On the Latimer-MacDuffee theorem for polynomials over finite fields

by

Jacobus Visser van Zyl

Dissertation presented for the degree of Doctor of Philosophy in the Faculty of Science in Mathematics at Stellenbosch University

Department of Mathematics and Applied Mathematics,
Rhodes University,
Grahamstown
6140, South Africa.

Promoter: Prof Florian Breuer

March 2011

Declaration

By submitting this dissertation electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Signature: .....
J.V. van Zyl

Date: .....

Abstract

On the Latimer-MacDuffee theorem for polynomials over finite fields

J.V. van Zyl

Department of Mathematics and Applied Mathematics,
Rhodes University,
Grahamstown
6140, South Africa.

Dissertation: PhD (Mathematics)

March 2011

Latimer & MacDuffee showed in 1933 that there is a one-to-one correspondence between equivalence classes of matrices with a given minimum polynomial and equivalence classes of ideals of a certain ring. In the case where the matrices are taken over the integers, Behn and Van der Merwe developed an algorithm in 2002 to produce a representative in each equivalence class. We extend this algorithm to matrices taken over the ring $\mathbb{F}_q[T]$ of polynomials over a finite field and prove a modified version of the Latimer-MacDuffee theorem which holds for *proper* equivalence classes of matrices.

Uittreksel

Oor die Latimer-MacDuffee stelling vir polinome oor eindige liggame

("On the Latimer-MacDuffee theorem for polynomials over finite fields")

J.V. van Zyl

Departement Wiskunde en Toegepaste Wiskunde,
Rhodes Universiteit,
Grahamstad
6140, Suid-Afrika.

Proefskrif: PhD (Wiskunde)

Maart 2011

Latimer & MacDuffee het in 1933 bewys dat daar 'n een-tot-een korrespondensie is tussen ekwivalensieklasse van matrikse met 'n gegewe minimumpolinoom en ekwivalensieklasse van ideale van 'n sekere ring. In die geval waar die matrikse heeltallige inskrywings het, het Behn en Van der Merwe in 2002 'n algoritme ontwikkel om verteenwoordigers in elke ekwivalensieklas voort te bring. Ons brei hierdie algoritme uit na die geval van matrikse met inskrywings in die ring $\mathbb{F}_q[T]$ van polinome oor 'n eindige liggaam en ons bewys 'n gewysigde weergawe van die Latimer-MacDuffee stelling wat geld vir klasse van streng ekwivalente matrikse.

Acknowledgments

I wish to thank my supervisor, professor Florian Breuer, for his support throughout the last five years with its ups and downs by providing advice and, ultimately, direction. Thank you to professor Bas Edixhoven for trying to steer me down the correct path, even if I was stubborn about it. My gratitude goes out towards professor Cristian González-Avilés for his ideas on how to tackle the inert imaginary case in my work and his wise words of encouragement.

I would like to thank the Harry Crossley foundation and the University of Stellenbosch without whose financial support this research would have been much harder, and the University of Leiden who kindly supported my visit to their Mathematics Department.

Lastly, a big thumbs up to the guys at PhD Comics for humouring me with their understanding of what being a grad student is all about.

Contents

Chapter 1

Introduction

Definition 1. A *binary quadratic form* over $\mathbb{Z}$ is an expression of the form

$$ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{Z},$$

with *discriminant* $b^2 - 4ac$. The form is said to be *primitive* if $\gcd(a, b, c) = 1$ and *positive definite* if $a > 0$ and $b^2 - 4ac < 0$.

The study of binary quadratic forms started with Lagrange in his 1773 work *Recherches d'Arithmetique* [8] who introduced the concepts of *discriminant*, *reduced* forms, (Lagrangian) *equivalence* of forms and *equivalence classes* of forms.

Lagrange studied these forms in order to solve some conjectures about primes representible in the form $x^2 + ny^2$ for various values for n. Legendre continued Lagrange's work and in his *Essai sur la Théorie des Nombres* [10] he introduced the concept of *composition* of binary quadratic forms. Legendre's composition was a many-valued operation, even on the equivalence classes of forms (the composition of two forms could lie in as many as four distinct classes).

In 1801, Gauß introduced the concept of *(proper) equivalence* (a restriction on Lagrangian equivalence) in his book *Disquisitiones Arithmeticae* [6]. With this new notion of equivalence, Gauß was able to define *direct composition* of binary quadratic forms, which is a well-defined binary operation on equivalence classes of forms. The direct composition of two binary quadratic forms $f(x, y)$, $g(x, y)$ is a binary quadratic form $F(X, Y)$ which satisfies

$$f(x, y)g(z, w) = F(B_1(x, y; z, w), B_2(x, y; z, w)),$$

where

$$B_i(x, y; z, w) = a_i xz + b_i xw + c_i yz + d_i yw, \quad i = 1, 2$$

and

$$a_1 b_2 - a_2 b_1 = f(1, 0), \quad a_1 c_2 - a_2 c_1 = g(1, 0).$$

Direct composition then makes the set of equivalence classes of primitive, positive definite binary quadratic forms into an Abelian group.

This definition of direct composition is awkard to work with, however, and in 1894 Dirichlet introduced *Dirichlet composition* [5] which is equivalent to direct composition whenever it is defined, and is much simpler to work with, as it provided an explicit method for finding the composition F of two binary quadratic forms f and g.

Over the integers, there is a nice bijection between 2×2 matrices with trace Γ and determinant $-\Delta$, and binary quadratic forms with discriminant $\Gamma^2 + 4\Delta$. The bijection is given by

$$ax^2 + (\Gamma - 2b)xy + cy^2 \longleftrightarrow \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}.$$

This bijection allows us to carry the concepts of *reduced* and *equivalent* forms over to matrices.

A 1933 paper by Latimer and MacDuffee [9] gives a correspondence between equivalence classes of $n \times n$ matrices and equivalence classes of ideals in a certain ring defined by a polynomial f. When $n = 2$, the matrix classes correspond to Lagrangian equivalence classes under the above bijection. Latimer and MacDuffee make the correspondence explicit and in 2002, Behn and Van der Merwe [2] develop an algorithm, using binary quadratic forms and continued fractions, for generating a representative in each Lagrangian class of matrices.

In this dissertation we extend the above work to $\mathbb{F}_q[T]$. Artin's dissertation [1] showed the remarkable analogy between integers and polynomials over finite fields, and indeed, the results mostly have analogous versions over $\mathbb{F}_q[T]$.

In attempting a study by starting with binary quadratic forms, one runs into the problem that binary quadratic forms are awkward to work with in characteristic two, necessitating a separate treatment for even characteristic. Also, the correspondence between binary quadratic forms and matrices breaks down (the correspondence becomes 2-to-1). For this reason, we opted to study

matrix classes directly from the Latimer-MacDuffee point of view. To enable a smooth transtion to the theory associated with proper equivalence classes of binary quadratic forms, we prove a modified version of the Latimer MacDuffee theorem which holds for proper equivalence classes when $n = 2$. When working with matrices, binary quadratic forms are implicit, even in characteristic 2.

The core of this dissertation is to extend the work done by Behn and Van der Merwe in [2], and the transition to $\mathbb{F}_q[T]$ is particularly smooth in that the proofs, while markedly different from the integral case, are independant of the characteristic. When dealing with the group structure on equivalence classes of matrices, the characteristic starts to play a role, but using suitable assumptions and restrictions, the results mostly stay characteristic-free.

Notation

The following notation will be used throughout the dissertation.

$\mathbb{F}_q$	The finite field with q elements.
$\mathbb{F}_q[T]$	The ring of polynomials in T over $\mathbb{F}_q$.
$\deg(x)$	The degree of x as a polynomial in T.
$\operatorname{sgn}(x)$	Leading coefficient of x as a polynomial in T.
$\det(A)$	The determinant of the matrix A.
$\mathbf{R}^\times$	The set of units of $\mathbf{R}$.
$\mathbb{M}_f$	The set of matrices with minimal polynomial f.
$\mathrm{GL}_n(\mathbf{R})$	The group of $n \times n$ matrices A over $\mathbf{R}$ such that $\det(A) \in \mathbf{R}^\times$.
$\mathrm{SL}_n(\mathbf{R})$	The group of $n \times n$ matrices A over $\mathbf{R}$ such that $\det(A) = 1$.
$\mathrm{PSL}_n(\mathbf{R})$	The projective special linear group.

Chapter 2

The Latimer-MacDuffee Theorem

2.1 Latimer and MacDuffee's proof

Let $\mathbf{A}$ be a principal ideal domain and let $f(X) = X^n + f_{n-1}X^{n-1} + \cdots + f_0 \in \mathbf{A}[X]$ be a separable polynomial such that $f_0 \neq 0$, with companion matrix

$$C = (c_{ij}) = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -f_0 & -f_1 & -f_2 & \dots & -f_{n-1} \end{bmatrix}.$$

Let $\mathbb{M}_f$ be the set of $n \times n$ matrices over $\mathbf{A}$ with minimal polynomial f. Let $\mathbf{R}$ be the ring of polynomials in C with coefficients in $\mathbf{A}$.

Definition 2. Two matrices $A,\ B \in \mathbb{M}_f$ are *equivalent* if $B = S^{-1}AS$ for some matrix $S \in \mathrm{SL}_n(\mathbf{A})$.

Definition 3. A *non-singular* ideal of $\mathbf{R}$ is an ideal that is, when viewed as a module over $\mathbf{A}$, free of rank n.

A *directed ideal* of $\mathbf{R}$ is a pair $(\mathfrak{A}, \mathbf{w})$ where $\mathfrak{A}$ is a proper, non-singular ideal of $\mathbf{R}$ and $\mathbf{w}$ is an element of $\mathbf{R}^n$ whose entries generate $\mathfrak{A}$ over $\mathbf{A}$.

Two directed ideals $(\mathfrak{A}, \mathbf{w})$ and $(\mathfrak{B}, \mathbf{v})$ are *equivalent* if there exist two elements $a, b \in \mathbf{R}$ and a matrix $S \in \mathrm{SL}_n(\mathbf{A})$ such that $a\mathfrak{A} = b\mathfrak{B}$ as ideals, and $a\mathbf{w} = bS\mathbf{v}$.

Latimer and MacDuffee's 1933 paper [9] used the notion of Lagrangian equivalence of matrices, that is, the matrix S in the Definition 2 is an element of $\mathrm{GL}_n(\mathbf{A})$, and used equivalence classes of ideals rather than directed ideals. They proved the following theorem in this setting and over the integers, but their proof adapts easily to any principal ideal domain and using the notions of equivalence defined above.

Theorem 1 (The Latimer-MacDuffee Theorem)**.** *There is a bijection between the equivalence classes of matrices in* $\mathbb{M}_f$ *and equivalence classes of directed ideals of* $\mathbf{R}$*.*

Proof. We follow the proof of Latimer and MacDuffee as set out in [9] and [11]. We may take the set $\{C^{i-1}\}_{i=1}^{n}$ as a basis for $\mathbf{R}$ over $\mathbf{A}$; let $e_i = C^{i-1}$, $\mathbf{e} = (e_1, e_2, \ldots, e_n)^t$ and let $(\mathfrak{A},\mathbf{w})$, with $\mathbf{w} = (w_1, w_2, \ldots, w_n)^t$, be a directed ideal of $\mathbf{R}$. We may uniquely write $w_i = \sum_{j=1}^{n} g_{ij}e_j$, that is, $\mathbf{w} = G\mathbf{e}$ for some matrix G over $\mathbf{A}$. Since $\mathfrak{A}$ is an ideal, $e_2 w_i \in \mathfrak{A}$, hence there exist unique elements $d_{ir} \in \mathbf{A}$ such that

$$e_2 w_i = \sum_{j=1}^{n} g_{ij} e_j e_2 = \sum_{r=1}^{n} d_{ir} w_r$$

for each $i = 1, \ldots, n$.

Now, $e_2 e_j = CC^{j-1} = C^j = \sum_{t=1}^{n} c_{jt} e_t$ and $w_r = \sum_{t=1}^{n} g_{rt} e_t$, so

$$\sum_{j=1}^{n} g_{ij} e_j e_2 = \sum_{j,t=1}^{n} g_{ij} c_{jt} e_t = \sum_{r=1}^{n} d_{ir} w_r = \sum_{r,t=1}^{n} d_{ir} g_{rt} e_t$$

for each $i = 1, \ldots, n$. Since the e_t are linearly independent, we have for each i, $t = 1, \cdots\ n$ that

$$\sum_{j}^{n} g_{ij} c_{jt} = \sum_{r}^{n} d_{ir} g_{rt},$$

that is, $GC = DG$ where D is the $n \times n$ matrix (d_{ij}). Since the ideal $\mathfrak{A}$ is non-singular, by definition, so is G, so $D = GCG^{-1}$. Associate the matrix D with the directed ideal $(\mathfrak{A},\mathbf{w})$.

We now show that if $\mathfrak{B}$ has basis $\mathbf{v} = r\mathbf{w}$ or $\mathbf{v} = S\mathbf{w}$ for some element $r \in \mathbf{R}$ or $S \in \mathrm{SL}_n(\mathbf{A})$ and D' is associated with $(\mathfrak{B}, \mathbf{v})$, then D and D' are equivalent. Firstly, if $\mathbf{v} = S\mathbf{w} = SG\mathbf{e}$, then the above process shows that $D' = SGC(SG)^{-1} = SGCG^{-1}S^{-1} = SDS^{-1}$. Suppose now that $\mathbf{v} = r\mathbf{w} = (rG)\mathbf{e}$. Then, since $r \in \mathbf{R}$, $r = g(C)$ can be viewed as a polynomial in C. Since the vector $r\mathbf{w}$ generates a non-singular ideal, it follows that $\det(g(C)) \neq 0$. Also, since $r \in \mathbf{R}$, r commutes with G and so

$$g(C) = Gg(C)G^{-1} = g(GCG^{-1}) = g(D).$$

Hence

$$D' = g(C)GCG^{-1}g(C)^{-1} = g(D)GCG^{-1}g(D)^{-1} = g(D)Dg(D)^{-1}.$$

Since D and $g(D)$ commute, it follows that $D' = Dg(D)g(D)^{-1} = D$.

Thus every equivalence class of ideals is mapped to a unique equivalence class of matrices. To show that this map is surjective, let D be an element of $\mathbb{M}_f$. Then, since D and C both have the same minimum polynomial, there exsists a matrix G over $\mathbf{A}$ such that the entries of G are relatively prime and $D = GCG^{-1}$. Then the directed ideal $(\mathfrak{A}, G\mathbf{e})$, where $\mathfrak{A}$ is the ideal generated by the entries of $G\mathbf{e}$ over $\mathbf{A}$, is mapped to the equivalence class of matrices containing D. (Note that $G\mathbf{e}$ indeed generates an ideal; if $r \in \mathbf{R}$, then as above, $r = g(C)$ is a polynomial in C, so $rG\mathbf{e} = g(C)G\mathbf{e}$, which shows that $G\mathbf{e}$ generates an ideal.)

This shows that there is a bijection between the equivalence classes of matrices in $\mathbb{M}_f$ and equivalence classes of directed ideals of $\mathbf{R}$. □

2.2 The irreducible case

Note that if $f(X)$ is irreducible and separable over $\mathbf{A}$, then the ring $\mathbf{R}$ is isomorphic to $\mathbf{A}[\alpha]$, where α satisfies $f(\alpha) = 0$. In this case, the above proof can be simplified considerably.

Theorem 2 (The Latimer-MacDuffee Theorem for irreducible polynomials)**.** *If f is an irreducible, separable polynomial, then there is a bijection between the equivalence classes of matrices in $\mathbb{M}_f$ and equivalence classes of directed ideals of $\mathbf{R}$.*

Proof. We follow the proof by Taussky in [12].

Let $A \in \mathbb{M}_f$. Then since f is the minimal polynomial of A, α is an eigenvalue of A. Let $\mathbf{w}_\alpha$ be an associated eigenvector - we may choose $\mathbf{w}_\alpha$ to contain only elements of $\mathbf{R}$. Let $\mathfrak{A}$ be the set of $\mathbf{A}$-linear combinations of the entries of $\mathbf{w}_\alpha$. The relation $\alpha\mathbf{w}_\alpha = A\mathbf{w}_\alpha$ shows that $\mathfrak{A}$ is in fact an ideal of $\mathbf{R}$, and since A is non-singular, it shows that the entries of $\mathbf{w}_\alpha$ form a basis for $\mathfrak{A}$. Associate with A the class of directed ideals containing $(\mathfrak{A}, \mathbf{w}_\alpha)$.

Any other choice of eigenvector is a multiple of $\mathbf{w}_\alpha$, and the directed ideal obtained in this way is clearly equivalent to $(\mathfrak{A}, \mathbf{w}_\alpha)$.

If $B = SAS^{-1}$ is equivalent to A, then $BS\mathbf{w}_\alpha = SA\mathbf{w}_\alpha = \alpha S\mathbf{w}_\alpha$, and so B has eigenvalue α with associated eigenvector $S\mathbf{w}_\alpha$. This matrix is associated with the directed ideal $(\mathfrak{A}, S\mathbf{w}_\alpha)$ which is also equivalent to $(\mathfrak{A}, \mathbf{w}_\alpha)$.

Now suppose that $(\mathfrak{B}, \mathbf{v})$ is a directed ideal of $\mathbf{A}[\alpha]$. Then the components of $\alpha\mathbf{v}$ are all elements of $\mathfrak{B}$, and since the components of $\mathbf{v}$ forms a basis for $\mathfrak{B}$ over $\mathbf{A}$, there exists an $n \times n$ matrix B over $\mathbf{A}$ such that $\alpha\mathbf{v} = B\mathbf{v}$. This implies that α is an eigenvalue of B.

Let β be any conjugate of α, and let ϕ be the isomorphism $\mathbf{A}[\alpha] \to \mathbf{A}[\beta]$. Then applying ϕ to the equation $\alpha\mathbf{v} = B\mathbf{v}$ yields $\beta\mathbf{v}' = B\mathbf{v}'$, where $\mathbf{v}'$ is obtained from $\mathbf{v}$ by applying ϕ componentwise. This shows that β is also an eigenvalue of B. Since β was arbitrary, it follows that B has minimal polynomial $f(X)$, and so $B \in \mathbb{M}_f$. Associate with $(\mathfrak{B}, \mathbf{v})$ the equivalence class of matrices containing B.

If $\mathbf{w}$ is any other basis for $\mathfrak{B}$ with $\mathbf{w} = S\mathbf{v}$, where $S \in \mathrm{SL}_n(A)$, a similar argument as above shows that there exists a matrix A over $\mathbf{A}$ such that $\alpha S\mathbf{v} = AS\mathbf{v}$. On the other hand, multiplying the equation $\alpha\mathbf{v} = B\mathbf{v}$ from the left by S gives $\alpha S\mathbf{v} = SB\mathbf{v}$, i.e. $(AS - SB)\mathbf{v} = 0$. Arguing similarly as above, the equation $(AS - SB)\mathbf{v}' = 0$ holds for all eigenvectors $\mathbf{v}'$ of B, and hence $AS = SB$, or $B = S^{-1}AS$. □

An alternative definition of a directed ideal.

In this dissertation we will mainly work with $\mathbf{A} = \mathbb{F}_q[T]$, f irreducible over $\mathbb{F}_q[T]$ with root α and $\mathbf{R} = \mathbb{F}_q[T][\alpha]$. In this case, we may simplify the definition of a directed ideal by using the following bijection of sets.

Proposition 3. *There is a one-to-one correspondence between the set of equivalence classes of directed ideals, and equivalence classes of pairs* $(\mathfrak{A}, \sigma)$ *where* $\mathfrak{A}$ *is an ideal of* $\mathbb{F}_q[T][\alpha]$*,* σ *is an element of* $\mathbb{F}_q^\times$ *and* $(\mathfrak{A}, \sigma_1)$ *and* $(\mathfrak{B}, \sigma_2)$ *are equivalent if there exist* $a, b \in \mathbb{F}_q[T][\alpha]$ *such that* $a\mathfrak{A} = b\mathfrak{B}$ *as ideals and* $\operatorname{sgn}(N(a))\sigma_1 = \operatorname{sgn}(N(b))\sigma_2$*, where* $N(x)$ *is the norm of* x*, that is, the product of the* n *conjugates of* x *in* $\mathbb{F}_q[T][\alpha]$*.*

Proof. Let $(\mathfrak{A}, \mathbf{w})$ be a directed ideal, and let G be the matrix such that $\mathbf{w} = G\mathbf{e}$ (as in the proof of Theorem 1). Let $\sigma = \operatorname{sgn}(\det(G))$ and associate with $(\mathfrak{A}, \mathbf{w})$ the pair $(\mathfrak{A}, \sigma)$. If $(\mathfrak{B}, \mathbf{v})$ is equivalent to $(\mathfrak{A}, \mathbf{w})$, then there exist $a, b \in \mathbb{F}_q[T][\alpha]$ and $S \in \mathrm{SL}_n(\mathbb{F}_q[T])$ such that $a\mathfrak{A} = b\mathfrak{B}$ as ideals, and $aS\mathbf{w} = b\mathbf{v}$. Let $\mathbf{v} = H\mathbf{e}$, so $(\mathfrak{B}, \mathbf{v})$ is associated with $(\mathfrak{B}, \operatorname{sgn}(\det(H)))$.

There are unique matrices R_a and R_b over $\mathbf{A}$ such that $a\mathbf{e} = R_a\mathbf{e}$ and $b\mathbf{e} = R_b\mathbf{e}$, hence $b\mathbf{v} = HR_b\mathbf{e}$, and similarly $aS\mathbf{w} = SGR_a\mathbf{e}$. Since $\mathbf{e}$ contains a basis for $\mathbf{R}$, it follows that $HR_b = SGR_a$. Note that $\det(R_b) = N(b)$, so $\det(HR_b) = \det(H)N(b)$, hence the directed ideal $(b\mathfrak{B}, b\mathbf{v})$ is associated with $(b\mathfrak{B}, \operatorname{sgn}(N(b)\det(H)))$ and $(a\mathfrak{A}, aS\mathbf{w})$ is associated with $(a\mathfrak{A}, \operatorname{sgn}(N(a))\sigma)$. But then we have that $(\mathfrak{A}, \sigma)$ is equivalent to $(a\mathfrak{A}, \operatorname{sgn}(N(a))\sigma)$ which equals $(b\mathfrak{B}, \operatorname{sgn}(N(b))\operatorname{sgn}(\det(H)))$ which is equivalent to $(\mathfrak{B}, \operatorname{sgn}(N(b)\det(H)))$.

Conversely, given the pair $(\mathfrak{A}, \sigma)$, let $\mathbf{w}$ be a vector whose entries generate $\mathfrak{A}$. As before, there exists a matrix G such that $\mathbf{w} = G\mathbf{e}$. If $\operatorname{sgn}(\det(G)) = \tau$, let S be a matrix in $\mathrm{GL}_n(\mathbf{A})$ with $\det(S) = \frac{\sigma}{\tau}$. Then the directed ideal $(\mathfrak{A}, S\mathbf{w})$ is associated with $(\mathfrak{A}, \sigma)$.

□

In the rest of this dissertation, we will refer to both pairs of the form $(\mathfrak{A}, \mathbf{w})$ and $(\mathfrak{A}, \sigma)$ as *directed ideals*. Note that for every $c \in \mathbb{F}_q^\times$, there is a natural bijection $(\mathfrak{A}, \sigma) \mapsto (\mathfrak{A}, c\sigma)$, which we will exploit in chapter 4.

Chapter 3

Equivalence Classes of Matrices

In this chapter we will consider $\mathbf{A} = \mathbb{F}_q[T]$ and $n = 2$. Let the polynomial $p(X) = X^2 - \Gamma X - \Delta \in \mathbb{F}_q[T][X]$ be irreducible. Note that if $p(X)$ is the minimal polynomial of a matrix A over $\mathbb{F}_q[T]$ and $k \in \mathbb{F}_q[T]$, then the polynomial $p(X + k)$ is the minimal polynomial of the matrix $B = A - kI_2$, where I_2 is the 2×2 identity matrix. By replacing X with $X + k$ for some $k \in \mathbb{F}_q[T]$ if necessary, we may assume that the degree of Δ is minimal. Specifically, if $d = \min\{\deg(p(x)) \,|x \in \mathbb{F}_q[T]\}$, where $\deg(x)$ denotes the degree of x as a polynomial in T, and k is an element of $\mathbb{F}_q[T]$ for which this minimum is attained, we may replace $p(X)$ with $p(X + k)$ (in which case $\deg(\Delta) = d$). Further, by replacing X with $\operatorname{sgn}(\Gamma)X$ and dividing the equation through by $\operatorname{sgn}(\Gamma)^2$, we may assume that Γ is monic in T.

The polynomial $p(X)$ now has the following property:

Proposition 4. *Let $p(X) = X^2 - \Gamma X - \Delta$ be a polynomial over $\mathbb{F}_q[T]$ such that Γ is monic in T and $\deg(p(x)) \geq \deg(\Delta)$ for all $x \in \mathbb{F}_q[T]$. If $\deg(\Gamma) = g$ and $\deg(\Delta) = d$, then one of the following holds:*

- *$d > 2g$ and d is odd;*
- *$d > 2g$, d is even and $\operatorname{sgn}(\Delta)$ is not a square in $\mathbb{F}_q$;*
- *$d = 2g$ and $\operatorname{sgn}(\Delta)$ is not of the form $\alpha^2 - \alpha$ for some $\alpha \in \mathbb{F}_q$, or*
- *$d < g$.*

Proof. We prove the contrapositive of the proposition by making use of the following observation: if $\deg(x^2 - \Gamma x) = d$ and $\operatorname{sgn}(x^2 - \Gamma x) = \operatorname{sgn}(\Delta)$, then $\deg(p(x)) < d$. We consider several cases:

- Suppose that $d > 2g$, $d = 2D$ is even and $\operatorname{sgn}(\Delta) = \alpha^2$ for some $\alpha \in \mathbb{F}_q^\times$. Set $x = \alpha T^D$. Then $\deg(x^2) = 2D > g + D = \deg(\Gamma x)$ and so $\deg(x^2 - \Gamma x) = 2D = d$ and $\operatorname{sgn}(x^2 - \Gamma x) = \operatorname{sgn}(x)^2 = \alpha^2 = \operatorname{sgn}(\Delta)$, which shows that $\deg(p(x)) < d$.

- Suppose that $d = 2g$ and $\operatorname{sgn}(\Delta) = \alpha^2 - \alpha$ for some $\alpha \in \mathbb{F}_q$. Set $x = \alpha T^g$. Then $\deg(x^2) = d = \deg(\Gamma x)$, so $\deg(x^2 - \Gamma x) = d$ (since $\alpha^2 - \alpha \neq 0$) and $\operatorname{sgn}(x^2 - \Gamma x) = \operatorname{sgn}(x)^2 - \operatorname{sgn}(x) = \alpha^2 - \alpha = \operatorname{sgn}(\Delta)$.

- Suppose that $g \leq d < 2g$ and set $x = -\operatorname{sgn}(\Delta) T^{d-g}$. Then we have that $\deg(x^2) = 2d - 2g < d = \deg(\Gamma x)$, hence $\deg(x^2 - \Gamma x) = d$ and $\operatorname{sgn}(x^2 - \Gamma x) = -\operatorname{sgn}(x) = \operatorname{sgn}(\Delta)$.

□

Let $\deg(\Gamma) = g$ and $\deg(\Delta) = d$ for the remainder of the chapter. We will consider the 2×2 matrices over $\mathbb{F}_q[T]$ which satisfy the equation

$$X^2 - \Gamma X - \Delta = 0. \tag{3.1}$$

3.1 Reduced matrices

Every matrix solution to (3.1) has the form $\begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ with $\Delta = b^2 - \Gamma b - ac$, $ac \neq 0$.

Definition 4. A matrix solution $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ to (3.1) is said to be *reduced* if $\deg(b) < \deg(a) < \max\{\frac{1}{2}d, g\}$, and is said to be *almost reduced* if $\deg(b) < \deg(a) = \max\{\frac{1}{2}d, g\}$.

In a reduced matrix, the degrees of a and b are bounded from above, and the field of coefficients $\mathbb{F}_q$ is finite. Also, given a and b, c is uniquely determined from $b^2 - \Gamma b - \Delta = ac$, so there is only a finite number of reduced matrices.

We have the following:

Proposition 5. *Every matrix solution to* (3.1) *is equivalent to a reduced matrix or an almost reduced matrix.*

Proof. We use the following algorithm to reduce a matrix $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$.

Step 1. If $\deg(b) \geq \deg(a)$, write $b = aq + r$ in the unique way such that $q,\ r \in \mathbb{F}_q[T]$ and $\deg(r) < \deg(a)$. Replace A with the equivalent matrix

$$\begin{bmatrix} 1 & -q \\ 0 & 1 \end{bmatrix} A \begin{bmatrix} 1 & q \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} r & -c' \\ a & \Gamma - r \end{bmatrix}$$

where $c' = -aq^2 + (\Gamma - 2r)q + c$.

Step 2. If $\deg(a) > \max\{\frac{1}{2}d, g\}$, replace A with the equivalent matrix

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} A \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \Gamma - b & -a \\ c & b \end{bmatrix},$$

and go back to step 1.

If this algorithm terminates, the resulting matrix will be reduced or almost reduced, by construction. It remains to show that the algorithm always terminates.

If, after performing step 1, the algorithm doesn't terminate, it means that $\deg(b) < \deg(a)$ and $\deg(a) > \max\{\frac{1}{2}d, g\}$ and step 2 has to be performed. In this case, since $ac = b^2 - \Gamma b - \Delta$, we have

$$\begin{aligned}
& \deg(c) \\
= \ & \deg(b^2 - \Gamma b - \Delta) - \deg(a) \\
\leq \ & \max\{2\deg(b), g + \deg(b), d\} - \deg(a) \\
= \ & \max\{\deg(b) - [\deg(a) - \deg(b)], g - [\deg(a) - \deg(b)], d - \deg(a)\} \\
< \ & \max\{\deg(b), g, \tfrac{1}{2}d\} \quad (\text{since } \deg(b), \tfrac{1}{2}d < \deg(a)) \\
< \ & \deg(a).
\end{aligned}$$

Thus, performing step 2 strictly decreases the degree of a. Since step 1 leaves the degree of a unchanged, it means that step 2 can only be performed a finite number of times, and so the process terminates. □

This proposition shows that there are only a finite number of equivalence classes of matrix solutions to (3.1).

Remark 1. Note that if $d \geq 2g$ and $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ is reduced (that is to say, $\deg(b) < \deg(a) < \frac{1}{2}d$), then

$$\begin{aligned} \deg(c) &= \deg(b^2 - \Gamma b - \Delta) - \deg(a) \\ &= d - \deg(a) \\ &> \tfrac{1}{2}d, \end{aligned}$$

hence $\deg(a) < \frac{1}{2}d < \deg(c)$ and $\deg(a) + \deg(c) = d$.

Similarly, if $d < g$, then $\deg(b) < \deg(a) < g$ and so

$$\begin{aligned} & \deg(c) \\ = \ & \deg(b^2 - \Gamma b - \Delta) - \deg(a) \\ = \ & \deg(\Gamma b) - \deg(a) \quad (\text{since } \deg(b^2), \deg(\Delta) < g + \deg(b) = \deg(\Gamma b)) \\ = \ & g - [\deg(a) - \deg(b)] \\ < \ & g. \end{aligned}$$

Hence $\deg(c) < g$ in this case, but $\deg(a) < \deg(c)$ does not necessarily hold.

Also note that in this case, if $\deg(a)$, $\deg(b)$, $\deg(c) < g$, then the matrix is automatically reduced. Indeed, the above equations show that

$$\deg(a) + \deg(c) = \deg(b^2 - \Gamma b - \Delta) = g + \deg(b).$$

Hence $\deg(b) = \deg(a) + \deg(c) - g < \min\{\deg(a), \deg(c)\}$ since both $\deg(a)$ and $\deg(c)$ are less than g.

3.2 Equivalence of (almost) reduced matrices

It is possible for two (almost) reduced matrices to be equivalent. We now investigate under which circumstances this is the case.

For the remainder of the section, let

$$\begin{bmatrix} b' & -c' \\ a' & \Gamma - b' \end{bmatrix} = \begin{bmatrix} x & w \\ y & z \end{bmatrix}^{-1} \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix} \begin{bmatrix} x & w \\ y & z \end{bmatrix},$$

where matrices $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ and $A' = \begin{bmatrix} b' & -c' \\ a' & \Gamma - b' \end{bmatrix}$ are almost reduced, with $\deg(a') \leq \deg(a)$, and $\begin{bmatrix} x & w \\ y & z \end{bmatrix} \in \mathrm{SL}_2(\mathbb{F}_q[T])$. Multiplying out the right hand side, we get

$$\begin{aligned} a' &= ax^2 + (\Gamma - 2b)xy + cy^2, && (3.2) \\ b' &= b - (awx + (\Gamma - 2b)wy + cyz), && (3.3) \\ c' &= aw^2 + (\Gamma - 2b)wz + cz^2. && (3.4) \end{aligned}$$

If $\alpha \in \mathbb{F}_q^\times$, then

$$\begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}^{-1} \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix} \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix} = \begin{bmatrix} b & -\alpha^{-2}c \\ \alpha^2 a & \Gamma - b \end{bmatrix},$$

so we will consider a and a' to be equivalent if they are equal modulo $(\mathbb{F}_q^\times)^2$ (that is, we consider the matrix $S = \begin{bmatrix} x & w \\ y & z \end{bmatrix}$ to be an element of $\mathrm{PSL}_2(\mathbb{F}_q[T])$, the projective special linear group).

If $y = 0$, then $a' = ax^2$ which forces $x \in \mathbb{F}_q^\times$ and $\deg(a') = \deg(a)$. Then, if $w \neq 0$, we have that $\deg(b') = \deg(b - awx) = \deg(awx) \geq \deg(a) = \deg(a')$, contradicting that A' is reduced. Hence $w = 0$ and so $A' = A$. In the sequel we may assume that $y \neq 0$. We will treat the four cases in Proposition 4 separately.

Case: d is odd and $d > 2g$.

From Remark 1 it follows that in this case, $\deg(b) < \deg(a) \leq \frac{1}{2}d \leq \deg(c)$ and in fact, all three inequalities are strict since d is odd. Note also that

$$\deg(\Gamma - 2b) \leq \max\{g, \deg(b)\} \leq \max\{g, \deg(a)\} < \tfrac{1}{2}d.$$

Since we are assuming that $y \neq 0$, $\deg(cy^2) \geq \deg(c) > \deg(a) \geq \deg(a')$. If $\deg(x) \leq \deg(y)$, then $\deg(ax^2) < \deg(cy^2)$ and

$$\deg((\Gamma - 2b)xy) < \tfrac{1}{2}d + \deg(x) + \deg(y) \leq \tfrac{1}{2}d + 2\deg(y) < \deg(cy^2)$$

which, using equation (3.2), leads to $\deg(a') = \deg(cy^2) > \deg(a)$, a contradiction. Thus we conclude that $\deg(x) > \deg(y)$.

To obtain equality in (3.2), at least two terms on the right hand side must have equal degree. However, since d is odd and $\deg(a) + \deg(c) = d$, we have that $\deg(ax^2)$ and $\deg(cy^2)$ have opposite parity. This means that we have one of the following situations:

$$\begin{aligned} \deg(ax^2) &= \deg((\Gamma - 2b)xy) > \deg(cy^2) \quad \text{or} \\ \deg(ax^2) &< \deg((\Gamma - 2b)xy) = \deg(cy^2). \end{aligned}$$

The former leads to

$$\begin{aligned} \deg(\Gamma - 2b) - \deg(a) &= \deg(x) - \deg(y) \text{ and} \\ \deg(x) - \deg(y) &> \deg(c) - \deg(\Gamma - 2b), \end{aligned}$$

which implies $\deg(\Gamma - 2b) > \frac{1}{2}d$ (since $\deg(a) + \deg(c) = d$), a contradiction. The latter leads to

$$\begin{aligned} \deg(c) - \deg(\Gamma - 2b) &= \deg(x) - \deg(y) \text{ and} \\ \deg(x) - \deg(y) &< \deg(\Gamma - 2b) - \deg(a), \end{aligned}$$

which also implies $\deg(\Gamma - 2b) > \frac{1}{2}d$. We conclude that in this case, no two reduced matrices are equivalent. Together with Proposition 5, this gives us

Theorem 6. *If* $\deg(\Delta)$ *is odd and* $\deg(\Delta) > 2\deg(\Gamma)$*, then every matrix solution to* (3.1) *is equivalent to a unique reduced matrix.*

Case: d is even, $d > 2g$ and $\operatorname{sgn}(\Delta)$ is not a square in $\mathbb{F}_q$.

As in the previous section, we have that $\deg(b) < \deg(a) \leq \frac{1}{2}d \leq \deg(c)$ and $\deg(\Gamma - 2b) < \frac{1}{2}d$. We first assume that $\deg(a) < \deg(c)$ (that is, the matrix A is reduced) or that $\deg(x) > 0$. As before, to obtain equality in (3.2), at least two terms on the right hand side must have equal degree. If $\deg(ax^2) = \deg((\Gamma - 2b)xy)$, then $\deg(y) = \deg(a) + \deg(x) - \deg(\Gamma - 2b)$ and so

$$\begin{aligned} \deg(cy^2) &= \deg(c) + \deg(y) + (\deg(a) + \deg(x) - \deg(\Gamma - 2b)) \\ &= \deg(x) + \deg(y) + d - \deg(\Gamma - 2b) (\text{since } \deg(a) + \deg(c) = d) \\ &> \deg(x) + \deg(y) + \deg(\Gamma - 2b) (\text{since } \deg(\Gamma - 2b) < \tfrac{1}{2}d) \\ &= \deg((\Gamma - 2b)xy), \end{aligned}$$

a contradiction.

Similarly, $\deg(cy^2) = \deg((\Gamma - 2b)xy)$ leads to $\deg(ax^2) > \deg((\Gamma - 2b)xy)$. Hence we must have that $\deg(ax^2) = \deg(cy^2) > \deg((\Gamma - 2b)xy)$ and that $\operatorname{sgn}(ax^2) + \operatorname{sgn}(cy^2) = 0$ which is equivalent to $\operatorname{sgn}(ac) = -(\frac{\operatorname{sgn}(ax)}{\operatorname{sgn}(y)})^2$. However, from the equation $ac = b^2 - \Gamma b - \Delta$ and $d > 2g$, we see that $\operatorname{sgn}(ac) = -\operatorname{sgn}(\Delta)$, which then implies that $\operatorname{sgn}(\Delta) = (\frac{\operatorname{sgn}(ax)}{\operatorname{sgn}(y)})^2$, contradicting that $\operatorname{sgn}(\Delta)$ is not a square in $\mathbb{F}_q$. This shows that no reduced matrix is equivalent to another reduced matrix, or an almost reduced matrix.

The case when $\deg(a) = \deg(c) = \frac{1}{2}d$ (that is, A is almost reduced) and $x \in \mathbb{F}_q$ remains. In this case $y \in \mathbb{F}_q$ is forced. From $xz - wy = 1$ we deduce that $\deg(w) = \deg(z)$, and since $\deg(a) = \deg(c) = \frac{1}{2}\, d$, it follows that $\deg(a') = \frac{1}{2}d$ and so $\deg(c') = \frac{1}{2}d$. We may now apply the above argument using equation (3.4) to show that $w, z \in \mathbb{F}_q$. From this, w and z are uniquely determined. Indeed, equations (3.2) and (3.3) imply $b'x + a'w = bx - cy$ and so $w = \frac{-\operatorname{sgn}(c)y}{\operatorname{sgn}(a')}$ (since $\deg(bx - b'x) < \deg(c)$). Using (3.2), this simplifies to (recalling that $b^2 - \Gamma b - \Delta = ac$, so $\operatorname{sgn}(ac) = -\operatorname{sgn}(\Delta)$)

$$w = \frac{\operatorname{sgn}(\Delta)y}{(\operatorname{sgn}(a)x)^2 - \operatorname{sgn}(\Delta)y^2}$$

and $z = \frac{1+wy}{x} = \frac{\operatorname{sgn}(a)^2 x}{(\operatorname{sgn}(a)x)^2 - \operatorname{sgn}(\Delta)y^2}$ now follows from $xz - wy = 1$. (Note that w is well-defined since $(\operatorname{sgn}(a)x)^2 - \operatorname{sgn}(\Delta)y^2 \neq 0$ unless $x = y = 0$.)

Therefore, there are $q^2 - 1$ matrices S such that $S^{-1}AS$ is again almost reduced, namely

$$S \in \left\{ \begin{bmatrix} x & \frac{\operatorname{sgn}(\Delta)y}{\tau} \\ y & \frac{\operatorname{sgn}(a)^2 x}{\tau} \end{bmatrix} : \quad (x, y) \in \mathbb{F}_q \times \mathbb{F}_q - (0, 0),\ \tau = (\operatorname{sgn}(a)x)^2 - \operatorname{sgn}(\Delta)y^2 \right\}.$$

Not all of them result in distinct matrices, however. Since we are considering equations modulo $(\mathbb{F}_q^\times)^2$, we may mod out the action on this set of $q^2 - 1$ matrices by the set of $q - 1$ matrices of the form $\begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}$ which leaves us with $\frac{q^2-1}{q-1} = q + 1$ possibilities (effectively, we work with the same set as above, where the matrices are considered to be in $\mathrm{PSL}_2(\mathbb{F}_q)$). We now investigate when these $q + 1$ possible matrices $S^{-1}AS$ are not distinct. It suffices to find S for which $S^{-1}AS = A$ and $y \neq 0$.

Now, if $S^{-1}AS = A$, then $x \times (3.4) + w \times (3.3)$ yields

$$(\Gamma - 2b)w + c(z - x) = 0.$$

Since $\deg(\Gamma - 2b) < \frac{d}{2} = \deg(c)$, we find that $x = z$ and $(\Gamma - 2b)w = 0$. Since we're assuming that $y \neq 0$, it follows that $w \neq 0$ and $\Gamma = 2b$. Substituting this back into (3.2), we find that $c = \frac{1-x^2}{y^2}a$. But then we have

$$\Delta = b^2 - \Gamma b - ac = -\frac{1}{4}\Gamma^2 + \frac{x^2-1}{y^2}a^2,$$

and so

$$\Gamma^2 + 4\Delta = (x^2-1)\left(\frac{2a}{y}\right)^2.$$

(Note that we may divide by two, since the hypothesis "$\deg(\Delta)$ is not a square in $\mathbb{F}_q$" implies that the characteristic is odd). So $x^2 - 1$ must be nonsquare, and also, since $\operatorname{sgn}(c) = -\frac{\operatorname{sgn}(\Delta)}{\operatorname{sgn}(a)}$, we see that $\frac{x^2-1}{y^2} = \frac{\operatorname{sgn}(\Delta)}{\operatorname{sgn}(a)^2}$.

Thus, A is of the form $\begin{bmatrix} \frac{1}{2}\Gamma & \frac{\operatorname{sgn}(\Delta)}{\operatorname{sgn}(a)^2}a \\ a & \frac{1}{2}\Gamma \end{bmatrix}$. Substituting back into equations (3.2)-(3.4), we find that any almost reduced matrix equivalent to A must take the form $\begin{bmatrix} \frac{1}{2}\Gamma & \frac{\operatorname{sgn}(\Delta)}{\beta\operatorname{sgn}(a)^2}a \\ \beta a & \frac{1}{2}\Gamma \end{bmatrix}$, where $\beta \in \mathbb{F}_q^\times$. Hence the only almost reduced matrices equivalent to A are A itself and $\begin{bmatrix} \frac{1}{2}\Gamma & \frac{a}{\operatorname{sgn}(a)^2} \\ \operatorname{sgn}(\Delta)a & \frac{1}{2}\Gamma \end{bmatrix}$ (where we choose $\beta = \operatorname{sgn}(\Delta)$ to be non-square).

Case: $d = 2g$ and $\operatorname{sgn}(\Delta)$ is not of the form $\alpha^2 - \alpha$, $\alpha \in \mathbb{F}_q$.

A similar argument as in the previous section shows that no two reduced matrices are equivalent, and an almost identical argument shows that there are $q+1$ almost reduced matrices equivalent to any given almost reduced matrix, unless the matrix is of the form $\begin{bmatrix} b & \frac{\operatorname{sgn}(\Delta)}{\operatorname{sgn}(a)^2}a \\ a & b + \frac{a}{\operatorname{sgn}(a)} \end{bmatrix}$. In this case the only almost reduced matrices equivalent to A are A itself and $\begin{bmatrix} b & \frac{\operatorname{sgn}(\Delta)}{\tau\operatorname{sgn}(a)^2}a \\ \tau a & b + \frac{a}{\operatorname{sgn}(a)} \end{bmatrix}$, where τ is a non-square element of $\mathbb{F}_q$.

The above arguments, together with Proposition 5 give us

Theorem 7. *If* $\deg(\Delta)$ *is even, and either* $\deg(\Delta) > 2\deg(\Gamma)$ *and* $\operatorname{sgn}(\Delta)$ *is not a square in* $\mathbb{F}_q$*, or* $\deg(\Delta) = 2\deg(\Gamma)$ *and* $\operatorname{sgn}(\Delta)$ *is not of the form* $\alpha^2 - \alpha$, $\alpha \in \mathbb{F}_q$*, then every matrix solution to* (3.1) *is either equivalent to a unique reduced matrix, or to a set of* $q+1$ *equivalent almost reduced matrices, except when said solution takes one of the following forms:*

- $\begin{bmatrix} \frac{1}{2}\Gamma & \frac{\operatorname{sgn}(\Delta)}{\operatorname{sgn}(a)^2}a \\ a & \frac{1}{2}\Gamma \end{bmatrix}$ *if* $\deg(\Delta) > 2\deg(\Gamma)$, *or*
- $\begin{bmatrix} b & \frac{\operatorname{sgn}(\Delta)}{\operatorname{sgn}(a)^2}a \\ a & b + \frac{a}{\operatorname{sgn}(a)} \end{bmatrix}$ *if* $\deg(\Delta) = 2\deg(\Gamma)$.

Case: $d < g$.

First note that if A is an almost reduced matrix, then adapting Remark 1 we can show that $\deg(c) = \deg(b) < \deg(a) < g$. Applying Step 2 of Proposition 5 to the matrix A will yield a reduced matrix equivalent to A, so we may disregard almost reduced matrices in this section.

To determine which reduced matrices are equivalent, we need to determine when the expression $ax^2 + (\Gamma - 2b)xy + cy^2$ has degree less than g (such that $\deg(a') < g$ in equation (3.2)). We first look at this expression when $y = 1$.

Proposition 8. *If* $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ *is a reduced matrix solution to* (3.1)*, then the expression* $ax^2 + (\Gamma - 2b)x + c$ *has degree less than* g *for exactly two distinct values of* x.

Proof. Since $\deg(c) < g$, a necessary and sufficient condition for the degree of $ax^2 + (\Gamma - 2b)x + c$ to be less than g is $\deg(ax^2 + (\Gamma - 2b)x) < g$. So we need to find x such that $x(ax + \Gamma - 2b)$ has degree less than g. One solution is clearly $x = 0$, so suppose that $x \neq 0$.

Now, unless $\deg(ax) = \deg(\Gamma - 2b) = g$, we have that $\deg(x(\Gamma - 2b + ax)) \geq \deg(\Gamma - 2b + ax) \geq g$, so we may assume that $\deg(x) = g - \deg(a)$. If $r = \Gamma - 2b + ax$, we have that

$$\deg(x(\Gamma - 2b + ax)) = \deg(xr) = \deg(x) + \deg(r) = g + \deg(r) - \deg(a).$$

For this to be less than g, it is necessary that $\deg(r) < \deg(a)$. Since $\deg(a) < g = \deg(\Gamma - 2b)$, there exist unique non-zero x and r with $\deg(r) < \deg(a)$ such that $\Gamma - 2b = -ax + r$. Then, since $\deg(x) = g - \deg(a)$ and $\deg(r) < \deg(a)$,

$$\deg(x(ax + \Gamma - 2b)) = \deg(xr) = g - \deg(a) + \deg(r) < g.$$

□

We now define a mapping on the (finite) set of reduced matrices.

Define the mapping ϕ to map the reduced matrix $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ to the matrix $S^{-1}AS$, where $S = \begin{bmatrix} x & -1 \\ 1 & 0 \end{bmatrix}$ and x is the unique non-zero polynomial from Proposition 8. Using the same notation as in Proposition 8 (that is, $\Gamma - 2b = -ax + r$ where $x \neq 0$ and $\deg(r) < \deg(a)$), we have

$$\phi(A) = \begin{bmatrix} b + r & -a \\ ax^2 + (\Gamma - 2b)x + c & \Gamma - b - r \end{bmatrix}.$$

We claim that this matrix is reduced. Indeed, we have that $\deg(a) < g$ and by construction, $\deg(ax^2 + (\Gamma - 2b)x + c) < g$. Remark 1, together with

$$\deg(b + r) \leq \max\{\deg(b), \deg(r)\} < \deg(a) < g$$

now imply that the matrix is reduced.

We now show that the mapping is injective. Suppose that there is a matrix B such that $\phi(B) = \phi(A)$. If $\phi(B) = R^{-1}BR$ with $R = \begin{bmatrix} y & -1 \\ 1 & 0 \end{bmatrix}$, then it follows that

$$B = RS^{-1}ASR^{-1} = \begin{bmatrix} b + ay - ax & -C \\ a & \Gamma - b - ay + ax \end{bmatrix}$$

for some C. Since B is reduced, it follows that $\deg(b + ay - ax) < \deg(a)$ which is only possible if $x = y$, in which case $A = B$. This shows that ϕ is an injective mapping on the finite set of reduced matrices, hence bijective. The inverse of ϕ is the mapping which sends $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ to the matrix $S^{-1}AS$ where $S = \begin{bmatrix} 0 & -1 \\ 1 & x' \end{bmatrix}$ and x' is the unique non-zero polynomial such that $\deg(\Gamma - 2b - cx') < \deg(c)$.

Since ϕ is injective, it induces a permutation on the set of reduced matrices. Writing the permutation in disjoint cycle notation, we see that all the matrices in each cycle are equivalent. It remains to show that all equivalent reduced matrices lie in the same cycle.

Theorem 9. *If* $\deg(\Delta) < \deg(\Gamma)$*, two reduced matrix solutions to* (3.1) *are equivalent if and only if* $B = \phi^k(A)$ *for some integer* k*.*

Proof. Let $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$, $B = \begin{bmatrix} b' & -c' \\ a' & \Gamma - b' \end{bmatrix}$ and let S be a matrix $\begin{bmatrix} x & w \\ y & z \end{bmatrix}$ with $xz - wy = 1$ such that $B = S^{-1}AS$. First assume that $\deg(y) \leq \deg(x)$. As in the comments following equation (3.4) (page 13), $y = 0$ quickly leads to $A = B$ (that is, $k = 0$), so we may assume that $y \neq 0$.

We wish to apply ϕ to the matrix A. Hence we need to find a non-zero polynomial X such that $\deg(aX^2 + (\Gamma - 2b)X + c) < g$. Since $\deg(y) \leq \deg(x)$, we can write $x = x_1 y - Y_1$ with $\deg(Y_1) < \deg(y)$ and x_1 non-zero. We claim that $X = x_1$ will suffice. Indeed,

$$\begin{aligned} & ax_1^2 + (\Gamma - 2b)x_1 + c \\ = \; & a\left(\frac{x + Y_1}{y}\right)^2 + (\Gamma - 2b)\left(\frac{x + Y_1}{y}\right) + c \\ = \; & \frac{1}{y^2}\left[ax^2 + (\Gamma - 2b)xy + cy^2 + 2axY_1 + (\Gamma - 2b)yY_1 + aY_1^2\right] \\ = \; & \frac{1}{y^2}\left[a' + 2axY_1 + (\Gamma - 2b)yY_1 + aY_1^2\right]. \end{aligned}$$

Since $\deg(Y_1) < \deg(y)$ and $\deg(a) < \deg(\Gamma - 2b) = g$, we have that

$$\begin{aligned} & \deg(ax_1^2 + (\Gamma - 2b)x_1 + c) \\ \leq \; & \max\{\deg(a'), \deg(aY_1^2), \deg((\Gamma - 2b)yY_1), \deg(axY_1)\} - 2\deg(y) \\ < \; & \max\{g, g + 2\deg(y), g + 2\deg(y), \deg(ax) + \deg(y)\} - 2\deg(y) \\ = \; & \max\{g, \deg(a) + \deg(x) - \deg(y)\}. \end{aligned}$$

Now, since $\deg(y) \leq \deg(x)$ and $\deg(c) < g = \deg(\Gamma - 2b)$, we have that $\deg(cy^2) < \deg((\Gamma - 2b)xy)$. On the other hand, $ax^2 + (\Gamma - 2b)xy + cy^2$ has degree less than g, so we must have that $\deg(ax^2) = \deg((\Gamma - 2b)xy)$ which leads to $\deg(a) + \deg(x) - \deg(y) = \deg(\Gamma - 2b) = g$ which shows that $\deg(ax_1^2 + (\Gamma - 2b)x_1 + c) < g$.

Applying ϕ to A, we find that $B = S_1^{-1}\phi(A)S_1$, where

$$S_1 = \begin{bmatrix} x_1 & -1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} x & w \\ y & z \end{bmatrix} = \begin{bmatrix} y & z \\ x_1 y - x & x_1 z - w \end{bmatrix} = \begin{bmatrix} X_1 & W_1 \\ Y_1 & Z_1 \end{bmatrix}.$$

Note that $\deg(Y_1) < \deg(y) = \deg(X_1)$, so we may repeat the above process. After a finite number of steps, we obtain $B = S_k^{-1}\phi^k(A)S_k$ with $S_k = \begin{bmatrix} X_k & W_k \\ 0 & Z_k \end{bmatrix}$, which, as before, implies that $\phi^k(A) = B$.

If $\deg(y) > \deg(x)$ but $\deg(y) \leq \deg(z)$, we may exchange the roles of A and B in the above argument. Suppose now that $\deg(y) > \deg(x)$ and $\deg(y) > \deg(z)$. The equation $xz - wy = 1$ now shows that $\deg(w) < \deg(x)$ and $\deg(w) < \deg(z)$, so we have $\deg(w) < \deg(x) < \deg(y)$. By exchanging the roles of A and B if necessary, we may assume that $\deg(b') < \deg(b)$. Now, $w\times(3.3) + x\times(3.4)$ yields

$$a'w + b'x = bx - cy$$

which simplifies to $x(b - b') = a'w + cy$.

If $\deg(x(b-b')) < \deg(cy)$ this implies that $\deg(cy) = \deg(a'w)$, or $\deg(y) - \deg(w) = \deg(a') - \deg(c)$. On the other hand, looking at equation (3.2) and remembering that $\deg(y) > \deg(x)$, we must have that $\deg(cy^2) = \deg((\Gamma - 2b)xy$ which leads to $\deg(y) - \deg(x) = g - \deg(c) > \deg(a') - \deg(c) = \deg(y) - \deg(w)$, contradicting that $\deg(w) < \deg(x)$.

Hence we must have that $\deg(x(b - b')) \geq \deg(cy)$ which yields $\deg(y) - \deg(x) \leq \deg(b - b') - \deg(c) = \deg(b) - \deg(c) < 0$ (by Remark 1), a contradiction. Hence the case $\deg(x) < \deg(y)$ is impossible under the assumptions, and the result follows.

□

To summarize, we have

Theorem 10. *If* $\deg(\Delta) < \deg(\Gamma)$*, then every matrix solution to* (3.1) *is equivalent to the reduced matrices in a unique orbit of* ϕ*.*

3.3 Composition of matrices

Under some circumstances, we can define a binary operation on the equivalence classes of matrices that will make the set of equivalence classes of matrices into an Abelian group. The binary operation we will use is an adaptation of Dirichlet composition as described by Cox in [4, §3], which we will also refer to as Dirichlet composition. To define Dirichlet composition, we will first need the following propositions.

Proposition 11. *Let* $p_1, p_2, \ldots, p_n, q_1, q_2, \ldots, q_n$ *and* m *be polynomials over* $\mathbb{F}_q$ *such that* $\gcd(p_1, p_2, \ldots, p_n, m) = 1$*. Then the system of congruences*

$$p_i B \equiv q_i \mod m, \quad i = 1, 2, \ldots, n$$

has a unique solution modulo m if and only if

$$p_i q_j \equiv p_j q_i \mod m$$

for every $i, j = 1, 2, \ldots, n$.

Proof. If B is a solution, then for each i, j, we have $p_i B \equiv q_i \mod m$ and $p_j B \equiv q_j \mod m$. Hence we have

$$p_i q_j \equiv p_i(p_j B) \equiv p_j(p_i B) \equiv p_j q_i \mod m.$$

Conversely, suppose that $p_i q_j \equiv p_j q_i \mod m$ for every $i, j = 1, 2, \ldots, n$. Since $\gcd(p_1, p_2, \ldots, p_n, m) = 1$, there exist polynomials $c, c_1, c_2, \ldots, c_n$ such that $cm + \sum_{i=1}^{n} c_i p_i = 1$. If B is any solution to the system of congruences, then for each i, $c_i p_i B \equiv c_i q_i \mod m$, and summing all n congruences yields

$$\sum_{i=1}^{n} c_i q_i \equiv B \sum_{i=1}^{n} c_i p_i \equiv B \mod m,$$

so if a solution exists, it is unique. We show that $B = \sum_{i=1}^{n} c_i q_i$ is a solution. Indeed, for each j,

$$\begin{aligned} p_j B &= p_j \sum_{i=1}^{n} c_i q_i \\ &= \sum_{i=1}^{n} c_i p_j q_i \\ &\equiv \sum_{i=1}^{n} c_i p_i q_j \mod m \\ &= (1 - cm) q_j \\ &\equiv q_j \mod m. \end{aligned}$$

□

Proposition 12. *Let a_1, a_2, b_1, b_2 be elements of $\mathbb{F}_q[T]$ such that $\gcd(a_1, a_2, \Gamma - b_1 - b_2) = 1$ and $b_i^2 \equiv \Gamma b_i + \Delta \mod a_i$ for $i = 1, 2$. Then there exists a unique polynomial B modulo $a_1 a_2$ such that*

$$\begin{aligned} B &\equiv b_1 \mod a_1 \\ B &\equiv b_2 \mod a_2 \\ B^2 &\equiv \Gamma B + \Delta \mod a_1 a_2. \end{aligned} \tag{3.5}$$

Proof. We may combine the first two congruences to obtain

$$B^2 - (b_1 + b_2)B + b_1 b_2 = (B - b_1)(B - b_2) \equiv 0 \mod a_1 a_2.$$

The above system is thus equivalent to

$$\begin{aligned} a_2 B &\equiv a_2 b_1 \mod a_1 a_2 \\ a_1 B &\equiv a_1 b_2 \mod a_1 a_2 \\ (\Gamma - b_1 - b_2)B &\equiv -\Delta - b_1 b_2 \mod a_1 a_2. \end{aligned}$$

This system satisfies the conditions of Proposition 11, hence has a unique solution modulo $a_1 a_2$. □

We can now define Dirichlet composition of equivalence classes of matrices.

Definition 5. Let $A_1 = \begin{bmatrix} b_1 & -c_1 \\ a_1 & \Gamma - b_1 \end{bmatrix}$ and $A_2 = \begin{bmatrix} b_2 & -c_2 \\ a_2 & \Gamma - b_2 \end{bmatrix}$ be matrix solutions to (3.1) such that $\gcd(a_1, a_2, \Gamma - b_1 - b_2) = 1$. Then the *Dirichlet composition* of the equivalence classes containing the matrices A_1 and A_2, respectively, is the equivalence class containing the matrix

$$A_1 \circ A_2 = \begin{bmatrix} B & -c \\ a_1 a_2 & \Gamma - B \end{bmatrix}$$

where B is the element modulo $a_1 a_2$ from Proposition 12 with minimal degree, and

$$c = -\frac{B^2 - \Gamma B - \Delta}{a_1 a_2}.$$

For some choices of Γ and Δ, Dirichlet composition may not be well-defined (or defined at all!) on equivalence classes of matrices. A sufficient condition for Dirichlet composition to be well-defined is that in each equivalence class of matrices there is a matrix such that $\gcd(a, \Gamma - 2b, c) = 1$ (it will become clear later why this is the case). Note that if $\gcd(a, \Gamma - 2b, c) = 1$ for one matrix in a class, it holds for *all* matrices in the class.

In even characteristic it suffices that Γ is irreducible. To see why, consider the classes in which Γ divides both a and c. Then, if the class contains a reduced matrix, then $\deg(a) < \deg(\Gamma)$ which means that Γ cannot divide a, and if the matrix class contains an almost reduced matrix, then the condition

that Γ divides both a and c means that the reduced matrix must be of the form given in the statement of Theorem 7, in which case $\Gamma = 0$ is forced.

In odd characteristic it suffices that $\Gamma^2 + 4\Delta$ is squarefree. Indeed, if $\gcd(a, \Gamma - 2b, c) = d$, then d^2 divides

$$(\Gamma - 2b)^2 - 4ac = \Gamma^2 + 4(b^2 - \Gamma b - ac) = \Gamma^2 + 4\Delta.$$

To prove that Dirichlet composition is well-defined on classes of matrices is possible using Definition 5, but rather cumbersome, so we will defer the proof to section 4.1 (Proposition 18). For the remainder of the chapter we will assume that, in odd characteristic, $\Gamma^2 + 4\Delta$ is squarefree and that, in even characteristic, Γ is irreducible.

Proposition 13. *Dirichlet composition of equivalence classes is a commutative and associative binary operation.*

Proof. Commutativity is clear, so let $A_1 = \begin{bmatrix} b_1 & -c_1 \\ a_1 & \Gamma - b_1 \end{bmatrix}$, $A_2 = \begin{bmatrix} b_2 & -c_2 \\ a_2 & \Gamma - b_2 \end{bmatrix}$ and $A_3 = \begin{bmatrix} b_3 & -c_3 \\ a_3 & \Gamma - b_3 \end{bmatrix}$ be three matrices such that $\gcd(a_1, a_2, \Gamma - b_1 - b_2) = 1$ and $\gcd(a_1a_2, a_3, \Gamma - B - b_3) = 1$, where B is the unique element modulo a_1a_2 from Proposition 12 when composing A_1 and A_2. Then $(A_1 \circ A_2) \circ A_3$ is defined, and let C be the unique element modulo $a_1a_2a_3$ obtained from Proposition 12 when composing $(A_1 \circ A_2)$ and A_3. Hence we have the congruences

$$\begin{aligned} B &\equiv b_1 && \bmod a_1 \\ B &\equiv b_2 && \bmod a_2 \\ B^2 &\equiv \Gamma B + \Delta && \bmod a_1a_2 \\ C &\equiv b_3 && \bmod a_3 \\ C &\equiv B && \bmod a_1a_2 \\ C^2 &\equiv \Gamma C + \Delta && \bmod a_1a_2a_3. \end{aligned} \tag{3.6}$$

Now, if t is any common prime factor of a_3 and a_2, then $\gcd(a_1a_2, a_3, \Gamma - B - b_3) = 1$ implies that t does not divide $\Gamma - B - b_3$. But $B \equiv b_2 \mod a_2$, so t does not divide $\Gamma - b_2 - b_3$. Hence $\gcd(a_2, a_3, \Gamma - b_2 - b_3) = 1$ and the composition $A_2 \circ A_3$ is defined; let D be the unique element modulo a_2a_3 obtained from Proposition 12 when composing A_2 and A_3.

Now let t be any common prime divisor of a_1 and a_2a_3 and suppose that t divides a_2. Then $\gcd(a_1, a_2, \Gamma - b_1 - b_2) = 1$ implies that t does not divide

$\Gamma - b_1 - b_2$, and since $D \equiv b_2 \mod a_2$, it follows that t does not divide $\Gamma - b_1 - D$. Similarly, if t divides a_3, then $\gcd(a_1a_2, a_3, \Gamma - B - b_3) = 1$ implies that t does not divide $\Gamma - B - b_3$. Since $B \equiv b_1 \mod a_1$ and $b_3 \equiv D \mod a_3$, it follows that t does not divide $\Gamma - b_1 - D$. Therefore, $\gcd(a_1, a_2a_3, \Gamma - b_1 - D) = 1$ and hence $A_1 \circ (A_2 \circ A_3)$ is defined; let E be the unique element modulo $a_1a_2a_3$ obtained from Proposition 12 when composing A_1 and $A_2 \circ A_3$. We have the following congruences:

$$\begin{aligned} D &\equiv b_2 && \mod a_2 \\ D &\equiv b_3 && \mod a_3 \\ D^2 &\equiv \Gamma D + \Delta && \mod a_2a_3 \\ E &\equiv b_1 && \mod a_1 \\ E &\equiv D && \mod a_2a_3 \\ E^2 &\equiv \Gamma E + \Delta && \mod a_1a_2a_3. \end{aligned} \tag{3.7}$$

Comparing the twelve congruences in (3.6) and (3.7), we see that

$$\begin{aligned} E \equiv b_1 \equiv B \equiv C &\mod a_1 \\ E \equiv D \equiv b_3 \equiv C &\mod a_3 \\ E \equiv D \equiv b_2 \equiv B \equiv C &\mod a_2 \\ (E - C)(\Gamma - E - C) \equiv 0 &\mod a_1a_2a_3, \end{aligned}$$

the last congruence following from $E^2 - \Gamma E \equiv C^2 - \Gamma C \equiv \Delta \mod a_1a_2a_3$.

We wish to show that $E \equiv C \mod a_1a_2a_3$ (so that the two compositions $A_1 \circ (A_2 \circ A_3)$ and $(A_1 \circ A_2) \circ A_3$ are equal), so first suppose that, without loss of generality, $E \not\equiv C \mod a_1a_2$. Since $E \equiv C$ modulo a_1 and a_2, it follows that there is a common prime factor t of a_1 and a_2 such that t^k divides a_1a_2 and t^{k-1} divides $E - C$, but t^k does not divide $E - C$ for some positive integer $k \geq 2$. The last congruence above then implies that t divides $\Gamma - E - C$, and hence t divides $(\Gamma - E - C) + (E - C) = \Gamma - 2C$.

Now, in odd characteristic, since t divides both a_1 and a_2, it follows that t^2 divides $(\Gamma - 2C)^2 - 4a_1a_2K$ for any K, and in particular, t^2 divides $\Gamma^2 + 4\Delta$, a contradiction. Hence $E \equiv C \mod a_ia_j$ for $i \neq j$.

Finally suppose that $E \not\equiv C \mod a_1a_2a_3$. Applying the above argument but replacing a_2 with a_2a_3 again yields a contradiction, so we conclude that, in odd characteristic, $E \equiv C \mod a_1a_2a_3$, which is what we needed to prove.

Applying the above argument to even characteristic shows that if $E \not\equiv C \mod a_1a_2$ and t is a common prime factor of a_1 and a_2 such that t^k divides

a_1a_2 and t^{k-1} divides $E-C$, but t^k does not divide $E-C$ for some positive integer $k \geq 2$, then t divides $\Gamma - E - C$ and $\Gamma - 2C = \Gamma$ which implies that $\Gamma = t$ since Γ is irreducible. Hence Γ divides $E + C$. However, since Γ divides both a_1 and a_2, it follows that $E \equiv b_1 \equiv C \equiv b_2 \mod \Gamma$. Hence Γ divides $\Gamma - b_1 - b_2$, which contradicts $(a_1, a_2, \Gamma - b_1 - b_2) = 1$. The rest of the proof in this case continues as above.

We conclude that $E \equiv C \mod a_1a_2a_3$, and so Dirichlet composition is associative. □

This result now paves the way for the following:

Proposition 14. *If $\Gamma^2 + 4\Delta$ is squarefree (if q is odd) or Γ is irreducible (if q is even), then the set of equivalence classes of matrix solutions to* (3.1) *with Dirichlet composition is an Abelian group with identity element the class containing the matrix $\begin{bmatrix} 0 & \Delta \\ 1 & \Gamma \end{bmatrix}$ and the inverse of the class containing $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ is the class containing $A^o = \begin{bmatrix} b & -a \\ c & \Gamma - b \end{bmatrix}$.*

Proof. Let $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ be any reduced matrix solution to (3.1). To compose A with the matrix $\begin{bmatrix} 0 & \Delta \\ 1 & \Gamma \end{bmatrix}$, we first need to check that the conditions of Proposition 12 are satisfied. Clearly, $(a, 1, \Gamma - b) = 1$ and also $B = b$ satisfies the system of congruences of Proposition 12. Hence the composition of A with $\begin{bmatrix} 0 & \Delta \\ 1 & \Gamma \end{bmatrix}$ is equal to $\begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix} = A$.

To compose A with A^{o}, we note that $\gcd(a, c, \Gamma - 2b) = 1$ and that $B = b$ is a solution to the system of congruences in Proposition 12. The composition of A with A^{o} is the matrix $\begin{bmatrix} b & -1 \\ ac & \Gamma - b \end{bmatrix}$ (since $b^2 - \Gamma b - \Delta = ac$). This matrix is equivalent to

$$\begin{bmatrix} 0 & -1 \\ 1 & \Gamma - b \end{bmatrix}^{-1} \begin{bmatrix} b & -1 \\ ac & \Gamma - b \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & \Gamma - b \end{bmatrix} = \begin{bmatrix} 0 & \Delta \\ 1 & \Gamma \end{bmatrix}.$$

□

We call the matrix $\begin{bmatrix} 0 & \Delta \\ 1 & \Gamma \end{bmatrix}$ the *principal matrix*, the class containing this matrix the *principal class* and the ϕ-orbit of this matrix the *principal cycle*.

3.4 Additional results

We will need the following results in the next chapter.

Definition 6. Let $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$. We call the matrix $A^{\mathrm{o}} = \begin{bmatrix} b & -a \\ c & \Gamma - b \end{bmatrix}$ the *opposite* of A, the matrix $A^{\tau} = \begin{bmatrix} b & -\tau^{-1}c \\ \tau a & \Gamma - b \end{bmatrix}$, where τ is a non-square element of $\mathbb{F}_q$, the *twist* of A and the matrix $A^{\mathrm{o}\tau} = \begin{bmatrix} b & -\tau a \\ \tau^{-1}c & \Gamma - b \end{bmatrix}$ the *opposite twist* of A.

We also define the classes containing these matrices as the *opposite*, *twist* and *opposite twist* of the class containing A.

Note that the twist of the opposite of A is equivalent to the opposite of the twist of A, which is equal to the opposite twist of A. That is to say, $(A^{\mathrm{o}})^{\tau} \sim (A^{\tau})^{\mathrm{o}} = A^{\mathrm{o}\tau}$, where $\sim$ indicates equivalence. Also note that $(A^{\mathrm{o}})^{\mathrm{o}} = A$ and $(A^{\tau})^{\tau} \sim A$ and that the class containing A^{o} is the inverse of the class containing A in the group defined in Proposition 14.

In all the following propositions, it is assumed that the matrices are solutions to (3.1).

Proposition 15. *Let* $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ *be reduced and* $\deg(\Delta) < \deg(\Gamma)$. *Then*

1. *if B is the opposite of A, then $\phi^{-1}(B)$ is the opposite of $\phi(A)$;*
2. *if B is the twist of A, then $\phi(B)$ is the twist of $\phi(A)$;*
3. *if B is the opposite twist of A, then $\phi^{-1}(B)$ is the opposite twist of $\phi(A)$.*

In other words, $\phi^{-1}(A^{o}) = \phi(A)^{o}$, $\phi(A^{\tau}) = \phi(A)^{\tau}$ and $\phi^{-1}(A^{o\tau}) = \phi(A)^{o\tau}$.

Proof. Suppose that $\phi(A) = S^{-1}AS = \begin{bmatrix} ax+\Gamma-b & -a \\ ax^2+(\Gamma-2b)x+c & b-ax \end{bmatrix}$ where $S = \begin{bmatrix} x & -1 \\ 1 & 0 \end{bmatrix}$. We need to show that

$$\phi(\phi(A)^{\mathrm{o}}) = A^{\mathrm{o}}.$$

Now,

$$\phi(A)^{\mathrm{o}} = \begin{bmatrix} ax+\Gamma-b & -(ax^2+(\Gamma-2b)x+c) \\ a & b-ax \end{bmatrix}$$

and to apply ϕ to this matrix using the definition (the paragraph after Proposition 8),we need to find a polynomial y such that

$$\deg(a) > \deg(\Gamma - 2(ax+\Gamma-b)+ay) = \deg(\Gamma - 2b + a(2x-y)).$$

However, we know that $\deg(\Gamma-2b+ax) < \deg(a)$, and moreover, x is uniquely determined (as in the proof of Proposition 8). Hence $y = x$, and we can apply ϕ to $\phi(A)^{\mathrm{o}}$:

$$\begin{aligned} \phi(\phi(A)^{\mathrm{o}}) &= \begin{bmatrix} x & -1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} ax+\Gamma-b & -(ax^2+(\Gamma-2b)x+c) \\ a & b-ax \end{bmatrix} \begin{bmatrix} x & -1 \\ 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} b & -a \\ c & \Gamma-b \end{bmatrix} \\ &= A^{\mathrm{o}}. \end{aligned}$$

A similar, but simpler, argument as above shows that $\phi(A^\tau) = \phi(A)^\tau$, and then

$$\begin{aligned} \phi(\phi(A)^{\mathrm{o}\tau}) &= \phi(\phi(A^\tau)^{\mathrm{o}}) \quad \text{(by part 2)} \\ &= (A^\tau)^{\mathrm{o}} \quad \text{(by part 1)} \\ &= A^{\mathrm{o}\tau}. \end{aligned}$$

□

Since the principal class is its own inverse, we must have that the principal matrix is equivalent to its opposite. In fact, we have:

Proposition 16. *If C is the principal matrix, then $\phi(C) = C^o$.*

Proof. We use the definition of ϕ to calculate $\phi(C)$. Since 1 has degree 0, it follows that $x = -\Gamma$ and $r = 0$ as in the definition, and so

$$\phi(C) = \begin{bmatrix} -\Gamma & -1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 0 & \Delta \\ 1 & \Gamma \end{bmatrix} \begin{bmatrix} -\Gamma & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ -\Delta & \Gamma \end{bmatrix} = C^{\mathrm{o}}.$$

□

Proposition 17. *If there is a matrix A which is equivalent to its twist, then every matrix is equivalent to its twist.*

Proof. From the definition of Dirichlet composition it is clear that

$$(A^{\tau} \circ B) = (A \circ B^{\tau}) = (A \circ B)^{\tau}.$$

Hence if $A \sim A^{\tau}$ and B is any matrix, then

$$B^{\tau} \sim (A \circ (A^{\mathrm{o}} \circ B))^{\tau} = A^{\tau} \circ (A^{\mathrm{o}} \circ B) \sim A \circ (A^{\mathrm{o}} \circ B) \sim B,$$

so B is equivalent to its twist. □

If a matrix A and its twist lie in the same cycle, suppose that $A^{\tau} = \phi^k(A)$ for some integer k. Then applying Proposition 15, we find that $\phi^k(A^{\tau}) = \phi^k(A)^{\tau} = (A^{\tau})^{\tau} = A$, hence $\phi^{2k}(A) = A$ and the cycle has even length, with A and A^{τ} lying at opposite ends of the cycle.

3.5 The connection to binary quadratic forms

In many of the proofs above, we made extensive use of the quadratic forms $ax^2 + (\Gamma - 2b)xy + cy^2$. This is no accident, since if q is odd, then there is a bijection between the set of matrix solutions to (3.1) and binary quadratic forms over $\mathbb{F}_q[T]$ with discriminant $\Gamma^2 + 4\Delta$. The correspondence is given by

$$\begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix} \longleftrightarrow [-y, x] \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = ax^2 + (\Gamma - 2b)xy + cy^2.$$

This bijection can be used to define equivalence classes of binary quadratic forms, develop reduction theory, calculate equivalence classes and define a binary operation that makes the set of equivalence classes of binary quadratic forms into a group.

González develops the theory of binary quadratic forms over $\mathbb{F}_q[T]$ in [7] and his results in binary quadratic forms mirror the results of this chapter under the above correspondence. González uses continued fractions to study the equivalent of the $d < g$ case in this chapter, with his continued fraction cycles closely correlating with the ϕ-orbits of reduced matrices in this chapter.

Lastly, Yu develops a more general notion of binary quadratic forms over $\mathbb{F}_q[T]$ in [13] and introduces oriented quadratic spaces, which correlates with the directed ideals used in this dissertation, under the mapping above and that of Latimer and MacDuffee.

Yu defines a correspondence between classes of binary quadratic forms and classes of lattices, which he then exploits, using Drinfeld modules, to derive a class number formula.

Chapter 4

Equivalence classes of ideals

If we apply the Latimer-MacDuffee Theorem (Theorem 1) to the irreducible polynomial $f(X) = X^2 - \Gamma X - \Delta$, we see that there is a bijection between equivalence classes of matrix solutions to (3.1) and equivalence classes of directed ideals of $\mathbb{F}_q[T][\alpha]$, where α is a root of $f(X)$. The proof of the Latimer-MacDuffee theorem in the irreducible case shows how to make this correspondence explicit.

Consider the the matrix $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$. Since α is an eigevalue of A, we find that an associated eigenvector is

$$\mathbf{w}_\alpha = \begin{bmatrix} b - \Gamma + \alpha \\ a \end{bmatrix} = \begin{bmatrix} b - \Gamma & 1 \\ a & 0 \end{bmatrix} \begin{bmatrix} 1 \\ \alpha \end{bmatrix}.$$

We find that the matrix $\begin{bmatrix} \Gamma - b & -1 \\ -a & 0 \end{bmatrix}$ is the matrix G as in the proof of Proposition 3 (recall that G is the matrix over $\mathbb{F}_q[T]$ such that $\mathbf{w}_\alpha = G\mathbf{e}$, where in this case, $\mathbf{e} = [1, \alpha]^{tr}$, the entries of which forms a basis for the ring $\mathbb{F}_q[T][\alpha]$ over $\mathbb{F}_q[T]$). Then $\operatorname{sgn}(\det(G)) = -\operatorname{sgn}(a)$, and so we associate, taking in consideration the comment at the end of the proof of Proposition 3 with $c = -1$, the class of matrices containing A to the ideal class containing the directed ideal $(\langle a, b - \Gamma + \alpha \rangle, \operatorname{sgn}(a))$.

4.1 The directed ideal class group

.

If $\Gamma^2 + 4\Delta$ is square-free (in odd characteristic) or Γ is irreducible (in even characteristic), we can make the set of directed ideal classes into an Abelian group using the composition

$$(\mathfrak{A}, \sigma_1) \circ (\mathfrak{B}, \sigma_2) = (\mathfrak{A}\mathfrak{B}, \sigma_1\sigma_2). \tag{4.1}$$

The conditions $\Gamma^2 + 4\Delta$ is square-free (in odd characteristic) or Γ is irreducible (in even characteristic) imply that $\mathbb{F}_q[T][\alpha]$ is a Dedekind domain (that is, $\mathbb{F}_q[T][\alpha]$ is integrally closed), and one can always make the set of directed ideals into an Abelian group if $\mathbb{F}_q[T][\alpha]$ is a Dedekind domain. In the odd characteristic case, $\Gamma^2 + 4\Delta$ is squarefree if and only if $\mathbb{F}_q[T][\alpha]$ is a Dedekind domain, but in the even characteristic case it need not be true that Γ is irreducible if $\mathbb{F}_q[T][\alpha]$ is a Dedekind domain. Either way, the assumptions imply that every directed ideal class contains a directed ideal $(\langle a, b - \Gamma + \alpha\rangle, \mathrm{sgn}(a))$ such that $\gcd(a, \Gamma - 2b, c) = 1$, where $b^2 - \Gamma b - \Delta = ac$ (see the discussion directly after Definition 5).

Proposition 18. *The set of ideal classes together with the above composition is an Abelian group with identity element the class containing* $(\langle 1, \alpha\rangle, 1)$ *and the inverse of the class containing* $(\langle a, b - \Gamma + \alpha\rangle, \sigma)$ *is the class containing* $(\langle a, b - \alpha\rangle, \sigma)$.

Proof. The composition as defined above is clearly commutative and associative, but we need to show that it is indeed well-defined on ideal classes.

Let $(\mathfrak{A}_1, \sigma_1)$ and $(\mathfrak{B}_1, \tau_1)$ be two directed ideals, equivalent to $(\mathfrak{A}_2, \sigma_2)$ and $(\mathfrak{B}_2, \tau_2)$ respectively. Then there exist $a_1, b_1, a_2, b_2 \in \mathbb{F}_q[T][\alpha]$ such that

$$\begin{aligned} a_1\mathfrak{A}_1 &= a_2\mathfrak{A}_2, & \mathrm{sgn}(N(a_1))\sigma_1 &= \mathrm{sgn}(N(a_2))\sigma_1 \\ b_1\mathfrak{B}_1 &= b_2\mathfrak{B}_2, & \mathrm{sgn}(N(b_1))\tau_1 &= \mathrm{sgn}(N(b_2))\tau_2. \end{aligned}$$

Then $(\mathfrak{A}_1, \sigma_1) \circ (\mathfrak{B}_1, \tau_1) = (\mathfrak{A}_1\mathfrak{B}_1, \sigma_1\tau_1)$, $(\mathfrak{A}_2, \sigma_2) \circ (\mathfrak{B}_2, \tau_2) = (\mathfrak{A}_2\mathfrak{B}_2, \sigma_2\tau_2)$ and

$$\begin{aligned} a_1b_1\mathfrak{A}_1\mathfrak{B}_1 &= a_2b_2\mathfrak{A}_2\mathfrak{B}_2 \quad \text{with} \\ \mathrm{sgn}(N(a_1b_1))\sigma_1\tau_1 &= \mathrm{sgn}(N(a_2b_2))\sigma_2\tau_2, \end{aligned}$$

since $\mathrm{sgn}(xy) = \mathrm{sgn}(x)\,\mathrm{sgn}(y)$ and $N(xy) = N(x)N(y)$. Hence $(\mathfrak{A}_1\mathfrak{B}_1, \sigma_1\tau_1)$ and $(\mathfrak{A}_2\mathfrak{B}_2, \sigma_2\tau_2)$ are equivalent, so the composition is well-defined on ideal classes.

The directed ideal $(\langle 1, \alpha\rangle, 1) = (\mathbb{F}_q[T][\alpha], 1)$ clearly acts as the identity element, so we need to prove the assertion about inverses. Now,

$$\begin{aligned}
& \langle a, b-\Gamma+\alpha\rangle\langle a, b-\alpha\rangle \\
= \; & \langle a^2, a(b-\alpha), a(b+\alpha-\Gamma), (b-\alpha)(b+\alpha-\Gamma)\rangle \\
= \; & \langle a^2, a(b-\alpha), a(\Gamma-2b), b^2-\alpha^2-\Gamma b+\Gamma\alpha\rangle \\
= \; & \langle a^2, a(b-\alpha), a(\Gamma-2b), b^2-\Gamma b-\Delta\rangle \\
= \; & \langle a^2, a(b-\alpha), a(\Gamma-2b), ac\rangle \\
= \; & a\langle a, c, \Gamma-2b, b-\alpha\rangle \\
= \; & a\langle 1, b-\alpha\rangle \quad (\text{since } (a, c, \Gamma-2b) = 1) \\
= \; & a\langle 1, \alpha\rangle.
\end{aligned}$$

Thus, $(\langle a, b-\Gamma+\alpha\rangle, \sigma) \circ (\langle a, b-\alpha\rangle, \sigma) = (a\langle 1, \alpha\rangle, \sigma^2)$ which is equivalent to $(\langle 1, \alpha\rangle, 1)$ since $a \in \mathbb{F}_q[T]$ and so $\operatorname{sgn}(N(a)) = \operatorname{sgn}(a^2) = \operatorname{sgn}(a)^2$.

□

The bijection described by the Latimer-MacDuffee theorem now induces a group structure on the set of equivalence classes of matrices. We now show that this group structure and the group structure obtained with Dirichlet composition are the same. It will be enough to show that the binary operation induced on the set of ideal classes by Dirichlet composition is the same as the binary operation (4.1).

Proposition 19. *Dirichlet composition of equivalence classes of matrices induces composition of directed ideals.*

Proof. We adapt the proof set out in [4, §7]. Let $A_1 = \begin{bmatrix} b_1 & -c_1 \\ a_1 & \Gamma - a_1 \end{bmatrix}$ and $A_2 = \begin{bmatrix} b_2 & -c_2 \\ a_2 & \Gamma - a_2 \end{bmatrix}$ with composition $A = \begin{bmatrix} B & -c \\ a_1a_2 & \Gamma - B \end{bmatrix}$ (note that this implies that $\gcd(a_1, a_2, \Gamma - b_1 - b_2) = 1$). Under the correspondence, the classes containing these matrices are associated with the classes containing the ideals

$$(\langle a_1, b_1-\Gamma+\alpha\rangle, \operatorname{sgn}(a_1)), (\langle a_2, b_2-\Gamma+\alpha\rangle, \operatorname{sgn}(a_2)), (\langle a_1a_2, B-\Gamma+\alpha\rangle, \operatorname{sgn}(a_1a_2)),$$

respectively. From the system of congruences (3.5) we see that $B \equiv b_1 \mod a_1$ and $B \equiv b_2 \mod a_2$, so the three directed ideals are equal to

$$(\langle a_1, D\rangle, \mathrm{sgn}(a_1)), (\langle a_2, D\rangle, \mathrm{sgn}(a_2)),\ (\langle a_1 a_2, D\rangle, \mathrm{sgn}(a_1 a_2)),$$

where $D = B - \Gamma + \alpha$. Observe that

$$\begin{aligned} & D^2 + D(\Gamma - 2B) \\ = \ & (B - \Gamma + \alpha)^2 + (B - \Gamma + \alpha)(\Gamma - 2B) \\ = \ & (\alpha + B - \Gamma)(\alpha - B) \\ = \ & \alpha^2 - \Gamma\alpha - (B^2 - \Gamma B) \\ \equiv \ & \alpha^2 - \Gamma\alpha - \Delta \mod a_1 a_2 \quad \text{(from (3.5))} \\ = \ & 0. \end{aligned}$$

Also, if d is a common divisor of a_1 and a_2, then the first two congruences in 3.5 imply that d divides $2B - b_1 - b_2 = (2B - \Gamma) + (\Gamma - b_1 - b_2)$. Since d is relatively prime to $\Gamma - b_1 - b_2$, it follows that d is relatively prime to $\Gamma - 2B$ as well. Hence

$$\begin{aligned} \langle a_1, D\rangle\langle a_2, D\rangle &= \langle a_1 a_2, a_1 D, a_2 D, D^2\rangle \\ &= \langle a_1 a_2, a_1 D, a_2 D, (\Gamma - 2B)D\rangle \\ &= \langle a_1 a_2, D\rangle \quad (\text{since } \gcd(a_1, a_2, \Gamma - 2B) = 1) \end{aligned}$$

and so

$$(\langle a_1, D\rangle, \mathrm{sgn}(a_1)) \circ (\langle a_2, D\rangle, \mathrm{sgn}(a_2)) = (\langle a_1 a_2, D\rangle, \mathrm{sgn}(a_1 a_2)),$$

as required. □

Definition 7. The Abelian group defined above is called the *directed ideal class group*, denoted by $\overrightarrow{\mathscr{C}}(\Gamma, \Delta)$. The order $\overrightarrow{h}(\Gamma, \Delta)$ of this group is called the *directed class number*.

Note that if Γ_1 and Δ_1 are polynomials such that $\Gamma_1^2 + 4\Delta_1 = \Gamma^2 + 4\Delta$ and $f(X) = X^2 - \Gamma_1 X - \Delta_1$ (in odd characteristic), then

$$\begin{aligned} f\left(X - \frac{\Gamma - \Gamma_1}{2}\right) &= \left(X - \frac{\Gamma - \Gamma_1}{2}\right)^2 - \Gamma_1\left(X - \frac{\Gamma - \Gamma_1}{2}\right) - \Delta_1 \\ &= X^2 - \Gamma X - \left(\Delta_1 - \Gamma_1\left(\frac{\Gamma - \Gamma_1}{2}\right) - \left(\frac{\Gamma - \Gamma_1}{2}\right)^2\right) \\ &= X^2 - \Gamma X - \tfrac{1}{4}\left(4\Delta_1 - (\Gamma^2 - \Gamma_1^2)\right) \\ &= X^2 - \Gamma X - \Delta. \end{aligned}$$

Hence $\overrightarrow{\mathscr{C}}(\Gamma,\Delta) \cong \overrightarrow{\mathscr{C}}(\Gamma_1,\Delta_1)$ (this follows from the discussion in the first paragrph on page 9), and we may speak of $\overrightarrow{\mathscr{C}}(\Gamma^2+4\Delta)$.

The relationship between the directed ideal class group and the classical ideal class group $\mathscr{C}(\Gamma,\Delta)$ is given by the following proposition.

Proposition 20. *If there exists a unit in $\mathbb{F}_q[T][\alpha]$ with non-square norm, then $\overrightarrow{\mathscr{C}}(\Gamma,\Delta) \cong \mathscr{C}(\Gamma,\Delta)$. If no such unit exists, then $\mathscr{C}(\Gamma,\Delta)$ is isomorphic to a subgroup of $\overrightarrow{\mathscr{C}}(\Gamma,\Delta)$ of index 2.*

Proof. If ϵ is a unit with nonsquare norm, then the directed ideal $(\mathfrak{A},1)$ is equivalent to the ideal $(\epsilon\mathfrak{A}, N(\epsilon)) = (\mathfrak{A}, N(\epsilon))$. Since $\mathbb{F}_q/\mathbb{F}_q^\times \cong \mathbb{Z}_2$, it follows that the group of directed ideals is isomorphic to the classical ideal class group.

If no such unit ϵ exists, then $(\mathfrak{A},1)$ and $(\mathfrak{A},\tau)$, where τ is a non-square element of $\mathbb{F}_q$, lie in different classes. Indeed, if $(\mathfrak{A},1) \sim (\mathfrak{A},\tau)$ for some ideal A, then there exists a matrix A such that A is equivalent to its twist. Then Proposition 17 implies that the principal class is equivalent to its twist. Equation (3.2) then shows that there exist elements x and y such that $x^2 + \Gamma xy - \Delta y^2 = \tau$, where τ is a non-square element of $\mathbb{F}_q$. Thus

$$\begin{aligned} N(x+\alpha y) &= (x+\alpha y)(x+\overline{\alpha}y) \\ &= x^2 + xy(\alpha+\overline{\alpha}) + \alpha\overline{\alpha}y^2 \\ &= x^2 + \Gamma xy - \Delta y^2 \\ &= \tau \end{aligned}$$

and so $x+\alpha y$ is a unit with non-square norm, a contradiction.

Alternatively, if $(\mathfrak{A},1) \sim (\mathfrak{A},\tau)$, then there exist $a, b \in \mathbb{F}_q[T][\alpha]$ such that $a\mathfrak{A} = b\mathfrak{A}$ and $\operatorname{sgn}(N(a)) = \tau \operatorname{sgn}(N(b))$. However, $a\mathfrak{A} = b\mathfrak{A}$ implies that there is a unit ϵ such that $a = \epsilon b$, and so

$$\operatorname{sgn}(N(a)) = \operatorname{sgn}(N(\epsilon b)) = \operatorname{sgn}(N(\epsilon))\operatorname{sgn}(N(b)) = N(\epsilon)\operatorname{sgn}(N(b)),$$

which, together with $\operatorname{sgn}(N(a)) = \tau\operatorname{sgn}(N(b))$ imply that $N(\epsilon)$ is non-square, a contradiction.

Hence the set of classes of directed ideals containing directed ideals of the form $(\mathfrak{A},1)$ is a subgroup of the directed ideal class group of index 2, and this group is isomorphic to the classical ideal class group. □

Proposition 21. *Let* $\deg(\Delta)$ *be odd and greater than* $2\deg(\Gamma)$*, and suppose that* $\Gamma^2+4\Delta$ *has* m *monic prime divisors. Then the 2-rank of* $\overrightarrow{\mathscr{C}}(\Gamma,\Delta)$ *is equal to* m*.*

Proof. To determine the 2-rank, we count the number of elements of the class group of order at most 2. Let the equivalence class containing the matrix $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ have order at most 2 - A must then be equivalent to its opposite, $\begin{bmatrix} \Gamma - b & -c \\ a & b \end{bmatrix}$. However, no two reduced matrices are equivalent, hence the reduction of this matrix must in fact equal A. That is, $\Gamma - b \equiv b \mod a$, so a divides $\Gamma - 2b$. This happens if and only if a divides $(\Gamma-2b)^2 - 4ac = \Gamma^2 + 4\Delta$, so a is a divisor of $\Gamma^2 + 4\Delta$.

The above argument reverses, so A is equivalent to its opposite if and only if a divides $\Gamma^2+4\Delta$. Now, $\Gamma^2+4\Delta$ has 2^m monic divisors, but since we require $\deg a < \frac{1}{2}\deg\Delta$, there are 2^{m-1} possibilities for a. However, if A is equivalent to its opposite, then the same holds for the twist of A, so in total there are $2 \times 2^{m-1} = 2^m$ elements of the group with order at most 2. Hence the 2-rank of the group equals m.

Note that the result also holds in even characteristic: the first half of the above argument shows that if A is equivalent to its opposite, then a divides Γ. Since we're assuming that Γ is irreducible, this means that $a = 1$ or $a = \Gamma$, which gives a 2-rank of $m = 1$ (in characteristic 2 the twist of a matrix is not defined, since every element of $\mathbb{F}_q$ is a square in $\mathbb{F}_q$). □

We have the following result by Zhang [14] about the 2-rank of the classical ideal class group.

Theorem 22. *Let* $\deg(\Delta) < \deg(\Gamma)$ *in odd characteristic and suppose that* $\Gamma^2 + 4\Delta$ *has* m *monic prime divisors. Then the 2-rank of* $\mathscr{C}(\Gamma,\Delta)$ *is* $m-2$ *if* $\Gamma^2 + 4\Delta$ *has a prime factor of odd degree, and* $m-1$ *otherwise.*

We can use this theorem to prove the following:

Proposition 23. *Let* $\deg(\Delta) < \deg(\Gamma)$ *in odd characteristic. Then the directed class number is odd if and only if* $\Gamma^2 + 4\Delta$ *is prime.*

Proof. Suppose the directed class number is odd. Then by Proposition 20 we must have that the classical class number is odd and that there exists a unit

with non-square norm. By Theorem 22, the former can only happen if $\Gamma^2+4\Delta$ (which has even degree) has at most 2 prime factors, and if it has exactly two prime factors, both factors must have odd degree.

Suppose that P is a prime factor of $\Gamma^2+4\Delta$ with odd degree, and that there is a unit $\epsilon = A + B\alpha$ with non-square norm, i.e. $A^2 - \Gamma AB - \Delta B^2 = \tau$, where τ is a non-square in $\mathbb{F}_q$. Then

$$\begin{aligned} 4\tau &= 4A^2 - 4\Gamma AB - 4\Delta B^2 \\ &= 4A^2 - 4\Gamma AB + \Gamma^2 B^2 - \Gamma^2 B^2 - 4\Delta B^2 \\ &= (\Gamma - 2A)^2 - (\Gamma^2 + 4\Delta)B^2, \end{aligned}$$

which implies that τ is a square mod P. Thus we have that, recalling that $\tau^{q^k} = \tau$ for all positive integers k,

$$1 = \tau^{\frac{q^{\deg(P)}-1}{2}} = \left(\tau^{q^{\deg(P)-1}+\cdots+1}\right)^{\frac{q-1}{2}} = \left(\tau^{\deg(P)}\right)^{\frac{q-1}{2}}.$$

Since $\deg(P)$ is odd, $\tau^{\deg P}$ is non-square, which implies that $\left(\tau^{\deg(P)}\right)^{\frac{q-1}{2}} = -1$, a contradiction. Hence, if $\Gamma^2+4\Delta$ is the product of two primes of odd degree, then there doesn't exist a unit with non-square norm. Thus, if the directed class number is odd, $\Gamma^2+4\Delta$ must be prime.

Conversely, if $\Gamma^2+4\Delta$ is prime, then Theorem 22 implies that the classical class number is odd, and Artin showed in [1, §14] that if $\Gamma^2+4\Delta$ is prime, then there exists a unit with non-square norm. □

Corollary 24. *If* $\deg(\Delta) < \deg(\Gamma) = 1$ *in odd characteristic, then the directed class number is 1 if and only if* $\Gamma^2+4\Delta$ *is prime, and 2 otherwise.*

Proof. If $\deg\Gamma = 1$, then the only reduced matrices are $A = \begin{bmatrix} 0 & \Delta \\ 1 & \Gamma \end{bmatrix}$ and its opposite. Hence the directed class number is either 1 or 2, and the above proposition implies that it is 1 exactly when $\Gamma^2+4\Delta$ is prime. □

Finally, we end off the chapter with a proof of a property of the principal cycle which we noticed in experimental data.

Theorem 25. *Suppose that* $\deg(\Delta) < \deg(\Gamma)$ *in odd characteristic and that* $\Gamma^2+4\Delta$ *is prime. Then the principal cycle has even length not divisible by 4.*

Proof. Let C be the principal matrix. Then $\phi(C) = C^{\mathrm{o}}$ by Proposition 16. Also, from Proposition 23, we find that directed class number is odd, hence every matrix is equivalent to its twist, and no matrix other than those in the princicpal cycle is equivalent to its opposite. Since C^{τ} lies in the principal cycle, it follows that the principal cycle has even length $2r$ and $\phi^r(C) = C^{\tau}$. We wish to show that r is odd.

It would suffice to show that the principal cycle contains a matrix B such that $B^{\mathrm{o}} = B^{\tau}$. Indeed, if B is such a matrix, then $B = \phi^k(C)$ for some positive integer k. Then, using Proposition 15 twice , we obtain

$$\phi^k(C^{\tau}) = \phi^k(C)^{\tau} = B^{\tau} = B^{\mathrm{o}} = \phi^k(C)^{\mathrm{o}} = \phi^{-k}(C^{\mathrm{o}}) = \phi^{1-k}(C)$$

which implies that $C^{\tau} = \phi^{1-2k}(C)$ and hence that r is odd.

We now show that such a matrix exists. Let τ be a non-square element of $\mathbb{F}_q$. Carlitz showed in [3] that if $\Gamma^2 + 4\Delta$ doesn't have a prime divisor of odd degree, then there exist polynomials X and Y such that

$$\Gamma^2 + 4\Delta = X^2 - \tau Y^2,$$

and $\deg(X) > \deg(Y)$. This implies that X is in fact monic of degree g. Set

$$a = \frac{Y}{2}, \quad b = \frac{\Gamma - X}{2}.$$

Note that $\deg(b), \deg(a) < g$. Then

$$\Gamma^2 + 4\Delta = X^2 - \tau Y^2 = (\Gamma - 2b)^2 - 4\tau a^2$$

and so the matrix $A = \begin{bmatrix} b & -\tau a \\ a & \Gamma - b \end{bmatrix}$ is a solution to (3.1) and moreover, since $\deg(b), \deg(a), \deg(\tau a) < g$, it is reduced, by Remark 1. Also, the matrix A satisfies $A^{\mathrm{o}} = A^{\tau}$. Finally, since A must necessarily be equivalent to its twist, it follows that A is equivalent to its opposite and hence A must lie in the principal cycle. □

Corollary 26. *Suppose that* $\deg(\Delta) < \deg(\Gamma)$. *If there exists a unit in* $\mathbb{F}_q[T][\alpha]$ *with non-square norm* τ *and* $\Gamma^2 + 4\Delta$ *does not have a prime divisor of odd degree or a divisor of degree* $\deg(\Gamma)$, *then there exists a cycle of even length not divisible by 4.*

Proof. From the proof of Theorem 25 it is clear that if $\Gamma^2 + 4\Delta$ doesn't have a prime divisor of odd degree, then there always exists a matrix A with $A^{\mathrm{o}} = A^{\tau}$. Since there exists a unit with non-square norm, by assumption, Proposition 20 now implies that every matrix is equivalent to its twist. We finally show that there exists a matrix C in the same class as the matrix A such that $\phi(C) = C^{\mathrm{o}}$.

In the cycle containing the matrix A, every matrix is equivalent to its opposite, since A is equivalent to its opposite. Suppose that $A^{\mathrm{o}} = \phi^k(A)$ for some integer k. If $k = 2r$ is even and $B = \phi^r(A)$, then

$$B^{\mathrm{o}} = \phi^r(A)^{\mathrm{o}} = \phi^{-r}(A^{\mathrm{o}}) = \phi^{-r}(\phi^{2r}(A)) = \phi^r(A) = B,$$

so B is equal to its opposite, and must thus be of the form $\begin{bmatrix} b & -a \\ a & \Gamma - 2b \end{bmatrix}$. But in this case, we find that

$$\Gamma^2 + 4\Delta = (\Gamma - 2b)^2 - 4a^2 = (\Gamma - 2b - 2a)(\Gamma - 2b + 2a)$$

has a divisor of degree $\deg(\Gamma)$, a contradiction.

If $k = 2r + 1$ is odd, let $C = \phi^r(A)$. Then, by Proposition 15,

$$\phi(C) = \phi^{r+1}(A) = \phi^{-r-1}(A^{\mathrm{o}})^{\mathrm{o}} = \phi^{-r-1}(\phi^{2r+1}(A))^{\mathrm{o}} = \phi^r(A)^{\mathrm{o}} = C^{\mathrm{o}},$$

as required.

Then, as in the proof of Theorem 25, we obtain

$$\phi^{-r}(C^{\tau}) = \phi^{-r}(C)^{\tau} = A^{\tau} = A^{\mathrm{o}} = \phi^{-r}(C)^{\mathrm{o}} = \phi^r(C^{\mathrm{o}}) = \phi^{r+1}(C)$$

which implies that $C^{\tau} = \phi^{2r+1}C$. The comments following the proof of Proposition 17 now shows that the cycle containing C has length $4r + 2$, as required. □

Chapter 5

Examples

5.1 Representatives of each equivalence class for some Γ and Δ

$\Gamma = T^2 + T + 1$, $\Delta = T^5 + 2$ in $\mathbb{F}_3[T]$.

Since $\deg(\Delta) > 2\deg(\Gamma)$ and $\deg(\Delta)$ is odd, Theorem 6 implies that each matrix class contains a unique reduced matrix. The reduced matrices are

$$\begin{bmatrix} 0 & T^5+2 \\ 1 & T^2+T+1 \end{bmatrix}; \quad \begin{bmatrix} 0 & 2T^5+1 \\ 2 & T^2+T+1 \end{bmatrix}$$

$$\begin{bmatrix} 2 & T^4+2T+2 \\ T & T^2+T+2 \end{bmatrix}; \quad \begin{bmatrix} 2 & 2T^4+T+1 \\ 2T & T^2+T+2 \end{bmatrix}$$

$$\begin{bmatrix} 0 & T^4+T^3+T^2+T+1 \\ T+2 & T^2+T+1 \end{bmatrix}; \quad \begin{bmatrix} 0 & 2T^4+2T^3+2T^2+2T+2 \\ 2T+1 & T^2+T+1 \end{bmatrix}$$

$$\begin{bmatrix} T+2 & T^3+T^2+2T+1 \\ T^2+2T & T^2+2 \end{bmatrix}; \quad \begin{bmatrix} T+2 & 2T^3+2T^2+T+2 \\ 2T^2+T & T^2+2 \end{bmatrix}.$$

Also, $\Gamma^2 + 4\Delta = T(T+2)(T^3+2T^2+T+1)$ is squarefree, so the classes form a group. Every element has order at most 2, so $\overrightarrow{\mathscr{C}}(\Gamma, \Delta) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

$\Gamma = T^2 + 1$, $\Delta = 3T^4 + 3T^3 + 2T + 3$ in $\mathbb{F}_5[T]$.

In this case $\deg(\Delta) = 2\deg(\Gamma)$ and $\operatorname{sgn}(\Delta) = 3$, which is not expressible as $\alpha^2 - \alpha$ in $\mathbb{F}_5$. Hence, by Theorem 7, the equivalence classes in this case either

contain a unique reduced matrix, or a set of $q+1 = 6$ almost reduced matrices. The reduced matrices in this case are

$$\begin{bmatrix} 0 & 3T^4+3T^3+2T+3 \\ 1 & T^2+1 \end{bmatrix}; \quad \begin{bmatrix} 0 & 4T^4+4T^3+T+4 \\ 2 & T^2+1 \end{bmatrix}$$
$$\begin{bmatrix} 2 & 3T^3+4T^2+2 \\ T+3 & T^2+4 \end{bmatrix}; \quad \begin{bmatrix} 2 & 4T^3+2T^2+1 \\ 2T+1 & T^2+4 \end{bmatrix}$$
$$\begin{bmatrix} 3 & 3T^3+4T^2+T+4 \\ T+3 & T^2+3 \end{bmatrix}; \quad \begin{bmatrix} 3 & 4T^3+2T^2+3T+2 \\ 2T+1 & T^2+3 \end{bmatrix}.$$

The almost reduced matrices are the following, with all the matrices in each column being equivalent.

$$\begin{bmatrix} 1 & 3T^2+4T+2 \\ T^2+3T+4 & T^2 \end{bmatrix} \quad \begin{bmatrix} 1 & 4T^2+2T+1 \\ 2T^2+T+3 & T^2 \end{bmatrix}$$
$$\begin{bmatrix} T+1 & 3T^2+T+2 \\ T^2+T+4 & T^2+4T \end{bmatrix} \quad \begin{bmatrix} T+1 & 4T^2+3T+1 \\ 2T^2+2T+3 & T^2+4T \end{bmatrix}$$
$$\begin{bmatrix} T+1 & 3T^2+3T+2 \\ T^2+2T+4 & T^2+4T \end{bmatrix} \quad \begin{bmatrix} T+1 & 4T^2+4T+1 \\ 2T^2+4T+3 & T^2+4T \end{bmatrix}$$
$$\begin{bmatrix} 2T+1 & 4T^2+2T+1 \\ 2T^2+4T+3 & T^2+3T \end{bmatrix} \quad \begin{bmatrix} 2T+1 & 3T^2+4T+2 \\ T^2+2T+4 & T^2+3T \end{bmatrix}$$
$$\begin{bmatrix} 2T+1 & 4T^2+3T+1 \\ 2T^2+T+3 & T^2+3T \end{bmatrix} \quad \begin{bmatrix} 2T+1 & 3T^2+T+2 \\ T^2+3T+4 & T^2+3T \end{bmatrix}$$
$$\begin{bmatrix} 3T+1 & 4T^2+4T+1 \\ 2T^2+2T+3 & T^2+2T \end{bmatrix} \quad \begin{bmatrix} 3T+1 & 3T^2+3T+2 \\ T^2+T+4 & T^2+2T \end{bmatrix}.$$

In this case we have $\Gamma^2+4\Delta = 3T^4+2T^3+2T^2+3T+3$ is irreducible, hence squarefree and so the above equivalence classes form a group. The class containing $\begin{bmatrix} 3 & 3T^3+4T^2+T+4 \\ T+3 & T^2+3 \end{bmatrix}$ has order 8, hence $\overrightarrow{\mathscr{C}}(\Gamma,\Delta) \cong \mathbb{Z}_8$.

$\Gamma = T^2+1$, $\Delta = 3$ in $\mathbb{F}_5[T]$.

In this example we have $\deg(\Delta) < \deg(\Gamma)$, so by Theorem 10, the reduced matrices in this case can be divided up into cycles of equivalent matrices. The

cycles of reduced matrices are

$$\begin{bmatrix} 0 & 3 \\ 1 & T^2+1 \end{bmatrix} \quad \begin{bmatrix} 3 & 3T+2 \\ T+1 & T^2+3 \end{bmatrix} \quad \begin{bmatrix} 4 & 4T+1 \\ T+1 & T^2+2 \end{bmatrix}$$
$$\begin{bmatrix} 0 & 4 \\ 2 & T^2+1 \end{bmatrix} \quad \begin{bmatrix} 4 & 4T+4 \\ T+4 & T^2+2 \end{bmatrix} \quad \begin{bmatrix} 3 & 4T+4 \\ 2T+3 & T^2+3 \end{bmatrix}$$
$$\begin{bmatrix} 3 & 4T+1 \\ 2T+2 & T^2+3 \end{bmatrix} \quad \begin{bmatrix} 4 & 2T+3 \\ 2T+2 & T^2+2 \end{bmatrix}$$
$$\begin{bmatrix} 4 & 2T+2 \\ 2T+3 & T^2+2 \end{bmatrix} \quad \begin{bmatrix} 3 & 3T+3 \\ T+4 & T^2+3 \end{bmatrix},$$

where ϕ applied to a matrix is equal to the matrix below it. In this case, $\Gamma^2 + 4\Delta = T^4 + 2T^2 + 3$ is irreducible, hence square-free, so $\overrightarrow{\mathscr{C}}(\Gamma, \Delta) \cong \mathbb{Z}_3$.

$\Gamma = T^5 + T^2 + 1$, $\Delta = T^4 + T^2 + T + 1$ in $\mathbb{F}_2[T]$.

In this characteristic 2 example, Γ is irreducible and $\deg(\Delta) < \deg(\Gamma)$, so we can divide the reduced matrices up into cycles of equivalent matrices. Due to space constraints, we represent the matrices by their first column $\begin{bmatrix} b \\ a \end{bmatrix}$. The arrows indicate application of ϕ.

$$\begin{aligned}
Id: &\quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \to \begin{bmatrix} 0 \\ T^4+T^2+T+1 \end{bmatrix} \to \begin{bmatrix} T^3+T+1 \\ T^4+T^2+T+1 \end{bmatrix} \\
A: &\quad \begin{bmatrix} 0 \\ T+1 \end{bmatrix} \to \begin{bmatrix} 1 \\ T^4+1 \end{bmatrix} \to \begin{bmatrix} T^2+T \\ T^3+T^2+1 \end{bmatrix} \\
B: &\quad \begin{bmatrix} 1 \\ T+1 \end{bmatrix} \to \begin{bmatrix} 0 \\ T^3+T^2+1 \end{bmatrix} \to \begin{bmatrix} T^2+T \\ T^4+1 \end{bmatrix} \\
C: &\quad \begin{bmatrix} 1 \\ T^2+1 \end{bmatrix} \to \begin{bmatrix} T+1 \\ T^4+T^3+1 \end{bmatrix} \to \begin{bmatrix} T^3+T^2+1 \\ T^4+T^2+T+1 \end{bmatrix} \to \begin{bmatrix} T^2+T \\ (T+1)(T^2+1) \end{bmatrix} \\
D: &\quad \begin{bmatrix} T+1 \\ T^2+1 \end{bmatrix} \to \begin{bmatrix} 1 \\ (T+1)(T^2+1) \end{bmatrix} \to \begin{bmatrix} T^2+T \\ T^4+T^2+T+1 \end{bmatrix} \to \begin{bmatrix} T^3+T^2+1 \\ T^4+T^3+1 \end{bmatrix}.
\end{aligned}$$

There are five cycles, and hence $\overrightarrow{\mathscr{C}}(\Gamma, \Delta) \cong \mathbb{Z}_5$. Explicitly, the group operation is given by the following:

$$A^2 = D \quad C^2 = A \quad AB = Id.$$

5.2 Directed class number frequencies

We used the theoretical framework of Section 3.2 to compile a table of the number of instances a particular directed class number appears for a given degree of Γ (under the assumption that $\deg(\Delta) < \deg(\Gamma)$). The table contains only instances where $\Gamma^2 + 4\Delta$ is squarefree.

Note that if $\deg(\Gamma)$ is fixed, the number of directed class groups with a given order is divisible by q, as expected, since if $k \in \mathbb{F}_q$, then $\overrightarrow{\mathscr{C}}(\Gamma(T), \Delta(T)) \cong \overrightarrow{\mathscr{C}}(\Gamma(T+k), \Delta(T+k))$. The notable exceptions arise when q divides $\deg(\Gamma)$ (in the table below, $q = 3$, $\overrightarrow{h} = 1, 6, 8, 12$). In this case, if Γ and Δ are polynomials in $\prod_{k \in \mathbb{F}_q}(T+k)$, then the transformation of $\Gamma^2 + 4\Delta$ using the map $T \to T + k$ will result in the exact same polynomial.

$q = 3$						$q = 5$					$q = 7$			
	$\deg(\Gamma)$						$\deg(\Gamma)$					$\deg(\Gamma)$		
$\overrightarrow{h}$	1	2	3	4	*Overall*	$\overrightarrow{h}$	1	2	3	*Overall*	$\overrightarrow{h}$	1	2	*Overall*
1	3	15	98	654	15.65%	1	10	125	2100	17.17%	1	21	462	23.00%
2	3	27	189	1305	30.98%	2	10	210	3980	32.26%	2	21	791	38.67%
3		3	3	90	1.95%	3		20	220	1.84%	3		84	4.00%
4		9	123	1128	25.61%	4		105	3000	23.85%	4		420	20.00%
5			6	30	0.73%	5		5	150	1.19%	5		42	2.00%
6			10	171	3.68%	6		20	330	2.69%	6		119	5.67%
7			9	15	0.49%	7		0	30	0.23%	8		119	5.67%
8			41	516	11.32%	8		15	1330	10.33%	12		21	1.00%
10			3	57	1.22%	9			50	0.38%				
11			0	12	0.24%	10			150	1.15%				
12			4	144	3.01%	11			20	0.15%				
13				6	0.12%	12			280	2.15%				
14				30	0.61%	14			150	1.15%				
16				129	2.62%	16			390	3.00%				
18				12	0.24%	18			40	0.31%				
20				39	0.79%	20			130	1.00%				
21				3	0.06%	21			10	0.08%				
22				6	0.12%	22			20	0.15%				
24				24	0.49%	24			80	0.61%				
30				3	0.06%	30			10	0.08%				
						32			20	0.15%				
						40			10	0.08%				

Bibliography

[1] Artin, E. 1924. Quadratische Körper im Gebiete der höheren Kongruenzen. I. *Math. Z.*, 19(1):153–206. ISSN 0025-5874.
Available at: `http://dx.doi.org/10.1007/BF01181074`

[2] Behn, A. and Van der Merwe, A.B. 2002. An algorithmic version of the theorem by Latimer and MacDuffee for 2×2 integral matrices. *Linear Algebra Appl.*, 346:1–14. ISSN 0024-3795.
Available at: `http://dx.doi.org/10.1016/S0024-3795(01)00518-3`

[3] Carlitz, L. 1933. On the representation of a polynomial in a Galois field as the sum of an even number of squares. *Trans. Amer. Math. Soc.*, 35(2):397–410. ISSN 0002-9947.
Available at: `http://dx.doi.org/10.2307/1989773`

[4] Cox, D.A. 1989. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. New York: John Wiley & Sons Inc. ISBN 0-471-50654-0; 0-471-19079-9. Fermat, class field theory and complex multiplication.

[5] Dirichlet, P.G.L. 1968. *Vorlesungen über Zahlentheorie*. Herausgegeben und mit Zusätzen versehen von R. Dedekind. Vierte, umgearbeitete und vermehrte Auflage. New York: Chelsea Publishing Co.

[6] Gauss, C.F. 1986. *Disquisitiones arithmeticae*. New York: Springer-Verlag. ISBN 0-387-96254-9. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[7] González, C.D. 1992. Class numbers of quadratic function fields and continued fractions. *J. Number Theory*, 40(1):38–59. ISSN 0022-314X.
Available at: `http://dx.doi.org/10.1016/0022-314X(92)90027-M`

[8] Lagrange, J.L. 1973. *Oeuvres. Tome 1.* Hildesheim: Georg Olms Verlag. Publiées par les soins de J.-A. Serret, Avec une notice sur la vie et les ouvrages de J.-L. Lagrange par J.-B. J. Delambre, Nachdruck der Ausgabe Paris 1867.

[9] Latimer, C.G. and MacDuffee, C.C. 1933. A correspondence between classes of ideals and classes of matrices. *Ann. of Math. (2)*, 34(2):313–316. ISSN 0003-486X.
Available at: `http://dx.doi.org/10.2307/1968204`

[10] Legendre, A.M. 1798. *Essai sur la Théorie des Nombres.* Paris. Reprint by Blanchard, Paris, 1955.

[11] MacDuffee, C.C. 1929. An introduction to the theory of ideals in linear associative algebras. *Trans. Amer. Math. Soc.*, 31(1):71–90. ISSN 0002-9947.
Available at: `http://dx.doi.org/10.2307/1989399`

[12] Taussky, O. 1949. On a theorem of Latimer and MacDuffee. *Canadian J. Math.*, 1:300–302. ISSN 0008-414X.

[13] Yu, J.-K. 1995. A class number relation over function fields. *J. Number Theory*, 54(2):318–340. ISSN 0022-314X.
Available at: `http://dx.doi.org/10.1006/jnth.1995.1122`

[14] Zhang, X.K. 1987. Ambiguous classes and 2-rank of class group of quadratic function field. *J. China Univ. Sci. Tech.*, 17(4):425–431. ISSN 0253-2778.