8-2022

DVR-Matroids of Algebraic Extensions

Anna L. Lawson
University of Tennessee, Knoxville, alitchfo@vols.utk.edu

To the Graduate Council:

I am submitting herewith a dissertation written by Anna L. Lawson entitled "DVR-Matroids of Algebraic Extensions." I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

Dustin A. Cartwright, Major Professor

We have read this dissertation and recommend its acceptance:

Dustin Cartwright, Luis Finotti, Marie Jameson, Michael Berry

Accepted for the Council:

Dixie L. Thompson

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

To the Graduate Council:
I am submitting herewith a dissertation written by Anna Lea Lawson entitled "DVR-Matroids of Algebraic Extensions." I have examined the final paper copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

_____
Dustin Cartwright, Major Professor

We have read this dissertation
and recommend its acceptance:

_____
Marie Jameson

_____
Luis Finotti

_____
Michael Berry

_____
Dustin Cartwright

Accepted for the Council:

_____
Dixie L. Thompson
Vice Provost and Dean of the Graduate School

To the Graduate Council:
I am submitting herewith a dissertation written by Anna Lea Lawson entitled "DVR-Matroids of Algebraic Extensions." I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

Dustin Cartwright, Major Professor

We have read this dissertation
and recommend its acceptance:

Marie Jameson

Luis Finotti

Michael Berry

Dustin Cartwright

Accepted for the Council:

Dixie L. Thompson

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

DVR-Matroids of Algebraic Extensions

A Dissertation Presented for the

Doctor of Philosophy

Degree

The University of Tennessee, Knoxville

Anna Lea Lawson

August 2022

Acknowledgements

I would like to thank my research advisor Dr. Dustin Cartwright for the support as I worked on this project and for the many hours of meetings over the years. I would also like to thank my parents for the constant encouragement as I prepared for every test and presentation throughout graduate school.

Abstract

A matroid is a finite set E along with a collection of subsets of E, called independent sets, that satisfy certain conditions. The most well-known matroids are *linear matroids*, which come from a finite subset of a vector space over a field K. In this case the independent sets are the subsets that are linearly independent over K. Algebraic matroids come from a finite set of elements in an extension of a field K. The independent sets are the subsets that are algebraically independent over K. Any linear matroid has a representation as an algebraic matroid, but the converse is not true [7]. One tool that helps us better understand algbraic matroids is the Lindström valuation which is defined on basis sets of a matroid. This valuation is explicitly defined in [3].

In Chapter 2, we will show that the Lindström valuated matroid can be further refined to a DVR-matroid, or matroid over a discrete valuation ring as defined in [5]. In Chapter 3, we focus on a class of examples of algebraic matroids that come from homomorphisms of algebraic groups. We show that the d-vectors for the corresponding DVR-matroid can be computed in two different ways.

Table of Contents

Chapter 1

Introduction

In this chapter, we will present background information on matroids, including two of many equivalent definitions of a matroid, and discuss their connection to linear algebra.

1.1 Basic Definitions

In this section, we will introduce essential definitions that will be used throughout this thesis.

Definition 1.1.1. A *matroid* M is a pair $(E, \mathcal{I})$ consisting of a finite set E and a collection of subsets of E satisfying

(i) $\mathcal{I}$ is non-empty.

(ii) Every subset of every member of $\mathcal{I}$ is also in $\mathcal{I}$.

(iii) If X and Y are in $\mathcal{I}$ and $\big|X\big| = \big|Y\big| + 1$, then there is an element x in $X \setminus Y$ such that $Y \cup \{x\}$ is in $\mathcal{I}$.

The set E is called the *ground set* and the members of $\mathcal{I}$ are called *independent sets*. Maximal independent sets are called *bases*.

As suggested by the terminology, matroids generalize the concept of linear independence of vectors in vector spaces. Property (iii) is analogous to the Steinitz Exchange Lemma, and it follows that for any $A \subseteq E$, all maximal independent subsets of A have the same cardinality. So, all bases of a matroid have the same cardinality, just like bases in a vector space.

Definition 1.1.2. Let M be a matroid on the ground set E. The *rank function* $r : 2^E \to \mathbb{Z}_{\geq 0}$ on M is the function that maps $A \subseteq E$ to the size of a maximal independent subset of A.

We call the rank of the ground set E the *rank of the matroid* which is analogous to the dimension of a vector space, and we can equivalently define a matroid in terms of a rank function.

Proposition 1.1.3. [8, Theorem 1.3.2] Let M be a matroid on the ground set E, and let $r : 2^E \to \mathbb{Z}_{\geq 0}$ be the rank function. Then the independent sets of M are the subsets $I \subseteq E$ for which $r(I) = \big|I\big|$, and r satisfies the following:

(i) We have $r(A) \leq \big|A\big|$ for every $A \subseteq E$.

(ii) If $A \subseteq B \subseteq E$, then $r(A) \leq r(B)$.

(iii) For any $A, B \subseteq E$, we have $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Moreover, if E is a set and $r : 2^E \to \mathbb{Z}_{\geq 0}$ is a function satisfying the above conditions, then r determines a matroid on E.

One class of matroids comes from linear independence of column vectors of a matrix over some given field. We call matroids that can be represented this way *linear matroids*. An example of a linear matroid is given below.

Example 1.1.4. [8, Example 1.1.2] Consider the following matrix over the field $\mathbb{R}$.

$$\psi = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Let $E = \{1, 2, 3, 4, 5\}$, and let $\mathcal{I} \subseteq 2^E$ be the collection of subsets $A \subseteq E$ such that the column vectors with indices in A are linearly independent over $\mathbb{R}$. Then $\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{4\}, \{5\}, \{1, 2\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{4, 5\}\}$, and $(E, \mathcal{I})$ is a matroid.

Definition 1.1.5. Let M be a matroid with ground set E.

(i) For $e \in E$, the *deletion* of e is a matroid on the ground set $E \setminus \{e\}$ where the independent sets are the independent sets in M that do not contain e.

(ii) For $e \in E$, the *contraction* of M by e is a matroid on the ground set $E \setminus \{e\}$. If $\{e\}$ is independent in M, the independent sets are subsets $I \subseteq E$ such that $I \cup \{e\}$ is independent in M. If $\{e\}$ is dependent in M, the independent sets coincide with the independent sets of M.

In terms of linear algebra, deletion is analogous to removing one vector from a finite list of vectors and restricting to the subspace spanned by the remaining vectors. Contraction is analogous to quotienting out by the span of a vector.

1.2 Valuated Matroids

As discussed in the previous section, given an $m \times n$ matrix A over a field K, we can obtain a linear matroid M on the ground set $E = \{1, \ldots, n\}$. The independent sets are the subsets of E for which the corresponding column vectors are linearly independent over K. If K has valuation $\nu : K \setminus \{0\} \to \mathbb{R}$, we can define a function ν' that maps each basis B of M to $\nu(\det A_B)$, where A_B is the submatrix of A that contains only the columns corresponding to B.

If A' is a matrix obtained from A by elementary row or column operations, the linear matroid of A' is equivalent to the matroid of A. The value of ν' on each basis is shifted by a constant (equal to the valuation of the determinant of the invertible matrix P for which $PA = A'$). First introduced in [4], the following definition generalizes this idea.

Definition 1.2.1. For a matroid M on the ground set E, a *matroid valuation* on M is a function ν from the set of bases of M into $\mathbb{R}$ such that for all pairs of bases B and B' with $i \in B \setminus B'$, there exists a $j \in B' \setminus B$ so that if $B - i + j$ and $B' + i - j$ are bases and

$$\nu(B) + \nu(B') \geq \nu(B - i + j) + \nu(B' + i - j).$$

We consider matroid valuations ν and μ to be equivalent if there exists $\lambda \in \mathbb{R}$ such that $\nu(B) = \mu(B) + \lambda$ for every basis B. If ν is a matroid valuation on M, then we call the pair $(M, [\nu])$ a *valuated matroid*, where $[\nu]$ is the equivalence class of ν.

Since shifting a matroid valuation by a constant results in an equivalent matroid valuation, the function described in the first paragraph does not depend on the matrix representation of the vector configuration.

1.3 Algebraic Matroids

Definition 1.3.1. Let L/K be a finite extension of fields, and let $x_1, x_2, \ldots, x_n \in L$. and, let $E = \{1, 2, \ldots, n\}$. For $A \subseteq E$, define $x_A = \{x_i : i \in A\}$, and define $\mathcal{I} \subseteq 2^E$ as follows:

$$\mathcal{I} = \{A \subseteq E : x_A \text{ is algebraically independent over } K\}$$

Then $\mathcal{I}$ satisfies the properties in Definition 1.1.1 so that $(E, \mathcal{I})$ is a matroid, called the *algebraic matroid of L/K associated to $x_1, \ldots, x_n$*.

In general, every linear matroid has an algebraic representation. Over fields of characteristic 0, the converse also holds. That is, every algebraic matroid over a field K of characteristic 0 has a linear representation over an algebraic closure of K. However, over a field of characteristic $p > 0$, there are algebraic matroids that are not linear [7].

In [2], a matroid flock is defined to be a collection of matroids for which all deletions and contractions satisfy certain conditions. They define an associated matroid, called

the *support matroid*, and show that a valuated matroid is equivalent to a matroid flock. They then define a specific flock of linear matroids, called the *Frobenius flock*, for which the support matroid is the algebraic matroid of the field extension. They call the equivalent valuated matroid the *Lindström valuated matroid.* A direct construction of this valuated matroid is given in [3]. This definition is given below.

Definition 1.3.2. [3] Let K be an algebraically closed field of characteristic $p > 0$, and let L be a finite extension of $K(x_1, \ldots, x_n)$. The *Lindström valuation* (up to equivalence) of the algebraic matroid of this field extension is given by

$$\nu(B) = \log_p[L : K(x_B)^{\text{sep}}]$$

for every basis B, where $K(x_B)^{\text{sep}}$ denotes the elements of L which are separable over $K(x_B)$.

Chapter 2

DVR-Matroids

In this chapter, given a finite field extension L of $K(x_1, \ldots, x_n)$, we construct a matroid over a discrete valuation ring, as defined in [5]. In order to accomplish this, we make use of an equivalence of matroids over a discrete valuation ring with functions mapping subsets of the ground set E to sequences of integers satisfying set conditions [5, Proposition 5.4]. We will now call a pair (E, d) of a ground set E and a function satisfying these conditions a *DVR-matroid*, and we will show that a matroid with valuation that arises from this construction is equal to the algebraic matroid of the field extension, along with the Lindström valuation. For the entirety of this chapter, we will assume that K is an algebraically closed field of characteristic $p > 0$, and L is a finite extension of $K(x_1, \ldots, x_n)$.

2.1 Matroids Over a Ring

In [5], Fink and Moci introduced the concept of a matroid over a commutative ring R. It is defined as follows:

Definition 2.1.1. Let R be a commutative ring and let R_{mod} be the set of finitely generated R-modules. Let E be a finite set (called the *ground set*), and let

$M : 2^E \to R_{\text{mod}}$ be a function. We call the pair (E, M) a *matroid over* R if for every $A \subseteq E$ and $b, c \in E$, there exist $x, y \in M(A)$ satisfying the following conditions:

(i) $M(A \cup \{b\}) \cong M(A)/(x)$

(ii) $M(A \cup \{c\}) \cong M(A)/(y)$

(iii) $M(A \cup \{b, c\}) \cong M(A)/(x, y)$

Two matroids over a ring, M_1 and M_2, are considered to be the same if $M_1(A) \cong M_2(A)$ for every $A \subseteq E$. If R is a field and $M(E)$ is trivial, then the function $A \mapsto \big|E\big| - \dim M(A)$ satisfies the conditions of a rank function. Hence, we obtain a classical matroid in this case [5, Proposition 2.6].

If R is a discrete valuation ring, then finitely generated R-modules can be written as a direct sum of cyclic R-modules, each isomorphic to either to R or R/m^n for some $n \in \mathbb{N}$. Thus, we have a bijection between finitely generated R-modules (up to isomorphism) and non-increasing sequences of nonnegative integers. The bijection maps a finitely generated R-module N to the sequence $\big(\text{len}(m^{i-1}N/m^iN)\big)_{i=1}^{\infty}$, where $\text{len}(m^{i-1}N/m^iN)$ is the maximum length of a chain of submodules of $m^{i-1}N/m^iN$ [5, Proposition 5.1]. The i^{th} entry is equal to the number of summands in the decomposition of N that are either free or isomorphic to R/m^n with $n \geq i$. The conditions in Definition 2.1.1 are characterized by conditions on these sequences in [5, Proposition 5.4], inspiring the following definition.

Definition 2.1.2. A *DVR-matroid* is a finite set E together with a function d assigning to each $A \subseteq E$ a non-increasing sequence of nonnegative integers $d(A) = (d_1(A), d_2(A), \dots)$ satisfying the following properties:

(L1) For any $A \subseteq E$ and $b \in E \setminus A$, $d_i(A) - d_i(A \cup \{b\})$ is either 0 or 1 for each $i \geq 1$.

(L2) For any $A \subseteq E$ and $b, c \in E \setminus A$, and $n \geq 1$

$$d_{\leq n}(A) - d_{\leq n}(A \cup \{b\}) - d_{\leq n}(A \cup \{c\}) + d_{\leq n}(A \cup \{b, c\}) \geq 0, \tag{L2a}$$

where $d_{\leq n}(A) = \sum_{i=1}^{n} d_i(A)$. In addition, for any $n \geq 1$ such that $d_n(A \cup \{b\}) \neq d_n(A \cup \{c\})$, equality holds, meaning:

$$d_{\leq n}(A) - d_{\leq n}(A \cup \{b\}) - d_{\leq n}(A \cup \{c\}) + d_{\leq n}(A \cup \{b, c\}) = 0 \tag{L2b}$$

The conditions a DVR-matroid satisfies are labeled to match Proposition 5.4 in [5]. The reason for this is that this definition makes use of an equivalence of DVR-matroids with certain matroids over a discrete valuation ring.

Proposition 2.1.3. [5, Proposition 5.4] Let E be a finite set. A DVR-matroid (E, d) is equivalent to a matroid over a discrete valuation ring whose residue field has more than 2 elements.

If (E, d) is a DVR-matroid with $\lim_{i\to\infty} d_i(E) = 0$, then we can obtain an ordinary matroid M on E of rank $r = \lim_{i\to\infty} d_i(\emptyset)$ by defining the rank function $r : 2^E \to \mathbb{Z}_{\geq 0}$ to be $r(A) = r - \lim_{i\to\infty} d_i(A)$. The bases of M are the subsets B of size r such that $d_i(B) = 0$ for sufficiently large i. Furthermore, the function $\sigma(B) = \sum_i d_i(B)$ where B is a basis defines a matroid valuation on M [5, Corollary 5.9].

2.2 The DVR-Matroid of an Algebraic Extension

Given a finite field extension L of $K(x_1, \ldots, x_n)$, where K is an algebraically closed field of characteristic $p > 0$, we now define a function d that maps subsets of $E = \{1, \ldots, n\}$ to non-increasing sequences of nonnegative integers. For $A \subseteq \{1, \ldots, n\}$, we denote the extension of K generated by $\{x_i : i \in A\}$ by $K(x_A)$.

Definition 2.2.1. Let L be a finite field extension of $K(x_1, \ldots, x_n)$, with K algebraically closed. For each $i \in \mathbb{N}$ and $A \subseteq \{1, \ldots, n\}$, define

$$d_i(A) = \log_p \left[L^{p^{i-1}} K(x_A) : L^{p^i} K(x_A) \right].$$

Define $d(A)$ to be the sequence $(d_1(A), d_2(A), \dots)$.

We have $d_i(A) < \infty$ for every $A \subseteq E$ since the field extensions $L^{p^{i-1}}K(x_A)/L^{p^i}K(x_A)$ are algebraic and finitely generated. Since these field extensions are also purely inseparable, it follows that $d_i(A)$ is an integer for every $i \in \mathbb{N}$. We will now show that the function d satisfies the conditions in Definition 2.1.2 so that (E, d) is a DVR-matroid. We will prove each of the properties in the following lemmas.

Lemma 2.2.2. Let D and F be finite extensions of a field K contained in a common field L. Then $[D : K] \geq [DF : KF]$.

Proof. Let $v_1, \dots, v_n$ be a basis for D as a K-vector space. Let $\alpha \in DF$. Then $\alpha = e_1 f_1 + \cdots + e_m f_m$ for some $e_i \in D$ and $f_i \in F$. Now, for each $i = 1, \dots, m$, we have $e_i = \sum_{j=1}^{n} \beta_{ij} v_j$ for some $\beta_{ij} \in K$. So,

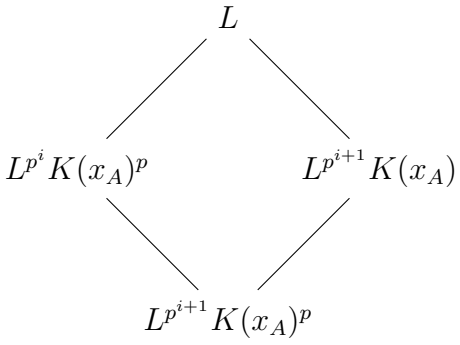
$$\alpha = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \beta_{ij} v_j \right) f_i = \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} v_j f_i = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} \beta_{ij} f_i \right) v_j.$$

Since α was arbitrary, we have that DF is spanned by $v_1, \dots, v_n$ as a KF-vector space. Hence, $[D : K] \geq [DF : KF]$. □

Lemma 2.2.3. For each $A \subseteq 1, \dots, n$ and $i \in \mathbb{N}$, the sequence $d(A)$ is a non-increasing sequence of nonnegative integers.

Proof. Since $L^{p^{i-1}}K(x_A)/L^{p^i}K(x_A)$ is a finitely generated algebraic extension, we have that $\left[L^{p^{i-1}}K(x_A) : L^{p^i}K(x_A)\right]$ is finite. Since for every $\alpha \in L^{p^{i-1}}K(x_A)$, we have $\alpha^p \in L^{p^i}K(x_A)$, $L^{p^{i-1}}K(x_A)/L^{p^i}K(x_A)$ is a purely inseparable extension. Hence, $\left[L^{p^{i-1}}K(x_A) : L^{p^i}K(x_A)\right]$ is a power of p and so $d_i(A)$ is a nonnegative integer.

To see that $d(A)$ is non-increasing, consider the following diagram:



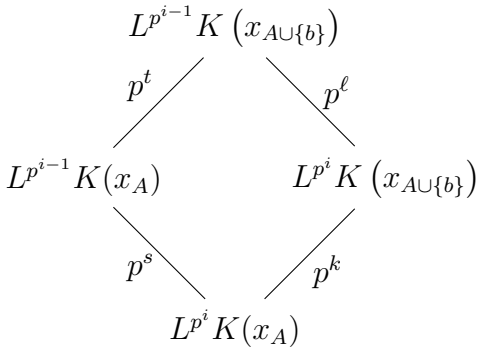
Applying the Frobenius endomorphism, we have $\left[L^{p^{i-1}}K(x_A) : L^{p^i}K(x_A)\right] = \left[L^{p^i}K(x_A)^p : L^{p^{i+1}}K(x_A)^p\right]$ since K is algebraically closed. By Lemma 2.2.2, we have $\left[L^{p^i}K(x_A)^p : L^{p^{i+1}}K(x_A)^p\right] \geq \left[L^{p^i}K(x_A) : L^{p^{i+1}}K(x_A)\right]$. Thus, $d(A)$ is a non-increasing sequence of nonnegative integers. □

Lemma 2.2.4. The function d defined in Definition 2.2.1 satisfies L1 from Definition 2.1.2.

Proof. Let $A \subseteq \{1, \ldots, n\}$, let $b \notin A$, and let $i \in \mathbb{N}$. We will show that

$$\log_p \left[L^{p^{i-1}}K(x_A) : L^{p^i}K(x_A)\right] - \log_p \left[L^{p^{i-1}}K(x_{A\cup\{b\}}) : L^{p^i}K(x_{A\cup\{b\}})\right] = 0 \text{ or } 1$$

Consider the following diagram of purely inseparable field extensions.



From multiplicativity of field extensions, we have $t + s = \ell + k$. By Lemma 2.2.2, we have $t \leq k$. Now, $L^{p^i}K\left(x_{A\cup\{b\}}\right)/L^{p^i}K(x_A)$ is a simple extension generated by x_b.

Let f be the minimal polynomial of x_b over $L^{p^{i-1}}K(x_A)$ so that $\deg(f) = p^t$. Then x_b is also a root of f^p which is a polynomial in $L^{p^i}K(x_A)[x]$. Hence, $p^k \leq \deg(f^p) = p^{t+1}$ and so $k \leq t+1$.

Thus, we have $t \leq k \leq t+1$ which implies $k = t$ or $k = t+1$. If $k = t$, then $s = \ell$ and so $d_i(A) = d_i(A \cup \{b\})$. If $k = t+1$, then $s = \ell + 1$, and so $d_i(A) = d_i(A \cup \{b\}) + 1$. Therefore, $d_i(A) - d_i(A \cup \{b\})$ is either 0 or 1. □

Lemma 2.2.5. The function d defined in Definition 2.2.1 satisfies L2a from Definition 2.1.2.

Proof. Observe that for any $n \in \mathbb{N}$ and $A \subseteq E$, $d_{\leq n}(A) = \log_p \left[L : L^{p^n}K(x_A)\right]$. So, for any $a, b \in E$, $A \subseteq E$, and $n \in \mathbb{N}$, we have

$$\begin{aligned}
&d_{\leq n}(A) - d_{\leq n}(A \cup \{b\}) - d_{\leq n}(A \cup \{c\}) + d_{\leq n}(A \cup \{b,c\}) \\
&= \log_p \left[L : L^{p^n}K(x_A)\right] - \log_p \left[L : L^{p^n}K(x_{A\cup\{b\}})\right] \\
&\quad - \log_p \left[L : L^{p^n}K(x_{A\cup\{c\}})\right] + \log_p \left[L : L^{p^n}K(x_{A\cup\{b,c\}})\right] \\
&= \log_p \frac{\left[L : L^{p^n}K(x_A)\right]\left[L : L^{p^n}K(x_{A\cup\{b,c\}})\right]}{\left[L : L^{p^n}K(x_{A\cup\{b\}})\right]\left[L : L^{p^n}K(x_{A\cup\{c\}})\right]} \\
&= \log_p \frac{\left[L^{p^n}K(x_{A\cup\{b\}}) : L^{p^n}K(x_A)\right]}{\left[L^{p^n}K(x_{A\cup\{b,c\}}) : L^{p^n}K(x_{A\cup\{c\}})\right]}
\end{aligned}$$

Now, by Lemma 2.2.2, we have that

$$\left[L^{p^n}K(x_{A\cup\{b\}}) : L^{p^n}K(x_A)\right] \geq \left[L^{p^n}K(x_{A\cup\{b,c\}}) : L^{p^n}K(x_{A\cup\{c\}})\right].$$

Thus,

$$\log_p \frac{\left[L^{p^n}K(x_{A\cup\{b\}}) : L^{p^n}K(x_A)\right]}{\left[L^{p^n}K(x_{A\cup\{b,c\}}) : L^{p^n}K(x_{A\cup\{c\}})\right]} \geq 0,$$

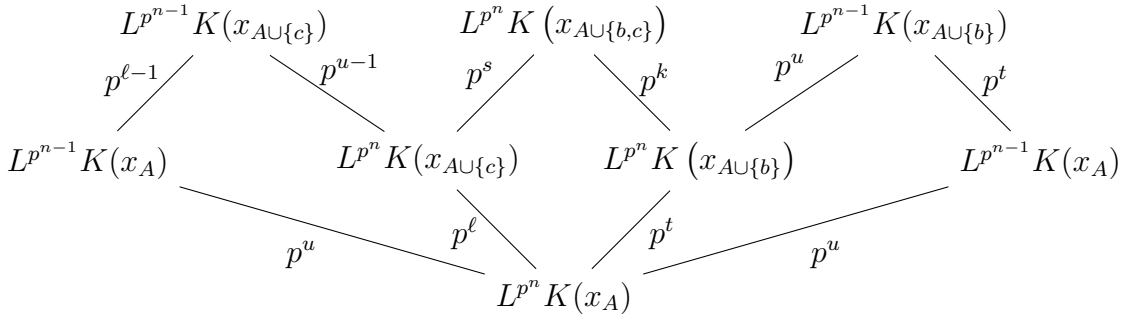
and so

$$d_{\leq n}(A) - d_{\leq n}(A \cup \{b\}) - d_{\leq n}(A \cup \{c\}) + d_{\leq n}(A \cup \{b,c\}) \geq 0.$$

Thus, d satisfies L2a. □

Lemma 2.2.6. The function d defined in Definition 2.2.1 satisfies L2b from Definition 2.1.2.

Proof. Let $A \subseteq E$ and $b, c \in E$. Suppose that $d_n(A \cup \{b\}) \neq d_n(A \cup \{c\})$. Since d satisfies L2a, we can assume that $d_n(A \cup \{b\}) = d_n(A)$ and $d_n(A \cup \{c\}) + 1 = d_n(A)$. So, we have the following diagram.



We claim that $k = \ell$. To see this, suppose to the contrary that $k \neq \ell$. Since by Lemma 2.2.2, $k \leq \ell$, this means $k < \ell$. Thus, $k \leq \ell - 1$. Since $\left[L^{p^{n-1}}K(x_A)(x_c) : L^{p^{n-1}}K(x_A)\right] = p^{\ell-1}$, we have $x_c^{p^{\ell-1}} \in L^{p^{n-1}}K(x_A)$. Since $k \leq \ell - 1$ and $\left[L^{p^n}K(x_A)(x_c, x_b) : L^{p^n}K(x_A)(x_b)\right] = p^k$, we have $x_c^{p^{\ell-1}} \in L^{p^n}K(x_A)(x_b)$. So, $x_c^{p^{\ell-1}} \in L^{p^{n-1}}K(x_A) \cap L^{p^n}K(x_A)(x_b)$. Since $L^{p^{n-1}}K(x_A)$ and $L^{p^n}K(x_A)(x_b)$ are linearly disjoint over $L^{p^n}K(x_A)$, we have $L^{p^{n-1}}K(x_A) \cap L^{p^n}K(x_A)(x_b) = L^{p^n}K(x_A)$. Thus, $x_c^{p^{\ell-1}} \in L^{p^n}K(x_A)$, a contradiction since $\left[L^{p^n}K(x_A)(x_c) : L^{p^n}K(x_A)\right] = p^\ell$. Therefore, $k = \ell$.

Thus, we have

$$\begin{aligned}
&d_{\leq n}(A) - d_{\leq n}(A \cup \{b\}) - d_{\leq n}(A \cup \{c\}) + d_{\leq n}(A \cup \{b, c\}) \\
&= \log_p \frac{\left[L^{p^n}K(x_{A\cup\{c\}}) : L^{p^n}K(x_A)\right]}{\left[L^{p^n}K(x_{A\cup\{b,c\}}) : L^{p^n}K(x_{A\cup\{b\}})\right]} \\
&= \log_p \frac{p^\ell}{p^k} \\
&= \log_p(1) \\
&= 0
\end{aligned}$$

Hence, we have equality in L2a. □

Theorem 2.2.7. Let L be a finite field extension of $K(x_1, \ldots, x_n)$, and assume K is algebraically closed. Let $E = \{1, \ldots, n\}$. Then (E, d) is a matroid over a DVR, where d is the function defined in Definition 2.2.1.

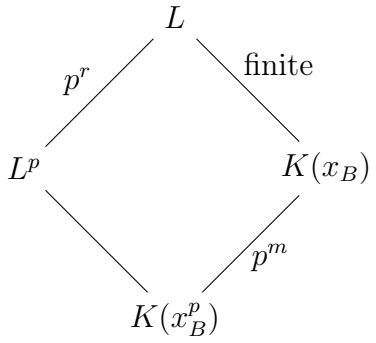
Proof. The result follows from Lemma 2.2.3, Lemma 2.2.4, Lemma 2.2.5, and Lemma 2.2.6. □

2.3 Compatibility with Algebraic Matroid

Let (E, d) be the DVR-matroid from Theorem 2.2.7, and let M be the classical matroid obtained as described in Section 2.1. In this section, we will show that this matroid is the same as the algebraic matroid of L/K associated to $x_1, \ldots, x_n$. Furthermore, the valuation σ on M is equal to the Lindström valuation.

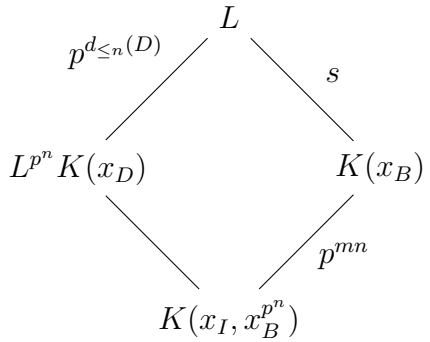
Theorem 2.3.1. Let K be an algebraically closed field of characteristic $p > 0$, and let L be a finite extension of $K(x_1, \ldots, x_n)$. Let M be the matroid described in Theorem 2.2.7. That is, the bases of M are the subsets B of E of size $r = \lim_{i \to \infty} d_i(\emptyset)$ such that $d_i(B) = 0$ for sufficiently large i. Then M is equal to the algebraic matroid of L/K associated to $x_1, \ldots, x_n$, and $\sigma = \sum_i d_i$ equals the Lindström valuation on M.

Proof. Let M' be the algebraic matroid of L/K associated to $x_1, \ldots, x_n$. It is enough to show that the bases of M and M' are the same. Let $B \subseteq E$ be a basis in M' with $\left|B\right| = m$. Then $L/K(x_B)$ is algebraic and hence finite, since $L/K(x_B)$ is finitely generated. Observe that for every $i \in \mathbb{N}$, we have $K(x_B) \subseteq L^{p^i}K(x_B) \subseteq L$. So, there must exist $\ell \in \mathbb{N}$ such that $L^{p^{i-1}}K(x_B) = L^{p^i}K(x_B)$ for $i \geq \ell$. Hence, $d_i(B) = \log_p \left[L^{p^{i-1}}K(x_B) : L^{p^i}K(x_B)\right]$ must be 0 for sufficiently large i. Now, we will show that $m = r$. We must have $[K(x_B) : K(x_B^p)] = p^m$ since the x_B are algebraically independent over K. Consider the following diagram of field extensions:



We have $[L : K(x_B)] = [L^p : K(x_B^p)]$ via the Frobenius endomorphism. Thus, we must have $m = r$, and so B is also a basis in M. Hence, the bases of M' are also bases of M. It follows that M and M' have the same rank.

Now, to show that bases of M are also bases in M', we will proceed by contrapositive. Suppose that $D \subseteq E$ is not a basis in M'. If $\left|D\right| \neq r$, then D is not a basis in M. So, assume that $\left|D\right| = r$. Since D is not a basis in M', we have that D must be dependent in M'. Let $I \subseteq D$ be a maximal independent (in M') subset of D so that $I \subsetneq B$ for some basis B. Then $[L : K(x_B)] < \infty$. Put $s = [L : K(x_B)]$ and $m = \left|B\right| - \left|I\right|$. Observe that for $n \in \mathbb{N}$, we have $\left[K(x_B) : K(x_I, x_B^{p^n})\right] = p^{mn}$ since x_B is algebraically independent over $K(x_I)$. Consider the following diagram of field extensions:



We claim that $\lim_{n\to\infty}[L^{p^n}K(x_D) : K(x_I, x_B^{p^n})] < \infty$. To see this, first observe that

$$[L^{p^n}K(x_D) : K(x_I, x_B^{p^n})] = [L^{p^n}K(x_D) : K(x_D, x_B^{p^n})][K(x_D, x_B^{p^n}) : K(x_I, x_B^{p^n})]$$

By Lemma 2.2.2, $[K(x_D, x_B^{p^n}) : K(x_I, x_B^{p^n})] \leq [K(x_D) : K(x_I)]$ which is equal to some $c < \infty$ since I is a maximal independent subset of D. Now, the extension $L^{p^n}K(x_D)/K(x_D, x_B^{p^n})$ is generated by elements $y_1^{p^n}, \ldots, y_\ell^{p^n}$ where $\{y_1, \ldots, y_\ell\}$ is a subset of the generators of $L/K(x_B)$. Now, if $f_i(t) \in K(x_B)[t]$ is the minimal polynomial of y_i over $K(x_B)$, let $f_i^{p^n}(t)$ be the polynomial obtained by raising the coefficients of $f_i(t)$ to the power p^n. Then $f_i^{p^n}(y_i^{p^n}) = 0$ and $f_i^{p^n}(t) \in K(x_B^{p^n})[t]$ has the same degree as f_i. Thus, we must have $[L^{p^n}K(x_D) : K(x_D, x_B^{p^n})] \leq s$. Hence, $[L^{p^n}K(x_D) : K(x_I, x_B^{p^n})] \leq sc$ for every $n \in \mathbb{N}$, and so $\lim_{n\to\infty}[L^{p^n}K(x_D) : K(x_I, x_B^{p^n})] < \infty$. Since $\lim_{n\to\infty}[L : K(x_I, x_B^{p^n})] = \infty$, it follows that $d_{\leq n}(D) = \infty$. Thus, there is no sufficiently large i for which $d_i(D) = 0$, and so D is not a basis of M.

We have shown that the bases of M and the bases of M' coincide. Now, we will show that σ agrees with the Lindström valuation on the bases. Let B be a basis so that $L/K(x_B)$ is algebraic and let N be the largest integer such that $d_i(B) \neq 0$. Then

$$\begin{aligned}
\sigma(B) &= \sum_{i=1}^{N} d_i(B) \\
&= \sum_{i=1}^{N} \log_p[L^{p^{i-1}}K(x_B) : L^{p^i}K(x_B)] \\
&= \log_p \prod_{i=1}^{N} [L^{p^{i-1}}K(x_B) : L^{p^i}K(x_B)] \\
&= \log_p[L : L^{p^N}K(x_B)]
\end{aligned}$$

Now, since $L/K(x_B)$ is finitely generated, there exists a nonnegative integer ℓ such that $L^{p^\ell}K(x_B)$ is separable over $K(x_B)$ [6, Proposition 6.1]. Assume that is the smallest such integer. Then $L^{p^\ell}K(x_B) \subseteq K(x_B)^{\text{sep}}$. Since $L/L^{p^\ell}K(x_B)$ is purely inseparable, we must have $K(x_B)^{\text{sep}} = L^{p^\ell}K(x_B)$. Now, $d_i(B) = 0$ for $i > \ell$ because $L^{p^{i-1}}K(x_B)/L^{p^i}K(x_B)$ is both separable and purely inseparable. Thus, $N \leq \ell$. By definition of N, we have $L^{p^N}K(x_B) = L^{p^\ell}K(x_B)$ which implies $L^{p^N}K(x_B)$ is separable

over $K(x_B)$. Thus, $\ell \leq N$, and so $\ell = N$. Therefore, we have

$$\begin{aligned}\sigma(B) &= \log_p[L : L^{p^N} K(x_B)] \\ &= \log_p[L : K(x_B)^{\text{sep}}] \\ &= \nu(B)\end{aligned}$$

where ν is the Lindström valuation on M. So, σ agrees with ν on bases of the algebraic matroid of L/K associated to $x_1, \ldots, x_n$. $\square$

Chapter 3

One-dimensional Algebraic Groups

A class of examples of algebraic matroids come from homomorphisms $G^d \to G^n$ where G is a connected one-dimensional algebraic group over an algebraically closed field K. In this chapter, we discuss how to obtain the d-vectors of the DVR-matroid of these algebraic matroids. Just as for the other chapters, we will assume that K is an algebraically closed field of characteristic $p > 0$.

3.1 Algebraic Matroids from Algebraic Groups

Given a homomorphism $G^d \to G^n$ of algebraic groups over a field K, we can construct an algebraic matroid of a field extension over K. These homomorphisms can be represented by $n \times d$ matrices with entries in the endomorphism ring of a connected one-dimensional algebraic group G over K. In this section, we will go through the construction of these matroids, as shown in [1].

Definition 3.1.1. An *algebraic group* over K is an algebraic variety G over K along with maps $\mu : G \times G \to G$ and $i : G \to G$, and an element $e \in G$ satisfying

(i) $\mu(a, e) = a$ for all $a \in G$,

(ii) $\mu(a, i(a)) = e$ for all $a \in G$,

(iii) $\mu(a, \mu(b, c)) = \mu(\mu(a, b), c)$ for every $a, b, c \in G$

Since connected one-dimensional algebraic groups are always commutative, we will denote the group operation additively. The set of endomorphisms of a fixed G forms a ring $\mathrm{End}(G)$ which we denote $\mathbb{E}$. Addition in this ring is defined by $(\alpha + \beta)(g) = \alpha(g) + \beta(g)$ for $\alpha, \beta \in \mathbb{E}$ and $g \in G$, and multiplication is function composition. Before we show how to construct algebraic matroids from algebraic groups, we will first give some key facts about these groups and their corresponding endomorphism rings.

There are three possibilities for connected one-dimensional groups G over K. The first possible group is the group $G_a = (K, +)$. The endomorphism ring in this case is $K[F]$, the ring of skew polynomials in F with coefficients in K, where $Fa = a^p F$ for every $a \in K$. The second possibility is the group $G_m = (K^*, \cdot)$ whose endomorphism ring is isomorphic to $\mathbb{Z}$. The last possibility is for G to be an elliptic curve over K, whose endomorphism ring is isomorphic to either $\mathbb{Z}$, an order in an imaginary quadratic number field, or an order in a quaternion algebra.

Given a connected one-dimensional algebraic group G, its endomorphism ring $\mathbb{E}$ satisfies certain conditions called the Ore conditions [9, Chapter 1]. Thus, $\mathbb{E}$ is contained in a division ring Q that is generated by $\mathbb{E}$, called the *Ore division ring of* $\mathbb{E}$. This ring is given by $Q = \{ab^{-1} : a, b \in \mathbb{E}\}$. We also have a valuation $\nu : \mathbb{E} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ that extends uniquely to the Ore division ring Q [1, Proposition 16].

Now, we will explain how to construct an algebraic matroid from a matrix representation of $G^d \to G^n$. Let G be a connected one-dimensional algebraic group over K, and let ψ be an $n \times d$ matrix with entries in $\mathbb{E}$, the endomorphism ring of G. Let $K(G)$ be the function field of G, meaning a finitely generated field extension of K, with transcendence degree 1. Then any $\alpha \in \mathbb{E}$ gives in injective homomorphism $\alpha^* : K(G) \to K(G)$.

Let $L = K(G^d)$ which is isomorphic to the field of fractions of $K(G) \otimes_K K(G) \otimes_K \cdots \otimes_K K(G)$. Then L is generated by subfields $E_1, \ldots, E_d$, each isomorphic to $K(G)$. For $j = 1, \ldots, n$, define $C_j = \psi_{j1}^*(E_1) \otimes_K \psi_{j2}^*(E_2) \otimes_K \cdots \otimes_K \psi_{jd}^*(E_d)$. Let t_j generate E_j over $K(G)$ for each j, and assume that $K(G)$ is separable over $K(t_j)$. Put $x_i = \psi_{j1}^*(t_1)\psi_{j2}^*(t_2)\cdots\psi_{jd}^*(t_d)$ for each $i = 1, \ldots, n$. Then let M be the algebraic matroid of the field extension L/K associated to $x_1, \ldots, x_n$.

Example 3.1.2. Let K be a field of characteristic $p > 0$, and let $G = G_m = (K \setminus \{0\}, \cdot)$ so that $\mathbb{E} \cong \mathbb{Z}$. Let ψ be an $n \times d$ matrix with entries in $\mathbb{Z}$. Then L is a finite extension of $K(t_1, \ldots, t_d)$, and M is the algebraic matroid of L/K associated to $x_1, \ldots, x_n$, where $x_j = t_1^{\psi_{j1}} \cdots t_d^{\psi_{jd}}$ for $j = 1, \ldots, n$.

3.2 Approximate Smith Normal Form

Let G be a connected one-dimensional algebraic group over K, and let ψ be a matrix with entries in $\mathbb{E} = \mathrm{End}(G)$. Let Q be the Ore division ring of $\mathbb{E}$ and put $R = \{q \in Q : v(q) \geq 0\}$. Then R is a discrete valuation ring with unique maximal ideal m, and $\mathbb{E} \subseteq R$. For $A \subseteq [n]$, define $M_A = R^d/\langle v_i : i \in A\rangle$ where v_i is the i^{th} column of ψ. If R is commutative, this defines a matroid over R with d-vectors given by $d_i(A) = \dim_{R/m}(m^{i-1}M_A/m^iM_A)$. We claim that these d-vectors are the same as the d-vectors of the DVR-matroid of the algebraic extension, regardless of the commutativity of R. We leave the proof of this claim for Section 3.3.

If a matrix over $\mathrm{End}(G)$ for some G has a Smith normal form, computing the d-vectors described above is more straight-forward. To see this, consider the case where $G = G_m$. We then have $\mathbb{E} = \mathbb{Z}$, R is the localization $\mathbb{Z}_{(p)}$, and ν is the p-adic valuation. If ψ is an $\mathbb{E}$-matrix, then ψ_A, the submatrix of ψ consisting of the columns in $A \subseteq [n]$, has a Smith normal form. That is, $\psi_A = PDS$ where P and S are invertible $\mathbb{Z}$-matrices and D is a diagonal $\mathbb{Z}$-matrix. So, taking $p^\infty\mathbb{Z}_{(p)}$ to be $\{0\}$, we

have

$$\begin{aligned} M_A &\cong \mathbb{Z}_{(p)}/b_1\mathbb{Z}_{(p)} \oplus \mathbb{Z}_{(p)}/b_2\mathbb{Z}_{(p)} \oplus \cdots \oplus \mathbb{Z}_{(p)}/b_d\mathbb{Z}_{(p)} \\ &\cong \mathbb{Z}_{(p)}/p^{\nu(b_1)}\mathbb{Z}_{(p)} \oplus \mathbb{Z}_{(p)}/p^{\nu(b_2)}\mathbb{Z}_{(p)} \oplus \cdots \oplus \mathbb{Z}_{(p)}/p^{\nu(b_d)}\mathbb{Z}_{(p)} \end{aligned}$$

where $b_1, \ldots, b_d$ are the diagonal entries of D. So, for $i \in \mathbb{N}$,

$$p^{i-1}M_A/p^iM_A \cong \oplus_{j=1}^{d} \left(p^{i-1}\mathbb{Z}_{(p)}/p^{k_j}\mathbb{Z}_{(p)}\right) / \left(p^i\mathbb{Z}_{(p)}/p^{k_j}\mathbb{Z}_{(p)}\right) \cong \oplus_{j=1}^{d} N_{ij}$$

where $N_{ij} = 0$ if $i-1 \geq \nu(b_j)$ and $N_{ij} \cong p^{i-1}\mathbb{Z}_{(p)}/p^i\mathbb{Z}_{(p)}$ if $i-1 < \nu(b_j)$. We can now easily compute the dimension over $\mathbb{Z}_{(p)}$.

For a general connected one-dimensional algebraic group G, a matrix ψ over $\mathrm{End}(G)$ does not necessarily have a Smith normal form. However, if $\psi = PDS$ where P and S are invertible and the off-diagonal entries of D have sufficiently large valuation, we can still compute the d-vectors like above.

Definition 3.2.1. Let V be a ring with valuation $\nu : V \to \mathbb{Z} \cup \{\infty\}$, and let A be an $n \times d$ matrix with entries in V. We say that A has an *approximate Smith normal form* if for every $H > 0$, there exist invertible matrices P and S over V such that the non-diagonal entries of the matrix PAS have valuation larger than H.

We will show that every matrix with entries in $\mathbb{E}$, for some connected one-dimensional algebraic group G, has an approximate Smith normal form, but first we need the following lemma. Since the proof relies only on algebraic properties of $\mathbb{E}$, we will work with an arbitrary valuation ring V with such properties.

Lemma 3.2.2. Let V be a ring with valuation v such that V is contained in a division ring $Q = \{ab^{-1} : a, b \in V\}$. Let $R = \{q \in Q : v(q) \geq 0\}$, and let m be the unique maximal ideal of R. Suppose that there exists $\pi \in V$ such that $v(\pi) = 1$ and that the natural map $V \to R/m$ is surjective. Let $H > 0$, and let $a, b \in V$ with $v(a) \leq v(b)$. Then there exists $c \in V$ such that $v(b - ca) > H$.

Proof. Fix $H > 0$, and let $a, b \in V$. Then there exist $r, s \in R \setminus m$ such that $a = r\pi^{v(a)}$ and $b = s\pi^{v(b)}$. Since $V \to R/m$ is surjective, there exists $\alpha \in V$ such that $\alpha + m = sr^{-1} + m$. So, $sr^{-1} - \alpha \in m$. Thus, $v(sr^{-1} - \alpha) \geq 1$. Let $c_1 = \alpha\pi^{v(b)-v(a)}$. Then $c_1 \in V$ and

$$\begin{aligned} v(b - c_1 a) &= v\left(s\pi^{v(b)} - \alpha\pi^{v(b)-v(a)} r\pi^{v(a)}\right) \\ &= v\left(s\pi^{v(b)} - \alpha r\pi^{v(b)}\right) \\ &= v\left((s - \alpha r)\pi^{v(b)}\right) \\ &= v\left(r(sr^{-1} - \alpha)\pi^{v(b)}\right) \\ &> v(b). \end{aligned}$$

Now, replacing b with $b - c_1 a$, we have by the same argument that there exists $c_2 \in V$ such that $v(b - c_1 a - c_2 a) > v(b - c_1 a)$. Continuing this process, we can find $c_1, \ldots, c_n \in V$ such that $v(b - (c_1 + \cdots + c_n)a) > H$. Put $c = c_1 + \cdots + c_n \in V$, and the result follows. □

For every endomorphism ring $\mathbb{E}$ of a connected one-dimensional algebraic group, there exists an element in $\mathbb{E}$ with valuation 1 [1, Lemma 4.4]. Now, we will show that the natural map $\mathbb{E} \to R/m$ is surjective.

Lemma 3.2.3. Let G be a connected one-dimensional algebraic group. Let $\mathbb{E}$ be the endomorphism ring of G, Q the Ore division ring of $\mathbb{E}$, and $R = \{q \in Q : v(q) \geq 0\}$. Then the natural map $\mathbb{E} \to R/m$, where m is the unique maximal ideal of R, is surjective.

Proof. We consider each of the cases in Proposition 25 of [1]. Suppose that $G \cong G_a$ so that $\mathbb{E} = K[F]$ and v is the F-adic valuation. First we claim that every $r \in R$ can be written as $r = F^n g h^{-1}$ where $g, h \in \mathbb{E} \setminus m$ and $n \geq 0$. To see this, let $r \in R$ so that $r = ab^{-1}$ with $a, b \in \mathbb{E}$ and $v(a) \geq v(b)$. Let $m = v(b)$. Then $b^{-1} = (b'F^m)^{-1}$ where $b' = bF^{-m} \in \mathbb{E}$ and $v(b') = 0$. Since $v(a) \geq m$, we have $a = a'F^m$ where

$a' = aF^{-m} \in \mathbb{E}$ and $v(a') \geq 0$. So,

$$r = ab^{-1} = a'F^m(b'F^m)^{-1} = a'F^mF^{-m}(b')^{-1} = a'(b')^{-1}$$

with $a', b' \in \mathbb{E}$ and $v(a') \geq 0,\ v(b') = 0$. Now, applying $F^{v(a')}$ to the coefficients of a' to obtain $a'' \in \mathbb{E}$, we have $r = a'(b')^{-1} = F^{v(a')}a''(b')^{-1}$ with $v(a'') = v(b') = 0$. Since m is generated by F, we have $a'', b' \notin m$. Putting $n = v(a') \geq 0$, $g = a''$, and $h = b'$, the claim follows.

Now, we'll show that $\mathbb{E} \to R/m$ is surjective for this case. Let $r \in R$ so that $r = F^n g h^{-1}$ for some $g, h \in \mathbb{E} \setminus m$ and $n \geq 0$. Let $g = a_0 + a_1F + \cdots + a_mF^m$ and let $h = b_0 + b_1F + \cdots + b_\ell F^\ell$. Since $h \notin m$, we have $b_0 \in K \setminus \{0\}$. Observe that

$$\begin{aligned} r - F^n a_0 b_0^{-1} &= F^n(a_0 + a_1F + \cdots + a_mF^m)h^{-1} - F^n a_0 b_0^{-1} h h^{-1} \\ &= F^n(a_0 + a_1F + \cdots + a_mF^m)h^{-1} - F^n a_0 b_0^{-1}(b_0 + b_1F + \cdots + b_\ell F^\ell)h^{-1} \\ &= F^n((a_0 + a_1F + \cdots + a_mF^m) - a_0 b_0^{-1}(b_0 + b_1F + \cdots + b_\ell F^\ell))h^{-1} \in m \end{aligned}$$

Thus, $r + m = F^n a_0 b_0^{-1} + m$, and so $F^n a_0 b_0^{-1} \in \mathbb{E}$ such that $F^n a_0 b_0^{-1} \mapsto r + m$. Therefore, if $G \cong G_a$, then $\mathbb{E} \to R/m$ is surjective.

Now, suppose that either $G \cong G_m$ or G is isomorphic to an elliptic curve with j-invariant not in $\overline{\mathbb{F}_p}$, so that $\mathbb{E} \cong \mathbb{Z}$ and v is the p-adic valuation. Since $R/m \cong \mathbb{Z}/p\mathbb{Z}$ which has no nontrivial subfields, the image of $\mathbb{E} \to R/m$ is R/m. Thus, $\mathbb{E} \to R/m$ is surjective in this case.

Now, if G is isomorphic to a non-supersingular elliptic curve with j-invariant in $\overline{\mathbb{F}_p}$, then by [1, Proposition 25], we have $R/m \cong \mathbb{Z}/p$. Thus, $\mathbb{E} \to R/m$ must be surjective.

Now, suppose that G is isomorphic to a supersingular elliptic curve. By [10, Paragraph 42.4.6], $\mathbb{E}/(\mathbb{E} \cap m) \cong \mathbb{F}_{p^2}$. Also, by [1, Proposition 25], we have that $\mathbb{E}$ is an order in a quaternion algebra. Since $\mathbb{E}$ is noncommutative, every element of R has degree at most 2 over Q. Thus, we must have that R/m has p^2 elements. Thus, the

map $\varphi : \mathbb{E}/(\mathbb{E} \cap m) \to R/m$ given by $\varphi(x + (\mathbb{E} \cap m)) = x + m$ is an isomorphism. It follows that $\mathbb{E} \to R/m$ is onto since the map $\mathbb{E} \to \mathbb{E}/(\mathbb{E} \cap m)$ is. □

We can now show that any $n \times d$ matrix representing a homomorphism of algebraic groups has an approximate Smith normal form.

Theorem 3.2.4. Let G be a connected one-dimensional algebraic group with endomorphism ring $\mathbb{E}$, and let ψ be an $n \times d$ matrix with entries in $\mathbb{E}$. Then ψ has an approximate Smith normal form.

Proof. Fix $H > 0$. First observe that all elementary row/column operations are invertible, with the exception of multiplying a row/column by a scalar. Let

$$\psi = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1d} \\ a_{21} & \ddots & & \\ \vdots & & \ddots & \\ a_{n1} & & & a_{nd} \end{bmatrix}$$

Let a_{i*} denote the i^{th} row of ψ and a_{*j} the j^{th} column of ψ. We can switch rows and columns in order to move an entry with least valuation to the top left. So, assume that a_{11} has the least valuation. So, for each $2 \leq j \leq d$, we have $v(a_{11}) \leq v(a_{1j})$. By the lemma, there exists $c_j \in \mathbb{E}$ such that $v(a_{1j} - a_{11}c_j) \geq H$. Thus, by replacing the column a_{*j} with $a_{*j} - a_{*1}c_j$, we obtain a matrix ψ' so that the elements in the first row (excluding a_{11}) have valuation at least H, and ψ' is equivalent to ψ.

Similarly, since for each $2 \leq i \leq n$ we have $v(a_{11}) \leq v(a_{i1})$, there exists $c_i' \in \mathbb{E}$ such that $v(a_{i1} - c_i'a_{11}) \geq H$. Thus, by replacing a_{i*} (row i) with $a_{i*} - c_i'a_{1*}$, we can then obtain a matrix ψ'' so that the elements in the first row and first column (excluding a_{11}) have valuation at least H, and ψ'' is equivalent to ψ.

Now, let B be the submatrix of ψ'' shown below.

$$\psi'' = \begin{bmatrix} a'_{11} & a'_{12} & \cdots & a'_{1d} \\ a'_{21} & & & \\ \vdots & & B & \\ a'_{n1} & & & \end{bmatrix}$$

By the same reasoning as above (on the submatrix B), we have that ψ'' is equivalent to a matrix ψ''' such that for $3 \leq j \leq d$, $v(b_{2j}) \geq H$ and for $3 \leq i \leq n$, $v(b_{i2}) \geq H$. Now, observe that for any $i, j = 2, \ldots, n$ (with $i \neq j$) and for any $e \in \mathbb{E}$, we have $v(a_{i1} - ea_{j1}) \geq \min\{v(a_{i1}), v(ea_{j1})\} \geq H$, and $v(a_{1i} - a_{1j}e) \geq \min\{v(a_{1i}), v(a_{1j}e)\} \geq H$. Thus, the entries in the first row and first column of ψ''' (excluding the upper left entry) must also have valuation at least H.

By continuing this process, we obtain a matrix D such that D is equivalent to ψ and the non-diagonal entries of D have valuation at least H. Since $H > 0$ was arbitrary, the result follows. □

3.3 Equality of DVR-Matroids

We have shown that every matrix representing a homomorphism of algebraic groups has an approximate Smith normal form. In this section, we will prove that the d-vectors described in Section 3.2 are the same as the d-vectors of the DVR-matroid of the algebraic matroid of this matrix.

Proposition 3.3.1. Let G be a connected one-dimensional algebraic group with endomorphism ring $\mathbb{E}$, and let ψ be an $n \times d$ matrix with entries in $\mathbb{E}$. Let $L = K(G^d)$ and let $E_1, \ldots, E_d$ be subfields of L that generate L, each isomorphic to $K(G)$. Put $C_j = \psi_{j1}(E_1) \cdots \psi_{jd}(E_d)$ for each $j = 1, \ldots, n$. For $A \subseteq [n]$, let $d_i(A) = \log_p \left[L^{p^{i-1}} K(C_A) : L^{p^i} K(C_A) \right]$ where C_A is the compositum of all C_j with $j \in A$,

and let $f_i(A) = \dim_{R/m}(m^{i-1}M_A/m^iM_A)$ where v_j is the j^{th} row of ψ and $M_A = R^d/\langle v_i : i \in A\rangle$. Then $d_i(A) = f_i(A)$ for every $A \subseteq [n]$.

Proof. By Theorem 3.2.4, ψ_A has an approximate Smith normal form $\psi_A = PBS$ over $\mathbb{E}$ where B has diagonal entries $b_1, \ldots, b_d$. Since all off diagonal entries of B have high valuation, we have

$$M_A \cong R/b_1R \oplus R/b_2R \oplus \cdots \oplus R/b_dR \cong R/m^{k_1}R \oplus R/m^{k_2}R \oplus \cdots \oplus R/m^{k_d}R$$

where $k_j = v(b_j)$ and we take $m^\infty R$ to be $\{0\}$. So,

$$m^{i-1}M_A/m^iM_A \cong \oplus_{j=1}^d \left(m^{i-1}R/m^{k_j}R\right) / \left(m^iR/m^{k_j}R\right) \cong \oplus_{j=1}^d N_{ij}$$

where $N_{ij} = 0$ if $i - 1 \geq k_j$ and $N_{ij} \cong m^{i-1}R/m^iR$ if $i - 1 < k_j$. Let

$$\ell_{ij} = \dim_{R/m}(N_{ij}) = \begin{cases} 0 & \text{if } k_j \leq i-1 \\ 1 & \text{if } k_j > i-1 \end{cases}$$

Then $f_i(A) = \sum_{j=1}^{d} \ell_{ij}$.

Now, we'll show that $d_i(A) = f_i(A)$ for each i. Since P and S are isomorphisms, there exist subfields $F_1, \ldots, F_d$ of L such that L is generated by $F_1, \ldots, F_d$ and $K(C_A) = K(b_1(F_1), \ldots, b_d(F_d))$ for every $A \subseteq [n]$. For each i, if $k \neq j$, then $v(b_{kj}) > i$

so that $b_{kj}(F_k) \subseteq L^{p^i}$. So, we have

$$\begin{aligned}
d_i(A) &= \log_p \left[L^{p^{i-1}} C_A : L^{p^i} C_A \right] \\
&= \log_p \left[L^{p^{i-1}} b_{1*}(F_1), \ldots, b_{d*}(F_d) : L^{p^i} b_{1*}(F_1), \ldots, b_{d*}(F_d) \right] \\
&= \log_p \left[L^{p^{i-1}} b_1(F_1), \ldots, b_d(F_d) : L^{p^i} b_1(F_1), \ldots, b_d(F_d) \right] \\
&= \log_p \left[F_1^{p^{i-1}} \cdots F_d^{p^{i-1}} (b_1(F_1), \ldots, b_d(F_d)) : F_1^{p^i} \cdots F_d^{p^i} (b_1(F_1), \ldots, b_d(F_d)) \right] \\
&= \log_p \left[(F_1^{p^{i-1}} b_1(F_1)) \cdots (F_d^{p^{i-1}} b_d(F_d)) : (F_1^{p^i} b_1(F_1)) \cdots (F_d^{p^i} b_d(F_d)) \right] \\
&= \log_p \left[F_1^{p^{\min\{i-1,k_1\}}} \cdots F_d^{p^{\min\{i-1,k_d\}}} : F_1^{p^{\min\{i,k_1\}}} \cdots F_d^{p^{\min\{i,k_d\}}} \right] \\
&= \log_p \prod_{j=1}^{d} [D_j : D_{j-1}]
\end{aligned}$$

where $D_j = F_1^{p^{\min\{i-1,k_1\}}} \cdots F_j^{p^{\min\{i-1,k_j\}}} F_{j+1}^{p^{\min\{i,k_{j+1}\}}} \cdots F_d^{p^{\min\{i,k_d\}}}$ for $j = 0, \ldots, d$. Observe that $[D_j : D_{j-1}] = p^{\ell_{ij}}$. Thus,

$$\begin{aligned}
\log_p \prod_{j=1}^{d} [D_j : D_{j-1}] &= \log_p \prod_{j=1}^{d} p^{\ell_{ij}} \\
&= \sum_{j=1}^{d} \log_p \left(p^{\ell_{ij}} \right) \\
&= \sum_{j=1}^{d} \ell_{ij} \\
&= f_i(A)
\end{aligned}$$

□

Proposition 3.3.2. Let G be a connected one-dimensional algebraic group, $L = K(G^d)$, and ψ an $n \times d$ matrix with entries in $\mathbb{E} = \mathrm{End}(G)$. Let $E_1, \ldots, E_d$ be subfields of L that generate L, each isomorphic to $K(G)$. Assume that for each $i = 1, \ldots, d$, we have $t_i \in E_i$ such that $E_i/K(t_i)$ is separable. Put $C_j = \psi_{j1}(E_1) \cdots \psi_{jd}(E_d)$ and $x_j = \psi_{j1}(t_1) \cdots \psi_{jd}(t_d)$ for each j. Let C_A be the compositum of all C_j with $j \in A$

for a subset $A \subseteq [n]$. Then $\left[L^{p^{i-1}}K(C_A) : L^{p^i}K(C_A)\right] = \left[L^{p^{i-1}}K(x_A) : L^{p^i}K(x_A)\right]$ for every $i \in \mathbb{N}$.

Proof. First observe that since E_i is separable over $K(t_i)$, we have that each of $\psi_{j1}(E_1), \ldots, \psi_{jd}(E_d)$ is separable over $K(\psi_{j1}(t_1)), \ldots, K(\psi_{jd}(t_d))$ respectively. Thus, C_j is separable over x_j for each j, and C_A is separable over $K(x_A)$ for any $A \subseteq [n]$.

Fix $\ell \in \mathbb{Z}_{\geq 0}$, and $A \subseteq [n]$. We claim that $L^{p^\ell}K(C_A) = L^{p^\ell}K(x_A)$. To see this, first observe that since C_A is separable over $K(x_A)$, we have $L^{p^\ell}K(C_A)$ is separable over $L^{p^\ell}K(x_A)$. Since for every $y \in L^{p^\ell}K(C_A)$, we have $y^{p^\ell} \in L^{p^\ell}K(x_A)$, the extension $L^{p^\ell}K(C_A)/L^{p^\ell}K(x_A)$ is also purely inseparable. Thus, $L^{p^\ell}K(C_A) = L^{p^\ell}K(x_A)$. It follows that for any $A \subseteq [n]$ and $i \in \mathbb{N}$, we have $\left[L^{p^{i-1}}K(C_A) : L^{p^i}K(C_A)\right] = \left[L^{p^{i-1}}K(x_A) : L^{p^i}K(x_A)\right]$. □

We can now prove the main result of the chapter.

Theorem 3.3.3. Let G be a connected one-dimensional algebraic group with endomorphism ring $\mathbb{E}$, and let ψ be an $n \times d$ matrix with entries in $\mathbb{E}$. Let $L = K(G^d)$ and let $E_1, \ldots, E_d$ be subfields of L that generate L, each isomorphic to $K(G)$. Assume that for each $i = 1, \ldots, d$, we have $t_i \in E_i$ such that $E_i/K(t_i)$ is separable, and put $x_j = \psi_{j1}(t_1) \cdots \psi_{jd}(t_d)$ for each $j = 1, \ldots, n$. For $A \subseteq [n]$, let $d_i(A) = \log_p \left[L^{p^{i-1}}K(x_A) : L^{p^i}K(x_A)\right]$, and let $f_i(A) = \dim_{R/m}(m^{i-1}M_A/m^iM_A)$ where v_j is the j^{th} row of ψ and $M_A = R^d/\langle v_i : i \in A\rangle$. Then $([n], d)$ and $([n], f)$ are equal DVR-matroids.

Proof. The proof follows from Proposition 3.3.1 and Proposition 3.3.2. □

Bibliography

[1] Bollen, G. P., Cartwright, D., and Draisma, J. (2022). Matroids over one-dimensional groups. *Int. Math. Res. Not. IMRN*, 2022(3):2298–2336. 17, 18, 21, 22

[2] Bollen, G. P., Draisma, J., and Pendavingh, R. (2018). Algebraic matroids and Frobenius flocks. *Adv. Math.*, 323:688–719. 4

[3] Cartwright, D. (2018). Construction of the Lindström valuation of an algebraic extension. *J. Combin. Theory Ser. A*, 157:389–401. iv, 5

[4] Dress, A. W. M. and Wenzel, W. (1992). Valuated matroids. *Adv. Math.*, 93(2):214–250. 3

[5] Fink, A. and Moci, L. (2016). Matroids over a ring. *J. Eur. Math. Soc.*, 18(4):681–731. iv, 6, 7, 8

[6] Lang, S. (2005). *Algebra*. Graduate Texts in Mathematics. Springer New York. 15

[7] Lindström, B. (1986). A non-linear algebraic matroid with infinite characteristic set. *Discrete Math.*, 59(3):319–320. iv, 4

[8] Oxley, J. (2011). *Matroid Theory*. Oxford Graduate Texts in Mathematics. OUP Oxford. 2

[9] Schofield, A. (1998). Skew fields: Theory of general division rings. *Bulletin of the London Mathematical Society*, 30(3):317–335. 18

[10] Voight, J. (2021). *Quaternion Algebras*. Number 288 in Graduate Texts in Mathematics. Springer. 22

Vita

Anna Litchford Lawson grew up in Carthage, Tennessee. She received her bachelor's degree from Tennessee Technological University in 2015 and graduated with a master's in math in May of 2017. Her research interests include commutative algebra and algebraic matroid theory.