

# MATROIDS OVER ONE-DIMENSIONAL GROUPS

GUUS P. BOLLEN, DUSTIN CARTWRIGHT, AND JAN DRAISMA

ABSTRACT. We develop the theory of matroids over one-dimensional algebraic groups, with special emphasis on positive characteristic. In particular, we compute the Lindström valuations and Frobenius flocks of such matroids. Building on work by Evans and Hrushovski, we show that the class of algebraic matroids, paired with their Lindström valuations, is not closed under duality of valuated matroids.

## 1. INTRODUCTION

Given an algebraically closed field  $K$  and a natural number  $n$ , any irreducible subvariety  $X \subseteq K^n$  gives rise to a matroid  $M(X)$  on the ground set  $[n] := \{1, \dots, n\}$  by declaring  $I \subseteq [n]$  to be independent if the coordinate projection  $X \rightarrow K^I$  is dominant, i.e., has dense image. The variety  $X$  is an *algebraic representation* of  $M(X)$  and  $M(X)$  is called an *algebraic matroid*. For an equivalent, but more algebraic interpretation, one considers the field  $K(X)$  of rational functions on  $X$ , and calls  $I$  independent if the coordinates  $x_i$ ,  $i \in I$  map to elements of  $K(X)$  that are algebraically independent over  $K$ . For an introduction to algebraic matroids we refer to [RST19].

The best-understood algebraic matroids are *linear matroids*, which are those coming from linear subvarieties  $X \subseteq K^n$ . However, the class of algebraic matroids is larger than just linear matroids. For example, in the first paper to study algebraic representability of matroids, Ingleton gave an algebraic representation of the non-Fano matroid, over any field, using a variety  $X \subseteq K^7$  parametrized by monomials [Ing71, Ex. 15], which we would now call a toric variety, the Zariski closure of a connected algebraic subgroup of  $(K^*)^n$ —a subtorus. More generally, such parametrizations can be used to show that any linear matroid over  $\mathbb{Q}$  is algebraic over any field. This construction is reviewed in Example 1.4.

In fact, linear spaces and subtori are examples of connected subgroups of  $G^n$ , where  $G$  is an arbitrary connected, one-dimensional algebraic group over  $K$ . The possibilities for  $G$  are the additive group  $\mathbb{G}_a = (K, +)$ , the multiplicative group  $\mathbb{G}_m = (K^*, \cdot)$ , and any elliptic curve over  $K$ . The purpose of this paper is to develop a unified theory for the algebraic matroids arising from such subgroups. In this theory, the linear parametrization of a linear space and the monomial parametrization of a subtorus are replaced by any homomorphism of algebraic groups  $\Psi : G^d \rightarrow G^n$  with image  $X$ , a closed and connected subgroup of  $G^n$ . The homomorphism  $\Psi$  is described by an  $n \times d$  matrix with elements in the ring  $\mathbb{E}$  of endomorphisms of the group  $G$ . For instance, with  $G = (K^*, \cdot)$  we have  $\mathbb{E} \cong \mathbb{Z}$  via the isomorphism  $\mathbb{Z} \ni a \mapsto (t \mapsto t^a)$ , and the rows of the matrix record the exponent vectors in the monomial parametrization  $\Psi$ . If  $K$  has characteristic zero, then the endomorphism  $\mathbb{E}$  is commutative for any connected, one-dimensional algebraic group  $G$  over  $K$ . But if  $K$  has positive characteristic, then  $\mathbb{E}$  can be non-commutative; see §2.2 for

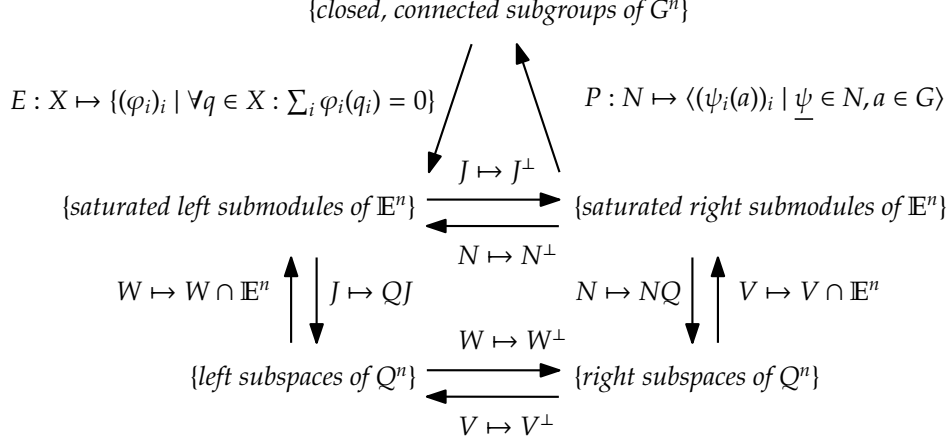


FIGURE 1. The diagram of Theorem 1.1.

details. These non-commutative rings give examples of non-linear matroids which are algebraic over all fields of positive characteristic [Lin86a].

All of our results are formulated uniformly over the three different types of algebraic groups, and only in the proofs do we sometimes distinguish between them.

For all one-dimensional groups  $G$ ,  $\mathbb{E}$  is both a left and right Ore domain, so it is contained in a division ring  $Q$  (generated by  $\mathbb{E}$ ), and the algebraic matroid represented by  $X$  has a linear representation over  $Q$ . Here, we write  $M(X)$  for the matroid whose bases are all sets  $I \subseteq [n]$  such that the projection of  $X$  to  $G^I$  is all of  $G^I$ . This matroid is equivalent to the algebraic matroid defined in the first paragraph because, if we choose a non-constant rational function  $h: G \dashrightarrow K$  and let  $Y \subset K^n$  be the coordinatewise image  $h^n(X)$ , then  $M(X) = M(Y)$ .

**Theorem 1.1.** *Let  $G$  be a connected, one-dimensional algebraic group over an algebraically closed field  $K$ . Then the maps in Figure 1 are bijections and the diagram commutes. Furthermore, for a closed, connected subgroup  $X \subseteq G^n$  the set  $M(X)$  is a matroid and coincides with the linear matroid on  $[n]$  defined by the right vector space  $P^{-1}(X)Q \subset Q^n$ .*

The map  $P$  in Figure 1 sends  $N$  to the subgroup of  $G^n$  generated by the elements of the form  $(\psi_i(a))_i$  with  $a \in G$  and  $\underline{\psi}$  running through  $N$ . We think of the right modules  $N$  and  $V$  as giving *parametrizations* of  $X$  and of the left modules  $J$  and  $W$  as giving *equations* for  $X$ , whence the notation  $E$  and  $P$ . The ring  $\mathbb{E}$  is left and right Noetherian, so a right module  $N \subseteq \mathbb{E}^n$  has a finite generating set. Use these vectors as the columns of an  $n \times d$ -matrix  $\Psi$ . Then  $\Psi$  gives a natural group homomorphism  $G^d \rightarrow G^n$ ;  $P(N)$  is the image of this homomorphism. A different choice of generators yields a different matrix  $\Psi$  with the same column space and a different homomorphism  $G^d \rightarrow G^n$  with the same image.

We note that our use of the column space of an  $n \times m$  matrix  $\Psi$ , in order to define a matroid on the ground set  $[n]$ , differs from the conventional use of row spaces in matroid theory, which define matroids on the set of columns. However, in our construction of  $\Psi$ , it is the rows which are labeled by  $[n]$ , because  $\Psi$  is a matrix defining a group homomorphism to  $G^n$ . Since  $\mathbb{E}$  is possibly non-commutative, the

column space of  $\Psi$  is not equivalent to the row space of its transpose, and so we use the column space to define our matroids consistently.

Because of Theorem 1.1, we call the matroids isomorphic to  $M(X)$  for some closed, connected  $X \subseteq G^n$   $\mathbb{E}$ -linear. An  $\mathbb{E}$ -linear matroid  $M$  admits an algebraic representation in the sense of the first paragraph of this paper: choosing a non-constant rational function  $h : G \dashrightarrow K$  defined near  $0 \in G$  we obtain a rational map  $h^n : G^n \dashrightarrow K^n$ , and the variety  $Y := \overline{h^n(X)} \subseteq K^n$  has  $M(Y) = M$ .

**Theorem 1.2.** *The class of  $\mathbb{E}$ -linear matroids is closed under contraction, deletion, and duality.*

**Example 1.3.** Let  $G = \mathbb{G}_a$  be the additive group over  $K = \overline{\mathbb{F}_2}$ . Then  $\mathbb{E}$  is isomorphic to the skew polynomial ring  $K[F]$  in which multiplication is governed by the rule  $Fa = a^2F$ . The (right) column space  $N$  of the matrix

$$\Psi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & F \end{pmatrix},$$

is saturated in  $K[F]^4$ , and  $P(N) = \{(a, b, a + b, a + b^2) \mid (a, b) \in \mathbb{G}_a^2\}$ . The matroid  $M(P(N))$  is the uniform matroid  $U_{2,4}$ . ♣

**Example 1.4.** Let  $G = \mathbb{G}_m$  be the multiplicative group over  $K$ . Then  $\mathbb{E} \cong \mathbb{Z}$  via the map  $\mathbb{Z} \rightarrow \mathbb{E}, a \mapsto (t \mapsto t^a)$ . Any matrix  $\Psi \in \mathbb{Z}^{n \times d}$  of full rank  $d$  gives rise to an algebraic group homomorphism  $\Psi : \mathbb{G}_m^d \rightarrow \mathbb{G}_m^n, t = (t_1, \dots, t_d) \mapsto (t_1^{\psi_{11}} \dots t_d^{\psi_{1d}})_{i=1}^n$  whose image  $X$  is a  $d$ -dimensional subtorus of the  $n$ -dimensional torus  $\mathbb{G}_m^n$ . The matroid  $M(X)$  is equal to the linear matroid over  $\mathbb{Q}$  in which  $I \subseteq [n]$  is an independent set if and only if the corresponding rows of  $\Psi$  are linearly independent.

This classical argument shows that matroids linear over  $\mathbb{Q}$  are algebraic over any field. The group homomorphism  $\Psi : \mathbb{G}_m^d \rightarrow \mathbb{G}_m^n$  is a closed embedding if and only if the  $\mathbb{Z}$ -column space of  $\Psi$  is a saturated submodule of  $\mathbb{Z}^n$ . Our framework is a common generalization of linear matroids and these toric matroids. ♣

**Positive characteristic.** In characteristic zero, by Ingleton's theorem [Ing71], the class of matroids that admit an  $\mathbb{E}$ -linear representation is the same as the class of matroids that admit a  $K$ -linear representation. Therefore, we next specialize to characteristic  $p > 0$ , and we study  $\mathbb{E}$ -linear matroids from the perspective of the theory developed in [BDP18, Car18]. There, for any irreducible variety  $Y \subseteq K^n$ , a canonical matroid valuation on  $M(Y)$  is constructed, called the *Lindström valuation*. Furthermore, in [BDP18], a so-called *Frobenius flock* is associated to the pair consisting of  $Y$  and a sufficiently general point of  $Y$ . Here, in § 4.5, we will define the Frobenius flock of a closed, connected subgroup  $X \subseteq G^n$ , use it to define the Lindström valuation on  $M(X)$ , and relate these definitions to the constructions of [BDP18] via a rational function  $G \dashrightarrow K$  as above. The goal is, then, to express these invariants of  $X$  in the data of Theorem 1.1.

To this end, we proceed as follows. In § 4.1 we construct a canonical valuation  $v : \mathbb{E} \rightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}$  such that  $v(a) > 0$  if and only if  $\alpha : G \rightarrow G$  is an inseparable morphism. A routine check shows that  $v$  extends to  $Q$ . Then, in § 3.1, we describe a general construction of a  $K$ -linear flock from a right vector subspace  $V \subset Q^n$ , and of a compatible valuation on the linear matroid on  $[n]$  determined by  $V$ . These are

related to the Frobenius flock and the Lindström valuation of  $X$  and to [BDP18] as follows.

**Theorem 1.5.** *Let  $X$  be a closed, connected subgroup of  $G^n$  and let  $N = P^{-1}(X)$  be the saturated right submodule of  $\mathbb{E}^n$  representing  $X$ . Then the Frobenius flock of  $X$  equals the linear flock of  $NQ$ , and the Lindström valuation of  $X$  equals the matroid valuation corresponding to  $NQ$ . Furthermore, let  $h : G \dashrightarrow K$  be a rational function defined near 0 and set  $Y := \overline{h^n(X)}$ . Under mild conditions on  $h$ , the point  $h^n(0) \in Y$  satisfies the genericity condition (\*) from [BDP18], and  $d_0 h^n$  restricts to a linear bijection between the Frobenius flock of  $X$  and the Frobenius flock of  $(Y, 0)$ .*

The mild conditions in this theorem are specified in Equation (\*\*) in § 4.6.

By Theorem 1.2, the algebraic matroids arising from groups are closed under duality. However, the method used to prove this duality does not dualize the Lindström valuation in the sense of [DW92, Proposition 1.4]. On the contrary, using results from [EH91], we prove:

**Theorem 1.6.** *The class of algebraic matroids equipped with their Lindström valuations is not closed under duality of valuated matroids. In particular, if  $K$  has positive characteristic, then there exists a closed, connected subgroup  $X \subset \mathbb{G}_a^n$ , with algebraic matroid  $M$  and Lindström valuation  $w$ , such that the dual valuated matroid  $(M^*, w^*)$  is not the algebraic matroid and Lindström valuation of any variety  $Y \subset K^n$ .*

To be clear, the dual matroid  $M^*$  from Theorem 1.6 is algebraic—indeed, this follows from Theorem 1.2—but the Lindström valuation of any realization of  $M^*$  is distinct from  $w^*$ .

**Relation to existing literature.** As noted, the use of endomorphisms of  $\mathbb{G}_m$  appears as an example in [Ing71]. The systematic use of endomorphisms of  $\mathbb{G}_a$  (dubbed *p-polynomials*) in matroid theory first appeared in [Lin88], though particular cases were studied in [Lin86a] and [Lin86b], which used *p*-polynomials to show that the non-Pappus matroid is algebraic over any field of positive characteristic. The first uniform treatment of endomorphism rings of all possible one-dimensional algebraic groups is in [EH91], which used model theory to show that each algebraic representation of certain matroids would have to be algebraically equivalent to an  $\mathbb{E}$ -linear representation for some one-dimensional algebraic group  $G$  with endomorphism ring  $\mathbb{E}$ .

There is no logical dependence between our work and the recent literature on matroids over tracts and hyperfields [BB19], although algebraic realizations of matroids in positive characteristic do yield matroids over natural *non-commutative* hyperfields [Pen18].

Modules over rings with a valuation feature both here and in [FM19], but there is no immediate connection between our results and theirs. Indeed, there, the input data consists of a finitely presented module over  $R$  for each subset of a ground set, subject to certain axioms that enhance properties of the rank function of an ordinary matroid; while here, a single submodule of  $\mathbb{E}^n$  represents a matroid over an algebraic group with endomorphism ring  $\mathbb{E}$ .

The rows of our matrix  $\Psi$  representing a parametrization  $G^d \rightarrow X \subseteq G^n$  give homomorphisms  $G^d \rightarrow G$ , and their kernels define a collection of codimension-one subgroups of  $G^d$ . There is currently much research activity on such (central) *Abelian arrangements*, especially in the case where the ground field is  $\mathbb{C}$

and the topology of the complement is studied via combinatorial techniques [DP05, DM13, DD18, DP19]. While the questions here are somewhat orthogonal to our focus, the progression from hyperplane arrangements to toric arrangements to elliptic arrangements mirrors the observation that toric varieties provide non-linear algebraic matroids, followed by the generalization to elliptic curves. However, our interest is primarily in characteristic- $p$  phenomena, and especially the non-commutative endomorphism rings that arise there.

**Organization.** The remainder is organized as follows. In Section 2 we recall basic facts about one-dimensional algebraic groups  $G$ , their endomorphism rings  $\mathbb{E}$ , and submodules of  $\mathbb{E}^n$ ; and we prove Theorems 1.1 and 1.2. In Section 4, we zoom in on characteristic  $p$  and establish Theorem 1.5. Finally, in Section 6 we give several examples of  $\mathbb{E}$ -linear matroids with  $G$  equal to  $\mathbb{G}_m$ ,  $\mathbb{G}_a$ , or an elliptic curve and prove Theorem 1.6.

**Acknowledgments.** JD was partially supported by the NWO Vici grant entitled *Stabilisation in Algebra and Geometry*. GPB was supported by the Stichting Computer Algebra Nederland. DC was partially supported by NSA Young Investigator grant H98230-16-1-0019. We thank Aurel Page for his MathOverflow answer at <https://mathoverflow.net/questions/309320>, which helped with the last case of Lemma 4.4. Work on this paper started at the Institut Mittag-Leffler during their program “Tropical Geometry, Amoebas, and Polyhedra”; we thank the institute and its staff for fantastic working conditions.

## 2. ARBITRARY CHARACTERISTIC

**2.1. One-dimensional algebraic groups.** Let  $G$  be a one-dimensional algebraic group over the algebraically closed field  $K$ . Thus,  $G$  is either the multiplicative group  $\mathbb{G}_m = (K^*, \cdot)$ , the additive group  $\mathbb{G}_a = (K, +)$ , or an elliptic curve (for a classification of the affine one-dimensional groups see [Bor91, Theorem III.10.9]; Hurwitz’ automorphism theorem rules out that the genus of  $G$  is strictly greater than 1). In particular,  $G$  is Abelian. We write the operation in  $G$  additively in the uniform treatment of these cases.

**2.2. The endomorphism ring.** The set  $\mathbb{E} := \text{End}(G)$  of endomorphisms of  $G$  as an algebraic group is a ring with operations  $\cdot = \circ$  (composition) as multiplication and  $(\varphi + \psi)(g) := \varphi(g) + \psi(g)$  as addition; for  $\varphi + \psi$  to be an endomorphism, the fact that  $G$  is Abelian is crucial.

If  $G = \mathbb{G}_m$ , then  $\mathbb{E} \cong \mathbb{Z}$  via the map  $\mathbb{Z} \rightarrow \mathbb{E}$ ,  $a \mapsto (t \mapsto t^a)$ . If  $G = \mathbb{G}_a$  and  $\text{char } K = 0$ , then  $\mathbb{E} \cong K$  via the map  $K \rightarrow \mathbb{E}$ ,  $c \mapsto (d \mapsto cd)$ . For  $G = \mathbb{G}_a$  in positive characteristic,  $\mathbb{E}$  is the skew polynomial ring  $K[F]$  whose elements are polynomials in  $F$  and multiplication is governed by the rule  $Fa = a^p F$  for all  $a \in K$ , because  $a \in K$  acts by scaling  $\mathbb{G}_a$  and  $F$  acts as the Frobenius operator. If  $G$  is an elliptic curve, then  $\mathbb{E}$  is either the ring of integers, an order in an imaginary quadratic number field, or an order in a quaternion algebra (only in positive characteristic) [Sil09, Theorem V.3.1]. For any one-dimensional group  $G$ , its endomorphism ring  $\mathbb{E}$  embeds into a division ring  $Q$  (generated by  $\mathbb{E}$ ):  $Q$  is either a number field, or a quaternion algebra, or  $K$  itself, or the division ring  $K(F)$  of the ring of  $p$ -polynomials constructed in [Lin88].

**Example 2.1.** Consider the elliptic curve  $G$  over  $\overline{\mathbb{F}}_2$  in the projective plane whose equation in the affine  $(x, y)$ -chart is  $y^2 + y = x^3 + x + 1$ . The Abelian group structure on  $G$  is uniquely determined by requiring that the point  $O := (0 : 1 : 0)$  is the neutral element and requiring that the intersection points with  $G$  of any line in the projective plane add up to  $O$ . The ring  $\mathbb{E}$  is isomorphic to the ring of *Hurwitz quaternions*: those quaternions  $a + bi + cj + dk$  with either  $a, b, c, d \in \mathbb{Z}$  or else  $a, b, c, d \in 1/2 + \mathbb{Z}$ ; see [Hus04, Chapter 3, §6 and Appendix IV], where explicit endomorphisms are described. Having a non-commutative endomorphism ring, the curve is supersingular.

**2.3. Submodules of  $\mathbb{E}^n$ .** Since  $\mathbb{E}$  is, in general, a non-commutative ring, we distinguish between left submodules  $J$  and right submodules  $N$  of  $\mathbb{E}^n$ . We define  $QJ$  (respectively,  $NQ$ ) to be the left (respectively, right)  $Q$ -subspace of  $Q^n$  generated by  $J$ . Linear algebra over a division ring  $Q$  works very similarly to linear algebra over fields—all modules are free and there are well-defined notions of basis and dimension—and this is why we use “ $Q$ -vector space” rather than “ $Q$ -module”. However, one needs to distinguish between left and right vector spaces, and for instance the dual of a left  $Q$ -vector space  $V$  is naturally a right vector space.

The dimension of  $QJ$  (respectively,  $NQ$ ) is called the *rank*  $\text{rk } J$  (respectively,  $\text{rk } N$ ) of  $J$  (respectively,  $N$ ). We call  $J^{\text{sat}} := QJ \cap \mathbb{E}^n$  and  $N^{\text{sat}} := NQ \cap \mathbb{E}^n$  the *saturations* of  $J$  and  $N$ , and we call  $J$  and  $N$  *saturated* if they are equal to their saturations. These are straightforward generalizations of the familiar notion of saturated lattice in  $\mathbb{Z}^n$ . In particular,  $J$  is saturated if and only if the following holds: if  $\alpha \underline{\varphi} \in J$  for some  $\underline{\varphi} \in \mathbb{E}^n$  and  $\alpha \in \mathbb{E} \setminus \{0\}$ , then  $\underline{\varphi} \in J$ ; and similarly for  $N$ . Furthermore,  $J \mapsto QJ$  and  $N \mapsto NQ$  are bijections between saturated submodules of  $\mathbb{E}^n$  and  $Q$ -subspaces in  $Q^n$ . In particular, if  $J \subseteq J'$  are both saturated and  $\text{rk } J = \text{rk } J'$ , then  $J = J'$ ; and similarly for  $N$ .

**2.4. Orthogonal complements.** We have the natural pairing  $\mathbb{E}^n \times \mathbb{E}^n \rightarrow \mathbb{E}$ :

$$\langle \underline{\varphi}, \underline{\psi} \rangle := \sum_i \varphi_i \psi_i.$$

This pairing is left- $\mathbb{E}$ -linear in the first argument and right- $\mathbb{E}$ -linear in the second argument. The orthogonal complement  $J^\perp$  of a left  $\mathbb{E}$ -submodule  $J \subseteq \mathbb{E}^n$  is:

$$J^\perp = \left\{ \underline{\psi} \mid \forall \underline{\varphi} \in J : \langle \underline{\varphi}, \underline{\psi} \rangle = 0 \right\};$$

it is a saturated right  $\mathbb{E}$ -module whose rank equals  $n - \text{rk } J$ , and similarly for the orthogonal complement of a right submodule  $N$ . The operation  $\perp$  also extends to left or right subspaces of  $Q^n$ .

**2.5. Connected subgroups.**

**Lemma 2.2.** *Let  $X$  be a closed, connected subgroup of  $G^n$  of dimension  $d$ . Then there exist surjective algebraic group homomorphisms  $\alpha: X \rightarrow G^d$  and  $\beta: G^d \rightarrow X$  and a natural number  $e$  such that  $\alpha \circ \beta$  and  $\beta \circ \alpha$  are the multiplication with  $e$  maps on  $G^d$  and  $X$ , respectively. Moreover, if  $G = \mathbb{G}_a$  or  $G = \mathbb{G}_m$ , then  $e$  can be taken equal to 1.*

*Proof.* For  $G = \mathbb{G}_m$ , this follows from [Bor91, Proposition III.8.5]. For  $G = \mathbb{G}_a$  in characteristic zero, a closed, connected subgroup of  $\mathbb{G}_a^n$  is just a linear subspace of  $K^n$ , and the result is basic linear algebra. For  $G = \mathbb{G}_a$  in positive characteristic, the result follows from [CGP10, Lemma B.1.10].

Now assume that  $G$  is an elliptic curve. Then the lemma follows from the fact that isogeny of Abelian varieties is an equivalence relation. We recall some details. Take any maximal subset  $I \subseteq [n]$  such that the projection  $\alpha : X \rightarrow G^I$  is dominant. Since algebraic group homomorphisms have a closed image,  $\alpha$  is surjective. Maximality implies that  $|I| = d$ , so that  $H := \ker \alpha$  is finite. Let  $e > 0$  be the exponent of the finite group  $H$ . Then the multiplication map  $\gamma : X \rightarrow X, x \mapsto ex$  has  $\ker \gamma \supseteq H$ . Therefore  $\gamma$  factors as  $\beta \circ \alpha$  for some algebraic group homomorphism  $\beta : G^I \cong X/H \rightarrow X$ . So  $\beta \circ \alpha$  is multiplication by  $e$ . Conversely, for  $a \in G^I$  there exists an  $x \in X$  such that  $\alpha(x) = a$ , and we find

$$\alpha(\beta(a)) = \alpha(\beta(\alpha(x))) = \alpha(ex) = ea(x) = ea,$$

so also  $\alpha \circ \beta$  is multiplication by  $e$ . Since multiplication by  $e$  is surjective—here we use that  $X$  is connected—both  $\alpha$  and  $\beta$  are surjective.  $\square$

**Remark 2.3.** The proof in the latter paragraph also works in the cases  $G = \mathbb{G}_m$ , except that it does not yield  $e = 1$ . It does not work for  $G = \mathbb{G}_a$ , since the exponent  $e$  of  $H$  in the proof might be  $p$ , so that multiplication with  $e$  is not surjective.

**2.6. Proof of Theorems 1.1 and 1.2.** The following lemmas establish Theorem 1.1.

**Lemma 2.4.** *The maps  $P$  and  $E$  in the diagram are well-defined.*

*Proof.* We begin with  $E$ . Let  $X$  be a closed, connected subgroup of  $G^n$  and define

$$J := E(X) = \{ \underline{\varphi} \in \mathbb{E}^n \mid \forall q \in X : \sum_i \varphi_i(q_i) = 0 \}.$$

A straightforward computation shows that  $J$  is a left  $\mathbb{E}$ -submodule of  $\mathbb{E}^n$ . To show that  $J$  is saturated, suppose that  $\alpha \underline{\varphi} \in J$  with  $\alpha \in \mathbb{E} \setminus \{0\}$  and  $\underline{\varphi} \in \mathbb{E}^n$ . Then for each  $q \in X$ ,  $\underline{\varphi}(q) := \sum_i \varphi_i(q_i)$  is in the kernel of the endomorphism  $\alpha$ . This kernel is a closed subset of the one-dimensional variety  $G$ , and since  $\alpha \neq 0$ , we find that  $\ker \alpha$  is a finite set of points. Since  $X$  is irreducible and since  $\underline{\varphi}$ , regarded as a map  $G^n \rightarrow G$ , is a morphism,  $\underline{\varphi}(X) \subseteq \ker \alpha$  is a single point. This point is 0 since  $\underline{\varphi}(0) = 0$ . Hence  $\underline{\varphi} \in J$ , and  $J$  is saturated as desired.

Next we show that  $P$  is well-defined. Let  $N$  be any right submodule of  $\mathbb{E}^n$  (not necessarily saturated) and let  $\underline{\psi}^{(1)}, \dots, \underline{\psi}^{(m)}$  be a generating set of  $N$ . Write  $\Psi = (\underline{\psi}^{(1)}, \dots, \underline{\psi}^{(m)})$ . We think of  $\Psi$  as an  $n \times m$ -matrix over  $\mathbb{E}$ . It gives rise to the group homomorphism

$$(1) \quad \Psi : G^m \rightarrow G^n, \quad (a_1, \dots, a_m) \mapsto \sum_{j=1}^m \underline{\psi}^{(j)}(a_j),$$

whose image  $X$  is closed, connected subgroup of  $G^n$ . A straightforward computation shows that  $X = P(N)$ .

The two maps at the bottom in the diagram are clearly well-defined if  $J$  is any left  $\mathbb{E}$ -submodule of  $\mathbb{E}^n$ , then  $J^\perp$  is a saturated right-submodule of  $\mathbb{E}^n$ , and vice versa.  $\square$

**Lemma 2.5.** *The maps  $J \mapsto J^\perp$  and  $N \mapsto N^\perp$  (when restricted to saturated modules) are inverse to each other.*

*Proof.* The module  $(J^\perp)^\perp$  is a saturated left  $\mathbb{E}$ -submodule of  $\mathbb{E}^n$  which on the one hand contains  $J$  and on the other hand has the same rank as  $J$ . Hence they are equal. The same argument applies to  $N$ .  $\square$

**Lemma 2.6.** *For any right  $\mathbb{E}$ -submodule  $N$  of  $\mathbb{E}^n$ ,  $P(N) = P(N^{\text{sat}})$ , and  $\dim P(N) = \text{rk } N$ .*

*Proof.* From  $N^{\text{sat}} \supseteq N$  we immediately find  $P(N^{\text{sat}}) \supseteq P(N)$ . Conversely, for  $\psi \in N^{\text{sat}}$  there exists an  $\alpha \in \mathbb{E}$  such that  $\psi\alpha \in N$ , and since the map  $\alpha: G \rightarrow G$  is surjective,  $\text{im}(\psi\alpha: G \rightarrow G^n) = \text{im}(\psi: G \rightarrow \overline{G}^n)$ . This proves the first statement.

This shows that  $P(\overline{N}) = P(N')$  where  $N' \subseteq N$  is any submodule of  $N$  of the same rank generated by vectors that are (right-)linearly independent over  $Q$ . The parametrization (1) shows that  $\dim X \leq \text{rk } N' = \text{rk } N$ . For the converse write  $d := \text{rk } N$ . Then exists a subset  $I \subseteq [n]$  with  $|I| = d$  such that the projection of  $N$  in  $\mathbb{E}^I$  has rank  $d$ , and one finds vectors  $v_i \in N, i \in I$  such that  $v_i$  has nonzero entry  $\alpha_i$  in position  $i$  and zero entries in positions  $j \in I \setminus \{i\}$ . Then the image of  $X$  in  $G^I$  contains the elements  $(\delta_{ij}\alpha_i(G))_{j \in I}$  for every  $i \in I$ , and these generate  $G^I$ . So  $\dim X \geq d$ .  $\square$

**Lemma 2.7.** *The diagram in Theorem 1.1 commutes.*

*Proof.* We concentrate on the upper triangle; the lower square was discussed in § 2.4. Let  $X \subseteq G^n$  be a closed and connected subgroup. By Lemma 2.2,  $X$  is the image of some homomorphism  $\beta: G^d \rightarrow G^n$  where  $d = \dim X$ . Then  $\beta = (\beta_1, \dots, \beta_n)$  where  $\beta_i: G^d \rightarrow G$  is a homomorphism. Write  $\beta_{ij}$  for the composition of the embedding  $G \rightarrow G^d, a \mapsto (0, \dots, 0, a, 0, \dots, 0)$  (with  $a$  in the  $j$ -th position) and  $\beta_i$ . Then  $\beta = (\beta_{ij})_{ij} \in \mathbb{E}^{n \times d}$ ; let  $N'$  be the right submodule of  $\mathbb{E}^n$  generated by the columns of  $\beta$ . Then  $X = P(N')$  by (1), and if we write  $N = (N')^{\text{sat}}$ , then  $X = P(N') = P(N)$  by Lemma 2.6.

Also by Lemma 2.6,  $\text{rk } N = d$ . Set  $J := N^\perp$ , a left module of rank  $n - d$ . The orthogonality to  $N$  implies that  $J$  is contained in  $E(X)$ . Let  $m \geq n - d$  be the rank of  $E(X)$ . Then there is a subset  $I \subseteq [n]$  of size  $m$  such that the projection of  $E(X)$  in  $\mathbb{E}^I$  has rank  $m$ . Then  $E(X)$  contains, for every  $i \in I$ , an element of the form  $\alpha_i e_i + \sum_{j \in [n] \setminus I} \alpha_{ij} e_j$ , where  $e_i$  is the  $i$ -th standard basis vector of  $\mathbb{E}^n$ . This implies that the projection  $X \rightarrow G^{[n] \setminus I}$  is finite-to-one. In particular,  $d = \dim X \leq n - m \leq d$ , so equality must hold everywhere and  $m = n - d$  and  $E(X) = J$ . Thus

$$X = P(N) = P((N^\perp)^\perp) = P(J^\perp) = P(E(X)^\perp).$$

To see that the triangle also commutes when we start at some saturated left  $\mathbb{E}$ -module  $J \subseteq \mathbb{E}^n$ , set  $X := P(J^\perp)$  and note that  $\dim X = n - \text{rk } J$  (by Lemma 2.6) and  $J \subseteq E(X)$ . If  $E(X)$  were strictly larger than  $J$ , then, since they are both saturated,  $\text{rk } E(X) > \text{rk}(J)$ , but then  $\text{rk}(E(X)^\perp) < \text{rk}(J^\perp)$  and

$$n - \text{rk } J = \dim X = \dim(P(E(X)^\perp)) = \text{rk}(E(X)^\perp) < n - \text{rk } J,$$

a contradiction (in the second equality we use that the triangle commutes when starting at  $X$ ). The same reasoning applies when we start at some saturated right  $\mathbb{E}$ -module  $N \subseteq \mathbb{E}^n$ .  $\square$

*Proof of Theorem 1.1.* By Lemma 2.7, the diagram of Figure 1 commutes. Now, let  $X \subseteq G^n$  be a closed, connected subgroup, and set  $N := P^{-1}(X) \subseteq \mathbb{E}^n$ . Let  $I \subseteq [n]$ , let  $X_I$  be the image of  $X$  in  $G^I$  ( $X_I$  is a closed, connected subgroup), and  $N_I$  be the saturation of the image of  $N$  in  $\mathbb{E}^I$ . Now we have  $X_I = P(N_I)$  and hence



$\dim X_I = \text{rk}(N_I) = \dim_Q N_I Q$  by Lemma 2.6. This proves that  $M(X)$  is (a matroid and) equal to the linear matroid on  $[n]$  defined by  $NQ$ .  $\square$

*Proof of Theorem 1.2.* Let  $A = M(X)$  for some closed, connected subgroup  $X \subseteq G^n$ . Let  $N := E(X)^\perp \subseteq \mathbb{E}^n$ . Then the right  $Q$ -vector space  $V := NQ$  of  $Q^n$  determines the same matroid  $A$  by Theorem 1.1. Now the results on deletion and contraction follow from linear algebra over  $Q$ .

For duality, we argue that  $Q$  has an anti-automorphism  $\tau$ . When  $Q$  is commutative, we take  $\tau = 1_Q$ . When  $G = \mathbb{G}_a$  in characteristic  $p > 0$ , there is a unique anti-isomorphism  $\tau : \mathbb{E} = K[F] \rightarrow K[F^{-1}] \subseteq Q$  that sends  $F$  to  $F^{-1}$  and that is the identity on  $K$ . This extends uniquely to an anti-automorphism of  $Q$  ( $\mathbb{E}$  itself does not have a natural anti-automorphism in this case!). When  $G$  is a supersingular elliptic curve in characteristic  $p > 0$ , we use the dual isogeny [Sil09, III.9, item (ii)].

Now  $V^\perp$  is a left vector space over  $Q$  determining the matroid dual to  $A$ , and  $\tau(V^\perp) \subseteq Q^n$  a right vector space also determining the matroid dual to  $A$ . Let  $N' := \tau(V^\perp) \cap \mathbb{E}^n$ . This is a saturated right module, and the group  $X := P(N')$  determines the matroid dual to  $E$ .  $\square$

**Example 2.8.** Take  $M$  and  $\Psi$  as in Example 1.3. The orthogonal complement  $M^\perp$  is the left submodule of  $K[F]^4$  given as the row space of the matrix

$$\Psi^\perp = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & F & 0 & 1 \end{pmatrix}.$$

The recipe in the proof of Theorem 1.2 involves taking the right  $Q$ -vector space spanned by the columns of

$$\begin{pmatrix} 1 & 1 \\ 1 & F^{-1} \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and intersecting with  $K[F]^4$ . This yields the right  $K[F]$ -module generated by the columns of

$$\begin{pmatrix} 1 & F \\ 1 & 1 \\ 1 & 0 \\ 0 & F \end{pmatrix}.$$

The corresponding subgroup is  $\{(a + b^2, a + b, a, b^2) \mid (a, b) \in K^2\}$ , a representation of the dual of  $U_{2A}$ , which of course is also  $U_{2A}$ .  $\clubsuit$

### 3. LINEAR FLOCKS FROM VECTOR SPACES OVER DIVISION RINGS

In this section we introduce some of the key structures featuring in the statement and proof of Theorem 1.5.

**3.1. Linear flocks.** *Frobenius flocks* are collections of vector spaces which are an enrichment of a valuated matroid, introduced in [BDP18]. Here, we describe a slight generalization called linear flocks, where the Frobenius automorphism is replaced by an arbitrary automorphism [Bol18, Ch. 4]. Throughout what follows, we write  $e_i$  for the  $i$ -th standard basis vector in  $\mathbb{Z}^n$ .

**Definition 3.1.** Let  $L$  be a field and let  $\varphi: L \rightarrow L$  an automorphism. Then a  $(L, \varphi)$ -linear flock is a collection of vector spaces  $(V_\alpha)_{\alpha \in \mathbb{Z}^n} \in L^n$ , of the same dimensions, such that

- (1) For any  $\alpha \in \mathbb{Z}^n$  and  $1 \leq i \leq n$ ,  $V_\alpha/i = V_{\alpha+e_i} \setminus i$  (here  $/i$  stands for intersecting with the  $i$ -th coordinate hyperplane and  $\setminus i$  stands for setting the  $i$ -th coordinate zero); and
- (2) For any  $\alpha \in \mathbb{Z}^n$ ,  $V_{\alpha+(1,\dots,1)} = \varphi(V_\alpha)$ , where  $\varphi$  refers to the coordinate-wise application of the automorphism to  $L^n$ .

A Frobenius flock is an  $(L, F^{-1})$ -linear flock where  $F$  is the Frobenius automorphism of a perfect field  $L$  of positive characteristic. As shown in [BDP18, Thm. 34], an algebraic variety over  $L$  defines a Frobenius flock.

**3.2. Linear flocks from right vector spaces.** We now construct a linear flock from a right vector space, as follows. Let  $Q$  be a division ring with a surjective, discrete valuation  $v: Q \rightarrow \mathbb{Z} \cup \{\infty\}$ . Valuations are well-known in commutative algebra, but they can also be generalized to non-commutative rings [Sch45]. We will only use the case of value group  $\mathbb{Z}$ .

**Definition 3.2.** A valuation on a ring  $R$  is a function  $v: R \rightarrow \mathbb{Z} \cup \{\infty\}$  such that:

- For all  $a, b \in R$ ,  $v(ab) = v(a) + v(b)$ .
- For all  $a, b \in R$ ,  $v(a + b) \geq \min\{v(a), v(b)\}$ .

Let  $R \subset Q$  be the valuation ring, which is the set of elements with non-negative valuation. The residue division ring  $L$  is the quotient of  $R$  by the maximal ideal consisting of all elements of positive valuation. For simplicity, we assume that  $L$  is commutative, and hence a field. We define the automorphism  $\varphi: L \rightarrow L$  by sending the residue class of  $x \in R$  to the residue class of  $\pi x \pi^{-1}$ , where  $\pi$  is any uniformizer, i.e., element of valuation 1. Thus, if  $R$  is commutative, then  $\varphi$  is the identity.

**Lemma 3.3.** *If  $Q$  is a division ring with a valuation, whose residue division ring  $L$  is commutative, then the automorphism  $\varphi: L \rightarrow L$  is well-defined.*

*Proof.* Let  $\pi'$  be another element of  $R$  such that  $v(\pi') = 1$  and let  $x'$  be another element of  $R$  with the same residue class as  $x$ . Thus,  $\pi' = u\pi$ , where  $u$  is a unit in  $R$ , and  $x' = x + t$ , where  $v(t) > 0$ . Then, using  $\bar{y}$  to denote the residue class in  $L$  of  $y \in R$ ,

$$\overline{\pi' x' (\pi')^{-1}} = \overline{u\pi(x+t)\pi^{-1}u^{-1}} = \bar{u} \cdot \overline{\pi x \pi^{-1}} \cdot \bar{u}^{-1} + \overline{u\pi t \pi^{-1}u^{-1}} = \overline{\pi x \pi^{-1}},$$

because  $L$  is commutative and  $v(u\pi t \pi^{-1}u^{-1}) = v(t) > 0$ .  $\square$

We recall the following lemma, and include a proof for completeness.

**Lemma 3.4.** *Let  $V \subseteq Q^n$  be a right vector space, and let  $v_1, \dots, v_r \in V \cap R^n$  map to a basis of the  $L$ -vector space  $\overline{V \cap R^n} \subseteq L^n$ . Then  $v_1, \dots, v_r$  are a  $Q$ -basis of  $V$ . In particular,  $\dim_Q V = \dim_L \overline{V \cap R^n}$ .*

*Proof.* Choose  $v_{r+1}, \dots, v_n \in R^n$  such that their reductions,  $\bar{v}_1, \dots, \bar{v}_n$  form a basis of  $L^n$ . By Nakayama's Lemma,  $v_1, \dots, v_n$  generate  $R^n$ , and therefore they generate  $Q^n$  as well, so  $v_1, \dots, v_n$  is a basis both for  $Q^n$  as a right vector space, and for  $R^n$  as a right  $R$ -module.

Now let  $w \in V$ , so that  $w = v_1 a_1 + \cdots + v_n a_n$  for some  $a_1, \dots, a_n \in Q$ . Set

$$u := v_{r+1} a_{r+1} + \cdots + v_n a_n = w - v_1 a_1 - \cdots - v_r a_r \in V.$$

Assume that  $u$  is non-zero. Then, by scaling by an appropriate power of  $\pi$ , we can assume that the minimum valuation of the coordinates of  $u$  is 0, so  $u \in R^n$  and  $\bar{u}$  is non-zero. Thus,  $u$  can be written as an  $R$ -linear combination of  $v_1, \dots, v_n$ , but we already know that  $u$  is uniquely written as  $v_{r+1} a_{r+1} + \cdots + v_n a_n$ , which means that  $a_{r+1}, \dots, a_n$  must be in  $R$ . Therefore,  $\bar{u}$  is a nonzero linear combination  $\overline{v_{r+1}}, \dots, \overline{v_n}$ , which implies that  $\bar{u}$  is not in  $\overline{V \cap R^n}$ , a contradiction. Therefore,  $u$  is 0, so  $w$  is in the span of  $v_1, \dots, v_r$ . This shows that  $\dim_Q V = r = \dim_L \overline{V \cap R^n}$ , as desired.  $\square$

Now fix a right vector space  $V \subset Q^n$ . For any  $\alpha \in \mathbb{Z}^n$ , we define

$$V_\alpha := \overline{(\pi^{-\alpha} V) \cap R^n} \subset L^n,$$

where  $\pi^{-\alpha}$  denotes the diagonal matrix with entries  $\pi^{-\alpha_1}, \dots, \pi^{-\alpha_n}$ .

**Lemma 3.5.** *The vector spaces  $(V_\alpha)_{\alpha \in \mathbb{Z}^n}$  defined above form a  $(L, \varphi^{-1})$ -linear flock.*

*Proof.* First, for each  $\alpha$  we have

$$\dim_L V_\alpha = \dim_Q \pi^{-\alpha} V = \dim_Q V =: r,$$

where the first equality follows from Lemma 3.4. Second, for  $1 \leq i \leq n$  and  $\alpha \in \mathbb{Z}^n$  we have

$$(\pi^{-\alpha} V) \cap R^n \supseteq \pi^{e_i} ((\pi^{-\alpha - e_i} V) \cap R^n).$$

Applying  $\pi^{e_i}$  to a vector in  $R^n$  and then reducing is the same thing as first reducing and then setting the  $i$ -th coordinate to zero, so we find that  $V_\alpha / i \supseteq V_{\alpha + e_i} \setminus i$ . If the latter vector space has dimension  $r$ , then, since the former vector space has dimension at most  $r$ , the two spaces are equal. Otherwise,  $V_{\alpha + e_i} \setminus i$  has dimension  $r - 1$ . Then  $V_{\alpha + e_i}$  contains the  $i$ -th standard basis vector of  $L^n$  and therefore  $\pi^{-\alpha - e_i} V$  contains an element of the form  $(a_1, \dots, 1, \dots, a_n)$  with  $v(a_j) > 0$  for  $j \neq i$ . Then  $\pi^{-\alpha} V$  contains the vector  $(\pi^{-1} a_1, \dots, 1, \dots, \pi^{-1} a_n)$  whose reduction has a nonzero  $i$ -th coordinate, hence  $V_\alpha / i$  has dimension  $r - 1$ , as well, so that again we have  $V_\alpha / i = V_{\alpha + e_i} \setminus i$ .

Third, every coordinate of every element of  $\pi((\pi^{-\alpha} V) \cap R^n)$  has positive valuation, and so  $\pi((\pi^{-\alpha} V) \cap R^n) \pi^{-1}$  is contained in  $R^n$ , and thus equal to  $(\pi^{-\alpha + (1, \dots, 1)} V) \cap R^n$ . Thus,  $V_{\alpha - (1, \dots, 1)}$  is equal to  $\varphi(V_\alpha)$ .  $\square$

By considering the matroid associated to each  $V_\alpha$ , a  $(L, \varphi^{-1})$ -linear flock defines a matroid flock, a notion cryptomorphic to that of a valuated matroid (up to adding scalar multiples of the all-one vector) by [BDP18, Theorem 7].

We will now show that for the flock from Lemma 3.5, this valuated matroid is the natural non-commutative generalization of the well-known construction of a matroid valuation from a vector space of a field with a non-Archimedean valuation. For this we recall that the *Dieudonné determinant* is the unique group homomorphism  $\det : \mathrm{GL}_r(Q) \rightarrow Q^*/[Q^*, Q^*]$  that sends a diagonal matrix  $\mathrm{diag}(c, 1, \dots, 1)$  to the class of  $c$  and matrices that differ from the identity matrix only in one off-diagonal entry to 1. We define the Dieudonné determinant of a non-invertible square matrix to be the symbol  $O$ , and we make  $Q^*/[Q^*, Q^*] \cup \{O\}$  into a commutative monoid by  $a \cdot O := O$ . Since commutators have valuation 0, the valuation  $v$  induces a group homomorphism  $v : Q^*/[Q^*, Q^*] \rightarrow \mathbb{Z}$ , and we set  $v(O) = \infty$ . The

Smith normal form algorithm shows that  $r \times r$ -matrix  $A \in R^{r \times r}$  has  $v(\det(A)) \geq 0$  with equality if and only if  $\bar{A} \in L^{r \times r}$  is invertible.

**Proposition 3.6.** *Let  $V \subset Q^n$  be a right vector space, and let  $\mu$  denote the matroid valuation corresponding to the matroid flock associated to the linear flock  $(V_\alpha)_\alpha$  (defined using any uniformizer  $\pi \in R$ ). Then the rank in  $\mu$  of a subset  $I \subseteq [n]$  is the dimension of the projection of  $V$  into  $Q^I$ ; and the valuated circuits are:*

$$\{(v(c_1), \dots, v(c_n)) \mid c_i \in Q, [c_1 \cdots c_n]V = 0, \text{ and the support of } c \text{ is minimal}\}.$$

Moreover, if  $V$  is given as the right column span of an  $n \times r$  matrix  $A$ , then the valuation  $\mu(B)$  of  $B \in \binom{[n]}{r}$  is equal to the valuation  $v(\det A[B])$  of the Dieudonné determinant of the submatrix of  $A$  consisting of the rows labeled by  $B$ .

*Proof.* By [BDP18, Theorem 7], the valuation  $\mu$  can be characterized as follows (again, modulo scalar multiples of the all-one vector): for all  $\alpha \in \mathbb{Z}^n$  the expression  $\mu(B) - e_B^T \alpha$ , where  $e_B := \sum_{i \in B} e_i$  is the characteristic vector of  $B$ , is minimized by  $B_0 \in \binom{[n]}{r}$  if and only if  $B_0$  is a basis for the matroid  $M(V_\alpha)$  on  $[n]$  defined by  $V_\alpha$ . It suffices to prove that the numbers  $v(\det A[B])$  have this property.

Suppose that  $B_0$  is a basis for  $M(V_\alpha)$ . Choose  $v_1, \dots, v_r \in (\pi^{-\alpha}V) \cap R^n$  such that  $\bar{v}_1, \dots, \bar{v}_r$  are a basis of  $V_\alpha$ . Let  $g \in \text{GL}_r(Q)$  be the unique matrix such that  $A' := \pi^{-\alpha}Ag$  has columns  $v_1, \dots, v_r$ . Then for any  $B \in \binom{[n]}{r}$  we have

$$\begin{aligned} v(\det(A[B])) - e_B^T \alpha &= v(\det(\pi^\alpha[B]) \det(A'[B]) \det(g^{-1})) - e_B^T \alpha \\ &= v(\det(A'[B])) + v(\det(g^{-1})) + (e_B^T \alpha - e_{B_0}^T \alpha) \\ &\geq v(\det(A'[B_0])) + v(\det(g^{-1})) \\ &= v(\det(A[B_0])) - e_{B_0}^T \alpha, \end{aligned}$$

where the inequality follows because  $A'$  has entries in  $R$ , and  $v(\det(A'[B_0])) = 0$  since  $A'[B_0]$  is invertible. Moreover, equality holds if and only if also  $B$  is a basis in the matroid  $M(V_\alpha)$ . This proves the last statement in the lemma, and also that  $B$  is a basis in the underlying matroid of  $\mu$  if and only if  $A[B]$  is invertible; this, in turn, implies the statement about the rank function.

Finally, recall that the valuated circuits corresponding to the basis valuation  $\mu$  are the vectors  $\gamma \in (\mathbb{Z} \cup \{\infty\})^n$  that are supported precisely on some circuit  $C \subseteq [n]$  of the matroid underlying  $\mu$  and have the property that for each  $i \in C$ , and for each  $j \in C - i := C \setminus \{i\}$  we have

$$\mu(C - i) + \gamma_j = \mu(C - j) + \gamma_i.$$

Without loss of generality, we may assume that  $C - i = [r]$  and that  $i = r + 1$ . After performing column operations on  $A$  over  $Q$ , we may assume that  $A[C - i]$  is the identity matrix, so that  $\mu(B) = 0$ .

Then the unique linear relation among the rows of  $A[[r + 1]]$  is the vector  $a = (a_{r+1,1}, \dots, a_{r+1,r}, -1, 0, \dots, 0)$ . We have, for each  $j = 1, \dots, r$ ,

$$\mu(C - i) + v(a_{r+1,j}) = v(a_{r+1,j}) = v(\det A[C - j]) = \mu(C - j) + v(-1),$$

which means that  $v(a)$  satisfies the condition on  $\gamma$  above. This proves the statement about valuated circuits.  $\square$

## 4. LINDSTRÖM VALUATIONS AND FROBENIUS FLOCKS

The goal of this section is to prove Theorem 1.5. Let  $p$  be a fixed prime number,  $K$  an algebraically closed field of characteristic  $p$ , and  $G$  a one-dimensional algebraic group over  $K$ . As before,  $\mathbb{E}$  denotes the endomorphism ring of  $G$ . We will construct a valuation on  $\mathbb{E}$ , introduce Frobenius flocks and Lindström valuations of closed, connected subgroups of  $G^n$ , and relate these to the constructions of Section 3.

**4.1. The valuation on  $\mathbb{E}$ .** In order to define the valuation  $v: \mathbb{E} \rightarrow \mathbb{Z} \cup \{\infty\}$ , we let  $\alpha \in \mathbb{E}$  be a nonzero endomorphism of  $G$  and then obtain an injective homomorphism  $\alpha^*: K(G) \rightarrow K(G)$  of function fields. If we let  $L$  be the set of elements of  $K(G)$  which are purely inseparable over  $\alpha^*K(G)$ , then  $L/\alpha^*K(G)$  is a purely inseparable extension of fields, and  $K(G)/L$  is a separable extension. The degree  $[L : \alpha^*K(G)]$  is a power of  $p$ , and is called the inseparable degree of the extension  $K(G)/\alpha^*K(G)$ , and denoted  $[K(G) : \alpha^*K(G)]_i$  [Lan02, §V.6]. We define our valuation by  $v(\alpha) = \log_p [K(G) : \alpha^*K(G)]_i$  for  $\alpha$  non-zero, and  $v(0) = \infty$ .

The main technical point to proving that  $v$  is a valuation is the following:

**Lemma 4.1.** *If  $K'$  is a subfield of  $K(G)$  such that  $K(G)/K'$  is purely inseparable, then  $K' = F^n K(G)$  for some integer  $n$ , where  $F$  is the Frobenius endomorphism of  $K(G)$ .*

*Proof.* Let  $x$  and  $y$  be two elements in  $K(G) \setminus K$ . Since  $K(G)/K$  has transcendence rank 1,  $x$  and  $y$  are algebraically dependent, meaning that they satisfy a polynomial relation  $f(x, y)$ , where  $f \in K[X, Y]$ . If every exponent of  $f$  is divisible by  $p$ , then  $f = g^p$ , using the fact that  $K$  is algebraically closed. We can assume that  $f$  is irreducible, which means that at least one exponent is not divisible by  $p$ . Therefore, either  $x$  is separable over  $K(y)$  or  $y$  is separable over  $K(x)$ . Thus, the purely inseparable subfields of  $K(G)$  are totally ordered by inclusion.

The fields  $K(G) \supset FK(G) \supset F^2K(G) \supset \dots$  also form a chain of purely inseparable subfields of  $K(G)$ . Each containment has index  $p$ , so there can't be any intermediate fields. Since  $K(G)/K'$  is purely inseparable, then  $K' \neq K$ , and so  $K'(G)/K$  has finite index. Therefore,  $K'$  can't be contained in all the  $F^n K(G)$ , but since the purely inseparable subfields are totally ordered, then it must be equal to  $F^n K(G)$  for some  $n$ .  $\square$

**Proposition 4.2.** *The function  $v: \mathbb{E} \rightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}$  defines a valuation on  $\mathbb{E}$  that extends uniquely to  $Q$ .*

*Proof.* In order to show that  $v$  is a valuation on  $\mathbb{E}$ , we first note that  $v(\alpha\beta) = v(\alpha) + v(\beta)$  because of the multiplicativity of inseparable degree [Lan02, Cor. V.6.4].

Second, we want to show that if  $\alpha$  and  $\beta$  are elements of  $\mathbb{E}$ , then  $v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\}$ . By Lemma 4.1,  $\alpha^*K(G)$  and  $\beta^*K(G)$  are contained in  $F^{v(\alpha)}K(G)$  and  $F^{v(\beta)}K(G)$ , respectively, and thus both are contained in  $F^{\min\{v(\alpha), v(\beta)\}}K(G)$ . Since  $(\alpha + \beta)^*K(G)$  is contained in the compositum of  $\alpha^*K(G)$  and  $\beta^*K(G)$ , then it is contained in  $F^{\min\{v(\alpha), v(\beta)\}}K(G)$ , and thus  $v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\}$ .

Next we want to show that  $v$  extends to a unique valuation on  $Q$ , which is an exercise in working with rings of fractions and the Ore condition. We refer to [Coh95, Chapter 1] for an introduction to Ore domains. Every element of  $Q$  can be written as a fraction  $\varphi^{-1}\psi$  for some  $\varphi, \psi \in \mathbb{E}$ , and we define  $v(\varphi^{-1}\psi) = -v(\varphi) + v(\psi)$ . If we write  $\varphi^{-1}\psi$  instead as  $(\tau\varphi)^{-1}\tau\psi$  for some  $\tau \in \mathbb{E}$ , then

$$v((\tau\varphi)^{-1}\tau\psi) = -v(\tau\varphi) + v(\tau\psi) = -v(\tau) - v(\varphi) + v(\tau) + v(\psi) = -v(\varphi) + v(\psi) = v(\varphi^{-1}\psi),$$

which shows that this valuation is well-defined. Since the valuation is defined using elements of  $\mathbb{E}$  and their reciprocals, this is the unique valuation which extends the one on  $\mathbb{E}$ .

Now we want to show that  $v$  defines a valuation on  $Q$ . Again, we write  $\varphi^{-1}\psi$  and  $\sigma^{-1}\tau$  for elements of  $Q$ , where  $\varphi, \psi, \sigma$ , and  $\tau$  are in  $\mathbb{E}$ . Then we take their product by finding  $\psi'$  and  $\sigma'$  in  $\mathbb{E}$  such that  $\sigma'\psi = \psi'\sigma$  (the existence of such elements is the left Ore condition), and then  $(\varphi^{-1}\psi)(\sigma^{-1}\tau) = (\sigma'\varphi)^{-1}\psi'\tau$ . The valuation of this product is:

$$\begin{aligned} v((\sigma'\varphi)^{-1}\psi'\tau) &= -v(\sigma'\varphi) + v(\psi'\tau) = -v(\sigma') - v(\varphi) + v(\psi') + v(\tau) \\ &= -v(\varphi) - v(\sigma) + v(\psi) + v(\tau) = v(\varphi^{-1}\psi) + v(\sigma^{-1}\tau), \end{aligned}$$

where the first equality on the second line is by our assumption that  $\sigma'\psi = \psi'\sigma$ .

Second, to compute the sum of  $\varphi^{-1}\psi$  and  $\sigma^{-1}\tau$ , we find  $\varphi'$  and  $\sigma'$  in  $\mathbb{E}$  such that  $\sigma'\varphi = \varphi'\sigma$  and then:

$$\varphi^{-1}\psi + \sigma^{-1}\tau = (\sigma'\varphi)^{-1}(\sigma'\psi + \varphi'\tau).$$

If we take the valuation of this sum, we get:

$$\begin{aligned} v((\sigma'\varphi)^{-1}(\sigma'\psi + \varphi'\tau)) &= -v(\sigma') - v(\varphi) + v(\sigma'\psi + \varphi'\tau) \\ &\geq -v(\sigma') - v(\varphi) + \min\{v(\sigma') + v(\psi), v(\varphi') + v(\tau)\} \\ &= \min\{-v(\varphi) + v(\psi), -v(\sigma') - v(\varphi) + v(\varphi') + v(\tau)\} \\ &= \min\{-v(\varphi) + v(\psi), -v(\sigma) + v(\tau)\} \\ &= \min\{v(\varphi^{-1}\psi), v(\sigma^{-1}\tau)\}, \end{aligned}$$

which completes the proof the  $v$  is a valuation on  $\mathbb{E}$ .  $\square$

The set of all elements with positive valuation is a two-sided ideal  $I$  in  $\mathbb{E}$ . If  $G$  is defined by equations with coefficients in  $\mathbb{F}_p$ , such as  $\mathbb{G}_a$  or  $\mathbb{G}_m$ , then the Frobenius homomorphism itself is an endomorphism of  $G$ . Moreover, this element  $F$  generates  $I$  as either a left, right or two-sided ideal. When  $G$  is an elliptic curve not defined over  $\mathbb{F}_p$ , then  $I$  need not be principal.

**4.2. Description of the valuation on  $\mathbb{E}$ .** Recall that an elliptic curve in positive characteristic is called *supersingular* if its ring of endomorphisms is non-commutative, and thus an order in a quaternion algebra [Sil09, §V.3].

**Proposition 4.3.** *For each connected one-dimensional algebraic group  $G$ , the valuation on  $\mathbb{E}$  is as follows:*

- (1) *If  $G \cong \mathbb{G}_a$ , so that  $\mathbb{E}$  is the ring of  $p$ -polynomials  $K[F]$ , then  $v$  is the  $F$ -adic valuation.*
- (2) *If  $G \cong \mathbb{G}_m$ , so that  $\mathbb{E} \cong \mathbb{Z}$ , with  $F$  corresponding to  $p$ , then  $v$  is the  $p$ -adic valuation.*
- (3) *If  $G \cong E$ , an elliptic curve with  $j$ -invariant not in  $\overline{\mathbb{F}_p}$ , then  $\mathbb{E} \cong \mathbb{Z}$  and  $v$  is the  $p$ -adic valuation.*
- (4) *If  $G \cong E$ , a non-supersingular elliptic curve with  $j$ -invariant in  $\overline{\mathbb{F}_p}$ , then  $\mathbb{E}$  is an order in a quadratic number field  $\mathbb{Q}(\sqrt{-D})$ . Let  $\mathcal{O} \supset \mathbb{E}$  denote the ring of integers in  $\mathbb{Q}(\sqrt{-D})$ . Then there exists a maximal ideal  $m \subset \mathcal{O}$  such that  $m\bar{m} = (p)$ , where  $\bar{m}$  denotes complex conjugation, and  $v$  is the restriction of the  $m$ -adic valuation.*

- (5) If  $G \cong E$ , a supersingular elliptic curve with  $j$ -invariant in  $\overline{\mathbb{F}_p}$  then  $\mathbb{E}$  is an order in a quaternion algebra, and  $v(\alpha)$  is the  $p$ -adic valuation of  $\alpha\bar{\alpha}$ .

*Proof.* The first two cases follow from the fact that in each case Frobenius is an endomorphism of  $G$ , corresponding to  $p$  and  $F$ , respectively.

In case (3), we know that multiplication by  $p$ , a morphism of degree  $p^2$  by [Sil09, Thm III.6.2(d)], is inseparable but not purely inseparable, and hence  $v(p) = 1$ . Thus,  $v$  must be the  $p$ -adic valuation.

In case (4), we know that any valuation on  $\mathbb{Q}(\sqrt{-D})$  corresponds to a maximal ideal  $m$  of  $\mathcal{O}$ , and the multiplication by  $p$  endomorphism is inseparable, but not purely inseparable so  $v(p) = 1$ . Thus, it remains to show that the rational prime  $p$  splits in  $\mathcal{O}$ . This is a standard fact in the theory of elliptic curves, but we include a proof for convenience.

We define  $G^{(p^i)}$  to be the elliptic curve obtained by applying the  $i$ th power of Frobenius to the defining equations of the elliptic curve  $G$ . Since  $G$  is defined over  $\overline{\mathbb{F}_p}$ ,  $G^{(p^k)} \cong G$  for some positive integer  $k$ , thus composition with the  $k$ th power of Frobenius followed by this isomorphism defines an endomorphism of  $G$ , which we will denote  $\alpha_k: G \rightarrow G$ . In particular,  $\alpha_k$  is a degree  $p^k$  purely inseparable endomorphism and thus  $v(\alpha_k) = k$ . The dual homomorphism of  $F$  is separable by equivalence (ii) of [Sil09, Thm. V.3.1(a)], and so the dual endomorphism  $\bar{\alpha}_k$  is separable, meaning that  $v(\bar{\alpha}_k) = 0$ . Since  $\alpha_k\bar{\alpha}_k = p^k$  by [Sil09, Thm. III.6.2(a)], then  $(p)$  is not a prime ideal, and  $\bar{\alpha}_k \notin m$ .

In case (5), the endomorphism  $p$  is purely inseparable by the equivalence (iii) of [Sil09, Thm. V.3.1(a)], and has degree  $p^2$  by [Sil09, Thm. III.6.2(d)]. Therefore,  $v(p) = 2$ . Let  $\alpha$  be any endomorphism in  $\mathbb{E}$ , and  $\bar{\alpha}$  its dual. Then  $\alpha\bar{\alpha} = d$ , where  $d$  is the degree of  $\alpha$  and of  $\bar{\alpha}$ , by [Sil09, Thm. III.6.2(a)]. If we write  $d = p^k e$ , where  $p$  does not divide  $e$ , so that  $k$  is the  $p$ -adic valuation of  $d$ , then  $v(d) = kv(p) + v(e) \geq 2k$ . On the other hand, the inseparable degree of  $\alpha$  divides  $d$  and is a power of  $p$ , so  $v(\alpha) \leq k$ , and similarly  $v(\bar{\alpha}) \leq k$ . By the multiplicativity of valuation,  $v(\alpha) = k$ , which is what we wanted to show.  $\square$

We next want to show that the valuation on  $\mathbb{E}$  is surjective. Since we already know that the residue division ring of  $Q$  is commutative, this means we can use the results of § 3.

**Lemma 4.4.** *There exists an element  $\pi \in \mathbb{E}$  with  $v(\pi) = 1$ .*

*Proof.* We consider each of the cases of Proposition 4.3. If  $G \cong \mathbb{G}_a$ , then we can take  $\pi = F$ . In cases (2) and (3),  $\mathbb{E} \cong \mathbb{Z}$ , with the  $p$ -adic valuation, and in case (4), the valuation restricts to the  $p$ -adic valuation on the subring of integers, and so in these case, we can take  $\pi = p$ .

In case (5), where  $G$  is a supersingular elliptic curve,  $v(p) = 2$ , and we have to find  $\pi \in \mathbb{E} \setminus \mathbb{Z}$ . By [Voi18, Thm. 42.1.9],  $Q$  is ramified at  $p$ , which means that  $Q \otimes_{\mathbb{Q}} \mathbb{Q}_p$  is a division algebra over  $\mathbb{Q}_p$ , the field of  $p$ -adics. Therefore, by [Voi18, Thm. 13.3.10(c)], there is an element  $\varphi \in Q \otimes_{\mathbb{Q}} \mathbb{Q}_p$  such that  $N(\varphi)$  has  $p$ -adic valuation 1. Since  $Q \otimes_{\mathbb{Q}} \mathbb{Q}_p$  is the  $p$ -adic completion of  $Q$ , then  $\varphi$  can be approximated by an element  $\varphi' \in Q$  with the same valuation. We can write  $\varphi' = a^{-1}\psi$ , where  $a \in \mathbb{Z}$  and  $\psi \in \mathbb{E}$ . Therefore,  $N(\psi) = a^2 N(\varphi')$  has odd  $p$ -adic valuation, say  $2k + 1$ , so we can write  $\psi = \psi' \circ F^{2k+1}$ , where  $\psi': G^{(p^{2k+1})} \rightarrow G$  is separable. Since  $G$  is defined over  $\mathbb{F}_{p^2}$  [Sil09, Thm. V.3.1(a)],  $G^{(p^{2k+1})} \cong G^{(p)}$ , and so we take  $\pi = \psi' \circ F$ .  $\square$

**4.3. The derivative homomorphism.** An element  $\alpha \in \mathbb{E}$  is, by definition, an algebraic group homomorphism  $G \rightarrow G$ . In particular, it maps 0 to 0, and the derivative  $d_0\alpha$  is a linear map from the tangent space  $T_0G$  into itself. Since  $T_0G$  is a one-dimensional vector space over  $K$ , we can identify  $d_0\alpha$  with a scalar in  $K$ . Concluding, we have a map

$$\ell : \mathbb{E} \rightarrow K, \quad \alpha \mapsto d_0\alpha.$$

In the case of an elliptic curve, this is the same map as constructed in [Sil09, Corollary III.5.6].

**Lemma 4.5.** *The map  $\ell$  is a (unitary) ring homomorphism,  $\text{im } \ell$  is a subfield of  $K$ , and  $\ker \ell$  is the ideal  $\{\varphi \in \mathbb{E} \mid v(\varphi) > 0\}$ .*

*Proof.* First, the multiplicative neutral element of  $\mathbb{E}$  is the identity  $G \rightarrow G$ , whose derivative is the scalar multiplication  $T_0G \rightarrow T_0G$  by  $1 \in K$ . Next, multiplicativity of  $\ell$  follows from the chain rule:

$$\ell(\alpha\beta) = d_0(\alpha \circ \beta) = (d_0\alpha) \circ (d_0\beta) = \ell(\alpha)\ell(\beta).$$

For additivity, we recall that for any algebraic group  $G$  with neutral element  $e$  the derivative of the group operation  $m: G \times G \rightarrow G$  at  $(e, e)$  is the addition map  $T_eG \times T_eG \rightarrow T_eG$ . So in our setting where  $e = 0$ ,

$$\ell(\alpha + \beta) = d_0(\alpha + \beta) = d_0(m \circ (\alpha, \beta)) = d_0\alpha + d_0\beta = \ell(\alpha) + \ell(\beta),$$

where we used the chain rule once more in the third equality.

To show that  $\text{im } \ell$  is a field, we use the classification of one-dimensional groups  $G$ . If  $G$  is  $\mathbb{G}_a$ , then  $\mathbb{E}$  is the ring of  $p$ -polynomials  $K[F]$ , and  $\ell(F) = 0$ , so  $\text{im } \ell = K[F]/K[F]F$  is isomorphic to  $K$ . In the other cases, when  $G$  is  $\mathbb{G}_m$  or an elliptic curve,  $\mathbb{E}$  is a finitely generated  $\mathbb{Z}$ -algebra. Since  $\text{im } \ell$  is a subring of a field of characteristic  $p$ , it must be a finitely generated  $\mathbb{F}_p$ -algebra, and also an integral domain, thus it is a field.

For the last statement, if  $\alpha \in \mathbb{E}$  has positive valuation, then it is inseparable, so its derivative vanishes. Conversely, let  $\alpha \in \mathbb{E}$  with  $\ell(\alpha) = d_0\alpha = 0$ . For  $h \in G$  let  $a_h: G \rightarrow G$  be the morphism  $g \mapsto g + h$ . Then  $\alpha \circ a_h = a_{\alpha(h)} \circ \alpha$  and therefore

$$(d_h\alpha) \circ (d_0a_h) = d_0(\alpha \circ a_h) = d_0(a_{\alpha(h)} \circ \alpha) = d_0(a_{\alpha(h)}) \circ 0 = 0$$

and using that  $d_0a_h$  is invertible with inverse  $d_h a_{-h}$  we find that  $d_h\alpha = 0$ . So  $\alpha$  is inseparable, so it has positive valuation.  $\square$

**Remark 4.6.** The first statement in the lemma also holds when  $\text{char } K = 0$ . Then the non-existence of inseparable morphisms implies immediately that  $\mathbb{E}$  embeds into  $K$  and is, in particular, a commutative ring.

Let  $R \subseteq Q$  be the valuation ring. For what follows, we need to extend  $\ell$  from  $\mathbb{E}$  to  $R$ . Let  $\alpha, \beta \in \mathbb{E}$  such that  $\alpha\beta^{-1} \in R$ . By [Sil09, Corollary II.2.12], we can write  $\beta = \beta' \circ F^e$  for some  $e \in \mathbb{Z}_{\geq 0}$ , where  $F^e: G \rightarrow G^{(p^e)}$  is the  $e$ -th power of Frobenius and  $\beta': G^{(p^e)} \rightarrow G$  is separable. It follows that  $v(\beta) = e$ . Similarly, write  $\alpha = \alpha'' \circ F^d$  with  $\alpha'': G^{(p^d)} \rightarrow G$  separable and hence  $v(\alpha) = d$ . Since  $\alpha\beta^{-1} \in R$ , we have  $d \geq e$ , and we set  $\alpha' := \alpha'' \circ F^{d-e}$ . Then  $\alpha', \beta'$  are both morphisms  $G^{(p^e)} \rightarrow G$  and  $\beta'$  is separable. This implies that  $d_0\beta': T_0G^{(p^e)} \rightarrow T_0G$  is multiplication by a nonzero scalar, and so an isomorphism. Then  $(d_0\alpha')(d_0\beta')^{-1}$  is a linear map  $T_0G \rightarrow T_0G$ , hence multiplication by a scalar, which we denote by  $\ell(\alpha\beta^{-1})$ .



**Lemma 4.7.** *The above is a well-defined extension of  $\ell: \mathbb{E} \rightarrow K$  to a ring homomorphism  $\ell: R \rightarrow K$  whose image is a field and whose kernel is the set of elements of positive valuation.*

*Proof.* First, taking  $\beta$  equal to the identity, the above reduces to the earlier definition of  $\ell: \mathbb{E} \rightarrow K$ . Second, let  $\gamma \in \mathbb{E} \setminus \{0\}$  and set  $\alpha_1 := \alpha\gamma$  and  $\beta_1 := \beta\gamma$ , so that  $\alpha_1\beta_1^{-1} = \alpha\beta^{-1}$ . Write  $\gamma = \gamma'F^c$  with  $c \in \mathbb{Z}_{\geq 0}$  and  $\gamma' : G^{(p^c)} \rightarrow G$  separable. Then, with notation as above,

$$\beta_1 = (\beta'F^e)(\gamma'F^c) = \beta'(F^e\gamma'F^{-e})F^{e+c} = \beta'\gamma''F^{e+c}$$

where  $\gamma'' = F^e\gamma'F^{-e}$  is a separable morphism  $G^{(p^{e+c})} \rightarrow G^{(p^e)}$ . Similarly, we have  $\alpha_1 = \alpha'\gamma''F^{e+c}$ . The definition of  $\ell(\alpha_1\beta_1^{-1})$  reads

$$(d_0\alpha'\gamma'')(d_0(\beta'\gamma''))^{-1} = (d_0\alpha')(d_0\gamma'')(d_0\gamma'')^{-1}(d_0\beta')^{-1} = (d_0\alpha')(d_0\beta')^{-1}.$$

This shows that the definitions of  $\ell$  on  $\alpha_1\beta_1^{-1}$  and on  $\alpha\beta^{-1}$  agree. More generally,  $\alpha\beta^{-1} = \alpha_1\beta_1^{-1}$  holds if and only if there exist nonzero  $\gamma, \delta \in \mathbb{E}$  such that  $\alpha\gamma = \alpha_1\delta$  and  $\beta\gamma = \beta_1\delta$ , and applying the above twice we find that  $\ell: R \rightarrow K$  is well-defined.

Second, to show that  $\ell$  is multiplicative, let  $r, r_1 \in R$ . If  $v(r) > 0$  or  $v(r_1) > 0$ , then  $v(rr_1) > 0$  and  $\ell(rr_1) = 0 = \ell(r)\ell(r_1)$ . So we may assume that  $v(r) = v(r_1) = 0$ . We may also write  $r$  and  $r_1$  with a common denominator:  $r = \alpha\beta^{-1}, r_1 = \alpha_1\beta^{-1}$  where  $v(\alpha) = v(\alpha_1) = v(\beta) =: e$ . Now find  $\gamma, \gamma_1 \in \mathbb{E} \setminus \{0\}$  such that  $\beta\gamma = \alpha_1\gamma_1$ , so that

$$s := (\alpha\beta^{-1})(\alpha_1\beta^{-1}) = (\alpha\gamma)(\beta\gamma_1)^{-1}$$

and also  $v(\gamma) = v(\gamma_1) =: c$ . Write  $\gamma = \gamma'F^c$  and  $\gamma_1 = \gamma'_1F^c$  and  $\alpha = \alpha'F^e$  and  $\alpha_1 = \alpha'_1F^e$  and  $\beta = \beta'F^e$  with  $\gamma', \gamma'_1 : G^{(p^c)} \rightarrow G$  and  $\alpha', \alpha'_1, \beta' : G^{(p^e)} \rightarrow G$  separable. Then we have, for the denominator of  $s$ ,

$$\beta\gamma_1 = \beta'F^e\gamma'_1F^c = \beta'\gamma''_1F^{e+c}$$

where  $\gamma''_1 = F^e\gamma'_1F^{-e} : G^{(p^{e+c})} \rightarrow G^{(p^e)}$  is separable. Similarly, for the numerator of  $s$ ,

$$\alpha\gamma = \alpha'\gamma''F^{e+c}$$

where  $\gamma'' = F^e\gamma'F^{-e} : G^{(p^{e+c})} \rightarrow G^{(p^e)}$  is separable. Now, by definition,

$$(2) \quad \ell(s) = (d_0\alpha'\gamma'')(d_0\beta'\gamma''_1)^{-1} = (d_0\alpha')(d_0\gamma'')(d_0\gamma''_1)^{-1}(d_0\beta')^{-1}$$

On the other hand, by a similar computation, the relation  $\beta\gamma = \alpha_1\gamma_1$  implies  $\beta'\gamma'' = \alpha_1\gamma''_1$ , so that

$$(d_0\beta')(d_0\gamma'') = (d_0\alpha'_1)(d_0\gamma''_1).$$

Writing this as  $d_0\gamma'' = (d_0\beta')^{-1}(d_0\alpha'_1)(d_0\gamma''_1)$  and substituting in (2) yields

$$\ell(s) = (d_0\alpha')(d_0\beta')^{-1}(d_0\alpha'_1)(d_0\beta')^{-1} = \ell(r)\ell(r_1),$$

as desired.

Third, for additivity of  $\ell$  we compute, still assuming  $r = \alpha\beta^{-1}, r_1 = \alpha_1\beta^{-1} \in R$  and notation as above, but no longer requiring  $v(r) = v(r_1) = 0$ ,

$$\ell(r + r_1) = \ell((\alpha + \alpha_1)\beta^{-1}) = d_0(\alpha' + \alpha'_1)(d_0\beta)^{-1} = (d_0\alpha' + d_0\alpha'_1)(d_0\beta)^{-1} = \ell(r) + \ell(r_1).$$

Finally,  $\ker \ell = \{r \in R \mid v(r) > 0\}$  follows directly from the definition. Since every element of  $R$  not in this ideal is invertible in  $R$ ,  $\text{im } \ell$  is a field.  $\square$

**4.4. The Lie algebra of a subgroup.** We return to the division ring  $Q$  generated by the endomorphism ring  $\mathbb{E}$  of a connected, one-dimensional algebraic group over  $K$ , equipped with the valuation from §4.1. Note that the residue field  $L$  here is commutative, since by Lemma 4.7,  $L$  embeds into the ground field  $K$  of our algebraic group  $G$ . We write  $\ell$  for the map  $R^n \rightarrow K^n$  defined by applying  $\ell$  component-wise. To prove Theorem 1.5 we need a description of the Lie algebra of a closed, connected subgroup  $X \subseteq G^n$  in terms of the right vector space representing it.

**Lemma 4.8.** *Let  $X \subseteq G^n$  be a closed, connected subgroup, let  $N = P^{-1}(X) \subseteq \mathbb{E}^n$  be the saturated right module representing it, and  $NQ$  the right subspace of  $Q^n$  generated by  $N$ . Let  $v$  be any vector spanning the one-dimensional space  $T_0G$ . Then we have*

$$T_0X = \langle \ell(NQ \cap R^n)v \rangle_K.$$

*Proof.* First,  $\dim_K T_0X = \dim X = \dim_Q NQ$  by Lemma 2.6. On the other hand, by Lemma 3.4 and the fact that  $\ell$  is just the reduction map followed by an embedding  $L \rightarrow K$ ,  $\dim_Q NQ = \dim_K \ell(NQ \cap R^n)$ . So the two spaces in the lemma have the same dimension. It therefore suffices to prove that the right-hand side is contained in the left-hand side. Since any finite set of elements in  $Q$  can be given common denominators, a general element of  $NQ \cap R^n$  is of the form  $\underline{\psi}\beta^{-1}$  with  $\beta \in \mathbb{E} \setminus \{0\}$  and  $\underline{\psi} \in N$ . Write  $\beta = \beta'F^e$  with  $e \in \mathbb{Z}_{\geq 0}$  and  $\beta' : G^{(p^e)} \rightarrow G$  separable, and write  $\psi_i = \psi'_i F^e$  where  $\psi'_i : G^{(p^e)} \rightarrow G$  is a not necessarily separable morphism. From  $\underline{\psi} \in N$  and  $\underline{\psi} = \underline{\psi}' \circ F^e$  and the fact that  $F^e : G \rightarrow G^{(p^e)}$  is surjective, it follows that  $\underline{\psi}'$  maps  $G^{(p^e)}$  into  $X$ . Hence  $d_0\underline{\psi}'$  maps  $T_0G^{(p^e)}$  into  $T_0X$ . On the other hand, by definition of  $\ell$  we have

$$\ell(\underline{\psi}\beta^{-1}) = (d_0\underline{\psi}')(d_0\beta')^{-1},$$

which, therefore, is a linear map  $T_0G \rightarrow T_0X$ , as desired.  $\square$

**4.5. Frobenius flocks of subgroups.** The last ingredient for Theorem 1.5 is the notion of Frobenius flock of a  $d$ -dimensional, closed, connected subgroup  $X$  of  $G^n$ . By Lemma 4.4 we can choose a uniformizer  $\pi$  of  $Q$  which is in fact an element of  $\mathbb{E}$ . For  $\alpha \in \mathbb{Z}_{\geq 0}^n$  and  $q \in G^n$  we write  $\pi^\alpha q := (\pi^{\alpha_1}(q), \dots, \pi^{\alpha_n}(q)) \in G^n$ . This determines an action of the additive monoid  $\mathbb{Z}_{\geq 0}^n$  on  $G^n$ , and  $\pi^\alpha X$  is a closed, connected subgroup of  $G^n$  for all  $\alpha \in \mathbb{Z}_{\geq 0}^n$  of dimension  $d$ .

We extend the definition of  $\pi^\alpha X$  to  $\alpha \in \mathbb{Z}^n$  as follows. Write  $\alpha = \beta - k(1, \dots, 1)$  where  $\beta \in \mathbb{Z}_{\geq 0}^n$  and  $k \in \mathbb{Z}_{\geq 0}$ . Then we let  $\pi^\alpha X$  be the connected component of 0 of the preimage of  $\pi^\beta X$  under the homomorphism  $\pi^{k(1, \dots, 1)} : G^n \rightarrow G^n$ . This preimage is clearly contained in the preimage of  $\pi^{\beta+(1, \dots, 1)} X$  under  $\pi^{(k+1)(1, \dots, 1)}$  and hence, since both preimages have dimension  $d$ , the connected components of 0 coincide, so  $\pi^\alpha X$  is independent of the choice of  $\beta$  as above. One readily checks that we have thus defined an action of  $\mathbb{Z}^n$  on the set of  $d$ -dimensional closed, connected subgroups of  $G^n$ .

**Definition 4.9.** The *Frobenius flock* of  $X \subseteq G^n$ , relative to  $\pi$ , is the collection of vector spaces  $(U_\alpha)_{\alpha \in \mathbb{Z}^n}$  defined by  $U_\alpha := T_0(\pi^{-\alpha} X) \subseteq (T_0G)^n$ .

In the case where  $G = \mathbb{G}_a$  and  $\pi = F$ , this notion coincides with the Frobenius flocks of [BDP18]. There,  $X$  was allowed to be an arbitrary irreducible closed subset of  $K^n$ , and consequently the base point at which we took the tangent spaces had

to be chosen somewhat carefully. In our current setting, where  $X$  is a subgroup, all points lead to equivalent Frobenius flocks, which is why we chose 0 as the base point. Also, in order to work with elliptic curves for which Frobenius is not an endomorphism, we allow  $\pi$  to be any endomorphism of valuation 1.

**4.6. Proof of Theorem 1.5.** The next proposition says that the Frobenius flock of  $X$  equals the linear flock of the corresponding right  $Q$ -subspace of  $Q^n$ , up to a natural identification. Recall that the residue field  $L$  of  $Q$  is a subfield of  $K$  via the homomorphism  $\ell$  from §4.3.

**Proposition 4.10.** *Let  $X \subseteq G^n$  be a closed, connected subgroup and  $N := P^{-1}(X) \subseteq \mathbb{E}^n$  the corresponding right module. Let  $v \in T_0G \setminus \{0\}$ . Let  $(V_\alpha)_\alpha$  be the  $L$ -linear flock of  $NQ$  and let  $(U_\alpha)_\alpha$  be the Frobenius flock of  $X$ . Then the map  $L^n \rightarrow (T_0G)^n, c = (c_1, \dots, c_n) \mapsto (\ell(c_1)v, \dots, \ell(c_n)v) = \ell(c)v$  induces a linear bijection  $(K \otimes_L V_\alpha) \rightarrow U_\alpha$  for each  $\alpha \in \mathbb{Z}^n$ .*

*Proof.* Let  $\alpha \in \mathbb{Z}^n$  and set  $Y := \pi^{-\alpha}X$ . A straightforward computation shows that  $P^{-1}(Y)Q = \pi^{-\alpha}NQ$ . By Lemma 4.8 applied to  $Y$ , we therefore have

$$U_\alpha = T_0Y = \langle \ell((\pi^{-\alpha}NQ) \cap R^n)v \rangle_K = (K \otimes_L \overline{(\pi^{-\alpha}NQ) \cap R^n})v = (K \otimes_L V_\alpha)v,$$

as desired.  $\square$

In what follows, we decompose  $\pi = \psi \circ F$  for some separable homomorphism  $\psi: G^{(p)} \rightarrow G$  and  $F$  the Frobenius map. Let  $h: G \dashrightarrow K$  be a rational function defined near 0 with  $h(0) = 0$  and such that  $d_0h: T_0G \rightarrow T_0K = K$  is nonzero, hence an isomorphism. Let  $h^{(p)}: G^{(p)} \dashrightarrow K$  be the Frobenius twist of  $h$ , i.e., the rational map making the diagram on the left commute:

$$\begin{array}{ccccc} & & \pi & & \\ & \curvearrowright & & \curvearrowleft & \\ G & \xrightarrow{F} & G^{(p)} & \xrightarrow{\psi} & G \\ \downarrow h & & \downarrow h^{(p)} & & \downarrow h \\ K & \xrightarrow{F} & K & & K \end{array} \quad \begin{array}{ccc} T_0G^{(p)} & \xrightarrow{d_0\psi} & T_0G \\ \downarrow d_0h^{(p)} & & \downarrow d_0h \\ K & \xlongequal{\quad} & K \end{array}$$

We want the diagram on the right, at the level of tangent spaces, to commute as well. *A priori*,  $d_0h^{(p)} = cd_0h \circ d_0\psi$  for some constant  $c \in K^*$ . Multiplying  $h$  by a scalar  $a \in K$ , the differential  $d_0h^{(p)}$  on the left side of the equation is multiplied by  $a^p$  and, on the right,  $d_0h$  is multiplied by  $a$ . Hence if we choose  $a$  such that  $a^{p-1} = 1/c$ , then we have the desired equality:

$$d_0h \circ d_0\psi = d_0h^{(p)}.$$

The mild conditions alluded to in Theorem 1.5 are as follows:

(\*\*)  $h: G \dashrightarrow K$  is defined near 0,  $d_0h \neq 0$ , and  $d_0h \circ d_0\psi = d_0h^{(p)}$ .

Applying the Frobenius twist to both sides, we obtain

$$d_0h^{(p)} \circ d_0\psi^{(p)} = d_0h^{(p^2)}$$

where  $\psi^{(p)}: G^{(p^2)} \rightarrow G^{(p)}$ . Combining the two formulas yields

$$d_0h \circ d_0\psi \circ d_0\psi^{(p)} = d_0h^{(p^2)}.$$

We abbreviate  $\psi \circ \psi^{(p)}$  to  $\psi^2$ . Then the above reads

$$d_0h \circ d_0\psi^2 = d_0h^{(p^2)}.$$

More generally, for each nonnegative integer  $k$ , writing  $\psi^k := \psi \circ \psi^{(p)} \circ \dots \circ \psi^{(p^{k-1})}$ , we have

$$d_0h \circ d_0\psi^k = d_0h^{(p^k)}.$$

Extending this component-wise to tuples we have

$$d_0h^n \circ d_0\psi^\alpha = d_0h^{(p^\alpha)} \text{ for all } \alpha \in \mathbb{Z}_{\geq 0}^n.$$

**Proposition 4.11.** *Set  $Y := \overline{h^n(X)}$  and assume that  $Y^{(p^\alpha)}$  is smooth at 0 for all  $\alpha \in \mathbb{Z}^n$ . Let  $(U_\alpha)_\alpha$  be the Frobenius flock of  $X$ , and for  $\alpha \in \mathbb{Z}^n$  set  $W_\alpha := T_0Y^{(p^\alpha)}$ . Then the matroid on  $[n]$  defined by  $W_\alpha$  equals the matroid defined by  $T_{F^\alpha y}Y^{(p^\alpha)}$  for  $y$  a general point in  $Y$ , and the Frobenius flock  $(W_\alpha)_\alpha$  of  $Y$  at 0 is the image of  $(U_\alpha)_\alpha$  under the linear isomorphism  $(d_0h)^n : T_0G^n \rightarrow T_0K^n$ .*

*Proof.* Since Frobenius flocks are uniquely determined by their restriction to the positive orthant, it suffices to prove both statements for  $\alpha \in \mathbb{Z}_{\geq 0}^n$ . For the last statement, consider the following two diagrams; here we have left out the obvious solid arrows between  $X, X^{(p^\alpha)}, \pi^\alpha X$  and between  $Y, Y^{(p^\alpha)}$  as well as the dashed arrows  $h^n : X \dashrightarrow Y$  and  $h^{(p^\alpha)} : X^{(p^\alpha)} \dashrightarrow Y^{(p^\alpha)}$ .

$$\begin{array}{ccccc}
 X & & X^{(p^\alpha)} & & \pi^\alpha X \\
 \downarrow \cap & & \downarrow \cap & & \downarrow \cap \\
 G^n & \xrightarrow{F^\alpha} & G^{(p^\alpha)} & \xrightarrow{\psi^\alpha} & G^n \\
 \downarrow h^n & & \downarrow h^{(p^\alpha)} & & \downarrow h^n \\
 K^n & \xrightarrow{F^\alpha} & K^n & & K^n \\
 \cup & & \cup & & \\
 Y & & Y^{(p^\alpha)} & & 
 \end{array}
 \quad
 \begin{array}{ccc}
 T_0G^{(p^\alpha)} & \xrightarrow{d_0\psi^\alpha} & T_0G^n \\
 \downarrow d_0h^{(p^\alpha)} & & \downarrow d_0h^n \\
 K^n & \xlongequal{\quad} & K^n
 \end{array}$$

The left-most diagram commutes by definition, and the right-most diagram commutes by the discussion above. So, by the left-most diagram,  $A := d_0h^{(p^\alpha)} \circ (d_0\psi^\alpha)^{-1}$  maps  $U_\alpha = T_0\pi^\alpha X$  into  $W_\alpha = T_0Y^{(p^\alpha)}$ , and by the right-most diagram  $A$  equals  $d_0h^n$ . This proves the last statement.

For the first statement, we will use the homogeneity of  $X$ . A general point  $y$  in  $Y$  has the same properties as 0:  $y$  is of the form  $h^n(x)$  for some  $x = (x_1, \dots, x_n) \in X$ ,  $d_{x_i}h$  is nonzero for each  $i$ , and  $d_x h^n$  is an isomorphism between  $T_x X$  and  $T_y Y$ . In that case, we have the commuting diagram of Figure 2, where all linear maps are isomorphisms and the right-most vertical map has a diagonal matrix relative to the standard basis. Consequently, the matroids represented by  $T_0Y$  and  $T_y Y$  are equal.  $\square$

## 5. EQUIVALENCE OF ALGEBRAIC REPRESENTATIONS

In our examples below we will need to characterize the algebraic representations of certain matroids, up to equivalence. Here we discuss briefly what this means. For this we go back to the original definition of algebraic matroids: let  $x_1, \dots, x_n$  be elements of an extension field  $L$  of our algebraically closed ground field  $K$ . In

$$\begin{array}{ccc}
 T_0 G^n & \xrightarrow{\quad} & K^n \\
 \downarrow \supseteq & \searrow^{d_0 h^n} & \downarrow \supseteq \\
 T_0 X & \xrightarrow{\quad} & T_0 Y \\
 \downarrow d_0 a_x & & \downarrow D \\
 T_x X & \xrightarrow{\quad} & T_y Y \\
 \downarrow \supseteq & \swarrow^{d_x h^n} & \downarrow \supseteq \\
 T_x G^n & \xrightarrow{\quad} & K^n
 \end{array}$$

$D = \text{diag} ((d_{x_i} h)(d_0 a_{x_i})(d_0 h)^{-1})_{i=1}^n$   
 $a_x : G^n \rightarrow G^n, g \mapsto x + g$   
 $a_{x_i} : G \rightarrow G, g \mapsto x_i + g$

FIGURE 2. The last commuting diagram in the proof of Proposition 4.11.

the matroid  $M$  on  $[n]$  determined by this data,  $I$  is independent if and only if the  $x_i, i \in I$  are algebraically independent over  $K$ . In the set-up of the introduction,  $L$  is the function field of  $X \subseteq K^n$  and the  $x_i$  are the coordinate functions. Clearly, if we enlarge  $L$ , the matroid remains the same, and if we add  $x'_1, \dots, x'_n \in L$  such that the algebraic closure of  $K(x_i)$  in  $L$  equals that of  $K(x'_i)$  for each  $i$ , then the corresponding elements  $i$  and  $i'$  are parallel. Thus, the matroid of the restriction to  $x'_1, \dots, x'_n$  is again  $M$ , and we call this algebraic realization *equivalent* to the original one.

In this section we will show that the Lindström valuations of equivalent algebraic representations differ only by a trivial valuation. This follows from a more general statement about valuations of matroids with parallel elements. We use the following lemma, which is a straightforward consequence of submodularity of matroid valuations.

**Lemma 5.1.** *Let  $v : \binom{E}{r} \rightarrow \mathbb{R} \cup \{\infty\}$  be a matroid valuation. Let  $S \in \binom{E}{r-2}$  and  $\{a, b, c, d\} \in \binom{E \setminus S}{4}$  be given. Then the minimum of*

$$\begin{aligned}
 &v(S \cup \{a, b\}) + v(S \cup \{c, d\}), \\
 &v(S \cup \{a, c\}) + v(S \cup \{b, d\}), \text{ and} \\
 &v(S \cup \{a, d\}) + v(S \cup \{b, c\})
 \end{aligned}$$

*is attained at least twice.* □

**Proposition 5.2.** *Let  $M$  be a matroid on  $E$ , and suppose  $i, j \in E$  are parallel in  $M$ . Let  $v$  be a valuation of  $M$ . Then there exists  $c_{i,j} \in \mathbb{R}$  such that*

$$v(S \cup \{i\}) - v(S \cup \{j\}) = c_{i,j}$$

*for all  $S \subseteq E \setminus \{i, j\}$  for which  $S \cup \{i\}$  (and hence also  $S \cup \{j\}$ ) is a basis of  $M$ .*

*Proof.* Suppose  $S, S'$  are such that

$$v(S \cup \{i\}) - v(S \cup \{j\}) \neq v(S' \cup \{i\}) - v(S' \cup \{j\}),$$

and  $|S \setminus S'|$  is minimal. Clearly  $S \neq S'$ . Using the basis exchange axiom of matroids, let  $a \in S \setminus S'$  and  $b \in S' \setminus S$  be given such that  $S \setminus \{a\} \cup \{b, i\}$  is a basis. Then

$$v(S \setminus \{a\} \cup \{b, i\}) - v(S \setminus \{a\} \cup \{b, j\}) = v(S' \cup \{i\}) - v(S' \cup \{j\})$$

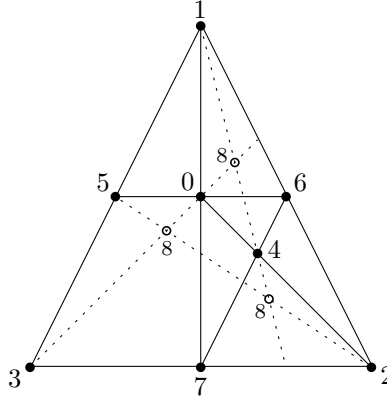


FIGURE 3. A matroid of rank 3 on 9 elements. A triple is collinear if and only if it is dependent in the matroid. The point 8 is the common intersection of the lines through  $\{0, 3\}$ ,  $\{1, 4\}$  and  $\{2, 5\}$ .

by minimality of  $|S \setminus S'|$ . Since  $i$  and  $j$  are parallel,  $v(S \setminus \{a\} \cup \{i, j\}) = \infty$ . By Lemma 5.1, we have

$$v(S \cup \{i\}) - v(S \cup \{j\}) = v(S \setminus \{a\} \cup \{b, i\}) - v(S \setminus \{a\} \cup \{b, j\}),$$

which is a contradiction.  $\square$

**Proposition 5.3.** *Let  $L \supseteq K$  be a field extension and let  $x_1, \dots, x_n, x'_1, \dots, x'_n \in L$  be elements. Suppose that, for each  $i$ , the algebraic closure of  $K(x_i)$  in  $L$  is the same as that of  $K(x'_i)$ , i.e., that the elements  $(x_1, \dots, x_n)$  and  $(x'_1, \dots, x'_n)$  determine equivalent algebraic representations of the same matroid  $M$ . Let  $\mu, \mu'$  be the Lindström valuations of these representations. Then there exists an  $\alpha \in \mathbb{R}^n$  such that*

$$\mu'(B) = \mu(B) + e_B^T \alpha \text{ for all bases } B \text{ of } M.$$

*Proof.* The tuple  $(x_1, \dots, x_n, x'_1, \dots, x'_n)$  is an algebraic representation of the matroid obtained from  $M$  by adding a parallel copy  $i'$  to each element  $i$ . Denote the Lindström valuation of this algebraic representation by  $v$ . From [Car18, Theorem 1] and multiplicativity of inseparable degree [Lan02, Cor. V.6.4], it follows that  $v$  restricts to  $\mu$  on the copy of  $[n]$  corresponding to  $x_1, \dots, x_n$  and to  $\mu'$  on the copy of  $[n]$  corresponding to  $x'_1, \dots, x'_n$ . Furthermore, by Proposition 5.2, for any basis  $\{i_1, \dots, i_r\}$  of  $M$ , we have

$$v(\{i_1, \dots, i_r\}) = v(\{i'_1, \dots, i'_r\}) + c_{i_1, i'_1} + \dots + c_{i_r, i'_r}.$$

Hence  $\mu$  and  $\mu'$  differ by the trivial valuation  $B \mapsto e_B^T \alpha$  with  $\alpha_i = c_{i, i'}$  for each  $i$ .  $\square$

## 6. EXAMPLES

**Example 6.1.** Consider the matroid  $M$  from Figure 3.

We construct a general matrix over a division ring  $S$  such that each dependent set of  $M$  is dependent in the matrix:

$$\Psi = \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \end{matrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & a \\ 1 & 0 & -1 \\ 1 & a & a \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & a & -1 \end{pmatrix},$$

where  $a \in K$  satisfies  $a^2 = -1$ . After choosing a basis and fixing row and column scalars, the remaining entries were chosen as freely as possible given the dependent triples of  $M$ . As it turns out, the only freedom that is left is the choice of  $a$ .

No assumptions on the characteristic or commutativity of  $S$  have been made at this point. If  $S$  has characteristic 2, then (among others) the rows corresponding to the basis  $\{3, 4, 5\}$  become dependent, so that  $\Psi$  cannot be a representation of  $M$ . So  $S$  must have characteristic  $\neq 2$ . If, for example,  $S = \mathbb{Q}(i)$  and  $a = i$ , then a subset of rows of  $\Psi$  is dependent if and only if it is dependent in  $M$ . Hence the column space of  $\Psi$  is a representation of  $M$  over  $\mathbb{Q}(i)$ .

Now suppose that  $K$  is a field of characteristic 2, and  $G$  is a connected one-dimensional algebraic group over  $K$ . Let  $X$  be a closed, connected subgroup of  $G^n$ , representing  $M$  algebraically. Then by Theorem 1.1, there is a linear representation of  $M$  over the endomorphism ring  $\mathbb{E}$  of  $G$ . Due to the above,  $M$  is not representable over  $\mathbb{Q}$ , nor over  $K(F)$ . Hence  $G$  cannot be either the additive or multiplicative group. So  $G$  must be an elliptic curve.

And indeed, for the supersingular elliptic curve  $G$  from Example 2.1,  $\mathbb{E}$  is isomorphic to the Hurwitz quaternions. So by taking  $a \in \mathbb{E}$  the element corresponding to  $i$ , we find that  $M$  is a matroid over the one-dimensional group  $G$ . To compute the Lindström valuation of this realization of  $M$ , we invoke Theorem 1.5 and Proposition 4.3(5), which says that the valuation  $v$  on  $\mathbb{E}$  maps  $\alpha$  to the 2-adic valuation of  $\alpha\bar{\alpha}$ . Then  $B \mapsto v(\det \Psi_B)$  is the corresponding Lindström valuation of  $M$ .

♣

**Example 6.2.** Let  $M$  be the non-Fano matroid. As is well-known,  $M$  is realizable over a division ring if and only if the characteristic is not 2, in which case there is a projectively unique realization, given by the rows of the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Nonetheless,  $M$  has algebraic realizations over a field of characteristic 2 using either the group  $G_m$  or an elliptic curve, both of whose endomorphism rings  $\mathbb{E}$  have characteristic 0.

If  $w$  denotes the Lindström valuation of one of these algebraic realizations, then, using Theorem 1.5 and Proposition 3.6, we can compute the following invariant:

$$\begin{aligned}\gamma(w) &:= w(\{4, 5, 6\}) - w(\{1, 2, 5\}) - w(\{1, 3, 6\}) - w(\{2, 3, 4\}) + 2w(\{1, 2, 3\}) \\ &= v(-2) - v(1) - v(-1) - v(1) + 2v(1) = v(2),\end{aligned}$$

where  $v$  is the valuation on  $\mathbb{E}$ . For each element of  $M$ , the sum of the coefficients of the valuations in which it appears in the definition of  $\gamma(w)$  is 0, and so  $\gamma$  is invariant under adding trivial valuations. By the classification of the valuations in Proposition 4.3,  $\gamma(w)$  is either 2 if the algebraic group  $G$  is a supersingular elliptic curve or 1 otherwise.

Moreover, we claim that by results in [EH91], every algebraic realization of  $M$  is equivalent to an  $\mathbb{E}$ -linear realization, and so by Proposition 5.3,  $\gamma(w)$  is either 1 or 2 for the Lindström valuation  $w$  on any algebraic realization of  $M$ . Indeed, [EH91, Thm. 2.1.2] states that any algebraic realization of the matroid  $M(K_4)$  of the complete graph on 4 vertices is equivalent to an  $\mathbb{E}$ -linear realization. The deletion of the 6th element of  $M$  is isomorphic to  $M(K_4)$ , and therefore in any algebraic realization of  $M$ , the elements other than the 6th are equivalent to an  $\mathbb{E}$ -linear realization. More specifically, if  $L$  is an algebraically closed field extension of  $K$  and  $x_1, \dots, x_7 \in L$  have the algebraic dependencies over  $K$  specified by  $M$ , then there exists a connected, one-dimensional algebraic group  $G$ , a connected subgroup  $X \subseteq G^7$ , and an embedding  $K(X) \rightarrow L$  that, for each  $i \in \{1, \dots, 5, 7\}$ , maps the  $i$ -th coordinate function to an element  $x'_i \in L$  such that the algebraic closures  $\overline{K(x_i)}$  and  $\overline{K(x'_i)}$  in  $L$  coincide. Now let  $x'_6 \in L$  be the image of the 6th coordinate. The fact that the rank-two flats in  $M$  spanned by 1,7 and by 2,3 intersect precisely in 7 implies that

$$\overline{K(x'_6)} = \overline{K(x'_1, x'_7)} \cap \overline{K(x'_2, x'_3)} = \overline{K(x_1, x_7)} \cap \overline{K(x_2, x_3)} = \overline{K(x_6)};$$

this proves the claim.

In conclusion, scaling the valuation on  $M$  coming from the  $G_m$ -realization by a positive integer yields infinitely many valuations, of which exactly two are realizable as the Lindström valuation of an algebraic realization over a field of characteristic 2. In contrast, all of these scaled valuations are realizable by Frobenius flocks over  $\mathbb{F}_2$  by scaling the original Frobenius flock.  $\clubsuit$

We can now prove the last of the results from the introduction. We refer to [DW92] for contractions, restrictions, and duality of matroid valuations.

*Proof of Theorem 1.6.* We use the universality construction in [EH91, Lem. 3.4.1] to construct the dual matroid  $M^*$ , from the following system of equations in  $p^3$



non-commuting variables  $u, y_0, \dots, y_{p^3-2}$ :

$$(3) \quad \begin{aligned} y_1 &= uy_0 \\ y_2 &= uy_1 \\ &\vdots \\ y_{p^3-2} &= uy_{p^3-3} \\ y_0 &= uy_{p^3-2} \\ y_p &= y_0u \end{aligned}$$

Then, by [EH91, Lem. 3.4.1], there exists a matroid  $M^*$  such that any algebraic realization of  $M^*$  is equivalent to a realization by a closed, connected subgroup  $Y \subset G^n$  for some one-dimensional algebraic group  $G$ . Moreover, setting  $\mathbb{E} := \text{End}(G)$  and letting  $Q$  be the division ring generated by  $\mathbb{E}$ , that subgroup realization corresponds to an assignment of distinct values from  $Q$  to the variables  $u, y_0, \dots, y_{p^3-2}$  such that the equations (3) are satisfied; and any such choice yields a subgroup realization. We now assume that we have such a realization and study the solutions in an endomorphism ring  $\mathbb{E}$  of some one-dimensional group.

In particular, we have  $y_i = u^i y_0$  for all  $i$ , and, by the second to last equation,  $y_0 = uy_{p^3-2} = u^{p^3-1} y_0$ , which means that  $u$  is a  $(p^3 - 1)$ -root of unity, and since the  $y_i$  are distinct,  $u$  is a primitive  $(p^3 - 1)$ -root of unity. Over  $\mathbb{Q}$ , primitive  $(p^3 - 1)$ -roots of unity have degree at least 6, but all elements in the endomorphism rings of  $\mathbb{G}_m$  and of elliptic curves have degree at most 2 over  $\mathbb{Q}$ . Therefore, any  $\mathbb{E}$ -linear realization of  $M^*$  comes from  $G = \mathbb{G}_a$  and  $\mathbb{E} = K[F]$ , and  $u$  is an element of  $\mathbb{F}_{p^3} \setminus \mathbb{F}_p$ . In addition, the last equation of (3) gives  $y_0 u = y_p = u^p y_0$ .

Now, consider the semidirect product  $K^* \rtimes \mathbb{Z}$ , where the generator of  $\mathbb{Z}$  acts on  $K^*$  by the Frobenius automorphism, and let  $\mu$  denote the homomorphism from the monoid  $(K[F] \setminus \{0\}, \cdot)$  to  $K^* \rtimes \mathbb{Z}$  defined by

$$\mu\left(\sum_{i=0}^d a_i F^i\right) = (a_d, d),$$

where  $d$  is chosen so that  $a_d$  is non-zero. Note that the valuation on  $K[F]$  is the projection of  $\mu$  onto the second coordinate. Since  $K^* \rtimes \mathbb{Z}$  is a group,  $\mu$  extends uniquely to a group homomorphism  $\mu: Q^* \rightarrow K^* \rtimes \mathbb{Z}$ , where  $Q^*$  is the division ring generated by  $\mathbb{E} = K[F]$ . Applying  $\mu$  to the equation  $y_0 u = u^p y_0$ , and using  $(a, d)$  to denote  $\mu(y_0)$ , we have:

$$\begin{aligned} (a, d) \cdot (u, 0) &= (u^p, 0) \cdot (a, d) \\ (au^{p^d}, d) &= (u^p a, d) \end{aligned}$$

Since  $K^*$  is commutative,  $u^{p^d} = u^p$ . Also,  $u$  is in  $\mathbb{F}_{p^3} \setminus \mathbb{F}_p$ , so the action of Frobenius on  $u$  has order 3, and so this means that  $d = v(y_0) \equiv 1 \pmod{3}$ .

The construction of  $M^*$  in [EH91, Lem. 3.4.1] represents the variable  $y_0$  as a cross-ratio, meaning that there are 4 elements in  $M^*$  (denoted  $x_0, x_\infty, x_1$ , and  $y_0$  in the proof there but denoted 1, 2, 3, 4 here) such that any  $Q$ -realization of  $M^*$  is

equivalent to one whose restriction to these 4 elements is:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & y_0 \end{pmatrix},$$

whose matroid is the uniform matroid  $U_{2,4}$ . By Proposition 3.6, the restriction of the Lindström valuation to this  $U_{2,4}$ , denoted  $w^*$ , satisfies:

$$(4) \quad \begin{aligned} w^*({1,4}) + w^*({2,3}) - w^*({1,3}) - w^*({2,4}) = \\ v(y_0) + v(-1) - v(1) - v(-1) = v(y_0), \end{aligned}$$

as does any valuation that differs from  $w^*$  by a trivial valuation.

We now construct a realization of the matroid  $M$  dual to  $M^*$ . First, we can construct a  $K[F]$ -realization of  $M^*$  by choosing  $u$  to be an element of  $\mathbb{F}_{p^3} \setminus \mathbb{F}_p$ ,  $y_i = u^i F$  for  $i = 1, \dots, p^3 - 2$ . Then, by Theorem 1.2,  $M$  also has a  $K[F]$ -realization, which is constructed by taking the orthogonal complement of the realization of  $M^*$ —this orthogonal complement is a left  $Q$ -vector space—and applying the anti-isomorphism  $\tau$  which sends  $F$  to  $F^{-1}$ . In particular, the contraction of all of  $M$  except the elements  $1, \dots, 4$  from the previous paragraph has the realization:

$$\begin{pmatrix} -1 & -1 \\ -1 & -F^{-1} \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Again, using Proposition 3.6 to compute the valuation  $w$  on this realization, we have:

$$w({1,4}) + w({2,3}) - w({1,3}) - w({2,4}) = v(-1) + v(F^{-1}) - v(1) - v(-1) = -1$$

Therefore, if  $w^*$  is the dual valuation of  $w$ , defined by  $w^*(B) = w({1,2,3,4} \setminus B)$ , then it satisfies:

$$w^*({2,3}) + w^*({1,4}) - w^*({2,4}) - w^*({1,3}) = -1.$$

This valuation is not the Lindström valuation of an algebraic realization by (4) and the requirement that  $v(y_0) \equiv 1 \pmod{3}$ .  $\square$

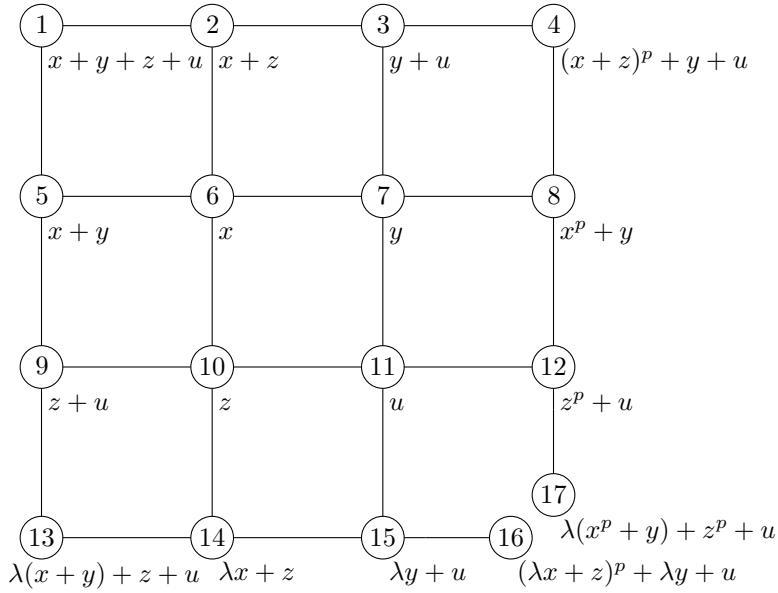


FIGURE 4. An algebraic matroid in  $K(x, y, z, u)$  [Lin86a].

**Example 6.3.** We take  $G = \mathbb{G}_a$  over any field of positive characteristic  $p$ , and let  $\lambda$  be any element of  $K \setminus \mathbb{F}_p$ . Then,  $N$  will be given by the matrix

$$\begin{array}{c}
 x \quad y \quad z \quad u \\
 \begin{array}{l}
 1 \\
 2 \\
 3 \\
 4 \\
 5 \\
 6 \\
 7 \\
 8 \\
 9 \\
 10 \\
 11 \\
 12 \\
 13 \\
 14 \\
 15 \\
 16 \\
 17
 \end{array}
 \begin{pmatrix}
 1 & 1 & 1 & 1 \\
 1 & 0 & 1 & 0 \\
 0 & 1 & 0 & 1 \\
 F & 1 & F & 1 \\
 1 & 1 & 0 & 0 \\
 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 \\
 F & 1 & 0 & 0 \\
 0 & 0 & 1 & 1 \\
 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 1 \\
 0 & 0 & F & 1 \\
 \lambda & \lambda & 1 & 1 \\
 \lambda & 0 & 1 & 0 \\
 0 & \lambda & 0 & 1 \\
 \lambda F & \lambda & F & 1 \\
 F\lambda & \lambda & F & 1
 \end{pmatrix}
 \end{array}$$

The first fifteen rows of this matrix can be obtained by interpreting the field elements in [Lin86a, Fig. 1] as group homomorphisms from  $\mathbb{G}_a^4$  to  $\mathbb{G}_a$ . In addition,  $N$

arises as a sort of Kronecker product of the matrices

$$N_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ \lambda & 1 \end{pmatrix} \quad \text{and} \quad N_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ F & 1 \end{pmatrix},$$

with the bottom row duplicated to have both possible ways of multiplying the bottom left elements  $\lambda$  and  $F$  of the matrices.

Then the matroid  $M$  for  $N$  is depicted in Figure 4, where the lines denote the rank 2 flats, each of which arise from fixing one row in either  $N_1$  or  $N_2$ . The matroid  $M$  is not linear over any field, but is linear over any non-commutative division ring. Indeed, the matrix  $N$  defines the same matroid if  $\lambda$  and  $F$  are any pair of non-commuting elements in any division ring, which they are in the endomorphism ring of  $\mathbb{G}_a$ , since we required that  $\lambda^p \neq \lambda$ . This implies, for instance, that the submatrix in rows 8, 12, 14, 15 has full rank, which it would not have if  $\lambda$  and  $F$  commuted. Since  $M$  is linear over the endomorphism ring of  $\mathbb{G}_a$  in any positive characteristic, it is algebraic over any field of positive characteristic. Many restrictions of  $M$  are also not linear over any field, such as the restriction to  $\{1, 4, 7, 8, 10, 11, 13, 14\}$ , which appears in [Ing71] and [Lin86a]. The restriction to  $\{3, 4, 7, 8, 9, 10, 13, 14\}$  appears in [Lin85, Fig. 3], where it is incorrectly said not to be realizable over a division ring, but an algebraic realization over  $\mathbb{F}_2$  is nonetheless given. ♣

#### REFERENCES

- [BB19] Matthew Baker and Nathan Bowler. Matroids over partial hyperstructures. *Adv. Math.*, 343:821–863, 2019.
- [BDP18] Guus P. Bollen, Jan Draisma, and Rudi Pendavingh. Algebraic matroids and Frobenius flocks. *Adv. Math.*, 323:688–719, 2018.
- [Bol18] Guus Pieter Bollen. *Frobenius Flocks and Algebraicity of Matroids*. PhD thesis, Eindhoven University of Technology, 2018. Available online at <https://research.tue.nl/>.
- [Bor91] Armand Borel. *Linear algebraic groups. 2nd enlarged ed.* New York etc.: Springer-Verlag, 2nd enlarged ed. edition, 1991.
- [Car18] Dustin Cartwright. Construction of the Lindström valuation of an algebraic extension. *J. Comb. Theory, Ser. A*, 157:389–401, 2018.
- [CGP10] Brian Conrad, Ofer Gabber, and Gopal Prasad. *Pseudo-reductive groups*. Cambridge: Cambridge University Press, 2010.
- [Coh95] P. M. Cohn. *Skew fields. Theory of general division rings.*, volume 57. Cambridge: Cambridge Univ. Press, 1995.
- [DD18] Alessio D’Alì and Emanuele Delucchi. Stanley-Reisner rings for symmetric simplicial complexes,  $g$ -semimatroids and abelian arrangements. 2018. Preprint, [arXiv:1804.07366](https://arxiv.org/abs/1804.07366).
- [DM13] Michele D’Adderio and Luca Moci. Arithmetic matroids, the Tutte polynomial and toric arrangements. *Adv. Math.*, 232(1):335–367, 2013.
- [DP05] C. De Concini and C. Procesi. On the geometry of toric arrangements. *Transform. Groups*, 10(3-4):387–422, 2005.
- [DP19] Emanuele Delucchi and Roberto Pagaria. The homotopy type of elliptic arrangements. 2019. Preprint, 1911.02905.
- [DW92] Andreas W. M. Dress and Walter Wenzel. Valuated matroids. *Adv. Math.*, 93(2):214–250, 1992.
- [EH91] David M. Evans and Ehud Hrushovski. Projective planes in algebraically closed fields. *Proc. London Math. Soc.*, s3-62(1):1–24, 1991.
- [FM19] Alex Fink and Luca Moci. Polyhedra and parameter spaces for matroids over valuation rings. *Adv. Math.*, 343:448–494, 2019.
- [Hus04] Dale Husemöller. *Elliptic curves. With appendices by Otto Forster, Ruth Lawrence, and Stefan Theisen. 2nd ed.*, volume 111. New York, NY: Springer, 2nd ed. edition, 2004.

- [Ing71] A.W. Ingleton. Representation of matroids. *Combinat. Math. Appl., Proc. Conf. math. Inst., Oxford 1969*, 149–167, 1971.
- [Lan02] Serge Lang. *Algebra*. Number 211 in Graduate Texts in Mathematics. Springer, rev. 3rd ed edition, 2002.
- [Lin85] Bernt Lindström. On the algebraic representations of dual matroids. Technical Report 5, Department of Math., Univ. of Stockholm, 1985.
- [Lin86a] Bernt Lindström. A non-linear algebraic matroid with infinite characteristic set. *Discrete Math.*, 59(3):319–320, 1986.
- [Lin86b] Bernt Lindström. The non-Pappus matroid is algebraic over any finite field. *Utilitas Math.*, 30:53–55, 1986.
- [Lin88] Bernt Lindström. On  $p$ -polynomial representations of projective geometries in algebraic combinatorial geometries. *Math. Scand.*, 63(1):36–42, 1988.
- [Pen18] Rudi Pendavingh. Field extensions, derivations, and matroids over skew hyperfields. 2018. Preprint, arXiv:1802.02447.
- [RST19] Zvi Rosen, Jessica Sidman, and Louis Theran. Algebraic matroids in action. *Am. Math. Mon.*, 2019. To appear, arXiv:1809.00865.
- [Sch45] O. F. G. Schilling. Noncommutative valuations. *Bull. Amer. Math. Soc.*, 51(4):297–304, 1945.
- [Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves. 2nd ed.*, volume 106. New York, NY: Springer, 2nd ed. edition, 2009.
- [Voi18] John Voight. *Quaternion algebras*. 2018. <https://math.dartmouth.edu/~jvoight/quat.html>, online book, v.0.9.14.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, EINDHOVEN UNIVERSITY OF TECHNOLOGY, P.O. BOX 513, 5600 MB, EINDHOVEN, THE NETHERLANDS  
*E-mail address:* `g.p.bollen@tue.nl`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TENNESSEE, 227 AYRES HALL, KNOXVILLE, TN 37996-1320, USA  
*E-mail address:* `cartwright@utk.edu`

MATHEMATISCHES INSTITUT, UNIVERSITÄT BERN, SIDLERSTRASSE 5, 3012 BERN, SWITZERLAND; AND DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, EINDHOVEN UNIVERSITY OF TECHNOLOGY, P.O. BOX 513, 5600 MB EINDHOVEN, THE NETHERLANDS  
*E-mail address:* `jan.draisma@math.unibe.ch`