# Elliptic Tori in $p$-adic Orthogonal Groups

Trinity Chinner

Thesis submitted in partial fulfillment of the requirements for the degree of
Master of Science Mathematics and Statistics[1]

Department of Mathematics and Statistics
Faculty of Science
University of Ottawa



[1]The M.Sc. program is a joint program with Carleton University, administered by the Ottawa-Carleton Institute of Mathematics and Statistics

# Abstract

In this thesis, we classify up to conjugacy the maximal elliptic toral subgroups of all special orthogonal groups $SO(V)$, where $(q, V)$ is a 4-dimensional quadratic space over a non-archimedean local field of odd residual characteristic. Our parameterization blends the abstract theory of Morris with a generalization of the practical work performed by Kim and Yu for Sp(4). Moreover, we compute an explicit Witt basis for each such torus, thereby enabling its concrete realization as a set of matrices embedded into the group. This work can be used explicitly to construct supercuspidal representations of $SO(V)$.

# Dedications

To the Blue and the Green.

# Acknowledgement

It is a pleasure to thank the many people who made this thesis possible, beginning with my supervisor, Dr. Monica Nevins. Her patient guidance, enthusiasm, and careful attention to detail has truly been invaluable throughout my time as her student. I am incredibly lucky to have gained a mentor who inspires me both academically and personally, one who invested many hours to introduce me to the world of mathematical research. It has been an absolute honour to work under Monica these past two years. I would also like to thank my examiners, Dr. Hadi Salmasian and Dr. Paul Mezo, for their thorough reviews of this work. This thesis would not be what it is today without their thoughtful suggestions.

I am eternally grateful for my peers in the mathematical community. In particular, thank you to Anish, Christine, Jeffrey, Jérémy, Lemonte, Maria, Mike, and Samuel. Your continued encouragement and genuine interest in my work have played an extremely crucial role in my studies. Regardless of the content of our conversations, I always left feeling both refreshed and motivated to learn.

To my non-math friends and family, thank you for being my biggest cheerleaders and always inspiring me to follow my dreams. I am especially thankful for my parents and grandparents, who supported me both emotionally and financially in the pursuit of this degree. Dad, thank you for teaching me the value of hard work and perseverance. Mom, thank you for always believing in me and for sharing my wish to complete this degree but caring enough to love me even if I never did.

Finally, a special thank you to my loving husband, Justin. Beyond proofreading countless pages of meaningless mathematics, I will be forever indebted to you for your constant love and support through every up and down of my research. Thank you and I love you.

# Contents

# List of Tables

# List of Symbols

# Chapter 1

# Introduction

The classification of subgroups has long been an important tool for studying the structure theory of groups. In particular, *elliptic toral subgroups* provide the key to understanding a $p$-adic group's actions on complex linear spaces, or equivalently, its representations.

In 2001, Jiu-Kang Yu [Yu01] provided a construction of supercuspidal representations of a $p$-adic group $G$, which was dependent, as a first ingredient of a *supercuspidal datum*, on a sequence of *twisted Levi subgroups* of $G$. The simplest twisted Levi subgroup is an elliptic torus. In this thesis, we explicitly classify the conjugacy classes of elliptic tori in each of the special orthogonal groups $G = SO(V)$, where $(q, V)$ is a 4-dimensional quadratic space defined over a non-archimedean local field $F$ of odd residual characteristic.

The central role of elliptic tori in the construction of supercuspidal representations can be seen in the pioneering work of Roger Howe in consideration of the general linear group $GL(V)$ [How77]. This specific classification for $GL(V)$ was later completed by Colin Bushnell and Philip Kutzko [BK93], however the first truly general constructions, applicable to all $p$-adic groups, were published much later by Jeff Adler [Adl98] and Jiu-Kang Yu [Yu01]. In 2008, Jeff Hakim and Fiona Murnaghan [HM08] furthered this theory, deriving a criterion for when two supercuspidal data produce isomorphic representations, and Ju-Lee Kim in 2007 [Kim07] showed under some hypotheses that Yu's construction produces all supercuspidal representations. In 2017, Jessica Fintzen [Fin17] achieved this proof under much weaker hypotheses, including all special orthogonal groups apart from $p = 2$.

Key publications specific to elliptic tori include the classification of maximal unramified tori by Stephen DeBacker [DeB06] and the concrete realization of tori in the symplectic group Sp(4) by Kim and Yu [KY11]. That said, conjugacy classes of tori are extremely difficult to characterize, hence the problem of classifying them concretely in $p$-adic groups remains open today. This thesis presents a new and valu-

able contribution to the literature and the explicit nature of our parameterization will allow these results to aid in tackling concrete open problems in $p$-adic representation theory.

As with most mathematical theses, this work has been designed to be as self-contained as possible, assuming some mathematical maturity and knowledge of linear algebra from the reader. The aim is in part to provide a precise reference to motivate future contributions, while assisting beginners in developing a basic intuition on these topics starting with the study of non-archimedean local fields.

The outline of the thesis is as follows. In Chapter 2, we discuss the structure theory of non-archimedean local fields required to study $p$-adic groups and their elliptic tori. We also explore some basic results from field theory over an arbitrary field, paying particular attention to non-normal (and hence non-Galois) extensions, as these arise in our parameterization. While most of this chapter serves as a literature review, we also determine the isomorphism classes of degree 4 field extensions of $F$, splitting up their discussion by ramification (Section 2.4, Tables 2.1 and 2.2).

In Chapter 3, we begin by giving an overview of tori in general, presenting key results from the literature and establishing examples which later aid in our construction. Our focus then turns specifically to the method developed by Lawrence Morris [Mor91] to completely determine the elliptic tori of all $n$-dimensional classical groups. We specialize this theory in the case when $G$ is orthogonal; in particular, we prove all results required to establish Morris' bijection (Theorem 3.4.5) in accessible language, reducing the characterization of elliptic tori to that of $n$-dimensional triples consisting of commutative, semisimple $F$-algebras and $\sigma$-Hermitian forms.

Chapter 4 is where we dive into the specifics of the degree 4 special orthogonal groups. The work of this chapter is primarily original and was initially inspired by Kim and Yu in [KY11]. In order to use the results from Morris practically, we first determine the equivalence classes of the triples, thereby forming an exhaustive, non-repeating list. We then must partition this list according to which group each triple bijects into, as there are eight 4-dimensional quadratic forms up to isometry, as well as five groups $G = SO(V)$ up to isomorphism.

In Section 4.3, we develop Algorithms 1 and 2, allowing us to determine for each triple, which group $SO(V)$ the torus is embedded into. These algorithms account for all possible equivalence classes of triples with no repetition, thereby bridging the abstract theory from Morris to a practical construction of tori in $SO(V)$. More precisely, we prove the following result (Theorem 4.2.2).

**Theorem.** *Fix a 4-dimensional, commutative, semisimple $F$-algebra $E'$ and involution $\sigma \in \mathrm{Aut}(E'/F)$ which non-trivially preserves each field component of $E'$. Choose $\mu \in E'^{\times}$ and let $q$ denote the corresponding quadratic form over $V \simeq E'$ output by the appropriate Algorithm (1 or 2).*

*Then, the group of norm 1 elements of $E'$, with respect to $\sigma$, is a* maximal elliptic

torus of $SO(V)$. *Moreover, two such tori are conjugate if and only if they arise from the same algorithm and parameters, up to the equivalence specified on Line 2.*

This theorem allows us to sort our tori into their respective special orthogonal groups, thereby yielding the complete classification of all maximal elliptic tori (up to conjugacy) in each of the groups $SO(V)$, as per Theorem 4.3.7. Beyond this, we also construct an explicit Witt basis for each of the tori, enabling their realization as matrices in $SO(V)$. This construction, summarized by Tables 4.2 and 4.3, relies on a deep analysis of the various isometries of quadratic forms, depending heavily upon whether $-1$ is a square in $F$ or not.

We prove several lemmas (2.5.6, 4.4.2, 4.5.2) which serve as the key to efficiently determining these Witt bases for each $E'$, with respect to which multiplication by the group of norm 1 elements acts by orthogonal transformations. We have omitted the details of this cumbersome process for brevity, however, numerous examples have been provided (see §4.4 and §4.5) which explicitly illustrate the methods used.

This work provides several opportunities for future research. For one, it would be interesting to determine the set of supercuspidal data associated to each torus $T$. The first step is to determine the point of the Bruhat–Tits building of $G$ associated to $T$, for which the Witt bases constructed in Tables 4.2 and 4.3 are essential. The rest of the data consists of characters; that is, one-dimensional representations of $T$. For this, knowing the isomorphism class of each torus is the key (Table 4.1).

Moreover, Algorithms 1 and 2 readily generalize to higher dimensions of $V$. Indeed, by gluing another copy of $F$ to our semisimple algebra $E'$, one can embed the tori constructed here into the special orthogonal group of degree 5 and efficiently classify them up to conjugacy.

# Chapter 2

# Non-Archimedean Local Fields

Let $F$ denote a non-archimedean local field and fix a prime $p \neq 2$. By [Tai75], $F$ is a finite algebraic extension of the $p$-adic numbers $\mathbb{Q}_p$ or is the field of Laurent series $\mathbb{F}_q((x))$ with coefficients in the finite field of $q$ elements, where $q = p^k$ for some $k \in \mathbb{Z}_{>0}$.

Throughout this chapter, we will be generalizing results from [Gou97, §5.3] to explore the various properties of $F$, beginning with basic structure theory and the establishment of notational conventions. Important results revolving around the algebraic norm and trace are reviewed in detail, and later explicitly applied to classify all quadratic and quartic field extensions of $F$ up to isomorphism. The chapter concludes with a brief introduction to quadratic forms and their respective special orthogonal groups, using results from [Lam05] to categorize the 4-dimensional forms up to isometry.

## 2.1 Structure Theory

By definition, our field $F$ is endowed with a non-archimedean discrete norm $|\ |\colon F \to \mathbb{R}_{\geq 0}$, with respect to which $F$ is complete. The norm is both multiplicative $|xy| = |x||y|$ and an ultrametric, meaning $|x+y| \leq \max\{|x|, |y|\}$ for all $x, y \in F$. Moreover, polynomial maps are continuous with respect to the topology induced by $|\ |$. We will now use this to define the following essential items.

**Definition 2.1.1.** *Let $F$ be a non-archimedean local field. We define the* integer ring *of $F$ to be $\mathcal{O} = \{a \in F \mid |a| \leq 1\}$.*

It is clear by the properties of the norm that $\mathcal{O}$ is a ring, but we will use the following lemma to delve further into the characteristics of $\mathcal{O}$.

**Lemma 2.1.2.** *The integer ring $\mathcal{O}$ is local with maximal prime ideal $\mathcal{P}$ given by*

$$\mathcal{P} \coloneqq \{a \in F \mid |a| < 1\}.$$

**Proof:** For all $x \in \mathcal{O}, y \in \mathcal{P}$, $|xy| = |x| \cdot |y| < |x| \cdot 1 \leq 1$ so $xy \in \mathcal{P}$. Similarly, $\mathcal{P}$ is closed under addition as consequence of the ultrametric. Furthermore, if $x_1, x_2 \in \mathcal{O}$ and $x_1 x_2 \in \mathcal{P}$, one of $x_1$ or $x_2$ must be in $\mathcal{P}$, because otherwise $|x_1 x_2| = 1 \cdot 1 \notin \mathcal{P}$, hence $\mathcal{P}$ is a prime ideal of $\mathcal{O}$.

We now prove the locality of $\mathcal{O}$. Consider the set $\mathcal{O} \setminus \mathcal{P} = \{a \in F \mid |a| = 1\}$. For all $x \in \mathcal{O} \setminus \mathcal{P}$, we have that $x^{-1} \in \mathcal{O} \setminus \mathcal{P}$ since $1 = |xx^{-1}| = 1 \cdot |x^{-1}|$, and hence $\mathcal{O} \setminus \mathcal{P} = \mathcal{O}^\times$. Since $\mathcal{P}$ is prime and everything outside $\mathcal{P}$ is invertible, every ideal of $\mathcal{O}$ is contained in $\mathcal{P}$. Therefore, $\mathcal{P}$ is the unique maximal ideal of $\mathcal{O}$, and hence $\mathcal{O}$ is local. ∎

It is also true that $\mathcal{P}$ is principal, so it is generated by a single element. Indeed, choose an element $a \in \mathcal{P}$ of maximal norm; this is possible since the norm is discrete. Given two such $a$ and $b$, our proof of Lemma 2.1.2 implies that $ab^{-1} \in \mathcal{O} \setminus \mathcal{P} = \mathcal{O}^\times$ since $|ab^{-1}| = 1$; thus $a$ and $b$ generate the same ideal, which therefore must be all of $\mathcal{P}$.

**Definition 2.1.3.** *A generator $\varpi$ of $\mathcal{P}$ is called a* uniformizer *for $F$.*

There are many choices for $\varpi$, however, we will fix one for the remainder of our discussion. Every element $a$ of $F^\times$ can be written uniquely as $u\varpi^n$ for some $u \in \mathcal{O}^\times, n \in \mathbb{Z}$. Indeed, choose the largest $n \in \mathbb{Z}$ so that $|a\varpi^{-n}| \leq 1$; in particular, we must have $1 \geq |a\varpi^{-n}| > |\varpi|$. Since $\varpi$ has the largest norm strictly less than 1, equality holds, so $a\varpi^{-n} = u \in \mathcal{O}^\times$. We write $\nu_F(a) = n$ and call this the *(F-normalized) valuation* on $F$.

Since $\mathcal{O}$ is local, the quotient $\mathcal{O}/\mathcal{P}$ is a field and hence is given a special name.

**Definition 2.1.4.** *Let $F$ be a non-archimedean local field with integer ring $\mathcal{O}$ and principal prime ideal $\mathcal{P}$. We call the field $\mathfrak{f} \coloneqq \mathcal{O}/\mathcal{P}$ the* residue field of $F$.

In fact, $\mathfrak{f}$ is finite. Let $q$ be its size; $q$ is a power of a prime $p$, where $p$ is the least positive integer such that $|p| < 1$. By convention, we replace the norm on $F$ by an equivalent one, if necessary, so that the following identity holds

$$|x| = q^{-\nu_F(x)}$$

for all $x \in F^\times$. Therefore, as needed, we may set $\nu_F(0) = \infty$. With this equality, the ultrametric induces the property $\nu_F(a+b) \geq \min\{\nu_F(a), \nu_F(b)\}$ for all $a, b \in F$.

A key feature of local fields is that many calculations can be reduced to the finite residue field. The following result, known as Hensel's Lemma, makes this precise, and we will see several instances of this philosophy throughout the thesis.

**Lemma 2.1.5** (Hensel's Lemma)**.** *Let $F$ be a non-archimedean local field and $\varpi$ a uniformizer. Let $f(x) \in \mathcal{O}[x]$ be a polynomial and suppose that there exists an $\alpha \in \mathcal{O}$ such that*

$$\begin{aligned} f(\alpha) &\equiv 0 \pmod{\varpi} \\ f'(\alpha) &\not\equiv 0 \pmod{\varpi} \end{aligned}$$

*where $f'(x)$ is the formal derivative of $f(x)$. Then, there exists a unique $\beta \in \mathcal{O}$ such that $\beta \equiv \alpha \pmod{\varpi}$ and $f(\beta) = 0$.*

**Proof:** We begin by proving the existence of such a $\beta$. We first construct an infinite sequence $\{\alpha_1, \alpha_2, \cdots \mid \alpha_i \in \mathcal{O}\}$ via induction on the following hypothesis $P(n)$, for $n \geq 1$:

i) $f(\alpha_n) \equiv 0 \pmod{\varpi^n}$;

ii) $f'(\alpha_n) \in \mathcal{O}^\times$;

iii) $\alpha_n \equiv \alpha_{n-1} \pmod{\varpi^{n-1}}$.

The hypotheses of the lemma assumes the existence of $\alpha_1 \coloneqq \alpha$, so the base case is satisfied. Suppose we have found $\alpha_n \in \mathcal{O}$ satisfying $P(n)$; we need to define an $\alpha_{n+1}$ which satisfies $P(n+1)$. In order to satisfy iii), $\alpha_{n+1} = \alpha_n + b\varpi^n$ for some $b \in \mathcal{O}$. For any $i \geq 1$, the binomial expansion gives

$$(\alpha_n + b\varpi^n)^i = (\alpha_n)^i + i(\alpha_n)^{i-1} b\varpi^n + \sum_{j=2}^{i} \binom{i}{j} (\alpha_n)^j (b\varpi^n)^{i-j}.$$

Since the sum has integral coefficients, we have

$$(\alpha_n + b\varpi^n)^i \equiv (\alpha_n)^i + i(\alpha_n)^{i-1} b\varpi^n \pmod{\varpi^{n+1}}.$$

It thus follows, noting the expression of the formal derivative, that for any polynomial $g(x) \in \mathcal{O}[x]$, we have

$$g(\alpha_n + b\varpi^n) \equiv g(\alpha_n) + g'(\alpha_n) b\varpi^n \pmod{\varpi^{n+1}}. \tag{2.1.1}$$

By taking $g = f'$ in (2.1.1), we conclude that for every $b \in \mathcal{O}$, $f'(\alpha_n + b\varpi^n) \equiv f'(\alpha_n) \pmod{\varpi}$, so $f'(\alpha_n + b\varpi^n) \in \mathcal{O}^\times$ and ii) is satisfied for all choices $b \in \mathcal{O}$.

Condition i) implies we can write $f(\alpha_n) = \gamma\varpi^n$ for some $\gamma \in \mathcal{O}$. By now applying (2.1.1) to $g = f$, we obtain

$$f(\alpha_n + b\varpi^n) \equiv \gamma\varpi^n + f'(\alpha_n) b\varpi^n \pmod{\varpi^{n+1}}.$$

Since $f'(\alpha_n) \in \mathcal{O}^\times$, we can set $b = -\gamma(f'(\alpha_n))^{-1} \in \mathcal{O}$ to give a value $\alpha_{n+1} = \alpha_n + b\varpi^n$ for which $f(\alpha_{n+1}) \equiv 0 \pmod{\varpi^{n+1}}$, hence satisfying $P(n+1)$.

We have now successfully constructed a sequence $\{\alpha_1, \alpha_2, \cdots \mid \alpha_i \in \mathcal{O}\}$ which satisfies i), ii), and iii). The sequence is Cauchy by construction and hence converges to a limit $\beta \in F$ such that $\beta \equiv \alpha_n \pmod{\varpi^n}$ for all $n \geq 1$. By the continuity of polynomials, $f(\beta) = 0$, thereby completing the proof of existence.

For uniqueness, suppose that we have two roots $\beta, \beta' \in \mathcal{O}$ which satisfy the lemma's hypotheses, so we can write $\beta' = \beta + a\varpi^n$ for some $n \in \mathbb{Z}_{>0}, a \in \mathcal{O}^\times$. By (2.1.1), we have

$$f(\beta') \equiv f(\beta) + f'(\beta)a\varpi^n \pmod{\varpi^{n+1}}$$

which implies that $a \not\equiv 0 \pmod{\varpi}$, a contradiction. ∎

Over a finite field of size $q$, quadratic reciprocity implies that $-1$ is a square if and only if $q \equiv 1 \pmod 4$. Thus, as a first consequence of Hensel's Lemma, we have that $-1 \in {F^\times}^2$ if and only if $|\mathfrak{f}| \equiv 1 \pmod 4$; a condition which will recur in the thesis.

## 2.2 General Field Theory

In this section only, we take $F$ to be an arbitrary field. Let $E$ be a finite algebraic extension of $F$, which is embedded, without loss of generality, into a fixed algebraic closure $\overline{F}$ of $F$. Prior to delving further into local field theory, we will explore some well known results that hold for any such $E/F$.

**Definition 2.2.1.** *An algebraic field extension $E/F$ is* separable *if the minimal polynomial of every $\alpha \in E$ is a separable polynomial; that is, an irreducible polynomial with distinct roots.*

**Example 2.2.2.** In a field of characteristic zero, every finite algebraic extension is separable [BJN94, Corollary 3.5].

**Example 2.2.3.** Consider $F = \mathbb{F}_p((t))$. Let $u$ be a root of the irreducible polynomial $r(x) = x^p - t$. By the binomial theorem, we see that

$$(x-u)^p = x^p - u^p = x^p - t = r(x)$$

so $u$ has multiplicity $p$, hence $F(u)$ is not a separable extension of $F$.

In this thesis, we will be focusing on quadratic and quartic extensions of local fields, hence by assuming $p \neq 2$ these extensions will all therefore be separable, even when $F$ has positive characteristic.

**Lemma 2.2.4.** *Suppose $E$ and $\tilde{E}$ are finite separable field extensions of $F$ and $\sigma\colon E \to \tilde{E}$ is a homomorphism fixing $F$. For every $\alpha \in E$, $\alpha$ and $\sigma(\alpha)$ have the same minimal polynomial over $F$.*

**Proof:** Let $m(x) = \sum_{i=1}^{n} a_i x^i \in F[x]$ be the minimal polynomial of $\alpha$ over $F$ and $\sigma \in \mathrm{Hom}_F(E, \tilde{E})$. It suffices to prove that $\sigma(\alpha)$ is a root of $m(x)$. Indeed, by the properties of $\sigma$

$$m(\sigma(\alpha)) = \sum_{i=1}^{n} a_i \sigma^i(\alpha) = \sigma(\sum_{i=1}^{n} a_i \alpha^i) = \sigma(m(\alpha)) = 0$$

so $\sigma(\alpha)$ is a root of $m(x)$. ∎

By viewing $E$ as a vector space over $F$, multiplication by $\alpha \in E$ is an invertible linear transformation, which we will denote by $m_\alpha$. The minimal polynomial of $\alpha$ over $F$ is identical to the minimal polynomial of $m_\alpha$, which coincides with its characteristic polynomial when $E$ is separable, hence allowing us to conclude the following result.

**Corollary 2.2.5.** *Let $\alpha$ be an element of a finite separable extension $E$ of $F$. If $\lambda$ is an eigenvalue of $m_\alpha$, then $\sigma(\lambda)$ is an eigenvalue of $m_\alpha$ for all $\sigma \in \mathrm{Aut}(E/F)$.*

**Definition 2.2.6.** *An algebraic field extension $E/F$ is* normal *if every irreducible polynomial over $F$ that has at least one root in $E$ splits over $E$.*

This is equivalent to saying that the roots of the minimal polynomial of $\alpha \in E$ over $F$ are all contained in $E$, for all $\alpha \in E$. When an extension $E/F$ is both separable and normal, it is *Galois* and we write $\mathrm{Gal}(E/F) \coloneqq \mathrm{Aut}(E/F)$.

We now state the most well known theorem of Galois Theory [Rot12, Theorem 63], which establishes a connection between $\mathcal{I}(E/F)$ the set of intermediate fields of a Galois extension $E/F$, and $\mathcal{S}(\mathrm{Gal}(E/F))$ the set of subgroups of $\mathrm{Gal}(E/F)$.

**Theorem 2.2.7** (The Fundamental Theorem of Galois Theory)**.** *Let $E/F$ be a Galois extension, and define the following maps:*

$$\begin{aligned} \Xi\colon \mathcal{I}(E/F) &\to \mathcal{S}(\mathrm{Gal}(E/F)) & \qquad \mathcal{F}\colon \mathcal{S}(\mathrm{Gal}(E/F)) &\to \mathcal{I}(E/F) \\ L &\mapsto \mathrm{Gal}(E/L) & H &\mapsto \mathcal{F}(H) \end{aligned}$$

*where $\mathcal{F}(H) \coloneqq \{\alpha \in E \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$ denotes the fixed field of $H$. Then, $\Xi$ and $\mathcal{F}$ are bijective inverses of one another and therefore establish a one-to-one correspondence between the intermediate fields of $E/F$ and the subgroups of* $\mathrm{Gal}(E/F)$.

This result is obviously incredibly powerful, its proof hinging on the fact that for any extension $E/F$, the order of a finite subgroup $H$ of $\mathrm{Aut}(E/F)$ is equal to $[E\colon \mathcal{F}(H)]$, the degree of $E$ over the fixed field of $H$ [DF04, §14.2 Theorem 9].

The field extensions we will be working with throughout the thesis, while always separable, will not always be normal, as per Example 2.2.9 below. It is useful to note that even in these non-Galois cases, a portion of the Theorem still holds true.

**Lemma 2.2.8.** *Suppose the maps $\Xi, \mathcal{F}$ are as defined in Theorem 2.2.7 for a finite non-Galois extension $E/F$ by replacing* $\mathrm{Gal}(E/F)$ *with* $\mathrm{Aut}(E/F)$*. Then, $\mathcal{F}$ is injective and $\Xi$ is surjective.*

**Proof:** Suppose $H_1$ and $H_2$ are two subgroups of $\mathrm{Aut}(E/F)$ that have the same fixed field $\tilde{F} \coloneqq \mathcal{F}(H_1) = \mathcal{F}(H_2)$. The subgroup $H$ generated by $H_1$ and $H_2$ also fixes the intermediate field $\tilde{F}$ which implies, by the key relationship of $|H| = [E : \mathcal{F}(H)]$, that $|H| = |H_1| = |H_2|$. Since $H_1, H_2 \subset H$ we deduce $H_1 = H_2 = H$, so $\mathcal{F}$ is injective.

Now, suppose $H_1$ is a subgroup of $\mathrm{Aut}(E/F)$ and set $H_2 = \Xi(\mathcal{F}(H_1)) = \mathrm{Aut}(E/\mathcal{F}(H_1))$. Then, we have $H_1 \subseteq H_2$, whence the fixed field of $H_2$ can be no bigger than the fixed field of $H_1$, and we conclude $\mathcal{F}(H_1) = \mathcal{F}(H_2)$. By injectivity of $\mathcal{F}$, $H_1 = H_2 = \Xi(\mathcal{F}(H_1))$, so $\Xi$ is surjective. ∎

We now illustrate this theory via an example of a separable non-normal extension which will recur in the thesis.

**Example 2.2.9.** Suppose $F$ is a field with $\mathrm{char}(F) \neq 2$, and $\alpha \in F^\times$ is such that $m(x) = x^4 - \alpha$ is irreducible over $F$. Let $\beta$ be a root of $m(x)$; then the roots of $m(x)$ are given by $\{\pm\beta, \pm i\beta\}$, where $i$ satisfies $i^2 = -1$. Therefore, if $i \notin F(\beta)$ then $F(\beta)$ is a separable but not normal quartic extension of $F$.

Suppose $i \notin F(\beta)$. A consequence of Lemma 2.2.4 is that $\mathrm{Aut}(F(\beta)/F)$ permutes the roots of $m(x)$ contained in $F(\beta)$, hence the automorphism group is given by

$$\mathrm{Aut}(F(\beta)/F) = \{\sigma_0 = \mathrm{id}, \sigma_1\colon \beta \mapsto -\beta\} \simeq \mathbb{Z}/2\mathbb{Z}$$

which has no non-trivial subgroups. Our field extension, however, does have a non-trivial subfield, namely the quadratic extension $F(\beta^2)$. In particular, we compute:

$$\begin{aligned} \mathcal{F}(\{\mathrm{id}\}) &= \{x \in F(\beta) \mid \mathrm{id}(x) = x\} \\ &= F(\beta) \end{aligned} \qquad \begin{aligned} \mathcal{F}(\mathbb{Z}/2\mathbb{Z}) &= \{x \in F(\beta) \mid \sigma_1(x) = x\} \\ &= F(\beta^2) \end{aligned}$$

thus $\mathcal{F}$ is indeed injective, but not surjective. Similarly,

$$\begin{aligned} \Xi(F) &= \mathrm{Aut}(F(\beta)/F) \\ &\simeq \mathbb{Z}/2\mathbb{Z} \end{aligned} \qquad \begin{aligned} \Xi(F(\beta^2)) &= \mathrm{Aut}(F(\beta)/F(\beta^2)) \\ &\simeq \mathbb{Z}/2\mathbb{Z} \end{aligned} \qquad \begin{aligned} \Xi(F(\beta)) &= \mathrm{Aut}(F(\beta)/F(\beta)) \\ &= \mathrm{id} \end{aligned}$$

hence $\Xi$ is surjective, but not injective, as expected.

### 2.2.1 Norms and Traces

In this section, we will establish formulas for the norm and trace that can easily be utilized for non-normal extensions. Let $E$ be a finite-dimensional field extension of $F$ and take $\alpha \in E$. As per our previous discussion, we can define an $F$-linear map $m_\alpha \colon E \to E$ given by multiplication by $\alpha$, which corresponds to a matrix $M_{[\alpha]}$ with respect to a choice of basis for $E/F$.

**Definition 2.2.10.** *The* (algebraic) norm from $E$ to $F$ *is defined by*

$$\mathrm{N}_{E/F}(\alpha) \coloneqq \det(M_{[\alpha]}).$$

It is clear from this definition and properties of the determinant that $\mathrm{N}_{E/F}$ is multiplicative and if $\lambda \in F$ then $\mathrm{N}_{E/F}(\lambda) = \lambda^{[E\colon F]}$. We now define the norm's counterpart, the trace.

**Definition 2.2.11.** *The* trace of $E$ over $F$ *is defined by*

$$\mathrm{Tr}_{E/F}(\alpha) \coloneqq \mathrm{trace}(M_{[\alpha]}).$$

While the trace does not have quite as nice of a multiplicative property as the norm, it is $F$-linear and $\mathrm{Tr}_{E/F}(\lambda) = [E\colon F]\lambda$ for all $\lambda \in F$. Moreover, $\mathrm{Tr}_{E/F}(\alpha_1\alpha_2) = \mathrm{Tr}_{E/F}(\alpha_2\alpha_1)$ for all $\alpha_1, \alpha_2 \in E$. We note that both the norm and trace are independent of our choice of basis for $E/F$.

**Lemma 2.2.12.** *Suppose $F(\alpha)/F$ is a field extension of degree $r$ and let $m(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_1x + a_0 \in F[x]$ be the minimal polynomial of $\alpha$ over $F$. Then, the norm and trace of $\alpha$ are given by*

$$\mathrm{N}_{F(\alpha)/F}(\alpha) = (-1)^r a_0, \qquad \mathrm{Tr}_{F(\alpha)/F}(\alpha) = -a_{r-1}.$$

**Proof:** Consider the basis of $F(\alpha)$ given by $\{1, \alpha, \ldots, \alpha^{r-1}\}$ and let $M_{[\alpha]}$ be the matrix representation of multiplication by $\alpha$. Since $M_{[\alpha]}(\alpha^i) = \alpha^{i+1}$ for all $0 \leq i \leq r-2$ and $M_{[\alpha]}(\alpha^{r-1}) = \alpha^r = -a_0 - a_1\alpha - \cdots - a_{r-1}\alpha^{r-1}$, the matrix $M_{[\alpha]}$ has 1's below the diagonal and zeros elsewhere, apart from the last column which has the entry $-a_i$ in row $i+1$ for $0 \leq i \leq r-1$. From this, it is clear that the trace is equal to $-a_{r-1}$ and we can compute via cofactor expansion:

$$\det(M_{[\alpha]}) = (-1)^{r-1}(-a_0)\det(I_{r-1}) = (-1)^r a_0.$$

∎

We will now show that computing the norm and trace of $\alpha$ over any separable extension $E/F$ reduces to computing it on $F(\alpha)$.

**Lemma 2.2.13.** *Let $E/F$ be a separable field extension. Then, for all $\alpha \in E$:*

$$\mathrm{N}_{E/F}(\alpha) = (\mathrm{N}_{F(\alpha)/F}(\alpha))^{[E\colon F(\alpha)]}$$
$$\mathrm{Tr}_{E/F}(\alpha) = [E\colon F(\alpha)]\,\mathrm{Tr}_{F(\alpha)/F}(\alpha)$$

**Proof:** Let $\alpha \in E$. We can construct an $F$-basis of $E$ by first finding a basis for $F(\alpha)$ over $F$ and then finding a basis for $E$ over $F(\alpha)$. Since $\alpha$ acts diagonally on a basis for $E/F(\alpha)$, we obtain a block matrix for $M_{[\alpha]}$ with $[E\colon F(\alpha)]$ copies of the smaller matrix $N_{[\alpha]} \coloneqq M_{[\alpha]}|_{F(\alpha)}$ on the diagonal. Computing the determinant yields

$$\mathrm{N}_{E/F}(\alpha) = \det(M_{[\alpha]}) = \det(N_{[\alpha]})^{[E\colon F(\alpha)]} = (\mathrm{N}_{F(\alpha)/F}(\alpha))^{[E\colon F(\alpha)]}$$

and the trace formula follows identically, completing the proof. ∎

Recall that the *normal closure* of a finite field extension $E/F$ is the smallest normal extension of $F$ containing $E$. We now prove an adapted version of [Ash13, Theorem 3.5.2] which will allow us to easily work with non-normal extensions.

**Lemma 2.2.14.** *Suppose $E/F$ is a separable extension of degree $n$. There are exactly $n$ $F$-embeddings of $E$ into the normal closure of $E/F$.*

**Proof:** Let $\tilde{E}$ denote the normal closure of $E/F$. We proceed by induction on the degree of $E$ over $F$. In the base case we have that $E = F$, and there is precisely 1 $F$-embedding, namely the identity.

Suppose $n > 1$ and take $\alpha \in E \backslash F$ with minimal polynomial $m(x) = \sum_{i=1}^{r} a_i x^i \in F[x]$. Let $\tau\colon F \hookrightarrow \tilde{E}$ be an embedding and define $g(x) \coloneqq \sum_{i=1}^{r} \tau(a_i)x^i$. Since $m(x)$ is necessarily separable and irreducible over $F$, $g(x)$ must also be over $\tau(F)$.

Let $\beta$ be a root of $g$. Then, there exists a unique isomorphism between $F(\alpha)$ and $(\tau(F))(\beta)$ such that for all $b_i \in F, r \in \mathbb{Z}_{>0}$

$$b_0 + b_1\alpha + \cdots + b_r\alpha^r \to \tau(b_0) + \tau(b_1)\beta + \cdots + \tau(b_r)\beta^r.$$

Since $[F(\alpha)\colon F] = \deg m = \deg g = r$, we have that $[E\colon F(\alpha)] = \frac{n}{r} < n$. By the separability of $g$, this implies that we have $r$ distinct choices for our root $\beta$. By induction, in each case there are $\frac{n}{r}$ distinct $F$-embeddings $F(\alpha)$ into $\tilde{E}$, and hence at least $\frac{n}{r} \times r = n$ distinct embeddings of $E$ into $\tilde{E}$. By Lemma 2.2.4, for every $F$-embedding of $F(\alpha)$, we obtain a root of $m(x)$. There are at most $r$ of these, thus we have equality. ∎

This result in combination with Lemma 2.2.4 allows us to conclude the following.

**Corollary 2.2.15.** *Let $E$ be a separable extension of $F$. Then, given any $\alpha \in E$, the roots of its minimal polynomial over $F$ are given by the set $\{\sigma_i(\alpha) \mid 1 \leq i \leq r\}$, where $r = [F(\alpha)\colon F]$ and the $\sigma_i$ are the $r$ distinct $F$-embeddings of $F(\alpha)$ into the normal closure of $E/F$.*

We now have the required set up to prove some equivalent characterizations of both the norm and trace.

**Proposition 2.2.16.** *Given a finite, separable extension $E/F$, the* norm from $E$ to $F$ *of $\alpha \in E$ is given by*

$$\mathrm{N}_{E/F}(\alpha) \coloneqq \prod_{\sigma} \sigma(\alpha)$$

*where $\sigma$ runs over $F$-embeddings of $E$ into the normal closure of $E/F$.*

**Proof:** Let $\alpha \in E$ have minimal polynomial $m(x) \in F[x]$. Let $\tilde{E}$ be the normal closure of $E/F$, namely $\tilde{E}$. The polynomial $m(x)$ splits completely over $\tilde{E}$, which by Corollary 2.2.15 looks like

$$m(x) = (x - \tau_1(\alpha))(x - \tau_2(\alpha)) \dots (x - \tau_r(\alpha)) \in \tilde{E}[x]$$

where $r = [F(\alpha)\colon F]$ and the $\tau_i\colon F(\alpha) \hookrightarrow \tilde{E}$ denote distinct $F$-embeddings. By Lemma 2.2.12,

$$\mathrm{N}_{F(\alpha)/F}(\alpha) = (-1)^r \cdot \prod_{i=1}^{r} -\tau_i(\alpha) = \prod_{i=1}^{r} \tau_i(\alpha)$$

hence the result holds for extensions $F(\alpha)/F$. We will now construct $F$-embeddings of $E$ to $\tilde{E}$, by first deciding how to act on $F(\alpha)$ by some $\tau\colon F(\alpha) \hookrightarrow \tilde{E}$, and then lifting this $\tau$ to $E$.

Our choices for $\tau$ have already been described; $\tau\colon \alpha \mapsto \tau_i(\alpha) \coloneqq \alpha_i$ for some $1 \leq i \leq r$. Once we fix a $\tau$, there are $[E\colon F(\alpha)]$ liftings of this embedding to $E \hookrightarrow \tilde{E}$ by Lemma 2.2.14. Hence in the proposed product formula with $\sigma\colon E \hookrightarrow \tilde{E}$ an $F$-embedding, each $\tau_i$ appears $[E\colon F(\alpha)]$ times. Therefore,

$$\prod_{\sigma} \sigma(\alpha) = \prod_{i} \tau_i(\alpha)^{[E\colon F(\alpha)]} = \mathrm{N}_{E/F}(\alpha)$$

where the final equality follows from Lemma 2.2.13. ∎

The following result is proven identically to Proposition 2.2.16, using the analogous formulas for the trace.

**Proposition 2.2.17.** *Given a finite, separable extension $E/F$, the* trace of $E$ over $F$ *of $\alpha \in E$ is given by*

$$\mathrm{Tr}_{E/F}(\alpha) \coloneqq \sum_{\sigma} \sigma(\alpha)$$

*where $\sigma$ runs over $F$-embeddings of $E$ into the normal closure of $E/F$.*

When $E/F$ is normal, these formulas imply

$$\mathrm{N}_{E/F}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha), \quad \mathrm{Tr}_{E/F}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)$$

where $G \coloneqq \mathrm{Gal}(E/F)$.

**Example 2.2.18.** Suppose $E = F(\sqrt{\alpha})$ for some non-square $\alpha \in F^\times$ and non-archimedean local field $F$. Then, $E/F$ is normal and separable, hence Galois, and its Galois group contains two automorphisms: the identity, and

$$\sigma \colon \sqrt{\alpha} \mapsto -\sqrt{\alpha}.$$

Let $\mathcal{B} = \{1, \sqrt{\alpha}\}$ be our chosen basis for $E/F$. By Proposition 2.2.16, the norm from $E$ to $F$ of some $x = v_1 + v_2\sqrt{\alpha} \in E, v_i \in F$ is given by $\mathrm{N}_{E/F}(x) = (v_1 + v_2\sqrt{\alpha})(v_1 - v_2\sqrt{\alpha}) = v_1^2 - \alpha v_2^2$. We confirm this coincides with our original formula from Definition 2.2.10 since, with respect to $\mathcal{B}$, the determinant of $M_{[x]}$ is given by

$$\det M_{[x]} = \det \begin{bmatrix} v_1 & v_2\alpha \\ v_2 & v_1 \end{bmatrix} = v_1^2 - v_2^2\alpha.$$

In an identical fashion, we compute the trace

$$\begin{aligned} \mathrm{Tr}_{E/F}(x) &= (v_1 + v_2\sqrt{\alpha}) + (v_1 - v_2\sqrt{\alpha}) \\ &= 2v_1 \\ &= \mathrm{trace}(M_{[x]}) \end{aligned}$$

so both formulas hold.

The following result is standard from field theory.

**Lemma 2.2.19.** *Let $\sigma \colon E \hookrightarrow \tilde{E}$ be an $F$-embedding of $E$ into the normal closure of $E/F$. Then, $\mathrm{Tr}_{E/F}(\alpha) = \mathrm{Tr}_{\sigma(E)/F}(\sigma(\alpha))$ and $\mathrm{N}_{E/F}(\alpha) = \mathrm{N}_{\sigma(E)/F}(\sigma(\alpha))$ for all $\alpha \in E$.*

**Proof:** It suffices to prove the result for $E \coloneqq F(\alpha)$ by Lemma 2.2.13. The norm and trace of $\alpha \in E$ are completely determined by its minimal polynomial over $F$ by Lemma 2.2.12. Since $\alpha$ and $\sigma(\alpha)$ have the same minimal polynomial as a consequence of Lemma 2.2.4, the result follows. ∎

It is worthy to note that when $E/F$ is Galois, this lemma is a direct consequence of Propositions 2.2.16 and 2.2.17, since $\sigma \in \mathrm{Gal}(E/F)$ permutes the elements of the group, however we have now established it for all separable (not necessarily normal) extensions $E/F$.

We end with the following powerful result over finite fields from [Lan13], which we will utilize in the following section to discuss unramified extensions of non-archimedean local fields.

**Lemma 2.2.20.** *Let $\mathfrak{e}$ be an extension of a finite field $\mathfrak{f}$. Then, $\mathrm{N}_{\mathfrak{e}/\mathfrak{f}}$ and $\mathrm{Tr}_{\mathfrak{e}/\mathfrak{f}}$ are both surjective.*

**Proof:** Suppose $\mathfrak{f}$ is a finite field with $q$ elements and $[\mathfrak{e}\colon \mathfrak{f}] = n$. In order to prove the norm's surjectivity, it suffices to consider the map $\mathrm{N}_{\mathfrak{e}/\mathfrak{f}}\colon \mathfrak{e}^\times \to \mathfrak{f}^\times$. Both $\mathfrak{e}^\times$ and $\mathfrak{f}^\times$ are cyclic, so we can take $a$ to be a generator of $\mathfrak{e}^\times$ which has order $\mathrm{ord}(a) = q^n - 1$. Since $\mathfrak{e}/\mathfrak{f}$ is a cyclic Galois extension, $\mathrm{Gal}(\mathfrak{e}/\mathfrak{f})$ is generated by the $q^{th}$ powers [Lan13, Chapter I,§5]. Thus, $\mathrm{N}_{\mathfrak{e}/\mathfrak{f}}(a) = a \cdot a^q \cdot a^{q^2} \cdot \ldots \cdot a^{q^{n-1}} = a^{\frac{q^n-1}{q-1}}$. We now show that $\mathrm{ord}(a^{\frac{q^n-1}{q-1}}) = q - 1$, which will imply it generates all of $\mathfrak{f}^\times$.

We know $(a^{\frac{q^n-1}{q-1}})^{q-1} = a^{q^n-1} = 1$ so $\mathrm{ord}(a^{\frac{q^n-1}{q-1}})$ divides $q-1$. Suppose that $\mathrm{ord}(a^{\frac{q^n-1}{q-1}}) = k < q - 1$. Then, we have that

$$a^{(q^n-1)(\frac{k}{q-1})} = (a^{\frac{q^n-1}{q-1}})^k = 1$$

which contradicts the fact that $\mathrm{ord}(a) = q^n - 1$ since $(q^n - 1)(\frac{k}{q-1}) < q^n - 1$, hence $\mathrm{N}_{\mathfrak{e}/\mathfrak{f}}$ is surjective.

Since the trace is an $\mathfrak{f}$-linear map and its image is contained in $\mathfrak{f}$, we see the image is at most 1-dimensional, thus the kernel must have dimension either $n$ or $n-1$. We note that $\mathrm{Tr}_{\mathfrak{e}/\mathfrak{f}}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{n-1}}$ is a polynomial of degree $q^{n-1}$ so it has at most $q^{n-1}$ roots. Since there are $q^n$ elements in $\mathfrak{e}$, there must be some $x \in \mathfrak{e}$ such that $\mathrm{Tr}_{\mathfrak{e}/\mathfrak{f}}(x) \neq 0$, and hence the dimension of the kernel must equal $n-1$ and the image of $\mathrm{Tr}_{\mathfrak{e}/\mathfrak{f}}$ is all of $\mathfrak{f}$. ∎

## 2.3 Ramification

Let $F$ be a non-archimedean local field and $E/F$ an algebraic extension of degree $n$, embedded into a fixed separable closure $\overline{F}$ of $F$. Then, $E$ is also a non-archimedean local field; we let $\mathcal{O}_E$, $\mathcal{P}_E$, $\varpi_E$ and $\mathfrak{e}$ denote its integer ring, its prime ideal, a uniformizer and its residue field, respectively.

By [Gou97, Theorem 5.3.5], we can relate the discrete norms and valuations of $E$ and $F$ through the use of the algebraic norm.

**Proposition 2.3.1.** *The discrete norm on $E$ can be chosen to satisfy $|x|_E = \sqrt[n]{|\mathrm{N}_{E/F}(x)|}$ and so $\nu_E(x) = \frac{1}{n}\nu_F(\mathrm{N}_{E/F}(x))$ for all $x \in E$.*

In particular, we have a map $\nu_E\colon E \to \mathbb{Q}$ whose restriction to $F$ gives $\nu_F$; thus we say we have extended $\nu_F$ to $E$. By normalizing $\nu_F$ to be such that $\nu_F(\varpi) = 1$, it follows that $\nu_E\colon E^\times \to \frac{1}{n}\mathbb{Z}$, whence it takes values in $\frac{1}{n}\mathbb{Z} \cup \{\infty\}$. However, this map need not be surjective.

**Proposition 2.3.2.** *The image of $E^\times$ under the map $\nu_E$ is of the form $\frac{1}{e}\mathbb{Z}$, where $e$ is an integer which divides $n = [E\colon F]$.*

**Proof:** For all $x, y \in E^\times$ we have

$$\nu_E(xy) = \nu_E(x) + \nu_E(y)$$

so $\nu_E$ is a homomorphism from $E^\times$ to $\frac{1}{n}\mathbb{Z}$. Since $\varpi \in F^\times \subset E^\times$, we have that $\varpi = u\varpi_E^e$ for some $u \in \mathcal{O}_E^\times, e \in \mathbb{Z}_{>0}$. Thus,

$$\nu_E(\varpi_E^e) = \nu_E(u\varpi_E^e) = \nu_E(\varpi) = \nu_F(\varpi) = 1$$

whence $\nu_E(\varpi_E) = \frac{1}{e}$. Since this generates $\nu_E(E^\times)$ and this is a subgroup of $\frac{1}{n}\mathbb{Z}$, the result follows. ∎

We note that for each $a \in \mathbb{Z}$, if $p = \mathrm{char}(\mathfrak{f})$ then $a \in \mathcal{O}^\times$ if and only if $p$ does not divide $a$. Results from [FV02], [Gou97], and [Kob12] will now be used to introduce the concept of ramification.

**Definition 2.3.3.** *Let $E/F$ be a finite extension of degree $n$ and let $e$ be the unique positive integer defined by*

$$\nu_E(E^\times) = \frac{1}{e}\mathbb{Z}$$

*where $\nu_E$ denotes the extension of the valuation $\nu_F$ to $E$. We call $e$ the* ramification index of $E$ over $F$. *The extension $E/F$ is* unramified *if $e = 1$ and* ramified *if $e > 1$. Furthermore, if $e = n$ then the extension $E/F$ is* totally ramified. *We let $f$ denote the integer $f \coloneqq n/e$.*

**Proposition 2.3.4.** *Let $E/F$ be an extension of degree $n = e \cdot f$ with ramification index $e$. The residue field of $E$ is a degree $f$ extension of the residue field of $F$.*

**Proof:** Let $\mathfrak{f}$ denote the residue field of $F$ and $\mathfrak{e}$ that of $E$. Set $m = [\mathfrak{e}\colon \mathfrak{f}]$; we want to show that $e \cdot m = n$. Choose a set $\alpha_1, \ldots, \alpha_m \in \mathcal{O}_E^\times$ such that their images $\overline{\alpha_1}, \ldots, \overline{\alpha_m} \in \mathfrak{e}$ form a basis of $\mathfrak{e}$ over $\mathfrak{f}$.

We claim that $\{\alpha_i \mid i = 1, \ldots, m\}$ form a linearly independent set over $F$. Indeed, if there exist some non-trivial $c_i \in F$ such that $\sum_{i=1}^m c_i\alpha_i = 0$, we can scale by $c_k^{-1}$ for a $k$ chosen such that $|c_k|$ is maximal, and then reduce modulo $\varpi_E$ to obtain a dependence relation in $\mathfrak{e}$.

Consider the set $\mathcal{C} \coloneqq \{(\varpi_E)^j\alpha_i \mid 0 \le j \le e-1, 1 \le i \le m\}$. We will now show that every $x \in \mathcal{O}_E$ is an $\mathcal{O}$-linear combination of elements in $\mathcal{C}$. Indeed, by reducing mod $\varpi_E$, we obtain $x = \overline{x} + n_1\varpi_E$ where $\overline{x} = \sum_{i=1}^m c_{1i}\alpha_i$ for some $c_{1i} \in \mathcal{O}, n_1 \in \mathcal{O}_E$. We

can perform the same process on $n_1\varpi_E$ to obtain $n_1\varpi_E = \sum_{i=1}^{m} c_{2i}\alpha_i\varpi_E + n_2(\varpi_E)^2$. By repeating $e-1$ times on consecutive powers of $\varpi_E$, we get

$$x = \sum_{i=1}^{m} c_{1i}\alpha_i + \sum_{i=1}^{m} c_{2i}\alpha_i\varpi_E + \cdots + \sum_{i=1}^{m} c_{e-1,i}\alpha_i(\varpi_E)^{e-1} + n_e(\varpi_E)^e$$

for $c_{ji} \in \mathcal{O}, n_e \in \mathcal{O}_E$. Since $(\varpi_E)^e$ and $\varpi$ have the same valuation, we can write $n_e(\varpi_E)^e = \varpi x'$ for some $x' \in \mathcal{O}_E$. Identical iterations can then be performed on $x'$, giving a new linear combination of $\mathcal{C}$ mod $\varpi^2$. Continuing this process gives a sequence in $\mathcal{O}$, which converges because the terms have increasing valuation. Taking the limit yields an expression of $x$ as a linear combination of the elements of $\mathcal{C}$ with coefficients in $\mathcal{O}$ as promised.

We now will show that elements of $\mathcal{C}$ are $F$-linearly independent. Indeed, suppose there exist some $x_{j,i} \in F$ such that

$$\sum x_{j,i}(\varpi_E)^j\alpha_i = 0.$$

We begin by scaling this equation by $x_{j,i}^{-1}$ as before, where $x_{j,i}$ is the element of largest norm, to ensure all $x_{j,i}$ are elements of $\mathcal{O}$, with at least one in $\mathcal{O}^\times$ not divisible by $\varpi$. Reducing mod $\varpi_E$ yields a dependence relation $\overline{x_{j,i}}$ for the $\overline{\alpha_i}$, and hence must be trivial. Thus, the $x_{0,i}$ are divisible by $\varpi$, and so we can divide the entire relation by $\varpi$. By sequentially reducing mod $\varpi_E$ as per [Gou97, Proposition 5.4.6], one concludes that all of the $x_{j,i}$ are divisible by $\varpi$. This contradicts our original assumption, so $\mathcal{C}$ is a linearly independent generating set of $\mathcal{O}_E$.

This allows us to conclude that $\mathcal{C}$ also forms an $F$-basis for $E$, since for all $x \in E$ we can find an $r \in \mathbb{Z}_{\geq 0}$ such that $\varpi^r x \in \mathcal{O}_E$. This completes the proof since $e \cdot m = [E\colon F] = n$. ∎

These results will now be used to classify all finite extensions of $F$, beginning with the unramified ones.

### 2.3.1 Unramified Extensions

Our next goal is to demonstrate that finite unramified extensions $E$ of $F$ are in one-to-one correspondence with finite extensions of the residue field $\mathfrak{f}$ of $F$. We begin with a consequence of Hensel's Lemma, which will aid in the proof of the uniqueness of these types of extensions.

**Lemma 2.3.5.** *Suppose $E$ is an extension of $F$ of degree $n = e \cdot f$ where $e$ is the ramification index and $|\mathfrak{f}| = q$. Then, $E$ contains the splitting field $\tilde{F}$ of $x^{q^f-1} - 1$ over $F$ and $[\tilde{F} : F] = f$.*

**Proof:** Let $\mathfrak{e}$ denote the residue field of $E$; by hypothesis it has $q^f$ elements so the cyclic group $\mathfrak{e}^\times$ has $q^f-1$ elements, precisely given by distinct roots of the polynomial $g(x) = x^{q^f-1} - 1$. Since $q^f = 0$ in $\mathfrak{f}$, it follows that $g'(\overline{\alpha}) = (q^f-1)\overline{\alpha}^{q^f-1}$ is non-zero for all $\overline{\alpha} \in \mathfrak{e}^\times$. Thus, by Hensel's Lemma 2.1.5, each $\overline{\alpha} \in \mathfrak{e}^\times$ lifts to a unique root $\alpha \in \mathcal{O}_E^\times$ of $g$, so $g$ splits in $E$. Let $\tilde{F} \subseteq E$ denote the splitting field of $g$; then, by the proof of Propostion 2.3.4, the above correspondence shows that $[\mathfrak{e} : \mathfrak{f}] = [\tilde{F} : F] = f$. ∎

In fact, one can show that the roots of $g(x) = x^{q^f-1} - 1$ form a cyclic subgroup of $\mathcal{O}_E^\times$ of order $q^f - 1$, denoted $\mu_{q^f-1}$ and called the $(q^f-1)$st roots of unity. It follows that

$$\mathcal{O}_E^\times/(1+\mathcal{P}_E) \simeq \mu_{q^f-1} \simeq \mathfrak{e}^\times. \tag{2.3.1}$$

Further, given two unramified extensions of degree $f$, the previous result implies they both contain the splitting field $\tilde{F}$. This splitting field is unique with respect to a choice of algebraic closure $\overline{F}$, hence we obtain the following consequence.

**Corollary 2.3.6.** *For each $f \in \mathbb{Z}_{>0}$, there is exactly one unramified extension of $F$ of degree $f$ and thus it is normal.*

Without loss of generality, we take $\varpi_E \coloneqq \varpi$ when $E/F$ is unramified. Moreover, the above Lemma can be interpreted as saying that the unique unramified extension of degree $f$ is given by $E = F(\xi)$ where $\xi$ is a primitive $(q^f-1)$st root of unity, but in fact there are more convenient choices of generators possible.

**Proposition 2.3.7.** *Let $\beta \in \mathcal{O}^\times$ be such that $g(x) = x^f - \beta$ is irreducible mod $\mathcal{P}$ and let $\tilde{F}$ denote the degree $f$ unramified extension of $F$. Then, for any root $\alpha$ of $g$, $\tilde{F} = F(\alpha)$.*

**Proof:** Since $g$ is irreducible mod $\mathcal{P}$, it is irreducible in $\mathcal{O}[x]$, since any factorization would descend to a factorization mod $\mathcal{P}$. Then, by [Gou97, Lemma 5.3.7.] $g$ is also irreducible in $F[x]$ and hence $E = F(\alpha)$ is a degree $f$ extension of $F$. Let $\mathfrak{e}$ denote the residue field of $E$ and $\overline{\alpha} \in \mathfrak{e}$ be the image of $\alpha$ mod $\mathcal{P}_E$. Denote by $\overline{g}(x)$ the polynomial $g(x)$ when viewed as an irreducible polynomial in $\mathfrak{f}[x]$; then, $\overline{\alpha}$ is a root of $\overline{g}(x)$.

Since $\overline{\alpha}$ generates the unique extension field of degree $f$ of $\mathfrak{f}$, we must have $[\mathfrak{e} : \mathfrak{f}] \geq f$. However, as the degree of the residue field extension is at most the degree of $E/F$, we conclude that equality holds and therefore that the extension is unramified. By Corollary 2.3.6, we must have $E = \tilde{F}$. ∎

This proof will be incredibly useful when classifying extensions of degree 2 and 4. For example, to generate the unramified quadratic extension of $F$, it suffices to choose any $\beta \in \mathcal{O}$ that is not a square mod $\mathcal{P}$.

We now come to the following result and subsequent proof from [Lan13, Chapter II,§4] regarding a powerful property of norm maps specific to unramified extensions.

**Proposition 2.3.8.** *If $E/F$ is unramified, then $\mathrm{N}_{E/F}$ maps $\mathcal{O}_E^\times$ surjectively onto $\mathcal{O}^\times$.*

**Proof:** Let $G = \mathrm{Gal}(E/F)$. Recall that since $E/F$ is unramified, we may take without loss of generality $\varpi_E = \varpi$. Then, for any $k \geq 1$ and $1 + x\varpi^k \in 1 + \mathcal{P}_E^k$, we have

$$\mathrm{N}_{E/F}(1 + x\varpi^k) = \prod_{\sigma \in G} \sigma(1 + x\varpi^k) = \prod_{\sigma \in G} (1 + \sigma(x)\varpi^k) \in 1 + \mathcal{P}^k.$$

Moreover, modulo $\mathcal{P}^{k+1}$ this gives

$$\mathrm{N}_{E/F}(1 + x\varpi^k) \equiv 1 + \sum_{\sigma \in G} \sigma(x)\varpi^k \equiv 1 + \varpi^k \,\mathrm{Tr}_{E/F}(x).$$

In particular $\mathrm{N}_{E/F}(1+\mathcal{P}_E) \subseteq 1+\mathcal{P}$, thus the norm induces a map from $\mathcal{O}_E^\times/(1+\mathcal{P}_E) \to \mathcal{O}^\times/(1+\mathcal{P})$, which coincides by (2.3.1) with the map $\mathrm{N}_{\mathfrak{e}/\mathfrak{f}} \colon \mathfrak{e}^\times \to \mathfrak{f}^\times$. We saw in Lemma 2.2.20 that $\mathrm{N}_{\mathfrak{e}/\mathfrak{f}}$ is surjective, which we will now use to show the surjectivity of $\mathrm{N}_{E/F}$. Let $x \in \mathcal{O}^\times$. Then, by our previous argument, there exists $\alpha_0 \in \mathcal{O}_E^\times$ such that $\mathrm{N}_{E/F}(\alpha_0) \equiv x \pmod{\mathcal{P}}$. We proceed by induction. Suppose $k \geq 0$ and we have constructed a sequence of $\alpha_k \in \mathcal{O}_E^\times$ such that

$$x \,\mathrm{N}_{E/F}(\alpha_0 \dots \alpha_k)^{-1} \equiv 1 \pmod{\mathcal{P}^{k+1}}.$$

Write $x \,\mathrm{N}_{E/F}(\alpha_0 \cdots \alpha_k)^{-1} = 1 + c\varpi^{k+1}$ for some $c \in \mathcal{O}$. In Lemma 2.2.20 we also showed the surjectivity of $\mathrm{Tr}_{\mathfrak{e}/\mathfrak{f}}$, so let $d \in \mathcal{O}$ be such that $\mathrm{Tr}_{E/F}(d) \equiv c \pmod{\mathcal{P}}$, and set $\alpha_{k+1} = 1 + d\varpi^{k+1}$. Then, we have

$$\mathrm{N}_{E/F}(\alpha_{k+1}) \equiv 1 + \mathrm{Tr}_{E/F}(d)\varpi^{k+1} \equiv 1 + c\varpi^{k+1} \pmod{\mathcal{P}^{k+1}},$$

completing the induction. Since $\lim_{k\to\infty} |\alpha_k - 1| = 0$, the product $\alpha = \prod \alpha_k$ converges in $\mathcal{O}_E$ and satisfies $\mathrm{N}_{E/F}(\alpha) = x$. ∎

This result yields the following corollary, which is our final statement prior to moving on to a different kind of field extension.

**Corollary 2.3.9.** *If $E/F$ is unramified, then $\mathrm{N}_{E/F}$ maps non-squares of $\mathcal{O}_E^\times$ to non-squares of $\mathcal{O}^\times$.*

**Proof:** Note that $\mathcal{O}^\times/(\mathcal{O}^\times)^2$ and $\mathcal{O}_E^\times/(\mathcal{O}_E^\times)^2$ have order 2 (we prove this in §2.4.1). Since the norm is multiplicative, $\mathrm{N}_{E/F}(\mathcal{O}_E^\times)^2 \subseteq (\mathcal{O}^\times)^2$. Let $\varepsilon_E \in \mathcal{O}_E^\times$ be a non-square; by multiplicativity we have $\mathrm{N}_{E/F}(\varepsilon_E(\mathcal{O}_E^\times)^2) \subseteq \mathrm{N}_{E/F}(\varepsilon_E)(\mathcal{O}^\times)^2$. By Proposition 2.3.8, the norm surjects onto $\mathcal{O}^\times$, thus $\mathrm{N}_{E/F}(\varepsilon_E)$ must be a non-square. ∎

### 2.3.2 Totally and Tamely Ramified Extensions

In §2.3.1, we considered field extensions $E/F$ such that $e = 1$; we now study the case when $f = 1$ under a certain "tameness" hypothesis, which will be satisfied for the duration of the thesis. We first need the following lemma, arising as another consequence of Hensel's Lemma.

**Lemma 2.3.10.** *Suppose $F$ has residue field $\mathfrak{f}$. If $e \in \mathbb{Z}_{>0}$ is relatively prime to $|\mathfrak{f}|$ then the map $\varphi\colon 1+\mathcal{P} \to 1+\mathcal{P}$ given by $\varphi(v) = v^e$ is surjective.*

**Proof:** If $|v| < 1$ then so is $|v^e| = |v|^e$, so $\varphi$ is well-defined. Let $u \in 1+\mathcal{P}$ and consider the polynomial $g(x) = x^e - u$. Then, $g(1) = 1 - u \in \mathcal{P}$ and $g'(1) = e$, which satisfies $|e| = 1$ by hypothesis. Therefore by Hensel's Lemma 2.1.5 there exists a unique $v \in 1+\mathcal{P}$ such that $g(v) = 0$, that is, such that $v^e = u$. ∎

**Corollary 2.3.11.** *Suppose $q = |\mathfrak{f}|$ and $e$ is relatively prime to $q$. Then, $\mathcal{O}^\times/(\mathcal{O}^\times)^e$ is a cyclic group with $\gcd(e, q-1)$ elements.*

**Proof:** By Lemma 2.3.10, we have $(1+\mathcal{P})^e = 1+\mathcal{P}$. The quotient map $\mathcal{O}^\times \to \mathfrak{f}^\times$ is a group homomorphism and thus factors through (by (2.3.1)) to a map $\varphi\colon \mathcal{O}^\times/(\mathcal{O}^\times)^e \to \mathfrak{f}^\times/(\mathfrak{f}^\times)^e$. This is an isomorphism by the third isomorphism theorem, hence it suffices to prove the result for $\mathfrak{f}^\times/(\mathfrak{f}^\times)^e$.

The group $\mathfrak{f}^\times$ is cyclic of order $q-1$, thus is given by

$$\mathfrak{f}^\times = \{\beta^i \mid 0 \le i \le q-2\}$$

for some generator $\beta \in \mathfrak{f}^\times$. This allows us to write $(\mathfrak{f}^\times)^e = \{\beta^{ie} \mid 0 \le i \le q-2\}$ which has kernel $\{\beta^n\}$ for $n$ such that $n \cdot e \equiv 0 \pmod{q-1}$ since $\operatorname{ord}(\beta) = q-1$. Thus, $(\mathfrak{f}^\times)^e = \langle\beta^k\rangle$ where $k = \gcd(e, q-1)$ and hence representatives for the quotient group $\mathfrak{f}^\times/(\mathfrak{f}^\times)^e$ are given by $\{1, \beta, \ldots, \beta^{k-1}\}$. ∎

These results motivate the following definition.

**Definition 2.3.12.** *Let $E/F$ be an extension of degree $n = e \cdot f$ with ramification index $e$ and $|\mathfrak{f}| = q$. Then, $E/F$ is* tamely ramified *if $q$ and $e$ are relatively prime.*

The work of this thesis will always be in the tamely ramified case, as we will be studying quadratic and quartic extensions where $p \neq 2$.

With these tools at our disposal, we now present the following theorem to complete the classification, which was originally adapted from [PR01, Theorem 7.2].

**Theorem 2.3.13.** *Suppose $E/F$ is a totally and tamely ramified extension of degree $e$. Then, $E = F(\alpha)$ where $\alpha$ is a root of some irreducible polynomial of the form $m(x) = x^e - u\varpi$ for some $u \in \mathcal{O}^\times$.*

**Proof:** Let $\varpi_E$ be a uniformizer of $E$. By the proof of Proposition 2.3.4, the elements $\{1, \varpi_E, \varpi_E^2, \cdots, \varpi_E^{e-1}\}$ are linearly independent over $F$. Since $E$ is an extension of degree $e$ over $F$, this set is a basis for $E/F$ and thus $E = F(\varpi_E)$. Since $E/F$ is totally ramified with ramification index $e$, we have $(|\varpi_E|_E)^e = |\varpi|$. It follows that $\varpi \in (\mathcal{P}_E)^e$ so $(\varpi_E)^e = a\varpi$ for some $a \in \mathcal{O}_E^\times$.

Consider the image $\overline{a} \in \mathfrak{e}$ of $a$. Since the extension is totally ramified, $\mathfrak{e} = \mathfrak{f}$. Let $u \in \mathcal{O}^\times$ be any element whose image in $\mathfrak{f}$ is $\overline{a}$. Then, $ua^{-1} \in 1 + \mathcal{P}_E$ so by Lemma 2.3.10, since $e$ is relatively prime to $|\mathfrak{e}| = q$, there exists $v \in 1 + \mathcal{P}_E$ such that $v^e = ua^{-1}$. Set $\alpha = v\varpi_E$. Since $v$ is invertible, $\alpha$ is another uniformizer of $E$. Thus, $\alpha$ generates $E$ over $F$ and satisfies

$$\alpha^e = v^e(\varpi_E)^e = ua^{-1}a\varpi = u\varpi$$

for some $u \in \mathcal{O}^\times$, as required. ∎

In contrast to the unramified extensions, extensions of this type are not unique.

**Corollary 2.3.14.** *If $q = |\mathfrak{f}|$ and $e$ is relatively prime to $q$ then there are exactly $\gcd(e, q-1)$ totally ramified extensions of $F$ of degree $e$ up to isomorphism.*

**Proof:** For any $u \in \mathcal{O}^\times$, the roots of $x^e - u\varpi$ in $\overline{F}$ have norm $|\varpi|^{1/e}$, so no product of these roots can lie in $F$, whence this polynomial is irreducible over $F$. If $u' = a^e u$ for some $a \in \mathcal{O}^\times$ and $\alpha$ is a root of the irreducible polynomial $x^e - u\varpi$, then $a\alpha$ is a root of $x^e - u'\varpi$ and $F(\alpha) = F(a\alpha)$.

Conversely, if an extension $E$ contains an $e$th root of $u\varpi$ and an $e$th root of $u'\varpi$, then $E$ also contains an $e$th root $u'u^{-1}$, say $\gamma$. Since $|u'u^{-1}|_E = 1$, we have that $\gamma \in \mathcal{O}_E^\times$, however we will now show that in fact $\gamma \in \mathcal{O}^\times$.

Consider the image $\overline{\gamma}$ of $\gamma$ in $\mathfrak{e}$. Since $E/F$ is totally ramified $\mathfrak{e} = \mathfrak{f}$. Thus, by Hensel's Lemma 2.1.5, $\overline{\gamma}$ can by lifted to a root in $\mathcal{O}^\times$, whence $u' = \gamma^e u$ for some $\gamma \in \mathcal{O}^\times$. Therefore, the totally ramified extensions obtained from distinct elements of $u \in \mathcal{O}^\times/(\mathcal{O}^\times)^e$ are non-isomorphic. The statement follows now from Corollary 2.3.11. ∎

In the section that follows, we see that there are more than $\gcd(4, q-1) = 2$ distinct (non-equal) totally ramified quartic extensions of $F$ when $-1 \notin F^{\times 2}$, however field isomorphisms exist between pairs of them.

## 2.4 Classifying Quartic Extensions

Our objective in this section is to identify all degree four field extensions of a non-archimedean local field $F$ up to isomorphism. In order to do so, we must first understand the quadratic extensions.

### 2.4.1 Quadratic Extensions

We begin by investigating the square class group of $F$ (when $p \neq 2$), given by the quotient $F^\times/F^{\times 2}$.

**Lemma 2.4.1.** *Let $a = u\varpi^k$ be an arbitrary element of $F^\times$ for some $u \in \mathcal{O}^\times$ and $k \in \mathbb{Z}$, and consider the quotient map $\mathcal{O} \to \mathfrak{f}$ which sends $u$ to $\overline{u} = u + \mathcal{P}$. Then, $a \in F^{\times 2}$ if and only if $k$ is even and $\overline{u} \in \mathfrak{f}^{\times 2}$.*

**Proof:** Let $a = u\varpi^k \in F^\times$ and suppose $k = 2n \in \mathbb{Z}_{\neq 0}$ and $u = x_0^2 + \varpi z$ for some $z \in \mathcal{O}^\times, x_0 \in \mathfrak{f}$. Consider the function $f(x) = x^2 - u$ which is such that $f(x_0) \equiv 0 \pmod{\varpi}$ and $f'(x_0) = 2x_0 \not\equiv 0 \pmod{\varpi}$ since $p \neq 2$. By Hensel's Lemma (Lemma 2.1.5), there exists a unique $\beta \in \mathcal{O}$ for which $f(\beta) = 0$. Hence $\beta^2 = u$ and $a = (\varpi^n\beta)^2 \in F^{\times 2}$.

Conversely, suppose $a = x^2$ for some $x \in F^\times$. Write $x = y\varpi^k$ for some $y \in \mathcal{O}^\times, k \in \mathbb{Z}$, so $a = y^2\varpi^{2k}$. If $\overline{y}$ is the image of $y$ in $\mathfrak{f}^\times$, then since $y \mapsto \overline{y}$ is a homomorphism of multiplicative groups, $\overline{(y^2)} = (\overline{y})^2 \in \mathfrak{f}^{\times 2}$, so the result follows. ∎

This lemma will now be used to prove the following result regarding the square class group of $F$.

**Proposition 2.4.2.** *Let $\varepsilon \in \mathcal{O}^\times$ be non-square. Then, a set of representatives for $F^\times/F^{\times 2}$ is given by $\{1, \varepsilon, \varpi, \varepsilon\varpi\}$.*

**Proof:** Denote by $[a]$ the class in $F^\times/F^{\times 2}$ of an element $a \in F^\times$. Let $\varepsilon \in \mathcal{O}^\times$ be a non-square, so $[\varepsilon] \neq [1]$. For any $a \in F^\times$, $\nu_F(a^2)$ is even so we cannot have $\varpi = 1a^2$ or $\varepsilon a^2$ for any $a$, and hence $[\varpi]$ represents its own class of non-squares.

In the group $F^\times/F^{\times 2}$, $[\varepsilon]$ and $[\varpi]$ are distinct elements of order 2. If $[\varepsilon\varpi] = [1]$ then $[\varepsilon] = [\varpi]^{-1} = [\varpi]$ which is a contradiction. Furthermore, if $[\varepsilon\varpi] = [\varepsilon]$, then $[\varpi] = [1]$ and if $[\varepsilon\varpi] = [\varpi]$, then $[\varepsilon] = [1]$. Thus $[1], [\varepsilon], [\varpi], [\varepsilon\varpi]$ are distinct.

We will now show that these classes cover all elements of $F^\times/F^{\times 2}$. Consider $a \in F^\times$ and write $a = u\varpi^k$ for some $u \in \mathcal{O}^\times$ Then, $[a] = [u]$ if $k$ is even and $[a] = [u][\varpi]$ if $k$ is odd. By Lemma 2.4.1, if $\overline{u} \in \mathfrak{f}^{\times 2}$, then $[u] = [1]$. Conversely, if $\overline{u} \notin \mathfrak{f}^{\times 2}$ then we can find a $\overline{z} \in \mathfrak{f}^2$ such that $\overline{u} = \overline{z}^2\varepsilon$. We can lift this $\overline{z}$ to some $z \in \mathcal{O}^\times$ to give $u = z^2\varepsilon$, and hence $[u] = [\varepsilon]$ which completes the proof. ∎

For each representative $\alpha$ of a non-trivial square class, let $\sqrt{\alpha}$ denote a choice of square root. Then, the extension $F(\sqrt{\alpha})$ is independent of both the choice of square root, since $F(\sqrt{\alpha}) = F(-\sqrt{\alpha})$, and of the choice of $\alpha$ in its square class, since $F(\sqrt{\alpha x^2}) = F(\sqrt{\alpha}x) = F(\sqrt{\alpha})$ for all $x \in F^\times$. In consequence, we have exactly three choices for quadratic field extensions of $F$ up to isomorphism, namely $F(\sqrt{\varepsilon}), F(\sqrt{\varpi}), F(\sqrt{\varepsilon\varpi})$.

Furthermore, since quadratic extensions are either unramified or totally ramified, Proposition 2.3.7 implies that $F(\sqrt{\varepsilon})$ for any non-square $\varepsilon \in \mathcal{O}^\times$ is the unique

quadratic unramified extension. The extensions $F(\sqrt{\varpi}) \not\simeq F(\sqrt{\varepsilon\varpi})$ on the other hand are both tamely and totally ramified.

We now explore the algebraic norm map with respect to these quadratic extensions.

**Lemma 2.4.3.** *Let $E/F$ be a quadratic extension. Then, $\mathrm{N}_{E/F}(E^\times)$ is a multiplicative subgroup of $F^\times$ which contains ${F^\times}^2$.*

**Proof:** Since the norm map is a homomorphism into $F^\times$, its image is necessarily a subgroup of $F^\times$. Further, $\mathrm{N}_{E/F}(x) = 0$ implies $x = 0$. Let $\lambda \in F^\times$. As per Example 2.2.18, $\mathrm{N}_{E/F}(\lambda) = \lambda^2$; hence ${F^\times}^2 \subseteq \mathrm{N}_{E/F}(E^\times)$ as required. ∎

Thus $F^\times/\mathrm{N}_{E/F}(E^\times)$ is a quotient of $F^\times/{F^\times}^2$, which we now narrow down further.

**Proposition 2.4.4.** *Let $E/F$ be a quadratic extension.*

*(1) If $E/F$ is ramified, then a set of representatives for $F^\times/\mathrm{N}_{E/F}(E^\times)$ is $\{1, \varepsilon\}$.*

*(2) If $E/F$ is unramified, then a set of representatives for $F^\times/\mathrm{N}_{E/F}(E^\times)$ is $\{1, \varpi\}$.*

**Proof:** Suppose $E/F$ is ramified, so $E \simeq F(\sqrt{\alpha})$ where $\alpha \in \{\varpi, \varepsilon\varpi\}$. As computed in Example 2.2.18, $\mathrm{N}_{E/F}(\sqrt{\alpha}) = -\alpha \notin {F^\times}^2$, so $\mathrm{Im}(\mathrm{N}_{E/F})$ is non-trivial. We will now show $\varepsilon \notin \mathrm{N}_{E/F}(E^\times)$ to conclude that the norm does not surject on the entire group $F^\times/{F^\times}^2$. Suppose for contradiction there exist $a, b \in F^\times$ such that $a^2 - \alpha b^2 = \varepsilon$. Since $\nu_F(a^2)$ is even and $\nu_F(\alpha b^2)$ is odd, we must have that

$$0 = \nu_F(a^2 - \alpha b^2) = \min\{\nu_F(a^2), \nu_F(\alpha b^2)\} = \nu_F(a^2)$$

so $\nu_F(a) = 0$. Then, $a^2 \equiv \varepsilon \pmod{\mathcal{P}}$ which is a contradiction; thus the quotient $F^\times/\mathrm{N}_{E/F}(E^\times)$ is given by $\{1, \varepsilon\}$.

We now consider the unramified case, so $E \simeq F(\sqrt{\varepsilon})$. By Proposition 2.3.8, $\mathrm{N}_{E/F}$ surjectively maps $\mathcal{O}_E^\times \to \mathcal{O}^\times$, so $\varepsilon \in \mathrm{N}_{E/F}(E^\times)$ and the image of the norm is non-trivial. As previously, it remains to show that $\mathrm{N}_{E/F}(E^\times)$ does not surject onto the entire square class group. Suppose for contradiction that $\varpi \in \mathrm{N}_{E/F}(E^\times)$, so there exist $a, b \in F^\times$ such that $a^2 - \varepsilon b^2 = \varpi$. This implies that $\nu_F(a^2 - \varepsilon b^2) = 1$, so both $\nu_F(a^2), \nu_F(\varepsilon b^2)$ equal some integer $k \geq 0$. Define $a' = a\varpi^k$ and $b' = b\varpi^k$; both are elements of $\mathcal{O}$ by construction. We compute

$$(a')^2 - \varepsilon(b')^2 = \varpi^{2k}(a^2 - \varepsilon b^2) \equiv 0 \pmod{\mathcal{P}}$$

which is a contradiction, as $\varepsilon$ is not a square mod $\mathcal{P}$. ∎

### 2.4.2 Quartic Extensions

We are now ready to classify the quartic extensions $E'$ of $F$ up to isomorphism, which will help us to later study the elliptic tori in the special orthogonal group of a 4-dimensional quadratic form.

The work in this section requires us to choose a root of the irreducible polynomial $x^4 - \alpha \in F[x]$ to adjoin to $F$; without loss of generality we will call this root $\sqrt[4]{\alpha}$. Indeed, because we are only interested in field extensions up to isomorphism, it does not matter which root we take; the resulting extensions are isomorphic.

These first two propositions correspond to the two main types of degree four extensions we encounter. Once these are well understood, we will delve into the specifics and prove that we have covered all possibilities.

**Proposition 2.4.5.** *Supppose $E' \simeq F(\sqrt[4]{\alpha})$ is a quartic extension of $F$ for some root $\sqrt[4]{\alpha}$ of an irreducible polynomial $x^4 - \alpha \in F[x]$. If $-1 \in F^{\times 2}$, then $E'$ is Galois with $\mathrm{Gal}(E'/F) \simeq \mathbb{Z}/4\mathbb{Z}$.*

**Proof:** We begin by noting that the minimal polynomial of $\sqrt[4]{\alpha}$ over $F$ is $m(x) = x^4 - \alpha$, which we recall from Example 2.2.9 has roots $\{\pm\sqrt[4]{\alpha}, \pm i\sqrt[4]{\alpha}\}$ where $i^2 = -1$. Thus, when $-1 \in F^{\times 2}$, $E'$ is separable and normal, and hence Galois.

By Lemma 2.2.4 the automorphism group is $\mathrm{Gal}(E'/F) = \{\sigma_k \colon 0 \leq k \leq 3\}$ where $\sigma_k$ is defined by the relation $\sigma_k \colon \alpha \mapsto i^k\sqrt[4]{\alpha}$. It is simple to verify that $\sigma_0 = \mathrm{id}$, $\sigma_1, \sigma_3$ are both order 4, and $\sigma_2$ is order 2, hence $\mathrm{Gal}(E'/F) \simeq \mathbb{Z}/4\mathbb{Z}$ as required. ∎

As promised, we note that there is a field isomorphism between $F(\sqrt[4]{\alpha}) \simeq F(i\sqrt[4]{\alpha})$ via the map $\sigma_1 \colon \sqrt[4]{\alpha} \mapsto i\sqrt[4]{\alpha}$.

**Proposition 2.4.6.** *Suppose $E' \simeq F(\sqrt{\alpha}, \sqrt{\beta})$ is a quartic extension of $F$ for some non-squares $\alpha, \beta \in F^\times$ representing distinct square classes. Then, $E'$ is Galois with $\mathrm{Gal}(E'/F) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

**Proof:** Let $E' \simeq F(\sqrt{\alpha}, \sqrt{\beta})$, so $E'$ is the splitting field of the separable polynomial $f(x) = (x^2 - \alpha)(x^2 - \beta) \in F[x]$. Elements $\sqrt{\alpha}$ and $\sqrt{\beta}$ cannot be mapped to one another via an automorphism of $E'/F$ since $g_1(x) = x^2 - \alpha, g_2(x) = x^2 - \beta \in F[x]$ are irreducible polynomials and hence their roots are closed under automorphism. Therefore the automorphism group consists of the maps $\{\mathrm{id}, \sigma, \tau, \sigma\tau\}$ where

$$\sigma \colon \sqrt{\alpha} \mapsto -\sqrt{\alpha}, \qquad \tau \colon \sqrt{\beta} \mapsto -\sqrt{\beta}$$

hence $\mathrm{Gal}(E'/F) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. ∎

We will now focus on the unramified quartic extension $E'$, which by Corollary 2.3.6 is unique. Furthermore, by Proposition 2.3.7, this extension can be obtained by first

adjoining $\sqrt{\varepsilon}$ and then adjoining $\sqrt{\varepsilon_E}$, for $\varepsilon$ a non-square in $F$ and $\varepsilon_E$ a non-square in the quadratic subfield $E = F(\sqrt{\varepsilon}) \subset E'$.

When $-1 \in {F^\times}^2$, we can take $\varepsilon_E = \sqrt{\varepsilon}$. Indeed, if we suppose for contradiction that $\sqrt{\varepsilon} \in (E^\times)^2$, we must have that

$$\sqrt{\varepsilon} = (a + b\sqrt{\varepsilon})^2 = a^2 + b^2\varepsilon + 2ab\sqrt{\varepsilon}$$

for some $a, b \in F$. This implies that $a^2 + b^2\varepsilon = 0$, or $a^2 = -b^2\varepsilon$ which would imply that $\varepsilon$ is a square in $F$, thereby yielding a contradiction.

When $-1 \notin {F^\times}^2$, we take $\varepsilon = -1$, however we need to be more careful in choosing $\varepsilon_E$ and will use the following lemma.

**Lemma 2.4.7.** *Suppose $-1 \notin {F^\times}^2$ and let $E = F(i)$ for $i$ such that $i^2 = -1$ be the unramified quadratic extension. Then, there exists a non-square in $E$ of the form $\varepsilon_E = x + iy \in \mathcal{O}_E^\times$, such that $\mathrm{N}_{E/F}(\varepsilon_E) = -1$ and $x, y \in {F^\times}^2$.*

**Proof:** Since $-1 \notin {F^\times}^2$, we take $\varepsilon = -1$ and write $i = \sqrt{\varepsilon} \in E$. By Corollary 2.3.9, $\mathrm{N}_{E/F}$ gives a surjective map from non-squares of $E^\times$ to non-squares of $F^\times$, hence we can choose $\varepsilon_E$ such that $\mathrm{N}_{E/F}(\varepsilon_E) = -1$. In fact there are several such choices, each corresponding to a solution $\varepsilon_E = x+iy$ of $N_{E/F}(x+iy) = x^2+y^2 = -1$. Further, since for each $a \in F^\times$, exactly one of $a, -a \in {F^\times}^2$ and $a^2 = (-a)^2$, we may further impose that $x$ and $y$ are squares in $F^\times$ by replacing $x, y$ with $\pm x, \pm y$. ∎

Our classification of the Galois group of unramified extensions $E'/F$ follows.

**Lemma 2.4.8.** *Suppose $E'$ is an unramified quartic extension. Then, $E'$ is unique up to isomorphism and Galois with $\mathrm{Gal}(E'/F) \simeq \mathbb{Z}/4\mathbb{Z}$.*

**Proof:** The uniqueness and normality follow from Corollary 2.3.6, hence $E'$ is Galois. Furthermore, since $|\mathrm{Gal}(E'/F)| = [E' : F] = 4$ and $E'$ has a unique quadratic subfield $E = F(\sqrt{\varepsilon})$ (any other choice would make $E'$ ramified), we conclude via The Fundamental Theorem of Galois Theory (2.2.7) that $\mathrm{Gal}(E'/F) \simeq \mathbb{Z}/4\mathbb{Z}$. ∎

We now turn our focus to the partially ramified extensions ($e = 2, f = 2$). By Lemma 2.3.5, they are built by adjoining a totally ramified quadratic extension to the unramified quadratic extension $E \simeq F(\sqrt{\varepsilon})$. As per our discussion at the end of §2.4.1, we have two distinct choices for the totally ramified portion, and hence our partially ramified quartic extensions are given by $F(\sqrt{\varepsilon}, \sqrt{\varpi})$ and $F(\sqrt{\varepsilon}, \sqrt{\varepsilon_E\varpi})$.

**Lemma 2.4.9.** *Let $E \simeq F(\sqrt{\varepsilon})$ for some non-square $\varepsilon \in \mathcal{O}^\times$. There are exactly two partially ramified extensions of degree four up to isomorphism given by*

$$E_1' \simeq E(\sqrt{\varpi}) = F(\sqrt{\varepsilon}, \sqrt{\varpi}) \quad \text{and} \quad E_2' \simeq E(\sqrt{\varepsilon_E\varpi}) = F(\sqrt{\varepsilon}, \sqrt{\varepsilon_E\varpi}).$$

*Moreover, $E_1', E_2'$ are both Galois with $\mathrm{Gal}(E_1'/F) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{Gal}(E_2'/F) \simeq \mathbb{Z}/4\mathbb{Z}$.*

**Proof:** The result for $E_1' \simeq F(\sqrt{\varepsilon}, \sqrt{\varpi})$ follows from Lemma 2.4.6. For $E_2' \simeq F(\sqrt{\varepsilon}, \sqrt{\varepsilon_E \varpi})$, we consider two cases. When $-1 \in F^{\times 2}$ we have that $E_2' \simeq F(\sqrt[4]{\varepsilon \varpi^2})$, hence the result follows from Proposition 2.4.5.

Conversely, suppose $-1 \notin F^{\times 2}$ so $E_2' \simeq F(i, \sqrt{\varepsilon_E \varpi})$ for $\varepsilon_E = x + iy \in E = F(i)$, chosen as per Lemma 2.4.7. The minimal polynomial of $\sqrt{\varepsilon_E \varpi}$ over $F$ is given by $m(z) = z^4 - (2x\varpi)z^2 + (x^2 + y^2)\varpi^2 \in F[z]$ which has roots $\pm\sqrt{\varepsilon_E \varpi}, \pm\sqrt{\overline{\varepsilon_E}\varpi}$, where $\overline{\varepsilon_E} \coloneqq x - iy$. We first prove that $\overline{\varepsilon_E}$ is also a non-square in the subfield $E \subseteq E_2'$. Suppose for contradiction that $x - iy = (a + bi)^2$ for some $a, b \in E$. This implies that $\varepsilon_E = x + iy = (-a + bi)^2$ which is a contradiction. Thus, we can write $\overline{\varepsilon_E} = \gamma^2 \varepsilon_E$ for some $\gamma \in E^\times$. Then,

$$\sqrt{\overline{\varepsilon_E}\varpi} = \gamma\sqrt{\varepsilon_E \varpi} \in E_2'$$

so the extension contains all the roots of $m(z)$ and hence is Galois. The proof that $\mathrm{Gal}(E_2'/F) \simeq \mathbb{Z}/4\mathbb{Z}$ is identical to that of Lemma 2.4.8. ∎

The final type to classify are the totally and tamely ramified, which differ greatly depending on whether or not $-1$ is a square.

**Lemma 2.4.10.** *When $-1 \in F^{\times 2}$, there are exactly 4 totally ramified quartic extensions $E'$ of $F$ up to isomorphism, all Galois with $\mathrm{Gal}(E'/F) \simeq \mathbb{Z}/4\mathbb{Z}$. Conversely, when $-1 \notin F^{\times 2}$, there are exactly 2 totally ramified quartic extensions $E'$ of $F$ up to isomorphism, both non-Galois with $\mathrm{Aut}(E'/F) \simeq \mathbb{Z}/2\mathbb{Z}$.*

**Proof:** These extensions are necessarily tame since $p \neq 2$. By Theorem 2.3.13, totally and tamely ramified quartic extensions $E'$ are given by adjoining roots of the polynomial $x^4 - u\varpi$ to $F$, where $u \in \mathcal{O}^\times/(\mathcal{O}^\times)^4$.

By Corollary 2.3.11, $\mathcal{O}^\times/(\mathcal{O}^\times)^4$ is a cyclic group with $\gcd(4, q-1)$ elements. We claim that any non-square $\varepsilon \in \mathcal{O}^\times$ is a generator. Indeed, if $-1$ is not a square, then $\gcd(4, q-1) = 2$ and $\mathcal{O}^\times/(\mathcal{O}^\times)^4 = \mathcal{O}^\times/(\mathcal{O}^\times)^2$ is represented by $\{1, \varepsilon\}$.

Conversely, if $-1$ is a square, then $\gcd(4, q-1) = 4$ and $\varepsilon^2 = a^4$ has no solution in $F$ unless $\varepsilon$ is a square. Thus, $\varepsilon$ has order 4 so it follows that $\{1, \varepsilon, \varepsilon^2, \varepsilon^3\}$ represent distinct classes of the cyclic group.

Thus, $E' \simeq F(\sqrt[4]{\alpha})$ where $\alpha \in \{\varepsilon^k \varpi \mid 0 \leq k \leq 3\}$ when $-1 \in F^{\times 2}$, and $\alpha \in \{\varepsilon^k \varpi \mid k = 0, 1\}$ when $-1 \notin F^{\times 2}$. When $-1 \in F^{\times 2}$, the rest follows from Proposition 2.4.5. Conversely, when $-1 \notin F^{\times 2}$, then since $E'$ is totally ramified we have that $-1 \notin E'^{\times 2}$. The rest follows from Example 2.2.9. ∎

We summarize our results from this section in the following two tables. The first describes the isomorphism classes of quartic extensions of $F$ when $-1$ is a square, and the second covers when $-1$ is not a square.

| **Ramification** | **Quadratic Subfield(s)** | **Type** | **Aut($E'/F$)** |
|---|---|---|---|
| Unramified | | | |
| $E' \simeq F(\sqrt[4]{\varepsilon})$ | $E \simeq F(\sqrt{\varepsilon})$ | Galois | $\mathbb{Z}/4\mathbb{Z}$ |
| Partially Ramified | | | |
| $E' \simeq F(\sqrt{\varepsilon}, \sqrt{\varpi})$ | $E \simeq F(\sqrt{\varepsilon}), F(\sqrt{\varpi}), F(\sqrt{\varepsilon\varpi})$ | Galois | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ |
| $E' \simeq F(\sqrt[4]{\varepsilon\varpi^2})$ | $E \simeq F(\sqrt{\varepsilon})$ | Galois | $\mathbb{Z}/4\mathbb{Z}$ |
| Totally Ramified | | | |
| $E' \simeq F(\sqrt[4]{\varpi})$ | $E \simeq F(\sqrt{\varpi})$ | Galois | $\mathbb{Z}/4\mathbb{Z}$ |
| $E' \simeq F(\sqrt[4]{\varepsilon\varpi})$ | $E \simeq F(\sqrt{\varepsilon\varpi})$ | Galois | $\mathbb{Z}/4\mathbb{Z}$ |
| $E' \simeq F(\sqrt[4]{\varepsilon^2\varpi})$ | $E \simeq F(\sqrt{\varpi})$ | Galois | $\mathbb{Z}/4\mathbb{Z}$ |
| $E' \simeq F(\sqrt[4]{\varepsilon^3\varpi})$ | $E \simeq F(\sqrt{\varepsilon\varpi})$ | Galois | $\mathbb{Z}/4\mathbb{Z}$ |

Table 2.1: Quartic Extensions of $F$ up to isomorphism when $-1 \in {F^\times}^2$

| **Ramification** | **Quadratic Subfield(s)** | **Type** | **Aut($E'/F$)** |
|---|---|---|---|
| Unramified | | | |
| $E' \simeq F(\sqrt{\varepsilon_E})$ | $E \simeq F(\sqrt{\varepsilon})$ | Galois | $\mathbb{Z}/4\mathbb{Z}$ |
| Partially Ramified | | | |
| $E' \simeq F(\sqrt{\varepsilon}, \sqrt{\varpi})$ | $E \simeq F(\sqrt{\varepsilon}), F(\sqrt{\varpi}), F(\sqrt{\varepsilon\varpi})$ | Galois | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ |
| $E' \simeq F(\sqrt{\varepsilon_E\varpi})$ | $E \simeq F(\sqrt{\varepsilon})$ | Galois | $\mathbb{Z}/4\mathbb{Z}$ |
| Totally Ramified | | | |
| $E' \simeq F(\sqrt[4]{\varpi})$ | $E \simeq F(\sqrt{\varpi})$ | Non-Galois | $\mathbb{Z}/2\mathbb{Z}$ |
| $E' \simeq F(\sqrt[4]{\varepsilon\varpi})$ | $E \simeq F(\sqrt{\varepsilon\varpi})$ | Non-Galois | $\mathbb{Z}/2\mathbb{Z}$ |

Table 2.2: Quartic Extensions of $F$ up to isomorphism when $-1 \notin {F^\times}^2$

## 2.5 Quadratic Forms

In order to understand the special orthogonal group of a quadratic form, we first explore some basic facts of (non-degenerate) quadratic spaces $(q, V)$, where $V$ denotes a finite-dimensional $F$-vector space.

It is well-known that all quadratic forms can be diagonalized $q \simeq \langle d_1, \ldots, d_n \rangle$ where the $d_n$ represent elements of $F^\times/{F^\times}^2$. Moreover, quadratic forms are in one-to-one

correspondence with symmetric bilinear forms, and we will often switch between the two for notational convenience.

**Definition 2.5.1.** *Suppose* $(q_1, V_1)$ *and* $(q_2, V_2)$ *are finite-dimensional quadratic spaces over* $F$*. Then,* $(q_1, V_1)$ *is* isometric *to* $(q_2, V_2)$ *if there exists a linear isomorphism* $\tau\colon V_1 \to V_2$ *such that*

$$q_2(\tau(v)) = q_1(v)$$

*for all* $v \in V_1$*. Isometry is denoted by* $(q_1, V_1) \simeq (q_2, V_2)$*, or equivalently* $q_1 \simeq q_2$*.*

Given an isometry of quadratic forms $q_1 \simeq q_2$, we have an *equivalence* of the corresponding bilinear forms $(\ ,\ )_1 \simeq (\ ,\ )_2$.

**Lemma 2.5.2.** *Let* $(\ ,\ )\colon V \times V \to F$ *be a non-degenerate symmetric bilinear form. If* $u, w \in V$ *are such that* $(w, v) = (u, v)$ *for all* $v \in V$*, then* $u = w$*.*

**Proof:** Suppose our form is given by $(\ ,\ )$ and that for all $v \in V$ we have that $(w, v) = (u, v)$ for some $u, w \in V$. Then, by bilinearity $(w - u, v) = 0$ for all $v \in V$ so $w - u = 0$ by non-degeneracy and $w = u$ as required. ∎

Recall that a quadratic form $q$ is *isotropic* if there exists a non-zero $v \in V$ such that $q(v) = 0$ (for example, the hyperbolic plane $\mathbb{H} = \langle 1, -1\rangle$ is isotropic); otherwise, $q$ is *anisotropic*. We will now explore some of the isometries of $\mathbb{H}$.

**Lemma 2.5.3.** *Let* $q(v_1, v_2) = \lambda v_1 v_2$ *be a form over* $V = F^2$ *for some fixed* $\lambda \in F^\times$*. Then* $q$ *is isometric to* $\mathbb{H}$*.*

**Proof:** We compute directly that $q(v_1 + v_2, \frac{v_1 - v_2}{\lambda}) = v_1^2 - v_2^2 = \mathbb{H}$. ∎

The following result shows that $\mathbb{H}$ is the only 2-dimensional form with determinant equal to $-1$, up to isometry.

**Lemma 2.5.4.** *Let* $(q, V)$ *be a non-degenerate 2-dimensional quadratic space. Then,* $q \simeq \mathbb{H}$ *if and only if* $\det(q) \equiv -1 \pmod{F^{\times 2}}$*.*

**Proof:** The forward direction is clear, so suppose $\det(q) \equiv -1 \pmod{F^{\times 2}}$ for some 2-dimensional non-degenerate form $q$. This implies that any diagonalization of $q$ has the form $q \simeq \langle \lambda a^2, -\lambda b^2\rangle$ for some $\lambda \in F^\times$. Thus, $q \simeq \mathbb{H}$ as required. ∎

T.Y. Lam in [Lam05, VI.§2] provides the complete classification of 2-dimensional quadratic forms over a non-archimedean local field $F$. Indeed, there are six 2-dimensional anisotropic forms up to isometry given by

$$\langle 1, -\varepsilon\rangle, \langle 1, \varpi\rangle, \langle 1, \varepsilon\varpi\rangle, \langle \varepsilon, \varpi\rangle, \langle \varepsilon, \varepsilon\varpi\rangle, \langle \varpi, -\varepsilon\varpi\rangle$$

and one 2-dimensional isotropic form $\mathbb{H} = \langle 1, -1\rangle$. This, in conjunction with the additional equivalences

$$\begin{aligned} \mathbb{H} \simeq \langle 1,1\rangle \simeq \langle \varepsilon,\varepsilon\rangle \simeq \langle \varpi,\varpi\rangle \simeq \langle \varepsilon\varpi,\varepsilon\varpi\rangle \ \text{ when } \ -1 \in {F^\times}^2 \\ \mathbb{H} \simeq \langle 1,\varepsilon\rangle \simeq \langle \varpi,\varepsilon\varpi\rangle \ \text{ and } \ \langle a,a\rangle \simeq \langle \varepsilon a,\varepsilon a\rangle \ \text{ when } \ -1 \notin {F^\times}^2 \end{aligned} \tag{2.5.1}$$

for all $a \in F^\times$ allows us to completely determine the 4-dimensional quadratic forms over $F$.

**Lemma 2.5.5.** *There are exactly eight 4-dimensional non-degenerate quadratic forms $q$ over $F$ up to isometry, given by*

*(a)* $q \simeq \langle 1, -\varepsilon, \varpi, -\varepsilon\varpi\rangle$, *which is anisotropic;*

*(b)* $q \simeq 2\mathbb{H}$, *which is totally isotropic;*

*(c)* $q \simeq p \perp \mathbb{H}$, *where* $p \in \{\langle 1,-\varepsilon\rangle, \langle 1,\varpi\rangle, \langle 1,\varepsilon\varpi\rangle, \langle \varepsilon,\varpi\rangle, \langle \varepsilon,\varepsilon\varpi\rangle, \langle \varpi,-\varepsilon\varpi\rangle\}$.

We will now concretely diagonalize a quadratic form which comes up frequently in §4.3, in order to determine its isometry class.

**Lemma 2.5.6.** *Let $\varepsilon = -1 \notin {F^\times}^2$ and define a quadratic form over $V = F^2$ by $p(v_1, v_2) := -v_1^2 x + 2v_1v_2y + v_2^2 x$, where $x, y \in F$ are such that $x^2 + y^2 \notin {F^\times}^2$. Then, $p \simeq \langle 1, 1\rangle$.*

**Proof:** The form $p$ has corresponding matrix

$$M_p = \begin{bmatrix} -x & y \\ y & x \end{bmatrix} \simeq \begin{bmatrix} -x & 0 \\ 0 & x + y^2/x \end{bmatrix}$$

so it diagonalizes as $p \simeq \langle -x, x + y^2/x\rangle$. Since $x^2 + y^2 \notin {F^\times}^2$, we can write $x^2 + y^2 = -a^2$ for some $a \in F^\times$. We will now condition on whether or not $x$ is a square.

If $x = -b^2 \notin {F^\times}^2$, then $x + y^2/x = (a/b)^2$ so we see that $p \simeq \langle 1, 1\rangle$. Conversely, if $x = b^2 \in {F^\times}^2$, then $x + y^2/x = -(a/b)^2$ so

$$p \simeq \langle -1, -1\rangle = \langle \varepsilon,\varepsilon\rangle \simeq \langle 1, 1\rangle$$

where the final isometry is as stated in (2.5.1). ∎

While diagonalizing the anisotropic portion of a quadratic form is always desirable, there are more convenient choices for the isotropic portion. Indeed, for each hyperbolic plane we instead want an orthogonal basis $\{e_i, f_i\}$, normalized so that

$$q(v_1e_i + v_2f_i) = 2v_1v_2$$

for all $v_1, v_2 \in F$. This discussion motivates the following definition.

**Definition 2.5.7.** *Let* $(\ ,\ )$ *be a non-degenerate symmetric bilinear form over* $V$*. Decompose the associated quadratic form as* $q = q_a \perp q_h$ *where* $q_a \coloneqq \langle a_1, \dots, a_k \rangle$ *denotes the form's anisotropic portion and* $q_h \coloneqq m\mathbb{H}$ *its hyperbolic portion. Then, the ordered set* $\mathcal{B}^* = \{g_1, \dots, g_k, e_1, f_1, \dots, e_m, f_m\}$ *is a* Witt basis of $V \simeq F^{k+2m}$ over $F$ with respect to the form $(\ ,\ )$ *if it satisfies:*

*(1)* $(g_i, g_j) = \delta_{ij} \cdot a_i$ *for all* $1 \leq i, j \leq k$*;*

*(2)* $(e_i, f_j) = \delta_{ij}$ *for all* $1 \leq i, j \leq m$*;*

*(3) All other combinations* $(e_i, e_j), (f_i, f_j), (g_\ell, e_j), (g_\ell, f_j)$ *are zero for all* $1 \leq \ell \leq k, 1 \leq i, j \leq m$*.*

These Witt bases will allow us to realize the tori in §4.4 and §4.5 in a consistent manner with respect to the "cleanest" version of the form.

### 2.5.1 Special Orthogonal Groups

We may now define the special orthogonal group of a quadratic form, given by the set of automorphisms of $V$ which preserve the form.

**Definition 2.5.8.** *Given an* $n$*-dimensional quadratic space* $(q, V)$*, we define the corresponding* special orthogonal group $SO(V)$ *by*

$$SO(V) \coloneqq \{A \in GL(V) \mid q(Av) = q(v)\ \forall\ v \in V \text{ and } \det(A) = 1\}.$$

When more convenient, we replace $V$ with the quadratic form $q$ itself, writing $SO(V) = SO(q)$.

**Example 2.5.9.** Consider the 2-dimensional non-degenerate quadratic form given by $\langle a_i, a_j \rangle$ for some $a_i, a_j \in F^\times$. By definition, a matrix $A$ is in $SO(\langle a_i, a_j \rangle)$ if and only if $\det(A) = 1$ and $(Av)^t J(Av) = v^t J v$ for all $v \in V$, where $J = \begin{bmatrix} a_i & 0 \\ 0 & a_j \end{bmatrix}$ denotes the matrix representation of $\langle a_i, a_j \rangle$. By conjugating by $v^t$, we see that the latter condition becomes $A^t J A = J$, or equivalently $JA = (A^t)^{-1} J$.

Let $A = \begin{bmatrix} w & x \\ y & z \end{bmatrix} \in M_2(F)$ be of determinant 1. Then $(A^t)^{-1} = \begin{bmatrix} z & -y \\ -x & w \end{bmatrix}$ and hence $A \in SO(\langle a_i, a_j \rangle)$ if and only if

$$\begin{bmatrix} a_i w & a_i x \\ a_j y & a_j z \end{bmatrix} = \begin{bmatrix} a_i z & -a_j y \\ -a_i x & a_j w \end{bmatrix}$$

which has solution $w = z, x = -y a_j / a_i$. Therefore, the special orthogonal group of $\langle a_i, a_j \rangle$ is given by

$$SO(\langle a_i, a_j \rangle) = \left\{ \begin{bmatrix} w & -y a_j / a_i \\ y & w \end{bmatrix} \;\middle|\; w, y \in F,\ \ w^2 + \frac{y^2 a_j}{a_i} = 1 \right\}.$$

**Lemma 2.5.10.** *Suppose $(q_1, V_1)$ and $(q_2, V_2)$ are $n$-dimensional isometric quadratic spaces over $F$. Then, $SO(V_1) \simeq SO(V_2)$.*

**Proof:** If $q_1 \simeq q_2$, then theres exists a linear isometry $\tau\colon V_1 \to V_2$ such that $q_2(\tau(v)) = q_1(v)$. Consider the map

$$\begin{aligned} \phi\colon SO(V_1) &\to GL(V_2) \\ A &\mapsto \tau A \tau^{-1}. \end{aligned}$$

We begin by noting that $\operatorname{Im}\phi \subseteq SO(V_2)$, since if $A \in SO(V_1)$ we have:

$$\begin{aligned} q_2(\tau A \tau^{-1}(v)) &= q_2(\tau(A\tau^{-1}v)) \\ &= q_1(A\tau^{-1}(v)) \\ &= q_1(\tau^{-1}(v)) \\ &= q_2(v) \end{aligned}$$

so $\tau A \tau^{-1} \in SO(V_2)$. By the same argument, conjugation by $\tau^{-1}$ maps $SO(V_2)$ to $SO(V_1)$, and these maps are mutual inverses. Therefore, the groups are isomorphic. ∎

Note, however, that the forms need not be isometric in order for the special orthogonal groups to be isomorphic. For example, if $q_2 = \lambda q_1$ for some $\lambda \in F^\times$, then it follows that $A \in SO(V_2)$ if and only if $\det(A) = 1$ and

$$q_2(Av) = q_2(v) \iff \lambda q_1(Av) = \lambda q_1(v) \iff q_1(Av) = q_1(v)$$

for all $v \in V$, hence $SO(V_1) = SO(V_2)$ are identical. We will now show that this is the only surprising equivalence.

**Example 2.5.11.** Consider two 2-dimensional non-degenerate forms $\langle a_i, a_j\rangle, \langle b_i, b_j\rangle$ and their corresponding special orthogonal groups. We claim that $SO(\langle a_i, a_j\rangle) = SO(\langle b_i, b_j\rangle)$ if and only if $\lambda\langle a_i, a_j\rangle = \langle b_i, b_j\rangle$ for some $\lambda \in F^\times$.

Suppose $SO(\langle a_i, a_j\rangle) = G = SO(\langle b_i, b_j\rangle)$, and let $J_1, J_1$ be the respective diagonal matrices corresponding to the forms $\langle a_i, a_j\rangle, \langle b_i, b_j\rangle$. Then, $A \in G$ if and only if $A^t J_i A = J_i$ or equivalently $A^t = J_i A^{-1} J_i^{-1}$. Thus, $A \in G$ if and only if

$$J_1 A^{-1} J_1^{-1} = J_2 A^{-1} J_2^{-1} = A^t$$

so $A J_1^{-1} J_2 = J_1^{-1} J_2 A$ for all $A \in G$. By construction, we have that

$$J_1^{-1} J_2 = \begin{bmatrix} a_i^{-1} b_i & 0 \\ 0 & a_j^{-1} b_j \end{bmatrix}$$

which commutes with all matrices $A \in G$ if and only if $a_i^{-1} b_i = a_j^{-1} b_j$. Set $\lambda = a_j^{-1} b_j$, which is in $F^\times$ by the non-degeneracy of our forms. Then, $J_1^{-1} J_2 = \lambda I_2$, and hence $J_2 = \lambda J_1$ as required.

The following lemma asserts that this condition actually holds for all groups $SO(V)$, of degrees larger than 2.

**Lemma 2.5.12.** *Let $(q_1, V)$ and $(q_2, V)$ be $n$-dimensional non-degenerate quadratic spaces over $F$. Then $SO(q_1)$ and $SO(q_2)$ are conjugate if and only if $q_1 \simeq \lambda q_2$ for some $\lambda \in F^\times$.*

**Proof:** We begin by noting that when determining if special orthogonal groups are conjugate by an element of $GL(V)$, it suffices (by replacing our form $q_1$ by an isometric form) to determine when they are equal.

We already proved the result for $n = 2$ in Example 2.5.11, so we will provide a sketch of the proof when $n > 2$.

Suppose $SO(q_1) = G = SO(q_2)$ and let $J_1, J_2$ be the respective diagonal matrices corresponding to the forms $q_1, q_2$. As per our proof in Example 2.5.11, we have that $AJ_1^{-1}J_2 = J_1^{-1}J_2A$ for all $A \in G$. This implies that $J_1^{-1}J_2$ lies in $C_{GL(V)}(G)$; the centralizer of $G$ in $GL(V)$. We will now prove that $C_{GL(V)}(G)$ is exactly the group of scalar matrices, which will allow us to conclude that $J_2 = \lambda J_1$ for some non-zero scalar $\lambda$, as required.

Without loss of generality, assume $J_1$ is diagonal with entries $a_i, 1 \leq i \leq n$. For each pair $a_i, a_j$, consider the corresponding 2-dimensional quadratic form $q_{ij} = \langle a_i, a_j \rangle$. By Example 2.5.9, its special orthogonal group is

$$SO(\langle a_i, a_j \rangle) = \left\{ \begin{bmatrix} w & -ya_j/a_i \\ y & w \end{bmatrix} \;\middle|\; w, y \in F, \;\; w^2 + \frac{y^2 a_j}{a_i} = 1 \right\}.$$

One can embed $SO(\langle a_i, a_j \rangle)$ in the submatrix defined by row $i$ and column $j$ of $G$, with 1s in the remaining diagonal entries; call this subgroup $H_{ij} \subset G$. The centralizer of $SO(\langle a_i, a_j \rangle)$ in $GL(F^2)$ is $\pm SO(\langle a_i, a_j \rangle)$, so it follows that the centralizer in $GL(V)$ of $H_{ij}$ is isomorphic to $\pm SO(\langle a_i, a_j \rangle) \times GL(F^{n-2})$. The intersection of all of these groups as $i, j$ run over all pairs of distinct indices between 1 and $n$ yields only scalar matrices, which completes the proof. ∎

This result yields the following conclusion.

**Corollary 2.5.13.** *There are 5 distinct classes of special orthogonal groups of 4-dimensional quadratic forms up to conjugacy, given by*

*(a)* $SO(\langle 1, -\varepsilon, \varpi, -\varepsilon\varpi \rangle)$;

*(b)* $SO(2\mathbb{H})$;

*(c)* $SO(\langle 1, \alpha \rangle \perp \mathbb{H})$, *where* $\alpha \in \{-\varepsilon, \varpi, \varepsilon\varpi\}$.

**Proof:** By Lemma 2.5.12 it suffices to determine which of the 4-dimensional forms in Lemma 2.5.5 are scalar multiples of one another. Since hyperbolic planes are preserved by scalar multiplication, the groups $SO(\langle 1, -\varepsilon, \varpi, -\varepsilon\varpi\rangle)$ and $SO(2\mathbb{H})$ are non-conjugate, and are also necessarily distinct from the special orthogonal groups of partially anisotropic forms.

The only 2-dimensional anisotropic forms which differ by a scalar are

$$\langle \varpi, -\varepsilon\varpi\rangle = \varpi\langle 1, -\varepsilon\rangle, \quad \langle \varepsilon, \varepsilon\varpi\rangle = \varepsilon\langle 1, \varpi\rangle, \quad \text{and} \quad \langle \varepsilon, \varpi\rangle \simeq \langle \varepsilon, \varepsilon^2\varpi\rangle = \varepsilon\langle 1, \varepsilon\varpi\rangle$$

whence the groups

$$\begin{aligned} SO(\langle 1, -\varepsilon\rangle \perp \mathbb{H}) &\simeq SO(\langle \varpi, -\varepsilon\varpi\rangle \perp \mathbb{H}) \\ SO(\langle 1, \varpi\rangle \perp \mathbb{H}) &\simeq SO(\langle \varepsilon, \varepsilon\varpi\rangle \perp \mathbb{H}) \\ SO(\langle 1, \varepsilon\varpi\rangle \perp \mathbb{H}) &\simeq SO(\langle \varepsilon, \varpi\rangle \perp \mathbb{H}) \end{aligned}$$

yield 3 different conjugacy classes and cover all partially anisotropic forms as required. ∎

Though this result demonstrates isomorphisms between the groups $SO(V)$, we will consider them separately (by the isometry class of the quadratic form) when classifying their tori.

### 2.5.2 Hermitian Forms

We now introduce a particular generalization of bilinear forms over quadratic field extensions $E$ of $F$, which will be discussed in more depth in the later chapters.

**Definition 2.5.14.** *Let $f : V \times V \to E$ be an $F$-bilinear form over $V$, where $E$ denotes a quadratic field extension of $F$ and $V$ is a vector space over $E$. Let $\sigma \in \mathrm{Gal}(E/F)$ be non-trivial. Then, $f$ is* $\sigma$-Hermitian *if it satisfies the following two properties for all $u, v, w \in V$ and $a, b \in E$:*

*(1)* $f(au + bv, w) = af(u, w) + bf(v, w)$.

*(2)* $f(v, w) = \sigma(f(w, v))$.

It follows from these properties that $f(v, au+bw) = \sigma(a)f(v, u)+\sigma(b)f(v, w)$, hence $f$ is $\sigma$-linear in the second coordinate. The next result allows us to completely determine 1-dimensional non-degenerate $\sigma$-Hermitian forms up to equivalence.

**Lemma 2.5.15.** *Let $E/F$ be a quadratic field extension and let $\sigma \in \mathrm{Gal}(E/F)$ be non-trivial. Then, $F^\times$ is in bijection with the set of non-degenerate, $\sigma$-Hermitian forms on $E$ via the map which sends each $\mu \in F^\times$ to the form $f(v, w) = \mu v\sigma(w)$ for all $v, w \in E$. Moreover, choices $\mu, \mu' \in F^\times$ yield equivalent forms if and only if they lie in the same coset mod $\mathrm{N}_{E/F}(E^\times)$.*

**Proof:** Let $\mu \in F^\times$. It is clear that the form $f(v,w) = \mu v\sigma(w)$ is non-degenerate since $\mu \neq 0$ and satisfies (1). Since $F$ is the fixed field of $\sigma$, it follows that $\sigma(\mu) = \mu$. Thus, $f$ satisfies (2) and defines a $\sigma$-Hermitian form on $E$. Conversely, given a non-degenerate $\sigma$-Hermitian form $f$ on $E$, set $\mu = f(1,1)$; since $f(1,1) = \sigma(f(1,1))$ we have $\mu \in F$; since $f$ is non-degenerate we have $\mu \neq 0$; and for any $v, w \in E$ we have $f(v,w) = v\sigma(w)f(1,1) = \mu v\sigma(w)$.
Suppose $\mu, \mu'$ lie in the same class mod $\mathrm{N}_{E/F}(E^\times)$, so we can write $\mu' = \mu a\sigma(a)$ for some $a \in E^\times$. If $f, f'$ are the corresponding forms, we compute that

$$f(av, aw) = \mu(av)\sigma(aw) = \mu' v\sigma(w) = f'(v,w)$$

for all $v, w \in E$. Since multiplication by $a$ is an $E$-linear transformation, we see that $f, f'$ are equivalent. Conversely, if $f$ and $f'$ are equivalent forms on $E$, then they are related by a change of basis, which implies that $f(1,1) = f'(a,a) = a\sigma(a)f'(1,1)$, as required. ∎

By Propostion 2.4.4, there are always two choices of $\mu$ up to equivalence for every quadratic extension $E/F$, and hence two inequivalent 1-dimensional $\sigma$-Hermitian forms over $E$.

**Example 2.5.16.** Let $E = F(\sqrt{\varepsilon})$ for a non-square $\varepsilon \in \mathcal{O}^\times$ and take $\varpi \in \mathcal{P}$ to be a uniformizer. By Propostion 2.4.4, $F^\times / \mathrm{N}_{E/F}(E^\times) = \{1, \varpi\}$, thus the two $\sigma$-Hermitian forms on $E$ up to equivalence are given by

$$f(v,w) = v\sigma(w), \quad f'(v,w) = \varpi v\sigma(w)$$

for all $v, w \in V$, where $\sigma \in \mathrm{Gal}(E/F)$ is defined by the relation $\sigma\colon \sqrt{\varepsilon} \mapsto -\sqrt{\varepsilon}$.

We study $\sigma$-Hermitian forms in a more general context in the following chapter; rather than working over a quadratic extension $E$, we will be working over a sum of finite, separable field extensions $E_i$ of $F$.

# Chapter 3

# Elliptic Tori in Orthogonal Groups

The focus of this chapter is the establishment of the bijection constructed by Morris in [Mor91, §1], which relates the conjugacy classes of maximal elliptic tori in an $n$-dimensional classical group $G$ to the isomorphism classes of maximal commutative, semisimple subalgebras of $\mathrm{End}(V)$.

We begin with a general introduction to tori, including both key results from the literature and motivating examples. By then proving theorems regarding finite-dimensional algebras and their modules, we establish the foundation of knowledge required to understand the abstract theory from Morris when specialized to the orthogonal case.

## 3.1 Toral Subgroups

Let $F$ be a non-archimedean local field and let $G = \mathbb{G}(F)$ be the $F$-points of an algebraic group defined over $F$. In particular, we identify $\mathbb{G} = \mathbb{G}(\overline{F})$ with its group of $\overline{F}$-points, where $\overline{F}$ denotes a fixed separable closure of $F$. We begin this section with the following important definition from [Mar91, Chapter I].

**Definition 3.1.1.** *A subgroup $\mathbb{T}$ of $\mathbb{G}$ is an* algebraic torus *if it is isomorphic to $(\overline{F}^{\times})^n$ for some $n \in \mathbb{Z}_{>0}$.*

This is equivalent to saying $\mathbb{T}$ is isomorphic to a diagonal matrix group of size $n$ over $\overline{F}$. Throughout the thesis, by *torus* we mean $T = \mathbb{T}(F)$, the $F$-points of an algebraic torus defined over $F$. Given a torus $T$ of $G$, it is not necessarily true that $T$ is isomorphic to $(F^{\times})^n$ for some $n \in \mathbb{Z}_{>0}$, hence we have the following notions:

**Definition 3.1.2.** *Let $T$ be a torus of $G$.*

*(a) The torus $T$ is* split *over $F$ if $T \simeq (F^{\times})^n$ for some $n \in \mathbb{Z}_{>0}$.*

*(b) The torus $T$ is* elliptic *over $F$ if all split subtori of $T$ lie in the center $Z(G)$ of $G$.*

**Remark 3.1.3.** In other literature, the words *minisotropic* or *compact modulo center* may be used to describe an elliptic torus.

The goal of this thesis is to classify all maximal, elliptic tori of the degree 4 special orthogonal groups. Since these groups have a finite center, our elliptic tori will all be compact, or equivalently anisotropic. We will now work through a few explicit examples of tori prior to moving on to more theory.

**Example 3.1.4.** Let $E/F$ be a separable field extension of degree $n > 1$ and consider $V \simeq E$ as a vector space over $F$. We will show that the multiplicative group $E^\times$ is a torus. Since $E^\times$ acts on itself via $F$-linear multiplication, we have that $E^\times \subset \mathrm{Aut}(E/F) \simeq GL(V)$. We can define $\mathbb{T}$ to be such that $\mathbb{T}(F) \coloneqq E^\times$ by regarding it as the set of $n \times n$ matrices whose entries are polynomial over $F$, given by expressing an element of $E^\times$ in terms of multiplication by a fixed basis of $E/F$.

For example, suppose $E = F(\sqrt{\alpha})$ is a quadratic field extension. We embed $E^\times \subset GL(V)$ as the algebraic group

$$E^\times = \left\{ \begin{bmatrix} a & b\alpha \\ b & a \end{bmatrix} \middle| a, b \in F, a^2 - b^2\alpha \neq 0 \right\}.$$

Then, for any field $F \subseteq K$, we define

$$\mathbb{T}(K) = \left\{ \begin{bmatrix} a & b\alpha \\ b & a \end{bmatrix} \middle| a, b \in K, a^2 - b^2\alpha \neq 0 \right\}.$$

We claim that $\mathbb{T}$ is an algebraic torus. By separability, the minimal polynomial $m(x)$ of any $a \in E^\times$ has distinct roots. The normal closure $\tilde{E}$ of $E/F$ contains all of these roots by definition, hence $a$ is diagonalizable in $\tilde{E}$. As we'll see in the proof of Lemma 3.1.10, the commutativity of $E^\times$ implies its elements can be simultaneously diagonalized over $\tilde{E}$. Thus, for any field $K$ containing $\tilde{E}$, we have that $\mathbb{T}(K) \simeq (K^\times)^n$, whence $\mathbb{T}$ is an algebraic torus.

No field can be written as a sum of fields, hence $E^\times \not\simeq (F^\times)^m$ for any $m$, so $E^\times$ is non-split. Furthermore, $E^\times$ contains exactly one non-trivial split subtorus, namely $F^\times$, which is embedded as scalar matrices in $GL(V)$. Since this lies in the center of $GL(V)$, $E^\times$ is elliptic.

**Example 3.1.5.** In an identical setting to that of the preceding example for any $n > 1$, consider the product $T' = E^\times \times E^\times$, embedded block diagonally in $GL(V)$ where $V \simeq F^{2n}$. This torus is again non-split and has a non-trivial split subtorus $F^\times \times F^\times$, however, this subtorus is not contained in the center of $GL(V)$. Therefore, $T'$ is a non-elliptic, non-split torus.

Prior to presenting our final example, we need the following imperative definition.

**Definition 3.1.6.** *Let $E'$ be an finite-dimensional, separable field extension of $F$ with subfield $F \subseteq E \subset E'$ such that $[E' : E] = 2$. Take $\sigma \in \mathrm{Gal}(E'/E)$ to be non-trivial. Then, the* group of norm 1 elements of $E'$ (with respect to $\sigma$)*, denoted by $E'^1$, is defined by*

$$E'^1 := \{u \in E' \mid u\sigma(u) = 1\}.$$

For all $u \in E'^1$, we remark that by Proposition 2.3.1 that $|u|_{E'} = \sqrt{|\mathrm{N}_{E'/E}(u)|_E} = 1$, thus $u \in \mathcal{O}_{E'}^\times$. By the proof of Proposition 2.3.4, every $u \in E'^1$ can be written as an $\mathcal{O}$-linear combination of the basis $\mathcal{C} = \{(\varpi_{E'})^j \alpha_i \mid 0 \leq j \leq e-1, 1 \leq i \leq m\}$ for $E'/F$, where the $\alpha_i \in \mathcal{O}_{E'}^\times$ are as defined in the proof.

**Lemma 3.1.7.** *Let $F \subseteq E \subset E'$ be a chain of finite separable extensions such that $[E' : E] = 2$. Then, the subgroup $E'^1$ of $E'^\times$ is an elliptic torus over $F$.*

**Proof:** Suppose we have a chain of finite separable extensions $F \subseteq E \subset E'$ such that $E'/E$ is quadratic. As seen in Definition 2.2.10, the norm map can be defined as a polynomial map over $F$ relative to the matrix form of the torus $\mathbb{T}(F) = E'^\times$ constructed in Example 3.1.4. Thus, the norm is an algebraic map so $E'^1 = \ker(\mathrm{N}_{E'/E})$ is again a torus; that is, we have identified a subgroup $\mathbb{S} \subset \mathbb{T}$ such that $\mathbb{S}(F) = E'^1$ [Bor91, III.8.5].
The intersection of $E'^1$ with the unique split subtorus of $E'^\times$ is $\{\pm 1\}$, so $E'^1$ contains no split subtori and is therefore always elliptic. ∎

We can illustrate this efficiently using a simple example.

**Example 3.1.8.** Let $E' = F(\sqrt{\alpha})$ for some $\alpha \in \{\varepsilon, \varpi, \varepsilon\varpi\}$, then since $\sigma(\sqrt{\alpha}) = -\sqrt{\alpha}$ we deduce

$$E'^1 = \left\{ \begin{bmatrix} a & b\alpha \\ b & a \end{bmatrix} \middle| a, b \in F, a^2 - b^2\alpha = 1 \right\}.$$

As per our discussion preceding this example, if $u = a + b\sqrt{\alpha} \in E'^1$ then $a, b \in \mathcal{O}$ since $\mathcal{C} = \{1, \sqrt{\alpha}\}$. Thus, the torus is given by the set

$$E'^1 = \left\{ \begin{bmatrix} a & b\alpha \\ b & a \end{bmatrix} \middle| a, b \in \mathcal{O}, a^2 - b^2\alpha = 1 \right\}$$

and hence $E'^1$ is indeed compact.

We now present the following definition from [Bor91, IV.12.2], allowing us to classify a set of elements which are crucial to our construction of tori in the following sections.

**Definition 3.1.9.** *An element $x \in G$ is* (strongly) regular *if its centralizer is a maximal torus.*

Similarly to before with our uniformizers, there are many choices for $x$, however we will fix one for our discussions. Moreover, since the dimension of a maximal torus is given by the rank of the group, this definition also tells us that $\dim(C_G(x)) = \text{rank}(G)$, where $C_G(x)$ denotes the centralizer of $x$ in $G$.

**Lemma 3.1.10.** *Suppose $x \in GL(V)$. Then, $x$ is regular if and only if it has distinct eigenvalues in some extension field of $F$.*

**Proof:** Begin by fixing a finite algebraic extension $E$ of $F$ over which $x$ is diagonalizable as an operator on $V^E := V \otimes_F E$ and set $G := GL(V)$. Suppose $x$ has $n$ distinct eigenvalues and $y \in C_G(x)$. Let $\lambda \in E$ be an eigenvalue of $x$ with corresponding eigenspace $V_\lambda \subseteq V^E$. Then, for $v \in V_\lambda$ :

$$x(yv) = y(xv) = y(\lambda v) = \lambda(yv)$$

so $yv \in V_\lambda$. By our initial assumption, $V_\lambda$ is 1-dimensional over $E$ so we must have $yv = \alpha v$ for some scalar $\alpha \in E$. Thus, $v$ is also an eigenvector of $y$ with eigenvalue $\alpha$. This implies that any basis of eigenvectors for $x$ is also a basis of eigenvectors for $y$, and that $x$ and $y$ are simultaneously diagonalizable with respect to this basis. Consequently, elements of $G$ are in $C_G(x)$ if and only if they are diagonalized by a basis of eigenvectors for $x$, so they form a torus and

$$\dim(C_G(x)) = n = \text{rank}(G)$$

which implies $x$ is regular. Now, suppose $x$ does not have distinct eigenvalues, so there exists at least one eigenspace $V_\lambda$ such that $\dim(V_\lambda) > 1$. Since $C_G(x)$ is the product of $GL(V_\lambda)$, this implies that $\dim(C_G(x)) > n$, so $x$ is not regular. ∎

This result tells us a lot about the regular elements of $GL(V)$, however even when $G \neq GL(V)$, regularity still is often equivalent to the distinctness of eigenvalues. There are a few exceptions in the orthogonal case, which we can write down explicitly as a consequence of Donna Testerman and A.E. Zalesski in [TZ15, Lemma 4.1].

**Lemma 3.1.11.** *Let $V$ be a finite-dimensional vector space over $F$, equipped with a non-degenerate symmetric bilinear form $(\ ,\ )$. Suppose $(\ ,\ )$ is preserved by special orthogonal group $G$ and $x \in G$ is a regular element. Then, we have the following:*

*(a) The set of eigenvalues of $x$ over some extension field $E$ of $F$ is given by $\{\lambda_1, \ldots, \lambda_k, \lambda_1^{-1}, \ldots, \lambda_k^{-1}\} \cup \{x_0\}$, where $x_0$ is absent if $\dim(V) = 2k$ and equal to 1 if $\dim(V) = 2k+1$, for some $k \in \mathbb{Z}_{>0}$.*

*(b) The $\lambda_i$ are distinct and $x$ is regular in $GL(V)$, apart from in the following exceptions:*

1. $\dim(V) = 2k+1$ *and* $-1$ *is an eigenvalue of* $x$ *with multiplicity* 2*;*
2. $\dim(V) = 2k$ *and either* 1 *or* $-1$ *or both are eigenvalues of* $x$ *with multiplicity* 2*.*

We note that $(a)$ implies that $\text{rank}(G) = k$. As per [Bor91, IV.12.3], the regular elements of a maximal torus form an open dense subset, hence we may choose for the following sections, without loss of generality, a regular $x \in G$ that does not fall into case 1. or 2., and therefore has distinct eigenvalues.

## 3.2 The Commuting Algebra

It is understood from the previous section that the maximal elliptic tori we are interested in will occur as $C_G(x)$ for certain regular $x$, however, classifying these tori is a relatively difficult process. We instead work with the commuting algebra of $x$ in $\text{End}(V)$ as per [Mor91], allowing us to use powerful tools from linear algebra and module theory.

Let $V$ denote an $n$-dimensional vector space over $F$, equipped with a (non-degenerate) symmetric bilinear form $(\ ,\ )$. We take $G = SO(V) \subset GL(V)$ to be the corresponding special orthogonal group and $x \in G$ a regular element explicitly selected (without loss of generality) to be regular in $GL(V)$, as per Lemma 3.1.11.

**Proposition 3.2.1.** *Given regular* $x \in G$ *and any* $y \in \text{End}(V)$*,* $x$ *and* $y$ *commute if and only if they are simultaneously diagonalizable over some extension field of* $F$*.*

**Proof:** We can apply the same reasoning as in the proof of Lemma 3.1.10 to $y \in \text{End}(V)$ (not necessarily in $G$), to conclude that if $x$ and $y$ commute, they must be simultaneously diagonalizable with respect to the same eigenbasis over some extension field $E$.

Suppose now that $x$ and $y$ are simultaneously diagonalizable over $E$ with respect to some basis $\mathcal{B} = \{v_1, \ldots, v_n\}$, such that $x$ has eigenvalues $\{\lambda_i\}_{i=1}^n$ and $y$ has eigenvalues $\{\beta_i\}_{i=1}^n$. Then,

$$x(yv_i) = x\beta_i v_i = \beta_i(xv_i) = \beta_i\lambda_i v_i = (\beta_i v_i)\lambda_i = y(v_i\lambda_i) = y(xv_i)$$

for all $i \in \{1, \ldots, n\}$, thus $xy$ and $yx$ agree on all vectors in $\mathcal{B}$ so we must have $xy = yx$. ∎

The latter part of the proof does not require the eigenvalues to be distinct; indeed if any two $y_1, y_2 \in \text{End}(V)$, not necessarily regular, are simultaneously diagonalizable over some $E/F$, then they must commute.

Let $x$ be a regular element of a maximal torus $T = C_G(x)$ in $G$. We define the corresponding commuting algebra of $x$ by $\mathscr{C}[x] = \{y \in \mathrm{End}(V) \mid xy = yx\}$, which by definition is such that $T = G \cap \mathscr{C}[x]$. By the proof of Proposition 3.2.1, $\mathscr{C}[x]$ is commutative; all its elements are simultaneously diagonalizable with $x$, and hence also with one another since $x$ has distinct eigenvalues. It is this same reasoning which allows us to conclude both the maximality of $\mathscr{C}[x]$ among all commutative subalgebras containing $x$ and that the commuting algebra $\mathscr{C}[T]$ of $T$ is equal to $\mathscr{C}[x]$. Thus, $\mathscr{C}[x]$ is independent of our choice of regular $x \in T$.

The following subsections work through all of the theory required to present the proof of the Weierstrass-Dedekind Theorem, ultimately letting us write $\mathscr{C}[x] = E_1 \oplus \cdots \oplus E_m$, where the $E_i$ denote finite, separable field extensions of $F$. This result is incredibly powerful and is the first step in classifying the tori in $G$.

### 3.2.1 Module Theory

For the remainder of the chapter, we let $M$ denote a (finite-length, unital, associative) module over an arbitrary, finite-dimensional $F$-algebra $A$, unless otherwise specified. The following results synthesized from [DK12, Chapter 1 & 2] will later be applied to further characterize the commuting algebra, taking $A = \mathscr{C}[x]$ and $M = V$.

**Definition 3.2.2.** *An $A$-module $M$ is* simple *if it is non-zero and has no non-trivial submodules. An $A$-module $M$ is* semisimple *if it is isomorphic to a direct sum of simple modules.*

**Example 3.2.3.** Every non-zero vector space $V$ is simple as an $\mathrm{End}(V)$-module. Indeed, we see this to be the case because every non-zero vector in $V$ generates the entire module under the action of $\mathrm{End}(V)$.

**Proposition 3.2.4.** *The following statements about an $A$-module $M$ are equivalent:*

1. *$M$ is semisimple;*
2. *$M$ is a direct sum of simple submodules;*
3. *Every submodule $N \subset M$ has a complement;*
4. *Every simple submodule $N \subset M$ has a complement.*

**Proof:** 1) $\Rightarrow$ 2) and 3) $\Rightarrow$ 4) are trivial.

2) $\Rightarrow$ 3): Let $N$ be a submodule $M$ and suppose $M$ is given as a sum of simple modules $M = \sum_{i=1}^{n} M_i$. By definition of $N$, $M = N + \sum_{i=1}^{n} M_i$. For every simple $M_j$, $j \in \{1, \ldots, n\}$, we must have that either $M_j \cap (N + \sum_{i=1}^{j-1} M_i) = 0$ or $M_j \subset (N + \sum_{i=1}^{j-1} M_i)$. If we omit those of the latter case, we create a set $\{N_k\} \coloneqq \{M_j \mid$

$M_j \cap (N + \sum_{i=1}^{j-1} M_i) = 0\}$ of simple submodules such that $N + \sum_k N_k = M$ and $N_k \cap (N + \sum_{\ell<k} N_\ell) = 0$. Thus, $M = N \oplus N'$ where $N' = \sum_k N_k$ is a complement of $N$.

4) $\Rightarrow$ 1): We will prove by induction on the length $\ell(M)$ of $M$, as defined in [HGK04, §3]. If $\ell(M) = 1$, $M$ is simple so therefore semisimple. Suppose $\ell(M) > 1$ and $U$ is a simple submodule of $M$. Then, $M = U \oplus U'$ where $U'$ is a complement of $U$ in $M$ and $\ell(U') = \ell(M) - 1$. If $N$ is a simple submodule of $U'$ and $N'$ denotes a complement of it in $M$, then every element $u \in U'$ is of the form $u = n + n'$, for some $n \in N, n' \in N'$. Thus, $n' = u - n \in N' \cap U'$. Therefore, $U' = N \oplus (N' \cap U')$, hence every simple submodule $N$ of $U'$ has a complement in $U'$. By induction, $U' \simeq \oplus_{i=2}^n M_i$ for simple submodules $M_i$, and so $M \simeq U \oplus \oplus_{i=2}^n M_i$ is semisimple as required. ∎

We now come to Schur's Lemma; a result that is fairly elementary to prove, however has many fundamental consequences in representation theory.

**Lemma 3.2.5** (Schur's Lemma)**.** *Given an algebra $A$, if $U$ and $V$ are simple $A$-modules, then every non-zero homomorphism $f\colon U \to V$ is an isomorphism.*

**Proof:** Let $f\colon U \to V$ be a non-zero homomorphism. By definition, $\emptyset \subsetneq \ker f \subseteq U$. Let $x, y \in \ker f$, then $f(x + y) = f(x) + f(y) = 0$ so $x + y \in \ker f$. Furthermore, for all $a \in A$ we have $f(ax) = af(x) = 0$ so $ax \in \ker f$. Thus, $\ker f$ is a submodule of $U$, and similarly one can show $\operatorname{Im} f$ is a submodule of $V$.

Since $f \neq 0$, we cannot have that $\ker f = U$ or $\operatorname{Im} f = 0$, hence by the simplicity of $U$ and $V$ we must have that $\ker f = 0, \operatorname{Im} f = V$ so $f$ is indeed an isomorphism. ∎

We now extend the notion of semisimplicity of $A$-modules to the algebra $A$ itself.

**Definition 3.2.6.** *A finite-dimensional algebra $A$ is* semisimple *if it is semisimple as an $A$-module.*

**Example 3.2.7.** Let $V_1, \ldots, V_n$ be finite-dimensional vector spaces over $F$ and take $A$ to be the product $\operatorname{End}_F(V_1) \times \cdots \times \operatorname{End}_F(V_n)$. The vector spaces $V_i$ are naturally $A$-modules; indeed, each $V_i$ is an $\operatorname{End}_F(V_i)$-module by definition, and thus also an $A$-module via the projection $\pi_i\colon A \to \operatorname{End}_F(V_i)$ which sends an element $a \in A$ to its multiplication map $a(v_i) \coloneqq a \cdot v_i$ for all $v_i \in V_i$. By Example 3.2.3, $V = \oplus V_i$ is a semisimple $A$-module.

Furthermore, each $\operatorname{End}_F(V_i)$ is semisimple since $\operatorname{End}_F(V_i) \simeq M_{n_i}(F)$, where $n_i$ denotes the dimension of $V_i$ over $F$, and we can write $M_{n_i}(F) = \oplus_{j=1}^{n_i} C_j$ where $C_j \simeq V_j$ is the simple submodule of $M_{n_i}(F)$ consisting of those matrices whose entries outside the $j$th column are zero. The algebra $A$ being the direct sum of these as an $A$-module allows us to conclude that $A$ is also semisimple.

Without loss of generality, we will view $A$ as a left $A$-module with respect to the usual multiplication map on $A$. Left ideals of $A$ correspond naturally to submodules of the

$A$-module. Further, minimal ideals of the algebra $A$, that is, non-zero ideals which contain no other non-zero ideals, correspond to simple submodules of the $A$-module.

### 3.2.2 Central Decompositions of the Identity

In order to understand algebra decompositions, we first study decompositions of the identity.

**Definition 3.2.8.** *An element $e$ of an algebra $A$ is an* idempotent *if $e^2 = e$.*

Two idempotents $e_1$ and $e_2$ which are such that $e_1e_2 = e_2e_1 = 0$ are called *orthogonal* and idempotents which belong to the center of the algebra are *central*. An equality $1 = e_1 + \cdots + e_m$, where $e_1, \ldots, e_m$ are pairwise orthogonal central idempotents, is called a *central decomposition of the identity* of an algebra $A$.

**Example 3.2.9.** Let $A$ be as in Example 3.2.7; let $e_i \in A$ be the element such that $\pi_i(e_i) = \mathrm{id}_{V_i}$ and $\pi_j(e_i) = 0$ for all $j \neq i$. Then $1 = e_1 + \cdots + e_n$ is a central decomposition of the identity of A.

**Example 3.2.10.** Let $A$ be a field; the unique idempotent is the multiplicative identity.

Recall that a two-sided ideal $I$ of $A$ is *nilpotent* if there exists some $n > 0$ such that $I^n = 0$. The following two results offer equivalent characterizations for the semisimplicity of an algebra and illustrate the practical role of idempotents in this theory.

**Lemma 3.2.11.** *If an algebra $A$ has no non-zero nilpotent two-sided ideals, then $A$ is semisimple.*

**Proof:** Suppose $A$ has no non-zero nilpotent two-sided ideals, and let $I$ be a minimal two-sided ideal of $A$. Then, $I^2 \neq 0$ so there exist $x, y \in I$ such that $xy \neq 0$. Thus, the map $f_x \colon I \to I$ given by $f_x(y) = xy$ is a non-zero homomorphism. By Schur's Lemma 3.2.5, $f_x$ is an isomorphism since $I$ is a simple module, hence we can set $e = f_x^{-1}(x) \in I$ so $x = xe$. Then $f_x(e) = xe = (xe)e = f_x(e^2)$ so $e = e^2$ and we conclude that $e$ is an idempotent. Since $e$ is non-zero and $eA \neq 0$ is a submodule of $I$, we have that $eA = I$.

Note that $eA \cap (1-e)A = \{0\}$. Indeed, suppose $a \in eA \cap (1-e)A$, so $a = ea_1 = (1-e)a_2$ for some $a_1, a_2 \in A$. This means

$$a = ea_1 = e^2a_1 = e(1-e)a_2 = (e-e^2)a_2 = (e-e)a_2 = 0.$$

Further, every $a \in A$ can be written as $a = ea + (1-e)a \in eA + (1-e)A$. Therefore, for every simple submodule $I$ of $A$, there exists a complement $I' = (1-e)A$ of $I$ such

that $A = I \oplus I'$. The result follows by Proposition 3.2.4. ∎

An $A$-module $M$ is *faithful* if for every non-zero $a \in A$, there exists some $m \in M$ such that the product $a \cdot m \neq 0$.

**Lemma 3.2.12.** *Given an algebra $A$, if there exists a faithful semisimple $A$-module, then $A$ is semisimple.*

**Proof:** Suppose $M = \oplus_{i=1}^{m} M_i$ is the decomposition of a faithful semisimple $A$-module into simple submodules $M_i$ and that $I$ is a non-zero ideal of $A$. Then $I \cdot M_i \neq 0$ for some $i$ since $M$ is faithful. But then since $M_i$ is simple we must have $I \cdot M_i = M_i$ and hence $I^k \cdot M_i = M_i$. Therefore $I^k \neq 0$ for all values of $k$, so by the previous Lemma 3.2.11, $A$ is semisimple. ∎

We now can develop a correspondence between idempotents of $\mathrm{End}_A(M)$ and decompositions of $M$.

**Lemma 3.2.13.** *There is a bijection between the decompositions of an $A$-module $M$ into a direct sum of submodules and the decompositions of the identity of* $\mathrm{End}_A(M)$.

**Proof:** Suppose $M = M_1 \oplus \cdots \oplus M_s$ is a direct sum decomposition of $M$ into submodules. This implies we can write every $m \in M$ uniquely as $m = \sum_{i=1}^{s} m_i$ for $m_i \in M_i$. Define a map $e_i \colon M \to M$ by $e_i(m) \coloneqq m_i$. The uniqueness of the sum implies that $e_i \in \mathrm{End}_A(M)$ and $m = e_1(m) + \cdots + e_s(m)$ so $\sum_{i=1}^{s} e_i = 1$. By definition, $e_i e_j(m) = e_i(m_j) = 0$ for all $i \neq j$, so the $e_i$ are pairwise orthogonal and also idempotents since $e_i^2(m) = e_i(m_i) = m_i = e_i(m)$. Thus, $\sum_{i=1}^{s} e_i$ is indeed a decomposition of the identity of $\mathrm{End}_A(M)$.

Now, suppose $\sum_{i=1}^{s} e_i = 1$ is a decomposition of the identity of $\mathrm{End}_A(M)$ and write $M_i \coloneqq \mathrm{Im}(e_i)$. Then, for all $m \in M : m = (e_1 + \cdots + e_s)m = e_1(m) + \cdots + e_s(m)$ where $e_i(m) \in M_i$. If $m = \sum_{i=1}^{s} m_s$ is some other decomposition of $m$ in the form of elements $m_i \in M_i$, then $m_i = e_i(x_i)$ for some $x_i \in M$. We then have the following:

$$e_i(m) = e_i(m_1) + \cdots + e_i(m_s) = e_i e_1(x_1) + \cdots + e_i e_s(x_s) = e_i(x_i) = m_i$$

by the orthogonality and idempotency of the $e_i$. Hence the sum $m = \sum_{i=1}^{s} m_s$ is unique so $M = M_1 \oplus \cdots \oplus M_s$ as required. ∎

**Lemma 3.2.14.** *Suppose $M = M_1 \oplus \cdots \oplus M_s$ is a direct sum decomposition of the $A$-module $M$ and $\sum_{i=1}^{s} e_i = 1$ is the corresponding decomposition of the identity of* $\mathrm{End}_A(M)$ *given by the bijection in Lemma 3.2.13. Then,*

$$e_i \mathrm{End}_A(M) e_j \simeq \mathrm{Hom}_A(M_j, M_i).$$

**Proof:** Let $f \in \mathrm{End}_A(M)$. For each $i, j \in \{1, \ldots, s\}$, consider the composition $e_i f e_j$ : we will show that $e_i f e_j$ defines an $A$-homomorphism from $M_j$ to $M_i$. First, let $m = \sum_{i=1}^{s} m_i \in M$ for $m_i \coloneqq e_i(m)$. We compute that $e_i f e_j(m) = e_i f m_j \in M_i$ and $e_i f e_j(m) = e_i f e_j^2(m) = e_i f e_j m_j$, therefore $e_i f e_j m$ is determined uniquely by the component $m_j$, so $e_i f e_j$ can be interpreted as a homomorphism from $M_j$ to $M_i$.
Conversely, let $g \in \mathrm{Hom}_A(M_j, M_i)$ and define the following map:

$$\begin{aligned} \tilde{g} : M &\to M \\ m &\mapsto e_i g(m_j) = e_i g e_j(m) \in M_i. \end{aligned}$$

So $\tilde{g}$ is in $\mathrm{End}_A(M)$ and in fact $\tilde{g} = e_i \tilde{g} e_j$ so $\tilde{g} \in e_i \mathrm{End}_A(M) e_j$ as required, which completes the isomorphism identifying $e_i \mathrm{End}_A(M) e_j$ with $\mathrm{Hom}_A(M_j, M_i)$. ∎

The following result is the last key piece required to prove the Weierstrass-Dedekind Theorem.

**Proposition 3.2.15.** *There is a bijective correspondence between:*

1. *Decompositions of $A$ into a direct product of algebras;*
2. *Central decompositions of the identity of $A$; and*
3. *Decompositions of $A$ into a direct sum of ideals.*

**Proof:** 1) $\Rightarrow$ 2) : Let $A = A_1 \times \cdots \times A_m$ be a decomposition of $A$ into a direct product of subalgebras $A_i$ and define $e_i$ to be the identity of the algebra $A_i$ in the $i^{th}$ position and zero elsewhere. By this definition, $\sum_{i=1}^{m} e_i$ is a decomposition of the identity of $A$. Further, let $a = (a_1, \cdots, a_m) \in A$. Then $e_i a = a_i = a e_i$ for all $i$, so the decomposition is indeed central.
2) $\Rightarrow$ 3) : Given a central decomposition of the identity $\sum_{i=1}^{m} e_i = 1$, we have $e_i A = e_i A e_i = A e_i$ and $e_i A e_j = e_i e_j A = 0$ for all $i \neq j$. Consequently, we can decompose $A$ as follows:

$$A = e_1 A + \cdots + e_m A = A e_1 + \cdots + A e_m.$$

Note that for all $i \neq j$ we have that $e_i A \cap e_j A = \{0\}$, so we obtain the direct sum $A = \oplus_{i=1}^{m} e_i A$.
Given a $z_i \in e_i A$, we write $z_i = e_i z$ for some $z \in A$. Then, for all $a \in A$: $a z_i = a \cdot e_i z = e_i \cdot az \in e_i A$, and similarly $z_i a \in e_i A$. Thus, the $e_i A$ are ideals of $A$ and we have successfully written $A$ as a direct sum of ideals.
3) $\Rightarrow$ 1) : Let $A = I_1 \oplus \cdots \oplus I_m$ where each of the $I_i$ are ideals, hence left submodules of $A$. By Lemma 3.2.13, there exists a corresponding decomposition of the identity; say $e_1 + \cdots + e_m = 1$, where $I_i = e_i A$. It follows that for all $i \neq j$, we have that

$e_iAe_j = 0$ and $e_iAe_i = e_iA = I_i$, so $I_i$ is an algebra with identity $e_i$ and hence we can write the following decomposition:

$$A = \oplus_{i,j=1}^{m} e_iAe_j \simeq A_1 \times \cdots \times A_m \text{ for } A_i = e_iAe_i = e_iA.$$

∎

### 3.2.3 The Weierstrass-Dedekind Theorem

We now will use the previous results from module theory to gain concrete insight on the properties of the commuting algebra $\mathscr{C}[x] = \{y \in \mathrm{End}(V) \mid xy = yx\}$.

**Theorem 3.2.16.** *If $x$ is a regular element of a maximal torus $T$ of $G$, then $\mathscr{C}[x]$ is a maximal commutative, semisimple algebra in* $\mathrm{End}(V)$ *of dimension equal to the dimension of $V$.*

**Proof:** We discussed the conditions verifying the maximality and commutativity of $\mathscr{C}[x]$ following the proof of Proposition 3.2.1. Further, the proof of Lemma 3.1.10 demonstrated that over some extension field $E$ of $F$, $V^E$ is a direct sum of 1-dimensional invariant subspaces. We now prove that $V$ itself is a direct sum of simple $\mathscr{C}[x]$-modules over $F$.

Since $x$ is diagonalizable over $\overline{F}$ with distinct eigenvalues, as an element of $\mathrm{End}(V)$ its minimal polynomial $m$ over $F$ coincides with its characteristic polynomial and has no repeated factors. Factor $m = \prod_{i=1}^{s} m_i$ into irreducible factors and for each $i$ let $V_i = \ker(m_i)$. As each $y \in \mathscr{C}[x]$ commutes also with $m_i$, we deduce that

$$V = \bigoplus_{i=1}^{s} V_i.$$

Since for any nonzero $v_i \in V_i$, the $F$-span of $\{v_i, xv_i, x^2v_i, \cdots\}$ is $V_i$, we see that each $V_i$ is simple as an $F[x]$-module, hence as an $\mathscr{C}[x]$-module. Thus, we have decomposed $V$ into a sum of simple $\mathscr{C}[x]$-submodules, so $V$ is semisimple. Since $V$ is faithful as an $\mathrm{End}(V)$ module, it is faithful as an $\mathscr{C}[x]$-module, so by Lemma 3.2.12, $\mathscr{C}[x]$ is a semisimple algebra.

In order to assert that $\dim_F \mathscr{C}[x] = n$, choose for each $i$ a non-zero element $v_i \in V_i$ and set $v_0 = \sum_{i=1}^{s} v_i$. Consider the homomorphism $\varphi\colon \mathscr{C}[x] \to V$ given by $y \mapsto yv_0$. The map is surjective, since every element of $V_i$ can be written as an $F$-linear combination of $x^kv_i$ for $k \geq 0$. Further, if $\varphi(y) = 0$, then each $yv_i = 0$. Since $y \in \mathscr{C}[x], xy = yx$ so we get that $yx^kv_i = 0$ for all $i, k$ and hence $y$ must be zero. Thus, $\varphi$ is injective and hence an isomorphism of left $\mathscr{C}[x]$-modules, whence $\dim(\mathscr{C}[x]) = \dim(V) = n$. ∎

We may now present the proof of the Weierstrass-Dedekind Theorem, which in conjunction with the previous theorem, will allow us to write $\mathscr{C}[x]$ as a sum of fields.

**Theorem 3.2.17** (Weierstrass-Dedekind)**.** *Every commutative, semisimple algebra is isomorphic to a direct product of fields. Conversely, every direct product of fields is a semisimple algebra.*

**Proof:** Let $A$ be a commutative, semisimple algebra and decompose it into a direct sum of modules $A = M_1 \oplus \cdots \oplus M_m$. Let $e_1 + \cdots + e_m = 1$ be the corresponding decomposition of the identity of $\mathrm{End}_A(A) = A$, as guaranteed by Lemma 3.2.13. The decomposition is central by the commutativity of $A$.

By the proof of Proposition 3.2.15, the $M_i$ are ideals of $A$ and we may write $A \simeq A_1 \times \cdots \times A_m$ where each $A_i \coloneqq e_i A$. Furthermore, Lemma 3.2.14 gives

$$e_i A = e_i A e_i \simeq \mathrm{Hom}_A(M_i, M_i) = \mathrm{End}_A(M_i).$$

Now, knowing that $A \simeq \mathrm{End}_A(M_1) \times \cdots \times \mathrm{End}_A(M_m)$, Schur's Lemma 3.2.5 implies every non-zero element of $\mathrm{End}_A(M_i)$ is an isomorphism, thus invertible. Since the $\mathrm{End}_A(M_i) \subset A$ are commutative, they are fields.

Conversely, suppose $A \simeq A_1 \times \cdots \times A_m$ where the $A_i$ are fields. Then, we can regard $A$ as a module and write $A = M_1 \oplus \cdots \oplus M_m$, where each of the $M_i$ is a simple $A_i$-module. By definition, $A$ is a semisimple algebra. ∎

**Corollary 3.2.18.** *The commuting algebra $\mathscr{C}[x]$ is a direct sum of finite separable field extensions of $F$.*

**Proof:** Combining the conclusions of Theorems 3.2.16 and 3.2.17, we see that $\mathscr{C}[x]$ is a direct product of fields. Since $\mathscr{C}[x]$ is finitely-generated, this direct product can be identified with a direct sum, hence $\mathscr{C}[x]$ is a direct sum of the fields $\mathrm{End}_A(M_i)$ for $i = 1, \ldots, m$. Since $\mathrm{End}_A(M_i)$ is an $F$-linear vector space, $F \subseteq \mathrm{End}_A(M_i)$ so $\mathrm{End}_A(M_i)$ is indeed a field extension of $F$. In fact, $\varphi(M_i) = V_i$ (so $s = m$) as per the notation of the proof of Theorem 3.2.16, and the fields are defined by the distinct factors of the characteristic polynomial of $x$, hence the extensions are separable. ∎

Therefore, we can write $\mathscr{C}[x] = E_1 \oplus \cdots \oplus E_m \simeq V$, where each $E_i$ is a finite, separable field extension of $F$.

## 3.3 Automorphisms of $\mathscr{C}[x]$

Recall, we set $G$ to be the group preserving a particular non-degenerate symmetric bilinear form $(\ ,\ )$ over $V$, where $\dim(V) = n$ for some $n > 2$. Concretely, this means

$G = \{g \in \mathrm{End}(V) \mid (gv, gw) = (v, w)\}$. By making a choice of basis, $G$ can be realized as a subgroup of $GL(V)$, with respect to which our form is given by $(v, w) = v^t Jw$ for some symmetric non-singular matrix $J$. Thus, all elements $g \in G$ necessarily satisfy $g^t Jg = J$ by definition.

**Lemma 3.3.1.** *There exists a unique map $\sigma\colon \mathrm{End}(V) \to \mathrm{End}(V)$ which satisfies the relation $(\phi(v), w) = (v, \sigma(\phi)w)$ for all $v, w \in V, \phi \in \mathrm{End}(V)$. Furthermore, $\sigma$ defines an $F$-linear anti-involution.*

**Proof:** Make a choice of basis as above, and define $\sigma$ as the map satisfying the above relation. We deduce that

$$(\phi(v))^t Jw = v^t J\sigma(\phi)w \iff \sigma(\phi) = J^{-1}\phi^t J \tag{3.3.1}$$

for all $v, w \in V, \phi \in \mathrm{End}(V)$, so $\sigma$ is indeed well-defined and unique. We will now show that $\sigma$ is an anti-homomorphism. By definition, $\sigma(1) = J^{-1}(I_n)^t J = I_n$ and for all $\lambda \in F, \phi \in \mathrm{End}(V)$ we have $\sigma(\lambda\phi) = J^{-1}\lambda\phi^t J = \lambda\sigma(\phi)$. Furthermore, for all $\phi_1, \phi_2 \in \mathrm{End}(V)$ we have that

$$\sigma(\phi_1 + \phi_2) = J^{-1}(\phi_1 + \phi_2)^t J = J^{-1}(\phi_1^t + \phi_2^t)J = \sigma(\phi_1) + \sigma(\phi_2)$$
$$\sigma(\phi_1\phi_2) = J^{-1}(\phi_1\phi_2)^t J = J^{-1}(\phi_2^t\phi_1^t)J = J^{-1}\phi_2^t(JJ^{-1})\phi_1^t J = \sigma(\phi_2)\sigma(\phi_1)$$

and thus $\sigma$ is indeed an anti-homomorphism. Finally, $(\phi(v), w) = (v, \sigma(\phi)(w)) = (\sigma(\phi)(w), v) = (w, \sigma^2(\phi)(v)) = (\sigma^2(\phi)(v), w)$ for all $v, w \in V, \phi \in \mathrm{End}(V)$ and so $\sigma$ has order 2 by Lemma 2.5.2, which completes the proof. ∎

We can now realize elements of our group $G$ via the map $\sigma$.

**Lemma 3.3.2.** *The group $G$ is given by the set $\{\phi \in \mathrm{End}(V) \mid \phi\sigma(\phi) = 1\}$.*

**Proof:** Let $g \in G$. Since $G$ preserves the form $(\ ,\ )$, for all $v, w \in V$ we have that $(v, w) = (gv, gw) = (v, \sigma(g)gw)$. Lemma 2.5.2 then implies that $\sigma(g)g = 1$, or equivalently $\sigma(g) = g^{-1}$ and $g\sigma(g) = 1$.

Conversely, suppose $\phi\sigma(\phi) = 1 = \sigma(\phi)\phi$ for some $\phi \in \mathrm{End}(V)$. Then, $(\phi(v), \phi(w)) = (v, \sigma(\phi)\phi(w)) = (v, 1 \cdot w) = (v, w)$ for all $v, w \in V$ so $\phi \in G$. ∎

Thus, given a regular element $x \in G$, the maximal torus $C_G(x) = \mathscr{C}[x] \cap G$ is given by the set $\{a \in \mathscr{C}[x] \mid a\sigma(a) = 1\}$. The following Proposition asserts that we can think of this torus as the set of norm 1 elements of $\mathscr{C}[x]$ with respect to the map $\sigma$.

**Proposition 3.3.3.** *The algebra $\mathscr{C}[x]$ is $\sigma$-invariant.*

**Proof:** Indeed, we compute that $\mathscr{C}[x] = \mathscr{C}[x^{-1}] = \mathscr{C}[\sigma(x)] = \sigma(\mathscr{C}[x])$. ∎

Though $\sigma$ is an anti-automorphism of $\mathrm{End}(V)$, moving forward we will often be focusing on its restriction to $\mathscr{C}[x]$, hence we will simply write $\sigma_{\mathscr{C}} := \sigma|_{\mathscr{C}[x]}$. The commutativity of $\mathscr{C}[x]$ and surjection of $\sigma_{\mathscr{C}}$ allows us to conclude that $\sigma$ restricts to an automorphism (and involution) of $\mathscr{C}[x]$.

The following results provide more specificity on how $\sigma_{\mathscr{C}}$ actually acts on $\mathscr{C}[x]$ or more precisely each component $E_i \subseteq \mathscr{C}[x]$. We first note that given a decomposition of the identity $1 = \sum_{i=1}^{m} e_i$ of $\mathscr{C}[x]$, each $e_i$ is an idempotent in the field $E_i$, and hence is the identity element in that field as per Example 3.2.10.

**Proposition 3.3.4.** *Suppose $\varphi$ is an $F$-linear automorphism of $\mathscr{C}[x] = E_1 \oplus \cdots \oplus E_m$. Then, $\varphi$ permutes the $E_i$.*

**Proof:** We proved that $E_i$ is an ideal of $\mathscr{C}[x]$ in Proposition 3.2.15 and will now show that $\varphi(E_i)$ is also an ideal. By definition of $\varphi$, $\varphi(E_i)$ is an $F$-linear subspace, so it remains to verify that for all $a \in \mathscr{C}[x], \alpha \in E_i$, we have $a\varphi(\alpha) \in \varphi(E_i)$.

Let $a \in \mathscr{C}[x], \alpha \in E_i$. Since $\varphi$ is surjective, we set $a' = \varphi^{-1}(a)$ for some $a' \in \mathscr{C}[x]$. Then, $a\varphi(\alpha) = \varphi(a')\varphi(\alpha) = \varphi(a'\alpha) \in \varphi(E_i)$ as required.

Consider now $e_k\varphi(E_i)$, where $e_k$ denotes the $k$th idempotent in the decomposition $\sum_{k=1}^{m} e_k = 1$. It must be non-zero for some value of $k$ since

$$0 \neq \varphi(E_i) = 1 \cdot \varphi(E_i) = (e_1 + \cdots + e_m)\varphi(E_i).$$

Moreover, $e_k\varphi(E_i) \subseteq E_k$ by definition of the $E_i$ and $\varphi(E_i)$ is an ideal so we also must have $e_k\varphi(E_i) \subseteq \varphi(E_i)$. Since $E_k$ and $\varphi(E_k)$ are simple ideals for all values of $k$, we have the equalities

$$E_k = e_k\varphi(E_i) = \varphi(E_i)$$

and hence $\varphi$ permutes the $E_i$. ∎

Therefore, for any given $m$-tuple $(a_1, \ldots, a_m) \in \mathscr{C}[x]$ such that $a_i \in E_i$, we can write $\sigma_{\mathscr{C}}(a_1, \ldots, a_m) = (\sigma_{\tau(1)}(a_{\tau(1)}), \ldots, \sigma_{\tau(m)}(a_{\tau(m)}))$ for some order 2 permutation $\tau \in S_m$ such that $\tau(j) = i$ if $\sigma(E_i) = E_j$ and $\sigma_{\tau(j)} \in \mathrm{Hom}_F(E_{\tau(j)}, E_j)$.

**Proposition 3.3.5.** *Suppose $C_G(x) = \mathscr{C}[x] \cap G$ is elliptic, so all its split subtori are contained in $Z(G)$. Then, $\sigma_{\mathscr{C}}$ preserves each $E_i$ and hence restricts to an $F$-linear automorphism of $E_i$, namely $\sigma_i$.*

**Proof:** Suppose for contradiction that $C_G(x)$ is elliptic and $\sigma_i(E_i) = E_j$ for some $i < j$. Since $\sigma_i$ is a field homomorphism, $\sigma_i(1) = 1$, so $\sigma_i$ maps the $i$th idempotent $e_i$ to the $j$th, $e_j$. We also note that the map acts as the identity on the base field. Indeed, for all $\lambda \in F$, $\sigma_i(\lambda e_i) = \lambda\sigma_i(e_i) = \lambda e_j$ by $F$-linearity.

Define a group $S = \{\sum_{k \neq i,j} e_k + \lambda e_i + \lambda^{-1} e_j \mid \lambda \in F^\times\}$. Then, for all $s \in S$

$$s\sigma(s) = (\sum_{k \neq i,j} e_k + \lambda e_i + \lambda^{-1} e_j)(\sum_{k \neq i,j} \sigma(e_k) + \sigma(\lambda e_i) + \sigma(\lambda^{-1} e_j)$$

$$
\begin{aligned}
&= (\sum_{k\neq i,j} e_k + \lambda e_i + \lambda^{-1} e_j)(\sum_{k\neq i,j} e_k + \lambda e_j + \lambda^{-1} e_i) \\
&= (\sum_{k\neq i,j} e_k^2 + (\lambda\lambda^{-1})e_i^2 + (\lambda^{-1}\lambda)e_j^2) \\
&= \sum_k e_k
\end{aligned}
$$

where the second last equality follows since $e_i e_j = 0$ for all $i \neq j$ and the last since $e_i^2 = e_i$. Thus, $s\sigma(s) = 1$ and $S \simeq F^\times$ so we conclude that $S$ is a split subtorus of $\mathscr{C}[x] \cap G$. Further, since $n > 2$ the center of $G$ is finite, and thus $S$ is non-central which yields a contradiction. ∎

Moving forward, we assume $C_G(x) = \mathscr{C}[x] \cap G$ is an elliptic torus in $G$, thereby yielding the following corollary.

**Corollary 3.3.6.** *If $\sigma_i$ is trivial, then $E_i = F$.*

**Proof:** Suppose, for some $i$, that $\sigma_i = \mathrm{id}$ and decompose the regular element as $x = \sum_{i=1}^m e_i x \in C_G(x)$, setting $e_i(x) \coloneqq x_i$. Since $x\sigma(x) = 1$,

$$1 = x_i(\sigma_i(x_i)) = x_i^2$$

so $x_i = \pm 1$ for all $i$ such that $\sigma_i = \mathrm{id}$. If $E_i/F$ is of degree $n_i$, then $E_i \simeq V_i$ where $V_i$ is an $n_i$-dimensional vector space over $F$. The idempotent $e_i$ acts by projection onto the subspace $V_i \subseteq V$, thus $e_i(x) = \pm \mathrm{id}_{V_i} = \pm I_{n_i \times n_i}$ and hence $x$ would have $n_i$ repeated eigenvalues. By our assumption that $x$ is regular in $GL(V)$ as per Lemma 3.1.11, we must have $n_i = 1$ and so $E_i = F$. ∎

The following result precisely refines the action of $\sigma$ on the field components $E_i$.

**Lemma 3.3.7.** *There is at most one index $i \in \{1, \ldots, m\}$ such that $\sigma_i = \mathrm{id}$.*

**Proof:** Suppose, for contradiction, that there exist two fields $E_i, E_j$ such that $\sigma_i = \sigma_j = \mathrm{id}$. Then, by the previous proof, $x$ must have eigenvalue $\lambda = \pm 1$ at positions $i$ and $j$. This is a contradiction by Lemma 3.1.11 and our assumption on $x$, which asserts that $x$ has $2k$ eigenvalues not equal to 1, where $\dim(V) = 2k$ or $2k+1$. ∎

We now have all of the ingredients required to state the following theorem from [Mor91, §1.3].

**Theorem 3.3.8.** *Let $C_G(x) = \mathscr{C}[x] \cap G$ be a maximal elliptic torus in $G$. We can write $\mathscr{C}[x] = E_1 \oplus \cdots \oplus E_m$ as a sum of finite, separable field extensions $E_i$ of $F$, where each $E_i$ is $\sigma$-invariant. Furthermore, if $\dim(V)$ is even, each of the $E_i$ are non-trivially stable by $\sigma$. If $\dim(V)$ is odd, then $\sigma_j = \mathrm{id}$ for exactly one $E_j = F$ and the rest of the $E_i$ are non-trivially $\sigma$-stable.*

The following examples provide further clarification of this result.

**Example 3.3.9.** Suppose $\mathscr{C}[x] \simeq F(\sqrt{\alpha})$ for a non-square $\alpha \in F^\times$. This extension is normal and thus the Galois group is $\mathrm{Gal}(\mathscr{C}[x]/F) \simeq \mathbb{Z}/2\mathbb{Z}$. The only non-trivial element of the group is given by the relation $\sigma\colon \sqrt{\alpha} \mapsto -\sqrt{\alpha}$ and

$$\begin{aligned} T &\coloneqq \{a + \sqrt{\alpha}b \in \mathscr{C}[x] \mid (a + \sqrt{\alpha}b)(a - \sqrt{\alpha}b) = 1\} \\ &= \{a + \sqrt{\alpha}b \in \mathscr{C}[x] \mid a^2 - b^2\alpha = 1\} \end{aligned}$$

defines a maximal torus in $G$, which by Lemma 3.1.7 $T \simeq E'^1$.

**Example 3.3.10.** Suppose now that $\mathscr{C}[x] \simeq E'$, where $E' = F(\sqrt[4]{\alpha})$ is a quartic extension of $F$ for some root $\sqrt[4]{\alpha}$ of the irreducible polynomial $x^4 - \alpha \in F[x]$. Recall from our computations in §2.4.2, the group $\mathrm{Aut}(E'/F)$ is isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}$, with the only order 2 element $\sigma$ defined by the relation $\sigma\colon \sqrt[4]{\alpha} \mapsto -\sqrt[4]{\alpha}$. Therefore, a maximal torus in $G$ is given by

$$T \coloneqq \{a \in \mathscr{C}[x] \mid a\sigma(a) = 1\} = \{a \in \mathscr{C}[x] \mid \mathrm{N}_{E'/E}(a) = 1\} \simeq E'^1$$

where $E$ denotes the unique quadratic subfield $F(\sqrt{\alpha}) \subset \mathscr{C}[x]$.

While Theorem 3.3.8 specifies the action of $\sigma$ on each field component $E_i$ of $\mathscr{C}[x]$, it has a few other notable consequences which are not explicitly outlined in [Mor91].

Begin by writing $x = \sum_{i=1}^m e_i(x)$ where $e_i(x) \coloneqq x_i \in E_i$. Let $E_i$ be degree $n_i \neq 1$ over $F$ and take $t$ to be an eigenvalue of $x_i$. Then, since $\sigma_i(x_i) = x_i^{-1}$, by Corollary 2.2.5 $t^{-1}$ is also an eigenvalue of $x_i$. Thus, each $E_i \not\simeq F$ gives $0.5n_i$ pairs of non-trivial eigenvalues, and hence each non-trivial extension $E_i$ is of even degree over $F$.

Moreover, we can consider the restriction of the form $(\ ,\ )$ to each of the $E_i$. Indeed, since $\sigma$ preserves the $E_i$ by Proposition 3.3.5, we have for every $v, w \in V$

$$(e_i(v), e_j(w)) = (v, \sigma(e_i)e_j(w)) = (v, e_ie_j(w)) = \begin{cases} 0 & i \neq j \\ (v, e_i(w)) & i = j \end{cases}$$

thus each $v \in E_i$ is orthogonal to $w \in E_j$ for $i \neq j$. By the non-degeneracy of $(\ ,\ )$, there must exist $b = \sum_{k=1}^m e_k(b) \in \mathscr{C}[x]$ such that $(e_i(a), \sum_{k=1}^m e_k(b)) \neq 0$. Then, by orthogonality $0 \neq (e_i(a), \sum_{k=1}^m e_k(b)) = (e_i(a), e_i(b))$ so there exists an $e_i(b) \in E_i$ such that $(e_i(a), e_i(b))$ is non-zero, hence $(\ ,\ )$ restricts to a non-degenerate $F$-bilinear form on each of the $E_i$.

We thus present the following consequence of Theorem 3.3.8.

**Corollary 3.3.11.** *Let $C_G(x) = \mathscr{C}[x] \cap G$ be a maximal elliptic torus in $G$ and write $\mathscr{C}[x] = E_1 \oplus \cdots \oplus E_m$. Then, the form $(\ ,\ )$ restricts to a non-degenerate $F$-bilinear form on each component $E_i$. Moreover, every $E_i \neq F$ is an even degree separable field extension of $F$ such that $\sigma$ restricts to a non-trivial automorphism $\sigma_i \in \mathrm{Gal}(E_i/K_i)$, where $K_i$ denotes a quadratic subfield of $E_i$. Thus, we identify $C_G(x) = T_1 \times \cdots \times T_m$ where $T_i \simeq E_i^1$ is the group of norm 1 elements of $E_i$ with respect to $\sigma$.*

## 3.4 Conjugacy Classes of Elliptic Tori

We now possess the theory required to construct Morris' bijection, allowing us to classify elliptic tori in $G$ up to conjugacy via maximal commutative, semisimple subalgebras of $\mathrm{End}(V)$.

Our first objective is to define a unique form $f$ on $V$ such that $(v,w) = \mathrm{Tr}_{\mathscr{C}[x]/F}(f(v,w))$ for all $v, w \in V$. Morris considers all sesquilinear forms $f$ and their similitudes, however we will be focusing on $\sigma$-Hermitian forms as discussed in §2.5.2, due to our primary interest being orthogonal groups. We require some setup prior to defining $f$ in order to make the jump from fields to algebras.

Let $A$ be a maximal commutative, semisimple subalgebra of $\mathrm{End}(V)$ equipped with a fixed involution $\sigma$. By Theorem 3.2.17, $A \simeq E_1 \oplus \cdots \oplus E_m$ for some finite, separable field extensions $E_i$ of $F$, with $V \simeq E_1 \oplus \cdots \oplus E_m$ as vector spaces over $F$. We assume $\sigma$ restricts to an automorphism $\sigma_i$ of each $E_i$ which acts non-trivially whenever $E_i \neq F$.

Beginning with an algebra $A$ as described, we can generalize Definition 2.5.14. The form $f\colon V \times V \to A$ over an $A$-module $V$ is *$\sigma$-Hermitian* if it is $F$-bilinear and $f(av, bw) = a\sigma(b)\sigma(f(w,v))$ for all $a, b \in A$, and $v, w \in V$.

**Lemma 3.4.1.** *Suppose there exists an $A$-form $f\colon V \times V \to A$ which satisfies the following properties:*

*(1) $(v,w) = \mathrm{Tr}_{A/F}(f(v,w))$ for all $v, w \in V$.*

*(2) $f$ is $A$-linear in the first component.*

*where $\mathrm{Tr}_{A/F}$ is given by $\sum_i \mathrm{Tr}_{E_i/F}$. Then, $f$ is non-degenerate and $\sigma$-Hermitian.*

**Proof:** The non-degeneracy of $f$ follows from the non-degeneracy of $(\ ,\ )$. In order to prove $f$ is $\sigma$-Hermitian, we first show that $f(v,w) = \sigma(f(w,v))$ for all $v, w \in V$. Define a non-degenerate, symmetric $F$-bilinear form $\langle\ ,\ \rangle\colon A \times A \to F$ by $\langle a, b\rangle := \mathrm{Tr}_{A/F}(ab)$. For all $a \in A, v, w \in V$

$$\langle a, f(v,w)\rangle = (av, w) = (v, \sigma(a)w)$$

by definition of $(\ ,\ )$ and $\sigma$ as per Lemma 3.3.1. The form $(\ ,\ )$ is symmetric, hence $(v, \sigma(a)w) = (\sigma(a)w, v)$ and we can further write

$$(\sigma(a)w, v) = \mathrm{Tr}_{A/F}(\sigma(a)f(w,v)) = \mathrm{Tr}_{A/F}(\sigma^2(a)\sigma(f(w,v))) = \mathrm{Tr}_{A/F}(a\sigma(f(w,v)))$$

where the second equality follows from Lemma 2.2.19 and the third since $\sigma$ is an involution. Thus, $\langle a, f(v,w)\rangle = \mathrm{Tr}_{A/F}(a\sigma(f(w,v))) = \langle a, \sigma(f(w,v))\rangle$, which by Lemma 2.5.2 implies $f(v,w) = \sigma(f(w,v))$.

Consequently, for any $a \in A$ and $v, w \in V$ we deduce

$$f(v, aw) = \sigma(f(aw, v)) = \sigma(af(w, v)) = \sigma(f(w, v))\sigma(a) = f(v, w)\sigma(a)$$

so $f$ is indeed $\sigma$-Hermitian. ∎

By definition, $V$ is a free $A$-module of rank 1. Indeed, given a generator $v_0 \in V$ we can write $V = \{av_0 \mid a \in A\}$. Without loss of generality, we set $v_0 \coloneqq \sum_{i=1}^{m} e_i = 1$. This allows us to write $f(v, w) = \mu v\sigma(w)$ for all $v, w \in V$ , where $\mu \coloneqq f(1, 1)$ as per Lemma 2.5.15. Thus, if we know how $f$ acts on $v_0$, we can determine how it acts on all vectors in $V$.

**Proposition 3.4.2.** *There exists a unique form $f$ which satisfies the conditions of Lemma 3.4.1.*

**Proof:** Let $\{a_1, \cdots, a_n\}$ be a basis for $A$ over $F$. It is simple to verify that the trace form is a non-degenerate symmetric $F$-bilinear form [Coh12], hence we can construct a dual basis $\{a_1^*, \cdots, a_n^*\}$ satisfying $\mathrm{Tr}_{A/F}(a_i^* a_j) = \delta_{ij}$.

If $f$ exists, then by identifying $V \simeq A$ by a choice of base point, it is given by $f(v, w) = \mu v\sigma(w)$ for some $\mu \neq 0$. Write $\mu = \sum_j c_j a_j$ for some unique $c_j \in F$. Then, conditions (1) and (2) of Lemma 3.4.1 imply that

$$(bv, w) = \mathrm{Tr}_{A/F}(\mu bv\sigma(w))$$

for all $b \in A$ and $v, w \in V$. In particular, if $b = a_i^*$, $v = w = 1$, we infer

$$(a_i^*, 1) = \mathrm{Tr}_{A/F} \sum_j c_j a_j a_i^* = \sum_j c_j \,\mathrm{Tr}_{A/F}(a_i^* a_j) = c_i.$$

Therefore, if $f$ exists, it is given by $\mu = \sum_j (a_j^*, 1)a_j$ with respect to any choice of basis $\{a_1, \cdots, a_n\}$ and thus is unique.

Now, by defining $\mu = \sum_{j=1}^{n} (a_j^*, 1)a_j$ as above, we will prove the existence of such an $f$. Given $v, w \in V$, set $f$ to be the form defined by $f(v, w) = \mu v\sigma(w)$. Since $v\sigma(w) \in A$, we can write it with respect to our secondary basis; $v\sigma(w) = \sum_{i=1}^{n} d_i a_i^*$ for some $d_i \in F$. We then write:

$$\mathrm{Tr}_{A/F}(f(v, w)) = \mathrm{Tr}_{A/F}(\sum_{i=1}^{n} d_i a_i^* \sum_{j=1}^{n} (a_j^*, 1)a_j) = \mathrm{Tr}_{A/F}(\sum_{i,j} d_i (a_j^*, 1)a_i^* a_j).$$

Since $d_i(a_j^*, 1) \in F$ for all $i, j$, this must equal $\sum_{i,j} d_i(a_j^*, 1)\,\mathrm{Tr}_{A/F}(a_i^* a_j)$ by the bilinearity of the trace. Thus, since $\mathrm{Tr}_{A/F}(a_i^* a_j) = \delta_{ij}$, we have that

$$\sum_{i,j} d_i(a_j^*, 1)\,\mathrm{Tr}_{A/F}(a_i^* a_j) = \sum_k d_k(a_k^*, 1) = (\sum_k d_k a_k^*, 1) = (v\sigma(w), 1)$$

and hence, by the properties of $(\ ,\ )$ and Lemma 3.3.1, we may conclude that $\mathrm{Tr}_{A/F}(f(v,w)) = (v\sigma(w),1) = (v,\sigma^2(w)) = (v,w)$ as required.
The form $f$ satisfies $A$-linearity in the first component by definition and hence all of the conditions of Lemma 3.4.1, which finishes the proof. ∎

We now have all of the pieces required to define the triples from [Mor91], whose equivalence classes will parameterize our tori.

**Definition 3.4.3.** *Let $V \simeq F^n$ denote an $F$-vector space equipped with a non-degenerate symmetric bilinear form $(\ ,\ )$ and $\sigma$ the anti-involution induced on $\mathrm{End}(V)$ as per Lemma 3.3.1. Take $G = SO(V)$ to be the corresponding special orthogonal group.*
*We define a set of triples $\mathscr{A}_G \coloneqq \{(A,\Phi,f_A)\}$ by the following criteria:*

*(1) An $F$-algebra $A$ and embedding $\Phi\colon A \hookrightarrow \mathrm{End}(V)$ whose image $\mathrm{Im}(\Phi)$ is a maximal commutative semisimple $F$-algebra in $\mathrm{End}(V)$;*

*(2) $\mathrm{Im}(\Phi)$ is given by a sum $E_1 \oplus \cdots \oplus E_m$ of finite separable field extensions which are all $\sigma$-stable and such that $\sigma$ acts trivially if and only if $E_i = F$ which occurs for at most one index $i$;*

*(3) A non-degenerate $\sigma$-Hermitian form $f_A\colon V \times V \to A$ which satisfies $(v,w) = \mathrm{Tr}_{A/F}(f_A(v,w))$, for all $v,w \in V$.*

In the work that follows, we identify $A$ with its image in $\mathrm{End}(V)$ and often suppress $\Phi$ from the notation; where it is helpful we will write $V_A$ to indicate $V$ when viewed as an $A$-module. When $x \in G = SO(V)$ is regular and $A = \mathscr{C}[x]$, $\Phi$ is given by the inclusion map. As per Theorem 3.3.8, $\mathscr{C}[x]$ is an algebra of the desired type, hence the above definition is satisfied with $f$ as in Lemma 3.4.1, so $(\mathscr{C}[x],\Phi,f) \in \mathscr{A}_G$.
Suppose $(A,\Phi,f_A)$ and $(A',\Phi',f_{A'})$ are two such triples. We say they are *equivalent* if there exists a pair of maps $\psi\colon A \to A'$ and $\widetilde{\psi}\colon V_A \to V_{A'}$ such that for all $a \in A$ and $v,w \in V$ we have

$$\widetilde{\psi}(\Phi(a)v) = \Phi'(\psi(a))\widetilde{\psi}(v) \tag{3.4.1}$$

$$f_{A'}(\widetilde{\psi}(v),\widetilde{\psi}(w)) = \psi(f_A(v,w)). \tag{3.4.2}$$

That is, the following diagrams commute:

$$\begin{array}{ccc} A & \xrightarrow{\Phi} & \mathrm{End}(V) \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\widetilde{\psi}\circ} \\ A' & \xrightarrow{\Phi'} & \mathrm{End}(V) \end{array} \qquad\qquad \begin{array}{ccc} V_A \times V_A & \xrightarrow{f_A} & A \\ {\scriptstyle\widetilde{\psi}\times\widetilde{\psi}}\downarrow & & \downarrow{\scriptstyle\psi} \\ V_{A'} \times V_{A'} & \xrightarrow{f_{A'}} & A' \end{array}$$

where the map from $\mathrm{End}(V) \to \mathrm{End}(V)$ sends $\phi \mapsto \widetilde{\psi} \circ \phi$ for all $\phi \in \mathrm{End}(V)$.

**Proposition 3.4.4.** *Suppose $(\psi, \widetilde{\psi})$ is an equivalence of two triples $(A, \Phi, f_A) \sim (A', \Phi', f_{A'}) \in \mathscr{A}_G$. Then, there exists $g \in G$ such that $\widetilde{\psi}(v) = gv$ and $\psi(a) = gag^{-1}$ for all $v \in V, a \in A$.*

**Proof:** Suppose $(\psi, \widetilde{\psi})$ is an equivalence and identify $A$ and $A'$ with their respective images in $\mathrm{End}(V)$. Since $\psi$ is an $F$-linear isomorphism, $\mathrm{Tr}_{A'/F}(\psi(a)) = \mathrm{Tr}_{A/F}(a)$ for all $a \in A$. Thus, by (3.4.2), we have that

$$\begin{aligned}(\widetilde{\psi}(v), \widetilde{\psi}(w)) &= \mathrm{Tr}_{A'/F}(f_{A'}(\widetilde{\psi}(v), \widetilde{\psi}(w))) = \mathrm{Tr}_{A'/F}(\psi(f_A(v, w))) \\ &= \mathrm{Tr}_{A/F}(f_A(v, w)) \\ &= (v, w)\end{aligned}$$

for all $v, w \in V$. Thus, $\widetilde{\psi} \in G$ and we can explicitly write $\widetilde{\psi} \colon V_A \to V_{A'}$ such that $\widetilde{\psi}(v) \coloneqq gv$ for some $g \in G$.

By (3.4.1), we have for all $a \in A$ and $v \in V$, $\widetilde{\psi}(av) = \psi(a)\widetilde{\psi}(v)$, which simplifies to $g(av) = \psi(a)(gv)$. Since $\widetilde{\psi}$ is an isomorphism, we can set $w \coloneqq gv \in V$, or equivalently $v = g^{-1}w$ which allows us to conclude $\psi(a)w = gag^{-1}w$, so $\psi$ acts by conjugation by $g$ as required. ∎

Let $(A, \Phi, f_A) \in \mathscr{A}_G$ and identify $A$ with its image in $\mathrm{End}(V)$ under the embedding $\Phi$. Set $T \coloneqq A \cap G = \{a \in A \mid a\sigma(a) = 1\}$. By construction of the triples, $T$ is a product of norm one elements (with respect to $\sigma$) of the field extensions $E_i$, and hence by Lemma 3.1.7, $T$ defines a maximal elliptic torus in $G$. With this step established, we now present the fundamental theorem from [Mor91, Theorem 1.6].

**Theorem 3.4.5.** *Let $\mathscr{A}_G$ denote the set of equivalence classes of triples $(A, \Phi, f_A)$ as defined previously, and let $\mathscr{T}_G$ denote the set of conjugacy classes of maximal elliptic tori in $G$. Then, the map*

$$\Theta \colon \begin{array}{c} \mathscr{A}_G \to \mathscr{T}_G \\ (A, \Phi, f_A) \mapsto A \cap G \end{array}$$

*induces an explicit bijection between these two sets.*

**Proof:** The forward direction is justified in the discussion preceding the statement. For the reverse, suppose we have a torus $T$ whose conjugacy class lies in $\mathscr{T}_G$. Let $A$ denote its commuting algebra, so $A = \mathscr{C}[T] = \mathscr{C}[x]$ for any regular $x \in T$. Our discussion following Definition 3.4.3 allows us to conclude that $A$ is an algebra of the type required and $V$ is an $A$-module equipped with a unique $\sigma$-Hermitian $A$-form $f_A$. Suppose $(\psi, \widetilde{\psi})$ is an equivalence of triples with corresponding tori $T, T'$. By Proposition 3.4.4, $\psi$ acts by conjugation by some $g \in G$, so $T' = \psi(T) = gTg^{-1}$ and thus $T, T'$ are indeed $G$-conjugate.

Finally, suppose two tori $T, T'$ with respective commuting algebras $A, A'$ lie in the same conjugacy class in $\mathscr{T}_G$, so $gTg^{-1} = T'$ for some $g \in G$. Then, we obtain a ring isomorphism $\psi\colon A \to A'$ given by conjugation by $g$, and a vector space isomorphism $\widetilde{\psi}\colon V \to V$ via the rule $\widetilde{\psi}(v) = gv$. It remains to prove that the maps $(\psi, \widetilde{\psi})$ satisfy (3.4.2). Indeed, by definition of $\psi$ we have

$$\mathrm{Tr}_{A'/F}(\psi(f_A(v,w))) = \mathrm{Tr}_{A'/F}(gf_A(v,w)g^{-1}) = \mathrm{Tr}_{A/F}(f_A(v,w)) = (v,w)$$

for all $v, w \in V$, where the last equality follows from the definition of $f_A$. On the other hand, we similarly compute for all $v, w \in V$ that

$$\mathrm{Tr}_{A'/F}(f_{A'}(\widetilde{\psi}(v), \widetilde{\psi}(w))) = \mathrm{Tr}_{A'/F}(f_{A'}(gv, gw)) = (gv, gw).$$

Since $g \in G$, we know that $(v,w) = (gv, gw)$ for all $v, w \in V$. With respect to the non-degenerate form $\langle a, b\rangle \coloneqq \mathrm{Tr}_{A'/F}(ab)$ defined in the proof of Lemma 3.4.1, we have

$$\langle \psi(f_A(v,w)), \psi(a)\rangle = \langle f_{A'}(\widetilde{\psi}(v), \widetilde{\psi}(w)), \psi(a)\rangle$$

for all $a \in A, v, w \in V$. Thus, by Lemma 2.5.2, $\psi(f_A(v,w)) = f_{A'}(\widetilde{\psi}(v), \widetilde{\psi}(w))$, which completes the proof. ∎

This bijection yields a concrete method to classify maximal elliptic tori up to conjugacy of an orthogonal group $G$ by first composing an exhaustive list of triples in $\mathscr{A}_G$. We apply this method explicitly to the degree 4 groups $G = SO(V)$ in the following chapter.

# Chapter 4

# Concrete Toral Embeddings into $SO(V)$

In this chapter, we classify the maximal elliptic toral subgroups up to conjugacy of $SO(V)$, where $V$ runs over the isometry classes of 4-dimensional quadratic forms. This work is a generalization of Kim and Yu in [KY11], who studied tori of the symplectic group.

Let $\mathscr{A}$ denote the union of sets $\mathscr{A}_G$ as described by Definition 3.4.3, where $G$ ranges over the groups $SO(V)$ for all the distinct isometry classes of 4-dimensional quadratic spaces $(q, V)$. We will begin by establishing an explicit list of equivalence classes of triples in $\mathscr{A}$, implementing an algorithm to generate, for each triple, a 4-dimensional (non-degenerate) symmetric bilinear form allowing us to determine which group $SO(V)$ the corresponding torus embeds into.

The final two sections focus on the development of a Witt basis (see Definition 2.5.7) for each torus, broken up by whether or not $-1$ is a square in $F$. We work through many interesting examples in order to streamline computation and aid in reader understanding. These examples also illustrate the immense value of the theory from Chapter 3 at the practical level.

The work of this chapter is performed over a non-archimedean local field $F$ of odd residual characteristic and vector space $V = F^4$. As in Chapter 2, we let $\varepsilon \in \mathcal{O}^\times$ denote a non-square and $\varpi \in \mathcal{P}$ a uniformizer, and use equivalent characterizations of $\varepsilon_E, \varpi_E$ for finite extensions $E$ of $F$.

## 4.1 Establishing Triples

Begin by defining a 4-dimensional, commutative, semisimple algebra $A$, which we recall from Theorem 3.2.17 is isomorphic to a direct sum of finite, separable field ex-

tensions $E_i$. We also fix an involution $\sigma\colon A \to A$, which restricts to an automorphism on each field component $E_i$ of $A$, acting non-trivially if and only if $E_i \neq F$. Recall from Corollary 3.3.11, every $E_i \neq F$ must be of even degree, hence $A$ is isomorphic to a quartic extension or a sum of quadratic extensions.

Fixing such a map $\sigma$ is equivalent to fixing a degree 2 subfield of each $E_i$ and taking $\sigma$ to map elements of this component to their non-trivial Galois conjugate with respect to the quadratic extension. When $A$ is quartic, denoted by $E'$, we thus take $\sigma \in \mathrm{Gal}(E'/E)$ to be non-trivial, where $E$ denotes a fixed quadratic subfield of $E'$. Alternatively, when $A$ is a sum of quadratics denoted by $E' = E_1 \oplus E_2$, we instead take $\sigma = (\sigma_1, \sigma_2)$ where $\sigma_i$ denotes the non-trivial element of $\mathrm{Gal}(E_i/F)$.

As used previously, left multiplication by $\alpha \in E'$ defines an $F$-endomorphism, so by a choice of identification $E' \simeq V$ we obtain an embedding $\Phi\colon E' \hookrightarrow \mathrm{End}(V)$.

Let $f\colon V \times V \to E'$ be a (non-degenerate) $\sigma$-Hermitian form. Since $V$ is one-dimensional over $E'$, by Lemma 2.5.15 $f$ is completely determined by a choice of $\sigma$-invariant element in $E'$, up to the equivalence as summarized below.

With these tools established, we now present the formal definition of a 4-dimensional triple $\xi := (E', \Phi, f) \in \mathscr{A}$, where $E', f$ are one of the following:

(1) A quartic field extension $E'$ of $F$ with fixed intermediate field $E$ and $\sigma$-Hermitian form $f(v, w) = \mu v \sigma(w)$ for a representative $\mu$ of $E^\times / \mathrm{N}_{E'/E}(E'^\times)$;

(2) A sum of quadratic extensions $E_1 \oplus E_2$ of $F$ with $\sigma$-Hermitian form $f = (f_1, f_2)$ such that $f_i(v_i, w_i) = \mu_i v_i \sigma_i(w_i)$ for representatives $\mu_i$ of $F^\times / \mathrm{N}_{E_i/F}(E_i^\times)$ with the additional equivalence relation $(\mu_1, \mu_2) \sim (\mu_2, \mu_1)$ imposed when $E_1 \simeq E_2$;

and $\Phi\colon E' \hookrightarrow \mathrm{End}(V)$ is an $F$-embedding of $E'$ into $\mathrm{End}(V)$. Each form $f$ gives rise to a non-degenerate quadratic form $q$; therefore $\xi$ is an element of $\mathscr{A}_G$, where $G = SO(q)$. We have yet to determine $q$ for our triples, so for the following results we work with all possible triples together in the set $\mathscr{A}$.

We now will discuss the equivalences $(\psi, \widetilde{\psi})$ of these triples to ensure our list of representatives in $\mathscr{A}$ is not only exhaustive but also non-repetitive.

Recall, an equivalence of two triples $(E'_A, \Phi, f), (E'_B, \Phi', f')$ is given by a ring isomorphism $\psi\colon E'_A \to E'_B$ and vector space isomorphism $\widetilde{\psi}\colon V \to V$, which together satisfy Equations 3.4.1 and 3.4.2. Indeed, if two triples contain non-isomorphic $F$-algebras $E'_A \not\simeq E'_B$, then they are necessarily inequivalent. The following proposition allows us to refine this condition even further.

**Proposition 4.1.1.** *Let $\xi = (E'_A, \Phi, f), \xi' = (E'_B, \Phi', f') \in \mathscr{A}$ be triples whose forms $f, f'$ correspond to choices $\mu, \mu'$ respectively. Then, $\xi \sim \xi'$ if and only if there exists an isomorphism $\psi\colon E'_A \to E'_B$ such that $(\mu')^{-1}\psi(\mu) \in \mathrm{N}_\sigma(E'^\times_B) = \{a\sigma(a) \mid a \in E'^\times_B\}$.*

**Proof:** Suppose $\xi \sim \xi'$, and hence $E'_A \simeq E'_B$ as $F$-algebras. They must either both be quartic or both sums of quadratic extensions; we consider these cases individually.

When both $E'_A, E'_B$ are quartic, we assume without loss of generality that $E'_A = E' = E'_B$, thus we have an algebra isomorphism $\psi \in \mathrm{Aut}(E'/F)$. Identify $E' \simeq F^4$ via an $F$-basis $\mathcal{B}$ and suppose $\widetilde{\psi}(1) = z \in F^4$. Note that the map $x \mapsto [x]_{\mathcal{B}}$ which sends elements $x$ of $E'$ to vectors in $F^4$ with respect to $\mathcal{B}$ is an isomorphism. Furthermore, for all $v \in E', a \in F^4$ we have $\widetilde{\psi}(av) = \psi(v)\widetilde{\psi}(a)$, and thus

$$\begin{aligned} \widetilde{\psi}\colon F^4 &\to F^4 \\ [v]_{\mathcal{B}} &\mapsto [z\psi(v)]_{\mathcal{B}}. \end{aligned}$$

Let $f(v,w) = \mu v\sigma(w)$ and $f'(v,w) = \mu' v\sigma(w)$ for all $v, w \in V$. The group $\mathrm{Aut}(E'/F)$ is abelian, so $\psi$ commutes with $\sigma$ and both sides of (3.4.2) become

$$f'(\widetilde{\psi}(v), \widetilde{\psi}(w)) = \mu' z\psi(v)\sigma(z\psi(w)) = \mu' z\sigma(z)\psi(v\sigma(w))$$

and

$$\psi(f(v,w)) = \psi(\mu v\sigma(w)) = \psi(\mu)\psi(v\sigma(w)).$$

For $(\psi, \widetilde{\psi})$ to be an equivalence, these expressions must be equal for all $v, w \in V$. This is true if and only if $\mu' z\sigma(z) = \psi(\mu)$, or equivalently, if $\psi(\mu)$ and $\mu'$ lie in the same class mod $\mathrm{N}_\sigma(E'^{\times}_B) = N_{E'/E}(E'^{\times})$ as required.

Suppose now that $E'_A, E'_B$ are given by a sum of two quadratic extensions. As in the previous case, we may take $E'_A = E_1 \oplus E_2 = E'_B$, however, we have two cases for our map $\psi$. When $E_1 \not\simeq E_2$, the map $\psi\colon E_1 \oplus E_2 \to E_1 \oplus E_2$ restricts to a field isomorphism of each factor $E_i$ and the proof follows identically to the above. However, when $E_1 \simeq E \simeq E_2$, we can additionally define a map $\psi\colon (a,b) \mapsto (b,a)$ for all $(a,b) \in E \oplus E$, so $\psi$ swaps the two components.

Given $(v, \tilde{v}) \in E \oplus E \simeq V$, we have $\widetilde{\psi}(v, \tilde{v}) = (z_2\tilde{v}, z_1 v)$ for some fixed $z_1, z_2 \in E$. Let $u = (v, \tilde{v}), u' = (w, \tilde{w}) \in V$ and take $\mu = (\mu_1, \mu_2), \mu' = (\mu'_1, \mu'_2)$; thus $f(u,u') = (\mu_1 v\sigma(w), \mu_2 \tilde{v}\sigma(\tilde{w}))$ and $f'(u,u') = (\mu'_1 v\sigma(w), \mu'_2 \tilde{v}\sigma(\tilde{w}))$.

Then, both sides of (3.4.2) become:

$$f'(\widetilde{\psi}(u), \widetilde{\psi}(u')) = f'((z_2\tilde{v}, z_1 v), (z_2\tilde{w}, z_1 w)) = (\mu'_1 z_2\sigma(z_2)\tilde{v}\sigma(\tilde{w}), \mu'_2 z_1\sigma(z_1)v\sigma(w))$$

and

$$\psi(f(u,u')) = \psi(\mu_1 v\sigma(w), \mu_2 \tilde{v}\sigma(\tilde{w})) = (\mu_2 \tilde{v}\sigma(\tilde{w}), \mu_1 v\sigma(w)).$$

As before, these are equal for all $u, u' \in E \oplus E$ if and only if $\mu'_1 z_2\sigma(z_2) = \mu_2$ and $\mu'_2 z_1\sigma(z_1) = \mu_1$, or equivalently if and only if $(\mu')^{-1}\psi(\mu) \in \mathrm{N}_\sigma((E \oplus E)^{\times})$, hence completing the proof. ∎

When $E'$ is quartic, Proposition 2.4.4 demonstrates that there are precisely two classes

of $E^\times/\mathrm{N}_\sigma(E'^\times) = E^\times/\mathrm{N}_{E'/E}(E'^\times)$, so since $\psi$ preserves $\mathrm{N}_\sigma(E'^\times) \subset E^\times$ we deduce that $\psi$ preserves the class of $\mu$. Thus, we have an even stronger statement; if we assume equality of our quartic extensions $E'_A = E' = E'_B$ then in fact the two triples are equivalent if and only if $(\mu')^{-1}\mu \in \mathrm{N}_\sigma(E'^\times)$.

Similarly, if we assume equality in the sum of quadratics $E_1 = E'_1$ and $E_2 = E'_2$, then the two triples are equivalent if and only if $(\mu'_1)^{-1}\mu_1 \in \mathrm{N}_\sigma(E_1^\times)$ and $(\mu'_2)^{-1}\mu_2 \in \mathrm{N}_\sigma(E_2^\times)$ or $E_1 = E_2$ and $(\mu_1, \mu_2) \sim (\mu'_2, \mu'_1)$.

This result is the key to concretely listing inequivalent representatives for each class in $\mathscr{A}$, which by Theorem 3.4.5 yields the maximal elliptic tori of *all* possible degree 4 special orthogonal groups. We thereby conclude this section with our first major result.

**Theorem 4.1.2.** *Let $\mathscr{T}$ denote the set of conjugacy classes of maximal elliptic tori in the union of groups $G = SO(V)$, as $V$ runs over the isometry classes of 4-dimensional quadratic forms. Then,*

$$|\mathscr{T}| = \begin{cases} 39 & \text{if } -1 \in F^{\times 2} \\ 35 & \text{if } -1 \notin F^{\times 2}. \end{cases}$$

**Proof:** By Theorem 3.4.5, it suffices to determine the size of $\mathscr{A}$. When $E'$ is quartic, we note that by Proposition 2.4.4 there are always two equivalence classes for $\mu$, and hence 2 non-conjugate tori arising from each distinct pairing $E \subset E'$, where $E'$ is quartic and $E$ quadratic. As per our classification in Tables 2.1 and 2.2, there are 9 isomorphism classes of $E \subset E'$ when $-1 \in F^{\times 2}$ and 7 when $-1 \notin F^{\times 2}$.

When $E' = E_1 \oplus E_2$, by §2.4.1, there are 3 choices for $E_i$ up to isomorphism, namely $F(\sqrt{\varepsilon}), F(\sqrt{\varpi}), F(\sqrt{\varepsilon\varpi})$. This implies that there are 6 unique (up to isomorphism) pairs $E_1 \oplus E_2$. When $E_1 \not\simeq E_2$, there are 4 distinct choices of $\mu$, however when $E_1 \simeq E_2$ there are only 3 because of the additional equivalence relation given by $(\mu_1, \mu_2) \sim (\mu_2, \mu_1)$.

Therefore, when $-1 \in F^{\times 2}$, we have $9 \times 2$ quartic tori and $(3 \times 4) + (3 \times 3)$ sum of quadratics tori, giving 39 total. When $-1 \notin F^{\times 2}$, there are 4 fewer due to the 2 fewer non-isomorphic quartic extensions $E'$. ∎

## 4.2 Generating Symmetric Forms

While knowing how many total tori there are is nice, in order to work with them explicitly we need to determine which group $SO(V)$ they are embedded into. By Lemma 2.5.5, there are exactly eight 4-dimensional quadratic spaces $(q, V)$ up to isometry, and hence eight distinct (non-equal) groups.

By inputting a triple into the following two algorithms, we will be able to determine which form $q$ it corresponds to, thereby establishing for each group $G = SO(V)$, the subset $\mathscr{A}_G \subset \mathscr{A}$ of triples whose equivalence classes are in bijective correspondence with the set of conjugacy classes of maximal elliptic tori in $G$.

As described by Corollary 2.5.13, some isomorphisms exist between special orthogonal groups of non-isometric quadratic forms. We will continue for the rest of the chapter to sort our tori by the corresponding quadratic space $(q, V)$, noting that tori of isomorphic groups $SO(V)$ are isomorphic to one another.

**Algorithm 1** Generating a Symmetric Bilinear Form from a Quartic Extension

1: Begin with a quartic field extension $E'$ of $F$ with fixed intermediate field $E$.
2: Choose an element $\mu \in E^\times$. Note $\mu \sim \mu'$ if and only if $(\mu')^{-1}\mu \in \mathrm{N}_{E'/E}(E'^\times)$.
3: Let $\sigma \in \mathrm{Gal}(E'/E)$ be non-trivial.
4: Define a form on $E'$ by $(v, w) \coloneqq \mathrm{Tr}_{E'/F}(\mu v \sigma(w))$ for all $v, w \in E'$.

We now develop a near-identical secondary algorithm for sums of quadratic extensions of $F$, given by $E' = E_1 \oplus E_2$.

**Algorithm 2** Generating a Symmetric Bilinear Form from Two Quadratic Extensions

1: Begin with a sum of quadratic field extensions of $F$ given by $E' = E_1 \oplus E_2$.
2: Choose an element $\mu \in F^\times \oplus F^\times$. Note $(\mu_1, \mu_2) \sim (\mu_1', \mu_2')$ if and only if $(\mu_i')^{-1}\mu_i \in F^\times / \mathrm{N}_{E_i/F}(E_i^\times)$ for $i = 1, 2$, or additionally when $E_1 \simeq E_2$, $(\mu_1, \mu_2) \sim (\mu_2, \mu_1)$.
3: Let $\sigma = (\sigma_1, \sigma_2) \in \mathrm{Aut}(E'/F)$ be such that $\sigma_i \in \mathrm{Gal}(E_i/F)$ is non-trivial.
4: Define a form on $E'$ by $((v, \tilde{v}), (w, \tilde{w})) \coloneqq \mathrm{Tr}_{E'/F}(\mu(v, \tilde{v})\sigma(w, \tilde{w}))$
$= \mu_1 \mathrm{Tr}_{E_1/F}(v\sigma_1(w)) + \mu_2 \mathrm{Tr}_{E_2/F}(\tilde{v}\sigma_2(\tilde{w}))$
for all $(v, \tilde{v}), (w, \tilde{w}) \in E'$.

To each form $(\ ,\ )$ as output by either algorithm, we simultaneously associate in one-to-one correspondence a quadratic form, $q(v) \coloneqq (v, v)$, so $(q, E')$ is a 4-dimensional quadratic space. We note that forms $q, q'$ arising from two inequivalent choices $\mu, \mu'$ are not necessarily isometric and can even correspond to different groups.

However, if $\mu = \lambda\mu'$ for some $\lambda \in F^\times$, the resulting quadratic forms $q, q'$ will be scalar multiples of one another since

$$q(v) = \mathrm{Tr}_{E'/F}(\mu v \sigma(v)) = \mathrm{Tr}_{E'/F}(\lambda\mu' v \sigma(v)) = \lambda \mathrm{Tr}_{E'/F}(\mu' v \sigma(v)) = \lambda q'(v)$$

and hence will correspond to isomorphic groups $SO(V)$ by Lemma 2.5.12.

We now provide the following theorem to justify the output of our algorithms.

**Theorem 4.2.1.** *For each triple $(E', \Phi, f)$, Algorithm 1 or 2 produces a well defined non-degenerate symmetric bilinear form $(\ ,\ )$ over $E'$. Furthermore, the resulting form is independent of the choice of representative $\mu$, with respect to the equivalence class as specified on Line 2.*

**Proof:** The bilinearity of $(\ ,\ )$ follows from the bilinearity of the trace. For every $v \neq 0$, we can define a $w := \sigma(\frac{1}{4}v^{-1}\mu^{-1})$ which yields

$$(v, w) = \mathrm{Tr}_{E'/F}(\mu v \frac{1}{4} v^{-1}\mu^{-1}) = \mathrm{Tr}_{E'/F}(\frac{1}{4} \cdot 1) = 1$$

so our form is non-degenerate. Moreover, we see that $(\ ,\ )$ is symmetric by computing

$$(v, w) = \mathrm{Tr}_{E'/F}(\mu v \sigma(w)) = \mathrm{Tr}_{E'/F}(\sigma(\mu v \sigma(w))) = \mathrm{Tr}_{E'/F}(\mu\sigma(v)w) = (w, v)$$

where the second equality follows from Lemma 2.2.19.

Suppose now that the choices $\mu, \mu'$ differ by an element of $\mathrm{N}_\sigma(E'^{\times})$. By Lemma 2.5.15, the resulting forms are equivalent. It remains to consider the case of $E_1 = E = E_2$ in Algorithm 2. Let $\mu_1, \mu_2 \in F^\times$ and define an $F$-linear automorphism $\psi\colon E \oplus E \to E \oplus E$ by $\psi(a, b) = (b, a)$. Then,

$$\begin{aligned}(\psi(v, \tilde{v}), \psi(w, \tilde{w}))_{\mu_1,\mu_2} &= ((\tilde{v}, v), (\tilde{w}, w))_{\mu_1,\mu_2} \\ &= \mu_1 \,\mathrm{Tr}_{E/F}(\tilde{v}\sigma_2(\tilde{w})) + \mu_2 \,\mathrm{Tr}_{E/F}(v\sigma_1(w)) \\ &= ((v, \tilde{v}), (w, \tilde{w}))_{\mu_2,\mu_1}\end{aligned}$$

hence these two forms are equivalent as required. ∎

Therefore, via Algorithm 1 and 2 we can partition $\mathscr{A}$ according to the group $G = SO(V)$ of the quadratic forms produced.

Suppose we have a Witt basis $\mathcal{B}^*$ with respect to the form $(\ ,\ )$ on $E'$; the process of obtaining such an identification is demonstrated later (see Examples 4.4.1, 4.4.4, and 4.5.4). We can then realize elements $a \in E' \simeq F^4$ in two different ways:

(1) As elements of $F^4$, denoted by $[a]_{\mathcal{B}^*}$, as in the proof of Proposition 4.1.1.

(2) As matrices with respect to multiplication by $\mathcal{B}^*$, denoted by $M_{[a]_{\mathcal{B}^*}}$.

We will use this notation to prove the following theorem, allowing us to explicitly describe the resulting conjugacy classes of tori promised by Theorem 3.4.5.

**Theorem 4.2.2.** *Fix a 4-dimensional, commutative, semisimple $F$-algebra $E'$ and involution $\sigma \in \mathrm{Aut}(E'/F)$ which non-trivially preserves each field component of $E'$. Choose $\mu \in E'^{\times}$ and let $q$ denote the corresponding quadratic form over $V \simeq E'$ output by the appropriate Algorithm (1 or 2).*

*Then, the group of norm 1 elements of $E'$, with respect to $\sigma$, is a* maximal elliptic torus of $SO(V)$. *Moreover, two such tori are conjugate if and only if they arise from the same algorithm and parameters, up to the equivalence specified on Line 2.*

**Proof:** Let $E' \simeq V$ and $\mu$ be chosen as above, together yielding a quadratic form $q(v) \coloneqq (v, v)$ upon performing the appropriate algorithm by Theorem 4.2.1. Let $E'^1$ denote the set of norm 1 elements of $E'$ with respect to $\sigma$. We claim that elements of $E'$ preserving the form $(\ ,\ )$ are exactly the group $E'^1$. Indeed, let $u \in E'^1$. Then,

$$(uv, uw) = \mathrm{Tr}_{E'/F}(\mu uv\sigma(uv)) = \mathrm{Tr}_{E'/F}(u\sigma(u) \cdot \mu v\sigma(w)) = \mathrm{Tr}_{E'/F}(\mu v\sigma(w)) = (v, w)$$

where the second last equality follows by Definition 3.1.6 of $E'^1$. Conversely, suppose $u \in E'$ preserves $(\ ,\ )$. Then, for all $v, w \in V$

$$(v, w) = (uv, uw) = \mathrm{Tr}_{E'/F}(\mu(uv)\sigma(uw)) = \mathrm{Tr}_{E'/F}(\mu v\sigma(u\sigma(u)w)) = (v, u\sigma(u)w)$$

so by Lemma 2.5.2, we have that $u\sigma(u) = 1$. Thus, elements $u \in E'^1$ correspond to elements of $SO(V)$ when written as multiplication by a fixed Witt basis $\mathcal{B}^*$, hence $M_{[u]_{\mathcal{B}^*}} \in SO(V)$.

Define a map $\varphi_\xi \colon E'^1 \to SO(V)$ which sends elements $u \in E'^1$ to their corresponding special orthogonal matrix $M_{[u]_{\mathcal{B}^*}}$ and take $T \coloneqq \mathrm{Im}\,\varphi_\xi$. By definition of the image, $T$ is a subgroup of $SO(V)$. Suppose $\varphi_\xi(x) = M_{[x]_{\mathcal{B}^*}}$ and $\varphi_\xi(y) = M_{[y]_{\mathcal{B}^*}}$ for some $x, y \in E'^1$ and $M_{[x]_{\mathcal{B}^*}}, M_{[y]_{\mathcal{B}^*}} \in T$. If $M_{[x]_{\mathcal{B}^*}} = M_{[y]_{\mathcal{B}^*}}$, then,

$$[x]_{\mathcal{B}^*} = M_{[x]_{\mathcal{B}^*}} \cdot [1]_{\mathcal{B}^*} = M_{[y]_{\mathcal{B}^*}} \cdot [1]_{\mathcal{B}^*} = [y]_{\mathcal{B}^*}.$$

Since $x \leftrightarrow [x]_{\mathcal{B}^*}$ is an isomorphism between $E'$ and $F^4$, we must have that $x = y$. Thus, $\varphi_\xi$ is injective and hence gives an isomorphism between $E'^1 \simeq T$. Furthermore, $T$ was proven to be elliptic in Lemma 3.1.7.

Conjugacy classes of tori are in bijection with the equivalence classes of triples by Theorem 3.4.5, hence two tori are conjugate if and only if the triples are equivalent. The equivalence of triples was built into Line 2 of the Algorithm using Proposition 4.1.1. ∎

## 4.3 Explicit Categorization of Forms

In this section, we explicitly identify the quadratic forms obtained via Algorithm 1 and 2 for each element of $\mathscr{T}$ as described by Theorem 4.1.2. This work relies heavily on the isomorphism classes of degree 4 field extensions, as summarized by Tables 2.1 and 2.2.

**Proposition 4.3.1.** *Pick a root $\sqrt[4]{\alpha}$ of the polynomial $x^4 - \alpha$ where $\alpha \in \{\varepsilon^k \varpi \mid 0 \leq k \leq 3\}$ and supppose $E' \simeq F(\sqrt[4]{\alpha})$ is a quartic field extension of $F$. Performing Algorithm 1 yields the following two forms up to equivalence:*

1. $\mu_1 \sim \frac{1}{4}$: $q_1 \simeq \langle 1, \alpha \rangle \perp \mathbb{H}$
2. $\mu_2 \sim \frac{1}{4}\varepsilon$: $q_2 \simeq \langle \varepsilon, \varepsilon\alpha \rangle \perp \mathbb{H}$

**Proof:** By constructing $E'$ in this way, we note that it is totally ramified and the only choice of intermediate field up to isomorphism is $E \simeq F(\sqrt{\alpha})$. By Proposition 2.4.4, $E^\times / \mathrm{N}_{E'/E}(E'^\times) = \{1, \varepsilon\}$, so there are two choices of $\mu$ up to equivalence. Without loss of generality, we can take $\mu_1 = \frac{1}{4}$ and $\mu_2 = \frac{1}{4}\varepsilon$ as our two coset representatives to eliminate extraneous scalars. Since $\mu_i \in F^\times$, $q_i := \mathrm{Tr}_{E'/F}(\mu_i v\sigma(v)) = \mu_i \mathrm{Tr}_{E'/F}(v\sigma(v))$ which implies that $q_2 = \varepsilon \cdot q_1$. Therefore, since $\langle \varepsilon, -\varepsilon \rangle \simeq \mathbb{H}$ it suffices to prove that $q_1 \simeq \langle 1, \alpha \rangle \perp \mathbb{H}$.

Write an arbitrary element $v$ of $E'$ as $v = v_1 + v_2\sqrt[4]{\alpha} + v_3\sqrt{\alpha} + v_4\sqrt[4]{\alpha}^3$ for some $v_i \in F$. The non-trivial map $\sigma \in \mathrm{Aut}(E'/E)$ is defined by the relation $\sqrt[4]{\alpha} \mapsto -\sqrt[4]{\alpha}$, hence

$$\begin{aligned} v\sigma(v) &= (v_1 + v_2\sqrt[4]{\alpha} + v_3\sqrt{\alpha} + v_4\sqrt[4]{\alpha}^3)(v_1 - v_2\sqrt[4]{\alpha} + v_3\sqrt{\alpha} - v_4\sqrt[4]{\alpha}^3) \\ &= \left(v_1^2 + \alpha v_3^2 - 2\alpha v_2 v_4\right) + \sqrt{\alpha}\left(2v_1v_3 - v_2^2 - \alpha v_4^2\right). \end{aligned}$$

The minimal polynomial for $\sqrt{\alpha}$ over $F$ is given by $x^2 - \alpha$, which implies by Lemma 2.2.12 that $\mathrm{Tr}_{E'/F}(\sqrt{\alpha}) = 0$. Furthermore, $\mathrm{Tr}_{E'/F}(\lambda) = [E' : F]\lambda = 4\lambda$ for all $\lambda \in F$, so with respect to the choice $\mu_1 = \frac{1}{4}$ we have that

$$q_1(v) = \mathrm{Tr}_{E'/F}(\mu_1 v\sigma(v)) = 4 \cdot \frac{1}{4}(v_1^2 + \alpha v_3^2 - 2\alpha v_2 v_4) \simeq \langle 1, \alpha \rangle \perp \mathbb{H}.$$

where the final isometry follows from Lemma 2.5.3. ∎

This result has covered all possible totally ramified extensions $E'/F$ up to isomorphism. When $\varepsilon = -1 \notin F^{\times 2}$ and the fixed subfield $E$ of $E'$ is unramified, our computations will become more complex. In this case, we are required to take $\varepsilon_E = x + iy$ as outlined by Lemma 2.4.7, which is much more involved than setting $\varepsilon_E = \sqrt{\varepsilon}$ when $-1 \in F^{\times 2}$.

**Proposition 4.3.2.** *Let $E'$ denote the unique unramified quartic extension of $F$. Performing Algorithm 1 yields the following two forms up to equivalence:*

1. $\mu_1 \sim \frac{1}{4}$: $q_1 \simeq \langle 1, -\varepsilon \rangle \perp \mathbb{H}$
2. $\mu_2 \sim \frac{1}{4}\varpi$: $q_2 \simeq \langle \varpi, -\varepsilon\varpi \rangle \perp \mathbb{H}$

**Proof:** As in our previous proof, Proposition 2.4.4 asserts that the choices $\mu_1 = \frac{1}{4}, \mu_2 = \frac{1}{4}\varpi$ are in different cosets of $E^\times / \mathrm{N}_{E'/E}(E'^\times) = \{1, \varpi\}$. Therefore $q_2 = \varpi \cdot q_1$, so it suffices to prove that

$$q_1 \simeq \langle 1, -\varepsilon \rangle \perp \mathbb{H} \simeq \begin{cases} \langle 1, \varepsilon \rangle \perp \mathbb{H} & -1 \in F^{\times 2} \\ \langle 1, 1 \rangle \perp \mathbb{H} & -1 \notin F^{\times 2}. \end{cases}$$

When $-1 \in F^{\times 2}$, $E' \simeq F(\sqrt[4]{\varepsilon})$. By taking identical steps to that of the previous proof with $\alpha = \varepsilon$, one obtains $q_1 \simeq \langle 1, \varepsilon \rangle \perp \mathbb{H}$ as required.

Suppose $-1 \notin F^{\times 2}$. We set $\varepsilon = -1$, and hence the unique quadratic subfield $E$ of $E'$ is given by $E = F(\sqrt{\varepsilon}) = F(i)$. Choose $\varepsilon_E = x + iy \notin E^{\times 2}$ as per Lemma 2.4.7; we note by definition $\sigma$ fixes $F(i)$ and maps $\sqrt{x+iy} \mapsto -\sqrt{x+iy}$. With respect to the ordered $F$-basis $\{1, i, \sqrt{x+iy}, i\sqrt{x+iy}\}$ of $E'$ and element $[v]_{\mathcal{B}} \coloneqq \begin{bmatrix} v_1 & v_2 & v_3 & v_4 \end{bmatrix}^T$ of $F^4$, we compute

$$\begin{aligned} v\sigma(v) &= (v_1 + v_2 i + v_3\sqrt{x+iy} + v_4 i\sqrt{x+iy})(v_1 + v_2 i - v_3\sqrt{x+iy} - v_4 i\sqrt{x+iy}) \\ &= \left(v_1^2 - v_2^2 - v_3^2 x + 2v_3 v_4 y + v_4^2 x\right) + i\left(2v_1 v_2 - v_3^2 y - 2v_3 v_4 x + v_4^2 y\right). \end{aligned}$$

As per our previous proof, the choice $\mu_1 = \frac{1}{4}$ gives the form

$$q_1(v) = v_1^2 - v_2^2 - v_3^2 x + 2v_3 v_4 y + v_4^2 x = \mathbb{H} \perp p(v_3, v_4) \simeq \mathbb{H} \perp \langle 1, 1 \rangle$$

where the final isometry follows from Lemma 2.5.6. ∎

We now will focus on the two isomorphism classes of partially ramified extensions, illustrating nicely that different choices of $\mu_i$ can yield tori in non-isomorphic groups $SO(V)$. Recall that the 4-dimensional anisotropic form is given by

$$q_1 \simeq \langle 1, -\varepsilon, \varpi, -\varepsilon\varpi \rangle \simeq \begin{cases} \langle 1, \varepsilon, \varpi, \varepsilon\varpi \rangle & -1 \in F^{\times 2} \\ \langle 1, 1, \varpi, \varpi \rangle & -1 \notin F^{\times 2} \end{cases}$$

and $q_2 \simeq 2\mathbb{H}$ is the unique 4-dimensional totally isotropic form.

**Proposition 4.3.3.** *Let $E' \simeq F(\sqrt{\varepsilon}, \sqrt{\varpi})$ with fixed intermediate field $E = F(\sqrt{\alpha})$ for some $\alpha \in F^\times \setminus F^{\times 2}$. We break our choices of $\mu_i$ into two cases:*

*(a) If $-1 \notin F^{\times 2}$ and $E/F$ is unramified, set $\mu_1 = \frac{1}{4}\varepsilon_E, \mu_2 = \frac{1}{4}$.*

*(b) In all other cases, set $\mu_1 = \frac{1}{4}, \mu_2 = \frac{1}{4}\sqrt{\alpha}$.*

*Then, performing Algorithm 1 with respect to $\mu_1$ yields the 4-dimensional anisotropic form, and with respect to $\mu_2$ yields the 4-dimensional totally isotropic form.*

**Proof:** Let $\{1, \sqrt{\alpha}, \sqrt{\beta}, \sqrt{\alpha\beta}\}$ be our ordered $F$-basis of $E'$ for an appropriate choice $\beta \in F^\times/F^{\times 2}$ such that $E' = E(\sqrt{\beta}) = F(\sqrt{\alpha}, \sqrt{\beta})$. Then, $\sigma\colon \sqrt{\beta} \mapsto -\sqrt{\beta}$, so one can compute for $[v]_{\mathcal{B}} \coloneqq \begin{bmatrix} v_1 & v_2 & v_3 & v_4 \end{bmatrix}^T \in F^4 \simeq E'$ that

$$v\sigma(v) = \left(v_1^2 + \alpha v_2^2 - \beta v_3^2 - \alpha\beta v_4^2\right) + \sqrt{\alpha}\left(2v_1v_2 - 2\beta v_3v_4\right).$$

Consider first Case $(a)$, where $\varepsilon = -1 \notin F^{\times 2}$ and $E = F(\sqrt{\varepsilon}) = F(i)$. Choose $\varepsilon_E = x + iy \notin E^{\times 2}$ as in Lemma 2.4.7. Then, by Proposition 2.4.4, $\mu_1 = \frac{1}{4}\varepsilon_E, \mu_2 = \frac{1}{4}$ are in different cosets of $E^\times/\operatorname{N}_{E'/E}(E'^\times)$. Based on the above computation of $v\sigma(v)$ for $\beta = \varpi$ and $\mu_1 = \frac{1}{4}(x + iy)$, we obtain

$$\begin{aligned} q_1(v) &= x(v_1^2 + \varepsilon v_2^2 - \varpi v_3^2 - \varepsilon\varpi v_4^2) + i^2 y(2v_1v_2 - 2\varpi v_3v_4) \\ &= xv_1^2 - 2yv_1v_2 - xv_2^2 + \varpi(xv_4^2 + 2yv_3v_4 - xv_3^2) \\ &= p(-v_2, v_1) \perp \varpi p(v_3, v_4) \simeq \langle 1, 1, \varpi, \varpi\rangle \end{aligned}$$

as required, where the final isometry follows from Lemma 2.5.6. Conversely, the choice $\mu_2 = \frac{1}{4}$ yields the form

$$q_2(v) = v_1^2 + \varepsilon v_2^2 - \varpi v_3^2 - \varepsilon\varpi v_4^2 = v_1^2 - v_2^2 - \varpi(v_3^2 - v_4^2) \simeq 2\mathbb{H}.$$

Suppose now that we are in Case $(b)$, so

(i) $E/F$ is ramified ($\alpha = \varpi$ or $\varepsilon\varpi$); or

(ii) $-1 \in F^{\times 2}$ and $\alpha = \varepsilon$.

One can verify by Proposition 2.4.4 that in both $(i)$ and $(ii)$, the choices $\mu_1 = \frac{1}{4}, \mu_2 = \frac{1}{4}\sqrt{\alpha}$ are in different cosets of $E^\times/\operatorname{N}_{E'/E}(E'^\times)$. Then,

$$q_1(v) = v_1^2 + \alpha v_2^2 - \beta v_3^2 - \alpha\beta v_4^2 = \langle 1, \alpha, -\beta, -\alpha\beta\rangle.$$

One can compute directly for $(i)$ that by choosing $\beta = \varepsilon$, $q_1 \simeq \langle 1, -\varepsilon, \varpi, -\varepsilon\varpi\rangle$ for both choices of $\alpha$. Similarly, choosing $\beta = \varpi$ or $\varepsilon\varpi$ in $(ii)$ implies that $q_1 \simeq \langle 1, \varepsilon, \varpi, \varepsilon\varpi\rangle$ as required. In both $(i)$ and $(ii)$, choosing $\mu_2 = \frac{1}{4}\sqrt{\alpha}$ gives

$$q_2(v) = \alpha(2v_1v_2 - 2\beta v_3v_4) \simeq 2\mathbb{H}$$

for all possible $\alpha$ by Lemma 2.5.3, which completes the proof. ∎

We now move to the final case remaining before we have covered all possible quartic extensions $E'/F$.

**Proposition 4.3.4.** *Let $E' \simeq F(\sqrt{\varepsilon_E\varpi})$ be a quartic field extension of $F$ with fixed intermediate field $E = F(\sqrt{\varepsilon})$. Performing Algorithm 1 yields the following two forms up to equivalence:*

1. $\mu_1 \sim \frac{1}{4}$: $q_1 \simeq \begin{cases} \langle 1, \varepsilon \rangle \perp \mathbb{H} & \text{if } -1 \in F^{\times 2} \\ \langle \varpi, \varpi \rangle \perp \mathbb{H} & \text{if } -1 \notin F^{\times 2} \end{cases}$

2. $\mu_2 \sim \frac{1}{4}\varepsilon_E$: $q_2 \simeq \varpi q_1$

**Proof:** First, suppose $-1 \in F^{\times 2}$. Recall from §2.4.2 that we can take $\varepsilon_E = \sqrt{\varepsilon}$, hence $E' \simeq F(\sqrt[4]{\varepsilon\varpi^2})$. One may compute similarly as in the preceding proofs for an element $v = v_1 + v_2\sqrt[4]{\varepsilon\varpi^2} + v_3\sqrt{\varepsilon} + v_4\sqrt[4]{\varepsilon^3\varpi^2} \in E'$, $v_i \in F$ that via the choice $\mu_1 = \frac{1}{4}$ we obtain

$$q_1(v) = \frac{1}{4}\operatorname{Tr}_{E'/F}(v\sigma(v)) = v_1^2 + \varepsilon v_3^2 - 2\varepsilon\varpi v_2 v_4 \simeq \langle 1, \varepsilon \rangle \perp \mathbb{H}$$

and via the choice $\mu_2 = \frac{1}{4}\sqrt{\varepsilon}$ we obtain

$$q_2(v) = \frac{1}{4}\operatorname{Tr}_{E'/F}(\sqrt{\varepsilon}v\sigma(v)) = \varepsilon(2v_1v_3 - \varpi v_2^2 - \varepsilon\varpi v_4^2) \simeq \langle \varpi, \varepsilon\varpi \rangle \perp \mathbb{H}$$

as required. Suppose now $-1 \notin F^{\times 2}$, so $E' \simeq F(\sqrt{\varpi(x+iy)})$ and $E = F(i)$. Let $v = v_1 + v_2 i + v_3\sqrt{\varpi(x+iy)} + v_4 i\sqrt{\varpi(x+iy)} \in E'$ for some $v_i \in F$. With respect to the choice $\mu_1 = \frac{1}{4}$,

$$q_1(v) = v_1^2 - v_2^2 + \varpi(-v_3^2 x + 2v_3v_4y + v_4^2 x) \simeq \mathbb{H} \perp \varpi p(v_3, v_4) \simeq \mathbb{H} \perp \langle \varpi, \varpi \rangle$$

by Lemma 2.5.6. Conversely, choosing $\mu_2 = \frac{1}{4}(x+iy)$ gives the form

$$\begin{aligned} q_2(v) &= x(v_1^2 - v_2^2 + \varpi(-v_3^2 x + 2v_3v_4y + v_4^2 x)) - y(2v_1v_2 + \varpi(-v_3^2 y - 2v_3v_4x + v_4^2 y)) \\ &\simeq p(-v_2, v_1) + \varpi\tilde{p}(v_3, v_4) \end{aligned}$$

where $\tilde{p}(v_3, v_4) \coloneqq x^2(v_4^2 - v_3^2) + 4v_3v_4xy - y^2(v_4^2 - v_3^2)$. The matrix corresponding to the form $\tilde{p}$ is given by

$$M_{\tilde{p}} = \begin{bmatrix} y^2 - x^2 & 2xy \\ 2xy & -(y^2 - x^2) \end{bmatrix}$$

which has determinant $\det(M_{\tilde{p}}) = -(x^2+y^2)^2 \equiv -1 \pmod{F^{\times 2}}$. By Lemma 2.5.4, this implies $\tilde{p} \simeq \mathbb{H}$, hence by Lemma 2.5.6, $q_2 \simeq \langle 1, 1 \rangle \perp \mathbb{H}$. ∎

One can verify via Tables 2.1 and 2.2 that these propositions have considered all possible quartic extensions $E'/F$ up to isomorphism. We now transition to Algorithm 2 and extensions of the form $E' = E_1 \oplus E_2$, where the $E_i$ denote quadratic field extensions of $F$. As discussed in the proof of Theorem 4.1.2, there are 6 unique pairs of these extensions, which we cover exhaustively in the following result.

**Proposition 4.3.5.** *Suppose $E' \simeq F(\sqrt{\alpha}) \oplus F(\sqrt{\beta})$ is a sum of quadratic extensions over $F$ for some non-squares $\alpha, \beta \in F^\times$. Let $\{1, \gamma_1\}, \{1, \gamma_2\}$ denote a set of representatives for $F^\times / \operatorname{N}_{F(\sqrt{\alpha})/F}(F(\sqrt{\alpha})^\times)$ and $F^\times / \operatorname{N}_{F(\sqrt{\beta})/F}(F(\sqrt{\beta})^\times)$ respectively. Performing Algorithm 2 yields the following four forms up to equivalence:*

1. $\mu_1 \sim (\frac{1}{2}, \frac{1}{2})$: $q_1 \simeq \langle 1, -\alpha, 1, -\beta\rangle$
2. $\mu_2 \sim (\frac{1}{2}\gamma_1, \frac{1}{2})$: $q_2 \simeq \langle \gamma_1, -\gamma_1\alpha, 1, -\beta\rangle$
3. $\mu_3 \sim (\frac{1}{2}, \frac{1}{2}\gamma_2)$: $q_3 \simeq \langle 1, -\alpha, \gamma_2, -\gamma_2\beta\rangle$
4. $\mu_4 \sim (\frac{1}{2}\gamma_1, \frac{1}{2}\gamma_2)$: $q_4 \simeq \langle \gamma_1, -\gamma_1\alpha, \gamma_2, -\gamma_2\beta\rangle$

*In the case that $F(\sqrt{\alpha}) \simeq F(\sqrt{\beta})$, we additionally note that $\mu_2 \sim \mu_3$ according to the equivalence relation as specified Line 2 of Algorithm 2, and hence $q_2 \simeq q_3$.*

**Proof:** Let $\{(1,0), (\sqrt{\alpha}, 0), (0,1), (0, \sqrt{\beta})\}$ be our ordered $F$-basis of $E'$. Let $(v, \tilde{v}) = (v_1 + v_2\sqrt{\alpha}, v_3 + v_4\sqrt{\beta}) \in E'$. Recall that $\sigma \in \mathrm{Aut}(E'/F)$ restricts to a non-trivial automorphism on both $F(\sqrt{\alpha}), F(\sqrt{\beta})$ and hence must be defined by the relations $\sqrt{\alpha} \mapsto -\sqrt{\alpha}, \sqrt{\beta} \mapsto -\sqrt{\beta}$.
Let $\mu_i = (\frac{1}{2}k_1, \frac{1}{2}k_2)$ for some $k_1, k_2 \in F^\times$. Then,

$$\begin{aligned} q_i(v, \tilde{v}) &= \frac{1}{2}k_1 \operatorname{Tr}_{F(\sqrt{\alpha})/F}(v\sigma(v)) + \frac{1}{2}k_2 \operatorname{Tr}_{F(\sqrt{\beta})/F}(\tilde{v}\sigma(\tilde{v})) \\ &= \frac{1}{2}k_1 \cdot 2(v_1^2 - \alpha v_2^2) + \frac{1}{2}k_2 \cdot 2(v_3^2 - \beta v_4^2) \\ &= \langle k_1, -k_1\alpha, k_2, -k_2\beta\rangle. \end{aligned}$$

While $\frac{1}{2}$ is not necessarily a square in $F$, $\mu$ is inequivalent to $\mu'$ if and only if $\lambda\mu$ is inequivalent to $\lambda\mu'$ for all $\lambda \in F$ and hence by construction, taking $(k_1, k_2) \in \{(1,1), (\gamma_1, 1), (1, \gamma_2), (\gamma_1, \gamma_2)\}$ yield inequivalent $\mu_i$ (apart from when $F(\sqrt{\alpha}) \simeq F(\sqrt{\beta})$ and $(\gamma_1, 1) \sim (1, \gamma_2)$), thereby completing the proof. ∎

As discussed in the proof of Theorem 4.1.2, we have a concrete list of triples $\xi \in \mathscr{A}$ up to equivalence, each of which corresponds to exactly one of the propositions above. These results tell us the isometry class of the quadratic form obtained under Algorithm 1 or 2, however, the form will not automatically be in its "desired" state. That is, the "natural" basis for $E'/F$ as chosen in the proof of each proposition is unlikely to coincidentally be a Witt basis for our preferred presentation of the form. The preferred presentation of the 8 isometry classes of 4-dimensional forms are:

$$\begin{gathered} -1 \in F^{\times 2}\colon \quad 2\mathbb{H}, \quad \langle 1, \varepsilon, \varpi, \varepsilon\varpi\rangle, \quad \text{or } p \perp \mathbb{H} \\ \text{where } p \in \{\langle 1, \varepsilon\rangle, \langle 1, \varpi\rangle, \langle 1, \varepsilon\varpi\rangle, \langle \varepsilon, \varpi\rangle, \langle \varepsilon, \varepsilon\varpi\rangle, \langle \varpi, \varepsilon\varpi\rangle\} \end{gathered} \tag{4.3.1}$$

and

$$\begin{gathered} -1 \notin F^{\times 2}\colon \quad 2\mathbb{H}, \quad \langle 1, 1, \varpi, \varpi\rangle, \quad \text{or } p \perp \mathbb{H} \\ \text{where } p \in \{\langle 1, 1\rangle, \langle 1, \varpi\rangle, \langle 1, \varepsilon\varpi\rangle, \langle \varepsilon, \varpi\rangle, \langle \varepsilon, \varepsilon\varpi\rangle, \langle \varpi, \varpi\rangle\} \end{gathered} \tag{4.3.2}$$

as described by Lemma 2.5.5. We will use the isometries listed in (2.5.1) to obtain, for each triple, *exactly* one of the aforementioned forms. The following example demonstrates the steps required.

**Example 4.3.6.** Let $E' \simeq F(\sqrt{\varepsilon}) \oplus F(\sqrt{\varpi})$. By Proposition 4.3.5, the choice $\mu_1 = (\frac{1}{2}, \frac{1}{2})$ yields the form $q_1 \simeq \langle 1, -\varepsilon, 1, -\varpi \rangle$. When $-1 \in F^{\times 2}$, $\langle -a \rangle \simeq \langle a \rangle$ for all $a \in F^\times$ and so $\langle 1, 1 \rangle \simeq \langle 1, -1 \rangle = \mathbb{H}$. Thus,

$$q_1 \simeq \langle 1, -\varepsilon, 1, -\varpi \rangle \simeq \langle \varepsilon, \varpi \rangle \perp \mathbb{H}.$$

Conversely, when $\varepsilon = -1 \notin F^{\times 2}$, we have that $\langle 1, \varepsilon \rangle = \mathbb{H}$, which in addition to the equivalence $\langle 1, 1 \rangle \simeq \langle \varepsilon, \varepsilon \rangle$ implies

$$q_1 \simeq \langle 1, -\varepsilon, 1, -\varpi \rangle = \langle 1, 1, 1, \varepsilon\varpi \rangle \simeq \langle \varepsilon, \varepsilon\varpi \rangle \perp \mathbb{H}.$$

In order to produce the following table, we repeat the process outlined above for all triples in $\mathscr{A}$ and their corresponding proposition, thereby yielding a 4-dimensional quadratic form in its desired representation, as specified by Equations 4.3.1 and 4.3.2.

| **Field Extensions** | **Parameter(s)** | $\mathbf{-1 \in F^{\times 2}}$ | $\mathbf{-1 \notin F^{\times 2}}$ |
|---|---|---|---|
| UNRAMIFIED | | | |
| $E' \simeq F(\sqrt{\varepsilon_E}), E \simeq F(\sqrt{\varepsilon})$ | $\mu_1 = \frac{1}{4}$<br>$\mu_2 = \frac{1}{4}\varpi$ | $\langle 1, \varepsilon \rangle \perp \mathbb{H}$<br>$\langle \varpi, \varepsilon\varpi \rangle \perp \mathbb{H}$ | $\langle 1, 1 \rangle \perp \mathbb{H}$<br>$\langle \varpi, \varpi \rangle \perp \mathbb{H}$ |
| $E' \simeq 2F(\sqrt{\varepsilon})$ | $\mu_1 = (\frac{1}{2}, \frac{1}{2}), \mu_3 = (\frac{1}{2}\varpi, \frac{1}{2}\varpi)$<br>$\mu_2 = (\frac{1}{2}, \frac{1}{2}\varpi)$ | $2\mathbb{H}$<br>$\langle 1, \varepsilon, \varpi, \varepsilon\varpi \rangle$ | $2\mathbb{H}$<br>$\langle 1, 1, \varpi, \varpi \rangle$ |
| PARTIALLY RAMIFIED | | | |
| $E' \simeq F(\sqrt{\varepsilon}, \sqrt{\varpi}), E \simeq F(\sqrt{\varepsilon})$ | $\mu_1 = \frac{1}{4}$<br>$\mu_2 = \frac{1}{4}\varepsilon_E$ | $\langle 1, \varepsilon, \varpi, \varepsilon\varpi \rangle$<br>$2\mathbb{H}$ | $2\mathbb{H}$<br>$\langle 1, 1, \varpi, \varpi \rangle$ |
| $E' \simeq F(\sqrt{\varepsilon}, \sqrt{\varpi}), E \simeq F(\sqrt{c\varpi})$<br>$c \in \{1, \varepsilon\}$ | $\mu_1 = \frac{1}{4}$<br>$\mu_2 = \frac{1}{4}\sqrt{c\varpi}$ | $\langle 1, \varepsilon, \varpi, \varepsilon\varpi \rangle$<br>$2\mathbb{H}$ | $\langle 1, 1, \varpi, \varpi \rangle$<br>$2\mathbb{H}$ |
| $E' \simeq F(\sqrt{\varepsilon_E\varpi}), E \simeq F(\sqrt{\varepsilon})$ | $\mu_1 = \frac{1}{4}$<br>$\mu_2 = \frac{1}{4}\varepsilon_E$ | $\langle 1, \varepsilon \rangle \perp \mathbb{H}$<br>$\langle \varpi, \varepsilon\varpi \rangle \perp \mathbb{H}$ | $\langle \varpi, \varpi \rangle \perp \mathbb{H}$<br>$\langle 1, 1 \rangle \perp \mathbb{H}$ |
| $E' \simeq F(\sqrt{\varepsilon}) \oplus F(\sqrt{\varpi})$ | $\mu_1 = (\frac{1}{2}, \frac{1}{2}), \mu_4 = (\frac{1}{2}\varpi, \frac{1}{2}\varepsilon)$<br>$\mu_2 = (\frac{1}{2}\varpi, \frac{1}{2}), \mu_3 = (\frac{1}{2}, \frac{1}{2}\varepsilon)$ | $\langle \varepsilon, \varpi \rangle \perp \mathbb{H}$<br>$\langle 1, \varepsilon\varpi \rangle \perp \mathbb{H}$ | $\langle \varepsilon, \varepsilon\varpi \rangle \perp \mathbb{H}$<br>$\langle 1, \varpi \rangle \perp \mathbb{H}$ |
| $E' \simeq F(\sqrt{\varepsilon}) \oplus F(\sqrt{\varepsilon\varpi})$ | $\mu_1 = (\frac{1}{2}, \frac{1}{2}), \mu_4 = (\frac{1}{2}\varpi, \frac{1}{2}\varepsilon)$<br>$\mu_2 = (\frac{1}{2}\varpi, \frac{1}{2}), \mu_3 = (\frac{1}{2}, \frac{1}{2}\varepsilon)$ | $\langle \varepsilon, \varepsilon\varpi \rangle \perp \mathbb{H}$<br>$\langle 1, \varpi \rangle \perp \mathbb{H}$ | $\langle \varepsilon, \varpi \rangle \perp \mathbb{H}$<br>$\langle 1, \varepsilon\varpi \rangle \perp \mathbb{H}$ |
| TOTALLY RAMIFIED | | | |
| $E' \simeq F(\sqrt[4]{c\varpi}), E \simeq F(\sqrt{\varpi})$<br>$c \in \{1, \varepsilon^2\}$ | $\mu_1 = \frac{1}{4}$<br>$\mu_2 = \frac{1}{4}\varepsilon$ | $\langle 1, \varpi \rangle \perp \mathbb{H}$<br>$\langle \varepsilon, \varepsilon\varpi \rangle \perp \mathbb{H}$ | $\langle 1, \varpi \rangle \perp \mathbb{H}$<br>$\langle \varepsilon, \varepsilon\varpi \rangle \perp \mathbb{H}$ |
| $E' \simeq F(\sqrt[4]{c\varpi}), E \simeq F(\sqrt{\varepsilon\varpi})$<br>$c \in \{\varepsilon, \varepsilon^3\}$ | $\mu_1 = \frac{1}{4}$<br>$\mu_2 = \frac{1}{4}\varepsilon$ | $\langle 1, \varepsilon\varpi \rangle \perp \mathbb{H}$<br>$\langle \varepsilon, \varpi \rangle \perp \mathbb{H}$ | $\langle 1, \varepsilon\varpi \rangle \perp \mathbb{H}$<br>$\langle \varepsilon, \varpi \rangle \perp \mathbb{H}$ |

| | | | |
|---|---|---|---|
| $E' \simeq F(\sqrt{\varpi}) \oplus F(\sqrt{\varepsilon\varpi})$ | $\mu_1 = (\frac{1}{2}, \frac{1}{2}), \mu_4 = (\frac{1}{2}\varepsilon, \frac{1}{2}\varepsilon)$<br>$\mu_2 = (\frac{1}{2}\varepsilon, \frac{1}{2}), \mu_3 = (\frac{1}{2}, \frac{1}{2}\varepsilon)$ | $\langle \varpi, \varepsilon\varpi \rangle \perp \mathbb{H}$<br>$\langle 1, \varepsilon \rangle \perp \mathbb{H}$ | $\langle 1, 1 \rangle \perp \mathbb{H}$<br>$\langle \varpi, \varpi \rangle \perp \mathbb{H}$ |
| $E' \simeq 2F(\sqrt{\varpi})$ | $\mu_1 = (\frac{1}{2}, \frac{1}{2}), \mu_3 = (\frac{1}{2}\varepsilon, \frac{1}{2}\varepsilon)$<br>$\mu_2 = (\frac{1}{2}, \frac{1}{2}\varepsilon)$ | $2\mathbb{H}$<br>$\langle 1, \varepsilon, \varpi, \varepsilon\varpi \rangle$ | $\langle 1, 1, \varpi, \varpi \rangle$<br>$2\mathbb{H}$ |
| $E' \simeq 2F(\sqrt{\varepsilon\varpi})$ | $\mu_1 = (\frac{1}{2}, \frac{1}{2}), \mu_3 = (\frac{1}{2}\varepsilon, \frac{1}{2}\varepsilon)$<br>$\mu_2 = (\frac{1}{2}, \frac{1}{2}\varepsilon)$ | $2\mathbb{H}$<br>$\langle 1, \varepsilon, \varpi, \varepsilon\varpi \rangle$ | $\langle 1, 1, \varpi, \varpi \rangle$<br>$2\mathbb{H}$ |

Table 4.1: 4-Dimensional Quadratic Forms Output by Algorithms 1 & 2

Take $F$ to be a non-archimedean local field with uniformizer $\varpi \in \mathcal{P}$ and non-square $\varepsilon \in \mathcal{O}^\times$. We let $V = F^4$ and $E' \subseteq \mathrm{End}(V)$ denote a commutative, semisimple subalgebra with quadratic form $q(v) = \mathrm{Tr}_{E'/F}(\mu_i v \sigma(v))$ over $V$. When $E'$ is quartic, we fix a quadratic subfield $E$ with non-square $\varepsilon_E$. Then, the $\mu_i$ are representatives of $E^\times / \mathrm{N}_{E'/E}(E'^\times)$ and the involution $\sigma \in \mathrm{Aut}(E'/F)$ acts non-trivially with respect to the extension $E'/E$. Conversely, when $E' = E_1 \oplus E_2$, $\mu_i$ is given by a pair $(\mu_{i1}, \mu_{i2})$ such that $\mu_{ij}$ are representatives of $F^\times / \mathrm{N}_{E_j/F}(E_j^\times)$ and $(\mu_{i1}, \mu_{i2}) \sim (\mu_{i2}, \mu_{i1})$ when $E_1 \simeq E_2$. The map $\sigma = (\sigma_1, \sigma_2)$ is such that each $\sigma_j \in \mathrm{Gal}(E_j/F)$ is non-trivial. When $-1 \notin F^{\times 2}$, the field extensions $F(\sqrt[4]{\varpi}) \simeq F(\sqrt[4]{\varepsilon^2\varpi})$ and $F(\sqrt[4]{\varepsilon\varpi}) \simeq F(\sqrt[4]{\varepsilon^3\varpi})$ are isomorphic, hence resulting in four fewer triples up to equivalence.

Recall that though we sort the tori with respect to the isometry class of the corresponding quadratic form, isomorphic groups $SO(V)$ have isomorphic tori.

For example, when $-1 \in F^{\times 2}$ the choices $E' \simeq F(\sqrt[4]{\varepsilon\varpi}), \mu_1 \sim \frac{1}{4}$ yield the form $q_1 \simeq \langle 1, \varepsilon\varpi \rangle \perp \mathbb{H}$ as per Table 4.1, and hence a torus in the group $SO(q_1)$. Conversely, the choice $\mu_2 \sim \frac{1}{4}\varepsilon$ yields the form $q_2 \simeq \langle \varepsilon, \varpi \rangle \perp \mathbb{H}$ and thus a torus in the group $SO(q_2)$, which by Corollary 2.5.13 is isomorphic to $SO(q_1)$. This implies that the resulting tori can by conjugated to one another by an element of $GL(V)$; we expand upon this in Example 4.4.1.

Thus, Table 4.1 enables us to partition our triples with respect to which of the 8 isometry classes of quadratic forms they correspond to, thereby providing more specificity to the tori in Theorem 4.1.2.

**Theorem 4.3.7.** *Let $\mathscr{T}_G$ denote the set of conjugacy classes of maximal elliptic tori in the group $G = SO(V)$, where $\dim(V) = 4$. Then, when $-1 \in F^{\times 2}$:*

$$|\mathscr{T}_G| = \begin{cases} 6 & \text{if } G \simeq SO(\langle 1, \varepsilon, \varpi, \varepsilon\varpi \rangle) \\ 9 & \text{if } G \simeq SO(2\mathbb{H}) \\ 4 & \text{if } G \simeq SO(\langle 1, \alpha \rangle \perp \mathbb{H}), \text{ where } \alpha \in \{\varepsilon, \varpi, \varepsilon\varpi\} \end{cases}$$

*and when* $-1 \notin F^{\times 2}$:

$$|\mathscr{T}_G| = \begin{cases} 8 & \text{if } G \simeq SO(\langle 1,1,\varpi,\varpi\rangle) \\ 7 & \text{if } G \simeq SO(2\mathbb{H}) \\ 4 & \text{if } G \simeq SO(\langle 1,1\rangle \perp \mathbb{H}) \\ 3 & \text{if } G \simeq SO(\langle 1,\alpha\rangle \perp \mathbb{H}), \text{ where } \alpha \in \{\varpi, \varepsilon\varpi\}. \end{cases}$$

## 4.4 The Full Classification of Tori when $-1 \in F^{\times 2}$

We are now ready to give the complete classification up to conjugacy of the maximal elliptic toral subgroups of $SO(V)$, where $V = F^4$. This section is dedicated to the determination of a Witt basis for each of the tori, with respect to one of the forms from (4.3.1), in the case that $-1 = i^2 \in F^{\times 2}$. Recall from Corollary 2.5.13, the following groups are isomorphic

$$\begin{aligned} SO(\langle 1,\varepsilon\rangle \perp \mathbb{H}) &\simeq SO(\langle \varpi, \varepsilon\varpi\rangle \perp \mathbb{H}) \\ SO(\langle 1,\varpi\rangle \perp \mathbb{H}) &\simeq SO(\langle \varepsilon, \varepsilon\varpi\rangle \perp \mathbb{H}) \\ SO(\langle 1,\varepsilon\varpi\rangle \perp \mathbb{H}) &\simeq SO(\langle \varepsilon, \varpi\rangle \perp \mathbb{H}) \end{aligned}$$

and hence their tori are isomorphic.

Finding a Witt basis is equivalent to giving the embedding of the torus into the group. The following example demonstrates the process of working out a suitable basis and using it to concretely realize the torus as matrices in $SO(V)$.

**Example 4.4.1.** Let $-1 \in F^{\times 2}$ and consider $E' \simeq F(\sqrt[4]{\varepsilon\varpi})$. As per Table 4.1, this extension yields a torus $T_1$ of $SO(\langle 1,\varepsilon\varpi\rangle \perp \mathbb{H})$ with respect to the choice $\mu_1 \sim \frac{1}{4}$.

We want to find a Witt basis $\mathcal{B}_1^* = \{g_1, g_2, e_1, f_1\}$ consisting of vectors in $E'$ such that $q_1(g_1) = 1, q_1(g_2) = \varepsilon\varpi$, and $q_1(ae_1 + bf_1) = 2ab$ for all $a, b \in F$, with all other combinations zero. As per the proof of Proposition 4.3.1, the resultant form $q_1$ with respect to $\mu_1 = \frac{1}{4}$ and the standard basis $\mathcal{B} = \{1, \sqrt[4]{\varepsilon\varpi}, \sqrt{\varepsilon\varpi}, \sqrt[4]{\varepsilon\varpi}^3\}$ is given by

$$q_1(v_1 + v_2\sqrt[4]{\varepsilon\varpi} + v_3\sqrt{\varepsilon\varpi} + v_4\sqrt[4]{\varepsilon\varpi}^3) = v_1^2 + \varepsilon\varpi v_3^2 - 2\varepsilon\varpi v_2 v_4$$

for all $v_i \in F$. From this, it is immediately clear that we can take $g_1 = 1, g_2 = \sqrt{\varepsilon\varpi}$. Furthermore, the vectors $\{\sqrt[4]{\varepsilon\varpi}, \sqrt[4]{\varepsilon\varpi}^3\}$ form a hyperbolic plane, however, it needs to be scaled by $(-\varepsilon\varpi)^{-1}$. Indeed, if we take $e_1 = \sqrt[4]{\varepsilon\varpi}$ and $f_1 = (-\varepsilon\varpi)^{-1}\sqrt[4]{\varepsilon\varpi}^3 = -(\sqrt[4]{\varepsilon\varpi})^{-1}$, we obtain

$$q_1(v_2\sqrt[4]{\varepsilon\varpi} + v_4\sqrt[4]{\varepsilon\varpi}^3(-\varepsilon\varpi)^{-1}) = -2\varepsilon\varpi \cdot (-\varepsilon\varpi)^{-1} = 2v_2v_4$$

as required. Thus, the basis

$$\mathcal{B}_1^* = \{1, \sqrt{\varepsilon\varpi}, \sqrt[4]{\varepsilon\varpi}, -(\sqrt[4]{\varepsilon\varpi})^{-1}\}$$

is a suitable Witt basis for $q_1$.

We will now use $\mathcal{B}_1^*$ to write down our torus $E'^1$ as matrices in $SO(V)$. Let $u \in E'^1$. Recall from our discussion following Definition 3.1.6 that this implies $u \in \mathcal{O}_{E'}^\times$, and hence $u$ can be written as an $\mathcal{O}$-linear combination of elements of the $F$-basis $\mathcal{C}$, as constructed in the proof of Proposition 2.3.4. Since $E'$ is totally ramified (so $e = 4$), the residue field of $E'$ is equal to the residue field of $F$ and $\varpi_{E'} = \sqrt[4]{\varepsilon\varpi}$. This implies that $\mathcal{C} = \mathcal{B}$, therefore, we can write every $u \in E'^1$ as

$$u = v_1 + v_2\sqrt[4]{\varepsilon\varpi} + v_3\sqrt{\varepsilon\varpi} + v_4\sqrt[4]{\varepsilon\varpi}^3$$

for some $v_i \in \mathcal{O}$, guaranteeing the compactness of the torus. We want to write elements of $E'^1$ with respect to our Witt basis, so by setting $v_1 = u_1, v_2 = u_3, v_3 = u_2$ and $v_4 = -u_4(\varepsilon\varpi)^{-1}$, we see we can write

$$u = u_1 + u_2\sqrt{\varepsilon\varpi} + u_3\sqrt[4]{\varepsilon\varpi} + u_4(-\sqrt[4]{\varepsilon\varpi}^{-1}) \in E'^1$$

for some $u_1, u_2, u_3 \in \mathcal{O}$ and $-u_4(\varepsilon\varpi)^{-1} \in \mathcal{O}$, or equivalently $u_4 \in \mathcal{P}$. The matrix of $u$ with respect to multiplication by $\mathcal{B}_1^*$ is given by

$$M_{[u]_{\mathcal{B}_1^*}} = \begin{bmatrix} u_1 & u_2\varepsilon\varpi & -u_4 & -u_3 \\ u_2 & u_1 & u_3 & u_4(\varepsilon\varpi)^{-1} \\ u_3 & -u_4 & u_1 & -u_2 \\ u_4 & -u_3\varepsilon\varpi & -u_2\varepsilon\varpi & u_1 \end{bmatrix}.$$

Moreover, since $u\sigma(u) = 1$, we obtain additional restrictions:

$$M_{[u]_{\mathcal{B}_1^*}} \cdot [\sigma(u)]_{\mathcal{B}_1^*} = M_{[u]_{\mathcal{B}_1^*}} \cdot \begin{bmatrix} u_1 \\ u_2 \\ -u_3 \\ -u_4 \end{bmatrix} = \begin{bmatrix} u_1^2 + u_2^2\varepsilon\varpi + 2u_3u_4 \\ 2u_1u_2 - u_3^2 - u_4^2(\varepsilon\varpi)^{-1} \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

This implies that the torus $T_1$ of $SO(\langle 1, \varepsilon\varpi\rangle \perp \mathbb{H})$ is given by

$$T_1 = \left\{ \begin{bmatrix} u_1 & u_2\varepsilon\varpi & -u_4 & -u_3 \\ u_2 & u_1 & u_3 & u_4(\varepsilon\varpi)^{-1} \\ u_3 & -u_4 & u_1 & -u_2 \\ u_4 & -u_3\varepsilon\varpi & -u_2\varepsilon\varpi & u_1 \end{bmatrix} \;\middle|\; \begin{array}{r} u_1, u_2, u_3 \in \mathcal{O}, u_4 \in \mathcal{P} \\ u_1^2 + u_2^2\varepsilon\varpi + 2u_3u_4 = 1 \\ 2u_1u_2 - u_3^2 - u_4^2(\varepsilon\varpi)^{-1} = 0 \end{array} \right\}.$$

As seen in Table 4.1, with respect to the same field extension $E' \simeq F(\sqrt[4]{\varepsilon\varpi})$, the choice $\mu_2 \sim \frac{1}{4}\varepsilon$ yields a quadratic form $q_2 \simeq \langle \varepsilon, \varpi\rangle \perp \mathbb{H}$ and hence a torus $T_2$ in the

group $SO(q_2)$. This group is isomorphic to the group $SO(\langle 1, \varepsilon\varpi\rangle \perp \mathbb{H})$ via a change of basis in $GL(V)$. It is this same change of basis that conjugates $T_1$ to $T_2$, however, they are tori of two non-equal groups and conjugate only by an element of $GL(V)$, not of the special orthogonal group.

In Example 4.4.1, the standard basis was almost a Witt basis; that is, it only required scaling. This will not always be the case for our computations. For example, we will often need to find a Witt basis $\{e_1, f_1\}$ for the quadratic form $q(v_1, v_2) = \lambda(v_1^2 - v_2^2) \simeq \mathbb{H}$ for some fixed $\lambda \in F^\times$. This requires a more sophisticated change of basis, as accomplished by the following lemma.

**Lemma 4.4.2.** *Suppose $u, w \in V$ are such that $q(v_1u + v_2w) = \lambda(v_1^2 - v_2^2)$ for some fixed $\lambda \in F^\times$. Then, $\{u + w, \frac{1}{2}\lambda^{-1}(u - w)\}$ is a Witt basis for $q$.*

**Proof:** Let $(\ ,\ )$ be the corresponding symmetric bilinear form to $q$; then we have $(u, u) = \lambda, (w, w) = -\lambda$ and $(u, w) = 0$. If we set $e_1 = u + w, f_1 = \frac{1}{2}\lambda^{-1}(u - w)$, we can compute that $(e_1, e_1) = (u, u) + 2(u, w) + (w, w) = \lambda + (-\lambda) = 0$. Similarly, $(f_1, f_1) = \frac{1}{4}\lambda^{-2}(u - w, u - w) = \frac{1}{4}\lambda^{-2}((u, u) - 2(u, w) + (w, w)) = 0$. Finally,

$$(e_1, f_1) = \frac{1}{2}\lambda^{-1}(u + w, u - w) = \frac{1}{2}\lambda^{-1}((u, u) - (w, w)) = \frac{1}{2}\lambda^{-1}(2\lambda) = 1$$

as required. ∎

In order to simplify notation in our tables, we define the following map to output such a pair $\{e_1, f_1\}$ as described by Lemma 4.4.2.

**Definition 4.4.3.** *Define a map $\zeta_\lambda \colon V \times V \to V \times V$ by the relation $\zeta_\lambda[u, w] \coloneqq (u + w, \frac{1}{2}\lambda^{-1}(u - w))$ for a fixed $\lambda \in F^\times$.*

The following example illustrates both the explicit use of $\zeta_\lambda$ to determine a Witt basis, as well as how Chapter 3's theory regarding the conjugacy classes of tori is incredibly valuable in practice.

**Example 4.4.4.** Consider the sum of extensions $E' \simeq F(\sqrt{\varepsilon}) \oplus F(\sqrt{\varpi})$ in the case when $-1 \in F^{\times 2}$. By Proposition 4.3.5, the choice $\mu_1 = (\frac{1}{2}, \frac{1}{2})$ yields a quadratic form

$$q_1(v_1 + v_2\sqrt{\varepsilon}, v_3 + v_4\sqrt{\varpi}) = v_1^2 - \varepsilon v_2^2 + v_3^2 - \varpi v_4^2$$

for all $v_i \in F$, which is isometric to $q_1 \simeq \langle \varepsilon, \varpi\rangle \perp \mathbb{H}$ by Example 4.3.6. Thus, we are looking for a Witt basis $\mathcal{B}_1^* = \{g_1, g_2, e_1, f_1\}$ for $E'/F$ such that $q_1(g_1) = \varepsilon, q_1(g_2) = \varpi$, and $\{e_1, f_1\}$ is a hyperbolic pairing as discussed previously in Example 4.4.1. Since $i \in F$, we can take $g_1 = (i\sqrt{\varepsilon}, 0)$ to obtain

$$q_1(g_1) = -\varepsilon \cdot i^2 = \varepsilon$$

as required. Similary, the vector $g_2 = (0, i\sqrt{\varpi})$ satisfies $q_1(g_2) = \varpi$. Finally, we note that the pair $\{(1,0),(0,i)\}$ is such that

$$q_1(v_1(1,0) + v_3(0,i)) = q_1(v_1, iv_3) = v_1^2 + (iv_3)^2 = v_1^2 - v_3^2$$

and hence forms a hyperbolic plane. By Lemma 4.4.2, the vectors $\zeta_1[(1,0),(0,i)] = \{(1,i), \frac{1}{2}(1,-i)\}$ form a Witt basis for this hyperbolic plane; the reader can verify this by substituting the sum of these vectors into the formula for $q_1$. Thus,

$$\mathcal{B}_1^* = \left\{(i\sqrt{\varepsilon}, 0), (0, i\sqrt{\varpi}), \zeta_1[(1,0),(0,i)]\right\}$$

is a Witt basis for $E'/F$ corresponding to $q_1$. Consider an element $u \in E'^1$ and write it with respect to the standard basis $\mathcal{B}$: $u = v_1(1,0) + v_2(\sqrt{\varepsilon}, 0) + v_3(0,1) + v_4(0, \sqrt{\varpi})$. By the same reasoning as to that of the previous example (4.4.1), we can take the coefficients $v_i$ to be in $\mathcal{O}$. Due to the complexity of the matrix $M_{[u]_{\mathcal{B}_1^*}}$, we will write down the matrices of the torus by using a change of basis matrix from $\mathcal{B}$ to $\mathcal{B}_1^*$. We first note that $M_{[u]_{\mathcal{B}}}$ is a block diagonal matrix given by

$$M_{[u]_{\mathcal{B}}} = \begin{bmatrix} B_1 & 0 \\ 0 & B_2 \end{bmatrix}, \text{ where } B_1 = \begin{bmatrix} v_1 & v_2\varepsilon \\ v_2 & v_1 \end{bmatrix} \text{ and } B_2 = \begin{bmatrix} v_3 & v_4\varpi \\ v_4 & v_3 \end{bmatrix}.$$

Moreover, the change of basis matrix $P_{\mathcal{B}\to\mathcal{B}_1^*} \in GL(V)$ from $\mathcal{B}$ to $\mathcal{B}_1^*$ is given by

$$P_{\mathcal{B}\to\mathcal{B}_1^*} = \begin{bmatrix} 0 & -i & 0 & 0 \\ 0 & 0 & 0 & -i \\ \frac{1}{2} & 0 & -\frac{1}{2}i & 0 \\ 1 & 0 & i & 0 \end{bmatrix}.$$

Therefore, the set

$$T_1 = \left\{ P_{\mathcal{B}\to\mathcal{B}_1^*} \cdot M_{[u]_{\mathcal{B}}} \cdot (P_{\mathcal{B}\to\mathcal{B}_1^*})^{-1} \;\middle|\; \begin{array}{r} v_1, v_2, v_3, v_4 \in \mathcal{O} \\ v_1^2 - v_2^2\varepsilon = 1 \\ v_3^2 - v_4^2\varpi = 1 \end{array} \right\}$$

is a torus in the group $SO(\langle \varepsilon, \varpi \rangle \perp \mathbb{H})$, where the additional restrictions arise from $u$ being a norm 1 element of $E'$.

Let us now consider the same $E'$ as above, but instead make the choice $\mu_4 = (\frac{1}{2}\gamma_1, \frac{1}{2}\gamma_2)$ as per Proposition 4.3.5, where $\gamma_1, \gamma_2$ denote representatives of the non-trivial classes of $F^\times / \mathrm{N}_{F(\sqrt{\varepsilon})/F}(F(\sqrt{\varepsilon})^\times)$ and $F^\times / \mathrm{N}_{F(\sqrt{\varpi})/F}(F(\sqrt{\varpi})^\times)$ respectively. By Proposition 2.4.4, we can take $\gamma_1 = \varpi$ and $\gamma_2 = \varepsilon$, hence

$$q_4(v_1 + v_2\sqrt{\varepsilon}, v_3 + v_4\sqrt{\varpi}) = \varpi v_1^2 - \varepsilon\varpi v_2^2 + \varepsilon v_3^2 - \varepsilon\varpi v_4^2$$

which is isometric to $q_4 \simeq \langle \varepsilon, \varpi \rangle \perp \mathbb{H}$ since $\langle -\varepsilon\varpi, -\varepsilon\varpi \rangle \simeq \langle \varepsilon\varpi, -\varepsilon\varpi \rangle \simeq \mathbb{H}$. Thus, we want a Witt basis $\mathcal{B}_4^*$ of the same form as $\mathcal{B}_1^*$, since $q_1 \simeq q_4$. By noting that $q_4(0,1) = \varepsilon$ and $q_4(1,0) = \varpi$, it is clear that we can take $g_1 = (0,1), g_2 = (1,0)$ without any scaling required. Furthermore,

$$q_4(v_2\sqrt{\varepsilon}, iv_4\sqrt{\varpi}) = -\varepsilon\varpi v_2^2 - \varepsilon\varpi(iv_4)^2 = \varepsilon\varpi(v_4^2 - v_2^2)$$

so the vectors $\{(0, i\sqrt{\varpi}), (\sqrt{\varepsilon}, 0)\}$ form a hyperbolic plane, scaled by $\lambda = \varepsilon\varpi$. Thus, by Lemma 4.4.2 we can take $\{e_1, f_1\} = \zeta_{\varepsilon\varpi}[(0, i\sqrt{\varpi}), (\sqrt{\varepsilon}, 0)]$ and hence

$$\mathcal{B}_4^* = \left\{(0,1), (1,0), \zeta_{\varepsilon\varpi}[(0, i\sqrt{\varpi}), (\sqrt{\varepsilon}, 0)]\right\}$$

is a Witt basis for $E'/F$ with respect to the form $q_4$. Similarly to with $T_1$, we obtain a second torus $T_4$ via the set

$$T_4 = \left\{ P_{\mathcal{B}\to\mathcal{B}_4^*} \cdot M_{[u]_{\mathcal{B}}} \cdot (P_{\mathcal{B}\to\mathcal{B}_4^*})^{-1} \;\middle|\; \begin{array}{r} v_1, v_2, v_3, v_4 \in \mathcal{O} \\ v_1^2 - v_2^2\varepsilon = 1 \\ v_3^2 - v_4^2\varpi = 1 \end{array} \right\}, \quad P_{\mathcal{B}\to\mathcal{B}_4^*} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & -\frac{1}{2}i \\ 0 & -\varepsilon\varpi & 0 & -i\varepsilon\varpi \end{bmatrix}$$

where $P_{\mathcal{B}\to\mathcal{B}_4^*}$ is the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}_4^*$. These toral subgroups $T_1, T_4$ of $SO(\langle \varepsilon, \varpi \rangle \perp \mathbb{H})$ are indeed isomorphic via a change of basis in $GL(V)$, however, they are non-conjugate by Theorem 3.4.5 and Proposition 4.1.1; a fact which would be incredibly difficult to conclude directly.

We now present Witt bases for all of our tori when $-1 \in F^{\times 2}$ in the table that follows. Many of the bases simply required scaling and reordering of our standard basis vectors, as exhibited by Example 4.4.1, however, some of the hyperbolic planes required use of the map $\zeta_\lambda$ to produce a suitable pairing $\{e_1, f_1\}$ as described by Lemma 4.4.2.

Moreover, the reader can verify these computations by inputting each $E', \mu$ into the appropriate Algorithm (1 or 2) to obtain a quadratic form, which with respect to the Witt basis, should be exactly the form $q$ in the header $SO(q)$ of Table 4.2.

Conversely, the explicit formulas for the quadratic forms have been precisely outlined in the proofs of the propositions from §4.3, granting the reader the opportunity to verify the Witt bases more efficiently.

| $E \subset E', \mu$ | Witt Basis of $E'/F$ |
|---|---|
| $SO(\langle 1, \varepsilon, \varpi, \varepsilon\varpi\rangle)$<br>6 Classes of Tori | $\{g_1,\ g_2,\ g_3,\ g_4\}$ |
| $2F(\sqrt{\varepsilon}),\ (\frac{1}{2}, \frac{1}{2}\varpi)$ | $\{(1,0),\ (i\sqrt{\varepsilon},0),\ (0,1),\ (0,i\sqrt{\varepsilon})\}$ |
| $F(\sqrt{\varepsilon}) \subset F(\sqrt{\varepsilon}, \sqrt{\varpi}),\ \frac{1}{4}$ | $\{1,\ \sqrt{\varepsilon},\ i\sqrt{\varpi},\ i\sqrt{\varepsilon\varpi}\}$ |
| $F(\sqrt{\varpi}) \subset F(\sqrt{\varepsilon}, \sqrt{\varpi}),\ \frac{1}{4}$ | $\{1,\ i\sqrt{\varepsilon},\ \sqrt{\varpi},\ i\sqrt{\varepsilon\varpi}\}$ |
| $F(\sqrt{\varepsilon\varpi}) \subset F(\sqrt{\varepsilon}, \sqrt{\varpi}),\ \frac{1}{4}$ | $\{1,\ i\sqrt{\varepsilon},\ i\sqrt{\varpi},\ \sqrt{\varepsilon\varpi}\}$ |
| $2F(\sqrt{\varpi}),\ (\frac{1}{2}, \frac{1}{2}\varepsilon)$ | $\{(1,0),\ (0,1),\ (i\sqrt{\varpi},0),\ (0,i\sqrt{\varpi})\}$ |
| $2F(\sqrt{\varepsilon\varpi}),\ (\frac{1}{2}, \frac{1}{2}\varepsilon)$ | $\{(1,0),\ (0,1),\ (0,i\sqrt{\varepsilon^{-1}\varpi}),\ (i\sqrt{\varepsilon\varpi},0)\}$ |
| $SO(2\mathbb{H})$<br>9 Classes of Tori | $\{e_1,\ f_1,\ e_2,\ f_2\}$ |
| $2F(\sqrt{\varepsilon}),\ (\frac{1}{2}, \frac{1}{2})$ | $\{\zeta_1[(1,0),(0,i)],\ \zeta_\varepsilon[(0,i\sqrt{\varepsilon}),(\sqrt{\varepsilon},0)]\}$ |
| $2F(\sqrt{\varepsilon}),\ (\frac{1}{2}\varpi, \frac{1}{2}\varpi)$ | $\{\zeta_\varpi[(1,0),(0,i)],\ \zeta_{\varepsilon\varpi}[(0,i\sqrt{\varepsilon}),(\sqrt{\varepsilon},0)]\}$ |
| $F(\sqrt{\varepsilon}) \subset F(\sqrt{\varepsilon}, \sqrt{\varpi}),\ \frac{1}{4}\sqrt{\varepsilon}$ | $\{1,\ \sqrt{\varepsilon}^{-1},\ \sqrt{\varpi},\ -\sqrt{\varepsilon\varpi}^{-1}\}$ |
| $F(\sqrt{\varpi}) \subset F(\sqrt{\varepsilon}, \sqrt{\varpi}),\ \frac{1}{4}\sqrt{\varpi}$ | $\{1,\ \sqrt{\varpi}^{-1},\ \sqrt{\varepsilon},\ -\sqrt{\varepsilon\varpi}^{-1}\}$ |
| $F(\sqrt{\varepsilon\varpi}) \subset F(\sqrt{\varepsilon}, \sqrt{\varpi}),\ \frac{1}{4}\sqrt{\varepsilon\varpi}$ | $\{1,\ \sqrt{\varepsilon\varpi}^{-1},\ \sqrt{\varepsilon}^{-1},\ -\sqrt{\varpi}^{-1}\}$ |
| $2F(\sqrt{\varpi}),\ (\frac{1}{2}, \frac{1}{2})$ | $\{\zeta_1[(1,0),(0,i)],\ \zeta_\varpi[(0,i\sqrt{\varpi}),(\sqrt{\varpi},0)]\}$ |
| $2F(\sqrt{\varpi}),\ (\frac{1}{2}\varepsilon, \frac{1}{2}\varepsilon)$ | $\{\zeta_\varepsilon[(1,0),(0,i)],\ \zeta_{\varepsilon\varpi}[(0,i\sqrt{\varpi}),(\sqrt{\varpi},0)]\}$ |
| $2F(\sqrt{\varepsilon\varpi}),\ (\frac{1}{2}, \frac{1}{2})$ | $\{\zeta_1[(1,0),(0,i)],\ \zeta_{\varepsilon\varpi}[(0,i\sqrt{\varepsilon\varpi}),(\sqrt{\varepsilon\varpi},0)]\}$ |
| $2F(\sqrt{\varepsilon\varpi}),\ (\frac{1}{2}\varepsilon, \frac{1}{2}\varepsilon)$ | $\{\zeta_\varepsilon[(1,0),(0,i)],\ \zeta_{\varepsilon^2\varpi}[(0,i\sqrt{\varepsilon\varpi}),(\sqrt{\varepsilon\varpi},0)]\}$ |
| $SO(\langle 1, \varepsilon\rangle \perp \mathbb{H})$<br>4 Classes of Tori | $\{g_1,\ g_2,\ e_1,\ f_1\}$ |
| $F(\sqrt{\varepsilon}) \subset F(\sqrt[4]{\varepsilon}),\ \frac{1}{4}$ | $\{1,\ \sqrt{\varepsilon},\ -(\sqrt[4]{\varepsilon})^{-3},\ \sqrt[4]{\varepsilon^3}\}$ |
| $F(\sqrt{\varepsilon}) \subset F(\sqrt[4]{\varepsilon\varpi^2}),\ \frac{1}{4}$ | $\{1,\ \sqrt{\varepsilon},\ -(\sqrt[4]{\varepsilon^3\varpi^2})^{-1},\ \sqrt[4]{\varepsilon^3\varpi^2}\}$ |
| $F(\sqrt{\varpi}) \oplus F(\sqrt{\varepsilon\varpi}),\ (\frac{1}{2}\varepsilon, \frac{1}{2})$ | $\{(0,1),\ (1,0),\ \zeta_{\varepsilon\varpi}[(0,i\sqrt{\varepsilon\varpi}),(\sqrt{\varpi},0)]\}$ |
| $F(\sqrt{\varpi}) \oplus F(\sqrt{\varepsilon\varpi}),\ (\frac{1}{2}, \frac{1}{2}\varepsilon)$ | $\{(1,0),\ (0,1),\ \zeta_\varpi[(0,i\sqrt{\varepsilon^{-1}\varpi}),(\sqrt{\varpi},0)]\}$ |
| $SO(\langle \varpi, \varepsilon\varpi\rangle \perp \mathbb{H})$<br>4 Classes of Tori | $\{g_1,\ g_2,\ e_1,\ f_1\}$ |
| $F(\sqrt{\varepsilon}) \subset F(\sqrt[4]{\varepsilon}),\ \frac{1}{4}\varpi$ | $\{1,\ \sqrt{\varepsilon},\ -\varpi^{-1}(\sqrt[4]{\varepsilon})^{-3},\ \sqrt[4]{\varepsilon^3}\}$ |
| $F(\sqrt{\varepsilon}) \subset F(\sqrt[4]{\varepsilon\varpi^2}),\ \frac{1}{4}\sqrt{\varepsilon}$ | $\{i\sqrt[4]{\varepsilon^{-1}\varpi^2},\ i\sqrt[4]{\varepsilon\varpi^2},\ \sqrt{\varepsilon}^{-1},\ 1\}$ |
| $F(\sqrt{\varpi}) \oplus F(\sqrt{\varepsilon\varpi}),\ (\frac{1}{2}, \frac{1}{2})$ | $\{(i\sqrt{\varpi},0),\ (0,i\sqrt{\varepsilon\varpi}),\ \zeta_1[(1,0),\ (0,i)]\}$ |
| $F(\sqrt{\varpi}) \oplus F(\sqrt{\varepsilon\varpi}),\ (\frac{1}{2}\varepsilon, \frac{1}{2}\varepsilon)$ | $\{(0,i\sqrt{\varepsilon^{-1}\varpi}),\ (i\sqrt{\varpi},0),\ \zeta_\varepsilon[(1,0),(0,i)]\}$ |

| $SO(\langle 1, \varpi\rangle \perp \mathbb{H})$<br>4 Classes of Tori | $\{g_1,\ g_2,\ e_1,\ f_1\}$ |
|---|---|
| $F(\sqrt{\varepsilon}) \oplus F(\sqrt{\varepsilon\varpi}),\ (\frac{1}{2}\varpi, \frac{1}{2})$ | $\{(0,1),\ (1,0),\ \zeta_{\varepsilon\varpi}[(0, i\sqrt{\varepsilon\varpi}), (\sqrt{\varepsilon}, 0)]\}$ |
| $F(\sqrt{\varepsilon}) \oplus F(\sqrt{\varepsilon\varpi}),\ (\frac{1}{2}, \frac{1}{2}\varepsilon)$ | $\{(1,0),\ (0, i\sqrt{\varepsilon^{-1}\varpi}),\ \zeta_{\varepsilon}[(0,1), (\sqrt{\varepsilon}, 0)]\}$ |
| $F(\sqrt{\varpi}) \subset F(\sqrt[4]{\varpi}),\ \frac{1}{4}$ | $\{1,\ \sqrt{\varpi},\ \sqrt[4]{\varpi},\ -\sqrt[4]{\varpi}^{-1}\}$ |
| $F(\sqrt{\varpi}) \subset F(\sqrt[4]{\varepsilon^2\varpi}),\ \frac{1}{4}$ | $\{1,\ \sqrt{\varpi},\ \sqrt[4]{\varepsilon^2\varpi},\ -\sqrt[4]{\varepsilon^2\varpi}^{-1}\}$ |
| $SO(\langle \varepsilon, \varepsilon\varpi\rangle \perp \mathbb{H})$<br>4 Classes of Tori | $\{g_1,\ g_2,\ e_1,\ f_1\}$ |
| $F(\sqrt{\varepsilon}) \oplus F(\sqrt{\varepsilon\varpi}),\ (\frac{1}{2}, \frac{1}{2})$ | $\{(i\sqrt{\varepsilon}, 0),\ (0, i\sqrt{\varepsilon\varpi}),\ \zeta_1[(1,0), (0,i)]\}$ |
| $F(\sqrt{\varepsilon}) \oplus F(\sqrt{\varepsilon\varpi}),\ (\frac{1}{2}\varpi, \frac{1}{2}\varepsilon)$ | $\{(0,1),\ (i\sqrt{\varepsilon}, 0),\ \zeta_{\varepsilon^2\varpi}[(\varepsilon, 0), (0, \sqrt{\varepsilon\varpi})]\}$ |
| $F(\sqrt{\varpi}) \subset F(\sqrt[4]{\varpi}),\ \frac{1}{4}\varepsilon$ | $\{1,\ \sqrt{\varpi},\ \sqrt[4]{\varpi},\ -(\varepsilon\sqrt[4]{\varpi})^{-1}\}$ |
| $F(\sqrt{\varpi}) \subset F(\sqrt[4]{\varepsilon^2\varpi}),\ \frac{1}{4}\varepsilon$ | $\{1,\ \sqrt{\varpi},\ \sqrt[4]{\varepsilon^2\varpi},\ -(\varepsilon\sqrt[4]{\varepsilon^2\varpi})^{-1}\}$ |
| $SO(\langle 1, \varepsilon\varpi\rangle \perp \mathbb{H})$<br>4 Classes of Tori | $\{g_1,\ g_2,\ e_1,\ f_1\}$ |
| $F(\sqrt{\varepsilon}) \oplus F(\sqrt{\varpi}),\ (\frac{1}{2}\varpi, \frac{1}{2})$ | $\{(0,1),\ (i\sqrt{\varepsilon}, 0),\ \zeta_{\varpi}[(1,0), (0, \sqrt{\varpi})]\}$ |
| $F(\sqrt{\varepsilon}) \oplus F(\sqrt{\varpi}),\ (\frac{1}{2}, \frac{1}{2}\varepsilon)$ | $\{(1,0),\ (0, i\sqrt{\varpi}),\ \zeta_{\varepsilon}[(0,1), (\sqrt{\varepsilon}, 0)]\}$ |
| $F(\sqrt{\varepsilon\varpi}) \subset F(\sqrt[4]{\varepsilon\varpi}),\ \frac{1}{4}$ | $\{1,\ \sqrt{\varepsilon\varpi},\ \sqrt[4]{\varepsilon\varpi},\ -\sqrt[4]{\varepsilon\varpi}^{-1}\}$ |
| $F(\sqrt{\varepsilon\varpi}) \subset F(\sqrt[4]{\varepsilon^3\varpi}),\ \frac{1}{4}$ | $\{1,\ \sqrt{\varepsilon\varpi},\ \sqrt[4]{\varepsilon^3\varpi},\ -\sqrt[4]{\varepsilon^3\varpi}^{-1}\}$ |
| $SO(\langle \varepsilon, \varpi\rangle \perp \mathbb{H})$<br>4 Classes of Tori | $\{g_1,\ g_2,\ e_1,\ f_1\}$ |
| $F(\sqrt{\varepsilon}) \oplus F(\sqrt{\varpi}),\ (\frac{1}{2}, \frac{1}{2})$ | $\{(i\sqrt{\varepsilon}, 0),\ (0, i\sqrt{\varpi}),\ \zeta_1[(1,0), (0,i)]\}$ |
| $F(\sqrt{\varepsilon}) \oplus F(\sqrt{\varpi}),\ (\frac{1}{2}\varpi, \frac{1}{2}\varepsilon)$ | $\{(0,1),\ (1,0),\ \zeta_{\varepsilon\varpi}[(0, i\sqrt{\varpi}), (\sqrt{\varepsilon}, 0)]\}$ |
| $F(\sqrt{\varepsilon\varpi}) \subset F(\sqrt[4]{\varepsilon\varpi}),\ \frac{1}{4}$ | $\{1,\ \sqrt{\varepsilon\varpi},\ \sqrt[4]{\varepsilon\varpi},\ -\sqrt[4]{\varepsilon\varpi}^{-1}\}$ |
| $F(\sqrt{\varepsilon\varpi}) \subset F(\sqrt[4]{\varepsilon^3\varpi}),\ \frac{1}{4}$ | $\{1,\ \sqrt{\varepsilon\varpi},\ \sqrt[4]{\varepsilon^3\varpi},\ -\sqrt[4]{\varepsilon^3\varpi}^{-1}\}$ |

Table 4.2: Maximal Elliptic Tori in $SO(V)$ when $\dim(V) = 4$ and $-1 \in F^{\times 2}$

Our notation in the above table remains consistent to that of Table 4.1. In this case, $-1 = i^2 \in F^{\times 2}$ and when $E/F$ is unramified we take $\varepsilon_E = \sqrt{\varepsilon}$; otherwise $\varepsilon_E = \varepsilon$. The map $\zeta_\lambda \colon V \times V \to V \times V$ performs a change of basis as per Definition 4.4.3. The groups $SO(\langle 1, \varepsilon\rangle \perp \mathbb{H}) \simeq SO(\langle \varpi, \varepsilon\varpi\rangle \perp \mathbb{H})$, $SO(\langle 1, \varpi\rangle \perp \mathbb{H}) \simeq SO(\langle \varepsilon, \varepsilon\varpi\rangle \perp \mathbb{H})$, and $SO(\langle 1, \varepsilon\varpi\rangle \perp \mathbb{H}) \simeq SO(\langle \varepsilon, \varpi\rangle \perp \mathbb{H})$ are isomorphic, and hence so are their tori.

## 4.5 The Full Classification of Tori when $-1 \notin F^{\times 2}$

We will now construct Witt bases in the case that $\varepsilon = -1 \notin F^{\times 2}$, setting $\sqrt{\varepsilon} = i$. We first remark that the field extensions $F(\sqrt[4]{\varpi}) \simeq F(\sqrt[4]{\varepsilon^2\varpi})$ and $F(\sqrt[4]{\varepsilon\varpi}) \simeq F(\sqrt[4]{\varepsilon^3\varpi})$ are isomorphic under these conditions, resulting in 4 fewer tori than when $-1 \in F^{\times 2}$.

Moreover, as in the preceding section, the groups

$$\begin{aligned} SO(\langle 1,1\rangle \perp \mathbb{H}) &\simeq SO(\langle \varpi,\varpi\rangle \perp \mathbb{H}) \\ SO(\langle 1,\varpi\rangle \perp \mathbb{H}) &\simeq SO(\langle -1,-\varpi\rangle \perp \mathbb{H}) \\ SO(\langle 1,-\varpi\rangle \perp \mathbb{H}) &\simeq SO(\langle -1,\varpi\rangle \perp \mathbb{H}) \end{aligned}$$

are isomorphic by Corollary 2.5.13, however, we will continue to sort the tori by the isometry class of the corresponding quadratic form.

Recall from Lemma 2.4.7 that when $E/F$ is unramified, we can set $\varepsilon_E = x + iy \in \mathcal{O}_E^\times$ as our non-square, for some $x, y \in F^{\times 2}$ such that $\mathrm{N}_{E/F}(\varepsilon_E) = -1$.

We will now explicitly take $x = s^2, y = t^2$ for some $s, t \in F^\times$ which are such that $\mathrm{N}_{E/F}(\varepsilon_E) = s^4 + t^4 = -1$.

When $-1 \notin F^{\times 2}$, the isometries of forms become more involved, hence so does the computation of Witt bases. For example, consider the equivalence $\langle 1,1\rangle \simeq \langle -1,-1\rangle$ and suppose $\{u, w\}$ is a diagonal basis for $\langle 1,1\rangle$. When $-1 \in F^{\times 2}$ (so $i \in F$), the simple basis change $\{u, w\} \to \{iu, iw\}$ yields a diagonal basis for $\langle -1,-1\rangle$. However, when $-1 \notin F^{\times 2}$ (so $i \notin F$), we instead must use the following lemma.

**Lemma 4.5.1.** *Let $s, t \in F$ be such that $s^4 + t^4 = -1$. Suppose the form $q$ over $V = F^2$ is given by $q(v_1u + v_2w) = v_1^2 + v_2^2$ for all $v_1, v_2 \in F$ with respect to some orthogonal vectors $u, w \in V$. Then $\{s^2u + t^2w, t^2u - s^2w\}$ is an orthogonal basis for the form $\langle -1,-1\rangle$.*

**Proof:** Take $g_1 = s^2u + t^2w, g_2 = t^2u - s^2w$ and let $(\ ,\ )$ denote the corresponding symmetric bilinear form to $q$. By definition of $u$ and $w$, we have that $(u,u) = 1 = (w,w)$ and $(u,w) = 0$. We need to show that the $g_i$ as defined are orthogonal and such that $(g_i, g_i) = -1$ for $i = 1, 2$. Indeed, since $s^4 + t^4 = -1$ we compute that

$$\begin{aligned} (g_1,g_1) &= s^4(u,u) + 2s^2t^2(u,w) + t^4(w,w) = s^4 + t^4 = -1 \\ (g_2,g_2) &= t^4(u,u) - 2s^2t^2(u,w) + s^4(w,w) = t^4 + s^4 = -1 \end{aligned}$$

as required. Furthermore, $(g_1, g_2) = s^2t^2(u,u) - s^4(u,w) + t^4(u,w) - s^2t^2(w,w) = 0$ and hence $\{g_1, g_2\}$ is an orthogonal basis for $\langle -1,-1\rangle$. ∎

We also will often need to compute a Witt basis for the 2-dimensional non-diagonal form $p(v_1, v_2) \simeq \langle 1,1\rangle$ defined in Lemma 2.5.6. The following result illustrates a valid choice to make.

**Lemma 4.5.2.** *Let $E/F$ be an unramified extension and set $\varepsilon_E = s^2 + it^2 \in \mathcal{O}_E^\times$ for some $s, t \in F$ such that $s^4 + t^4 = -1$. Suppose that the form $p$ is given by*

$$p(v_1u + v_2w) = -v_1^2s^2 + 2v_1v_2t^2 + v_2^2s^2$$

*for all $v_1, v_2 \in F$ with respect to some orthogonal vectors $u, w \in V = F^2$. Then, $\{su - t^2s^{-1}w, s^{-1}w\}$ is a Witt basis for $p$.*

**Proof:** Recall from Lemma 2.5.6 that $p$ has corresponding matrix $M_p = \begin{bmatrix} -s^2 & t^2 \\ t^2 & s^2 \end{bmatrix}$. Using a matrix $B = \begin{bmatrix} s & 0 \\ -t^2s^{-1} & s^{-1} \end{bmatrix} \in M_2(F)$, we can diagonalize $M_p$ as follows:

$$B^T M_p B = \begin{bmatrix} s & 0 \\ -t^2s^{-1} & s^{-1} \end{bmatrix}^T \begin{bmatrix} -s^2 & t^2 \\ t^2 & s^2 \end{bmatrix} \begin{bmatrix} s & 0 \\ -t^2s^{-1} & s^{-1} \end{bmatrix} = \begin{bmatrix} -(s^4+t^4) & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

since $s^4 + t^4 = -1$ by our initial assumption. Thus, since

$$B \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} s \\ -t^2s^{-1} \end{bmatrix} \text{ and } B \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ s^{-1} \end{bmatrix}$$

we see that $\{su - t^2s^{-1}w, s^{-1}w\}$ is an orthogonal basis for the form $\langle 1, 1\rangle$, and hence a Witt basis for $p$. ∎

We now define a map $\kappa$ corresponding to this change of basis in order to simplify notation in our table.

**Definition 4.5.3.** *Define a map $\kappa\colon V \times V \to V \times V$ by the relation $\kappa[u, w] := (su - t^2s^{-1}w, s^{-1}w)$.*

We now provide an example which requires use of both maps $\kappa$ and $\zeta_\lambda$ (as per Definition 4.4.3 of the previous section) in order to determine a suitable Witt basis for the torus. We will also provide the matrix representation of the torus in $SO(\langle\varpi, \varpi\rangle \perp \mathbb{H})$ up to conjugation by an explicit change of basis matrix $P_{\mathcal{B}\to\mathcal{B}_1^*} \in GL(V)$.

**Example 4.5.4.** Let $\varepsilon = -1 \notin F^{\times 2}$ and consider the chain of extensions $E = F(i) \subset F(\sqrt{\varepsilon_E\varpi}) \simeq E'$. As per Lemma 2.4.7, set $\varepsilon_E = s^2 + it^2$ for some $s, t \in F$ such that $\mathrm{N}_{E/F}(\varepsilon_E) = s^4 + t^4 = -1$.

As per Table 4.1, this extension yields two tori $T_1, T_2$ of the groups $SO(\langle\varpi, \varpi\rangle \perp \mathbb{H})$ and $SO(\langle 1, 1\rangle \perp \mathbb{H})$ respectively. We will first focus on $T_1$, corresponding to the choice $\mu_1 \sim \frac{1}{4}$. By Proposition 4.3.4, setting $\mu_1 = \frac{1}{4}$ produces a form $q_1$ with respect to the standard basis $\mathcal{B} = \{1, i, \sqrt{\varpi(s^2 + it^2)}, i\sqrt{\varpi(s^2 + it^2)}\}$ by

$$q_1\big(v_1 + v_2i + v_3\sqrt{\varpi(s^2 + it^2)} + v_4i\sqrt{\varpi(s^2 + it^2)}\big) = v_1^2 - v_2^2 + \varpi p(v_3, v_4)$$

for all $v_i \in F$, where $p$ denotes the quadratic form from Lemma 2.5.6 for $x = s^2, y = t^2$. Since $q_1 \simeq \langle \varpi, \varpi \rangle \perp \mathbb{H}$, we want to find a Witt basis $\mathcal{B}_1^* = \{g_1, g_2, e_1, f_1\}$ consisting of vectors in $E'$ such that $q_1(g_1) = \varpi = q(g_2)$ and $q_1(ae_1 + bf_1) = 2ab$ for all $a, b \in F$, with all other combinations zero.

We can use our change of basis maps to find a suitable $\mathcal{B}_1^*$. Indeed, by Lemma 4.4.2 we can take $(e_1, f_1) = \zeta_1[1, i]$, and by Lemma 4.5.2 we can take $(g_1, g_2) = \kappa[\sqrt{\varpi(s^2 + it^2)}, i\sqrt{\varpi(s^2 + it^2)}]$. Thus,

$$\mathcal{B}_1^* = \{\kappa[\sqrt{\varpi(s^2 + it^2)}, i\sqrt{\varpi(s^2 + it^2)}], \zeta_1[1, i]\}$$

is a Witt basis for $q_1$. Recall from previous discussion, the proof of Proposition 2.3.4 allows us to write any element $u$ of $E'^1$ as $u = v_1 + v_2 i + v_3\sqrt{\varpi(s^2 + it^2)} + v_4 i\sqrt{\varpi(s^2 + it^2)}$ for some $v_i \in \mathcal{O}$ (since here $\mathcal{B} = \mathcal{C}$). We then can compute that

$$M_{[u]_\mathcal{B}} = \begin{bmatrix} v_1 & -v_2 & \varpi(v_3 s^2 - v_4 t^2) & -\varpi(v_3 t^2 + v_4 s^2) \\ v_2 & v_1 & \varpi(v_3 t^2 + v_4 s^2) & \varpi(v_3 s^2 - v_4 t^2) \\ v_3 & -v_4 & v_1 & -v_2 \\ v_4 & v_3 & v_2 & v_1 \end{bmatrix}.$$

The change of basis matrix from $\mathcal{B}$ to $\mathcal{B}_1^*$ is a block matrix $P_{\mathcal{B}\to\mathcal{B}_1^*} \in GL(V)$ of the form

$$P_{\mathcal{B}\to\mathcal{B}_1^*} = \begin{bmatrix} 0 & A_\kappa \\ A_\zeta & 0 \end{bmatrix}, \text{ where } A_\kappa = \begin{bmatrix} s^{-1} & 0 \\ t^2 s^{-1} & s \end{bmatrix} \text{ and } A_\zeta = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 1 & -1 \end{bmatrix}.$$

Therefore, the torus $T_1$ of $SO(\langle \varpi, \varpi \rangle \perp \mathbb{H})$ is given by

$$T_1 = \left\{ P_{\mathcal{B}\to\mathcal{B}_1^*} \cdot M_{[u]_\mathcal{B}} \cdot (P_{\mathcal{B}\to\mathcal{B}_1^*})^{-1} \;\middle|\; \begin{array}{r} v_1, v_2, v_3, v_4 \in \mathcal{O} \\ v_1^2 - v_2^2 + \varpi p(v_3, v_4) = 1 \\ 2v_1 v_2 + \varpi(-v_3^2 t^2 - 2v_3 v_4 s^2 + v_4^2 t^2) = 0 \end{array} \right\}$$

where the additional restrictions arise from $u$ being a norm 1 element of $E'$.

We now consider the second torus $T_2$ of the extension $E' \simeq F(\sqrt{\varpi(s^2 + it^2)})$, corresponding to $\mu_2 \sim \frac{1}{4}(s^2 + it^2)$. This torus lies in the group $SO(\langle 1, 1 \rangle \perp \mathbb{H})$ and due to the complexity of $\mu_2$, involves heavy computation to find a suitable basis. Indeed, our map $\kappa$ will be used once again, however, we will also need to find a hyperbolic Witt basis $\{e_1, f_1\}$ for the form given by $\tilde{p}(v_3, v_4) \coloneqq x^2(v_4^2 - v_3^2) + 4v_3 v_4 xy - y^2(v_4^2 - v_3^2)$ from Proposition 4.3.4. As per our previous computations, the notation $x = s^2, y = t^2$ will be implemented.

**Example 4.5.5.** Let us now compute a Witt basis for the torus $T_2$ corresponding to the chain of extensions $E = F(i) \subset F(\sqrt{\varpi(s^2 + it^2)}) \simeq E'$ and choice $\mu_2 = \frac{1}{4}\varepsilon_E = \frac{1}{4}(s^2 + it^2)$. Recall, these parameters yield the form

$$q_2(v_1 + v_2 i + v_3\sqrt{\varpi(s^2 + it^2)} + v_4 i\sqrt{\varpi(s^2 + it^2)}) = p(-v_2, v_1) + \varpi\tilde{p}(v_3, v_4)$$

for all $v_i \in F$, where $\tilde{p}(v_3, v_4) \coloneqq s^4(v_4^2 - v_3^2) + 4v_3v_4s^2t^2 - t^4(v_4^2 - v_3^2) \simeq \mathbb{H}$. Let our Witt basis be denoted by $\mathcal{B}_2^* = \{g_1, g_2, e_1, f_1\}$. As per our previous computations, we can take $(g_1, g_2) = \kappa[i, -1]$, however, we need to find a hyperbolic pairing $\{e_1, f_1\}$ for the form $\tilde{p}$. The matrix corresponding to $\tilde{p}$ is given by

$$M_{\tilde{p}} = \begin{bmatrix} t^4 - s^4 & 2s^2t^2 \\ 2s^2t^2 & -(t^4 - s^4) \end{bmatrix}.$$

By defining a matrix $C = \begin{bmatrix} s^2 - t^2 & -\frac{1}{2}(s^2 + t^2) \\ -(s^2 + t^2) & -\frac{1}{2}(s^2 - t^2) \end{bmatrix} \in M_2(F)$ we see that

$$C^T M_{\tilde{p}} C = \begin{bmatrix} 0 & (s^4 + t^4)^2 \\ (s^4 + t^4)^2 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

since $s^4 + t^4 = -1$. Thus, $C$ transforms $M_{\tilde{p}}$ into its desired state, and hence we can use the column vectors of $C$ and the standard basis $\mathcal{B}$ to find a suitable pair $\{e_1, f_1\}$. Indeed, the basis

$$\mathcal{B}_{\tilde{p}} = \left\{(s^2-t^2)\sqrt{\varepsilon_E\varpi} - (s^2+t^2)i\sqrt{\varepsilon_E\varpi},\ -\frac{1}{2}(s^2+t^2)\sqrt{\varepsilon_E\varpi} - \frac{1}{2}(s^2-t^2)i\sqrt{\varepsilon_E\varpi}\right\} \quad (4.5.1)$$

for $\varepsilon_E = s^2 + it^2$ is a Witt basis of $\tilde{p} \simeq \mathbb{H}$; therefore $\mathcal{B}_2^* = \{\kappa[i, -1], \mathcal{B}_{\tilde{p}}\}$. The change of basis matrix from $\mathcal{B}$ to $\mathcal{B}_2^*$ is a block matrix $P_{\mathcal{B}\to\mathcal{B}_2^*}$ of the form

$$P_{\mathcal{B}\to\mathcal{B}_2^*} = \begin{bmatrix} A'_\zeta & 0 \\ 0 & C^{-1} \end{bmatrix}, \text{ where } A'_\zeta = \begin{bmatrix} 0 & s^{-1} \\ -s & t^2s^{-1} \end{bmatrix} \text{ and } C \text{ is as defined above.}$$

Thus, the toral subgroup $T_2$ of $SO(\langle 1, 1\rangle \perp \mathbb{H})$ is given by

$$T_2 = \left\{ P_{\mathcal{B}\to\mathcal{B}_2^*} \cdot M_{[u]_\mathcal{B}} \cdot (P_{\mathcal{B}\to\mathcal{B}_2^*})^{-1} \;\middle|\; \begin{array}{r} v_1, v_2, v_3, v_4 \in \mathcal{O} \\ v_1^2 - v_2^2 + \varpi p(v_3, v_4) = 1 \\ 2v_1v_2 + \varpi(-v_3^2t^2 - 2v_3v_4s^2 + v_4^2t^2) = 0 \end{array} \right\}.$$

We are now ready to present our computed Witt bases in the case when $\varepsilon = -1 \notin F^{\times 2}$. As mentioned previously, the quadratic forms for this section required more intricate changes of basis than in §4.4, as illustrated by Lemmas 4.5.1 and 4.5.2, as well as by Example 4.5.5 and the production of $\mathcal{B}_{\tilde{p}}$.

Our computations may be verified using the identical process described in §4.4; through the use of Algorithm 1 or 2, or via the explicit formulas for the quadratic forms given in the proofs of the propositions from §4.3. The resulting form when written with respect to the Witt basis provided should be exactly the form $q$ in the header $SO(q)$ of Table 4.3.

| $E \subset E', \mu$ | Witt Basis of $E'/F$ |
|---|---|
| $SO(\langle 1,1,\varpi,\varpi\rangle)$<br>8 Classes of Tori | $\{g_1,\ g_2,\ g_3,\ g_4\}$ |
| $2F(i),\ (\frac{1}{2},\frac{1}{2}\varpi)$ | $\{(1,0),\ (i,0),\ (0,1),\ (0,i)\}$ |
| $F(i)\subset F(i,\sqrt{\varpi}),\ \frac{1}{4}(s^2+it^2)$ | $\{\kappa[i,-1],\ \kappa[\sqrt{\varpi},i\sqrt{\varpi}]\}$ |
| $F(\sqrt{\varpi})\subset F(i,\sqrt{\varpi}),\ \frac{1}{4}$ | $\{1,\ i,\ \sqrt{\varpi},\ i\sqrt{\varpi}\}$ |
| $F(i\sqrt{\varpi})\subset F(i,\sqrt{\varpi}),\ \frac{1}{4}$ | $\{1,\ i,\ is^2\sqrt{\varpi}-t^2\sqrt{\varpi},\ it^2\sqrt{\varpi}+s^2\sqrt{\varpi}\}$ |
| $2F(\sqrt{\varpi}),\ (\frac{1}{2},\frac{1}{2})$ | $\{(1,0),\ (0,1),\ (s^2\sqrt{\varpi},t^2\sqrt{\varpi}),\ (t^2\sqrt{\varpi},-s^2\sqrt{\varpi})\}$ |
| $2F(\sqrt{\varpi}),\ (-\frac{1}{2},-\frac{1}{2})$ | $\{(s^2,t^2),\ (t^2,-s^2),\ (\sqrt{\varpi},0),\ (0,\sqrt{\varpi})\}$ |
| $2F(i\sqrt{\varpi}),\ (\frac{1}{2},\frac{1}{2})$ | $\{(1,0),\ (0,1),\ (i\sqrt{\varpi},0),\ (0,i\sqrt{\varpi})\}$ |
| $2F(i\sqrt{\varpi}),\ (-\frac{1}{2},-\frac{1}{2})$ | $\{(s^2,t^2),\ (t^2,-s^2),\ (is^2\sqrt{\varpi},it^2\sqrt{\varpi}),\ (it^2\sqrt{\varpi},-is^2\sqrt{\varpi})\}$ |
| $SO(2\mathbb{H})$<br>7 Classes of Tori | $\{e_1,\ f_1,\ e_2,\ f_2\}$ |
| $2F(i),\ (\frac{1}{2},\frac{1}{2})$ | $\{\zeta_1[(i,0),(s^2,t^2)],\ \zeta_1[(0,i),(t^2,-s^2)]\}$ |
| $2F(i),\ (\frac{1}{2}\varpi,\frac{1}{2}\varpi)$ | $\{\zeta_\varpi[(i,0),(s^2,t^2)],\ \zeta_\varpi[(0,i),(t^2,-s^2)]\}$ |
| $F(i)\subset F(i,\sqrt{\varpi}),\ \frac{1}{4}$ | $\{\zeta_1[1,i],\ \zeta_\varpi[\sqrt{\varpi},i\sqrt{\varpi}]\}$ |
| $F(\sqrt{\varpi})\subset F(i,\sqrt{\varpi}),\ \frac{1}{4}\sqrt{\varpi}$ | $\{1,\ i,\ \sqrt{\varpi}^{-1},\ i\sqrt{\varpi}^{-1}\}$ |
| $F(i\sqrt{\varpi})\subset F(i,\sqrt{\varpi}),\ \frac{1}{4}i\sqrt{\varpi}$ | $\{1,\ i,\ -i\sqrt{\varpi}^{-1},\ \sqrt{\varpi}^{-1}\}$ |
| $2F(\sqrt{\varpi}),\ (\frac{1}{2},-\frac{1}{2})$ | $\{\zeta_1[(1,0),(0,1)],\ \zeta_\varpi[(0,\sqrt{\varpi}),(\sqrt{\varpi},0)]\}$ |
| $2F(i\sqrt{\varpi}),\ (\frac{1}{2},-\frac{1}{2})$ | $\{\zeta_1[(1,0),(0,1)],\ \zeta_\varpi[(0,i\sqrt{\varpi}),(i\sqrt{\varpi},0)]\}$ |
| $SO(\langle 1,1\rangle\perp\mathbb{H})$<br>4 Classes of Tori | $\{g_1,\ g_2,\ e_1,\ f_1\}$ |
| $F(i)\subset F(\sqrt{s^2+it^2}),\ \frac{1}{4}$ | $\{\kappa[\sqrt{s^2+it^2},i\sqrt{s^2+it^2}],\ \zeta_1[1,i]\}$ |
| $F(i)\subset F(\sqrt{\varpi(s^2+it^2)}),\frac{1}{4}(s^2+it^2)$ | $\{\kappa[i,-1],\ \mathcal{B}_{\tilde{p}}\}$ |
| $F(\sqrt{\varpi})\oplus F(i\sqrt{\varpi}),\ (\frac{1}{2},\frac{1}{2})$ | $\{(1,0),\ (0,1),\ \zeta_\varpi[(0,i\sqrt{\varpi}),(\sqrt{\varpi},0)]\}$ |
| $F(\sqrt{\varpi})\oplus F(i\sqrt{\varpi}),\ (-\frac{1}{2},-\frac{1}{2})$ | $\{(s^2,t^2),\ (t^2,-s^2),\ \zeta_\varpi[(\sqrt{\varpi},0),(0,i\sqrt{\varpi})]\}$ |
| $SO(\langle\varpi,\varpi\rangle\perp\mathbb{H})$<br>4 Classes of Tori | $\{g_1,\ g_2,\ e_1,\ f_1\}$ |
| $F(i)\subset F(\sqrt{s^2+it^2}),\ \frac{1}{4}\varpi$ | $\{\kappa[\sqrt{s^2+it^2},i\sqrt{s^2+it^2}],\ \zeta_\varpi[1,i]\}$ |
| $F(i)\subset F(\sqrt{\varpi(s^2+it^2)}),\ \frac{1}{4}$ | $\{\kappa[\sqrt{\varpi(s^2+it^2)},i\sqrt{\varpi(s^2+it^2)}],\ \zeta_1[1,i]\}$ |
| $F(\sqrt{\varpi})\oplus F(i\sqrt{\varpi}),\ (-\frac{1}{2},\frac{1}{2})$ | $\{(\sqrt{\varpi},0),\ (0,i\sqrt{\varpi}),\ \zeta_1[(0,-1),(1,0)]\}$ |
| $F(\sqrt{\varpi})\oplus F(i\sqrt{\varpi}),\ (\frac{1}{2},-\frac{1}{2})$ | $\{(s^2\sqrt{\varpi},it^2\sqrt{\varpi}),\ (t^2\sqrt{\varpi},-is^2\sqrt{\varpi}),\ \zeta_1[(1,0),(0,-1)]\}$ |

| $SO(\langle 1,\varpi\rangle \perp \mathbb{H})$<br>3 Classes of Tori | $\{g_1,\ g_2,\ e_1,\ f_1\}$ |
|---|---|
| $F(i)\oplus F(\sqrt{\varpi}),\ (\frac{1}{2}\varpi,\frac{1}{2})$ | $\{(0,1),\ (1,0),\ \zeta_\varpi[(i,0),(0,\sqrt{\varpi})]\}$ |
| $F(i)\oplus F(\sqrt{\varpi}),\ (\frac{1}{2},-\frac{1}{2})$ | $\{(i,0),\ (0,\sqrt{\varpi}),\ \zeta_1[(1,0),(0,1)]\}$ |
| $F(\sqrt{\varpi})\subset F(\sqrt[4]{\varpi}),\ \frac{1}{4}$ | $\{1,\ \sqrt{\varpi},\ \sqrt[4]{\varpi},\ -\sqrt[4]{\varpi}^{-1}\}$ |
| $SO(\langle -1,-\varpi\rangle \perp \mathbb{H})$<br>3 Classes of Tori | $\{g_1,\ g_2,\ e_1,\ f_1\}$ |
| $F(i)\oplus F(\sqrt{\varpi}),\ (\frac{1}{2},\frac{1}{2})$ | $\{(s^2,t^2),\ (0,\sqrt{\varpi}),\ \zeta_1[(i,0),(t^2,-s^2)]\}$ |
| $F(i)\oplus F(\sqrt{\varpi}),\ (\frac{1}{2}\varpi,-\frac{1}{2})$ | $\{(0,1),\ (s^2,t^2\sqrt{\varpi}),\ \zeta_\varpi[(i,0),(t^2,-s^2\sqrt{\varpi})]\}$ |
| $F(\sqrt{\varpi})\subset F(\sqrt[4]{\varpi}),\ -\frac{1}{4}$ | $\{1,\ \sqrt{\varpi},\ \sqrt[4]{\varpi},\ \sqrt[4]{\varpi}^{-1}\}$ |
| $SO(\langle 1,-\varpi\rangle \perp \mathbb{H})$<br>3 Classes of Tori | $\{g_1,\ g_2,\ e_1,\ f_1\}$ |
| $F(i)\oplus F(i\sqrt{\varpi}),\ (\frac{1}{2}\varpi,\frac{1}{2})$ | $\{(0,1),\ (s^2,it^2\sqrt{\varpi}),\ \zeta_\varpi[(i,0),(t^2,-is^2\sqrt{\varpi})]\}$ |
| $F(i)\oplus F(i\sqrt{\varpi}),\ (\frac{1}{2},-\frac{1}{2})$ | $\{(i,0),\ (0,i\sqrt{\varpi}),\ \zeta_1[(1,0),(0,1)]\}$ |
| $F(i\sqrt{\varpi})\subset F(\sqrt[4]{-\varpi}),\ \frac{1}{4}$ | $\{1,\ i\sqrt{\varpi},\ \sqrt[4]{-\varpi},\ \sqrt[4]{-\varpi}^{-1}\}$ |
| $SO(\langle -1,\varpi\rangle \perp \mathbb{H})$<br>3 Classes of Tori | $\{g_1,\ g_2,\ e_1,\ f_1\}$ |
| $F(i)\oplus F(i\sqrt{\varpi}),\ (\frac{1}{2},\frac{1}{2})$ | $\{(it^2,-s^2),\ (0,i\sqrt{\varpi}),\ \zeta_1[(1,0),(is^2,t^2)]\}$ |
| $F(i)\oplus F(i\sqrt{\varpi}),\ (\frac{1}{2}\varpi,-\frac{1}{2})$ | $\{(0,1),\ (1,0),\ \zeta_\varpi[(i,0),(0,i\sqrt{\varpi})]\}$ |
| $F(i\sqrt{\varpi})\subset F(\sqrt[4]{-\varpi}),\ -\frac{1}{4}$ | $\{1,\ i\sqrt{\varpi},\ \sqrt[4]{-\varpi},\ -\sqrt[4]{-\varpi}^{-1}\}$ |

Table 4.3: Maximal Elliptic Tori in $SO(V)$ when $\dim(V)=4$ and $-1\notin F^{\times 2}$

Our notation in the above table remains consistent to that of Table 4.1. Without loss of generality, we have taken $\varepsilon=-1\notin F^{\times 2}$ and $\sqrt{\varepsilon}=i$. When $E/F$ is unramified, we set $\varepsilon_E=s^2+it^2\in\mathcal{O}_E^\times$ to be such that $\mathrm{N}_{E/F}(\varepsilon_E)=-1$; otherwise $\varepsilon_E=-1$. The maps $\zeta_\lambda,\kappa\colon V\times V\to V\times V$ perform changes of basis as per Definitions 4.4.3 and 4.5.3 respectively, and $\mathcal{B}_{\bar{p}}$ is the Witt basis stated in (4.5.1). The groups $SO(\langle 1,1\rangle \perp \mathbb{H})\simeq SO(\langle \varpi,\varpi\rangle \perp \mathbb{H})$, $SO(\langle 1,\varpi\rangle \perp \mathbb{H})\simeq SO(\langle -1,-\varpi\rangle \perp \mathbb{H})$, and $SO(\langle 1,-\varpi\rangle \perp \mathbb{H})\simeq SO(\langle -1,\varpi\rangle \perp \mathbb{H})$ are isomorphic and we also remark that the field extensions $F(\sqrt[4]{\varpi})\simeq F(\sqrt[4]{\varepsilon^2\varpi})$ and $F(\sqrt[4]{\varepsilon\varpi})\simeq F(\sqrt[4]{\varepsilon^3\varpi})$ are isomorphic, which results in 4 fewer non-conjugate tori than in Table 4.2.

By adapting theory from Morris into modern language and generalizing the methods implemented by Kim and Yu for the symplectic group, we have thus obtained an exhaustive list of the non-conjugate toral subgroups of all degree 4 special orthogonal groups, as listed above. Beyond this, we have also provided the concrete embedding of each torus into the group via a choice of Witt basis, offering many possible future directions for research on this topic.

# Bibliography


[Adl98] Jeffrey D. Adler. *Refined Anisotropic K-types and Supercuspidal Representations*. Pacific Journal of Mathematics. **185**(1), 1–32, 1998.

[Ash13] Robert B. Ash. *Basic Abstract Algebra: For Graduate Students and Advanced Undergraduates*. Courier Corporation, 2013.

[BJN94] Phani B. Bhattacharya, Surender K. Jain, and S.R. Nagpaul. *Basic Abstract Algebra*. Cambridge University Press, 1994.

[BK93] Colin J. Bushnell and Philip C. Kutzko. *The Admissible Dual of GL(N) via Compact Open Subgroups*. Volume 129 of *Annals of Mathematics Studies*, Princeton University Press, Princeton, NJ, 1993.

[Bor91] Armand Borel. *Linear Algebraic Groups*. Volume 126 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, Second Edition, 1991.

[Coh12] Paul M. Cohn. *Basic Algebra: Groups, Rings and Fields*. Springer Science & Business Media, 2012.

[DeB06] Stephen DeBacker. *Parameterizing Conjugacy Classes of Maximal Unramified Tori via Bruhat-Tits Theory*. The Michigan Mathematical Journal. **54**(1), 157–178, 2006.

[DF04] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Volume 3, Wiley Hoboken, New York, 2004.

[DK12] Yurj A. Drozd and Vladimir V. Kirichenko. *Finite Dimensional Algebras*. Springer Science & Business Media, 2012.

[Fin17] Jessica Fintzen. *Types for tame p-adic groups*. Annals of Mathematics. Second Series. **193**(1), 303–346, 2017.

[FV02] Ivan B. Fesenko and Sergei V. Vostokov. *Local Fields and their Extensions*. Volume 121 of *American Mathematical Society*, 2002.

[Gou97] Fernando Q. Gouvêa. *p-adic Numbers*. Universitext. Springer-Verlag, Berlin, Second Edition, 1997.

[HGK04] Michiel Hazewinkel, Nadiya Gubareni, and Vladimir V. Kirichenko. *Algebras, Rings and Modules*. Volume 1, Springer Science & Business Media, 2004.

[HM08] Jeffrey Hakim and Fiona Murnaghan. *Distinguished Tame Supercuspidal Representations*. International Mathematics Research Papers. IMRP. (2), 2008.

[How77] Roger E. Howe. *Some Qualitative Results on the Representation Theory of GL(n) over a p-adic field*. Pacific Journal of Mathematics. **73**(2), 479–538, 1977.

[Kim07] Ju-Lee Kim. *Supercuspidal Representations: An Exhaustion Theorem*. Journal of the American Mathematical Society. **20**(1), 273–320, 2007.

[Kob12] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Volume 58, Springer Science & Business Media, 2012.

[KY11] Ju-Lee Kim and Jiu-Kang Yu. Twisted Levi Sequences and Explicit Types on Sp(4). In *Harmonic analysis on reductive, p-adic groups*, volume 543 of *American Mathematical Society*, pages 135–154. Contemporary Mathematics, 2011.

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

[Lan13] Serge Lang. *Algebraic Number Theory*. Volume 110, Springer Science & Business Media, 2013.

[Mar91] Gregori A Margulis. *Discrete Subgroups of Semisimple Lie Groups*. Volume 17, Springer Science & Business Media, 1991.

[Mor91] Lawrence Morris. *Some Tamely Ramified Supercuspidal Representations of Symplectic Groups*. Proceedings of the London Mathematical Society. **3**(3), 519–551, 1991.

[PR01] Sebastian Pauli and Xavier-François Roblot. *On the Computation of all Extensions of a p-adic field of a Given Degree*. Mathematics of Computation. **70**(236), 1641–1659, 2001.

[Rot12] Joseph J. Rotman. *Galois Theory*. Universitext. Springer, New York, 2012.

[Tai75] M. H. Taibleson. *Fourier Analysis on Local Fields*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1975.

[TZ15] D.M. Testerman and A.E. Zalesski. *Subgroups of Simple Algebraic Groups Containing Regular Tori, and Irreducible Representations with Multiplicity 1 non-zero Weights*. Transformation Groups. **20**(3), 831–861, 2015.

[Yu01] Jiu-Kang Yu. *Construction of Tame Supercuspidal Representations*. Journal of the American Mathematical Society. **14**(3), 579–622, 2001.