The Pennsylvania State University
The Graduate School

ENDOMORPHISM RINGS AND ALGEBRAS OF JACOBIANS OF CERTAIN SUPERELLIPTIC CURVES

A Dissertation in
Mathematics
by
Tigran Eritsyan

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Doctor of Philosophy

December 2022

The dissertation of Tigran Eritsyan was reviewed and approved by the following:

Yuriy Zarkhin
Professor of Mathematics
Dissertation Advisor
Chair of Committee

John Lesieutre
Assistant Professor of Mathematics

Mihran Papikian
Professor of Mathematics

Mark Strikman
Distinguished Professor of Physics

Alexei Novikov
Professor of Mathematics
Chair of Graduate Program

Abstract

In this article we explore the endomorphism rings and algebras of Jacobians of trigonal curves of the form $y^3 = f(x)$, where $f(x)$ is a separable polynomial with coefficients in k, irreducible over field k of characteristic zero and with $Gal(f)$ isomorphic to one of the 2-transitive Ree groups in the series ${}^2G_2(q)$ with $q = 3^{2m+1}$ for positive integers m. We show that the endomorphism algebras $End^0(J)$ of such Jacobians are simple and their centers are isomorphic to the number field $\mathbb{Q}(\zeta_3)$, where ζ_3 (the third root of unity) is the solution to to the polynomial equation over the ring of integers $x^2 + x + 1$. For $m \in ABS_m \cup COMP_m$ (see page 2), we determine that the endomorphism algebras of such Jacobians are absolutely simple and are isomorphic to the number field $\mathbb{Q}(\zeta_3)$, while the rings of endomorphisms of such Jacobians are isomorphic to the ring $\mathbb{Z}[\zeta_3]$.

Contents

List of Figures

Acknowledgments

First, I am extremely grateful to my adviser Professor Yuri Zarhin. This dissertation would not be possible without his patience, guidance and support. His mentorship and work shaped my understanding of algebraic geometry, of mathematics and of other sciences that have mathematics at their core. I consider myself undeservingly lucky to have him as my adviser.

Second, I would like to mention and thank Professors Svetlana Katok, Jack Huizenga and Jan Reimann for their enormous help and care.

Third, I would like to thank members of my committee Professors John Lesieutre, Mihran Papikian and Mark Strikman for taking the time to attend my examinations and to read this manuscript.

A special thanks belongs to my undergraduate mentor Professor Edward Frenkel for his immense help early on in my career. His linear algebra and abstract algebra courses provided me with excellent fundamentals. I will always cherish our conversations that were critical in my early formation as a researcher and a mathematician.

This dissertation would not be possible without the encouragement, support and love of my immediate family. George, Richard and Sarah, thank you for always being there for me – I love you guys! Richard deserves a special thanks for the countless times he gave me rides to the department – thank you, brother!

I would like to mention and thank my closest friends Nawaf Al-Ansari, Daniel Levine, Dmitrii Pedchenko and Alp Uzman. It is impossible for me to imagine graduate years without their friendship. Dmitrii and Nawaf deserve a special thanks for their support and help during certain critical moments in my Ph.D. program.

Last, but certainly not least, I want to thank my friends and fellow graduate students for their advice, camaraderie and encouragement: Maria Teresa Chiri, Anirban Das, Ayush Khaitan, Jim Kowalski, Juliana Londono-Alvarez, Angel Roman, Jesus Sanchez, Gabrille Scullard, Farruh Shahidi, Caleb Springer, Dom Veconi, Will Wright and Agnieszka Zelerowicz.

Dedication

To my parents

Chapter 1 Introduction

Let k be a field of characteristic zero that contains the third root of unity ($\zeta_3 \in k$) and C be a smooth projective model of the k-curve defined by the equation $y^3 = f(x)$.

Notation: By ζ_3 we denote the third root of unity, i.e. the solution $x = \zeta_3$ to the polynomial equation $x^2 + x + 1$ with integer coefficients.

We assume $f(x)$ is separable polynomial with coefficients in k, irreducible over k of degree

$$n := \deg(f) = q^3 + 1$$

with $q = 3^{2m+1}$ for positive integers m. We fix an algebraic closure $\bar{k}$ of k and use $\mathfrak{R}_f \subset \bar{k}$ for the set of roots of $f(x)$, $K(\mathfrak{R}_f) \supset k$ for the splitting field of $f(x)$ and

$$Gal(f) = Gal(K(\mathfrak{R}_f), k).$$

Notation: J stands for the Jacobian of C, $End_k(J)$ is used for the ring of k–endomorphisms, $End_k^0(J) := End_k(J) \otimes \mathbb{Q}$ for the $\mathbb{Q}$-algebra and $End_{\bar{k}}(J) := End(J)$ for the ring of $\bar{k}$-endomorphisms and $End^0(J) := End(J) \otimes \mathbb{Q}$ for the $\mathbb{Q}$-algebra.

We are interested in the endomorphism algebras $End^0(J)$ and the endomorphism rings $End(J)$ of Jacobians J of C and we investigate the restrictions placed on $End^0(J)$ and $End(J)$ when $Gal(f)$ coincides with one of the 2-transitive small Ree groups in the series defined in our theorems below.

Notation: By $\mathbb{Q}(\zeta_3)$ we denote the number field over the field of rational numbers $\mathbb{Q}$ by adjoining the third root of unity ζ_3. Equivalently, by $\mathbb{Z}[\zeta_3]$ we denote the ring extension over the ring of integers $\mathbb{Z}$ by adjoining the third root of unity ζ_3.

We state the main results of this article:

Theorem 1.0. Let f be a polynomial with coefficients in k and of degree

$$n := \deg(f) = q^3 + 1.$$

Let C be the trigonal curve it describes via the equation $y^3 = f(x)$. If $Gal(f)$ coincides with one of the 2-transitive Ree groups in the series

$$Ree(q) = {}^2G_2(q)$$

for $q = 3^{2m+1}$, then the endomorphism algebra $End^0(J)$ of the Jacobian J of C is a simple algebra over its center

$$C_J \cong \mathbb{Q}(\zeta_3).$$

We prove Theorem 1.0 at the end of Chapter 4 of this article.

For certain values of m, see Remark 1.1, we determine that the Endomorphism algebra actually coincides with its center C_J, i.e., it is isomorphic to $\mathbb{Q}(\zeta_3)$. Furthermore, we obtain that the ring of endomorphisms of J

$$End(J) \cong \mathbb{Z}[\zeta_3].$$

N.B.: We define the embeddings of $\mathbb{Q}(\zeta_3)$ and $\mathbb{Z}[\zeta_3]$ into $End^0(J)$ and $End(J)$ in formulas (1) and (2) of Chapter 2.

Below, we define the sets ABS_m and $COMP_m$, which consist of values of m for which the ring of endomorphisms $End(J)$ of the Jacobian J of C is isomorphic to $\mathbb{Z}[\zeta_3]$ and J is absolutely simple in the next theorem.

Notation:

$$ABS_m := \{m \in \mathbb{Z}^+ | \quad \frac{q-1}{2} \text{ is prime}\},$$

$$COMP_m := \{m \in \mathbb{Z} |\ 1 \leq n \leq 752\}.$$

Recall:

$$q = 3^{2m+1}.$$

$\boxed{\textbf{Theorem 1.1.}}$ Let f be a polynomial with coefficients in k and of degree

$$n := \deg(f) = q^3 + 1.$$

Let C be the trigonal curve it describes via the equation $y^3 = f(x)$. Suppose $Gal(f)$ coincides with one of the 2-transitive Ree groups in the series

$$Ree(q) = {}^2G_2(q)$$

for $q = 3^{2m+1}$ and

$$m \in ABS_m \cup COMP_m,$$

then the endomorphism algebra $End^0(J)$ of the Jacobian of C is isomorphic to $\mathbb{Q}(\zeta_3)$ and the endomorphism ring $End(J)$ of the Jacobian of C is isomorphic to $\mathbb{Z}[\zeta_3]$,

$$End(J) \cong \mathbb{Z}[\zeta_3].$$

The proof of Theorem 1.1 will be carried out in steps throughout the further Chapters of this article. We start with a setup in **Chapter 2**, where we also define the Galois action on the endomorphism ring of the Jacobian. In **Chapter 3** we construct an irreducible Galois representation $J[\lambda]$ arising from the Galois action on the 3-torsion points of the Jacobian. We obtain a more explicit description V_f of the Galois module $J[\lambda]$ in **Chapter 5**. In **Chapter 5** (Theorem 5.2) we also show the absolute simplicity of this Galois module. In **Chapter 6** we consider the notion of very simple modules (as in in Yu. Zarhin's paper Endomorphism Algebras of Abelian Varieties with Special Reference to Superelliptic Jacobians [Zar05b]) and obtain conditions for the Galois-module $J[\lambda]$ to be very simple. The conditions we obtain in **Chapter 6** bring us to the theory of weights for Lie algebras in **Chapter 7**, where we consider the Galois-module $J[\lambda]$ as a restriction coming from its parent algebraic group $\mathbb{G}_2$ and establish the very simplicity of the Galois-module $J[\lambda]$ in

Theorem 7.3. In **Chapter 8**, the very simplicity along with results about the center of the endomorphism algebra of the Jacobian (Theorems 4.14 and 4.16 from Yu. Zarhin's article Endomorphism algebras of superelliptic jacobians [Zar05a]), help us prove Theorem 1.1.

Remark 1.1 : We expect Theorem 1.1 to hold for all $m \geq 1$. However, currently, we are unable to solve it for the case of all m. Showing the result for all $m \geq 1$ comes down to proving either the statement of Lemma 7.4 for all $m \geq 1$ (we were only able to verify it for explicit cases of $m \in COMP_m$ by employing MAGMA [BCP97]) or try to expand the set $m \in ABS_m$ to account for all integer values of m. The author is grateful to Yu. Zarhin for his help with the set ABS_m. For more details we refer the reader to Remark 7.6 of Chapter 7.

Chapter 2 Setup

Throughout the paper we assume $Gal(f) \cong Ree(q)$ and $q = 3^{2m+1} = 3^d$ with positive integer m or odd $d > 1$. The requirement for $m \geq 1$ comes from the fact that $Ree(3)$ (the first group in the series) fails to be simple. $Ree(q)$ is a 2-transitive group of order $q^3(q^3 + 1)(q - 1)$ and its action on the set of $q^3 + 1$ roots of $f(x)$ is 2-transitive. We denote $n = q^3 + 1$ for the degree of $f(x)$. One can use the Riemann-Hurwitz formula to obtain the genus g of C and, thus, the dimension g of J:

$$g = \frac{(3-1)(n-1)}{2} = n - 1 = q^3.$$

Our curve C has an automorphism of order 3 denoted δ and the corresponding cyclic subgroup of order 3 it generates in the automorphism group of C,

$$\mathbb{Z}/3\mathbb{Z} \cong < \delta > \subset Aut(C).$$

Since $\zeta_3 \in k$, we have a Galois cover of $\mathbb{P}^1$ corresponding to the action of δ:

$$\begin{tikzcd} C \arrow[d, dash, "\delta"'] \\ \mathbb{P}^1 = C/ < \delta > \end{tikzcd}$$

By Albanese functoriality, δ induces an automorphism $\delta : J \to J$ which satisfies the polynomial

$$\mathcal{P}(t) = \frac{t^3 - 1}{t - 1} = t^2 + t + 1.$$

This gives rise to a $\mathbb{Q}$-algebra embedding of the number field $E = \mathbb{Q}(\zeta_3)$ (as in Section 3 of Yu. Zarhin's paper "Endomorphism Algebras of Abelian Varieties with Special Reference to Superelliptic Jacobians" [Zar18]):

$$i : E = \mathbb{Q}(\zeta_3) \hookrightarrow End_k^0(J) \subset End^0(J) \tag{2.1}$$

such that $\zeta_3 \mapsto \delta$ and $i(1) = 1_J$. We denote $End^0(J, i)$ for the centralizer of $i(E)$ in $End^0(J)$ and $End_k^0(J, i)$ for the centralizer of $i(E)$ in $End_k^0(J)$. We have

$$i(E) \subset End_k^0(J, i) \subset End^0(J, i) \subset End^0(J) \quad \text{and} \quad End_k^0(J, i) \subset End_k^0(J, i) \subset End^0(J).$$

There is, equivalently, a ring embedding of the ring $\mathcal{O}_E = \mathbb{Z}[\zeta_3]$:

$$i : \mathcal{O}_E = \mathbb{Z}[\zeta_3] \hookrightarrow End_k(J) \subset End(J) \tag{2.2}$$

Remark 2.1 : The centralizer $End^0(J, i)$ will be one of the crucial objects in our proof of both **Theorem 1.0** and **Theorem 1.1**. For both theorems, the restrictions we have placed on $Gal(f)$ will result in $End^0(J, i) \cong E$. In the case of **Theorem 1.1**, $End^0(J, i) \cong E$ turns out to being the maximal commutative subalgebra of $End^0(J)$. These facts in conjunction with Theorem 4.16 of Yu. Zarhin's "Endomorphism algebras of superelliptic jacobians" [Zar05a] yield the isomorphism

$$End^0(J) \cong \mathbb{Q}(\zeta_3) = E.$$

We define the Galois action on the endomorphism ring of the Jacobian. Since J is defined over k, we have a continuous group homomorphism:

$$\eta_k : Gal(k) \longrightarrow Aut(End(J)), \quad \text{with the image} \quad \eta_k(Gal(k)) = \Gamma_k \tag{2.3}$$

where $\eta_k(\sigma)(u) =^{\sigma} u$ for $\sigma \in Gal(k)$, $u \in End(J)$ and ${}^{\sigma}u(x) = \sigma(u(\sigma^{-1}x))$ for all $x \in J(\bar{k})$.

It is known that $End_k(J)$ coincides with the subring $End(J)^{Gal(k)}$, where

$$End(J)^{Gal(k)} = \{u \in End(J) | \ {}^{\sigma}u = u \quad \forall \sigma \in Gal(k)\}.$$

The kernel $Ker(\eta_k)$ is a closed normal subgroup of finite index in $Gal(k)$, hence (Theorem 1.3.11 in Szamuely's "Central Simple Algebras and Galois Cohomology" book [Sza09]) it is open and coincides with $Gal(L)$ for some overfield $L \supset k$ and

$$End_L(J) = End(J).$$

If $N \supset k$ is a finite separable extension, then $Gal(N)$ is an open subgroup of finite index in $Gal(k)$ and the restriction of η_k to $Gal(N)$ coincides with

$$\eta_N : Gal(N) \longrightarrow Aut(End(J))$$

and $End_N(J) = End(J)^{Gal(N)} = \{u \in End(J) | \ {}^{\sigma}u = u \quad \forall \sigma \in Gal(N)\}$. Clearly, $End_N(J) = End(J)$ (*all endomorphisms are defined over* N) if and only if $N \supset L$.

Chapter 3
Modular representations

We construct modular representations from the action of the Galois group on the torsion points of the Jacobian J. It is known, A. Silverberg's paper "Fields of definition for homomorphisms of abelian varieties" [Sil92], that all endomorphisms of J are defined over the field of definition of the 3-torsion points $J[3]$, denoted by $K(J[3]) \supset k$. Hence, $K(J[3]) \supset L$ and

$$Gal(K(J[3])) \subset ker(\eta_k) \cong Gal(L).$$

Since the equations that define J and the group law have coefficients in k and for all $P \in J(\bar{k})$ we have $[3]\sigma(P) = \sigma([3]P)$, $J[3]$ is $Gal(k)$-stable subgroup of $J(\bar{k})$ and we can define a faithful linear representation:

$$\rho_{3,k} : Gal(k) \to \mathbf{Aut}_{\mathbb{F}_3}(J[3]) \qquad \text{with image} \quad \rho_{3,k}(Gal(k)) = \tilde{G}_{3,k}. \tag{3.1}$$

This representation fails to be irreducible and, thus, we consider the subgroup of δ-fixed elements of J.

λ-torsion:

We are going to use the subgroup of δ-fixed points $(J)^{\delta} \subset J$ to construct an irreducible representation. We take a closer look at the fixed points of δ-action on J.

We have the subgroup of δ-fixed points $(J)^{\delta} = \Psi = ker(1-\delta)|_J$ with cardinality

$$\#\Psi = 3^{\frac{2dimJ}{\varphi(3)}} = 3^{dimJ},$$

where φ is the Euler totient function.

Consider $\lambda = (1-\delta) \subset \mathcal{O}_E$, the only prime ideal that divides $3\mathcal{O}_E$. It is known that $\Psi = J[\lambda]$ (λ-torsion points of $J(\bar{k})$). Hence, $\Psi = J[\lambda] \subset J[3]$ is a module over $k(\lambda) = \mathcal{O}_E/\lambda = \mathbb{F}_3$ and $J[\lambda] \cong \mathbb{F}_3^{dimJ}$. Since under our assumptions $J[\lambda]$ is defined over $K(\mathfrak{R}_f)$, we have

$$K(\mathfrak{R}_f) \cong K(J[\lambda]) \subset K(J[3]),$$

where $K(J[\lambda]) \supset k$ is the field over which $J[\lambda]$ is defined.

Using the fact that $J[\lambda]$ is $Gal(k)$-stable subgroup of $J[3]$, we define a faithful representation:

$$\rho_{\lambda,k} : Gal(k) \to \mathrm{Aut}_{\mathbb{F}_3}(J[\lambda]) \quad \text{with image } \rho_{\lambda,k}(Gal(k)) = \tilde{G}_{\lambda,k} \cong Gal(f) \tag{3.2}$$

which will turn out to be absolutely irreducible in the next section. We will use a more explicit definition of the $Gal(f)$-module $J[\lambda]$ to show that the representation (3) is simple in Section 5.

Chapter 4
Restrictions on $End^0(J)$ and its center C_J

In this section we continue with the setup of previous sections and obtain some restrictions on the structure of endomorphism algebra $End^0(J)$ of J and its center C_J. First, we use results from Yu. Zarhin's paper "Endomorphism Algebras of Abelian Varieties with Special Reference to Superelliptic Jacobians" [Zar18] to show that $End^0(J)$ is simple in Theorem 4.1. In addition to the simplicity of algebra $End^0(J)$, this theorem provides us with the following inclusion for its center C_J

$$C_J \subset \mathbb{Q}(\delta) \cong \mathbb{Q}(\zeta_3),$$

which implies that C_J is isomorphic to either $\mathbb{Q}$ or $\mathbb{Q}(\zeta_3)$. In Theorem 4.2 we show that C_J must be isomorphic to $\mathbb{Q}(\zeta_3)$.

Consider the centralizers $End^0_k(J,i)$ and $End^0(J,i)$ of $i(E)$ in $End^0_k(J)$ and $End^0(J)$ respectively. Recall that these were obtained from the displayed formula (1) of Section 2 above.

Lemma 4.1. With our setup we have $End^0_k(J,i) \cong \mathbb{Q}(\zeta_3)$ and $End_k(J,i) \cong \mathbb{Z}[\zeta_3]$.

Proof. Since $Gal(f)$ is 2-transitive, then by Theorem 5.1 and Remark 5.5 (see Section 5 for more details), we have

$$\mathrm{End}_{Gal(f)}(J[\lambda]) \cong \mathbb{F}_3.$$

This fact allows us to use results from Section 3 of [Zar18], which allow us to determine the algebra centralizers $End_k^0(J,i)$ and $End^0(J,i)$ and ring centralizers centralizers $End_k(J,i)$ and $End(J,i)$. In particular, now we can apply Lemma 3.12 and Corollary 3.13 from [Zar18] with

$$X_\lambda := J[\lambda],\ k(\lambda) := \mathcal{O}_E/\lambda \cong \mathbb{F}_3,\ i(\mathcal{O}) := \mathbb{Q}(\delta) \cong \mathbb{Q}(\zeta_3) \text{ and } i(E) := \mathbb{Q}(\delta) \cong \mathbb{Q}(\zeta_3)$$

to obtain

$$End_k^0(J,i) = i(E) = \mathbb{Q}(\delta) \cong \mathbb{Q}(\zeta_3),$$

$$End_k(J,i) = i(\mathcal{O}) = \mathbb{Z}[\delta] \cong \mathbb{Z}[\zeta_3].$$

□

In the next step, we are going after the simplicity of $End^0(J)$ using Theorem 3.14 of Section 3 of [Zar18]. Theorem 3.14 of [Zar18] allows one to establish the simplicity of $End^0(J)$ when the group in question, $Gal(f)$ in our case, and its subgroups satisfy a certain criterion on the possible indices. Specifically, Theorem 3.14 of [Zar18] is employed in the proof of the Theorem 4.1 below to obtain the simplicity of the $\mathbb{Q}$-algebra $End^0(J)$.

Before proceeding further, we are going to require a couple of additional ingredients to be used in our application of Theorem 3.14 from [Zar18]. We define these ingredients along the lines of Section 3.1 of [Zar18]. Note that Section 3.1 of [Zar18] tackles the cases when the endomorphism algebra of an abelian variety contains a given number field (field $\mathbb{Q}(\delta) \cong \mathbb{Q}(\zeta_3)$ in our case). Let us recall the $\mathbb{Q}$-algebra embedding (1) of Section 2:

$$i : \mathbb{Q}(\zeta_3) \hookrightarrow End_k^0(J) \subset End^0(J),$$

where $i(1) = 1_J$. For $E = \mathbb{Q}(\zeta_3)$, similar to the definition in Section 3.1 of [Zar18], we define

$$d_J = \frac{2 \cdot dim(J)}{[E : \mathbb{Q}]} = \frac{2g}{[\mathbb{Q}(\zeta_3) : \mathbb{Q}]} = \frac{2g}{2} = g = q^3.$$

Theorem 4.1. With our setup we have:

(i) $End^0(J)$ is a simple $\mathbb{Q}$-algebra (and J is isotypic);

(ii) the center of $End^0(J, i)$ is $i(\mathbb{Q}(\zeta_3)) = \mathbb{Q}(\delta) \cong \mathbb{Q}(\zeta_3)$;

(iii) the center C_J of $End^0(J)$ is contained in $i(\mathbb{Q}(\zeta_3)) = \mathbb{Q}(\delta) \cong \mathbb{Q}(\zeta_3)$;

(iv) $End^0(J, i)$ is CSA over $i(\mathbb{Q}(\zeta_3)) = \mathbb{Q}(\delta) \cong \mathbb{Q}(\zeta_3)$.

Proof. We want to employ Theorem 3.14 of [Zar18] with

$$G_{\lambda,X,K} := Gal(f), \quad X := J \quad \text{and} \quad X_\lambda := J[\lambda].$$

To apply this theorem we need to meet its two conditions. Since $Gal(f)$ is 2-transitive, then by Theorem 5.1 and Remark 5.5 (see Section 5 for more details), we have

$$\text{End}_{Gal(f)}(J[\lambda]) \cong \mathbb{F}_3,$$

thus, satisfying the first condition of Theorem 3.14 in [Zar18]. Next, we want to satisfy the second condition by showing that $Gal(f)$ does not contain a proper subgroup whose index divides d_J. Since the order of any maximal subgroup M of $Gal(f)$ must satisfy

$$\#M \leq q^3(q-1),$$

see Remark 5.4, then the index of any subgroup H of $Gal(f)$ must be $\geq q^3 + 1$, while $d_J = q^3$. Clearly, $d_J = q^3$ is not divisible by such indices. Now, since both conditions of Theorem 3.14 of [Zar18] are satisfied we obtain the following:

- $End^0(J)$ is simple $\mathbb{Q}$-algebra;
- center of $End^0(J, i)$ is $i(\mathbb{Q}(\zeta_3)) = \mathbb{Q}(\delta)$;
- center C_J of $End^0(J)$ is contained in $i(\mathbb{Q}(\zeta_3)) = \mathbb{Q}(\delta)$;

- $End^0(J, i)$ is CSA over $i(\mathbb{Q}(\zeta_3)) = \mathbb{Q}(\delta)$;

□

Next we concentrate on the center C_J of $End^0(J)$. Theorem 4.1 (iii) tells us that C_J is contained in $i(\mathbb{Q}(\zeta_3)) = \mathbb{Q}(\delta) \cong \mathbb{Q}(\zeta_3)$. Thus, we have that C_J is isomorphic either to $\mathbb{Q}$ or to $\mathbb{Q}(\zeta_3)$. In the last part of this section we eliminate the case of C_J isomorphic to $\mathbb{Q}$ using results from Yu. Zarhin's article "Endomorphism algebras of superelliptic jacobians" [Zar05a]. Specifically, we apply Corollary 2.2 of [Zar05a] to our setup. Corollary 2.2 defines certain conditions on subfields of endomorphism algebras $End^0(J)$ of Jacobians of superelliptic curves upon whose satisfactions one obtains the isomorphism class for their centers

$$C_J \subset End^0(J).$$

In order to use Corollary 2.2 of [Zar05a], we need to define the tangent space $Lie(J)$ of J and the space of differentials of the first kind $\Omega^1(J)$ of J. For more thorough details we refer the reader to D. Mumford's canonical book on the subject "Abelian varieties" [Mum70].

In the following part of this section we consider the Jacobian J to be defined over the field of complex numbers $\mathbb{C}$, which we denote by $J(\mathbb{C})$. We consider $J(\mathbb{C})$ to be defined over $\mathbb{C}$ by picking a field embedding

$$\tau : \mathbb{Q}(\delta) \hookrightarrow \mathbb{C},$$

recall that $\mathbb{Q}(\delta) \cong \mathbb{Q}(\zeta_3)$. $J(\mathbb{C})$ is a projective variety and, thus, inherits a complex structure as a submanifold of a projective space over the complex numbers. In particular, the group structure becomes holomorphic.

Thus, $J(\mathbb{C})$ is a compact connected complex Lie group of dimension g with a group structure defined by holomorphic maps. Let $Lie(J)$ be the tangent space of $J(\mathbb{C})$ at the identity point $e \in J(\mathbb{C})$, it is a complex vector space. For every tangent vector v to $J(\mathbb{C})$ at identity e, there is a unique holomorphic map

$$\phi_v : \mathbb{C} \to J(\mathbb{C})$$

such that $\phi_v(0) = e$ and $(d\phi_v(1)) = v$. The exponential map is defined

$$\exp : Lie(J) \to J(\mathbb{C})$$

such that

$$t \mapsto \exp(tv) : \mathbb{C} \to Lie(J) \to J(\mathbb{C})$$

is ϕ_v for all v, and, thus $\exp(v) = \phi_v(1)$. When we identify the tangent space at 0 of Lie(J) with itself, then the differential of $\exp$ at 0 becomes the identity map

$$Lie(J) \to Lie(J).$$

As shown in Mumford's book [Mum70] on page 2, the exponential map

$$\exp : Lie(J) \to J(\mathbb{C})$$

is a surjective homomorphism of Lie groups with kernel a lattice L in $Lie(J)$. Moreover, it induces an isomorphism

$$Lie(J)/L \cong J(\mathbb{C}),$$

i.e. $J(\mathbb{C})$ is a complex torus.

Remark 4.1: The tangent space $Lie(J)$ of $J(\mathbb{C})$ at the identity carries a natural $\mathbb{Q}(\delta) \otimes_{\mathbb{Q}} \mathbb{C}$-module structure. For each field embedding $\tau : \mathbb{Q}(\delta) \hookrightarrow \mathbb{C}$ we define

$$Lie(J)_\tau = \{z \in Lie(J)| \ i(e)z = \tau(e)z \ \ \forall e \in \mathbb{Q}(\delta)\}$$

$$n_{\tau_i} = dim_{\mathbb{C}}(Lie(J)_{\tau_i}).$$

We note that for $\mathbb{Q}(\delta)$, we can define two such embeddings

$$\tau_i : \mathbb{Q}(\delta) \hookrightarrow \mathbb{C}$$

where $\delta \mapsto \zeta_3^{-i}$ and $i = 1, 2$.

We define the space of differentials of the first kind $\Omega^1(J)$ on $J(\mathbb{C})$ following Mumford's book [Mum70] on page 4. As above, the tangent space $Lie(J)$ is regarded as a complex vector space and let $T = Hom_{\mathbb{C}}(Lie(J), \mathbb{C})$ be the complex cotangent space to $J(\mathbb{C})$ at the identity. By translation with respect to the group law on $J(\mathbb{C})$, every complex covector $\alpha \in T$ extends to a translation invariant holomorphic form ω_α on $J(\mathbb{C})$. Moreover, the map $\alpha \mapsto \omega_\alpha$ defines an isomorphism

$$\mathcal{O}_X \otimes_{\mathbb{C}} T \cong \Omega^1.$$

In other words, Ω^1 is a globally free sheaf of $\mathcal{O}_X$-modules. And since the only global sections of $\mathcal{O}_X$ are constants, then the global sections of Ω^1 are the translation invariant forms ω_α.

More generally, Mumford's book [Mum70] on page 4 utilizes the complex compact manifold structure of $J(\mathbb{C})$ to compute the cohomology groups $H^q(J(\mathbb{C}), \Omega^p)$, where Ω^p is a sheaf of holomorphic p-forms on $J(\mathbb{C})$.

Remark 4.2: Let $\Omega^1(J)$ be the space of differentials of the first kind on J. It is well-known [Zar05a] that the natural map

$$\Omega^1(J) \to Hom_{\mathbb{C}}(Lie(J), \mathbb{C})$$

is an isomorphism. This isomorphism allows us to define, via duality,

$$\mathbb{Q}(\delta) \to End_{\mathbb{C}}(Hom_{\mathbb{C}}(Lie(J), \mathbb{C})) = End_{\mathbb{C}}(\Omega^1(J)).$$

This provides $\Omega^1(J)$ with the structure of $\mathbb{Q}(\delta) \otimes \mathbb{C}$-module in such a way that

$$\Omega^1(J)_{\tau_i} := \mathbb{C}_{\tau_i}\Omega^1(J) \cong Hom_{\mathbb{C}}(Lie(J)_{\tau_i}, \mathbb{C})$$

where

$$\mathbb{C}_{\tau_i}\Omega^1(J) = \{a \in Lie(J) \mid ea = \tau_i(e)a \ \ \forall e \in \mathbb{Q}(\delta)\}.$$

Now we have all the necessary ingredients to apply Corollary 2.2 from Yu. Zarhin's article Endomorphism algebras of superelliptic jacobians [Zar05a].

Theorem 4.2. With our setup, the center C_J of $End^0(J)$ is isomorphic to $\mathbb{Q}(\zeta_3)$.

Proof. We consider J as a complex abelian variety along with the two embeddings ($i = 1, 2$) of $\mathbb{Q}(\delta)$

$$\tau_i, : \mathbb{Q}(\delta) \hookrightarrow \mathbb{C} \quad \text{where } \delta \mapsto \zeta^{-i}.$$

Our goal is to apply Corollary 2.2 of [Zar05a], which will provide us with

$$C_J = \mathbb{Q}(\delta) \cong \mathbb{Q}(\zeta_3).$$

For this we need to satisfy the three conditions of Corollary 2.2 of [Zar05a]. Since $n = q^3 + 1$ and $p = 3$ are relatively prime numbers, it only remains to determine the multiplicities n_{τ_1} and n_{τ_2} to satisfy (iii) of Corollary 2.2 of [Zar05a]. We use the first displayed formula (1) of Section 2 in [Zar05a] (its second equality sign):

$$dim_{\mathbb{C}}(Lie(J)_{\tau_i}) = dim_{\mathbb{C}}(\Omega^1(J))_{\tau_i}). \tag{4.1}$$

We use the action of $i(E) = \mathbb{Q}(\delta)$ on $\Omega^1(J))$ to determine the multiplicities n_{τ_1} and n_{τ_2} using equality (6) above. In particular, since δ generates the field $\mathbb{Q}(\delta) \cong \mathbb{Q}(\zeta_3)$ over $\mathbb{Q}$, $\Omega^1(J)_{\tau_1}$ and $\Omega^1(J)_{\tau_2}$ are eigenspaces corresponding to eigenvalues $\tau_1(\delta) = \zeta_3^{-1}$ and $\tau_2(\delta) = \zeta_3^{-2} = \zeta_3$ respectively. Therefore n_{τ_i} coincides with the multiplicity of the eigenvalue ζ_3^{-i}. It follows from Remark 4.13 in [Zar05a] that

$$n_{\tau_1}(J, i) = \lfloor \frac{q^3 + 1}{3} \rfloor = \lfloor \frac{3^{6m+3} + 1}{3} \rfloor = \lfloor \frac{3^{6m+3}}{3} + \frac{1}{3} \rfloor = 3^{6m+3-1} = 3^{6m+2}$$

$$n_{\tau_2}(J, i) = \lfloor \frac{2(q^3 + 1)}{3} \rfloor = \lfloor \frac{2 \cdot 3^{6m+3} + 2}{3} \rfloor = \lfloor \frac{2 \cdot 3^{6m+3}}{3} + \frac{2}{3} \rfloor = 2 \cdot 3^{6m+3-1} = 2 \cdot 3^{6m+2}.$$

Now this coincides with the requirement (iii) of Corollary 2.2 in [Zar05a]. Thus, we obtain the required isomorphism

$$C_J = \mathbb{Q}(\delta) \cong \mathbb{Q}(\zeta_3).$$

□

Now we have all the necessary ingredients to prove Theorem 1.0 of Section 1.

Theorem 1.0. Let f be a polynomial with coefficients in k and of degree $n := \deg(f) = q^3 + 1$. Let C be the trigonal curve it describes via the equation $y^3 = f(x)$.

If $Gal(f)$ coincides with one of the 2-transitive Ree groups in the series $Ree(q) = {}^2G_2(q)$ for $q = 3^{2m+1}$, then the endomorphism algebra $End^0(J)$ of the Jacobian J of C is a simple algebra over its center

$$C_J \cong \mathbb{Q}(\zeta_3).$$

Proof. By Theorem 4.1, $End^0(J)$ is a simple algebra and, by Theorem 4.2, its center C_J is isomorphic to $\mathbb{Q}(\zeta_3)$. □

Chapter 5 | Explicit description of $J[\lambda]$

In this section we after a more explicit description of $J[\lambda]$ using constructions and definitions from Section 4 of Yu. Zarhin's paper "Hyperelliptic jacobians and modular representations" [Zar01]. This will allow us to obtain the absolute simplicity of $J[\lambda]$ when considered as a $Gal(f)$-module (see Theorem 5.3). We point out that these constructions and definitions are also covered in Section 7 of [Zar18].

Consider $\mathbb{F}_3^{\mathfrak{R}_f}$, the n-dimensional $\mathbb{F}_3$-vector space of maps $h : \mathfrak{R}_f \to \mathbb{F}_3$. The space $\mathbb{F}_3^{\mathfrak{R}_f}$ is provided with a natural action of $Perm(\mathfrak{R}_f)$, where each $s \in Perm(\mathfrak{R}_f)$ sends a map $h : \mathfrak{R}_f \to \mathbb{F}_3$ into $sh : r \mapsto h(s^{-1}(r))$ for $r \in \mathfrak{R}_f$. Furthermore, the action of $Gal(f) \subset \mathrm{Perm}(\mathfrak{R}_f)$ on $\mathfrak{R}_f$ gives rise to an n-dimensional linear representation

$$Gal(f) \to \mathrm{Aut}(\mathbb{F}_3^{\mathfrak{R}_f}),$$

where for $s \in Gal(f) \subset \mathrm{Perm}(\mathfrak{R}_f)$, $h \in \mathbb{F}_p^{\mathfrak{R}_f}$ and $r \in \mathfrak{R}_f$, we have $s \cdot h : r \to h(s^{-1}(r))$ for all $r \in \mathfrak{R}_f$.

The representation space contains the invariant line of constant functions $\mathbb{F}_3 \cdot 1_{\mathfrak{R}_f}$ and the $(n-1)$-dimensional stable hyperplane of functions

$$(\mathbb{F}_3^{\mathfrak{R}_f})^0 = \{h : \mathfrak{R}_f \to \mathbb{F}_3 | \sum_{\alpha \in \mathfrak{R}_f} h(\alpha) = 0\}.$$

$V_f = (\mathbb{F}_3^{\mathfrak{R}_f})^0$ is called the heart of $Gal(f)$ acting on the set $\mathfrak{R}_f$ over the field $\mathbb{F}_3$.

Consider the following remarks, similar to remarks of Section 4 of [Zar01].

Remark 5.1: The above construction can be carried out with an arbitrary field F instead of $\mathbb{F}_3$, consider the above construction with $F = \mathbb{Q}$. By [Ser77] Exercise 2.2, the character of $\mathbb{Q}^{\mathbb{R}_f}$ sends each element of the group into the number of its fixed points and takes values in $\mathbb{Z}$, it is called the permutation character of $\mathbb{R}_f$. We denote by $\chi_{\mathbb{R}_f}$ the character of $(\mathbb{Q}^{\mathbb{R}_f})^0$ and $1 + \chi_{\mathbb{R}_f}$ is the permutation character. It is known ([Ser77] Exercise 2.6) that the $Gal(f)$-module $(\mathbb{Q}^{\mathbb{R}_f})^0$ is absolutely simple if and only if $Gal(f)$ acts double-transitively on $\mathbb{R}_f$.

Remark 5.2: Let $Gal(f)^3$ be the set of 3-regular elements of $Gal(f)$. Clearly, the Brauer character of the $Gal(f)$-module $\mathbb{F}_3^{\mathfrak{R}_f}$ coincides with the restriction of $1 + \chi_{\mathbb{R}_f}$ to $Gal(f)^3$. Thus, the Brauer character of the $Gal(f)$-module $(\mathbb{F}_3^{\mathfrak{R}_f})^0$ coincides with the restriction of $\chi_{\mathbb{R}_f}$ to $Gal(f)^3$.

Remark 5.3: In case $Gal(f)$ acts 2-transitively on $\mathbb{R}_f$, $\#\mathbb{R}_f$ is not divisible by 3 and $\#\mathbb{R}_f - 1$ coincides with the highest power of 3 dividing $\#Gal(f)$, then by a theorem of Brauer-Nesbitt ([Hum87] pp.249) $(\mathbb{F}_3^{\mathfrak{R}_f})^0$ is an absolutely simple $Gal(f)$-module. In particular, it is the reduction of the Steinberg representation.

We also have the following result, as in Yu. Zarhin's paper [Zar18] Lemma 8.1 (we are in $p \nmid n$ case):

Theorem 5.1. $\mathrm{End}_{Gal(f)}((\mathbb{F}_3^{\mathfrak{R}_f})^0) \cong \mathbb{F}_3$ if and only if $Gal(f)$ is 2-transitive.

Proof. See proof of Lemma 8.1 in [Zar18]. □

Remark 5.4:

Let M be a maximal subgroup of $Ree(q)$. Theorem C on page 60 in [Kle88] tells us that any such group M is conjugate to one of the maximal groups listed in the table of Theorem C on page 60 in [Kle88]. Let us go through the list and determine their respective orders. We use the structure column of the table on page 61 of Theorem C in [Kle88] to determine the orders:

1. groups of order $q^3(q-1)$ with group structure $[q^3] : Z_{q-1}$;
2. groups of order $q^3 - q$ with group structure $2 \times L_2(q)$;

3. groups of order $12 \cdot (q-1)$ with group structure $(2^2 \times D_{(1/2)(q+1)}) : 3$;

4. groups of order $2^3 \cdot 7 \cdot 3$ with group structure $2^3 : 7 : 3$, only for $q = 3$;

5. groups of order $6(q + \sqrt{3q} + 1)$ with group structure $Z_{q+\sqrt{3q}+1} : Z_6$;

6. groups of order $6(q - \sqrt{3q} + 1)$ with group structure $Z_{q-\sqrt{3q}+1} : Z_6$;

7. groups of order $q_0^3(q_0^3+1)(q_0-1)$ for $q = q_0^a$ with group structure ${}^2G_2(q_0)$, where a and q_0 are positive integers;

8. groups of order 504 with group structure $L_2(8)$, only for $q = 3$.

   Note: We start at the top of the table and use the table's Structure column to compute the orders. For the sake of consistent ordering between our list and that of Theorem C on page 60 in [Kle88], we include cases for $q = 3$. As mentioned above, we use the group structure to determine the orders listed above.

From the orders of the groups in the list above one can easily tell that the maximal group of highest possible order must be conjugate to the maximal parabolic subgroup P of order $q^3(q-1)$. Thus, the order of M must satisfy:

$$\#M \leq q^3(q-1).$$

We can use the above results to show:

Theorem 5.2. $Gal(f)$-module $(\mathbb{F}_3^{\mathfrak{R}_f})^0$ is absolutely simple for $Gal(f) = Ree(q)$ and $q > 3$.

Proof. Let M be a maximal subgroup of $Ree(q)$, then, by Remark 5.4, we have $\#M \leq q^3(q-1)$. Thus, each subgroup of $Ree(q)$ has index $\geq q^3 + 1 = \#\mathbb{R}_f$, which implies that $Ree(q)$ acts transitively on $\mathbb{R}_f$. If a stabilizer $Ree(q)_r$ for some $r \in \mathbb{R}_f$ has index q^3+1, then it is a maximal subgroup by the same classification. Moreover, $Ree(q)_r$ is conjugate to the Borel subgroup B (normalizer of 3-Syllow subgroup) and the $Ree(q)$-set $\mathbb{R}_f$ is isomorphic to an ovoid $Ree(q)/B$ where the action of $Ree(q)$ is known to be 2-transitive ([B1̈4] Prop 3.2). Finally, we obtain our result by Remark 5.3, since

$$\#\mathbb{R}_f = q^3 + 1$$

and

$$\#\mathbb{R}_f - 1 = q^3$$

is the highest power of 3 dividing $\#Ree(q)$. □

Remark 5.5: It is known, see Section 7 of [Zar18], that $Gal(f)$-modules $V_f = (\mathbb{F}_3^{\mathfrak{R}_f})^0$ and $J[\lambda]$ are canonically isomorphic.

Theorem 5.3. $Gal(f)$-module $J[\lambda]$ is absolutely simple for $Gal(f) = Ree(q)$ and $q > 3$.

Proof. By Theorem 5.2 and Remark 5.5, $Gal(f)$-module $J[\lambda]$ is absolutely simple. □

Chapter 6 Very Simple

In this section we first use the definitions established in Yu. Zarhin's paper "Very Simple Representations: Variations on a Theme of Clifford" [Zar05b]. Results and definitions from [Zar05b] help us establish conditions in Corollary 6.2 for the very-simplicity (see Definition 6.1 below) of $Gal(f)$-module $J[\lambda]$. In the second part of this section we use definitions and results from R. Steinberg's paper "Representations of algebraic groups" [Ste63] and J. Humphrey's book "Ordinary and modular representations of Chevalley groups" [Hum76], all in pursuit of satisfying the conditions of Corollary 6.2.

We consider the notion of a very simple module as in Section 1 of [Zar05b] :

Definition 6.1: Let G be a group, V a vector space over a field F and

$$\rho : G \to \mathrm{Aut}_F(V)$$

a linear representation of G in V. We say G-module V is **very simple** if it satisfies the following property:
for any subalgebra $R \subset \mathrm{End}_F(V)$ containing the identity operator Id that is normal, i.e.,

$$\rho(\sigma)R\rho(\sigma)^{-1} \subset R \quad \text{for all } \sigma \in G$$

we have that $R = F \cdot Id$ or $R = \mathrm{End}_F(V)$.

Our goal is to show that the $Gal(f)$-module $V_f = (\mathbb{F}_3^{\mathfrak{R}_f})^0$ is very simple and, since $(\mathbb{F}_3^{\mathfrak{R}_f})^0$ and $J[\lambda]$ are canonically isomorphic $Gal(f)$-modules, the result will imply the very simplicity of the $Gal(f)$-module $J[\lambda]$.

Remark 6.1: What will the very simplicity of the $Gal(f)$-module $J[\lambda]$ achieve for us? It is known (Theorem 3.18 and Theorem 4.14 in [Zar05a]) that in characteristic 0 the very simplicity of the $Gal(f)$-module $J[\lambda]$ results in $E = \mathbb{Q}(\delta)$ coinciding with the centralizer $End^0(J, i)$ and it being the maximal commutative subalgebra in $End^0(J)$. This along with the fact that the center of $End^0(J)$ coincides with E, Theorem 4.16 in [Zar05a], will provide us with the required isomorphism of Theorem 1.1.

We establish conditions for the $Gal(f)$-modules $(\mathbb{F}_3^{\mathfrak{R}_f})^0$ to be very simple as in [Zar05b] .

Note: Since the Schur multiplier of $Ree(q)$ is trivial for $q > 3$, every projective (irreducible) representation of $Ree(q)$ (over an algebraically closed field) lifts to a linear (irreducible) representation.

Corollary 6.1. **(Corollary 4.2 in [Zar05b])**
Let us assume that either k is algebraically closed or G is a perfect and k is finite. Suppose V is a non-zero finite dimensional k-vector space and

$$\rho : G \to Aut_k(V)$$

is a linear representation of a group G over k. Then the G-module V is very simple if and only if all the following conditions hold:

(i) The G-module V is absolutely simple;

(ii) The G-module V does not admit a projective absolutely simple splitting;

(iii) The G-module V is not induced from a representation of a proper subgroup of finite index in G.

Proof. See proof of Corollary 4.2 in [Zar05b].

□

Since we know that all the projective representations of $Gal(f) = Ree(q)$ for $q > 3$, this allows us to obtain the following result by adjusting the result in [Zar05b] (Corollary 4.3 and its proof).

Corollary 6.2. **(Corollary 4.3 in [Zar05b])**
Suppose V is a non-zero finite-dimensional vector space over $\mathbb{F}_3$ and

$$G = Ree(q) \to Aut_{\mathbb{F}_3}(V)$$

is a linear representation. Then the G-module V is very simple if and only if all the following conditions hold:

(i) The G-module V is absolutely simple;

(ii) The G-module V does not split into a tensor product $V \cong V_1 \otimes_{\mathbb{F}_3} V_2$ of two absolutely simple $Ree(q)$-modules V_1 and V_2, both of dimension strictly greater than 1;

(iii) The G-module V is not induced from a representation of a proper subgroup of finite index in G.

Proof. See proof of Corollary 4.3 in [Zar05b].

□

Remark 6.2: If V is absolutely simple in the tensor product splitting

$$V \cong V_1 \otimes_{\mathbb{F}_3} V_2,$$

then V_1 and V_2 are both absolutely simple.

We have already established the absolute simplicity of the $Ree(q)$-module $(\mathbb{F}_3^{\mathfrak{R}_f})^0$, so we continue by establishing (ii).

Let's take a closer look at the construction of groups of Lie type. Recall that any twisted group G of Lie type is of the form $\mathbb{G}^{\mathcal{F}}$ where $\mathcal{F}$ is a Steinberg endomorphism (surjective homomorphism of $\mathbb{G}$ fixing only finitely many points) and $\mathbb{G}$ is a simply-connected algebraic group associated to G.

In our case, $G = Ree(q)$ with $q = 3^{2m+1} = 3^d > 3$ is a finite group of Lie type arising from a connected reductive algebraic group $\mathbb{G}_2$ over an algebraically closed filed $\overline{\mathbb{F}}_q$ of characteristic 3, which we denote by $\mathbb{G}_2(q)$. Since this group is defined over $\mathbb{F}_q$, the Frobenius map $\tau : u \mapsto u^3$ of $\overline{\mathbb{F}}_3$ induces a Frobenius endomorphism τ

of $\mathbb{G}_2(q)$. From the Dynkin diagram of $\mathbb{G}_2$ we can observe that $\mathbb{G}_2(q)$ has a special isogeny $\mathcal{F}$, such that $\mathcal{F}^2 = \tau$. For any positive odd integer $d > 1$ we have

$$Ree(3^d) = \mathbb{G}_2(q)^{\mathcal{F}^d},$$

a finite subgroup of $\mathcal{F}^d$-fixed points of $\mathbb{G}_2(q)$.

The irreducible representations of $Ree(q)$ over $\overline{\mathbb{F}}_3$ turn out to be the restrictions of irreducible representations of the algebraic group $\mathbb{G}_2(q)$ by the next theorem of Steinberg.

Theorem 6.3. (Steinberg's Restriction Theorem, Thm 1.3 in [Ste63]) Let $\mathbb{G}$ be a simple algebraic group over the field $\mathbb{F}_3$, let $\mathcal{F}$ be a Steinberg endomorphism on $\mathbb{G}$, then every simple $\mathbb{G}^{\mathcal{F}}$-module is the restriction of a simple $\mathbb{G}$-module.

Proof. See proof of Theorem 1.3 in [Ste63]. □

Since $Ree(q)$-module $V_f = (\mathbb{F}_3^{\mathfrak{R}_f})^0$ is absolutely simple by Theorem 5.3, Theorem 6.3 allows us to view it as a restriction of a simple $\mathbb{G}_2(q)$-module.

Definition: For any $\mathbb{G}_2(q)$-module M, we denote by $M^{[i]}$ the $\mathbb{G}_2(q)$-module obtained by composing the representation $\mathbb{G}_2(q) \to GL(M)$ with the endomorphism $\mathcal{F}^i$, we call such module the i**-th Frobenius twist** of M. Note that the isomorphism type of this module does not depend on the basis chosen for M.

The following part of this section involves the theory of weights and we refer the reader to the next section (**Section 7**) for details.

Since $\mathbb{G}_2(q)$ is simply connected, its group of rational characters $X(T)$ ($X(T)$ is the set of characters w.r.t maximal torus T, see Section 7) is a full lattice of weights of rank 2 with a basis consisting of the fundamental dominant weights $\{\bar{\omega}_1, \bar{\omega}_2\}$. The fundamental weight $\bar{\omega}_1$ corresponds to the short fundamental root α_1 in the root system Φ of $\mathbb{G}_2(q)$, while $\bar{\omega}_2$ corresponds to the long fundamental root α_2 ($< \bar{\omega}_i, \alpha_j^{\vee} >= \delta_{i,j}$, see Section 7). Theorem 7.1 in Section 7 allows us to characterize all simple $\mathbb{G}_2(q)$-modules M via their unique highest weight μ and we set $M = L(\mu)$ for such modules. Another result of Steinberg shows that these $\mathbb{G}_2(q)$-modules $L(\mu)$ can be described in terms of a finite number of them. In fact, we know more –

all simple $\mathbb{G}_2(q)$-modules $L(\mu)$ can be constructed out of a finite number of simple $\mathbb{G}_2(q)$-modules that correspond to the 3-restricted weights

$$X(T)_3 = \{c_1\bar{\omega}_1 + c_2\bar{\omega}_2 \mid 0 \le c_1, c_2 < 3\}.$$

Theorem 6.4. (see Humphrey's book [Hum76], §2.1)
For an arbitrary dominant weight μ consider its 3-adic expansion

$$\mu = \sum_{i=0}^{d-1} 3^i \bar{\omega}_i,$$

where $\bar{\omega}_i$ is a 3-restricted weight. Then

$$L(\mu) = L(\bar{\omega}_0) \otimes L(\bar{\omega}_1)^{[1]} \otimes \ldots \otimes L(\bar{\omega}_{d-1})^{[d-1]}$$

where $L(\bar{\omega}_j)^{[i]}$ is the i-th Frobenius twist of $L(\bar{\omega}_j)$.

Proof. See §2.1 (Theorem of Steinberg) in [Hum76]. □

We restrict our attention to the case of $Ree(q)$ in Theorem 2.4 in [Ble99], which provides us with a classification of the simple modules for the finite group $Ree(q)$ in terms of restrictions of simple $\mathbb{G}_2(q)$-modules. It actually tells us that all simple $Ree(q)$-modules can be constructed out of restrictions of the simple $\mathbb{G}_2(q)$-modules that correspond to the 3-restricted weights $\{c_1\bar{\omega}_1 \mid 0 \le c_1 < 3\}$.

Theorem 6.5. (Thm 2.4 in [Ble99] or Thm 7.4 and Thm 12.2 in [Ste63])
Let G be a Ree group of type $Ree(q)$ defined over $\mathbb{F}_q$ with $q = 3^d$,

$$X(T)'_3 = \{\mu = c_1\bar{\omega}_1 \mid 0 \le c_1 < 3\}$$

and $\mathcal{M}' = \{M_\mu \mid \mu \in X'_3\}$. Then every simple $Ree(q)$-module can be expressed uniquely as a tensor product

$$M_0 \otimes M_1^{[1]} \otimes \ldots \otimes M_{d-1}^{[d-1]}$$

with $M_i \in \mathcal{M}'$ and $M_j^{[i]}$ is the i-th Frobenius twist of M_j.

Proof. See proof of Thm 2.4 in [Ble99]. □

Theorem 7.1 in Section 7 allows us to characterize the irreducible representations of $\mathbb{G}_2(q)$ via their unique highest weights and we set $(\mathbb{F}_3^{\mathfrak{R}_f})^0 = L(\mu)$ for the $\mathbb{G}_2(q)$-module for some highest weight $\mu \in X(T)$.

Consider the tensor splitting of the $Ree(q)$-module $L(\mu) = V_1 \otimes_{\mathbb{F}_3} V_2$ as in (ii) of Corollary 6.2 and suppose that both of dimension of V_i are greater than 1. Since the dimension of $L(\mu)$ is equal to q^3 (multiple of 3) and it is absolutely simple, the modules V_i in the tensor splitting must have both dimensions that are multiples of 3 and must also be absolutely simple by Remark 6.1. By Theorem 6.3 and Theorem 6.4, such V_i can be constructed from the restrictions of $\mathbb{G}_2(q)$-modules that correspond to the 3-restricted weights whose dimensions are multiples of 3 and with $c_2 = 0$. Using the proof of Theorem 12.5 in [Ste63], we find out that there is only one such module $L(2\bar{\omega}_1)$ of dimension 27 corresponding to the 3-restricted weight $2\bar{\omega}_1$. Thus, if dimensions of V_i in the splitting $L(\mu) = V_1 \otimes_{\mathbb{F}_3} V_2$ are both greater than 1, then they both must be multiples of 3 and constructed from the restrictions of the simple $\mathbb{G}_2(q)$-module $L(2\bar{\omega}_1)$ and its Frobenius twists. We show in **Chapter 7** that no such modules V_i of dimension less than q^3 are possible over $\mathbb{F}_3$, thus eliminating the possibility of the tensor splitting into modules of dimensions greater than 1.

Chapter 7 | Weight theory

In this section we introduce the theory of weights to better understand the $\mathbb{G}_2(q)$-module structure of $L(2\bar{\omega}_1)$. Our goal is to show that $Ree(q)$-module V_f satisfies condition (ii) in Corollary 6.2, i.e. eliminating the possibility of its tensor splitting as in (ii) of Corollary 6.2.

Consider $\mathbb{G}_2$, a simply-connected reductive group over an algebraically closed field $\overline{\mathbb{F}}_q$ of characteristic 3, which we denote by $\mathbb{G}_2(q)$. Let $T \subset \mathbb{G}_2(q)$ be a maximal torus, then there is an associated root datum for $\mathbb{G}_2(q)$ given by $(X(T), \Phi, Y(T), \Phi^\vee)$ (see 7.4, 9.6 in [Spr09]) . We denote

$$X(T) = Hom(T, \overline{\mathbb{F}}_3^\times) \cong \mathbb{Z}^2$$

for the set of characters of T and

$$Y(T) = Hom(\overline{\mathbb{F}}_3^\times, T) \cong \mathbb{Z}^2$$

for its co-character group. Let $\{\alpha_1, \alpha_2\} \subset X(T)$ be a set of simple roots of $\mathbb{G}_2(\overline{\mathbb{F}}_3)$ with respect to the torus T and, similarly, $\{\alpha_1^\vee, \alpha_2^\vee\}$ is the set of co-roots. If M is any finite-dimensional $\mathbb{G}_2(q)$-module, then we may consider it as a T-module. This allows us to decompose the restriction of M to T as a sum of irreducible T-modules

$$M = \bigoplus_{\mu \in X(T)} M_\mu$$

where $t \in T$ acts by multiplication $\mu(t)$ on M. Note that only a finite number of M_μ in the sum decomposition are nonzero. Those μ for which M_μ is non-zero are called

weights, and M_μ are called **weight spaces**. The Weyl group

$$W = N_{\mathbb{G}_2(q)}(T)/T,$$

where $N_{\mathbb{G}_2(q)}(T)$ is the normalizer of T in $\mathbb{G}_2(q)$, acts on $X(T)$ and on $V = \mathbb{R} \otimes X(T)$, and permutes the weights of M. The weights of $\mathbb{G}_2(q)$-action on its own Lie algebra (adjoint representation) are called roots.

Not all of the elements of $X(T)$ can be weights of $\mathbb{G}_2(q)$-modules. The groups $X(T)$ and $Y(T)$ are in duality via a natural pairing

$$< \cdot, \cdot >: X(T) \times Y(T) \to \mathbb{Z},$$

which can be extended to an induced pairing on $(X(T) \otimes \mathbb{R}) \times (Y(T) \otimes \mathbb{R})$. This allows us to define weights in $X(T)$ as elements μ such that $< \mu, \alpha^\vee >$ is an integer for all roots α. The Euclidean space $X(T) \otimes \mathbb{R}$ allows us to define the fundamental weights $\bar{\omega_1}, \bar{\omega_2} \in X(T) \otimes \mathbb{R}$ as the dual $\mathbb{Z}$-basis of $\{\alpha_1^\vee, \alpha_2^\vee\}$, such that $< \bar{\omega_i}, \alpha_j^\vee >= \delta_{i,j}$. We have a partial ordering on the weights, where $\bar{\omega_1} \geq \bar{\omega_2}$ if and only if $\bar{\omega_2} - \bar{\omega_1}$ is a non-negative linear combination of simple roots. A weight μ is dominant if it is non-negative linear combination of the fundamental weights and we denote this set by $X(T)^+$. The group of p-restricted weights is denoted

$$X(T)_p = \{\sum c_i \bar{\omega_i} \mid 0 \leq c_i \leq p-1\}.$$

The Weyl group W is generated by reflections along α_i and under this action each orbit contains a unique dominant weight. Every weight is a conjugate under W to a unique dominant weight.

Let M be a simple $\mathbb{G}_2(q)$-module, the following result characterizes all such simple $\mathbb{G}_2(q)$-modules via their set of weights.

Theorem 7.1. (Theorem 2.1 in [Lü01]) With our setup $\mathbb{G}_2(q)$ and M.

(i) If M is irreducible then the set of weights of M contains a unique element μ such that for all weights ω of M we have $\omega \leq \mu$. The μ is called the highest weight of M and it is dominant.

(ii) An irreducible $\mathbb{G}_2$-module M is determined up to isomorphism by its highest weight.

(iii) For each dominant weight $\mu \in X(T)$ there is an irreducible $\mathbb{G}_2$-module $L(\mu)$ with highest weight μ.

Proof. See proof of Theorem 2.1 in [Lü01]. □

Definition: We define the **Weyl module** $V(\mu)$ for a highest weight μ to the distinguished finite-dimensional $\mathbb{G}_2(q)$-module $V(\mu)$, which is constructed in steps from the Lie Algebra of $\mathbb{G}_2(q)$ with the highest weight μ. This Lie Algebra posses a $\mathbb{Z}$-lattice which has a form that allows us to obtain the "generic" Weyl module over the integers $V(\mu)_{\mathbb{Z}}$, whose reduction module 3 provides us with $V(\mu)$, see chapter 3 in [Lü01] for details of construction.

By this theorem we can attach a highest weight $\mu \in X(T)$ to the simple $\mathbb{G}_2(q)$-module M. We denote $L(\mu)$ for the $\mathbb{G}_2(q)$-module corresponding to the highest weight μ and $V(\mu)$ denotes the Weyl module. Weyl module has a unique simple quotient isomorphic to $L(\mu)$. Theorem 6.4 tells us that all simple $\mathbb{G}_2(q)$-modules $L(\mu)$ can be constructed out of a finite number of simple $\mathbb{G}_2(q)$-modules that correspond to the 3-restricted weights

$$X(T)_3 = \{\sum c_i \bar{\omega_i} \mid 0 \leq c_1, c_2 < 3\}.$$

We are interested in those $\mathbb{G}_2(q)$-modules that restrict to simple $Ree(q)$-modules and Theorem 6.5 tells us that these modules are $L(0)$, $L(\bar{\omega_1})$ and $L(2\bar{\omega_1})$. Note that $0, \mu_1, 2\mu_1 \in X(T)_3^{'}$ from Theorem 6.5. Next, the proof of Theorem 12.5 in [Ste63] provides us with the dimensions of $L(0)$, $L(\bar{\omega_1})$ and $L(2\bar{\omega_1})$, they are 1,7, and 27 respectively. It is known (proof of Lemma 2.1 in [Sin93]) that

$$L(\bar{\omega_1}) \cong V(\bar{\omega_1})$$

and

$$L(2\bar{\omega_1}) \cong V(2\bar{\omega_1}).$$

Remark 7.1: We want to establish (ii) of Corollary 6.2 for the $Ree(q)$-module

V_f. In Section 6 we have determined that if dimensions of V_i in the tensor splitting

$$V_f = V_1 \otimes_{\mathbb{F}_3} V_2$$

are both greater than 1, then they both must be multiples of 3 and constructed from the restrictions of the simple $\mathbb{G}_2(q)$-modules corresponding to the 3-restricted weights. The only $\mathbb{G}_2(q)$-module that satisfies these conditions is $L(2\bar{\omega}_1)$, the 27-dimensional $\mathbb{G}_2(q)$-module that corresponds to the 3-restricted weight $2\bar{\omega}_1$.

We compute the character of the 27-dimensional irreducible $\mathbb{G}_2(q)$-module $L(2\bar{\omega}_1)$. For this we construct the fundamental weights for $\mathbb{G}_2(q)$ explicitly with the help of results in [Spr68] Section 4.9.

The character group $X(T)$ is spanned by 3 elements x_1, x_2, x_3 and the root system of type $\mathbb{G}_2$ is

$$\Phi = \{\pm x_i,\ x_i - x_j \mid i \neq j,\ \ i, j = 1, 2, 3\}$$

where $x_1 + x_2 + x_3 = 0$. For the sake of symmetry, we consider x_1, x_2, x_3 to be vectors living in a hyperplane of $\mathbb{R}^3$. The Weyl group of Φ is of order 12 and acts on $X(T)$ as follows: $w(x_i) = ex_{\pi(i)}$, where π is a permutation of $\{1, 2, 3\}$ and $e = \pm 1$. This is summarized in the **Figure 7.1** below:

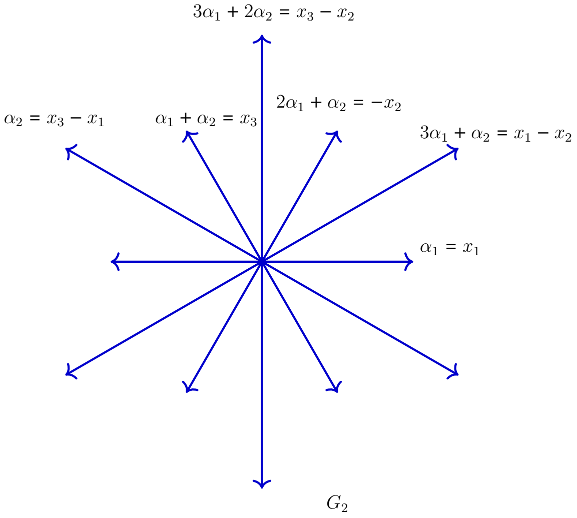
$3\alpha_1 + 2\alpha_2 = x_3 - x_2$
$2\alpha_1 + \alpha_2 = -x_2$
$\alpha_2 = x_3 - x_1$
$\alpha_1 + \alpha_2 = x_3$
$3\alpha_1 + \alpha_2 = x_1 - x_2$
$\alpha_1 = x_1$
G_2

Figure 7.1

The inner product is given by $< x_i, x_i >= 1$ and $< x_i, x_j >= -\frac{1}{2}$ if $i \neq j$. The fundamental weights are $\bar{\omega_1} = 2\alpha_1 + \alpha_2 = x_2 + x_3$ and $\bar{\omega_2} = 3\alpha_1 + 2\alpha_2 = x_3 - x_2$.

We denote by $\chi_V(\bar{\omega_1})$, $\chi_V(2\bar{\omega_1})$ the formal characters of the Weyl-modules $V(\bar{\omega_1})$, $V(2\bar{\omega_1})$. We use the table of weight decomposition numbers in characteristic 0 (Table 1 in [Spr68]) to compute them below. Note that the weight $\bar{\omega_1}$ corresponds to the index "11" in Table 1 – which means the character consists of the terms corresponding to the element $x_2 + x_3$ and its conjugates under the action of the Weyl group and the trivial one (we denote it as a (0)):

$$\chi_V(\bar{\omega_1}) = [(-x_2) + (x_2) + (-x_3) + (x_3) + (-x_2 - x_3) + (x_2 + x_3)] + (0).$$

Similarly, the weight $2\bar{\omega_1}$ corresponds to the index "20" in Table 1 of [Spr68]. The terms that are conjugate under the action of the Weyl group are arranged in square brackets:

$$\begin{aligned} \chi_V(2\bar{\omega_1}) = {} & [(-2x_2) + (2x_2) + (-2x_3) + (2x_3) + (-2x_2 - 2x_3) + (2x_2 + 2x_3)] \\ & + 2[(-x_2) + (x_2) + 2(-x_3) + (x_3) + (-x_2 - x_3) + (x_2 + x_3)] \\ & + [(-x_2 + x_3) + (x_2 - x_3) + (-2x_2 - x_3) + (x_2 + 2x_3) \\ & + (-x_2 - 2x_3) + (2x_2 + x_3)] + 3(0). \end{aligned}$$

Note: One can also use the functionality of the CHEVIE [MGP96] package (its scripts for recursive Freudentahl's formula) for GAP [GAP21] (requires version 4 or above) to verify these multiplicities.

We denote by $\chi_L(\bar{\omega_1})$, $\chi_L(2\bar{\omega_1})$ the formal characters of the $\mathbb{G}_2(q)$-modules $L(\bar{\omega_1})$, $L(2\bar{\omega_1})$ in characteristic 3.

Theorem 7.2. We have $\chi_L(\bar{\omega_1}) = \chi_V(\bar{\omega_1})$ and $\chi_L(2\bar{\omega_1}) = \chi_V(2\bar{\omega_1})$ in characteristic 3.

Proof. To show this we use Table 2 in [Spr68], which provides us with decomposition numbers in characteristic 3. In this table the weight $\bar{\omega_1}$ is indexed by "10" and the weight $2\bar{\omega}_1$ by "20". Looking at the values we can see that, after the reduction to characteristic 3 the Weyl module is actually simple and has only the trivial quotient. This results in the equality of their characters as required.

□

Let $\rho(0)$, $\rho(\bar{\omega}_1)$ and $\rho(\bar{\omega}_2)$ denote the 3-Brauer characters of $Ree(q)$ afforded by $L(0)$, $L(\bar{\omega}_1)$ and $L(2\bar{\omega}_1)$. For $\mathcal{F}$, the special isogeny of $Ree(q)$ whose square is the Frobenius, we define $\rho^{\mathcal{F}} = \rho \circ \mathcal{F}$. The special isogeny $\mathcal{F}$ comes from an automorphism of order 2 of the parent Chevalley group $\mathbb{G}_2$, which switches long roots and short roots and $Ree(q)$ is actually a set of fixed points of $\mathbb{G}_2$ under this action, see Chapter 12 in [Ste63]. Let $I = \mathbb{Z}/d\mathbb{Z}$, where $q = 3^{2m+1} = 3^d$, for any subset $J \subset I$ we denote $S(J)$ for set of all functions into the set $\{0, 1, 2\} \subset \mathbb{Z}$. An element $s \in S(I)$ can be written as $(s(0), s(1), ..., s(d-1))$, where $s(i)$ is the image of $i \in I$ under the function s.

For $s \in S$, we define

$$\rho_s = \prod_{s\in S} \rho(s(i)\mu_1)^{\mathcal{F}^i} \tag{7.1}$$

Remark 7.2: We use $I = \mathbb{Z}/d\mathbb{Z}$, since for any irreducible $Ree(q)$-module M its d-th Frobenius twist is isomorphic to the 0-th twist of M.

Remark 7.3: By our results in **Section 6** (Theorem 6.4 and Theorem 6.5),

$$\mathcal{B} = \{\rho_s \quad | \quad s \in S\} \tag{7.2}$$

is the set of all irreducible Brauer characters of $Ree(q)$.

We want to eliminate the possibility of tensor splitting of $V_f = (\mathbb{F}_3^{\mathfrak{R}_f})^0$ (as in (ii) of Corollary 6.2) by showing that the 27-dimensional representation $L(2\bar{\omega}_1)$, its Frobenius twists and their certain tensor products cannot be defined over the field $\mathbb{F}_3$. Recall from **Section 6**, we want to show $V_f = (\mathbb{F}_3^{\mathfrak{R}_f})^0$ is the smallest possible non-trivial $Ree(q)$-module of dimension a multiple of 3 that is defined over $\mathbb{F}_3$. With this goal in mind, we first determine how to compute the trace of character of $L(2\bar{\omega}_1)$ for $Ree(q)$ explicitly. Next lemma allows us to write down the Brauer character

$\rho(2\bar{\omega}_1)$ in terms of $\rho(\bar{\omega}_1)$ (character of the 7-dimensional irreducible module $L(\bar{\omega}_1)$).

Lemma 7.3. We have

(i) $\rho(2\bar{\omega}_1) = \rho(\bar{\omega}_1)^2 - 2\rho(\bar{\omega}_1) - \rho(\bar{\omega}_1)^{\mathcal{F}} - 1$

(ii) $\rho(2\bar{\omega}_1)\rho(\bar{\omega}_1) = \rho(\bar{\omega}_1)^{\mathcal{F}^2} + 2\rho(\bar{\omega}_1)\rho(\bar{\omega}_1)^{\mathcal{F}} + \rho(2\bar{\omega}_1) + 4\rho(\bar{\omega}_1) + 4\rho(\bar{\omega}_1)^{\mathcal{F}} + 1$

(iii) $\rho(2\bar{\omega}_1)^2 = \rho(\bar{\omega}_1)\rho(\bar{\omega}_1)^{\mathcal{F}^2} + 6\rho(\bar{\omega}_1)\rho(\bar{\omega}_1)^{\mathcal{F}} + \rho(2\bar{\omega}_1)\rho(\bar{\omega}_1)^{\mathcal{F}} + 2\rho(2\bar{\omega}_1) + 2\rho(2\bar{\omega}_1)^{\mathcal{F}} + 5\rho(\bar{\omega}_1) + 6\rho(\bar{\omega}_1)^{\mathcal{F}} + \rho(\bar{\omega}_1)^{\mathcal{F}^2} + 5$

Proof. See the proof of Lemma 2.1 in [Sin93]. □

In order to compute the trace of $\rho(2\bar{\omega}_1)$ explicitly, we obtain explicit formulas for the trace of $\rho(\bar{\omega}_1)$. We consider the matrix generators for the 7-dimensional representation $L(\bar{\omega}_1)$ as in [LN85]. Let $\theta = 3^m$ (where $q = 3^{2m+1}$), for $z \in \mathbb{F}_q$ and $a \in \mathbb{F}_q^\times$ we have:

$$\alpha(z) = \begin{bmatrix} 1 & z^{\theta} & 0 & 0 & -z^{3\theta+1} & -z^{3\theta+2} & z^{4\theta+2} \\ 0 & 1 & z & z^{\theta+1} & -z^{2\theta+1} & 0 & -z^{3\theta+2} \\ 0 & 0 & 1 & z^{\theta} & -z^{2\theta} & 0 & z^{3\theta+1} \\ 0 & 0 & 0 & 1 & z^{\theta} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -z & z^{\theta+1} \\ 0 & 0 & 0 & 0 & 0 & 1 & -z^{\theta} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{7.3}$$

$$\beta(z) = \begin{bmatrix} 1 & 0 & -z^{\theta} & 0 & -z & 0 & -z^{\theta+1} \\ 0 & 1 & 0 & z^{\theta} & 0 & -z^{2\theta} & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & z \\ 0 & 0 & 0 & 1 & 0 & z^{\theta} & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & z^{\theta} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{7.4}$$

$$\gamma(z) = \begin{bmatrix} 1 & 0 & 0 & -z^{\theta} & 0 & -z & -z^{2\theta} \\ 0 & 1 & 0 & 0 & -z^{\theta} & 0 & z \\ 0 & 0 & 1 & 0 & 0 & z^{\theta} & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & -z^{\theta} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{7.5}$$

$$h(a) = diagonal(a^{\theta}, a^{1-\theta}, a^{2\theta-1}, 1, a^{1-2\theta}, a^{\theta-1}, a^{-\theta}) \tag{7.6}$$

$$\Psi = antidiagonal(-1, -1, -1, -1, -1, -1, -1). \tag{7.7}$$

Remark 7.4: Using these generators we can define the Ree group as in [LN85]:

$$Ree(q) = \{\alpha(z), \beta(z), \gamma(z), h(a), \Psi \mid z \in \mathbb{F}_q, a \in \mathbb{F}_q^{\times}\}.$$

We define the subgroups of $Ree(q)$ consisting of upper triangular and diagonal matrices:

$$U(q) = \{\alpha(z), \beta(z), \gamma(z) \mid z \in \mathbb{F}_q\}$$
$$D(q) = \{h(a) \mid a \in \mathbb{F}_q^{\times}\}.$$

It is known (see [LN85]) that each element of $U(q)$ can be expressed uniquely as $S(a, b, c) = \alpha(a)\beta(b)\gamma(c)$ for $a, b, c \in \mathbb{F}_q$. We can notice that $U(q)$ is a Sylow 3-subgroup of $Ree(q)$ and $D(q) \cong \mathbb{F}_q^{\times}$.

Remark 7.5: An element $\zeta \in \mathbb{F}_q$ is called primitive if $\zeta \neq 0$ and its multiplicative order is $q - 1$ in the cyclic group $\mathbb{F}_q^{\times}$. Let $M < q - 1$ be a positive integer, then the set

$$\mu_M(\mathbb{F}_q) = \{a \in \mathbb{F}_q | a^M = 1\}$$

is a cyclic multiplicative subgroup of $\mathbb{F}_q^\times$ and its order M' divides both M and $q-1$. Since $M < q-1$ and $q-1$ is an even integer and $2 \le (q-1)/M'$, we have

$$M' = \#(\mu_M(\mathbb{F}_q) \le (q-1)/2.$$

Recall:

$$ABS_m := \{m \in \mathbb{Z}^+ | \quad \frac{q-1}{2} \text{ is prime}\},$$

$$COMP_m := \{m \in \mathbb{Z} | \;\; 1 \le n \le 752\}.$$

Remark 7.6: Why do we have

$$m \in ABS_m \cup COMP_m?$$

In Theorem 7.3, we show the non-existence of absolutely simple non-trivial $Ree(q)$-modules of dimension $< q^3$ that are multiples of 3, while the representation of dimension q^3 turns out to be the (reduction of) Steinberg representation (Remark 5.3) for $q = 3^{2m+1}$ and

$$m \in ABS_m \cup COMP_m.$$

This is done in two parts. Lemma 7.5 takes care of cases for

$$m \in COMP_m$$

with the aid of Lemma 7.4. In Lemma 7.4 we show that one can always find $\zeta \in \mathbb{F}_q^\times$ whose image under the explicit trace function, Lemma 7.3 (i), along with certain powers of this image, denoted by M (see Lemma 7.5), all do not lie in $\mathbb{F}_3$. We employ MAGMA [BCP97] to verify directly the statement of Lemma 7.4 for explicit cases of $m \in COMP_m$. If one can show the validity of Lemma 7.4 for all m, then Theorem 1.1 will hold for all cases of m. Lemma 7.6, kindly provided by Yu. Zarhin, takes care of cases for

$$m \in ABS_m.$$

Additionally, in the proof of Lemma 7.4 we explicitly verify the case of $m = 1$ by hand.

Let $u(\zeta) \in G$ be the pre-image of

$$h(\zeta) = diagonal(\zeta^{\theta}, \zeta^{1-\theta}, \zeta^{2\theta-1}, 1, \zeta^{1-2\theta}, \zeta^{\theta-1}, \zeta^{-\theta})$$

under the natural 7-dimensional representation $\rho(\bar{\omega_1})$ for a root of unity $\zeta \in \mathbb{F}_q$.

Lemma 7.4. Let $q = 3^{2m+1} = 3^d$ and $m \in COMP_m$, then there exists a root of unity $\zeta \in \mathbb{F}_q$ such that its image under the trace map $tr[\rho(2\bar{\omega_1})]$ has order:

$$\text{Order}(tr[\rho(2\bar{\omega_1})(u(\zeta))]) \geq \frac{(q-1)}{2}.$$

Additionally, we prove that the image $a := tr[\rho(2\bar{\omega_1})(u(\zeta))]$ has the property that $a^n \neq -1$ for any positive integer $n < (q-1)/8$. In particular, $a^n \notin \mathbb{F}_3$ for $n < (q-1)/8$.

Proof. The proof and verification consist of multiple parts:

1) Explicit trace formula computation;

Here we derive and compute the explicit formula (formula (14) below) for the trace of the 27-dimensional $tr[\rho(2\bar{\omega_1})]$ in terms of the 7-dimenisional $tr[\rho(\bar{\omega_1})]$.

2) Proof of the second part of lemma;

Here we prove the following statement: If image $a := tr[\rho(2\bar{\omega_1})(u(\zeta))]$ has order

$$order(a) \geq (q-1)/2$$

then $a^n \neq -1$ for any positive integer $n < (q-1)/8$.
Note: if we guarantee the existence of image a of $order(a) \geq (q-1)/2$, then $a^n \notin \mathbb{F}_3$ for any positive integer $n < (q-1)/8$.

3) Explicit verification for $m = 1$;

Here we explicitly verify lemma for $m = 1$ using the isomorphism $\mathbb{F}_{27} \cong \mathbb{F}_3[x]/(x^3 + 2x + 1)$ to show that the element $x \in \mathbb{F}_3[x]/(x^3 + 2x + 1)$ satisfies the conditions of our lemma, i.e., its image under the trace map $tr[\rho(2\bar{\omega_1})]$ has order equal to 26, and $26 \geq 13 = \frac{q-1}{2}$.

4) Outline of MAGMA verification;

Here we go over Python and MAGMA algorithms we've used to verify the lemma for values of $m \in COMP_m$. We use a Python algorithm to generate MAGMA script files $Magma\_m.txt$ for varying m. The MAGMA script $Magma\_m.txt$ contains MAGMA code on finding and verifying an element of order$\geq \frac{q-1}{2}$ (as required by the statement of the lemma) for specific value of m. These $Magma\_m.txt$ files (for multiple values of m) are then executed in parallel using threading and system calls to MAGMA (this allows us to compute multiple cases of m concurrently). We have verified the lemma for$m \in ABS_m \cap \{n \in \mathbb{Z} | n \leq 719\}$.

5) Description of contents/files of GitHub repository.

Here we go over the actual files used and their contents. All code used is available in our repository.

1) Explicit trace formula computation.

We derive explicit formula for the trace of the 27-dimensional $\rho(2\bar{\omega_1})$ in terms of the 7-dimensional $\rho(\bar{\omega_1})$ via Lemma 7.3 (i):

$$\rho(2\bar{\omega_1}) = \rho(\bar{\omega_1})^2 - 2\rho(\bar{\omega_1}) - \rho(\bar{\omega_1})^{\mathcal{F}} - 1.$$

One can find out (the last line of the first cont. paragraph on pp.328 of [Sin93]) that $\mathcal{F} := 3^{(d+1)/2}$ (or one can think of it as a square root of the Frobenius map), thus

$$\rho(2\bar{\omega_1}) = \rho(\bar{\omega_1})^2 - 2\rho(\bar{\omega_1}) - \rho(\bar{\omega_1})^{3^{(d+1)/2}} - 1.$$

Now we can compute the explicit formula for the trace of the 27-dimensional representation $tr(\rho(2\bar{\omega_1}))$ using the trace of the 7-dimensional

$$h(\zeta) = diagonal(\zeta^{\theta}, \zeta^{1-\theta}, \zeta^{2\theta-1}, 1, \zeta^{1-2\theta}, \zeta^{\theta-1}, \zeta^{-\theta})$$

with $\theta = 3^m$. We split the computation into three parts corresponding to the three non-constant terms in the above displayed formula.

- $\rho(\bar{\omega_1})^2$:

$$(\zeta^{\theta}+\zeta^{1-\theta}+\zeta^{2\theta-1}+1+\zeta^{1-2\theta}+\zeta^{\theta-1}+\zeta^{-\theta})^2 = \zeta^{2\theta}+\zeta^{-2\theta}+\zeta^{2\theta-2}+\zeta^{-2\theta+2}+\zeta^{4\theta-2}+\zeta^{-4\theta+2}+1+$$

$$+2[\zeta^1+\zeta^{-1}+\zeta^{3\theta-1}+2\zeta^{\theta}+2\zeta^{-\theta}+2\zeta^{1-\theta}+2\zeta^{\theta-1}+2\zeta^{2\theta-1}+2\zeta^{-2\theta+1}+\zeta^{2-3\theta}+\zeta^{3\theta-2}+3];$$

- $2\rho(\bar{\omega_1})$:

$$2(\zeta^{\theta}+\zeta^{1-\theta}+\zeta^{2\theta-1}+1+\zeta^{1-2\theta}+\zeta^{\theta-1}+\zeta^{-\theta});$$

- $\rho(\bar{\omega_1})^{3^{(d+1)/2}}$:

  since $3^{(d+1)/2} = 3^{\frac{2m+1+1}{2}} = 3^{m+1} = 3\theta$ and since $x^{3\theta^2} = x$ for all $x \in \mathbb{F}_q$, we have $3\theta^2 = 1$ (in the exponent):

$$(\zeta^{\theta}+\zeta^{1-\theta}+\zeta^{2\theta-1}+1+\zeta^{1-2\theta}+\zeta^{\theta-1}+\zeta^{-\theta})^{3\theta} = \zeta^{3\theta^2}+\zeta^{3\theta-3\theta^2}+\zeta^{6\theta^2-3\theta}+1+\zeta^{3\theta-6\theta^2}+\zeta^{3\theta^2-3\theta}+\zeta^{-3\theta^2}$$

$$= \zeta^1+\zeta^{3\theta-1}+\zeta^{2-3\theta}+1+\zeta^{3\theta-2}+\zeta^{1-3\theta}+\zeta^{-1}.$$

Now we combine all the terms:

$$tr[\rho(2\bar{\omega_1})(\zeta)] =$$

$\zeta^{2\theta}+\zeta^{-2\theta}+\zeta^{2\theta-2}+\zeta^{-2\theta+2}+\zeta^{4\theta-2}+\zeta^{-4\theta+2}+1+2[\zeta^1+\zeta^{-1}+\zeta^{3\theta-1}+2\zeta^{\theta}+2\zeta^{-\theta}+2\zeta^{1-\theta}+2\zeta^{\theta-1}+2\zeta^{2\theta-1}+2\zeta^{-2\theta+1}+\zeta^{2-3\theta}+\zeta^{3\theta-2}+3]-2(\zeta^{\theta}+\zeta^{1-\theta}+\zeta^{2\theta-1}+1+\zeta^{1-2\theta}+\zeta^{\theta-1}+\zeta^{-\theta})-(\zeta^1+\zeta^{3\theta-1}+\zeta^{2-3\theta}+1+\zeta^{3\theta-2}+\zeta^{1-3\theta}+\zeta^{-1})-1.$

Now we combine the like terms and obtain:

$$tr[\rho(2\bar{\omega_1})(\zeta)] = [\zeta^{2\theta} + \zeta^{-2\theta}] + [\zeta^{2\theta-2} + \zeta^{-2\theta+2}] + [\zeta^{4\theta-2} + \zeta^{-4\theta+2}] + [\zeta^{1} + \zeta^{-1}]+$$

$$+[\zeta^{1-3\theta} + \zeta^{3\theta-1}] + [2\zeta^{\theta} + 2\zeta^{-\theta}] + [2\zeta^{1-\theta} + 2\zeta^{\theta-1}] + [2\zeta^{2\theta-1} + 2\zeta^{-2\theta+1}]+$$

$$[\zeta^{2-3\theta} + \zeta^{3\theta-2}] + 1. \tag{7.8}$$

Proof of the second part of lemma :

In this part we show that the image $a := tr[\rho(2\bar{\omega_1})(u(\zeta))]$ of order $order(a) \geq (q-1)/2$ has the property that $a^n \neq -1$ for any positive integer $n < (q-1)/8$. We employ an argument by contradiciton to show this.

Suppose there exists some positive integer $k < (q-1)/8$ such that $a^k = -1$. Then we have

$$a^k \cdot a^k = (-1) \cdot (-1) = 1,$$

which implies $a^{2k} = 1$. Now since $2k < (q-1)/4 < (q-1)/2$ we arrive at a contradiction, since by assumption $order(a) \geq (q-1)/2$.

Explicit verification for m=1 :

Let $m = 1$, then

$$tr[\rho(2\bar{\omega_1})(\zeta)] = [\zeta^{6} + \zeta^{-6}] + [\zeta^{4} + \zeta^{-4}] + [\zeta^{10} + \zeta^{-10}]+$$

$$+[\zeta^{1} + \zeta^{-1}] + [\zeta^{-8} + \zeta^{8}] + [2\zeta^{3} + 2\zeta^{-3}] + [2\zeta^{-2} + 2\zeta^{2}] + [2\zeta^{5} + 2\zeta^{-5}]+$$

$$[\zeta^{-7} + \zeta^{7}] + 1.$$

For $q = 27$ we have $\mathbb{F}_{27} \cong \mathbb{F}_3[x]/(x^3+2x+1)$. Let $\zeta = x \in \mathbb{F}_3[x]/(x^3+2x+1)$, then

$$tr[\rho(2\bar{\omega}_1)(x)] = [x^6 + x^{-6}] + [x^4 + x^{-4}] + [x^{10} + x^{-10}]+$$

$$+[x^1 + x^{-1}] + [x^{-8} + x^8] + [2x^3 + 2x^{-3}] + [2x^{-2} + 2x^2] + [2x^5 + 2x^{-5}] + [x^{-7} + x^7] + 1 =$$

$$[x^6 + x^{20}] + [x^4 + x^{22}] + [x^{10} + x^{16}]+$$

$$+[x^1 + x^{25}] + [x^{18} + x^8] + [2x^3 + 2x^{23}] + [2x^{24} + 2x^2] + [2x^5 + 2x^{21}] + [x^{19} + x^7] + 1$$

since $x^3 + 1 = -2x = x$, we have $x^3 = x - 1$;

since $x^4 + 2x^2 + x = 0$, we have $x^4 = -2x^2 - x = x^2 + 2x$;

we have $2x^2 = 2(x^3 + 1)^2 = 2x^6 + x^3 + 2$, while also $2x^2 = -x^4 - x = 2x^4 + 2x$;

we have $2x^5 = 2x^2x^3 = 2(2x^4 + 2x)(x - 1) = x^5 + 2x^4 + x^3 + 2x$;

we have $x^6 = (x^3)^2 = (x - 1)^2 = x^2 + x + 1$;

we have $x^7 = x^3x^4 = (x - 1)(-2x^2 - x) = x^3 + x^2 + x$;

we have $x^8 = (x^4)^2 = (x^2 + 2x)^2 = x^4 + x^3 + x^2 = x^2 + 2x + x^3 + x^2 = x^3 + 2x^2 + 2x$;

we have $x^9 = (x^3)^3 = (x - 1)^3 = x^3 - 1$;

we have $x^{10} = x^6x^4 = (x^2 + x + 1)(x^2 + 2x) = x^4 + 2x = x^2 + 2x + 2x = x^2 + x$;

we have $x^{16} = x^{10}x^{6} = (x^4 + 2x)(x^2 + x + 1) = x^6 + x^5 + x^4 + 2x^3 + 2x^2 + 2x = 2x + 1;$

we have $x^{18} = (x^9)^2 = (x^3 - 1)^2 = x^6 - 2x^3 + 1 = x^2 + x + 1 + x^3 + 1 = x^3 + x^2 + x + 2;$

we have $x^{19} = x^{10}x^{9} = (x^4 + 2x)(x^3 - 1) = x^7 + x^4 + x = x^3 + x^2 + x + x^4 + x = x^4 + x^3 + x^2 + 2x = x^2 + 2x + x^3 + x^2 + 2x = x^3 + 2x^2 + x$

we have $x^{20} = (x^{10})^2 = (x^2 + x)^2 = x^4 + 2x^3 + x^2 = x^2 + 2x + 2x^3 + x^2 = 2x^3 + 2x^2 + 2x;$

we have $x^{21} = (x^{10})^2 x = (x^2 + x)^2 x = x^5 + 2x^4 + x^3 = x^5 + x^3 + 2x^2 + x;$

we have $x^{22} = x^{21}x = (x^5 + 2x^4 + x^3)x = x^6 + 2x^5 + x^4 = 2x^5 + x^2 + x + 1 + x^2 + 2x = 2x^5 + 2x^2 + 1;$

we have $x^{23} = x^{21}x^2 = (x^5 + 2x^4 + x^3)x^2 = x^7 + 2x^6 + x^5 = x^3 + x^2 + x + 2(x^2 + x + 1) + x^5 = x^5 + x^3 + 2;$

we have $x^{24} = x^{23}x = (x^5 + x^3 + 2)x = x^6 + x^4 + 2x = x^2 + x + 1 + x^2 + 2x + 2x = 2x^2 + 2x + 1;$

we have $x^{25} = x^{24}x = (2x^2 + 2x + 1)x = 2x^3 + 2x^2 + x.$

we plugin the above equations and obtain:

$$[x^2 + x + 1 + 2x^3 + 2x^2 + 2x] + [x^2 + 2x + 2x^5 + 2x^2 + 1] + [x^2 + x + 2x + 1] +$$

$$+ [x + 2x^3 + 2x^2 + x] + [x^3 + x^2 + x + 2 + x^3 + 2x^2 + 2x] + [2x - 2 + 2x^5 + 2x^3 + 1]$$

$$+ [4x^2 + 4x + 2 + 2x^2] + [2x^5 + 2(x^5 + x^3 + 2x^2 + x)] + [x^3 + 2x^2 + x + x^3 + x^2 + x] + 1 =$$

$$[2x^3+1]+[2x^5+2x+1]+[x^2+1]+$$

$$+[2x^3+2x^2+2x]+[2x^3+2]+[2x^5+2x^3+2x+2]+$$

$$+[4x+2]+[x^5+2x^3+x^2+2x]+[2x^3+2x]+1=$$

$$2x^3+1+2x^5+2x+1+x^2+1+2x^3+2x^2+2x+2x^3+2+2x^5+2x^3+2x+2+$$

$$+4x+2+x^5+2x^3+x^2+2x+2x^3+2x+1=2x^5+x^2+2x+1=$$

$$x^5+2x^4+x^3+2x+x^2+2x+1=x^5+2x^2+x+x^3+2x+x^2+2x+1=$$

$$x^5+x^3+2x+1=x^5$$

The last equality sign follows from the fact that $x^3+2x+1=0$.

Clearly, the order of $x^5 \in \mathbb{F}_3[x]/(x^3+2x+1)$ is 26 and $26 \geq \frac{27-1}{2} = 13$.

Outline of MAGMA verification:
We employ MAGMA [BCP97] and Python [VRD09] to verify the statement of our lemma for fixed values $m \in ABS_m \cap \{n \in \mathbb{Z} | n \leq 719\}$. For each case of m with $q = 3^{2m+1}$ in this range, we have verified that one can pick a primitive root of unity $\zeta \in \mathbb{F}_q$ such that its image under the trace map, $image := tr[\rho(2\bar{\omega}_1)(u(\zeta))]$, has order greater or equal to $(q-1)/2$.

This verification is carried out in steps, where we first use Python to generate MAGMA templates for various cases of m and then execute these templates in parallel instances of MAGMA, i.e., we use threading to outsource each computation (for a single instance of m) to the available cores of the CPU using system calls to MAGMA. For example: one can use shell (command line) to run any magma script by executing MAGMA script file (say with name filename)

```
> magma filename
```

Thus, we execute our Python generated script $Magma\_m.txt$ for some m via executing in shell:

```
> magma Magma_m.txt
```

The reader can find the code in our GitHub repository. Also, in the next subsection we describe the files and contents of our Github repository.

Let us first go over the Python-part of the code. In

$$magma\_script\_generator\_dickson.py$$

a user can set a range for m by setting the global variables M (first value of m) and END_VALUE (last value of m). Executing this script will generate MAGMA template files $Magma\_m.txt$ for m set in the range from M to End_Value. For more details on the Python algorithm see the next subsection describing the contents of

$$magma\_script\_generator\_dickson.py.$$

Let us go over the contents of one such file $Magma\_1.txt$ for $m = 1$.

Below are the contents of the file $Magma\_1.txt$ with our comments that explain the steps:

(comments are given after //, MAGMA's parser ignores the text that follows after)

```
F:=FiniteField(3,3);       // Defines the finite field F_27
a:= PrimitiveElement(F);  // Provides a primitive root of unity
P<x>:=PolynomialRing(F);  // Polynomial ring over F in x
b:= a+a^-1;               // Element a+1/a using primitive root a
```

```
tr:=DicksonFirst(6, 1)+DicksonFirst(4, 1)+ DicksonFirst(10, 1)+
    DicksonFirst(1, 1)+DicksonFirst(8, 1)+2*DicksonFirst(3, 1)+
    2*DicksonFirst(2, 1)+2*DicksonFirst(5, 1)+DicksonFirst(7, 1)+1;

    // we define trace (11) as a linear combination of Dickson
    // polynomials for optimization purposes.

image:= Evaluate(tr, b); // Defines the value of b under tr

if Order(image) lt 13 then PrintFile("Output_1", "False"); end if;

// We check the order of image, if it is <(q-1)/2 we create a file
// Output_1.txt and write "False" inside.
```

Let us go over the steps of a general algorithm (we generate the specific values template for fixed m using Python, see $magma\_script\_generator\_dickson.py$ in the next subsection). First we define the field F based on the odd power of 3 using the built-in function $F := FiniteField(3, 2m + 1)$. Then we define the polynomial ring P in variable x via

$$P < x >:= PolynomialRing(F)$$

and element b which is the sum of a primitive root of unity $a \in F$ and its inverse a^{-1}. Next we define the trace function tr as a linear combination of Dickson polynomials using formula (14), this optimization was communicated by the author's advisor Y. Zarhin. We note that $DicksonFirst(n, 1) = x^n$ and our formula (14) is a polynomial in a variable $x = \zeta + \frac{1}{\zeta}$. In the next step we evaluate trace function tr at the element b using $image := Evaluate(tr, b)$. Now in the last step we need to verify that the order of $image$ is greater or equal to $(q - 1)/2$, we do this with the $If...then$ statement in MAGMA. In case $Order(image) < (q - 1)/2$, our algorithm creates a file $Output\_m.txt$ with entry (a string) $False$ using

$$PrintFile("Output\_1", "False").$$

Next part of our algorithm is a Python script $magma\_threading.py$, which is used to execute multiple *Magma_m.txt* scripts concurrently using system calls to MAGMA via shell command

```
> magma Magma_m.txt
```

User can set the range of m in Python file *magma_threading.py* in our repository by defining *start* and *end* values for the function *run_threaded_magma_scripts*().

Verification has been carried out for values of $m \in COMP_m$.

Description of contents/files of GitHub repository
Our script consists of two parts:

- *magma_script_generator_dickson.py*:

  Contains the function *main*() with attributes/global-variables of M and End_Value, which define the range of m when generating MAGMA script templates. For a set values of m this function computes related values used in MAGMA template code, such as q and exponents c_i used in the i^{th} Dickson polynomial $DicksonFirst(c\_i, 1)$. Note that $DicksonFirst(c\_i, 1) = x^{c\_i}$ and c_i comes from the exponents of (14) considered as a polynomial in $x = \zeta + 1/\zeta$ and we can express (14) as a linear combination of Dickson polynomials $DicksonFirst(c\_i, 1)$. Below is a snippet of our Python-code, where we define the required values and MAGMA code template line by line:

```
for m in range(M, END_VALUE):
    q = 3 ** (2 * m + 1)
    q_minus_1_over_2 = int((q - 1) / 2)
    q_minus_1_over_8 = int((q - 1) / 8)
    field_entry = 2 * m + 1
    t = 3 ** m
    # here we compute the exponent coefficients
    # (pairwise positive and negative)
    c_1 = 2 * t
    c_2 = 2 * t - 2
    c_3 = 4 * t - 2
    c_4 =  3 * t -1
```

```
c_5 = t - 1
c_6 = 2 * t - 1
c_7 = 3 * t - 2

# last digit indicates line number in magma script file
finite_field_1 = f’F:=FiniteField(3,{field_entry});’
primitive_2 = f’a:= PrimitiveElement(F);’
polynomial_ring_3 = f’P<x>:=PolynomialRing(F);’
sum_inverse_4 = f’b:= a+a^-1;’

dickson_1 = f’d_1:=DicksonFirst({c_1}, 1);’
dickson_2 = f’d_2:=DicksonFirst({c_2}, 1);’
dickson_3 = f’d_3:=DicksonFirst({c_3}, 1);’
dickson_4 = f’d_4:=DicksonFirst(1, 1);’
dickson_5 = f’d_5:=DicksonFirst({c_4}, 1);’
dickson_6 = f’d_6:=DicksonFirst({t}, 1);’
dickson_7 = f’d_7:=DicksonFirst({c_5}, 1);’
dickson_8 = f’d_8:=DicksonFirst({c_6}, 1);’
dickson_9 = f’d_9:=DicksonFirst({c_7}, 1);’

trace_formula_6 = f’tr:=DicksonFirst({c_1}, 1)+
DicksonFirst({c_2}, 1) + DicksonFirst({c_3}, 1)+
DicksonFirst(1, 1)+DicksonFirst({c_4}, 1)
+2*DicksonFirst({t}, 1)+2*DicksonFirst({c_5}, 1)+
2*DicksonFirst({c_6}, 1) +
DicksonFirst({c_7}, 1)+1;’
image_6 = f’image:= Evaluate(tr, b);’
order_image_7 = f’if Order(image) lt {q_minus_1_over_2}
then PrintFile("Output_{m}", "False"); end if;’
```

We use this code to generate a string template of MAGMA code in the file $Magma\_m.txt$, where we plug-in those computed values for respective parts. For example if one sets $M = 1$ and $End\_Value = 10$ and executes this script, it will generate ten files $Magma\_1.txt$, $Magma\_2.txt$, ... , $Magma\_10.txt$. Each such file contains code for the specific value of m, we provide an example of contents for $Magma\_7.txt$ below (some lines are cut to fit the page):

```
F:=FiniteField(3,15);
a:= PrimitiveElement(F);
P<x>:=PolynomialRing(F);
b:= a+a^-1;
tr:=DicksonFirst(4374, 1)+DicksonFirst(4372, 1)+
DicksonFirst(8746, 1)+ DicksonFirst(1, 1)+
DicksonFirst(6560, 1)+2*DicksonFirst(2187, 1)+
2*DicksonFirst(2186, 1)+2*DicksonFirst(4373, 1)+
DicksonFirst(6559, 1)+1;



image:= Evaluate(tr, b);
if Order(image) lt 7174453 then PrintFile("Output_7", "False");
end if;
```

- $magma\_threading.py$:

  These files defines a function $run\_threaded\_magma\_scripts(start, end)$, where the user can set the range for m by setting start and end values, which takes $Magma\_m.txt$ as inputs and runs them concurrently using threading and system calls:

  ```
      > magma Magma_m.txt
  ```

  The user can set the variable $THREADS$ according to number of CPU cores available for computation.

- $magma\_script\_generator.py$:

  Version of MAGMA script generator that uses direct trace computation without the use of Dickson polynomials.

□

We can finally prove that the only irreducible representation of $Ree(q)$ with dimension a multiple of 3 which is defined over $\mathbb{F}_3$ is the (reduction of) Steinberg representation. The following result is an adjustment of Lemma 4.2 in [Zar03] to our case.

Lemma 7.5. Let $G = Ree(q)$ with $q = 3^{2m+1} = 3^d > 3$ for $m \in COMP_m$ and let $\zeta \in \mathbb{F}_q$ be a primitive root of unity, we denote by $u = u(\zeta) \in G$ the preimage of

$$h(\zeta) = diagonal(\zeta^{\theta}, \zeta^{1-\theta}, \zeta^{2\theta-1}, 1, \zeta^{1-2\theta}, \zeta^{\theta-1}, \zeta^{-\theta})$$

under the natural faithful 7-dimensional representation $\rho(\mu_1)$. For all $j = 1, ..., d-1$, we denote $W_j = L(2\mu_1)^{[j]}$ for the j-th Frobenius twist of $L(2\mu_1)$ with

$$\rho_j : G \to GL(W_j)$$

Let S be a subset of $\{0, 1, ..., d-1\}$, we define an $\bar{\mathbb{F}}_3$-representation ρ_S of G as the tensor product of the representations ρ_i for all $i \in S$. If S is a proper subset of $\{0, 1, ..., d-1\}$, then there exists an element $u \in G$ such that the trace $\rho_S(u)$ does not belong to $\mathbb{F}_3$.

Proof. For any $u \in G$ we have $tr(\rho_i(u)) = tr(\rho_0(u))^{3^i}$ by our above results, which clearly implies

$$tr(\rho_S(u)) = \prod_{i \in S} tr(\rho_i(u)) = tr(\rho_0(u))^M$$

where $M = \sum_{i \in S} 3^i$. For a proper subset S of $\{0, 1, ..., d-1\}$, we have

$$0 < M < \sum_{i=0}^{d-1} 3^i = \frac{3^d - 1}{2} = \frac{q-1}{2}.$$

Actually, we can make this bound better (the author is grateful to Yu. Zarhin, who suggested the new bound and communicated its proof over email):

The trace formula is (14) in the proof of Lemma 7.4 is a degree $4\theta - 2$ polynomial $P(x)$ in $x = \zeta + \zeta^{-1}$. The set

$$U = \{\zeta + \zeta^{-1} \mid \zeta \in \mathcal{F}_q^*\}$$

consists of $(q-1)/2 = (3\theta^2 - 1)/2$ elements. We need to check that for each proper subset S of $A = \{0, 1, \dots, 2m\}$ there is $b \in U$ such that $b^{M(S)} \notin \mathcal{F}_3$ where

$$M(S) = \sum_{i \in S} 3^i.$$

Suppose that it's not true. We call a proper subset S of A bad if for all $b \in U$ $b^{M(S)} \in \mathcal{F}_3$ (i.e., $b^{M(S)}$ is $0, 1$ or -1). Notice that if S is bad then its complement

$$A \setminus S$$

is also bad. We have

$$M(S) + M(A \setminus S) = (q-1)/2.$$

On the other hand, if bad S does NOT contain 0 then $T = \{i-1, i \in S\}$ is also bad, because

$$b^{M(S)} = (b^{M(T)})^3.$$

Let S be a bad set with the smallest possible $M(S) =: M$. Then it must contain 0. We need to arrive to a contradiction. The complement $S_1 = A \setminus S$ is bad and does NOT contain 0, hence, there is bad T_1 such that $M(S_1) = 3M(T_1)$. By assumption

$$M(T_1) \geq M(S) = M.$$

We have

$$3M \leq 3M(T_1) = M(S_1) = (q-1)/2 - M,$$

i.e.,

$$3M \leq (q-1)/2 - M,$$

i.e.,

$$M \leq (q-1)/8.$$

Actually, the inequality is strong, because $(q-1)$ is not divisibly by 8 and even by 4.

Thus, since $(q-1)/2$ is odd we have $M < (q-1)/8$. Next, by Lemma 7.4, for $1 \leq m \leq 719$ there exists a primitive root of unity $\zeta \in F_q^{\times}$ such that for $u = u(\zeta)$ with $a = tr(\rho_S(u))$ we have

$$\text{Order}[a] = \text{Order}[tr(\rho_S(u))] \geq \frac{(q-1)}{2}$$

and $a^M \neq \pm 1$. Hence, if we pick $u = u(\zeta)$ for such ζ, then we have

$$tr(\rho_S(u)) = tr(\rho_0(u))^M = a^M \notin \mathbb{F}_3$$

By Remark 7.3, we know that ρ_S exhaust the list of all absolutely irreducible representations of G. The case of empty S corresponds to the trivial representation and the case $S = \{1, ..., d-1\}$ is the (reduction of) Steinberg representation (Remark 5.3).

□

Notation: we recall

$$ABS_m := \{m \in \mathbb{Z}^+ | \quad \frac{q-1}{2} \text{ is prime}\},$$

$$COMP_m := \{m \in \mathbb{Z} | \ 1 \leq n \leq 752\}.$$

The next lemma and its proof (kindly provided by Yu. Zarhin) take care of cases for

$$m \in ABS_m.$$

Lemma 7.6. Let $G = Ree(q)$ with $q = 3^{2m+1}$ and $m \in ABS_m$, then we can find $b \in \mathbb{F}_q$ such that

$$tr[\rho(2\bar{\omega}_1)(b)]^M \notin \mathbb{F}_3, \quad \text{for } \ 1 \leq M \leq (q-1)/8.$$

Proof. First, recall $q = 3^{2m+1}$ for positive integers m and $\theta = 3^m$. Note that the explicit trace formula (14) tells us that $tr[\rho(2\bar{\omega}_1)]$ can be considered to be a degree $4\theta - 2$ polynomial $P(x)$ in $x = \zeta + \zeta^{-1}$ for which we define the set

$$U = \{\zeta + \zeta^{-1} \mid \zeta \in \mathcal{F}_q^*\},$$

which consists of $(q-1)/2 = (3\theta^2 - 1)/2$ elements. We will show that for $m \in ABS_m$ there is a $b \in U$ which satisfies the conditions of the Lemma, by showing that $P(x)$ takes more than three distinct values on the set U, i.e., we can always pick $b \in U$

such that

$$tr[\rho(2\bar{\omega}_1)(b)]^M = P(b)^M \notin \mathbb{F}_3 \quad \text{for} \quad 1 \le M \le (q-1)/8.$$

We need to check that for each proper subset S of

$$A = \{0, 1, \ldots, 2m\}$$

there is $b \in U$ such that

$$b^{M(S)} \notin \mathcal{F}_3$$

where

$$M(S) = \sum_{i \in S} 3^i.$$

We call a proper subset S of A bad if for all $b \in U$

$$b^{M(S)} \in \mathbb{F}_3$$

(i.e., $b^{M(S)}$ is $0, 1$ or -1). In other words, we need to check that there are NO bad sets for $m \in ABS_m$. Notice that if S is bad then its complement $A \setminus S$ is also bad. Indeed, we have

$$M(S) + M(A \setminus S) = (q-1)/2.$$

and therefore

$$b^{(q-1)/2} = b^{M(S)} b^{M(A \setminus S)}.$$

It remains to note that $b^{q-1)/2}$ always lies in $\mathbb{F}_3$.

On the other hand, if bad S does NOT contain 0 then $T = \{i-1, i \in S\}$ is also bad, because

$$b^{M(S)} = (b^{M(T)})^3.$$

Let S be a bad set with the smallest possible $M(S) =: M$. Then it must contain 0. We need to arrive to a contradiction, so suppose it does contain 0. Then the complement $S_1 = A \setminus$ is bad as well and does not contain 0. Hence, there is s bad T_1 such that $M(S_1) = 3M(T_1)$. By assumption

$$M(T_1) \ge M(S) = M.$$

We have

$$3M \leq 3M(T_1) = M(S_1) = (q-1)/2 - M,$$

i.e.,

$$3M \leq (q-1)/2 - M,$$

i.e.,

$$M \leq (q-1)/8.$$

Actually, the inequality is strong, because $(q-1)$ is not divisibly by 8 and even by 4.

Thus, since $(q-1)/2$ is odd we have $M < (q-1)/8$.

Let us put

$$N = N(S) := gcd(M, (q-1)/2).$$

Clearly, if $b \in \mathbb{F}_q$ then $b^M \in \mathbb{F}_3$ iff $b^N \in \mathbb{F}_3$.

If $m > 2$, then

$$3 < \frac{(3^{2m+1}-1)/2}{4 \cdot 3^m - 2} = \frac{\#(U)}{deg(P)}. \tag{7.9}$$

Lets verify the inequality (15) for $m > 2$:

$$\frac{(3^{2m+1}-1)/2}{4 \cdot 3^m - 2} = \frac{3^{2m+1}-1}{8 \cdot 3^m - 4}$$

and clearly,

$$\frac{3^{2m+1}-1}{3^{m+2}} < \frac{3^{2m+1}-1}{3^{m+2}} < \frac{3^{2m+1}-1}{3^{m+2}-4} = \frac{3^{2m+1}-1}{9 \cdot 3^m - 4} < \frac{3^{2m+1}-1}{8 \cdot 3^m - 4},$$

while

$$3 < 3^{m-1} - \frac{1}{3^{m+2}} = \frac{3^{2m+1}}{3^{m+2}} - \frac{1}{3^{m+2}} = \frac{3^{2m+1}-1}{3^{m+2}}.$$

This implies that polynomial $P(x)$ takes more than three distinct values on U. In particular, there is $b \in U$ such that

$$P(b) \notin \mathbb{F}_3.$$

This implies that if $m > 2$ and $N(S) = 1$ then S is not bad. Thus, we show that for $m \in ABS_m$, cases when $(q-1)/2$ is a prime, there are no bad subsets. Indeed, in this case every $M = M(S)$ (for proper S) is prime to $(q-1)/2$, therefore $N(S) = 1$

and the result follows.

□

Remark 7.7: Lemma 7.5 and Lemma 7.6 tell us that the 27-dimensional representation $L(2\bar{\omega}_1)$ along with its Frobenius twists and their certain tensor products cannot be defined over the field $\mathbb{F}_3$. Thus we get that the $Ree(q)$-module $V_f = (\mathbb{F}_3^{\mathfrak{R}_f})^0$ is the (reduction of) Steinberg representation (Remark 5.3) and thus cannot be split into a tensor product.

Now we have everything needed to show the very simplicity of the $Ree(q)$-module $V_f = (\mathbb{F}_3^{\mathfrak{R}_f})^0$:

$\boxed{\textbf{Theorem 7.3.}}$ With our setup, we claim that the $Ree(q)$ module $V_f = (\mathbb{F}_3^{\mathfrak{R}_f})^0$ is very simple for the following values of m:

$$m \in ABS_m \cup COMP_m.$$

Proof. To show the very simplicity of the $G = Ree(q)$-module $V_f = (\mathbb{F}_3^{\mathfrak{R}_f})^0$ we show that it satisfies the conditions of Corollary 5.2:

(i) The G-module $V_f = (\mathbb{F}_3^{\mathfrak{R}_f})^0$ is absolutely simple by Theorem 5.2.

(ii) By Lemmas 7.5 and 7.6 and Remark 7.7, there are no absolutely simple nontrivial G-modules of dimension $< q^3$ which are multiples of 3 for $m \in ABS_m \cup COMP_m$. Therefore, $V_f = (\mathbb{F}_3^{\mathfrak{R}_f})^0$ is not isomorphic to a tensor product of absolutely simple G-modules of dimension > 1 for the required values of m.

(iii) By the classification of maximal subgroups in [KM20] Theorem 2.1 and by Remark 5.3 of this article, each subgroup of $Ree(q)$ has index $\geq q^3 + 1 > q^3 = dim_{\mathbb{F}_3}(V_f)$.

Thus, by Corollary 6.2, the $Ree(q)$-module $V_f = (\mathbb{F}_3^{\mathfrak{R}_f})^0$ is very simple.

□

Remark 7.8: Theorem 7.3 establishes the very simplicity of the $Gal(f)$-module $V_f = (\mathbb{F}_3^{\mathfrak{R}_f})^0$. It is known [Zar18] that $Gal(f)$-modules $V_f = (\mathbb{F}_3^{\mathfrak{R}_f})^0$ and $J[\lambda]$ are canonically isomorphic. Hence, $Gal(f)$-module $J[\lambda]$ is very simple.

Chapter 8
Proof of Theorem 1.1

We have all the necessary ingredients to prove Theorem 1.1. We note that Remarks 2.1 and 6.1 have already outlined the way we are going to use the very-simplicity of $Gal(f)$-module $J[\lambda]$ in our proof of Theorem 1.1.

Theorem 1.1. Let f be a polynomial with coefficients in k and of degree

$$n := \deg(f) = q^3 + 1.$$

Let C be the trigonal curve it describes via the equation $y^3 = f(x)$. Suppose $Gal(f)$ coincides with one of the 2-transitive Ree groups in the series

$$Ree(q) = {}^2G_2(q)$$

for $q = 3^{2m+1}$ and

$$m \in ABS_m \cup COMP_m,$$

then the endomorphism algebra $End^0(J)$ of the Jacobian of C is isomorphic to $\mathbb{Q}(\zeta_3)$ and the endomorphism ring $End(J)$ of the Jacobian of C is isomorphic to $\mathbb{Z}[\zeta_3]$,

$$End(J) \cong \mathbb{Z}[\zeta_3].$$

Proof. First, by Remark 7.7, $Gal(f)$-module $J[\lambda]$ (Section 3, formula (5)) is very simple. Since the characteristic of k is zero, Theorem 4.14 in [Zar05a] (with $n = q^3+1$, $p = 3$ and $r = 1$) tells us that $E = \mathbb{Q}(\delta)$ (the image of $\mathbb{Q}(\delta) \to End^0(J)$) is isomorphic to $\mathbb{Q}(\zeta_3)$ and it is a maximal commutative subalgebra in $End^0(J)$. Since it is a maximal commutative subalgebra in $End^0(J)$, we have

$$\mathbb{Q}(\zeta_3) \cong \mathbb{Q}(\delta) = End^0(J,i),$$

where $End^0(J,i)$ is the centralizer of $i : \mathbb{Q}(\zeta_3) \to End^0(J)$. Now we can employ Theorem 4.16 from [Zar05a], which provides us with the required isomorphisms

$$End^0(J) \cong \mathbb{Q}(\zeta_3);$$
$$End(J) \cong \mathbb{Z}[\zeta_3].$$

In particular, J is an absolutely simple abelian variety.

□

Appendix

Python and MAGMA code

```
import sympy
import os
import glob
import sys
import os
import hashlib
from multiprocessing import Pool
from subprocess import call
import pandas as pd
from pathlib import Path
import subprocess
from sympy import Symbol
from sympy.parsing.sympy_parser import parse_expr
```

```
# Stating value of N for verification of the trace formula
M = 1
END_VALUE = 100
```

```
# Number of cores available
THREADS = 9




# saving location for the LOG.txt
PATH = Path().resolve()
BASIC_LOG_FILE = PATH / ’basic_log.txt’


def main(starting_value=M, end_value=END_VALUE, threads=THREADS):
    print(f’Verifying the trace formula, starting at m={M}’)
    # here we create Threads for our calls to MAGMA from the command line shell
    pool = Pool(processes=THREADS)

    # here we create the variables and pass the required string for processing to M

    m = Symbol(’m’)





    for m in range(M, END_VALUE):
        q = 3 ** (2 * m + 1)
        q_minus_1_over_2 = int((q - 1) / 2)
        q_minus_1_over_8 = int((q - 1) / 8)
        field_entry = 2 * m + 1
        t = 3 ** m
        # here we compute the exponent coefficients
         (pairwise positive and negative)


        c_1 = 2 * t
```

```
c_2 = 2 * t - 2
c_3 = 4 * t - 2
c_4 =  3 * t -1
c_5 = t - 1
c_6 = 2 * t - 1
c_7 = 3 * t - 2

# last digit indicates line number in magma script file
finite_field_1 = f’F:=FiniteField(3,{field_entry});’
primitive_2 = f’a:= PrimitiveElement(F);’



polynomial_ring_3 = f’P<x>:=PolynomialRing(F);’
sum_inverse_4 = f’b:= a+a^-1;’

dickson_1 = f’d_1:=DicksonFirst({c_1}, 1);’
dickson_2 = f’d_2:=DicksonFirst({c_2}, 1);’
dickson_3 = f’d_3:=DicksonFirst({c_3}, 1);’
dickson_4 = f’d_4:=DicksonFirst(1, 1);’
dickson_5 = f’d_5:=DicksonFirst({c_4}, 1);’
dickson_6 = f’d_6:=DicksonFirst({t}, 1);’
dickson_7 = f’d_7:=DicksonFirst({c_5}, 1);’
dickson_8 = f’d_8:=DicksonFirst({c_6}, 1);’
dickson_9 = f’d_9:=DicksonFirst({c_7}, 1);’

trace_formula_6 = f’tr:=DicksonFirst({c_1}, 1)+
DicksonFirst({c_2}, 1)
+ DicksonFirst({c_3}, 1)+ DicksonFirst(1, 1)+
DicksonFirst({c_4}, 1)+2*DicksonFirst({t}, 1)
+2*DicksonFirst({c_5}, 1)+2*DicksonFirst({c_6}, 1)
+DicksonFirst({c_7}, 1)+1;’
image_6 = f’image:= Evaluate(tr, b);’
```

```
        order_image_7 = f'if Order(image)
         lt {q_minus_1_over_2}
         then PrintFile("Output_{m}", "False"); end if;'



        magma_command_list =
        [finite_field_1,primitive_2,polynomial_ring_3,
         sum_inverse_4, trace_formula_6, image_6, order_image_7  ]




        # create the string for Template


        # create a Template file for MAGMA
        FILE_PATH = PATH / f'magma_{m}.txt'


        # we create and save a file which magma will be executing
        with open(FILE_PATH, "w") as f:
            f.write("\n".join(magma_command_list))



if __name__ == '__main__':
    main(sys.argv[1])




    # Stating value of N for verification of the trace formula
M = 1
END_VALUE = 100
```

```
# Number of cores available
THREADS = 9

# saving location for the LOG.txt
PATH = Path().resolve()
BASIC_LOG_FILE = PATH / ’basic_log.txt’


def main(starting_value=M, end_value=END_VALUE, threads=THREADS):
    print(f’Verifying the trace formula, starting at m={M}’)
    # here we create Threads for our calls to MAGMA from the command line shell


    pool = Pool(processes=THREADS)

    # here we create the variables and pass the required string for
     processing to MAGMA

    m = Symbol(’m’)




    for m in range(M, END_VALUE):
        q = 3 ** (2 * m + 1)
        q_minus_1_over_2 = int((q - 1) / 2)
        q_minus_1_over_8 = int((q - 1) / 8)
        field_entry = 2 * m + 1
        t = 3 ** m
        # here we compute the exponent coefficients
        (pairwise positive and negative)


        c_1 = 2 * t
        c_2 = 2 * t - 2
```

```
c_3 = 4 * t - 2
c_4 = 1 - 3 * t
c_5 = t - 1
c_6 = 2 * t - 1
c_7 = 3 * t - 2

# last digit indicates line number in magma script file
finite_field_1 = f’F:=FiniteField(3,{field_entry});’
primitive_2 = f’a:= PrimitiveElement(F);’
# order_3 = f’Order(a);’


function_field_4 = f’P<x>:=FunctionField(F);’
trace_formula_5 = f’f:=x^({c_1}) + x^(-{c_1})+
x^({c_2}) + x^(-{c_2})+ x^({c_3}) + x^(-{c_3})+
x + x^(-1)+ x^({c_4}) + x^(-{c_4})+2*x^({t}) +
 2*x^(-{t})+ 2*x^({c_5}) + 2*x^(-{c_5})+2*x^({c_6})
 + 2*x^(-{c_6})+x^({c_7}) + x^({c_7})+1;’
image_6 = f’image:= Evaluate(f, a);’


order_image_7 = f’if Order(image) ne {q-1}
 then image:= Evaluate(f, a^2); end if;’
# powers_8 = f’Powers:=[];’
check_8_1 = f’b:= F! -1;’
# loop_9 = f’for i in [1..{q_minus_1_over_8}]
 do if i mod 3 ne 0 then Powers:=Append(Powers, image^i);
 end if; end for;’
loop_9 = f’for i in [1..{q_minus_1_over_8}]
do if i mod 3 ne 0 and image^i eq b
 then PrintFile("Output_{m}", "False"); end if; end for;’
# last_11 = f’result:=b in Powers;’
# last_12 = f’ if result then PrintFile("Output_{m}", "False");
 end if; ’
```

```
        magma_command_list = [finite_field_1,primitive_2,
                              function_field_4,trace_formula_5,
                              image_6,
                              order_image_7,check_8_1, loop_9, ]



        # create the string for Template


        # create a Template file for MAGMA
        FILE_PATH = PATH / f’magma_{m}.txt’


        # we create and save a file which magma will be executing
        with open(FILE_PATH, "w") as f:
            f.write("\n".join(magma_command_list))



if __name__ == ’__main__’:
    main(sys.argv[1])
```

```
import sympy
import os
import glob
import sys
import os
import hashlib
from multiprocessing import Pool
from subprocess import call
import pandas as pd
from pathlib import Path
import subprocess
from sympy import Symbol
from sympy.parsing.sympy_parser import parse_expr







# Number of cores available
THREADS = 3


# Running a thread pool masks debug output. Set DEBUG to 1 to run
DEBUG = False

DEVNULL = open(os.devnull, "w")

def run_threaded_magma_scripts(start, end):
    list_of_m=[]
    pool = Pool(processes=THREADS)
    for i in range(start, end):
        list_of_m.append(i)

    pool.map(run_magma, list_of_m)
```

```
def run_magma(m):
    magma_commad = f’magma magma_{m}.txt’
    os.system(magma_commad)

if __name__ == ’__main__’:
    main(sys.argv[1])
```

```
import sympy
import os
import glob
import sys
import os
import hashlib
from multiprocessing import Pool
from subprocess import call
import pandas as pd
from pathlib import Path
import subprocess
from sympy import Symbol
from sympy.parsing.sympy_parser import parse_expr
```

```
# Stating value of N for verification of the trace formula
M = 1
END_VALUE = 100



# Number of cores available
THREADS = 9




# saving location for the LOG.txt
PATH = Path().resolve()
BASIC_LOG_FILE = PATH / ’basic_log.txt’


def main(starting_value=M, end_value=END_VALUE, threads=THREADS):
    print(f’Verifying the trace formula, starting at m={M}’)
    # here we create Threads for our calls to MAGMA from the command line shell
    pool = Pool(processes=THREADS)

    # here we create the variables and pass the required string for processing to M

    m = Symbol(’m’)



    for m in range(M, END_VALUE):
        q = 3 ** (2 * m + 1)
        q_minus_1_over_2 = int((q - 1) / 2)
        q_minus_1_over_8 = int((q - 1) / 8)
        field_entry = 2 * m + 1
        t = 3 ** m
```

```
# here we compute the exponent coefficients
(pairwise positive and negative)


c_1 = 2 * t
c_2 = 2 * t - 2
c_3 = 4 * t - 2
c_4 = 1 - 3 * t
c_5 = t - 1
c_6 = 2 * t - 1
c_7 = 3 * t - 2

# last digit indicates line number in magma script file
finite_field_1 = f'F:=FiniteField(3,{field_entry});'
primitive_2 = f'a:= PrimitiveElement(F);'
# order_3 = f'Order(a);'


function_field_4 = f'P<x>:=FunctionField(F);'
trace_formula_5 = f'f:=x^({c_1}) + x^(-{c_1})+ x^({c_2}) +
 x^(-{c_2})+ x^({c_3}) + x^(-{c_3})+ x + x^(-1)+ x^({c_4}) +
 x^(-{c_4})+2*x^({t}) + 2*x^(-{t})+ 2*x^({c_5}) + 2*x^(-{c_5})+2*x^({c_6})
image_6 = f'image:= Evaluate(f, a);'




order_image_7 = f'if Order(image) ne {q-1} then image:=
Evaluate(f, a^2); end if;'
# powers_8 = f'Powers:=[];'
check_8_1 = f'b:= F! -1;'
# loop_9 = f'for i in [1..{q_minus_1_over_8}]
do if i mod 3 ne 0 then Powers:=Append(Powers, image^i);
 end if; end for;'
```

```
loop_9 = f'for i in [1..{q_minus_1_over_8}]
do if i mod 3 ne 0 and image^i eq b then PrintFile("Output_{m}", "False");


# last_11 = f'result:=b in Powers;'
# last_12 = f' if result then PrintFile("Output_{m}", "False");
 end if; '


magma_command_list = [finite_field_1,primitive_2,
                      function_field_4,trace_formula_5,
                      image_6,
                      order_image_7,check_8_1, loop_9, ]


# create the string for Template


# create a Template file for MAGMA
FILE_PATH = PATH / f'magma_{m}.txt'


# we create and save a file which magma will be executing
with open(FILE_PATH, "w") as f:
    f.write("\n".join(magma_command_list))
```

```
if __name__ == ’__main__’:
    main(sys.argv[1])
```

Bibliography

[B̈14] H. Bäärnhielm. Recognizing the small Ree groups in their natural representations. *J. Algebra*, 416:139–166, 2014.

[BCP97] W. Bosma, J. C., and Catherine P. The Magma algebra system. I. The user language. pages 235–265, 03 1997. Computational algebra and number theory (London, 1993).

[Ble99] F. Bleher. Finite groups of Lie type of small rank. *Pacific Journal of Mathematics*, 187:215–239, 1999.

[GAP21] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.11.1*, 2021.

[Hum76] J. E. Humphreys. *Ordinary and modular representations of Chevalley groups*. Springer-Verlag, 1976.

[Hum87] J. E. Humphreys. The Steinberg representation. *Bulletin of the American Mathematical Society*, 16(2):247–264, 1987.

[Kle88] P. B. Kleidman. The maximal subgroups of the Chevalley groups G2(q) with q odd, the Ree groups 2G2(q), and their automorphism groups. *Journal of Algebra*, 117(1):30–71, 1988.

[KM20] J. Key and J. Moori. Designs from maximal subgroups and conjugacy classes of Ree groups. *Advances in Mathematics of Communicationss*, 14(4):603–611, 2020.

[LN85] V. M. Levchuk and Ya. N. Nuzhin. Structure of Ree groups. *Algebra and Logic*, 24(1):16–26, 1985.

[Lü01] F. Lübeck. Small degree representations of finite chevalley groups in defining characteristic. *LMS Journal of Computation and Mathematics*, 4:135–169, 2001.

[MGP96] F. Lübeck G. Malle M. Geck, G. Hiss and G. Pfeiffer. Chevie – a system for computing and processing generic character tables for finite groups of Lie type, Weyl groups and Hecke algebras. *Appl. Algebra Engrg. Comm. Comput.*, 7:175–210, 1996.

[Mum70] D. Mumford. *Abelian varieties*. Published for the Tata Institute of fundamental research by the Oxford University Press, 1970.

[Ser77] J.P Serre. Linear representations of finite groups. *Springer-Verlag*, 1977.

[Sil92] A. Silverberg. Fields of definition for homomorphisms of abelian varieties. *Pure Appl. Algebra*, page 339–362, 1992.

[Sin93] P. Sin. Extensions of simple modules for $G_2(3^n)$ and ${}^2G_2(3^m)$. *Proceedings of the London Mathematical Society*, s3-66(2):327–357, 1993.

[Spr68] T.A. Springer. Weyl's character formula for algebraic groups. *Invent Math 5*, page 85–105, 1968.

[Spr09] T.A Springer. *Linear algebraic groups*. Birkhäuser, 2009.

[Ste63] R. Steinberg. Representations of algebraic groups. *Nagoya Math. J.*, 22:33–56, 1963.

[Sza09] T. Szamuely. *Galois Groups and Fundamental Groups*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2009.

[VRD09] Guido Van Rossum and Fred L. Drake. *Python 3 Reference Manual*. CreateSpace, Scotts Valley, CA, 2009.

[Zar01] Yu. Zarhin. *Hyperelliptic Jacobians and Modular Representations*, pages 473–490. Birkhäuser Basel, Basel, 2001.

[Zar03] Yu. Zarhin. Hyperelliptic Jacobians and simple groups $\mathrm{U}_3(2^m)$. *Proceedings of the American Mathematical Society*, 131(1):95–102, 2003.

[Zar05a] Yu. Zarhin. Endomorphism algebras of superelliptic jacobians. *Progress in Mathematics Geometric Methods in Algebra and Number Theory*, page 339–362, 2005.

[Zar05b] Yu. Zarhin. Very simple representations: Variations on a theme of clifford. In Helmut Voelklein and Tanush Shaska, editors, *Progress in Galois Theory*, pages 151–168, Boston, MA, 2005. Springer US.

[Zar18] Yu. Zarhin. Endomorphism algebras of abelian varieties with special reference to superelliptic jacobians. In *Geometry, Algebra, Number Theory, and Their Information Technology Applications*, pages 477–528, Cham, 2018. Springer International Publishing.

Vita

Tigran Eritsyan

Education

The Pennsylvania State University Ph.D in Mathematics, Advised by Professor Yuri Zarhin	Aug 2016- Aug 2022
University of California at Berkeley B.A. in Mathematics,	Aug 2010- Dec 2015