid \gcd_\infty(A,B)$ when $\deg(A)$ and $\deg(B)$ are both even and $\gcd_\infty(A,B)$ contains only finite primes of even degree.

As we want to prove a reciprocity law on three entries, they have to pairwise satisfy the above condition. We obtain the following definition.

Definition 5.4. Let $A, B, C \in k^*/k^{*2}$ be non-trivial classes represented by squarefree polynomials $A, B, C \in \mathbb{F}_q[x]$ that satisfy

$$\gcd_\infty(A,B,C) = 1, \tag{5.2}$$
$$(A,B)_P = (A,C)_P = (B,C)_P = 1 \quad \text{for all primes } P. \tag{5.3}$$

We call a minimally ramified extension F as in definition 5.3 *minimally ramified over* $k(\sqrt{A}, \sqrt{B})$ *with respect to* C if one of the following holds:

1. $k(\sqrt{AB}) \subset F$ is unramified outside $\gcd_\infty(A,B)$, or
2. $\deg(A)$ and $\deg(B)$ are both even, $\gcd_\infty(A,B)$ contains only irreducible parts of even degree, and there is an extra ramified prime $Q \in \mathbb{F}_q[x]$ as in item 2 from definition 5.3 satisfies

$$Q \text{ has odd degree, and } \left(\frac{Q}{P}\right) = 1 \text{ for all finite primes } P \text{ dividing } ABC. \tag{5.4}$$

Lemma 5.5. *For non-trivial $A, B, C \in k^*/k^{*2}$ satisfying equation (5.2) and equation (5.3) there exists an extension $F_{A,B}$ that is minimally ramified over E with respect to C.*

Proof. Let (X,Y,Z) be a primitive solution in $\mathbb{F}_q[x]$ to equation (5.1) and F/K the resulting quartic extension. First consider a finite prime P that does not divide AB. Then P cannot divide both $\beta = X + Y\sqrt{A}$ and $\alpha = 2(X + Z\sqrt{B})$, as it would imply that P divides both $N(\beta) = BZ^2$ and $N(\alpha) = AY^2$ making it a common divisor of X, Y and Z contradicting our assumption. Thus without loss of generality β is a unit at a prime above P in $k(\beta)$, implying that the extension $K \subset F = k(\sqrt{AB}, \sqrt{A}, \sqrt{\beta})$ is unramified at a prime $\mathfrak{p}$ dividing P.

Next, consider a finite prime P dividing AB. Without loss of generality assume it divides A. As $P \nmid B$ the field $E = K(\sqrt{B}) = K_A(\sqrt{B})$ is a quadratic extension unramified at P of both K and K_A. Thus F/K is unramified in primes above P if and only if F/K_A is. Write $F = K_A(\sqrt{\beta}, \sqrt{\beta'})$ with $\beta\beta' = X^2 - AY^2 = BZ^2$. A prime $\mathfrak{p} \mid P$ is unramified in F/K_A if and only if β and β' have an even valuation at $\mathfrak{p}$. Since we assumed that $P \mid A$, there is a unique $\mathfrak{p} \mid P$ in K_A with ramification index 2. We obtain

$$2\,\mathrm{ord}_{\mathfrak{p}}(\beta) = \mathrm{ord}_{\mathfrak{p}}(\beta\beta') = 2\,\mathrm{ord}_P(BZ^2) = 2 \cdot 2\,\mathrm{ord}_P(Z) \equiv 0 \pmod 4,$$

which shows that P is unramified in F/K.

For the infinite prime P_∞ of k we will do a similar construction. Let $\mathfrak{p}_\infty$ be a prime in K_A dividing P_∞ with ramification index e. We obtain

$$2\,\mathrm{ord}_{\mathfrak{p}_\infty}(\beta) = \mathrm{ord}_{\mathfrak{p}}(\beta\beta') = e(\mathfrak{p}_\infty/P_\infty)\,\mathrm{ord}_{P_\infty}(BZ^2) = e(\mathrm{ord}_{P_\infty}(B) + 2\,\mathrm{ord}_{P_\infty}(Z)).$$

Assume first that P_∞ divides A but not B (without loss of generality). Then A is of odd degree and P_∞ ramifies in K_A/k. As B is of even degree $\mathrm{ord}_{P_\infty}(B) \equiv 0 \pmod 2$ and we find $\mathrm{ord}_{\mathfrak{p}_\infty}(\beta) \equiv 0 \pmod 2$. When both $\deg(A)$ and $\deg(B)$ are odd we allow ramification of the inifinite prime. In the case they are both even the previous valuation argument does not hold, as the ramification index of $\mathfrak{p}_\infty \mid P_\infty$ in K_A is 1. The result is that $\mathrm{ord}_{\mathfrak{p}_\infty}(\beta)$ is even if and only if $\deg(B)/2 \equiv \deg(Z) \pmod 2$. As this is not guaranteed by the primitive solution to equation (5.1), we need to apply a quadratic twist to $F_{A,B}$ whenever $\mathrm{ord}_{\mathfrak{p}_\infty}(\beta)$ is odd. Twisting with an odd degree irreducible polynomial $Q \in \mathbb{F}_q[x]$ causes the desired change in parity and hence non-ramification of $\mathfrak{p}_\infty$. However, it also causes potential ramification at primes $\mathfrak{q} \mid Q$ in $k(\sqrt{AB})$. If there is an odd degree irreducible in $\gcd_\infty(A,B)$ we can take that one. Otherwise we have to allow for some Q outside $\gcd_\infty(A,B)$ to be ramified. By the Chebotarev density theorem we can take it to satisfy equation (5.4). □

From the proof above it is not at all clear when the extra twist at Q is required in item 2 of definition 5.4. We have for example the following lemma, which shows that there may exist extension $F_{A,B}$ that are unramified outside $\gcd_\infty(A,B)$ even in the 'bad case'.

Lemma 5.6. *Let $A,B,C \in k^*/k^{*^2}$ satisfy the conditions of definition 5.4 such that A and B are both non-trivial, have even degree, and $G := \gcd_\infty(A,B)$ contains only irreducible parts of even degree. Then there exists an extension $F_{A,B}$ that is minimally ramified with respect to C and unramified outside* $\gcd_\infty(A,B)$ *if one of the following holds:*

- *A and B are coprime and $D = AB$ is a decomposition of the second type,*
- *$B \mid A$ and $D = A/B \cdot B$ is a decomposition of the second type,*
- *$A \mid B$ and $D = B/A \cdot A$ is a decomposition of the second type.*

Proof. In each of these cases, we can use item 1 of lemma 4.2 to find an extension $F_{A,B}$ that lies in the Hilbert class field of D and is therefore unramified over $k(\sqrt{D})$. Because $k(\sqrt{AB}) \subset k(\sqrt{D})$ is unramified outside $\gcd(A,B)$ we can take $F_{A,B}$ as the desired extension. □

***Remark* 5.7.** In the case that there is at least one odd degree irreducible polynomial dividing AB, the conditions of lemma 5.6 can be changed to

- A and B are coprime, or
- $B \mid A$, $\left(\frac{A/B}{P}\right) = 1$ for all $P \mid B$ and the class group of $k(\sqrt{A})$ has $r_2 > 0$, or
- $A \mid B$, $\left(\frac{B/A}{P}\right) = 1$ for all $P \mid A$ and the class group of $k(\sqrt{B})$ has $r_2 > 0$.

Note that in each case we don't have to concern ourselves with an irregular ambiguous ideal. Because we assumed that $(A,B)_P = 1$ for all $P \leq \infty$ the requirements above ensure that item 3 of lemma 4.2 is satisfied. △

***Example* 5.8.** Contrary to number fields [Ste22, Lemma 7.7], there does not always exists a cyclic quartic extension of $k(\sqrt{AB})$ that is unramified outside $\gcd(A,B)$. Consider for example monic polynomials $A = x^4 + 2x^3 + x + 1$ and $B = +x + 2$ over the finite field $\mathbb{F}_3$. There exists a solution to

$$X^2 = AY^2 + BZ^2$$

by taking $X = x^3 + x^2 + x, Y = 1, Z = x^2 + 2x + 1$. The extension $k(\sqrt{A}, \sqrt{\beta}, \sqrt{\beta'})/k(\sqrt{AB})$ is ramified at the infinite prime. Because $\gcd(A,B) = 1$ any twist of β (see lemma 4.5) will cause new ramification. The extra ramified prime that has to satisfy equation (5.4) is thus a necessity for function fields. More examples of this type can be generated using the Magma code in appendix A △

5.2 The Rédei symbol

Using the existence of minimally ramified extensions we can define the general version of the Rédei symbol.

Definition 5.9 (Rédei symbol, version 2)**.** Let $A, B, C \in k^*/k^{*2}$ be non-trivial classes represented by squarefree polynomials $A, B, C \in \mathbb{F}_q[x]$ that satisfy

$$\gcd_\infty(A, B, C) = 1, \tag{5.5}$$
$$(A, B)_P = (A, C)_P = (B, C)_P = 1 \quad \text{for all primes } P. \tag{5.6}$$

Let $F_{A,B}/K$ be minimally ramified over E with respect to C. Then the *Rédei symbol*

$$[A, B, C] \in \mathrm{Gal}(F_{A,B}/E) \cong \{\pm 1\}$$

is defined as

$$[A, B, C] = \begin{cases} \mathrm{Art}(\mathfrak{c}, F_{A,B}/K) & \text{if } 2 \mid \deg(C), \\ \mathrm{Art}(\infty\mathfrak{c}, F_{A,B}/K) & \text{if } 2 \nmid \deg(C), \end{cases} \tag{5.7}$$

where the ideal $\mathfrak{c}$ is an integral $\mathcal{O}_K$-ideal of norm C and ∞ is an infinite prime of K. If one of A, B, C is trivial in k^*/k^{*2} we define $[A, B, C] = 1$.

Note that this definition also captures the special case $A = B$, where the minimally ramified extension F is cyclic over k. We now check that definition 5.9 is well-defined, i.e. that it does not depend on the choice of $\mathfrak{c}$ and that $[A, B, C]$ indeed lies in $\mathrm{Gal}(F_{A,B}/E)$.

Let A, B, C be non-trivial squarefree polynomials satisfying the conditions of definition 5.9. Let F/K be minimally ramified over $E = k(\sqrt{A}, \sqrt{B})$ with respect to C, which exists by lemma 5.5. Consider a prime P dividing C. Then P splits or ramifies in K_A and K_B by equation (5.3), and is unramified in at least one of them by equation (5.2). Thus a prime $\mathfrak{p}_K \mid P$ in K will have degree 1, and is split in the extension E/K. The prime $\mathfrak{p}_K$ is also unramified in F/K since F is minimally ramified with respect to C. Thus $\mathrm{Art}(\mathfrak{p}_K, F/K) \in \mathrm{Gal}(F/E)$ is well-defined. Since $\mathrm{Gal}(F/E)$ is contained in the center of $\mathrm{Gal}(F/k)$, $\mathrm{Art}(\mathfrak{p}_K, F/K)$ is also well-defined as element in $\mathrm{Gal}(F/k)$ and only depends on F and P, and not on the choice of $\mathfrak{p}_K \mid P$. For such a P dividing C we can therefore define the *local Rédei symbol*

$$[A, B, C]_{F,P} := \mathrm{Art}(\mathfrak{p}_K, F/K) \in \mathrm{Gal}(F/E). \tag{5.8}$$

Whenever P does not divide C we set $[A, B, C]_{F,P} := \mathrm{id}_F$. The local symbol is also defined for the infinite prime. The Rédei symbol can now be written as a product of its local parts

$$[A, B, C] = \prod_{P \le \infty} [A, B, C]_{F,P} \in \mathrm{Gal}(F/E).$$

There are only finitely many non-trivial elements in the infinite product, namely the parts for P dividing C, so the infinite product is a well-defined element in $\mathrm{Gal}(F/E)$. Moreover, this shows that the Rédei symbol does not depend on the choice of ideal $\mathfrak{c}$ but only on C.

The local Rédei symbols can be interpreted in the following way. A prime $\mathfrak{p}_K$ splits in E/K whenever P divides C, so $[A, B, C]_{F,P}$ can be calculated by the Artin symbol $\mathrm{Art}(\mathfrak{p}_E, F/E)$ for some prime $\mathfrak{p}_E \mid P$ in E, implying that $[A, B, C]$ lies in $\mathrm{Gal}(F/E)$. Since $\mathfrak{p}_E$ is unramified in F/E, its norm $N_{E/K_A}(\mathfrak{p}_E) = \mathfrak{p}$ in K_A is unramified in at least one of the extensions $K_A(\sqrt{\beta})$ and $K_A(\sqrt{\beta'})$. Replacing $\mathfrak{p}$ with a conjugate prime in K_A if necessary, we may assume that $\mathfrak{p}$ is unramified in $K_A(\sqrt{\beta})/K_A$. The P-part of the Rédei symbol can now be calculated as

$$[A, B, C]_{F,P} = \mathrm{Art}(\mathfrak{p}, K_A(\sqrt{\beta})/K_A).$$

Essentially, $[A, B, C]_{F,P}$ is the quadratic symbol $\left(\frac{\beta}{\mathfrak{p}}\right)$ in the quadratic field K_A. We can also write the P-part of the Rédei symbol as the Hilbert symbol

$$[A, B, C]_{F,P} = (\beta, \pi)_{\mathfrak{p}}, \tag{5.9}$$

where π is a uniformiser of K_A at $\mathfrak{p}$.

***Remark* 5.10.** When $\deg(A)$ and $\deg(B)$ are even, we may end up in the special case of adding a quadratic twist $\beta \to Q\beta$ for some irreducible $Q \in \mathbb{F}_q[x]$. By the assumption that $\left(\frac{Q}{P}\right) = 1$ for all finite P dividing C, we know obtain $(Q, \pi)_{\mathfrak{p}} = 1$ for any choice of $\mathfrak{p} \mid P$ in K_A. Thus the twisting by Q has no influence on the local Rédei symbols for any finite prime P. △

***Remark* 5.11.** The infinite part of the Rédei symbol only needs to be calculated when C has odd degree and thus at least one of A, B has even degree. A prime at infinity in K is also unramified in F/K. Thus $K_A(\beta)/K_A$ is also unramified at infinity (after potentially taking conjugates) and by the same reasoning as above the ∞-part of the Rédei symbol can also be calculated as a quadratic Hilbert symbol

$$[A, B, C]_{F,\infty} = (\beta, \pi)_{\mathfrak{p}_\infty} \in \{\pm 1\}$$

where π is a uniformiser at $\mathfrak{p}_\infty$. Here we may also have to apply a twist $\beta \to Q\beta$. △

Before moving to the reciprocity law, we give a property of the Rédei symbol.

Proposition 5.12. *Suppose that $D \in \mathbb{F}_q[x]$ is a squarefree polynomial with at least one irreducible component of odd degree. Let $D = D_1 D_2$ be a decomposition of the second type as in lemma 4.2. Then the Rédei symbol $[D_1, D_2, -D_1 D_2]$ is defined and trivial.*

Proof. The fact that $D_1 D_2$ is a decomposition of the second type implies that $(D_1, D_2)_P = 1$ for all primes P by item 3 of lemma 4.2. Indeed, for finite primes $P \nmid D$ we have $(D_1, D_2)_P = 1$. When P divides D, say D_1, it holds that $(D_1, D_2)_P = \left(\frac{D_2}{P}\right) = 1$. The vanishing of the symbol at infinity follows from the product formula [AT68, theorem $X.ii$, 4.13]. Multiplying $(D_1, D_2)_P$ with the trivial symbols $(D_1, -D_1)_P$ and $(-D_2, D_2)_P$ implies $(D_1, -D_1 D_2)_P = (-D_1 D_2, D_2)_P = 1$ so that the triple satisfies equation (5.2). Condition 5.3 is also satisfied because at most one of D_1 and D_2 is of odd degree and D is a squarefree polynomial. Thus $[D_1, D_2, -D_1 D_2]$ is a well-defined Rédei symbol.

Since D_1 and D_2 are relatively prime and D contains an irreducible component of odd degree, a minimally ramified extension F with respect to $-D_1 D_2$ is unramified over $K = k(\sqrt{D})$. We can even take F to lie in the Hilbert class field by lemma 4.2. Consider the ideal $\mathfrak{c} = (\sqrt{D})$ of norm $-D$. This ideal is trivial in the class group $C(D)$ of K. Because F is a subextension of the Hilbert class field of K, we use Artin reciprocity to find that $\mathfrak{c}$ has trivial Artin symbol in the extension F/K. Since the infinite primes split completely in F/K, the Artin symbol at infinity is also trivial. □

5.3 Rédei reciprocity

In this subsection we prove the main result about Rédei symbols, which by definition is symmetric in its first two arguments. We will show that the symbol is symmetric in all three of its arguments by proving the following theorem.

Theorem 5.13. *For $A, B, C \in k^*/k^{*2}$ satisfying the conditions of definition 5.9, the Rédei symbol is multiplicative in each of its arguments and satisfies*

$$[A, B, C] = [B, A, C] = [A, C, B].$$

We call this the Rédei reciprocity law.

In order to prove Rédei reciprocity, let us give an overview of all the field extensions. Choose a minimally ramified extension $F = E(\sqrt{\beta})$ over E of $K = k(\sqrt{AB})$ with respect to C. Similarly, choose a minimally ramified extension $F' = E'(\sqrt{\gamma})$ over E' of $K' = k(\sqrt{AC})$ with respect to B. We obtain local symbols $[A, B, C]_{F,P}$ and $[A, C, B]_{F',P}$ for all primes P. The elements $\beta, \gamma \in K_A$ have norm $B, C \pmod{k^{*^2}}$ respectively. The diagram of extensions can be seen in figure 1.

Lemma 5.14. *Let $A, B, C \in k^*/k^{*^2}$ satisfy the conditions of definition 5.9 and let $F = E(\sqrt{\beta})$ minimally ramified over E with respect to C and $F' = E'(\sqrt{\gamma})$ minimally ramified over E' with respect to B. For all primes P of k it holds that*

$$[A, B, C]_{F,P} [A, C, B]_{F',P} = \prod_{\mathfrak{p} \mid P \text{ in } K_A} (\beta, \gamma)_{\mathfrak{p}}. \tag{5.10}$$

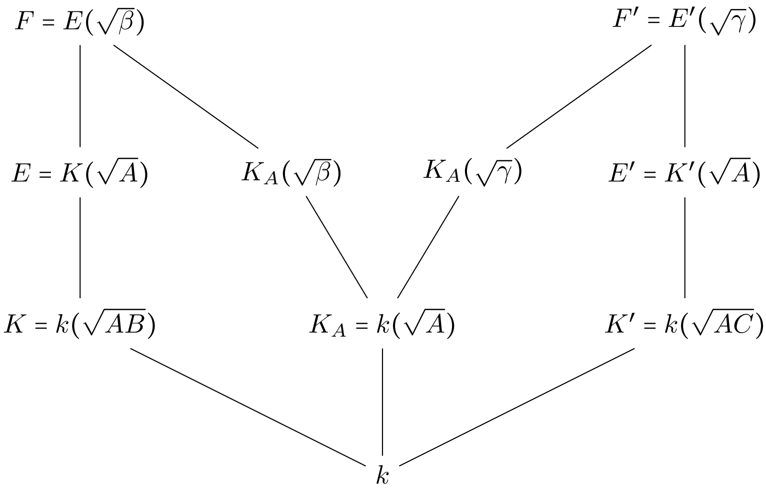

Figure 1: The field extensions used in lemma 5.14.

Proof. Denote the left- and right-hand side of equation (5.10) by L_P and R_P respectively. Note that both sides of equation (5.10) are symmetric in B and C. We may also replace β (or γ) in R_P with its conjugate, because the product equals

$$\prod_{\mathfrak{p}|P}(\beta,\gamma)_{\mathfrak{p}}\prod_{\mathfrak{p}|P}(\beta',\gamma)_{\mathfrak{p}} = \prod_{\mathfrak{p}|P}(B,\gamma)_{\mathfrak{p}} = (B,C)_P = 1.$$

At most one of F and F' can require an extra twist $\beta \mapsto Q\beta$. Without loss of generality we may assume the twist, if it occurs, happens for F. Write therefore $\beta = Q\beta_0$ where Q is either trivial when no twist is required or it is an irreducible polynomial satisfying equation (5.4). Let P be a prime not equal to Q. By condition 5.3 P divides at most 2 of A, B, C. If P divides B it is either split or ramified in K_A/k. In the ramified case β_0 is, up to squares, a uniformiser at $\mathfrak{p}_1 \mid P$ in K_A. The twist with Q does not matter because equation (5.4) implies that Q is a unit at $\mathfrak{p}_1$. In the split case, $(P) = \mathfrak{p}_1\mathfrak{p}_2$ in K_A, β is a unit at the other prime $\mathfrak{p}_2$. When P does not divide B, the fact that F/K is minimally ramified implies that β is a unit at primes $\mathfrak{p} \mid P$ in K, up to squares. Analogous statements hold for C and γ.

We are now ready to check that equality in equation (5.10) holds for any prime P not equal to Q.

- Suppose first that P does not divide BC. Then $L_P = 1$ by definition of the symbol. The elements β, γ are both units at all $\mathfrak{p} \mid P$, so that the symbols $(\beta,\gamma)_{\mathfrak{p}}$ are all trivial, making $R_P = 1$.
- Next assume that P divides exactly one of B and C, say without loss of generality P divides C. Then β is a is a P-unit and F is unramified over P, while γ is a uniformiser at a prime $\mathfrak{p}_1 \mid P$ in K_A up to squares. Thus we can apply equation (5.9) and write $L_P = (\beta,\gamma)_{\mathfrak{p}_1}$. In the case that P ramifies in K_A we have equality to R_P. In the split case both β and γ are units at $\mathfrak{p}_2 \mid P$, giving a Hilbert symbol $(\beta,\gamma)_{\mathfrak{p}_2} = 1$ and the right hand side also equals $(\beta,\gamma)_{\mathfrak{p}_1}$.
- Finally, when P divides both B and C, it cannot divide A and we are in the split case in K_A. After replacing β by its conjugate β' if necessary, we may assume that β is a unit at $\mathfrak{p}_1$ and a uniformiser at $\mathfrak{p}_2$, up to squares, while γ is a uniformiser at $\mathfrak{p}_1$ and a unit at $\mathfrak{p}_2$. By equation (5.9) we find

$$L_P = [A,B,C]_{F,P}[A,C,B]_{F',P} = (\beta,\gamma)_{\mathfrak{p}_1}(\beta,\gamma)_{\mathfrak{p}_2} = R_P.$$

When Q is non-trivial, the local reciprocity in equation (5.10) still holds at Q. As Q does not divide BC we get $L_Q = 1$ by definition. By equation (5.4) Q splits in K_A and both β_0 and γ are units at primes $\mathfrak{q} \mid Q$ in K_A. Thus R_Q equals

$$\prod_{\mathfrak{q}|Q \text{ in } K_A} (\beta, \gamma)_{\mathfrak{q}} = \prod_{\mathfrak{q}|Q \text{ in } K_A} (Q, \gamma)_{\mathfrak{q}} (\beta_0, \gamma)_{\mathfrak{q}} = (Q, C)_Q = 1 = L_Q.$$

□

Proof of Theorem 5.13 By lemma 5.14 the product of Rédei symbols $[A, B, C][A, C, B]$ is the product local symbols as in equation (5.8) over all primes $\mathfrak{p} \leq \infty$ in K_A. We write

$$[A, B, C][A, C, B] = \prod_{P \leq \infty \text{ in } \mathbb{F}_q(x)} [A, B, C]_{F,P} [A, C, B]_{F',P} = \prod_{\mathfrak{p} \leq \infty \text{ in } K_A} (\beta, \gamma)_{\mathfrak{p}} = 1.$$

The last equality follows from the product formula. Hence we have symmetry of the Rédei symbol in the last two arguments. By construction we also have symmetry in the first two arguments. The multiplicativity of the Rédei symbol in C follows from its construction as a product of all its P-parts. Multiplicativity in all its arguments then follows from the symmetry. □

The reciprocity law gives us a faster way of showing that definition 5.9 is well-defined.

Lemma 5.15. *The definition of Rédei symbols in definition 5.9 is independent of the choice of minimally unramified $F_{A,B}$ and ideal $\mathfrak{c}$.*

Proof. We already saw the independence of $\mathfrak{c}$ by writing $[A, B, C]$ as a product of P-symbols. The fact that it does not depend on the choice of $F_{A,B}$ follows from the reciprocity law $[A, B, C] = [A, C, B]$, because the right hand side is independent of $F_{A,B}$. This also works when $C = B$ by using that $[A, B, B] = [B, B, A]$. □

6 Governing fields

As an application of Rédei reciprocity, we will show the existence of a governing field for the 8-rank whenever D has an irreducible component of odd degree. This assumption is needed to avoid the case that there exists an extra irregular ambiguous ideal class. We recall the definition of a governing field from definition 1.1.

Definition 6.1 (Governing fields)**.** Let q an odd prime and $D \in \mathbb{F}_q[x]$ squarefree. A Galois extension $\Omega_{2^j}(D)/\mathbb{F}_q(x)$ is called a *governing field for the* 2^j*-rank* of $C(DP)$ if the Frobenius conjugacy class of an unramified prime $P \in \mathbb{F}_q[x]$ in $\mathrm{Gal}(\Omega_{2^j}(D)/\mathbb{F}_q(x))$ completely determines the 2^k-rank for all $k \leq j$.

***Remark* 6.2.** In the original formulation for number fields, Cohn and Lagarias showed that if there exists a governing field for the 2^j-rank, there is a unique one with smallest degree [CL83, theorem 1.1]. The proof of this theorem also holds for function fields. We have not required $\Omega_j(D)$ to have the smallest degree, so we are considering *a* governing field instead of *the* governing field. △

Let D be a squarefree polynomial. The governing field $\Omega_{2^0}(D) = \mathbb{F}_q(x)$ exists trivially. By theorem 3.1 the 2-rank of $C(DP)$, with P an irreducible monic polynomial, depends on the leading coefficient of D, the parity of the degrees of the irreducible components of D, and the parity of $\deg(P)$. A governing field for the 2-rank therefore only needs to govern the parity of $\deg(P)$. Since the splitting behaviour of P in the extension $\mathbb{F}_q(x) = k \subset k(\sqrt{g})$ is determined by the quadratic symbol $\left(\frac{g}{P}\right) = (-1)^{\deg(P)}$, we find that

$$\Omega_2(D) = k(\sqrt{g}) \cong \mathbb{F}_{q^2}(x)$$

is a governing field for the 2-rank of $C(DP)$.

By the Rédei map from equation (3.7), the 4-rank of $C(DP)$ depends on the Artin symbols $\mathrm{Art}(\mathfrak{a}_j, k(\sqrt{A_i})/k)$ where the $\mathfrak{a}_j$ generate the ambiguous ideal classes and the $\sqrt{A_i}$ generate the genus field H_2 in equation (3.1). Recall from equation (3.8) that these Artin symbols are determined by genus characters. In particular it holds that

$$\mathrm{Art}(\mathfrak{a}_j, k(\sqrt{A_i})/k) = \chi_{A_i}(N(\mathfrak{a}_j)) = \left(\frac{A_i}{N(\mathfrak{a}_j)}\right),$$

whenever A_i and $N(\mathfrak{a}_j)$ are relatively prime.

Most of the generating ambiguous ideals $\mathfrak{a}_j$ have a norm that is an irreducible polynomial $P_i \mid D$, except for the potential irregular ambiguous ideal class. In that case we can write $D = c(U^2 - gV^2)$ with $\deg(U) > \deg(V)$ [Art24], so that the irregular class is generated by an ideal α with $N(\alpha) = U$ (or V). Note that $N(\alpha)$ is a nonsquare modulo every prime divisor of D, so the symbols $\left(\frac{P_i}{N(\alpha)}\right)$ are fixed. The only symbol that might vary in the column of the Rédei matrix for the ideal α is the quadratic symbol $\left(\frac{g}{N(\alpha)}\right)$. For a fixed D, we have found that the 4-rank of $C(DP)$ will be determined by

- $\left(\frac{g}{P}\right)$ and $\left(\frac{P_i}{P}\right)$ for each $P_i \mid D$ monic irreducible, and
- $\left(\frac{g}{N(\alpha)}\right) = (-1)^{\deg(N(\alpha))} = (-1)^{\deg(DP)/2}$ when $\mathrm{sgn}(D) = g$ and DP consists of only irreducible parts of even degree.

The symbol $\left(\frac{g}{N(\alpha)}\right)$, if applicable, is determined by the degree of P modulo 4. Since 2-divisibility of $\deg(P)$ is governed by the splitting behaviour in $k(\sqrt{g}) \cong \mathbb{F}_{q^2}(x)$, the 4-divisibility will be governed a further splitting in the constant field extension $k(\sqrt[4]{g}) \cong \mathbb{F}_{q^4}(x)$. We can conclude that a governing field for the 4-rank of $C(DP)$ is given by

$$\Omega_4(D) = \begin{cases} k(\sqrt[4]{g}, \{\sqrt{P_i} : P_i \mid D \text{ monic irreducible}\}) & \text{if } \mathrm{sgn}(D) \text{ and each irreducible} \\ & \qquad \text{part of } D \text{ is of even degree,} \\ k(\sqrt{g}, \{\sqrt{P_i} : P_i \mid D \text{ monic irreducible}\}) & \text{otherwise.} \end{cases}$$

***Remark* 6.3.** The governing field that we have written above may not be the smallest governing field of $C(D)$. △

Theorem 6.4. *Let $D = eP_1 \dots P_s \in \mathbb{F}_q[x]$ a squarefree polynomial with all P_i monic irreducible polynomials and assume at least one of the P_i is of odd degree. Then $\Omega_8(D)$ exists.*

Proof. We have already seen that $\Omega_{4,D} = \mathbb{F}_q(x)(\sqrt{g}, \{\sqrt{P_i} : P_i \mid D\})$ is a governing field for the 4-rank of $C(DP)$. Now suppose that P and P' are primes that are unramified in $\Omega_{4,D}$ and have the same Artin symbol in $\mathrm{Gal}(\Omega_{4,D}/\mathbb{F}_q(x))$. If we number the primes in DP and DP' in the obvious compatible way, the Rédei matrices R_4 and R_4' as given in equation (3.7) will coincide. To calculate the 8-rank via equation (4.2), we can choose compatible bases and compare R_8 and R_8' by each entry. In particular, if $DP = D_1D_2$ is a splitting of the second type then $DP' = D_1'D_2'$ is also a splitting of the second type, where $D_i' = P'D_i/P$.

An entry in R_8 is determined the Artin symbol $\mathrm{Art}(\mathfrak{m}, E(\beta)/K) \in \mathrm{Gal}(F/E)$ of some ideal $\mathfrak{m}$ of norm M and a quartic extension $F = E(\sqrt{\beta})/K$ belonging to a splitting $DP = D_1D_2$ of the second type. We would like to write this entry of R_8 as a Rédei symbol $[D_1, D_2, M]$. As we excluded the possibility of an irregular ambiguous ideal, we can take M to divide DP. At most one of D_1 and D_2 is of odd degree, because $DP = D_1D_2$ is a splitting of the second type. Hence the triple (D_1, D_2, M) will satisfy condition 5.2. By lemma 4.2 all Hilbert symbols $(D_1, D_2)_P$ are trivial. The fact that $\mathfrak{m}$ is a generator of $\ker(R_4)$ implies that it is a square in the class group. Thus there exists an ideal $\mathfrak{I}$ in $k(\sqrt{D})$ of some norm $I \in k^*$ such that $\mathfrak{I}^2\mathfrak{m} = (Z)$ is principal with some generator $Z = A + B\sqrt{D} \in O_{k(\sqrt{D})}$. Taking norms of these ideals in k, it follows that $I^2M = A^2 - DB^2$ which means that M is a norm in $k(\sqrt{D})$. In particular the Hilbert symbols $(D, M)_Q = (D_1, M)_Q(D_2, M)_Q$ are trivial for all primes $Q \leq \infty$, giving the terms on the right hand side the same value. We still need to show that both are trivial.

Consider a finite prime Q. Whenever $Q \nmid M$, we can take the D_i that is not divisible by Q (because $\gcd(D_1, D_2) = 1$), making them both Q-units and $(D_i, M)_Q = 1$. When Q divides M, Q must split either in k_{D_1} or k_{D_2} because it is a decomposition of the second type, implying that at least one of $(D_1, M)_Q$ and $(D_2, M)_Q$ is 1. Hence $(D_1, M)_Q = (D_2, M)_Q = 1$ for all finite primes Q. The Hilbert symbol at infinity follows from the product formula [AT68, theorem XII.4.13]. We conclude that $[D_1, D_2, M]$ is a well-defined Rédei symbol. The same reasoning holds for the entries of R'_8.

By possibly switching D_1 and D_2, we may assume that P divides D_2. When P also divides M we can use the trivial symbol $[D_1, D_2, -D_1D_2]$ from proposition 5.12 and additivity of the Rédei symbol to write

$$[D_1, D_2, M] = [D_1, D_2, 1/M] = [D_1, D_2, -D_1D_2/M],$$

where P does not divide $-D_1D_2/M$. All entries in R_8 can thus be written as $[D_1, D_2, M]$ where $P \nmid D_1M$. Similarly, the entries of R'_8 (where the splittings of the second type are written as $DP' = D'_1D'_2$) have become $[D'_1, D'_2, M']$, where $P' \nmid D_1M$. Recalling that $D'_i = P'D_i/P$ we have rewritten the entries of R'_8 as $[D_1, D'_2, M]$

After this reduction we can apply Rédei reciprocity (theorem 5.13) and rewrite the entries of R_8 as

$$[D_1, D_2, M] = [D_1, M, D_2].$$

The triple (D_1, M, D_2) still satisfies the conditions of definition 5.4, so there exists an extension $F_{D_1,M}$ that is minimally ramified over $E_{D_1,M} = k(\sqrt{M}, \sqrt{D_1})$ with respect to D_2. In fact, we claim that there is an extension $F_{D_1,M}$ that lands in case 1 of definition 5.4.

Claim 1. *The extension $E_{D_1,M} \subset F_{D_1,M}$ is unramified outside* $\gcd_\infty(D_1, M)$.

Writing $F_{D_1,M} = E_{D_1,M}(\beta_{D_1,M})$, the result is that $[D_1, M, D_2] = [D_1, M, D'_2]$ whenever P and P' have the same Artin symbol in $\mathrm{Gal}(\Omega_{4,D}(\sqrt{\beta_{D_1,M}})/\Omega_{4,D})$. Letting $\Omega_8(D)$ be the compositum of the fields $\Omega_{4,D}(\sqrt{\beta_{D_1,M}})$ ranging over all the entries of R_8 gives us the desired governing field. □

Proof of claim 1. For the triple (D_1, M, D_2) we want to show that there exists a minimal ramified extension $F_{D_1,M}$ over $k(\sqrt{D_1}, \sqrt{M})$ with respect to D_2 that satisfies item 1 of definition 5.4, i.e. unramified outside $\gcd_\infty(D_1, M)$. Let us recall what D_1 and M actually can be. In the construction of the matrix R_8 we are free to choose a basis of $\ker(R_4)$ (representing classes in $C^2 \cap C[2]$) and a basis of $\widehat{C}[4]/\widehat{C}[2]$ (which can be represented by quadratic characters via lemma 4.2). We can therefore use an explicit description of the basis of $C[2]$ to narrow down the possibilities for M. Let $D = eQ_1 \dots Q_{s_1}P_1 \dots P_{s_2}$ be the decomposition of D into irreducible parts with $s_1 > 0$ by assumption. In section 3.1 we found that $C[2]$ can be generated by the classes of all finite primes dividing DP. We can therefore take M to be in

$$M \in \{Q_1, \dots, Q_{s_1}, P_1, \dots, P_{s_2}\} \cup \{-D\}, \tag{6.1}$$

By making the changes $P_j \mapsto Q_1P_j$ for all j and the extra change $P \mapsto Q_1P$ when $\deg(D)$ is even to the basis of $C[2]$, all the options for M will have odd degree. In other words we may assume that

$$M \in \{Q_1, \dots, Q_{s_1}, Q_1P_1, \dots, Q_1P_{s_2}\} \cup \{-D \text{ or } -D/Q_1\}. \tag{6.2}$$

That implies the pair (D, M) always lands in case 1 of definition 5.4 as it can never land in case 2 by a degree argument. □

Further research We have shown that item 2 (the 'bad case') of minimally ramified extensions as in definition 5.4 cannot be avoided on certain occasions. A next step would be to give necessary and sufficient conditions when a triple (A, B, C) lands in the bad case.

Furthermore, one may wonder whether governing fields for the 8-rank exist when all irreducibe part of the discriminant have even degree. Then the 8-rank is much harder to control by the existence of an irregular ambiguous ideal. We might compare this case to the 16-rank of certain quadratic number fields, as described by Milovic [Mil17]. In both situations the discriminant can be written as a difference $D = A^2 - gB^2$ for some unit g. For number fields, Koymans and Milovic [KM21] showed that governing fields for the 16-rank do not exist for such discriminants and their methods may be applied to function fields as well.

Funding The author is supported by the Dutch Research Council (NWO) as part of the Quantum Software Consortium programme (project number 024.003.037) and the Quantum Delta NL programme (project number NGF.1623.23.023).

Acknowledgements Part of the results were obtained in the author's Master's thesis [Sto24]. I want to thank Gunther Cornelissen for his supervision and helpful suggestions during the project. I would also like to thank Peter Koymans and Jonathan Love for the useful discussions, and Peter Bruin for proofreading the document and useful suggestions.

References

[Art24] Emil Artin. Quadratische Körper im Gebiete der höheren Kongruenzen. i. *Mathematische Zeitschrift*, 19:153–206, 1924.

[AT68] Emil Artin and J. Tate. *Class field theory.* American Mathematical Society, 1968.

[CL83] Harvey Cohn and Jeffrey C. Lagarias. On the existence of fields governing the 2-invariants of the classgroup of $\mathbb{Q}(\sqrt{dp})$ as p varies. *Mathematics of Computation*, 41(164):711–730, 1983.

[CLJ84] Henri Cohen and Hendrik W. Lenstra Jr. Heuristics on class groups of number fields. In *Number Theory Noordwijkerhout 1983: Proceedings of the Journées Arithmétiques held at Noordwijkerhout, The Netherlands July 11–15, 1983*, volume 1068 of *Lecture Notes in Mathematics*, pages 33–62. Springer, 1984.

[Cor99] Gunther Cornelissen. Zeroes of Eisenstein series, quadratic class numbers and supersingularity for rational function fields. *Math. Ann.*, 314:175–196, 1999. doi:10.1007/s002080050291.

[Cor01] Gunther Cornelissen. The 2-primary class group of certain hyperelliptic curves. *Journal of Number Theory*, 91:174–185, 2001. arXiv:https://arxiv.org/abs/math/9908175.

[Cor07] Jens Corsman. *Rédei symbols and governing fields.* PhD thesis, McMaster University, 2007. URL: https://www.collectionscanada.gc.ca/obj/thesescanada/vol2/002/NR36051.PDF.

[FW87] Eduardo Friedman and Lawrence C. Washington. On the distribution of divisor class groups of curves over a finite field. In *Théorie des nombres*, pages 227–239. de Gruyter Berlin, 1987. doi:10.1515/9783110852790.

[Gau01] Carl F. Gauss. *Disquisitiones arithmeticae.* 1801.

[Hu98] Weiqun Hu. On imaginary quadratic function fields with the ideal class group to be exponent ≤ 2. *Chinese science bulletin*, 43:2055–2059, 1998. doi:10.1007/BF03183504.

[KM21] Peter Koymans and Djordjo Milovic. Joint distribution of spins. *Duke Mathematical Journal*, 170(8):1723–1755, 2021. doi:10.1215/00127094-2020-0068.

[Lam05] T.Y. Lam. *Introduction to Quadratic Forms over Fields*, volume 67 of *Graduate Studies in Mathematics.* American Mathematical Society, 2005.

[Mil17] Djordjo Milovic. On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-8p})$ for $p \equiv -1 \pmod 4$. *Geometric and Functional Analysis*, 27:973–1016, 2017. doi:10.1007/s00039-017-0419-6.

[Pen03] Guohua Peng. The genus fields of Kummer function fields. *Journal of Number Theory*, 98(2):221–227, 2003. doi:10.1016/S0022-314X(02)00042-2.

[Réd34] László Rédei. Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.*, 171:55–60, 1934.

[Réd39] László Rédei. Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. i. *J. Reine Angew. Math.*, 180:1–43, 1939.

[Ros87] Michael Rosen. The Hilbert class field in function fields. In *Exposition. Math*, volume 5, pages 365–378, 1987.

[Ros00] Michael Rosen. *Number Theory in Function Fields.* Springer-Verlag, 2000.

[Sém98] Stéphan Sémirat. Genus theory for quadratic function fields and applications. *Preprint Université Paris VI*, 1998.

[Ste89] Peter Stevenhagen. Ray class groups and governing fields. *Publications mathématiques de la Faculté des sciences de Besancon. Théorie des nombres*, (1):1–93, 1989.

[Ste22] Peter Stevenhagen. Rédei reciprocity, governing fields and negative Pell. *Mathematical Proceedings of the Cambridge Philosophical Society*, 172(3):627–654, 2022. doi:10.1017/S0305004121000335.

[Sto24] Joppe Stokvis. Class groups of global fields. Master's thesis, Utrecht University, 2024. URL: https://studenttheses.uu.nl/bitstream/handle/20.500.12932/46866/Thesis_JStokvis.pdf.

[Wit07] Christian Wittmann. ℓ-class groups of cyclic function fields of degree ℓ. *Finite Fields and Their Applications*, 13(2):327–347, 2007. doi:10.1016/j.ffa.2005.09.001.

[Zha87] Xianke Zhang. Ambiguous classes and 2-rank of class group of quadratic function field. *J. China Univ. Sci. Tech*, 17:425–431, 1987.

A Magma

The following Magma code generates examples of minimally ramified extensions where the extra ramified prime from definition 5.3 is necessary. It generates one example for each prime $q \equiv 3 \pmod 4$ smaller than 200.

```
//Input: q = field size, f and g make up the decomposition of the second type,
//  C is a point on the conic (X^2=f*Y^2+g*Z^2).
//Output: Decomposition type of an infinite place in the extension F_q(t, sqrt(f),
//  sqrt(X-sqrt(f)*Y)) / F_q(t, sqrt(f)). We want this to be unramified.
ramification := function(q,f,g,C)
    R<t> := FunctionField(GF(q));
    P<y> := PolynomialRing(R);
    X:= Numerator(C[1]);
    Y:= Numerator(C[2]);
    FF1<alpha> := FunctionField(y^2-f);
    P := Places(R,1);
    inf:=P[1];

    //The infinite prime should split in F_q(t, sqrt(f)) / F_q(t)
    DecompositionType(FF1, inf);

    Q<z> :=PolynomialRing(FF1);
    FF2<beta>:= FunctionField(z^2 - (X+alpha*Y));
    P := Places(FF1, 1);
    inf:=P[1];
    return (DecompositionType(FF2, inf));
end function;

for q in [3..200] do
    if q mod 4 eq 3 and IsPrimePower(q) then
        q;
        R<t>:= RationalFunctionField(GF(q));
        S<u>:=PolynomialRing(R);
        P<x,y,z> := ProjectiveSpace(R, 2);
        F<t>:=PolynomialRing(GF(q));
        f:= RandomIrreduciblePolynomial(GF(q),4);
```

```
            for g in AllIrreducblePolynomials(GF(q), 2) do
            C := Conic(P, x^2 -f*y^2 - g*z^2);
            if HasRationalPoint(C) then
                RP:=RationalPoint(C);
                if Degree(Numerator(RP[1])) mod 2 eq 1 then
                    f,g;
                    RP;
                    ramification(q,f,g, RP);
                    clgroup(q,f,g);
                    break;
                end if;
            end if;
            end for;
        end if;
    end for;
```