Algebraic Properties of Quadrics over Finite Fields and their Symmetry Groups

Bachelorarbeit aus der Physik

Vorgelegt von
Ludwig Peschik

27.02.2019

Institut für Theoretische Physik I
Friedrich-Alexander-Universität Erlangen-Nürnberg

Betreuer: Prof. Dr. Klaus Mecke

Contents

1 Introduction

Since its publication Einstein's *General Relativity* has been one of the most influential classical works in the past century. It combines properties of the considered matter with the geometry of the background spacetime upon the matter exists. A few decades later the standard model of particle physics grew in acceptance due to its experimental verification which showed that a quantization of matter in the context of quantum field theory is necessary to describe all the fundamental interactions between particles on very tiny scales. Therefore, in the last decades scientist have been trying to combine the quantum nature of matter with the classical theory of general relativity.

In a new approach by Klaus Mecke the field of real numbers is discarded as the underlying number field of the theory in favour of a finite field and a projective space equipped with a biquadric is used instead of a Lorentzian spacetime manifold. Herein, the four-dimensionality of the directly observable universe and the signature of the Minkwoski metric come up quite naturally.

In this thesis we want to study some algebraic properties of the standard quadric used in this new approach and, in particular, of the symmetry group of this quadric. This symmetry group is in close relation to the Lorentz group used in special relativity but we will see that it has some features which come up by using a finite field and a projective space instead of real numbers and a smooth manifold, respectively. In particular, we will discuss the application of the Cartan-Dieudonné theorem which describes a decomposition of the elements of such symmetry groups into reflections whose geometrical interpretation is a lot easier than the one of a general element of the symmetry group. At the end we also want to sketch an idea of finding a connection between the structure of the quadric and a field extension of the finite field.

2 Mathematical Background

Before we can get into the more physical theory, we need to recall, introduce and explain some mathematical concepts and notions upon which the topics of this thesis are based.

In the following we will discuss finite fields, quadratic forms over finite fields, in particular the number of solutions of a quadratic equation, projective spaces, projective quadrics over finite fields, orthogonal matrices and the Cartan-Dieudonné theorem.

We will assume a basic exposure to topics of (linear) algebra but nevertheless recall some mandatory definitions and theorems whose proofs can be found, e. g., in [6] or [7].

2.1 Groups

Before we may study properties of the Lorentz group which will later be defined, we need to define and discuss the concept of a *group*. Groups can be found in many very different subjects of interest, e. g., the addition of real numbers or in symmetry groups used in, e. g., quantum field theory, and are defined as follows.

Definition 2.1.1.

1. *A* ***group*** $(G, *)$ *is a set* G *equipped with a binary operation* $* : G \times G \to G$*, called multiplication, satisfying the following conditions:*
   a) *Associativity:* $\forall g, h, k \in G : (g * h) * k = g * (h * k)$*,*
   b) *Neutral Element:* $\exists\, e \in G : \forall g \in G : e * g = g * e = g$*,*
   c) *Inverses:* $\forall g \in G\ \exists\, h \in G : g * h = h * g = e$*, notation:* $g^{-1} := h$*.*
2. *A group* G *is called* ***abelian*** *if* $\forall g, h \in G : g * h = h * g$*. The operation* $*$ *is then said to be* ***commutative****.*
3. *The number of elements of* G *is called* ***order*** *of* G*, denoted* $|G|$*. If* $|G| = n < \infty$*,* G *is called* ***finite group of order*** n*.*
4. *A subset* $H \subseteq G$ *is called* ***subgroup*** *if* $(H, *_H)$ *forms a group by restricting* $*$ *to elements of* H*. If* $H \neq G$*,* H *is said to be a* ***proper*** *subgroup of* G*.*

Example 2.1.2.

1. *Integers with addition* $(\mathbb{Z}, +)$ *are an abelian group of infinite order.*
2. *The real numbers* $(\mathbb{R}, +)$ *equipped with addition form an abelian group of infinite order.*
3. *Invertible* $n \times n$*-matrices* $GL\,(n, \mathbb{R}) := \{M \in Mat(n \times n, \mathbb{R}) \mid \exists\, M^{-1} \in Mat(n \times n, \mathbb{R})\}$ *with entries in* $\mathbb{R}$ *with standard matrix multiplication form a non-abelian group of infinite order for* $n > 1$*.*
4. *Integers modulo* n $\mathbb{Z}/n\mathbb{Z}$ *equipped with addition modulo* n *form a finite abelian group.*

Remark 2.1.3. *It is common to use + as the symbol for a commutative group multiplication. Herein the inverse of an element g is usually denoted $-g$.*

To study properties of groups it is useful to use maps between different groups G and H which preserve the structure of both. These are called *group homomorphisms* and are defined as follows.

Definition 2.1.4. *Let $(G, *)$ and $(H, \cdot)$ be groups.*

1. *A map $\varphi : G \to H$ is called a* ***group homomorphism*** *if $\forall g, h \in G : \varphi(g * h) = \varphi(g) \cdot \varphi(h)$.*

2. *If φ is bijective, it is called a* ***group isomorphism****.*

3. *If $H = G$, a group homomorphism is called a* ***group endomorphism*** *and an group isomorphism is called* ***group automorphism****.*

4. *If there exists a group isomorphism between two groups G and H, they a are said to be* ***isomorphic****, denoted $G \cong H$.*

If two groups are isomorphic, they cannot be distinguished by tools of group theory, i. e., they have the same properties as groups. This can be understood by thinking about isomorphic groups as merely a re-labelling of the elements. This is often useful if one of the groups is well established such that we can reduce the study of a possibly more abstract group to an already studied group to which it is isomorphic.

Let us recall the definition of a finite-dimensional vector space V over a field $\mathbb{K}$. $(V, +)$ has to be an abelian group which is compatible with scalar multiplication of elements of $\mathbb{K}$. Since V is finite-dimensional, there exists a finite basis of V whose linear combinations form the whole vector space. An analogue of the concept of a basis can be formulated for groups by so-called *generators*. As in the case of vector spaces, this can simplify the study of properties of the whole space by reducing it to a few special elements of it.

Definition 2.1.5. *A group G is called* ***finitely generated*** *if there exists a finite subset $M \subset G, |M| < \infty$, such that $\{g_1 g_2 \cdots g_n \mid n \in \mathbb{N}_0, \forall i \in \{1, \ldots, n\} : g_i \in M \cup M^{-1}\} = G$ with $M^{-1} := \{g^{-1} \mid g \in M\}$ and $g_1 g_2 \cdots g_n = e$ for $n = 0$. Elements of M are called* ***generators*** *and we write $G = \langle M \rangle$. If $|M| = 1$, G is said to be* ***cyclic****.*

Example 2.1.6. *An easy example of a cyclic group is the group $(\mathbb{Z}, +)$ of integers which is generated by $1 \in \mathbb{Z}$. This means that every $z \in \mathbb{Z}$ can be written as a finite sum of either 1 or -1: $n = \underbrace{1 + \cdots + 1}_{n \text{ times}}$ and $-n = \underbrace{(-1) + \cdots + (-1)}_{n \text{ times}}$*

There are many quite useful theorems about cyclic groups. We want to list two of them here.

Theorem 2.1.7. *Let G be a cyclic group. Then one of the following holds:*

1. $G \cong (\mathbb{Z}, +)$ *if* $|G| = \infty$,

2. $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$ *if* $|G| = n < \infty$.

In particular, every cyclic group is abelian.

Both $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ which is generated by the equivalence class of 1, are well-known and well understood, so instead of thinking about an abstract cyclic group G, one may w.l.o.g. assume $G \in \{\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}\}$.

Theorem 2.1.8. *Subgroups of cyclic groups are cyclic.*

2.2 Finite Fields

The next concept we want to introduce, is a generalization of the idea of "numbers": the concept of *fields*. Fields are commonly used in most branches of mathematics and, of course, in physics. Usually, physicists tend to refer to the fields of real or complex numbers $\mathbb{R}$ or $\mathbb{C}$, respectively, to perform their calculations. Now, we want to take a step back and abstract from the usual operations done with real numbers to get to the bones of a field. We will see that other types of fields can behave very differently compared to $\mathbb{R}$ or $\mathbb{C}$.

Definition 2.2.1. *A* ***field*** $(\mathbb{K}, +, \cdot)$ *is a set with two binary operations* $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$, $(a, b) \mapsto a + b$ *and* $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}, (a, b) \mapsto a \cdot b =: ab$ *such that the following axioms are satisfied:*

1. Associativity:

$$\forall a, b, c \in \mathbb{K} : (a + b) + c = a + (b + c) \textit{ and}$$
$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

2. Existence of Neutral Elements:

$$\exists\, a \in \mathbb{K} : \forall k \in \mathbb{K} : a + k = k + a = k, \textit{ notation: } a =: 0, \textit{ and}$$
$$\exists\, b \in \mathbb{K}\backslash\{0\} : \forall k \in \mathbb{K} : b \cdot k = k \cdot b = k, \textit{ notation: } b =: 1$$

3. Existence of Inverses:

$$\forall k \in \mathbb{K} : \exists\, g : k + g = g + k = 0, \textit{ notation: } g =: -k, \textit{ and}$$
$$\forall k \in \mathbb{K}\backslash\{0\} : \exists\, f : k \cdot f = f \cdot k = 1, \textit{ notation: } f =: k^{-1}$$

4. Commutativity:

$$\forall k, h \in \mathbb{K} : k + h = h + k \textit{ and}$$
$$\forall k, h \in \mathbb{K} : k \cdot h = h \cdot k$$

5. Distributivity:

$$\forall k, h, g \in \mathbb{K} : k \cdot (h + g) = k \cdot h + k \cdot g.$$

A field $(\mathbb{K}, +, \cdot)$ is called ***finite*** *if $\mathbb{K}$ as a set has a finite number of elements, denoted $|\mathbb{K}|$. If $|\mathbb{K}| = q \in \mathbb{N}$, we write $\mathbb{K} = \mathbb{F}_q$ and call it* ***finite field of order q****.*

Remark 2.2.2.

1. *With the notion of groups and $\mathbb{K}^\times := \mathbb{K}\backslash\{0\}$ this definition may be rewritten as follows. Both $(\mathbb{K}, +)$ and $(\mathbb{K}^\times, \cdot)$ form an abelian group and are compatible in the sense of distributivity.*

2. *It can be proven that the groups $(\mathbb{K}, +)$ and $(\mathbb{K}^\times, \cdot)$ are cyclic for a finite field $\mathbb{K}$.*

3. *The concept of group homomorphisms can be translated to field homomorphism which preserve both the additive and the multiplicative structure and map 0 to 0 and 1 to 1. The other notions are analogous.*

The concept of a field should be very familiar since one of the prime examples for an infinite field is the field of real numbers $\mathbb{R}$. Another well-known example are integers modulo p, p prime, denoted $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\} = \{\overline{-\frac{p-1}{2}}, \dots, \overline{\frac{p-1}{2}}\}$ where $\overline{a}$ represents the equivalence class of a in $\mathbb{Z}/p\mathbb{Z}$.

Definition 2.2.3. *The* ***characterstic*** *char$(\mathbb{K})$ of a field $\mathbb{K}$ is defined as the smallest $n \in \mathbb{N}$ such that $\underbrace{1 + \cdots + 1}_{n\times} = 0$ if such a number n exists, and 0 otherwise.*

One can immediately see that $\mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{C}) = 0$ and $\mathrm{char}(\mathbb{F}_p) = p$.

When studying finite sets of order q, one will observe that not every $q \in \mathbb{N}$ allows a finite field. This fact is stated in the following theorem whose proof can be found in [7]. As before, we will refer to [7] for most of the upcoming theorems, facts and proofs.

Theorem 2.2.4. *A finite field $\mathbb{F}_q$ has prime power order, i. e., $q = p^r$ with p prime and $r \in \mathbb{N}$.*

Since there are possibly many different fields of a given order, the following theorem is useful to classify fields of a given order and, when restricting to purely prime order, to find a field with an easy use in calculations.

Theorem 2.2.5. *Finite fields of the same order are isomorphic.*

This means that instead of an arbitrary, possibly very abstract field of order p, p prime, we can use a more suitable field of the same order, e. g., $\mathbb{Z}/p\mathbb{Z}$ in our calculations. In the following we will use $\mathbb{F}_p$ for a prime field of order p, p prime, and $\mathbb{F}_q$ for a general finite field of prime power order.

2.3 Field Extensions and Galois Theory

If $\mathbb{F}_q$ is a field of order $q = p^r$, p prime, $r \in \mathbb{N}$, the field $\mathbb{F}_p \subseteq \mathbb{F}_q$ is called **prime field** of $\mathbb{F}_q$, i. e., the field which has no proper, i. e., strictly smaller subfields. $\mathbb{F}_q$ can also be understood as an extension field of $\mathbb{F}_p$ of degree r and, thus, as an r-dimensional vector space over $\mathbb{F}_p$. The concept of a field extension can be formulated for arbitrary fields and is a useful tool to construct new fields from already known ones.

It should be noted that the characteristic of a subfield is the same as the characteristic of the larger field. This means that the characteristic is not changed by a field extension.

Definition 2.3.1. *A field $\mathbb{L}$ is called an **extension field** of a field $\mathbb{K}$ if it contains $\mathbb{K} \subseteq \mathbb{L}$ as a subfield, i. e., $\mathbb{K} \subseteq \mathbb{L}$ forms a field with operations obtained by restricting the operations of $\mathbb{L}$ to $\mathbb{K}$. This construction is referred to as **field extension** and denoted by $\mathbb{L}/\mathbb{K}$. The **degree** of a field extension, denoted $[\mathbb{L} : \mathbb{K}]$, is the dimension of $\mathbb{L}$ as a vector space over $\mathbb{K}$. The extension is said to be **finite** if the degree $[\mathbb{L} : \mathbb{K}]$ of the extension is finite.*

Example 2.3.2. *A well-known example of an extension field in the infinite case is the field of complex numbers $\mathbb{C}$ as a field extension of $\mathbb{R}$ of degree 2. This is done by adjoining a root of the polynomial $p = X^2 + 1 \in \mathbb{R}[X]$ which is irreducible in $\mathbb{R}[X]$, i. e., $p \in \mathbb{R}[X]$ is non-constant and $\nexists\, q, r \in \mathbb{R}[X]$, q, r non-constant: $p = q \cdot r$. This root is denoted i and usually called imaginary unit. Now, the field of complex numbers $\mathbb{C}$ is given as $\mathbb{R}(i)$ which means that $\mathbb{C}$ is the smallest field extension containing i and $\mathbb{R}$.*

This procedure is completely analogous to taking the quotient ring $\mathbb{R}[X]/(p)$ where (p) denotes the ideal in $\mathbb{R}[X]$ generated by $p \in \mathbb{R}[X]$. Since p is irreducible in $\mathbb{R}[X]$, the quotient ring $\mathbb{R}[X]/(p)$ forms a field and by taking $p = X^2 + 1$ it is isomorphic to $\mathbb{C}$.

By construction we can immediately see that $\{1, i\}$ forms a basis of $\mathbb{R}(i) = \mathbb{C}$ as a vector space over $\mathbb{R}$ since elements $z \in \mathbb{C}$ can be written as $z = x + yi$ with $x, y \in \mathbb{R}$. Thus, the degree $[\mathbb{C} : \mathbb{R}]$ of the extension is equal to 2. Furthermore, the degree of the polynomial p coincides with the degree of the field extension.

This recipe can be generalized and adapted to the case of finite fields.

Example 2.3.3. *If we want to construct a field $\mathbb{F}_q$ with $q = p^r$, p prime, $r \in \mathbb{N}$, we start by picking an irreducible polynomial $k \in \mathbb{F}_p[X]$ with $\deg(k) = r$. It can be shown that such a polynomial always exists in $\mathbb{F}_p[X]$. Then, by taking the quotient ring $\mathbb{F}_p[X]/(k)$ we have constructed a field. a so-called splitting field, of order $q = p^r$ which by theorem 2.2.5 is isomorphic to our desired field $\mathbb{F}_q$.*

This construction can be made more explicit. Since k has no roots in $\mathbb{F}_p$, we symbolize one of the roots with α. By adjoining the set $\{\alpha, \alpha^2, \dots, \alpha^{r-1}\}$ to the prime field $\mathbb{F}_p$ we get a field of order $q = p^r$. This can also be seen as constructing an r-dimensional vector space over $\mathbb{F}_p$ and referring to the base vectors as $\alpha^i, i \in \{0, \dots, r-1\}$. An element $a \in \mathbb{F}_q$ can be expanded in terms of α such that $a = x_0 + x_1 \cdot \alpha + x_2 \cdot \alpha^2 + \dots + x_{r-1} \cdot \alpha^{r-1}$ with $x_i \in \mathbb{F}_p$ $\forall i \in \{0, \dots, r-1\}$. All α^i commute with elements of $\mathbb{F}_p$ and multiplication in $\mathbb{F}_q$ is done by first multiplying in the usual sense and collecting all powers of α and afterwards reducing the powers of α by using the property $k(\alpha) = 0$.

A useful tool when studying finite field extensions is the so-called *Galois group*. Group-theoretic properties of it can be used to describe properties of the field extension. It has also a close connection to permutation groups which we will briefly discuss later.

Definition 2.3.4. *The **Galois group** $Gal(\mathbb{L}/\mathbb{K})$ of a field extension $\mathbb{L}/\mathbb{K}$ is the subgroup of the group of field automorphisms $Aut(\mathbb{L})$ of the field $\mathbb{L}$ which leaves all elements of $\mathbb{K} \subseteq \mathbb{L}$ invariant, i. e., $Gal(\mathbb{L}/\mathbb{K}) \coloneqq \{\varphi \in Aut(\mathbb{L}) \mid \forall k \in \mathbb{K} : \varphi(k) = k\}$. The field extension $\mathbb{L}/\mathbb{K}$ is said to be a **Galois extension** if $|Gal(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$.*

Remark 2.3.5. *If we consider a splitting field $\mathbb{L} \coloneqq \mathbb{K}[X]/(p)$ with $p \in \mathbb{K}[X]$ irreducible and $\deg(p) = n < \infty$, it can be shown that $Gal(\mathbb{L}/\mathbb{K})$ acts as a permutation group on the roots $\alpha^i, i \in \{1, \dots, r-1\}$ of p.*

Example 2.3.6. *Let us inspect an example, namely the field extension $\mathbb{C}/\mathbb{R}$. As discussed above, $\mathbb{C} \cong \mathbb{R}[X]/(p)$ with $p = X^2 + 1 \in \mathbb{R}[X]$. The roots of p are $\pm i$. The Galois group of $\mathbb{C}/\mathbb{R}$ is given by $Gal(\mathbb{C}/\mathbb{R}) = \{id, \varphi\}$ with $\varphi : \mathbb{C} \to \mathbb{C},\ z \mapsto \overline{z}$, the complex conjugation. It is obvious that $\forall x \in \mathbb{R} : id(x) = x = \varphi(x) = \overline{x}$. We can also immediately see that $\varphi^2 = id$ and $Gal(\mathbb{C}/\mathbb{R}) = \langle \varphi \rangle$, i. e., $Gal(\mathbb{C}/\mathbb{R})$ is generated by φ and, thus, cyclic. It is also quite easy to construct a map $|\cdot|^2 : \mathbb{C} \to \mathbb{C}$ whose image is invariant under $Gal(\mathbb{C}/\mathbb{R})$, i. e., $|\cdot|^2(\mathbb{C}) \subseteq \mathbb{R}$ by forming the point-wise product of the elements of the Galois group, i. e., $|z|^2 \coloneqq |\cdot|^2(z) \coloneqq (id \cdot \varphi)(z) \coloneqq id(z) \cdot \varphi(z) = z\overline{z},\ z \in \mathbb{C}$. It is straight forward to see that $|z|^2$ is invariant under the action of $Gal(\mathbb{C}/\mathbb{R})$ by using the fact that $\mathbb{C}$ is abelian and that $Gal(\mathbb{C}/\mathbb{R})$ is cyclic. $|z|^2$ is often referred to as the norm of z.*

Example 2.3.7. *The Galois group of a field extension simplifies when considering finite field extension of finite fields, i. e., fields of the form $\mathbb{F}_q$ with $q = p^r$, p prime and $r \in \mathbb{N}$. $Gal(\mathbb{F}_q/\mathbb{F}_p)$ is cyclic with r elements and is generated by the Frobenius map $\varphi : \mathbb{F}_q \to \mathbb{F}_q,\ x \mapsto x^p$, i. e., $Gal(\mathbb{F}_q/\mathbb{F}_p) = \{\varphi, \varphi^2, \dots, \varphi^{r-1}, \varphi^r = id\}$. By basic tools of algebra the reader may convince himself/herself that $\forall x \in \mathbb{F}_p^\times : x^{|\mathbb{F}_p^\times|} = x^{p-1} = 1$. This fact is sometimes referred to as "Fermat's little theorem". We can conclude that $\forall x \in \mathbb{F}_p : x^p = x^{p-1}x = 1 \cdot x = x$ and see that φ, indeed, fixes the subfield $\mathbb{F}_p \subseteq \mathbb{F}_q$.*

2.4 Quadratic Forms over Finite Fields

We want to get an analogue of the notion of distance on our spacetime which is usually given by a metric. At first we want to abstract from this concept and consider the polynomial ring $\mathbb{K}[X_0, \dots, X_{n-1}]$ of polynomials in n variables over the field $\mathbb{K}$.

Definition 2.4.1. *A **homogeneous polynomial of degree** k is a polynomial $p \in \mathbb{K}[X_0, \dots, X_{n-1}]$ such that each non-zero term of p is of degree k, i. e., the sum of exponents of the variables $X_0, \dots, X_{n-1}$ is equal to k.*

In the special case of $k = 2$ a homogeneous polynomial $p \in \mathbb{K}[X_0, \dots, X_{n-1}]$ may be represented by an $n \times n$-matrix $M \in \mathrm{Mat}(n \times n, \mathbb{K})$. Let $x = (X_0, \dots, X_{n-1}) \in \mathbb{K}^n$. Then M is defined by the equation $p(x) = x^T M x$. We will call M *representation matrix* of p and define the determinant $\det(p) \coloneqq \det(M)$.

Example 2.4.2. *Consider the quadratic form* $f(x_0, x_1) = x_0^2 + x_0x_1 + x_1^2$ *over a field* $\mathbb{K}$ *with* $char(\mathbb{K}) \neq 2$. $f(x_0, x_1) \overset{!}{=} (x_0, x_1)M(x_0, x_1)^T$ *for a* 2×2 *matrix* $M \in Mat(2 \times 2, \mathbb{K})$. *Then* M *is given by* $M = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$.

These homogeneous polynomials of degree 2 can be used to realize the following definition.

Definition 2.4.3. *Let* V *be a finite-dimensional vector space over the field* $\mathbb{K}$.
A ***quadratic form*** f *is a map* $f : V \to \mathbb{K}$ *such that* $\forall \lambda \in \mathbb{K}, v \in V : f(\lambda v) = \lambda^2 f(v)$.

We can immediately see that a quadratic form may be represented by a homogeneous polynomial of degree 2 with vanishing constant terms.

If we consider $\mathbb{K} = \mathbb{F}_q$, q odd prime power, to be a finite field, the following theorem provides a simplification to the study of quadratic forms.

Theorem 2.4.4. *Every quadratic form in* $n + 1$ *variables over* $\mathbb{F}_q$, q *odd, is equivalent to a diagonal quadratic form, i. e.,* $a_0x_0^2 + \cdots + a_nx_n^2$ *with* $a_0, \ldots, a_n \in \mathbb{F}_q$.

As we discussed, a quadratic form may be represented by a homogeneous polynomial of degree 2 which may be represented by an $n \times n$-matrix. Thus, this theorem tells us that the representation matrix can be brought into a diagonal form and we may assume w.l.o.g. that the quadratic form which we later will consider, is already diagonal. In the following we will assume the representation matrix to be *non-degenerate*, i. e., none of the $a_i, i \in \{0, \ldots n\}$, from the theorem above vanish.

Since a finite field is by definition finite, everything is countable. Thus, let us consider an equation of the form $f(x_0, \ldots, x_n) = b$ with f a non-degenerate quadratic form in $n + 1$ variables over $\mathbb{F}_q$ and $b \in \mathbb{F}_q$. The number of solutions $(x_0, \ldots, x_n) \in \mathbb{F}_q^{n+1}$ is not obvious since not every element in $\mathbb{F}_q$ needs necessarily to be a square, i. e., there might exist $a \in \mathbb{F}_q : \nexists r \in \mathbb{F}_q : r^2 = a$.

Therefore, we will introduce the so-called *Legendre symbols* which indicates whether an element $a \in \mathbb{F}_p$ is a square or not. Their values for small p can be found in the literature.

Definition 2.4.5. *Let* $a \in \mathbb{F}_p$ *with* p *prime.*
The ***Legendre symbol*** $\left(\frac{a}{p}\right)$ *is defined as*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \textit{if } a \textit{ is a square in } \mathbb{F}_p \textit{ and } a \neq 0 \in \mathbb{F}_p, \\ -1 & \textit{if } a \textit{ is a non-square in } \mathbb{F}_p, \textit{ and} \\ 0 & \textit{if } a = 0 \in \mathbb{F}_p. \end{cases}$$

For $b \in \mathbb{F}_q, q = p^r, r \in \mathbb{N}$, *we define the* ***Jacobi Symbol*** *as* $\left(\frac{b}{q}\right) = \left(\frac{b}{p}\right)^r$, *where on the right hand side the above defined Legendre symbol is used.*

A simple calculation shows that the Legendre symbol is multiplicative, i. e., $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Furthermore, a simple consideration shows that prime numbers $p \neq 2$ are either congruent to $1 \mod 4$ or $3 \mod 4$. It can be shown that only in the first case $a = -1$ is, indeed, a square. This can be used to prove that in a field $\mathbb{F}_p$ with $p \equiv 3 \mod 4$ either a or $-a$ is a square in $\mathbb{F}_p$.

Herewith, the number of solutions of the considered equation $f(x_0, \dots, x_n) = b$ with f a non-degenerate quadratic form over $\mathbb{F}_q$, q odd, in $n+1$ variables and $b \in \mathbb{F}_q$ can be explicitly given in the cases of n being odd or even [7, p. 282f].

Theorem 2.4.6.

1. *For $b \in \mathbb{F}_q$ and f a non-degenerate quadratic form over $\mathbb{F}_q$ in n variables the number of the solutions of the equation $f(x_1, \dots, x_n) = b$, n **even**, is*

$$q^{n-1} + \nu(b) q^{(n-2)/2} \eta\left((-1)^{n/2}\Delta\right),$$

where $\nu : \mathbb{F}_q \to \mathbb{Z}$, $\nu(b) = -1$ for $b \in \mathbb{F}_q \backslash \{0\}$ and $\nu(b) = q-1$ for $b = 0$, η is the quadratic character of $\mathbb{F}_q$ which coincides with the Jacobi symbol, and $\Delta = \det(f)$.

2. *For $b \in \mathbb{F}_q$ the number of the solutions of the equation $f(x_1, \dots, x_n) = b$, n **odd**, is*

$$q^{n-1} + q^{(n-1)/2} \eta\left((-1)^{(n-1)/2} b\Delta\right),$$

where η is the quadratic character of $\mathbb{F}_q$ and $\Delta = \det(f)$.

This theorem will later be used to calculate, e. g., the number of possible solutions of entries in an orthogonal group and the number of points in a so-called *quadric* which will be discussed later.

2.5 Projective Spaces and Quadrics over Finite Fields

Instead of using a usual vector space of the form $\mathbb{K}^n$ for a field $\mathbb{K}$ we want to introduce so-called *projective spaces* $\mathrm{P}\mathbb{K}^n$ which have some interesting additional properties and are in a sense more symmetric. They will also be a useful tool to define *quadrics* which will give a notion of distance and provide a "measure" for neighbourhood. We refer to Artin's book [1] for a more in-depth study of projective geometry and orthogonal groups.

Definition 2.5.1. *Let $\mathbb{K}$ be a field and V an $(n+1)$-dimensional vector space over $\mathbb{K}$.*

*A **projective space** $\mathrm{P}\mathbb{K}^n$ of dimension n is defined as the quotient space $(V\backslash\{0\})/\sim$, where the equivalence relation $\sim$ is defined as $x \sim y \iff x = \lambda y$ for $\lambda \in \mathbb{K}^\times$, $x, y \in V$.*

Equivalently, we may define $\mathrm{P}\mathbb{K}^n$ as the space whose points are the lines in V through the origin, i. e., $\mathrm{P}\mathbb{K}^n = \{\langle x\rangle |\ 0 \neq x \in V\}$, where $\langle x\rangle$ denotes the line generated by $x \in V$, i. e., $\langle x\rangle = \{v \in V \mid v = tx, t \in \mathbb{K}\}$.

Remark 2.5.2. *A projective space can also be constructed by adding hyperplanes at infinity to an affine $\mathbb{K}$-space A which may be embedded in an $(n+1)$-dimensional vector space V. These hyperplanes at infinity, denoted H^∞, are the lines, planes, ... that are parallel to $A \subset V$ if A is considered as a hyperplane in V. Points in $\mathrm{P}\mathbb{K}^n$ are then given by the intersection of the hyperplane with lines through the origin of V.This procedure gives a decomposition of the projective space in terms of lower dimensional vector spaces which can be transformed into the affine spaces by an affine transformation: $\mathrm{P}\mathbb{K}^n = \mathbb{K}^n \cup \mathbb{K}^{n-1} \cup \cdots \cup \mathbb{K}^1 \cup \mathbb{K}^0$.*

Thus, we may also work with points in the affine space and use the coordinates of them in the vector space V with the additional restriction that two points are equivalent if and only if their coordinate representation differs only by a multiplicative non-zero factor $\lambda \in \mathbb{K}^\times$.

The idea should be the following. If we "move" the affine space along a perpendicular line through the origin and consider the intersection of this translated space with a line through the origin, this will lead to the same point in the projective space as the intersection of the same line through the origin and the original affine space.

Hence, we may define a new coordinate representation which intrinsically captures this property.

Definition 2.5.3. *Let $\mathbb{K}$ be a field, V an $(n+1)$-dimensional vector space over $\mathbb{K}$ and $\mathrm{P}\mathbb{K}^n$ an n-dimensional projective space over $\mathbb{K}$.*

The ***homogeneous coordinates*** *of $x \in \mathrm{P}\mathbb{K}^n$, denoted $[x_0 : \cdots : x_n]$, are the coordinates of $y \in V$ with $\langle y \rangle = x$ with the property $[\lambda x_0 : \cdots : \lambda x_n] = [x_0 : \cdots : x_n], \lambda \in \mathbb{K}^\times$.*

The notation $[x_0 : \cdots : x_n]$ underlines the property of the equivalence relation defining the projective space, i. e., that a common factor in front of all coordinates can simply be neglected and only the quotients of them have significant meaning. Therefore, when working with affine coordinates we may always choose $x_n = 1$ for a point x in the affine space. Points in the hyperplanes at infinity are then given by setting the last $k, k \in \{1, \ldots, n\}$, coordinates to zero and the last non-vanishing coordinate $x_{n-k} = 1$.

The setting of a projective space is very suitable to define so-called *quadrics.* These are often considered as generalizations of conic sections, e. g., circles, ellipses, hyperbolae. In the case of $\mathbb{K} = \mathbb{R}$ this gives a good geometrical interpretation of this algebraic structure. Since finite fields are, unlike $\mathbb{R}$, not continuous and not naturally ordered, this interpretation fails in the case of $\mathbb{K} = \mathbb{F}_q$. Nevertheless, it can provide a basic idea of the properties and purposes of quadrics.

Definition 2.5.4. *A* ***(projective) quadric*** *Q is the zero-locus of one quadratic form in an n-dimensional projective space $\mathrm{P}\mathbb{K}^n$, i. e., $Q = \{x \in \mathrm{P}\mathbb{K}^n \mid f(x) = 0\}$ where f is a quadratic form in $n+1$ variables over $\mathbb{K}$.*

Remark 2.5.5.

1. *It should be noted that a quadratic form is necessary and cannot be replaced by an ordinary second-order polynomial since it has to be homogeneous to be well-defined*

as a function on the projective space $\mathrm{P}\mathbb{K}^n$: Let $f(x) = 0,\ x \in \mathrm{P}\mathbb{K}^n$. Then, for $x = [x_0 : \cdots : x_n]$, we get $f(\lambda x) = f(\lambda x_0, \ldots, \lambda x_n) = \lambda^2 f(x_0, \ldots, x_n), \lambda \in \mathbb{K}^\times \implies (f(\lambda x) = 0 \iff f(x) = 0)$ which is suitable since $\mathrm{P}\mathbb{K}^n \ni x = [x_0, \ldots, x_n] = [\lambda x_0, \ldots, \lambda x_n]$ in homogeneous coordinates.

2. *Since by earlier consideration every quadratic form in $n+1$ variables may be represented by a $(n+1) \times (n+1)$-matrix $M \in Mat((n+1) \times (n+1), \mathbb{K})$, the quadric Q is given by $Q = \{x \in \mathrm{P}\mathbb{K}^n \mid x^T M x = 0\}$. Thus, the quadric Q may be represented by the matrix M.*

3. *It can be shown that for the finite case $\mathbb{K} = \mathbb{F}_p$ in even dimension n there is only one type of quadric which can be represented by either of the two canonical forms $M = diag(-1, 1, \ldots, 1, \pm g^2)$ with $g \in \mathbb{F}_p^\times$ [9]. For $g = 1$ we will call M standard (Minkowski) form, denoted $\eta^\pm$, based on the Minkowski metric used in special relativity.*

Based on the use of a metric in classical Riemannian geometry a quadric Q will later define points with a given distance to a centre point $c \in \mathrm{P}\mathbb{K}^n$ which is defined with respect to a given hyperplane at infinity in the following way. Let H_N^∞ be the normal covector of a hyperplane at infinity H^∞, i. e., $\forall h \in H^\infty : H_N^\infty h = 0$ with usual vector-covector multiplication, and M be the representation matrix of the quadric Q, then $c^T = H_N^\infty (M^{-1})^T$. Usually, $H_N^\infty = (0, \ldots, 0, 1)$ is chosen for convenience.

2.6 Orthogonal Matrices and Cartan-Dieudonné Theorem

If we consider a quadratic form f in $n+1$ variables, we may ask whether a given coordinate transformation $\phi : \mathrm{P}\mathbb{K}^n \to \mathrm{P}\mathbb{K}^n$ leaves the quadratic form invariant if considered as a function on $\mathrm{P}\mathbb{K}^n$, i. e., $\forall x \in \mathrm{P}\mathbb{K}^n : f(\phi(x)) = f(x)$. In terms of the representation matrix M of f this translates to the question if for a given $O \in \mathrm{Mat}((n+1) \times (n+1), \mathbb{K})$ with $\det(O) \neq 0$ the equation $O^T M O = M$ holds. It should be noted that matrices acting on the projective space $\mathrm{P}\mathbb{K}^n$ are only defined up to a non-zero scalar factor as in the case of elements of the projective space.

Since f is considered to be non-degenerate, its representation matrix M can be identified with a representation matrix of a non-degenerate *bilinear form* $B : \mathbb{K}^{n+1} \times \mathbb{K}^{n+1} \to \mathbb{K}$, i. e., for $x, y \in \mathbb{K}^{n+1} : B(x, y) := x^T M y$. B has to be linear in both arguments, i. e., $\forall x, y, z \in \mathbb{K}^{n+1}, \lambda \in \mathbb{K} : B(x + \lambda y, z) = B(x, z) + \lambda B(y, z)$ and analogously for the second argument. If M is symmetric, the bilinear form B is also symmetric, i. e., $\forall x, y \in \mathbb{K}^{n+1} : B(x, y) = B(y, x)$. Thus, we may use the notion of *orthogonal matrices* to describe the symmetries of the quadratic form f.

Definition 2.6.1. *Let V be an n-dimensional vector space over a field $\mathbb{K}$ and let $B : V \times V \to \mathbb{K}$ be a symmetric bilinear form.*

*The **orthogonal group** O_B of the bilinear form B is defined as the subgroup of V-endomorphisms which leave B invariant, i. e., $O_B := \{\phi \in End(V) \mid \forall x, y \in V : B(\phi(x), \phi(y)) = B(x, y)\}$.*

Remark 2.6.2.

1. *For a symmetric bilinear form B on an n-dimensional vector space V the orthogonal group O_B is, in fact, a subgroup of $Aut(V)$, the group of automorphism of V.*

2. *If $M \in Mat(n \times n, \mathbb{K})$ is the representation matrix of B and $F \in Mat(n \times n, \mathbb{K})$ is the representation matrix of $\phi \in O_B$, then F is invertible with $F^{-1} = M^{-1}F^TM = M^{-1}(MF)^T = (MFM^{-1})^T$ since B and, thus, M and M^{-1} is considered to be symmetric. That is because in the matrix representation the property for a matrix $F \in Mat(n \times n, \mathbb{K})$ to be an element of O_B is given by $F^TMF = M$.*

Example 2.6.3. *Consider the standard Euclidean scalar product $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ on $\mathbb{R}^n$ which is defined as follows: For $x, y \in \mathbb{R}^n : \langle x, y \rangle := \sum_{i=1}^n x_i y_i$.*

The orthogonal group $O_{\langle \cdot, \cdot \rangle}$ acting on $\mathbb{R}^n$ is known as the orthogonal group $O(n)$. In the special case of $n = 2$ its matrix representation is given by matrices $M \in Mat(2 \times 2, \mathbb{R})$ of the form $M = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \pm\sin(\varphi) & \pm\cos(\varphi) \end{pmatrix}$ for some $\varphi \in \mathbb{R}$. These can be interpreted geometrically as rotations or reflections about the origin of the plane of $\mathbb{R}^2$ depending on the sign of the determinant of M.

As the example showed, reflections about a fixed vector or point are a special case of orthogonal matrices and can be generalized to arbitrary symmetric bilinear forms. These are known as *Householder matrices.*

Definition 2.6.4. *Let V be an n-dimensional vector space over the field $\mathbb{K}$, $B : V \times V \to \mathbb{K}$ be a symmetric bilinear form on V and $M \in Mat(n \times n, \mathbb{K})$ its matrix representation.*

The ***Householder reflection*** *$S_v : V \to V$ with respect to a vector $v \in V \backslash \{0\}$ is given by its action on an arbitrary vector $w \in V$:*

$$S_v(w) = w - \frac{2}{B(v,v)} B(v,w)v.$$

Its representation matrix is called ***Householder matrix*** *and is given by*

$$S_v = I_n - \frac{2}{v^TMv} vv^TM,$$

where I_n denotes the identity matrix in n dimensions.

Remark 2.6.5.

1. *The vector v in the above definition is orthogonal to the hyperplane of reflection, i. e., it is a normal vector of the hyperplane with respect to the symmetric bilinear form B.*

2. *These maps are called reflections because of the following property. Consider a fixed vector $v \in V$. If another vector $w \in V$ is orthogonal to v, i. e., $B(v, w) = 0$, and w is, thus, in the hyperplane of reflection, then the action of the householder reflection is given by $S_v(w) = w$. If we consider the action of S_v on v, we get $S_v(v) = v - 2v = -v$. This means that S_v has the eigenvalue $+1$ with multiplicity 1 and an eigenvalue -1 with multiplicity $n - 1$ where n is the dimension of the underlying vector space V. In a sense, it reverts the sign of all vector in the 1-dimensional subspace spanned by $v \in V$ and leaves the orthogonal rest invariant.*

3. *A simple calculation shows that S_v is, indeed, an orthogonal matrix with respect to the bilinear form B, i. e., $B(S_v(w), S_v(z)) = B(w, z)\ \forall w, z \in V$ or $S_v^T M S_v = M$ in the matrix representation.*

4. *Since the determinant of a matrix is the product of its eigenvalues, reflections S_v have* $\det(S_v) = -1$.

These maps are of special interest since their geometrical interpretation over a general field $\mathbb{K}$ is much easier than of a general orthogonal V-automorphism. Furthermore, they can be used to decompose every element of an orthogonal group and are, thus, generators of this orthogonal group. An upper limit for the number of such reflections is given by the following theorem which was first proven in the real and complex case by Cartan [2] and later for a general field by Dieudonné [4].

Theorem 2.6.6 (Cartan-Dieudonné)**.** *Let V be an n-dimensional vector space over a field $\mathbb{K}$ with char$(\mathbb{K}) \neq 2$ and let $B : V \times V \to \mathbb{K}$ be a non-degenerate symmetric bilinear form on V.*

Then, every element of the orthogonal group O_B is a composition of at most n reflections.

This theorem tells us that such a decomposition is always possible over an arbitrary field with characteristic not being 2 and for every symmetric bilinear form and we can see the number of reflections is limited by the dimension of the vector space on which it acts. Thus, if the dimension is even, the number of reflections which are necessary for the decomposition of $A \in O_B$ with $\det(A) = -1$ is lowered by 1 since the determinant of a reflection is -1 and the determinant is multiplicative. Analogously, in the case of odd dimension n every $C \in O_B$ with $\det(C) = 1$ can be written as the product of at most $n - 1$ reflections.

3 Symmetries of Projective Quadrics over Finite Fields

In the following we want to discuss two special subgroups of the symmetry group of the standard quadric which is the orthogonal group corresponding to the standard Minkowski form $\eta\pm$, namely Lorentz transformation and what we will call gauge transformations, in a $(n = 1 + 1)$- and a $(n = 1 + 3)$-dimensional projective space $\mathrm{P}\mathbb{F}_p^n$ over a finite field $\mathbb{F}_p$, p prime. For simplicity, we will always assume $p > 3$ such that $p > \dim_{\mathbb{F}_p}(\mathrm{P}\mathbb{F}_p^n) = n$.

At first, we start by taking an n-dimensional projective space $\mathrm{P}\mathbb{F}_p^n$ over a finite field $\mathbb{F}_p$. In contrast to a usual vector space, a projective space has some advantageous properties since, for example, translations can be formulated linearly. Furthermore, as we have seen in remark 2.5.2, a projective space of given dimension is a union of equally- and lower-dimensional vector spaces. Thus, it has more degrees of freedom than a usual vector space of the same dimension.

A finite field $\mathbb{F}_p, p$ prime, $p \equiv 3 \mod 4$ such that -1 is not a square, is considered because on one hand it gives the space built upon it an intrinsic discretization which could in principle be very useful for a description of a quantum world, in particular of quantum gravity. On the other hand, as shown in the previous Chapter, finite fields have peculiar properties which we are not used to when working with the field of real numbers $\mathbb{R}$, e. g., that there exist "positive" numbers that are not a square in $\mathbb{F}_p$ such as $p - 1 = -1$ in $\mathbb{F}_p, p \equiv 3 \mod 4$. In particular, $\mathbb{R}$ is filled with many assumptions and a lot of structure, such as topological closure or infinitely small elements which led to the definition of derivatives and unpleasing infinities. THus, the use of finite fields may lead to a better understanding of the conceptual structure of a description of the universe and the physics in it.

If we consider an event-based interpretation of this physical space described by a projective space where points are actually events and reoccurring events make up objects, it seems quite natural to impose the condition that every point should have at least two neighbours, a previous and a subsequent event. This condition is easily satisfied when imposing a quadratic form (field) on the projective space. As we have seen, the choice of a finite field as the underlying field of the projective space yields (locally) the standard Minkowski form $\eta^\pm$ as representation for the quadratic form. Therefore, the special role of one of the coordinates, usually associated with time, comes quite naturally in contrast to postulate such a form in special relativity.

Let us summarize this construction at this point. We consider an n-dimensional projective space $\mathrm{P}\mathbb{F}_p^n$ over a finite field $\mathbb{F}_p, p \equiv 3 \mod 4, p > 3$ prime. On this projective space we impose for the above mentioned reason a quadratic form which can locally be transformed into the standard Minkowski form $\eta^\pm = \mathrm{diag}(-1, 1, \ldots, 1, \pm 1)$ in matrix representation [3]. This structure will then be called *spacetime* and its first component will be called *time* and the next $n - 1$ components will be referred to as *space*. If we consider the zero-loci of $\eta^\pm$, respectively, we get two standard quadrics $Q^\pm$ which can be shown to be equivalent with $Q^\pm := \{x \in \mathrm{P}\mathbb{F}_p^n \mid x^T \eta^\pm x = 0\}$. The elements $x \in Q^\pm$ with $x_n \neq 0$, i. e., points in the intersection of the affine plane with the quadric, can be thought of as time- or space-like unit vectors when comparing it to the concepts used in special relativity. But, since we consider a projective space, there is even structure contained in these quadrics. If we consider a point in a hyperplane at infinity which is an element of the quadric, it can be understood as a light-like vector when considering the standard of using $n-1$ coordinates, and, thus, is part of the light cone spanned at the centre of the quadric. In the later discussion we will choose as a toy model a $(1+1)$-dimensional spacetime and afterwards a $(1+3)$-dimensional spacetime equipped with the standard Minkowski form. The dimension 4 is used since it can be shown that higher dimensions cannot be directly observed in such a spacetime [9].

In order to get a better understanding of the structure of the quadric, we consider those linear transformations which leave the quadric invariant, i. e., the orthogonal group corresponding to the symmetric bilinear form $\eta^{\pm}$ which defines the quadric. These vector space automorphisms are defined on the $(n+1)$-dimensional vector space which underlies the projective space $\mathrm{P}\mathbb{F}_p^n$ used in the construction of our spacetime. As in the construction of the projective space, two linear transformations are identified if they only differ by a non-zero factor and, likewise, their matrix representation. Thus, we may always set one of the entries of the matrix to unity. This can be used to define two subgroups of the full orthogonal group, namely the subgroup of Lorentz transformations in analogy to the Lorentz group usually considered in special relativity which leaves the distance of two points invariant, and, additionally, the group of gauge transformations which leave invariant the coordinate of time. Both will be discussed and in accordance to the Cartan-Dieudonné theorem decomposed in the two cases mentioned above.

3.1 Lorentz Transformations

The first subgroup of the orthogonal group $O_{\eta^{\pm}}$ of the standard Minkowski form $\eta^{\pm}$ we want to consider, is the subgroup of Lorentz transformations.

Definition 3.1.1. *Let $\eta^{\pm}$ be the standard Minkowski form on an n-dimensional projective space $\mathrm{P}\mathbb{F}_p^n$ with p prime, $p \equiv 3 \mod 4$, and $O_{\eta^{\pm}}$ the corresponding orthogonal group.*

*A **Lorentz transformation** Λ is an Element $\Lambda \in O_{\eta^{\pm}}$ which leaves the last coordinate of a point invariant, i. e., the matrix representation of Λ is given by $\begin{pmatrix} L & 0 \\ 0 & 1 \end{pmatrix}$ with $L \in Mat(n \times n, \mathbb{F}_p)$.*

*A Lorentz transformation is called **proper** if its determinant is equal to 1. Otherwise it is called **improper**.*

Remark 3.1.2.

1. *The $n \times n$ matrix L which we will call **reduced Lorentz matrix** has to satisfy a reduced equation in contrast to the Lorentz transformation Λ in the above definition, namely*
$$L^T M L = M$$
with $M = diag(-1, 1, \ldots, 1) \in Mat(n \times n, \mathbb{F}_p)$ as in special relativity with the difference of the used field.

2. *One can easily verify that the set of Lorentz transformations acting on an finite dimensional projective space forms a group when equipped with the usual composition of maps or standard matrix multiplication for their matrix representation. The group of Lorentz transformations acting on an n-dimensional projective space over the finite field $\mathbb{F}_p$ is denoted $L(n,p)$.*

   In particular, the set of proper Lorentz transformations is a subgroup of this group because the determinant is multiplicative. This group is then denoted $L^+(n,p)$.

3. *Furthermore, since we have already set one of the entries in the matrix to unity, there is no projective freedom in the reduced Lorentz matrix.*

Now, we want to specify the structure of these Lorentz transformation in their matrix representation or for short, these Lorentz matrices in two special cases. At first, we will consider a $(1+1)$-dimensional spacetime as our toy model. Afterwards, we will consider the "full" $(1+3)$-dimensional spacetime.

3.1.1 Lorentz Transformations in (1+1)-dimensional Projective Spacetime

Theorem 3.1.3. *The group $L(2,p)$ of Lorentz transformations on $\mathrm{P}\mathbb{F}_p^2$ is given by*

$$L(2,p) = \left\{ \begin{pmatrix} a & b & 0 \\ \pm b & \pm a & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid a = a(\lambda) = \frac{\lambda + \lambda^{-1}}{2},\ b = b(\lambda) = \frac{\lambda - \lambda^{-1}}{2},\ \lambda \in \mathbb{F}_p^\times \right\}.$$

Proof. Let $A \in \mathrm{Mat}(3{\times}3, \mathbb{F}_p)$ be a matrix of the form $A = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}$ with $a, b, c, d \in \mathbb{F}_p$. For A to be a Lorentz transformation, A needs to satisfy the equation $A^T \eta^\pm A = \eta^\pm$. Since the last row and line of A has only one non-vanishing entry in the diagonal which is equal to 1, this problem reduces to the matrix equation

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Solving this system of equations leads to the conditions $d = \pm a, c = \pm b$ and $a^2 - b^2 = 1$ where the sign is to be taken simultaneously for both equations.

Let $\lambda \in \mathbb{F}_p^\times$ be a non-zero scalar and consider $a = a(\lambda) = \frac{\lambda+\lambda^{-1}}{2},\ b = b(\lambda) = \frac{\lambda-\lambda^{-1}}{2}$. It follows that $a^2 - b^2 = \frac{1}{4}\left((\lambda + \lambda^{-1})^2 - (\lambda - \lambda^{-1})^2\right) = \frac{1}{4}\left(\lambda^2 + \lambda^{-2} + 2 - \lambda^2 - \lambda^{-2} + 2\right) = 1$. Therefore, $a^2 - b^2 = 1$ and $(a(\lambda), b(\lambda))$ is contained in the set $\{(a,b) \in \mathbb{F}_p^2 \mid a^2 - b^2 = 1\}$.

Using the formula given in 2.4.6 we find that there are $p-1$ solutions of pairs (a,b) to this equation. Since $|\mathbb{F}_p^\times| = p-1$, $\lambda = a(\lambda) + b(\lambda)$ and, thus, $a(\lambda) \neq a(\lambda'),\ b(\lambda) \neq b(\lambda')$ for $\lambda \neq \lambda'$, we have found all solutions already.

Hence, the matrix representation of a Lorentz transformation on a $(1+1)$-dimensional projective spacetime is precisely given by

$$\begin{pmatrix} a & b & 0 \\ \pm b & \pm a & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ with } a = a(\lambda) = \frac{\lambda + \lambda^{-1}}{2},\; b = b(\lambda) = \frac{\lambda - \lambda^{-1}}{2},\; \lambda \in \mathbb{F}_p^\times.$$

□

In the following a and b will always be of this form if not stated otherwise. The proper Lorentz transformations are those with a $+$ in front of a and b in the second row. These will be of special interest since they form a subgroup of the group of Lorentz transformation which we will be discussed later.

In our further analysis we will drop the last row and line for better readability and clarity since it does not give any interesting information, and only consider the reduced Lorentz matrix.

In order to test the Cartan-Dieudonné theorem 2.6.6, we would like to find a decomposition of these Lorentz matrices in at most two reflections as stated in the theorem since we reduced the dimension of the space by one by the restriction done in the definition of Lorentz transformations.

Since the determinant of a reflection is -1, we should be able to find a vector $v \in \mathbb{F}_p^2$ such that an improper Lorentz transformations $\Lambda \in L(2,p)$ in $1+1$ dimensions is given by the Householder reflection S_v with respect to v.

This vector v can be directly computed by looking for eigenvectors of Λ with eigenvalue -1 since $S_v(v) = -v$.

Theorem 3.1.4. *Let $\Lambda \in L(2,p)$ be an improper Lorentz transformation, i. e.,* $\det(\Lambda) = -1$, $L_{2D}^- = \begin{pmatrix} a & b \\ -b & -a \end{pmatrix}$ *be its reduced matrix representation and $\eta = diag(-1,1)$ be the reduced matrix representation of the Minkowski form $\eta^\pm$.*

Then:

1. $(L_{2D}^-)^2 = id.$
2. $L_{2D}^- = S_v$ *with the Householder reflection S_v in two dimensions with respect to* $v = \begin{pmatrix} 1-a \\ b \end{pmatrix}$ *and the reduced Minkowski form η.*

Proof.

1. $(L_{2D}^-)^2 = \begin{pmatrix} a & b \\ -b & -a \end{pmatrix}^2 = \begin{pmatrix} a^2-b^2 & ab-ba \\ ab-ba & a^2-b^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ since $a^2 - b^2 = 1$.
2. The Householder reflection S_v is defined as $S_v = I_2 - \frac{2}{v^T \eta v} v v^T \eta$ with the identity matrix I_2 in two dimensions. Then, $v^T \eta v = -(1-a)^2 + b^2 = -1 + (-a^2 + b^2) + 2a = 2(a-1)$. In the last step we used $a^2 - b^2 = 1$.

Hence,

$$S_v = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{1-a} \begin{pmatrix} -(1-a)^2 & (1-a)b \\ -(1-a)b & b^2 \end{pmatrix} = \begin{pmatrix} a & b \\ -b & -a \end{pmatrix}$$

since $\frac{b^2}{1-a} = \frac{a^2-1}{1-a} = -a-1$.

□

Remark 3.1.5. *Since the full matrix representation L^- of Λ only differs by a single* 1 *on the diagonal on an additional line and row, one can easily check that*

$$L^- = S_v \text{ with } v = \begin{pmatrix} 1-a \\ b \\ 0 \end{pmatrix}.$$

This procedure of adding a zero as an additional component will work analogously for all reduced matrix representations we will consider later.

The decomposition into reflections will become more interesting if we consider proper Lorentz transformations since their determinant is equal to 1. Thus, we will need at least two Householder reflections in the decomposition and because of the Cartan-Dieudonné theorem we will need exactly two reflections.

Theorem 3.1.6. *Let $\Lambda \in L(2,p)$ be a proper Lorentz transformation, i. e.,* $\det(\Lambda) = +1$, $L^+_{2D} = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$ *be its reduced matrix representation and $\eta = diag(-1,1)$ be the reduced matrix representation of the Minkowski form $\eta^\pm$.*

Then:

1. $(L^+_{2D})^2 = (L^+_{2D}(\lambda))^2 = L^+_{2D}(\lambda^2)$ *with $a = a(\lambda)$ and $b = b(\lambda)$ as defined earlier.*
2. $L^+_{2D} = S_u S_w$ *with the Householder reflections S_u and S_w in two dimensions with respect to $u = \begin{pmatrix} a \\ b \end{pmatrix}$ and $w = \begin{pmatrix} a+1 \\ b \end{pmatrix}$, respectively, and the reduced Minkowski form η.*
3. *In particular, if $\lambda \in \mathbb{F}_p^\times$ is a square, i. e., $\exists\, x \in \mathbb{F}_p^\times : x^2 = \lambda$, $L^+_{2D} = S_{u(\lambda)} S_{u(x)}$ with $u = \begin{pmatrix} a \\ b \end{pmatrix}$.*

Proof.

1. At first we compute the square of L^+_{2D}:

$$(L^+_{2D})^2 = \begin{pmatrix} a & b \\ b & a \end{pmatrix}^2 = \begin{pmatrix} a^2+b^2 & 2ab \\ 2ab & a^2+b^2 \end{pmatrix}.$$

We notice that $a^2+b^2 = \left(\frac{\lambda+\lambda^{-1}}{2}\right)^2 + \left(\frac{\lambda-\lambda^{-1}}{2}\right)^2 = \frac{1}{4}(\lambda^2+\lambda^{-2}+2+\lambda^2+\lambda^{-2}-2) = \frac{\lambda^2+\lambda^{-2}}{2} = a(\lambda^2)$ and $2ab = \frac{\lambda+\lambda^{-1}}{2}(\lambda-\lambda^{-1}) = \frac{\lambda^2-\lambda^{-2}}{2} = b(\lambda^2)$.

Therefore, $(L^+_{2D}(\lambda))^2 = L^+_{2D}(\lambda^2)$.

2. The relation $a^2 - b^2 = 1$ and the definition of a Householder matrix yields

$$S_u = \begin{pmatrix} -a(\lambda^2) & b(\lambda^2) \\ -b(\lambda^2) & a(\lambda^2) \end{pmatrix} \text{ and } S_w = \begin{pmatrix} -a(\lambda) & b(\lambda) \\ -b(\lambda) & a(\lambda) \end{pmatrix}.$$

   Using the result in 1., it immediately follows that $S_u = (L^+_{2D})^2\eta$ and $S_w = L^+_{2D}\eta$. Since $(L^+_{2D})^T\eta L^+_{2D} = \eta$ by definition and $(L^+_{2D})^T = L^+_{2D}$, $S_uS_w = (L^+_{2D})^2\eta L^+_{2D}\eta = L^+_{2D}L^+_{2D}\eta L^+_{2D}\eta = L^+_{2D}\eta\eta = L^+_{2D}$ where in the last step we used that $\eta^2 = I_2$.

3. The result in 1. and 2. imply that if $\lambda \in \mathbb{F}_p^\times$ is a square in $\mathbb{F}_p$, i. e., $\exists x \in \mathbb{F}_p^\times : x^2 = \lambda$, $S_{w(\lambda)} = L^+_{2D}(\lambda)\eta = L^+_{2D}(x^2)\eta = (L^+_{2D}(x))^2\eta = S_{u(x)}$.

□

Remark 3.1.7.

1. *The choices of u and w in theorem 3.1.6 are not unique since, e. g, every multiple of u and w, respectively, will define the same Householder reflections because of the normalization in the definition of a Householder reflection.*

2. *It should be pointed out that we have used the unit time-like vector u which is only defined in 2 dimensions. If we embed u into the affine plane in our projective space $\mathrm{P}\mathbb{F}_p^2$ by $u \mapsto (u, 1)^T$ we can recover one of the quadric points of Q^+ in the intersection of the quadric and the affine plane. By switching the roles of a and b we can also construct a quadric point of Q^-.*

   Furthermore, it can be shown that there is a one-to-one correspondence between quadric points in the affine plane $\mathcal{A}$ in 2 dimensions and the components of the Lorentz matrices, i. e., $Q^+ \cap \mathcal{A} = \{[a : b : 1] \in \mathrm{P}\mathbb{F}_p^2\}$ and $Q^- \cap \mathcal{A} = \{[b : a : 1] \in \mathrm{P}\mathbb{F}_p^2\}$ with a and b as used in the Lorentz matrices.

   The whole quadric is the given by $Q^\pm = (Q^\pm \cap \mathcal{A}) \cup \{[\pm 1 : 1 : 0] \in \mathrm{P}\mathbb{F}_p^2\}$ which can easily be verified by using the formula given in 2.4.6 and using the decomposition of the projective space into regular vector spaces of increasingly lower dimension.

After this test of the Cartan-Dieudonné theorem we want to inspect the algebraic structure of the group of proper Lorentz transformations in two dimensions. We will find that it has a nice relation to the field $\mathbb{F}_p$ upon it is defined and because of that it is cyclic. This fact can be used to study even more features of this group by using properties of its generator.

Theorem 3.1.8. *The group of proper Lorentz transformations $L^+(2, p)$ which acts on $\mathrm{P}\mathbb{F}_p^2$ is isomorphic to the multiplicative group $\mathbb{F}_p^\times$ of $\mathbb{F}_p$. In particular, it is cyclic.*

Proof. Let $f : \mathbb{F}_p^\times \to L^+(2, p), \lambda \mapsto L^+_{2D}(\lambda)$. The map ϕ is bijective since its inverse is obviously given by $g : L^+(2, p) \to \mathbb{F}_p^\times, L^+_{2D}(\lambda) \mapsto (L^+_{2D}(\lambda))_{11} + (L^+_{2D}(\lambda))_{12} = \lambda$.

It is left to show that f defines a group homomorphism.

Let us inspect the multiplication of two proper Lorentz matrices.

$$\begin{aligned} L^+_{2D}(\lambda)L^+_{2D}(\lambda') &= \begin{pmatrix} a(\lambda) & b(\lambda) \\ b(\lambda) & a(\lambda) \end{pmatrix} \begin{pmatrix} a(\lambda') & b(\lambda') \\ b(\lambda') & a(\lambda') \end{pmatrix} \\ &= \begin{pmatrix} a(\lambda)a(\lambda') + b(\lambda)b(\lambda') & a(\lambda)b(\lambda') + b(\lambda)a(\lambda') \\ a(\lambda)b(\lambda') + b(\lambda)a(\lambda') & a(\lambda)a(\lambda') + b(\lambda)b(\lambda') \end{pmatrix} = L^+_{2D}(\lambda\lambda') \end{aligned}$$

since $a(\lambda)a(\lambda') + b(\lambda)b(\lambda') = \frac{\lambda+\lambda^{-1}}{2}\frac{\lambda'+\lambda'^{-1}}{2} + \frac{\lambda-\lambda^{-1}}{2}\frac{\lambda'-\lambda'^{-1}}{2} = \frac{\lambda\lambda'+(\lambda\lambda')^{-1}}{2} = a(\lambda\lambda')$ and $a(\lambda)b(\lambda') + b(\lambda)a(\lambda') = \frac{\lambda+\lambda^{-1}}{2}\frac{\lambda'-\lambda'^{-1}}{2} + \frac{\lambda-\lambda^{-1}}{2}\frac{\lambda'+\lambda'^{-1}}{2} = \frac{\lambda\lambda'-(\lambda\lambda')^{-1}}{2} = b(\lambda\lambda')$. We can immediately conclude that f is, indeed, a homomorphism of groups since it preserves the group multiplication as seen in the calculation.

Because the multiplicative group $\mathbb{F}_p^\times$ of a finite field $\mathbb{F}_p$ is cyclic as mentioned in 2.2.2 and $L^+(2,p)$ is isomorphic to $\mathbb{F}_p^\times$, it follows that $L^+(2,p)$ is cyclic. Its generator is given by $L^+_{2D}(a)$ with $\langle a \rangle = \mathbb{F}_p^\times$, i. e., $a \in \mathbb{F}_p^\times$ is a generator of $\mathbb{F}_p^\times$. □

Since the group of Lorentz transformation leaves the quadric invariant, we want to consider the action of a Lorentz transformation on a quadric point in its vector representation in affine coordinates. We will see that, similar to the multiplication of two Lorentz matrices, the rule of multiplication in $\mathbb{F}_p^\times$ comes up naturally.

Theorem 3.1.9. *Let $Q^\pm \subset \mathrm{P}\mathbb{F}_p^2$ be the quadrics defined by the standard Minkowski form $\eta^\pm$ and $L^+(\lambda) \in L^+(2,p), \lambda \in \mathbb{F}_p^\times$ be a proper Lorentz transformation.*

Then, for quadric points $p(\lambda') \in Q^\pm \cap \mathcal{A}, \lambda' \in \mathbb{F}_p^\times$ in the intersection of the quadric $Q^\pm$ and the affine plane $\mathcal{A}$ the action of $L^+(\lambda)$ is given by

$$L^+(\lambda)(p(\lambda')) = p(\lambda\lambda').$$

For quadric points q at infinity the action of $L^+(\lambda)$ is trivial for all $\lambda \in \mathbb{F}_p^\times$.

Proof. For points $p(\lambda') \in Q^\pm \cap \mathcal{A}, \lambda' \in \mathbb{F}_p^\times$ we will disregard the last component since it is not affected by a Lorentz transformation, and use the reduced matrix representation of $L^+(\lambda), \lambda \in \mathbb{F}_p^\times$.

Let $p(\lambda') \in Q^+ \cap \mathcal{A}$. Then $p(\lambda') = [a(\lambda') : b(\lambda') : 1]$.

$$\begin{aligned} L^+_{2D}(\lambda)p_{2D}(\lambda') &= \begin{pmatrix} a(\lambda) & b(\lambda) \\ b(\lambda) & a(\lambda) \end{pmatrix} \begin{pmatrix} a(\lambda') \\ b(\lambda') \end{pmatrix} = \begin{pmatrix} a(\lambda)a(\lambda') + b(\lambda)b(\lambda') \\ b(\lambda)a(\lambda') + a(\lambda)b(\lambda') \end{pmatrix} \\ &= \begin{pmatrix} a(\lambda\lambda') \\ b(\lambda\lambda') \end{pmatrix} = p(\lambda\lambda') \end{aligned}$$

where we have use the results from the last proof.

Now, let $p(\lambda') \in Q^- \cap \mathcal{A}$. Then $p(\lambda') = [b(\lambda') : a(\lambda') : 1]$.

$$\begin{aligned} L^+_{2D}(\lambda)p_{2D}(\lambda') &= \begin{pmatrix} a(\lambda) & b(\lambda) \\ b(\lambda) & a(\lambda) \end{pmatrix} \begin{pmatrix} b(\lambda') \\ a(\lambda') \end{pmatrix} = \begin{pmatrix} a(\lambda)b(\lambda') + b(\lambda)a(\lambda') \\ b(\lambda)b(\lambda') + a(\lambda)a(\lambda') \end{pmatrix} \\ &= \begin{pmatrix} b(\lambda\lambda') \\ a(\lambda\lambda') \end{pmatrix} = p(\lambda\lambda') \end{aligned}$$

in complete analogy to the first case.

Quadric points p at infinity in both cases are given by $p = [\pm 1 : 1 : 0]$. Thus,

$$L^+_{2D}(\lambda)p_{2D} = \begin{pmatrix} a(\lambda) & b(\lambda) \\ b(\lambda) & a(\lambda) \end{pmatrix} \begin{pmatrix} \pm 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \pm a(\lambda) + b(\lambda) \\ \pm b(\lambda) + a(\lambda) \end{pmatrix} = \begin{pmatrix} \pm\lambda^{\pm 1} \\ \lambda^{\pm 1} \end{pmatrix}$$

which is projectively equivalent to $\begin{pmatrix} \pm 1 \\ 1 \end{pmatrix} = p_{2D}$. Thus, the action of a Lorentz transformation on a quadric point at infinity is trivial. □

Remark 3.1.10. *Using the law of the action of a proper Lorentz transformation on a quadric point in the affine plane we can immediately conclude that every quadric point in the affine plane can be obtained by the action of a Lorentz transformation on the point* $p(\lambda = 1) = \begin{cases} [1:0:1] & \textit{for } p \in Q^+ \cap \mathcal{A} \\ [0:1:1] & \textit{for } p \in Q^- \cap \mathcal{A} \end{cases}$.

Remark 3.1.11. *Since the multiplication in $\mathbb{F}_p^\times$ with a fixed element is basically just a permutation of the $p-1$ elements of $\mathbb{F}_p^\times$, the multiplication table of $\mathbb{F}_p^\times$ can be used to fine the permutation of quadric points $p(\lambda')$ in the affine plane labelled by λ' with $\lambda' \in \{1, \dots, p-1\}$ corresponding to the multiplication of a fixed proper Lorentz matrix $L^+(\lambda)$ with lambda $\in \mathbb{F}_p^\times$ with the quadric points in the affine plane. Let us consider for example the finite field $\mathbb{F}_7$ with 7 elements. Then, the multiplication table is given by*

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

.

The permutation can be read off by taken the line starting with λ corresponding to the fixed Lorentz transformation $L^+(\lambda)$. For example, for $\lambda = 3$ the permutation $\sigma \in S_6$ is then given by $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 5 & 1 & 4 \end{pmatrix}$.

Thus, it would be possible to map the quadric points in the affine plane to base vectors of a $(p-1)$-dimensional vector space labelled again by $\lambda \in \{1, \dots, p-1\}$ and use permutation matrices corresponding to the permutation constructed above to compute the action of a proper Lorentz transformation on the quadric points in the affine plane.

The multiplication table can also be used to find the product of two proper Lorentz matrices since their group is isomorphic to $\mathbb{F}_p^\times$.

3.1.2 Lorentz Transformations in (1+3)-dimensional Projective Spacetime

We have seen that in two dimensions the group of proper Lorentz transformations is cyclic and every Lorentz transformation can be easily decomposed into up to two Householder reflections.

Now, we want to study the group of Lorentz transformation in a $(1+3)$-dimensional projective spacetime. We will see that a decomposition into reflections is also easily describable and the group of proper Lorentz transformations is generated by four different elements, namely a boost and three spatial rotations acting on 2-dimensional subspaces, respectively. This is in contrast to the case in special relativity and the usage of the real numbers where every Lorentz transformation can be written as a product of a boost, a spatial rotation in four dimensions, and possibly a spatial or temporal inversion.

At first, we need to specify a few special cases of Lorentz transformations, namely boosts and spatial rotation, which did not come up in the discussion of a 2-dimensional spacetime.

Definition 3.1.12. *Let $L(4,p)$, $p \equiv 3 \mod 4$, $p > 3$ prime, be the Lorentz group acting on a 4-dimensional spacetime.*

An element $B \in L(4,p)$ is called ***basic boost*** *if its reduced matrix representation is of the form $B = \begin{pmatrix} L^{+}_{2D}(\lambda) & 0 \\ 0 & I_2 \end{pmatrix}$ with $L^{+}_{2D}(\lambda) = \begin{pmatrix} a(\lambda) & b(\lambda) \\ b(\lambda) & a(\lambda) \end{pmatrix}, \lambda \in \mathbb{F}_p^{\times}$, a Lorentz transformation in two dimensions in its reduced matrix representation and I_2 the identity matrix in two dimensions.*

An element $R \in L^{+}(4,p)$ is called ***(spatial) rotation*** *or* ***space rotation*** *if its reduced matrix representation is of the form $R = \begin{pmatrix} 1 & 0 \\ 0 & R' \end{pmatrix}$ with $R' \in Mat(3 \times 3, \mathbb{F}_p)$ and $R'^{T} R' = I_3$ where I_3 denotes the identity matrix in three dimensions.*

R is called a ***basic rotation*** *if R' leaves one of the 1-dimensional subspaces invariant.*

Remark 3.1.13.

1. *Spatial rotations, basic boosts and conjugations of basic boosts with a rotation (called boosts) form a subgroup of $L(4,p)$, respectively.*

2. *Sometimes, basic boosts are defined for $\lambda \in \mathbb{F}_p^{\times}$ which is a square in $\mathbb{F}_p$ in order to get the analogy of a velocity which is non-negative and, thus, a square in $\mathbb{R}$. For our purposes this is not necessary and some of the results in the last section may not be applicable.*

Later we will see that these special Lorentz transformation will be very useful to describe the structure of the Lorentz group. Thus, we want to further discuss these special cases of Lorentz transformations in terms of their parametrization, their decomposition into reflections and, furthermore, the algebraic structure of their groups.

At first, we notice that basic boosts are completely defined by their 2-dimensional reduced Lorentz matrix. Thus, the group of basic boosts behaves as discussed in section 3.1.1. In analogy to the definition of a boost in special relativity we want to consider a special form of boosts which is not closed under multiplication but still a useful tool to transfer the knowledge about $L(2,p)$ to $L(4,p)$.

Lemma 3.1.14. *Let $\tilde{x} = [x_0 : x_1 : x_2 : x_3 : 1] \in Q^{+}$ and $x := (x_1, x_2, x_3)^T$.*

Then,

$$B_{\tilde{x}} = \begin{pmatrix} x_0 & x^T \\ x & I_3 + \frac{xx^T}{x_0+1} \end{pmatrix}$$

is the reduced matrix representation of a Lorentz transformation in $L(4,p)$. Its decompositions into reflections is given by $B_{\tilde{x}} = S_u S_w$ where S_u, S_w are the reduced matrix representations of Householder reflections in four dimensions with respect to $u = (x_0, x^T)^T$ and $w = (x_0+1, x^T)^T$, respectively.

Proof. A direct calculation using $-x_0^2 + x^T x = -1$ shows:

$$B_{\tilde{x}}^T \eta B_{\tilde{x}} = \begin{pmatrix} -x_0^2 + x^T x & (-x_0 + 1 + \frac{x^T x}{x_0+1})x^T \\ (-x_0 + 1 + \frac{x^T x}{x_0+1})x & I_3 + (-1 + \frac{2x_0+2+x^T x}{(x_0+1)^2})xx^T \end{pmatrix} = \operatorname{diag}(-1,1,1,1) = \eta$$

since $-x_0 + 1 + \frac{x^T x}{x_0+1} = \frac{1-x_0^2+x^T x}{x_0+1} = \frac{1-1}{x_0+1} = 0$ and $-1 + \frac{2x_0+2+x^T x}{(x_0+1)^2} = \frac{-(x_0+1)^2+2x_0+2+x^T x}{(x_0+1)^2} = \frac{-x_0^2+1+x^T x}{x_0+1} = 0$.

By inserting u and w into the formula of Householder reflections with I_4 the identity matrix in four dimensions and using $u^T \eta u = -x_0^2 + x^T x = -1$ and $w^T \eta w = -(x_0+1)^2 + x^T x = -2(x_0+1)$ we get the reduced matrix representations:

$$S_u = I_4 - \frac{2}{u^T \eta u} u u^T \eta = \begin{pmatrix} 1 - 2x_0^2 & 2x_0 x^T \\ -2x_0 x & I_3 + 2xx^T \end{pmatrix} \text{ and } S_w = \begin{pmatrix} -x_0 & x^T \\ -x & I_3 + \frac{xx^T}{x_0+1} \end{pmatrix}.$$

Hence,

$$\begin{aligned} S_u S_w &= \begin{pmatrix} -x_0 + 2x_0(x_0^2 - x^T x) & (1 - 2x_0^2 + 2x_0 + 2x_0 \frac{x^T x}{x_0+1})x^T \\ (1 - 2x_0^2 + 2x_0 + 2x_0 \frac{x^T x}{x_0+1})x & I_3 + (-2x_0 + 2 + \frac{1}{x_0+1} + 2\frac{x^T x}{x_0+1})xx^T \end{pmatrix} \\ &= \begin{pmatrix} -x_0 + 2x_0 & (1 - 2x_0^2 + 2x_0 + 2x_0 \frac{x_0^2-1}{x_0+1})x^T \\ (1 - 2x_0^2 + 2x_0 + 2x_0 \frac{x_0^2-1}{x_0+1})x & I_3 + (-2x_0 + 2 + \frac{1}{x_0+1} + 2\frac{x_0^2-1}{x_0+1})xx^T \end{pmatrix} \\ &= \begin{pmatrix} x_0 & (1 - 2x_0(x_0-1) + 2x_0(x_0-1))x^T \\ (1 - 2x_0(x_0-1) + 2x_0(x_0-1))x & I_3 + (-2(x_0-1) + \frac{1}{x_0+1} + 2(x_0-1))xx^T \end{pmatrix} \\ &= \begin{pmatrix} x_0 & x^T \\ x & I_3 + \frac{xx^T}{x_0+1} \end{pmatrix} = B_{\tilde{x}}. \end{aligned}$$

□

This concludes our discussion of boosts. Now, we want to consider rotations, in particular basic rotations. These can later be used to describe what we will call gauge transformations in 2-dimensional projective spacetime for η^+. Thus, every aspect of the discussion here can be used later on.

Theorem 3.1.15. *Let $R_1, R_2, R_3 \in Mat(3 \times 3, \mathbb{F}_p)$ be the reduced form of a basic rotation which leaves the first, second and third spatial component invariant, respectively.*

Then, $R_3^{\pm} = \begin{pmatrix} c & -s & 0 \\ \pm s & \pm c & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $R_2^{\pm} = \begin{pmatrix} c & 0 & s \\ 0 & 1 & 0 \\ \mp s & 0 & \pm c \end{pmatrix}$ *and* $R_1^{\pm} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & -s \\ 0 & \pm s & \pm c \end{pmatrix}$ *where the sign for each matrix has to be taken simultaneously, respectively, and* $c, s \in \mathbb{F}_p$ *with* $c^2+s^2 = 1$*. A possible parametrization is* $\{(c,s) \in \mathbb{F}_p^2 \mid c^2+s^2 = 1\} = \{(\frac{\lambda-\lambda^{-1}}{\lambda+\lambda^{-1}}, \frac{2}{\lambda+\lambda^{-1}}) \mid \lambda \in \mathbb{F}_p^\times\} \cup \{(\pm 1, 0)\}$*.*

Furthermore, $(R_i^-)^2 = I_3, i = 1,2,3$*, with the identity matrix* I_3 *in three dimensions.*

Proof. We only consider the case of R_3 in its reduced form, the rest follows analogously.

Let $R_{3,2D} = \begin{pmatrix} c & d \\ e & f \end{pmatrix} \in \mathrm{Mat}(2 \times 2, \mathbb{F}_p)$. Then, $R_{3,2D}$ has to satisfy the condition $R_{3,2D}^T R_{3,2D} = I_2$ where I_2 is the identity matrix in two dimensions. This leads to the set of equations $c^2 + d^2 = e^2 + f^2 = 1$ and $ce + df = 0$. A consistent solution is given by $e = \mp d, f = \pm c$ where the sign has to be taken simultaneously, and $c^2 + d^2 = 1$. To get a more familiar look we define $s := -d$. Thus, $R_{3,2D} = \begin{pmatrix} c & -s \\ \pm s & \pm c \end{pmatrix}$.

Let $\lambda \in \mathbb{F}_p^\times, c = c(\lambda) := \frac{\lambda-\lambda^{-1}}{\lambda+\lambda^{-1}}$ and $s = s(\lambda) := \frac{2}{\lambda+\lambda^{-1}}$. Then, $c^2+s^2 = \frac{\lambda^2+\lambda^{-2}-2+2^2}{\lambda^2+\lambda^{-2}+2} = 1$. Thus, this parametrization of (c,s) yields a subset of the set of solutions to $c^2 + s^2 = 1$. We can also see that in this parametrization s is always non-zero and the tuples $(c,s) = (\pm 1, 0)$ are also a solution to $c^2 + s^2 = 1$. Hence, we have to add these two solutions to our parametrization.

Using theorem 2.4.6 we find that there are $p+1$ pairs $(c,s) \in \mathbb{F}_p^2$ which are solutions to $c^2 + s^2 = 1$. Since $|\mathbb{F}_p^\times| = p-1$, the number of solutions covered by our parametrization is given by $|\{(\frac{\lambda-\lambda^{-1}}{\lambda+\lambda^{-1}}, \frac{2}{\lambda+\lambda^{-1}}) \mid \lambda \in \mathbb{F}_p^\times\} \cup \{(\pm 1, 0)\}| = |\mathbb{F}_p^\times| + 2 = p - 1 + 2 = p + 1 = |\{(c,s) \in \mathbb{F}_p^2 \mid c^2 + s^2 = 1\}|$. We conclude that we have found all possible solutions.

Since R_i^- for $i \in \{1,2,3\}$ is symmetric, i. e., $(R_i^-)^T = R_i^-$, and using the defining equation $(R_i^-)^T R_i^- = I_3$, it immediately follows that $(R_i^-)^2 = (R_i^-)^T R_i^- = I_3$. □

In the following we will only consider the case of the basic rotation $R_3^{\pm}$ in its reduced form. If not otherwise stated, $c, s \in \mathbb{F}_p$ will be of such form that $c^2 + s^2 = 1$ as found in the above theorem.

As in the case of Lorentz transformation we want to test the Cartan-Dieudonné theorem and further study the structure of the group of basic rotation of one type. We will see that as in the case of real rotations there is a connection to the unit circle in a degree two extensions field.

Theorem 3.1.16. *Let* $R_{3,2D}^{\pm}$ *be the reduced form of the basic rotation* $R_3^{\pm}$*.*

Then:

1. $R_{3,2D}^+ = S_u S_w$ *with the Householder reflections* S_u *and* S_w *in two dimensions with respect to* $u = \begin{pmatrix} c \\ s \end{pmatrix}$ *and* $w = \begin{pmatrix} c+1 \\ s \end{pmatrix}$*.*

2. $R_{3,2D}^- = S_v$ *with the Householder reflection* S_v *in two dimensions with respect to* $v = \begin{pmatrix} 1-c \\ s \end{pmatrix}$*.*

Proof. Inserting u, w, v into the formula for the matrix representation of a Householder reflection and using $c^2 + s^2 = 1$, we find

$$\begin{aligned}
S_u &= I_2 - \frac{2}{u^T u} uu^T = \begin{pmatrix} 1-2c^2 & -2cs \\ -2cs & 1-2s^2 \end{pmatrix}, \\
S_w &= I_2 - \frac{2}{w^T w} ww^T = I_2 - \frac{2}{c^2+1+2c+s^2} \begin{pmatrix} (c+1)^2 & (c+1)s \\ (c+1)s & s^2 \end{pmatrix} \\
&= I_2 - \frac{2}{2(c+1)} \begin{pmatrix} (c+1)^2 & (c+1)s \\ (c+1)s & 1-c^2 \end{pmatrix} = \begin{pmatrix} -c & -s \\ -s & c \end{pmatrix}
\end{aligned}$$

and

$$\begin{aligned}
S_v &= I_2 - \frac{2}{v^T v} vv^T = I_2 - \frac{2}{1+c^2-2c+s^2} \begin{pmatrix} (1-c)^2 & (1-c)s \\ (1-c)s & s^2 \end{pmatrix} \\
&= I_2 - \frac{2}{2(1-c)} \begin{pmatrix} (1-c)^2 & (1-c)s \\ (1-c)s & 1-c^2 \end{pmatrix} = \begin{pmatrix} c & -s \\ -s & -c \end{pmatrix} = R^-_{3,2D}
\end{aligned}$$

which shows the second part. Left to show is $R^+_{3,2D} = S_u S_w$.

$$\begin{aligned}
S_u S_w &= \begin{pmatrix} 1-2c^2 & -2cs \\ -2cs & 1-2s^2 \end{pmatrix} \begin{pmatrix} -c & -s \\ -s & c \end{pmatrix} = \begin{pmatrix} -c+2c^3+2cs^2 & -s+2sc^2-2c^2s \\ 2c^2s-s+2s^3 & 2cs^2+c-2s^2c \end{pmatrix} \\
&= \begin{pmatrix} -c+2c(c^2+s^2) & -s \\ -s+2s(c^2+s^2) & c \end{pmatrix} = \begin{pmatrix} -c+2c & -s \\ -s+2s & c \end{pmatrix} = \begin{pmatrix} c & -s \\ s & c \end{pmatrix} = R^+_{3,2D}.
\end{aligned}$$

□

Remark 3.1.17.

1. *In this case we want to stress that such a decomposition into reflection is not unique, i. e., $R^+_{3,2D} = S_{w'} S_{u'}$ with $w' = \begin{pmatrix} c-1 \\ s \end{pmatrix}$ and $u' = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, since $S_{w'} S_{u'} = \begin{pmatrix} c & s \\ s & -c \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} c & -s \\ s & c \end{pmatrix} = R^+_{3,2D}$.*
2. *Since $\det(R^\pm_i) = \pm 1$ and because of the multiplicative property of the determinant, we conclude that for each $i = 1, 2, 3$ the set of basic rotation with positive determinant, i. e., $\{R^+_i\}$, forms a subgroup of the group of basic rotations, respectively.*

Corollary 3.1.18. *Let $i \in \{1, 2, 3\}$.*

The group of basic rotations $O^+_i = \{R^+_i\}$ with positive determinant is isomorphic to the subgroup $\{z = a + ib \in \mathbb{F}_{p^2} \mid a^2 + b^2 = 1\} \subset \mathbb{F}_{p^2}$ of elements of the extension field $\mathbb{F}_{p^2}$ with unit norm. In particular, O^+_i is cyclic.

Proof. Since we only consider prime numbers $p \in \mathbb{N}$ with $p \equiv 3 \mod 4$, the polynomial $X^2 + 1 \in \mathbb{F}_p[X]$ is irreducible and, thus, the quotient ring $\mathbb{F}_p[X]/(X^2 + 1)$ forms an extension field of degree 2 which is given by the adjunction of an element called i which satisfies the condition $i^2 = -1$, i. e., $\mathbb{F}_p[X]/(X^2+1) = \{a+ib \mid a, b \in \mathbb{F}_p\} = \mathbb{F}_{p^2}$. Note that also $-i$ satisfies this condition. The Galois group is then given by $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p) = \{\mathrm{id}, \sigma\}$ with $\sigma : \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}, a+ib \mapsto a-ib$, i. e., a permutation of i and $-i$. For every $z \in \mathbb{F}_{p^2}$ the map $z = a+ib \mapsto z\sigma(z) = a^2+b^2$ is multiplicative since elements of the Galois group are field automorphisms. Thus, the set $S^1 := \{z \in \mathbb{F}_{p^2} \mid z\sigma(z) = 1\}$ is a subgroup of $\mathbb{F}_{p^2}^\times$ and, since $\mathbb{F}_{p^2}^\times$ is cyclic, also S^1 is cyclic due to theorem 2.1.8.

Now, we only have to establish the isomorphism between O_i^+ and S^1. We will only consider the case of $i = 3$ in the reduced representation, the rest follows analogously. Since the number of elements in both O_i^+ and S^1 is given by the number of solutions (c, s) of $c^2 + s^2 = 1$, there is hope to find such an isomorphism. Consider the map $\varphi : O_3^+ \to S^1, \begin{pmatrix} c & -s \\ s & c \end{pmatrix} \mapsto c + is$. φ is obviously bijective. It is also a group homomorphism since

$$\begin{aligned}\varphi\left(\begin{pmatrix} c & -s \\ s & c \end{pmatrix}\begin{pmatrix} c' & -s' \\ s' & c' \end{pmatrix}\right) &= \varphi\left(\begin{pmatrix} cc'-ss' & -(cs'+sc') \\ sc'+cs' & -ss'+cc' \end{pmatrix}\right) \\ &= (cc'-ss') + i(cs'+sc') = (c+is)(c'+is')\end{aligned}$$

using $i^2 = -1$. Thus, we have established the isomorphism between O_3^+ and S^1 and, since S^1 is cyclic, also O_3^+ is cyclic with the generator given by the preimage of the generator of S^1. □

Remark 3.1.19. *In 2.3.7 it was stated that the generator of the Galois group Gal*$(\mathbb{F}_q/\mathbb{F}_p)$ *with* $q = p^r, r \in \mathbb{N}$, *is the Frobenius map* $\varphi : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x^p$. *In the case of* $r = 2$ *and* $p \equiv 3 \mod 4$ *we find that the order of* $i \in \mathbb{F}_q$ *is 4, i. e., 4 is the smallest natural number* n *such that* $i^n = 1$. *Thus,* $i^p = i^{4k+3} = i^3 = -i$ *for* $k \in \mathbb{N}$ *such that* $p = 4k+3$. *Hence, the Frobenius map coincides in this case with the finite field analogue of complex conjugation.*

Since there may not only be pure basic rotations but also products of such, we want to consider a finite field analogue of the parametrization of a rotation about an axis given by a unit vector in three dimensions.

Theorem 3.1.20. *Every space rotation* R *in three dimensions with positive determinant is of the form*

$$R = R(n, c, s) = \begin{pmatrix} n_1^2(1-c)+c & n_1n_2(1-c)-n_3s & n_1n_3(1-c)+n_2s \\ n_2n_1(1-c)+n_3s & n_2^2(1-c)+c & n_2n_3(1-c)-n_1s \\ n_3n_1(1-c)-n_2s & n_3n_2(1-c)+n_1s & n_3^2(1-c)+c \end{pmatrix}$$

with $n = (n_1, n_2, n_3) \in \mathbb{F}_p^3$ *with* $n_1^2+n_2^2+n_3^2 = 1$ *and* $c, s \in \mathbb{F}_p$ *with* $c^2+s^2 = 1$.

Proof. In complete analogy to the case of real numbers a direct calculation shows that $R^TR = I_3$ which is omitted here. There exists a formula which can be found in [1], for the number of orthogonal matrices in the usual meaning or in our language rotations in three dimensions over a field $\mathbb{F}_q$ which is given by $|O_{I_3}(3, q)| = 2(q^3-q)$ with the identity matrix

I_3 in three dimensions. Since we only consider rotations with positive determinant, the number is reduced by a factor of 2. Using the formulae in 2.4.6 in the case of the field $\mathbb{F}_p$ we find that there are $p+1$ pairs of (c, s) with $c^2+s^2 = 1$ and p^2-1 elements $n \in \mathbb{F}_p^3$ with $nn^T = 1$. If we consider the product $(p+1)(p^2-p) = p^3+p^2-p^2-p = p^3-p$ and, since both n and (c, s) can be taken independently, we conclude that this parametrization covers the whole group of rotations in three dimensions over the field $\mathbb{F}_p$. □

Theorem 3.1.21. *Let $n = (n_1, n_2, n_3) \in \mathbb{F}_p^3$ with $n_1^2 + n_2^2 + n_3^2 = 1$ and $c, s \in \mathbb{F}_p$ with $c^2 + s^2 = 1$.*

Then, a possible decomposition of $R(n, c, s)$ as in theorem 3.1.20 is given by $R(n, c, s) = S_u S_w$ with the Householder rotations S_u and S_w in three dimensions with respect to $u = \begin{pmatrix} (c+1)n_1n_3 + sn_2 \\ (c+1)n_2n_3 - sn_1 \\ -(c+1)(n_1^2+n_2^2) \end{pmatrix}$ and $w = \begin{pmatrix} cn_1n_3 + sn_2 \\ cn_2n_3 - sn_1 \\ -c(n_1^2+n_2^2) \end{pmatrix}$.

Proof. We want to reduce the case of a rotation in three dimensions to the case of a basic rotation in two dimensions. Thus, we assume $n \neq (0, 0, 1)$ which would give the basic rotation R_3^+. Now, let d be a symbol such that $d^2 = n_1^2 + n_2^2$ which does not have to exist in $\mathbb{F}_p$. Then, a direct computation shows that $R(n, c, s) = PR_3^+P^{-1}$ with

$$P = \begin{pmatrix} \frac{n_1n_3}{d} & -\frac{n_2}{d} & n_1 \\ \frac{n_2n_3}{d} & \frac{n_1}{d} & n_2 \\ -d & 0 & n_3 \end{pmatrix}.$$

Let $R_3^+ = S_{u'}S_{w'}$ be a decomposition of R_3^+, e.g., $u' = \begin{pmatrix} c+1 \\ -s \\ 0 \end{pmatrix}$ and $w' = \begin{pmatrix} c \\ -s \\ 0 \end{pmatrix}$. Then, $R(n, c, s) = PR_3^+R^{-1} = PS_{u'}S_{w'}P^{-1} = (PS_{u'}P^{-1})(PS_{w'}P^{-1})$. Since $S_{u'} = I_3 - \frac{2}{u'^Tu'}u'u'^T$ and $P^{-1} = P^T$, $PS_{u'}P^{-1} = I_3 - \frac{2}{u'^TP^TPu'}Pu'u'^TP^T = S_{Pu'}$ and analogously for $PS_{w'}P^{-1} = S_{Pw'}$. Since the formula of a Householder reflection is the same with respect to a vector v and λv with $\lambda \in \mathbb{F}_p^\times$, we can multiply both u and w by d to get the desired result. Therefore,

$$u = dPu' = \begin{pmatrix} (c+1)n_1n_3 + sn_2 \\ (c+1)n_2n_3 - sn_1 \\ -(c+1)d^2 \end{pmatrix} = \begin{pmatrix} (c+1)n_1n_3 + sn_2 \\ (c+1)n_2n_3 - sn_1 \\ -(c+1)(n_1^2+n_2^2) \end{pmatrix}$$

and

$$w = dPw' = \begin{pmatrix} cn_1n_3 + sn_2 \\ cn_2n_3 - sn_1 \\ -cd^2 \end{pmatrix} = \begin{pmatrix} cn_1n_3 + sn_2 \\ cn_2n_3 - sn_1 \\ -c(n_1^2+n_2^2) \end{pmatrix}.$$

□

After this discussion of special cases of elements of the Lorentz group we want to consider a result found in [5] which is based on the work of Dickson [3] and gives us more information about the structure of the proper Lorentz group.

Theorem 3.1.22. *Let $L^{+}(4,p)$ be the group of proper Lorentz transformations acting on a 4-dimensional spacetime over the field $\mathbb{F}_p$, $p \equiv 3 \mod 4$, $p > 3$ prime.*

Then, $L^{+}(4,p)$ is generated by basic boosts, basic rotations and spacetime reversal.

Using the results found up to now we may conclude the following refinement of this theorem.

Corollary 3.1.23. *Let $L^{+}(4,p)$ be the group of proper Lorentz transformations acting on a 4-dimensional spacetime over the field $\mathbb{F}_p$, $p \equiv 3 \mod 4$, $p > 3$ prime.*

Then, $L^{+}(4,p)$ is generated by four elements, i. e., by the generator of basic boosts and by the three generators of the three types of basic rotations, respectively.

Proof. Since we have shown that the group of basic boosts and the three groups of basic rotations are cyclic, there exists one element which generates this groups, respectively. The spacetime reversal which is given by the negative identity matrix in four dimensions can be constructed by a product of a basic boost with $(a,b) = (-1,0)$ and a basic rotation R_1^{+} with $(c,s) = (-1,0)$. □

Remark 3.1.24. *A general element of the group of proper Lorentz transformations is then given by a product of basic boosts and basic rotations. Its decomposition can be deduced by using the decomposition of a 3-dimensional rotation which every product of basic rotations will yield, and using the trick of conjugation as shown in the proof of the decomposition of a rotation in three dimensions, i. e., in symbols, e. g., $RBR' = (RBR^{-1})RR'$ which again can be decomposed into $2+2$ reflections.*

This concludes our study of the algebraic properties of the group of Lorentz transformations in $1+1$ and $1+3$ dimensions. We have seen that the proper types of both groups can be reduced to just a few generators, respectively, which can be very useful computational-wise. We also discussed the application of the Cartan-Dieudonné theorem in both cases and gave an explicit parametrization.

3.2 Gauge Transformations

The second subgroup of the orthogonal group $O_{\eta^\pm}$ of the standard Minkowski form $\eta^\pm$ we want to consider, is the subgroup of *gauge transformations*. We will only consider them at one specific point since in their full definition they are used to describe a gauge transformation in the sense of gauge field theory between two points which is given by a conjugation of the original transformation by another which describes the propagation between the two points.

Definition 3.2.1. *Let $\eta^\pm$ be the standard Minkowski form on an n-dimensional projective space $\mathrm{P}\mathbb{F}_p^n$ with p prime, $p \equiv 3 \mod 4$, and $O_{\eta^\pm}$ the corresponding orthogonal group.*

A ***gauge transformation*** *$\alpha_\pm$ is an Element $\alpha_\pm \in O_{\eta^\pm}$ which leaves the time coordinate of a point invariant, i. e., the matrix representation of $\alpha_\pm$ is given by $\begin{pmatrix} 1 & 0 \\ 0 & A^\pm \end{pmatrix}$ with $A^\pm \in Mat(n \times n, \mathbb{F}_p)$.*

A gauge transformation is called ***proper*** *if its determinant is equal to* 1*. Otherwise it is called* ***improper****.*

Remark 3.2.2.

1. *The $n \times n$ matrix $A_\pm$ has to satisfy a reduced equation in contrast to the gauge transformation $\alpha_\pm$ in the above definition, namely*

$$A_\pm^T M_\pm A_\pm = M_\pm$$

   with $M_\pm = diag(1, \ldots, 1, \pm 1) \in Mat(n \times n, \mathbb{F}_p)$. This immediately shows that the matrix representation of a gauge transformation of $-$-type is given by the matrix representation of a the Lorentz transformations by mirroring all lines and rows at the diagonal perpendicular to the usual diagonal used in the context of matrices.

2. *One can easily verify that the set of gauge transformations acting on a finite-dimensional projective space forms a group when equipped with the usual composition of maps or standard matrix multiplication for their matrix representation. The group of gauge transformations acting on an n-dimensional projective space over the finite field $\mathbb{F}_p$ is denoted $G_\pm(n,p)$.*

   In particular, the set of proper gauge transformations is a subgroup of this group because the determinant is multiplicative. This group is then denoted $G_\pm^\uparrow(n,p)$.

3. *Furthermore, since we have already set one of the entries in the matrix to unity, there is no projective freedom in the reduced gauge transformation matrix.*

4. *Note that unlike Lorentz transformations these gauge transformations do not leave the centre of the quadric and the corresponding hyperplane at infinity invariant.*

To get a better understanding of the structure of the group of gauge transformations we consider a $(1+1)$-dimensional spacetime as a toy model and afterwards the full $(1+3)$-dimensional spacetime. Since the gauge transformations of $-$-type are essentially identical to Lorentz transformations, we will only consider gauge transformations of $+$-type in the following.

3.2.1 Gauge Transformations in (1+1)-dimensional Projective Spacetime

In two dimensions we will see that our previous work on and study of basic rotations in the Lorentz group will come in very handy.

Theorem 3.2.3. *The group $G_+(2,p)$ of gauge transformations of $+$-type on $\mathrm{P}\mathbb{F}_p^2$ is given by*

$$G_+(2,p) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & -s \\ 0 & \pm s & \pm c \end{pmatrix} \mid c, s \in \mathbb{F}_p : c^2 + s^2 = 1 \right\}.$$

Proof. Let $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} \in G_+(2,p)$. Then, $A \in \mathrm{Mat}(2 \times 2, \mathbb{F}_p)$ has to satisfy the condition $A^T A = I_2$ with I_2 the identity matrix in two dimensions. This is exactly the same condition as for the basic rotations R_1 as discussed in theorem 3.1.15. □

The proof shows that the gauge transformations of $+$-type in two dimensions are identical to the basic rotations which leave the first spatial coordinate invariant. Thus, everything we established for basic rotations, can be also used in this case. For completeness we will sum up the essential result in the following theorem.

Theorem 3.2.4. *Let $A_+^\pm = \begin{pmatrix} c & -s \\ \pm s & \pm c \end{pmatrix} \in Mat(2 \times 2, \mathbb{F}_p)$ be the reduced matrix representations of $\alpha_+^\pm \in G_+(2,p)$. Then the following holds:*

1. *$A_+^+ = S_u S_w$ with the Householder reflections S_u and S_w in two dimensions with respect to $u = \begin{pmatrix} c \\ s \end{pmatrix}$ and $w = \begin{pmatrix} c+1 \\ s \end{pmatrix}$.*

2. *$A_+^- = S_v$ with the Householder reflection S_v in two dimensions with respect to $v = \begin{pmatrix} 1-c \\ s \end{pmatrix}$. In particular, $(A_+^-)^2 = I_2$ with I_2 the identity matrix in two dimensions.*

3. *$G_+^+(2,p) = \{\alpha \in G_+(2,p) \mid \det(\alpha) = 1\}$ is isomorphic to $S^1 = \{a + ib \in \mathbb{F}_{p^2} \mid a^2 + b^2 = 1\}$ and, thus, cyclic.*

Remark 3.2.5. *In two dimensions the gauge transformations of $-$-type are precisely given by the Lorentz transformations in two dimensions because of the symmetry of signs in the second row in the matrix representation of a Lorentz transformation.*

We conclude that the decomposition of a gauge transformation in two dimensions can be written with one reflection with respect to a unit vector and the groups of both types of gauge transformations are cyclic, respectively.

3.2.2 Gauge Transformations in (1+3)-dimensional Projective Spacetime

If we now consider the gauge transformations in four dimensions, it immediately follows that the gauge transformations of $-$-type are given by the Lorentz transformations in four dimensions with the first two rows and lines swapped with the second last and last rows and lines because of the symmetries in signs an the exchange symmetry of the spatial coordinate axes. Thus, we only consider gauge transformations of $+$-type. The first result we want to discuss, is a finite field analogue of a decomposition of a gauge transformation of $+$-type which can also be interpreted as a rotation in four dimensions. This formula is due to Van Elfrinkhof [10].

Lemma 3.2.6 (Van Elfrinkhof). *Let $a, b, c, d, p, q, r, s \in \mathbb{F}_p$ with $a^2 + b^2 + c^2 + d^2 = p^2 + q^2 + r^2 + s^2 = 1$. Then,*

$$
\begin{aligned}
A &= \begin{pmatrix} ap - bq - cr - ds & -aq - bp + cs - dr & -ar - bs - cp + dq & -as + br - cq - dp \\ bp + aq - dr + cs & -bq + ap + ds + cr & -br + as - dp - cq & -bs - ar - dq + cp \\ cp + dq + ar - bs & -cq + dp - as - br & -cr + ds + ap + bq & -cs - dr + aq - bp \\ dp - cq + br + as & -dq - cp - bs + ar & -dr - cs + bp - aq & -ds + cr + bq + ap \end{pmatrix} \\
&= \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \begin{pmatrix} p & -q & -r & -s \\ q & p & s & -r \\ r & -s & p & q \\ s & r & -q & p \end{pmatrix} =: LR \in G_+^+(4, p).
\end{aligned}
$$

In particular, $\forall B \in G_+^+(4, p)$ $\exists\, a, b, c, d, p, q, r, s \in \mathbb{F}_p$ with $a^2 + b^2 + c^2 + d^2 = p^2 + q^2 + r^2 + s^2 = 1$ such that B is of the form above.

Proof. A direct calculation which is omitted here, shows the second equality sign and that with this parametrization $A^T A = I_4$ with I_4 the identity matrix in four dimensions. Furthermore, using 2.4.6 we find that there are $p^3 - p$ solutions $(a, b, c, d) \in \mathbb{F}_p^4$ to the equation $a^2+b^2+c^2+d^2 = 1$. With the existing formula for the usual orthogonal group in four dimensions over the field $\mathbb{F}_p$ as found in, e. g., [1], we see that $|O_{I_4}(4, p)| = 2(p^3-p)^2$. Since $(a, b, c, d), (p, q, r, s) \in \mathbb{F}_p^4$ can be taken independently and since we only consider rotations with positive determinant, we conclude that we have found a parametrization of every element of $G_+^+(4, p)$. □

Unfortunately, we did not find a direct parametrization of the decomposition of this parametrization of gauge transformations in four dimensions into Householder reflections. It seems reasonable to assume that it should be possible to decompose the two matrices L, R whose product forms A in the above lemma, into two reflections, respectively. The naive ansatz of choosing one of the defining vectors of the reflections to be either (a, b, c, d) or (p, q, r, s), respectively, failed because the remaining matrix after multiplying L, R with the inverse of the Householder reflection from either side, respectively, was not symmetric. This means that as in the case of rotations in three dimensions another parametrization should be established which can be more easily transferred into a lower dimensional rotation whose decomposition is already known.

Due to the work of Dickson [3] we deduce the following result in analogy to the Lorentz group.

Theorem 3.2.7. *Let $G_+^+(4, p)$ be the group of proper gauge transformations of $+$-type acting on a 4-dimensional spacetime over the field $\mathbb{F}_p$, $p \equiv 3 \mod 4$, $p > 3$ prime.*

Then, $G_+^+(4, p)$ is generated by rotations which leave a 2-dimensional subspace invariant, and spacetime reversal.

Remark 3.2.8.

1. *The reduced matrix representation of such rotations which only rotate in a 2-dimensional subspace and leave the rest invariant, are very similar to the ones*

of basic rotations used in the study of the Lorentz group. The only difference is that there are more possibilities of combining the four different axes to get a 2*-dimensional plane. Thus, the group containing all such rotations which act on the same plane, is cyclic and isomorphic to* $S^1 \subset \mathbb{F}_{p^2}$ *which leads to a refinement of the statement above.*

2. *The decomposition into Householder reflections in accordance to the Cartan-Dieudonné theorem is then obtain by using the already known decompositions of the rotations in a* 2*- and* 3*-dimensional hyperplane and using the trick of conjugation as described before.*

We have seen that the two types of gauge transformations are intrinsically different but share common features such as their generation by their lowest-dimensional constituents and their possible parametrization by using tuples $(x_1, \ldots, x_m) \in \mathbb{F}_p^m, m > 2$, with the condition $\pm x_1^2 + x_2^2 + \cdots + x_m^2 = \pm 1$. This resembles the defining equation of the quadric which is left invariant by both Lorentz transformations and gauge transformations. We have also seen that gauge transformations of $-$-type are basically Lorentz transformation with another special coordinate axis which resembles time in the case of Lorentz transformations. We want to stress that the gauge transformations of $+$-type leave invariant the set of points with unit time-like distance to the centre point in the affine plane whereas the gauge transformations of $-$-type leave invariant the set of points with unit space-like distance. This shows that the fundamental difference between space- and time-like vectors leads to a different form of the corresponding group of gauge transformations which coincide also with the Lorentz group in the 3-dimensional spatial subspace.

4 The Search for a Connection between the Standard Quadric and a Field Extension

In this last section we want discuss an experimental idea of establishing a connection between the standard quadric and a field extension which uses the fact that an extension field $\mathbb{F}_{p^r}$ of finite degree $r \in \mathbb{N}$ of a finite field $\mathbb{F}_p$ can be seen as an r-dimensional vector space over $\mathbb{F}_p$ with additional multiplicative structure. These two structures seem to be very fitting in the context of quadrics and their symmetry groups.

We will try to sketch two ideas to connect the standard quadric or, in particular, the defining equation of it with forms that come up naturally in a field extension of $\mathbb{F}_p$ of degree 4. Both ideas have, ultimately, not led to a positive result yet.

At first, we notice that using 2.4.6 iteratively for solutions in the affine plane and the hyperplanes at infinity there are in total $|Q^{\pm}| = p^3 + p^2 + p + 1$ points in the standard quadric $Q^{\pm}$ in four dimensions over the field $\mathbb{F}_p, p \equiv 3 \mod 4$. Furthermore, since an extension field $\mathbb{F}_{p^4}$ of $\mathbb{F}_p$ of degree 4 has p^4 elements, its multiplicative group $\mathbb{F}_{p^4}^{\times}$ contains $p^4 - 1$ elements. If we now consider the factor group $\mathbb{F}_{p^4}^{\times}/\mathbb{F}_p^{\times}$, it contains $|\mathbb{F}_{p^4}^{\times}/\mathbb{F}_p^{\times}| = \frac{p^4-1}{p-1} = \frac{(p^3+p^2+p+1)(p-1)}{p-1} = p^3 + p^2 + p + 1 = |Q^{\pm}|$ elements. This possibly suggests that there might exist a bijection between $\mathbb{F}_{p^4}^{\times}/\mathbb{F}_p^{\times}$ and $Q^{\pm}$.

Now, there are two main challenges to connect the structures of the quadric and the one of the quotient group $\mathbb{F}_{p^4}^{\times}/\mathbb{F}_p^{\times}$. Firstly, one has to establish a group multiplication between two points in the quadric and, secondly, one has to determine the most useful parametrization of the extension field.

If we only consider the case of Q^+, 3.1.14 suggests using this kind of 4-dimensional boost which is directly defined by a point in the quadric, as part of the rule for multiplication between two quadric points $p, q \in Q^+$, i. e., $p * q := B_p q$. The advantage is that one can use points in the affine plane as well as ones at infinity and a direct translation between p and B_p is possible. The downside is that these boosts in four dimensions are not closed under standard matrix multiplication which leads in classical special relativity to Thomas precession. In group theoretic considerations this leads to the loss of associativity, i. e., $p * (q * r) = B_p(B_q r) \neq (p * q) * r = B_{B_p q} r$, which, ultimately, means the loss of the group structure with this proposed multiplication of two quadric points.

The second challenge concerns the construction of the field extension $\mathbb{F}_{p^4}/\mathbb{F}_p$. This can be done by using an irreducible polynomial $t \in \mathbb{F}_p[X]$ of degree 4. Then, the quotient ring $\mathbb{F}_p[X]/(t)$ forms a degree 4 extension field of $\mathbb{F}_p$ and is constructed by adjoining a symbol α and its second and third power such that $t(\alpha) = 0$, i. e., $\mathbb{F}_p[X]/(t) \cong \{a + b\alpha + c\alpha^2 + d\alpha^3 \mid a, b, c, d \in \mathbb{F}_p\}$. The structure of the multiplication of two elements heavily depends on the polynomial t since it is done by first multiplying in the usual way and collecting powers of α and afterwards reducing these powers according to $t(\alpha) = 0$. A rather canonical choice for t would be $t = x^4 + x^3 + x^2 + x + 1$ since it is irreducible for all p with $p \equiv 3 \mod 4$. For some primes p it would be more advantageous to chose another polynomial which makes this a possibly impossible search for special cases for every prime p.

Another idea of connecting the structure of the standard quadric to a field extension of degree 4 concerns the defining equation of the standard quadric and a product of elements of the Galois group acting on an element of the extension field. We recall that the defining equation of an element $[x_0 : x_1 : x_2 : x_3 : x_4] \in \mathrm{P}\mathbb{F}_p^4$ to be in one of the standard quadrics $Q^{\pm}$ is given by $-x_0^2 + x_1^2 + x_2^2 + x_3^2 \pm x_4^2 = 0$. After using the projective properties of $\mathrm{P}\mathbb{F}_p^4$ and a rescaling of the equation we find a polynomial in four variables $M \coloneqq -x_0^2 + x_1^2 + x_2^2 + x_3^2 \in \mathbb{F}_p[X_0, X_1, X_2, X_3]$. Points q in the quadric $Q^{\pm}$ are then solutions of $M(q) = \mp 1$.

As before, consider now an extension field $\mathbb{F}_{p^4} = \mathbb{F}_p[X]/(t)$ of $\mathbb{F}_p$ for some irreducible polynomial $t \in \mathbb{F}_p[X]$. The Galois group of this field extension is generated by the Frobenius map $\varphi : \mathbb{F}_{p^4} \to \mathbb{F}_{p^4}, x \mapsto x^p$. The Galois group consists of four elements and is given by $\mathrm{Gal}(\mathbb{F}_{p^4}/\mathbb{F}_p) = \{\mathrm{id}, \varphi, \varphi^2, \varphi^3\}$. If we now consider for $x = x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3 \in \mathbb{F}_{p^4}$ the product $\tilde{x} \coloneqq x\varphi(x)\varphi^2(x)\varphi^3(x)$, we see that it is invariant under the action of elements of the Galois group, i. e., $\varphi(\tilde{x}) = \tilde{x}$ since $\varphi^4 = \mathrm{id}$ and the multiplication is commutative, and, thus, $\forall x \in \mathbb{F}_{p^4} : \tilde{x} \in \mathbb{F}_p$. It is also a polynomial in four variables x_0, x_1, x_2, x_3 of degree 4. Since the Galois group contains field automorphisms, the product $\tilde{x}$ is multiplicative, i. e., $\forall x, y \in \mathbb{F}_{p^4} : \widetilde{(xy)} = \tilde{x}\tilde{y}$. Because of the reduction of powers of α according to $t(\alpha) = 0$, the product $\tilde{x}$, again, heavily depends on t.

The hope is to find a suitable polynomial t such that M is divisor of $\tilde{x}$, i. e., $\exists\, u \in \mathbb{F}_p[X_0, X_1, X_2, X_3] : \tilde{x} = Mu$. Then, we would have found a reasonable connection between the standard quadric and a field extensions of $\mathbb{F}_p$. Since a quadric points q is given be $M(q) = \pm 1$, this would translate to searching for solutions to $\tilde{x} = \pm u(x)$ which becomes extremely easy if, e. g., $u(x) = \pm 1$, i. e., $\tilde{x} = M^2$.

Unfortunately, next to the freedom in choosing t we also have the freedom to choose the right parametrization of x. The most canonical way would be to directly translate a quadric point $[x_0 : x_1 : x_2 : x_3 : 1]$ to $x = x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3$. But it would also be possible to use any non-degenerate transformation, e. g., $x_0 \to x_0 + x_1, x_1 \to x_0 - x_1$. With symbolic calculations in Maple™[8] in the case of $p = 7$ using the method of finding the intersection of two polynomial ideals, i. e., in this case the ideals generated by M and $\tilde{x}$, and using the parametrizations described above, we did not find the intersection of both ideals to be generated by a polynomial whose degree is lower than the degree of the product of M and $\tilde{x}$. This would be the case if we would have found a real divisor in M since $(\tilde{x}) \subset (M) \iff M$ divides $\tilde{x}$. Since symbolic finite field arithmetic is not properly included in Maple™, a trial and error search using different parametrizations of x while using the same polynomial t led to an unreasonable amount of computational time. Thus, we did not find a suitable parametrization of x and have to stay looking for a connection between the standard quadric and a field extension of $\mathbb{F}_p$.

We conclude that it is hard to find a canonical relation between the standard Minkwoski quadric and a field extension of degree 4 of $\mathbb{F}_p$ since there are too many degrees of freedom in choosing the polynomial t which, ultimately, depends on the prime p, and the parametrization of x. Thus, it seems unreasonable to assume that a proper guess of t and x might lead to the right result which could be in the worst case only appropriate for a few primes p and not in full generality.

5 Resume and Outlook

In this thesis we have discussed some algebraic properties of two subgroups of the symmetry group of the standard Minkwoski quadric, namely, the group of Lorentz transformations and the one of gauge transformations. We have seen that there are two types ($\pm$) of gauge transformations and that the $-$-type of them is closely related to the group of Lorentz transformations. It was shown that in two dimensions the groups of both types of gauge transformations as well as the Lorentz group are cyclic, i. e., are generated by only one element. We have also established isomorphisms between the group of basic rotations in one plane and the group of elements of unit norm in the multiplicative group of the extensions field $\mathbb{F}_{p^2}$ and between the group of Lorentz transformations in two dimensions and the multiplicative group of the finite field $\mathbb{F}_p$. Where possible, a direct parametrization of the decomposition of symmetry transformations into Householder reflections according to the Cartan-Dieudonné theorem was given and discussed. In future work this could be made more explicit in some cases. In the end we gave two ideas of connecting the structure of the standard quadric and a field extension of degree 4, namely a direct translation using products with 4-dimensional boosts and the multiplicative group of the extension field and, secondly, a more structural connection using the polynomial which is given by the product of Galois automorphisms acting on an element of the extension field and the standard Minkowski form. Unfortunately, both ideas did not yield positive results. This problem may be solved in future research and would give another reason to use a finite field instead of the field of real numbers since there are a lot more field extensions possible than in the case of the field of real numbers $\mathbb{R}$. Ultimately, this freedom is also the downfall of the idea presented.

The steps performed in this thesis could be translated to the case of a non-flat spacetime, i. e., with a non-Minkowski quadratic form which may lead to new insight into the structure of this spacetime and their quadrics. Also the structure of the group of gauge transformations of $+$-type in more generality could be studied in the context of a theory of interactions as in quantum field theory. One could also follow a conjecture that a intersection of two quadrics may be left invariant by the group of gauge transformations with the full definition of such transformations.

Danksagung

Zuallererst möchte ich mich bei Prof. Dr. Klaus Mecke für die Möglichkeit, an einem so interessanten Thema arbeiten zu können, und für die regelmäßigen neuen Ideen und Hilfestellungen bedanken. Außerdem danke ich Alexander Laska für die gute Unterstützung, das Korrekturlesen der Arbeit und die wertvollen Tipps im Rahmen der Besprechung dieser Arbeit. Zudem richte ich meinen Dank an meine Freunde, insbesondere an Hans Liegener, der durch hilfreiche Ideen und das Beantworten einiger Fragen bei mathematischen Unklarheiten den Entstehungsprozess wie die zuvor genannten Personen wohlwollend und konstruktiv begleitet hat. Zuletzt möchte ich meiner Familie danken, die mich bei der Ausarbeitung der Arbeit mental unterstützt hat.

References

[1] Emil Artin. *Geometric algebra.* Courier Dover Publications, 2016.

[2] Élie Cartan. *The theory of spinors.* Courier Corporation, 2012.

[3] Leonard Eugene Dickson. Determination of the structure of all linear homogeneous groups in a galois field which are defined by a quadratic invariant. *American Journal of Mathematics*, 21(3):193–256, 1899.

[4] Jean Dieudonné. *Sur les Groupes Classiques*, volume 1040 of *Actualités scientifiques et industrielles.* Hermann, Paris, 1967.

[5] Stephan Foldes. The lorentz group and its finite field analogs: Local isomorphism and approximation. *Journal of Mathematical Physics*, 49(9):093512, 2008.

[6] C. Karpfinger and K. Meyberg. *Algebra: Gruppen - Ringe - Körper.* Springer Berlin Heidelberg, 2017.

[7] Rudolf Lidl and Harald Niederreiter. *Finite Fields.* Encyclopedia of Mathematics and its Applications. Cambridge University Press, second edition, 1996.

[8] Maple (2017.0). Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario, 2017. Maple is a trademark of Waterloo Maple Inc.

[9] Klaus Mecke. Biquadrics configure finite projective geometry into a quantum spacetime. *EPL (Europhysics Letters)*, 120(1):10007, 2017.

[10] L. van Elfrinkhof. Eene eigenschap van de orthogonale substitutie van de vierde orde. In *Handelingen van het zesde Nederlandsch Natuuren Geneeskundig Congres*, pages 237–240, 1897.

Erklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, dass alle Stellen der Arbeit, die wörtlich oder sinngemäß aus anderen Quellen übernommen wurden, als solche kenntlich gemacht sind und dass die Arbeit in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegt wurde.

Erlangen, den 27. Februar 2019 ______________________________