universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Arithmetic matroids and an application to number theory“

verfasst von / submitted by

Marcus Schönfelder BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2024 / Vienna, 2024

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	UA 066821
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Mathematik
Betreut von / Supervisor:	Univ. Prof. Dr. Christian Krattenthaler

Acknowledgements

I thank my supervisor Univ. Prof. Dr. Christian Krattenthaler not only for suggesting the fascinating topic of this thesis, but also for his constant support in matters of scientific writing, LaTeX–programming and quality assurance. Additionally he allowed me the freedom to independently plan and execute my thesis, so that I actually had some fun doing the research and writing. I am very grateful.

Moreover I want to thank my family and friends for all their support and joy during my bachelor's and master's studies as well as during the pandemic. It is mostly to you, that I have finally achieved all of my ambitious goals. You turned a hard and difficult time into a great adventure and I will never forget that.

Abstract

Matroids are combinatorial structures that abstract the notion of linear independence on finite sets. In their most famous examples they closely connect finite dimensional linear algebra with graph theory. In applications they are mostly regarded together with their most important invariant: the Tutte polynomial $T(x, y)$. This bivariate polynomial is encoding a huge amount of combinatorial data of the underlying matroid (for example the number of spanning trees and possible colourings of a graph).

Now arithmetic matroids form a true combinatorial generalisation of the notion of ordinary matroids. While classical matroids are only concerned with the dependency relations of the underlying structure, an arithmetic matroid is also equipped with a certain *multiplicity function* that contains additional combinatorial information. These multiplicities are also used to construct the so-called *arithmetic Tutte polynomial* $M(x, y)$. This advanced version of the Tutte polynomial may now encode various useful new data of the underlying structure, depending on the choice of the multiplicities. For example, if we consider a zonotope in $\mathbb{R}^n$ whose corners lie in a lattice $\Lambda \subseteq \mathbb{R}^n$, then we will see that we can associate an arithmetic matroid to the zonotope whose arithmetic Tutte polynomial specialises to the Ehrhart polynomial of the zonotope. This theory was mainly developed by the insights of Luca Moci in his pioneering paper *A tutte polynomial for toric arrangements* [Moc11] from 2011. The abstract concept of an arithmetic matroid was then firstly defined by Moci and D'Adderio [MD12] in 2012.

In this thesis we summarize the essential aspects of the theory of arithmetic matroids and arithmetic Tutte polynomials. In the first part we start with an introduction to standard matroid theory to establish the basic concepts and terminology.

Afterwards in the second part, we discuss the different axiomatisations as well as the most important structural properties of arithmetic matroids. We will see the main examples and talk about how to adapt the concepts of representability, duality, direct sums, deletion and contraction of matroids to the arithmetic situation such that their essential qualities are preserved.

The third part of this thesis is committed to the arithmetic Tutte polynomial, for which we list generalisations of many of the identities known from the standard matroid case. Eventually we talk about possible specialisations of the arithmetic Tutte polynomials in the concrete cases of arithmetic matroids over lattice points and labeled graphs.

The fourth and final part of the thesis is dedicated to the construction of a class of quasi-arithmetic matroids inside the realms of number theory. We will call them *radical matroids* since they will have radicals as multiplicities. We aim for analysing cases where radical matroids are also arithmetic matroids and will give a full characterisation of the representable radical matroids.

Kurzfassung

Ein Matroid ist eine kombinatorische Struktur, die das Konzept von linearer Abhängigkeit auf ganz verschiedene endliche Mengen verallgemeinert. Klassischerweise werden Matroide über endlichen Mengen von Vektoren oder über Graphen betrachtet. Wir erhalten dadurch eine Theorie, die die strukturellen Grundkonzepte der Linearen Algebra mit denen der Graphentheorie verbindet. Von besonderem Interesse ist hierbei das Tutte-Polynom $T(x, y)$ als strukturelle Invariante eines jeden Matroids. Dieses Polynom kodiert allerlei nützliche kombinatorische Information der zu Grunde liegenden mathematischen Struktur. So finden sich etwa die Anzahlen aller Möglichkeiten, einen Graphen mit einer gegebenen Anzahl an Farben einzufärben, in seinem Tutte-Polynom versteckt.

Allerdings berücksichtigen gewöhnliche Matroid-Strukturen wirklich nur Sachverhalte die aus der Unabhängigkeit der Teilmengen resultieren. Die italienischen Mathematiker Luca Moci und Michele D'Adderio konfrontieren dieses Problem mit der von ihnen entwickelten Theorie der arithmetischen Matroide. *Arithmetische Matroide* sind nun Matroide, welche zusätzlich mit einer sogenannten *Vielfachheitsfunktion* ausgestattet sind. Diese kann nun je nach Wahl ganz beliebige kombinatorische Daten beinhalten, welche schließlich auch in die Definition des *arithmetischen Tutte-Polynoms* $M(x, y)$ einfließen. Dieses erweiterte Tutte-Polynom kann nun allerlei weitere Daten der zu Grunde liegenden mathematischen Struktur in sich tragen. Beispielsweise werden wir sehen, dass wir einen arithmetischen Matroid über einem Zonotop im $\mathbb{R}^n$ definieren können, dessen arithmetisches Tutte-Polynom zum Ehrhart-Polynom des Zonotops spezialisiert werden kann.

Diese Arbeit umfasst vier Teile, in denen wir die wichtigsten Aspekte der Theorie arithmetischer Matroide und ihrer arithmetischen Tutte-Polynome zusammenfassen. Im ersten Teil wiederholen wir die Grundbegriffe der klassischen Matroidtheorie. Anschließend betrachten wir im zweiten Teil die Definition eines arithmetischen Matroids. Wir sehen uns einige grundlegende Beispiele an und formulieren Konzepte wie Darstellbarkeit und Dualität nun für den arithmetischen Fall.

Der dritte und größte Teil ist dem arithmetischen Tutte-Polynom gewidmet. Wir sehen einige Verallgemeinerungen von Formeln, die aus der klassischen Matroidtheorie bekannt sind. Anschließend schauen wir uns Anwendungen und Interpretationen des arithmetischen Tutte-Polynoms in konkreten Fällen an.

Zu guter Letzt konstruieren wir eine neue Klasse an quasi-arithmetischen Matroiden über Objekten der Zahlentheorie. Diese werden wir schließlich *Radikalmatroide* taufen, da ihre Vielfachheitsfunktionen durch die Radikalfunktion gegeben sind. Wir erforschen ihren Zusammenhang mit den arithmetischen Matroiden und geben eine vollständige Charakterisierung aller darstellbaren Radikalmatroide an.

Contents

Acknowledgements i

Abstract iii

Kurzfassung v

List of Figures ix

1 Introduction 1
- 1.1 Notations and conventions . . . 1
- 1.2 Essentials of matroid theory . . . 2
  - 1.2.1 Basic definitions . . . 3
  - 1.2.2 Duality . . . 9
  - 1.2.3 Deletion and contraction . . . 12
  - 1.2.4 The Tutte polynomial . . . 15

2 Arithmetic matroids 19
- 2.1 Basic definitions and examples of arithmetic matroids . . . 19
  - 2.1.1 Multiplicities . . . 20
  - 2.1.2 The main examples of arithmetic matroids . . . 29
- 2.2 Duality and representability . . . 39
  - 2.2.1 Duality . . . 39
  - 2.2.2 Representability . . . 41
- 2.3 Deletion, contraction and direct sums of arithmetic matroids . . . 45

3 The arithmetic Tutte polynomial 47
- 3.1 Identities for the arithmetic Tutte polynomial . . . 47
  - 3.1.1 Arithmetic Tutte polynomials of direct sums . . . 47
  - 3.1.2 Deletion and contraction recurrences . . . 48
  - 3.1.3 External activity expansion of the arithmetic Tutte polynomial . . . 50
  - 3.1.4 The generalisation of Crapo's theorem . . . 57
  - 3.1.5 A convolution formula . . . 61
- 3.2 Specialisations, interpretations and generalisations of the arithmetic Tutte polynomial . . . 63
  - 3.2.1 Arithmetic matroids over lattice points . . . 63
  - 3.2.2 Arithmetic colourings and flows . . . 69
  - 3.2.3 Generalisations of the arithmetic Tutte polynomial . . . 77

4 Radical matroids **81**
4.1 The basic construction 81
4.1.1 Algebra prerequisites 82
4.1.2 The radical function 84
4.1.3 The definition of radical matroids 86
4.2 Basic properties of radical matroids 88
4.2.1 Arithmetic radical matroids 88
4.2.2 Representable radical matroids 94
4.3 Final comments 99

Bibliography **101**

List of Figures

1.1 Visualisation of the graph $G = (V, E)$. 3
1.2 Circuits in red and green on the left and a basis marked in blue on the right. 6
1.3 A graph (black) and its dual graph (red). 9
1.4 Loops, bridges/coloops and proper edges of a graph. 11
1.5 A graph with an distinct edge $e = (u, v)$. 13
1.6 Deletion of edge e. 13
1.7 Contraction of edge e. 13

2.1 $\mathcal{P}(\{a, b, c\})$ is isomorphic to the boolean poset B_3. 25
2.2 The zonotope $\mathcal{Z}(X)$. 36
2.3 A labelled graph with regular edges (black) and dotted edges (brown). . . 37
2.4 labelled deletion and contraction of the former regular edge e. 38

3.1 Integer points and the dilation of a zonotope. 65
3.2 Integer points of a simple zonotope and its dilation by 2. 68
3.3 A proper arithmetic 4-colouring marked in green. 70
3.4 The simple counterexample. 72

1 Introduction

In the first part of this thesis we give a brief introduction to the basics of matroid theory. The aim is to enable students and interested readers with various mathematical backgrounds to follow the theory and comprehend the main results and their consequences. However, basic knowledge of linear algebra and graph theory is required. We start by giving an overview of the different notations and conventions we will use throughout the thesis. After that we define the notion of a matroid in many of its possible ways. We strengthen our intuition with several examples, then talk about duality and representability. Finally we define the famous Tutte polynomial, maybe the most important structural invariant encoding a lot of the matroid's combinatorial data.

1.1 Notations and conventions

Before we head straight into the depths of matroid theory I would like to state some notations and conventions to which this thesis complies.

Definition. A *list* or *multiset* X is a collection of elements which occur together with a certain multiplicity. More precisely it is a set, whose elements could be contained multiple times. For lists element- and sublist-relations, as well as list operations like union or intersection are defined analogously to set theory. Clearly, every set is also a list.

Example (Lists and sets). $X = \{a, b, b, c, c, c, c, d\}$ and $Y = \{a, b, c, d\}$ are lists with $Y \subseteq X$ but $X \neq Y$. Here Y is also a set, while X is not.

Notation. The *cardinality* of a list X is denoted by $|X|$. Since we work mainly with finite lists, the cardinality of X is just the number of elements counted with their multiplicities. Sometimes the cardinality of an instance X will also be denoted by $\#X$ but only in rare occasions where readability outweighs consistency.

If we want to stress that a union of lists X and Y is disjoint, we will denote it by $X \sqcup Y$ instead of simply writing $X \cup Y$.

As usual, the *empty list* is denoted by $\emptyset$ and the *power list of* X, i.e. the list of all sublists A of X, is denoted by $\mathcal{P}(X)$. Formally,

$$\mathcal{P}(X) = \{A \mid A \subseteq X\}.$$

For a sublist $A \subseteq X$ we write A^C for the complement of A in X, i.e. $A^C = X \setminus A$.

Example. Let $X = \{a, a, b\}$. Then $|X| = 3$ and

$$\mathcal{P}(X) = \{\emptyset, \{a\}, \{a\}, \{b\}, \{a, a\}, \{a, b\}, \{a, b\}, \{a, a, b\}\}$$

Moreover if $A = \{a\} \subseteq X$ is a sublist. Then we have the complement given by $A^C = X \setminus A = \{a, b\}$.

Notation. We denote by $[n]$ the set $\{1, 2, 3, \ldots, n\}$ containing the positive integers from 1 to $n \in \mathbb{N}$.

In matroid theory working with lists instead of sets yields some technical advantages. It is simply more convenient if we do not have to worry whether some constructions could lead to multiple elements in a set. Moreover lists are natural objects to observe when working in non-simple graphs with multiple edges between its nodes.

Definition (Graphs)**.** A *graph* is a pair $G = (V, E)$ of a list V of *vertices* or *nodes* and E a list of elements of the form $\{v_i, v_j\}, v_i, v_j \in V$ representing *edges* connecting the vertices v_i and v_j. In this thesis, we will always assume G to be a finite graph, i.e $|V| < \infty$.

- A *path* is a series of vertices $(v_1, v_2, \ldots, v_n), v_i \in V, i \in [n]$, such that $\{v_i, v_{i+1}\} \in E, \forall i \in [n-1]$. I.e. it is a walk starting from v_1 to reach v_n by moving along edges $\{v_i, v_{i+1}\}$. Moreover we are only allowed to pass any edge just once. [1]
- A *circuit* or *cycle* is a path $(v_1, v_2, \ldots, v_n)$ with $v_1 = v_n$. In words it is a path along edges whose starting point is also its destination point.
- A graph is called *connected* if for all vertices $x, y \in V$ there exists a path $(v_1, v_2, \ldots, v_n)$ with $x = v_1$ and $y = v_n$. I.e. there exists a path connecting any two vertices $x, y \in V$.
- A *forest* is a graph without any cycles.
- A connected forest is called a *tree*.

Example. Let $V = \{a, b, c, d, e\}$ be the set of vertices, and let

$$E = \{\{a, b\}, \{a, b\}, \{a, b\}, \{c, d\}, \{a, d\}, \{b, e\}, \{b, e\}\}$$

be our list of edges. Then the graph $G = (V, E)$ can be visualised by Figure 1.1. Then a path from c to e would be given by $P = (c, d, a, b, e)$. A circuit on the other hand is given by $C = (b, e, b)$. A tree would be induced by the sublist of edges $T = \{\{c, d\}, \{a, d\}, \{a, b\}, \{b, e\}\}$.

1.2 Essentials of matroid theory

It is now time to start working with matroids. Generally speaking, matroids are a combinatorial construction abstracting the notion of linear independence. Matroids are defined on systems of finite sets and appear in several different fields of mathematics

[1] In literature one often demands for a *path* to consist of vertices which are pairwise distinct. However, we stick to our less restricted definition.

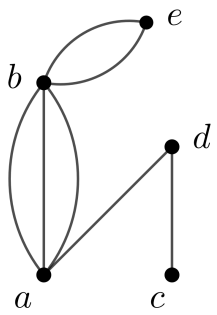

Figure 1.1: Visualisation of the graph $G = (V, E)$.

that do not seem to be be related to each other, at least at first sight. However, matroid theory is building bridges between them, extracting only the essence of their notions of independence. In this manner matroid theory is connecting graph theory with linear algebra. Further on we will see matroids defined upon finitely generated abelian groups and eventually also matroids that are given only by lists of rational numbers.

In applications matroids are used to count objects. Depending on where our matroid is defined we may count hyperplane arrangements in vector spaces, proper colourings of vertices in graphs or lattice points in convex zonotopes. All those concrete structures abstract to matroid theoretic objects that are encoded as specialisations of the so-called Tutte polynomial. There matroid theory does its magic and then eventually the abstract objects are realised and interpreted in the concrete setting.

In this section we give an introduction to the fundamental objects of this theory. We start by defining matroids via several different families of axioms and introduce the special terminology used in this field. Afterwards we discuss the aspects of duality and representability. Those concepts stress the strong connections between vector spaces and graphs. To do so, we follow the work of Oxley in his book *Matroid Theory* [Oxl92]. However, the notions presented could be found in any introductory script on matroid theory. At the end of this section we make ourselves familiar with the Tutte polynomial and its various forms and properties. All of this should serve as a solid backbone before we concern ourselves with the quite more advanced topic of *arithmetic matroids* which will truly generalise standard matroid theory.

1.2.1 Basic definitions

Let V be some vector space over a field $\mathbb{K}$, and let $X \subseteq V$ be a finite sublist of vectors. E.g. let $P \in M_{n\times m}(\mathbb{K})$ be an $n \times m$-matrix and let X be the list of its columns. Considering

this system of finite lists, we call an element $A \in \mathcal{P}(X)$ *independent*, if the elements in A are linearly independent as vectors in V. Let $\mathcal{I} \subseteq \mathcal{P}(X)$ be the *list of independent sublists of* X. We observe that the following properties are fulfilled:

(I1) $\emptyset \in \mathcal{I}$.

(I2) If $A \in \mathcal{I}$ and $B \subset A$ then also $B \in \mathcal{I}$. I.e. sublists of independent lists are independent.

(I3) $A, B \in \mathcal{I}$ and $|A| < |B|$ then there exists $e \in B \backslash A$ such that $A \cup \{e\} \in \mathcal{I}$.

This is rather obvious. The empty set is independent per default. Sublists of linearly independent lists are always linearly independent themselves and property (I3) refers to completing independent lists to a vector space basis.

Example. Let $P \in M_{3\times 4}(\mathbb{R})$ be given by

$$P = \begin{pmatrix} 1 & 0 & 1 & 4 \\ 0 & 0 & 0 & 5 \\ 1 & 0 & 1 & 4 \end{pmatrix}.$$

Therefore we get the list of its columns

$$X = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 4 \end{pmatrix} \right\},$$

and further the list of independent sublists

$$\mathcal{I} = \left\{ \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 4 \\ 5 \\ 4 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 4 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 4 \end{pmatrix} \right\} \right\}.$$

Considering this case it becomes rather clear why we prefer working with lists rather than sets. If we do not want to restrict the choice of our matrix P, multiple entries may occur naturally.

Now we change the setting. Let $G = (V, E)$ be a finite graph, with vertices $v \in V$ and edges $e \in E$. Regarding the system $\mathcal{P}(E)$ we call subsets of edges $A \in \mathcal{P}(E)$ *independent* if the subgraph $H = (V, A)$ induced by $A \subseteq E$ forms a forest, i.e. a graph without circuits. Let again $\mathcal{I} \subseteq \mathcal{P}(E)$ be the set of independent subsets of E. Then, astonishingly, we observe that $\mathcal{I}$ again fulfils the properties (I1)–(I3) from above: the empty set can not contain a circuit (since it does not contain anything) and subgraphs of forests remain being forests. This yields (I1) and (I2). For (I3) the reasoning is a little longer. Let $A, B \in \mathcal{I}$ be two independent sublists of edges with $|A| < |B|$. Additionally denote by $G_A := (V, A)$ and $G_B := (V, B)$ the subgraphs of G induced by A and B, respectively. Because of the independence, G_B must have less connected components than G_A. (Since there are no circuits, each edge is connecting two components that are not connected

otherwise.) Hence there are vertices $u, v \in V$ that are contained in the same component in G_B but are distributed to two different components in G_A. However, this tells us that there is a path leading from u to v in G_B that must pass an edge $e \in B \setminus A$. But now we already conclude that $A \cup \{e\}$ has to be independent, since if e was part of a circuit in $A \cup \{e\}$ then u and v would already have been connected in G_A, a contradiction.

However, thus we have found some notion of independence given by the axioms (I1)–(I3) which exists above classical linear algebra and graph theory. Therefore we are able to generalise, creating a new abstract concept of being independent.

Definition. A *matroid* $\mathcal{M}_X$ over a finite *groundlist* X is a pair $(X, \mathcal{I})$ with $\mathcal{I} \subseteq \mathcal{P}(X)$, such that $\mathcal{I}$ fulfils the axioms (I1), (I2) and (I3) stated above. The elements of $\mathcal{I}$ are called *independent lists*.

The name *matroid* originates from the term *matrix*. This is rather intuitive, as we have already seen, that the columns of any matrix over a field form a matroid.

Even though matroid theory is nowadays a discipline in mathematics on its own, strongly related to combinatorics, geometry or discrete optimisation, much of its terminology still refers to vector spaces and graph theory where the first matroids were defined. We will now give some basic notions of matroid theory as well as some reference to their origin.

Definition. Let $\mathcal{M}_X = (X, \mathcal{I})$ be a matroid over a finite list X.

- An element $B \in \mathcal{I}$ is called a *basis* if B is maximal in $\mathcal{I}$. I.e.

$$B \in \mathcal{I} \text{ is basis} :\Leftrightarrow (\forall A \in \mathcal{I} : B \subseteq A \Rightarrow B = A).$$

- A minimal dependent subset $C \subseteq X$ is called a *circuit*. Formally:

$$C \in \mathcal{P}(X) \setminus \mathcal{I} \text{ is a circuit} :\Leftrightarrow (\forall A \subsetneq C : A \in \mathcal{I}).$$

Clearly the term *basis* originates from finite dimensional linear algebra, where the bases of a vector space are exactly the maximal linearly independent subsets. However, the name *circuit* refers to the graph theoretical setting. There, by the definition of independence of sets of edges, the circuits are exactly given by those edges forming a cycle! Meanwhile, a basis of a graph is realised by a spanning tree. In Figure 1.2 we have two examples of identical graphs, where in the first one we marked their circuits, while in the second one we marked a possible basis (i.e. a spanning tree).

It is a well known fact that the matroid structure $\mathcal{M}_X$ is already determined by $\mathcal{B} \subseteq \mathcal{I}$ the list of bases. This can be deduced by the observation, that any independent list is contained in a basis, i.e.

$$A \in \mathcal{I} \Leftrightarrow \exists B \in \mathcal{B} : A \subseteq B.$$

The same is true for $\mathcal{C} \subseteq \mathcal{P}(X)$, the set of circuits, since a subset $A \subset X$ is *dependent* (i.e. not independent) if and only if there is some $C \in \mathcal{C}$ such that $C \subseteq A$. Therefore the following two definitions are strongly related to the one given above. In fact all collections of axioms deliver equivalent matroid structures. Some papers refer to this

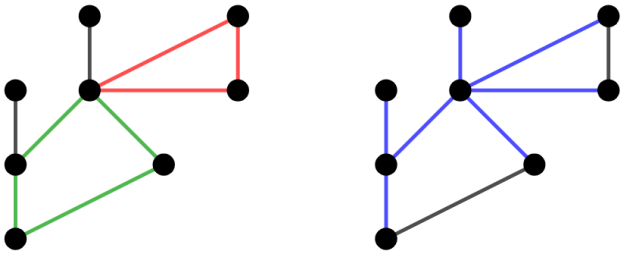

Figure 1.2: Circuits in red and green on the left and a basis marked in blue on the right.

property of matroids of being described in many different equivalent ways, as having *cryptomorphic* definitions (e.g. in [Pag20, Section 1]).

Definition (Basis axioms)**.** Let X be a finite list, $\mathcal{B} \subset \mathcal{P}(X)$, then the pair $(X, \mathcal{B})$ defines a matroid $\mathcal{M}_X$ if the following axioms hold:

(B1) $\mathcal{B} \neq \emptyset$.

(B2) For all bases $B_1, B_2 \in \mathcal{B}$ and for all $x \in B_1 \backslash B_2$ we have that there exists an element $y \in B_2 \backslash B_1$ such that
$$(B_1 \backslash \{x\}) \cup \{y\} \in \mathcal{B}.$$

Remark. The axiom (B2) is the matroid theoretical generalisation of the famous *Steinitz exchange lemma* from linear algebra. It also implies, that all bases of a matroid share the same cardinality. I.e. if $B_1, B_2 \in \mathcal{B}$ then $|B_1| = |B_2|$.

Corollary 1.2.1. *Let $G = (V, E)$ be a graph with k connected components ($k \in \mathbb{N}$), then all spanning forests in G contain the same number of edges, namely $|V| - k$. This is true since every spanning forest corresponds to a basis in the according graph matroid.*

Definition (Circuit axioms)**.** Let X be a finite list, $\mathcal{C} \subset \mathcal{P}(X)$, then the pair $(X, \mathcal{C})$ defines a matroid $\mathcal{M}_X$ if the following axioms hold:

(C1) $\emptyset \notin \mathcal{C}$.

(C2) If $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$ then $C_1 = C_2$.

(C3) For all $C_1, C_2 \in \mathcal{C}$ with $C_1 \neq C_2$ and $x \in C_1 \cap C_2$ we have the existence of a circuit $D \in \mathcal{C}$ such that
$$D \subseteq (C_1 \cup C_3) \backslash \{x\}.$$

Example. Observe the small real valued matrix given by
$$P = \begin{pmatrix} 1 & 0 & 0 & 4 \\ 0 & 1 & 0 & 3 \end{pmatrix}.$$

We let again X be the list of its columns. If we consider the induced matroid $\mathcal{M}_X$ then we obtain the following list of bases:

$$\mathcal{B} = \left\{ \left\{ \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \right\}, \left\{ \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}4\\3\end{pmatrix} \right\}, \left\{ \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}4\\3\end{pmatrix} \right\} \right\}.$$

The independent sets in $\mathcal{I}$ are then given as all possible subsets of elements of $\mathcal{B}$. Moreover we obtain the following list of circuits:

$$\mathcal{C} = \left\{ \left\{ \begin{pmatrix}0\\0\end{pmatrix} \right\}, \left\{ \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}4\\3\end{pmatrix} \right\} \right\}.$$

The relation with linear algebra suggests another crucial definition. In a vector space V the cardinality of a maximal independent set (hence a basis) is called the *dimension* of V and is usually denoted by $\dim(V)$. In the more general case of a module M over a ring R the derived notion is then called the *rank* of the module and is denoted by $\mathrm{rk}(M)$. We have already seen, that in a matroid $\mathcal{M}_X = (X, \mathcal{B})$ all bases have the same cardinality. Therefore the *rank of* $\mathcal{M}_X$ is well defined: $\mathrm{rk}(\mathcal{M}_X) = |B|$, where $B \in \mathcal{B}$ is an arbitrary basis.
Moreover, given a matroid $\mathcal{M}_X$ on a groundlist X it is easy to check that for each $A \subseteq X$ we obtain an induced matroid $\mathcal{M}_A$ with A as new groundlist. (Use: $C \subseteq A$ is independent in $\mathcal{M}_A$ if C is independent as a subset of X in $\mathcal{M}_X$.) Therefore also the value $\mathrm{rk}(\mathcal{M}_A)$ is well defined.
In conclusion we have established a *rank function*:

$$\begin{aligned} \mathrm{rk} : \mathcal{P}(X) &\to \mathbb{N} \cup \{0\} \\ A &\mapsto \mathrm{rk}(\mathcal{M}_A). \end{aligned}$$

By abuse of notation we will simply write $\mathrm{rk}(A)$ instead of $\mathrm{rk}(\mathcal{M}_A)$.
Using the notion of the rank, one can characterise the bases of a matroid as the minimal lists (with respect to inclusion) which have maximal rank. Therefore since the rank function determines the bases, which again determine the matroid, it is no wonder that we are able to define the whole matroid structure in terms of the rank function.

Definition (Rank axioms)**.** A matroid $\mathcal{M}_X = (X, \mathrm{rk})$ is a finite list X together with a rank function $\mathrm{rk} : \mathcal{P}(X) \to \mathbb{N} \cup \{0\}$ such that the following axioms are satisfied:

(R1) If $A \subseteq X$, then $\mathrm{rk}(A) \leq |A|$.

(R2) If $A, B \subseteq X$ and $A \subseteq B$ then $\mathrm{rk}(A) \leq \mathrm{rk}(B)$.

(R3) If $A, B \subseteq X$, then $\mathrm{rk}(A \cup B) + \mathrm{rk}(A \cap B) \leq \mathrm{rk}(A) + \mathrm{rk}(B)$.

The following proposition gives a formal characterisation of our basic objects using the rank function. (See also [Oxl92, Prop. 1.3.5].)

Proposition 1.2.2. *Let $\mathcal{M}_X$ be a matroid with rank function* rk *and let $A \subseteq X$. Then*

(i). A is independent if and only if $\mathrm{rk}(A) = |A|$.

(ii). A is a basis if and only if $\mathrm{rk}(A) = |A| = \mathrm{rk}(\mathcal{M}_X)$.

(iii). A is a circuit if and only if $A \neq \emptyset$ and for all $x \in A$:

$$\mathrm{rk}(A \backslash \{x\}) = \mathrm{rk}(A) = |A| - 1.$$

Proof. The proof follows immediately from the definitions already given and is rather intuitive considering the basic examples of matroids over vector spaces or graphs. □

The mathematician Poincaré once said: *Mathematics is the art of giving the same name to different things.* And indeed, matroid theory is a formidable example for this, finding similar structures by comparing fairly different things. The main tool for showing that two mathematical structures are abstractly the same is the notion of an *isomorphism*. These are also well defined for the matroid setting.

Definition. An *isomorphism* between matroids $\mathcal{M}_X$ and $\mathcal{M}_Y$ is a bijection $\phi : X \to Y$, such that ranks are preserved. I.e. if we have $X = \{x_1, x_2, \ldots, x_n\}$ and $Y = \{y_1, y_2, \ldots, y_n\}$, and if $\phi : X \to Y$ with $\phi(x_i) = y_i$ for all $i \in [n]$ is a bijection between those lists, then ϕ also lifts to a bijection $\phi : \mathcal{P}(X) \to \mathcal{P}(Y)$ and vice versa. In this case, ϕ is an isomorphism of matroids if $\mathrm{rk}_X(A) = \mathrm{rk}_Y(\phi(A))$ holds for all $A \subseteq X$. If such an isomorphism exists, we call $\mathcal{M}_X$ and $\mathcal{M}_Y$ *isomorphic* and write $\mathcal{M}_X \cong \mathcal{M}_Y$.

Remark. As matroid theory adapts and unifies many classical properties from either vector spaces or graphs, the question arises, if there is some kind of morphism relating their independence structures. Indeed, following the instructions of [Moc11, Remark 2.3.], we consider a graph $G = (V, E)$ with $V = \{v_1, \ldots, v_n\}$ its set of vertices and E its list of edges. Now we take a vector space $\widetilde{U}$ with basis $\{e_1, e_2, \ldots, e_n\}$ bijective to V. With an edge $\{v_i, v_j\} \in E$ we associate the vector $e_i - e_j \in \widetilde{U}$. By doing so we obtain a list $X = \{e_i - e_j \mid \{v_i, v_j\} \in E\}$ bijective to E and spanning a hyperplane U in $\widetilde{U}$. Under the bijection $X \leftrightarrow E$ forests correspond to linearly independent subsets and ranks are preserved. Hence the construction delivers an isomorphism of matroids $\mathcal{M}_E \cong \mathcal{M}_X$.

Definition. A matroid $\mathcal{M}_X$ is called a *graph matroid* (sometimes also *graphoid*) if it is isomorphic to a matroid $\mathcal{M}_E$ with E the set of edges of a graph $G = (V, E)$. Moreover, a matroid is called $\mathbb{K}$-*representable* if it is isomorphic to a matroid $\mathcal{M}_A$ given by a matrix A with entries $a_{ij} \in \mathbb{K}$.

Corollary 1.2.3. *By the previous remark, every graph matroid is representable over any field* $\mathbb{K}$.

Representability is a central property one might ask for a matroid. Of all used to construct matroids, vector spaces appear to be the computationally most practical. Moreover, linear algebra is a throughout well studied field. Hence, once you know that a

given matroid is representable, you might prefer to transfer it to a matrix and do your operations there, where even a computer algebra system may help out.

Another major topic is *duality*. The duality relation originates from planar graphs but adapts smoothly into matroid theory opening the door for different duality concepts in various mathematical setups. We start by the intuitive description in planar graphs and then move on to generalising the notion for abstract matroids.

1.2.2 Duality

A graph G is called planar if it can be embedded in the plane, i.e. simply speaking it can be drawn on a sheet of paper such that none of its edges are intersecting each other. In such a visualisation of a graph G we obtain another graph G^* by following certain construction steps:

1. In every area surrounded by edges of G, as well as in the unique unbound region, draw a vertex associated to the very region.

2. Every edge in G has a region to its left and one to its right. For every edge in G connect the vertices drawn in the left and right region by a line leading through the regarded edge of G. If the region at both sides of the edge is the same, then connect the vertex of it with itself.

The vertices set in the regions will be the vertices of G^*, the lines connecting them will be its edges. In Figure 1.3 we see a visual example of the stated construction.

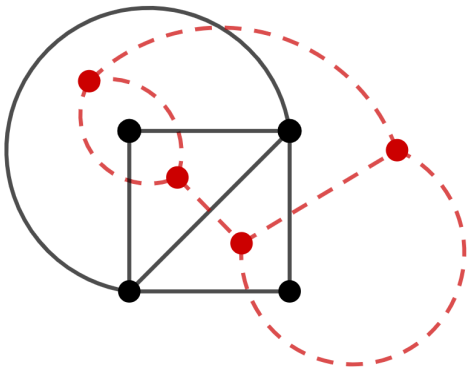

Figure 1.3: A graph (black) and its dual graph (red).

It is a result from graph theory that G^* is well defined, independent of the visualisation of G in the plane, and is unique up to isomorphism. The newly constructed graph G^* is

then called the *dual graph of* G.

At least in the picture above (Fig. 1.3) one can convince themselves that $(G^*)^* = G$ holds. This is a general result from graph theory which we will not prove here. Instead we translate this concept into matroid theory. The following statements and definitions as well as their proofs can be found in [Oxl92, 2.1.].

Theorem 1.2.4 (Dual matroid)**.** *Let $\mathcal{M}_X = (X, \mathcal{B})$ be a matroid defined by its list of bases $\mathcal{B}$. Define $\mathcal{B}^* := \{X\backslash B \mid B \in \mathcal{B}\}$. Then $\mathcal{B}^*$ is the list of bases of a matroid on X.*

Definition. The matroid $\mathcal{M}_X^* := (X, \mathcal{B}^*)$ given by the previous theorem is called the *dual of* $\mathcal{M}_X$. By the definition of $\mathcal{M}_X^*$ it is clear that $(\mathcal{M}_X^*)^* = \mathcal{M}_X$.

Definition. A basis of $\mathcal{M}_X^*$ is called a *cobasis* of $\mathcal{M}_X$.
In the same manner, circuits and independent sets of $\mathcal{M}_X^*$ are *cocircuits* and *coindependent sets* of $\mathcal{M}_X$.
Given a matroid $\mathcal{M}_X$, the *rank function of its dual* is denoted by rk^* and is called the *corank*.

By definition, we have $\mathrm{rk}(X) = |B|$ for some basis $B \in \mathcal{B}$. However, if $B \in \mathcal{B}$ then $X\backslash B \in \mathcal{B}^*$ and therefore $\mathrm{rk}^*(X) = |X\backslash B|$. Hence for a matroid $\mathcal{M}_X$ over a finite list X we have (see [Oxl92, 2.1.8]):

$$\mathrm{rk}(X) + \mathrm{rk}^*(X) = |X|.$$

With a little more reasoning on the correlation between bases and cobases one can deduce the following:

Proposition 1.2.5. *Let X be a finite list inducing a matroid $\mathcal{M}_X$. Then for all sublists $A \subseteq X$ the rank of A in the dual $\mathcal{M}_X^*$ is given by*

$$\mathrm{rk}^*(A) = |A| - \mathrm{rk}(X) + \mathrm{rk}(X\backslash A).$$

Statement and detailed *proof* can be found in [Oxl92, 2.1.9 & 2.1.10]. Sometimes when studying matroids we find ourselves confronted with very small dependent subsets. In fact, it can easily happen that a single element of the groundlist is already dependent. Conversely, an element can be crucial to be contained in any basis. This leads to the distinction of loops, coloops and so-called proper vectors, which has turned out very useful in induction proofs of matroid identities.

Definition. Let $\mathcal{M}_X$ be a matroid. As a reference to the linear case, the elements of the groundlist X are also called *vectors*.

- A vector $v \in X$ is called a *loop* if $\{v\}$ is a circuit.
- A vector $v \in X$ is called a *coloop* if $\mathrm{rk}(X\backslash\{v\}) = \mathrm{rk}(X) - 1$.
- A vector v is called *proper* if it is neither a loop nor a coloop.

The terminology originates from graph theory, where the name loop becomes very visual. A coloop is called a **co**loop since it is a loop in the dual. The following examples give intuitive descriptions of loops and coloops in the most prominent cases of graphs and vector spaces.

Example. In graphs and vector spaces, loops and coloops are very easy to detect.

(1) In a graph matroid, a loop is given by an edge $e = \{v, v\}$ having the same starting- and ending node, while a coloop is also called a *bridge* i.e. an edge f which is not contained in any cycle. See Figure 1.4 for a visual example.

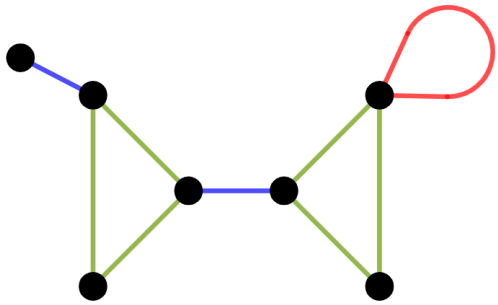

Figure 1.4: Loops, bridges/coloops and proper edges of a graph.

(2) In a matroid given by a matrix over a field $\mathbb{K}$, a loop is given by a zero vector $0 \in \mathbb{K}^d$, while a coloop is a vector linearly independent of all other vectors in the matroid. For example if X is the list of columns of the real matrix

$$\begin{pmatrix} 0 & 3 & 4 & 5 \\ 0 & 6 & 7 & 8 \\ 9 & 0 & 0 & 0 \end{pmatrix}$$

then the first column-vector $(0, 0, 9)$ is the only coloop.

It turns out that loops and coloops behave very pleasantly when regarding duality. Their relations are summarised in the next proposition.

Proposition 1.2.6. *If $x \in X$ is a loop in a matroid $\mathcal{M}_X$, then x is a coloop in $\mathcal{M}_X^*$. Vice versa, if x is a coloop in $\mathcal{M}_X$ then it is a loop in $\mathcal{M}_X^*$. However, x proper remains proper in the dual.*

Proof. Let $v \in X$ be a loop. Then by using Proposition 1.2.5 we compute

$$\begin{aligned}\mathrm{rk}^*(X\backslash\{v\}) &= |X\backslash\{v\}| - \mathrm{rk}(X) + \mathrm{rk}(X\backslash(X\backslash\{v\})) = \\ &= |X| - 1 - \mathrm{rk}(X) + \mathrm{rk}(\{v\}) = \\ &= |X| - 1 - \mathrm{rk}(X) = \mathrm{rk}^*(X) - 1.\end{aligned}$$

Therefore v is a coloop in the dual.
If however v is coloop in the original matroid then

$$\begin{aligned}\mathrm{rk}^*(\{v\}) &= |\{v\}| - \mathrm{rk}(X) + \mathrm{rk}(X\backslash\{v\}) = \\ &= 1 - \mathrm{rk}(X) + \mathrm{rk}(X) - 1 = 0.\end{aligned}$$

Hence, $\{v\}$ is a cocircuit. The rest of the statement follows by $(\mathcal{M}_X^*)^* = \mathcal{M}_X$. □

Remark. Loops and coloops are very important objects in the theory of arithmetic matroids, as they form so called *molecules* (see Section 2.1.1), a very simple matroid structure at the basis of the theory. We may therefore give another very useful and maybe more intuitive characterisation of loops and coloops.

- $v \in X$ is a loop $\Leftrightarrow$ v is not contained in any basis.
- $v \in X$ is a coloop $\Leftrightarrow$ v is not contained in any circuit $\Leftrightarrow$ v is contained in every basis.

1.2.3 Deletion and contraction

We are now going to introduce two very fundamental transformations on matroids. Those will let us reduce more complex matroids step by step to a collection of simple ones. Many statements in matroid theory, especially about the so called Tutte polynomial (see Section 1.2.4), are proven by simplifying an arbitrary matroid to a very basic form, where the statement might be trivial.

To give an overview of what is actually happening, we again train our intuition in the setting of graphs! Let $G = (V, E)$ be a graph with edges in E. Choose an edge $e \in E$. Now consider two new graphs:
The *deletion of* G by e, often denoted as $G\backslash e$ is the subgraph of G given by

$$G\backslash e := (V, E\backslash\{e\}).$$

However, the *contraction of* G by $e = \{v_1, v_2\}$ $(v_1, v_2 \in V)$ is the graph G/e given by

$$G/e := (\widetilde{V}, \widetilde{E})$$

where $\widetilde{V} := V\backslash\{v_1, v_2\} \cup \{\widetilde{v}\}$ and for all $x, y \in \widetilde{V}$ we have that $\{x, y\} \in \widetilde{E}$ if and only if $\{x, y\} \in E$, or $x = \widetilde{v}$ and $\exists i \in \{1, 2\} : \{v_i, y\} \in E$. What the last definition essentially means is, that we take the edge e and contract it. Therefore its start- and ending node fall together and are identified with each other, $v_1 = v_2 = \widetilde{v}$. Both operations are visualised

in the three pictures below. Here we have a given graph in Figure 1.5 with a marked edge $e = \{u, v\}$, followed by Figures 1.6 and 1.7 visualising the deletion and contraction of the graph by e, respectively. Here we beautifully see how the edge e vanishes in the deletion of the graph, while in the contraction graph the vertices v and u simply fall together.

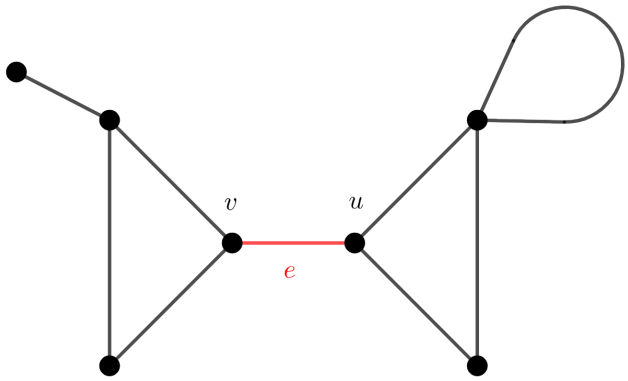

Figure 1.5: A graph with an distinct edge $e = (u, v)$.

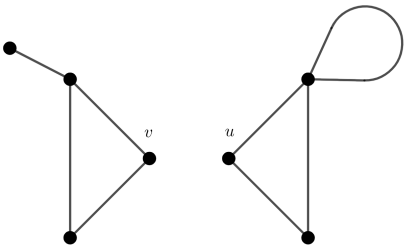

Figure 1.6: Deletion of edge e.

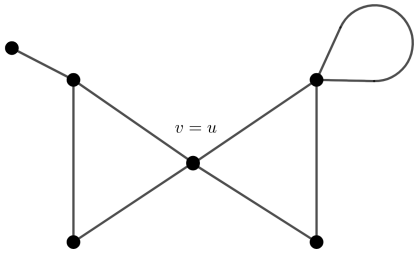

Figure 1.7: Contraction of edge e.

Remark. To stress the importance of these operations we consider again the situation of graphs. Since the birth of graph theory mathematicians all over the world have concerned themselves with the possible colourings of the vertices of a graph in a way that neighbouring vertices are assigned different colours. Such a colouring is called *proper* if neighbouring vertices are assigned different colours. Indeed, many questions in computational science and combinatorics are closely related to the colouring of a graph with a given number $\lambda \in \mathbb{N}$ of colours.
The *chromatic polynomial* of a graph G is the function $\chi_G : \mathbb{N} \to \mathbb{N}$ that assigns to every number λ of colours the number $\chi_G(\lambda)$ of different proper colourings of G. One can

prove that χ_G fulfils the deletion-contraction recurrence:

$$\chi_G(\lambda) = \chi_{G\setminus e}(\lambda) + \chi_{G/e}(\lambda), \quad \forall \lambda \in \mathbb{N}, \forall e \in E.$$

Using this, it is shown that $\chi_G(\lambda)$ is indeed a polynomial in λ for all graphs G, moreover it is possible to compute $\chi_G(\lambda)$ recursively.

Now we would like to generalise these operations to matroids.

Definition ([Oxl92, p.22, p.106])**.** Let $\mathcal{M}_X$ be a matroid on a finite list X and let $Y, Z \subseteq X$.

- The *restriction* of $\mathcal{M}_X$ to Y is the matroid $\mathcal{M}_{X|Y}$ whose groundlist is Y and $A \subseteq Y$ is independent if A is independent in X.
- The *deletion* of $\mathcal{M}_X$ by Z is the matroid $\mathcal{M}_{X\setminus Z}$ whose groundlist is $X\setminus Z$ and $A \subseteq X\setminus Z$ is independent if A is independent in X.
- The *contraction* of $\mathcal{M}_X$ to $X\setminus Z$ is the matroid $\mathcal{M}_{X/Z}$ whose groundlist is again $X\setminus Z$ and if B_Z is a basis for $\mathcal{M}_{X|Z}$ then $A \subset X\setminus Z$ is independent if $A \cup B_Z$ is independent in $\mathcal{M}_X$.

Remark. Clearly, the restriction of $\mathcal{M}_X$ to Y is the same as the deletion of $\mathcal{M}_X$ by $X\setminus Y$. I.e. $\mathcal{M}_{X\setminus(X\setminus Y)} = \mathcal{M}_{X|Y}$. Moreover the contraction $\mathcal{M}_{X/Z}$ can be interpreted as the dual construction of the deletion. In particular we have that (see [Oxl92, Prop. 3.1.4])

$$\mathcal{M}_{X/Z} = (\mathcal{M}^*_{X\setminus Z})^*.$$

Proposition 1.2.7 ([Oxl92, Prop. 3.1.6])**.** *Let $\mathcal{M}_X$ be a matroid and $T \subseteq X$. Then for all sublists $A \subseteq X \setminus T$ we have*

(a) $\mathrm{rk}_{\mathcal{M}_{X\setminus T}}(A) = \mathrm{rk}_{\mathcal{M}_X}(A)$,

(b) $\mathrm{rk}_{\mathcal{M}_{X/T}}(A) = \mathrm{rk}_{\mathcal{M}_X}(A \cup T) - \mathrm{rk}_{\mathcal{M}_X}(T)$.

Proof. The assertion in (a) is obvious from the definition of independent lists of $\mathcal{M}_{X\setminus T}$. It remains to check (b).

(b): By the remark above we have $\mathrm{rk}_{\mathcal{M}_{X/T}}(A) = \mathrm{rk}_{(\mathcal{M}^*_{X\setminus T})^*}(A)$.
Using $\mathrm{rk}^*(A) = |A| - \mathrm{rk}\, X + \mathrm{rk}(X\setminus A)$ we compute:

$$\begin{aligned}
\mathrm{rk}_{\mathcal{M}_{X/T}}(A) &= |A| - \mathrm{rk}_{M^*_{X\setminus T}}(X \setminus T) + \mathrm{rk}_{M^*_{X\setminus T}}(X\setminus A) \\
&= |A| - \mathrm{rk}^*(X \setminus T) + \mathrm{rk}^*(X \setminus (A \cup T)) \\
&= |A| - \big(|X \setminus T| - \mathrm{rk}(X) + \mathrm{rk}(T)\big) + \\
&\quad + \big(|X \setminus (A \cup T)| - \mathrm{rk}(X) + \mathrm{rk}(A \cup T)\big)
\end{aligned}$$

Now as $A \subseteq X \setminus T$ we obtain $|A| - |X \setminus T| + |X \setminus (A \cup T)| = 0$ and therefore indeed

$$\mathrm{rk}_{\mathcal{M}_{X/T}}(A) = \mathrm{rk}_{\mathcal{M}_X}(A \cup T) - \mathrm{rk}_{\mathcal{M}_X}(T).$$

□

Notation. We will write $\mathcal{M} := \mathcal{M}_X$ and for $T \subseteq X$ let $\mathcal{M} \setminus T := \mathcal{M}_{X \setminus T}$ denote the deletion by T and $\mathcal{M}/T := \mathcal{M}_{X/T}$ the contraction by T, respectively.

The following three results are important for the definition of minors, but as they will not play any major role in the further theory of arithmetic matroids I refer to their proofs in [Oxl92].

Proposition 1.2.8 ([Oxl92, 3.1.24])**.** *Let X be a finite list defining a matroid $\mathcal{M}$ and let $T \subseteq X$ be a sublist. Then we have*

$$\mathcal{M} \setminus T = \mathcal{M}/T \Leftrightarrow \mathrm{rk}(T) + \mathrm{rk}(X \setminus T) = \mathrm{rk}(X).$$

Corollary 1.2.9 ([Oxl92, 3.1.25])**.** *Using the same notations as before, we deduce that $\mathcal{M} \setminus e = \mathcal{M}/e$ if and only if $e \in X$ is either loop or coloop.*

Eventually the following proposition tells us that deletion and contraction fulfil very fine commutativity relations. In other words, we do not have to mind which operation we apply first or last. The result will remain the same up to isomorphism.

Proposition 1.2.10 ([Oxl92, 3.1.26])**.** *Let again X be a finite list generating a matroid $\mathcal{M}$. Moreover let $T_1, T_2 \subseteq X$ be disjoint sublists. Then the following three identities hold.*

(i). $(\mathcal{M} \setminus T_1) \setminus T_2 = (\mathcal{M} \setminus T_2) \setminus T_1 = \mathcal{M} \setminus (T_1 \sqcup T_2)$.

(ii). $(\mathcal{M}/T_1)/T_2 = (\mathcal{M}/T_2)/T_1 = \mathcal{M}/(T_1 \sqcup T_2)$.

(iii). $(\mathcal{M} \setminus T_1)/T_2 = (\mathcal{M}/T_2) \setminus T_1$.

Definition ([Oxl92, p.109])**.** By the proposition above, every sequence of deletions and contractions in a matroid $\mathcal{M} = \mathcal{M}_X$ can be summarised by an expression of the form $(\mathcal{M} \setminus T)/S$ for a pair of disjoint subsets $T, S \subseteq X$. Matroids of this structure are called *minors* of $\mathcal{M}$.

Deletion and restriction play a major role when it comes to analysing or computing Tutte polynomials, as we will see in the next section.

1.2.4 The Tutte polynomial

In this last section of the first chapter we discuss the basic properties of the ordinary Tutte polynomial. This serves more or less as an orientation for readers, who are familiar with classical matroid theory. Thus for experts, the following identities will be common knowledge. We also will not prove any of the results stated here, because in the next two parts of this thesis we will define so-called *arithmetic* Tutte polynomials which embody a true generalisation of ordinary Tutte polynomials. We will see proofs for their generalised identities. The statements of this section will therefore follow as corollaries. However, we start directly with the crucial definition.

Definition ([Moc11, 2.1])**.** Given a matroid $\mathcal{M}$ over a finite list X, its *Tutte polynomial* is defined as

$$T_{\mathcal{M}}(x,y) := \sum_{A \subseteq X} (x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)}.$$

This simple expression may be one of the most important invariants of matroids, since it encodes a lot of the underlying matroid's combinatorial structure. For example, just by regarding the definition, one concludes that $T(1,1)$ equals the number of bases in $\mathcal{M}_X$. In graphs, the Tutte polynomial was originally called the *dichromatic polynomial* because of its strong relation to the chromatic polynomial defined above (see [Tut54, 3.] and compare with 1.2.14).

We are now going to list several well known identities for the classical Tutte polynomial. Firstly, just like the chromatic polynomial, the Tutte polynomial acts very nicely when it comes to deletion and contraction of matroids. In particular the following famous recursion holds (see for example [Moc11, Thm. 3.1]).

Proposition 1.2.11. *Let $\mathcal{M} = \mathcal{M}_X$ be a matroid over a list X and let $e \in X$ be a proper vector. Then for the Tutte polynomial $T_{\mathcal{M}}$ of $\mathcal{M}$ we have*

$$T_{\mathcal{M}}(x,y) = T_{\mathcal{M}\setminus e}(x,y) + T_{\mathcal{M}/e}(x,y),$$

where $\mathcal{M}\setminus e$ and $\mathcal{M}/e$ again denote the deletion and contraction by e respectively.

There are several ways to build up a complicated matroid out of multiple simpler ones. Beside the deletion-contraction recurrence, matroids may also be given as a so-called *direct sum* of smaller matroids.

Definition ([MD12, 4.6.], [Oxl92, 4.2.12])**.** Given matroids $\mathcal{M} = (X, \mathcal{I})$ and $\mathcal{N} = (Y, \mathcal{J})$ with independence-lists $\mathcal{I}$ and $\mathcal{J}$ and such that $X \cap Y = \emptyset$, we can construct a new matroid denoted by $\mathcal{M} \oplus \mathcal{N} = (Z, \mathcal{K})$ with $Z = X \sqcup Y$ and $\mathcal{K} = \{A \cup B \mid A \in \mathcal{I} \text{ and } B \in \mathcal{J}\}$. This creation is called the *direct sum* of matroids.

This corresponds directly with the direct sum of vector spaces and the disjoint union of graphs. Again we observe that the Tutte polynomial behaves very well when in symbiosis with the direct sum.

Proposition 1.2.12. *One has in terms of Tutte polynomials:*

$$T_{\mathcal{M}\oplus\mathcal{N}}(x,y) = T_{\mathcal{M}}(x,y) \cdot T_{\mathcal{N}}(x,y).$$

A recursion is not only given by deletion and contraction. Also when concerning restriction and contraction, the Tutte polynomial fulfils astonishing identities. Kook, Reiner and Stanton [KRS99, Thm. 1] established a so-called *convolution formula* for the Tutte polynomial $T_{\mathcal{M}}$ of a matroid $\mathcal{M}$ over a groundlist X.

Theorem 1.2.13. *The Tutte polynomial of a matroid $\mathcal{M}$ fulfils*

$$T_{\mathcal{M}}(x,y) = \sum_{A \subseteq X} T_{\mathcal{M}|_A}(0,y) T_{\mathcal{M}/A}(x,0),$$

where $\mathcal{M}|_A$ denotes the restriction of $\mathcal{M}$ to $A \subseteq X$ and $\mathcal{M}/A$ the contraction.

Since its first appearance the Tutte polynomial has risen to undeniable relevance for the whole field of graph- and matroid theory. As always, mathematicians are both delighted and fascinated when they discover that certain structures behave polynomially. However, such an insight comes with a difficult task. Because if we have a polynomial, whose values come with various combinatorial meanings, then what about the single coefficients? We have to ask, how can the coefficients of the Tutte polynomial be interpreted?

This leads to another important notion in matroid theory, namely the one of *internal* and *external activity*. This will deliver a combinatorial formula for the Tutte polynomial over a matroid by a famous theorem of Crapo [Cra69]. In fact, Tutte himself originally defined his *dichromatic polynomial*, which finally was named after him, using the concept of internal/external activity in graphs (see [Tut54, 3.]). Crapo then proved that this coincides with our modern definition of the Tutte polynomial.
The following definition for the matroid theoretic setup is taken from [MD12, Section 4.1].

Definition. Let X be the groundlist of a matroid. Fix a total order on X and extract a basis B of X. We call $v \in X \setminus B$ *externally active on* B if v is dependent on the list of elements of B following it (with respect to the total order). On the other hand, we call $v \in B$ *internally active on* B if v is externally active on the complement $B^C = X \setminus B$ in the dual matroid. (There B^C is a basis.)
The number of externally active elements on B is denoted by $e(B)$ and is called the *external activity on* B. Dually, $i(B) = e^*(B^C)$ denotes the number of internally active elements on B, called the *internal activity on* B.

Using this, we get the following theorem by Crapo:

Theorem 1.2.14. *The Tutte polynomial of a matroid $\mathcal{M}_X$ over a list X can be written in the following way:*

$$T_{\mathcal{M}_X}(x,y) = \sum_{\substack{B \subseteq X, \\ B \text{ basis}}} x^{e^*(B^C)} y^{e(B)}.$$

Remark. In particular, observe that although we fixed an arbitrary total ordering on X, inducing our external and internal activities, the resulting Tutte polynomial is independent of our choice of the ordering. For graphs this was already proven by Tutte. [Tut54, p. 85–88]

Remark. Gessel and Sagan [GS96] give some more comprehensible and less abstract definitions of external/internal activity in the case of graphs:
In a graph $G = (V, E)$ a basis is given by a spanning forest $T \subseteq E$. Given a total ordering on E, an edge $e \in E \setminus T$ is called *externally active on* T if it is the least edge in the

unique cycle of $T \cup \{e\}$ (according to the total ordering). On the other hand $e \in T$ is *internally active* if it is the least edge in the unique cocycle contained in $(G \setminus T) \cup \{e\}$ ([GS96, p.2]) (in this setting, a *cocycle* is a minimal seperating set).

All of the identities stated above are also fulfilled in the case of arithmetic matroids. Also we will see proofs for them in Chapter 3. Our main goal is now to generalise the theory introduced here to the arithmetic case. There, many structural advantages apply. The major purpose of considering an arithmetic matroid is that we are able to capture a lot more information in our arithmetic Tutte polynomial than only simple dependency relations. That insight opens great new opportunities for modern matroid theory and may be one of the latest big steps in this active research field.

2 Arithmetic matroids

In this chapter we finally start our journey into the depths of the modern theory of arithmetic matroids. In 2011 Luca Moci [Moc11] established his Tutte polynomial for toric arrangements encoding combinatorial data of subgroups and quotients of (geometric) lattices. Being finitely generated abelian groups, they are always isomorphic to a free group $F \cong \mathbb{Z}^r$ times a torsion group $T \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$. While the lattice structure of F provides a matroid in a canonical way, the combinatorial data given by T, e.g. the number of *toric arrangements*, is lost when only observing independence relations. Moci confronted this problem by equipping the resulting matroid with a so called *multiplicity function* that captures further combinatorial information of the underlying structure.

This construction yields a perfect setup to study toric arrangements and zonotopes. But shortly afterwards Moci and D'Adderio [MD12] extracted the necessary axioms to generalise their ideas to the notion of arithmeitic matroids. Since then the topic emerged to a beautiful theory of never ending possibilities, with applications in combinatorics, geometry, graph theory and abstract algebra.

The focus of this chapter will lie on the purely structural aspects of arithmetic matroids. We introduce the notion of *multiplicity functions* on matroids and will state the necessary axioms that this function has to satisfy to generate an arithmetic matroid. Moreover we will construct the two main examples of arithmetic matroids, which correspond to finitely generated abelian groups and labelled graphs.

After that we show how the notions of *duality* and *representability* extend to arithmetic matroid theory. Eventually we are going to define *deletion*, *contraction* and *restriction* operations on arithmetic matroids as a preparation to prove identities for the arithmetic Tutte polynomial in the next chapter.

2.1 Basic definitions and examples of arithmetic matroids

In this section we discuss the possibilities of regarding certain multiplicity functions on matroids. In the most general case this will lead to so-called *multiplicity matroids*. If those multiplicities fulfil further properties we might get what we will call an *arithmetic matroid*. In the first subsection we state the different systems of axioms, provided by different sources, that define arithmetic matroids. Eventually we will discuss their equivalence. We also introduce the notion of so-called *molecules* which embody a central structure in this field.

Afterwards we construct arithmetic matroids over finitely generated abelian groups and give some examples. Those are especially important since later on we are going to

refer to them as exactly being the *representable arithmetic matroids*.

2.1.1 Multiplicities

Like described before, the main purpose of considering the little more complicated case of *arithmetic* matroids is to involve more of the underlying combinatorial information on the matroid in our Tutte polynomial. This is done by considering a second function $\mathfrak{m} : \mathcal{P}(X) \to \mathbb{Z}$ besides the rank function. This *multiplicity function* assigns to every sublist $A \subseteq X$ an integer $\mathfrak{m}(A)$ that could represent some data. However, a priori we may allow any kind of function to apply. This directly leads to the definition of a matroid with a multiplicity ([Moc11, 2.1]).

Definition. A *multiplicity matroid* is a pair $(\mathcal{M}, \mathfrak{m})$, with $\mathcal{M}$ a matroid over a finite list X and $\mathfrak{m}$ a mapping $\mathfrak{m} : \mathcal{P}(X) \to \mathbb{Z}$.
Its *multiplicity Tutte polynomial* is then defined by

$$M(x, y) = \sum_{A \subseteq X} \mathfrak{m}(A)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)}.$$

For the definition of a multiplicity matroid, we do not demand any further constraints on the multiplicity function. Any arbitrary function on any arbitrary matroid delivers a multiplicity matroid. Therefore also the multiplicity Tutte polynomial could appear in various shapes. In particular also negative coefficients are possible, hence the multiplicity Tutte polynomial cannot be considered a *combinatorial object* in general. Nevertheless choosing an appropriate multiplicity could yield a new Tutte polynomial containing an enormous amount of encoded combinatorial information.

Moci and D'Adderio defined the essential properties for $\mathfrak{m}$ to generate a whole new class of combinatorial structures generalising and adapting classical matroid theory, namely so-called *arithmetic matroids*. The first defining system of axioms was given in [MD12, 2.3.] and they were formulated as follows:

Definition. A multiplicity matroid $(\mathcal{M}_X, \mathfrak{m})$ is called an *arithmetic matroid* if the multiplicity function $\mathfrak{m} : \mathcal{P}(X) \to \mathbb{N}\setminus\{0\}$ fulfils the following five properties:

(AM1) If $A \subseteq X$ and $v \in X$ is dependent of A, then $\mathfrak{m}(A \cup \{v\})$ divides $\mathfrak{m}(A)$.

(AM2) If $A \subseteq X$ and $v \in X$ is independent of A, then $\mathfrak{m}(A)$ divides $\mathfrak{m}(A \cup \{v\})$.

(AM3) If $A \subseteq B \subseteq X$ and $B = A \sqcup F \sqcup T$ is a disjoint union such that for all $A \subseteq C \subseteq B$ we have that $\mathrm{rk}(C) = \mathrm{rk}(A) + |C \cap F|$, then there holds

$$\mathfrak{m}(A) \cdot \mathfrak{m}(B) = \mathfrak{m}(A \cup F) \cdot \mathfrak{m}(A \cup T).$$

(AM4) If $A \subseteq B \subseteq X$ and $\mathrm{rk}(A) = \mathrm{rk}(B)$, then

$$\rho_B(A) := \sum_{A \subseteq T \subseteq B} (-1)^{|T|-|A|}\mathfrak{m}(T) \geq 0.$$

(AM5) If $A \subseteq B \subseteq X$ and $\mathrm{rk}^*(A) = \mathrm{rk}^*(B)$, then

$$\rho^*_B(A) := \sum_{A \subseteq T \subseteq B} (-1)^{|T|-|A|} \mathfrak{m}(X \setminus T) \geq 0.$$

In this case we call the multiplicity Tutte polynomial $M(x, y)$ the *arithmetic Tutte polynomial* of $(\mathcal{M}_X, \mathfrak{m})$.

All those axioms from the definition are independent of each other, in the sense that one can find multiplicity matroids that fulfil all but one axiom. The following matroids serve as our first simple examples of multiplicity matroids, which are not yet arithmetic matroids. They are all taken from [MD12, Rem. 4.3.].

Example. In the following example we observe matroids that contain no proper vectors, i.e. they consist only of loops denoted by l and coloops denoted by c. Such matroids are also first examples for so-called *molecules*.

- Let $X_1 = \{l\}$, then we obtain a matroid structure in the sense of the rank axioms by setting $\mathrm{rk}(\{l\}) = \mathrm{rk}(X_1) = 0$. Furthermore we turn it into a multiplicity matroid by setting $\mathfrak{m}(\emptyset) = 3$ and $\mathfrak{m}(X_1) = 2$. Then simple calculations show, that this construction fulfils all axioms of an arithmetic matroid but the first one.

- However, considering $X_2 = \{c\}$ with $\mathrm{rk}(X_2) = 1$ and letting $\mathfrak{m}(X_2) = 3$ and $\mathfrak{m}(\emptyset) = 2$ then the resulting multiplicity matroid fulfils all axioms but the second one. (Although the first one is satisfied trivially because of a lack of dependent elements.)

- Now consider the the matroid on $X_3 = \{l, c\}$ given by $\mathrm{rk}(\{c\}) = \mathrm{rk}(\{c, l\}) = 1$ and $\mathrm{rk}(\{l\}) = \mathrm{rk}(\emptyset) = 0$. Setting $\mathfrak{m}(\{c\}) = \mathfrak{m}(\{c, l\}) = \mathfrak{m}(\emptyset) = 2$ and $\mathfrak{m}(\{l\}) = 1$. This yields a multiplicity matroid satisfying all axioms from above but the third one. Moreover, the multiplicity Tutte polynomial is computed as $M(x, y) = x+y+xy-1$.

- Considering the matroid on $X_4 = \{l_1, l_2, l_3, l_4\}$ defined by $\mathrm{rk}(X_4) = 0$ (this means $\mathrm{rk}(A) = 0$ for all $A \subseteq X_4$, i.e. X_4 is consisting only of loops). If we set $\mathfrak{m}(\emptyset) = 4$, $\mathfrak{m}(l_i) = 2$ $\forall i \in \{1, 2, 3, 4\}$ and $\mathfrak{m}(A) = 1$ for any other sublist $A \subseteq X$, we obtain a multiplicity matroid fulfilling all but the fourth axiom. Its multiplicity Tutte polynomial is given by $M(x, y) = y^4 + 4y - 1$.

- Finally observe the matroid on $X_5 = \{c_1, c_2, c_3, c_4\}$ with $\mathrm{rk}(A) = |A|$ for all $A \subseteq X_5$ (i.e. X_5 is does only contain coloops). Using multiplicities (dual to the last example) $\mathfrak{m}(X_5) = 4$, $\mathfrak{m}(A) = 2$ if $|A| = 3$ and $\mathfrak{m} = 1$ else, we obtain that every axioms is fulfilled but the fifth one and for the multiplicity Tutte polynomial we have: $M(x, y) = x^4 + 4x - 1$.

Considering the examples from above, note that if (AM3), (AM4) or (AM5) fail, it is possible to gather a multiplicity Tutte polynomial with negative coefficients and thus a *non-combinatorial object*. Indeed we will see that those axioms guarantee the positivity of the coefficients of the multiplicity Tutte polynomial in case of arithmetic matroids.

Example. ([MD12, Rem. 2.3.]) A trivial, yet important first example of arithmetic matroids is constructed by taking an arbitrary matroid $\mathcal{M}_X$ over a list X and setting $\mathfrak{m}(A) = 1$ for all $A \subseteq X$. Clearly the constant function $\mathfrak{m} \equiv 1$ fulfils all five axioms. In other words, every matroid can be considered an arithmetic matroid with trivial multiplicity. Due to this, arithmetic matroids really can be viewed as a generalisation of standard matroids. However, in this case we do not get any further structure on $\mathcal{M}_X$. In particular the arithmetic Tutte polynomial coincides with the ordinary Tutte polynomial since

$$\begin{aligned} M(x,y) &= \sum_{A\subseteq X} \mathfrak{m}(A)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)} \\ &= \sum_{A\subseteq X} 1(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)} = T(x,y). \end{aligned}$$

Even though we have already seen, that the axioms (AM1)–(AM5) are kind of independent of each other, mathematicians found simpler descriptions of arithmetic matroids reducing the originally five conditions to three. Those definitions usually make use of the notion of so-called *molecules*. They are essentially minors of the matroid that correspond to the situation of (AM3), where we observe sets $A \subseteq B \subseteq X$ such that $B = A \sqcup F \sqcup T$ and for all $A \subseteq C \subseteq B$ we have $\mathrm{rk}(C) = \mathrm{rk}(A) + |C \cap F|$. In words: The superset B consists of A, a *free part* F whose elements are coloops in $(\mathcal{M}_{X|B})/A$, and a *torsion part* T consisting of loops (w.r.t. $(\mathcal{M}_{X|B})/A$).

Definition. In literature the definition of molecules varies and the formulations are not all equivalent. However, they are strongly related. We state here the most common variants.

(i) A *molecule* is an arithmetic matroid that has no proper vectors. I.e. it consists only of loops and coloops. [MD12, 4.1]

(ii) Let $\mathcal{M}_X$ be a matroid, $R \subseteq S \subseteq X$. Then the set

$$[R,S] := \{A : R \subseteq A \subseteq S\}$$

is called a *molecule* if S can be written as the disjoint union $S = R \sqcup F \sqcup T$ and for each $A \in [R,S]$ we have $\mathrm{rk}(A) = \mathrm{rk}(R) + |A \cap F|$ ([BM14, Section 2] or also [BL20, Def 14]).

(iii) A *molecule* in a matroid $\mathcal{M}_X$ is a triple $\alpha := (R,F,T)$ of disjoint subsets of X such that for every $A \subseteq X$ with $R \subseteq A \subseteq R \sqcup F \sqcup T$ we have $\mathrm{rk}(A) = \mathrm{rk}(R) + |A \cap F|$. [DM16, Def 1]

(iv) A *molecule* in a matroid $\mathcal{M}_X$ is a pair (A,B) of sets $A \subset B \subseteq X$ such that the matroid $(\mathcal{M}/A) \setminus B^C$ has a unique basis. [Pag20, Def 1.4]

Remark. We should at least state *why*, and *how* these four definitions are related with each other. Firstly, (ii) and (iii) are basically the same structure. Only in (ii) we call

the whole interval $[R, S]$ a molecule. There we factorise the endpoint $S = R \cup F \cup T$ (as we are allowed by (ii)) and see that this already yields the triple (R, F, T) defining a molecule in the sense of (iii). Conversely, given such a triple (R, F, T) being a molecule in the sense of (iii), we instantly obtain a (ii)-molecule by observing the interval of sets $[R, R \cup F \cup T]$.
Now given a molecule (R, F, T) in the sense of (iii) we set $A := R$ and $B := R \cup F \cup T$. Then the matroid $(\mathcal{M}_X/A) \setminus B^C$ is isomorphic to the matroid $\mathcal{M}_{F \sqcup T}$ where we assume every $c \in F$ to be a coloop and every $l \in T$ to be a loop. (This is implied by the rank-property stated in (iii)). Therefore $(\mathcal{M}_X/A) \setminus B^C$ has a unique basis given by F, the set of coloops, and (A, B) is a molecule in the sense of (iv).
Naturally, every matroid with a unique basis cannot have any proper vector. Otherwise the basis axiom (B2) would let us construct at least one other basis. Therefore $(\mathcal{M}_X/A) \setminus B^C$ given by a molecule in the sense of (iv) is already a molecule as described in (i).
Finally definition (i) translates into definition (ii) in the sense that given R and $S = R \cup F \cup T$ as described above, the sets F and T define such a (i)-molecule in an appropriate minor and therefore determine the rank of all sets $A \subseteq [R, S]$.

In matroid theory, very simple matroids consisting only of singletons are called *atoms*. Therefore the name *molecule* for a matroid consisting of several atoms seems intuitive. However, using the notion of molecules we can reduce the definition of arithmetic matroids to the following more compact version.

Definition ([BM14, Section 2] or [BL20, Def. 14])**.** An *arithmetic matroid* is a multiplicity matroid $(\mathcal{M}_X, \mathfrak{m})$ such that the multiplicity function $\mathfrak{m} : \mathcal{P}(X) \to \mathbb{N} \setminus \{0\}$ satisfies the following three axioms:

(P) For each molecule $[R, S]$ the following inequality holds:

$$\rho(R, S) := (-1)^{|T_{RS}|} \sum_{A \in [R,S]} (-1)^{|S|-|A|} \mathfrak{m}(A) \geq 0,$$

where T_{RS} denotes the torsion part in the classical factorisation of the molecule: $S = R \sqcup F_{RS} \sqcup T_{RS}$.

(A1) For all $A \subseteq X$ and $e \in X$: if $\mathrm{rk}(A \cup \{e\}) = \mathrm{rk}(A)$ then $\mathfrak{m}(A \cup \{e\})$ divides $\mathfrak{m}(A)$. Otherwise $\mathfrak{m}(A)$ divides $\mathfrak{m}(A \cup \{e\})$.

(A2) If $[R, S]$ is a molecule, then $\mathfrak{m}(R)\mathfrak{m}(S) = \mathfrak{m}(R \cup F)\mathfrak{m}(R \cup T)$, where again $S = R \sqcup F \sqcup T$ is the molecule factorisation of S.

It is one advantage of this system of axioms that we are now able to define two important pre-stages of arithmetic matroids. Especially quasi-arithmetic matroids play a major role in some algebraic generalisations of arithmetic matroid theory.

Definition ([BM14, Section 2] or [BL20, Def. 14])**.** A multiplicity matroid, that satisfies (P) is called *pseudo-arithmetic matroid*. On the other hand, a multiplicity matroid that satisfies (A1) and (A2) is called a *quasi-arithmetic matroid*.

The pair $(\mathcal{M}_X, \mathfrak{m})$ is an *arithmetic matroid* if it is a quasi-arithmetic matroid as well as a pseudo-arithmetic matroid.

Another, even more compact equivalent definition of arithmetic matroids is given by Delucchi and Moci [DM16] using the language of posets in a very elegant way. Since we aim for a complete introduction to the topic of arithmetic matroids based on only fundamental knowledge in discrete mathematics, we will now repeat the fundamentals of poset-theory. Most of it can be found in any course book on combinatorics, or even in Delucchi-Moci [DM16, 2.1.].

First of all, we need some basic definitions that will turn out very useful later on.

Definition. Let P be a set and $\preccurlyeq$ an order-relation on P, that is, $\preccurlyeq$ is reflexive, transitive and antisymmetric. Then $(P, \preccurlyeq)$ is called a *partially ordered set*, or *poset* for short.
In a poset P an *interval* is any subset of P of the form $[x, y] := \{z \in P | x \preccurlyeq z \preccurlyeq y\}$ for some $x, y \in P, x \preccurlyeq y$. We will denote the set of all intervals of P by $I(P)$.

Remark. Since we are working with arithmetic matroids which are defined on finite lists, also all posets occurring throughout this thesis will be finite. Thus in the following we assume all our posets to be finite.

Definition. The *Möbius function* of a finite poset P is the function

$$\mu : I(P) \to \mathbb{Z}$$

defined via the following recursion:

$$\begin{cases} \mu(x,x) = 1 & \text{for all } x \in P \\ \sum\limits_{x \leq z \leq y} \mu(x,z) = 0 & \text{for all } x < y \in P, \end{cases}$$

where we simply write $\mu(x, y)$ for $\mu([x, y])$.
For a function on posets $\mathfrak{m} : P \to \mathbb{R}$ the *Möbius transform* of $\mathfrak{m}$ is given by

$$\begin{aligned} \mathfrak{m}^\mu : P &\to \mathbb{R} \\ x &\mapsto \sum_{z \geq x} \mu(x,z)\mathfrak{m}(z). \end{aligned}$$

It is characterised by $\mathfrak{m}(x) = \sum\limits_{z \geq x} \mathfrak{m}^\mu(z)$.

Definition. Consider two elements $x_1, x_2 \in P$ of a poset. A *minimal upper bound* for x_1, x_2 is an element $y \in P$ such that for all $z \in P$ we have:

$$(z \geq x_1 \text{ and } z \geq x_2) \iff z \geq y.$$

By antisymmetry, such an element y is unique. We denote it as $y = x_1 \vee x_2$ and call it the *join of* x_1 *and* x_2. A poset, in which every pair $x_1, x_2 \in P$ admits a join, is called a *join-semilattice*.

We summarise some of the abstract definitions given above in the following famous example.

Example (Boolean poset). Take $B_n = \{0,1\}^n$ the set of ordered n-tuples with entries 0 or 1. On B define the following partial order: For all $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ let

$$x \preccurlyeq y :\Longleftrightarrow (x_i \leq y_i, \quad \forall i \in [n]).$$

Then B_n is a locally finite poset called the *Boolean poset* and additionally it is a join-semilattice where the join of x and y is given by

$$x \vee y = (\max\{x_i, y_i\})_{i=1}^n.$$

Moreover, let X be a set of n elements (i.e. $X \cong [n]$). Then the poset $(\mathcal{P}(X), \subseteq)$ is isomorphic to B_n. In general, the isomorphism is constructed by labelling the elements of X with numbers $1, 2, ..., n$. Further, to a subset $Y = \{i_1, ..., i_k\} \subseteq X$ we assign exactly the element of $\{0,1\}^n$ which shows a 1 at the i_j'th position for $j = 1, 2, ..., k$ and 0 elsewhere. This gives a bijection $\mathcal{P}(X) \leftrightarrow \{0,1\}^n$ that preserves the orders of the posets. To see this, regard for example Figure 2.1.

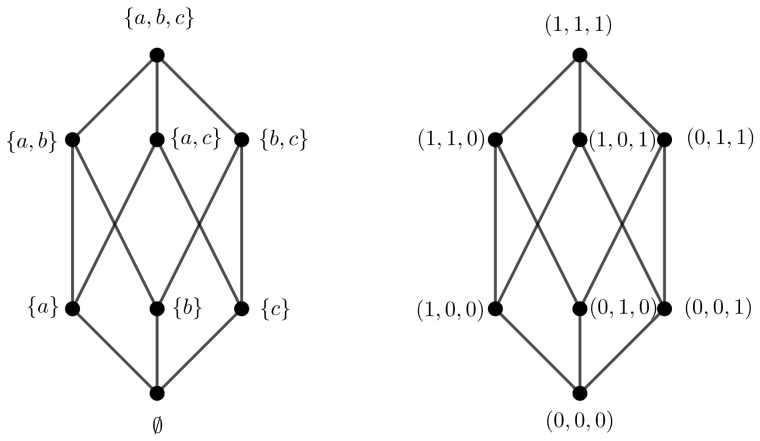

Figure 2.1: $\mathcal{P}(\{a, b, c\})$ is isomorphic to the boolean poset B_3.

We now state two results of general poset theory that will come in handy when proving positivity theorems for arithmetic matroids.

Lemma 2.1.1 ([DM16, Lemma 1])**.** *Let P be a finite join-semilattice and $D : P \to Sets$ be a function such that $D(x) \cap D(y) = D(x \vee y)$ for all $x, y \in P$. Then*

$$\sum_{z \geq x} \mu(x, z)|D(z)| \geq 0$$

for all $x \in P$.

Proof. For all $x \in P$ we define

$$G(x) := D(x) \setminus \bigcup_{z>x} D(z).$$

and set $f(x) := |G(x)| \geq 0$. We claim that: $D(x) = \bigsqcup_{z \geq x} G(z)$.

$\supseteq$: $z \geq x$ means $z = x \vee z$. Therefore $G(z) \subseteq D(z) = D(z) \cap D(x) \subseteq D(x)$.

$\subseteq$: Let $d \in D(x)$. The set $P_d := \{y \in P \mid d \in D(y)\}$ has a unique maximal element $\hat{p}$ (since $d \in D(y)$ and $d \in D(y')$ imply $d \in D(y) \cap D(y') = D(y \vee y')$, and hence $y \vee y' \in P_d$). We observe that $d \in D(\hat{p}) \setminus \bigcup_{z>\hat{p}} D(z) = G(\hat{p})$. The uniqueness of $\hat{p}$ implies that the union is indeed disjoint. This proves the claim.

Thus we deduce that for all $x \in P$ we have

$$|D(x)| = \sum_{z \geq x} f(z)$$

and therefore by Möbius inversion

$$\sum_{z \geq x} \mu(x,z)|D(z)| = f(x) \geq 0.$$

□

With this lemma we are able to prove the following theorem.

Theorem 2.1.2 ([DM16, Thm. 1])**.** *Let P be a join-semilattice, and consider two functions $\mathfrak{m}_1, \mathfrak{m}_2 : P \to \mathbb{Z}$. If $(\mathfrak{m}_i)^\mu(x) \geq 0$ for all $x \in P, i \in \{1,2\}$, then $(\mathfrak{m}_1\mathfrak{m}_2)^\mu(x) \geq 0$ for all $x \in P$.*

Proof. We define a family of sets. For every $i = 1, 2$ and $x \in P$ let

$$G_i(x) := \{Y_1^{i,x}, \ldots, Y_{\mathfrak{m}_i^\mu(x)}^{i,x}\},$$

where the $Y_j^{i,x}$ are formal elements - i.e. $Y_j^{i,x} = Y_j^{\prime i',x'}$ if and only if $i = i', x = x'$ and $j = j'$. Note that the $G_i(x)$ are well defined due to the positivity condition on $\mathfrak{m}_i^\mu$. Furthermore let $A_i(x) := \bigsqcup_{z \geq x} G_i(z)$ be the disjoint union. Then we have

$$A_i(x') \cap A_i(x'') = A_i(x' \vee x'').$$

By the definition of $\mathfrak{m}_i^\mu$ we also observe that

$$|A_i(x)| = \sum_{z \geq x} \mathfrak{m}_i^\mu(z) = \mathfrak{m}_i(x).$$

Finally we define another family of sets $(A_{12}(x))_{x \in P}$ given by

$$A_{12}(x) := A_1(x) \times A_2(x)$$

and again we see (since Cartesian products commute with intersections):

$$A_{12}(x') \cap A_{12}(x'') = (A_1(x') \cap A_1(x'')) \times (A_2(x') \cap A_2(x'')) = A_{12}(x' \vee x'').$$

By now, we have collected all the information we need. We apply Lemma 2.1.1 and get

$$(\mathfrak{m}_1\mathfrak{m}_2)^\mu(x) = \sum_{z \geq x} \mu(x,z)|A_{12}(z)| \geq 0.$$

Now the claim follows since $|A_{12}(z)| = \mathfrak{m}_1(z)\mathfrak{m}_2(z)$ for all $z \in P$. □

Finally we can define arithmetic matroids combining the languages of molecules and posets. Following Delucchi and Moci [DM16, Section 2.2], to each molecule $\alpha = (R, F, T)$ we associate a poset

$$B_\alpha = \{(F', T') \mid F' \subseteq F, T' \subseteq T\}$$

ordered by $(F', T') \preccurlyeq (F'', T'') :\Leftrightarrow F' \supseteq F''$ and $T' \subseteq T''$.
Observe that B_α is bounded, having a unique minimal element $\hat{0} = (F, \emptyset)$ and a unique maximal element $\hat{1} = (\emptyset, T)$. Additionally, every interval in B_α (e.g. $[(F', T'), (F'', T'')]$) is the poset $B_{\alpha'}$ for another molecule given by $\alpha' = (R \cup F'' \cup T', F' \setminus F'', T'' \setminus T')$.
Now given any multiplicity $\mathfrak{m} : \mathcal{P}(X) \to \mathbb{Z}$ and a molecule $\alpha = (R, F, T)$ of a matroid $\mathcal{M}_X$ over a set X, we define the function $\mathfrak{m}_\alpha : B_\alpha \to \mathbb{Z}$ via

$$\mathfrak{m}_\alpha(F', T') := \mathfrak{m}(R \cup F' \cup T').$$

Definition. [DM16, Def. 2] An *arithmetic matroid* is a multiplicity matroid $(\mathcal{M}_X, \mathfrak{m})$ where the multiplicity function $\mathfrak{m} : \mathcal{P}(X) \to \mathbb{Z}$ satisfies the following three axioms:

(P) For every molecule α of the underlying matroid $(\mathcal{M}, \mathrm{rk})$ we have

$$\mathfrak{m}_\alpha^\mu(\hat{0}) \geq 0.$$

(Q) For every molecule $\alpha = (R, F, T)$ of $(\mathcal{M}, \mathrm{rk})$ it holds that

$$\mathfrak{m}(R)\mathfrak{m}(R \cup F \cup T) = \mathfrak{m}(R \cup F)\mathfrak{m}(R \cup T).$$

(A) For all $A \subseteq X$ and all $v \in X$ we have

$$\Big(\frac{\mathfrak{m}(A \cup \{v\})}{\mathfrak{m}(A)}\Big)^{2(\mathrm{rk}(A \cup \{v\}) - \mathrm{rk}(A)) - 1} \in \mathbb{Z},$$

which is again just a very fancy way of expressing that $\mathfrak{m}(A)$ has to divide $\mathfrak{m}(A \cup \{v\})$ whenever v is independent from A and $\mathfrak{m}(A \cup \{v\})$ divides $\mathfrak{m}(A)$ if v is dependent on A.

Remark. [DM16, Rem. 2] Comparing this definition directly with the second one above, one can easily see that (Q) and (A2) are equivalent. Same holds for the axioms (A)

and (A1) using only fundamental calculations. Still, we need to remark that also the positivity axioms (P) give equivalent statements. To see this, observe that for a molecule $\alpha = (R, F, T)$ we have that the according poset B_α is boolean and the length of the interval $(B_\alpha)_{\leq (T', F')}$ is $|T'| + |F \setminus F'|$. Hence the Möbius function μ of B_α fulfils

$$\mu(\hat{0}, (T', F')) = (-1)^{|T'|+|F \setminus F'|}.$$

Therefore a little computation shows:

$$\begin{aligned}
(\mathfrak{m}_\alpha)^\mu(\hat{0}) &= \sum_{\substack{T' \subseteq T \\ F' \subseteq F}} \mu(\hat{0}, (T', F'))\mathfrak{m}(R \cup F' \cup T') \\
&= \sum_{\substack{T' \subseteq T \\ F' \subseteq F}} (-1)^{|T'|+|F \setminus F'|}\mathfrak{m}(R \cup F' \cup T') \\
&= (-1)^{|T|} \sum_{\substack{T' \subseteq T \\ F' \subseteq F}} (-1)^{|T \setminus T'|+|F \setminus F'|}\mathfrak{m}(R \cup F' \cup T') \\
&= (-1)^{|T|} \sum_{R \subseteq A \subseteq R \cup F \cup T} (-1)^{|(R \cup F \cup T) \setminus A|}\mathfrak{m}(A) = \rho(R, R \cup F \cup T),
\end{aligned}$$

where the last expression is the one used in our second definition. Hence our second and third definition are indeed equivalent. Still we have to check, that these two really coincide with our first definition of arithmetic matroids. I refer to the originally five axioms (AM1)–(AM5). Firstly, we may recognise that axiom (A) is a combination of (AM1) and (AM2), containing both of their statements, and vice versa. As (Q) is formulated over molecules, this is exactly (AM3). Therefore it remains to check whether (P) represents both (AM4) and (AM5). We recall the conditions for (AM4): If $A \subseteq B \subseteq X$ and $\mathrm{rk}(A) = \mathrm{rk}(B)$, then

$$\rho_B(A) := \sum_{A \subseteq T \subseteq B} (-1)^{|T|-|A|}\mathfrak{m}(T) \geq 0.$$

Now we may observe, that such an A and B form a molecule $\alpha = (A, A \cup \emptyset \cup B \setminus A)$ where the free part F_{AB} is empty (since $\mathrm{rk}(A) = \mathrm{rk}(B)$). Therefore (P) implies (AM4) as (P) demands positivity for all molecules. Now (AM5) is the dual version of (AM4), hence there we observe the same molecule, but now the torsion part is empty. Again (P) implies (AM5).
Conversely (AM4) and (AM5) induce (P) since we can reduce the sum in the molecule case to a double sum representing both the situation of (AM4) and (AM5) sequentially. To sum things up, all our three definitions are equivalent and in future proofs we will always refer to the one most convenient for our current situation.

For example, using the third definition and our knowledge of posets, we are already able to prove the following magnificent result:

Lemma 2.1.3 ([DM16, Lem. 2])**.** *Fix a matroid $\mathcal{M}_X = (X, \mathrm{rk})$ over a set X. Let $\mathfrak{m}', \mathfrak{m}'' : \mathcal{P}(X) \to \mathbb{Z}$ both be multiplicities on $\mathcal{M}_X$. If both $\mathfrak{m}'$ and $\mathfrak{m}''$ satisfy axiom (P),*

then so does $\mathfrak{m} = \mathfrak{m}'\mathfrak{m}''$.

Proof. Consider a molecule α. The poset B_α is boolean, in particular it is a join-semi-lattice. We already remarked, that every interval of B_α defines again a molecule in our matroid and therefore $\mathfrak{m}'$ and $\mathfrak{m}''$ fulfil the conditions of Theorem 2.1.2 about the positivity of Möbius transforms. Hence $(\mathfrak{m}'\mathfrak{m}'')^\mu(\hat{0}) \geq 0$, as desired. □

The consequences of this lemma are far-reaching since now we can deduce a certain algebraic structure on the sets of arithmetic multiplicities on a given matroid. The following two statements specify this observation.

Theorem 2.1.4 ([DM16, Thm. 2])**.** *If both* $(\mathcal{M}_X, \mathfrak{m}_1)$ *and* $(\mathcal{M}_X, \mathfrak{m}_2)$ *are arithmetic matroids, then also* $(\mathcal{M}_X, \mathfrak{m}_1\mathfrak{m}_2)$ *is an arithmetic matroid.*

Proof. By the previous lemma, $\mathfrak{m}_1\mathfrak{m}_2$ fulfils axiom (P). Axioms (A) and (Q) are satisfied trivially. □

Corollary 2.1.5 ([DM16, Rem. 3])**.** *Given a matroid* $\mathcal{M}_X$*, the set*

$$\{(\mathcal{M}_X, \mathfrak{m}) \mid \mathfrak{m} : \mathcal{P}(X) \to \mathbb{Z}, \mathfrak{m} \text{ fulfils (P), (Q) and (A)}\}$$

of arithmetic matroids defined on $\mathcal{M}_X$ *forms a commutative monoid with respect to the natural product of multiplicities.*

With this we conclude our chapter of the basic definitions of arithmetic matroids. We may move on to constructing our first concrete examples.

2.1.2 The main examples of arithmetic matroids

After we have seen a lot of different formulations to abstractly define arithmetic matroids, it is now time to study explicit examples of our object of interest. Like so often new mathematics is created as an offspring when one is confronted with some other difficult objective. As already noted, Luca Moci, father of this very theory, humbled over arithmetic matroids while studying geometric lattices and their so-called toric arrangements. In this section we will closely follow his work in [Moc11] to examine the main example of an arithmetic matroid. Afterwards we will study examples of arithmetic matroids defined on labelled graphs.

Let X be a finite list of vectors spanning a real vector space U. If we denote with $\mathcal{I}$ the set of linearly independent subsets of X then we arrive at our classical example of a matroid $\mathcal{M}_X = (X, \mathcal{I})$. The rank of a subset $A \subseteq X$ is therefore simply given as $\mathrm{rk}(A) = \dim(\langle A \rangle_\mathbb{R})$, the dimension of its linear span $\langle A \rangle_\mathbb{R} \subseteq U$.

Definition ([Moc11, 2.2.])**.** A (geometric) *lattice* Λ of rank n is a discrete subgroup of $\mathbb{R}^n$ which spans the whole $\mathbb{R}^n$ as a real vector space. Every such Λ can be obtained from some basis of the vector space by taking all linear combinations of its elements with integer coefficients. Therefore $\Lambda \cong \mathbb{Z}^n$ as additive groups. In particular any lattice is a finitely generated abelian group.

Let X be a finite list of elements in a lattice Λ and consider the resulting matroid. For every $A \subseteq X$ we denote by $\langle A \rangle_{\mathbb{Z}}$ the according sublattice of Λ generated by the elements of A, and by $\langle A \rangle_{\mathbb{R}}$ the subspace of $U := \Lambda \otimes \mathbb{R}$ spanned by A. Moreover we define

$$\Lambda_A := \Lambda \cap \langle A \rangle_{\mathbb{R}},$$

which gives the largest sublattice of Λ in which $\langle A \rangle_{\mathbb{Z}}$ has finite index. Therefore the multiplicity $\mathfrak{m} : \mathcal{P}(X) \to \mathbb{Z}$ given by

$$\mathfrak{m}(A) := [\Lambda_A : \langle A \rangle_{\mathbb{Z}}]$$

is well-defined, turning $(\mathcal{M}_X, \mathfrak{m})$ into a multiplicity matroid. (By $[G : H]$ we denote the index of a subgroup $H \subseteq G$.)

We now claim that any such pair $(\mathcal{M}_X, \mathfrak{m})$ is already an arithmetic matroid.

We will prove this even for the slightly more general case of abstract finitely generated abelian groups. Each such group is basically a direct sum of a lattice structure and a finite abelian group. To be more precise, the following theorem is one of the main statements of any advanced course in abstract algebra.

Theorem 2.1.6. *Let G be a finitely generated abelian group. Then there exist unique $r, t \in \mathbb{N} \cup \{0\}$ and a series of positive integers $d_1, d_2, \ldots, d_t$, where d_i divides d_{i+1} for all $i = 1, \ldots t-1$, such that*

$$G \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{t} \mathbb{Z}/d_i\mathbb{Z}.$$

*In particular, any such G is isomorphic to a direct sum $G_f \oplus G_t$, with G_f a free abelian group, called the **free part** of G, and a finite group G_t, called the **torsion subgroup** of G. The integer $r \in \mathbb{N} \cup \{0\}$ is called the **rank** of G.*

Now let X be a finite list of elements of a finitely generated abelian group G. For any $A \subseteq X$ we denote by $\langle A \rangle \subseteq G$ the subset of G generated by the elements of A. Naturally every $\langle A \rangle$ is again a finitely generated abelian subgroup and the theorem above can be applied. We let $\mathrm{rk}(A)$ be the rank of $\langle A \rangle$ as described in the theorem.
One can easily see, that this describes a matroid structure (X, rk). Nevertheless one may also notice, that this matroid is indifferent to the matroid described by the projection of X onto the free part G_f since the rank $\mathrm{rk} : \mathcal{P}(X) \to \mathbb{N}$ does ignore the torsion parts of the induced subgroups. In other words, we really do lose structural information when considering only classical matroids on X. We remind the reader that this is the reason why multiplicities were introduced in the first place: to capture combinatorial information that would have been lost otherwise. In our case, the multiplicity function of our choice is again the according index. For any $A \subseteq X$ let G_A be the maximal subgroup of G, such that $\langle A \rangle$ has finite index in G_A. Then similarly to before, we define

$$\mathfrak{m}(A) := [G_A : \langle A \rangle].$$

Again we obtain a multiplicity matroid $(X, \mathrm{rk}, \mathfrak{m})$. Moreover we instantly observe that $\mathfrak{m}(\emptyset) = |G_t|$ and we have $\mathfrak{m}(\emptyset) = 1$ if and only if G is a free abelian group. [MD12, 2.4.]

Theorem 2.1.7 ([MD12, Section 2.4])**.** *Let X be a finite list of elements of a finitely generated abelian group G. Let $\mathcal{M}_X$ be the canonical matroid defined by X and let the function $\mathfrak{m} : \mathcal{P} \to \mathbb{Z}$ be defined as in the last paragraph. Then $(\mathcal{M}_X, \mathfrak{m})$ is an arithmetic matroid.*

The proof of the theorem uses various other statements, also about general duality and representability of arithmetic matroids. Both notions will be covered in the next section. Nevertheless we state the proof and refer in certain situations to the results in the future chapters. For now we gather some theorems of algebra and group theory as well as some simple observations that will turn out very useful in the proof. Firstly, we remind ourselves of the generalised theorem of Lagrange:

Lemma 2.1.8. *Let $U \subseteq H \subseteq G$ be a chain of subgroups of a finite group G. Then we have for their indices, that*

$$[G : U] = [G : H] \cdot [H : U].$$

Moreover we will make use of the following isomorphism-theorems.

Lemma 2.1.9 (Isomorphism theorems)**.**

I. Let G be a group, N a normal subgroup and H a subgroup of G. Then

$$H/(H \cap N) \cong HN/N$$

with $HN := \{hn \mid h \in H, n \in N\}$.

II. Let G be a group, H a normal subgroup of G and N a subgroup of H which is also normal in G. Then

$$(G/N)/(H/N) \cong G/H.$$

All of these are commonly known statements of algebra and can be found in any good coursebook (e.g. in [KM17, Thm. 3.13, Thm. 4.12, Thm. 4.14]).

Remark. [MD12, Rem. 2.7] If we have a finitely generated abelian group G with a subgroup $H \subseteq G$, we can factorise $G = G_f \oplus G_t$ and $H = H_f \oplus H_t$ into free- and torsion parts according to Theorem 2.1.6. Then necessarily H_t is a subgroup of G_t. By the first isomorphism theorem we get

$$\frac{H + G_t}{G_t} \cong \frac{H}{H \cap G_t} \cong H_f.$$

Now choose a suitable subgroup $H'_f \leq G_f$ such that $H + G_t = H'_f \oplus G_t$, for which we observe

$$H'_f = \frac{H'_f \oplus G_t}{G_t} = \frac{H + G_t}{G_t} \cong H_f.$$

In a similar manner we also deduce

$$\frac{G}{H+G_t} \cong \frac{G/G_t}{(H+G_t)/G_t} = \frac{(G_f \oplus G_t)/G_t}{(H'_f \oplus G_t)/G_t} \cong \frac{G_f}{H'_f}$$

and

$$\frac{H+G_t}{H} \cong \frac{G_t}{H \cap G_t} = \frac{G_t}{H_t}.$$

Therefore

$$[G:H] = [G:H+G_t] \cdot [H+G_t:H] = [G_f:H'_f] \cdot [G_t:H_t].$$

Hence, whenever we are only interested in multiplicities, replacing $H = H_f \oplus H_t$ by $H' = H'_f \oplus H_t$ when necessary, we can always assume $H_f \subseteq G_f$. Moreover, for our matroid and $A \subseteq X$ a list we get

$$\begin{aligned}\mathfrak{m}(A) = [G_A : \langle A\rangle] &= [(G_A)_f \oplus (G_A)_t : \langle A\rangle_f \oplus \langle A\rangle_t] = \\ &= [(G_A)_f : \langle A\rangle_f] \cdot [(G_A)_t : \langle A\rangle_t].\end{aligned}$$

Now, last but not least, in order to give a full proof, we need to talk about **toric arrangements** in finitely generated abelian groups. For the following definitions and the resulting lemma, we refer to [Moc11, Section 5.2].
Let $\Gamma := \Lambda \times \Gamma_t$ be a finitely generated abelian group with Λ a lattice and Γ_t its torsion group. Define

$$T_\Gamma := Hom(\Gamma, \mathbb{C}^*),$$

where $\mathbb{C}^*$ denotes the multiplicative complex group.
T_Γ can be viewed as the direct product of a complex torus T_Λ and the finite group Γ_t^* Pontryagin-dual (and isomorphic) to Γ_t, which yields the structure of an abelian linear algebraic group. Topologically we have a disjoint union of $|\Gamma_t|$ copies of the complex torus $T_\Lambda = Hom(\Lambda, \mathbb{C}^*)$.[MD12, Section 3.1]
Additionally, we can identify Γ with the *group of multiplicative characters* of T_Γ, i.e. $\Gamma \cong Hom(T_\Gamma, \mathbb{C}^*)$: given $\gamma \in \Gamma$ and $t \in T_\Gamma$ we may simply set

$$\gamma(t) := t(\gamma).$$

Now let $X \subset \Lambda$ be a finite subset spanning a sublattice of Λ with finite index. For every character $\lambda \in X$ we study its kernel:

$$H_\lambda := \ker(\lambda) = \{t \in T_\Gamma \mid \lambda(t) = 1\}.$$

This is a (non-connected) subvariety of T_Γ. The family $\mathcal{T}(X) := \{H_\lambda | \lambda \in X\}$ is called the *generalised toric arrangement* induced by X on T_Γ.

By $\mathcal{C}(X)$ we denote the set of all the connected components of all intersections of the subvarieties H_λ, ordered by reverse inclusion. Its minimal elements are the connected components of T_Γ. Observe that since $\dim(T_\Gamma)$ equals the rank of Λ, the maximal

elements of $\mathcal{C}(X)$ are 0-dimensional and as they are connected they are in fact points. Let $\mathcal{C}_0(X)$ denote the set of those points.

Finally, for $A \subseteq X$ we set

$$H_A := \bigcap_{\lambda \in A} H_\lambda.$$

With all of this in mind, we obtain the following result:

Lemma 2.1.10 ([Moc11, Lem. 5.4])**.** *The multiplicity* $\mathfrak{m}(A)$ *equals the number of connected components of* H_A*.*

Proof. By definition we have for every $A \subseteq X$ that $\mathfrak{m}(A) = [G_A : \langle A \rangle]$. But from a different perspective if we set $G'_A = (G/\langle A \rangle)_t$ to be the torsion group of the quotient, then we deduce straightforwardly that $\mathfrak{m}(A) = |G'_A|$.

With this we have practically by definition that $\mathfrak{m}(X) = |H_X|$ and this coincides with the number of points in the arrangement. However, then for every $A \subseteq X$ we have

$$|\overline{H}_A| = \mathfrak{m}(A),$$

where $\overline{H}_A$ denotes the set of points of the restricted toric arrangement $\mathcal{T}(A)$ induced by A in T_{Γ_A}. Now we denote by H_A^0 the connected component of H_A that contains the identity. This is a subtorus of T_Γ, moreover the quotient map

$$T_\Gamma \to T_\Gamma / H_A^0 \cong T_{\Gamma_A}$$

yields a bijection between the points in $\overline{H}_A$ and the connected components of H_A. □

Eventually we have gathered everything we need to prove Theorem 2.1.7.

Proof (of the theorem). We prove axioms (AM1)–(AM5).

(AM1) Let $A \subseteq X$ and let $v \in X$ be dependent on A. This means, if $\langle A \rangle \cong \mathbb{Z}^r \oplus H_t$ with H_t its torsion group, then $\langle A \cup \{v\} \rangle \cong \mathbb{Z}^r \oplus H'_t$. Since clearly $\langle A \rangle \subseteq \langle A \cup \{v\} \rangle$ we can assume $H_t \subseteq H'_t$ and clearly $G_A \subseteq G_{A \cup \{v\}}$ is a subgroup. Moreover we observe that $\langle A \rangle$ has finite index in $\langle A \cup \{v\} \rangle$ by dependence of v, hence we get by Lagrange

$$[G_{A \cup \{v\}} : \langle A \rangle] = [G_{A \cup \{v\}} : \langle A \cup \{v\} \rangle] \cdot [\langle A \cup \{v\} \rangle : \langle A \rangle] < \infty$$

Therefore truly $G_A = G_{A \cup \{v\}}$ by definition of G_A. In conclusion we obtain

$$\mathfrak{m}(A) = [G_A : \langle A \rangle] = [G_{A \cup \{v\}} : \langle A \rangle] = \mathfrak{m}(A \cup \{v\}) \cdot [\langle A \cup \{v\} \rangle : \langle A \rangle]$$

which yields the claim.

(AM2) We will see soon, that (AM2) can be considered *dual* to (AM1). Hence (AM2) follows if we show that the dual multiplicity matroid again can be considered a matroid over a list of elements of a finitely generated abelian group. This is indeed true and will be shown in the next section. (See Theorem 2.2.2.)

(AM3) Let $[A, B]$ a molecule in $\mathcal{M}_X$, $B = A \sqcup F \sqcup T$. By the isomorphism theorem we get

$$\langle B\rangle/\langle A \cup F\rangle \cong \langle A \cup T\rangle/(\langle A \cup T\rangle \cap \langle A \cup F\rangle) \tag{2.1.1}$$

Now we claim that we already have $\langle A \cup T\rangle \cap \langle A \cup F\rangle = \langle A\rangle$. We prove $\subseteq$, since the right-to-left inclusion is trivial.
Let $g \in \langle A \cup T\rangle \cap \langle A \cup F\rangle$. Hence we find expansions

$$g = \sum_{a\in A} \alpha_a a + \sum_{t\in T} \beta_t t = \sum_{a\in A} \gamma_a a + \sum_{f\in F} \delta_f f,$$

with $\alpha_a, \beta_t, \gamma_a, \delta_f \in \mathbb{Z}$. Let $F' \subseteq F$ be the subset, for which the corresponding coefficients $\delta_{f'}$, for $f' \in F'$, are nonzero. If $F' = \emptyset$, then $g = \sum_{a\in A} \gamma_a a$ and hence $g \in \langle A\rangle$. Therefore we assume $F' \neq \emptyset$. We define $C = A \cup F'$ and by assumption we have

$$\mathrm{rk}(C) = \mathrm{rk}(A) + |F'|.$$

Nevertheless,

$$\sum_{f'\in F'} \delta_{f'} f' = \sum_{f\in F} \delta_f f = \sum_{a\in A} \alpha_a a + \sum_{t\in T} \beta_t t - \sum_{a\in A} \gamma_a a \ \in \langle A \cup T\rangle,$$

and $\mathrm{rk}(A \cup T) = \mathrm{rk}(A)$ ($[A, B]$ molecule). Therefore we conclude

$$\mathrm{rk}(C) \leq \mathrm{rk}(A \cup T) + |F'| - 1 = \mathrm{rk}(A) + |F'| - 1,$$

which yields a contradiction.
Hence we indeed have $\langle A \cup T\rangle \cap \langle A \cup F\rangle = \langle A\rangle$.
Going back to equation (2.1.1) we observe that

$$\langle B\rangle/\langle A \cup F\rangle \cong \langle A \cup T\rangle/\langle A\rangle. \tag{2.1.2}$$

Using that $\mathrm{rk}(B) = \mathrm{rk}(A \cup F)$ and $\mathrm{rk}(A \cup T) = \mathrm{rk}(A)$ as well as our previous remark we compute:

$$\begin{aligned}
\frac{\mathfrak{m}(A \cup F)}{\mathfrak{m}(B)} &= \frac{[G_{A\cup F} : \langle A \cup F\rangle]}{[G_B : \langle B\rangle]} = \frac{[G_B : \langle A \cup F\rangle]}{[G_B : \langle B\rangle]} \\
\text{(Lagrange)} &= [\langle B\rangle : \langle A \cup F\rangle] \\
\text{(2.1.2)} &= [\langle A \cup T\rangle : \langle A\rangle] \\
&= \frac{[G_A : \langle A\rangle]}{[G_A : \langle A \cup T\rangle]} = \frac{[G_A : \langle A\rangle]}{[G_{A\cup T} : \langle A \cup T\rangle]} \\
&= \frac{\mathfrak{m}(A)}{\mathfrak{m}(A \cup T)}.
\end{aligned}$$

This proves (AM3).

(AM4) For sets $A \subset B \subset X$ with $\mathrm{rk}(A) = \mathrm{rk}(B)$ one observes by using the Lemma 2.1.10 above and the principle of inclusion-exclusion that $\rho_B(A)$ is equal to the number of connected components of

$$H_A \setminus \bigcup_{B \supseteq T \supset A} H_T,$$

and therefore clearly is a non-negative integer.

(AM5) Again, this axiom can be considered to be the dual of (AM4). Hence by proving that a so-called *representable multiplicity matroid* has a representable dual one can deduce (AM5). This will happen in the next section. (See again Theorem 2.2.2.)

This yields that a finite list of elements of a finitely generated abelian group indeed induces an arithmetic matroid. □

We study a first example of this class of arithmetic matroids.

Example. Let $G = \mathbb{Z}^2 \oplus \mathbb{Z}/2\mathbb{Z}$. In G we regard the finite list

$$X = \Big\{ \underbrace{\begin{pmatrix} 1 \\ 2 \\ \bar{0} \end{pmatrix}}_{a}, \underbrace{\begin{pmatrix} 4 \\ 8 \\ \bar{1} \end{pmatrix}}_{b} \Big\}.$$

Then $\mathfrak{m}(\emptyset) = 2$ and for the singletons we compute that $G_{\{a\}} = \langle (1,2) \rangle_{\mathbb{Z}} \oplus (\mathbb{Z}/2\mathbb{Z})$ and also $G_{\{b\}} = \langle (1,2) \rangle_{\mathbb{Z}} \oplus (\mathbb{Z}/2\mathbb{Z})$. Thus we deduce that $\mathfrak{m}(\{a\}) = 2$ and for $\mathfrak{m}(\{b\})$ we compute

$$\begin{aligned} \mathfrak{m}(\{b\}) &= [(G_{\{b\}})_f : \langle b \rangle_f] \cdot [(G_{\{b\}})_t : \langle b \rangle_t] \\ &= [\langle (1,2) \rangle_{\mathbb{Z}} : \langle (4,8) \rangle_{\mathbb{Z}}] \cdot [(\mathbb{Z}/2\mathbb{Z}) : \emptyset] \\ &= 4 \cdot 2 = 8. \end{aligned}$$

Now for $\mathfrak{m}(X)$ we observe that b is dependent on $\{a\}$. Hence we have that $\mathfrak{m}(X)$ divides $\mathfrak{m}(\{a\}) = 2$. Therefore $\mathfrak{m}(X) = 1$ or 2. And indeed $G_X = \langle (1,2) \rangle_{\mathbb{Z}} \oplus (\mathbb{Z}/2\mathbb{Z}) = \langle X \rangle_{\mathbb{Z}}$. Thus $\mathfrak{m}(X) = 1$. For the arithmetic Tutte polynomial we have

$$\begin{aligned} M(x,y) &= \mathfrak{m}(\emptyset)(x-1) + \mathfrak{m}(\{a\}) + \mathfrak{m}(\{b\}) + \mathfrak{m}(X)(y-1) \\ &= 2x - 2 + 2 + 8 + y - 1 = 2x + y + 7. \end{aligned}$$

For lattices we now want to regard their arithmetic Tutte polynomial $M(x,y)$. Therefore let $\Lambda \subset \mathbb{R}^n$ be such a lattice and let $X \subseteq \Lambda$ be a finite list of elements.

Definition. To such a list X we associate a *zonotope*, that is, a convex polytope defined as follows (see [Moc11, Section 2.2]):

$$\mathcal{Z}(X) := \Big\{ \sum_{x \in X} \lambda_x x \mid 0 \leq \lambda_x \leq 1 \Big\}.$$

In case that X is a linearly independent subset of vectors in $\mathbb{R}^d$, $\mathcal{Z}(X)$ is also called the *parallelepiped* spanned by the elements of X.

Example. If we consider the list $X = \left\{ \begin{pmatrix} -3 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\} \subseteq \mathbb{Z}^2$, then the corresponding zonotope $\mathcal{Z}(X)$ is given as in Figure 2.2.

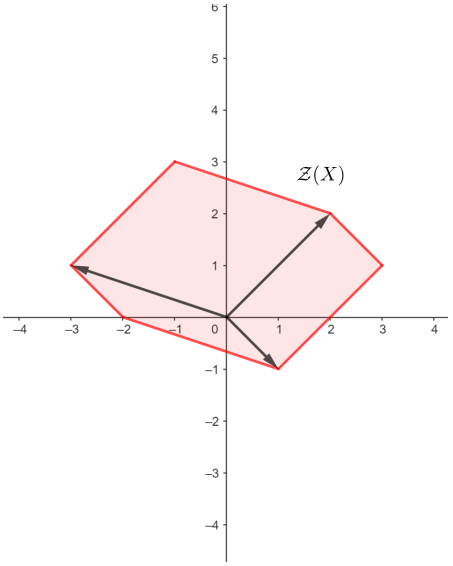

Figure 2.2: The zonotope $\mathcal{Z}(X)$.

Remark. If we identify Λ with $\mathbb{Z}^d$, we obtain that for every sublist $A \subseteq X$ with maximal rank that

$$\mathfrak{m}(A) = [\Lambda_A : \langle A \rangle_{\mathbb{Z}}] = \gcd(\det(B) \mid B \subseteq A, \text{basis}).$$

Proposition 2.1.11 ([Moc11, Prop. 2.2.])**.** *$M_X(1,1)$ is equal to the volume of the zonotope $\mathcal{Z}(X)$.*

Proof. By [She74, Section 5], the zonotope $\mathcal{Z}(X)$ can be divided into a family of polytopes $\{\Pi_B\}$, where B varies over all bases extracted from our list X. Moreover, every Π_B is a translation of the zonotope $\mathcal{Z}(B)$ generated by the $B \subseteq X$. This may again be seen in Figure 2.2 above. Therefore

$$\text{vol}(\Pi_B) = |\det(B)|$$

However, since B is a basis,

$$\mathfrak{m}(B) = [\Lambda : \langle B \rangle_{\mathbb{Z}}] = |\det(B)|.$$

Now we remember the definition

$$M_X(x,y) = \sum_{A \subseteq X} \mathfrak{m}(A)(x-1)^{\text{rk}(X)-\text{rk}(A)}(y-1)^{|A|-\text{rk}(A)}$$

and hence obtain

$$M_X(1,1) = \sum_{\substack{B \subseteq X \\ B \text{basis}}} \mathfrak{m}(B),$$

which yields the assertion. □

One can also prove, and this is done in [Moc11, Section 4], that the arithmetic Tutte polynomial counts the *integer points* inside the zonotope. Let us be more specific. Given again Λ a lattice and $V = \Lambda \otimes \mathbb{R}$ the vector space spanned by it, then a point $x \in V$ is called *integer* if it is also contained in Λ. Thus one has the following.

Theorem 2.1.12 ([Moc11, Prop. 4.5])**.** *Let X be a list of elements of a lattice Λ. Then X induces a zonotope $\mathcal{Z}(X)$ and an arithmetic matroid with arithmetic Tutte polynomial $M_X(x,y)$. Then the number $|\mathcal{Z}(X) \cap \Lambda|$ of integer points contained in the zonotope is equal to $M_X(2,1)$.*

In the next part we will see that the arithmetic Tutte polynomial even does specialise to the Ehrhart polynomial of the zonotope $\mathcal{Z}(X)$ (see Theorem 3.2.1). However, we now want to talk about our second classical example of arithmetic matroids. Namely arithmetic matroids over labelled graphs.

Graphs and vector spaces were the inspiring objects for general matroid theory. While the relation between vector spaces and finitely generated abelian groups seems obvious, the question arises, if we are also able to define arithmetic matroids over graphs? Due to the beauty of mathematics, the answer is yes.
The following construction and the necessary definitions are originally taken from [DM13], but one can also find them summed up in [BL20, Section 2.3]. We start defining our basic objects. For preparation we consider a graph $G = (V, E)$ with V its set of vertices and E its list of edges. Within this section G might have multiple parallel edges, but *without any loops*. Now we divide E into two distinguished lists R and D. Hence we assume that $E = R \sqcup D$ is a disjoint union, by which we further call the elements of R *regular edges*, while D will contain the so-called *dotted edges*.

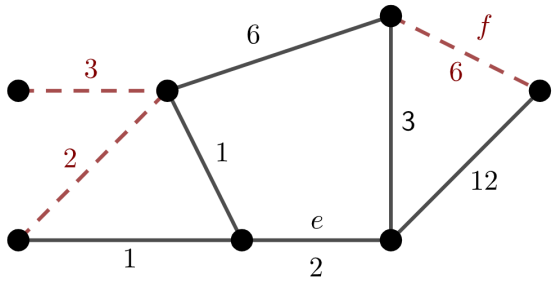

Figure 2.3: A labelled graph with regular edges (black) and dotted edges (brown).

Definition ([DM13, Section 1])**.** In this context a *labelled graph* is a pair (G, l), where $G = (V, E) = (V, R \cup D)$ is a graph and $l : E \to \mathbb{N} \cup \{0\}$ a *labelling*. For $e \in E$ we call $l(e)$ the *label* of e.

For this kind of labelled graphs we also define an adapted concept of *deletion* and *contraction*.

- The *(labelled) deletion* of a **regular edge** $e \in R$ corresponds to the pair $(G \setminus e, l_1)$ where $G \setminus e$ coincides with the classical deletion of graphs and $l_1 : E \setminus \{e\} \to \mathbb{N} \cup \{0\}$ is simply the restriction of l to $E \setminus \{e\}$.
- The *(labelled) contraction* of a **regular edge** $e \in R$ is given by the pair $(G/e, l_2)$ where $G/e = (V, E_2)$ is obtained from G by removing e from R and putting it into D. (i.e. if $E_2 = R_2 \cup D_2$ then $R_2 = R \setminus \{e\}$ and $D_2 = D \cup \{e\}$) In this case l_2 still coincides with l.

Example. In the pictures below (Figure 2.4), we regard the *labelled deletion* and the *labelled contraction* of the regular edge e of the labelled graph (G, l) from Figure 2.3. Nevertheless, we leave out the labels to preserve visibility.

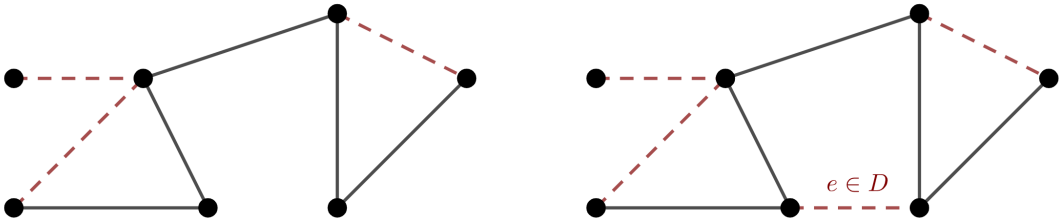

Figure 2.4: labelled deletion and contraction of the former regular edge e.

However, we do not only want our graphs be labelled but also directed. We put forward the following definition.

Definition ([DM13, Section 1])**.** A *directed graph* is a pair (V, E) with V again a finite set of vertices and E now a list of ordered pairs of vertices. Elements of E are called *directed edges* and are hence of the form (v_1, v_2) with $v_1, v_2 \in V$. Let $G = (V, E)$ be a normal, not directed, graph. An *orientation* $E_\theta = R_\theta \cup D_\theta$ of the edges $E = R \cup D$ is a list of ordered pairs of elements of V, such that by forgetting the ordering we would again obtain E. I.e for every $(v, u) \in E_\theta$ we find a $\{v, u\} \in E$.

Now, following [DM13, Section 2.3], we want to associate an arithmetic matroid $\mathcal{M}_{G,l}$ to a labelled graph (G, l). As a first step, we enumerate the elements of $V = \{v_1, \ldots, v_n\}$ and fix an orientation E_θ on E. After that, for each element $e = (v_i, v_j) \in E_\theta$ we define the vector $x_e \in \mathbb{Z}^n$ by the following rule: The i'th coordinate of x_e equals $l(e)$ while its

j'th coordinate is given by $-l(e)$. All other values shall be set to zero. To sum things up we have

$$(x_e)_k = \begin{cases} l(e) & \text{if } k = i \\ -l(e) & \text{if } k = j \\ 0 & \text{else.} \end{cases}$$

In a next step we may define X_R and X_D containing the x_e constructed via edges of R and D respectively. Finally we regard the group $G = \mathbb{Z}^n/\langle X_D \rangle$, where we identify elements of X_R with their corresponding cosets in G. Since G clearly is a finitely generated abelian group, X_R induces an arithmetic matroid. We set $\mathcal{M}_{G,l} := \mathcal{M}_{X_R}$ and obtain our arithmetic matroid over the labelled graph (G, l).

By now we have constructed the most important examples of arithmetic matroids, namely those defined over finitely generated abelian groups. These do not only let us define arithmetic matroids over graphs but do also serve as blueprints for a *typical* object of our interest. In that manner all arithmetic matroids, which can be realised over lists of elements of finitely generated abelian groups are called *representable*. This directly refers to representability in classical matroid theory, where one observes finite dimensional vector spaces instead of abelian groups. The study this very fundamental concept, together with the essential notion of duality, will be our next big goal.

2.2 Duality and representability

Duality and representability are both central concepts in matroid theory. Every matroid has a unique dual and its information is also encoded in the primal Tutte polynomial. The development of a notion of duality for arithmetic matroids, which in the end fulfils similar properties, is a huge achievement of arithmetic matroid theory.

On the other hand, representability is a quality that an arithmetic matroid might satisfy or not. However, in many cases it yields various computational advantages if one works with representable arithmetic matroids.

In this section we want to generalise both concepts to the situation of arithmetic matroids. Moreover we also show that these generalised notions satisfy the same essential qualities.

2.2.1 Duality

We start off by reminding ourselves of the definition of duality in classical matroid theory: If $\mathcal{M}_X = (X, \mathcal{B})$ is a matroid over a set X with $\mathcal{B}$ its family of bases, then the dual matroid $\mathcal{M}_X^*$ is also defined over X but now its family of bases is given by $\mathcal{B}^* = \{X \setminus B \mid B \in \mathcal{B}\}$.

Now we concern ourselves with the case that $\mathcal{M}_X$ is not only a matroid but is also equipped with a multiplicity function $\mathfrak{m}$ fulfilling the necessary axioms such that $(\mathcal{M}_X, \mathfrak{m})$ is an arithmetic matroid. The question is how to construct a *dual multiplicity* $\mathfrak{m}^*$ which also turns the dual $\mathcal{M}_X^*$ into an arithmetic matroid.

The answer is given in [MD12, Section 2.3] and is very simple. We put forward the following definition.

Definition (Dual multiplicity matroids)**.** Let $(\mathcal{M}_X, \mathfrak{m})$ be a multiplicity matroid. Its *dual multiplicity matroid* is defined by $(\mathcal{M}_X^*, \mathfrak{m}^*)$, where $\mathcal{M}_X^*$ is the classical dual matroid of $\mathcal{M}_X$ and $\mathfrak{m}^* : \mathcal{P}(X) \to \mathbb{Z}$ is given by

$$\mathfrak{m}^*(A) = \mathfrak{m}(X \setminus A).$$

Again (or still) by abuse of notation we may simply write $\mathcal{M}_X$ for the whole multiplicity matroid $(\mathcal{M}_X, \mathfrak{m})$ and in the same manner denote the dual multiplicity matroid just by $\mathcal{M}_X^*$. Just by definition we then again observe the easy relation $(\mathcal{M}_X^*)^* = \mathcal{M}_X$. This coincides with the classical notion. In addition, in the case of not only multiplicity- but already arithmetic matroids, we obtain the following beautiful result.

Lemma 2.2.1 ([MD12, Lem. 2.2])**.** *The dual of an arithmetic matroid is again an arithmetic matroid.*

Proof. We check (AM1)–(AM5) from our first definition of arithmetic matroids. Firstly, we see that (AM1) and (AM2) are *dual* to each other in the sense that (AM2) is equivalent to

(AM1*) If $A \subseteq X$ and $v \in X$ is independent of A in the dual (this means $\mathrm{rk}^*(A \cup \{v\}) = \mathrm{rk}^*(A) + 1$), then $\mathfrak{m}^*(A)$ divides $\mathfrak{m}^*(A \cup \{v\})$,

while on the other hand (AM1) is equivalent to

(AM2*) If $A \subseteq X$ and $v \in X$ is dependent on A in the dual (i.e. $\mathrm{rk}^*(A \cup \{v\}) = \mathrm{rk}^*(A)$), then $\mathfrak{m}^*(A \cup \{v\})$ divides $\mathfrak{m}^*(A)$.

Now, since (AM1) and (AM2) are fulfilled in the original arithmetic matroid, by the equivalence the according axioms also have to be satisfied in the dual multiplicity matroid.

Observe that, in this case simply by their formulation, axioms (AM4) and (AM5) are dual to each other too. Hence it remains to check (AM3).

However, the third axiom turns out to be *self-dual*. Let $A \subseteq B \subseteq X$ form a molecule in the dual, i.e. B can be written as a disjoint union $B = A \cup T \cup F$ and for all $A \subseteq C \subseteq B$ one has $\mathrm{rk}^*(C) = \mathrm{rk}^*(A) + |C \cap F|$. In particular this implies that $\mathrm{rk}^*(B) = \mathrm{rk}^*(A) + |F|$.

Now using the formula for rk^* given in Proposition 1.2.5 from the introductory part we get that

$$|B| - \mathrm{rk}(X) + \mathrm{rk}(X \setminus B) = |A| - \mathrm{rk}(X) + \mathrm{rk}(X \setminus A) + |F|,$$

which in addition yields

$$\mathrm{rk}(X \setminus A) = \mathrm{rk}(X \setminus B) + |B| - |A| - |F| = \mathrm{rk}(X \setminus B) + |T|. \tag{2.2.1}$$

Moreover we may observe that $X \setminus A$ can be written as a disjoint union $X \setminus A = (X \setminus B) \cup T \cup F$. Additionally we have for every C with $A \subseteq C \subseteq B$ that $(X \setminus B) \subseteq (X \setminus C) \subseteq (X \setminus A)$. We may thus compute:

$$\begin{aligned} |C| - \mathrm{rk}(X) + \mathrm{rk}(X \setminus C) &= \mathrm{rk}^*(C) \\ &= \mathrm{rk}^*(A) + |C \cap F| \\ \text{(again by 1.2.5)} &= |A| - \mathrm{rk}(X) + \mathrm{rk}(X \setminus A) + |C \cap F|. \end{aligned}$$

Hence we deduce that

$$\begin{aligned} \mathrm{rk}(X \setminus C) &= \mathrm{rk}(X \setminus A) + |A| + |C \cap F| - |C| \\ &= \mathrm{rk}(X \setminus A) - |C \cap T| \\ \text{(use (2.2.1)} &= \mathrm{rk}(X \setminus B) + |T| - |C \cap T| \\ &= \mathrm{rk}(X \setminus B) + |(X \setminus C) \cap T|. \end{aligned}$$

In conclusion, we have shown that if $[A, B]$ is a molecule in the dual, then $[X \setminus B, X \setminus A]$ is a molecule in the primal matroid. Hence axiom (AM3) applies in this situation and we finally compute for the dual multiplicities that

$$\begin{aligned} \mathfrak{m}^*(A) \cdot \mathfrak{m}^*(B) &= \mathfrak{m}(X \setminus A) \cdot \mathfrak{m}(X \setminus B) \\ \text{(by primal (AM3))} &= \mathfrak{m}((X \setminus B) \cup F) \cdot \mathfrak{m}((X \setminus B) \cup T) \\ &= \mathfrak{m}((X \setminus B) \cup (X \setminus (X \setminus F))) \cdot \mathfrak{m}((X \setminus B) \cup (X \setminus (X \setminus T))) \\ &= \mathfrak{m}(X \setminus (B \cap (X \setminus F))) \cdot \mathfrak{m}(X \setminus (B \cap (X \setminus T))) \\ &= \mathfrak{m}(X \setminus (A \cup T)) \cdot \mathfrak{m}(X \setminus (A \cup F)) \\ &= \mathfrak{m}^*(A \cup T) \cdot \mathfrak{m}^*(A \cup F). \end{aligned}$$

Therefore we have verified (AM3) in the dual and we are done. □

Having this quite handy and well-behaved notion of duality up our sleeve we may now go on studying the little more complex concept of representability. We want to know, how to generalise the classical notion in ordinary matroids, such that it gets on well with the multiplicity function. Furthermore we will see how duality interferes with representability. The very satisfying answer to that question will eventually complete the proof of Theorem 2.1.7.

2.2.2 Representability

We already have given a formal definition of representability in the introductory part. Nevertheless I would like to discuss the concept again in more detail.

We remind ourselves that some of the first matroids ever studied were finite lists of vectors over a finite dimensional vector space. Such a list of vectors can always be depicted as a matrix where its columns coincide exactly with the entries of our list. Even the name *matroid* originates from the term *matrix*.

In other words, a matrix can be viewed as the most classical or most simple form of a matroid. The other origin of matroid theory is graph theory. However, we have already remarked in the introductory part, that every graphical matroid is isomorphic to a matroid over a vector space and hence given by a matrix too. We notice that it can be useful to study matroids that can be *represented by a matrix* since this property seems to be incident on all fundamental examples of matroids.

We pour our observations into a detailed definition.

Definition. A matroid $\mathcal{M}_X$ over a finite set X is called *representable* over $\mathbb{K}^n$ if it can be realised by a list of vectors in $\mathbb{K}^n$. In other words, $\mathcal{M}_X$ is representable if there is a matroid-isomorphism to the matroid induced by a finite list of vectors, where the rank is given by the dimension of the span of subsets.

In our context we are mostly interested in matroids representable over $\mathbb{R}$. Luca Moci and Michele D'Adderio call this class of matroids *0-representable* (compare [MD12, Section 3]). For arithmetic matroids they generalise the notion of representability as follows: Firstly, representability is always a notion considered stable under isomorphisms. Therefore, one needs to make precise, what it means for two arithmetic matroids to be isomorphic to each other.

Definition. An isomorphism ϕ between two arithmetic matroids $(X, \mathrm{rk}_X, \mathfrak{m}_X)$ and $(Y, \mathrm{rk}_Y, \mathfrak{m}_Y)$ is a bijection $\phi : X \to Y$ such that ranks and multiplicities are preserved under ϕ. Concretely this means that for all $B \subseteq Y$ and $A \subseteq X$ with $\phi(A) = B$ one has $\mathrm{rk}_Y(B) = \mathrm{rk}_X(A)$ and $\mathfrak{m}_Y(B) = \mathfrak{m}_X(A)$.

Now representability of arithmetic matroids is defined in the following way.

Definition (arithmetic representability, [MD12, Section 3])**.** Let $\mathcal{M}_X \widehat{=} (\mathcal{M}_X, \mathfrak{m})$ be an arithmetic matroid. Then $\mathcal{M}_X$ is considered *representable* if it can be realised by a list of elements of a finitely generated abelian group. I.e. it is isomorphic to one of the matroids described in Section 2.1.2. Furthermore we call the arithmetic matroid $\mathcal{M}_X$

- *0-representable* if the underlying matroid is 0-representable;
- *torsion-free* if $\mathfrak{m}(\emptyset) = 1$; and
- *GCD* if its multiplicity function fulfils the so-called *GCD-rule*: $\mathfrak{m}(A)$ is equal to the greatest common divisor (GCD) of the multiplicities of the maximal independent sublists of A. Formally:

$$\mathfrak{m}(A) = \gcd(\{\mathfrak{m}(B) \mid B \subseteq A \text{ and } |B| = \mathrm{rk}(B) = \mathrm{rk}(A)\}).$$

Remark ([MD12, Rem. 3.1])*.* These properties fulfil certain relations. Firstly, if an arithmetic matroid is representable, then it clearly is also 0-representable. One may take for example the tensor with $\mathbb{Q}$ to see this.

If an arithmetic matroid is representable and torsion-free, then one can conclude, that it is already GCD (see [MD12, Rem. 3.9]).

Observing the definition, we see that for arithmetic matroids, finitely generated abelian groups take the place of vector spaces in standard matroid theory. But since arithmetic representability demands strong criteria not only on the rank but also on the multiplicity function it is possible to construct arithmetic matroids that are 0-representable but not representable in the arithmetic context. The following example is taken from [MD12, Example 3.3].

Example. Let $X = \{a, b, c\}$. We obtain a matroid structure on X by fixing the three bases $\{a, b\}$, $\{a, c\}$ and $\{b, c\}$. Clearly the resulting matroid is 0-representable. It is realised by three pairwise non-parallel vectors in the plane. Take for example $a \leftrightarrow (1, 0)$, $b \leftrightarrow (1, 1)$ and $c \leftrightarrow (0, 1)$.

Clearly one can define a representable arithmetic matroid on X. Just observe the lattice $\Lambda = \langle (1, 0), (1, 1), (0, 1) \rangle_{\mathbb{Z}} \cong \mathbb{Z}^2$ and set the multiplicities as discussed in the last section. Since the construction is torsion-free, the resulting matroid would also be GCD.

However, one could also take some other multiplicities. Let us set the multiplicities of the bases $\mathfrak{m}(\{a, b\}) = \mathfrak{m}(\{a, c\}) = \mathfrak{m}(\{b, c\}) = 2$ and let $\mathfrak{m}(A) = 1$ for any other subset $A \subseteq X$. Then one can easily check that (AM1)–(AM5) are satisfied and we therefore obtain an arithmetic matroid that is also torsion-free. But since $\mathfrak{m}(X) = 1 \neq 2 = \gcd(\{B \mid B \text{ is a basis}\})$ we have that the arithmetic matroid is not GCD. Reviewing the previous remark it therefore cannot be representable.

Example. Since arithmetic representability implies 0-representability and every matroid can become an arithmetic matroid when equipped with suitable (maybe trivial) multiplicities, clearly every matroid that is **not** 0-representable yields an example for a non-representable arithmetic matroid. E.g. in [MD12, Example 3.2] the *Fano matroid* is suggested. It is given by the seven non-zero elements of $\mathbb{F}_2^3$, where $\mathbb{F}_2$ denotes the field with two elements.

By now we have a well behaved and understandable concept of representability. Like in ordinary matroid theory it covers the main examples, in this case arithmetic matroids over lattices, finitely generated abelian groups and graphs. The next step will be to combine both the notion of representability and duality. Their symbiosis can be summarised in the following statement.

Theorem 2.2.2 (Representability of the dual [MD12, Section 3.4])**.** *Let $\mathcal{M}_X$ be a representable arithmetic matroid. Then its dual $\mathcal{M}_X^*$ also is representable.*

Proof. We need an abelian group G' and a finite list $X' \subseteq G'$ such that the resulting arithmetic matroid $\mathcal{M}_{X'}$ is isomorphic to $\mathcal{M}_X^*$. Clearly we must have $|X| = |X'|$ and also the relation $\operatorname{rk}(X') = |X| - \operatorname{rk}(X)$ needs to hold.

To construct the desired object we start from our given matroid $\mathcal{M}_X$. Since this one is representable we extract a finitely generated abelian group G whose elements realise $\mathcal{M}_X$. Recall that Theorem 2.1.6 guarantees us a representation of G as

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \cdots \oplus \mathbb{Z}/d_s\mathbb{Z},$$

where d_i divides d_{i+1} for all $i = 1, \ldots, s-1$. It is a well known fact from abstract algebra that this representation is also unique. We realize it as $\mathbb{Z}^{r+s}/\langle Q \rangle$, with $Q =$

$\{q_1, \ldots, q_s\} \subset \mathbb{Z}^{r+s}$, where q_i is defined by having d_i in the $(r+i)$'th position and 0 elsewhere. We fix the order in which the elements of Q are given.

The finite list $X \subseteq G$, which is inducing our matroid, is then given as a list of cosets $X = \{\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n\}$. Here $\bar{x}_i = x_i + \langle Q \rangle$ for some $x_i \in \mathbb{Z}^{r+s}$. We choose suitable such representatives x_i for all $i = 1, \ldots, n$ and collect them in a new list $\widetilde{X} = \{x_1, \ldots, x_n\}$. Moreover we remember the order of the elements in $\widetilde{X}$.

Now we regard the $(r+s) \times (n+s)$ matrix $(\widetilde{X}, Q) = (x_1, \ldots, x_n, q_1, \ldots, q_s)$, whose columns are given by the elements of $\widetilde{X}$ and Q respectively in the fixed orders. Its transpose $(\widetilde{X}, Q)^T$ shall then be interpreted as the list of the rows of $(\widetilde{X}, Q)$ in order from up to down. Its elements are now vectors in $\mathbb{Z}^{n+s}$. Finally we set $G' := \mathbb{Z}^{n+s}/\langle (\widetilde{X}, Q)^T \rangle$ and $X' = \{\bar{e}_1, \ldots, \bar{e}_n\}$ the demanded list of cosets, where as usual e_i denotes the i'th unit vector with 1 at the i'th position and 0 elsewhere.

Let $\mathcal{M}'_X$ denote the arithmetic matroid induced by the pair (G', X').

Claim ([MD12, Thm. 3.8]). The matroid $\mathcal{M}'_X$ is already isomorphic to the dual $\mathcal{M}^*_X$.

At first, we introduce some useful notations.

- We denote the set $\{1, 2, \ldots, n\}$ simply by $[n]$.
- For $J \subseteq [n]$ we let $\bar{x}_J := \{\bar{x}_i \in X \mid i \in J\}$ and also $\bar{e}_J := \{\bar{e}_i \in X' \mid i \in J\}$.
- Just like before, given a finite list $Y \subset \mathbb{Z}^m$ with a fixed order on it, we denote by (Y) the $m \times |Y|$ matrix whose columns are the elements of Y.

Now in order to prove the claim, we give an intuitive bijection between $\mathcal{M}'_X$ and $\mathcal{M}^*_X$ and then show that it is rank- and multiplicity preserving. Hence let $A \subseteq X$, then A is uniquely given by a finite list $J \subseteq [n]$. (The same is true for each $B \subseteq X'$). In particular in this case we have $A = \bar{x}_J$. Therefore an intuitive choice of a bijection is given by $\bar{x}_J \leftrightarrow \bar{e}_J$.

We need to show, that this mapping preserves ranks and multiplicities. At first we make the following observation: Let $A \subseteq \widetilde{X}$ be a sublist with elements in $\mathbb{Z}^{r+s}$ and let $\overline{A} = \{\bar{a} \mid a \in A\} \subseteq X$ be the according list of cosets with elements in G. Now we use

$$\langle A \cup Q \rangle / \langle Q \rangle \cong \langle \bar{A} \rangle,$$

and therefore conclude, that the rank of $\overline{A}$ is equal to the rank of $\langle A \cup Q \rangle$ minus the rank of $\langle Q \rangle$. $(*)$

Moreover the multiplicity of $\overline{A}$ in G equals the multiplicity of $A \cup Q$ in $\mathbb{Z}^{r+s}$. Indeed, let $\langle H \rangle / \langle Q \rangle$ be the maximal subgroup of G, in which $\langle \bar{A} \rangle$ has finite index, where $H \subseteq \mathbb{Z}^{r+s}$. Thus we have

$$[\langle H \rangle / \langle Q \rangle : \langle A \cup Q \rangle / \langle Q \rangle] = [\langle H \rangle : \langle A \cup Q \rangle].$$

Note that $\langle H \rangle$ clearly is the maximal subgroup in $\mathbb{Z}^{r+s}$ in which $\langle A \cup Q \rangle$ has finite index. Analogous reasoning applies also to sublists of G' using $(\widetilde{X}, Q)^T$ instead of Q. This shows we can reduce the problem of computing ranks and multiplicities in G or G' to computing them in $\mathbb{Z}^{r+s}$ and $\mathbb{Z}^{n+s}$, respectively.

Therefore let $J \in [n]$. We want to compute the rank of $\bar{e}_J$. By the above it suffices to find at first the rank of the matrix $(e_J \cup (\widetilde{X}, Q)^T)$, where $e_J = \{e_i \mid i \in J\}$ is a set of unit vectors in $\mathbb{Z}^{n+s}$. This matrix takes the following form:

$$\begin{pmatrix} & (e_J) & & (\widetilde{X})^T \\ 0 & \dots & 0 & \\ \vdots & & \vdots & (Q)^T \\ 0 & \dots & 0 & \end{pmatrix}.$$

Thus, the rank of $(e_J \cup (\widetilde{X}, Q)^T)$ is given by $|J|$ plus the rank of $x_{J^C} \cup Q$ where $x_{J^C} = \{x_i \mid i \in J^C\}$ and $J^C = [n] \setminus J$. Observe that the rank of $\bar{e}_J$ is simply the rank of $(e_J \cup (\widetilde{X}, Q)^T)$ minus the rank of $(\widetilde{X}, Q)^T$. The last one clearly equals the rank of $\widetilde{X} \cup Q$. We put all this information together and obtain:

$$\begin{aligned} \operatorname{rk}(\bar{e}_J) &= |J| - \operatorname{rk}(\widetilde{X} \cup Q) + \operatorname{rk}(x_{J^C} \cup Q) \\ &= |J| - (\operatorname{rk}(\widetilde{X} \cup Q) - \operatorname{rk}(Q)) + (\operatorname{rk}(x_{J^C} \cup Q) - \operatorname{rk}(Q)) \\ (*) &= |J| - \operatorname{rk}(X) + \operatorname{rk}(\bar{x}_{J^C}). \end{aligned}$$

Now using $\bar{x}_{J^C} = X \setminus \bar{x}_J$ and Proposition 1.2.5 we get exactly $\operatorname{rk}(\bar{e}_J) = \operatorname{rk}^*(\bar{x}_J)$ as demanded.

It is still left to compute the multiplicity $\mathfrak{m}'(\bar{e}_J)$ of $\bar{e}_J$ in $\mathcal{M}'_X$. We use the fact that in $\mathbb{Z}^{n+s}$ the multiplicity of a sublist can be computed by taking the greatest common divisor of all minors of maximal rank in the matrix $(e_J \cup (\widetilde{X}, Q)^T)$ (compare with [MD12, Rem. 3.9], this is because arithmetic matroids in $\mathbb{Z}^m$ are GCD). Now note that each such minor must involve all rows indexed by J, otherwise one could find a nonzero minor of higher order taking the missing rows. Nevertheless, such a nonzero minor of maximal rank is clearly plus or minus a nonzero minor of maximal rank of the matrix $(x_{J^C} \cup Q)$. However, those are exactly the minors observed when computing the multiplicity of $\bar{x}_{J^C}$. Therefore

$$\mathfrak{m}'(\bar{e}_J) = \mathfrak{m}(\bar{x}_{J^C}) = \mathfrak{m}(X \setminus \bar{x}_J) = \mathfrak{m}^*(\bar{x}_J).$$

This completes the proof of the claim and therefore of the theorem. □

Besides duality, there exist several other operations on matroids. For the end of this chapter we would like to generalise them too to the arithmetic case. This is done in the next section.

2.3 Deletion, contraction and direct sums of arithmetic matroids

We have already introduced *deletion* and *contraction* by a proper vector $v \in X$ in an ordinary matroid $\mathcal{M} = (X, \operatorname{rk})$. These fundamental constructions have been denoted $\mathcal{M} \setminus v$ for the deletion by v and $\mathcal{M}/v$ for the contraction by v. (See Section 1.2.3 to refresh the details.)

Also the direct sum $\mathcal{M}_1 \oplus \mathcal{M}_2$ of two matroids $\mathcal{M}_1$ and $\mathcal{M}_2$ has been defined in the introductory part. (Find the definition just before Proposition 1.2.12.)

We now want to briefly discuss how these constructions generalise to the case of arithmetic matroids. In particular, we want to state how to choose the resulting multiplicity functions of the deletion, contraction and direct sum, such that the arithmetic Tutte polynomial inherits the beautiful properties of the ordinary Tutte polynomial in the non-arithmetic case.

This is done in a simple definition. See [MD12, Sections 4.3 and 4.6] for further details.

Definition. Let $\mathcal{M} = (X, \mathrm{rk})$, $\mathcal{M}_1 = (X_1, \mathrm{rk}_1)$ and $\mathcal{M}_2 = (X_2, \mathrm{rk}_2)$ be matroids and let $\mathfrak{m}$, $\mathfrak{m}_1$ and $\mathfrak{m}_2$ be suitable multiplicity functions such that $(\mathcal{M}, \mathfrak{m})$, $(\mathcal{M}_1, \mathfrak{m}_1)$ and $(\mathcal{M}_2, \mathfrak{m}_2)$ form arithmetic matroids.

Moreover let $v \in X$ be a *proper vector* (i.e. neither loop nor coloop). We define

- *the deletion of* $(\mathcal{M}, \mathfrak{m})$ *by* v as the arithmetic matroid $(\mathcal{M} \setminus v, \mathfrak{m}_{\setminus v})$, where $\mathcal{M} \setminus v$ denotes the classical deletion of the underlying matroid and the multiplicity is given by $\mathfrak{m}_{\setminus v} := \mathfrak{m}(A)$ for all $A \subseteq X \setminus v$;
- *the contraction of* $(\mathcal{M}, \mathfrak{m})$ *by* v as the arithmetic matroid $(\mathcal{M}/v, \mathfrak{m}_{/v})$, where $\mathcal{M}/v$ denotes the classical contraction of the underlying matroid and the multiplicity is given by $\mathfrak{m}_{/v} := \mathfrak{m}(A \cup \{v\})$ for all $A \subseteq X \setminus v$;
- *the direct sum of* $(\mathcal{M}_1, \mathfrak{m}_1)$ *and* $(\mathcal{M}_2, \mathfrak{m}_2)$ as the arithmetic matroid $(\mathcal{M}_1 \oplus \mathcal{M}_2, \mathfrak{m}_\oplus)$ where $\mathcal{M}_1 \oplus \mathcal{M}_2$ denotes the classical direct sum of matroids and the multiplicity is given by $\mathfrak{m}_\oplus(A) := \mathfrak{m}_1(A \cap X_1) \cdot \mathfrak{m}_2(A \cap X_2)$ for all $A \subseteq X_1 \cup X_2$.

Remark. All the constructions given above are indeed arithmetic matroids themselves. In case of deletion and contraction this is straightforward to see: $\mathfrak{m}_{\setminus v}$ and $\mathfrak{m}_{/v}$ are both defined via $\mathfrak{m}$ and hence they fulfil the defining axioms (AM1)–(AM5) since $\mathfrak{m}$ does so.

In case of $\mathfrak{m}_\oplus$ we may argue by writing

$$\mathfrak{m}_\oplus = \mathfrak{m}_1' \cdot \mathfrak{m}_2',$$

where $\mathfrak{m}_i'$ for $i = 1, 2$ may be defined by $\mathfrak{m}_i'(A) = \mathfrak{m}_i(A \cap X_i)$. Clearly $\mathfrak{m}_i'$ is an arithmetic multiplicity on $X_1 \cup X_2$ fulfilling all the necessary axioms since $\mathfrak{m}_i$ fulfils them on X_i. Therefore $(\mathcal{M}_1 \oplus \mathcal{M}_2, \mathfrak{m}_1')$ and $(\mathcal{M}_1 \oplus \mathcal{M}_2, \mathfrak{m}_2')$ are both arithmetic matroids. But since the arithmetic matroids on a given underlying matroid form a commutative monoid with respect to the product of multiplicities (compare with Theorem 2.1.4), also $(\mathcal{M}_1 \oplus \mathcal{M}_2, \mathfrak{m}_\oplus)$ has to be an arithmetic matroid.

3 The arithmetic Tutte polynomial

Even though arithmetic matroids are very fascinating mathematical structures on their own, at the end of the day we still want to do combinatorics with them. To do this, we regard their most important combinatorial invariant: the arithmetic Tutte polynomial. For an arithmetic matroid $\mathcal{M} = (X, \mathrm{rk}, \mathfrak{m})$ over a set X we recall its definition:

$$M_{\mathcal{M}}(x, y) = \sum_{A \subseteq X} \mathfrak{m}(A)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)}.$$

In the case of representable arithmetic matroids we already have stated some of its marvelous properties, as well as some possible interpretations of special values. In this chapter we want to further analyse its structure in relation to the underlying arithmetic matroid. We will look at proofs for some formulas similar to the ones fulfilled by the Tutte polynomial in the case of ordinary matroids, which we also mentioned in the introductory part. Eventually we are going to give an overview on some more possible interpretations of its values in the concrete settings of geometric lattices and labelled graphs.

3.1 Identities for the arithmetic Tutte polynomial

In this section we want to generalise the identities presented in the introductory part and fulfilled by the ordinary Tutte polynomial to the arithmetic case. We will see that the same or very similar statements hold. In any case will the results for the ordinary Tutte polynomial follow directly from the theorems stated in this section just by regarding $\mathfrak{m} \equiv 1$, the trivial multiplicity.

We start by showing how the arithmetic Tutte polynomial behaves with respect to direct sums of the underlying arithmetic matroids. Afterwards we show some deletion-contraction recurrences satisfied by the arithmetic Tutte polynomial. Those will be used to prove an expansion of the arithmetic Tutte polynomial into so-called *external activity polynomials*. They are strongly related to a generalised version of Crapo's theorem (see Theorem 1.2.14) which we show afterwards. Finally we discuss a beautiful convolution-like formula abstracting the one given by Kook, Reiner and Stanton in [KRS99, Thm. 1] and stated as Theorem 1.2.13 in the introductory part.

3.1.1 Arithmetic Tutte polynomials of direct sums

We start with a very easy result concerning the direct sum of arithmetic matroids. It tells us how to compute the arithmetic Tutte Polynomial of the sum by knowing the arithmetic Tutte polynomial of the summands.

Proposition 3.1.1 ([MD12, Section 4.6])**.** *Let $\mathcal{M}_1 \oplus \mathcal{M}_2$ be the direct sum of two arithmetic matroids $\mathcal{M}_1$ and $\mathcal{M}_2$. Then their arithmetic Tutte polynomials fulfil:*

$$M_{\mathcal{M}_1 \oplus \mathcal{M}_2}(x, y) = M_{\mathcal{M}_1}(x, y) \cdot M_{\mathcal{M}_2}(x, y).$$

Proof. We remind ourselves that every $A \subseteq X_1 \sqcup X_2$ can be written as a decomposition $A = B \sqcup C$, with $B = A \cap X_1$ and $C = A \cap X_2$. Then we simply have by definition $\mathfrak{m}_\oplus(A) = \mathfrak{m}_1(B) \cdot \mathfrak{m}_2(C)$ and $\mathrm{rk}_\oplus(A) = \mathrm{rk}_1(B) + \mathrm{rk}_2(C)$. Hence clearly we have

$$\begin{aligned}
M_{\mathcal{M}_1 \oplus \mathcal{M}_2}(x, y) &= \sum_{A \subseteq X_1 \cup X_2} \mathfrak{m}_\oplus(A)(x-1)^{\mathrm{rk}_\oplus(X_1 \cup X_2) - \mathrm{rk}_\oplus(A)}(y-1)^{|A| - \mathrm{rk}_\oplus(A)} \\
&= \sum_{\substack{B \subseteq X_1 \\ C \subseteq X_2}} \mathfrak{m}_\oplus(B \cup C)(x-1)^{\mathrm{rk}_\oplus(X_1 \cup X_2) - \mathrm{rk}_\oplus(B \cup C)}(y-1)^{|B \cup C| - \mathrm{rk}_\oplus(B \cup C)} \\
&= \sum_{\substack{B \subseteq X_1 \\ C \subseteq X_2}} \mathfrak{m}_1(B)\mathfrak{m}_2(C)(x-1)^{\mathrm{rk}_1(X_1) + \mathrm{rk}_2(X_2) - \mathrm{rk}_1(B) - \mathrm{rk}_2(C)}(y-1)^{|B| + |C| - \mathrm{rk}_1(B) - \mathrm{rk}_2(C)} \\
&= M_{\mathcal{M}_1}(x, y) \cdot M_{\mathcal{M}_2}(x, y).
\end{aligned}$$

□

3.1.2 Deletion and contraction recurrences

We continue with maybe the most important relations satisfied by the arithmetic Tutte polynomial, the *deletion and contraction recurrence*. It will let us reduce critical observations to the case of molecules, where everything is quite easy. The lemma proven in this section will be crucial to prove the more involved *external activity expansion* of the arithmetic Tutte polynomial and was originally used to prove the *combinatorial formula* generalising Crapo's theorem ([MD12, Section 6]).

We state it right away. For simplicity we reuse the notations of the situation of ordinary matroids. Thus, if $\mathcal{M} = (X, \mathrm{rk}, \mathfrak{m})$ is an arithmetic matroid and $v \in X$ is a proper vector, then we denote by $\mathcal{M} \setminus v$ and $\mathcal{M}/v$ the deletion and contraction of $\mathcal{M}$ by v in terms of arithmetic matroids, respectively.

Lemma 3.1.2 ([MD12, Lem. 5.4])**.** *Let $\mathcal{M} = (X, \mathrm{rk}, \mathfrak{m})$ be an arithmetic matroid and let $v \in X$ be a proper vector. Then the arithmetic Tutte polynomial fulfils the following recursion:*

$$M_{\mathcal{M}}(x, y) = M_{\mathcal{M} \setminus v}(x, y) + M_{\mathcal{M}/v}(x, y),$$

where $M_{\mathcal{M} \setminus v}(x, y)$ and $M_{\mathcal{M}/v}(x, y)$ denote the arithmetic Tutte polynomials of the deletion and contraction, respectively.

Proof. Recall Proposition 1.2.7 that tells us that $\mathrm{rk}_d(A) = \mathrm{rk}(A)$ and $\mathrm{rk}_c(A) = \mathrm{rk}(A \cup \{v\}) - \mathrm{rk}(\{v\})$ for all $A \subseteq X \setminus \{v\}$, where rk_d and rk_c denote the rank functions in the

underlying deletion- and contraction matroids, respectively. Then we simply compute

$$\begin{aligned}
M_{\mathcal{M}}(x,y) &= \sum_{A\subseteq X} \mathfrak{m}(A)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)} \\
&= \sum_{v\notin A\subseteq X} \mathfrak{m}(A)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)} + \\
&\quad + \sum_{v\in A\subseteq X} \mathfrak{m}(A)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)} \\
&= \sum_{v\notin A\subseteq X} \mathfrak{m}_{\setminus v}(A)(x-1)^{\mathrm{rk}_d(X\setminus\{v\})-\mathrm{rk}_d(A)}(y-1)^{|A|-\mathrm{rk}_d(A)} + \\
&\quad + \sum_{v\in A\subseteq X} \mathfrak{m}_{/v}(A\setminus\{v\})(x-1)^{\mathrm{rk}_c(X\setminus\{v\})-\mathrm{rk}_c(A\setminus\{v\})}(y-1)^{|A\setminus\{v\}|-\mathrm{rk}_c(A\setminus\{v\})} \\
&= M_{\mathcal{M}\setminus v}(x,y) + M_{\mathcal{M}/v}(x,y).
\end{aligned}$$

□

Some properties of the arithmetic Tutte polynomial correspond very well to this deletion and contraction recurrence. Hence when proving them, the previous lemma allows us to reduce the problem to the case, where no proper vectors are left. I.e. to the case of molecules. If we want to further simplify the situation, and we do, we may use the following result.

Lemma 3.1.3 ([MD12, Lem. 5.7])**.** *Let $\mathcal{M} = (X, \mathrm{rk}, \mathfrak{m})$ be an arithmetic matroid with **no proper vectors**. Assume $v \in X$ is a coloop, then we have*

$$M_{\mathcal{M}}(x,y) = (x-1)M_{\mathcal{M}\setminus v}(x,y) + M_{\mathcal{M}/v}(x,y).$$

Proof. Since $v \in X$ is a coloop, we observe that for $v \in A \subseteq X$ we have $\mathrm{rk}_d(A\setminus\{v\}) = \mathrm{rk}_c(A\setminus\{v\}) = \mathrm{rk}(A) - 1$, where rk_d and rk_c denote the rank functions in the deletion and the contraction, respectively. Therefore we may compute that

$$\begin{aligned}
M_{\mathcal{M}}(x,y) &= \sum_{A\subseteq X} \mathfrak{m}(A)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)} \\
&= \sum_{v\notin A\subseteq X} \mathfrak{m}(A)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)} + \\
&\quad + \sum_{v\in A\subseteq X} \mathfrak{m}(A)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)} \\
&= \sum_{v\notin A\subseteq X} \mathfrak{m}_{\setminus v}(A)(x-1)^{\mathrm{rk}_d(X\setminus\{v\})+1-\mathrm{rk}_d(A)}(y-1)^{|A|-\mathrm{rk}_d(A)} + \\
&\quad + \sum_{v\in A\subseteq X} \mathfrak{m}_{/v}(A\setminus\{v\})(x-1)^{\mathrm{rk}_c(X\setminus\{v\})-\mathrm{rk}_c(A\setminus\{v\})}(y-1)^{|A\setminus\{v\}|-\mathrm{rk}_c(A\setminus\{v\})} \\
&= (x-1)M_{\mathcal{M}\setminus v}(x,y) + M_{\mathcal{M}/v}(x,y),
\end{aligned}$$

just as desired. □

By duality we can conclude the following statement immediately.

Lemma 3.1.4 ([MD12, Lem. 5.9])**.** *Let $\mathcal{M} = (X, \mathrm{rk}, \mathfrak{m})$ be an arithmetic matroid with* ***no proper vectors****. Assume $v \in X$ is a loop, then we have*

$$M_{\mathcal{M}}(x, y) = M_{\mathcal{M} \setminus v}(x, y) + (y - 1)M_{\mathcal{M}/v}(x, y).$$

Since an arithmetic matroid without any proper vectors only consists of loops and coloops the two lemmas above let us reduce the underlying matroid step by step, vector by vector, to the empty matroid. There some *a priori* difficult questions may be answered trivially. The combination of all three lemmas in this section lets us reduce *every (arithmetic) matroid* to the empty one. We will use this technique to prove the more advanced formulas of the arithmetic Tutte polynomial waiting ahead in the next section.

3.1.3 External activity expansion of the arithmetic Tutte polynomial

In this section we are going to analyse an expansion of the arithmetic Tutte polynomial in terms of *external* and *internal activity polynomials*. We remind ourselves of the definition of *external activity on a basis B*. We observe an (arithmetic) matroid $\mathcal{M}_X$ on a list X and fix a total order on its elements. Then a vector $v \in X \setminus B$ is called externally active on the basis B if v is dependent on the elements of B following it in the fixed order. On the other hand $v \in B$ is *internally active on B* if it is externally active on B^C in the dual matroid.

Now following the instructions in [MD12, Section 5.1] we let $\mathcal{M} = (\mathcal{M}_X, \mathfrak{m})$ be an arithmetic matroid. Again we fix a total order on the vectors in X. Now we take a basis $B \subseteq X$ and a list T with $B \subseteq T \subseteq X$.

Definition (Local activities)**.** For every pair (B, T), with B a basis and T a list as described in the paragraph above we define the *local external activity* of the basis B in the list T as the number $e(B, T)$ of vectors $v \in T$ which are externally active on B.

Dually we define $e^*(B^C, \widetilde{T})$, with $B^C \subseteq \widetilde{T}$, to be the number of vectors in $\widetilde{T}$ externally active on B^C in the dual matroid (where B^C is a basis).

Remark. Note that loop vectors in T are never in B (since B is a basis) and are always externally active.

Using this we are able to define the *external and internal activity polynomials*.

Definition. For a sublist $A \subseteq X$ we set

$$\rho(A) := \sum_{T \supseteq A} (-1)^{|T|-|A|} \mathfrak{m}(T).$$

Now the *external activity polynomial* of a basis B in X is defined as

$$E_B(x) = \sum_{T \supseteq B} \rho(T) \cdot x^{e(B,T)},$$

while the *internal activity polynomial* of a basis B in X is defined in $\mathcal{M}_X^*$ as the dual polynomial:

$$E_{B^C}^*(x) = \sum_{\widetilde{T} \supseteq B^C} \rho^*(\widetilde{T}) \cdot x^{e^*(B^C, \widetilde{T})}.$$

With those in our repertoire we are able to construct the following expression:

$$\widetilde{M}_{\mathcal{M}}(x,y) := \sum_{\substack{B \subseteq X \\ B \text{ basis}}} \frac{1}{\mathfrak{m}(B)} E_{B^C}^*(x) \cdot E_B(y).$$

However, the new name turns out to be redundant, due to the following theorem of D'Adderio and Moci.

Theorem 3.1.5 ([MD12, Thm. 5.1])**.** *The arithmetic Tutte polynomial of an arithmetic matroid $\mathcal{M} = (\mathcal{M}_X, \mathfrak{m})$ coincides with $\widetilde{M}_{\mathcal{M}}(x,y)$, i.e. we have*

$$M_{\mathcal{M}}(x,y) = \sum_{\substack{B \subseteq X \\ B \text{ basis}}} \frac{1}{\mathfrak{m}(B)} E_{B^C}^*(x) \cdot E_B(y).$$

Remark. Since B is a basis, the term $\rho(T)$ inside the external activity polynomial, as well es its dual expression, fulfil the setting of axioms (AM4) and (AM5), respectively. Hence we have that $\rho(T) \geq 0$ and $\rho^*(\widetilde{T}) \geq 0$ for all summands in the polynomials. In particular we conclude, that the arithmetic Tutte polynomial $M_{\mathcal{M}}(x,y)$ does indeed have *positive coefficients*.

To prove the theorem above we apply the strategy discussed in the last section. We will prove separately that the polynomial $\widetilde{M}_{\mathcal{M}}(x,y)$ fulfils the same deletion and contraction recurrences. The first recurrence will reduce the question of equality to the case of molecules and the second one will further reduce it to the special situation where the arithmetic matroid is given by the empty list. But there the question is trivial, since

$$M_{\emptyset}(x,y) = \mathfrak{m}(\emptyset) = \widetilde{M}_{\emptyset}(x,y).$$

Therefore we need to prove both recurrences.

Lemma 3.1.6 ([MD12, Lem. 5.4])**.** *Let $\mathcal{M} = (X, \mathrm{rk}, \mathfrak{m})$ be an arithmetic matroid. We fix a total order on X and let $v \in X$ be* ***the greatest proper vector****. Then we have*

$$\widetilde{M}_{\mathcal{M}}(x,y) = \widetilde{M}_{\mathcal{M} \setminus v}(x,y) + \widetilde{M}_{\mathcal{M}/v}(x,y).$$

Proof. We observe that

$$\begin{aligned}\widetilde{M}_{\mathcal{M}}(x,y) &= \sum_{\substack{B\subseteq X\\ B \text{ basis}}} \frac{1}{\mathfrak{m}(B)} E^*_{B^C}(x)\cdot E_B(y)\\ &= \sum_{\substack{B\subseteq X\\ v\in B \text{ basis}}} \frac{1}{\mathfrak{m}(B)} E^*_{B^C}(x)\cdot E_B(y) + \sum_{\substack{B\subseteq X\\ v\notin B \text{ basis}}} \frac{1}{\mathfrak{m}(B)} E^*_{B^C}(x)\cdot E_B(y)\end{aligned}$$

Claim. The first sum already equals the polynomial $\widetilde{M}_{\mathcal{M}/v}(x,y)$ for the contraction matroid by the vector v.

Actually for each basis B, the set $B\setminus\{v\}$ remains a basis in the contraction, and every externally active vector on B remains externally active in the contraction on $B\setminus\{v\}$. On the other hand, what was not externally active on B, is still not active on $B\setminus\{v\}$ in the contraction. Therefore $e(B,T) = e_c(B\setminus\{v\},T)$, for all (B,T), $v\in B$.

Now if we use the short notation $\mathfrak{m}_c$ for the multiplicity in the contraction by v, then we remind ourselves that $\mathfrak{m}_c(A) = \mathfrak{m}(A\cup\{v\})$ for all subsets $A\subseteq X\setminus\{v\}$ (which is the groundlist of $\mathcal{M}/v$). Thus we also deduce that for all $S\subseteq X\setminus\{v\}$ such that $S\supseteq B\setminus\{v\}$ we have $\rho_c(S) = \rho(S\cup\{v\})$. However, this already yields that $E_B(y)$ is the external activity polynomial of the basis $B\setminus\{v\}$ in the contraction by v.

Additionally, in the dual, v cannot be externally active on B^C, just because v is the greatest proper vector. Hence in the contraction of $\mathcal{M}$ by v, which corresponds to the deletion of v dually, we also have that vectors being externally active on B^C in the dual, remain active, while on the other hand, what was not active on B^C before is still not active in the dual after contraction. We get $e^*(B,T) = e^*_c(B,T)$, for all (B,T), $v\in B$.

Eventually, for all $S\subseteq X\setminus\{v\}$ with $S\supseteq B^C$ we compute

$$\begin{aligned}\rho^*(S)+\rho^*(S\cup\{v\}) &= \sum_{T\supseteq S}(-1)^{|T|-|S|}\mathfrak{m}^*(T) + \sum_{T\supseteq S\cup\{v\}}(-1)^{|T|-|S|}\mathfrak{m}^*(T)\\ &= \sum_{T\supseteq S}(-1)^{|T|-|S|}\mathfrak{m}^*(T) - \sum_{\substack{T\supseteq S\\ v\in T}}(-1)^{|T|-|S|}\mathfrak{m}*(T)\\ &= \sum_{\substack{T\supseteq S\\ v\notin T}}(-1)^{|T|-|S|}\mathfrak{m}^*(T)\\ &= \sum_{\substack{T\supseteq S\\ v\notin T}}(-1)^{|T|-|S|}\mathfrak{m}(X\setminus T)\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{T \supseteq S \\ v \notin T}} (-1)^{|T|-|S|} \mathfrak{m}((X \setminus \{v\}) \setminus T \cup \{v\}) \\
&= \sum_{\substack{T \supseteq S \\ v \notin T}} (-1)^{|T|-|S|} \mathfrak{m}_c((X \setminus \{v\}) \setminus T) \\
&= \sum_{\substack{T \supseteq S \\ v \notin T}} (-1)^{|T|-|S|} \mathfrak{m}_c^*(T) = \rho_c^*(S).
\end{aligned}
$$

Therefore when we observe for the internal activity polynomial that

$$
\begin{aligned}
E^*_{B^C}(x) &= \sum_{\widetilde{T} \supseteq B^C} \rho^*(\widetilde{T}) \cdot x^{e^*(B^C, \widetilde{T})} \\
&= \sum_{v \notin \widetilde{T} \supseteq B^C} \left(\rho^*(\widetilde{T}) \cdot x^{e^*(B^C, \widetilde{T})} + \rho^*(\widetilde{T} \cup \{v\}) \cdot x^{e^*(B^C, \widetilde{T} \cup \{v\})}\right) \\
(*) &= \sum_{v \notin \widetilde{T} \supseteq B^C} (\rho^*(\widetilde{T}) + \rho^*(\widetilde{T} \cup \{v\})) \cdot x^{e^*(B^C, \widetilde{T})},
\end{aligned}
$$

where we used at $(*)$ that v is not active on B^C; we deduce by applying $\rho^*(T) + \rho^*(T \cup \{v\}) = \rho *_c (T)$ that $E^*_{B^C}(x)$ is already the internal activity polynomial in the contraction matroid. With this, we proved our claim.

By dual reasoning, it immediately follows that the second summand equals $\widetilde{M}_{\mathcal{M} \setminus v}(x, y)$ and we are done. □

With this and using Lemma 3.1.2 the problem stated by the theorem reduces to the molecular case. It remains to prove the second recurrence for $\widetilde{M}_{\mathcal{M}}(x, y)$.

Lemma 3.1.7 ([MD12, Lem. 5.10])**.** *If $\mathcal{M} = (X, \mathrm{rk}, \mathfrak{m})$ is an arithmetic matroid **with no proper vectors** and $v \in X$ is a coloop, then the following equation holds:*

$$\widetilde{M}_{\mathcal{M}}(x, y) = (x - 1)\widetilde{M}_{\mathcal{M} \setminus v}(x, y) + \widetilde{M}_{\mathcal{M}/v}(x, y).$$

Proof. Let B be the *unique* basis of our matroid. Then we have

$$\widetilde{M}_{\mathcal{M}}(x, y) = \frac{1}{\mathfrak{m}(B)} E^*_{B^C}(x) \cdot E_B(y).$$

Now we do the usual decomposition with $E^*_{B^C}(x)$:

$$E^*_{B^C}(x) = \sum_{\substack{\widetilde{T} \supseteq B^C \\ v \in \widetilde{T}}} \rho^*(\widetilde{T}) \cdot x^{e^*(B^C, \widetilde{T})} + \sum_{\substack{\widetilde{T} \supseteq B^C \\ v \notin \widetilde{T}}} \rho^*(\widetilde{T}) \cdot x^{e^*(B^C, \widetilde{T})} \tag{3.1.1}$$

We mind that v is a coloop and hence it is contained in B. Thus it can *never act on* B. On the other hand, v is a loop in the dual and $v \notin B^C$. Therefor it is *always externally*

active on B^C in the dual. By this, we observe that

$$\sum_{\substack{\widetilde{T}\supseteq B^C\\ v\in\widetilde{T}}} \rho^*(\widetilde{T})\cdot x^{e^*(B^C,\widetilde{T})} = x\cdot \sum_{\substack{\widetilde{T}\supseteq B^C\\ v\in\widetilde{T}}} \rho^*(\widetilde{T})\cdot x^{e^*(B^C,\widetilde{T}\setminus\{v\})}.$$

For $v\in\widetilde{T}$ we are able to compute:

$$\begin{aligned}
\rho_d^*(\widetilde{T}\setminus\{v\}) &= \rho^*_{X\setminus\{v\}}(\widetilde{T}\setminus\{v\})\\
&= \sum_{\widetilde{T}\setminus\{v\}\subseteq A\subseteq X\setminus\{v\}} (-1)^{|A|-|\widetilde{T}\setminus\{v\}|}\cdot \mathfrak{m}_d^*(A)\\
&= \sum_{\widetilde{T}\setminus\{v\}\subseteq A\subseteq X\setminus\{v\}} (-1)^{|A|-|\widetilde{T}\setminus\{v\}|}\cdot \mathfrak{m}_d((X\setminus\{v\})\setminus A)\\
&= \sum_{\widetilde{T}\setminus\{v\}\subseteq A\subseteq X\setminus\{v\}} (-1)^{|A|-|\widetilde{T}\setminus\{v\}|}\cdot \mathfrak{m}_d(X\setminus(A\cup\{v\}))\\
&= \sum_{\widetilde{T}\subseteq A'\subseteq X} (-1)^{|A'|-|\widetilde{T}|}\cdot \mathfrak{m}_d(X\setminus A')\\
&= \sum_{\widetilde{T}\subseteq A'\subseteq X} (-1)^{|A'|-|\widetilde{T}|}\cdot \mathfrak{m}_d^*(A') = \rho_X^*(\widetilde{T}) = \rho^*(\widetilde{T}).
\end{aligned}$$

By this we obtain, that the left summand of equation (3.1.1) already equals the internal activity polynomial $E^*_{d,B^C}(x)$ times x for the deletion of v. Moreover for the other summand we have

$$\sum_{\substack{\widetilde{T}\supseteq B^C\\ v\notin\widetilde{T}}} \rho^*(\widetilde{T})\cdot x^{e^*(B^C,\widetilde{T})} = \sum_{\widetilde{T}\supseteq B^C} \rho^*(\widetilde{T}) x^{e^*(B^C,\widetilde{T}\setminus\{v\})} - \sum_{\substack{\widetilde{T}\supseteq B^C\\ v\in\widetilde{T}}} \rho^*(\widetilde{T}) x^{e^*(B^C,\widetilde{T}\setminus\{v\})}.$$

By our previous calculations the right summand in this equation clearly coincides with $-E_d^*(\widetilde{T})$. For the first summand we make the same observations and computations as in the proof of Lemma 3.1.6 to show that for $B^C\subseteq\widetilde{S}\subseteq X\setminus\{v\}$ we have $\rho^*(\widetilde{S})+\rho^*(S\cup\{v\}) = \rho_c^*(\widetilde{S})$. This yields that the first summand is indeed equal to $E^*_{c,B^C}(x)$, the internal activity polynomial for the contraction of the coloop v.

We make a short recap of what we have proven so far. By now we have shown that

$$\begin{aligned}
\widetilde{M}_{\mathcal{M}}(x,y) &= \frac{1}{\mathfrak{m}(B)} E^*_{B^C}(x)\cdot E_B(y)\\
&= \frac{1}{\mathfrak{m}(B)}\Big(x\cdot E^*_{d,B^C}(x) + E^*_{c,B^C}(x) - E^*_{d,B^C}(x)\Big)E_B(y)\\
&= (x-1)\Big(\frac{1}{\mathfrak{m}(B)} E^*_{d,B^C}(x)E_B(y)\Big) + \frac{1}{\mathfrak{m}(B)} E^*_{c,B^C}(x)E_B(y). \qquad (3.1.2)
\end{aligned}$$

It remains to consider the external activity polynomial $E_B(y)$. Mind that v is a coloop, therefore the local external activities remain the same both in the deletion and the contraction of v. I.e $e(B,T) = e(B\setminus\{v\}, T\setminus\{v\})$. Also in the proof of Lemma 3.1.6 we already remarked that $\rho_c(T\setminus\{v\}) = \rho(T)$ for $T \supseteq B$ in the contraction. On the other hand in the deletion we compute:

$$\begin{aligned}
\rho_d(T\setminus\{v\}) &= \sum_{T\setminus\{v\}\subseteq A\subseteq X\setminus\{v\}} (-1)^{|T\setminus\{v\}|-|A|}\mathfrak{m}_d(A)\\
&= \sum_{T\setminus\{v\}\subseteq A\subseteq X\setminus\{v\}} (-1)^{|T\setminus\{v\}|-|A|}\mathfrak{m}(A)\\
(*) &= \sum_{T\setminus\{v\}\subseteq A\subseteq X\setminus\{v\}} (-1)^{|T\setminus\{v\}|-|A|}\mathfrak{m}_d(A\cup\{v\})\frac{\mathfrak{m}(B\setminus\{v\})}{\mathfrak{m}(B)}\\
&= \sum_{T\subseteq A'\subseteq X} (-1)^{|T|-|A'|}\mathfrak{m}_d(A')\frac{\mathfrak{m}(B\setminus\{v\})}{\mathfrak{m}(B)} = \rho(T)\frac{\mathfrak{m}(B\setminus\{v\})}{\mathfrak{m}(B)},
\end{aligned}$$

where at $(*)$ we use (AM3), which yields that $\mathfrak{m}(B\setminus\{v\})\mathfrak{m}(A\cup\{v\}) = \mathfrak{m}(A)\mathfrak{m}(B)$. By all this we conclude that

$$E_B(y) = E_{c,B}(y) = \frac{\mathfrak{m}(B)}{\mathfrak{m}(B\setminus\{v\})}E_{d,B}(y).$$

Hence, finally we can continue at equation (3.1.2) and conclude

$$\begin{aligned}
\widetilde{M}_{\mathcal{M}}(x,y) &= (x-1)\Big(\frac{1}{\mathfrak{m}(B)}E^*_{d,B^C}(x)E_B(y)\Big) + \frac{1}{\mathfrak{m}(B)}E^*_{c,B^C}(x)E_B(y)\\
&= (x-1)\Big(\frac{1}{\mathfrak{m}(B)}\frac{\mathfrak{m}(B)}{\mathfrak{m}(B\setminus\{v\})}E^*_{d,B^C}(x)E_{d,B}(y)\Big) + \frac{1}{\mathfrak{m}(B)}E^*_{c,B^C}(x)E_{c,B}(y)\\
&= (x-1)\Big(\frac{1}{\mathfrak{m}_d(B\setminus\{v\})}E^*_{d,B^C}(x)E_{d,B}(y)\Big) + \frac{1}{\mathfrak{m}_c(B\setminus\{v\})}E^*_{c,B^C}(x)E_{c,B}(y)\\
&= (x-1)\widetilde{M}_{\mathcal{M}\setminus v}(x,y) + \widetilde{M}_{\mathcal{M}/v}(x,y).
\end{aligned}$$

This completes the proof. □

Again by duality we also obtain the dual statement.

Lemma 3.1.8 ([MD12, Lem. 5.11])**.** *If $\mathcal{M} = (X, \mathrm{rk}, \mathfrak{m})$ is an arithmetic matroid and $v \in X$ is a loop, then the following equation holds:*

$$\widetilde{M}_{\mathcal{M}}(x,y) = \widetilde{M}_{\mathcal{M}\setminus v}(x,y) + (y-1)\widetilde{M}_{\mathcal{M}/v}(x,y).$$

However, with this and our observations before we can also consider Theorem 3.1.5 proven. Both expressions $M_{\mathcal{M}}(x,y)$ and $\widetilde{M}_M(x,y)$ fulfil the same recurrences, and they both coincide on the empty matroid. Hence they have to coincide in general.

We conclude this section with an example to visualise the proven assertions.

Example. We regard the following example taken from [MD12, Example 5.3]. Let $\mathcal{M}$ be the representable arithmetic matroid given by the list

$$X = \left\{ \underbrace{\begin{pmatrix}1\\2\\\bar{0}\end{pmatrix}}_{a:=}, \underbrace{\begin{pmatrix}2\\0\\\bar{1}\end{pmatrix}}_{b:=}, \underbrace{\begin{pmatrix}0\\0\\\bar{2}\end{pmatrix}}_{c:=}, \underbrace{\begin{pmatrix}0\\0\\\bar{3}\end{pmatrix}}_{d:=} \right\} \subseteq G := \mathbb{Z}^2 \oplus \mathbb{Z}/6\mathbb{Z}.$$

Simple calculations yield the following multiplicities:
$\mathfrak{m}(\emptyset) = 6$, $\mathfrak{m}(\{a\}) = 6$, $\mathfrak{m}(\{b\}) = 12$, $\mathfrak{m}(\{c\}) = 2$, $\mathfrak{m}(\{d\}) = 3$, $\mathfrak{m}(\{a,b\}) = 24$, $\mathfrak{m}(\{a,c\}) = 2$, $\mathfrak{m}(\{a,d\}) = 3$, $\mathfrak{m}(\{b,c\}) = 4$, $\mathfrak{m}(\{b,d\}) = 6$, $\mathfrak{m}(\{c,d\}) = 1$, $\mathfrak{m}(\{a,b,c\}) = 8$, $\mathfrak{m}(\{a,b,d\}) = 12$, $\mathfrak{m}(\{a,c,d\}) = 1$, $\mathfrak{m}(\{b,c,d\}) = 2$ and finally $\mathfrak{m}(X) = 4$. In this example $B := \{a,b\}$ is the only basis of this matroid, while $B^C = \{c,d\}$ is therefore the only basis in the dual. We compute the ρ-expressions:

$$\begin{aligned}
&\rho(X) = \mathfrak{m}(X) = 4,\\
&\rho(\{a,b,c\}) = \mathfrak{m}(\{a,b,c\}) - \mathfrak{m}(X) = 8 - 4 = 4,\\
&\rho(\{a,b,d\}) = \mathfrak{m}(\{a,b,d\}) - \mathfrak{m}(X) = 12 - 4 = 8,\\
&\rho(\{a,b\}) = \mathfrak{m}(\{a,b\}) - \mathfrak{m}(\{a,b,d\}) - \mathfrak{m}(\{a,b,c\}) + \mathfrak{m}(X) = 24 - 8 - 12 + 4 = 8,
\end{aligned}$$

and dually

$$\begin{aligned}
&\rho^*(X) = \mathfrak{m}^*(X) = \mathfrak{m}(\emptyset) = 6,\\
&\rho^*(\{a,c,d\}) = \mathfrak{m}^*(\{a,c,d\}) - \mathfrak{m}^*(X) = \mathfrak{m}(\{b\}) - \mathfrak{m}(\emptyset) = 12 - 6 = 6,\\
&\rho^*(\{b,c,d\}) = \mathfrak{m}^*(\{b,c,d\}) - \mathfrak{m}^*(X) = \mathfrak{m}(\{a\}) - \mathfrak{m}(\emptyset) = 6 - 6 = 0,\\
&\rho^*(\{c,d\}) = \mathfrak{m}^*(\{c,d\}) - \mathfrak{m}^*(\{a,c,d\}) - \mathfrak{m}^*(\{b,c,d\}) + \mathfrak{m}^*(X) = \cdots = 12.
\end{aligned}$$

The next thing to calculate are the local activities. This turns out to be rather easy in our case since we only have one unique basis and all elements outside are loops and therefore always externally active. We obtain for $e(B,T) = |T| - |B|$ for all lists $T \supseteq B$ containing the basis. Dually we have $e(B^C, \widetilde{T}) = |\widetilde{T}| - |B^C|$. By all of this we deduce that

$$\begin{aligned}
E_B(y) &= 4y^2 + 4y + 8y + 8 = 4y^2 + 12y + 8 \quad \text{and}\\
E^*_{B^C}(x) &= 6x^2 + 6x + 0x + 12 = 6x^2 + 6x + 12.
\end{aligned}$$

Hence we have indeed

$$\begin{aligned}\widetilde{M}_{\mathcal{M}}(x,y) &= \frac{1}{\mathfrak{m}(\{a,b\})} E_B(y) E_{B^C}(x) \\ &= \frac{1}{24}(4y^2+12y+8)(6x^2+6x+12) \\ &= 4+6y+2x+2x^2+3x^2y+3xy+2y^2+x^2y^2+xy^2 \\ &= 6(x-1)^2+(6+12)(x-1)+(2+3)(x-1)^2(y-1)+24+(2+3+4+6)(x-1)(y-1)+ \\ &+ 1(x-1)^2(y-1)^2+(8+12)(y-1)+(1+2)(x-1)(y-1)^2+4(y-1)^2 \\ &= M_{\mathcal{M}}(x,y).\end{aligned}$$

3.1.4 The generalisation of Crapo's theorem

The aim of this section is to generalise Theorem 1.2.14 to the case of arithmetic matroids. I.e. we would like to have an explicit formula for the arithmetic Tutte polynomial that gives us a direct interpretation of the coefficients. A first proof was given by D'Adderio and Moci in [MD12, Section 6]. However, we follow the later work of Brändén and Moci in [BM14]. In fact, they have shown an even more generalised identity for the *multivariate version of the the arithmetic Tutte polynomial*. We will adapt their proof to the bivariate situation.

The form of the Tutte polynomial in Crapo's theorem is given in terms of external activities. To be more precise, we have

$$T_{\mathcal{M}}(x,y) = \sum_{\substack{B\subseteq X,\\ B \text{ basis}}} x^{e^*(B^C)} y^{e(B)}.$$

For the generalised version in arithmetic matroid theory one may already guess that we might need to express the arithmetic Tutte polynomial in terms of *local activities*, like they were introduced in the last section (see Section 3.1.3).

Therefore the aim is to prove a formula for the arithmetic Tutte polynomial, which is similar to

$$M_{\mathcal{M}}(x,y) = \sum_{(B,T)\in\mathcal{B}} x^{e^*(B^C,\widetilde{T})} y^{e(B,T)},$$

where the sum is taken over a suitable list $\mathcal{B}$ of pairs (B,T), with B a basis and $T \supseteq B$.

To do so, firstly we need a lemma which lets us control the molecular case.

Lemma 3.1.9 ([BM14, Lem. 4.3])**.** *Let $[R,S] = [R, R\cup F\cup T]$ be a molecule in a matroid $\mathcal{M}_X$. Then for an arbitrary multiplicity function $\mathfrak{m}: \mathcal{P}(X) \to \mathbb{R}$ we have*

$$\begin{aligned}&\sum_{R\subseteq A\subseteq S} \mathfrak{m}(A)(x-1)^{\mathrm{rk}(S)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)} \\ &\quad = (y-1)^{|R|-\mathrm{rk}(R)} \sum_{\substack{K\subseteq F\\ L\subseteq T}} \rho(R\cup L, S\setminus K) x^{|K|} y^{|L|}.\end{aligned}$$

Additionally, if $(\mathcal{M}_X, \mathfrak{m})$ *is a quasi-arithmetic matroid, we observe that*

$$\sum_{R\subseteq A\subseteq S} \mathfrak{m}(A)(x-1)^{\mathrm{rk}(S)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)} =$$
$$= (y-1)^{|R|-\mathrm{rk}(R)}\left(\sum_{K\subseteq F}\frac{\rho(R,R\cup(F\setminus K))}{\mathfrak{m}(R)}x^{|K|}\right)\cdot\left(\sum_{L\subseteq T}\rho(R\cup L,R\cup T)y^{|L|}\right).$$

Remark. Recall that, by axiom (AM1), $\frac{\rho(R,R\cup(F\setminus K))}{\mathfrak{m}(R)}$ is an integer.

Proof of the lemma. For $R\subseteq A\subseteq S$ we set $A_1 := A\cap T$ and $A_2 := A\cap F$. Then we manipulate the following expression and may compute:

$$\begin{aligned}
&\sum_{A_1\subseteq T, A_2\subseteq F}\mathfrak{m}(R\cup A_1\cup A_2)(x-1)^{\mathrm{rk}(S)-\mathrm{rk}(R\cup A_1\cup A_2)}(y-1)^{|A_1\cup A_2|-\mathrm{rk}(A_1\cup A_2)} =\\
&= \sum_{A_1\subseteq T, A_2\subseteq F}\mathfrak{m}(R\cup A_1\cup A_2)(x-1)^{|F\setminus A_2|}(y-1)^{|A_1|}\\
&= \sum_{A_1\subseteq T, A_2\subseteq F}\mathfrak{m}(R\cup A_1\cup A_2)\sum_{K\subseteq F\setminus A_2, L\subseteq A_1}x^{|K|}y^{|L|}(-1)^{|A_1|+|A_2|+|F|+|K|+|L|}\\
&= \sum_{L\subseteq T, K\subseteq F}x^{|K|}y^{|L|}\sum_{\substack{L\subseteq A_1\subseteq T\\ K\subseteq A_2\subseteq F\setminus K}}(-1)^{|A_1|+|A_2|+|F|+|K|+|L|}\cdot\mathfrak{m}(R\cup A_1\cup A_2)\\
&= \sum_{L\subseteq T, K\subseteq F}x^{|K|}y^{|L|}\rho(R\cup L, S\setminus K).
\end{aligned}$$

We obtain the first formula from the assertion by multiplying this equation with the factor $(y-1)^{|R|-\mathrm{rk}(R)}$. Now the second formula in case of quasi-arithmetic matroids follows from the first one by using (AM3), which yields

$$\mathfrak{m}(R\cup L\cup A_1\cup A_2) = \frac{\mathfrak{m}(R\cup L\cup A_1)\mathfrak{m}(R\cup A_2)}{\mathfrak{m}(R)}.$$

Hence also

$$\rho(R\cup L, S\setminus K) = \frac{\rho(R\cup L, R\cup T)\rho(R, R\cup F\setminus K)}{\mathfrak{m}(R)},$$

by which we obtain the desired decomposition. □

Now that we have analysed the molecular case, the strategy is again to reduce arbitrary matroids to molecules. The next proposition provides the necessary technical details to achieve this. However, at first we need again a piece of new notation.

Notation. Let $\mathcal{M}_X$ be a matroid over a list X and let B be a basis. We denote by $E(B)$ the list of externally active elements on B in X. Similarly let $I(B) = E^*(B)$ denote the list of elements in X internally active on B. Then just as before we have

- $e(B) = |E(B)|$ and

- $e^*(B) = |I(B)|$.

With this we are able to state the crucial proposition. Note that this is a statement valid for arbitrary (not necessarily arithmetic) matroids.

Proposition 3.1.10 ([BM14, Prop. 4.4])**.** *Let $\mathcal{M}_X$ be a matroid over a list X and denote by $\mathcal{B}$ the list of its bases. Then we have:*

(i). $\mathcal{P}(X)$ can be decomposed into a disjoint union

$$\mathcal{P}(X) = \bigcup_{B\in\mathcal{B}} [B \setminus I(B), B \cup E(B)],$$

(ii). for each $B \in \mathcal{B}$, $[B \setminus I(B), B \cup E(B)]$ is a molecule with free part $F = I(B)$ and torsion part $T = E(B)$.

Proof. For the first assertion see [Bj2, Prop. 7.3.6] for reference.

(i). We need to show, that for all $A \subseteq X$ there is a unique basis $B_A \in \mathcal{B}$ such that $A \in [B_A \setminus I(B_A), B_A \cup E(B_A)]$.

Therefore let $A \subseteq X$ be arbitrary. Now in the restriction matroid $\mathcal{M}_{X|A}$ induced by A, we denote by $\mathfrak{b}_A$ the largest basis with respect to lexicographic order. (Recall that X is totally ordered and inherits its order to A.) As a list $\mathfrak{b}_A$ is independent in X. By the result [Bj2, Prop. 7.2.2 and (7.9)] there exists a unique basis B_A such that $B_A \setminus I(B_A) \subseteq \mathfrak{b}_A \subseteq B_A$.

Now let $a \in A \setminus B_A = A \setminus \mathfrak{b}_A$, and assume that a is **not** externally active on B_A. But then there exists an element $b \in B_A$ with $b < a$ and $(B_A \setminus\{b\}) \cup \{a\}$ is again a basis. In a next step, we observe that if $b \notin A$ then this would imply that $\mathfrak{b}_A \cup \{a\} \subseteq A$ was independent. However, this is impossible since $\mathfrak{b}_A$ is a basis of $\mathcal{M}_{X|A}$ and $a \notin \mathfrak{b}_A$.

Nevertheless, if we assume $b \in A$ then this yields again a contradiction, because then $b \in B_A \cap A = \mathfrak{b}_A$ with $b < a$. However, then $\mathfrak{b}_A < ((\mathfrak{b}_A \setminus\{b\}) \cup \{a\})$ in the lexicographic order. This cannot be since $\mathfrak{b}_A$ was constructed maximal. Therefore all elements of $A \setminus B_A$ have to be externally active. Hence, by now we have shown $B_A \setminus I(B_A) \subseteq \mathfrak{b}_A \subseteq A \subseteq B_A \cup E(B_A)$.

To prove *uniqueness*, we assume another basis B with $B \setminus I(B) \subseteq A \subseteq B \cup E(B)$.

Claim. $E(B)$ is contained in $cl(B \setminus I(B))$, where

$$cl(D) := \{x \in X \mid \mathrm{rk}(D \cup \{x\}) = \mathrm{rk}(D)\},$$

is the *closure* of a subset $D \subseteq X$.

To prove the claim let $p \in E(B)$. We denote by C the unique *circuit* established in $B \cup \{p\}$. Moreover we denote by C' the according *broken circuit* $C \setminus\{p\}$. Since p is externally active, we have for all $q \in C'$ that $p < q$ and $(B \setminus q) \cup p$ is a basis. Thus

q is **not** internally active. (Compare with the characterisation given in the remarks below Theorem 1.2.14.) Now since p lies in the closure of C' and $C' \subseteq B \setminus I(B)$ the claim follows.

However, from this we may deduce that $\mathfrak{b} := B \cap A$ is a basis of $\mathcal{M}_{X|A}$. Now we suppose that $\mathfrak{b} \neq \mathfrak{b}_A$. We may write explicitly $\mathfrak{b} = \{x_1, x_2, \ldots, x_a\}$ and $\mathfrak{b}_A = \{y_1, y_2, \ldots, y_a\}$. Since $\mathfrak{b}_A$ was chosen to be maximal with respect to the lexicographic order there is an index k such that $x_i = y_i$ for $i = 1, 2, \ldots, k-1$ and $x_k < y_i$ for $i \geq k$. Now by the matroid basis axiom (B2) the set $(\mathfrak{b} \setminus \{x_k\}) \cup \{y_j\}$, for some $j \geq k$, is again a basis. But then y_j cannot be externally active on $\mathfrak{b}$ and therefore not in B. But this contradicts the assumption $A \subseteq B \cup E(B)$. Thus $\mathfrak{b} = \mathfrak{b}_A$ and by $B \setminus I(B) \subseteq \mathfrak{b} \subseteq B$ we obtain $B = B_A$.

(ii). We set $R = B \setminus I(B)$ and $S = R \sqcup I(B) \sqcup E(B)$. We need to argue that for $A \in [R, S]$ we have

$$\mathrm{rk}(A) = \mathrm{rk}(R) + |A \cap I(B)|.$$

Write $A = R \cup (A \cap I(B)) \cup (A \cap E(B))$. Remember that the claim above said $E(B) \subseteq cl(B \setminus I(B))$ and hence $E(B) \subseteq cl(R)$. That means that

$$\begin{aligned} \mathrm{rk}(A) &= \mathrm{rk}(R \cup (A \cap I(B)) \cup (A \cap E(B))) = \\ &= \mathrm{rk}(R \cup (A \cap I(B))). \end{aligned}$$

Now we remind ourselves that $R \subseteq B$ and $A \cap I(B) \subseteq B$ a basis. Therefore we continue:

$$\ldots = |R \cup (A \cap I(B))| = |R| + |A \cap I(B)| = \mathrm{rk}(R) + |A \cap I(B)|.$$

This completes the proof. □

We now follow the further instructions of [BM14, Section 4] to generalise Crapo's theorem. Hence let $\mathcal{M}_X$ be a *pseudo-arithmetic matroid* over a list X with multiplicity function $\mathfrak{m} : \mathcal{P}(X) \to \mathbb{Z}$. We define $\widetilde{\mathcal{B}}$ to be the list of pairs (B, T) with B a basis and $T \subseteq E(B) \cup I(B)$. Moreover every pair (B, T) shall occur in $\widetilde{\mathcal{B}}$ exactly $\rho((B \cup T) \setminus I(B), (B \setminus T) \cup E(B))$ times. Then eventually we have the following result (see [MD12, Thm. 6.1] or [BM14, Thm. 4.6]).

Theorem 3.1.11 (Generalisation of Crapo's theorem)**.** *Let $\mathcal{M}$ be a pseudo-arithmetic matroid over a list X. Then its multiplicity Tutte polynomial is obtained by*

$$M_{\mathcal{M}_X}(x, y) = \sum_{(B,T) \in \widetilde{B}} x^{i(B,T)} y^{e(B,T)},$$

where $i(B, T) = |T \cap I(B)|$ and $e(B, T) = |T \cap E(B)|$ refer to local activities.

Proof. The statement follows immediately from Proposition 3.1.10, which let us decompose the underlying matroid into molecules, and Lemma 3.1.9 which handles the

molecular case. In particular, notice that we decompose our matroid in molecules $[R, S]$, where R is of the form $R = B \setminus I(B)$ for a basis B. Therefore we have $|R| - \mathrm{rk}(R) = 0$ and the factor $(y-1)^{|R|-\mathrm{rk}(R)}$ in Lemma 3.1.9 vanishes. □

Proposition 3.1.10 and Lemma 3.1.9 are particularly useful tools. From them one can deduce the following theorem, which is a result from general multiplicity matroid theory.

Theorem 3.1.12 ([BM14, Thm. 4.5])**.** *Pseudo-arithmetic matroids form the most general class of multiplicity matroids closed under deletion and contraction such that the associated multiplicity Tutte polynomials have positive coefficients.*

Remark. This justifies the name *positivity axiom* for axiom (P), which is equivalent to (AM4) and (AM5).

Proof. Let $\mathcal{M}_X$ be a pseudo-arithmetic matroid. The generalised theorem of Crapo yields the positivity of all coefficients and since deletion and contraction of pseudo-arithmetic matroids stay pseudo-arithmetic this class fulfils the demanded qualities.

Now let $\mathcal{C}$ be another class of multiplicity matroids, whose multiplicity Tutte polynomials have positive coefficients and assume $\mathcal{C}$ is closed under deletion and contraction. Let $\mathcal{M} \in \mathcal{C}$ be a multiplicity matroid over a list X. If $[R, S]$ is an arbitrary molecule in $\mathcal{M}$, we may contract all elements in R and delete all elements in $X \setminus S$. The resulting matroid still has to be in $\mathcal{C}$. However, by the first equation of Lemma 3.1.9 the associated multiplicity Tutte polynomial has constant coefficient $\rho(R, S)$. By the positivity property of matroids in $\mathcal{C}$ we have $\rho(R, S) \geq 0$. Hence $\mathcal{M} \in \mathcal{C}$ already has to be pseudo-arithmetic. □

Proposition 3.1.10 and Lemma 3.1.9 also enable us to give an exorbitantly simpler proof of Theorem 3.1.5 from the last section. For interested readers I refer to it in [BM14, Thm. 4.8]. However, we move on to show the generalised convolution identity for the arithmetic Tutte polynomials.

3.1.5 A convolution formula

In this section we aim to generalise the convolution formula of the Tutte polynomial of ordinary matroids $\mathcal{M}$ over a list X to the case of multiplicity matroids. This convolution formula (Theorem 1.2.13) has been stated in the introductory part. It says that

$$T_{\mathcal{M}}(x, y) = \sum_{A \subseteq X} T_{\mathcal{M}|_A}(0, y) T_{\mathcal{M}/A}(x, 0),$$

where $\mathcal{M}|_A$ and $\mathcal{M}/A$ denote the restriction and contraction matroids by a sublist $A \subseteq X$, respectively.

Spencer Backman and Matthias Lenz (see [BL20]) proved the following generalisation.

Theorem 3.1.13. *Let $(\mathcal{M}, \mathfrak{m})$ be a multiplicity matroid over a list X. As before, we denote by $M_{\mathcal{M}}(x, y)$ its multiplicity Tutte polynomial and by $T_{\mathcal{M}}(x, y)$ its ordinary Tutte*

polynomial. Then the following equations hold:

$$\begin{aligned} M_{\mathcal{M}}(x,y) &= \sum_{A\subseteq X} M_{\mathcal{M}|_A}(0,y)\cdot T_{M/A}(x,0) \\ &= \sum_{A\subseteq X} T_{\mathcal{M}|_A}(0,y)\cdot M_{M/A}(x,0). \end{aligned}$$

Remark. A direct corollary of Theorem 3.1.13 would be again, that the coefficients of a pseudo-arithmetic matroid are indeed positive.

However, Theorem 3.1.13 can again be generalised. We already know, if $\mathcal{M}$ is a matroid over a list X and $\mathfrak{m}_1, \mathfrak{m}_2 : \mathcal{P}(X) \to \mathbb{Z}$ are two multiplicity functions, then $(\mathcal{M}, \mathfrak{m}_1), (\mathcal{M}, \mathfrak{m}_2)$ and also $(\mathcal{M}, \mathfrak{m}_1 \cdot \mathfrak{m}_2)$ arise to three multiplicity matroids over X. Especially if both $(\mathcal{M}, \mathfrak{m}_1)$ and $(\mathcal{M}, \mathfrak{m}_2)$ are arithmetic matroids, then also $(\mathcal{M}, \mathfrak{m}_1 \cdot \mathfrak{m}_2)$ is arithmetic (compare with Theorem 2.1.4). With this in mind we get the following convolution formula for the multiplicity Tutte polynomial (see [BL20, Thm. 4]).

Theorem 3.1.14 (Convolution theorem)**.** *Let $(\mathcal{M}, \mathfrak{m}_1)$ and $(\mathcal{M}, \mathfrak{m}_2)$ be defined as above, then we have in terms of multiplicity Tutte polynomials:*

$$M_{(\mathcal{M},\mathfrak{m}_1\mathfrak{m}_2)}(x,y) = \sum_{A\subseteq X} M_{(\mathcal{M},\mathfrak{m}_1)|_A}(0,y) M_{(\mathcal{M},\mathfrak{m}_2)/A}(x,0).$$

Remark. If we choose $\mathfrak{m}_2 \equiv 1$, then we obtain again Theorem 3.1.13.

A compact proof for Theorem 3.1.14 is provided by Ye Liu, Tan Nhat Tran and Masahiko Yoshinaga ([LTY21]). There the researchers proved a similar identity for so-called *G-Tutte polynomials* which form a generalisation of standard multiplicity Tutte polynomials. We adapt their proof in [LTY21, Thm. 8.6] to our case.

Proof of Theorem 3.1.14. Recall that $\mathfrak{m}_{|_A}(T) = \mathfrak{m}(T)$ and $\mathfrak{m}_{/A}(S) = \mathfrak{m}(S \cup A)$ in case of restriction to A and contraction of A, respectively. Then the right-hand side of the formula is equal to

$$\begin{aligned} &\sum_{A\subseteq X} \Big(\sum_{T\subseteq A} \mathfrak{m}_1(T)(-1)^{\mathrm{rk}(A)-\mathrm{rk}(T)}(y-1)^{|T|-\mathrm{rk}(T)} \Big) \\ &\cdot \Big(\sum_{A\subseteq S\subseteq X} \mathfrak{m}_2(S)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)-(\mathrm{rk}(S)-\mathrm{rk}(A))}(-1)^{|S|-|A|-(\mathrm{rk}(S)-\mathrm{rk}(A))} \Big) \\ &= \sum_{T\subseteq A\subseteq S\subseteq X} \mathfrak{m}_1(T)\mathfrak{m}_2(S)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(S)}(y-1)^{|T|-\mathrm{rk}(T)}(-1)^{|S|-|A|-\mathrm{rk}(S)-\mathrm{rk}(T)} \\ &= \sum_{T=A=S\subseteq X} \mathfrak{m}_1(T)\mathfrak{m}_2(S)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(S)}(y-1)^{|T|-\mathrm{rk}(T)} \\ &+ \sum_{T\subsetneq S\subseteq X} \Big(\mathfrak{m}_1(T)\mathfrak{m}_2(S)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(S)}(y-1)^{|T|-\mathrm{rk}(T)} \sum_{T\subseteq A\subseteq S} (-1)^{|S|-|A|-\mathrm{rk}(S)-\mathrm{rk}(T)} \Big). \end{aligned}$$

Eventually we observe that the first big sum is equal to $M_{(\mathcal{M},\mathfrak{m}_1\mathfrak{m}_2)}(x,y)$, while the second

sum vanishes because, when $T \subsetneq S$ then we have

$$\sum_{T \subseteq A \subseteq S} (-1)^{|A|} = 0.$$

This concludes the proof. □

With this we have completely adapted the formulas stated in the introduction. Our final task for this part is to work with the arithmetic Tutte polynomial in concrete settings. This emphasises the relevance and elegance of arithmetic matroid theory in applications.

3.2 Specialisations, interpretations and generalisations of the arithmetic Tutte polynomial

In the last section of this part I would like to list some known identities which the arithmetic Tutte polynomial fulfils in explicit situations. Just like the ordinary Tutte polynomial also its arithmetic version admits certain characteristic functions when providing special values for either one or both variables.

The focus will lie on representable arithmetic matroids, since this class is the one most thoroughly studied. This means we will again enter the realms of lattice geometry, where the arithmetic Tutte polynomial yields a lot of information about lattice points inside of the zonotope spanned by a list of vectors. We will indeed see, that the arithmetic Tutte polynomial specialises to the Ehrhart polynomial, which counts intersections with the underlying lattice (see [DM12]).

After that, we concern ourselves again with the situation of labelled graphs. There one defines so-called *arithmetic colourings* and *arithmetic flows* on these graphs (see [BM14, Sections 8, 9] or [BL20, p. 4]). One then observes that the arithmetic Tutte polynomial fulfils simple relations with the characteristic polynomials counting these flows and colourings.

3.2.1 Arithmetic matroids over lattice points

We briefly recall the setup. Let $\Lambda \subset \mathbb{R}^n$ be a lattice with $\dim(\Lambda) = n$. Then a finite list $X \subset \Lambda$ of lattice points defines a matroid $\mathcal{M}_X$ via the usual relations of linear independence in $\mathbb{R}^n$. In particular we have for all $A \subseteq X$ that

$$\mathrm{rk}(A) = \dim(\langle A \rangle_{\mathbb{R}}),$$

where $\langle A \rangle_{\mathbb{R}}$ denotes the classical *span of* A in the vector space $\mathbb{R}^n$.

Moreover $\mathcal{M}_X$ arises to an arithmetic matroid due to the multiplicity function $\mathfrak{m} : \mathcal{P}(X) \to \mathbb{Z}$ associating to every subset $A \subseteq X$ the value

$$\mathfrak{m}(A) = [\Lambda_A : \langle A \rangle_{\mathbb{Z}}].$$

Here $\langle A\rangle_{\mathbb{Z}}$ denotes the subgroup of Λ generated by $A \subseteq X$, while $\Lambda_A \leq \Lambda$ is defined as the largest subgroup of the lattice such that $\langle A\rangle_{\mathbb{Z}}$ has finite index and finally $[G : H]$ just denotes the index of a subgroup H in a group G. We have proven in Section 2.1.2 that the triple $(X, \mathrm{rk}, \mathfrak{m})$ fulfils all axioms defining an arithmetic matroid. Again we will simply denote it by $\mathcal{M}$. Since Λ is a lattice, the arithmetic matroid is torsion-free and clearly representable. Therefore it is also GCD as we remarked in Section 2.2.2. This means that we have

$$\mathfrak{m}(A) = \gcd(\{\mathfrak{m}(B) \mid B \subseteq A \text{ and } |B| = \mathrm{rk}(B) = \mathrm{rk}(A)\})$$

for all sublists $A \subseteq X$.

Now we would like to place our focus on the arithmetic Tutte polynomial $M_{\mathcal{M}}(x, y)$. In Section 2.1.2 we already have mentioned some identities fulfilled by it in this setup. I remind that the *zonotope* $\mathcal{Z}(X)$ induced by the list X is the convex polytope defined as follows:

$$\mathcal{Z}(X) := \Big\{ \sum_{x\in X} \alpha_x x \ : \ 0 \leq \alpha_x \leq 1 \Big\}.$$

Then we proved that $M_{\mathcal{M}}(1, 1)$ is equal to the volume of $\mathcal{Z}(X)$ (see Proposition 2.1.11). We also mentioned that $M_X(2, 1) = |\mathcal{Z}(X) \cap \Lambda|$, thus $M_{\mathcal{M}}(x, y)$ encodes the number of lattice points inside of the associated zonotope $\mathcal{Z}(X)$ (see Theorem 2.1.12).

We now want to emphasise this relation by showing that the arithmetic Tutte polynomial specialises to the Ehrhart polynomial. To do so, firstly we gather some general theory about Ehrhart polynomials. For the following see e.g. [DM12].

Definition ([DM12, Section 2.1])**.** Let P be a convex n-dimensional polytope in $\mathbb{R}^n$ such that all its vertices lie in a lattice Λ. This means, there exist lattice points $v_1, v_2, \ldots, v_k \in \Lambda$, with $k \in \mathbb{N}$, such that

$$P = \mathrm{conv}(v_1, v_2, \ldots, v_k) := \Big\{ \sum_{i=1}^{k} t_i v_i \ : \ t_i \geq 0, \sum_{i=1}^{k} t_i = 1 \Big\},$$

and $Vol_n(P) > 0$. The *dilation* of P by the factor $k \in \mathbb{N}$ is defined as

$$kP = \mathrm{conv}(kv_1, kv_2, \ldots, kv_n),$$

the convex hull of the vertices multiplied by k. For such a polytope P we define the *Ehrhart polynomial* $\mathcal{E} : \mathbb{N} \to \mathbb{N}$ by

$$\mathcal{E}(k) = |kP \cap \Lambda|,$$

i.e. $\mathcal{E}(k)$ equals the number of lattice points in kP. Analogously, if we denote by P° the interior of P, then we define $\mathcal{I} : \mathbb{N} \to \mathbb{N}$ by

$$\mathcal{I}(k) = |(kP)^\circ \cap \Lambda|,$$

counting the interior lattice points of kP.

Remark. Clearly if P has vertices in Λ then also kP is a polytope with vertices in Λ. Moreover if $X \subseteq \Lambda$ is a finite list of lattice points, then the induced zonotope $\mathcal{Z}(X)$ is indeed such a convex polytope with vertices in Λ.

Example. The following Figure 3.1 visualises the concepts described in the last definition. Here we have the zonotope $\mathcal{Z}(X)$ from a previous example marked in red together with its dilation $2\mathcal{Z}(X)$ in pink. Also we see the $\mathbb{Z}^2$-lattice points contained in $\mathcal{Z}(X)$.

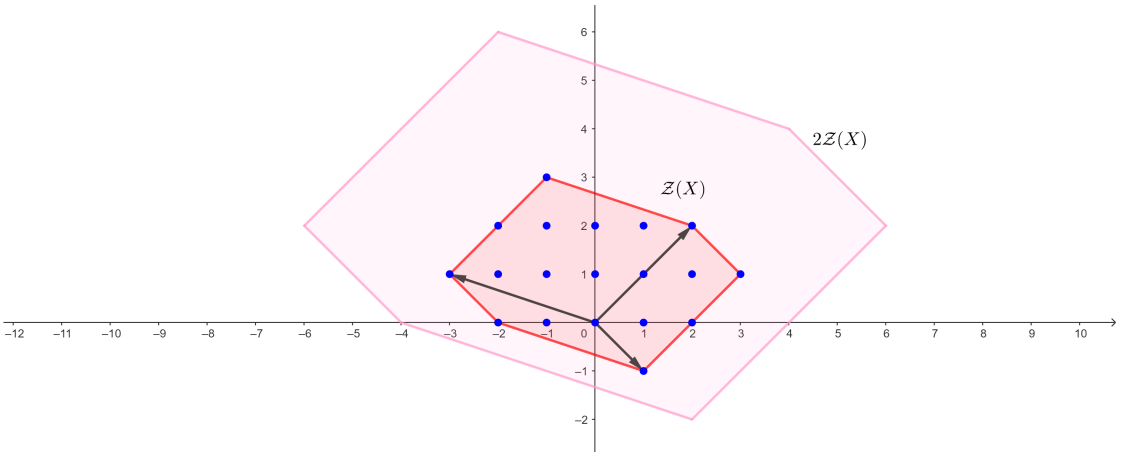

Figure 3.1: Integer points and the dilation of a zonotope.

Although the name already suggests this, Ehrhart has shown that $\mathcal{E}(k)$ is indeed a polynomial in k of degree n (see [Ehr62] or compare with [BHHL11] or [DM12, Section 2.1]). Additionally, also $\mathcal{I}(k)$ is a polynomial and one observes that

$$\mathcal{I}(k) = (-1)^n \mathcal{E}(-k).$$

This formula is called *Ehrhart-Macdonald reciprocity* (see [BR15, Theorem 4.1]). In case of zonotopes $\mathcal{Z}(X)$ generated by a finite list of lattice points $X \subseteq \Lambda$ we would like to connect those two functions with our arithmetic Tutte polynomial. Our goal is to show the following theorem.

Theorem 3.2.1 ([DM12, Thm. 3.2])**.** *Let X be a finite list of elements of an n-dimensional lattice, such that the induced zonotope $\mathcal{Z}(X)$ is also n-dimensional. Moreover let $\mathcal{E}(k)$ be the Ehrhart polynomial of $\mathcal{Z}(X)$ and let $\mathcal{M}_X$ be the arithmetic matroid given by X. Then we have*

$$\mathcal{E}(k) = k^n M_X(1 + 1/k, 1)$$

where $M_X(x, y)$ denotes the arithmetic Tutte polynomial of $\mathcal{M}_X$ in abuse of notation.

To prove this we need a lemma and the notion of the *dilation of a list.*

Definition ([DM12, Section 3])**.** For a finite list of lattice points $X = \{x_1, x_2 \ldots, x_m\}$ we define its *dilation by* $k \in \mathbb{N}$ as the list

$$kX := \{kx_1, kx_2, \ldots, kx_m\}.$$

Remark. Note that clearly $\mathcal{Z}(kX) = k\mathcal{Z}(X)$.

Then the following lemma compares the arithmetic Tutte polynomial of the arithmetic matroid $\mathcal{M}_X$ with the one of the related arithmetic matroid $\mathcal{M}_{kX}$ induced by the dilation of X by $k \in \mathbb{N}$.

Lemma 3.2.2 ([DM12, Lem. 3.1])**.** *Let $\mathcal{M}_X$ be an arithmetic matroid generated by a list of lattice points $X \subseteq \Lambda$ and let $\mathcal{M}_{kX}$ be the according arithmetic matroid over the dilated list kX, $k \in \mathbb{N}$. Then for the arithmetic Tutte polynomials we have*

$$M_{kX}(x, y) = k^n M_X\Big(\frac{x-1}{k} + 1, y\Big).$$

Proof. By definition of the arithmetic Tutte polynomial we write

$$M_{kX}(x, y) = \sum_{A \subseteq X} \mathfrak{m}(kA)(x-1)^{n-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)}.$$

Additionally again by simply using the definition of $\mathfrak{m}$ in a lattice matroid we have $\mathfrak{m}(kA) = k^{\mathrm{rk}(A)}\mathfrak{m}(A)$ (this gets apparent for example when recalling the GCD-rule). However, inserting this into the formula we compute

$$k^n \sum_{A \subseteq X} \mathfrak{m}(A)\Big(\frac{x-1}{k}\Big)^{n-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)} = k^n M_X\Big(\frac{x-1}{k} + 1, y\Big).$$

□

Another observation, that we will not prove here, concerns the coefficients of the Ehrhart polynomial. Namely, if $\mathcal{Z}(X)$ is a zonotope with Ehrhart polynomial $\mathcal{E}(k)$, we write

$$\mathcal{E}(k) = \sum_{i=0}^{n} a_i \cdot k^i,$$

with $a_i \in \mathbb{R}$ its coefficients. Then by [Sta97, Exer. 31, p. 272] or also [BHHL11, Section 2] we have

$$a_i = \sum_{\substack{A \subseteq X \\ \mathrm{rk}(A) = |A| = i}} \gcd(i\text{-minors of } A).$$

In particular, the sum is taken over all independent sublists $A \subseteq X$ with $|A| = i$. Then we remind the reader, that our matroid is GCD. Hence the sum translates into multiplicities:

$$a_i = \sum_{\substack{A \subseteq X \\ A \text{ indep.}}} \mathfrak{m}(A). \tag{3.2.1}$$

Now Michele D'Adderio and Luca Moci give two different proofs for Theorem 3.2.1. One uses Theorem 2.1.12 which states that $M_X(2,1) = |\mathcal{Z}(X) \cap \Lambda|$ and combines it with Lemma 3.2.2. The other one relies heavily on the representation of the coefficients in equation (3.2.1). We repeat both beautiful proofs from [DM12, Thm. 3.2].

Proof 1. By Theorem 2.1.12 we have

$$\mathcal{E}(k) = M_{kX}(2,1) = k^n M_X(1+1/k, 1),$$

where the second equality follows immediately from Lemma 3.2.2. □

Proof 2. By definition we have

$$M_X(t+1,1) = \sum_{\substack{A \subseteq X \\ A \text{ indep.}}} \mathfrak{m}(A) t^{n-\mathrm{rk}(A)} = \sum_{\substack{A \subseteq X \\ A \text{ indep.}}} \mathfrak{m}(A) t^{n-|A|}.$$

Here we used that for independent $A \subseteq X$ the equation $\mathrm{rk}(A) = |A|$ holds. However, using equation (3.2.1) we conclude for the Ehrhart polynomial that

$$\mathcal{E}(k) = \sum_{\substack{A \subseteq X \\ A \text{ indep.}}} \mathfrak{m}(A) k^{|A|}.$$

Eventually we compute

$$\begin{aligned} k^n M_X(1/k+1,1) &= k^n \sum_{\substack{A \subseteq X \\ A \text{ indep.}}} \mathfrak{m}(A) \Big(\frac{1}{k}\Big)^{n-|A|} \\ &= \sum_{\substack{A \subseteq X \\ A \text{ indep.}}} \mathfrak{m}(A) k^{|A|} = \mathcal{E}(k). \end{aligned}$$

□

By using the Ehrhart-Macdonald reciprocity we can also relate the function $\mathcal{I}(k)$ of inner lattice points with the arithmetic Tutte polynomial.

Corollary 3.2.3 ([DM12, Cor. 3.3])**.** *Let $\mathcal{Z}(X)$ be a n-dimensional zonotope generated by a finite list X of points in a lattice Λ. We denote by $M_X(x,y)$ the resulting arithmetic Tutte polynomial of the representable arithmetic matroid given by X. Then for the polynomial $\mathcal{I}(k)$ counting the lattice points in $(k\mathcal{Z}(X))^\circ$ we have*

$$\mathcal{I}(k) = k^n M_X(1-1/k, 1).$$

One may notice that the second proof of the theorem above did not use the statement of Theorem 2.1.12 saying that $M_X(2,1) = |\mathcal{Z}(X) \cap \Lambda|$. Therefore we get this statement again as a corollary.

Example. The almost simplest thinkable example is the one of a rectangle in the plane. E.g. let $X = \{(3,0),(0,4)\}$. Then we compute the corresponding arithmetic Tutte polynomial:

$$\begin{aligned} M_X(x,y) &= \sum_{A\subseteq X} \mathfrak{m}(A)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)} \\ &= \mathfrak{m}(\emptyset)(x-1)^2 + (\mathfrak{m}(\{(3,0)\}) + \mathfrak{m}(\{(0,4)\}))(x-1) + \mathfrak{m}(X) \\ &= (x-1)^2 + 7(x-1) + 12 \\ &= x^2 - 2x + 1 + 7x - 7 + 12 \\ &= x^2 + 5x + 6. \end{aligned}$$

Then we first observe, that $M_X(2,1) = 20$ really does coincide with the number of lattice

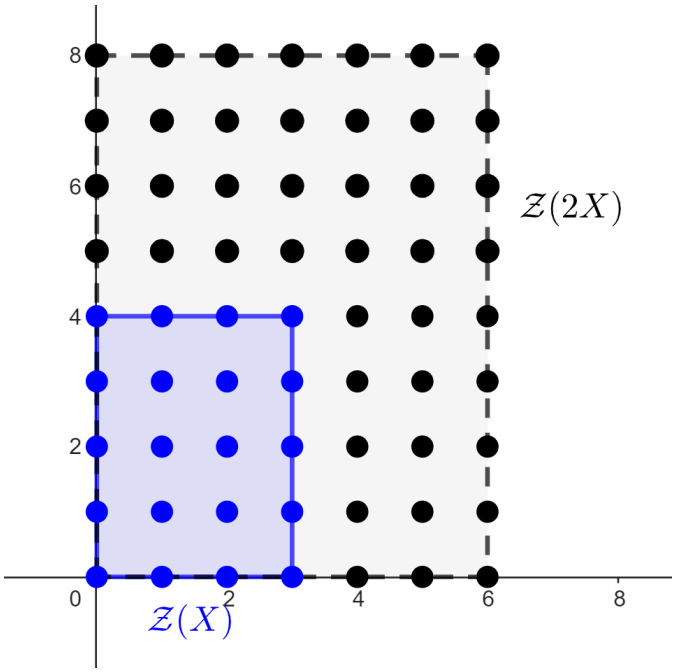

Figure 3.2: Integer points of a simple zonotope and its dilation by 2.

points in the associated zonotope $\mathcal{Z}(X)$ (check with Figure 3.2). Now if we dilate our list by a non-negative integer $k \in \mathbb{Z}$ then clearly the number of lattice points in $\mathcal{Z}(kX)$ is given by

$$\mathcal{E}(k) = (k \cdot 3 + 1)(k \cdot 4 + 1).$$

On the other hand, we compute

$$\begin{aligned}\mathcal{E}(k) &= (k \cdot 3 + 1)(k \cdot 4 + 1) \\ &= 12k^2 + 7k + 1 \\ &= k^2\Big(\frac{1}{k^2} + \frac{7}{k} + 12\Big) \\ &= k^2\Big(\Big(1 + \frac{1}{k}\Big)^2 + 5\Big(1 + \frac{1}{k}\Big) + 6\Big) \\ &= k^2 M_X\Big(1 + \frac{1}{k}, 1\Big).\end{aligned}$$

Especially for $k = 2$ we obtain $\mathcal{E}(2) = 63$ (compare with Figure 3.2).

3.2.2 Arithmetic colourings and flows

Since the very beginning of graph theory mathematicians wanted to colour the vertices of a graph in such a way that neighbouring vertices are assigned different colours. Such a colouring is called proper. The *Four-colour problem* is concerned with the problem to dye the vertices of every planar graph in such a proper way while only using four different colours in total. This problem, which is a theorem by now, kept mathematicians busy over generations. In the end it took very efficient computer systems to eventually prove that four colours are indeed enough. However, the theoretical offspring of all the failed attempts to attack this problem can be considered quite fruitful. Some may say that matroid theory itself was mainly developed to understand graph colourings. In particular remember that even Tutte called his famous polynomial the *dichromatic polynomial* (Greek: *chroma* = colour, see [Tut54]). With this in mind it seems natural to assume that it might be possible to relate the arithmetic Tutte polynomial with some kind of *colouring* on graphs as well. After all arithmetic matroids are a true generalisation of ordinary matroids.

In fact this was done again by Michele D'Adderio and Luca Moci in [DM13]. In this section we summarise their pioneering achievements on this topic.

Firstly I want you to consider the following. Arithmetic matroids are matroids equipped with some *extra structure*. Ordinary matroids appear as special cases where this extra structure (in our case the multiplicity function $\mathfrak{m}$) takes certain values (here: $\mathfrak{m} = 1$ constant). If we translate this principle to graphs it becomes reasonable why arithmetic matroids are defined on *labelled graphs*. The labels provide this *extra structure*, which is in the end determining the multiplicities of the induced arithmetic matroids. If all edges are labelled trivially with 1, then also the resulting arithmetic matroid will be an ordinary matroid, at least from the combinatorial point of view.

I refer to Section 2.1.2 where we introduced the construction of arithmetic matroids over labelled graphs with regular and dotted edges. These will be the central objects of this section. And on these labelled graphs we want to study so-called *arithmetic colourings*.

Definition ([DM13, Section 3.1])**.** Let (G, l) be a labelled graph as described in Section 2.1.2, $G = (V, R \sqcup D)$, and choose a positive integer $q \in \mathbb{N}$. Then an *arithmetic (proper) q-colouring* is a map $\mathfrak{c} : V \to \mathbb{Z}/q\mathbb{Z}$ such that the following two conditions are fulfilled:

(i). If $u, v \in V$ and $e = \{u, v\} \in R$ then $l(e) \cdot \mathfrak{c}(u) \neq l(e) \cdot \mathfrak{c}(v)$.

(ii). If $u, v \in V$ and $e = \{u, v\} \in D$ then $l(e) \cdot \mathfrak{c}(u) = l(e) \cdot \mathfrak{c}(v)$.

Example. If we take our labelled graph from our previous examples (with a minor change of the labels) and set $q = 4$ then we get a proper arithmetic q-colouring in the following way: see Figure 3.3.

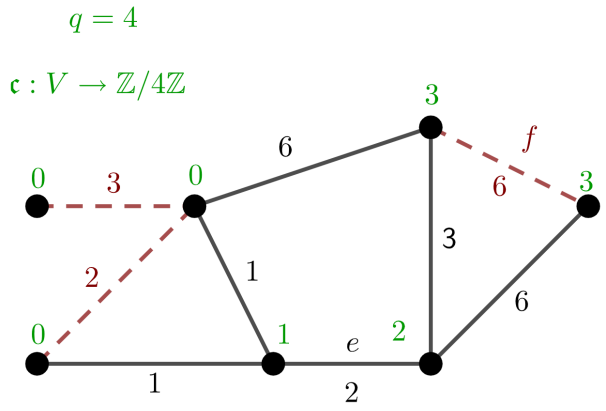

Figure 3.3: A proper arithmetic 4-colouring marked in green.

Remark ([DM13, Rem. 3.1]). The idea of the disjoint decomposition $E = R \sqcup D$ of the set of edges into regular and dotted edges is that vertices connected via a dotted edge are kind of identified with each other. This becomes apparent when recalling the contraction operation with this kind of labelled graphs. When contracting a regular edge $e \in R$ then it switches sets and becomes dotted. This now relates to the classical contraction operation in graphs where two neighboring vertices collide into a new one. The same principle applies again in condition (ii) for arithmetic colourings. Two vertices connected via a dotted edge are vaguely identified with each other and should have similar colours. (I say similar and not identical because $l(e) \cdot \mathfrak{c}(u) = l(e) \cdot \mathfrak{c}(v)$ does not imply $\mathfrak{c}(u) = \mathfrak{c}(v)$ since $\mathfrak{c}(u), \mathfrak{c}(v) \in \mathbb{Z}/q\mathbb{Z}$.)

However, observe that if $l(e) = 1$ for all edges e and $D = \emptyset$, then we obtain the classical notion of colouring the underlying graph properly with q different colours.

In the case $l(e) = 1$ constantly for all $e \in E$ but $D \neq \emptyset$ we still would get a classical q-colouring on the graph G' obtained from G via classically contracting all dotted edges $e \in D$.

More generally, for every dotted edge $e \in D$ with $l(e) = 1$ if we apply a classical contraction of e, we obtain a new graph $\overline{G}$ which possesses the same number of arithmetic q-colourings.

The beautiful results of D'Adderio and Moci only apply to $q \in \mathbb{Z}$ that behave well with the arithmetics of the labels. The crucial condition is stated in the following definition.

Definition ([DM13, Section 3.1])**.** Given a labelled graph (G, l) a positive integer $q \in \mathbb{N}$ is called *admissible* if it is a multiple of $l(e)$ for all edges e. I.e.

$$q \in \mathbb{N}_{>0} \text{ admissible } :\Longleftrightarrow \forall e \in E : l(e) | q.$$

Example. In our last example, where we produced an arithmetic 4-colouring, the number of colours 4 was indeed **not** admissible. However, if we take $q = 12$, which is admissible, then the same colouring yields an arithmetic 12-colouring.

We are now interested in the number of arithmetic q-colourings, for a given $q \in \mathbb{N}\backslash\{0\}$. To study this we regard the characteristic function of this problem.

Definition ([DM13, Section 3.1])**.** Given a labelled graph (G, l) let $\chi_{G,l} : \mathbb{N}\backslash\{0\} \to \mathbb{N} \cup \{0\}$ be the function, that associates to every positive integer $q \in \mathbb{N}\backslash\{0\}$ the number of arithmetic q-colourings on (G, l).

Remark. We will see in the proof that when restricted to the set of *admissible* positive integers q, the function

$$\chi_{G,l}(q) = \#\text{arithmetic } q\text{-colourings on } (G, l)$$

becomes polynomial in q. Therefore $\chi_{G,l} : \mathbb{N}\backslash\{0\} \to \mathbb{N} \cup \{0\}$ is called the *arithmetic chromatic polynomial* of (G, l).

Remark ([DM13, Rem. 3.2]). Note that in general $\chi_{G,l}$ does not behave like a polynomial anymore when applied to arbitrary q. In that case $\chi_{G,l}$ is a *quasipolynomial* function in q.

Remark ([DM13, Rem. 3.3]). In the case $l \equiv 1$ every $q \in \mathbb{N}\backslash\{0\}$ becomes admissible and if additionally $D = \emptyset$ then $\chi_{G,l}$ reduces to the classical chromatic polynomial χ_G of the underlying graph G, counting proper colourings with q colours (compare with [Tut54]).

We may now state how the arithmetic chromatic polynomial $\chi_{G,l}$ of a labelled graph (G, l) is connected to the arithmetic Tutte polynomial $M_{G,l}(x, y)$ of the arithmetic matroid induced by (G, l). In particular, the following theorem also yields the polynomial structure of $\chi_{G,l}$ when applied to an admissible positive integer q. However, to state the result properly we first introduce some notation.

Notation. Let (G, l) be a labelled graph with list of edges $E = R \sqcup D$. We denote by $\overline{G} = (\overline{V}, \overline{E})$ the new graph obtained from G by classically contracting all edges in D. Note that the graph $\overline{G}$ may now have loops.

Theorem 3.2.4 ([DM13, Thm. 3.1])**.** *Let (G, l) be a labelled graph, $\mathcal{M}_{G,l}$ the associated arithmetic matroid with $M_{G,l}(x, y)$ its arithmetic Tutte polynomial. Moreover let k be the number of connected components of the graph G. Then, if $q \in \mathbb{N}\backslash\{0\}$ is **admissible** we have*

$$\chi_{G,l}(q) = (-1)^{|\overline{V}|-k} q^k M_{G,l}(1 - q, 0).$$

Corollary 3.2.5 ([DM13, Cor. 3.2])**.** *If $l \equiv 1$ constant and $D = \emptyset$ we obtain the equation for the ordinary chromatic polynomial*

$$\chi_G(q) = (-1)^{|V|-k} q^k T_G(1-q, 0),$$

where k is again the number of connected components of the graph $G = (V, E)$ and $T_G(x, y)$ denotes the (classical) Tutte polynomial associated to G.

Remark ([DM13, Rem. 3.4])*.* The condition on q to be admissible is necessary. We take the example from the paper, where (G, l) is a given labelled graph with vertices $V = \{a, b, c\}$ no regular edges (i.e. $R = \emptyset$) and dotted edges $D = \{\{a, b\}, \{b, c\}\}$, on which we have labels $l(\{a, b\}) = 2$ and $l(\{b, c\}) = 6$. If we now set $q = 2$, then the conditions for an arithmetic 2-colouring are trivially satisfied for all possible colourings. Hence we obtain $2^3 = 8$ different arithmetic 2-colourings (compare with Figure 3.4).

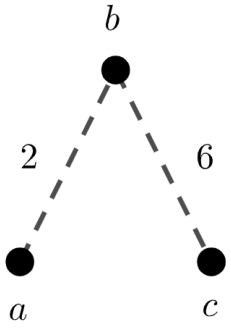

Figure 3.4: The simple counterexample.

Now following the construction for a representation of the corresponding arithmetic graph matroid we fix the orientation $E_\theta = \{(a, b), (c, b)\}$ and obtain the lists $X_D = \{(2, -2, 0), (0, -6, 6)\} \subseteq \mathbb{Z}^3$ and $X_R = \emptyset \subseteq H = \mathbb{Z}^3/\langle X_D \rangle = \mathbb{Z}^3/\langle (2, -2, 0), (0, -6, 6) \rangle$. Some easy computation yields $M_{G,l}(x, y) = 12$ constantly. Thus by the theorem above we would obtain

$$\chi_{G,l}(q) = q M_{G,l}(1-q, 0) = 12q.$$

However, this would tell us that $\chi_{G,l}(2) = 12 \cdot 2 = 24 \neq 8$ a contradiction. Therefore we really have to demand for q to be admissible.

The proof of the theorem follows a strategy that is similar to the one in the proof of Theorem 3.1.5 in Section 3.1.3. To prove the equality of the two polynomials we show at first that both expressions fulfil the same recursions. Due to that we may reduce the problem to a trivial case where equality is obvious (or at least easier to prove). Now for the start let us introduce a short notation for the right-hand-side formula in the theorem. We write

$$\widetilde{\chi}_{G,l}(q) := (-1)^{|\overline{V}|-k} q^k M_{G,l}(1-q, 0).$$

Thus our aim is to prove $\chi_{G,l}(q) = \widetilde{\chi}_{G,l}(q)$ for every admissible q.

In a first step we want to get rid of all regular edges. As before, for a labelled graph (G, l) and a regular edge $e \in R$ we denote by $G \setminus e$ and G/e the *labelled* deletion and contraction, respectively. (Review Section 2.1.2 for definitions.) Then the following recursion formula for $\chi_{G,l}(q)$ is deduced immediately from its definition.

Lemma 3.2.6 ([DM13, Lem. 4.1])**.** *Let (G, l) be a labelled graph and let $q \in \mathbb{N}\setminus\{0\}$ be an admissible integer. Then for a regular edge $e \in R$ we have*

$$\chi_{G,l}(q) = \chi_{G\setminus e,l}(q) - \chi_{G/e,l}(q).$$

Following our strategy we now need to show that $\widetilde{\chi}_{G,l}$ fulfils the same recursion.

Lemma 3.2.7 ([DM13, Lem. 4.2])**.** *Let (G, l) be a labelled graph and let $q \in \mathbb{N}\setminus\{0\}$ be an admissible integer. Then for a regular edge $e \in R$ we have*

$$\widetilde{\chi}_{G,l}(q) = \widetilde{\chi}_{G\setminus e,l}(q) - \widetilde{\chi}_{G/e,l}(q).$$

Proof. Clearly we want to use the various deletion and contraction recursions fulfilled by $M_{G,l}(x, y)$. They all have been proven in Section 3.1.2. To apply them properly we have to distinguish three cases.

Case 1: e is a proper edge. This means the corresponding edge in $\overline{G}$ is neither a loop nor a coloop which means it is contained in a circuit. Then we may compute

$$\begin{aligned}
\widetilde{\chi}_{G,l}(q) &= (-1)^{|\overline{V}|-k} q^k M_{G,l}(1-q,0) \\
\text{(Lem. 3.1.2)} &= (-1)^{|\overline{V}|-k} q^k \big(M_{G\setminus e,l}(1-q,0) + M_{G/e,l}(1-q,0)\big) \\
&= (-1)^{|\overline{V}_d|-k} q^k M_{G\setminus e,l}(1-q,0) - (-1)^{|\overline{V}_c|-k} q^k M_{G/e,l}(1-q,0) \\
&= \widetilde{\chi}_{G\setminus e,l}(q) - \widetilde{\chi}_{G/e,l}(q),
\end{aligned}$$

where $|\overline{V}_d| = |\overline{V}|$ and $|\overline{V}_c| = |\overline{V}| - 1$ denote the sets of vertices of the deletion and and contraction graphs, or rather their cardinalities.

Case 2: e is a coloop. In this case the corresponding edge in $\overline{G}$ is not a loop and is not contained in a circuit. Then we may compute

$$\begin{aligned}
\widetilde{\chi}_{G,l}(q) &= (-1)^{|\overline{V}|-k} q^k M_{G,l}(1-q,0) \\
\text{(Lem. 3.1.3)} &= (-1)^{|\overline{V}|-k} q^k \big(-qM_{G\setminus e,l}(1-q,0) + M_{G/e,l}(1-q,0)\big) \\
&= (-1)^{|\overline{V}_d|-(k+1)} q^{(k+1)} M_{G\setminus e,l}(1-q,0) - (-1)^{|\overline{V}_c|-k} q^k M_{G/e,l}(1-q,0) \\
&= \widetilde{\chi}_{G\setminus e,l}(q) - \widetilde{\chi}_{G/e,l}(q),
\end{aligned}$$

since $G \setminus e$ has now one more component, $|\overline{V}_d| = |\overline{V}|$ and $|\overline{V}_c| = |\overline{V}| - 1$.

Case 3: e is a loop. In this case the corresponding edge in $\overline{G}$ is also a loop. Therefore we have

$$\begin{aligned}
\widetilde{\chi}_{G,l}(q) &= (-1)^{|\overline{V}|-k} q^k M_{G,l}(1-q,0) \\
\text{(Lem. 3.1.4)} &= (-1)^{|\overline{V}|-k} q^k \big(M_{G\setminus e,l}(1-q,0) - M_{G/e,l}(1-q,0)\big) \\
&= (-1)^{|\overline{V_d}|-k} q^k M_{G\setminus e,l}(1-q,0) - (-1)^{|\overline{V_c}|-k} q^k M_{G/e,l}(1-q,0) \\
&= \widetilde{\chi}_{G\setminus e,l}(q) - \widetilde{\chi}_{G/e,l}(q),
\end{aligned}$$

since $|\overline{V}_d| = |\overline{V}|$ and $|\overline{V}_c| = |\overline{V}|$.

□

Due to this result it remains to prove Theorem 3.2.4 for the case where $R = \emptyset$, i.e. there are no regular edges. For our next step we reduce the problem to the case of connected graphs where we only have one connected component.

Proposition 3.2.8 ([DM13, Section 4])**.** *If Theorem 3.2.4 applies to connected labelled graphs with no regular edges, then it is also true for labelled graphs with several components and no regular edges.*

Proof. Let (G,l) be a labelled graph with k connected components denoted by $G_1, G_2, \ldots, G_k$, each of them equipped with a labelling $l_1, l_2, \ldots, l_k$, respectively. Then the associated arithmetic matroid $\mathcal{M}_{G,l}$ is the direct sum of the arithmetic matroids given by the single components $\mathcal{M}_{G_i,l_i}$. Hence the arithmetic Tutte polynomial $M_{G,l}(x,y)$ is the *product* of the arithmetic Tutte polynomials M_{G_i,l_i} of the components. Moreover observe that for all $i = 1, \ldots, k$ the graph $\overline{G}_i$ consists only of one single vertex (since all dotted edges are contracted and there are no regular ones). Therefore we have $|\overline{V}| = k$. Now assuming that the questioned assertion holds on connected graphs we deduce

$$\begin{aligned}
\widetilde{\chi}_{G,l}(q) &= (-1)^{|\overline{V}|-k} q^k M_{G,l}(1-q,0) \\
&= q^k M_{G,l}(1-q,0) \\
&= q^k \cdot \prod_{i=1}^{k} M_{G_i,l_i}(1-q,0) \\
&= \prod_{i=1}^{k} q \cdot M_{G_i,l_i}(1-q,0) \\
\text{(assumption)} \quad &= \prod_{i=1}^{k} \chi_{G_i,l_i}(q) = \chi_{G,l}(q).
\end{aligned}$$

Note that the last equation follows immediately from the definition of $\chi_{G,l}(q)$. □

To sum things up, to show Theorem 3.2.4 it is enough to prove the following statement.

Lemma 3.2.9 ([DM13, Lem. 4.3])**.** *Let (G,l) be a connected labelled graph without any regular edges (i.e. $R=\emptyset$) and let q be an admissible positive integer. Then the following equation holds:*

$$\chi_{G,l}(q) = \widetilde{\chi}_{G,l}(q).$$

Proof. In such a connected graph without any regular edges, observe that we have

$$\widetilde{\chi}_{G,l}(q) = q \cdot M_{G,l}(1-q,0) = q \cdot \mathfrak{m}(\emptyset).$$

Recall the algebraic construction for the representability of $\mathcal{M}_{G,l}$ given in Section 2.1.2. Note that then $\mathfrak{m}(\emptyset)$ is equal to the cardinality of the torsion subgroup of $\mathbb{Z}^{|V|}/X_D$. This can be computed as the GCD of the non-zero minors of maximal rank of the matrix $[X_D]$, which contains the elements of X_D as its columns.

To compute the number of arithmetic q-colourings we set $h := |X_D| = |D|$ and $n = |V|$. Since G is assumed to be connected we have $h \geq n-1$. We may now lay our focus at $[X_D]^T$, the transpose of the matrix $[X_D]$. This can be considered as a linear operator acting on the left, i.e. if we think of the elements of $(\mathbb{Z}/q\mathbb{Z})^n$ and $(\mathbb{Z}/q\mathbb{Z})^h$ as column vectors and have

$$[X_D]^T : (\mathbb{Z}/q\mathbb{Z})^n \to (\mathbb{Z}/q\mathbb{Z})^h.$$

Each element of $(\mathbb{Z}/q\mathbb{Z})^n$ refers to a possible but not yet proper arithmetic q-colouring. I remind that for $e \in D$ the associated element $x_e \in X_D$ is defined as

$$(x_e)_k = \begin{cases} l(e) & \text{if } k = i \\ -l(e) & \text{if } k = j \\ 0 & \text{else.} \end{cases}$$

Hence, applying the transpose $[X_D]^T$ to a colouring $\mathfrak{c} \in (\mathbb{Z}/q\mathbb{Z})^n$ refers to checking condition (ii) of the definition of proper q-colourings. Since checking condition (i) is obsolete as we do not have any regular edges, we obtain the following relation:

$$\mathfrak{c} \in (\mathbb{Z}/q\mathbb{Z})^n \text{ is proper } \iff \mathfrak{c} \in \ker([X_D]^T).$$

Thus we need to count the elements in $\ker([X_D]^T)$. To do so we look at the following exact sequence. (Recall that a sequence is exact if the image of each homomorphism equals the kernel of the successive one.)

$$0 \to \ker([X_D]^T) \overset{\iota}{\hookrightarrow} (\mathbb{Z}/q\mathbb{Z})^n \overset{[X_D]^T}{\longrightarrow} (\mathbb{Z}/q\mathbb{Z})^h \overset{\pi}{\longrightarrow} \frac{(\mathbb{Z}/q\mathbb{Z})^h}{\operatorname{im}[X_D]^T} \to 0,$$

where ι is simply the inclusion and π denotes the canonical quotient map. Now since we have $(\mathbb{Z}/q\mathbb{Z})^n/\ker([X_D]^T) \cong \operatorname{im}[X_D]^T$ we obtain that

$$\frac{|(\mathbb{Z}/q\mathbb{Z})^h|}{|\operatorname{im}[X_D]^T|} = \frac{|(\mathbb{Z}/q\mathbb{Z})^h|}{|(\mathbb{Z}/q\mathbb{Z})^n|} \cdot |\ker([X_D]^T)| = q^{h-n} |\ker([X_D]^T)|.$$

Next, we note again by the isomorphism theorem that the left-hand side equals

$$[(\mathbb{Z}/q\mathbb{Z})^h : \mathrm{im}[X_D]^T] = [\mathbb{Z}^h : \mathrm{im}[X_D^T \mid q \cdot I_h]\ ], \tag{3.2.2}$$

where $[X_D^T \mid q \cdot I_h]$ denotes the $h \times (n+h)$-matrix whose first n columns are given by the columns of $[X_D]^T$ and the other h columns are given by the columns of q-times the $h \times h$-identity matrix I_h. Again we interpret $[X_D^T \mid q \cdot I_h]$ as a linear operator

$$[X_D^T \mid q \cdot I_h] : \mathbb{Z}^{n+h} \to \mathbb{Z}.$$

However, if we want to compute the index on the right-hand side of equation (3.2.2) we get $\mathfrak{m}(\emptyset) \cdot q^{h-n+1}$. This is true due the fact that we calculate in $\mathbb{Z}^h$ and thus the GCD-rule applies. Hence $\mathfrak{m}(\emptyset) \cdot q^{h-n+1}$ equals the GCD of the minors of maximal rank of $[X_D^T \mid q \cdot I_h]$. However, since $l(e)$ divides q for every edge $e \in E = D$, it is enough to compute the GCD of only those minors of maximal rank which contain $n-1$ columns of $[X_D]^T$ (which correspond to the edges of a spanning tree) and where the rest is filled up with columns of $q \cdot I_h$ (all other minors are multiples of these). But this tells us that the solution is q^{h-n+1} times the GCD of the minors of rank $n-1$ in $[X_D]^T$, which are the same as in $[X_D]$. However, we have already seen that this last number equals $\mathfrak{m}(\emptyset)$. This yields the computation of the index.

Combining all this information we deduce that

$$\chi_{G,l}(q) = |\ker([X_D]^T)| = q \cdot \mathfrak{m}(\emptyset) = q \cdot M_{G,l}(1-q, 0) = \widetilde{\chi}_{G,l}(q),$$

just as demanded. □

This also concludes the proof of Theorem 3.2.4 and Corollary 3.2.5. Moreover this yields that the *(arithmetic) chromatic polynomial* is indeed a polynomial when applied to admissible integers q.

Now we want to concern ourselves with the kind of *dual* concept of so-called *arithmetic flows*. We start by giving the formal definition.

Definition ([DM13, Section 5.1])**.** Let (G, l) be a labelled graph. On G fix an orientation θ and denote by G_θ the resulting directed graph. Again choose q to be a positive integer and let $H = \mathbb{Z}/q\mathbb{Z}$.

Now to each directed edge $e = (u, v) \in E_\theta$ associate a weight $w(e) \in H$, and to every vertex $v \in V$ we associate the value

$$u(v) := \sum_{e \in\ out(v)} l(e) \cdot w(e) - \sum_{e \in\ in(v)} l(e) \cdot w(e) \in H,$$

where $out(v)$ and $in(v)$ denote the sets of outgoing and incoming edges of v, respectively. Then we call the function $w : E \to H$ an *arithmetic (nowhere zero) q-flow* if the following conditions are satisfied:

(i). For every $v \in V$ we have $u(v) = 0 \in H$.

(ii). For every regular edge $e \in R_\theta$ we have $w(e) \neq 0 \in H$.

Remark ([DM13, Rem. 5.1]). Again we restrict our observations to the case where q is admissible. And if $l \equiv 1$ is the trivial label and $D = \emptyset$ we obtain the classical notion of a nowhere zero q-flow on an oriented labelled graph.

Definition ([DM13, Rem. 5.2])**.** The *arithmetic flow polynomial* of a labelled graph (G, l) is defined as the function $\chi^*_{G,l} : \mathbb{N}\setminus\{0\} \to \mathbb{N}$ that assigns to every positive integer the number of arithmetic q-flows on (G, l). In the trivial case $l \equiv 1$ constant and $D = \emptyset$ we recover the classical flow polynomial $\chi^*_G(q)$ of the underlying graph G.

Remark ([DM13, Lem. 5.1]). Note that the orientation of the edges of G does not appear in the definition of $\chi^*_{G,l}$. However, it turns out that the arithmetic flow polynomial is independent of the orientation θ. This is true due to the fact that if we change the orientation of an edge $e \in E_\theta$, then for every flow $w : E_\theta \to H$ we may simply change the sign of $w(e)$ and get a flow on the new orientation.

For the arithmetic flow polynomial we have some results that are similar to those for the arithmetic chromatic polynomial. First of all, also $\chi^*_{G,l}$ is polynomial for admissible q.

Theorem 3.2.10 ([DM13, Thm. 5.2])**.** *Let (G, l) a labelled graph with k connected components and let q be an admissible integer. Then we have*

$$\chi^*_{g,l}(q) = (-1)^{|R|-|\overline{V}|+k} q^{|D|-|V|+|\overline{V}|} M_{G,l}(0, 1-q),$$

where $\overline{G} = (\overline{V}, \overline{E})$ is again the graph obtained from G by classically contracting all edges in D.

In the trivial case of $l \equiv 1$ and $D = \emptyset$ we obtain the following immediate corollary.

Corollary 3.2.11 ([DM13, Cor. 5.3])**.** *For a graph $G = (V, E)$ with k connected components and Tutte polynomial $T_G(x, y)$ we have*

$$\chi^*_G(q) = (-1)^{|E|-|V|+k} T_G(0, 1-q).$$

The proof for Theorem 3.2.10 uses similar methods as in the proof of Theorem 3.2.4 for the arithmetic chromatic polynomial. Thus for the interested reader we refer to [DM13, Section 6] for the details. We have finished our work on possible specialisations. In the last section of this chapter we dedicate ourselves to possible further generalisations of arithmetic Tutte polynomials.

3.2.3 Generalisations of the arithmetic Tutte polynomial

The aim of this section is to give an overview of the current state of research in the field of arithmetic matroids and arithmetic Tutte polynomials. Moreover it should serve as an orientation for interested readers who want to further deepen their knowledge. We freely mention some of the directions researchers have taken to expand the theory.

We begin with the **multivariate arithmetic Tutte polynomial**. In classical matroid theory, the Tutte polynomial $T_{\mathcal{M}}(x,y)$ is a bivariate invariant of a given matroid $\mathcal{M}$. If $\mathcal{M} = (X, \mathrm{rk})$ then Sokal [Sok05] generalised this construction to the *multivariate Tutte polynomial* in the variables q and $\mathbf{v} = (v_x)_{x\in X}$ given by

$$Z_{\mathcal{M}}(q, \mathbf{v}) = \sum_{A\subseteq X} q^{-\mathrm{rk}(A)} \prod_{x\in A} v_x.$$

Then Brändén and Moci [BM14] adapted this concept to the case of arithmetic matroids. For $\mathcal{A} = (X, \mathrm{rk}, \mathfrak{m})$ being an arithmetic matroid they defined the *multivariate arithmetic Tutte polynomial* as

$$Z_{\mathcal{A}}(q, \mathbf{v}) = \sum_{A\subseteq X} \mathfrak{m}(A) q^{-\mathrm{rk}(A)} \prod_{x\in A} v_x.$$

This polynomial fulfils again a contraction and deletion recurrence as well as a generalised Crapo-like formula (see [BM14, Thm. 4.6] and compare with Theorem 3.1.11). Additionally we can recover the bivariate arithmetic Tutte polynomial, because simply by the definitions we deduce that

$$Z_{\mathcal{A}}((x-1)(y-1), (y-1)) = (x-1)^{-rk(X)} M_{\mathcal{A}}(x,y),$$

where $\mathbf{v} = (y-1)$ means that every $v_e = (y-1)$ for all $e \in X$ (see [BM14, Section 2]).

Another big step of abstraction was achieved by Ye Liu, Tan Nhat Tran and Masahiko Yoshinaga in their publication about so-called **G-Tutte polynomials** [LTY21].

Definition ([LTY21, Def. 4.6])**.** Let Γ be a finitely generated abelian group, X a finite list of elements in Γ and let G be a torsionwise finite abelian group. Then the *G-multiplicity* $\mathfrak{m}(X, G) \in \mathbb{Z}$ is defined by

$$\mathfrak{m}(X, G) := \#\mathrm{Hom}((\Gamma/\langle X\rangle)_{\mathrm{tor}}, G),$$

where H_{tor} denotes the torsion group of an abelian group H.

Definition ([LTY21, Def. 4.8])**.** Let $\Gamma, X \subseteq \Gamma$ and G be defined as described above. Then the *G-Tutte polynomial* of X and G is defined as

$$T_X^G(x,y) := \sum_{A\subseteq X} \mathfrak{m}(A, G)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)}.$$

Again this polynomial fulfils several identities one might expect from a Tutte-like polynomial. Moreover it is a real generalisation of the arithmetic Tutte polynomial, at least for representable arithmetic matroids, due to the following proposition.

Proposition 3.2.12 ([LTY21, Prop. 4.13])**.** *Let X be a finite list of elements in the finitely generated abelian group Γ, and let $G = \mathbb{C}^*$. Then $T_X^G(x,y) = M_X(x,y)$.*

Proof. The proof relies on the observation that for $A \subseteq X$ we have

$$\#\mathrm{Hom}((\Gamma/\langle A\rangle)_{\mathrm{tor}}, \mathbb{C}^*) = |(\Gamma/\langle A\rangle)_{\mathrm{tor}}|$$

which is equal to the arithmetic multiplicity $\mathfrak{m}(A)$. □

A generalisation that is dedicated to rather structural aspects was examined by Roberto Pagaria. He successfully combined the two abstract notions of *orientable matroids* and *arithmetic matroids*. His results on **orientable arithmetic matroids** can be found in [Pag20].

The notions of arithmetic colourings and flows on graphs can be transferred to **CW complexes**. This was done by Emanuele Delucchi and Luca Moci in [DM16]. There again characteristic functions $\chi(q)$ and $\chi^*(q)$ are observed and it is shown that these are specialisations of the so-called *Tutte quasi-polynomial*.

Last but by far not least, Alex Fink and Luca Moci abstracted the concept of a matroid as a whole in their article **Matroids over a ring** [FM16]. There they give purely algebraic descriptions of matroids and arithmetic matroids by interpreting a matroid as a mapping $\mathcal{M}$ that assigns to each sublist A of a groundlist X a finitely generated R-module, where R is a ring (see [FM16, Def. 2.1] for more details).

We have now finished our summery of the basic theory of arithmetic matroids. In the final chapter of this thesis I would like to introduce a new class of (quasi-) arithmetic matroids with a strong connection to elementary number theory: The so-called *radical matroids*.

4 Radical matroids

In the final chapter of this thesis we apply the theory, we gathered by now, to elementary number theory. More precisely we want to develop (quasi-) arithmetic matroid structures on lists of integers and rationals. The independence relations will emerge from divisibility by prime factors, while the multiplicity arises from a derived form of the radical function. This yields another interesting example for arithmetic matroids outside the realms of graphs and vector spaces. We start with the general construction of those *radical matroids* in abstract *unique factorisation domains* (UFD) and then head on to the examination of their basic properties in the case of rational numbers.

There we will see some explicit examples. We remark that not all radical matroids can also be considered as arithmetic matroids. However, we will discuss some criteria on the underlying list $X \subseteq \mathbb{Q}$ such that we obtain an arithmetic matroid. Afterwards we give a full characterisation of the representable radical matroids.

4.1 The basic construction

Let $\mathcal{M} = (X, \mathrm{rk}, \mathfrak{m})$ be a multiplicity matroid. Recall that $\mathcal{M}$ is called a quasi-arithmetic matroid if the following two axioms are fulfilled.

(A) If $A \subseteq X$ and $v \in X$ is dependent of A, then $\mathfrak{m}(A \cup \{v\})$ divides $\mathfrak{m}(A)$. However, if $A \subseteq X$ and $v \in X$ is independent of A, then $\mathfrak{m}(A)$ divides $\mathfrak{m}(A \cup \{v\})$.

(Q) If $[R, S]$ is a molecule of $\mathcal{M}$ then we have

$$\mathfrak{m}(R) \cdot \mathfrak{m}(S) = \mathfrak{m}(R \cup F) \cdot \mathfrak{m}(R \cup T),$$

where F and T denote as always the *free part* and the *torsion part* of the molecule, respectively.

To be a fully arithmetic matroid $\mathcal{M}$ would also have to satisfy the positivity axiom:

(P) For each molecule $[R, S]$ the following inequality holds:

$$\rho(R, S) := (-1)^{|T|} \sum_{A \in [R,S]} (-1)^{|S|-|A|} \mathfrak{m}(A) \geq 0.$$

While the positivity requires $\mathfrak{m} : \mathcal{P}(X) \to \mathbb{Z}$, the axioms (A) and (Q) work for multiplicities with values in arbitrary UFDs. Therefore we would like to start our construction in this rather abstract setting. For this we will recall some terminology and basic notions from abstract algebra.

4.1.1 Algebra prerequisites

The following definitions and constructions are taken from [KM17]. However, this content may be found in any script on advanced or commutative algebra. Let $\mathcal{R}$ be a commutative ring. By $\mathcal{R}^*$ we denote the multiplicative group of units in $\mathcal{R}$. Additionally $\mathcal{R}$ is called an *integral domain* if it does not contain any zero-divisors (compare with [KM17, Section 13]). In such a ring we establish the following definitions.

Definition ([KM17, Section 16.1])**.** Let $x, z \in \mathcal{R}$. We say that x *divides* z in $\mathcal{R}$ and write as usual $x|z$ if there exists another element $y \in \mathcal{R}$ with $xy = z$. Let $p \in \mathcal{R} \setminus \mathcal{R}^*$.

- p is called *irreducible* if there **do not** exist any $a, b \in \mathcal{R} \setminus \mathcal{R}^*$ with $ab = p$.
- p is called *prime* if for all $a, b \in \mathcal{R}$ we have that $p|ab$ implies $p|a$ or $p|b$.

It is a well known fact that *prime* implies *irreducible*. The converse is not true in general. However, the cases where irreducibility already yields prime are the most interesting ones. Such a ring deserves its own definition.

Definition ([KM17, Thm. 17.1])**.** An integral domain $\mathcal{R}$ where every irreducible element is already a prime element is called a *unique factorisation domain* (short UFD). Equivalently, $\mathcal{R}$ is a UFD if and only if every non-zero element $x \in \mathcal{R}$ can be factorised

$$x = p_1 \cdot p_2 \cdot \dots \cdot p_k \cdot u$$

into prime elements $p_1, p_2, \dots, p_k \in \mathcal{R}$, $u \in \mathcal{R}^*$ a unit and this factorisation is unique up to the order of the primes and the multiplication with units.

Example ([KM17, Section 19.1])*.* The classical example for a UFD would be the ring of integers $\mathbb{Z}$. However, if $\mathbb{K}$ is a field then the ring of polynomials $\mathbb{K}[X]$ is a UFD. More generally, if $\mathcal{R}$ is a UFD then so is $\mathcal{R}[X]$.

Remark. Concerning the multiplication with units, observe that if $u \in \mathcal{R}^*$ is a unit and $p \in \mathcal{R}$ is a prime element, then also $u \cdot p$ is prime. For instance, 7 is a prime number in $\mathbb{Z}$ and -1 is a unit. Clearly also $-7 \in \mathbb{Z}$ is a prime element. For the prime factorisation of 42 we obtain

$$42 = 2 \cdot 3 \cdot 7 = (-1) \cdot (-2) \cdot (-3) \cdot (-7).$$

In this sense we say that 7 and -7 are associated to each other. In general we can state the following.

Definition. Let $\mathcal{R}$ be a UFD and let $p, q \in \mathcal{R}$ be prime elements. We say p and q are *associated with each other* if there exists a unit $u \in \mathcal{R}^*$ such that $p = u \cdot q$.

Example. In $\mathbb{Z}$ we have that 3 and -3 or p and $-p$ are associated with each other for all positive primes p. Another example could be made in $\mathbb{C}[X]$, the ring of complex polynomials. In $\mathbb{C}[X]$ the prime elements are given as the linear factors $f(x) = ax + b$ for $a, b \in \mathbb{C}, a \neq 0$. Now $(\mathbb{C}[X])^* = \mathbb{C} \setminus \{0\}$ and we have for example that $x + 1$ is associated to $ix + i$. Moreover, the factorisation into prime elements in $\mathbb{C}[X]$ refers directly to the fundamental theorem of algebra.

It is easy to see, that this defines an equivalence relation on the set of prime elements in a UFD. We now would like to make the prime decomposition unique up to the order of factors. This is done by choosing one representative of each equivalence class of prime elements.

Notation. Let $\mathcal{R}$ be a UFD. We denote by $\widehat{\mathcal{P}}$ the set of prime elements in $\mathcal{R}$. Additionally, we write $\mathcal{P}$ for any fixed system of representatives of prime elements. Hence we have $\mathcal{P} \subseteq \widehat{\mathcal{P}}$ given in a way, such that for all prime elements $\hat{p} \in \widehat{\mathcal{P}}$ there exists exactly one $p \in \mathcal{P}$ such that $\hat{p} = u \cdot p$ for a unit $u \in \mathcal{R}^*$. If $\mathcal{R} = \mathbb{Z}$ then we write $\mathbb{P}$ for the positive prime numbers.

Example. In the set integers $\mathbb{Z}$, the set of positive prime numbers $\mathbb{P}$ does indeed provide such a system of representatives. On the other hand, in $\mathbb{C}[X]$ one may choose $\mathcal{P}$ to be the set of monic linear factors, i.e. $\mathcal{P} = \{x - c \mid c \in \mathbb{C}\}$.

With a fixed system $\mathcal{P}$ of representatives in a unique factorisation domain $\mathcal{R}$, the prime factorisation of every $x \in \mathcal{R}$ with $x \neq 0$ becomes unique up to the order of factors. More precisely, there exist unique factors $p_1, \ldots, p_n \in \mathcal{P}$ and a unique unit $u_x \in \mathcal{R}^*$ such that

$$x = p_1 \cdot p_2 \cdot \cdots \cdot p_k \cdot u_x.$$

Definition. Let $\mathcal{R}$ be a UFD and let $x, y \in \mathcal{R}$. We write x and y in their unique prime factorisations $x = p_1 \cdot p_2 \cdot \cdots \cdot p_k \cdot u_x$ and $y = q_1 \cdot q_2 \cdot \cdots \cdot q_m \cdot u_y$ with respect to a fixed system of prime representatives $\mathcal{P}$. We call x and y *coprime* if the two elements do not share any common prime divisors. I.e. we have $\{p_1, p_2, \ldots, p_k\} \cap \{q_1, q_2, \ldots, q_m\} = \emptyset$.

UFDs will provide the formal setting for the divisibility demanded by axiom (A) of quasi-arithmetic matroids. The underlying matroid structure will come from the following construction.

Definition ([KM17, Section 13.8.1])**.** Let $\mathcal{R}$ be an integral domain. On $\mathcal{R} \times (\mathcal{R} \setminus \{0\})$ we define the following equivalence relation:

$$(a, b) \sim (c, d) :\Longleftrightarrow ad = bc.$$

We denote by the fraction $\frac{a}{b}$ the equivalence class of (a, b). Then the *quotient field* $\mathcal{Q}$ of $\mathcal{R}$ is given by

$$\mathcal{Q} := \operatorname{quot}(\mathcal{R}) = \left\{ \frac{a}{b} : a, b \in \mathcal{R}, b \neq 0 \right\}$$

together with the operations

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{and}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

It is easy to check that $\mathcal{Q} = \operatorname{quot}(\mathcal{R})$ is indeed a field. In the case of $\mathcal{R}$ being a UFD we can now deduce the following theorem.

Theorem 4.1.1. *Let $\mathcal{R}$ be a UFD with quotient field $\mathcal{Q}$. Then every element $x \in \mathcal{Q}$ can be written as*

$$x = \frac{p_1 \cdot p_2 \cdot \dots \cdot p_k}{q_1 \cdot q_2 \cdot \dots \cdot q_m} \cdot u_x = p_1 \cdot p_2 \cdot \dots \cdot p_k \cdot q_1^{-1} \cdot q_2^{-1} \cdot \dots \cdot q_m^{-1} \cdot u_x,$$

where $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_m \in \mathcal{P}$ are representative prime elements, $p_i \neq q_j$ for all $i \in [k], j \in [m]$ and $u_x \in \mathcal{R}^*$ is a unit of the ring. Moreover this representation is unique up to the order of the prime elements.

Sketch of proof. The idea of the proof works simply by observing that every $x \in \mathcal{Q}$ can be written as unique fraction $x = \frac{a}{b}$ with $a, b \in \mathcal{R}$ being coprime. Then one just inserts the unique prime factorisations $a = p_1 \cdot p_2 \cdot \dots \cdot p_k \cdot u_a$ and $b = q_1 \cdot q_2 \cdot \dots \cdot q_m \cdot u_b$ in $\mathcal{R}$ into the formula and we are done by setting $u_x := u_a \cdot u_b^{-1} \in \mathcal{R}^*$. □

Example. Let $\mathcal{R} = \mathbb{Z}$, then $\mathbb{Q} = \mathrm{quot}(\mathbb{Z})$. Then for example we have

$$\frac{420}{198} = \frac{70}{33} = \frac{2 \cdot 5 \cdot 7}{3 \cdot 11}.$$

Now with this notation and the previous theorem we obtain the following as an immediate corollary.

Lemma 4.1.2. *Let $\mathcal{Q}^* = \mathcal{Q} \setminus \{0\}$ be the multiplicative group of units. Then*

$$\mathcal{Q}^* = \mathcal{R}^* \cdot \langle \mathcal{P} \rangle_{\mathbb{Z}},$$

i.e. $\mathcal{Q}^*/\mathcal{R}^*$ is generated by the prime elements as a group.

This observation will yield the matroid structure for our radical matroids, since from Lemma 4.1.2 we get that every finite list $X \subseteq \mathcal{Q}^*$ is contained in a finitely generated abelian group. What is left to obtain a quasi-arithmetic matroid is a suitable multiplicity function. This will be constructed in the following section.

4.1.2 The radical function

Let $z \in \mathbb{N}$ be an integer with prime factorisation $z = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}$ where $a_i \in \mathbb{N}$ for all $i \in [k]$ and the p_i are pairwise distinct. Then the *radical of* z is defined as

$$\mathrm{rad}(z) = \mathrm{rad}(p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}) = p_1 \cdot p_2 \cdot \dots \cdot p_k.$$

In other words, the radical is the product of all primes occurring in the factorisation but each only taken once. This function plays a major role in some questions of number theory. The most prominent may be the famous *abc-conjecture* which is also connected to Fermat's last theorem. (Compare with [LS11, Section 1] or [Oes88].)

Example. We compute the radical for the numbers $2, 4, 6, 60, 99 \in \mathbb{Z}$. Then $\mathrm{rad}(2) = 2$, $\mathrm{rad}(4) = 2$, $\mathrm{rad}(6) = 6$, $\mathrm{rad}(60) = 30$ and $\mathrm{rad}(99) = 33$.

The idea is to establish the radical as the multiplicity function for our quasi-arithmetic matroid. To do so we have to generalise the notion of the radical step by step, first to arbitrary UFDs and their quotient fields and eventually to a radical of a list of fractions. The radical for a UFD and its quotient field may be defined analogously to the integer case.

Definition. Let $\mathcal{R}$ be a UFD, $\mathcal{P} \subseteq \mathcal{R}$ a system of prime representatives and let $\mathcal{Q}$ be its quotient field. By Theorem 4.1.1 we can write every element $x \in \mathcal{Q}$ as

$$x = u_x \prod_{p \in \mathcal{P}} p^{a_p}$$

with $u_x \in \mathcal{R}^*$ a unit, $a_p \in \mathbb{Z}$ and $a_p = 0$ for all but finitely many exponents. Then we define the *radical of* x (with respect to $\mathcal{P}$) by

$$\operatorname{rad}(x) = \operatorname{rad}_{\mathcal{P}}(x) := \prod_{\substack{p \in \mathcal{P} \\ a_p \neq 0}} p \quad \in \mathcal{R}.$$

Again one may say that $\operatorname{rad}(x)$ equals the product of all prime elements occurring in its unique prime factorisation but taken only once.

Remark. We observe the following useful property of the radical. If $x, y_1, y_2, \ldots, y_k \in \mathcal{R}$ (a UFD) and $x = y_1 \cdot y_2 \cdot \cdots \cdot y_k$ where the y_i are not necessarily prime elements, then we have

$$\operatorname{rad}(x) = \operatorname{rad}\Big(\prod_{i=1}^{k} \operatorname{rad}(y_i)\Big).$$

The proof works simply by noticing that each prime element occurring on either side also appears on the other. However, we will use a similar structure to define a radical for lists of elements in $\mathcal{Q}$.

Definition. Let $\mathcal{Q}$ be the quotient field of a UFD $\mathcal{R}$. For a finite list $A \subseteq \mathcal{Q}$ we set

$$\operatorname{rad}(A) := \operatorname{rad}\Big(\prod_{a \in A} \operatorname{rad}(a)\Big).$$

Again one could say that the $\operatorname{rad}(A)$ is the product of all prime elements, occurring in any factorisation of elements of A, taken once.

Remark. In this thesis we follow the convention that the empty product is equal to 1. Thus we also have $\operatorname{rad}(1) = 1$. In the same manner we also set $\operatorname{rad}(\emptyset) = 1$.

We summarise our insights in two examples.

Example. Let $A = \{20, \frac{21}{46}, \frac{8}{25}\} \subseteq \mathbb{Q}$. We fix $\mathcal{P} = \mathbb{P}$, the set of positive prime numbers.

Then we compute

$$\begin{aligned}\operatorname{rad}(A) &= \operatorname{rad}\Big(\prod_{a\in A}\operatorname{rad}(a)\Big)\\ &= \operatorname{rad}\Big(\operatorname{rad}(20)\cdot\operatorname{rad}\Big(\frac{21}{46}\Big)\cdot\operatorname{rad}\Big(\frac{8}{25}\Big)\Big)\\ &= \operatorname{rad}(10\cdot\operatorname{rad}(21)\cdot\operatorname{rad}(46)\cdot\operatorname{rad}(8)\cdot\operatorname{rad}(25))\\ &= \operatorname{rad}(10\cdot 21\cdot 46\cdot 2\cdot 5)\\ &= 2\cdot 3\cdot 5\cdot 7\cdot 23 = 4830.\end{aligned}$$

Example. Let $A = \left\{\frac{x^3-2x^2-5x+6}{x^2+25}, x^2-2x-8\right\} \subseteq \mathbb{C}(X) = \operatorname{quot}(\mathbb{C}[X])$. We choose $\mathcal{P} = \{x+c \mid c\in\mathbb{C}\}$ the set of monic linear factors. Then

$$\begin{aligned}\operatorname{rad}(A) &= \operatorname{rad}\Big(\operatorname{rad}\Big(\frac{x^3-2x^2-5x+6}{x^2+25}\Big)\cdot\operatorname{rad}(x^2-2x-8)\Big)\\ &= \operatorname{rad}(\operatorname{rad}(x^3-2x^2-5x+6)\cdot\operatorname{rad}(x^2+25)\cdot\operatorname{rad}(x^2-2x-8))\\ &= \operatorname{rad}((x-1)(x+2)(x-3)\cdot(x+i5)(x-i5)\cdot(x+2)(x-4))\\ &= (x-1)(x+2)(x-3)(x+i5)(x-i5)(x-4)\\ &= x^6-6x^5+28x^4-124x^3+51x^2+650x-600.\end{aligned}$$

By now we have collected everything we need to define a quasi-arithmetic matroid on some finite list $X \subseteq \mathcal{Q}^*$ with radical multiplicities.

4.1.3 The definition of radical matroids

Let $\widetilde{X} \subseteq \mathcal{Q}^*$ be a finite list of elements, where $\mathcal{Q}$ denotes again the quotient field of a unique factorisation domain $\mathcal{R}$. Just like before we call $\mathcal{P} \subseteq \mathcal{R}$ a fixed set of prime elements. Since we do not want to concern ourselves with the technical details of associated primes and the non-uniqueness induced by them, we would like to identify elements of $\mathcal{Q}^*$ if they differ only by a unit of the underlying ring. Algebraically this is done by taking a quotient of abelian groups:

$$\mathcal{Q}^* \to \mathcal{Q}^*/\mathcal{R}^*.$$

We introduce the following notations.

Notation. For a finite list $\widetilde{X} \subseteq \mathcal{Q}^*$ we denote by X the same list, but now interpreted as $X \subseteq \mathcal{Q}^*/\mathcal{R}^*$, a sublist of the quotient group. We let $\mathcal{P}_X \subseteq \mathcal{P}$ be the set of prime elements that appear in the unique factorisations of elements of X. Since X is finite, also the set $\mathcal{P}_X$ has to be finite.

Now we use Lemma 4.1.2 to see that

$$X \subseteq \langle\mathcal{P}_X\rangle_{\mathbb{Z}} \subseteq \mathcal{Q}^*/\mathcal{R}^* \cong \langle\mathcal{P}\rangle_{\mathbb{Z}}.$$

We deduce that X is a sublist of $\Lambda := \langle \mathcal{P}_X \rangle_{\mathbb{Z}}$ a finitely generated abelian group, since clearly $\Lambda \cong \mathbb{Z}^{|\mathcal{P}_X|}$. Thus Λ is even a *lattice*. This induces a matroid structure via the classical rank function in $\mathbb{Z}^{|\mathcal{P}_X|}$. Now one could easily obtain a torsion-free arithmetic matroid by associating the classical multiplicity $\mathfrak{m} : \mathcal{P}(X) \to \mathbb{Z}$ for lattices. Therefore we obtain an arithmetic Tutte polynomial $M_{\mathfrak{m}}(x, y) \in \mathbb{Z}[x, y]$. However, we want to equip the matroid (X, rk) with a radical multiplicity $\mathrm{rad}(A)$ for $A \subseteq X$. Note that this is now a function $\mathrm{rad} : \mathcal{P}(X) \to \mathcal{R}$. Therefore, in general, we get a multiplicity Tutte polynomial $M_{\mathrm{rad}}(x, y) \in \mathcal{R}[x, y]$.

Definition. We call the multiplicity matroid $\mathcal{M} = (X, \mathrm{rk}, \mathrm{rad})$ a *radical matroid*. Its multiplicity Tutte polynomial is then given by

$$M_{\mathcal{M}}(x, y) = \sum_{A \subseteq X} \mathrm{rad}(A)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)}.$$

Conversely, we say that an arbitrary multiplicity matroid $\mathcal{N}$ is *radical* if it is isomorphic to some radical matroid.

The combinatorial meaning of a Tutte polynomial in $\mathcal{R}[x, y]$ may be questionable. Nevertheless we prove that such a radical matroid gets as close to an arithmetic matroid as possible in this abstract setting.

Theorem 4.1.3. *Let $\mathcal{M} = (X, \mathrm{rk}, \mathrm{rad})$ be a radical matroid. Then $\mathcal{M}$ is also an (abstract) quasi-arithmetic matroid.*

Proof. We need to check axioms (A) and (Q) stated at the beginning of this section.

(A) Let $A \subseteq X$ be a sublist and let $v \in X \setminus A$. Firstly, we notice that by definition of the radical the identity $\mathrm{rad}(A) | \mathrm{rad}(A \cup \{v\})$ holds in any case, since v can only contribute new factors and will not delete any old ones. Thus it remains to show that when v is dependent on A, then also $\mathrm{rad}(A \cup \{v\})$ divides $\mathrm{rad}(A)$.
But this is easily seen to be true. Because if the factorisation of $\mathrm{rad}(A \cup \{v\})$ would contain any prime elements that were not included in the factorisation of $\mathrm{rad}(A)$, then those additional prime elements must originate from the factorisation of the element v. However, if v was built upon prime elements that are not contained in any factorisation of elements of A, then v could not be *dependent* on A.
Hence $\mathrm{rad}(A \cup \{v\})$ and $\mathrm{rad}(A)$ are factorised into the same prime elements and since in the radical every prime element is taken exactly once, we have that $\mathrm{rad}(A \cup \{v\})$ divides $\mathrm{rad}(A)$. (We even have that $\mathrm{rad}(A \cup \{v\}) = \mathrm{rad}(A)$ in this case.)

(Q) Let $[R, S]$ be a molecule of $\mathcal{M}$. Therefore we have $S = R \sqcup F \sqcup T$ and for all $C \in [R, S]$ it holds that $\mathrm{rk}(C) = \mathrm{rk}(R) + |C \cap F|$. We need to show that

$$\mathrm{rad}(R) \cdot \mathrm{rad}(S) = \mathrm{rad}(R \cup F) \cdot \mathrm{rad}(R \cup T).$$

Now by construction we have that every element of T is dependent on R. Therefore by our observations in the paragraph before we know that $\mathrm{rad}(R) = \mathrm{rad}(R \cup T)$.

Since the radical function takes its values in $\mathcal{R}$ an integral domain, we can therefore reduce the problem to the question, whether we have $\operatorname{rad}(S) = \operatorname{rad}(R \cup F)$?

However, again this can be verified by comparing prime elements in the factorisation of either side. If we write $B := R \cup F$, then we have $S = B \cup T$ and again the elements of T are dependent on B. Therefore we obtain $\operatorname{rad}(B \cup T) = \operatorname{rad}(B)$ or in other words

$$\operatorname{rad}(S) = \operatorname{rad}(R \cup F),$$

just as demanded.

Therefore we have proven that a radical matroid is indeed a quasi-arithmetic matroid. □

Now we would like to reenter the realms of integers and rationals, where we additionally have a notion of positivity. There we want to check whether our construction already leads to an arithmetic matroid. The answer is *maybe*. There are radical matroids which are also arithmetic matroids, however some others are not. This very fascinating correspondence between being arithmetic and being radical is the main subject of the next chapter.

4.2 Basic properties of radical matroids

In this section we restrict ourselves again to the most interesting case of $\mathcal{R} = \mathbb{Z}$. We choose again the positive primes $\mathbb{P}$ to be our system of representatives. In this situation the quotient field $\mathcal{Q}$ is simply given by the field of rationals $\mathbb{Q}$ and radical matroids $\mathcal{M} = (X, \operatorname{rk}, \operatorname{rad})$ are defined finite lists of invertible rational numbers $X \subseteq \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. Moreover, in the way we constructed the radical of sublists, we have again that $\operatorname{rad}(A) \in \mathbb{Z}$ for any $A \subseteq X$. This means that we may consider again whether our radical matroid fulfils positivity (P) and therefore may already be an arithmetic matroid. In this case we also have an arithmetic Tutte polynomial $M_{\mathcal{M}}(x, y)$ with positive integer coefficients.

4.2.1 Arithmetic radical matroids

In this chapter we want to analyse in which cases we might get an arithmetic radical matroid, i.e. which constraints has the list $X \subseteq \mathbb{Q}$ to obey. This is indeed a matter of discussion because **not** every radical matroid in $\mathbb{Q}$ will fulfil positivity. It is a shame, but even a short list may already give a counterexample.

Example. Let $X = \{4, 6\} \subseteq \mathbb{Q}$ then $[\emptyset, X]$ is a molecule and

$$\begin{aligned}\rho(\emptyset, X) &= \sum_{A \subseteq X} (-1)^{|X \setminus A|} \operatorname{rad}(A) \\ &= (-1)^2 \operatorname{rad}(\emptyset) + (-1)^1 \operatorname{rad}(\{4\}) + (-1)^1 \operatorname{rad}(\{6\}) + (-1)^0 \operatorname{rad}(\{4, 6\}) \\ &= 1 - 2 - 6 + 6 = -1 \not\geq 0.\end{aligned}$$

And indeed, if we compute the multiplicity Tutte polynomial we obtain

$$\begin{aligned} M(x,y) &= \sum_{A\subseteq X} \operatorname{rad}(A)(x-1)^{\operatorname{rk}(X)-\operatorname{rk}(A)}(y-1)^{|A|-\operatorname{rk}(A)} \\ (\operatorname{rk}(A)=|A|) &= \sum_{A\subseteq X} \operatorname{rad}(A)(x-1)^{\operatorname{rk}(X)-\operatorname{rk}(A)} \\ &= \operatorname{rad}(\emptyset)(x-1)^2 + \operatorname{rad}(4)(x-1) + \operatorname{rad}(6)(x-1) + \operatorname{rad}(4\cdot 6) \\ &= x^2+6x-1. \end{aligned}$$

On the other hand, there also exist radical matroids that satisfy positivity like the following example shows.

Example. Let $X=\{2,3,5\}$. Then each pair of sublists $A\subseteq B\subseteq X$ yields a molecule $[A,B]$. However, by the multiplicativity of the radical in this case we deduce that if $A\neq\emptyset$ then we have

$$\rho(A,B)=\operatorname{rad}(A)\rho(\emptyset,B\setminus A).$$

Thus it is enough to check positivity for molecules of the form $[\emptyset,A]$ with $A\subseteq X$. We compute:

$$\begin{aligned} \rho(\emptyset,\emptyset) &= \operatorname{rad}(\emptyset)=1\geq 0, \\ \rho(\emptyset,\{2\}) &= (-1)^1\operatorname{rad}(\emptyset)+(-1)^0\operatorname{rad}(2)=-1+2=1\geq 0. \end{aligned}$$

Analogously we deduce that $\rho(\emptyset,\{3\})=2$ and $\rho(\emptyset,\{5\})=4$ and both are greater than zero. For the lists with two elements we have

$$\begin{aligned} \rho(\emptyset,\{2,3\}) &= (-1)^2\operatorname{rad}(\emptyset)+(-1)^1\operatorname{rad}(2)+(-1)^1\operatorname{rad}(3)+(-1)^0\operatorname{rad}(2\cdot 3) \\ &= 1-2-3+6=2\geq 0, \\ \rho(\emptyset,\{2,5\}) &= (-1)^2\operatorname{rad}(\emptyset)+(-1)^1\operatorname{rad}(2)+(-1)^1\operatorname{rad}(5)+(-1)^0\operatorname{rad}(2\cdot 5) \\ &= 1-2-5+10=4\geq 0, \\ \rho(\emptyset,\{3,5\}) &= (-1)^2\operatorname{rad}(\emptyset)+(-1)^1\operatorname{rad}(3)+(-1)^1\operatorname{rad}(5)+(-1)^0\operatorname{rad}(3\cdot 5) \\ &= 1-3-5+15=8\geq 0, \end{aligned}$$

and finally:

$$\begin{aligned} \rho(\emptyset,\{2,3,5\}) &= (-1)^3\operatorname{rad}(\emptyset)+(-1)^2(\operatorname{rad}(2)+\operatorname{rad}(3)+\operatorname{rad}(5))+ \\ &\quad +(-1)^1(\operatorname{rad}(2\cdot 3)+\operatorname{rad}(2\cdot 5)+\operatorname{rad}(3\cdot 5))+(-1)^0\operatorname{rad}(2\cdot 3\cdot 5) \\ &= -1+10-31+30=8\geq 0. \end{aligned}$$

Hence we also expect the arithmetic Tutte polynomial to have non-negative coefficients.

Indeed,

$$\begin{aligned} M(x,y) &= \sum_{A\subseteq X} \operatorname{rad}(A)(x-1)^{\operatorname{rk}(X)-\operatorname{rk}(A)}(y-1)^{|A|-\operatorname{rk}(A)} \\ (\operatorname{rk}(A)=|A|) &= \sum_{A\subseteq X} \operatorname{rad}(A)(x-1)^{\operatorname{rk}(X)-\operatorname{rk}(A)} \\ &= \operatorname{rad}(\emptyset)(x-1)^3 + (x-1)^2(\operatorname{rad}(2)+\operatorname{rad}(3)+\operatorname{rad}(5))+ \\ &+ (x-1)(\operatorname{rad}(2\cdot 3)+\operatorname{rad}(2\cdot 5)+\operatorname{rad}(3\cdot 5))+\operatorname{rad}(2\cdot 3\cdot 5) \\ &= (x-1)^3+10(x-1)^2+31(x-1)+30 \\ &= x^3+7x^2+14x+8. \end{aligned}$$

So $X=\{2,3,5\}$ really does deliver an arithmetic matroid.

Regarding these two examples the question arises, what did go wrong in the first one or rather why did the second one work out? A superficial survey on the elements of both underlying lists points out that $2,3$ and 5 are primes while 4 and 6 are definitely not. This suggests a connection. However, it turns out that the elements of the list X do not have to be prime to generate an arithmetic matroid. It is enough that they are *pairwise coprime*. Since we consider $X\subseteq\mathbb{Q}$ a list of rationals, we need to clarify what we mean by this term in our context.

Definition. Let $\mathcal{R}$ be an UFD and $\mathcal{Q}$ its quotient field. We say that $x,y\in\mathcal{Q}$ are *coprime* if their radicals $\operatorname{rad}(x)$ and $\operatorname{rad}(y)$ are coprime in $\mathcal{R}$, i.e. they do not share any common prime factors in their factorisation.
Additionally a list $A\subseteq\mathcal{Q}$ is called *coprime* if all its elements are pairwise coprime.

Remark. In our situation this means, that two rationals are coprime if their radicals are coprime in the classical integer-sense. For example $\frac{7}{2}$ and $\frac{3}{5}$ are coprime while $\frac{15}{80}$ and $\frac{1}{111}$ are not since their radicals share a 3.

With this new notion we obtain the following crucial result.

Proposition 4.2.1. *Let $X=\{p_1,p_2,\dots,p_n\}\subseteq\mathbb{Q}$ be coprime and such that $|p_i|\neq 1$ for all $i\in[n]$. Then $\mathcal{M}=(X,\operatorname{rk},\operatorname{rad})$ defines an arithmetic matroid.*

Proof. We already know that $\mathcal{M}$ is a quasi-arithmetic matroid due to Theorem 4.1.3. Thus it remains to check positivity.
Since all elements of X are pairwise coprime and not equal to plus or minus one we conclude that the list X does only consist of coloops. Therefore we have that every pair of sublists $A\subseteq B\subseteq X$ gives a molecule $[A,B]$. Now since also all elements of B are pairwise coprime we obtain for every $C\in[A,B]$ that

$$\operatorname{rad}(C)=\operatorname{rad}(A\cup(C\cap(B\setminus A)))=\operatorname{rad}(A)\cdot\operatorname{rad}(C\cap(B\setminus A)).$$

And this yields that we have

$$\rho(A,B)=\operatorname{rad}(A)\cdot\rho(\emptyset,B\setminus A).$$

Hence, just like in the previous example, it is enough to show $\rho(\emptyset, Z) \geq 0$ for all sublists $Z \subseteq X$. By abuse of notation we write $Z = \{p_1, p_2, \ldots, p_k\}$, $k \leq n$. Then we prove

$$\rho(\emptyset, Z) = \sum_{A \subseteq Z} (-1)^{|Z|-|A|} \operatorname{rad}(A) \geq 0$$

by induction on k, the number of elements in Z. (Note that the factor $(-1)^{|T|}$ from the definition of $\rho(R, S)$ vanishes since we do not have any loops, i.e. $T = \emptyset$.)
$\underline{k = 0}$: In this case we have $Z = \emptyset$ and

$$\rho(\emptyset, \emptyset) = (-1)^0 \operatorname{rad}(\emptyset) = 1 \geq 0.$$

$\underline{\text{k} > 0}$: Assume we have $\rho(\emptyset, Z') \geq 0$ for all $Z' \subseteq X$ with $|Z'| < k$. Then we compute for $Z = \{p_1, \ldots, p_k\}$:

$$\begin{aligned}
\rho(\emptyset, Z) &= \sum_{A \subseteq Z} (-1)^{|Z|-|A|} \operatorname{rad}(A) \\
&= \sum_{p_k \in A \subseteq Z} (-1)^{|Z|-|A|} \operatorname{rad}(A) + \sum_{p_k \notin A \subseteq Z} (-1)^{|Z|-|A|} \operatorname{rad}(A) \\
(*) &= \sum_{A' \subseteq Z'} (-1)^{|Z'|-|A'|} \operatorname{rad}(A') \cdot \operatorname{rad}(\{p_k\}) + \sum_{A' \subseteq Z'} (-1)^{|Z'|-|A'|+1} \operatorname{rad}(A') \\
&= \big(\operatorname{rad}(p_k) - 1\big) \cdot \sum_{A' \subseteq Z'} (-1)^{|Z'|-|A'|} \operatorname{rad}(A') \\
&= \underbrace{\big(\operatorname{rad}(p_k) - 1\big)}_{\geq 0} \cdot \underbrace{\rho(\emptyset, Z')}_{\geq 0} \geq 0,
\end{aligned}$$

where at $(*)$ we set $A' := A \setminus \{p_k\}$ and $Z' := Z \setminus \{p_k\}$. In the last line we used our induction hypothesis for Z'. This yields the proof. □

We now would like to analyse the case, where we also include loops. In our setting a loop is either a 1 or -1. Since both give us the same radical and do not interfere with any independences we can assume without loss of generality that all loops included are equal to plus one. Moreover 1 is trivially coprime with any other number and thus we get the following.

Proposition 4.2.2. *Let* $X = \{p_1, p_2, \ldots, p_n, \overbrace{1, 1, \ldots, 1}^{m \text{ times}}\} \subseteq \mathbb{Q}$ *be coprime such that* $|p_i| \neq 1$ *for all* $i \in [n]$. *Then* $\mathcal{M} = (X, \mathrm{rk}, \mathrm{rad})$ *defines an arithmetic matroid.*

Proof. Following the reasoning of the proof of the last Proposition 4.2.1 we deduce that it is enough to show $\rho(\emptyset, Z) \geq 0$ for all sublists $Z \subseteq X$. Once more we write $Z = \{p_1, p_2, \ldots, p_k, \overbrace{1, \ldots, 1}^{l \text{ times}}\}$ by abuse of notation. We operate again by induction, this time on l the number of loops contained in Z.
$\underline{l = 0}$: This case is already covered by the proof of Proposition 4.2.1. Hence we move on.

$\underline{l > 0}$: Set $\mathbf{1}_l := \{1, 1, \ldots, 1\}$ be the list containing 1 exactly l times. Choose one of this loops in $\mathbf{1}_l$ and mark it as $\hat{1}$. Then for Z we compute:

$$\begin{aligned}
\rho(\emptyset, Z) &= (-1)^l \sum_{A \subseteq Z} (-1)^{|Z|-|A|} \operatorname{rad}(A) \\
&= (-1)^l \sum_{\hat{1} \in A \subseteq Z} (-1)^{|Z|-|A|} \operatorname{rad}(A) + (-1)^l \sum_{\hat{1} \notin A \subseteq Z} (-1)^{|Z|-|A|} \operatorname{rad}(A) \\
(*) &= (-1)^l \sum_{A' \subseteq Z'} (-1)^{|Z'|-|A'|} \operatorname{rad}(A') + (-1)^{l+1} \sum_{A' \subseteq Z'} (-1)^{|Z'|-|A'|} \operatorname{rad}(A') \\
&= (-1)^l (\rho(\emptyset, Z') - \rho(\emptyset, Z')) = 0 \geq 0.
\end{aligned}$$

Here, at $(*)$ we define Z' to be the list that contains the same elements as Z but with one 1 less. Note that deleting a 1 also does not change the radical! However, this proves the assertion. □

Remark. The very attentive reader might have noticed that the *proof by induction* given above did not use any induction hypothesis. And that is right. The proof is not really an induction but a simple case distinction. However, since it obviously has the shape of an induction, even reducing the problem to the lower case, I decided to leave it that way. Moreover this yields the fascinating observation that for radical matroids $\rho(R, S) = 0$ whenever S contains a loop which is not already contained in R.

In the first example given above the list $X = \{4, 6\}$ did not give an arithmetic matroid. Clearly 4 and 6 are not coprime. However, this is not the main reason why this list fails to induce an arithmetic matroid. Indeed it is easy to give an example of a list X that is not coprime, but satisfies positivity (P).

Example. Let $X = \{15, 21\}$. Then X is not coprime since $\gcd(15, 21) = 3$. However, one can compute that

$$\begin{aligned}
\rho(A, A) = \operatorname{rad}(A) \geq 0, \ \forall A \subseteq X, \\
\rho(\emptyset, \{15\}) = -1 + 15 = 14, \\
\rho(\emptyset, \{21\}) = -1 + 21 = 20, \\
\rho(\emptyset, \{15, 21\}) = 1 - 15 - 21 + 105 = 70 \\
\rho(\{15\}, \{15, 21\}) = -15 + 105 = 90 \\
\rho(\{21\}, \{15, 21\}) = -21 + 105 = 84.
\end{aligned}$$

Thus we checked that X really induces an arithmetic matroid even though it is not coprime.

We deduce that it is not a simple matter of being coprime or not that decides whether positivity works out. The following result states simple conditions to check, whether positivity fails and their proof will explain why.

Lemma 4.2.3. *Let $X = \{\alpha, x_1, \ldots, x_n\} \subseteq \mathbb{Q}^*$ be a list with $|\alpha| \neq 1$. Now if there exists a sublist $A \subseteq X \setminus \{\alpha\}$ such that*

- α *is independent of* A *and*
- $\mathrm{rad}(\alpha)$ *divides* $\mathrm{rad}(A)$,

then the resulting multiplicity matroid $\mathcal{M} = (X, \mathrm{rk}, \mathrm{rad})$ *is* ***not*** *arithmetic.*

Proof. Let $A = \{a_1, a_2, \ldots, a_k\} \subseteq X \setminus \{\alpha\}$ be minimal such that $\mathrm{rad}(\alpha) | \mathrm{rad}(A)$. I.e if $a \in A$ then $\mathrm{rad}(\alpha)$ does not divide $\mathrm{rad}(A \setminus \{a\})$. Now $|\alpha| \neq 1$ implies that A is not empty, hence there exists an $a_1 \in A$. Additionally, the minimality condition on A yields that $\mathrm{rad}(A \setminus \{a_1\}) \neq \mathrm{rad}(A)$. Therefore the element a_1 must introduce new primes to the radical, which tells us that a_1 is independent of A.

By all this we conclude that $[A \setminus \{a_1\}, A \cup \{\alpha\}]$ is a molecule with free set $F = \{a_1, \alpha\}$ and empty torsion set $T = \emptyset$. But for this molecule we compute

$$\begin{aligned}
\rho(A \setminus \{a_1\}, A \cup \{\alpha\}) &= (-1)^{|T|} \sum_{A \setminus \{a_1\} \subseteq C \subseteq A \cup \{\alpha\}} (-1)^{|A \cup \{\alpha\}| - |C|} \mathrm{rad}(C) \\
&= \mathrm{rad}(A \setminus \{a_1\}) - \mathrm{rad}(A) - \mathrm{rad}((A \cup \{\alpha\}) \setminus \{a_1\}) + \underbrace{\mathrm{rad}(A \cup \{\alpha\})}_{=\mathrm{rad}(A)} \\
&= \mathrm{rad}(A \setminus \{a_1\}) - \underbrace{\mathrm{rad}((A \cup \{\alpha\}) \setminus \{a_1\})}_{= l \cdot \mathrm{rad}(A \setminus \{a_1\})} < 0.
\end{aligned}$$

In the last line we used that α is independent of A and hence also independent of $A \setminus \{a_1\}$. In terms of multiplicities this yields that $\mathrm{rad}(A \setminus \{a_1\})$ divides $\mathrm{rad}((A \cup \{\alpha\}) \setminus \{a_1\})$. Moreover we cannot have equality because then we would get $\mathrm{rad}(\alpha) | \mathrm{rad}(A \setminus \{a_1\}) = \mathrm{rad}((A \cup \{\alpha\}) \setminus \{a_1\})$ which contradicts the minimality condition on A. Hence we have

$$\mathrm{rad}((A \cup \{\alpha\}) \setminus \{a_1\}) = l \cdot \mathrm{rad}(A \setminus \{a_1\})$$

for some integer $l \geq 2$ and thus the negativity stated above. Therefore we found a molecule not satisfying positivity. Hence $\mathcal{M}$ cannot be an arithmetic matroid. □

Remark. The lemma above applies to the example of $X = \{4, 6\}$, since 4 is independent of $\{6\}$ in the multiplicative $\mathbb{Z}$–lattice $\langle 2, 3 \rangle_{\mathbb{Z}}$ spanned by the underlying primes. However, we have that $\mathrm{rad}(4) = 2$ divides $6 = \mathrm{rad}(\{6\})$.

Remark. The independence condition in Lemma 4.2.3 is crucial. If we take $X = \{2, 4\}$ then the construction $[\emptyset, \{2, 4\}]$ from the proof of the lemma, is not a molecule. And indeed, since $\mathrm{rk}(X) = 1$, if we compute the multiplicity Tutte polynomial we get

$$\begin{aligned}
M(x, y) &= \sum_{A \subseteq X} \mathrm{rad}(A)(x-1)^{\mathrm{rk}(X) - \mathrm{rk}(A)}(y-1)^{|A| - \mathrm{rk}(A)} \\
&= \underbrace{(x-1)}_{A=\emptyset} + \underbrace{2}_{\{2\}} + \underbrace{2}_{\{4\}} + \underbrace{2(y-1)}_{\{2,4\}} \\
&= x + 2y + 1.
\end{aligned}$$

Also the division condition is necessary. We have already shown that $X = \{15, 21\}$ gives an arithmetic matroid out of a not-coprime list.

Remark. Examples suggest that a list $X \subseteq \mathbb{Q}^*$ induces an arithmetic matroid whenever Lemma 4.2.3 does not apply. This would then give an *if and only if* statement which fully characterises the family of arithmetic radical matroids in $\mathbb{Q}^*$. However, whether this statement is true or not is left as an open problem for the moment and may be content of further studies.

Our next topic will be the question on how to relate radical matroids with known examples of arithmetic matroids from other domains. Naturally this question refers mainly to arithmetic radical matroids and the crucial property, which one might ask for, is the one of representability.

4.2.2 Representable radical matroids

First things first, a radical matroid can only be representable if it fulfils positivity. Hence in this section we assume all our radical matroids to be arithmetic. Another crucial observation yields the following: Since we have in every radical matroid that $\mathrm{rad}(\emptyset) = 1$ we get the next statement trivially.

Corollary 4.2.4. *An arithmetic radical matroid $\mathcal{M} = (X, \mathrm{rk}, \mathrm{rad})$ is always torsion-free.*

This is easy to see, as soon as we remind ourselves that the definition of a torsion-free arithmetic matroid $(X, \mathrm{rk}, \mathfrak{m})$ simply demands $\mathfrak{m}(\emptyset) = 1$. We recall that a representable, torsion-free matroid $\mathcal{M} = (X, \mathrm{rk}, \mathfrak{m})$ already has to be GCD. I.e. its multiplicities satisfy the GCD-rule: $\forall A \subseteq X$:

$$\mathfrak{m}(A) = \gcd(\{\mathfrak{m}(B) \mid B \subseteq A \text{ and } |B| = \mathrm{rk}(B) = \mathrm{rk}(A)\}).$$

Hence the next question to ask would be whether arithmetic radical matroids fulfil this rule or not. Fortunately, we obtain the following result.

Proposition 4.2.5. *A radical matroid $\mathcal{M} = (X, \mathrm{rk}, \mathrm{rad})$ is always GCD.*

Proof. Let $\mathcal{M} = (X, \mathrm{rk}, \mathrm{rad})$ be a radical matroid and choose an arbitrary sublist $A \subseteq X$. Inside of A let B be a maximal rank sublist. I.e. $B \subseteq A$ with $|B| = \mathrm{rk}(B) = \mathrm{rk}(A)$. Now we recall that for $v \in A$, dependent on B, we have $\mathrm{rad}(B) = \mathrm{rad}(B \cup \{v\})$. (Remember this is true due the fact that v cannot contribute further prime elements without being independent.)

However, since every element of A is dependent on B because it is of maximal rank, we obtain that

$$\mathrm{rad}(A) = \mathrm{rad}(B).$$

Furthermore we conclude for any two maximal rank sublists B and B' in A we have

$$\mathrm{rad}(B) = \mathrm{rad}(B'),$$

and therefore we deduce that

$$\mathrm{rad}(A) = \mathrm{rad}(B) = \gcd(\{\mathrm{rad}(B') \mid B' \subseteq A \text{ and } |B'| = \mathrm{rk}(B') = \mathrm{rk}(A)\}).$$

Hence, since A was arbitrary, $\mathcal{M}$ is GCD. □

Remark. Note that the last proposition as well as its proof do also work in the more general case where X lies in the quotient field $\mathcal{Q}$ of a UFD $\mathcal{R}$.

To sum things up: we know that all our arithmetic radical matroids are torsion-free and GCD. This kind of suggests that all arithmetic radical matroids could also be representable. Unfortunately this is not the case. It turns out that only a special family of arithmetic radical matroids is representable. The next definition yields a hint, what to look for.

Definition. Let $X \subseteq \mathbb{Q}^*$ be a list defining a radical matroid. Then we call X *essentially coprime* if all independent sublists of X are coprime.

We will see that an arithmetic radical matroid is representable if and only if the defining list X is essentially coprime. To show this will be our next big achievement. Nevertheless to prove this assertion we need to further study the structure of arithmetic radical matroids. The one crucial thing we know is, that Lemma 4.2.3 from the last section may not apply to them. However, this already leads to strong conditions, that we summarise in the following corollary.

Corollary 4.2.6. *Let $X \subseteq \mathbb{Q}^*$ and let $\mathcal{M} = (X, \mathrm{rk}, \mathrm{rad})$ be the induced radical matroid. Assume that $\mathcal{M}$ is also an arithmetic matroid, then we have for any sublist $A \subseteq X$ and every element $v \in X$ that*

- *v is dependent on $A \iff \mathrm{rad}(v)$ divides $\mathrm{rad}(A) \iff \mathrm{rad}(A \cup \{v\}) = \mathrm{rad}(A)$.*
- *v is independent of $A \iff$ there exists a prime $p \in \mathbb{P}$ that divides $\mathrm{rad}(v)$ but does not divide $\mathrm{rad}(A)$.*

I.e. every independent element must contribute new primes to the radical.

Proof. The second equivalence of the first bullet point is always true. For the rest compare with Lemma 4.2.3. □

Remark. Recall that this was not true for the list $\{4, 6\}$. Here 4 was independent of $\{6\}$ but did not contribute new primes to its radical. Hence the resulting radical matroid could not be arithmetic. However, the list $\{2, 4\}$ indeed did yield an arithmetic radical matroid because 2 and 4 are dependent on each other.

We will use these observations to prove the main result of this section.

Theorem 4.2.7. *Let $X \subseteq \mathbb{Q}^*$ be a finite list of invertible rationals such that the resulting radical matroid $\mathcal{M} = (X, \mathrm{rk}, \mathrm{rad})$ is also an arithmetic matroid. Then $\mathcal{M}$ is representable* ***if and only if*** *X is essentially coprime.*

Proof. We prove the theorem by constructing an arithmetic matroid isomorphism ϕ between $\mathcal{M}$ and the canonical arithmetic matroid of some sublattice in $\mathbb{Z}^n$. Without loss of generality, we may assume that all of the elements in X are positive, since the multiplication with $-1 \in \mathbb{Z}^*$ neither changes the matroid structure nor the multiplicities on the sublists. Then, first of all we denote by $\mathbb{P}_X$ the set of primes that occur in any factorisation of any element of X. Equivalently, $\mathbb{P}_X$ is the set of prime factors of $\operatorname{rad}(X)$. Then, since X is finite, also $\mathbb{P}_X$ is finite. Fix a total order on $\mathbb{P}_X$, for example according to the total order in $\mathbb{Z}$, and write

$$\mathbb{P}_X = \{p_1, p_2, \dots, p_n\},$$

where all p_i are different and $p_i \leq p_j$ if $i \leq j$. Now every element $v \in X$ has a unique representation in terms of primes in $\mathbb{P}_X$:

$$v = \prod_{i=1}^{n} p_i^{v_i} = p_1^{v_1} \cdot \dots \cdot p_n^{v_n} \quad \text{with } v_i \in \mathbb{Z} \text{ for } i \in [n].$$

We obtain a bijection $v \leftrightarrow (v_1, v_2, \dots, v_n)$ and call $(v_1, v_2, \dots, v_n) \in \mathbb{Z}^n$ the *coordinate vector* of v in the prime-lattice.

We are now able to define our morphism $\phi : X \to Y \subseteq \mathbb{Z}^n$. Let $v \in X$ then we set

$$\phi(v) := \operatorname{rad}(v) \cdot (1 - \delta_{0,v_i})_{i=1}^{n},$$

where the vector $(1 - \delta_{0,v_i})_{i=1}^{n}$ is the vector whose i'th component is given by

$$1 - \delta_{0,v_i} = \begin{cases} 1 & \text{if } v_i \neq 0 \\ 0 & \text{if } v_i = 0. \end{cases}$$

In words you could say, to get $\phi(v)$ you put a 1 in each component, where the according prime is represented in the factorisation of v and a 0 for each prime that does not appear, and then you multiply everything by $\operatorname{rad}(v)$.

Note that ϕ is not injective in the classical set theoretic sense. For example if we have $X = \{2, 3, 5, 25\}$ then $\mathbb{P}_X = \{2, 3, 5\}$ so ϕ maps into $\mathbb{Z}^3$. We get that $\phi(2) = (2, 0, 0)$, $\phi(3) = (0, 3, 0)$, $\phi(5) = (0, 0, 5)$ but also $\phi(25) = (0, 0, 5)$. However, that does not matter since we are working with lists. Hence the image list would then be given by

$$Y = \left\{ \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 5 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 5 \end{pmatrix} \right\}.$$

Here we consider Y as a sublist of the lattice $\mathbb{Z}^3$. Thus we get a classical arithmetic matroid over a lattice. In this simple example one may already see that ϕ preserved both ranks and multiplicities of sublists. Nevertheless it remains to prove this in general. Let X again be arbitrary and essentially coprime. We need to show that for all $A \subseteq X$ we have $\operatorname{rk}_{\mathcal{M}}(A) = \operatorname{rk}_{\mathbb{Z}^n}(\phi(A))$ and also $\operatorname{rad}(A) = \mathfrak{m}(\phi(A))$. We start by showing that ϕ

preserves ranks.

We prove this by induction on the cardinality of A. For reasons of simplicity we will denote both $\mathrm{rk}_{\mathcal{M}}$ and $\mathrm{rk}_{\mathbb{Z}^n}$ by rk. It will be always clear from the context where we study our ranks. Then the assertion is clearly true for the empty set. For singletons $\{v\} \subseteq X$ we compute:

$v = 1$: Then $\mathrm{rk}(\{1\}) = 0 = \mathrm{rk}(\{\mathbf{0}\})$ where $\mathbf{0} = \phi(1)$ is the zero vector in $\mathbb{Z}^n$.

$v \neq 1$: Then $\mathrm{rk}(\{v\}) = 1$ but since then $\phi(v) \neq \mathbf{0}$ also $\mathrm{rk}(\phi(v)) = 1$.

Now assume that $|A| = k$ and ϕ preserves ranks for all lists $C \subseteq X$ with $|C| \leq k$. Take any $v \in X \setminus A$. We need to consider again two cases, whether v is independent of A or dependent on it. If $\phi(v)$ remains independent of $\phi(A)$ or dependent, respectively, then we know ϕ preserves also the rank of $A \cup \{v\}$.

Case 1: Let v be independent of A. Then we know by Corollary 4.2.6 that the factorisation of v includes a prime $p_j \in \mathbb{P}_X$ that is not included in any factorisation of elements of A. Then by construction of ϕ we have that the j'th component of $\phi(v)$ equals $\mathrm{rad}(v)$ while the j'th components of all elements in $\phi(A)$ must be zero. Thus $\phi(v)$ is independent of $\phi(A)$.

Case 2: Let v be dependent on A. If we add $\mathrm{rad}(v)$ to our list X, then $\mathcal{M}$ is simply the deletion of $(X \cup \{rad(v)\}, \mathrm{rk}, \mathrm{rad})$ by $\mathrm{rad}(v)$. Multiplicities and ranks stay the same. Therefore without loss of generality we can assume $\mathrm{rad}(v) \in X$ (even $v = \mathrm{rad}(v)$ is possible). Now v dependent on A implies $\mathrm{rad}(v)$ dependent on A and vice versa due to Corollary 4.2.6. However, we have $\phi(v) = \phi(\mathrm{rad}(v))$. Hence again w.l.o.g. we may assume that $v = \mathrm{rad}(v)$. In the same manner we can assume that $a = \mathrm{rad}(a)$ for all elements $a \in A$.

Now assume that $\phi(v)$ was independent of $\phi(A)$. Observe that by construction of ϕ we have that $\phi(v)$ is independent of $\phi(A)$ if and only if the coordinate vector $(v_1, \ldots, v_n)$ of v is dependent on the coordinate vectors $(a_1, \ldots, a_n)$ of the elements $a \in A$. This is true since $(v_1, \ldots, v_n) = (1 - \delta_{0,v_i})_{i=1}^n$ and also $(a_1, \ldots, a_n) = (1 - \delta_{0,a_i})_{i=1}^n$ for all $a \in A$ since we assumed $v = \mathrm{rad}(v)$ and $a = \mathrm{rad}(a)$. Eventually we remind that independence of the coordinate vectors translates directly to independence in $\mathcal{M}$, since the underlying matroid structure was induced by the multiplicative $\mathbb{Z}$–lattice of primes in $\mathbb{P}_X$ just by definition of radical matroids. Hence we would have v independent of A which yields the contradiction we were looking for.

Note that ϕ preserves ranks in any case, since we never used that X was essentially coprime. Finally we need to check if ϕ also preserves multiplicities if and only if X was essentially coprime.

For such an essentially coprime X also each sublist A is essentially coprime. The multiplicity $\mathfrak{m}(\phi(A))$ can then be computed as the GCD of all multiplicities of all maximal rank sublists $\phi(B)$ of $\phi(A)$, where also $B \subseteq A$ has full rank. However, $\mathfrak{m}(\phi(B))$ can be

calculated as the GCD of all full-rank-minors of $\phi(B)$ as a matrix. Now observe that all vectors of $\phi(B)$ are of the shape $\mathrm{rad}(v) \cdot (1 - \delta_{0,v_i})_{i=1}^{n},\ v \in B$. Hence if $\phi(B)'$ is a full-rank submatrix of $\phi(B)$, such that $\det(\phi(B)')$ gives such a minor, we may compute

$$\det(\phi(B)') = \prod_{v \in B} \mathrm{rad}(v) \det(\overline{\phi(B)}),$$

where $\overline{\phi(B)}$ is the matrix resulting from $\phi(B)'$ after we put every factor $\mathrm{rad}(v)$ outside using the multi-linearity of the determinant. Then $\overline{\phi(B)}$ has only values 1 or 0 and since we have full rank we deduce that $\det(\overline{\phi(B)}) = 1$ or -1.

Since X is essentially coprime, B is coprime and we deduce that

$$\prod_{v \in B} \mathrm{rad}(v) = \mathrm{rad}(B).$$

Now since all $w \in A$ are dependent on B we have $\mathrm{rad}(B) = \mathrm{rad}(A)$. Eventually we deduce that $\mathfrak{m}(\phi(A))$ is the GCD of multiplicities which are plus or minus $\mathrm{rad}(A)$. Therefore we have $\mathfrak{m}(\phi(A)) = \mathrm{rad}(A)$ as demanded. This proves that all arithmetic radical matroids defined upon essentially coprime lists are representable.

Finally it only remains to prove that the arithmetic radical matroid $\mathcal{M}$ is not representable if the underlying list X is not essentially coprime. This means there exist elements $v, w \in X$ independent of each other such that there is a prime p that divides both $\mathrm{rad}(v)$ and $\mathrm{rad}(w)$. Now we assume indirectly that there existed a morphism $\psi : X \to \mathbb{Z}^d$ that preserved both ranks and multiplicities ($d \in \mathbb{N}$ some dimension). First we observe that

$$\mathfrak{m}(\psi(v)) = \mathrm{rad}(v)$$

implies that $\mathrm{rad}(v) = \gcd(\{\psi(v)_i \mid i \in [d]\})$, due to the GCD rule. Here $\psi(v)_i$ just denotes the i'th component of the vector $\psi(v) \in \mathbb{Z}^d$. The same is true for $\psi(w)$, i.e $\mathrm{rad}(w) = \gcd(\{\psi(w)_i \mid i \in [d]\})$. Now we analyse the set $A = \{v, w\}$. All full-rank minors of $\psi(A) = (\psi(v), \psi(w))$ as a matrix include both nonzero entries of $\psi(v)$ and $\psi(w)$. Both columns of $\psi(A)$ are divisible by the prime p, hence each full-rank minor is divisible by p^2. Therefore again by the GCD rule we have that p^2 must divide $\mathfrak{m}(\psi(A))$. However, clearly p^2 cannot divide $\mathrm{rad}(A)$. Thus

$$\mathfrak{m}(\psi(A)) \neq \mathrm{rad}(A)$$

and therefore the radical arithmetic matroid cannot be representable. □

Remark. If X is essentially coprime, then we could choose an arbitrary basis $B = \{b_1, \ldots, b_r\}$, where $r = \mathrm{rk}(X)$. Using the second basis axiom (B2) and Corollary 4.2.6 we deduce that for every other basis B' there exists an ordering of its elements $B' = \{b'_1, \ldots, b'_r\}$ such that

$$\mathrm{rad}(b_i) = \mathrm{rad}(b'_i), \text{ for all } i \in [r].$$

Moreover for every proper vector $v \in X$ we have exactly one $j \in [r]$ such that $\mathrm{rad}(v) =$

$\mathrm{rad}(b_j)$ and therefore v is dependent on b_j. With this in mind we can find a simpler morphism $\theta : X \to \mathbb{Z}^r$ with

$$\theta(v) := (\mathrm{rad}(b_j) \cdot \delta_{j,i})_{i=1}^{r},$$

where again $\delta_{j,i}$ denotes the *Kronecker-delta*. One can then show again that θ preserves both ranks and multiplicities.

Observe that X being essentially coprime prohibits that we get into the situation of Lemma 4.2.3. For, if $\alpha \in X$ is independent of some sublist $A \subseteq X$, then α is also independent of a maximal independent sublist $B \subseteq A$. Therefore $\mathrm{rad}(\alpha)$ and $\mathrm{rad}(B) = \mathrm{rad}(A)$ are coprime since X was essentially coprime. Therefore α could never divide $\mathrm{rad}(A)$. Using this, we also get the following corollary immediately from the proof of Theorem 4.2.7.

Corollary 4.2.8. *Let $\mathcal{M}$ be a radical matroid that is defined upon a list X which is essentially coprime. Then $\mathcal{M}$ is an arithmetic radical matroid.*

Proof. In this situation we get by $\phi : X \to \mathbb{Z}^n$ an isomorphism between $\mathcal{M}$ and an arithmetic matroid in $\mathbb{Z}^n$. Hence $\mathcal{M}$ has to be arithmetic itself. □

This is another minor step towards the full characterisation of all arithmetic radical matroids. Another interesting conclusion from Theorem 4.2.7 is that there are arithmetic radical matroids that are not representable.

Example. We have already seen that $X = \{15, 21\}$ gives an arithmetic matroid. However, it is not essentially coprime. This tells us that we have constructed an example of an arithmetic matroid which is torsion-free, GCD, but *not representable*.

By this we conclude that we have found a new class of arithmetic matroids that exists independent of the representable ones.

4.3 Final comments

The combinatorial relevance of radical matroids remains uncertain. For example the interpretation of special values of the arithmetic Tutte polynomial could be content of future studies. However, the concept of radical matroids opens a new application of arithmetic matroid theory inside the realms of number theory. Matroid theory in general is a science of connecting mathematical structures living in (a priori) very unfamiliar domains. Now we are able to associate arithmetic matroids to a large class of lists of rational numbers. This may enable us to further use methods from geometry and graph theory on number theoretical questions.

Especially the radical function arises in the original formulation of the so-called *abc-conjecture*, whose verification would have a strong connection to Fermat's last theorem (compare with [Lan93] or [Oes88]).

Definition ((Masser, Oesterle, 1986) or [Lan93, p. 95])**.** A so-called *abc-triple* is a triple of positive integers $a, b, c \in \mathbb{N}$, where a and b are coprime and $c = a + b$. Then clearly the whole set $\{a, b, c\}$ is coprime.

In its classical form, the *abc*-conjecture is then formulated in the following way.

Conjecture 4.3.1. *For all real $\epsilon > 0$ there exists a $K_\epsilon \in \mathbb{R}$ such that for each abc-triple we have*

$$c < K_\epsilon\big(\operatorname{rad}(abc)\big)^{1+\epsilon}.$$

Now since for every *abc*-triple the set $X = \{a, b, c\}$ is coprime, we obtain an arithmetic radical matroid $\mathcal{M} = (X, \mathrm{rk}, \mathrm{rad})$. For this we calculate its arithmetic Tutte polynomial (observing $|A| = \mathrm{rk}(A)$ for all $A \subseteq X$):

$$\begin{aligned} M_{abc}(x, y) &= \sum_{A \subseteq \{a,b,c\}} \operatorname{rad}(A)(x-1)^{\mathrm{rk}(X)-\mathrm{rk}(A)}(y-1)^{|A|-\mathrm{rk}(A)} \\ &= (x-1)^3 + (\operatorname{rad}(a) + \operatorname{rad}(b) + \operatorname{rad}(c))(x-1)^2 + \\ &\quad + (\operatorname{rad}(ab) + \operatorname{rad}(ac) + \operatorname{rad}(bc))(x-1) + \operatorname{rad}(abc). \end{aligned}$$

Therefore $\operatorname{rad}(abc) = \operatorname{rad}(X) = M_{abc}(1, y)$. In particular we have $\operatorname{rad}(abc) = M_{abc}(1, 1)$ and $M_{abc}(1, 1)$ is equal to the volume of the zonotope spanned by the representation $\phi(X)$ of $\mathcal{M} = (X, \mathrm{rk}, \mathrm{rad})$. This yields just another small link of this famous conjecture into the realms of geometry.

However, this concludes our study of arithmetic matroids and their arithmetic Tutte polynomials. Its a fascinating field of research with inexhaustible possibilities for applications. Other multiplicities will give other specialisations of the arithmetic Tutte polynomial and therefore we await a rich and fruitful series of results to be discovered in the future.

Bibliography

[BHHL11] Christian Bey, Martin Henk, Matthias Henze, and Eva Linke. Notes on lattice points of zonotopes and lattice-face polytopes. *Discrete Math.*, 311(8-9):634–644, 2011.

[Bj2] Anders Björner. The homology and shellability of matroids and geometric lattices. In *Matroid applications*, volume 40 of *Encyclopedia Math. Appl.*, pages 226–283. Cambridge Univ. Press, Cambridge, 1992.

[BL20] Spencer Backman and Matthias Lenz. A convolution formula for Tutte polynomials of arithmetic matroids and other combinatorial structures. *Sém. Lothar. Combin.*, 78:Art. B78c, 17, [2018–2020].

[BM14] Petter Brändén and Luca Moci. The multivariate arithmetic Tutte polynomial. *Trans. Amer. Math. Soc.*, 366(10):5523–5540, 2014.

[BR15] Matthias Beck and Sinai Robins. *Computing the continuous discretely.* Undergraduate Texts in Mathematics. Springer, New York, second edition, 2015. Integer-point enumeration in polyhedra, With illustrations by David Austin.

[Cra69] Henry H. Crapo. The tutte polynomial. *Aequationes Math.*, 3:211–229, 1969.

[DM12] Michele D'Adderio and Luca Moci. Ehrhart polynomial and arithmetic Tutte polynomial. *European J. Combin.*, 33(7):1479–1483, 2012.

[DM13] Michele D'Adderio and Luca Moci. Graph colorings, flows and arithmetic Tutte polynomial. *J. Combin. Theory Ser. A*, 120(1):11–27, 2013.

[DM16] Emanuele Delucchi and Luca Moci. Colorings and flows on cw complexes, tutte quasi-polynomials and arithmetic matroids, 2016.

[Ehr62] Eugène Ehrhart. Sur les polyèdres rationnels homothétiques à n dimensions. *C. R. Acad. Sci. Paris*, 254:616–618, 1962.

[FM16] Alex Fink and Luca Moci. Matroids over a ring. *J. Eur. Math. Soc. (JEMS)*, 18(4):681–731, 2016.

[GS96] Ira M. Gessel and Bruce E. Sagan. The tutte polynomial of a graph, depth-first search, and simplicial complex partitions. volume 3, pages Research Paper 9, approx. 36. 1996. The Foata Festschrift.

[KM17] Christian Karpfinger and Kurt Meyberg. *Algebra*. Springer Spektrum Berlin, Heidelberg, fourth edition, 2017.

[KRS99] Woong Kook, Victor Reiner, and Dennis W. Stanton. A convolution formula for the Tutte polynomial. *J. Combin. Theory Ser. B*, 76(2):297–300, 1999.

[Lan93] Serge Lang. Die abc-vermutung. *Elemente der Mathematik*, 48:89–99, 1993.

[LS11] Jeffrey C. Lagarias and Kannan Soundararajan. Smooth solutions to the *abc* equation: the *xyz* conjecture. *J. Théor. Nombres Bordeaux*, 23(1):209–234, 2011.

[LTY21] Ye Liu, Tan Nhat Tran, and Masahiko Yoshinaga. *G*-Tutte polynomials and abelian Lie group arrangements. *Int. Math. Res. Not. IMRN*, (1):152–190, 2021.

[MD12] Luca Moci and Michele D'Adderio. Arithmetic matroids, the tutte polynomial and toric arrangements. *Advances in Mathematics*, 2012.

[Moc11] Luca Moci. A tutte polynomial for toric arrangements. *Transactions of the mathematical society*, 2011.

[Oes88] Joseph Oesterlé. Nouvelles approches du "théorème" de Fermat. Number 161-162, pages Exp. No. 694, 4, 165–186. 1988. Séminaire Bourbaki, Vol. 1987/88.

[Oxl92] James G. Oxley. *Matroid Theory*. Oxford University Press, New York, first edition, 1992.

[Pag20] Roberto Pagaria. Orientable arithmetic matroids. *Discrete Math.*, 343(6):111872, 8, 2020.

[She74] Geoffrey C. Shephard. Combinatorial properties of associated zonotopes. *Canadian J. Math.*, 26:302–321, 1974.

[Sok05] Alan D. Sokal. The multivariate Tutte polynomial (alias Potts model) for graphs and matroids. In *Surveys in combinatorics 2005*, volume 327 of *London Math. Soc. Lecture Note Ser.*, pages 173–226. Cambridge Univ. Press, Cambridge, 2005.

[Sta97] Richard P. Stanley. *Enumerative combinatorics. Vol. 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997. With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.

[Tut54] William T. Tutte. A contribution to the theory of chromatic polynomials. *Canad. J. Math.*, 1954.