TECHNISCHE
UNIVERSITÄT
WIEN

DIPLOMARBEIT

Reducts of Countable Vector Spaces over Finite Fields

ausgeführt am

Institut für
Diskrete Mathematik und Geometrie
TU Wien

unter der Anleitung von

Associate Prof. Dipl.-Ing. Dr.techn. Michael Pinsker

durch

Felix Schiffer

Matrikelnummer: 01326508

Wien, am 17.Mai 2021

Kurzfassung

Wir untersuchen die Redukte eines abzählbar unendlichen Vektorraums über einem Primkörper ungerader Charakteristik. Insbesondere beantworten wir die Frage, ob die Anzahl solcher Redukte bis auf Interdefinierbarkeit endlich ist oder nicht.

Wir verwenden eine Verbindung, die durch das Ryll-Nardzewski--Theorem gegeben ist: die Redukte einer abzählbaren ω-kategorischen Struktur entsprechen, bis auf Interdefinierbarkeit, genau den abgeschlossenen Permutationsgruppen auf der Domäne der Struktur, die deren Automorphismen enthalten. Nachdem ein abzählbar unendlicher Vektorraum über einem endlichen Körper ω-kategorisch ist, untersuchen wir also die abgeschlossenen Permutationsgruppen auf der Menge der Vektoren, die über den Vektorraumautomorphismen liegen. Wir beginnen mit den Permutationsgruppen, die den Nullvektor festhalten, und gehen danach über zu den Permutationsgruppen, die den Nullvektor verschieben können. Wir können zeigen, dass es tatsächlich nur endlich viele solcher Gruppen gibt. Insbesondere schließen wir daraus, dass ein abzählbar unendlicher Vektorraum über einem endlichen Primkörper ungerader Charakteristik, bis auf Interdefinierbarkeit, nur endlich viele Redukte hat.

Abstract

We investigate the first-order reducts of a countably infinite vector space over a prime field of odd characteristic. In particular we answer the question whether or not the number of such reducts is finite up to interdefinability.

We utilize a connection given by the Ryll-Nardzewski Theorem, namely that the first-order reducts of an ω-categorical structure are, up to interdefinability, in one-to-one correspondence with the closed permutation groups on the domain of said structure which contain its automorphisms. Since any countable vector space over a finite field is ω-categorical, we examine the closed permutation groups on the set of vectors which contain the vector space automorphisms. We start with the closed permutation groups on the set of vectors which fix the zero vector, and then continue with groups which specifically do move the zero vector. We are able to show that there exist indeed only finitely many such groups. From this we immediately obtain that there are, up to interdefinability, only finitely many first-order reducts of our structure.

Contents

Introduction

Given a structure $\mathcal{A}$, another structure $\mathcal{B}$ is a *first-order reduct* of $\mathcal{A}$ if $\mathcal{A}$ and $\mathcal{B}$ have the same domain and all operations and relations of $\mathcal{B}$ are first-order definable in $\mathcal{A}$. Two structures which are first-order reducts of one another are called *interdefinable*. In this thesis the role of the first structure $\mathcal{A}$ is taken by a countably infinite dimensional vector space $\mathcal{V}$ over a finite prime field of uneven characteristic. Our goal is to show that the number of first-order reducts of $\mathcal{V}$ is finite up to interdefinability.

A first-order reduct of $\mathcal{V}$ which is not interdefinable with $\mathcal{V}$ is for example the structure (V, R), where V is the set of vectors of $\mathcal{V}$, and the four-ary relation R is given by $(a, b, c, d) \in R$ iff $a + b = c + d$. Any translation is an automorphism of the structure (V, R). As a consequence, the zero vector cannot be first-order definable in (V, R), hence (V, R) and $\mathcal{V}$ are not interdefinable.

In the case of an ω-categorical structure $\mathcal{A}$ its first-order reducts are, up to interdefinability, in one-to-one correspondence with the closed permutation groups on its domain which contain the automorphism group of $\mathcal{A}$. Therefore, instead of directly searching for first-order reducts of $\mathcal{V}$, we may investigate the closed permutation groups lying between the automorphism group of $\mathcal{V}$ and the full symmetric group on its domain.

The structure of this thesis is as follows. In Chapter 1 we recall some basic definitions from Algebra and Model Theory and establish a fixed notation we will be using throughout the thesis. In Chapter 2, we state the theorems that enable us to study the closed supergroups of the automorphism group of a structure instead of its first-order reducts. We also observe that our assumptions suffice to apply said theorems. For the rest of the thesis we will solely tread this path and investigate the closed supergroups of the automorphism group of $\mathcal{V}$. In Chapter 3 we consider the case in which a permutation group on the set of vectors fixes the zero vector. In Chapter 4 we investigate permutation groups that do not fix the zero vector.

This master thesis is based on a paper draft written by Bertalan Bodor, Kenda Kalina and Csaba Szabó. The main contributions of this master thesis are closing gaps, adapting the Fundamental Theorems of Projective and Affine Geometry to a countable infinite setting, generalizing results, most notably Section 3.1 and Lemma 4.10, as well as adapting and clarifying various proof ideas.

I would like to thank M. Pinsker for his feedback and many helpful suggestions.

1. Notation

We recall some basic facts from Algebra, in particular from Linear Algebra, which we are going to need on a regular basis. For proof of said facts as well as an introduction to Algebra we refer to [8], [7] or [5].

1.1. **Relations.** Let S be a set and let $n \geq 0$. The cardinality of S is denoted by $|S|$. A subset R of S^n is an *n-ary relation* R of S. If R is a binary relation on S and (a, b) an ordered pair in S^2, we write $a\ R\ b$ iff $(a, b) \in R$. Let $\sim$ be an equivalence relation on S. For an element $s \in S$ the equivalence class of s is denoted by $[s]_\sim$. Every element in $[s]_\sim$ is called a *representative of the equivalence class* $[s]_\sim$.

1.2. **Operations.** Let S be a set and let $n \geq 0$. An n-ary *operation* on S is a function from S^n into the set S. A zero-ary operation is called a *constant*; it takes only a single element of S as value.

1.3. **Structures.** A tuple $\mathcal{A} = (A, (t_i)_{i\in I}, (R_j)_{j\in J})$ is called a *(first-order) structure* in the signature $((t_i, m_i)_{i\in I}, (R_j, m_j)_{j\in J})$ iff

- A is a set, called the *domain of* $\mathcal{A}$,
- $(t_i)_{i\in I}$ is a tuple of operations on A,
- $(R_j)_{j\in J}$ is a tuple of relations on A,
- for all $i \in I$ the operation t_i is of arity m_i,
- for all $j \in J$ the relation R_j is of arity n_j.

If the signature is known from context, we usually refrain from mentioning it explicitly. We will, if not otherwise specified, denote structures by a letter in calligraphic font, such as $\mathcal{A}$, and the corresponding domain by the same letter in plain font, such as A. The tuple of relations might be empty; a structure of this form is called an *algebraic structure* or *algebra*. For example a group may be formalized as an algebraic structure in the signature $(((0, 0), (+, 2), (-, 1)), \emptyset)$. On the other hand a structure without operations is called a *relational structure*.

1.4. **Groups.** Let $\mathcal{G}$ be a group. For a subgroup $\mathcal{H}$ of $\mathcal{G}$ we write $\mathcal{H} \leq \mathcal{G}$. If a subgroup $\mathcal{N}$ is normal in $\mathcal{G}$ we denote this by $\mathcal{N} \lhd \mathcal{G}$. The *order* of an element $g \in G$ is the size of the smallest subgroup of $\mathcal{G}$ which contains g. For $\mathcal{H} \leq \mathcal{G}$ and $\mathcal{N} \lhd \mathcal{G}$ the group $\mathcal{G}$ is the *semi-direct product* $\mathcal{H} \ltimes \mathcal{N}$ iff $G = HN = \{h + n : h \in H, n \in N\}$ and $H \cap N = \{0\}$, if $+$ denotes the binary group operation of $\mathcal{G}$ and 0 its neutral element.

Let $f\colon A \to B$ and $g\colon B \to C$ be functions. Then $f \circ g$ denotes the composition such that for all $a \in A : (f \circ g)(a) := g(f(a))$. Sometimes we write a^{fg} for $(f \circ g)(a)$, in line with the notation $a^f := f(a)$. For a set $S \subseteq A$ we define $S^f := \{s^f : s \in S\}$. We denote the restriction of f to S by $f|_S \colon S \to B$. In this case f is an *extension of* $f|_S$. The identity function on S is denoted by $\mathrm{id}_S \colon S \to S$.

The group of all bijective functions on A is *the full symmetric group on* A and is denoted by $\mathrm{Sym}(A)$. Let G be a set of bijective functions such that all $f \in G$ have domain and codomain A, and

- the identity on A is an element of G,
- for every $f \in G$ also $f^{-1} \in G$, and
- for all $f, g \in G$ also $f \circ g \in G$.

Then $\mathcal{G} = (G, \mathrm{id}_A, \circ, \cdot^{-1})$ is a *permutation group* on A and a subgroup of $\mathrm{Sym}(A)$.

For a subset S of A the subgroup of $\mathcal{G}$ consisting of all functions of $\mathcal{G}$ which fix S element-wise is called the *stabilizer of* S and is denoted by $\mathcal{G}_S$. If S consists only of finitely many elements $x_1, \ldots, x_n \in A$ we write $\mathcal{G}_{x_1,\ldots,x_n}$ instead of $\mathcal{G}_{\{x_1,\ldots,x_n\}}$. For a function $f \in \mathrm{Sym}(A)$ and two sets of functions $S, K \subseteq \mathrm{Sym}(A)$ we introduce the following notation:

$$\begin{aligned} f \circ S &:= \{f \circ g : g \in S\} \subseteq \mathrm{Sym}(A), \\ S \circ f &:= \{g \circ f : g \in S\} \subseteq \mathrm{Sym}(A), \text{ and} \\ S \circ K &:= \{g \circ h : g \in S, h \in K\} \subseteq \mathrm{Sym}(A). \end{aligned}$$

Let $\mathcal{A} = (A, (t_i)_{i \in I}, (R_j)_{j \in J})$ be a first-order structure in the signature $((t_i, m_i)_{i \in I}, (R_j, n_j)_{j \in J})$. The *automorphism group of* $\mathcal{A}$, denoted by $\mathrm{Aut}(\mathcal{A})$, is the subgroup of $\mathrm{Sym}(A)$ consisting of all $g \in \mathrm{Sym}(A)$ such that for all $i \in I$

$$\forall a = (a_1, \ldots, a_{m_i}) \in A^{m_i} : \; g(t_i(a)) = t_i(g(a_1), \ldots, g(a_{m_i})),$$

and for every $j \in J$

$$\forall a = (a_1, \ldots, a_{n_j}) \in A^{n_j} : a \in R_j \iff (g(a_1), \ldots, g(a_{n_j})) \in R_j.$$

1.5. **Closedness.** Let A be a set. A subset S of $\mathrm{Sym}(A)$ is *closed with respect to the pointwise convergence topology* iff for all $f \in \mathrm{Sym}(A)$ such that for every finite subset $F \subseteq A$ there exists a function $g \in S$ such that $g|_F = f|_F$ we have $f \in S$.

A sequence $(f_n)_{n \geq 0}$ of functions in $\mathrm{Sym}(A)$ is *convergent* iff there exists a function $f \in \mathrm{Sym}(A)$ such that for all $a \in A$ exists $n \geq 0$ such that for all $N > n : f_N(a) = f(a)$. The function f is the *limit of* $(f_n)_{n \geq 0}$. Using this we give an alternative and equivalent definition of closedness: a subset S of $\mathrm{Sym}(A)$ is closed iff the limit of every convergent sequence of functions in S lies in S.

A permutation group $\mathcal{G} \leq \mathrm{Sym}(S)$ on S is *closed* iff G is.

1.6. **Fields.** For a field $\mathcal{F} = (F, 0, +, 1, \cdot)$ the constant 0 denotes the neutral element of the addition $+$ and the constant 1 denotes the neutral element of the multiplicative group with domain $F^\times := F \setminus \{0\}$. For any two elements $a \in F$ and $b \in F^\times$ we write $\frac{a}{b} := a \cdot b^{-1}$, where b^{-1} denotes the multiplicative inverse of b.

The *characteristic* of a field $\mathcal{F}$, denoted by $\operatorname{char} \mathcal{F}$, is the order of 1 in the group $(F, 0, +, -)$ if the order is finite, otherwise $\operatorname{char} \mathcal{F}$ is zero. For every prime number p and every $n \geq 1$ the field containing exactly p^n elements is denoted by $\mathbb{F}_{p^n}$. This field is unique up to isomorphism.

The characteristic of $\mathbb{F}_{p^n}$ is always p. The multiplicative group $\mathbb{F}_{p^n}^\times$ is cyclic.

Two important identities which hold in every finite field $\mathbb{F}_{p^n}$ are

- for every $a \in \mathbb{F}_{p^n} : a^{p^n} = a$, and
- for all $a, b \in \mathbb{F}_{p^n} : (a \pm b)^p = a^p \pm b^p$.

The prime field $\mathbb{F}_p$ is isomorphic to the integers modulo p.

1.7. **Vector Spaces.** Let $\mathcal{V} = (V, \mathbf{0}, +, -, (s_f)_{f \in F})$ be a vector space over a field $\mathcal{F}$. The constant $\mathbf{0}$ denotes the zero vector of $\mathcal{V}$ and for every $f \in F$ the operation s_f denotes the scalar multiplication which maps a vector $v \in V$ to $fv \in V$.

The *linear closure* of a set $S \subseteq V$, denoted by $\langle S \rangle$, is the set of all possible linear combinations $\sum_{s \in S} c_s s$ such that *almost all*, i.e., all but finitely many, coefficients $c_s \in F$ are equal to zero. For finitely many vectors $v_1, \ldots, v_n \in V$ we write $\langle v_1, \ldots, v_n \rangle$ instead of $\langle \{v_1, \ldots, v_n\} \rangle$. We say that $W \subseteq V$ is a *subspace of* $\mathcal{V}$ if W induces a substructure of the vector space $\mathcal{V}$, in this case we write $W \leq \mathcal{V}$. We denote the set of all subspaces of $\mathcal{V}$ by $\mathrm{S}(\mathcal{V})$ and the set of all one-dimensional subspaces of $\mathcal{V}$ by $\mathrm{S}_1(\mathcal{V})$. The dimension of a subspace $W \leq \mathcal{V}$ is denoted by $\dim W$. Moreover, for two subspaces $W, U \leq \mathcal{V}$ the *sum* $W + U$ is the linear closure of $W \cup U$. This notation can be extended to an arbitrary family of subspaces $(W_i)_{i \in I}$ of $\mathcal{V}$ and we write in this case $\sum_{i \in I} W_i$.

For another vector space $\mathcal{W}$ over the same field $\mathcal{F}$ and $\alpha \in \operatorname{Aut}(\mathcal{F})$, a function $\varphi \colon V \to W$ is *semi-linear with respect to* α iff for all $v, w \in V$ and all $c \in F$

- $\varphi(v + w) = \varphi(v) + \varphi(w)$, and
- $\varphi(cv) = c^\alpha \varphi(v)$.

The inverse of a bijective semi-linear function is also semi-linear. The group of all invertible semi-linear functions from $\mathcal{V}$ to $\mathcal{V}$ is denoted by $\Gamma\mathrm{L}(\mathcal{V})$. Clearly $\Gamma\mathrm{L}(\mathcal{V}) \leq \operatorname{Sym}(V)$. A semi-linear function with respect to $\mathrm{id}_F \in \operatorname{Aut}(\mathcal{F})$ is a *linear function*. The linear invertible functions from $\mathcal{V}$ to $\mathcal{V}$ are exactly the automorphisms of $\mathcal{V}$.

1.8. **Affine Spaces.** Let $\mathcal{V} = (V, \mathbf{0}, +, (s_f)_{f\in F})$ be a vector space. An *affine space* is a set A and an action $+_A\colon A \times V \to V$ of the additive group of $\mathcal{V}$ on A such that for all $a \in A$ and $v, w \in V$ we have

- $a +_A \mathbf{0} = a$,
- $(a +_A v) + w = a +_A (v + w)$, and
- the mapping $\mathcal{V} \to A\colon v \mapsto a +_A v$ is a bijection.

We will always assume A to be a subset of V and $+_A$ will always be the addition in the vector space $\mathcal{V}$. In this case we call A an *affine subspace of* $\mathcal{V}$. We have that A is an affine subspace of $\mathcal{V}$ iff for any $v \in A$ the set $A - v = \{a - v \in V : a \in A\}$ is a subspace of $\mathcal{V}$. This subspace does not depend on the choice of $v \in A$. The *dimension* of an affine subspace of $\mathcal{V}$ is the dimension of the corresponding subspace of $\mathcal{V}$. For a set of vectors $S \subseteq V$ we write $\operatorname{Aff}(S)$ for the *affine closure* of S in V which is the set of all *affine combinations*, i.e., all $\sum_{s\in S} c_s s$ such that almost all $c_s \in F$ are zero and the sum $\sum_{s\in S} c_s$ equals $1 \in F$. For finitely many $v_1, \dots, v_n \in V$ we write $\operatorname{Aff}(v_1, \dots, v_n)$ instead of $\operatorname{Aff}(\{v_1, \dots, v_n\})$. The affine closure $\operatorname{Aff}(S)$ is the smallest affine subspace of $\mathcal{V}$ containing S.

Given $\alpha \in \operatorname{Aut}(\mathcal{F})$ a *semi-affine mapping with respect to* α is a function $\psi\colon A \to A'$ from one affine subspace A of $\mathcal{V}$ to another affine subspace A' of $\mathcal{V}$ such that for all $S \subseteq A$ and all affine combinations $\sum_{s\in S} c_s s$ we have

$$\psi\left(\sum_{s\in S} c_s s\right) = \sum_{s\in S} c_s \psi(s).$$

A bijective semi-affine mapping with respect to id_F is called an *affine mapping*. The set of all affine mappings from V to V is denoted by $\operatorname{AGL}(\mathcal{V})$ and the set of all bijective semi-affine functions from V to V is denoted by $\mathrm{A\Gamma L}(\mathcal{V})$.

2. First-order Reducts and Permutation Groups

We will state the exact relation between the first-order reducts of an ω-categorical structure and the closed permutation groups containing its automorphism group. At the end of this chapter we show that this relation applies in the case of a countably infinite dimensional vector space over a finite field, and we will fix the structure we consider in this thesis. For an introduction into Model Theory we recommend [6].

Let S be a set, let $\mathcal{G}$ be a permutation group on S and let $s = (s_1, \ldots, s_n) \in S^n$ for some $n \geq 1$. Then the *n-orbit of s* is the set $G(s) := \{s^g : g \in G\}$, where $s^g := (s_1^g, \ldots, s_n^g)$.

Definition 2.1. Let S be a set and let $\mathcal{G}$ be a permutation group on S. The group $\mathcal{G}$ is *oligomorphic* iff for every $n \geq 1$ the set of n-orbits $\{G(s) : s \in S^n\}$ is finite.

We note that by expanding a permutation group the number of orbits can only decrease, therefore any supergroup of an oligomorphic group is still oligomorphic.

A *theory* is a set of first-order *sentences*, i.e., first-order formulas without free variables, over a signature L. We say that a structure $\mathcal{A}$ in the signature L is a *model* of a theory T iff every sentence ψ of T is true in $\mathcal{A}$, which we denote by $\mathcal{A} \vDash \psi$. *The theory of a structure* is the set of all first-order sentences which are true in the structure.

Definition 2.2. A theory is *ω-categorical* iff it has, up to isomorphism, only one countable model. A structure is *ω-categorical* iff its theory is ω-categorical.

Theorem 2.3. *Let $\mathcal{A}$ be a structure on a countably infinite domain. Then $\mathcal{A}$ is ω-categorical iff the automorphism group* $\mathrm{Aut}(\mathcal{A})$ *is oligomorphic.*

This is only a part of the Theorem of Engeler, Ryll-Nardzewski and Svenonius. For the full theorem and proof thereof see [6, p. 171].

Definition 2.4. Let $\mathcal{A}$ be a structure and $n \geq 0$. An n-ary operation $d \colon A^n \to A$ is *first-order definable over $\mathcal{A}$* iff there exists a first-order formula $\psi(x, y)$ over the signature of $\mathcal{A}$ such that

$$\forall a \in A^n \; \forall b \in A : \; d(a) = b \leftrightarrow \mathcal{A} \vDash \psi(a, b).$$

Similarly an n-ary relation $R \subseteq A^n$ is *first-order definable over $\mathcal{A}$* iff there exists a first-order formula $\psi(x)$ over the signature of $\mathcal{A}$ such that

$$\forall a \in A^n : \; a \in R \leftrightarrow \mathcal{A} \vDash \psi(a).$$

Definition 2.5. Let $\mathcal{A}$ be a structure. A structure $\mathcal{B}$ on the same domain A is a *first-order reduct* of $\mathcal{A}$ iff all operations and all relations of $\mathcal{B}$ are first-order definable over $\mathcal{A}$. Two structures which are first-order reducts of each other are called *interdefinable*.

Since we are only interested in first-order reducts we omit "first-order" from now on and write "$\mathcal{A}$ is a reduct of $\mathcal{B}$". If a structure is a reduct of another structure, then the two automorphism groups relate in the following way.

Theorem 2.6. *Let $\mathcal{B}$ be a reduct of a structure $\mathcal{A}$. Then* $\mathrm{Aut}(\mathcal{B})$ *is a supergroup of* $\mathrm{Aut}(\mathcal{A})$*.*

Proof. Given an arbitrary relation $R \subseteq A^n$ of $\mathcal{B}$ there is a first-order formula $\psi(x_1, \dots, x_n)$ over the signature of $\mathcal{A}$ such that for all tuples $(a_1, \dots, a_n) \in A^n$ we have $(a_1, \dots, a_n) \in R \leftrightarrow \mathcal{A} \models \psi(a_1, \dots, a_n)$. Let α be an arbitrary automorphism of $\mathcal{A}$. For every $(a_1, \dots, a_n) \in A^n$ we have

$$\mathcal{A} \models \psi(a_1^\alpha, \dots, a_n^\alpha) \leftrightarrow \mathcal{A} \models \psi(a_1, \dots, a_n).$$

By the same argument this also holds for all operations of $\mathcal{B}$, hence $\alpha \in \mathrm{Aut}(\mathcal{B})$. □

Let $\mathcal{A}$ be a structure. If for an arbitrary function $f \in \mathrm{Sym}(\mathcal{A})$ for every finite subset $F \subseteq A$ there exists $\alpha \in \mathrm{Aut}(\mathcal{A})$ such that $\alpha|_F = f|_F$, then f satisfies the conditions for being an automorphism and thus lies in $\mathrm{Aut}(\mathcal{A})$. Therefore the automorphism group of a structure is always closed.

The proof of Theorem 2.7 follows from the full version of Theorem 2.3 and shall be omitted.

Theorem 2.7. *Let $\mathcal{A}$ be a structure and let $\mathcal{G}$ be a closed permutation group on A containing* $\mathrm{Aut}(\mathcal{A})$*. Then there exists a reduct $\mathcal{B}$ of $\mathcal{A}$ such that* $\mathrm{Aut}(\mathcal{B}) = \mathcal{G}$*.*

For an ω-categorical structure Theorem 2.6 and Theorem 2.7 show that its reducts are, up to interdefinability, in one-to-one correspondence with the closed permutation groups lying between the automorphism group of said structure and the full symmetric group on its domain.

It remains to be shown that the structure we are interested in, i.e., a countably infinite dimensional vector space over a finite field, is ω-categorical.

Lemma 2.8. *Let $\mathcal{W}$ be a countably infinite dimensional vector space over a finite field $\mathcal{F}$. Then $\mathcal{W}$ is ω-categorical.*

Proof. Let T be the theory of $\mathcal{W}$. The vector space axioms are contained in T, hence every countably infinite model of T is a vector space over $\mathcal{F}$. Let $\mathcal{M}$ be such a model. The dimension of $\mathcal{M}$ cannot be finite, since if $\dim \mathcal{M} = n \geq 0$, then the number of vectors would total $|F|^n < \infty$. The number of elements in $\mathcal{M}$ is countably infinite, thus the dimension of $\mathcal{M}$ cannot be of higher cardinality. Therefore, $\dim \mathcal{M}$ is countably infinite, hence $\mathcal{M}$ and $\mathcal{W}$ are isomorphic. □

We note that a countably infinite vector space has to be over a finite field for it to be ω-categorical. To see this let $\mathcal{W}$ be a vector space over a field $\mathcal{R}$. Let v be a non-zero vector of $\mathcal{W}$. For distinct $r_1, r_2 \in R$ the tuples $(v, r_1 v)$ and $(v, r_2 v)$ lie in different two-orbits of $\mathrm{Aut}(\mathcal{W})$. If R is infinite there are infinitely many different possibilities for r_1 and r_2 and none of the corresponding orbits coincide. But then $\mathcal{W}$ does not have an oligomorphic automorphism group and is therefore not ω-categorical.

We now fix the structure we are considering in the first sections of this thesis. From Section 3.2 on we will further restrict us to prime fields. But for now and until we explicitly state otherwise let p be an odd prime, let $m \geq 1$, and

let $\mathcal{V}$ be a countably infinite dimensional
vector space over the field $\mathbb{F}_{p^m}$.

We will restate this, and any further fixed assumptions of a chapter or section, only in the main results to ensure that they may be read on their own.

Our goal is to show that there are only finitely many reducts of $\mathcal{V}$ up to interdefinability. We only manage to do so for the case $m = 1$. Nevertheless, the results of the first few sections also hold in the general case. We know by Theorem 2.6 and Theorem 2.7 that it suffices to show that the number of closed permutation groups on its domain which contain $\mathrm{Aut}(\mathcal{V})$ is finite. We will start in Chapter 3 with the supergroups of $\mathcal{V}$ which fix $\mathbf{0}$.

3. The closed supergroups of $\mathrm{Aut}(\mathcal{V})$ fixing $\mathbf{0}$

For the rest of this chapter let $\mathcal{G}$ be a closed permutation group on V such that

$$\mathrm{Aut}(\mathcal{V}) \leq \mathcal{G} \leq \mathrm{Sym}(V)_{\mathbf{0}}.$$

Our goal is to investigate the structure of $\mathcal{G}$. In particular we examine the action of $\mathcal{G}$ on the set of equivalence classes of a suitable equivalence relation.

Definition 3.1. Let Γ be a multiplicative subgroup of $\mathbb{F}_{p^m}^{\times}$. We define an equivalence relation $\sim_\Gamma$ on V by setting for all $v, w \in V$:

$$v \sim_\Gamma w \text{ iff } \text{ for some } \lambda \in \Gamma\colon v = \lambda w.$$

We note that for all $\Gamma \leq \mathbb{F}_{p^m}^{\times}$:

- This is an equivalence relation since Γ is a group.
- Two linearly independent vectors can never be equivalent, i.e., for all $v \in V$ the equivalence class $[v]_{\sim_\Gamma}$ is contained in $\langle v \rangle$.
- The equivalence class of $\mathbf{0}$ is $\{\mathbf{0}\}$.

If we want $\mathcal{G}$ to act on the equivalence classes of $\sim_\Gamma$ we we need that $\sim_\Gamma$ is $\mathcal{G}$*-invariant*, i.e., for every $g \in G$ and for all $v, w \in V$ we have that $v \sim_\Gamma w$ implies $v^g \sim_\Gamma w^g$. The subgroup Γ of $\mathbb{F}_{p^m}^{\times}$ needs to be of a specific form for this to be possible. To find such Γ we look for another equivalence relation which will obviously be $\mathcal{G}$-invariant and then show that there is a group $\Gamma \leq \mathbb{F}_{p^m}^{\times}$ such that the two definitions describe the same equivalence relation.

The automorphisms of $\mathcal{V}$ are not able to split two vectors which lie in the same one-dimensional subspace of $\mathcal{V}$ – “split” meaning that the vectors would be mapped into different one-dimensional subspaces of $\mathcal{V}$ by an element of $\mathrm{Aut}(\mathcal{V})$. However, $\mathcal{G}$ might be able to split two vectors which are linearly dependent. With this in mind, another auspicious relation is the following.

Definition 3.2. Let $\mathcal{H}$ be a subgroup of $\mathrm{Sym}(V)_{\mathbf{0}}$. We define an equivalence relation $\sim_{\mathcal{H}}$ on V such that for all vectors $v, w \in V$:

$$v \sim_{\mathcal{H}} w \text{ iff for all } h \in H\colon \langle v^h \rangle = \langle w^h \rangle.$$

We note that for all $\mathcal{H} \leq \mathrm{Sym}(V)_{\mathbf{0}}$:

- Two linearly independent vectors can never be equivalent under $\sim_{\mathcal{H}}$. In particular for every $v \in V$ we have $[v]_{\sim_{\mathcal{H}}} \subseteq \langle v \rangle$.
- The relation $\sim_{\mathcal{H}}$ is invariant under $\mathcal{H}$:

$$\forall h \in H\ \forall v, w \in V\colon\ v \sim_{\mathcal{H}} w \iff v^h \sim_{\mathcal{H}} w^h. \tag{1}$$

- The equivalence class of $\mathbf{0}$ is just $\{\mathbf{0}\}$.

This already looks similar to what we noted about $\sim_\Gamma$. Indeed we can show that for any $\mathcal{H} \leq \mathrm{Sym}(V)_{\mathbf{0}}$ which contains $\mathrm{Aut}(\mathcal{V})$ there exists a group $\Gamma \leq \mathbb{F}_{p^m}^\times$, whose domain we also denote by Γ, such that the two equivalence relations $\sim_\mathcal{H}$ and $\sim_\Gamma$ coincide.

Lemma 3.3. *Let $\mathcal{H}$ be a subgroup of $\mathrm{Sym}(V)_{\mathbf{0}}$ containing $\mathrm{Aut}(\mathcal{V})$. Then there exists a group $\Gamma \leq \mathbb{F}_{p^m}^\times$ such that $\sim_\mathcal{H} = \sim_\Gamma$.*

Proof. We fix an arbitrary vector $v \neq \mathbf{0}$ and consider the set

$$M_v := \{\lambda \in \mathbb{F}_{p^m}^\times : v \sim_\mathcal{H} \lambda v\}.$$

We claim that M_v does not depend on v. This holds, as for any other vector $w \neq \mathbf{0}$ there exists an automorphism φ of $\mathcal{V}$ which maps v to w. Therefore, $\lambda v \sim_\mathcal{H} v$ iff $\lambda w \sim_\mathcal{H} w$ because of (1).

Now $\Gamma := M_v$ contains $1 \in \mathbb{F}_{p^m}$ because $\sim_\mathcal{H}$ is reflexive. For any $\lambda \in \Gamma$ its inverse λ^{-1} is also an element of Γ since $\sim_\mathcal{H}$ is symmetric. Furthermore, Γ is closed under multiplication due to $\sim_\mathcal{H}$ being transitive.

This shows that Γ is a subgroup of $\mathbb{F}_{p^m}^\times$. For all elements $\lambda \in \mathbb{F}_{p^m}^\times$ and for all vectors $v \in V \setminus \{\mathbf{0}\}$ we have

$$v \sim_\Gamma \lambda v \iff \lambda \in \Gamma \iff v \sim_\mathcal{H} \lambda v.$$

Any vector outside of $\langle v \rangle$ cannot be equivalent to v under $\sim_\mathcal{H}$ or $\sim_\Gamma$, and we have already seen $[\mathbf{0}]_{\sim_\mathcal{H}} = [\mathbf{0}]_{\sim_\Gamma} = \{\mathbf{0}\}$. This shows that $\sim_\mathcal{H}$ and $\sim_\Gamma$ coincide. □

We now apply Lemma 3.3 to our fixed group $\mathcal{G}$ and fix $\Gamma \leq \mathbb{F}_{p^m}^\times$ for the rest of Chapter 3 such that $\sim_\mathcal{G} = \sim_\Gamma$. Both equivalence relations will be denoted by $\sim$.

In the case $\Gamma = \mathbb{F}_{p^m}^\times$ we have to distinguish two cases, namely whether or not $\mathcal{G}$ maps two-dimensional subspaces of $\mathcal{V}$ to two-dimensional subspaces $\mathcal{V}$. The former will be discussed in Section 3.1, the latter will be considered together with the remaining case where $\Gamma \lneq \mathbb{F}_{p^m}^\times$ in Section 3.2.

3.1. **The group $\mathcal{G}$ preserves projective lines.** In this section we are going to assume that Γ is equal to $\mathbb{F}_{p^m}^\times$ and that $\mathcal{G}$ *preserves projective lines*. Since for all $v \in V \setminus \{\mathbf{0}\}$ the equivalence class $[v]_\sim$ is equal to the linear closure of v without $\mathbf{0}$ and since the group $\mathcal{G}$ fixes $\mathbf{0}$, the action of $\mathcal{G}$ on the $\sim$-equivalence classes is isomorphic to its action on the one-dimensional subspaces $\mathrm{S}_1(\mathcal{V})$ of $\mathcal{V}$. Our goal is to show that in this case the action of $\mathcal{G}$ on $\mathrm{S}_1(\mathcal{V})$ is the same as the action of a subgroup of $\Gamma\mathrm{L}(\mathcal{V})$ thereon.

Definition 3.4. Let $\mathcal{W}$ be a vector space. A bijective function $g\colon \mathrm{S}_1(\mathcal{W}) \to \mathrm{S}_1(\mathcal{W})$ *preserves projective lines* iff for all $L_0, L_1, L_2 \in \mathrm{S}_1(\mathcal{W})$ we have

$$L_0 \subseteq L_1 + L_2 \iff L_0^g \subseteq L_1^g + L_2^g. \tag{2}$$

A group $\mathcal{H} \leq \mathrm{Sym}(\mathrm{S}_1(\mathcal{W}))$ *preserves projective lines* iff every element of H preserves projective lines.

Let $\mathcal{W}$ be a vector space and let $g\colon \mathrm{S}_1(\mathcal{W}) \to \mathrm{S}_1(\mathcal{W})$ be a bijective function which preserves projective lines. Given a two-dimensional subspace $P \leq \mathcal{W}$, there are $L_1, L_2 \in \mathrm{S}_1(\mathcal{W})$ such that $P = L_1 + L_2$, thus by (2) every one-dimensional subspace $L_0 \subseteq P$ of $\mathcal{W}$ is mapped into $L_1^g + L_2^g$ by g which, since g is bijective on $\mathrm{S}_1(\mathcal{W})$, is a two-dimensional subspace. For any $L \in \mathrm{S}_1(\mathcal{V})$ such that $L \subseteq L_1^g + L_2^g$ we have $L^{g^{-1}} \subseteq L_1 + L_2 = P$. Therefore we obtain

$$P^g = \bigcup\{L^g : L \leq P \wedge L \in \mathrm{S}_1(\mathcal{W})\} = L_1^g + L_2^g.$$

In particular g maps every two-dimensional subspace of $\mathcal{W}$ (a "projective line", see for example [5, p.165]) to a two-dimensional subspace of $\mathcal{W}$.

When we say that $\mathcal{G}$ *preserves projective lines* we indicate that the action of $\mathcal{G}$ on $\mathrm{S}_1(\mathcal{V})$ preserves projective lines. Assuming this, we want to show that for any element $g \in G$ there exists a semi-linear function $\varphi \in \Gamma\mathrm{L}(\mathcal{V})$ such that their action on $\mathrm{S}_1(\mathcal{V})$ is the same. In particular, we want to show that our Definition 29 coincides with the definition of "collinearity" as it is defined in [5, p.174].

First we need a few easy properties of bijective semi-linear functions.

Lemma 3.5. *Let $\mathcal{W}$ be a vector space over a field $\mathcal{F}$ and let $\varphi\colon V \to V$ be a bijective semi-linear function with respect to $\alpha \in \mathrm{Aut}(\mathcal{F})$. Then for all $M, U \in \mathrm{S}(\mathcal{W})$ the following holds:*

(a) $(M + U)^\varphi = M^\varphi + U^\varphi$,
(b) $\dim U = \dim U^\varphi$, *and*
(c) *The action of φ on $\mathrm{S}_1(\mathcal{V})$ preserves projective lines.*

Proof. All items (a)-(c) follow immediately from the definition of semilinearity. □

The next part of this section until Theorem 3.7 is a slight generalisation of Section 2.10 of [1, p.87ff] from finite-dimensional to countably infinite-dimensional vector spaces.

If a function preserves projective lines, then it also preserves arbitrary subspaces of a vector space in the sense of condition (3) below. We will need this for the proof of Theorem 3.7.

Lemma 3.6. *Let $\mathcal{W}$ be a vector space and let $g\colon S_1(\mathcal{W}) \to S_1(\mathcal{W})$ be a bijective function that preserves projective lines. Then for every set $S \subseteq \mathrm{S}_1(\mathcal{W})$ and all $L_0 \in \mathrm{S}_1(\mathcal{W})$*

$$L_0 \subseteq \sum_{L \in S} L \iff L_0^g \subseteq \sum_{L \in S} L^g. \tag{3}$$

Proof. We first show the statement for all finite sets $S \subseteq \mathrm{S}_1(\mathcal{W})$. We show via induction over $n \geq 1$ that for all one-dimensional subspaces $L_0, L_1, \ldots, L_n$ of $\mathcal{W}$ the function g satisfies

$$L_0 \subseteq \sum_{i=1}^{n} L_i \iff L_0^g \subseteq \sum_{i=1}^{n} L_i^g. \tag{4}$$

The case $n = 1$ is obvious and the case $n = 2$ is exactly condition (2). Let $n > 2$ and assume we have already shown (4) for $n - 1$. We show the implication from left to right.

Let $L_0, L_1, \ldots, L_n \in \mathrm{S}_1(\mathcal{W})$ be given and assume that $L_0 \subseteq \sum_{i=1}^{n} L_i$. There exist vectors $v, w \in W$ such that v is an element of $L_1 + \cdots + L_{n-1}$, the vector w is an element of L_n and the vector $v + w$ spans L_0. We apply (2) to $L_0 \subseteq \langle v \rangle + L_n$ and our induction hypothesis (4) to $\langle v \rangle \subseteq L_1 + \cdots + L_{n-1}$ and obtain:

$$L_0^g \overset{(2)}{\subseteq} \langle v \rangle^g + L_n^g \overset{(4)}{\subseteq} L_1^g + \cdots + L_{n-1}^g + L_n^g.$$

Condition (2) also holds for g^{-1}. Therefore, the implication from left to right of (4) holds for g^{-1} by what we just showed. This shows that for g both sides of (4) are equivalent.

Let I be an arbitrary infinite set and let $\{L_i : i \in I\}$ be a set of one-dimensional subspaces of $\mathcal{W}$. If a one-dimensional subspace $L_0 \in \mathrm{S}_1(\mathcal{W})$ is contained in $\sum_{i \in I} L_i$ then there is a finite subset I' of I such that $L_0 \subseteq \sum_{i \in I'} L_i$. By (4) we obtain that $L_0^g \subseteq \sum_{i \in I'} L_i^g \subseteq \sum_{i \in I} L_i^g$. The other implication follows in the same way as before. □

We are now able to show that if a function that acts bijectively on the one-dimensional subspaces of a vector space preserves projective lines, then this action is the same as the action of a semi-linear function on the one-dimensional subspaces of said vector space.

Theorem 3.7. *Let $g \in \mathrm{Sym}(\mathrm{S}_1(\mathcal{V}))$ preserve projective lines. Then there exists a bijective semi-linear function $\varphi\colon V \to V$ with respect to some $\alpha \in \mathrm{Aut}(\mathbb{F}_{p^m})$ such that the action of φ on $\mathrm{S}_1(\mathcal{V})$ is g.*

Moreover if $\psi\colon V \to V$ is an arbitrary bijective semi-linear function with respect to $\beta \in \mathrm{Aut}(\mathbb{F}_{p^m})$ whose action on $\mathrm{S}_1(\mathcal{V})$ is equal to g, then there exists $c \in \mathbb{F}_{p^m}$ such that for every $v \in V$ we have $\varphi(v) = \psi(cv)$ and for every $x \in \mathbb{F}_{p^m} : \alpha(x) = \beta(cxc^{-1})$.

Proof. To prevent cluttered notation in this proof we will refer to "subspaces of $\mathcal{V}$" simply as "subspaces".

Let $\{v_i : i \geq 1\}$ be a basis of $\mathcal{V}$. For all $i \geq 1$ define $L_i := \langle v_i \rangle$. Every L_i is mapped by g to another one-dimensional subspace $\tilde{L}_i$. For every $i \geq 1$ there exists a vector $\tilde{v}_i$ such that $\tilde{L}_i = \langle \tilde{v}_i \rangle$.

Claim: The set $\{\tilde{v}_i : i \geq 1\}$ is a basis of $\mathcal{V}$.

We prove this claim by showing that $\{\tilde{v}_i : i \geq 1\}$ is a minimal generating subset of $\mathcal{V}$. Let $v \in V$ be arbitrary. The function g acts bijectively on the one-dimensional subspaces of $\mathcal{V}$, thus there exists a one-dimensional subspace L such that $L^g = \langle v \rangle$. The subspace L is contained in $\sum_{i\geq 1} L_i$, thus by Lemma 3.6 $\langle v \rangle = L^g \subseteq \sum_{i \geq 1} \tilde{L}_i$. Hence, v is an element of $\langle \{\tilde{v}_i : i \geq 1\} \rangle$.

It remains to show that $\{\tilde{v}_i : i \geq 1\}$ is minimal with the property of generating V. Without loss of generality we show that $\tilde{v}_1 \notin \langle \{\tilde{v}_i : i \geq 2\} \rangle$. We strive for a contradiction. Suppose there exist coefficients $(c_i)_{i\geq 2}$ in $\mathbb{F}_{p^m}$, almost all of them 0, such that $\sum_{i\geq 2} c_i \tilde{v}_i = \tilde{v}_1$. Then the one-dimensional subspace $\tilde{L}_1 = \langle \tilde{v}_1 \rangle$ is contained in the subspace $\sum_{i \geq 2} \tilde{L}_i$. By Lemma 3.6 the one-dimensional subspace L_1 is therefore contained in $\sum_{i\geq 2} L_i$, contradicting the fact that $\{v_i : i \geq 1\}$ is a basis of $\mathcal{V}$. This shows our claim.

Our next goal is to construct a suitable field automorphism α. For every $i \geq 2$ the one-dimensional subspace $\langle v_1 + v_i \rangle$ is contained in $L_1 + L_i$. Since g preserves projective lines the subspace $\langle v_1 + v_i \rangle^g$ is contained in $\langle \tilde{v}_1 \rangle + \langle \tilde{v}_i \rangle$. There exists a uniquely determined $c_i \in \mathbb{F}_{p^m}$ such that $\langle v_1 + v_i \rangle^g$ is spanned by a vector of the form $\tilde{v}_1 + c_i \tilde{v}_i$. This c_i cannot be 0 since if $c_i = 0$, then both $\langle v_i \rangle$ and $\langle v_1 + v_i \rangle$ would be mapped to $\langle \tilde{v}_1 \rangle$ which is a contradiction. The set $\{\tilde{v}_i : i \geq 1\}$ is a basis of $\mathcal{V}$ iff $\{\tilde{v}_1\} \cup \{c_i \tilde{v}_i : i \geq 2\}$ is. Therefore, we may assume without loss of generality that for all $i \geq 2 : c_i = 1$.

For any $c \in \mathbb{F}_{p^m}$ and for every $i \geq 2$ the subspace $\langle v_1 + cv_i \rangle^g$ is contained in $\langle \tilde{v}_1 \rangle + \langle \tilde{v}_i \rangle$. There exists a unique $\tilde{c} \in \mathbb{F}_{p^m}$ such that

$\langle v_1 + cv_i \rangle^g$ is spanned by $\tilde{v}_1 + \tilde{c}\tilde{v}_i$. We define a function $\alpha_i \colon \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ by $c \mapsto \tilde{c}$. This function α_i is injective because g is. Since $\langle v_1 + 1v_i \rangle^g = \langle \tilde{v}_1 + \tilde{v}_i \rangle$ we obtain $\alpha_i(1) = 1$. Clearly $\alpha_i(0)$ is equal to 0. We now want to show that for all $i, j \geq 2$ the functions α_i and α_j coincide.

Let $c \in \mathbb{F}_{p^m}$ and $i, j \geq 2$ be arbitrary such that $i \neq j$. The one-dimensional subspace $\langle cv_i - cv_j \rangle$ is contained in $\langle v_i \rangle + \langle v_j \rangle$ as well as in $\langle v_1 + cv_i \rangle + \langle v_1 + cv_j \rangle$. Therefore, the one-dimensional subspace $\langle cv_i - cv_j \rangle^g$ is spanned by a vector which lies in the intersection

$$\Big(\langle \tilde{v}_i \rangle + \langle \tilde{v}_j \rangle \Big) \cap \Big(\langle \tilde{v}_1 + c^{\alpha_i} \tilde{v}_i \rangle + \langle \tilde{v}_1 + c^{\alpha_j} \tilde{v}_j \rangle \Big).$$

Since $\tilde{v}_1$ is not an element of the left-hand side, the subspace $\langle cv_i - cv_j \rangle^g$ is spanned by a vector of the form $c^{\alpha_i}\tilde{v}_i - c^{\alpha_j}\tilde{v}_j$.

For $c = 1$ we end up with

$$\langle v_i - v_j \rangle^g = \langle 1^{\alpha_i}\tilde{v}_i - 1^{\alpha_j}\tilde{v}_j \rangle = \langle \tilde{v}_i - \tilde{v}_j \rangle .$$

For arbitrary $c \in \mathbb{F}_{p^m}$ since $\langle cv_i - cv_j \rangle = \langle v_i - v_j \rangle$ we obtain

$$\langle c^{\alpha_i}\tilde{v}_i - c^{\alpha_j}\tilde{v}_j \rangle = \langle cv_i - cv_j \rangle^g = \langle \tilde{v}_i - \tilde{v}_j \rangle ,$$

hence $c^{\alpha_i} = c^{\alpha_j}$. Since c was arbitrary for all $i, j \geq 1$ we have $\alpha_i = \alpha_j =: \alpha$.

We show that α is indeed a field automorphism. To this end we are going to show that for all coefficients $(c_i)_{i \geq 2}$ in $\mathbb{F}_{p^m}$, almost all of them 0, we have

$$\left\langle v_1 + \sum_{i \geq 2} c_i v_i \right\rangle^g = \left\langle \tilde{v}_1 + \sum_{i \geq 2} c_i^{\alpha} \tilde{v}_i \right\rangle . \tag{5}$$

We prove via induction over $n \geq 2$ that for all $c_2, \dots, c_n \in \mathbb{F}_{p^m}$

$$\left\langle v_1 + \sum_{i=2}^{n} c_i v_i \right\rangle^g = \left\langle \tilde{v}_1 + \sum_{i=2}^{n} c_i^{\alpha} \tilde{v}_i \right\rangle . \tag{6}$$

The base case $n = 2$ holds by definition. Assume we have already shown (6) for all $c_2, \dots, c_n \in \mathbb{F}_{p^m}$.

Let $c_2, \dots, c_n, c \in \mathbb{F}_{p^m}$ be given. The one-dimensional subspace $\langle v_1 + \sum_{i=2}^{n} c_i v_i + cv_{n+1} \rangle$ is contained in

$$\left\langle v_1 + \sum_{i=2}^{n} c_i v_i \right\rangle + \langle cv_{n+1} \rangle \text{ and } \langle v_1 + cv_{n+1} \rangle + \left\langle \sum_{i=2}^{n} c_i v_i \right\rangle .$$

Therefore $\langle v_1 + \sum_{i=2}^{n} c_i v_i + c v_{n+1}\rangle^g$ is contained in

$$\left\langle v_1 + \sum_{i=2}^{n} c_i v_i \right\rangle^g + \langle v_{n+1}\rangle^g \text{ and } \langle v_1 + c v_{n+1}\rangle^g + \left\langle \sum_{i=2}^{n} c_i v_i \right\rangle^g .$$

By our induction hypothesis and the base case $n = 2$ these sets equal

$$\left\langle \tilde{v}_1 + \sum_{i=2}^{n} c_i^\alpha \tilde{v}_i \right\rangle + \langle \tilde{v}_{n+1}\rangle \text{ and } \langle \tilde{v}_1 + c^\alpha \tilde{v}_{n+1}\rangle + \left\langle \sum_{i=2}^{n} c_i v_i \right\rangle^g .$$

Thus the linear closure

$$\left\langle v_1 + \sum_{i=2}^{n} c_i v_i + c v_{n+1} \right\rangle^g$$

is spanned by a vector of the form

$$\tilde{v}_1 + \sum_{i=2}^{n} c_i^\alpha \tilde{v}_i + c^\alpha \tilde{v}_{n+1}.$$

Since linear combinations are finite, this shows (5).

For any $(c_i)_{i\geq 2}$ in $\mathbb{F}_{p^m}$, almost all of them 0, the subspace $\langle \sum_{i\geq 2} c_i v_i \rangle$ is contained in $\langle v_1 + \sum_{i\geq 2} c_i v_i\rangle + \langle v_1 \rangle$ as well as in $\sum_{i\geq 2}\langle v_i\rangle$. By (5) we obtain that $\langle \sum_{i\geq 2} c_i v_i\rangle^g$ is contained in $\langle \tilde{v}_1 + \sum_{i\geq 2} c_i^\alpha \tilde{v}_i\rangle + \langle \tilde{v}_1\rangle$ as well as in $\sum_{i\geq 2}\langle \tilde{v}_i\rangle$, thus

$$\left\langle \sum_{i\geq 2} c_i v_i \right\rangle^g = \left\langle \sum_{i\geq 2} c_i^\alpha \tilde{v}_i \right\rangle . \tag{7}$$

We now want to show that for all $x, y \in \mathbb{F}_{p^m} : (x+y)^\alpha = x^\alpha + y^\alpha$. For any $x, y \in \mathbb{F}_{p^m}$ the subspace $\langle v_1 + (x+y)v_2 + v_3\rangle$ is contained in

$$\langle v_1 + x v_2\rangle + \langle v_2\rangle + \langle v_3\rangle \text{ and } \langle v_1 + y v_2\rangle + \langle v_2\rangle + \langle v_3\rangle .$$

We obtain $\langle v_1 + (x+y)v_2 + v_3\rangle^g = \langle \tilde{v}_1 + (x^\alpha + y^\alpha)\tilde{v}_2 + \tilde{v}_3\rangle$ by our definition of α. By (5):

$$\langle v_1 + (x+y)v_2 + v_3\rangle^g = \langle \tilde{v}_1 + (x+y)^\alpha \tilde{v}_2 + \tilde{v}_3\rangle .$$

As a consequence $(x+y)^\alpha = x^\alpha + y^\alpha$. To show $(xy)^\alpha = x^\alpha y^\alpha$ consider

$$\langle v_1 + xyv_2 + xv_3\rangle \subseteq \langle v_1\rangle + \langle yv_2 + v_3\rangle .$$

There exists $c \in \mathbb{F}_{p^m}$ such that $\langle v_1 + xyv_2 + xv_3\rangle^g$ is spanned by $\tilde{v}_1 + c y^\alpha \tilde{v}_2 + c\tilde{v}_3$. On the other hand $\langle v_1 + xyv_2 + xv_3\rangle^g$ is equal to $\langle \tilde{v}_1 + (xy)^\alpha \tilde{v}_2 + x^\alpha \tilde{v}_3\rangle$, hence $c = x^\alpha$. Together, we obtain $(xy)^\alpha = x^\alpha y^\alpha$.

Since α is compatible with $0, +, 1$ and $\cdot$, it is injective. By finiteness it follows that α is bijective and therefore $\alpha \in \mathrm{Aut}(\mathbb{F}_{p^m})$.

We have already shown for all coefficients $(c_i)_{i\geq 2} \in \mathbb{F}_{p^m}$, almost all but not all of them 0, that $\left\langle v_1 + \sum_{i\geq 2} c_i v_i \right\rangle^g$ is equal to $\left\langle \tilde{v}_1 + \sum_{i\geq 2} c_i^\alpha \tilde{v}_i \right\rangle$. For any additional coefficient $c_1 \in \mathbb{F}_{p^m}^\times$, since $\left\langle c_1 v_1 + \sum_{i\geq 2} c_i v_i \right\rangle$ is the same as $\left\langle v_1 + \sum_{i\geq 2} c_1^{-1} c_i v_i \right\rangle$ and since α is a field automorphism, we obtain

$$\left\langle \sum_{i\geq 1} c_i v_i \right\rangle^g = \left\langle \sum_{i\geq 1} c_i^\alpha \tilde{v}_i \right\rangle. \tag{8}$$

We can finally define a semi-linear function $\varphi\colon V \to V$. Let $v \in V$ be a vector, which is represented over the basis $\{v_i : i \geq 1\}$ by the linear combination $\sum_{i\geq 1} c_i v_i$ with coefficients $(c_i)_{i\geq 1}$ in $\mathbb{F}_{p^m}$, we define:

$$v^\varphi = \left(\sum_{i\geq 1} c_i v_i \right)^\varphi := \left(\sum_{i\geq 1} c_i^\alpha \tilde{v}_i \right).$$

By (8) the function φ acts on $\mathrm{S}_1(\mathcal{V})$ as g. It remains to show the uniqueness of φ and α up to a factor $c \in \mathbb{F}_{p^m}$.

Let ψ be an injective semi-linear function with respect to a field automorphism β and assume the action of ψ on $\mathrm{S}_1(\mathcal{V})$ is g. For any vector $v \in V \setminus \{\mathbf{0}\}$ the functions φ and ψ coincide on $\langle v \rangle$, thus there exists $c_v \in \mathbb{F}_{p^m}$ such that $\varphi(v) = \psi(c_v v)$. For any other vector $w \in V \setminus \langle v \rangle$

$$\begin{aligned} \varphi(v+w) &= \psi(c_{v+w}v) + \psi(c_{v+w}w) \text{ equals} \\ \varphi(v) + \varphi(w) &= \psi(c_v v) + \psi(c_w w), \end{aligned}$$

hence for all $v, w \in \mathbb{F}_{p^m}$ we obtain $c_v = c_{v+w} = c_w =: c$. Therefore for all $x \in V$ we have $\varphi(x) = \psi(cx)$. For all $k \in \mathbb{F}_{p^m}$ and all $v \in V$

$$k^\alpha \varphi(v) = \varphi(kv) = \psi(ckv) = \psi((ckc^{-1}c)v) = (ckc^{-1})^\beta \psi(cv),$$

thus $k^\alpha = (ckc^{-1})^\beta$. □

Theorem 3.7 is a variation of the Fundamental Theorem of Projective Geometry (Theorem 2.26 [1, p.88]). We remark two points about the proof.

- We used that there exist at least three linearly independent vectors in the vector space, i.e., the dimension of the corresponding projective space is at least 2. In fact Theorem 3.7 also holds for finite-dimensional vector spaces of dimension at least three over arbitrary fields, but does not hold in this form for vector spaces of lower dimension than three. See for example Remark 2 [1, p.88] and Section 11 [1, p.89].

- Furthermore we used the finiteness of the underlying field $\mathbb{F}_{p^m}$. This is not necessary and the proof can be easily adjusted to accommodate an infinite field.

By Theorem 3.7 if we assume that all functions of $\mathcal{G}$ when acting on $\mathrm{S}_1(\mathcal{V})$ preserve projective lines, we obtain that $\mathcal{G}$ acts as a subgroup of $\Gamma\mathrm{L}(\mathcal{V})$ on $\mathrm{S}_1(\mathcal{V})$. With this in mind we want to give a more detailed description of the bijective semi-linear functions on a vector space.

Let $\mathcal{W}$ be a vector space over a field $\mathcal{F}$. We define an action of $\mathrm{Aut}(\mathcal{F})$ on W in the following way. Let $\{v_i : i \in I\} =: B$ be a basis of $\mathcal{W}$. For every $\alpha \in \mathrm{Aut}(\mathcal{F})$ we define a mapping α_B such that for all elements $(c_i)_{i\in I}$ of the field $\mathcal{F}$, almost all of them 0,

$$\alpha_B\left(\sum_{i\in I} c_i v_i\right) := \sum_{i\in I} c_i^\alpha v_i.$$

We denote $\mathrm{Aut}_B(\mathcal{F}) := \{\alpha_B : \alpha \in \mathrm{Aut}(\mathcal{F})\}$. Clearly $(\mathrm{id}_F)_B = \mathrm{id}_V$ and for any $\alpha, \beta \in \mathrm{Aut}(\mathcal{F})$ we have $\alpha_B \circ \beta_B = (\alpha\circ\beta)_B$, hence $\mathrm{Aut}_B(\mathcal{F})$ is a group.

Lemma 3.8. *Let $\mathcal{W}$ be a vector space over a field $\mathcal{F}$ and let B be a basis of $\mathcal{W}$. Then the group $\Gamma\mathrm{L}(\mathcal{W})$ is the semi-direct product $\mathrm{Aut}_B(\mathcal{F}) \ltimes \mathrm{Aut}(\mathcal{W})$.*

Proof. Let $B = \{v_i : i \in I\}$ be for a set I. Every function in $\mathrm{Aut}_B(\mathcal{F})$ is bijective and semi-linear, hence $\mathrm{Aut}_B(\mathcal{F}) \leq \Gamma\mathrm{L}(\mathcal{W})$. Moreover $\mathrm{Aut}(\mathcal{W})$ is normal in $\Gamma\mathrm{L}(\mathcal{W})$ since for any $\psi \in \Gamma\mathrm{L}(\mathcal{W})$, all $\varphi \in \mathrm{Aut}(\mathcal{W})$, and all coefficients $(c_i)_{i\in I}$ in F, almost all of them 0, we have

$$\left(\sum_{i\in I} c_i v_i\right)^{\psi\varphi\psi^{-1}} = \sum_{i\in I} c_i v_i^{\psi\varphi\psi^{-1}}.$$

This shows that $\psi\circ\varphi\circ\psi^{-1}$ is an automorphism of $\mathcal{W}$, thus $\psi \circ \mathrm{Aut}(\mathcal{W}) \circ \psi^{-1} \subseteq \mathrm{Aut}(\mathcal{W})$ and $\mathrm{Aut}(\mathcal{W}) \lhd \Gamma\mathrm{L}(\mathcal{W})$.

For all $(c_i)_{i\in I}$ in F, almost all of them 0, every bijective semi-linear function ψ with respect to some $\alpha \in \mathrm{Aut}(\mathcal{F})$ maps any vector $\sum_{i\in I} c_i v_i$ to $\sum_{i\in I} c_i^\alpha v_i^\psi$. The function which maps any linear combination $\sum_{i\in I} c_i v_i$ to $\sum_{i\in I} c_i v_i^\psi$ defines a function $\varphi \in \mathrm{Aut}(\mathcal{W})$. We obtain $\psi = \alpha_B \circ \varphi$, i.e., $\Gamma\mathrm{L}(\mathcal{W}) = \mathrm{Aut}_B(\mathcal{F}) \circ \mathrm{Aut}(\mathcal{W})$. Clearly the only function which simultaneously lies in $\mathrm{Aut}(\mathcal{W})$ and $\mathrm{Aut}_B(\mathcal{F})$ is the identity on W.

□

By Theorem 3.7 the action of $\mathcal{G}$ on $\mathrm{S}_1(\mathcal{V})$ is equal to the action of some subgroup of $\Gamma\mathrm{L}\,(\mathcal{V})$. Since $\mathcal{G}$ contains $\mathrm{Aut}(\mathcal{V})$ we are interested in the subgroups of $\mathrm{Aut}_B(\mathbb{F}_{p^m}) \ltimes \mathrm{Aut}(\mathcal{V})$ containing $\mathrm{Aut}(\mathcal{V})$.

Lemma 3.9. *Let $\mathcal{M}$ be a group, $\mathcal{N}, \mathcal{H} \leq \mathcal{M}$ and $\mathcal{M} = \mathcal{H} \ltimes \mathcal{N}$. Then for all subgroups $\mathcal{S} \leq \mathcal{M}$ such that $\mathcal{N} \leq \mathcal{S}$, there exists $\mathcal{K} \leq \mathcal{H}$ such that $\mathcal{S}$ is the semi-direct product $\mathcal{K} \ltimes \mathcal{N}$.*

Proof. Let $\mathcal{S}$ be given and $\mathcal{M}$ be formalized as $\mathcal{M} = (M, 0, +, -)$. We define $K := H \cap S$ and show that this induces an appropriate subgroup of $\mathcal{H}$. To start with, $\mathcal{N}$ is still normal in $\mathcal{S}$ since $\mathcal{S} \leq \mathcal{M}$. Also $N \cap K = N \cap H \cap S = \{0\}$ and K induces a subgroup $\mathcal{K}$ of $\mathcal{S}$.

It remains to show $NK = S$. Clearly $NK \subseteq S$. For the other inclusion let $s \in S$ be given and let $h \in H$ and $n \in N$ such that $s = n + h$. Since $\mathcal{N} \leq \mathcal{S}$ also $(-n) + n + h = h \in S$, hence $h \in S \cap H$. This concludes the proof. □

We remark that the dual statement also holds, i.e., if $\mathcal{S}$ a subgroup of $\mathcal{H} \ltimes \mathcal{N}$ and $\mathcal{H} \leq \mathcal{S}$, then there exists $\mathcal{K} \leq \mathcal{N}$ such that $\mathcal{S} = \mathcal{H} \ltimes \mathcal{K}$.

If $\mathcal{S}$ is a subgroup of $\mathcal{H} \ltimes \mathcal{N}$ and neither $\mathcal{H} \leq \mathcal{S}$ nor $\mathcal{N} \leq \mathcal{S}$, we cannot conclude that $\mathcal{S}$ is again a semi-direct product. Consider for example any group $\mathcal{M}$ with $+$ as its group operation and 0 its neutral element. Let $\mathcal{M}_1$ be the isomorphic group with domain $M_1 = \{(m, 0) : m \in M\}$ and likewise $\mathcal{M}_2$ with domain $M_2 = \{(0, m) : m \in M\}$, both with component-wise addition. Then $\mathcal{M}_1 \ltimes \mathcal{M}_2$ is a semi direct product with domain $\{(m, k) : m, k \in M\}$. The diagonal $\{(m, m) : m \in M\}$ induces a subgroup of $\mathcal{M}_1 \ltimes \mathcal{M}_2$ not equal to a semi-direct product of the form $\mathcal{H} \ltimes \mathcal{N}$ for some $\mathcal{H} \leq \mathcal{M}_1$ and $\mathcal{N} \leq \mathcal{M}_2$.

The automorphisms of a finite field are generated by the Frobenius automorphism.

Definition 3.10. Let q be a prime number and let $n \geq 1$. The function $\sigma \colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ defined by $x \mapsto x^q$ is called the *Frobenius automorphism of* $\mathbb{F}_{q^n}$.

Let $\sigma \colon \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ be the Frobenius automorphism of $\mathbb{F}_{p^m}$. By [1, p.246] the automorphisms of $\mathbb{F}_{p^m}$ are of the form

$$\mathrm{Aut}(\mathbb{F}_{p^m}) = \{\mathrm{id}_{\mathbb{F}_{p^m}}, \sigma, \ldots, \sigma^{m-1}\}.$$

This is a cyclic group, thus we know the exact form of its subgroups. For a proof of Lemma 3.11 see for example [8, p. 23f].

Lemma 3.11. *Let $\mathcal{M}$ be a cyclic group. Then every subgroup of $\mathcal{M}$ is cyclic. For every divisor k of the order of $\mathcal{M}$ there is exactly one subgroup $\mathcal{H} \leq \mathcal{M}$ such that the order of $\mathcal{H}$ is k.*

We recall that $\mathcal{V}$ is a countably infinite dimensional vector space over the finite field $\mathbb{F}_{p^m}$ which has odd characteristic and that $\mathcal{G}$ is a closed supergroup of $\operatorname{Aut}(\mathcal{V})$ which fixes $\mathbf{0}$. If $\mathcal{G}$ preserves projective lines, by Theorem 3.7, we obtain that there exist $k, n \geq 1$ such that $kn = m$ and the action of $\mathcal{G}$ on $\mathrm{S}_1(\mathcal{V})$ is the same as the action of

$$\{\sigma^n, \sigma^{2n}, \ldots, \sigma^{kn} = \mathrm{id}_{\mathbb{F}_{p^m}}\} \ltimes \operatorname{Aut}(\mathcal{V}) \leq \operatorname{Sym}(\mathrm{S}_1(\mathcal{V})).$$

From the next section onwards we are going to restrict ourselves to a vector space $\mathcal{V}$ over a prime field $\mathbb{F}_p$ of uneven characteristic.

The finite field $\mathbb{F}_p$ is isomorphic to the integers modulo p, in particular $\mathbb{F}_p$ is generated by 1 and the addition in $\mathbb{F}_p$, therefore $\operatorname{Aut}(\mathbb{F}_p) = \{\mathrm{id}_{\mathbb{F}_p}\}$. Thus in that case the semi-linear functions $\Gamma\mathrm{L}(\mathcal{V})$ are the same as $\operatorname{Aut}(\mathcal{V})$. We have shown the following theorem.

Theorem 3.12. *Let $\mathcal{V}$ be a countably infinite-dimensional vector space over a finite prime field $\mathbb{F}_p$ of odd characteristic and let $\mathcal{G}$ be a closed supergroup of $\operatorname{Aut}(\mathcal{V})$ fixing $\mathbf{0}$ and acting on $\mathrm{S}_1(\mathcal{V})$ as well as preserving projective lines. Then $\mathcal{G}$ acts on $\mathrm{S}_1(\mathcal{V})$ and on the set of $\sim$-equivalence classes in the same way as $\operatorname{Aut}(\mathcal{V})$ does.*

3.2. **The remaining cases for $\mathcal{G} \leq \mathrm{Sym}(V)_{\mathbf{0}}$.** From now on until the end of this thesis, we only consider the case that $\mathcal{V}$ is a countably infinite vector space over a prime field $\mathbb{F}_p$ of odd characteristic p.

We consider the remaining cases, namely

- $\Gamma = \mathbb{F}_p^\times$ and the action of $\mathcal{G}$ on $\mathrm{S}_1(\mathcal{V})$ does not preserve projective lines, or
- $\Gamma \lneq \mathbb{F}_p^\times$.

Our goal is to show that under these assumptions $\mathcal{G}$ acts on the set of those $\sim$-equivalence classes which are not $\{\mathbf{0}\}$ as the full symmetric group.

Theorem 3.13. *Assume that one of the following conditions holds.*

- $\Gamma = \mathbb{F}_p^\times$ *and the action of* $\mathcal{G}$ *on* $\mathrm{S}_1(\mathcal{V})$ *does not preserve projective lines, or*
- $\Gamma \lneq \mathbb{F}_p^\times$.

Then $\mathcal{G}$ *acts as the full symmetric group on* $(V \setminus \{\mathbf{0}\})/_{\sim}$.

The proof is split into the following three steps:

(i) every tuple of vectors of $V \setminus \{\mathbf{0}\}$ can be mapped into a "sufficiently small" subspace of $\mathcal{V}$ by an element of $\mathcal{G}$;
(ii) $\mathcal{G}$ acts transitively on arbitrary large tuples of non-equivalent elements of $V \setminus \{\mathbf{0}\}$;
(iii) $\mathcal{G}$ acting on $(V \setminus \{\mathbf{0}\})/_{\sim}$ is a closed permutation group.

From (ii) and (iii) it immediately follows that $\mathcal{G}$ acts on $(V \setminus \{\mathbf{0}\})_{\sim}$ as the full symmetric group.

The first step (i) will carry most of the weight. The second step (ii) will follow quite easily from (i). The third step (iii) does not depend on (i) and (ii) and will follow from the fact that all $\sim$-equivalence classes are finite.

We start with a few easy observations for stabilizers.

Lemma 3.14. *Let S be a finite subset of V. Then for all $v \in V$ the following are equivalent:*

(1) $G_S(v)$ is infinite,
(2) $G_S(v)$ contains some vector $u \notin \langle S \rangle$,
(3) $G_S(v) \supseteq V \setminus \langle S \rangle$.

Proof. Let $v \in V$ be given.

(1) $\Rightarrow$ (2): Assume $G_S(v)$ to be infinite. Since $\langle S \rangle$ is finite $G_S(v)$ has to contain some element outside of $\langle S \rangle$.

(2) $\Rightarrow$ (3): Already $\mathrm{Aut}(\mathcal{V})_S$ acts transitively on the elements of $V \setminus \langle S \rangle$. Since there exists a vector in $G_S(v)$ which lies in $V \setminus \langle S \rangle$, any element outside of $\langle S \rangle$ is also an element of $G_S(v)$.

(3) $\Rightarrow$ (1): Since $V \setminus \langle S \rangle$ is infinite, so is $G_S(v)$.

□

Lemma 3.15. *Let S be a subset of $V \setminus \{\mathbf{0}\}$. Then for all $v \in V$ and all $g \in G$ the following holds:*

(1) $g^{-1} \circ G_S \circ g = G_{S^g}$.
(2) $G_S(v)^g = G_{S^g}(v^g)$.
(3) $|G_S(v)| = \infty \iff |G_{S^g}(v^g)| = \infty$.

Proof. Let $v \in V$ and $g \in G$ be given. If $h \in G_S$ then $g^{-1} \circ h \circ g$ fixes every element $s^g \in S^g$ since $s^{g(g^{-1}hg)} = s^{hg} = s^g$. For the same reason if $f \in G_{S^g}$, then $g \circ f \circ g^{-1}$ fixes S element-wise. This proves (1).

For (2) we consider $G_S(v)^g$ which is equal to:

$$\begin{aligned}\{v^h : h \in G_S\}^g &= \{v^{gfg^{-1}} : f \in G_{S^g}\}^g \\ &= \{(v^g)^f : f \in G_{S^g}\}^{g^{-1}g} = G_{S^g}(v^g).\end{aligned}$$

Finally (3) follows immediately from (2). □

Definition 3.16. Let $S \subseteq V \setminus \{\mathbf{0}\}$ and let $k \geq 1$. Then $A_k(S)$ is defined as the set of vectors $v \in V$ for which the set $\{v\} \cup S$ can be mapped into a k-dimensional subspace of $\mathcal{V}$ by an element of $\mathcal{G}$.

For any set $S \subseteq V \setminus \{\mathbf{0}\}$ and any $k \geq 1$ as soon as $A_k(S) \neq \emptyset$ the zero vector is an element of $A_k(S)$ since $\mathcal{G}$ fixes $\mathbf{0}$.

The set $A_k(S)$ has some useful and easy to show properties.

Lemma 3.17. *Let S be a subset of $V \setminus \{\mathbf{0}\}$ and let $k \geq 1$. Then*

(1) for all $g \in G$: $A_k(S) = A_k(S^g)^{g^{-1}}$,
(2) for all $M \supseteq S$: $A_k(S) \supseteq A_k(M)$ (antitonicity),
(3) for all $v \in A_k(S)$: $G_S(v) \subseteq A_k(S)$.

Proof. (1): A vector v is an element of $A_k(S)$ iff $\{v\} \cup S$ can be mapped into a k-dimensional subspace by an element of $\mathcal{G}$. For all $g \in G$ this is the case iff $\{v^g\} \cup S^g$ can be mapped into a k-dimensional subspace by an element of $\mathcal{G}$. The equality $A_k(S) = A_k(S^g)^{g^{-1}}$ follows.

(2): Let $M \supseteq S$ be given. For any $v \in V$ if the set $\{v\} \cup M$ can be mapped into some other given set by a function, then so can any subset of $\{v\} \cup M$ by the same function. In particular this is the case for $\{v\} \cup S$.

(3): Let v be an element of $A_k(S)$. Any element w in $G_S(v)$ can be mapped to v by some function of $\mathcal{G}_S$. Therefore, since $\{v\} \cup S$ can be mapped into a k-dimensional subspace by an element of $\mathcal{G}$, so can $\{w\} \cup S$. □

As it turns out the set $A_k(S)$ has always one of three shapes.

Lemma 3.18. *Let S be a subset of $V \setminus \{\mathbf{0}\}$ and let $k \geq 1$. Then exactly one of the following holds:*

(1) $A_k(S) = \emptyset$.
(2) There exists a k-dimensional subspace W of $\mathcal{V}$ and there exists $g \in G$ such that $A_k(S) = W^g$.
(3) $A_k(S) = V$.

Proof. For $S = \emptyset$ the set $A_k(S)$ is equal to V, thus let $S \neq \emptyset$. If S cannot be mapped into a k-dimensional subspace of $\mathcal{V}$ by any element of $\mathcal{G}$, then $A_k(S) = \emptyset$ which is the case (1). Otherwise clearly $S \subseteq A_k(S)$.

Let $g \in G$ be a function which maps S into a k-dimensional subspace W of $\mathcal{V}$. By Lemma 3.17 (1) it suffices to prove the statement for $A_k(S^g)$. The subspace W is contained in $A_k(S^g)$. If $A_k(S^g) = W$, then case (2) follows. Otherwise there is an element $w \in A_k(S^g) \setminus W$. We show that from this $A_k(S^g) = V$, i.e., case (3), follows.

Since $\langle S^g \rangle \subseteq W$ the element w cannot lie in $\langle S^g \rangle$, thus by Lemma 3.14 the set $G_{S^g}(w)$ contains $V \setminus W$. By applying Lemma 3.17 (3) we obtain $V \setminus W \subseteq A_k(S^g)$ and (3) follows. □

Let $S \subseteq V \setminus \{\mathbf{0}\}$ and $k \geq 1$ be given. As it turns out, (2) occurs only if the number of non-equivalent elements in S is equal to the number of non-equivalent elements in a k-dimensional subspace of $\mathcal{V}$ minus one.

Clearly the number of non-equivalent elements in S cannot be greater than the number of $\sim$-equivalence classes in a k-dimensional subspace of $\mathcal{V}$ minus one, since otherwise $A_k(S) = \emptyset$. For the other inequality assume we already know that Theorem 3.13 holds. In particular every tuple containing non-equivalent elements of $V \setminus \{\mathbf{0}\}$ can be mapped to any other tuple containing non-equivalent elements of $V \setminus \{\mathbf{0}\}$ by an element of $\mathcal{G}$. As a consequence, the number of non-equivalent elements in S cannot be strictly lower than the number of elements in a k-dimensional subspace of $\mathcal{V}$ minus one, since otherwise any other non-zero element in V can be mapped alongside S into a k-dimensional subspace of $\mathcal{V}$ by an element of $\mathcal{G}$, which would imply $A_k(S) = V$.

Since all equivalence classes of $\sim$ except $\{\mathbf{0}\}$ are of equal size, the number of equivalence classes contained in a subspace of $\mathcal{V}$ only depends on its dimension. Hence k already determines how many non-equivalent elements may appear in S.

Nevertheless, for our proof of Theorem 3.13 the only case which is interesting to use is case (2). Cases (1) and (3) in Lemma 3.18 we call *trivial*. Some of the following properties are also true for the trivial cases but are so obviously and are of no significance for us.

Lemma 3.19. *Let S be a subset of $V \setminus \{\mathbf{0}\}$ and let $k \geq 1$. Assume that $A_k(S)$ is non-trivial. Then the following holds:*

(1) $S \subseteq \bigcup_{s\in S}[s]_\sim \subseteq A_k(S) \subseteq \langle S\rangle$.
(2) $A_k(A_k(S)) = A_k(S)$.
(3) For all $g \in G$:

$$\textit{If } S^g \subseteq A_k(S), \textit{ then } A_k(S) = A_k(S)^g \ (= A_k(S^g)).$$

Proof. We prove (1). The first inclusion is trivial. Let $g \in G$ map S into a k-dimensional subspace W. Then $g\left(\bigcup_{s\in S}[s]_\sim\right) \subseteq W$. We show the last inclusion, $A_k(S) \subseteq \langle S\rangle$, by contradiction. Suppose there exists an element $v \in A_k(S)$ which lies outside of $\langle S\rangle$. By Lemma 3.14 we know that $|G_S(v)| = \infty$ and by Lemma 3.17 and Lemma 3.18 we obtain that $A_k(S)$ equals V. This contradicts the non-triviality of $A_k(S)$, whence $A_k(S) \subseteq \langle S\rangle$.

(2): The inclusion $A_k(S) \subseteq A_k(A_k(S))$ follows from (1). The other inclusion follows because of antitonicity.

(3): Let $g \in G$ be given. If $S^g \subseteq A_k(S)$ we obtain, by antitonicity, that

$$A_k(S^g) \supseteq A_k(A_k(S)) \overset{(2)}{=} A_k(S).$$

Since $A_k(S) \neq V$ we obtain by Lemma 3.17 (1) that $A_k(S^g) \neq V$. Thus, both are non-trivial and are therefore equal. We already saw in Lemma 3.17 (1) that $A_k(S)^g = A_k(S^g)$. □

Corollary 3.20 states that, if we assume that S is a linearly independent subset of V, then the set $A_k(S)$ always contains specific linear combinations. We say a tuple $t = (t_1, \ldots, t_n)$ of arity n is *linearly independent* iff no component t_i of t can be written as linear combination of the components $\{t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n\}$.

Corollary 3.20. *Let S be a linearly independent subset of V, let $k, n \geq 1$, and let $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ be linearly independent tuples containing elements of $A_k(S)$. Then for all $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_p$ the following holds:*

$$\sum_{i=1}^{n} \lambda_i x_i \in A_k(S) \iff \sum_{i=1}^{n} \lambda_i y_i \in A_k(S). \tag{9}$$

Proof. In the cases of $A_k(S) = V$ and $A_k(S) = \emptyset$ this is trivially true. We assume otherwise. Since $\{x_1, \ldots, x_n\} \subseteq A_k(S) \subseteq \langle S\rangle$ and $(x_1, \ldots, x_n)$ is linearly independent we have $\dim\langle S\rangle \geq n$. We fix n arbitrary elements of S. There exists $\varphi_x \in \mathrm{Aut}(\mathcal{V})$ mapping those elements to $x_1, \ldots, x_n$ and fixing the rest of S. Likewise there exists

$\varphi_y \in \operatorname{Aut}(\mathcal{V})$ doing the same for $y_1, \dots, y_n$. Now applying Lemma 3.19 (3) yields $A_k(S) = A_k(S)^{\varphi_x} = A_k(S)^{\varphi_y} = A_k(S)^{\varphi_x \varphi_y^{-1}}$. Since linear combinations are preserved by $\operatorname{Aut}(\mathcal{V})$ the statement follows. □

In the assumptions of Corollary 3.20 we have to require the set S to be linearly independent, otherwise the statement does not hold. To see this, assume again that we already know Theorem 3.13. Choose an arbitrary $k \geq 1$. Let n_k be one less than the number of equivalence classes of $\sim$ in any k-dimensional subspace of $\mathcal{V}$. We take an arbitrary set of $n_k - 1$ linearly independent vectors $\{s_1, \dots, s_{n_k-1}\}$ and define $S := \{s_1, \dots, s_{n_k-1}, s_1 + s_2\}$. Since $\mathcal{G}$ preserves $\sim$-equivalence classes, the set $A_k(S)$ cannot contain any vector which is not already equivalent to a vector in S. On the other hand, S is contained in $A_k(S)$, therefore if Corollary 3.20 were true, it would imply that $s_2 + s_3$ is an element of $A_k(S)$. This is not possible since $s_2 + s_3$ is not equivalent to any vector in S.

Even for linearly independent S Corollary 3.20 will turn out to be an empty statement. If Theorem 3.13 holds, as we already discussed, the only case in which $A_k(S)$ is non-trivial is if the number of equivalence classes of $\sim$ represented in S is the same as the number of equivalence classes in k-dimensional subspaces of $\mathcal{V}$ minus one. Any linear combination of vectors in S with more than one coefficient unequal to zero would yield a vector non-equivalent to any element of S. Therefore if S is linearly independent and $A_k(S)$ is non-trivial, it cannot contain any linear combination over S with more than one coefficient unequal to zero.

Clearly for every element $v \in A_k(S)$ the whole equivalence class $[v]_\sim$ is contained in $A_k(S)$. Provided that S is linearly independent we can show even more: unless $A_k(S)$ is already V, no other element of $\langle v \rangle$ is contained in $A_k(S)$.

Lemma 3.21. *Let $S \subseteq V$ be linearly independent and let $k \geq 1$. Suppose that $A_k(S)$ is non-trivial. Then for all $v \in A_k(S) \setminus \{\mathbf{0}\}$:*

$$\forall \lambda \in \mathbb{F}_p^\times : \lambda v \in A_k(S) \iff \lambda \in \Gamma. \tag{10}$$

Proof. Let $v \in A_k(S) \setminus \{\mathbf{0}\}$ be given. If $v \in \langle S \rangle \setminus S$, then there exists $\varphi \in \operatorname{Aut}(\mathcal{V})$ and $w \in S$ such that $S^\varphi = S \setminus \{w\} \cup \{v\}$. By Lemma 3.19 (3) we obtain $A_k(S^\varphi) = A_k(S)$. Therefore we can assume without loss of generality that $v \in S$.

The implication right to left of (10) has already been shown in Lemma 3.19 (1). For the other implication let $\lambda \in \mathbb{F}_p^\times \setminus \Gamma$. We show $\lambda v \notin A_k(S)$ by contradiction. Assume that $\lambda v \in A_k(S)$. Since $\lambda \notin \Gamma$ there exists $h \in G$ such that $\left\langle (\lambda v)^h \right\rangle \neq \left\langle v^h \right\rangle$. Let $M \subseteq V$ be linearly independent such that $M^h \cup \{v^h, (\lambda v)^h\}$ is linearly independent and of size $|S|+1$.

There exists $\varphi \in \mathrm{Aut}(\mathcal{V})$ such that $S^\varphi = M \cup \{v\}$ and such that $v^\varphi = v$. Then $\left\langle (S \cup \{\lambda v\})^{\varphi h} \right\rangle$ is a $|S|+1$-dimensional subspace of $\mathcal{V}$. Now $\lambda v \in A_k(S)$ implies $(S \cup \{\lambda v\})^{\varphi h} \subseteq A_k(S^{\varphi h})$ which is itself contained in $\left\langle S^{\varphi h} \right\rangle$ by Lemma 3.19 (1). The dimension of $\left\langle S^{\varphi h} \right\rangle$ is at most $|S|$, thus this is a contradiction.

□

We will need the following affine subspace criterion.

Lemma 3.22. *Let $\mathcal{W}$ be a vector space over a field $\mathcal{F}$ with* $\mathrm{char}\,\mathcal{F} \neq 2$. *Let A be a non-empty subset of W such that for all distinct $x, y \in A$ also* $\mathrm{Aff}(x, y) \subseteq A$. *Then A is an affine subspace of $\mathcal{V}$.*

Proof. We show by induction over $n \geq 2$ that for all subsets $\{x_1, \ldots, x_n\} \subseteq A$ of size n every affine combination over said set is an element of A.

The case $n = 2$ holds by assumption. Assume we have shown that every affine combination of n distinct elements of A is contained in A. Let $x_1, \ldots, x_{n+1}$ be distinct elements in A and let $c_1, \ldots, c_{n+1} \in F$ be arbitrary coefficients which sum up to 1.

We distinguish two cases. First we assume that there exists a coefficient unequal to 1. Without loss of generality let this coefficient be c_1. Then

$$\sum_{i=1}^{n+1} c_i x_i = \left(1 - \sum_{i=2}^{n+1} c_i\right) x_1 + \sum_{i=2}^{n+1} c_i x_i.$$

We set $\lambda := \sum_{i=2}^{n+1} c_i \neq 0$. The affine combination $\sum_{i=2}^{n+1} \frac{c_i}{\lambda} x_i$ is an element of A by our induction hypothesis. If $x_1 = \sum_{i=2}^{n+1} \frac{c_i}{\lambda} x_i$, then $(1-\lambda)x_1 + \lambda \left(\sum_{i=2}^{n+1} \frac{c_i}{\lambda} x_i\right) = x_1 \in A$ and we are done. Otherwise by the property of A the element

$$(1-\lambda)x_1 + \lambda \left(\sum_{i=2}^{n+1} \frac{c_i}{\lambda} x_i\right) = \sum_{i=1}^{n+1} c_i x_i,$$

is an element of A.

Now assume that all coefficients are equal to 1. In this case $\sum_{i=1}^{n+1} c_i = \sum_{i=1}^{n+1} 1 = 1$ and we write

$$\sum_{i=1}^{n+1} x_i = x_1 + x_2 + \sum_{i=3}^{n+1} x_i$$

Since $\operatorname{char}\mathcal{F} \neq 2$ we have $1 + 1 = 2 \neq 0$, hence $\frac{1}{2} \in F$. We have $\sum_{i=3}^{n+1} 1 = 1 - 2 = -1$. By our induction hypothesis and the property of A we obtain

$$\frac{1}{2}x_1 + \frac{1}{2}x_2 \in A \quad \text{and} \quad \sum_{i=3}^{n+1} \frac{1}{-1}x_i \in A.$$

Similar to before, if both coincide, then we are done. Otherwise, our element $\sum_{i=1}^{n+1} x_i$ can be written as affine combination

$$2\left(\frac{1}{2}x_1 + \frac{1}{2}x_2\right) + (-1)\left(\sum_{i=3}^{n+1} \frac{1}{-1}x_i\right),$$

which is an element of A.

Therefore $\operatorname{Aff}(A) = A$ and A is an affine subspace of $\mathcal{W}$. □

The condition $\operatorname{char}\mathcal{F} \neq 2$ in Lemma 3.22 is necessary. In order to see this, let $\mathcal{W}$ be a vector space over $\mathcal{F} = \mathbb{F}_2$. Now for all distinct elements $x, y \in A$ we have $\operatorname{Aff}(x, y) = \{x, y\}$, thus the condition in Lemma 3.22 holds for any subset A of W. However, if $\mathcal{W}$ has at least dimension 3, there are subsets of W which are not affine subspaces. For example any three distinct elements $u, v, w \in W$ have the affine closure $\{u, v, w, u + v + w\} \neq \{u, v, w\}$.

We call any one-dimensional affine space, i.e., a set of the form $\operatorname{Aff}(v, w)$ or $v + \langle w - v\rangle$ for some non-zero vectors $v, w \in V$, an *affine line*.

If S is a linearly independent subset of V we use Lemma 3.22 to show that if $A_k(S)$ contains an affine line not containing $\mathbf{0}$, then it contains certain affine spaces.

Lemma 3.23. *Let $S \subseteq V$ be linearly independent, let $A_k(S)$ contain an affine line not containing $\mathbf{0}$ and let $n \geq 2$. Then for any set $\{a_1, \dots, a_n\} \subseteq A_k(S)$ of pairwise linearly independent elements, $A_k(S)$ contains the affine subspace $\operatorname{Aff}(a_1, \dots, a_n)$ of $\mathcal{V}$.*

Proof. Let a set of pairwise linearly independent elements $\{a_1, \dots, a_n\} \subseteq A_k(S)$ be given. By Lemma 3.22 we need to show that for all distinct $i, j \leq n$ we have that the affine line $\operatorname{Aff}(a_i, a_j)$ is contained in $A_k(S)$.

By assumption there exist distinct $v, w \in V$ such that the affine line $\operatorname{Aff}(v, w)$ is contained in $A_k(S)$ and $\mathbf{0} \notin \operatorname{Aff}(v, w)$. Since $\operatorname{Aff}(v, w)$ does not contain $\mathbf{0}$ the set $\{v, w\}$ is linearly independent. Therefore, for all $\lambda \in \mathbb{F}_p$ the linear combination $\lambda v + (1-\lambda)w$ is an element of $A_k(S)$ and by applying Lemma 3.20 to the tuples (v, w) and (a_i, a_j) we obtain that every affine combination $\lambda a_i + (1 - \lambda)a_j$ is also an element of $A_k(S)$. By Lemma 3.22 we have $\operatorname{Aff}(a_1, \dots, a_n) \subseteq A_k(S)$. □

The pairwise linear independence of the set $\{a_1, \ldots, a_n\}$ in Lemma 3.23 is necessary. In particular, for a linearly independent set $S \subseteq V$ it does not hold in general that $A_k(S)$ is an affine subspace of $\mathcal{V}$. Since $A_k(S)$ contains $\mathbf{0}$, if $A_k(S)$ was an affine subspace of $\mathcal{V}$, it would also be an actual subspace of $\mathcal{V}$. For $\Gamma \neq \mathbb{F}_p^\times$ this contradicts Lemma 3.21.

One possible way to prove that $A_k(S)$ contains an affine line not containing $\mathbf{0}$ is Lemma 3.24.

Lemma 3.24. *Let $S \subseteq V$ be linearly independent and let $k, n \geq 1$. Assume that $A_k(S)$ contains a linearly independent set $\{a_1, \ldots, a_n\}$ of size n and a vector $v = \lambda_1 a_1 + \cdots + \lambda_n a_n$ such that:*

- *not all coefficients $\lambda_1, \ldots, \lambda_n$ are the same,*
- *at least three coefficients are not equal to zero.*

Then $A_k(S)$ contains an affine line not containing $\mathbf{0}$.

Proof. Without loss of generality we assume that $\lambda_1 \neq \lambda_2$ and define $\lambda := \lambda_1 - \lambda_2 \neq 0$. We apply Corollary 3.20 to the tuples $(a_1, a_2, a_3, \ldots, a_n)$ and $(a_2, a_1, a_3, \ldots, a_n)$ and we obtain that $v' \in A_k(S)$ where

$$\begin{aligned} v' &= \lambda_1 a_2 + \lambda_2 a_1 + \sum_{k=3}^{n} \lambda_k a_k \\ &= \sum_{k=1}^{n} \lambda_k a_k + \lambda(a_2 - a_1) = v + \lambda(a_2 - a_1). \end{aligned}$$

Since v as a linear combination of $a_1, \ldots, a_n$ has at least three coefficients not equal to zero, the set $\{v, a_1, a_2\}$ is linearly independent. Thus the set $\{v', a_1, a_2\}$ is linearly independent as well. By reapplying Corollary 3.20 to the tuples (v, a_2, a_1) and (v', a_2, a_1) we obtain

$$\begin{aligned} v + \lambda(a_2 - a_1) = v' \in A_k(S) \\ \implies v' + \lambda(a_2 - a_1) =: v'' \in A_k(S). \end{aligned}$$

On the other hand v'' is equal to $v + 2\lambda(a_2 - a_1)$. We continue in this fashion and eventually obtain that $v + \mu\lambda(a_2 - a_1) \in A_k(S)$ for all $\mu \in \mathbb{F}_p$. Since $\lambda \neq 0$ we obtain

$$L := \{v + \mu(a_2 - a_1) : \mu \in \mathbb{F}_p\} \subseteq A_k(S).$$

The set $\{v, a_2, a_1\}$ is linearly independent, hence the affine line L does not contain $\mathbf{0}$. □

The proof of Lemma 3.24 relies heavily on $\mathbb{F}_p$ being a prime field, since any non-prime field is not generated by 1 and the addition.

The next lemma states that it is sufficient to consider linearly independent tuples in the step:

(i) Every tuple of vectors of $V \setminus \{\mathbf{0}\}$ can be mapped into a "sufficiently small" subspace of $\mathcal{V}$ by an element of $\mathcal{G}$;

from the beginning of Section 3.2.

We define the *dimension* of a tuple t as the dimension of the subspace spanned by its components. Furthermore we abuse notation and write $\langle t \rangle$ for the linear closure of the components of the tuple t and write $\dim t := \dim \langle t \rangle$.

Lemma 3.25. *Let $n, k \geq 1$. If some linearly independent n-tuple can be mapped into a k-dimensional subspace of $\mathcal{V}$ by an element of $\mathcal{G}$, then every n-tuple can be mapped into a k-dimensional subspace of $\mathcal{V}$ by an element of $\mathcal{G}$.*

Proof. We fix an arbitrary $k \geq 1$ and prove this statement via induction over n. The base case $n = 1$ is obvious. For the induction step we assume the statement holds for n and show it also holds for $n + 1$.

Assume there exists a linearly independent tuple x of size $n+1$ which can be mapped into a k-dimensional subspace of $\mathcal{V}$. Every linearly independent tuple of size $n+1$ can be mapped to x via an automorphism of $\mathcal{V}$. Therefore we only have to consider linearly dependent tuples.

Let a tuple $t = (t_1, \ldots, t_{n+1})$ of dimension smaller than $n+1$ be given. The tuple t has at least one component which is a linear combination of all other components of t. Without loss of generality let t_{n+1} be such a component. By our induction hypothesis the initial segment $\tilde{t} = (t_1, \ldots, t_n)$ of t can be mapped into a k-dimensional subspace W of $\mathcal{V}$ by some $g \in G$. Moreover $\langle \tilde{t}^g \rangle$ is a subset of W, thus if $t_{n+1}^g \in \langle \tilde{t}^g \rangle$, then $t_{n+1}^g \in W$ and we are done. Assume otherwise, i.e., $t_{n+1}^g \notin \langle \tilde{t}^g \rangle$. In that case, by Lemma 3.14 we obtain $|G_{\{t_1,\ldots,t_n\}^g}(t_{n+1}^g)| = \infty$, whence $|G_{\{t_1,\ldots,t_n\}}(t_{n+1})| = \infty$ by Lemma 3.15 (3). Therefore there exists $h \in G_{\{t_1,\ldots,t_n\}}$ such that $t_{n+1}^h \notin \langle \{t_1, \ldots, t_n\} \rangle$, hence $\dim t^h = 1 + \dim t$.

If t^h is linearly independent, we are done. Otherwise the size of t^h is still $n + 1$ and $\dim t^h < n + 1$, thus we can repeat this process. Eventually we end with an element $g \in G$ such that t^g is linearly independent. By assumption t^g can be mapped into a k-dimensional subspace of $\mathcal{V}$ by an element of $\mathcal{G}$, whence so can t. □

Let $S \subseteq V \setminus \{\mathbf{0}\}$ be of size $n \geq 1$. We want to map S into a sufficiently small subspace of $\mathcal{V}$ by an element of $\mathcal{G}$. Since $\mathcal{G}$ preserves $\sim$-equivalence classes and S might contain non-equivalent elements, such a subspace of $\mathcal{V}$ has to contain at least $n|\Gamma|$ elements. As it turns out for the sake of induction it will be convenient to have the subspace contain one additional equivalence class. This means $|\Gamma|$ additional elements. Since every subspace of $\mathcal{V}$ also contains $\mathbf{0}$, this sums up to at least $(n|\Gamma|+|\Gamma|+1)$ elements. For any $k \geq 0$, a k-dimensional subspace of $\mathcal{V}$ contains p^k elements. Therefore the following inequalities have to hold:

$$\begin{aligned} (n+1)|\Gamma|+1 \leq p^k &\iff \\ n \leq \frac{p^k-1}{|\Gamma|} - 1. & \end{aligned} \tag{11}$$

Since $|\Gamma|$ divides $p-1$ it also divides p^k-1, thus the right hand side of (11) is always a natural number.

Lemma 3.26. *Assume that one of the following conditions holds.*

(1) $\Gamma = \mathbb{F}_p^\times$ *and the action of* $\mathcal{G}$ *on* $\mathrm{S}_1(\mathcal{V})$ *does not preserve projective lines, or*

(2) $\Gamma \lneq \mathbb{F}_p^\times$.

Then for all $n \geq 3$ *and all* $k \geq 2$ *such that (11) holds, every* n*-tuple of elements in* $V \setminus \{\mathbf{0}\}$ *can be mapped into a* k*-dimensional subspace of* $\mathcal{V}$ *by an element of* $\mathcal{G}$*.*

Proof. We proof this by induction over n. For the proof assume k to be the smallest natural number which is at least 2 such that (11) holds. For the base case, $n = 3$, we have to distinguish whether the assumption (1) or (2) holds.

Case 1: We assume that (1) holds. The inequality (11) holds for $n = 3$ and $k = 2$. Thus we have to show the statement for $k = 2$. There exists a function $g \in G$ whose action on $\mathrm{S}_1(\mathcal{V})$ does not preserve projective lines. Thus there exist distinct one-dimensional subspaces $L_0 \subseteq L_1 + L_2$ of $\mathcal{V}$ such that $L_0^g \not\subseteq L_1^g + L_2^g$. There are vectors $v_0, v_1, v_2 \in L_1 + L_2$ such that $\langle v_i \rangle = L_i$, for $i = 0, 1, 2$. The tuple (v_0^g, v_1^g, v_2^g) is linearly independent and mapped by g^{-1} into the two-dimensional subspace $L_1 + L_2$ of $\mathcal{V}$. By Lemma 3.25 we are done.

Case 2: We assume that (2) holds. Again $k = 2$ since the right hand side of (11) only increases with smaller Γ. Moreover, because $\Gamma \lneq \mathbb{F}_p^\times$, there are at least two elements $v, w \in V$ which lie in the same one-dimensional subspace of $\mathcal{V}$ and are split by some $g \in G$, i.e., $\langle v \rangle = \langle w \rangle$ and $\dim\langle \{v^g, w^g\} \rangle = 2$. We now choose a vector $u \notin \langle \{v^g, w^g\} \rangle$. Then (v^g, w^g, u) is a linearly independent triple, which is mapped by g^{-1} into the at most two-dimensional subspace $\langle \{u^{g^{-1}}, v, w\} \rangle$ of $\mathcal{V}$. Again by Lemma 3.25 we are done.

This concludes the base case. The right hand side of (11) is strictly increasing in k. Therefore if in the induction step n increases to $n+1$

and (11) does not hold for $n+1$ and k anymore, then it has to hold again for $n+1$ and $k+1$. In the base case $n=3$ and $k=2$, thus $n>k$ in every step of the induction.

We assume we have already shown that every n-tuple can be mapped into a k-dimensional subspace of $\mathcal{V}$ by an element of $\mathcal{G}$.

If

$$n+1 > \frac{p^k-1}{|\Gamma|} - 1,$$

then we are done. This is because given an $(n+1)$-tuple t, the n-tuple obtained by removing one component of t can be mapped into a k-dimensional subspace of $\mathcal{V}$ by some $g \in G$ by our induction hypothesis. Therefore the $(n+1)$-tuple t is mapped by g into a subspace of $\mathcal{V}$ of dimension at most $k+1$.

Thus for the rest of the proof we assume

$$(12) \qquad n+1 \leq \frac{p^k-1}{|\Gamma|} - 1 \iff n|\Gamma| + 2|\Gamma| \leq p^k - 1.$$

By Lemma 3.25 it suffices to find one linearly independent $(n+1)$-tuple which is mapped into a k-dimensional subspace of $\mathcal{V}$ by some element of $\mathcal{G}$. Let $t = (t_1, \ldots, t_{n+1}) \in V^{n+1}$ be a linearly independent tuple and let $\tilde{t} := (t_1, \ldots, t_n)$. If $A_k(\{t_1, \ldots, t_n\}) = V$, then we are done.

Striving for a contradiction, suppose $A_k(\{t_1, \ldots, t_n\}) \neq V$. By the induction hypothesis $\tilde{t}$ can be mapped into a k-dimensional subspace M of $\mathcal{V}$ by some $h \in G$, whence $A_k(\{t_1, \ldots, t_n\}) \neq \emptyset$. By Lemma 3.18 there exists $g \in G$ and a k-dimensional subspace W of $\mathcal{V}$ such that $A_k(\{t_1, \ldots, t_n\}) = W^g$. We want to apply Lemma 3.24. The tuple t is linearly independent, hence so is $\tilde{t}$.

Claim: $A_k(\{t_1, \ldots, t_n\})$ contains at least one element v and a linearly independent set $\{a_1, \ldots, a_n\}$ of size n such that for some $\lambda_1, \ldots, \lambda_n \in F$ we have $v = \lambda_1 a_1 + \cdots + \lambda_n a_n$ and

- not all coefficients $\lambda_1, \ldots, \lambda_n$ are the same,
- at least three of them are non-zero.

From the inequality (12) we obtain that M contains two "extra" equivalence classes, i.e., when $\tilde{t}$ is mapped into the k-dimensional subspace $M \leq \mathcal{V}$ by h, there exist two non-equivalent vectors $v, w \neq \mathbf{0}$ such that $[v^h]_\sim, [w^h]_\sim$ are contained in M but $t_1^h, \ldots, t_n^h$ are neither elements of $[v^h]_\sim$ nor of $[w^h]_\sim$. In particular, v, w are in $A_k(\{t_1, \ldots, t_n\}) \subseteq \langle\{t_1, \ldots, t_n\}\rangle$ and non-equivalent to any component of $\tilde{t}$.

Thus there exist coefficients $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_p$ and $\mu_1, \ldots, \mu_n \in \mathbb{F}_p$ such that $v = \lambda_1 t_1 + \cdots + \lambda_n t_n$ and $w = \mu_1 t_1 + \cdots + \mu_n t_n$. By Lemma

3.21 at least two coefficients of each of these linear combinations have to be non-zero. By the same lemma $\langle v\rangle \neq \langle w\rangle$, thus at least one set of coefficients cannot be all the same. Without loss of generality assume that $\lambda_1, \dots, \lambda_n$ are not all equal. If more than three of these coefficients are not equal to zero we are done. Otherwise without loss of generality $\lambda_3 = \cdots = \lambda_n = 0$, hence

$$v = \lambda_1 t_1 + \lambda_2 t_2, \text{ with } \lambda_1, \lambda_2 \neq 0.$$

We apply Corollary 3.20 to the tuples (t_1, t_2) and (t_3, t_2). We obtain that $u := \lambda_1 t_3 + \lambda_2 t_2$ is an element of $A_k(\{t_1, \dots, t_n\})$ too. By combining the two equations we obtain

$$v = \lambda_1 t_1 + (u - \lambda_1 t_3).$$

The set $\{t_1, u, t_3, t_4, \dots, t_n\}$ is linearly independent and v as a linear combination of these vectors has three coefficients which are not zero. The coefficients are not all equal since $\operatorname{char} \mathbb{F}_p \neq 2$. This shows our claim.

We are finally able to apply Lemma 3.24, which tells us that $A_k(\{t_1, \dots, t_n\})$ contains an affine line not containing $\mathbf{0}$. Moreover we can apply Lemma 3.23 to any set of pairwise linear independent elements contained in $A_k(S)$. In particular $\operatorname{Aff}(\{t_1, \dots, t_n\})$ is contained in $A_k(\{t_1, \dots, t_n\})$.

We distinguish two cases:

Case 1: $\Gamma = \{1\}$**:** In this case the $\sim$-equivalence class of any $v \in V$ contains only v. Together with Lemma 3.21 this implies that for any v in $A_k(\{t_1, \dots, t_n\})$ the vector λv is an element of $A_k(\{t_1, \dots, t_n\})$ iff λ is either 1 or 0. Furthermore since $\langle\{t_1, \dots, t_n\}\rangle = \bigcup_{v \in \operatorname{Aff}(\{t_1, \dots, t_n\})} \langle v\rangle$ and $A_k(\{t_1, \dots, t_n\}) \subseteq \langle\{t_1, \dots, t_n\}\rangle$, the set $A_k(\{t_1, \dots, t_n\})$ is equal to $\operatorname{Aff}(\{t_1, \dots, t_n\}) \cup \{\mathbf{0}\}$.

By Lemma 3.18 the set $A_k(\{t_1, \dots, t_n\})$ contains p^k elements. The set $\operatorname{Aff}(\{t_1, \dots, t_n\}) \cup \{\mathbf{0}\}$ contains $p^{(n-1)} + 1$ elements. This is a contradiction.

Case 2: $\{1\} \subsetneq \Gamma$**:** Since $\operatorname{Aff}(\{t_1, \dots, t_n\})$ does not contain $\mathbf{0}$, it contains pairwise linearly independent elements. By Lemma 3.21 for any element $v \in A_k(\{t_1, \dots, t_n\})$ and any element $\lambda \in \Gamma$ also $\lambda v \in A_k(\{t_1, \dots, t_n\})$. We choose an arbitrary $\lambda \in \Gamma \setminus \{1\}$. Now $\operatorname{Aff}(\{t_1, \dots, t_n\}) \setminus \{t_1\} \cup \{\lambda t_1\}$ is pairwise linearly independent, thus its affine closure is contained in $A_k(\{t_1, \dots, t_n\})$. We have

$$\operatorname{Aff}\left(\operatorname{Aff}(t_1, \dots, t_n) \setminus \{t_1\}\right) = \operatorname{Aff}(t_1, \dots, t_n).$$

Therefore $\mathrm{Aff}\left(\mathrm{Aff}(t_1, \ldots, t_n) \setminus \{t_1\} \cup \{\lambda t_1\}\right)$ is an affine subspace of $\mathcal{V}$ which contains t_1 and λt_1 and in particular $\mathbf{0}$. Hence it is a subspace of $\mathcal{V}$ and we obtain $\langle\{t_1, \ldots, t_n\}\rangle \subseteq A_k(\{t_1, \ldots, t_n\}) \subseteq \langle\{t_1, \ldots, t_n\}\rangle$.

The set $\langle\{t_1, \ldots, t_n\}\rangle$ contains p^n elements, while the cardinality of $A_k(\{t_1, \ldots, t_n\})$ is p^k, which contradicts $n > k$. □

This concludes the step

(i) Every tuple of vectors of $V \setminus \{\mathbf{0}\}$ can be mapped into a "sufficiently small" subspace of $\mathcal{V}$ by an element of $\mathcal{G}$.

The next step from the beginning of Section 3.2 is

(ii) $\mathcal{G}$ acts transitively on arbitrary large tuples of non-equivalent elements of $V \setminus \{\mathbf{0}\}$.

To show this we restrict Lemma 3.26 to tuples containing non-equivalent elements such that the tuples are of specific but still strictly increasing sizes.

Corollary 3.27. *Under the assumptions of Lemma 3.26, for all $k \geq 2$ every tuple t which contains exactly $\frac{p^k-1}{|\Gamma|} - 1$ non-equivalent non-zero elements of $\mathcal{V}$ can be mapped into a k-dimensional subspace W of $\mathcal{V}$ by an element g of $\mathcal{G}$. There is exactly one equivalence class $[v]_\sim$ in $W \setminus \{\mathbf{0}\}$ such that for all components x of t we have $x^g \notin [v]_\sim$.*

Lemma 3.28. *Assume that one of the following conditions holds.*

(1) $\Gamma = \mathbb{F}_p^\times$ and the action of $\mathcal{G}$ on $\mathrm{S}_1(\mathcal{V})$ does not preserve projective lines, or

(2) $\Gamma \lneq \mathbb{F}_p^\times$.

Then for every $n \geq 1$ the group $\mathcal{G}$ acts n-transitively on $(V \setminus \{\mathbf{0}\})/_\sim$.

Proof. For every $k > 2$ we define

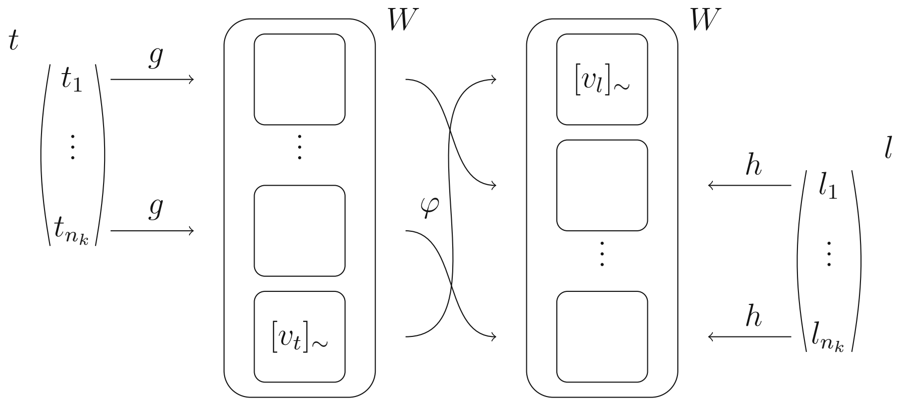
$$n_k := \frac{p^k - 1}{|\Gamma|} - 1.$$

Since $(n_k)_{k>2}$ is a strictly increasing sequence it suffices to show that $\mathcal{G}$ acts n_k-transitively on $(V \setminus \{\mathbf{0}\})/_\sim$ for all $k > 2$.

Let $k > 2$ and $t = (t_1, \ldots, t_{n_k}) \in (V \setminus \{\mathbf{0}\})^{n_k}$ containing non-equivalent elements be given. Since $\mathcal{G}$ acts transitively on linearly independent tuples of arbitrary size, it is enough to show that t can be mapped to some linearly independent n_k-tuple by an element of $\mathcal{G}$.

We fix a linearly independent n_k-tuple $l = (l_1, \ldots, l_{n_k}) \in (V \setminus \{\mathbf{0}\})^{n_k}$. By Corollary 3.27 both t and l can be mapped into a k-dimensional subspace of $\mathcal{V}$ by $g \in G$ and $h \in G$ respectively. Since $\mathrm{Aut}(\mathcal{V}) \leq \mathcal{G}$ without loss of generality we may assume that both t and l are mapped into the same k-dimensional subspace $W \leq \mathcal{V}$.

Let $[v_t]_\sim \subseteq W \setminus \{\mathbf{0}\}$ be the unique equivalence class such that t^g does not contain any element of $[v_t]_\sim$, and let $[v_l]_\sim \subseteq W \setminus \{\mathbf{0}\}$ be the unique equivalence class such that l^h does not contain any element of $[v_l]_\sim$. There exists an automorphism φ of $\mathcal{V}$ which maps v_t to v_l and such that $\varphi(W) = W$. We obtain the following picture.



Thus $t^{g\varphi h^{-1}} = l$ up to the order of the components of l. Since we only needed some linearly independent tuple to map t to, this concludes the proof. □

The last step from the beginning of Section 3.2 is still missing:

(iii) The action of $\mathcal{G}$ on $(V \setminus \{\mathbf{0}\})/_\sim$ is closed.

Currently we only know that $\mathcal{G}$ is closed as an action on the elements of V. Since $\sim$ has only finite equivalence classes we can show that the closedness from $\mathcal{G}$ acting on V is inherited to $\mathcal{G}$ acting on $(V \setminus \{\mathbf{0}\})/_\sim$.

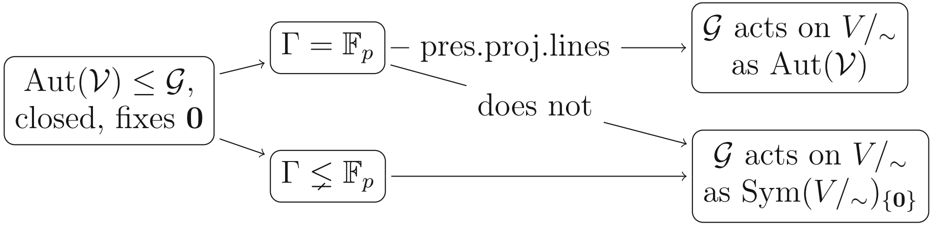
Lemma 3.29. *Let S be a countable set, let $\mathcal{M} \leq \mathrm{Sym}(S)$ be closed, and let $\simeq$ be an $\mathcal{M}$-invariant equivalence relation on S such that all its equivalence classes are finite. Then the action of $\mathcal{M}$ on the set $S/_\simeq$ of equivalence classes is closed.*

Proof. Let $\{E_n : n \geq 0\}$ be an enumeration of the $\simeq$-equivalence classes and let $(f_n)_{n\geq 0}$ be a sequence in $\mathcal{M}$ which converges in the action of $\mathcal{M}$ on $S/_{\simeq}$ to a function $f \in \mathrm{Sym}(S/_{\simeq})$.

By restricting to a subsequence we may assume that for all $n \geq 0$ we have that for all $k \geq n : f_k(E_n) = f(E_n)$. For every $n \geq 0$ the equivalence class E_n is finite, thus there are infinitely many distinct $i, j \geq n$ such that $f_i|_{E_n} = f_j|_{E_n}$. Again by restricting to subsequences we may assume that for all n we have that $\forall i, j \geq n : f_i|_{E_n} = f_j|_{E_n}$. Now the sequence $(f_n)_{n\geq 0}$ converges in the action of $\mathcal{M}$ on S to a function $\tilde{f} \in \mathrm{Sym}(S)$. Since $\mathcal{M}$ is closed we obtain $\tilde{f} \in M$. The action of $\tilde{f}$ on $S/_{\simeq}$ is equal to f, thus the action of $\mathcal{M}$ on $S/_{\simeq}$ is closed. □

This shows step (iii), and completes the proof of Theorem 3.13. We now know the action of $\mathcal{G}$ on the $\sim$-equivalence classes. With the help of this we may now continue our investigation of the structure of $\mathcal{G}$ as permutation group on V.

3.3. **$\mathcal{G}$ as the composition of two groups.** In Section 3 to Section 3.2 we showed for a permutation group $\mathcal{G}$ on V and Γ and $\sim$ as in Section 3 the following connections.

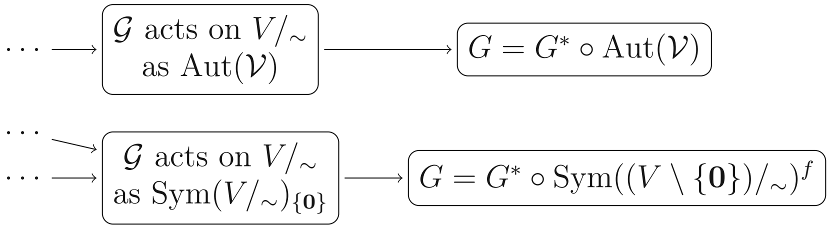

$\mathrm{Aut}(\mathcal{V}) \leq \mathcal{G}$, closed, fixes $\mathbf{0}$
$\Gamma = \mathbb{F}_p$
pres.proj.lines
$\mathcal{G}$ acts on $V/_\sim$ as $\mathrm{Aut}(\mathcal{V})$
does not
$\Gamma \lneq \mathbb{F}_p$
$\mathcal{G}$ acts on $V/_\sim$ as $\mathrm{Sym}(V/_\sim)_{\{\mathbf{0}\}}$

Instead of looking at the action of $\mathcal{G}$ on the $\sim$-equivalence classes we now consider the elements of $\mathcal{G}$ as functions on V. In order to do this we decompose every element $g \in G$ into two parts, one that acts on $V/_\sim$ as the identity and one that may move the $\sim$-equivalence classes.

We define

$$\mathrm{Sym}^*(V) := \{g \in \mathrm{Sym}(V) : g \text{ acts on } V/_\sim \text{ as the identity}\}.$$

Continuing the picture above our goal this section is to show:


. . .
$\mathcal{G}$ acts on $V/_\sim$ as $\mathrm{Aut}(\mathcal{V})$
$G = G^* \circ \mathrm{Aut}(\mathcal{V})$
. . .
. . .
$\mathcal{G}$ acts on $V/_\sim$ as $\mathrm{Sym}(V/_\sim)_{\{\mathbf{0}\}}$
$G = G^* \circ \mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$

Here, $G^* := \mathrm{Sym}^*(V) \cap G$, which clearly is the domain of a closed subgroup $\mathcal{G}^*$ of $\mathcal{G}$. The set $\mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$ will be a subgroup of $\mathrm{Sym}(V)$ which still acts like $\mathrm{Sym}(V/_\sim)_{\mathbf{0}}$ on $V/_\sim$ and "fixes the insides" of the $\sim$-equivalence classes. We will define it later.

The case that $\Gamma = \mathbb{F}_p^\times$ and the action of $\mathcal{G}$ on $\mathrm{S}_1(\mathcal{V})$ preserves projective lines turns out to be rather simple. We recall that in this case the equivalence classes of $\sim$ are exactly the zero-dimensional subspace $\{\mathbf{0}\}$ and the one-dimensional subspaces of $\mathcal{V}$ without $\mathbf{0}$.

Lemma 3.30. *Assume that $\Gamma = \mathbb{F}_p^\times$ and the action of $\mathcal{G}$ on $\mathrm{S}_1(\mathcal{V})$ preserves projective lines. Then*

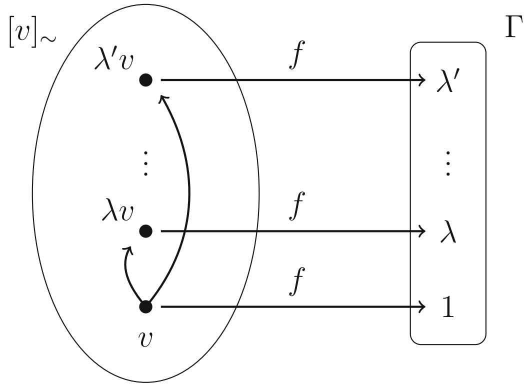
$$G = G^* \circ \mathrm{Aut}(\mathcal{V}).$$

Proof. We only need to show the inclusion $G \subseteq G^* \circ \mathrm{Aut}(\mathcal{V})$. By Theorem 3.12 for all $g \in G$ there exists a function $\varphi \in \mathrm{Aut}(\mathcal{V}) \leq G$ such that the action φ on $\mathrm{S}_1(\mathcal{V})$ is the same as the one of g. Thus, $g \circ \varphi^{-1}$ acts as the identity on $(V/\{\mathbf{0}\})/_\sim$ and is therefore an element of $\mathcal{G}^*$. □

In order to talk about how an element $g \in G$ "fixes the insides" of the $\sim$-equivalence classes we need to label the elements of the equivalence classes in a consistent way.

Definition 3.31. For any $\Lambda \leq \mathbb{F}_p^\times$ a function $f\colon V \to \Lambda$ is a Λ-*labelling* iff for all $v \in V$ and all $\lambda \in \Lambda$ we have $f(\lambda v) = \lambda f(v)$.

We recall that Γ is the subgroup of $\mathbb{F}_p^\times$ such that for all $v \in V$ the equivalence class $[v]_\sim$ is equal to $\Gamma v = \{\lambda v : \lambda \in \Gamma\}$. We can define a Γ-labelling $f\colon V \to \Gamma$ by choosing for each $\sim$-equivalence class an arbitrary representative v and setting $f(v) := 1 \in \Gamma$. Since the equivalence class $[v]_\sim$ is equal to Γv this already determines f fully. We end up with the following picture.



This also shows the existence of Γ-labellings. For all $v \in V$ and any Γ-labelling f we call $f(v)$ the *label of* v.

Definition 3.32. Let g be an element of $\mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)$ and let $f\colon V \to \Gamma$ be a Γ-labelling. Then the function $g^f \in \mathrm{Sym}(V)_{\mathbf{0}}$ is defined by

- g^f preserves $\sim$,
- the action of g^f on $(V \setminus \{\mathbf{0}\})/_\sim$ is equal to g, and
- for all $v \in V$ we have $f(v^{g^f}) = f(v)$.

For a set $S \subseteq \mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)$ we define $S^f := \{g^f : g \in S\}$.

Our goal is to show that, if $\Gamma \lneq \mathbb{F}_p$ or $\Gamma = \mathbb{F}_p$ and the action of $\mathcal{G}$ on $\mathrm{S}_1(\mathcal{V})$ does not preserves projective lines, then for all Γ-labellings f the set $\mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$ is contained in G. From this it will easily follow that $G = G^* \circ \mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$.

In order to do this we need to know how a given $g \in G$ acts on the "inside of a $\sim$-equivalence class". We define the following.

Definition 3.33. Let f be a Γ-labelling, let $v \in V$ and let $g \in G$. A function $\sigma_f(g,v)\colon \Gamma \to \Gamma$ is defined by, for any $\lambda \in \Gamma$:

$$\lambda \quad \longmapsto f\left(\left(\lambda\left(\frac{1}{f(v)}v\right)\right)^g\right). \tag{13}$$

Step by step what happens in (13) is the following. Let f, v, g be as in Definition 3.33.

(1) The element $\frac{1}{f(v)}v$ is the element in $[v]_\sim$ which has label $1 \in \Gamma$.

(2) The element $\lambda(\frac{1}{f(v)}v) =: x$ is the element in $[v]_\sim$ which has label λ.

(3) x^g is an element in the $\sim$-equivalence class $g([v]_\sim)$.

(4) Finally $f(x^g)$ is the label of x^g.

In conclusion $\sigma_f(g,v)$ tells us how g acts on the labels of the elements of $[v]_\sim$.

Lemma 3.34. *Let f be a Γ-labelling. Then for all $v \in V$ and all $g \in G$ the following holds.*

(1) $\sigma_f(g,v) \in \mathrm{Sym}(\Gamma)$.

(2) For all $w \in [v]_\sim$ we have $\sigma_f(g,v) = \sigma_f(g,w)$.

(3) For all $w \in V$ we have $\sigma_f(g,w) = \mathrm{id}_\Gamma$ iff $g \in \mathrm{Sym}((V\setminus\{\mathbf{0}\})/_\sim)^f$.

Proof. All items follow directly from the definitions. □

Lemma 3.35. *Let g, h be elements of $\mathcal{G}$ and let f be a Γ-labelling. Then for all $v \in V$*

$$\sigma_f(gh,v) = \sigma_f(g,v) \circ \sigma_f(h,v^g). \tag{14}$$

Proof. Let $v \in V$ be given. By Lemma 3.34 (2) we may assume without loss of generality that $f(v) = 1$. There exist $u, w \in V$ such that $[w]_\sim = [u^h]_\sim = [v^{gh}]_\sim$ and $f(u) = f(w) = 1$. For all $\lambda \in \Gamma$, there exist $\mu, \nu \in \Gamma$ such that $(\lambda v)^{gh} = (\mu u)^h = \nu w$. Then the following picture holds.

$$\begin{tikzcd}
\lambda v \arrow[r, "g"] \arrow[d, "f"] \arrow[rr, bend left, "g \circ h"] & (\lambda v)^g \arrow[r, "h"] \arrow[d, "f"] & (\lambda v)^{gh} \arrow[d, "f"] \\
\lambda \arrow[r, "\sigma_f(g,v)"] \arrow[rr, bend right, "\sigma_f(gh,v)"'] & \mu \arrow[r, "\sigma_f(h,u)"] & \nu
\end{tikzcd}$$

Since $\sigma_f(h, v^g) = \sigma_f(h, u)$ this concludes the proof. □

From Lemma 3.35 it follows immediately that for all Γ-labellings f, all $g \in G$ and all $v \in V$ the inverse of $\sigma_f(g, v)$ is $\sigma_f(g^{-1}, v)$. Additionally Lemma 3.35 shows that $\mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$ is a subgroup of $\mathrm{Sym}(V)$.

We are now able to find a function in $G \cap \mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$ which acts cyclically on an infinite linearly independent set of vectors.

Lemma 3.36. *Let f be a Γ-labelling. Assume that $\mathcal{G}$ acts as the full symmetric group on the equivalence classes $(V \setminus \{\mathbf{0}\})/_\sim$. Then for all infinite and linearly independent sets $\{v_i : i \in \mathbb{Z}\} \subseteq V$ such that $|V \setminus \langle \{v_i : i \in \mathbb{Z}\}\rangle| = \infty$ there exists $g \in G \cap \mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$ such that*

$$\cdots \xrightarrow{g} [v_{-1}]_\sim \xrightarrow{g} [v_0]_\sim \xrightarrow{g} [v_1]_\sim \xrightarrow{g} \cdots$$

and g acts as the identity on $(V/_\sim) \setminus \{[v_i]_\sim : i \in \mathbb{Z}\}$.

Proof. Let an infinite and linearly independent set $\{v_i : i \in \mathbb{Z}\}$ such that $V \setminus \langle \{v_i : i \in \mathbb{Z}\}\rangle$ is infinite be given. Without loss of generality we may assume that for every $i \in \mathbb{Z}$ we have $f(v_i) = 1$.

Since $\mathcal{G}$ acts as the full symmetric group on $(V \setminus \{\mathbf{0}\})/_\sim$ there exists an element $g \in G$ such that for all $i \in \mathbb{Z}$ we have $g([v_i]_\sim) = [v_{i+1}]_\sim$ and such that g acts as the identity on $(V/_\sim) \setminus \{[v_i]_\sim : i \in \mathbb{Z}\}$. From this g we now construct a function h which acts like g on the $\sim$-equivalence classes and additionally for all $v \in V$ we have $\sigma_f(h, v) = \mathrm{id}_\Gamma$.

Since $\{v_i : i \in \mathbb{Z}\}$ is linearly independent there exists an automorphism $\varphi \in \mathrm{Aut}(\mathcal{V})$ such that $\varphi([v_i]_\sim) = [v_{i+1}]_\sim$ for all $i \in \mathbb{Z}$.

The label of every v_i is 1 and since every vector space automorphism is compatible with scalar multiplication we obtain for all $i \in \mathbb{Z}$:

$$\sigma_f(\varphi, v_i) = \mathrm{id}_\Gamma\,.$$

For all $n \geq 0$ we define $g_n := \varphi^{-n} \circ g \circ \varphi^n$. Since g acts as the identity on $(V/_\sim) \setminus \{[v_i] : i \in \mathbb{Z}\}$ so does g_n. By Lemma 3.35 we obtain for all $n \geq 0$ and all $i \in \mathbb{Z}$:

$$\sigma_f(g_n, v_i) = \sigma_f(g, v_{i-n}).$$

Moreover, for all $n \geq 0$ an all $i \in \mathbb{Z}$ the function g_n maps $[v_i]_\sim$ to $[v_{i+1}]_\sim$. We define $g' := g_0 \circ g_1 \circ \cdots \circ g_{|\Gamma|!-1}$ and obtain for all $i \in \mathbb{Z}$:

$$\begin{aligned}\sigma_f(g', v_i) &= \sigma_f(g_0, v_i) \circ \sigma_f(g_1, v_{i+1}) \circ \cdots \circ \sigma_f(g_{|\Gamma|!-1}, v_{i+|\Gamma|!-1})\\ &= \sigma_f(g, v_i)^{|\Gamma|!} = \mathrm{id}_\Gamma\,.\end{aligned}$$

The last equality follows since $|\mathrm{Sym}(\Gamma)| = |\Gamma|!$.

We found g' such that for all $i \in \mathbb{Z}$ we have $\sigma_f(g', v_i) = \mathrm{id}_\Gamma$. We now want g'' such that additionally g'' acts as the identity inside the equivalence classes $(V/_\sim) \setminus \{[v_i] : i \in \mathbb{Z}\}$. For this we set $g'' := (g')^{|\Gamma|!}$. For all $i \in \mathbb{Z}$ we still have $\sigma_f(g'', v_i) = \mathrm{id}_\Gamma$. The function g' acts as the identity on the $\sim$-equivalence classes which are not elements of $\{[v_i]_\sim : i \in \mathbb{Z}\}$, therefore for every $u \in V$ which is not equivalent to an element in $\{v_i : i \in \mathbb{Z}\}$ we obtain

$$\sigma_f(g'', u) = \sigma_f(g', u)^{|\Gamma|!} = \mathrm{id}_\Gamma\,.$$

By Lemma 3.34 (3) we obtain that $g'' \in G \cap \mathrm{Sym}((V \setminus \{0\})/_\sim))^f$.

We set $k := |\Gamma|!|\Gamma|!$. Now g'' acts on $\{v_i : i \in \mathbb{Z}\}$ in the following way

$$\begin{array}{ccccccccc}
\cdots & \xrightarrow{g''} & v_{-k} & \xrightarrow{g''} & v_0 & \xrightarrow{g''} & v_k & \xrightarrow{g''} & \cdots\,, \\
\cdots & \xrightarrow{g''} & v_{1-k} & \xrightarrow{g''} & v_1 & \xrightarrow{g''} & v_{1+k} & \xrightarrow{g''} & \cdots\,, \\
 & & & & \vdots & & & & \\
\cdots & \xrightarrow{g''} & v_{(k-1)-k} & \xrightarrow{g''} & v_{(k-1)} & \xrightarrow{g''} & v_{(k-1)+k} & \xrightarrow{g''} & \cdots\,,
\end{array}$$

and inside the equivalence classes $(V/_\sim)\setminus\{[v_i]_\sim : i \in \mathbb{Z}\}$ as the identity.

Let a finite set $F \subseteq V$ be given. Since $V \setminus \langle\{v_i : i \in \mathbb{Z}\}\rangle$ is infinite there exists an automorphism $\varphi_F \in \mathrm{Aut}(\mathcal{V})$ such that φ_F restricted to $\langle\{v_{jk} : j \in \mathbb{Z}\}\rangle$ is the identity and

$$\varphi_F\left(F \setminus \langle\{v_{jk} : j \in \mathbb{Z}\}\rangle\right) \subseteq V \setminus \langle\{v_i : i \in \mathbb{Z}\}\rangle\,.$$

Since g'' acts as the identity on $V \setminus \langle\{v_i : i \in \mathbb{Z}\}\rangle$ the composition $\varphi_F \circ g'' \circ \varphi_F^{-1}$ acts as the identity on

$$F \setminus \langle\{v_{jk} : j \in \mathbb{Z}\}\rangle\,.$$

Now $(\varphi_F \circ g'' \circ \varphi_F^{-1})$ preserves the labels of all elements in F. Since $G \cap \mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$ is closed there exists a function h therein such that

$$\cdots \xrightarrow{h} v_{-k} \sim \xrightarrow{h} v_0 \xrightarrow{h} v_k \xrightarrow{h} \cdots\,,$$

and h acts as the identity on the complement of $\bigcup\{[v_{jk}]_\sim : j \in \mathbb{Z}\}$.

There exists $\varphi \in \mathrm{Aut}(\mathcal{V})$ such that for all $i \in \mathbb{Z}$ we have $v_i^\varphi = v_{ik}$. Now $\varphi \circ h \circ \varphi^{-1}$ proves our statement. □

With the help of Lemma 3.36 we are now able to show that any transposition of two equivalence classes can be achieved by a function in $G \cap \mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$. From this, we quickly obtain the following.

Lemma 3.37. *Let f be a Γ-labelling. Assume that $\mathcal{G}$ acts on $(V \setminus \{\mathbf{0}\})/_\sim$ as the full symmetric group. Then*

$$\mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f \leq \mathcal{G}.$$

Proof. First, let two linearly independent vectors $v, w \in V$ such that $f(v) = f(w)$ be given. Let $\{v_i : i \in \mathbb{Z}\}$ be an infinite linearly independent subset of V as in Lemma 3.36 and such that $v_{-1} = v$ and $v_0 = w$. By Lemma 3.36 there exists $g \in G \cap \operatorname{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$ such that g is the identity on $V \setminus \{[v_i]_\sim : i \in \mathbb{Z}\}$ and

$$\cdots \xrightarrow{g} v_{-1} \xrightarrow{g} v_0 \xrightarrow{g} v_1 \xrightarrow{g} \cdots .$$

The set $\{v_i : i \in \mathbb{Z} \setminus \{0\}\}$ still satisfies the assumptions of Lemma 3.36, thus there exists $h \in G \cap \operatorname{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$ such that h is the identity on $V \setminus \{[v_i]_\sim : i \in \mathbb{Z} \setminus \{0\}\}$ and

$$\cdots \xrightarrow{h} v_{-1} \xrightarrow{h} v_1 \xrightarrow{h} v_2 \xrightarrow{h} \cdots .$$

For all $i \neq -1, 0$ we have $v_i^{gh^{-1}} = v_{i+1}^{h^{-1}} = v_i$ and

$$v_{-1}^{gh^{-1}} = v_0^{h^{-1}} = v_0 = w \quad \text{and} \quad v_0^{gh^{-1}} = v_1^{h^{-1}} = v_0 = v.$$

Therefore, since g and h act as the identity on $V \setminus \{[v_i]_\sim : i \in \mathbb{Z}\}$, we obtain that $g \circ h^{-1} \in G \cap \operatorname{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$ is the function which swaps exactly $[v]_\sim$ and $[w]_\sim$ while fixing everything else. We denote this function by $\pi_{[v]_\sim,[w]_\sim}$.

For two vectors $v \not\sim w$ such that $\langle v \rangle = \langle w \rangle$ we choose $u \in V \setminus \langle v \rangle$. By Lemma 3.36 and by what we showed $\pi_{[v]_\sim,[u]_\sim}$ and $\pi_{[w]_\sim,[u]_\sim}$ are both in $G \cap \operatorname{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$. Since

$$\pi_{[v]_\sim,[u]_\sim} \circ \pi_{[w]_\sim,[u]_\sim} \circ \pi_{[v]_\sim,[u]_\sim} = \pi_{[v]_\sim,[w]_\sim}$$

we obtain that every function which swaps exactly two $\sim$-equivalence classes and preserves labels is an element of $G \cap \operatorname{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$. Those functions generate the group $\operatorname{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$ and therefore $G \cap \operatorname{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$ equals $\operatorname{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$. □

From here we show as in Lemma 3.30 that $\mathcal{G}$ decomposes into two groups.

Corollary 3.38. *Let f be a Γ-labelling. Assume that $\mathcal{G}$ acts on $(V \setminus \{\mathbf{0}\})/_\sim$ as the full symmetric group. Then*

$$G = G^* \circ \operatorname{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f.$$

Proof. The inclusion $G \supseteq G^* \circ \operatorname{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$ holds by Lemma 3.37. For the other inclusion let an arbitrary $g \in G$ be given. Again by Lemma 3.37 there exists $g' \in \operatorname{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$ which acts like g on the $\sim$-equivalence classes, hence $g \circ g'^{-1} \in G^*$. □

3.4. **Finiteness of the set of 0-defining reducts of $\mathcal{V}$.** The goal of this section is to show that there are only finitely many reducts of $\mathcal{V}$ which define $\mathbf{0}$, i.e., there are only finitely many possibilities for the group $\mathcal{G} \leq \mathrm{Sym}(V)_{\mathbf{0}}$ being closed and containing $\mathrm{Aut}(\mathcal{V})$.

In Section 3.3 we have seen in Lemma 3.38 and Lemma 3.30 that $\mathcal{G}$ can always be decomposed into $\mathrm{Aut}(\mathcal{V})$ or $\mathrm{Sym}((V \setminus \{\mathbf{0}\})/_{\sim})^f$ for some Γ-labelling f and the subgroup $\mathcal{G}^*$ of $\mathcal{G}$. In this section we will show that $\mathcal{G}^*$ is already fully determined by two subgroups $\mathcal{H}$ and $\mathcal{N}$ of $\mathrm{Sym}(\Gamma)$. Since $\mathrm{Sym}(\Gamma)$ is finite this will yield the desired result. For the rest of this section we fix a Γ-labelling,

$$f \colon V \to \Gamma.$$

First we will define the sets N and H which will later turn out to be the domains of two permutation groups on Γ.

Definition 3.39. The set H is defined as the set of permutations $\sigma \in \mathrm{Sym}(\Gamma)$ such that

- there exists a function $g \in G^*$ and a vector $v \in V$ such that $\sigma_f(g, v) = \sigma$.

The set N is defined as the set of permutations $\sigma \in \mathrm{Sym}(\Gamma)$ such that

- there exists a function $g \in G^*$ and a vector $v \in V$ such that $\sigma_f(g, v) = \sigma$, and
- for all $\mathbf{0} \neq w \in V \setminus [v]_\sim$ we have $\sigma_f(g, w) = \mathrm{id}_\Gamma$, i.e., $g|_{V\setminus[v]_\sim}$ is the identity on $V \setminus [v]_\sim$.

For any $\lambda \in \Gamma$ we denote the function which acts on Γ by multiplication by $\lambda \colon \Gamma \to \Gamma$.

Lemma 3.40. *Let γ be an automorphism of $\mathcal{V}$, let $v \in V \setminus \{\mathbf{0}\}$ and let $g \in \mathrm{Sym}^*(V)$. Then*

$$\sigma_f(\gamma g \gamma^{-1}, v) = \left(\frac{f(v^\gamma)}{f(v)}\right) \circ \sigma_f(g, v^\gamma) \circ \left(\frac{f(v)}{f(v^\gamma)}\right).$$

Proof. By Lemma 3.35 we obtain

$$\sigma_f(\gamma g \gamma^{-1}, v) = \sigma_f(\gamma, v) \circ \sigma_f(g, v^\gamma) \circ \sigma_f(\gamma^{-1}, v^{\gamma g}),$$

and

$$\mathrm{id}_\Gamma = \sigma_f(\gamma^{-1}\gamma, v^{\gamma g}) = \sigma_f(\gamma^{-1}, v^{\gamma g}) \circ \sigma_f(\gamma, v^{\gamma g \gamma^{-1}}).$$

The function g fixes the $\sim$-equivalence classes, hence $[v]_\sim = [v^{\gamma g \gamma^{-1}}]_\sim$. Combining those two equations we obtain

$$\sigma_f(\gamma g \gamma^{-1}, v) = \sigma_f(\gamma, v) \circ \sigma_f(g, v^\gamma) \circ \sigma_f(\gamma, v)^{-1}.$$

Finally for all $\lambda \in \Gamma$ the function $\sigma_f(\gamma, v)$ maps λ to

$$f\left(\left(\lambda \frac{v}{f(v)}\right)^{\gamma}\right) = f\left(\lambda \frac{v^{\gamma}}{f(v)}\right) = \lambda \frac{f(v^{\gamma})}{f(v)}.$$

This concludes the proof. □

A special case of Lemma 3.40 which we will use repeatedly is the following: let g be an element of $\mathcal{G}^*$, if $\gamma \in \mathrm{Aut}(\mathcal{V})$ maps a vector $v \in V \setminus \{\mathbf{0}\}$ to a vector v^{γ} of the same f-label, then

$$\sigma_f(\gamma g \gamma^{-1}, v) = \sigma_f(g, v^{\gamma}). \tag{15}$$

In the definition of H and N we only required the existence of some vector. We show that we can in fact always choose a vector.

Lemma 3.41. *Let v be an element of $V \setminus \{\mathbf{0}\}$. The following holds.*

- *For all $h \in H$ there exists $g_h \in G^*$ such that $\sigma_f(g_h, v) = h$.*
- *For all $n \in N$ there exists $g_n \in G^*$ such that $\sigma_f(g_n, v) = n$ and for all $\mathbf{0} \neq w \in V \setminus [v]_\sim$ we have $\sigma_f(g_n, w) = \mathrm{id}_\Gamma$.*

Proof. We prove only the second item; the proof of the first item is identical. Let $n \in N$ be given. By Definition 3.39 there exists $g \in G^*$ and $u \in V$ such that $\sigma_f(g, u) = n$ and for all non-zero vectors $w \in V \setminus [u]_\sim$ we have $\sigma_f(g, w) = \mathrm{id}_\Gamma$. Without loss of generality we assume $f(v) = f(u) = 1$. Let γ be an automorphism of $\mathcal{V}$ such that $v^{\gamma} = u$. We define $g' := \gamma \circ g \circ \gamma^{-1}$. The function g acts as the identity on $V/\sim$, hence $g' \in G^*$. Moreover, since $g|_{V\setminus[u]_\sim} = \mathrm{id}_{V\setminus[u]_\sim}$ we obtain $g'|_{V\setminus[v]_\sim} = \mathrm{id}_{V\setminus[v]_\sim}$. By Lemma 3.35 and because $f(v) = f(v^{\gamma}) = 1$ we have

$$\sigma_f(g', v) = \sigma_f(\gamma, v) \circ \sigma_f(g, u) \circ \sigma_f(\gamma^{-1}, v) = \mathrm{id}_\Gamma \circ n \circ \mathrm{id}_\Gamma = n.$$

□

We can now show that N and H are the domains of two subgroups $\mathcal{N}$ and $\mathcal{H}$ of $\mathrm{Sym}(\Gamma)$ and that $\mathcal{N}$ is normal in $\mathcal{H}$.

Lemma 3.42. *N and H induce permutation groups $\mathcal{N}$ and $\mathcal{H}$ in Γ.*

Proof. Let h_1, h_2 be functions of H. Then by Lemma 3.41 there exist a vector $v \in V$ and $g_1, g_2 \in G^*$ such that $\sigma_f(g_1, v) = h_1$ and $\sigma_f(g_2, v) = h_2$. By Lemma 3.35 since $[v^{g_1}]_\sim = [v]_\sim$ we obtain $\sigma_f(g_1 g_2, v) = h_1 \circ h_2$, hence $h_1 \circ h_2 \in H$. Clearly the same holds for N, and so both H and N are domains of permutation groups $\mathcal{H}$ and $\mathcal{N}$ in Γ. □

Lemma 3.43. *$\mathcal{N}$ is normal in $\mathcal{H}$.*

Proof. Let $n \in N$ and $h \in H$ be given. Then by Lemma 3.41 there exists a vector $v \in V$ and $g_h, g_n \in G^*$ such that $\sigma_f(g_n, v) = n$ and $\sigma_f(g_h, v) = h$. Moreover $g_h^{-1} \circ g_n \circ g_h \in G^*$ and we obtain

$$\sigma_f(g_h^{-1} g_n g_h, v) = \sigma_f(g_h^{-1}, v) \circ \sigma_f(g_n, v) \circ \sigma_f(g_h, v) = h^{-1} \circ n \circ h.$$

Since g_n fixes every element in $V \setminus [v]_\sim$ so does $g_h^{-1} \circ g_n \circ g_h$, hence $h^{-1} \circ n \circ h \in N$. □

We now want to reconstruct $\mathcal{G}^*$ from $\mathcal{N}$ and $\mathcal{H}$. If we manage to do so, then since

(1) $G = G^* \circ \mathrm{Aut}(\mathcal{V})$, or
(2) $G = G^* \circ \mathrm{Sym}((V \setminus \{\mathbf{0}\})/\sim)^f$,

there are only finitely many different closed groups fixing $\mathbf{0}$ between $\mathrm{Aut}(\mathcal{V})$ and $\mathrm{Sym}(V)$.

Definition 3.44. Let $\mathcal{N}'$ and $\mathcal{H}'$ be two permutation groups on Γ. We define $S(\mathcal{N}', \mathcal{H}')$ as the set of all $g \in \mathrm{Sym}^*(V)$ such that for all $v, w \in V \setminus \{\mathbf{0}\}$:

(1) $\sigma_f(g, v) \in H'$, and
(2) $\sigma_f(g, v) \circ \sigma_f(g, w)^{-1} \in N'$.

Our goal is to show that $S(\mathcal{N}, \mathcal{H})$ is equal to $\mathcal{G}^*$. By Lemma 3.30 and Corollary 3.38 there are two cases:

(1) $G = G^* \circ \mathrm{Aut}(\mathcal{V})$, or
(2) $G = G^* \circ \mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$.

The second case turns out to be straightforward since $\mathcal{G}$ can map any $\sim$-equivalence class to any other $\sim$-equivalence class, while still preserving the insides of the $\sim$-equivalence classes.

We define for any subset S of V the set $[S]_\sim := \bigcup_{s \in S} [s]_\sim$.

Lemma 3.45 through Lemma 3.47 are very easy observations dealing with the second case. Finally, Lemma 3.48 will show that in the second case $S(\mathcal{N}, \mathcal{H})$ is equal to $\mathcal{G}^*$.

Lemma 3.45. *Let S be a subset of $V \setminus \{\mathbf{0}\}$ and let $n \in N$. Then there exists $g \in G^*$ such that for all $v \in S$ we have $\sigma_f(g, v) = n$ and $g|_{V \setminus [S]_\sim} = \mathrm{id}_{V \setminus [S]_\sim}$.*

Proof. Let $M \subseteq [S]_\sim$ such that $[M]_\sim = S$ and no two elements of M are $\sim$-equivalent. By Lemma 3.41 for every $v \in M$ there exists $g_v \in G^*$ such that $\sigma_f(g_v, v) = n$ and $g_v|_{V \setminus [v]_\sim} = \mathrm{id}_{V \setminus [v]_\sim}$. If S is finite then the composition of all g_v such that $v \in M$ in any order proves the statement. Since $\mathcal{G}^*$ is closed, this holds for all infinite $S \subseteq V$ as well. □

If an element g of $\mathcal{G}$ acts on an infinite subset of V as the identity, then the action of g on the labels of any $\sim$-equivalence class is in N.

Lemma 3.46. *Let S be an infinite subset of V and let $g \in G^*$. Assume that $G = G^* \circ \mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$. If $g|_{[S]_\sim} = \mathrm{id}_{[S]_\sim}$, then for all $v \in V \setminus \{\mathbf{0}\}$ we have $\sigma_f(g, v) \in N$.*

Proof. Let $v \in V \setminus \{\mathbf{0}\}$ be given. We need to show the existence of $g' \in G^*$ such that $\sigma_f(g', v) = \sigma_f(g, v)$ and $g'|_{V\setminus[v]_\sim} = \mathrm{id}_{V\setminus[v]_\sim}$. Let F be a finite subset of V. Since $\mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f \leq \mathcal{G}$ there exists $\bar{g} \in G$ such that $v^{\bar{g}} = v$ and $\bar{g}(F \setminus [v]_\sim) \subseteq [S]_\sim$. We obtain $v^{\bar{g}g\bar{g}^{-1}} = v^g$ and $\bar{g} \circ g \circ \bar{g}^{-1}|_{F\setminus[v]_\sim} = \mathrm{id}_{F\setminus[v]_\sim}$. The function $\bar{g} \circ g \circ \bar{g}^{-1}$ is an element of $\mathcal{G}^*$ and $\mathcal{G}^*$ is closed, hence there exists $g' \in G^*$ with the desired properties. □

Lemma 3.47. *Let S be an infinite subset of $V \setminus \{\mathbf{0}\}$ and let $g \in G^*$. Assume that $G = G^* \circ \mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$. If for all $v, w \in S$ we have $\sigma_f(g, v) = \sigma_f(g, w) =: h$, then there exists $g' \in G^*$ such that for all $u \in V \setminus \{\mathbf{0}\}$ we have $\sigma_f(g', u) = h$.*

Proof. As in the proof of Lemma 3.46 for any finite $F \subseteq V \setminus \{\mathbf{0}\}$ there exists $\bar{g} \in G$ such that $\bar{g}(F) \subseteq [S]_\sim$. Thus for all $v \in [F]_\sim$ we have $\sigma_f(\bar{g}g\bar{g}^{-1}|_{[F]_\sim}, v) = h$ and hence there exits $g' \in G^*$ such that for all $u \in V \setminus \{\mathbf{0}\}$ we have $\sigma_f(g', u) = h$. Since $\mathcal{G}$ is closed this proves the statement. □

Lemma 3.48. *Let g be an element of $\mathcal{G}^*$. Assume that $G = G^* \circ \mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$. Then for all $v, w \in V$ the function $\sigma_f(g, v) \circ \sigma_f(g, w)^{-1}$ is an element of $\mathcal{N}$.*

Proof. The group $\mathrm{Sym}(\Gamma)$ is finite, therefore there is an infinite set $S \subseteq V$ such that for all $v, w \in S$ we have $\sigma_f(g, v) = \sigma_f(g, w) =: h \in \mathrm{Sym}(\Gamma)$. By Lemma 3.47 there exists $g' \in G^*$ such that for every $u \in V$ the function $\sigma_f(g', u)$ is equal to h. The composition $g \circ g'^{-1}$ is the identity on S, thus by Lemma 3.46 for any given $v, w \in V$ both $\sigma_f(g, v) \circ h^{-1}$ and $\sigma_f(g, w) \circ h^{-1}$ are elements of $\mathcal{N}$. By Lemma 3.42 we obtain that $\sigma_f(g, v) \circ \sigma_f(g, w)^{-1} = (\sigma_f(g, v) \circ h) \circ (\sigma_f(g, w) \circ h)^{-1}$ is an element of $\mathcal{N}$. □

We have the following immediate consequence.

Corollary 3.49. *Assume that $G = G^* \circ \mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$. Then $S(\mathcal{N}, \mathcal{H}) = \mathcal{G}^*$.*

Proof. The inclusion $S(\mathcal{N}, \mathcal{H}) \leq \mathcal{G}^*$ follows from Lemma 3.48 and the definition of $S(\mathcal{N}, \mathcal{H})$. For the other inclusion let g be an element of

$S(\mathcal{N},\mathcal{H})$. We show that for any finite subset F of V there exists $g' \in \mathcal{G}^*$ such that $g|_F = g'|_F$. Since $\mathcal{G}^*$ is closed this will be enough.

Let F be a finite subset of V. For some $n \geq 1$ we fix a subset $M = \{v_1, \dots, v_n\}$ of $F \setminus \{\mathbf{0}\}$ such that $[M]_\sim \supseteq F \setminus \{\mathbf{0}\}$ and for all distinct $i, j \leq n$ we have $[v_i]_\sim \neq [v_j]_\sim$. By the Definition 3.44 we have $\sigma_f(g, v_1) \in H$, thus there exists $\tilde{g} \in G^*$ such that $\sigma_f(\tilde{g}, v_1) = \sigma_f(g, v_1)$. By Lemma 3.48 we have for all $i \leq n$ that $\sigma_f(\tilde{g}, v_1) \circ \sigma_f(\tilde{g}, v_i)^{-1} \in N$. Since $g \in S(\mathcal{N},\mathcal{H})$ for all $i \leq n$ we have $\sigma_f(g, v_i) \circ \sigma_f(g, v_1)^{-1}$. By $\sigma_f(g, v_1) = \sigma_f(\tilde{g}, v_1)$ we obtain for all $i \leq n$ that $\sigma_f(g, v_i) \circ \sigma_f(\tilde{g}, v_i)^{-1} \in N$. This implies for every $i \leq n$ the existence of $g_i \in G^*$ such that

$$\sigma_f(g_i, v_i) = \sigma_f(g, v_i) \circ \sigma_f(\tilde{g}, v_i)^{-1} \text{ and } g_i|_{V \setminus [v_i]_\sim} = \mathrm{id}_{V \setminus [v_i]_\sim}.$$

We set $g' := (g_2 \circ g_3 \circ \cdots g_n) \circ \tilde{g} \in G^*$ and obtain for all $i \leq n$

$$\sigma_f(g', v_i) = \sigma_f(g, v_i).$$

Thus $g|_F = g'|_F$ which since $\mathcal{G}^*$ is closed concludes the proof. □

We still need to show that in the first case

(1) $G = G^* \circ \mathrm{Aut}(\mathcal{V})$,

we also have $S(\mathcal{N},\mathcal{H}) = \mathcal{G}^*$. For this we need a finite version of Lemma 3.46.

Lemma 3.50. *There exists $N_G \geq 0$ such that for any subspace $U \leq \mathcal{V}$ with $\dim U \geq N_G$, for any $g \in G^*$ and for any $v \in U \setminus \{\mathbf{0}\}$ the following holds:*

$$(\forall w \in U \setminus ([v]_\sim \cup \{\mathbf{0}\}) : \sigma_f(g, w) \in N) \implies \sigma_f(g, v) \in N.$$

Proof. We aim for a contradiction. Assume that the statement does not hold. Then there exist subspaces $(U_i)_{i\geq 0}$ of finite dimension such that $(\dim U_i)_{i \geq 0}$ is strictly increasing, non-zero vectors $(v_i)_{i\geq 0}$ such that $v_i \in U_i$ and functions $(g_i)_{i \geq 0}$ in $\mathcal{G}^*$ such that for all $i \geq 0$ we have

$$\forall w \in U_i \setminus ([v_i]_\sim \cup \{\mathbf{0}\}) : \sigma_f(g_i, w) \in N \text{ and } \sigma_f(g_i, v_i) \notin N.$$

Without loss of generality we assume that for all $i \geq 0$ we have $f(v_i) = 1$. By (15) and the fact that $\mathrm{Aut}(\mathcal{V})$ acts transitively on subspaces of a fixed dimension we may further assume that for all $i, j \geq 0$ we have $v_i = v_j =: v$ as well as

$$U_0 \subseteq U_1 \subseteq \cdots \text{ and } \bigcup_{i \geq 0} U_i = V.$$

By Lemma 3.45 for every $i \geq 0$ there exists $g_i' \in G^*$ such that $\sigma_f(g_i', v) = \sigma_f(g_i, v)$ and $g_i'|_{V \setminus [v_i]_\sim} = \mathrm{id}\,|_{V \setminus [v_i]_\sim}$. Since $\sigma_f(g_i', v)$ is always an element of $\mathrm{Sym}(\Gamma)$, which is finite, we are able to restrict ourselves to a subsequence of $(g'_i)_{i\geq 0}$ and $(U_i)_{i\geq 0}$ such that for all $i,j\geq 0$ we have $\sigma_f(g'_i,v)=\sigma_f(g'_j,v)=:\sigma$. Since $\mathcal{G}^*$ is closed, there exists $g'\in G^*$ such that $\sigma_f(g',v)=\sigma$ and $g'|_{V\setminus[v]_\sim}=\mathrm{id}_{V\setminus[v]_\sim}$. This implies $\sigma\in N$ which is a contradiction and concludes our proof. □

For our proof of Lemma 3.51 we need the following slight variation of Lemma 3.50 with two vectors: there exists $N'_G\geq 0$ such that for all subspaces $U\leq\mathcal{V}$ with $\dim U\geq N'_G$ and all $v,w\in U\setminus\{\mathbf{0}\}$ we have

$$(\forall u\in U\setminus[\{v,w,\mathbf{0}\}]_\sim:\sigma_f(g,u)\in N)\implies\sigma_f(g,v),\sigma_f(g,w)\in N.$$

If we assume $G=G^*\circ\mathrm{Aut}(\mathcal{V})$ this follows directly from Lemma 3.50. Since in this case $[v]_\sim=\langle v\rangle\setminus\{\mathbf{0}\}$, thus if $[v]_\sim\neq[w]_\sim$, then v,w are linearly independent. For $[v]_\sim=[w]_\sim$ the statement coincides with the one of Lemma 3.50. Otherwise, if N'_G is big enough we can always restrict to a subspace $W\leq\mathcal{V}$ contained in $U\setminus[w]_\sim$ such that $\dim W\geq N_G$ and such that $v\in W$. This implies $\sigma_f(g,v)\in N$ and subsequently $\sigma_f(g,w)\in N$.

We want to show if $G=G^*\circ\mathrm{Aut}(\mathcal{V})$, then for all $g\in G^*$ and all $v,w\in V\setminus\{\mathbf{0}\}$ the group $\mathcal{N}$ contains $\sigma_f(g,v)\circ\sigma_f(g,w)^{-1}$. Striving for a contradiction we will assume that there exists $g\in G^*$ and $v,w\in V\setminus\{\mathbf{0}\}$ such that this is not the case. First we show that there exists some $g'\in G^*$ with the same property such that a certain set of commutators are contained in N. We will then use those commutators to derive a contradiction.

Lemma 3.51. *Let U be a subspace of $\mathcal{V}$ of finite dimension $\dim U>N'_G$. Assume that $G=G^*\circ\mathrm{Aut}(\mathcal{V})$. If there exist a function $g\in G^*$ and $v,w\in U\setminus\{\mathbf{0}\}$ such that*

$$\sigma_f(g,v)\circ\sigma_f(g,w)^{-1}\notin N,$$

then there exist $g'\in G^*$ and $v',w'\in U$ such that $\sigma_f(g',v')\circ\sigma_f(g',w')^{-1}\notin N$ and for all $x,y\in U\setminus\{\mathbf{0}\}$ we have

$$\sigma_f(g',x)\circ\sigma_f(g',y)\circ\sigma_f(g',x)^{-1}\circ\sigma_f(g',y)^{-1}\in N. \tag{16}$$

Proof. For any $h\in G^*$ we define a subset $W(h)$ of U by

$$W(h):=\{v\in U:\sigma_f(h,v)\in N\}. \tag{17}$$

Clearly $[W(h)]_\sim=W(h)$. Since $G=G^*\circ\mathrm{Aut}(\mathcal{V})$ the variation of Lemma 3.50 we mentioned holds, thus whenever for any two vectors $v,w\in U$ we have $U\setminus[\{v,w\}]_\sim\subseteq W(h)$ then already $W(h)=U$.

Let $h\in G^*$ be such that

$$\exists v,w\in U\text{ such that }\sigma_f(h,v)\circ\sigma_f(h,w)^{-1}\notin N \tag{18}$$

and $|W(h)|$ is maximal under all functions in G^* satisfying (18).

We want to show that $W(h)$ contains at least one element. Let, as in the statement, a function $g \in G^*$ and $v, w \in U$ be given such that $\sigma_f(g,v) \circ \sigma_f(g,w)^{-1} \notin N$. Then there exists an automorphism $\varphi \in \operatorname{Aut}(\mathcal{V})$ such that $v^\varphi = w$ and φ fixes an arbitrary vector $u \in U$. The function $\varphi \circ g \circ \varphi^{-1} \circ g^{-1}$ is an element of $\mathcal{G}^*$ and

$$\sigma_f(\varphi g \varphi^{-1} g^{-1}, v) = \sigma_f(g,v) \circ \sigma_f(g,w)^{-1} \notin N.$$

therefore $\varphi \circ g \circ \varphi^{-1} \circ g^{-1}$ satisfies (18). On the other hand

$$\sigma_f(\varphi g \varphi^{-1} g^{-1}, u) = \sigma_f(g,u) \circ \sigma_f(g,u)^{-1} = \mathrm{id}_\Gamma \in N,$$

thus $|W(\varphi g \varphi^{-1} g^{-1})| \geq 1$. Because of maximality $|W(h)| \geq 1$.

First we note that if for any $x \in U$ we have $\sigma_f(h,x) \in N$, then by $\mathcal{N} \lhd \mathcal{H}$ we obtain for all $y \in V \setminus \{\mathbf{0}\}$

$$\underbrace{\sigma_f(h,x)}_{\in N} \circ \underbrace{\sigma_f(h,y) \circ \overbrace{\sigma_f(h,x)^{-1}}^{\in N} \circ \sigma_f(h,y)^{-1}}_{\in N} \quad \in N.$$

This shows that for all $x, y \in U$, if

$$\sigma_f(h,x) \circ \sigma_f(h,y) \circ \sigma_f(h,x)^{-1} \circ \sigma_f(h,y)^{-1} \notin N,$$

then neither $\sigma_f(g,x)$ nor $\sigma_f(g,y)$ is an element of $\mathcal{N}$.

We have to show that the chosen h satisfies (16) for all $x, y \in U \setminus \{\mathbf{0}\}$. Striving for a contradiction we assume that there are vectors such that (16) does not hold. By Lemma 3.50 and by what we noted we may fix three non-equivalent elements x, y, z such that (16) does not hold. By what we just noted, x, y, z are not elements of $W(h)$. Without loss of generality let $f(x) = f(y) = f(z)$. We construct a function h' satisfying (18) such that $W(h) \subsetneq W(h')$ which contradicts the maximality of h.

There exists $\gamma \in \operatorname{Aut}(\mathcal{V})$ such that $y^\gamma = x$ and $z^\gamma = w$ for some arbitrary fixed $w \in W(h) \neq \emptyset$. We define $g' := \gamma \circ h \circ \gamma^{-1} \in G^*$ and obtain

$$\sigma_f(g',y) = \sigma_f(h,x) \text{ and } \sigma_f(g',z) = \sigma_f(\gamma h \gamma^{-1}, z) = \sigma_f(h,w) \in N.$$

Furthermore, we define $h' := h \circ g' \circ h^{-1} \circ g'^{-1} \in G^*$ and show that h' satisfies (18). Since $\mathcal{N} \lhd \mathcal{H}$ we obtain for z

$$\sigma_f(h',z) = \underbrace{\sigma_f(h,z) \circ \sigma_f(h,w) \circ \sigma_f(h,z)^{-1}}_{\in N} \circ \underbrace{\sigma_f(h,w)^{-1}}_{\in N} \in N. \tag{19}$$

The elements x, y are such that

$$\sigma_f(h',y) = \sigma_f(h,y) \circ \sigma_f(h,x) \circ \sigma_f(h,y)^{-1} \circ \sigma_f(h,x)^{-1} \notin N.$$

Because $\sigma_f(h',z)$ is an element of $\mathcal{N}$ we have $\sigma_f(h',y) \circ \sigma_f(h',z)^{-1} \notin N$, hence h' satisfies (18).

For all $v \in W(h)$ by $\mathcal{N} \lhd \mathcal{H}$ we have

$$\sigma(h', v) = \underbrace{\sigma_f(h, v)}_{\in N} \circ \sigma_f(g', v) \circ \underbrace{\sigma_f(h, v)^{-1}}_{\in N} \circ \sigma_f(g', v)^{-1} \in N.$$

We already saw in (19) that $z \in W(h') \setminus W(h)$, hence $W(h) \subsetneq W(h')$. This contradicts the maximality of h. Therefore for h all $x, y \in U$ satisfy (16). □

Since $\mathcal{N} \lhd \mathcal{H}$ we obtain under the assumptions of Lemma 3.51 that for any $k \geq 2$ and all $x_1, \dots, x_k \in U$ we have

$$\sigma_f(g', x_1) \circ \dots \circ \sigma_f(g', x_k) \circ \sigma_f(g', x_1)^{-1} \circ \dots \circ \sigma_f(g', x_k)^{-1} \in N.$$

Consequently for any $x_1, \dots, x_k \in U$ and any $\{i_1, \dots, i_k\} = \{1, \dots, k\}$ there exists $n \in N$ such that

$$n \circ (\sigma_f(g', x_{i_1}) \circ \dots \circ \sigma_f(g', x_{i_k})) = \sigma_f(g', x_1) \circ \dots \circ \sigma_f(g', x_k). \tag{20}$$

In the proof of Lemma 3.54 we will obtain a Γ-labelling which might differ from our fixed Γ-labelling. Lemma 3.52 shows that this is in fact not a problem.

Lemma 3.52. *Let f_1 and f_2 be Γ-labellings. Then for all $g \in \mathrm{Sym}^*(V)$, all $v \in V \setminus \{\mathbf{0}\}$ and $\lambda := \frac{f_2(v)}{f_1(v)}$ we have*

$$\sigma_{f_2}(g, v) = \lambda^{-1} \circ \sigma_{f_1}(g, v) \circ \lambda. \tag{21}$$

Proof. We claim that for all $w \in [v]_\sim$ we have $f_2(w) = \lambda f_1(w)$. This is true since there exists $\mu \in \Gamma^\times$ such that $\mu v = w$ and

$$f_2(w) = \frac{f_2(w)}{f_1(w)} f_1(w) = \frac{f_2(\mu v)}{f_1(\mu v)} f_1(w) = \frac{\mu f_2(v)}{\mu f_1(v)} f_1(w) = \lambda f_1(w).$$

Let $w \in [v]_\sim$ be such that $f_2(w) = 1$, then $f_1(\lambda w) = 1$. Now for any $\mu \in \Gamma$ we have $\sigma_{f_2}(g, v)(\mu) = f_2((\mu v)^g)$ and

$$\begin{aligned}\sigma_{f_1}(g, v)(\mu) &= f_1((\mu(\lambda w))^g) = \lambda^{-1} f_2(((\lambda\mu)w)^g) \\ &= \lambda^{-1}\sigma_{f_2}(g, v)(\lambda\mu) = (\lambda \circ \sigma_{f_2}(g, v) \circ \lambda^{-1})(\mu).\end{aligned}$$

□

For the proof of Lemma 3.54 we need for every n-dimensional subspace U of $\mathcal{V}$ an element in $\mathrm{Aut}(U)$ of order $p^n - 1$, a so called *singer cycle*. Such an ele

ment always exists since we may identify U with $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^n}^\times$ is cyclic and therefore generated by a single element, which then has to have order $p^n - 1$. Since the multiplication by a field element generates an automorphism this shows that there exists an automorphisms of U of order $p^n - 1$. This argument is taken from [3, p.5].

Euler's Phi function $\varphi\colon \mathbb{N} \to \mathbb{N}$ assigns to every $n \in \mathbb{N}$ the number of positive integers $k \leq n$ which are coprime to n, *coprime* meaning that k and n do not share a common divisor in $\mathbb{N}$ besides 1.

Theorem 3.53 (Euler's Theorem)**.** *Let $\varphi\colon \mathbb{N} \to \mathbb{N}$ be Euler's Phi function. Then for all $n, q \geq 1$ which are coprime $q^{\varphi(n)} - 1$ divides n.*

For a proof of Euler's Theorem see Theorem 11 in [4].

Lemma 3.54. *Let g be an element of $\mathcal{G}^*$. Assume that $G = G^* \circ \mathrm{Aut}(\mathcal{V})$. Then for all $v, w \in V \setminus \{\mathbf{0}\}$ the function $\sigma_f(g, v) \circ \sigma_f(g, w)^{-1}$ is an element of $\mathcal{N}$.*

Proof. We strive for a contradiction. Assume that there exists $g \in G^*$ and $\bar{u}, \hat{u} \in V \setminus \{\mathbf{0}\}$ such that $\sigma_f(g, \bar{u}) \circ \sigma_f(g, \hat{u})^{-1} \notin N$. Without loss of generality let $\bar{u}$ and $\hat{u}$ be such that their f-labels are 1. Let n be some natural number greater that N'_G from Lemma 3.50 which we will specify later.

Let U be an $n+1$-dimensional subspace of $\mathcal{V}$ which contains $\{\bar{u}, \hat{u}\}$ and let A' be an n-dimensional affine subspace of U which also contains $\{\bar{u}, \hat{u}\}$ but does not contain $\{\mathbf{0}\}$. We set $U' := A - \bar{u} = A - \hat{u}$ a subspace of $\mathcal{V}$ contained in U. Since A does not contain $\mathbf{0}$ the set A is linearly independent, thus there exists a Γ-labelling which is constant on A. By Lemma 3.52 since $\lambda \in H$ and $\mathcal{N} \lhd \mathcal{H}$ for any $\lambda \in \mathbb{F}_p$ we may assume that f already coincides with this Γ-labelling. Moreover by Lemma 3.51 we may assume that $\sigma_f(g, \bar{u}) \circ \sigma_f(g, \hat{u})^{-1} \notin N$ and for all $x, y \in U$ we have

$$\sigma_f(g, x) \circ \sigma_f(g, y) \circ \sigma_f(g, x)^{-1} \circ \sigma_f(g, y)^{-1} \in N. \tag{22}$$

There exists $\gamma \in \mathrm{Aut}(U')$ of order $p^n - 1$ such that for any $u \in U' \setminus \{\mathbf{0}\}$

$$\{u^{\gamma^i} : 1 \leq i \leq p^n - 1\} = U' \setminus \{\mathbf{0}\}. \tag{23}$$

Let $\bar{\gamma}$ and $\hat{\gamma}$ in $\mathrm{Aut}(\mathcal{V})$ be extensions of γ such that $\bar{u}^{\bar{\gamma}} = \bar{u}$ and $\hat{u}^{\hat{\gamma}} = \hat{u}$. The set $U' = \bar{\gamma}(U')$ is equal to $\bar{\gamma}(A - \bar{u}) = \bar{\gamma}(A) - \bar{u}$, thus $\bar{\gamma}(A) = A$. By similar reasoning $\hat{\gamma}(A) = A$. We define for all $i \leq p^n - 2$ the functions

$$\bar{g}_i := \bar{\gamma}^i \circ g \circ \bar{\gamma}^{-i} \text{ and } \hat{g}_i := \hat{\gamma}^i \circ g \circ \hat{\gamma}^{-i}.$$

For any $a \in A$ and all $i \leq p^n - 2$ we obtain $\sigma_f(\bar{g}_i, a) = \sigma_f(g, a^{\bar{\gamma}^i})$ and $\sigma_f(\hat{g}_i, a) = \sigma_f(g, a^{\hat{\gamma}^i})$. We further define

$$\bar{h} := \bar{g} \circ \bar{g}_1 \circ \bar{g}_2 \circ \cdots \circ \bar{g}_{p^n-2} \text{ and } \hat{h} := \hat{g} \circ \hat{g}_1 \circ \hat{g}_2 \circ \cdots \circ \hat{g}_{p^n-2}.$$

Because of (23) we obtain for all $a \in A \setminus \{\bar{u}\}$:

$$\{a^{\bar{\gamma}^i} : 0 \leq i \leq p^n - 2\} = A \setminus \{\bar{u}\},$$

and likewise for all $a \in A\setminus\{\hat{u}\}$ we have $\{a^{\hat{\gamma}^i} : 0 \leq i \leq p^n-2\} = A\setminus\{\hat{u}\}$.

We enumerate A such that $A = \{u_i : 1 \leq i \leq p^n - 1\}$ and $\hat{u} = u_1$ as well as $\bar{u} = u_2$. We now fix $n > N'_G$ such that n is a multiple of $\varphi((p-1)!)$. By Euler's Theorem we obtain that $(p-1)!$ divides $p^{\varphi((p-1)!)} - 1$ which implies that $(p-1)!$ divides $p^n - 1$. The function $\sigma_f(\bar{h}, \bar{u})$ is equal to $\sigma_f(g, \bar{u})^{p^n-1}$. Together we obtain $\sigma_f(\bar{h}, \bar{u}) = \mathrm{id}_{\mathbb{F}_p^\times}$.

For all $a \in A \setminus \{\bar{u}\}$ we arrive at

$$\sigma_f(\bar{h}, a) = \sigma_f(g, u_{k_1}) \circ \cdots \circ \sigma_f(g, u_{k_{p^n-2}})$$

such that $\{u_{k_i} : 1 \leq i \leq p^n - 2\} = A \setminus \{\bar{u}\}$. By Lemma 3.51 and by what we remarked in (20) we obtain that for every $a \in A \setminus \{\bar{u}\}$ there exists $n_a \in N$ such that

$$n_a \circ \sigma_f(\bar{h}, a) = (\sigma_f(g, u_1) \circ \cdots \circ \sigma_f(g, u_{p^n-2})) \circ \sigma_f(g, \bar{u})^{-1} =: \bar{\sigma}.$$

Likewise we define $\hat{\sigma} := (\sigma_f(g, u_1) \circ \cdots \circ \sigma_f(g, u_{p^n-2})) \circ \sigma_f(g, \hat{u})^{-1}$. With this $\bar{\sigma}^{-1} \circ \hat{\sigma} = \sigma_f(g, \hat{u}) \circ \sigma_f(g, \bar{u})^{-1}$ which is by assumption not an element of $\mathcal{N}$. This implies that either $\bar{\sigma}$ or $\hat{\sigma}$ is not an element of $\mathcal{N}$. Without loss of generality let $\bar{\sigma} \notin N$. Let $\psi \in \mathrm{Aut}(\mathcal{V})$ be a function which fixes every element in $U' \setminus [\bar{u}]_\sim$ but not $\bar{u}$. We define $h := \bar{h} \circ \psi \circ \bar{h}^{-1} \circ \psi^{-1} \in G^*$. For all $v \in U' \setminus [\bar{u}]_\sim$ we obtain

$$\begin{aligned}\sigma_f(h, v) &= \sigma_f(\bar{h}, v) \circ \big(\sigma_f(\psi\bar{h}\psi^{-1}, v)\big)^{-1}\\ &= \sigma_f(\bar{h}, v) \circ \sigma_f(\bar{h}, v)^{-1} = \mathrm{id}_\Gamma \in N.\end{aligned}$$

For any $v \in U \setminus (U' \cup [\{\bar{u}, \bar{u}^{\psi^{-1}}\}]_\sim)$ there exists $a \in A \setminus \{\bar{u}, \bar{u}^{\psi^{-1}}\}$ such that $\langle a \rangle = \langle v \rangle$. We obtain

$$\begin{aligned}\sigma_f(h, v) &= \sigma_f(\bar{h}, a) \circ \big(\sigma_f(\psi\bar{h}\psi^{-1}, a)\big)^{-1}\\ &= \sigma_f(\bar{h}, a) \circ \sigma_f(\bar{h}, a^\psi)^{-1} = (n_a \circ \bar{\sigma}) \circ (n_{a^\psi} \circ \bar{\sigma})^{-1}\\ &= n_a \circ n_{a^\psi} \in N.\end{aligned}$$

Therefore for all elements $v \in U \setminus [\{\bar{u}, \bar{u}^{\psi^{-1}}\}]_\sim$ we have $\sigma_f(h, v) \in N$, hence by Lemma 3.50 also $\sigma_f(h, \bar{u}) \in N$. But

$$\begin{aligned}\sigma_f(h, \bar{u}) &= \sigma_f(\bar{h}, \bar{u}) \circ \big(\sigma_f(\psi\bar{h}\psi^{-1}, \bar{u})\big)^{-1}\\ &= \sigma_f(\bar{h}, \bar{u}^\psi)^{-1} = (n_{\bar{u}^{\psi^{-1}}} \circ \bar{\sigma})^{-1}\end{aligned}$$

The second to last equality follows since $\sigma_f(\bar{h}, \bar{u}) = \mathrm{id}_\Gamma$. This contradicts $\bar{\sigma} \notin N$ and therefore concludes the proof. □

Corollary 3.55. *Assume that $G = G^* \circ \mathrm{Aut}(\mathcal{V})$. Then $S(\mathcal{N}, \mathcal{H}) = \mathcal{G}^*$.*

Proof. The proof is identical to the one of Corollary 3.49 only using Lemma 3.54 instead of Lemma 3.48. □

We showed that for every closed group $\mathcal{G}$ such that

$$\mathrm{Aut}(\mathcal{V}) \leq \mathcal{G} \leq \mathrm{Sym}(V)_{\mathbf{0}}$$

the corresponding group $\mathcal{G}^*$ is equal to $S(\mathcal{N}, \mathcal{H})$ from Definition 3.44, thus $\mathcal{G}^*$ is uniquely determined by its corresponding groups $\mathcal{N} \lhd \mathcal{H} \leq \mathrm{Sym}(\Gamma)$ from Definition 3.39. Since there are only finitely many possibilities for $\mathcal{N}$ and $\mathcal{H}$ as subgroups of $\mathrm{Sym}(\Gamma)$ we have shown the following.

Theorem 3.56. *Let $\mathcal{V}$ be a countably infinite dimensional vector space over a finite prime field of uneven characteristic. Then there are only finitely many first-order reducts of $\mathcal{V}$ which first-order define the zero vector.*

4. The closed supergroups of $\mathrm{Aut}(\mathcal{V})$ not fixing $\mathbf{0}$

We are still considering the countably infinite dimensional vector space $\mathcal{V}$ over a finite field $\mathbb{F}_p$ of characteristic $p > 2$. Theorem 3.56 showed that there exist only finitely many reducts of $\mathcal{V}$ which do first-order define the zero vector. The goal for this section is to show that there are only two reducts of $\mathcal{V}$ which do not first-order define $\mathbf{0}$. To this end we are interested in the supergroups of $\mathrm{Aut}(\mathcal{V})$ which shift the zero vector. Therefore, for the rest of the chapter let $\mathcal{G}$ be a closed permutation group on V such that

$$\mathrm{Aut}(\mathcal{V}) \leq \mathcal{G} \leq \mathrm{Sym}(V) \text{ and } \exists g \in G : g(\mathbf{0}) \neq \mathbf{0}\,.$$

If we restrict ourselves to the subgroup $\mathcal{G}_{\mathbf{0}}$ of $\mathcal{G}$ we may apply all results of the previous sections. With this in mind we consider the equivalence relation $\sim$ given by $\mathcal{G}_{\mathbf{0}}$ as before together with $\Gamma \leq \mathbb{F}_p^\times$ as defined before.

The group $\mathrm{Aut}(\mathcal{V})$ acts transitively on $V \setminus \{\mathbf{0}\}$. Since $\mathbf{0}$ is not fixed by $\mathcal{G}$ we immediately obtain that $\mathcal{G}$ acts transitively on V.

The first observation we make is that in this case Γ may only be one of the two trivial subgroups of $\mathbb{F}_p^\times$.

Lemma 4.1. *The group $\Gamma \leq \mathbb{F}_p^\times$ satisfies $\Gamma = \{1\}$ or $\Gamma = \mathbb{F}_p^\times$.*

Proof. We assume that $\Gamma \neq \{1\}$ and show that the only other possibility is $\Gamma = \mathbb{F}_p^\times$. Let g be a function of $\mathcal{G}$ such that $v := \mathbf{0}^g \neq \mathbf{0}$. Since $\Gamma \neq \{1\}$ there exists some element $\hat{v} \in [v]_\sim$ different from v. We set $\hat{w} := \hat{v}^{g^{-1}}$. The zero vector is an element of $g^{-1}([v]_\sim)$, thus there exists at least one element $w \sim \hat{w}$ such that $w^g \not\sim \hat{w}^g$. We make a case distinction.

Case 1: $w^g \neq \mathbf{0}$: Let h be a function of $\mathcal{G}_{\mathbf{0}}$ such that h fixes v and $(w^g)^h \in V \setminus \langle v \rangle^g$. Since h preserves $\sim$ and $\hat{v} \sim v$ the element $\hat{v}^h$ is contained in $[v]_\sim \subseteq \langle v \rangle$. We obtain

$$\begin{pmatrix} \mathbf{0} \\ \hat{w} \\ w \end{pmatrix} \overset{g}{\mapsto} \begin{pmatrix} v \\ \hat{v} \\ w^g \end{pmatrix} \overset{h}{\mapsto} \begin{pmatrix} v \\ \hat{v}^h \\ w^{gh} \end{pmatrix} \overset{g^{-1}}{\mapsto} \begin{pmatrix} \mathbf{0} \\ \hat{v}^{hg^{-1}} \\ \hat{w}^{ghg^{-1}} \end{pmatrix}.$$

Since $\hat{w}^{gh} \notin \langle v \rangle^g$ we have $\hat{w}^{ghg^{-1}} \not\sim \hat{v}^{hg^{-1}}$ but $\hat{w} \sim w$ and $g \circ h \circ g^{-1} \in G_{\mathbf{0}}$ which is a contradiction.

Case 2: The only possible element $w \sim \hat{w}$ such that $w^g \not\sim v$ is mapped to $\mathbf{0}$ by g and there exist $u \sim \hat{u} \in V \setminus [w]_\sim$ such that $u^g \not\sim \hat{u}^g$.

By mapping v to either u or u' and since w is the only element in $[\hat{w}]_\sim$ such that $w^g \not\sim v$ we may assume without loss of generality that v and

$\hat{v}$ are such that there exists a vector space automorphism φ mapping v to u and $\hat{v}$ to $\hat{u}$. We obtain

$$\begin{pmatrix} \mathbf{0} \\ \hat{w} \\ w \end{pmatrix} \overset{g}{\mapsto} \begin{pmatrix} v \\ \hat{v} \\ \mathbf{0} \end{pmatrix} \overset{\varphi}{\mapsto} \begin{pmatrix} u \\ \hat{u} \\ \mathbf{0} \end{pmatrix} \overset{g}{\mapsto} \begin{pmatrix} u^g \\ \hat{u}^g \\ v \end{pmatrix}.$$

Now $w \sim \hat{w}$ and $\hat{u}^g \not\sim v \neq \mathbf{0}$, hence the composition $g \circ \varphi \circ g$ satisfies the condition for our first case.

Case 3: The only possible element $w \sim \hat{w}$ such that $w^g \not\sim v$ is mapped to $\mathbf{0}$ by g and for all distinct $u \sim \hat{u} \in V \setminus [w]_\sim$ we have $u^g \not\sim \hat{u}^g$.

Let $u, \hat{u}$ be elements like in the case assumption. By Theorem 3.12 and Theorem 3.13 the group $\mathcal{G}_\mathbf{0}$ acts either as the full symmetric group or in the same way as $\mathrm{Aut}(\mathcal{V})$ on the equivalence classes $(V\setminus\{\mathbf{0}\})/_\sim$. We assume that $\mathcal{G}_\mathbf{0}$ acts full symmetric group on $(V \setminus \{\mathbf{0}\})/_\sim$. Then there exists $h \in G_\mathbf{0}$ such that $v^h = v$ and $(u^g)^h \in [u^g]_\sim$ and $(\hat{u}^g)^h \in V \setminus [u^g]^g_\sim$. We obtain

$$\begin{pmatrix} \mathbf{0} \\ u \\ \hat{u} \end{pmatrix} \overset{g}{\mapsto} \begin{pmatrix} v \\ u^g \\ \hat{u}^g \end{pmatrix} \overset{h}{\mapsto} \begin{pmatrix} v \\ u^{gh} \\ \hat{u}^{gh} \end{pmatrix} \overset{g^{-1}}{\mapsto} \begin{pmatrix} \mathbf{0} \\ u^{ghg^{-1}} \\ \hat{u}^{ghg^{-1}} \end{pmatrix}.$$

Now $g \circ h \circ g^{-1} \in G_\mathbf{0}$ but $u^{ghg^{-1}} \not\sim \hat{u}^{ghg^{-1}}$. Therefore $\mathcal{G}_\mathbf{0}$ cannot act on $(V \setminus \{\mathbf{0}\})/_\sim$ as the full symmetric group, consequently the only possibility for Γ is to be equal to $\mathbb{F}_p^\times$. □

Theorem 4.2. *Assume that* $\Gamma = \{1\}$. *Then* $\mathcal{G} = \mathrm{Sym}(V)$.

Proof. By Theorem 3.13 the group $\mathcal{G}_\mathbf{0}$ acts as $\mathrm{Sym}((V/_\sim))_\mathbf{0}$ on the equivalence classes $(V/_\sim)$. The equivalence classes consist only of one element and there exists $g \in G$ such that $g(\mathbf{0}) \neq \mathbf{0}$. □

From now on we assume

$$\Gamma = \mathbb{F}_p^\times.$$

Definition 4.3. Let S be a set and let $\mathcal{H}$ be a permutation group on S. For all $\tilde{S} \subseteq S$ the *algebraic closure of* $\tilde{S}$ is defined as the union of all finite orbits of $H_{\tilde{S}}$ on S. We denote this set is by $\mathrm{acl}(\tilde{S})$.

As for the linear closure, for finitely many elements $v_1, \ldots, v_n \in V$ we are going to write $\mathrm{acl}(v_1, \ldots, v_n)$ instead of $\mathrm{acl}(\{v_1, \ldots, v_n\})$.

If S is a set, $\mathcal{H} \leq \mathrm{Sym}(S)$, and $\simeq$ is an equivalence relation on S which is $\mathcal{H}$-invariant, then for all finite equivalence classes $[a]_\simeq \subseteq S$ and all $b \in [a]_\simeq$ we have $b \in \mathrm{acl}(a)$. Clearly $\tilde{S} \subseteq \mathrm{acl}(\tilde{S})$ for any $\tilde{S}$.

In our case the set S is the set of vectors V and the group $\mathcal{H}$ is $\mathcal{G}$. Furthermore $\operatorname{Aut}(\mathcal{V}) \leq \mathcal{G}$ and for all $v, w \in V$ and all $u \in V \setminus \langle v, w\rangle$ the orbit $\operatorname{Aut}(\mathcal{V})_{v,w}(u)$ is already V, thus infinite. The orbit $G_{v,w}(v)$ contains only v and $G_{v,w}(w) = \{w\}$, thus

$$\{v, w\} \subseteq \operatorname{acl}(v, w) \subseteq \langle v, w\rangle\,. \tag{24}$$

By what we argued about finite equivalence classes of an equivalence relation we have for all $w \in V$ that

$$w \sim v \implies w \in \operatorname{acl}(\mathbf{0}, v).$$

Together with (24) and since $\Gamma = \mathbb{F}_p^\times$ we obtain the following.

Lemma 4.4. *Let v be a vector in V. Then*

$$\operatorname{acl}(\mathbf{0}, v) = \langle v\rangle\,. \tag{25}$$

For arbitrary vectors $v, w \in V$ the structure of $\operatorname{acl}(v, w)$ is a little more complex to determine. For all $u \in V$, if there is a function in $\mathcal{G}_{v,w}$ which maps u to a vector outside of $\langle v, w\rangle$ then u cannot be in $\operatorname{acl}(v, w)$. On the other hand, if the orbit $G_{v,w}(u)$ is fully contained in $\langle v, w\rangle$, then it is finite and u is an element of the algebraic closure. Therefore

$$\operatorname{acl}(v, w) = \{u \in V : G_{v,w}(u) \subseteq \langle v, w\rangle\}. \tag{26}$$

Since $\mathcal{G}$ acts transitively on V we are able to map any pair of vectors to a pair which contains $\mathbf{0}$. From this we obtain the following.

Lemma 4.5. *Let v, w be distinct vectors in V and let $g \in G$. Then*

(1) $\operatorname{acl}(v, w)^g = \operatorname{acl}(v^g, w^g)$, *and*
(2) $|\operatorname{acl}(v, w)| = p$.

Proof. Clearly for all $u \in V$ we have

$$|G_{v,w}(u)| = \infty \iff |G_{v^g,w^g}(u^g)| = \infty.$$

This shows (1). Item (2) follows from (1) and Lemma 4.4. □

Lemma 4.6. *Let v, w be distinct vectors in V. For all distinct elements x, y of* $\operatorname{acl}(v, w)$*, we have*

$$\operatorname{acl}(v, w) = \operatorname{acl}(x, y).$$

Proof. We claim that it suffices to show this in the case that $v = \mathbf{0}$. Let u be a non-zero vector and $g \in G$ such that $(v, w)^g = (\mathbf{0}, u)$. Assume we know that for all distinct $a, b \in \operatorname{acl}(\mathbf{0}, u)$ we have

$$\operatorname{acl}(\mathbf{0}, u) = \operatorname{acl}(a, b).$$

For all distinct elements $x, y \in \mathrm{acl}(v, w)$ the elements x^g, y^g are in $\mathrm{acl}(\mathbf{0}, u)$, thus by our assumption and (1) of Lemma 4.5:

$$\mathrm{acl}(x, y)^g = \mathrm{acl}(x^g, y^g) = \mathrm{acl}(\mathbf{0}, u) = \mathrm{acl}(v, w)^g.$$

Therefore without loss of generality $v = \mathbf{0}$.

Now for any $x, y \in \mathrm{acl}(\mathbf{0}, w) = \langle w \rangle$, we have $\mathrm{acl}(x, y) \subseteq \langle x, y \rangle = \langle w \rangle$. By (2) of Lemma 4.5 we obtain equality. □

Together with (1) of Lemma 4.5 we obtain the following.

Corollary 4.7. *Let $v, w \in V$ distinct and let $g \in G$ be a function such that $v^g, w^g \in \mathrm{acl}(v, w)$. Then $\mathrm{acl}(v, w)^g = \mathrm{acl}(v, w)$.*

Lemma 4.8. *Let v, w be distinct vectors in V. If $\mathbf{0} \notin \mathrm{acl}(v, w)$, then every pair (x, y) of distinct elements of $\mathrm{acl}(v, w)$ is linearly independent.*

Proof. If x, y were distinct linearly dependent elements in $\mathrm{acl}(v, w)$, then by Lemma 4.6 and Lemma 4.4 we would obtain $\mathrm{acl}(v, w) = \mathrm{acl}(x, y) = \langle x \rangle$. □

Lemma 4.9. *Let $v, w \in V$ be two vectors which are linearly independent. For all distinct $x, y \in \mathrm{acl}(v, w)$ and all distinct $\lambda, \mu \in \mathbb{F}_p$ we have, if $\lambda v + \mu w \in \mathrm{acl}(v, w)$, then $\lambda x + \mu y \in \mathrm{acl}(v, w)$.*

Proof. Let $x, y \in \mathrm{acl}(v, w)$ be distinct and $\lambda, \mu \in \mathbb{F}_p$ such that $\lambda v + \mu w \in \mathrm{acl}(v, w)$ be given. The set $\{x, y\}$ is linearly independent.Therefore, there exists $\varphi \in \mathrm{Aut}(\mathcal{V})$ such that $v^\varphi = x$ and $w^\varphi = y$. By Corollary 4.7 the set $\mathrm{acl}(v, w)^\varphi$ is $\mathrm{acl}(v, w)$. The automorphisms of $\mathcal{V}$ respect linear combinations, hence $(\lambda v + \mu w)^\varphi = \lambda x + \mu y$ is an element of $\mathrm{acl}(v, w)$. □

Lemma 4.10. *Let v, w be two vectors in V. Then the algebraic closure $\mathrm{acl}(v, w)$ is the affine line $\mathrm{Aff}(v, w)$.*

Proof. If $\{v, w\}$ is linearly dependent, then since $|\mathrm{acl}(v, w)| = p$ and $\mathrm{acl}(v, w) \subseteq \langle v, w \rangle = \langle v \rangle$, we have $\mathrm{acl}(v, w) = \langle v \rangle = \mathrm{Aff}(v, w)$.

We assume that $\{v, w\}$ is linearly independent and define the set I as set of all tuples $(\lambda, \mu) \in \mathbb{F}_p^2$ such that there exist distinct $x, y \in \mathrm{acl}(v, w)$ for which we have: $\lambda x + \mu y \in \mathrm{acl}(v, w)$.

Because of Lemma 4.9 for all $(\lambda, \mu) \in \mathbb{F}_p^2$ the existence of distinct elements $x, y \in \mathrm{acl}(v, w)$ such that $\lambda x + \mu y \in \mathrm{acl}(v, w)$ is equivalent to all distinct elements $x, y \in \mathrm{acl}(v, w)$ fulfilling $\lambda x + \mu y \in \mathrm{acl}(v, w)$.

If $(\lambda, \mu) \in I$, then $\frac{1}{\lambda}(\lambda v + \mu w) - \frac{\mu}{\lambda} w = v$ and since all three $(\lambda v + \mu w), v, w$ are elements of $\mathrm{acl}(v, w)$ we obtain

$$\forall (\lambda, \mu) \in I, \lambda \neq 0 \implies \left(\frac{1}{\lambda}, -\frac{\mu}{\lambda} \right) \in I. \tag{27}$$

Furthermore for all $(\lambda,\mu)\in I$ such that $\lambda\neq 0$, the element $(\frac{1}{\lambda}v-\frac{\mu}{\lambda}w)+\mu v$ is contained in $\operatorname{acl}(v,w)$ and equal to $v-\mu w+\mu v=(1+\mu)v-\mu w$. Thus

$$\forall(\lambda,\mu)\in I,\lambda\neq 0 \implies (1+\mu,-\mu)\in I. \tag{28}$$

If $1+\mu\neq 0$ by (28) we obtain $(\mu,1-\mu)\in I$.

Claim: For all $\mu\in\mathbb{F}_p$ if $(\mu,0)\in I$, then $\mu=1$.

This is clear since $(1,0)\in I$ and two non-equivalent elements cannot lie in $\operatorname{acl}(v,w)$.

Claim: For all $\lambda\in\mathbb{F}_p$ if $(1,\lambda)\in I$, then $\lambda=0$.

We assume otherwise, i.e., $\lambda\neq 0$. By (27) we obtain

$$\left(\frac{1}{\lambda},-\frac{1}{\lambda}\right),\ (1,-\lambda)\in I.$$

Therefore

$$\operatorname{acl}(v,w)\ \ni\ \frac{1}{\lambda}\underbrace{(v+\lambda w)}_{\in\ \operatorname{acl}(v,w)}-\frac{1}{\lambda}\underbrace{(v-\lambda w)}_{\in\ \operatorname{acl}(v,w)}=2v.$$

Which cannot be since $\operatorname{acl}(v,w)$ contains only pairwise non-equivalent elements and $2v\sim v$.

Claim: For all $(\lambda,\mu)\in I$ if $\lambda\neq 0$, then $\lambda=1-\mu$.

If $\lambda\neq 0$, then $\mu v+(1-\mu)w,\ v\in\operatorname{acl}(v,w)$ and

$$1\cdot(\mu v+(1-\mu)w)+(\lambda-(1-\mu))w=\mu v+\lambda w\in\operatorname{acl}(v,w)$$

Thus $(1,\lambda-(1-\mu))\in I$ and by our second claim $\lambda=1-\mu$.

Our three claims show that $\operatorname{acl}(v,w)\subseteq\operatorname{Aff}(v,w)$, both have cardinality p hence equality holds.

□

We nowhere needed the fact that $\mathbb{F}_p$ is a prime field, hence Lemma 4.10 also holds in the more general setting of a non-prime field. Lemma 4.5 (1) and Lemma 4.10 immediately show the following.

Corollary 4.11. *$\mathcal{G}$ preserves affine lines, i.e., maps affine lines to affine lines.*

We denote for every $v\in V$ the translation which maps any $w\in V$ to $w+v$ by τ_v.

We recall Definition 3.4 which states that a bijective function $f\colon \mathrm{S}_1(\mathcal{V})\to\mathrm{S}_1(\mathcal{V})$ preserves projective lines iff for all $L_0,L_1,L_2\in\mathrm{S}_1(\mathcal{V})$ we have

$$L_0\subseteq L_1+L_2 \iff L_0^f\subseteq L_1^f+L_2^f. \tag{29}$$

For all $v, w \in V$ and $L_1, L_2 \in \mathrm{S}_1(\mathcal{V})$ two affine lines $v + L_1$ and $w + L_2$ are said to be *parallel* iff $L_1 = L_2$. For a more general definition of parallelity, see [5, p.146].

Theorem 4.12. *Let g be an element of $\mathcal{G}$. Then there exists $\varphi \in \mathrm{Aut}(\mathcal{V})$ such that $g = \varphi \circ \tau_{g(\mathbf{0})}$.*

Proof. For all $u, v, w \in V$ we have that $\mathrm{Aff}(v, w)^{\tau_u} = \mathrm{Aff}(v^{\tau_u}, w^{\tau_u})$. By Corollary 4.11 the same holds for $g \circ \tau_{-g(\mathbf{0})} =: \tilde{g}$. Since $\tilde{g}$ is an element of $\mathcal{G}_{\mathbf{0}}$ it acts on $\mathrm{S}_1(\mathcal{V})$.

Claim: The action of $\tilde{g}$ on $\mathrm{S}_1(\mathcal{V})$ preserves projective lines.

Let three arbitrary vectors $u, v, w \in V$ be given. We want to show that (29) holds for $L_0 = \langle u \rangle, L_1 = \langle v \rangle$ and $L_2 = \langle w \rangle$. Assume that $\langle u \rangle \subseteq \langle v \rangle + \langle w \rangle$. For any $x \in \langle u \rangle$ there are $v_x \in \langle v \rangle$ and $w_x \in \langle w \rangle$ such that $x \in \mathrm{Aff}(v_x, w_x)$. We obtain $x^{\tilde{g}} \in \mathrm{Aff}(v_x^{\tilde{g}}, w_x^{\tilde{g}}) \subseteq \left\langle v^{\tilde{g}} \right\rangle + \left\langle w^{\tilde{g}} \right\rangle$. By repeating the same argument for $\tilde{g}^{-1}$ this shows (29).

By Theorem 3.7 there exists $\varphi \in \mathrm{Aut}(\mathcal{V})$ such that the actions of φ and $\tilde{g}$ on $\mathrm{S}_1(\mathcal{V})$ coincide. We set $h := \tilde{g} \circ \varphi^{-1}$ which acts as the identity on $\mathrm{S}_1(\mathcal{V})$. Our goal is to show that $h = c \cdot \mathrm{id}_V$ for some $c \in \mathbb{F}_p^\times$.

Since for any $\lambda \in \mathbb{F}_p^\times$ the function $x \mapsto \lambda x^\varphi$ is again an automorphism of $\mathcal{V}$ and has the same action on $\mathrm{S}_1(\mathcal{V})$ as φ we may assume without loss of generality that there exists at least one $v \in V$ such that $h(v) = v$.

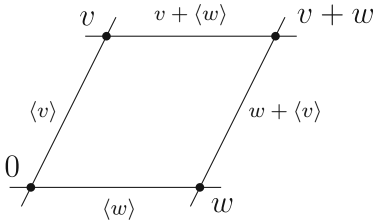
Claim: For all $u, w \in V$ the function h maps the affine line $w + \langle u \rangle = \mathrm{Aff}(u + w, w)$ to the affine line $w^h + \langle u \rangle$ parallel to $\langle u \rangle$.

Since h preserves projective lines we have that $h(\langle u, w \rangle) = \langle u, w \rangle$. Additionally we have $\mathrm{Aff}(u + w, w)^h = \mathrm{Aff}((u + w)^h, w^h)$, therefore $h(w + \langle u \rangle) = w^h + \langle u + \lambda w \rangle$ for some $\lambda \in \mathbb{F}_p$. The function h is bijective and $w + \langle v \rangle \cap \langle u \rangle = \emptyset$, hence $w^h + \langle u + \lambda w \rangle \cap \langle u \rangle$ is empty too. Since $w^h \in \langle w \rangle$ it follows that $\lambda = 0$, showing our claim.

We are now in position to finish our proof. Let $w \in V \setminus \langle v \rangle$ be given. Then $\{v + w\} = v + \langle w \rangle \cap w + \langle v \rangle$, thus

$$\{h(v + w)\} = h(v + \langle w \rangle) \cap h(w + \langle v \rangle).$$

Since $h(v + w) \in \langle v + w \rangle$ we obtain $h(v + w) = \lambda v + \lambda w$ for some $\lambda \in \mathbb{F}_p$. By our last claim $h(v + \langle w \rangle) = v + \langle w \rangle$ and $h(w + \langle v \rangle) = w^h + \langle v \rangle$, thus $\lambda = 1$ and in further consequence $w^h = w$.



This implies that $h = \mathrm{id}_V$. Therefore $g \circ \tau_{-g(\mathbf{0})} = \varphi$.

$\square$

Note that in the proof of Theorem 4.12 we never used the structure of the underlying field of $\mathcal{V}$, hence the statement holds for arbitrary underlying fields.

By Theorem 6.3.3. of [5, p.153] every affine mapping in $\mathrm{A\Gamma L}(\mathcal{V})$ is a composition of a translation and a vector space automorphism. With this, Theorem 4.12 is a variant of the Fundamental Theorem of Affine Geometry which states that a bijective function which preserves affine lines is a semi-affine function with regards to some field automorphism, see e.g. [2, p.52]. As we have seen, this holds for a countably infinite dimensional vector space. It does not hold for dimensions smaller than 2; again [2] gives a counterexample in the beginning of Chapter 2.6.

Since $\mathrm{Aut}(\mathbb{F}_p)$ contains only the identity we have $\mathrm{A\Gamma L}(\mathcal{V}) = \mathrm{AGL}(\mathcal{V})$. Theorem 4.12 shows that $\mathcal{G} \leq \mathrm{A\Gamma L}(\mathcal{V}) = \mathrm{AGL}(\mathcal{V})$. We now show the other inclusion.

Lemma 4.13. *$\mathcal{G}$ is equal to the group of all affine mappings from V to V.*

Proof. By Theorem 4.12 we have $\mathcal{G} \leq \mathrm{AGL}(\mathcal{V})$. Since $\mathcal{G}$ does not fix $\mathbf{0}$ there exists an element which is the composition of a vector space automorphism and a translation. Since $\mathrm{Aut}(\mathcal{V}) \leq \mathcal{G}$ there exists at least one $v \in V \setminus \{\mathbf{0}\}$ such that $\tau_v \in G$.

Let $u \in V \setminus \{\mathbf{0}\}$ be an arbitrary vector. There exists $\varphi \in \mathrm{Aut}(\mathcal{V}) \leq \mathcal{G}$ which maps u to v. For any $w \in V$ we have

$$w^{\varphi^{-1}\tau_v\varphi} = (w^{\varphi^{-1}})^{\tau_v\varphi} = (w^{\varphi^{-1}} + v)^{\varphi} = w + u,$$

hence $\varphi^{-1} \circ \tau_v \circ \varphi = \tau_u \in G$.

Since $\mathcal{G}$ contains all automorphisms of $\mathcal{V}$ and all translations, by Theorem 6.3.3 [5, p.153] we have $\mathcal{G} = \mathrm{AGL}(\mathcal{V})$. $\square$

We define a relation $R \subseteq V^4$ by

$$(a, b, c, d) \in R :\iff a + b = c + d.$$

The structure (V, R) is clearly a reduct of $\mathcal{V}$. Every translation and every automorphism of $\mathcal{V}$ preserves R, hence by Theorem 6.3.3. [5, p.153] we have $\mathrm{AGL}(\mathcal{V}) \leq \mathrm{Aut}((V, R))$. By what we showed, the only other possibility for the automorphisms of (V, R) would be $\mathrm{Sym}(V)$, but not all functions in $\mathrm{Sym}(V)$ preserve R, hence $\mathrm{Aut}((V, R)) = \mathrm{AGL}(\mathcal{V})$.

We obtain the following.

Theorem 4.14. *Assume that a closed permutation group $\mathcal{G}$ on V containing $\operatorname{Aut}(\mathcal{V})$ does not fix zero. Then one of the following holds.*

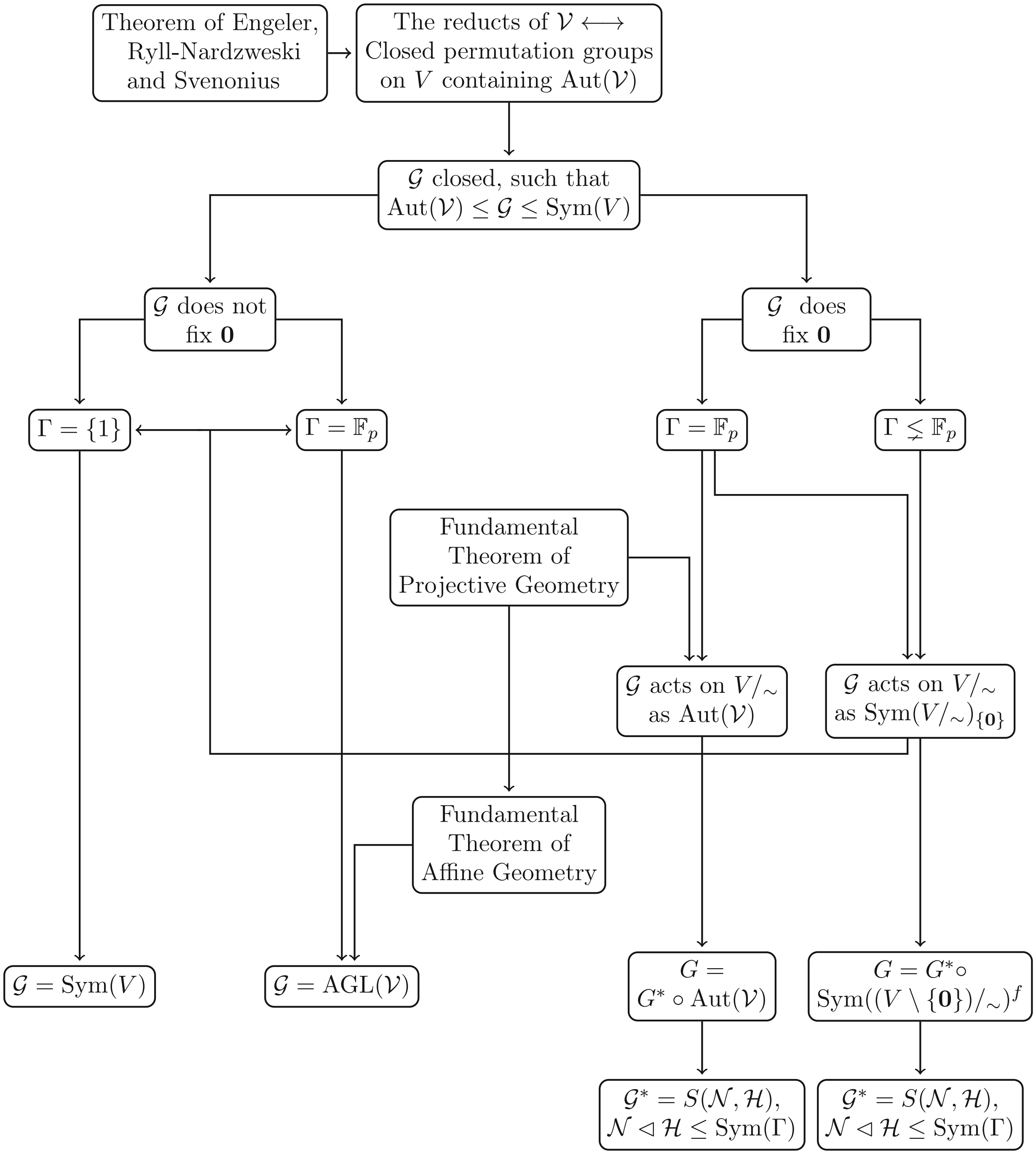
(1) $\mathcal{G} = \operatorname{Sym}(V)$, *or*
(2) $\mathcal{G} = \operatorname{AGL}(\mathcal{V})$.

In particular there are, up to interdefinability, two first-order reducts of $\mathcal{V}$ which do not first-order define $\mathbf{0}$*:*

- *The pure set with domain V and no operations or relations.*
- *The structure* (V, R) *containing no operations.*

Together with Theorem 3.56, Theorem 4.14 shows that every countably infinite vector space over a finite prime field of odd characteristic has, up to interdefinability, only finitely many first-order reducts.

Summarising we obtain the following picture.


Theorem of Engeler, Ryll-Nardzweski and Svenonius
The reducts of $\mathcal{V}$ $\longleftrightarrow$ Closed permutation groups on V containing $\mathrm{Aut}(\mathcal{V})$
$\mathcal{G}$ closed, such that $\mathrm{Aut}(\mathcal{V}) \leq \mathcal{G} \leq \mathrm{Sym}(V)$
$\mathcal{G}$ does not fix $\mathbf{0}$
$\mathcal{G}$ does fix $\mathbf{0}$
$\Gamma = \{1\}$
$\Gamma = \mathbb{F}_p$
$\Gamma = \mathbb{F}_p$
$\Gamma \lneq \mathbb{F}_p$
Fundamental Theorem of Projective Geometry
$\mathcal{G}$ acts on $V/_\sim$ as $\mathrm{Aut}(\mathcal{V})$
$\mathcal{G}$ acts on $V/_\sim$ as $\mathrm{Sym}(V/_\sim)_{\{\mathbf{0}\}}$
Fundamental Theorem of Affine Geometry
$\mathcal{G} = \mathrm{Sym}(V)$
$\mathcal{G} = \mathrm{AGL}(\mathcal{V})$
$G = G^* \circ \mathrm{Aut}(\mathcal{V})$
$G = G^* \circ \mathrm{Sym}((V \setminus \{\mathbf{0}\})/_\sim)^f$
$\mathcal{G}^* = S(\mathcal{N}, \mathcal{H})$, $\mathcal{N} \lhd \mathcal{H} \leq \mathrm{Sym}(\Gamma)$
$\mathcal{G}^* = S(\mathcal{N}, \mathcal{H})$, $\mathcal{N} \lhd \mathcal{H} \leq \mathrm{Sym}(\Gamma)$

References

[1] Emil Artin. *Geometric algebra*. John Wiley & Sons, Inc., New York, 1988.

[2] Marcel Berger. *Geometry I*. Springer-Verlag, Berlin, 2009.

[3] Tom Brookfield. *Overgroups of a linear Singercycle in classical groups*. 2014.

[4] Leonhard Euler. *Theoremata arithmetica nova methodo demonstrata*. 1. 1763, pp. 74–104.

[5] Hans Havlicek. *Lineare Algebra für technische Mathematiker*. Heldermann Verlag, Berlin, 2006.

[6] Wilfrid Hodges. *A shorter model theory*. Cambridge University Press, Cambridge, 1997.

[7] Thomas W. Hungerford. *Algebra*. Springer-Verlag, New York-Berlin, 1980.

[8] Serge Lang. *Algebra*. third. Graduate Texts in Mathematics. Springer-Verlag, New York, 2002.