Inhaltsverzeichnis

0 Einleitung

Diese Arbeit beruht auf dem Artikel *Arithmetic Matroids, Tutte Polynomial and Toric Arrangements* von Michele D'Adderio und Luca Moci (siehe [1]).

Wir führen den Begriff des arithmetischen Matroids ein und betrachten dabei vor allem arithmetische Matroide, die über endlich erzeugte, abelsche Gruppen gebildet werden. Wir werden arithmetische Matroide dabei über Mengen bilden. In [1] wird in einem arithmetischen Matroid $\mathfrak{M}_X$ stattdessen X als Liste gefordert. Eine Liste kann dabei aufgefasst werden als eine indizierte Multimenge, also als Menge $X = \{(x_i, i) \mid i \in I\}$ für eine Menge I. In dieser Schreibweise entsprechen dann die in [1] beschriebenen Operationen Durchschnitt, Vereinigung und Komplementbildung von Teillisten von X den entsprechenden mengentheoretischen Operationen. Unsere Definitionen und die aus [1] sind dann bezüglich Rang- und Vielfachheitsfunktion analog, siehe dazu Bemerkung 2.3.3 (ii). Inwiefern die Axiome (3), (4) und (5) arithmetischer Matroide über Listen mit unseren Axiomen (m3), (m4) und (m5) zusammenhängen, wird in dieser Arbeit nicht genauer untersucht.

Ziel dieser Arbeit ist es, Definitionen im Hinblick auf die *Darstellbarkeit* arithmetischer Matroide zu finden, die ohne die Verwendung von Listen auskommen, sondern intuitiver über Mengen gebildet werden. Dies soll möglichst analog zu den Definitionen in [1] geschehen.

Es gibt viele äquivalente Möglichkeiten, Matroide zu definieren. In Kapitel 1 geben wir zwei für uns nützliche Definitionen von Matroiden sowie weitere elementare Definitionen an und untersuchen einige Eigenschaften. Wir werden die Begriffe des *Matroide-Homomorphismus* und der Darstellbarkeit von Matroiden definieren, um diese später für arithmetische Matroide zu konkretisieren.

In Kapitel 2 definieren wir den Begriff des arithmetischen Matroids und dessen Duals über (endliche) Mengen. Duale arithmetischer Matroide sind bei uns zentrales Instrument für einige wichtige Beweise. Wir definieren weiter den Begriff des *Arithmetischen-Matroide-Homomorphismus* (kurz: *AM-H*) und zeigen, dass die Axiome (m1) bis (m4) „rückwärts" vererbt werden.

Alle Untersuchungen bis dort hin treffen wir in Hinblick auf Abschnitt 2.3, in dem wir die *Dargestelltheit* und Darstellbarkeit zunächst von Tripeln (X, rk, m) definieren, um dann zu zeigen, dass dargestellte Tripel tatsächlich arithmetische Matroide sind und darstellbare Tripel (m1) bis (m4) erfüllen. Ein *darstellbares arithmetisches Matroid* definieren wir dann einfach als ein darstellbares Tripel, das ein arithmetisches Matroid ist.

In Kapitel 4 beenden wir den Beweis, dass dargestellte Tripel arithmetische Matroide sind und befassen uns hierzu mit der Geometrie dargestellter Tripel.

Die natürlichen Zahlen beinhalten bei uns die Null.

1 Matroide

Zunächst geben wir eine Definition von Matroiden an und betrachten einige Eigenschaften.

Definition 1.0.1. Ein *Matroid* $\mathfrak{M} = \mathfrak{M}_X = (X, \mathcal{I})$ ist eine Menge X von *Elementen* des Matroids mit einer Menge *unabhängiger Teilmengen* $\mathcal{I} \subseteq \mathbb{P}(X)$, die folgende Axiome erfüllt:

(I1) die leere Menge ist unabhängig:

$\emptyset \in \mathcal{I}$,

(I2) jede Teilmenge einer unabhängigen Menge ist wieder unabhängig:

$\forall A \in \mathbb{P}(X) \forall I \in \mathcal{I} : A \subseteq I \Rightarrow A \in \mathcal{I}$,

(I3) seien I und J zwei unabhängige Teilmengen von X und I habe mehr Elemente als J, dann gibt es ein $i \in I \backslash J$ mit $J \cup \{i\}$ unabhängig:

$\forall I, J \in \mathcal{I} : (|I| > |J| \Rightarrow \exists i \in I \backslash J : J \cup \{i\} \in \mathcal{I})$,

(I4) es gibt eine obere Schranke für die Kardinalität der unabhängigen Mengen:

$\exists n \in \mathbb{N} \forall I \in \mathcal{I} : |I| \leq n$.

Jede maximale unabhängige Teilmenge von X heißt *Basis*. Die Menge aller Basen bezeichnen wir mit $\mathcal{B}$.

Mit (I3) haben alle Basen gleich viele Elemente. Damit ist jedes Matroid durch die Menge seiner Basen eindeutig bestimmt: die unabhängigen Mengen sind genau die Basen und alle ihre Teilmengen.

Wir betrachten nur Matroide mit endlich vielen Elementen, womit (I4) nicht zu beachten ist. Sofern nicht anders angegeben, sei in diesem Kapitel stets $(X, \mathcal{I})$ ein Matroid (und X endlich).

Beispiel 1.0.2. (i) Für jede beliebige (endliche) Menge X und jede natürliche Zahl n ist $(X, \{A \subseteq X \mid |A| \leq n\})$ ein Matroid. Insbesondere auch $(X, \emptyset)$ und $(X, \mathbb{P}(X))$.

(ii) Für $X \subseteq V$ mit V Vektorraum ist $(X, \mathcal{I})$ mit

$$\mathcal{I} = \{I \subseteq X \mid I \text{ ist linear unabhängig } \}$$

ein Matroid.

(iii) Sei $X \subseteq G$ mit G endliche Gruppe und

$$\mathcal{I} = \{I \subseteq X \mid \forall g, h \in I, n \in \mathbb{N} : g \neq h^n \vee g = h\}$$

die Menge der Mengen, deren einelementige Teilmengen zyklische Untergruppen von G erzeugen, in deren Schnitt paarweise nur das neutrale Element liegt. Beachte, dass keine Menge aus $\mathcal{I}$ das neutrale Element enthält. Im Allgemeinen ist (X, I) kein Matroid:

(I1) und (I2) gelten per Definition.

Zu (I3): Seien $g \in X \backslash \{e\}$, p und q Primzahlen mit $|g| = p \cdot q$. Dann gibt es $h, k \in \langle g \rangle$ mit $|h| = p$ und $|k| = q$. Gibt es nun $n, m \in \mathbb{N}$ mit $e \neq h^n \in X$ und $e \neq k^m \in X$, so sind $\{g\}$ und $\{h^n, k^m\}$ unabhängige Mengen, aber weder $\{g, h^n\}$ noch $\{g, k^m\}$ ist unabhängig, also gilt (I3) in diesem Fall nicht.

Ein Beispiel, in dem (X, I) mit diesen Definitionen ein Matroid ist, ist $X = S_3$, die Gruppe der Permutationen auf $\{1, 2, 3\}$.

Ein Beispiel, in dem (X, I) mit diesen Definitionen kein Matroid ist, ist $X = S_4$. Allerdings erhalten wir mit $X = \{(12), (13)(24), (1234)\} \subseteq S_4$ ebenfalls ein Matroid.

Lemma 1.0.3. *Seien I und J zwei unabhängige Teilmengen von X und I habe mehr Elemente als J. Dann gibt es ein $K \subseteq I \backslash J$ mit $J \cup K$ unabhängig und $|J \cup K| = |I|$.*

Beweis. Folgt direkt aus der $(|J| - |I|)$-maligen Anwendung von (I3). $\square$

Definition 1.0.4. Jedes Matroid $(X, \mathcal{I})$ besitzt eine *Rangfunktion*:

$$\begin{aligned} rang\colon \mathbb{P}(X) &\to \mathbb{N}_0 \\ A &\mapsto \max\{|I| \mid I \subseteq A,\ I \in \mathcal{I}\} \end{aligned}$$

Bemerkung 1.0.5. (i) Mit (I4) ist die Rangfunktion beschränkt.

(ii) Ist I eine unabhängige Teilmenge von $A \subseteq X$, so ist nach obiger Definition $|I| \leq rang(A)$.

(iii) Für eine beliebige Teilmenge A von X gilt $rang(A) = |A|$ genau dann, wenn A unabhängig ist.

1.1 Die Rangfunktion eines Matroids

Wir können ein Matroid alternativ über die Rangfunktion definieren, was für uns oft nützlicher ist. In diesem Abschnitt geben wir zunächst die alternative Definition an und betrachten einige Eigenschaften. Dann beweisen wir die Äquivalenz beider Beschreibungen.

Definition/Satz 1.1.1. Ein Matroid $\mathfrak{M} = \mathfrak{M}_X = (X, rk)$ ist eine Menge X von *Elementen* des Matroids mit einer Funktion $rk : \mathbb{P}(X) \to \mathbb{N}$, die folgende Axiome erfüllt:

(rk1) $A \subseteq X \Rightarrow rk(A) \leq |A|$,

(rk2) $A \subseteq B \subseteq X \Rightarrow rk(A) \leq rk(B)$,

(rk3) $A, B \subseteq X \Rightarrow rk(A \cup B) + rk(A \cap B) \leq rk(A) + rk(B)$,

(rk4) rk ist beschränkt.

Sofern nicht anders angegeben, sei in diesem Kapitel stets (X, rk) ein Matroid.

Bemerkung. Da wir nur endliche Mengen betrachten, ist $\mathbb{P}(X)$ endlich und (rk4) bei uns immer erfüllt.

Lemma 1.1.2. *Die Funktion rk ist subadditiv.*

Beweis. Für alle $A, B \subseteq X$ gilt nach (rk3):

$$rk(A \cup B) \leq rk(A) + rk(B) - rk(A \cap B) \leq rk(A) + rk(B) \qquad \square$$

Definition 1.1.3. Für $A \subseteq X$ sagen wir $x \in X$ ist *abhängig* von A, falls $rk(A \cup \{x\}) = rk(A)$ und *unabhängig* von A, falls $rk(A \cup \{x\}) = rk(A) + 1$.

Bemerkung 1.1.4. (i) Wegen der Subadditivität von rk und $rk(\{x\}) \leq |\{x\}| = 1$ erfüllt jedes $x \in X$ bezüglich einer beliebigen Menge $A \subseteq X$ immer genau eine von beiden Eigenschaften.

(ii) Ist $x \in A \subseteq X$, so ist $rk(A \cup \{x\}) = rk(A)$, also x abhängig von A. Damit gilt auch:

(iii) Ist $x \in X$ unabhängig von $A \subseteq X$ so ist $x \notin A$.

Lemma 1.1.5. *(i) Ist $x \in X$ abhängig von $A \subseteq X$, dann ist x auch abhängig von jeder Obermenge $B \subseteq X$ von A.*

(ii) Ist $x \in X$ unabhängig von $A \subseteq X$, dann ist x auch unabhängig von jeder Teilmenge $B \subseteq X$ von A.

Beweis. (i) Sei $x \in X$ abhängig von $A \subseteq B \subseteq X$.

Ist $x \in B$ so ist x schon abhängig von B nach Bemerkung 1.1.4 (i). Sei also $x \notin B$. Dann ist

$$\begin{aligned} rk(B \cup \{x\}) + rk(A) &\leq rk(B) + rk(A \cup \{x\}) && \text{nach (rk3)} \\ &= rk(B) + rk(A) && \text{da } x \text{ abhängig von } A \\ &\leq rk(B \cup \{x\}) + rk(A) && \text{nach (rk2)} \end{aligned}$$

und damit $rk(B \cup \{x\}) \leq rk(B) \leq rk(B \cup \{x\})$, also $rk(B \cup \{x\}) = rk(B)$. □

(ii) Beweis durch Widerspruch:

Sei $x \in X$ unabhängig von $A \subseteq X$ (insbesondere $x \notin A$ nach Bemerkung 1.1.4 (iii)) und $B \subseteq A$ so, dass x abhängig von B ist. Dann ist

$$\begin{aligned} rk(A) + rk(B) &= rk(A) + rk(B \cup \{x\}) && \text{da } x \text{ abhängig von } B \\ &\geq rk(A \cup \{x\}) + rk(B) && \text{nach (rk3)} \\ &= rk(A) + 1 + rk(B) \; \lightning && \text{da } x \text{ unabhängig von } A. \end{aligned}$$

□

Lemma 1.1.6. *Sei $A \subseteq B \subseteq X$ und seien alle $x \in B \setminus A$ abhängig von A. Dann gilt für alle $C \subseteq B \setminus A$, dass $rk(C \cup A) = rk(A)$. Insbesondere ist dann $rk(B) = rk(A)$.*

Beweis. Wir zeigen die Behauptung mittels Induktion über die Kardinalität von C.

Induktionsanfang: Für $|C| = 0$ gilt $rk(C \cup A) = rk(\emptyset \cup A) = rk(A)$.

Induktionsvorraussetzung: Für ein $n \in \mathbb{N}$, $n < |B \setminus A|$ und für alle $C \subseteq B \setminus A$ mit $|C| = n$ gelte, dass $rk(C \cup A) = rk(A)$.

Induktionsschritt: Sei $C \subseteq B \setminus A$ mit $|C| = n + 1$ Dann ist $C = (C \setminus \{x\}) \cup \{x\}$ für ein beliebiges $x \in C$. Nach Voraussetzung ist x abhängig von A und nach Lemma 1.1.5 ist x dann auch abhängig von $(C \setminus \{x\}) \cup A$. Mit Induktionsvoraussetzung haben wir dann:

$$rk(A) = rk((C \setminus \{x\}) \cup A) = rk((C \setminus \{x\}) \cup A \cup \{x\}) = rk(C \cup A).$$

□

Theorem 1.1.7. *Sei $(X, \mathcal{I})$ ein Matroid nach Definition 1.0.1 und rk dessen Rangfunktion nach Definition 1.0.4. Dann ist (X, rk) ein Matroid nach Definition 1.1.1.*

Sei (X, rk) ein Matroid nach Definition 1.1.1, und $\mathcal{I}$ sei die Menge, die genau die Teilmengen A von X mit $rk(A) = |A|$ enthält. Dann ist $(X, \mathcal{I})$ ein Matroid nach Definition 1.0.1 und rk ist dessen Rangfunktion.

Beweis. Sei zunächst $(X, \mathcal{I})$ ein Matroid wie in Definition 1.0.1 und rk definiert als dessen Rangfunktion.

(rk1): Für alle Teilmengen A von X ist $rk(A) \leq |A|$ nach Definition von rk. ✓

(rk2): Sei $A \subseteq B \subseteq X$ und sei $I \subseteq A$ mit $I \in \mathcal{I}$ und $|I| = rk(A)$. Dann ist insbesondere $I \subseteq B$, also $rk(A) = |I| \leq rk(B)$ nach Bemerkung 1.0.5 (ii). ✓

(rk3): Sei $A, B \subseteq X$. Wähle $I, J \in \mathcal{I}$ so, dass

$$I \subseteq A \cup B,\ |I| = rk(A \cup B), \tag{1}$$

$$J \subseteq A \cap B,\ |J| = rk(A \cap B)$$

$$\text{und } I \cap A \cap B \text{ maximal unter diesen Voraussetzungen.} \tag{2}$$

Es ist $I \cap A \cap B \in \mathcal{I}$ als Teilmenge von $I \in \mathcal{I}$ nach (I1) und
$I \cap A \cap B \subseteq A \cap B$, also gilt mit Bemerkung 1.0.5 (ii):

$$|I \cap A \cap B| \leq rk(A \cap B)$$

Wir zeigen durch Widerspruch, dass Gleichheit gelten muss:

Sei $|I \cap A \cap B| < rk(A \cap B) = |J|$. Dann gibt es nach (I3) ein $j \in J \backslash (I \cap A \cap B)$ so, dass $(I \cap A \cap B) \cup \{j\}$ unabhängig ist. Nach Lemma 1.0.3 gibt es weiter ein $C \subseteq I \backslash ((I \cap A \cap B) \cup \{j\})$ mit

$$\begin{aligned} \widetilde{I} &:= C \cup ((I \cap A \cap B) \cup \{j\}) \in \mathcal{I} \\ \text{und } |\widetilde{I}| &= |I| = rk(A \cup B). \end{aligned}$$

Es ist $\widetilde{I} \subseteq A \cup B$, also gilt (1) mit I ersetzt durch $\widetilde{I}$. Weiter ist

$$|\widetilde{I} \cap A \cap B| = |(I \cap A \cap B) \cup \{j\}| > |I \cap A \cap B|.$$

Damit haben wir insgesamt einen Widerspruch zu (2).

Es muss also $|I \cap A \cap B| = |J|$ gelten. Dann folgt:

$$\begin{aligned} rk(A \cup B) + rk(A \cap B) &= |I| + |J| \\ &= |I| + |I \cap A \cap B| \\ &= |I \cap A| + |I \backslash A| + |I \cap A \cap B| \\ &= |I \cap A| + |(I \backslash A) \cup (I \cap A \cap B)| \\ &= |I \cap A| + |I \cap B| && \text{da } I \subseteq A \cup B \\ &\leq rk(A) + rk(B). && \checkmark \end{aligned}$$

Die letzte Ungleichung folgt mit Bemerkung 1.0.5 (ii), da $I \cap A$ und $I \cap B$ unabhängig nach (I1).

Mit (rk1), (rk2) und (rk3) ist (X, rk) ein Matroid nach 1.1.1. □

Sei nun (X, rk) ein Matroid wie in Definition 1.1.1 und $\mathcal{I} := \{A \subseteq X \mid rk(A) = |A|\}$.

(I1): Nach (rk1) ist $rk(\emptyset) \leq |\emptyset| = 0$, also $rk(\emptyset) = 0$, da rk nicht-negativ. Damit ist nach Definition $\emptyset \in \mathcal{I}$. ✓

(I2): Sei A Teilmenge einer Menge $I \in \mathcal{I}$. Dann ist

$$\begin{aligned} |A| &= |I| - |I \backslash A| \\ &= rk(I) - |I \backslash A| \\ &\leq rk(I) - rk(|I \backslash A|) && \text{nach (rk1)} \\ &= rk(I) + rk(A) - (rk(I \backslash A) + rk(A)) \\ &\leq rk(I) + rk(A) - (rk(A \cup (I \backslash A)) + rk(A \cap (I \backslash A))) && \text{nach (rk3)} \\ &= rk(I) + rk(A) - (rk(I) + rk(\emptyset)) \\ &= rk(A) \\ &\leq |A| && \text{nach (rk1),} \end{aligned}$$

also insgesamt $|A| \leq rk(A) \leq |A|$ und damit $|A| = rk(A)$, also $A \in \mathcal{I}$. ✓

(I3): Seien $I, J \in \mathcal{I}$ mit $|I| > |J|$ Nach Bemerkung 1.1.4 (i) ist jedes $x \in I \backslash J$ entweder abhängig oder unabhängig von J. Wären alle $x \in I \backslash J$ abhängig von J, dann hätten wir mit Lemma 1.1.6:

$$|I| = rk(I) = rk(J) = |J|,$$

ein Widerspruch zur Annahme $|I| > |J|$. Es muss also ein $x \in I \backslash J$ geben, das unabhängig von J ist. Für so ein x gilt dann:

$$rk(J \cup \{x\}) = rk(J) + 1 = |J| + 1 = |J \cup \{x\}|,$$

das heißt $J \cup \{x\} \in \mathcal{I}$. ✓

Mit (I1), (I2) und (I3) ist $(X, \mathcal{I})$ ein Matroid nach Definition 1.0.1. Bleibt zu zeigen, dass rk gleich der Rangfunkion $rang$ von $(X, \mathcal{I})$ ist.

Sei $A \subseteq X$ beliebig. Es ist

$$\begin{aligned} rang(A) &= \max\{|I| \mid I \in \mathcal{I}, I \subseteq A\} \\ &= \max\{rk(I) \mid I \in \mathcal{I}, I \subseteq A\} && \text{nach obigem Beweis.} \end{aligned}$$

Sei also $rang(A) = rk(I)$ für eine unabhängige Teilmenge $I \subseteq A$. Dann sind alle $x \in A \backslash I$ abhängig von I, denn sonst wäre $I \cup \{x\}$ unabhängige Teilmenge von A mit $|I \cup \{x\}| > |I|$. Mit Lemma 1.1.6 folgt:

$$rk(A) = rk(I) = rang(A).$$

Da $A \subseteq X$ beliebig war, folgt $rk = rang$. □

Bemerkung. Wir nennen die Rangfunktion von nun an rk und unterscheiden entsprechend Theorem 1.1.7 nicht zwischen Matroiden $(X, \mathcal{I})$ und Matroiden (X, rk).

Insbesondere gilt für alle Teilmengen A von X und alle unabhängigen Teilmengen I von A:

$$rk(A) = |I| \Leftrightarrow I \text{ ist maximale unabhängige Teilmenge von } A.$$

Lemma 1.1.8. *Ist $x \in X$ abhängig von $A \subseteq X$, dann ist x auch abhängig von jeder maximalen unabhängigen Teilmenge I von A.*

Beweis. Beweis durch Widerspruch:

Sei $x \in X$ abhängig von $A \subseteq X$ (insbesondere $x \notin A$ nach Bemerkung 1.1.4 (iii)) und I maximale unabhängige Teilmenge von A also $rk(A) = |I|$ nach Theorem 1.1.7. Sei weiter x unabhängig von I, also

$$rk(I \cup \{x\}) = rk(I) + 1 = |I| + 1.$$

Wieder nach Theorem 1.1.7 ist $I \cup \{x\}$ dann unabhängig. Es folgt:

$$\begin{aligned} |I| &= rk(A) \\ &= rk(A \cup \{x\}) && \text{da } x \text{ abhängig von } A \\ &= \max\{|J| \mid J \subseteq A \cup \{x\},\ J \in \mathcal{I}\} \\ &\geq |I \cup \{x\}|. \end{aligned}$$

Ein Widerspruch. □

1.2 Das Dual eines Matroids

Wir definieren das Dual eines Matroids und zeigen, dass dieses selbst ein Matroid ist. Für den Beweis benutzen wir folgendes Lemma:

Lemma 1.2.1. *Die Rangfunktion rk eines Matroids lässt sich schreiben als*

$$\begin{aligned} rk\colon \mathbb{P}(X) &\to \mathbb{N} \\ A &\mapsto \max\{|A \cap B| \mid B \in \mathcal{B}\}, \end{aligned}$$

wobei $\mathcal{B}$ wie angegeben die Menge der Basen des Matroids bezeichnet. Damit ist insbesondere $rk(X) = |B|$ für jede Basis B.

Beweis. Sei $A \subseteq X$ beliebig. Wir zeigen zwei Ungleichungen:
Sei $\widetilde{B}$ eine Basis mit $|A \cap \widetilde{B}| = \max\{|A \cap B| \mid B \in \mathcal{B}\}$. Mit (I2) und $\widetilde{B}$ unabhängig ist auch $A \cap \widetilde{B}$ unabhängig. Außerdem ist $A \cap \widetilde{B} \subseteq A$, also folgt mit Bemerkung 1.0.5 (ii):

$$\max\{|A \cap B| \mid B \in \mathcal{B}\} = |A \cap \widetilde{B}| \leq rk(A).$$

Sei nun $B \in \mathcal{B}$ beliebige Basis und $I \subseteq A$ unabhängig mit $rk(A) = |I|$. Nach Lemma 1.0.3 gibt es ein $K \in B \backslash I$ mit $I \cup K$ unabhängig und $|I \cup K| = |B|$, das heißt $I \cup K$ ist eine Basis. Dann ist weiter

$$\begin{aligned} |I| &\leq |A \cap (I \cup K)| && \text{da } I \subseteq A \\ &= rk(A \cap (I \cup K)) && \text{da } A \cap (I \cup K) \in \mathcal{I} \text{ nach (I2)} \\ &\leq rk(A) && \text{nach (rk2)} \\ &= |I|, \end{aligned}$$

also $rk(A) = |A \cap (I \cup K)|$ und damit

$$rk(A) \leq \max\{|A \cap B| \mid B \in \mathcal{B}\}.$$

Aus beiden Ungleichungen folgt $rk(A) = \max\{|A \cap B| \mid B \in \mathcal{B}\}$. □

Definition 1.2.2. Das *Dual* $\mathfrak{M}^*$ eines Matroids $\mathfrak{M} = (X, \mathcal{I})$ ist definiert als das Tupel $(X, \mathcal{I}^*)$ mit $A \in \mathcal{I}^*$ genau dann, wenn es eine Basis $B \in \mathcal{B}$ gibt, so dass $A \subseteq (X \backslash B)$.

Satz 1.2.3. *Das Dual eines Matroids ist selbst ein Matroid und dessen Rangfunktion rk^* ist gegeben durch:*

$$\begin{aligned} rk^*\colon \mathbb{X} &\to \mathbb{N} \\ A &\mapsto |A| - rk(X) + rk(X \backslash A). \end{aligned}$$

Notation. Wenn wir in dieser Arbeit Axiome für eine bestimmte Funktion zeigen, akzentuieren wir oft die Bezeichnungen dieser Axiome so, wie wir die Funktion akzentuiert haben und meinen damit das Axiom für genau diese Funktion. Beispielsweise soll „(rk*1)“ gleichbedeutend sein mit „(rk1) für rk^*“.

von Satz 1.2.3. Wir wollen Theorem 1.1.7 anwenden. Dazu definieren wir rk^* wie angegeben und zeigen zunächst, dass für $A \subseteq X$ gilt, dass $rk^*(A) = |A|$ genau dann, wenn

$A \in \mathcal{I}^*$. Anschließend zeigen wir, dass (X, rk^*) ein Matroid ist. Wir haben

$$\begin{aligned} rk^*(A) &= |A| - rk(X) + rk(X \backslash A) \\ &= |A| - rk(X) + \max\{|(X \backslash A) \cap B| \mid B \in \mathcal{B}\} && \text{nach 1.2.1} \\ &= |A| - \min\{rk(X) - |(X \backslash A) \cap B| \mid B \in \mathcal{B}\} \\ &= |A| - \min\{|B| - |(X \backslash A) \cap B| \mid B \in \mathcal{B}\} && \text{da } \forall B \in \mathcal{B} : rk(X) = |B| \\ &= |A| - \min\{|B \backslash (X \backslash A)| \mid B \in \mathcal{B}\} \\ &= |A| - \min\{|B \cap A| \mid B \in \mathcal{B}\} \\ &\leq |A| \end{aligned}$$

mit Gleichheit genau dann, wenn es eine Basis B gibt, so dass der Schnitt von A und B leer ist. Das gilt genau dann, wenn A Teilmenge von $X \backslash B$ ist und nach Definition ist A genau dann in $\mathcal{I}^*$. ✓

Bleibt zu zeigen, dass (X, rk^*) ein Matroid ist.

(rk*1): Sei $A \subseteq X$. Nach (rk1) ist $rk(X \backslash A) \leq rk(X)$. Damit ist

$$rk^*(A) = |A| - rk(X) + rk(X \backslash A) \leq |A|. \qquad ✓$$

(rk*2): Sei $A \subseteq B \subseteq X$. Dann ist

$$\begin{aligned} rk^*(A) &= |A| - rk(X) + rk(X \backslash A) \\ &= |A| - rk(X) + rk((X \backslash B) \cup (B \backslash A)) \\ &\leq |A| - rk(X) + rk(X \backslash B) + rk(B \backslash A) && \text{da } rk \text{ subadditiv} \\ &\leq |A| - rk(X) + rk(X \backslash B) + |B \backslash A| && \text{nach (rk2)} \\ &= |B| - rk(X) + rk(X \backslash B) \\ &= rk^*(B). && ✓ \end{aligned}$$

(rk*3): Sei $A, B \subseteq X$ und A^c, B^c seien deren Komplemente in X. Es ist

$$\begin{aligned} rk(A^c) + rk(B^c) &\geq rk(A^c \cup B^c) + rk(A^c \cap B^c) && \text{nach (rk3)} \\ &= rk((A \cap B)^c) + rk((A \cup B)^c), \end{aligned}$$

also

$$\begin{aligned} rk^*(A) + rk^*(B) &= |A| + |B| - 2rk(X) + rk(A^c) + rk(B^c) \\ &= |A \cup B| + |A \cap B| - 2rk(X) + rk(A^c) + rk(B^c) \\ &\geq (|A \cup B| - rk(X) + rk((A \cup B)^c)) \\ &\qquad + (|A \cap B| - rk(X) + rk((A \cap B)^c)) \\ &= rk^*(A \cup B) + rk^*(A \cap B). && ✓ \end{aligned}$$

Wir haben also gezeigt, dass (X, rk^*) ein Matroid ist und dass eine beliebige Teilmenge $A \subseteq X$ genau dann in I^* ist, wenn $rk^*(A) = |A|$. Nach Theorem 1.1.7 ist dann $(X, \mathcal{I}^*)$ ein Matroid. □

Notation. Bei gegebenem Matroid $\mathfrak{M}$ bezeichnen wir mit $\mathfrak{M}^*$ dessen Dual, mit $\mathcal{I}^*$ die Menge der unabhängigen Mengen des Duals, mit rk^* die Rangfunktion des Duals und mit $\mathcal{B}^*$ die Menge der Basen des Duals.

Bemerkung. Offensichtlich ist für jedes Matroid mit unendlichem X das Dual kein Matroid, da dann (M4) beziehungsweise (rk4) für das Dual nicht erfüllt ist.

Lemma 1.2.4. *Die Basen des Duals eines Matroids sind genau die Komplemente der Basen des Matroids:* $\mathcal{B}^* = \{X \backslash B \mid B \in \mathcal{B}\}$.

Beweis. Nach Definition der unabhängigen Mengen $\mathcal{I}^*$ des Duals, sind die maximalen unabhängigen Mengen genau die Mengen $X\backslash B$ mit $B \in \mathcal{B}$. □

Da die Komplemente der Komplemente der Basen wieder die Basen selbst sind, folgt direkt:

Satz 1.2.5. *Das Dual des Duals eines Matroids ist das Matroid selbst:* $(\mathfrak{M}^*)^* = \mathfrak{M}$.

1.3 Matroide-Homomorphismen

In diesem Abschnitt definieren wir den Homomorphismenbegriff für Matroide und zeigen, inwiefern solche Homomorphismen strukturerhaltend sind.

Definition 1.3.1. Sei X eine endliche Menge, rk eine Abbildung von der Potenzmenge von X in die natürlichen Zahlen und $\mathfrak{M}' = (X', rk')$ ein Matroid. Wir nennen eine Funktion

$$\nu \colon X \to X'$$

Matroide-Homomorphismus von $\mathfrak{M} := (X, rk)$ *nach* $\mathfrak{M}'$, falls $rk = rk' \circ \nu$, also falls das folgende Diagramm kommutiert:

$$\begin{tikzcd} \mathbb{P}(X) \arrow[rr, "\nu"] \arrow[dr, "rk"'] & & \mathbb{P}(X') \arrow[dl, "rk'"] \\ & \mathbb{N} & \end{tikzcd} .$$

Satz 1.3.2. *Sei ν ein Matroide-Homomorphismus von $\mathfrak{M} = (X, rk)$ nach $\mathfrak{M}'$. Dann gilt:*

(i) Das Tupel $\mathfrak{M}$ ist ein Matroid.

(ii) Für beliebige Teilmengen A von X und A' von X' gelten folgende Implikationen:

$$A \text{ ist unabhängig in } \mathfrak{M} \Rightarrow \nu(A) \text{ ist unabhängig in } \mathfrak{M}' \text{ und } \nu\big|_A \text{ ist injektiv,}$$
$$A' \text{ ist unabhängig in } \mathfrak{M}' \text{ und } \nu\big|_{\nu^{-1}(A')} \text{ ist injektiv } \Leftrightarrow \nu^{-1}(A') \text{ ist unabhängig in } \mathfrak{M}.$$

(iii) Für alle Elemente x aus X und alle Teilmengen A von X gilt: x ist genau dann (un-)abhängig von A in $\mathfrak{M}$, wenn $\nu(x)$ (un-)abhängig von $\nu(A)$ in $\mathfrak{M}'$ ist.

Beweis. (i) Zu Zeigen sind die Axiome (rk1), (rk2) und (rk3).

(rk1): Für jede Teilmenge A von X gilt:

$$\begin{aligned} rk(A) &= rk'(\nu(A)) \\ &\leq |\nu(A)| && \text{nach (rk}'1) \\ &\leq |A|. && \checkmark \end{aligned}$$

(rk2): Für alle Teilmengen A und B von X gilt: ist A Teilmenge von B, so ist auch $\nu(A)$ Teilmenge von $\nu(B)$. Dann folgt:

$$\begin{aligned} rk(A) &= rk'(\nu(A)) \\ &\leq rk'(\nu(B)) && \text{nach (rk}'2) \\ &= rk(B). && \checkmark \end{aligned}$$

(rk3): Für alle Teilmengen A und B von X gilt:

$$\begin{aligned} rk(A \cup B) + rk(A \cap B) &= rk'(\nu(A \cup B)) + rk'(\nu(A \cap B)) \\ &= rk'(\nu(A) \cup \nu(B)) + rk'(\nu(A \cap B)) \\ &\leq rk'(\nu(A) \cup \nu(B)) + rk'(\nu(A) \cap \nu(B)) && \text{nach (rk}'2) \\ &\leq rk'(\nu(A)) + rk'(\nu(B)) && \text{nach (rk}'3) \\ &= rk(A) + rk(B). && \checkmark \end{aligned}$$

Damit ist (X, rk) ein Matroid. □

(ii) Zur ersten Implikation: Sei A eine unabhängige Menge in $\mathfrak{M}$. Dann folgt:

$$\begin{aligned} |\nu(A)| &\geq rk'(\nu(A)) && \text{nach (rk}'1) \\ &= rk(A) \\ &= |A| && \text{nach Theorem 1.1.7} \\ &\geq |\nu(A)|, \end{aligned}$$

also $|\nu(A)| = rk'(\nu(A)) = |A|$, insbesondere ist $\nu\big|_A$ injektiv. Nach Theorem 1.1.7 ist dann außerdem $\nu(A)$ unabhängig in $\mathfrak{M}'$. ✓

Zur zweiten und dritten Implikation: Für alle Teilmengen A' von X' gilt:

$$|\nu^{-1}(A')| \geq |A'| \geq rk'(A') = rk'(\nu(\nu^{-1}(A'))) = rk(\nu^{-1}(A'))$$

mit Gleichheit genau dann, wenn $|\nu^{-1}(A')| = |A'|$, also $\nu^{-1}\big|_{A'}$ injektiv, und A' unabhängig in $\mathfrak{M}'$. □

(iii) Folgt direkt aus der Tatsache, dass für alle x aus X und alle Teilmengen A von X nach Definition gilt: $rk'(\nu(A) \cup \{\nu(x)\}) = rk'(\nu(A \cup \{x\})) = rk(A \cup \{x\})$ und $rk(A) = rk'(\nu(A))$. □

1.4 Darstellbarkeit

In diesem Abschnitt werden wir unseren Begriff der Darstellbarkeit eines Matroids definieren. Dieser stellt eine Verallgemeinerung zum gewöhnlichen Begriff der Darstellbarkeit von Matroiden über endliche Teilmengen von $\mathbb{Z}^n$ dar. Wir definieren zunächst den Begriff der Dargestelltheit eines Tupels (X, rk) und beweisen, dass es sich dabei tatsächlich um ein Matroid handelt. Darauf aufbauend definieren wir die Darstellbarkeit von Matroiden.

In diesem Abschnitt betrachten wir stets X als endliche Teilmenge einer endlich erzeugten, abelschen Gruppe G. Beachte, dass dann nach dem Hauptsatz über endlich erzeugte, abelsche Gruppen (siehe [2]) gilt:

$$G \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{s} \mathbb{Z}_{p_i} \tag{3}$$

mit $r, s \in \mathbb{N}$ und p_i prim für $i = 1, \dots, s$.

Zunächst eine abkürzende Schreibweise:

Notation 1.4.1. Für eine endlich erzeugte, abelsche Gruppe $G \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{s} \mathbb{Z}_{p_i}$ mit $r, s \in \mathbb{N}$ und p_i prim für $i = 1, \dots, s$ schreiben wir oft „*sei* $G = G_f \oplus G_t$" oder rechnen direkt mit G_f oder G_t und legen damit fest, dass außer $G = G_f \oplus G_t$ gelte:

(i) Es ist $G_t = \{g \in G \mid |\langle g \rangle| \in \mathbb{N}\}$, das heißt G_t ist isomorph zu $\bigoplus_{i=1}^{s} \mathbb{Z}_{p_i}$.

(ii) Es ist G_f isomorph zu $\mathbb{Z}^r$, also G_f frei, abelsch.

So ein G_f mit $G = G_f \oplus G_t$ existiert nach dem *Hauptsatz über endlich erzeugte, abelsche Gruppen* (siehe [2]), ist aber im Allgemeinen nicht eindeutig.

Beachte, dass für eine endlich erzeugte, freie abelsche Gruppe G – also $G \cong \mathbb{Z}^r$ mit einem eindeutig bestimmten $r \in \mathbb{N}$ – der Rang von G definiert ist als $Rang(G) := r$ (siehe [3]).

Definition 1.4.2. Sei X Teilmenge einer endlich erzeugten, abelschen Gruppe $G = G_f \oplus G_t$. Dann nennen wir das Tupel (X, rk) *dargestellt (durch G)*, falls:

$$\begin{aligned} rk\colon X &\to \mathbb{N} \\ A &\mapsto Rang(\langle A \rangle_f). \end{aligned}$$

Bemerkung. (i) Nach Definition haben alle $\langle A \rangle_f$ gleichen Rang, rk ist also wohldefiniert.

(ii) Da Gruppenisomorphismen auf einer endlich erzeugten, freien abelschen Gruppe rangerhaltend sind, können wir dann bei Betrachtung dargestellter Tupel (X, rk) ohne Einschränkung annehmen, dass in (3) Gleichheit gilt.

(iii) Für $H \subseteq G$ sprechen wir vom Rang von H, wenn H endlich ist oder wenn H Untergruppe von G ist und meinen in beiden Fällen $Rang(\langle H \rangle_f)$.

Sofern nicht anders angegeben, sei in diesem Kapitel stets (X, rk) dargestellt durch G.

Für den Beweis, dass (X, rk) dann tatsächlich ein Matroid ist, benutzen wir folgende Schreibweise und Lemmata:

Notation. Sei $n, r \in \mathbb{N}$, $K = \{k_1, \dots, k_n\} \subseteq \mathbb{N}$, $k_j < k_{j+1}$ für $j = 1, \dots, n-1$ und $A = \{a_{k_1}, \dots, a_{k_n}\} \subseteq \mathbb{Z}^r$. Wir bezeichnen mit

$$[A] := ((a_{k_j})_i)_{\substack{1 \le i \le r \\ 1 \le j \le n}} \in M(r \times n, \mathbb{Q})$$

die Matrix mit den Spalten $[A]^{(j)} = a_{k_j}$ für $j = 1, \dots, n$.

Geben wir K nicht an, so spielt die Reihenfolge der Spalten für uns keine Rolle.

Lemma 1.4.3. *Sei G frei abelsch, also ohne Einschränkung $G = \mathbb{Z}^r$ für ein $r \in \mathbb{N}$. Dann gilt für alle $A \subseteq X$:*

(i) $rk(A) = \max\{|B| \mid B \text{ linear unabhängig in } \mathbb{Q}^r, B \subseteq A\}$,

(ii) $rk(A) = Rang([A])$.

Beachte, dass es für den Rang der Matrix keine Rolle spielt, ob wir die Elemente aus A mehrfach in die Spalten schreiben. Insbesondere gilt auch für alle $A, B \subseteq X$, dass $rk(A \cup B) = Rang(([A] \mid [B]))$

Beweis. Beachte zunächst, dass in $\mathbb{Z}^r$ für alle $A \subseteq G$ gilt, dass $\langle A \rangle_f = \langle A \rangle$.

(i) Für alle in $\mathbb{Q}^r$ linear unabhängigen Teilmengen B von A gilt:

$$rk(A) = Rang(\langle A\rangle) \geq Rang(\langle B\rangle) = |B|,$$

also

$$rk(A) \geq \max\{|B| \mid B \text{ linear unabhängig in } \mathbb{Q}^r, B \subseteq A\}.$$

Bleibt zu zeigen, dass $rk(A) \leq \max\{|B| \mid B \text{ linear unabhängig in } \mathbb{Q}^r, B \subseteq A\}$. Sei hierzu $B' = \{b_1, \ldots, b_{rk(A)}\}$ Basis von $\langle A\rangle$, also $rk(A) = |B'|$. Es ist B' linear unabhängig in $\mathbb{Q}^r$, denn sonst gibt es $n_i \in \mathbb{N}$, $m_i \in \mathbb{N}\backslash\{0\}$ für $i = 1, \ldots, rk(A)$, sodass $n_k \neq 0$ für ein $k \in \{1, \ldots, rk(A)\}$ und

$$0 = 0 \cdot \prod_{i=1}^{rk(A)} m_i = \left(\sum_{i=1}^{rk(A)} \frac{n_i}{m_i} b_i\right) \cdot \prod_{j=1}^{rk(A)} m_j = \sum_{i=1}^{rk(A)} \left(n_i \cdot \prod_{j=1, j\neq i}^{rk(A)} m_j\right) b_i.$$

Insbesondere sind die Koeffizienten der b_i ganze Zahlen und der k-te Koeffizient ist ungleich null. Ein Widerspruch dazu, dass B' Basis von $\langle A\rangle$ ist. B' ist also in $\mathbb{Q}^r$ minimal, sodass die erzeugte Untergruppe A enthält. Dann lässt sich auch eine in $\mathbb{Q}^r$ linear unabhängige Menge $B \subseteq A$ wählen mit $|B| \geq rk(A)$, denn hätten alle in $\mathbb{Q}^r$ linear unabhängigen Teilmengen von A weniger als $rk(A) = |B'|$ Elemente, so wäre B' nicht minimal. Ein Widerspruch. Damit haben wir

$$rk(A) \leq |B| \leq \max\{|C| \mid C \text{ linear unabhängig in } \mathbb{Q}^r, C \subseteq A\}. \qquad \square$$

(ii) Sei $A = \{a_i \mid i \in I\}$ für ein $I \subseteq \mathbb{N}$. Dann ist

$$\begin{aligned} Rang[A] &= \max\{|J| \mid J \subseteq I, \{[A]^j \mid j \in J\} \text{ linear unabhängig in } \mathbb{Q}^r\} \\ &= \max\{|J| \mid J \subseteq I, \{a_j \mid j \in J\} \text{ linear unabhängig in } \mathbb{Q}^r\} \\ &= \max\{|B| \mid B \subseteq A, B \text{ linear unabhängig in } \mathbb{Q}^r\} \\ &= rk(A) \qquad \text{nach (i).} \quad \square \end{aligned}$$

Bemerkung 1.4.4. Für den Fall, dass $G = \mathbb{Z}^r \oplus \bigoplus_{i=1}^s \mathbb{Z}_{p_i}$ nicht frei ist, können wir analog für

$$A = \{a_1, \ldots, a_n\} = \left\{((a_1)_f, (a_1)_t), \ldots, ((a_n)_f, (a_n)_t)\right\} \subseteq X$$

mit $(a_i)_f \in \mathbb{Z}^r$ und $(a_i)_t \in \bigoplus_{i=1}^s \mathbb{Z}_{p_i}$ für $i = 1, \ldots, n$ die Menge

$$A_f := \{((a_1)_f, 0), \ldots, ((a_n)_f, 0)\} \subseteq \mathbb{Z}^r \oplus \{0\}$$

betrachten und obiges Lemma anwenden, da der Rang nur von A_f abhängt. Das heißt:

(i) $rk(A) = \max\{|B| \mid B \text{ linear unabhängig in } \mathbb{Q}^r, B \subseteq A_f\}$,

(ii) $rk(A) = Rang([A_f])$.

Lemma 1.4.5. *Sei G frei und (X, rk) dargestellt durch G. Dann ist (X, rk) ein Matroid.*

Beweis. Wir definieren $\mathcal{I}$ als

$$\begin{aligned} \mathcal{I} &= \{A \subseteq X \mid rk(A) = |A|\} \\ &= \{A \subseteq X \mid A \text{ ist linear unabhängig in } \mathbb{Q}^r\} \qquad \text{nach Lemma 1.4.3.} \end{aligned}$$

Dann ist $(X, \mathcal{I})$ bekanntermaßen ein Matroid und nach Theorem 1.1.7 auch (X, rk). $\square$

Satz 1.4.6. *Sei X Teilmenge einer endlich erzeugten, abelschen Gruppe G und (X, rk) dargestellt durch G. Dann ist (X, rk) ein Matroid.*

Beweis. Betrachte für $X \subseteq G = G_f \oplus G_t$ und rk wie angegeben die endliche Teilmenge $X' := X \cap (G_f \oplus \{0\})$ der endlich erzeugten, freien, abelschen Gruppe $G' := G_f \oplus \{0\}$ und $rk' := rk\big|_{X'}$. Nach Lemma 1.4.5 ist (X', rk') ein Matroid. Betrachte die Projektion

$$\begin{aligned} \nu\colon G &\to G_f \\ x &\mapsto x_f \text{ für } x = (x_f, x_t) \text{ mit } x_f \in G_f, x_t \in G_t. \end{aligned}$$

Für jedes $A \subseteq X$ haben A und $\nu(A)$ gleichen Rang, also ist $rk(A) = rk' \circ \nu(A)$. Dann folgen (rk2) und (rk3) direkt aus (rk′2) und (rk′3). Außerdem folgt mit (rk′1) für alle Teilmengen A von X

$$rk(A) = rk'(\nu(A)) \leq |\nu(A)| \leq |A|,$$

also gilt (rk1). Damit ist (X, rk) ein Matroid. □

Beispiel 1.4.7. Wir betrachten $X \subseteq G := \mathbb{Z}^3/\langle(7, 8, 9)^T\rangle$ (als additive Gruppe) wie folgt:

$$X := \left\{\overline{\begin{pmatrix}0\\1\\1\end{pmatrix}}, \overline{\begin{pmatrix}1\\1\\1\end{pmatrix}}, \overline{\begin{pmatrix}2\\1\\0\end{pmatrix}}, \overline{\begin{pmatrix}56\\1\\9\end{pmatrix}}\right\},$$

mit der eben definierten Rangfunktion rk, wobei $\overline{v} := v + \langle(7, 8, 9)^T\rangle$ die Nebenklasse mit dem Repräsentanten v sei. Zunächst schreiben wir G als direkte Summe zyklischer Gruppen. Wir zeigen, dass G frei ist, indem wir nachweisen, dass $\{(1, 0, 0)^T, (0, 1, 1)^T\}$ eine Basis B repräsentiert. Offensichtlich sind die repräsentierten Nebenklassen keine ganzzahligen Vielfachen voneinander. Da die Standardbasis von $\mathbb{Z}^3$ ein Erzeugendensystem von G repräsentiert und

$$\begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\end{pmatrix}, \quad \begin{pmatrix}0\\1\\0\end{pmatrix} = 7 \cdot \begin{pmatrix}1\\0\\0\end{pmatrix} + 9 \cdot \begin{pmatrix}0\\1\\1\end{pmatrix} - \begin{pmatrix}7\\8\\9\end{pmatrix}, \quad \begin{pmatrix}0\\0\\1\end{pmatrix} = -7 \cdot \begin{pmatrix}1\\0\\0\end{pmatrix} - 8 \cdot \begin{pmatrix}0\\1\\1\end{pmatrix} + \begin{pmatrix}7\\8\\9\end{pmatrix},$$

ist B außerdem Erzeugendensystem von G und damit tatsächlich eine Basis. Es ist also G isomorph zu $\mathbb{Z}^2$. Für jede Teilmenge A von X und jeden Isomorphismus ϕ von G nach $\mathbb{Z}^2$ ist der Rang von A gleich dem Rang von $\phi(A)$. Wir wählen ϕ als folgenden Isomorphismus:

$$\begin{aligned} \phi\colon \quad & G \to \mathbb{Z}^2, \\ \lambda \cdot \overline{\begin{pmatrix}1\\0\\0\end{pmatrix}} + \mu \cdot \overline{\begin{pmatrix}0\\1\\1\end{pmatrix}} &\mapsto \begin{pmatrix}\lambda\\\mu\end{pmatrix}. \end{aligned}$$

Dann ist

$$\phi(X) = \left\{\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}9\\9\end{pmatrix}, \begin{pmatrix}0\\-63\end{pmatrix}\right\},$$

also ist die Menge der Basen von X genau

$$\begin{aligned} \mathcal{B} &:= \phi^{-1}\left(\left\{\{u, v\} \;\middle|\; u \in \left\{\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\-63\end{pmatrix}\right\}, v \in \left\{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}9\\9\end{pmatrix}\right\}\right\}\right) \\ &= \left\{\{\overline{u}, \overline{v}\} \;\middle|\; u \in \left\{\begin{pmatrix}0\\1\\1\end{pmatrix}, \begin{pmatrix}56\\1\\9\end{pmatrix}\right\}, v \in \left\{\begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}2\\1\\0\end{pmatrix}\right\}\right\}. \end{aligned}$$

Für jede Teilmenge A von X ist nach Definition $rk(A)$ die maximale Kardinalität der unabhängigen Teilmengen von A und lässt sich direkt aus der Menge der Basen $\mathcal{B}$ ablesen.

Definition 1.4.8. Wir nennen ein Matroid $\mathfrak{M} = \mathfrak{M}_X = (X, rk)$ *darstellbar (durch G)*, wenn es ein dargestelltes Matroid $\mathfrak{M}' = \mathfrak{M}'_{X'} = (X', rk')$ durch G und einen Matroide-Homomorphismus ν von $\mathfrak{M}$ nach $\mathfrak{M}'$ gibt, also wenn es eine endliche Teilmenge X' einer endlich erzeugten, abelschen Gruppe G gibt und eine Abbildung $\nu\colon X \to X'$, sodass folgendes Diagramm kommutiert:

$$\begin{tikzcd} \mathbb{P}(X) \arrow[rr, "\nu"] \arrow[dr, "rk"'] & & \mathbb{P}(X') \arrow[dl, "Rang(\langle\cdot\rangle_f)"] \\ & \mathbb{N} & \end{tikzcd} .$$

In dem Fall heißt ν *(Matroid-)Darstellung (von $\mathfrak{M}$ nach $\mathfrak{M}'$)* und $\mathfrak{M}'$ heißt *darstellendes Matroid von $\mathfrak{M}$*. Wir sagen auch $\mathfrak{M}'$ *stellt* $\mathfrak{M}$ *dar*.

Bemerkung. In Abschnitt 2.3 werden wir sehen, dass das Dual (X, rk^*) eines darstellbaren Matroids (X, rk) wieder darstellbar ist.

2 Arithmetische Matroide

Definition 2.0.1. Ein *arithmetisches Matroid* $(\mathfrak{M}_X, m) = (X, rk, m)$ ist ein Matroid $\mathfrak{M}_X$ über einer Menge von Elementen X mit einer *Vielfachheitsfunktion* $m\colon \mathbb{P}(X) \to \mathbb{N}$, die folgende Axiome erfüllt:

(m1): ist $A \subseteq X$ und $x \in X$ abhängig von A, dann gilt: $m(A \cup \{x\})$ teilt $m(A)$,

(m2): ist $A \subseteq X$ und $x \in X$ unabhängig von A, dann gilt: $m(A)$ teilt $m(A \cup \{x\})$,

(m3): ist $A \subseteq B \subseteq X$ und sind $F, T \subseteq B \backslash A$ so, dass $B = A \dot\cup F \dot\cup T$ und für alle $A \subseteq C \subseteq B$ gilt, dass $rk(C) = rk(A) + |C \cap F|$, dann gilt auch:

$$m(A) \cdot m(B) = m(A \cup F) \cdot m(A \cup T),$$

(m4): ist $A \subseteq B \subseteq X$ und $rk(A) = rk(B)$, dann gilt:

$$\mu_B(A) \coloneqq \sum_{A \subseteq C \subseteq B} (-1)^{|C|-|A|} m(C) \geq 0,$$

(m5): ist $A \subseteq B \subseteq X$ und $rk^*(A) = rk^*(B)$, dann gilt:

$$\mu^*_B(A) \coloneqq \sum_{A \subseteq C \subseteq B} (-1)^{|C|-|A|} m(X \backslash C) \geq 0.$$

Wir schreiben dann auch $\mathfrak{M}_X$ oder $\mathfrak{M}$ statt $(\mathfrak{M}_X, m)$.

Lemma 2.0.2. *(i) Nach den Annahmen zu (m3) enthält F genau die Elemente aus $B \backslash A$, die unabhängig von A sind, und T enthält genau die Elemente aus $B \backslash A$, die abhängig von A sind. Damit sind solche F, T für gegebene $A \subseteq B \subseteq X$ bei Existenz eindeutig bestimmt.*

(ii) Nach den Annahmen zu (m3) ist F unabhängig.

(iii) Nach den Annahmen zu (m3) gilt für alle unabhängigen Teilmengen I von A, dass $I \cup F$ unabhängig ist.

Beweis. Sei $A \subseteq B \subseteq X$ mit $B = A \dot\cup F \dot\cup T$ und für alle $A \subseteq C \subseteq B$ gelte $rk(C) = rk(A) + |C \cap F|$.

(i) Sei $f \in F$ abhängig von A. Dann folgt:

$$rk(A \cup \{f\}) = rk(A) \neq rk(A) + 1 = rk(A) + |\{f\}| = rk(A) + |(A \cup \{f\}) \cap F|.$$

Für die Wahl $C := A \cup \{f\}$ ist dies ein Widerspruch zur Voraussetzung. Es sind also alle $f \in F$ unabhängig von A. Sei weiter $t \in T$ unabhängig von A. Dann folgt:

$$rk(A \cup \{t\}) = rk(A) + 1 \neq rk(A) = rk(A) + |\emptyset| = rk(A) + |(A \cup \{t\}) \cap F|.$$

Für die Wahl $C := A \cup \{t\}$ ist dies ein Widerspruch zur Voraussetzung. Es sind also alle $t \in T$ abhängig von A. Mit $B = A \dot\cup F \dot\cup T$ ist $F \dot\cup T = B \backslash A$, also sind alle Elemente aus $B \backslash A$ entweder in F oder in T enthalten. Damit enthält F tatsächlich alle von A unabhängigen Elemente aus $B \backslash A$ und T alle von A abhängigen Elemente aus $B \backslash A$. □

(ii) Sei F nicht unabhängig, also $rk(F) < |F|$. Dann ist

$$\begin{aligned} rk(B) &= rk(A \cup F \cup T) \\ &= rk(A \cup F) && \text{nach (i) mit Lemma 1.1.6} \\ &= rk(A \cup F) + rk(\emptyset) \\ &= rk(A \cup F) + rk(A \cap F) \\ &\leq rk(A) + rk(F) && \text{nach (rk3)} \\ &< rk(A) + |F|, \end{aligned}$$

ein Widerspruch zur Annahme.

(iii) Sei zunächst I maximale unabhängige Teilmenge von A, das heißt $rk(A) = |I|$ und jedes Element aus A ist abhängig von I. Sei weiter $I \cup F$ nicht unabhängig, also $rk(I \cup F) < |I \cup F|$. Dann ist

$$\begin{aligned} rk(A \cup F) &= rk(A) + |F| && \text{nach Vorraussetzung} \\ &= |I| + |F| \\ &= |I \cup F| && \text{da } I, F \text{ disjunkt nach Vorraussetzung} \\ &> rk(I \cup F) \\ &= rk(A \cup F) && \text{nach Lemma 1.1.5 und Lemma 1.1.6.} \end{aligned}$$

Ein Widerspruch. Die Aussage gilt also für maximale unabhängige Teilmengen von A und mit (I2) auch für beliebige unabhängige Teilmengen von A. □

2.1 Das Dual eines arithmetischen Matroids

Definition 2.1.1. Das *Dual* eines arithmetischen Matroids $(\mathfrak{M}_X, m)$ ist definiert als das Tupel $(\mathfrak{M}^*_X, m^*)$, wobei $\mathfrak{M}^*_X$ das Dual des Matroids $\mathfrak{M}_X$ sei und $m^*(A) := m(X \backslash A)$ für alle $A \subseteq X$.

Satz 2.1.2. *Das Dual eines arithmetischen Matroids ist selbst ein arithmetisches Matroid.*

Beweis. Nach Satz 1.2.3 ist $\mathfrak{M}_X^*$ ein Matroid. Zu zeigen ist also, dass m^* Vielfachheitsfunktion ist.

(m^*1): Sei $A \subseteq X$ und $x \in X$ unabhängig von A bezüglich $\mathfrak{M}^*$, insbesondere ist dann $x \notin A$. Dann folgt, dass

$$\begin{aligned}|A| - rk(X) + rk(X\backslash A) &= rk^*(A)\\ &= rk^*(A \cup \{x\}) - 1\\ &= |A \cup \{x\}| - rk(X) + rk(X\backslash(A \cup \{x\})) - 1\\ &= |A| - rk(X) + rk(X\backslash(A \cup \{x\})),\end{aligned}$$

also ist $rk(X\backslash A) = rk(X\backslash(A \cup \{x\}))$, also ist x abhängig von $X\backslash(A \cup \{x\})$ bezüglich $\mathfrak{M}$. Das heißt $m(X\backslash A) = m^*(A)$ teilt $m(X\backslash(A \cup \{x\})) = m^*(A \cup \{x\})$ nach (m2). □

(m^*2): Sei $A \subseteq X$ und $x \in X$ abhängig von A bezüglich $\mathfrak{M}^*$. Ist $x \in A$, so ist $A \cup \{x\} = A$ und die Behauptung trivial erfüllt. Sei also $x \notin A$. Dann folgt, dass

$$\begin{aligned}|A| - rk(X) + rk(X\backslash A) &= rk^*(A)\\ &= rk^*(A \cup \{x\})\\ &= |A \cup \{x\}| - rk(X) + rk(X\backslash(A \cup \{x\}))\\ &= |A| + 1 - rk(X) + rk(X\backslash(A \cup \{x\})),\end{aligned}$$

also ist $rk(X\backslash A) = 1 + rk(X\backslash(A \cup \{x\}))$, also ist x unabhängig von $X\backslash(A \cup \{x\})$ bezüglich $\mathfrak{M}$. Das heißt $m(X\backslash(A \cup \{x\})) = m^*(A \cup \{x\})$ teilt $m(X\backslash(A)) = m^*(A)$ nach (m1). □

(m^*3:) Sei $A \subseteq B \subseteq X$ und $B = A \,\dot\cup\, F \,\dot\cup\, T$ so, dass für alle $A \subseteq C \subseteq B$ gilt, dass $rk^*(C) = rk^*(A) + |C \cap F|$. Insbesondere ist dann

$$\begin{aligned}|B| - rk(X) + rk(X\backslash B) &= rk^*(B)\\ &= rk^*(A) + |F|\\ &= |A| - rk(X) + rk(X\backslash A) + |F|\end{aligned}$$

und nach Umstellen der Gleichung

$$rk(X\backslash A) = rk(X\backslash B) + |B| - |A| - |F| = rk(X\backslash B) + |T|. \tag{4}$$

Es ist $X\backslash A = (X\backslash B) \,\dot\cup\, F \,\dot\cup\, T$ nach Voraussetzung und $A \subseteq C \subseteq B$ genau dann, wenn $X\backslash B \subseteq X\backslash C \subseteq X\backslash A$. Wir zeigen, dass $rk(X\backslash C) = rk(X\backslash B) + |(X\backslash C) \cap T|$ für alle C mit $X\backslash B \subseteq X\backslash C \subseteq X\backslash A$, um dann (m3) anwenden zu können:

$$\begin{aligned}|C| - rk(X) + rk(X\backslash C) &= rk^*(C)\\ &= rk^*(A) + |C \cap F|\\ &= |A| - rk(X) + rk(X\backslash A) + |C \cap F|\end{aligned}$$

und nach Umstellen der Gleichung

$$\begin{aligned}rk(X\backslash C) &= rk(X\backslash A) + |A| + |C \cap F| - |C|\\ &= rk(X\backslash A) - |C \cap T|\\ &= rk(X\backslash B) + |T| - |C \cap T| && \text{nach (4)}\\ &= rk(X\backslash B) + |(X\backslash C) \cap T|.\end{aligned}$$

Damit können wir (m3) anwenden auf $m(X\backslash A) \cdot m(X\backslash B)$:

$$\begin{aligned} m^*(A) \cdot m^*(B) &= m(X\backslash A) \cdot m(X\backslash B) \\ &= m((X\backslash B) \cup F) \cdot m((X\backslash B) \cup T) && \text{nach (m3)} \\ &= m(X\backslash(A \cup T)) \cdot m(X\backslash(A \cup F)) \\ &= m^*(A \cup T) \cdot m^*(A \cup F). \end{aligned}$$ □

(m*4): Sei $A \subseteq B \subseteq X$ und $rk^*(A) = rk^*(B)$. Nach (m5) gilt dann $\mu_B^*(A) \geq 0$. □

(m*5): Sei $A \subseteq B \subseteq X$ und $(rk^*)^*(A) = (rk^*)^*(B)$. Nach Satz 1.2.5 gilt dann $rk(A) = (rk^*)^*(A) = (rk^*)^*(B) = rk(B)$ und nach (m4) gilt $(\mu_B^*)^*(A) = \mu_B(A) \geq 0$. □

Lemma 2.1.3. *Bei gegebenem Matroid mit einer Funktion $m\colon X \to \mathbb{N}$ gelten für die Aussagen $(m1)\ldots(m5)$ und $(m^*1)\ldots(m^*5)$ folgende Äquivalenzen:*

$$\begin{aligned} &(m1) \Leftrightarrow (m^*2), \\ &(m2) \Leftrightarrow (m^*1), \\ &(m3) \Leftrightarrow (m^*3), \\ &(m4) \Leftrightarrow (m^*5), \\ &(m5) \Leftrightarrow (m^*4). \end{aligned}$$

Beweis. Im Beweis von (m*1) haben wir nur (m2) verwendet, also folgt (m*1) aus (m2). Nach Satz 1.2.5 folgt dann auch (m1) aus (m*2). Im Beweis von (m*2) haben wir nur (m1) verwendet, also folgt (m*2) aus (m1). Nach Satz 1.2.5 folgt dann auch (m2) aus (m*1). Damit gilt (m1) genau dann, wenn (m*2) gilt und (m2) genau dann, wenn (m*1) gilt.

Dass (m4) genau dann gilt, wenn (m*5) gilt und (m5) genau dann, wenn (m*4) gilt, folgt analog.

Im Beweis von (m*3) haben wir nur (m3) verwendet, also folgt (m*3) aus (m3). Nach Satz 1.2.5 folgt dann auch (m3) aus (m*3). Damit gilt (m3) genau dann, wenn (m*3) gilt. □

2.2 Arithmetische-Matroide-Homomorphismen

In diesem Abschnitt definieren wir den Homomorphismenbegriff für arithmetische Matroide und zeigen, inwiefern solche Homomorphismen strukturerhaltend sind.

Definition 2.2.1. Seien $\mathfrak{M} = (X, rk, m)$ und $\mathfrak{M}' = (X', rk', m')$ sei arithmetische Matroide. Wir nennen eine Funktion

$$\nu\colon X \to X'$$

Arithmetische-Matroide-Homomorphismus (oder kürzer *A-M-Homomorphismus* oder *AM-H*) *von $\mathfrak{M}$ nach $\mathfrak{M}'$*, falls $rk = rk' \circ \nu$ und $m = m' \circ \nu$, also falls folgende Diagramme kommutieren:

$$\begin{tikzcd} \mathbb{P}(X) \arrow[rr, "\nu"] \arrow[dr, "rk"'] & & \mathbb{P}(X'), \arrow[dl, "rk'"] \\ & \mathbb{N} & \end{tikzcd} \qquad \begin{tikzcd} \mathbb{P}(X) \arrow[rr, "\nu"] \arrow[dr, "m"'] & & \mathbb{P}(X') . \arrow[dl, "m'"] \\ & \mathbb{N} & \end{tikzcd}$$

Bemerkung. Jeder A-M-Homomorphismus von (X, rk, m) nach (X', rk', m') ist nach Definition und mit Satz 1.3.2 auch ein Matroide-Homomorphismus von (X, rk) nach (X', rk').

Theorem 2.2.2. *Sei (X, rk) ein Matroid, m eine Abbildung von der Potenzmenge von X in die natürlichen Zahlen, $\mathfrak{M}' = (X', rk', m')$ ein arithmetisches Matroid und ν ein Matroide-Homomorphismus von (X, rk) nach (X', rk') mit $m = m' \circ \nu$. Dann gilt:*

(i) Es erfüllt $\mathfrak{M} := (X, rk, m)$ die Axiome (m1) bis (m4).

(ii) Für $A \subseteq B \subseteq X$ mit $rk(A) = rk(B)$ gilt:

$$\mu_B(A) = \begin{cases} \mu'_{\nu(B)}(\nu(A)), & \text{falls } \nu(A) \cap \nu(B \backslash A) = \emptyset, \\ 0, & \text{falls } \nu(A) \cap \nu(B \backslash A) \neq \emptyset. \end{cases}$$

Beweis. (i) Mit Lemma 1.3.2 (iii) werden (m1) und (m2) direkt von $\mathfrak{M}'$ vererbt. Bleiben (m3) und (m4) zu zeigen.

(m3): Sei $A \subseteq B \subseteq X$ und $B = A \dot\cup F \dot\cup T$, sodass für alle $A \subseteq C \subseteq B$ gilt, dass $rk(C) = rk(A) + |C \cap F|$. Wir wollen (m′3) anwenden. Beachte, dass für alle Teilmengen D von X' gilt:

$$D \subseteq \nu(B) \Rightarrow \nu\left(\nu\big|_B^{-1}(D)\right) = D. \tag{5}$$

Nach Lemma 2.0.2 (i) enthält F genau die Elemente aus $B \backslash A$, die unabhängig von A sind und T enthält genau die Elemente aus $B \backslash A$, die abhängig von A sind. Nach Lemma 1.3.2 (iii) enhält $\nu(F)$ dann genau alle Elemente aus $\nu(B \backslash A)$, die unabhängig von $\nu(A)$ sind und $\nu(T)$ enthält genau alle Elemente aus $\nu(B \backslash A)$, die abhängig von $\nu(A)$ sind. Es ist

$$\nu(B \backslash A) = (\nu(B) \backslash \nu(A)) \cup (\nu(B \backslash A) \cap \nu(A)),$$

also enthält F nur Elemente aus $\nu(B) \backslash \nu(A)$ (denn die übrigen Elemente von $\nu(B \backslash A)$ sind aus $\nu(A)$, also insbesondere abhängig von $\nu(A)$). Dann ist

$$\nu(B) = \nu(A) \dot\cup \nu(F) \dot\cup (\nu(T) \backslash \nu(A)). \tag{6}$$

Weiter ist nach Lemma 2.0.2 (ii) ist F unabhängig, also ist $\nu\big|_F$ nach Lemma 1.3.2(ii) injektiv. Dann gilt für alle $\nu(A) \subseteq D \subseteq \nu(B)$:

$$\begin{aligned}
rk'(D) &= rk'\left(\nu\left(\nu\big|_B^{-1}(D)\right)\right) && \text{nach 5} \\
&= rk\left(\nu\big|_B^{-1}(D)\right) \\
&= rk(A) + \left|F \cap \nu\big|_B^{-1}(D)\right| && \text{nach Vorraussetzung} \\
&= rk'(\nu(A)) + \left|\nu\left(F \cap \nu\big|_B^{-1}(D)\right)\right| && \text{da } \nu\big|_F \text{ injektiv} \\
&= rk'(\nu(A)) + \left|\nu(F) \cap \nu\left(\nu\big|_B^{-1}(D)\right)\right| && \text{da } \nu\big|_F \text{ injektiv} \\
&= rk'(\nu(A)) + |\nu(F) \cap D|,
\end{aligned}$$

zusammen mit (6) sind die Voraussetzungen für (m′3) erfüllt:

$$\begin{aligned} m(A)\cdot m(B) &= m'(\nu(A))\cdot m'(\nu(B)) \\ &= m'(\nu(A)\cup\nu(F))\cdot m'(\nu(A)\cup(\nu(T)\backslash\nu(A))) \quad \text{nach (m}'3) \\ &= m'(\nu(A\cup F))\cdot m'(\nu(A\cup T)) \\ &= m(A\cup F)\cdot m(A\cup T). \qquad \checkmark \end{aligned}$$

(m4): Folgt direkt aus Teil (ii) des Theorems.
Damit erfüllt $\mathfrak{M}$ die Axiome (m1) bis (m4). □

(ii) Sei $A \subseteq B \subseteq X$ mit $rk(A) = rk(B)$. Es ist

$$rk'(\nu(A)) = rk(A) = rk(B) = rk'(\nu(B)),$$

womit $\mu'_{\nu(B)}(\nu(A))$ definiert ist und

$$\begin{aligned} \mu_B(A) &= \sum_{A\subseteq C\subseteq B} (-1)^{|C\backslash A|} m(C) \qquad \text{nach Definition} \\ &= \sum_{A\subseteq C\subseteq B} (-1)^{|C\backslash A|} m'(\nu(C)) \\ &= \sum_{\nu(A)\subseteq K\subseteq \nu(B)} \left(\sum_{\substack{J\subseteq B\backslash A \\ \nu(J\cup A)=K}} (-1)^{|J|} \right) m'(K). \end{aligned}$$

Es ist also hinreichend zu zeigen, dass für alle $\nu(A) \subseteq K \subseteq \nu(B)$ gilt:

$$\sum_{\substack{J\subseteq B\backslash A \\ \nu(J\cup A)=K}} (-1)^{|J|} = \begin{cases} (-1)^{|K\backslash \nu(A)|}, & \text{falls } \nu(A)\cap\nu(B\backslash A)=\emptyset, \\ 0, & \text{falls } \nu(A)\cap\nu(B\backslash A)\neq\emptyset. \end{cases} \tag{7}$$

Wir zeigen dies mittels Induktion über die Kardinalität von $K\backslash\nu(A)$. Beachte, dass $\nu(A)\cap\nu(B\backslash A)$ genau dann leer ist, wenn $\nu^{-1}(\nu(A))\cap B\backslash A$ leer ist.
Induktionsanfang: Sei $|K\backslash\nu(A)| = 0$ und sei $m = |\nu^{-1}(\nu(A))\cap(B\backslash A)|$. Dann ist $K = \nu(A)$ und $(-1)^{|K\backslash\nu(A)|} = 1$. Es folgt

$$\begin{aligned} \sum_{\substack{J\subseteq B\backslash A \\ \nu(J\cup A)=K}} (-1)^{|J|} &= \sum_{\substack{J\subseteq B\backslash A \\ \nu(J\cup A)=\nu(A)}} (-1)^{|J|} = \sum_{J\subseteq \nu^{-1}(\nu(A))\cap(B\backslash A)} (-1)^{|J|} \\ &= \sum_{i=0}^{m} \binom{m}{i} (-1)^i = \sum_{i=0}^{m} \binom{m}{i} (-1)^i 1^{m-i} \\ &= (1-1)^m \qquad \text{nach binomischem Lehrsatz} \\ &= \begin{cases} (-1)^{|K\backslash\nu(A)|}, & \text{falls } m=0, \text{ also falls } \nu(A)\cap\nu(B\backslash A)=\emptyset, \\ 0, & \text{falls } m\neq 0, \text{ also falls } \nu(A)\cap\nu(B\backslash A)\neq\emptyset. \end{cases} \end{aligned}$$

Induktionsvoraussetzung: Für festes $n\in\mathbb{N}$, $n < |\nu(B)|$ und alle $\nu(A)\subseteq K\subseteq\nu(B)$ mit $|K\backslash\nu(A)| = n$ gelte:

$$\sum_{\substack{J\subseteq B\backslash A \\ \nu(J\cup A)=K}} (-1)^{|J|} = \begin{cases} (-1)^{n}, & \text{falls } \nu(A)\cap\nu(B\backslash A)=\emptyset, \\ 0, & \text{falls } \nu(A)\cap\nu(B\backslash A)\neq\emptyset. \end{cases} \tag{8}$$

Induktionsschritt: Sei $\nu(A) \subseteq K \subseteq \nu(B)$ mit $|K \backslash \nu(A)| = n+1$, also $K \backslash \nu(A) \neq \emptyset$. Da K Teilmenge von $\nu(B)$ ist, gilt dann auch $\nu^{-1}(K \backslash \nu(A)) \cap B \neq \emptyset$. Wir können also ein $b \in \nu^{-1}(K) \cap B$ mit $\nu(b) \notin \nu(A)$ wählen und erhalten damit

$$\begin{aligned}\{J \subseteq B \backslash A \mid \nu(J \cup A) = K\} = \{I \mid\ & I \subseteq (B \backslash \{b\}) \backslash A,\ \nu(I \cup A) = K\} \\ &\dot\cup\, \{I \cup \{b\} \mid I \subseteq (B \backslash \{b\}) \backslash A,\ \nu(I \cup A) = K\} \\ &\dot\cup\, \{I \cup \{b\} \mid I \subseteq (B \backslash \{b\}) \backslash A,\ \nu(I \cup A) = K \backslash \{\nu(b)\}\}.\end{aligned}$$

Hierbei stehen in der ersten der drei rechts vereinigten Mengen die Elemente aus $\{J \subseteq B \backslash A \mid \nu(J \cup A) = K\}$, die b nicht enthalten. In der zweiten Menge stehen die Elemente, die b und auch andere Elemente, die durch ν auf $\nu(b)$ abgebildet werden, enthalten. In der dritten Menge stehen die Elemente, die b und keine anderen Elemente, die durch ν auf $\nu(b)$ abgebildet werden, enthalten. Damit folgt:

$$\begin{aligned}\sum_{\substack{J \subseteq B \backslash A \\ \nu(J \cup A) = K}} (-1)^{|J|} &= \sum_{\substack{I \subseteq (B \backslash \{b\}) \backslash A \\ \nu(I \cup A) = K}} (-1)^{|I|} + \sum_{\substack{I \subseteq (B \backslash \{b\}) \backslash A \\ \nu(I \cup A) = K}} (-1)^{|I \cup \{b\}|} + \sum_{\substack{I \subseteq (B \backslash \{b\}) \backslash A \\ \nu(I \cup A) = K \backslash \{\nu(b)\}}} (-1)^{|I \cup \{b\}|} \\ &= \sum_{\substack{I \subseteq (B \backslash \{b\}) \backslash A \\ \nu(I \cup A) = K}} (-1)^{|I|} - \sum_{\substack{I \subseteq (B \backslash \{b\}) \backslash A \\ \nu(I \cup A) = K}} (-1)^{|I|} - \sum_{\substack{I \subseteq (B \backslash \{b\}) \backslash A \\ \nu(I \cup A) = K \backslash \{\nu(b)\}}} (-1)^{|I|} \\ &= -\sum_{\substack{I \subseteq (B \backslash \{b\}) \backslash A \\ \nu(I \cup A) = K \backslash \{\nu(b)\}}} (-1)^{|I|}\end{aligned}$$

Es ist $\nu(A) \subseteq K \backslash \{\nu(b)\} \subseteq \nu(B)$ und nach Wahl von b ist

$$|(K \backslash \{\nu(b)\}) \backslash \nu(A)| = |K \backslash \nu(A)| - 1 = n,$$

also nach Induktionsvoraussetzung

$$\sum_{\substack{J \subseteq B \backslash A \\ \nu(J \cup A) = K}} (-1)^{|J|} = \begin{cases} -(-1)^n = (-1)^{n+1}, & \text{falls } \nu(A) \cap \nu(B \backslash A) = \emptyset, \\ 0, & \text{falls } \nu(A) \cap \nu(B \backslash A) \neq \emptyset. \end{cases}$$

□

Scholium 2.2.3. *Seien $\mathfrak{M} = (X, rk)$, $\mathfrak{M}' = (X', rk')$ Matroide, m, m' Funktionen, die von den Potenzmengen von X und X' respektive in die natürlichen Zahlen abbilden und ν sei ein Matroide-Homomorphismus von $\mathfrak{M}$ nach $\mathfrak{M}'$ mit $m = m' \circ \nu$. Dann gelten nach obigem Beweis folgende Implikationen:*

$$\begin{aligned}(m1) &\Leftarrow (m'1) \\ (m2) &\Leftarrow (m'2) \\ (m3) &\Leftarrow (m'3) \\ (m4) &\Leftarrow (m'4)\end{aligned}$$

Bemerkung. Es ist noch zu prüfen, ob in Theorem 2.2.2 auch (m5) folgt.

2.3 Darstellbarkeit

In diesem Abschnitt werden wir analoge Begriffe zur Darstellbarkeit eines arithmetischen Matroids über Listen entsprechend [1] definieren (siehe Einleitung). Hierzu definieren wir für arithmetische Matroide über Mengen zunächst den Begriff des *dargestellten Tripels*, verallgemeinern ihn dann auf den Begriff des *darstellbaren Tripels* und zeigen, dass dargestellte Tripel arithmetische Matroide sind, die war ebenfalls *dargestellt* nennen. Im Rahmen dieses Beweises zeigen wir weiter, dass das Dual eines dargestellten arithmetischen Matroids darstellbar ist.

In diesem Abschnitt betrachten wir wie in Abschnitt 1.4 stets X als endliche Teilmenge einer endlich erzeugten, abelschen Gruppe G, also

$$G \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{s} \mathbb{Z}_{p_i}$$

mit $r, s \in \mathbb{N}$ und p_i prim für $i = 1, \ldots, s$.

Für jede Teilmenge A von X bezeichne G_A im folgenden stets die maximale Untergruppe von G, sodass $\langle A \rangle$ Untergruppe von G_A ist und der Index $|G_A : \langle A \rangle|$ endlich. (Für eine Untergruppe H_1 von H_2 bezeichnet der Index $|H_2 : H_1|$ die Anzahl der Linksnebenklassen von H_1 in H_2, siehe [2].) Beachte außerdem Bemerkung (1.4.1): Für jede Untergruppe H von G bezeichne stets H_f eine (beliebig gewählte) freie Untergruppe von H maximalen Rangs und $H_t = G_t \cap H$ die Elemente endlicher Ordnung von H.

Wir nehmen stets an, dass $\langle X \rangle$ endlichen Index in G hat, ansonsten ersetzen wir einfach G durch G_X.

Bemerkung 2.3.1 (zur eindeutigen Existenz von G_A). Wir schreiben $\oplus$ als direktes inneres Produkt und wählen eine Basis B von $\langle A \rangle_f$. Wähle ϕ als Isomorphismus von G nach $\mathbb{Z}^r \oplus \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i}$, so, dass die Elemente aus B durch ϕ auf Einheitsvektoren oder Vielfache von Einheitsvektoren in $\mathbb{Z}^r$ abgebildet werden. Dann ist das Bild von $\langle A \rangle_f$ unter ϕ gleich $\bigoplus_{i=1}^{r} m_i \cdot \mathbb{Z}$ für bestimmte $m_1, \ldots, m_r \in \mathbb{N}$. Es folgt

$$\begin{aligned}
\phi(\langle A \rangle) &= \phi(\langle A \rangle_f \oplus \langle A \rangle_t) \\
&= \phi(\langle A \rangle_f) \oplus \phi(\langle A \rangle_t) && \text{da } \phi \text{ Isomorphismus} \\
&= \left(\bigoplus_{i=1}^{r} m_i \cdot \mathbb{Z} \right) \oplus \phi(\langle A \rangle_t) \\
&=: \langle A' \rangle.
\end{aligned}$$

Beachte, dass die Elemente aus $\phi(\langle A \rangle_t)$ alle endlicher Ordnung sind. Sei $\chi \colon \mathbb{N} \to \{0, 1\}$ die Indikatorfunktion von $\mathbb{N} \backslash \{0\}$. Dann gilt für die maximale Untergruppe $G'_{A'}$, sodass der Index von $\langle A' \rangle$ in $G'_{A'}$ endlich ist:

$$G'_{A'} = \left(\bigoplus_{i=1}^{r} \chi(m_i) \cdot \mathbb{Z} \right) \oplus \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i}$$

und damit

$$
\begin{aligned}
G_A &= \phi^{-1}\left(\left(\bigoplus_{i=1}^{r}\chi(m_i)\cdot\mathbb{Z}\right)\oplus\bigoplus_{i=1}^{k}\mathbb{Z}_{p_i}\right)\\
&= \phi^{-1}\left(\bigoplus_{i=1}^{r}\chi(m_i)\cdot\mathbb{Z}\right)\oplus\phi^{-1}\left(\bigoplus_{i=1}^{k}\mathbb{Z}_{p_i}\right) && \text{da } \phi^{-1} \text{ Isomorphismus}\\
&= \underbrace{\phi^{-1}\left(\bigoplus_{i=1}^{r}\chi(m_i)\cdot\mathbb{Z}\right)}_{=:(G_A)_f}\oplus G_t,
\end{aligned}
$$

insbesondere existiert G_A, ist eindeutig bestimmt und hängt nur von $\chi(m_1),\dots,\chi(m_r)$ ab. Beachte, dass dann außerdem für alle Teilmengen A und B von X gilt:

$$(A\subseteq B\wedge Rang(\langle A\rangle_f)=Rang(\langle B\rangle_f))\Rightarrow G_A=G_B. \tag{9}$$

(Allerdings ist $(G_A)_f$ nicht eindeutig: sei $\langle f_1,\dots,f_l\rangle$ Erzeuger von $(G_A)_f$, dann gilt für alle $t_1,\dots,t_l\in G_t$, dass $\langle f_1,\dots f_l,\rangle+G_t=\langle f_1+t_1,\dots,f_l+t_l\rangle+G_t$, wobei die rechte Summe ebenfalls direkt ist.)

2.3.1 Dargestelltheit

Definition 2.3.2. Sei X endliche Teilmenge einer endlich erzeugten, abelschen Gruppe G und seien rk, m Funktionen mit:

(i) rk ist definiert durch

$$
\begin{aligned}
rk\colon \mathbb{P}(X) &\to \mathbb{N}\\
A &\mapsto Rang(\langle A\rangle_f),
\end{aligned}
$$

(ii) m ist definiert durch

$$
\begin{aligned}
m\colon \mathbb{P}(X) &\to \mathbb{N}\\
A &\mapsto |G_A:\langle A\rangle_f|.
\end{aligned}
$$

Dann nennen wir das Tripel $(\mathfrak{M}_X,m)=(X,rk,m)$ *dargestellt (durch G)*.
Wir schreiben dann auch $\mathfrak{M}_X$ oder $\mathfrak{M}$ statt $(\mathfrak{M}_X,m)$.

Sofern nicht anders angegeben, sei in diesem Unterabschnitt stets (X,rk,m) dargestellt durch eine endlich erzeugte, abelschen Gruppe G.

Bemerkung 2.3.3. (i) Wir werden in diesem Abschnitt beweisen, dass dargestellte Tripel auch arithmetische Matroide sind. Das heißt, wir haben den Begriff der Dargestelltheit für arithmetische Matroide definiert.

(ii) Bezüglich rk und m steht unsere Definition der Dargestellheit zur Definition der Darstellbarkeit in [1] wie folgt in Beziehung:

Sei (X',rk',m') ein darstellbares arithmetisches Matroid nach [1], also X' eine Liste. Wir können X' schreiben als $X'=\{(x_i,i)\mid i\in I\}$ für ein endliches $I\subseteq\mathbb{N}$ und (X',rk',m') auffassen als arithmetisches Matroid mit X' als Menge. Betrachte die Abbildung $\nu\colon(x_i,i)\mapsto x_i$ mit Definitionsbereich X', setze $X=\nu(X')$ und betrachte (X, rk, m) mit rk und m so, dass das Tripel dargestellt ist. Da für jedes $J \subseteq I$ und $A = \{(x_i, i) \mid i \in J\}$ die Rang- und Vielfachheitsfunktion in [1] nur von der erzeugten Untergruppe von $\{x_i \mid i \in J\}$ abhängen, ist $rk' = rk \circ \nu$ und $m' = m \circ \nu$.

(iii) Wir haben rk und m gruppentheoretisch definiert, das heißt: Ist $\phi\colon G \to G'$ ein Gruppenisomorphismus, so ist $(\phi(X), rk \circ \phi^{-1}, m \circ \phi^{-1})$ dargestellt durch G' und für alle $A \subseteq X$ ist $rk(A) = (rk \circ \phi^{-1})(\phi(A))$ und $m(A) = (m \circ \phi^{-1})(\phi(A))$. Wir können in dem Fall ohne Einschränkung annehmen, dass $G = G'$ gilt.

Bemerkung 2.3.4. Nach Satz (1.4.6) ist (X, rk) ein Matroid. Um zu zeigen, dass (X, rk, m) ein arithmetisches Matroid ist, muss also nur noch $(m1)$ bis $(m5)$ gezeigt werden. In diesem Abschnitt werden wir (m1), (m3) und (m4) zeigen. Aus dem nachfolgenden Abschnitt wird $(m2)$ und $(m5)$ folgen.

Beim Nachweis der Axiome helfen uns folgende Lemmata:

Lemma 2.3.5. *Falls in dargesellten Tripeln (X, rk, m) gilt, dass $A \subseteq B \subseteq X$ und $rk(A) = rk(B)$ ist, dann ist auch $G_A = G_B$.*

Beweis. Die Aussage ist genau (9). □

Lemma 2.3.6. *Wir können bei Betrachtung von $m(A)$ in dargestellten Tripeln (X, rk, m) ohne Einschränkung annehmen, dass für $\langle A\rangle = \langle A\rangle_f \oplus \langle A\rangle_t$ gilt: $\langle A\rangle_f$ ist Teilmenge von G_f.*

Beweis. Sei H Untergruppe von $G = G_f \oplus G_t$ und $H = H_f \oplus H_t$ entsprechend Notation (1.4.1). Außerdem habe H endlichen Index in G. Wähle H'_f als Untergruppe von G_f so, dass $H'_f \oplus G_t = H + G_t = H_f \oplus G_t$. Mit dem zweiten Isomorphiesatz (siehe [2]) ist:

$$\frac{G}{H + G_t} \cong \frac{G/G_t}{(H + G_t)/G_t} = \frac{(G_f \oplus G_t)/G_t}{(H'_f \oplus G_t)/G_t} = \frac{G_f/G_t}{H'_f/G_t} \cong G_f/H'_f \tag{10}$$

und mit dem ersten Isomorphiesatz:

$$\frac{H + G_t}{H} \cong \frac{G_t}{H \cap G_t} = \frac{G_t}{H_t}. \tag{11}$$

Dann haben wir:

$$\begin{aligned}
\frac{|G : H|}{|G_t : H_t|} &= \frac{|G/H|}{|G_t/H_t|} && \text{per Definition}\\
&= \frac{|G/H|}{|(H + G_t)/H|} && \text{nach (11)}\\
&= |(G/H) : (H + G_t)/H| && \text{nach Satz von Lagrange (siehe [2])}\\
&= |G/(H + G_t)| && \text{nach 2. Isomorphiesatz}\\
&= |G_f : H'_f| && \text{nach (10)}
\end{aligned}$$

und damit

$$|G : H| = |G_f : H'_f| \cdot |G_t : H_t|. \tag{12}$$

Insbesondere hängt $|G : H|$ nicht von der Wahl von H_f ab und ist durch H'_f eindeutig bestimmt. (Wir erinnern uns, dass H_t bei gegebener Grupe H ebenfalls eindeutig bestimmt ist.) Da für $A \subseteq X$ die Funktion m gerade über den (endlichen) Index von $\langle A\rangle$ in G_A definiert ist, folgt die Behauptung. □

Mit (12) ergibt sich folgende nützliche Rechenregel:

Scholium 2.3.7. *Es ist*

$$m(A) = |(G_A)_f : \langle A\rangle_f| \cdot |G_t : \langle A\rangle_t|,$$

wobei wir entsprechend Lemma (2.3.6) davon ausgehen, dass $\langle A\rangle_f$ Teilmenge von $(G_A)_f$ ist.

Bemerkung 2.3.8. Wir können die Funktionen $rk, m \colon \mathbb{P}(X) \to \mathbb{N}$ auf die Menge $\varepsilon(G)$ der endlichen Teilmengen von G fortsetzen durch:

$$\hat{rk} \colon \varepsilon(G) \to \mathbb{N} \qquad\qquad \hat{m} \colon \varepsilon(G) \to \mathbb{N}$$
$$A \mapsto Rang(\langle A\rangle_f), \qquad\qquad A \mapsto |G_A : \langle A\rangle_f|.$$

Dann ist nach Definition für alle Y aus $\varepsilon(G)$ das Tripel $\left(Y, \hat{rk}\big|_Y, \hat{m}\big|_Y\right)$ dargestellt durch G_Y.

Da die Abbildungsvorschrift für alle Y aus $\varepsilon(G)$ und für alle endlich erzeugten Gruppen G die gleiche ist, schreiben wir – unabhängig von der Wahl von Y und G – einfach rk für $\hat{rk}\big|_Y$ und m für $\hat{m}\big|_Y$, solange G klar ist.

Satz 2.3.9. *Sei $\mathfrak{M} = (X, rk, m)$ dargestellt durch G. Dann erfüllt $\mathfrak{M}$ die Axiome (m1), (m3) und (m4).*

Beweis. (m1): Sei $A \subseteq X$ und $x \in X$ abhängig von A, das heißt $rk(A) = rk(A \cup \{x\})$. Da A Teilmenge von $A \cup \{x\}$ ist, folgt mit Lemma 2.3.5, dass $G_A = G_{A\cup\{x\}}$. Dann ist

$$\begin{aligned}
m(A \cup \{x\}) &= |G_{A\cup\{x\}} : \langle A \cup \{x\}\rangle| \\
&= |G_A : \langle A \cup \{x\}\rangle| \\
&= \left|\frac{G_A/\langle A\rangle}{\langle A \cup \{x\}\rangle/\langle A\rangle}\right| && \text{nach zweitem Isomorphiesatz} \\
&= \frac{|G_A/\langle A\rangle|}{|\langle A \cup \{x\}\rangle/\langle A\rangle|} && \text{nach Satz von Lagrange}
\end{aligned}$$

und damit

$$m(A \cup \{x\}) \cdot |\langle A \cup \{x\}\rangle : \langle A\rangle| = |G_A : \langle A\rangle| = m(A),$$

das heißt $m(A \cup \{x\})$ teilt $m(A)$. □

(m4): Werden wir in Lemma 4.1.12 zeigen. □

(m3): Sei $A \subseteq B \subseteq X$ und $B = A \,\dot\cup\, F \,\dot\cup\, T$ so, dass für alle $A \subseteq C \subseteq B$ gilt, dass $rk(C) = rk(A) + |C \cap F|$. Beachte, dass nach Lemma 2.0.2 (i) alle Elemente aus T abhängig von A (und auch von B) sind und alle Elemente aus F unabhängig von A. Es ist

$$\begin{aligned}
m(B) &= |G_B : \langle B\rangle| \\
&= \left|\frac{G_B : \langle A \cup F\rangle}{\langle B\rangle : \langle A \cup F\rangle}\right| && \text{nach 2. Isomorphiesatz} \\
&= \frac{|G_B : \langle A \cup F\rangle|}{|\langle B\rangle : \langle A \cup F\rangle|} && \text{nach Satz von Lagrange} \\
&= \frac{|G_{A\cup F} : \langle A \cup F\rangle|}{|\langle B\rangle : \langle A \cup F\rangle|} && \text{nach Lemma (2.3.6)} \\
&= \frac{m(A \cup F)}{|\langle B\rangle : \langle A \cup F\rangle|}
\end{aligned}$$

und

$$\begin{aligned}
m(A \cup T) &= |G_{A\cup T} : \langle A \cup T\rangle| & \\
&= |G_A : \langle A \cup T\rangle| & \text{nach Lemma (2.3.6)}\\
&= \left|\frac{G_A : \langle A\rangle}{\langle A \cup T\rangle : \langle A\rangle}\right| & \text{nach 2. Isomorphiesatz}\\
&= \frac{|G_A : \langle A\rangle|}{|\langle A \cup T\rangle : \langle A\rangle|} & \text{nach Satz von Lagrange}\\
&= \frac{m(A)}{|\langle A \cup T\rangle : \langle A\rangle|},
\end{aligned}$$

also

$$\frac{m(A)}{|\langle A \cup T\rangle : \langle A\rangle|} \cdot m(B) = m(A \cup T) \cdot \frac{m(A \cup F)}{|\langle B\rangle : \langle A \cup F\rangle|}. \tag{13}$$

Nach erstem Isomorphiesatz ist

$$\frac{\langle B\rangle}{\langle A \cup F\rangle} = \frac{\langle A \cup T\rangle + \langle A \cup F\rangle}{\langle A \cup F\rangle} \cong \frac{\langle A \cup T\rangle}{\langle A \cup T\rangle \cap \langle A \cup F\rangle}$$

Wir zeigen, dass $\langle A \cup T\rangle \cap \langle A \cup F\rangle = \langle A\rangle$:

Beweis. Mit $\langle A\rangle \subseteq \langle A \cup T\rangle$ und $\langle A\rangle \subseteq \langle A \cup F\rangle$ folgt $\langle A\rangle \subseteq \langle A \cup T\rangle \cap \langle A \cup F\rangle$. Sei weiter

$$\langle A \cup T\rangle \cap \langle A \cup F\rangle \supsetneq \langle A\rangle,$$

das heißt es gibt ein $h \in (\langle A \cup T\rangle \cap \langle A \cup F\rangle)\backslash\langle A\rangle$. Dann gibt es $\widetilde{a_1}, \widetilde{a_2} \in \langle A\rangle$, $\widetilde{t} \in \langle T\rangle\backslash\{e\}$ und $\widetilde{f} \in \langle F\rangle\backslash\{e\}$ mit

$$h = \widetilde{a_1} + \widetilde{t} = \widetilde{a_2} + \widetilde{f}.$$

Insbesondere ist dann

$$\widetilde{f} = (\widetilde{a_1} - \widetilde{a_2}) + \widetilde{t} \in \langle A \cup T\rangle.$$

Nach Lemma 2.0.2 (i) sind alle Elemente aus T abhängig von A, so dass wir mit Lemma 1.1.6 erhalten:

$$rk(A \cup \{\widetilde{f}\}) \geq rk(A) = rk(A \cup T) = rk(A \cup T \cup \{\widetilde{f}\}) \geq rk(A \cup \{\widetilde{f}\}),$$

also $rk(A \cup \{\widetilde{f}\}) = rk(A)$. Das heißt, dass $\widetilde{f}$ abhängig von A ist, wobei wir rk entsprechend Lemma 2.3.8 auf $\mathbb{P}(X \cup \{\widetilde{f}\})$ fortsetzen. Sei nun I unabhängige Teilmenge von A mit $rk(A) = |I|$. Dann ist $\widetilde{f}$ abhängig von I nach Lemma 1.1.8 und $F \cup I$ unabhängig nach Lemma 2.0.2 (iii). Nach Bemerkung 1.4.4 bedeutet das mit den dort definierten Schreibweisen, dass $F_f \dot{\cup} I_f$ linear unabhängig bezüglich $\mathbb{Q}$ ist und $\widetilde{f_f} \in \langle F\rangle_f$ linear abhängig von I_f ist. Ein Widerspruch.
Also ist $\langle A \cup T\rangle \cap \langle A \cup F\rangle = \langle A\rangle$. □

Also ist $\langle B\rangle/\langle A \cup F\rangle$ isomorph zu $\langle A \cup T\rangle/\langle A\rangle$ und damit

$$|\langle A \cup T\rangle : \langle A\rangle| = |\langle B\rangle : \langle A \cup F\rangle|.$$

Mit (13) folgt die Behauptung. □

2.3.2 Darstellbarkeit

In diesem Abschnitt werden wir den Begriff des darstellbaren Tripels (X, rk, m) definieren. Wir werden zeigen, dass das „Dual" (X, rk^*, m^*) eines dargestellten Tripels (X, rk, m) darstellbar ist. Daraus werden wir (m2) und (m5) für dargestellte Tripel folgern, sodass mit vorigem Abschnitt dargestellte Tripel tatsächlich arithmetische Matroide sind, die wir *dargestellte arithmetische Matroide* nennen werden. Wir werden weiter folgern, dass darstellbare Tripel (m1) bis (m4) erfüllen und die Definition des *darstellbaren arithmetischen Matroids* darauf aufbauen. Schließlich werden wir wie angekündigt folgern, dass das Dual eines dargestellten arithmetischen Matroids darstellbar ist.

Definition 2.3.10. Wir nennen das Tripel $\mathfrak{M} = \mathfrak{M}_X = (X, rk, m)$ *darstellbar (durch G)*, wenn es ein dargestelltes Tripel $\mathfrak{M}' = \mathfrak{M}'_{X'} = (X', rk', m')$ durch G und eine surjektive Abbildung $\nu\colon X \to X'$ gibt mit $rk = rk' \circ \nu$ und $m = m' \circ \nu$.

In dem Fall heißt ν *(Arithmetische-Matroide- oder AM-)Darstellung (von* $\mathfrak{M}$ *nach* $\mathfrak{M}'$*)* und $\mathfrak{M}'$ heißt *darstellendes Tripel von* $\mathfrak{M}$. Wir sagen auch $\mathfrak{M}'$ *stellt* $\mathfrak{M}$ *dar*.

Bemerkung. Für jedes dargestellte Tripel (X, rk, m) ist die Identität auf X eine Darstellung. Insbesondere ist jedes dargestellte Tripel auch darstellbar.

Sofern nicht anders angegeben, sei in diesem Unterabschnitt im Folgenden stets (X, rk, m) dargestelltes bezüglich der endlich erzeugten, abelschen Gruppe G. Nach Bemerkung 2.3.3 (iii) nehmen wir außerdem ohne Einschränkung an, dass $G = \mathbb{Z}^r \oplus \bigoplus_{i=1}^{s} \mathbb{Z}_{p_i}$ mit $r, s, p_i \in \mathbb{N}$ und p_i prim für $i = 1 \ldots, s$.

Theorem 2.3.11. *Sei* $(\mathfrak{M}_X, m)$ *dargestelltes Tripel. Dann ist* $(\mathfrak{M}^*_X, m^*)$ *darstellbar, wobei* $\mathfrak{M}^*$ *das Dual des Matroids* $\mathfrak{M}$ *sei und* $m^*(A) := m(X \backslash A)$ *für alle* $A \subseteq X$.

Beim Beweis des Theorems benutzen wir nachfolgende Schreibweisen und Lemmata:

Notation. Sei $n, r \in \mathbb{N}$, $K = \{k_1, \ldots, k_n\} \subseteq \mathbb{N}$, $k_j < k_{j+1}$ für $j = 1, \ldots, n-1$ und $A = \{a_{k_1}, \ldots, a_{k_n}\} \subseteq \mathbb{Z}^r$. Wir bezeichnen mit

$$[A] := ((a_{k_j})_i)_{\substack{1 \le i \le r \\ 1 \le j \le n}} \in M(r \times n, \mathbb{Q})$$

die Matrix mit den Spalten $[A]^{(j)} = a_{k_j}$ für $j = 1, \ldots, n$.

Geben wir K nicht an, so spielt die Reihenfolge der Spalten für uns keine Rolle.

Lemma 2.3.12. *Sei G frei abelsch, also ohne Einschränkung* $G = \mathbb{Z}^r$. *Dann gilt für jede Teilmenge A von X:* $m(A)$ *ist der größte gemeinsame Teiler der Minoren der Ordnung* $rk(A) = Rang([A])$ *der Matrix* $[A]$, *das heißt für* $A = \{a_1, \ldots, a_k\}$ *gilt:*

$$m(A) = ggT\left\{\det\left(((a_j)_i)_{\substack{i \in I \\ j \in J}}\right) \,\middle|\, I \subseteq \{1, \ldots, r\}, J \subseteq \{1, \ldots, k\}, |I| = |J| = rk(A)\right\},$$

wobei wir $ggT(\emptyset) = 1$ *setzen. Beachte, dass wir auf die Forderung des vollen Rangs der Untermatrizen verzichten können, da die Determinante einer Untermatrix, die nicht vollen Rang hat, null ist, also von jeder Zahl geteilt wird und wir den größten gemeinsamen Teiler über einer von* $\{0\}$ *verschiedenen Menge bilden.*

Beachte außerdem, dass es keine Rolle spielt, ob wir die Elemente aus A mehrfach in die Spalten schreiben, da wir ohne Einschränkung nur quadratische Untermatrizen mit vollem Rang betrachten. Insbesondere gilt für alle Teilmengen A, B von X: $m(A \cup B)$ *ist der größte gemeinsame Teiler der Minoren der Ordnung* $rk(A \cup B) = Rang\,(([A] \mid [B]))$ *der Matrix* $([A] \mid [B])$.

Beweis. Siehe [4], Theorem 2.2.

Notation. Bei gegebener $(n \times m)$ Matrix A bezeichnen wir für $k \in \{1, \ldots, \min\{n, m\}\}$ die Menge der Minoren der Ordnung k von A mit $Minors_k(A)$. Insbesondere können wir dann in obigem Lemma einfacher schreiben:

$$m(A) = \mathrm{ggT}(Minors_{rk(A)}([A])).$$

Beweis von Theorem 2.3.11. Sei $\mathfrak{M} = (X, rk, m)$ dargestellt durch die endlich erzeugte, abelsche Gruppe

$$G = \mathbb{Z}^r \oplus \bigoplus_{i=1}^{s} \mathbb{Z}_{p_i},$$

wobei $r, s \in \mathbb{N}$ und p_i prim für $i = 1, \ldots, s$. Beachte im folgenden Beweis Bemerkung 2.3.3 (iii) bezüglich Gruppenisomorphismen.

Wir suchen ein dargestelltes Tripel $\mathfrak{M}' = (X', rk', m')$, das $\mathfrak{M}^* := (X, rk^*, m^*)$ darstellt.

Betrachte die Menge

$$Q = \left\{ q_i \in \mathbb{Z}^{r+s} \;\middle|\; (q_i)_j = \begin{cases} p_i & \text{für } j = r + i \\ 0 & \text{sonst} \end{cases}, i \in \{1, \ldots, s\} \right\} = (p_1 \cdot e_{r+1}, \ldots, p_s \cdot e_{r+s}),$$

wobei die e_i die Einheitsvektoren in $\mathbb{Z}^{r+s}$ bezeichnen. Dann ist

$$G = \mathbb{Z}^r \oplus \bigoplus_{i=1}^{s} \mathbb{Z}_{p_i} \cong \mathbb{Z}^{r+s}/\langle Q \rangle$$

und die Elemente von X können geschrieben werden als Nebenklassen $\overline{x_i} = x_i + \langle Q \rangle$ für $i = 1 \ldots n$, wobei $n = |X|$. Wir wählen zu jeder Nebenklasse $\overline{x_i}$ aus X einen beliebigen Repräsentanten x_i und setzen

$$\widetilde{X} := \{x_1, \ldots, x_n\} \subseteq \mathbb{Z}^{r+s}.$$

Betrachte die $(r + s) \times (n + s)$-Matrix $\left([\widetilde{X}] \,\middle|\, [Q]\right)$, deren Spalten die Vektoren $x_1, \ldots, x_n$ gefolgt von den Vektoren $q_1, \ldots, q_s$ sind, also

$$\left([\widetilde{X}] \,\middle|\, [Q]\right) = \begin{pmatrix} (x_1)_1 & \ldots & (x_n)_1 & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ (x_1)_r & \ldots & (x_n)_r & p_1 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ (x_1)_{r+s} & \ldots & (x_n)_{r+s} & 0 & \ldots & p_s \end{pmatrix}.$$

Bezeichne mit Q' die Menge der Zeilen von $\left([\widetilde{X}] \,\middle|\, [Q]\right)$, also

$$\begin{aligned} Q' &= \left\{ \left([\widetilde{X}] \,\middle|\, [Q]\right)_{(i)} \,\middle|\, i \in \{1, \ldots, r + s\} \right\} \\ &= \left\{ \begin{pmatrix} (x_1)_1 \\ \vdots \\ (x_n)_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} (x_1)_{r-1} \\ \vdots \\ (x_n)_{r-1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} (x_1)_r \\ \vdots \\ (x_n)_r \\ p_1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} (x_1)_{r+s} \\ \vdots \\ (x_n)_{r+s} \\ 0 \\ \vdots \\ p_s \end{pmatrix} \right\} \subseteq \mathbb{Z}^{n+s}. \end{aligned}$$

Sei nun $G' := \mathbb{Z}^{n+s}/\langle Q'\rangle$ und $X' \subseteq G'$ definiert als

$$X' := \{e_i + \langle Q'\rangle \bigm| i \in \{1,\dots,n\}\},$$

wobei die e_i Einheitsvektoren in $\mathbb{Z}^{n+s}$ bezeichnen. Wir schreiben wieder $\overline{e_i} = e_i + \langle Q'\rangle$ für die entsprechenden Nebenklassen von $\langle Q'\rangle$. Betrachte das dargestellte Tripel $\mathfrak{M}' = (X', rk', m')$ durch $G' := \mathbb{Z}^{n+s}/\langle Q'\rangle$, das heißt wir wählen

$$\begin{aligned} rk' \colon \mathbb{P}(X') &\to \mathbb{N} \\ A &\mapsto Rang(\langle A\rangle_f), \end{aligned} \qquad\qquad \begin{aligned} m' \colon \mathbb{P}(X') &\to \mathbb{N} \\ A &\mapsto |G'_A : \langle A\rangle_f|. \end{aligned}$$

Wir wollen zeigen, dass die surjektive Abbildung

$$\begin{aligned} \nu \colon X &\to X' \\ \overline{x_i} &\mapsto \overline{e_i} \end{aligned}$$

Darstellung von $\mathfrak{M}^*$ nach $\mathfrak{M}'$ ist.

Wir setzen aus Gründen der einfacheren Lesbarkeit für $I \subseteq \{1,\dots,n\}$:

$$\begin{aligned} x_I &:= \{x_i \mid i \in I\} \subseteq \widetilde{X} \subseteq \mathbb{Z}^{r+s} \\ \overline{x_I} &:= \{\overline{x_i} \mid i \in I\} \subseteq X \subseteq G \\ e_I &:= \{e_i \mid i \in I\} \qquad\ \subseteq \mathbb{Z}^{n+s} \\ \overline{e_I} &:= \{\overline{e_i} \mid i \in I\} \subseteq X' \subseteq G' \end{aligned}$$

Sei also $I \subseteq \{1,\dots,n\}$. Es ist $rk^*(\overline{x_I}) = |I| - rk(X) + rk(X\backslash\overline{x_I})$, $m^*(\overline{x_I}) = m(X\backslash\overline{x_I})$ und $\nu(\overline{x_I}) = \overline{e_I}$. Zu zeigen ist also

$$rk'(\overline{e_I}) = |I| - rk(X\backslash\overline{x_I}) + rk(X) \tag{14}$$

und

$$m'(\overline{e_I}) = m(X\backslash\overline{x_I}) \tag{15}$$

Zunächst machen wir ein paar Beobachtungen zu rk und rk' sowie zu m und m'. Im folgenden schreiben wir bei gegebener endlicher Teilmenge A einer der betrachteten endlich erzeugten, abelschen Gruppen $H \in \{\mathbb{Z}^{r+s}, G, \mathbb{Z}^{n+s}\}$ oft $rk(A)$ oder $m(A)$ und meinen damit entsprechend Bemerkung 2.3.8 das dargestellte Tripel (A, rk, m) durch H.

Beachte, dass $\overline{x_i} = x_i + \langle Q\rangle$. Dann ist

$$\langle x_I \cup Q\rangle/\langle Q\rangle = \langle x_I\rangle/\langle Q\rangle \cong \langle\overline{x_I}\rangle,$$

wobei wir links erzeugte Untergruppen in $\mathbb{Z}^{r+s}$ betrachten und rechts die erzeugte Untergruppe in G. Dann haben wir:

$$\begin{aligned} rk(\overline{x_I}) &= Rang(\langle\overline{x_I}\rangle_f) \\ &= Rang((\langle x_I \cup Q\rangle/\langle Q\rangle)_f) \\ &= Rang(\langle x_I \cup Q\rangle_f) - Rang(\langle Q\rangle_f) \qquad\qquad \text{da } \langle Q\rangle \subseteq \langle A \cup Q\rangle \\ &= rk(x_I \cup Q) - rk(Q). \end{aligned} \tag{16}$$

Analog erhalten wir

$$rk'(\overline{e_I}) = rk(e_I \cup Q') - rk(Q'). \tag{16'}$$

Sei weiter $T \subseteq \mathbb{Z}^{r+s}$ so gewählt, dass $\langle T\rangle/\langle Q\rangle$ die maximale Untergruppe von G ist, in der $\langle\overline{x_I}\rangle$ endlichen Index hat. Dann ist nach zweitem Isomorphiesatz (siehe [2])

$$\left|\frac{\langle T\rangle/\langle Q\rangle}{\langle x_I \cup Q\rangle/\langle Q\rangle}\right| = \left|\frac{\langle T\rangle}{\langle x_I \cup Q\rangle}\right|$$

und der Index auf der rechten Seite ist der maximale endliche Index von $\langle x_I \cup Q\rangle$ in Untergruppen von $\mathbb{Z}^{r+s}$ (sonst wäre $\langle T\rangle/\langle Q\rangle$ auf der linken Seite nicht maximal). Dann ist

$$m(\overline{x_I}) = m(x_I \cup Q) \tag{17}$$

und analog

$$m'(\overline{e_I}) = m(e_I \cup Q'). \tag{17'}$$

Wir können also um (14) und (15) zu zeigen in $\mathbb{Z}^{r+s}$ und $\mathbb{Z}^{n+s}$ rechnen.

Betrachten wir zunächst (14). Gemäß (16') bestimmen wir zunächst den Rang von $e_I \cup Q'$. Nach Lemma 1.4.3 (2) betrachten wir die $(n+s)\times(|I|+r+s)$-Matrix $([e_I] \mid [Q'])$ in deren ersten k Spalten die Elemente von e_I stehen und in deren letzten $(r+s)$ Spalten die Elemente von Q' stehen. $([e_I] \mid [Q'])$ hat nach Wahl von Q' die Form

$$([e_I] \mid [Q']) = \left(\begin{array}{c|c} [e_I] & [\widetilde{X}]^t \\ \hline 0 & [Q]^t \end{array}\right),$$

wobei wir hier zur Veranschaulichung die Elemente von e_I als Elemente aus $\mathbb{Z}^n$ betrachten, also $[e_I]$ als $n\times|I|$-Matrix. Nach Lemma 1.4.3 ist $rk(e_I \cup Q')$ gleich dem Rang der Matrix, also

$$rk(e_I \cup Q') = |I| + Rang(([x_{I^c}] \mid [Q])) = |I| + rk(x_{I^c} \cup Q) \quad \text{nach Lemma 1.4.3 (2)},$$

wobei $I^c := \{1, \dots, n\}\backslash I$ das Komplement von I in $\{1, \dots, n\}$ bezeichnet. Damit folgt:

$$\begin{aligned}
rk'(\overline{e_I}) &= rk(e_I \cup Q') - rk(Q') && \text{nach (16')}\\
&= |I| + rk(x_{I^c} \cup Q) - rk(Q') && \text{nach (16)}\\
&= |I| + rk(x_{I^c} \cup Q) - Rang\,([Q']) && \text{nach Lemma (1.4.3) (2)}\\
&= |I| + rk(x_{I^c} \cup Q) - Rang\left([Q']^t\right) && \text{siehe [5]}\\
&= |I| + rk(x_{I^c} \cup Q) - Rang\left(\left([\widetilde{X}] \;\middle|\; [Q]\right)\right) &&\\
&= |I| + rk(x_{I^c} \cup Q) - rk(\widetilde{X} \cup Q) && \text{nach Lemma (1.4.3) (2)}\\
&= |I| + (rk(x_{I^c} \cup Q) - rk(Q)) - (rk(\widetilde{X} \cup Q) - rk(Q)) && \text{nach Wahl von } Q'\\
&= |I| + rk(\overline{x_{I^c}}) - rk(X) && \text{nach (16)}\\
&= |I| + rk(X\backslash\overline{x_I}) - rk(X) &&\\
&= rk^*(\overline{x_I}), &&
\end{aligned}$$

also gilt (14). ✓

Zu (15): Nach (17') ist $m'(\overline{e_I}) = m(e_I \cup Q')$ und nach Lemma 2.3.12 müssen wir zur Berechnung von $m(e_I \cup Q')$ den größten gemeinsamen Teiler der Minoren der Ordnung $Rang\,([e_I] \mid [Q'])$ der Matrix

$$([e_I] \mid [Q']) = \left(\begin{array}{c|c} [e_I] & [\widetilde{X}]^t \\ \hline 0 & [Q]^t \end{array}\right),$$

bestimmen. In den ersten $|I|$ Spalten stehen paarweise verschiedene Einheitsvektoren. Für einen Minor der Ordnung $Rang\,([e_I] \mid [Q'])$ müssen dann offensichtlich die ersten $|I|$ Spalten der Matrix verwendet werden. Entwickeln wir bei der Berechnung dieser Minoren die entsprechende Determinante nach den ersten $|I|$ Spalten (nach Entwicklungssatz von Laplace, siehe [6]), so erhalten wir die Determinante einer Matrix, die durch Streichen der durch I indizierten Zeilen und der ersten $|I|$ Spalten entsteht. Da wir nur nach Spalten entwickelt haben, in denen Einheitsvektoren standen, ändert sich höchstens das Vorzeichen der Untermatrix, was auf die Teilbarkeit keine Auswirkung hat. Insbesondere ist $m(\overline{e_I})$ dann gleich dem größten gemeinsamen Teiler der Minoren der Ordnung

$$rk(e_I \cup Q') = Rang\Big(([e_I] \,\Big|\, [Q'])\Big) - |I| = Rang\Big(([x_{I^c}] \mid [Q])^t\Big) = rk(x_{I^c} \cup Q) \qquad (18)$$

der $(n - |I| + s) \times (r + s)$-Untermatrix $([x_{I^c}] \mid [Q])^t$. Insgesamt erhalten wir mit diesen Beobachtungen:

$$\begin{aligned}
m'(\overline{e_I}) &= m(e_I \cup Q') && \text{nach (17')}\\
&= \mathrm{ggT}\Big(Minors_{rk(e_I \cup Q')}\Big(([e_I] \mid [Q'])\Big)\Big) && \text{nach Lemma 2.3.12}\\
&= \mathrm{ggT}\Big(Minors_{rk(e_I \cup Q')-|I|}\Big(([x_{I^c}] \mid [Q])^t\Big)\Big) && \text{nach Entwicklungssatz von Laplace}\\
&= \mathrm{ggT}\Big(Minors_{rk(x_{I^c} \cup Q)}\Big(([x_{I^c}] \mid [Q])^t\Big)\Big) && \text{nach (18)}\\
&= \mathrm{ggT}\Big(Minors_{rk(x_{I^c} \cup Q)}\Big(([x_{I^c}] \mid [Q])\Big)\Big) &&\\
&= m(x_{I^c} \cup Q) && \text{nach Lemma 2.3.12}\\
&= m(\overline{x_{I^c}}) && \text{nach (17)}\\
&= m(X \backslash \overline{x_I}) &&\\
&= m^*(\overline{x_I}), &&
\end{aligned}$$

also gilt (15). ✓

Damit ist ν eine Darstellung von $\mathfrak{M}^*$ nach $\mathfrak{M}'$, also ist $\mathfrak{M}$ nach Definition darstellbar. □

Scholium 2.3.13. *Sei $\mathfrak{M}$ ein dargestelltes Matroid. Dann ist nach obigem Beweis das Dual $\mathfrak{M}^*$ ein darstellbares Tripel.*

Theorem 2.3.14. *Dargestellte Tripel sind arithmetische Matroide.*

Beweis. Sei $\mathfrak{M} = (X, rk, m)$ dargestellt durch G und $\mathfrak{M}^* = (X, rk^*, m^*)$. Nach Theorem 2.3.11 gibt es ein dargestelltes Tripel $\mathfrak{M}' = (X', rk', m')$ durch eine endlich erzeugte, abelsche Gruppe G', das $\mathfrak{M}^*$ darstellt. Insbesondere können wir eine Darstellung ν von $\mathfrak{M}^*$ nach $\mathfrak{M}'$ wählen. Es wurde bereits gezeigt, dass (X, rk) ein Matroid ist und dass (m1),(m3) und (m4) gelten. Bleiben (m2) und (m5) zu zeigen.

(m2): Da $\mathfrak{M}'$ dargestellt ist, gilt insbesondere (m′1). Mit $m^* = m' \circ \nu$ und Scholium 2.2.3 folgt (m*1) und nach Lemma 2.1.3 folgt dann (m2). ✓

(m5): Da $\mathfrak{M}'$ dargestellt ist, gilt insbesondere (m4). Mit $m^* = m' \circ \nu$ und Scholium 2.2.3 folgt (m*4) und nach Lemma 2.1.3 folgt (m5). ✓

Damit ist $\mathfrak{M}$ ein arithmetisches Matroid. □

Definition/Satz 2.3.15. (i) Nach obigem Theorem nennen wir dargestellte Tripel ab jetzt *dargestellte arithmetische Matroide*.

(ii) Beachte, dass nach Theorem 2.2.2 eine Darstellung von $\mathfrak{M}$ nach $\mathfrak{M}'$ genau dann ein A-M-Homomorphismus ist, wenn $\mathfrak{M}$ (m5) erfüllt. Dementsprechend definieren wir ein *darstellbares arithmetisches Matroid* als darstellbares Tripel, das zusätzlich (m5) erfüllt.

(iii) Mit Scholium 2.3.13 sind Duale dargestellter arithmetischer Matroide per Definition darstellbar.

3 Das arithmetische Tutte-Polynom

Definition 3.0.1. Das *Tutte-Polynom* $T_X(x, y) = T(\mathfrak{M}_X, x, y)$ eines Matroids $\mathfrak{M}_X = (X, rk)$ ist definiert als:

$$T_X(x, y) := \sum_{A \subseteq X} (x-1)^{rk(X)-rk(A)}(y-1)^{|A|-rk(A)}$$

(siehe [7]).

Bemerkung. Es ist $rk(X) = rk(A) = |A|$ genau dann, wenn A maximalen Rang in $\mathfrak{M}_X$ hat und unabhängig ist, also genau dann, wenn A eine Basis ist. Damit ist

$$0^{rk(X)-rk(A)} \cdot 0^{|A|-rk(A)} = 1$$

genau dann, wenn A eine Basis ist, also ist $T_X(1, 1) = |\mathcal{B}|$ die Anzahl der Basen.

Definition 3.0.2. Das *arithmetische Tutte-Polynom* $M_X(x, y) = M(\mathfrak{M}_X, x, y)$ eines arithmetischen Matroids $\mathfrak{M}_X = (X, rk, m)$ ist definiert als

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

4 Geometrie verallgemeinerter torischer Anordnungen

In diesem Kapitel befassen wir uns mit den geometrischen Zusammenhängen dargestellter arithmetischer Matroide. Zudem werden wir (m4) für dargestellte, arithmetische Matroide beweisen, womit alle noch offenen Beweise abgeschlossen werden.

Nach wie vor sei X stets endliche Teilmenge einer endlich erzeugten, abelschen Gruppe G mit endlichem Index von $\langle X \rangle$ in G.

4.1 Verallgemeinerte Tori

Definition 4.1.1. Sei G endlich erzeugte, abelsche Gruppe. Wir definieren $T(G)$ als

$$T(G) := Hom(G, \mathbb{S}^1),$$

die Menge der Homomorphismen der Gruppe G in die multiplikative Gruppe $\mathbb{S}^1$.

Bemerkung. Man rechnet leicht nach, dass $T(G)$ mit der Multiplikation von Funktionen eine Gruppe bildet.

Definition 4.1.2. Sei n eine natürliche Zahl, dann setzen wir

$$\mathbb{S}^1_n := \left\{ e^{2\pi i \frac{k}{n}} \;\middle|\; k = 1, \dots, n \right\}$$

die Menge der n-ten Einheitswurzeln. Diese Schreibweise wählen wir als Analogie zu $\mathbb{Z}_n$.

Satz 4.1.3. *Sei $G = \mathbb{Z}^r \oplus \bigoplus_{k=1}^s \mathbb{Z}_{p_k}$ endlich erzeugte, abelsche Gruppe, wobei $r, s \in \mathbb{N}$ und p_k prim sei für $k = 1, \dots, s$. Dann gilt:*

$$T(G) \cong \mathbb{S}^r \otimes \bigotimes_{k=1}^{s} \mathbb{S}^1_{p_k},$$

wobei wir für $\mathbb{S}^r \otimes \bigotimes_{k=1}^s \mathbb{S}^1_{p_k}$ die parameterweise Multiplikation als Gruppenoperation wählen.

Notation 4.1.4. Es sei in diesem Abschnitt stets E_r die Standardbasis von $\mathbb{Z}^r$ und $\overline{E_s} := \{\overline{e_j} \mid j = 1, \dots, s\}$, wobei wir $\overline{e_j} \in \bigoplus_{k=1}^s \mathbb{Z}_{p_k}$ für $j = 1, \dots, s$ definieren durch

$$(\overline{e_j})_k = \begin{cases} 0 + p_k \cdot \mathbb{Z}, & \text{falls } k \neq j, \\ 1 + p_k \cdot \mathbb{Z}, & \text{falls } k = j. \end{cases}$$

Dann ist insbesondere $E := (E_r \oplus \{0\}) \cup (\{0\} \oplus \overline{E_s})$ ein minimales Erzeugendensystem von G.

Beweis von Satz 4.1.3. Jedes $t \in T(G)$ ist durch die Bilder von E eindeutig bestimmt. Wir zeigen, dass sich eine beliebige Abbildung f von E nach $\mathbb{S}^1$ genau dann auf einen Homomorphismus in $T(G)$ fortsetzen lässt, wenn f jedes Element $(0, \overline{e_j})$ aus $\{0\} \oplus \overline{E_s}$ auf $\mathbb{S}^1_{p_j}$ abbildet. Dafür zeigen wir zwei Richtungen:

„$\Rightarrow$“: Sei $f \in T(G)$. Dann gilt für alle $\overline{e_j} \in \overline{E_s}$:

$$\begin{aligned} f((0, \overline{e_j}))^{p_j} &= f(p_j \cdot (0, \overline{e_j})) && \text{nach Homomorphismuseigenschaft, siehe [2]} \\ &= f((0, p_j \cdot \overline{e_j})) \\ &= f((0, 0)) && \text{nach Definition von } \overline{e_j} \\ &= 1 && \text{nach Homomorphismuseigenschaft, siehe [2],} \end{aligned}$$

das heißt jedes $f((0, \overline{e_j}))$ ist eine p_j-te Einheitswurzel. ✓

„$\Leftarrow$“: Sei f eine Abbildung von E nach $\mathbb{S}^1$, sodass für $k = 1, \dots, s$ gilt, dass

$$f((0, \overline{e_k})) \in \mathbb{S}^1_{p_k}.$$

Wir definieren eine Fortsetzung $\hat{f}$ von f auf G wie folgt: Für alle ganzen Zahlen $\lambda_1, \dots, \lambda_r$ und $\mu_1, \dots, \mu_r$ sei

$$\hat{f}\left(\left(\sum_{l=1}^{r} \lambda_l e_l, \sum_{k=1}^{s} \mu_k \overline{e_k}\right)\right) := \prod_{l=1}^{r} f((e_l, 0))^{\lambda_l} \cdot \prod_{k=1}^{s} f((0, \overline{e_k}))^{\mu_k}.$$

Wir zeigen zunächst, dass $\hat{f}$ so wohldefiniert ist: Seien λ_l, $\widetilde{\lambda_l}$, μ_k, $\widetilde{\mu_k}$ für $l = 1, \dots, r$, $k = 1, \dots, s$ ganze Zahlen mit

$$\left(\sum_{l=1}^{r} \lambda_l e_l, \sum_{k=1}^{s} \mu_k \overline{e_k}\right) = \left(\sum_{l=1}^{r} \widetilde{\lambda_l} e_l, \sum_{k=1}^{s} \widetilde{\mu_k} \overline{e_k}\right).$$

Da E_r Basis von $\mathbb{Z}^r$ ist, ist dann $\lambda_l = \widetilde{\lambda_l}$ für $l = 1, \ldots, r$. Nach Wahl der $\overline{e_k}$ ist außerdem $\mu_k \overline{e_k} = \widetilde{\mu_k}\overline{e_k}$ und weiter $\mu_k = \widetilde{\mu_k} - z_k p_k$ für $k = 1, \ldots, s$ und bestimmte ganze Zahlen $z_1, \ldots, z_s$. Nach Vorraussetzung ist

$$f(0, \overline{e_k}) = e^{2\pi i \frac{n_k}{p_k}}$$

mit bestimmten $n_k \in \{1, \ldots, p_k\}$ für $k = 1, \ldots, s$. Damit folgt

$$\begin{aligned} f((0, e_k))^{\mu_k} &= f((0, \overline{e_k}))^{\mu_k} \\ &= e^{2\pi i \frac{n_k}{p_k} \mu_k} \\ &= e^{2\pi i \frac{n_k}{p_k} (\widetilde{\mu_k} - z_k p_k)} \\ &= e^{2\pi i \frac{n_k}{p_k} \widetilde{\mu_k}} \cdot e^{-2\pi i n_k z_k} \\ &= f((0, \overline{e_k}))^{\widetilde{\mu_k}} \cdot 1^{n_k z_k} \\ &= f((0, \overline{e_k}))^{\widetilde{\mu_k}} \end{aligned}$$

für $k = 1, \ldots, s$ und weiter

$$\begin{aligned} \hat{f}\left(\left(\sum_{l=1}^{r} \lambda_l e_l, \sum_{k=1}^{s} \mu_k \overline{e_k}\right)\right) &= \prod_{l=1}^{r} f((e_l, 0))^{\lambda_l} \cdot \prod_{k=1}^{s} f((0, \overline{e_k}))^{\mu_k} \\ &= \prod_{l=1}^{r} f(e_l, 0)^{\widetilde{\lambda_l}} \cdot \prod_{k=1}^{s} f(0, \overline{e_k})^{\widetilde{\mu_k}} \\ &= \hat{f}\left(\left(\sum_{l=1}^{r} \widetilde{\lambda_l} e_l, \sum_{k=1}^{s} \widetilde{\mu_k}\overline{e_k}\right)\right). \end{aligned}$$

Es ist also $\hat{f}$ repräsentantenunabhängig. Da f auf $\mathbb{S}^1$ abbildet und $\mathbb{S}^1$ abgeschlossen unter Multiplikation ist, bildet außerdem $\hat{f}$ auf $\mathbb{S}^1$ ab. Dann ist $\hat{f}$ tatsächlich wohldefinierte Abbildung von G nach $\mathbb{S}^1$ und per Konstruktion ein Homomorphismus. ✓

Wir finden also genau zu jeder Wahl $f((e_l, 0)) \in \mathbb{S}^1$ für $l = 1, \ldots, r$ und $f((0, \overline{e_k})) \in \mathbb{S}^1_{p_k}$ für $k = 1, \ldots, s$ genau einen Homomorphismus $\hat{f} \in T(G)$. Dann ist

$$\begin{aligned} \phi \colon T(G) &\to \mathbb{S}^r \otimes \bigotimes_{k=1}^{s} \mathbb{S}^s_{p_k} \\ t &\mapsto \Big(t((e_1, 0)), \ldots, t((e_r, 0)), t((0, \overline{e_1})), \ldots, t((0, \overline{e_s}))\Big) \end{aligned} \tag{19}$$

also bijektiv und in natürlicher Weise ein Homomorphismus. □

Bemerkung 4.1.5. (i) Beachte, dass $\left|\bigotimes_{k=1}^{s} \mathbb{S}^1_{p_k}\right| = |G_t|$. Nach obigem Satz können wir also $T(G)$ topologisch als $|G_t|$-fache Kopie eines r-dimensionalen Torus $\mathbb{S}^r$ beziehungsweise $T(G_f)$ auffassen. Hierzu identifizieren wir nach obigem Beweis $T(G)$ mit $\mathbb{S}^r \otimes \bigotimes_{k=1}^{s} \mathbb{S}^1_{p_k}$ durch den in (19) angegebenen Isomorphismus.

(ii) Wir können einen r-dimensionalen Torus topologisch auffassen als Faktorraum von $\mathbb{R}^r$ bezüglich der Äquivalenzrelation $\sim$ mit

$$x \sim y \Leftrightarrow x_k - \lfloor x_k \rfloor = y_k - \lfloor y_k \rfloor \text{ für } k = 1, \ldots, r.$$

In einer Äquivalenzklasse stehen also genau alle Elemente aus $\mathbb{R}^r$ mit koordinatenweise gleichen Nachkommastellen und

$$\mathbb{S}^r \simeq \mathbb{R}^r/\sim\, \simeq [0, 1]^r/\sim .$$

Beachte, dass jede Restklasse $[\varphi]$ in $\mathbb{R}^r/\sim$ genau einen Repräsentanten in $[0,1)^r$ hat. Wir können uns dann einen r-dimensionalen Torus als Hyperwürfel $[0,1]^r$ mit identifizierten gegenüberliegenden Seiten veranschaulichen.

Definition 4.1.6. Wir identifizieren jedes Element λ aus G mit einem Element aus $Hom(T(G), \mathbb{S}^1)$ durch

$$\begin{aligned} \lambda\colon T(G) &\to \mathbb{S}^1 \\ t &\mapsto t(\lambda) \end{aligned}$$

und definieren:

(i) Es sei H_λ der Kern der Abbildung λ, also

$$H_\lambda := \{t \in T(G) \mid t(\lambda) = 1\}.$$

Beachte, dass dann H_λ eine Untermannigfaltigkeit von $T(G)$ ist.

(ii) Für $A \subseteq X$ setzen wir

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

(iii) Für endliche Teilmengen X von G nennen wir

$$\mathcal{T}(X) := \{H_\lambda \mid \lambda \in X\}$$

die *verallgemeinerte torische Anordnung* von X in $T(G)$.

Lemma 4.1.7. *Sei (X, rk, m) dargestelltes arithmetisches Matroid durch G. Dann ist für jede Teilmenge A von X die Vielfachheit $m(A)$ gleich der Anzahl Zusammenhangskomponenten von H_A.*

Beweis. Siehe [8], Lemma 5.4.

Bemerkung 4.1.8. Wir führen die Beobachtungen von Bemerkung 4.1.5 aus, um uns H_λ zu veranschaulichen:

Sei enstprechend Notation 4.1.4

$$\lambda = \sum_{j=1}^{r} \lambda_j (e_j, 0) + \sum_{j=1}^{s} \lambda_{r+j}(0, \overline{e_j}) \in G$$

mit ganzzahligen $\lambda_1, \ldots, \lambda_{r+s}$. Dann ist

$$\begin{aligned}
H_\lambda &= \{t \in T(G) \mid t(\lambda) = 1\} \\
&= \left\{ t \in T(G) \,\middle|\, \prod_{j=1}^{r} t(e_j, 0)^{\lambda_j} \prod_{j=1}^{s} t(0, \overline{e_j})^{\lambda_{r+j}} = 1 \right\} \\
&\qquad \text{nach Homomorphismuseigenschaft der } t \in T(G) \\
&\cong \left\{ t \in \mathbb{S}^r \otimes \bigotimes_{k=1}^{s} \mathbb{S}^1_{p_k} \,\middle|\, \prod_{j=1}^{r+s} t_j^{\lambda_j} = 1 \right\} \qquad \text{nach Satz 4.1.3} \\
&\simeq \left\{ ([\varphi]_\sim, k_1, \ldots, k_s) \in (\mathbb{R}^r/\sim) \times \prod_{j=1}^{s} \{1, \ldots, p_j\} \,\middle|\, \sum_{j=1}^{r} \lambda_j \varphi_j + \sum_{j=1}^{s} \lambda_{r+j} \frac{k_j}{p_j} \in \mathbb{Z} \right\} \\
&\qquad \text{siehe Bemerkung 4.1.5} \\
&=: H'_\lambda.
\end{aligned}$$

Sei außerdem für $k \in \prod_{j=1}^{s}\{1,\dots,p_j\}$

$$Rep\,(H'_\lambda,k) := \{\varphi \in \mathbb{R}^r \mid ([\varphi]_\sim,k) \in H'_\lambda\}$$

die Menge der *Repräsentanten* von H'_λ im durch k indizierten Torus. Beachte, dass $Rep\left(H'_\lambda,k\right)$ durch $Rep\left(H'_\lambda,k\right)\cap[0,1)^r$ bereits eindeutig bestimmt ist. Wir unterscheiden nun zwei Fälle:

Fall 1: λ ist endlicher Ordnung, also $\lambda_1 = \ldots = \lambda_r = 0$. Dann ist H_λ topologisch eine endliche Vereinigung r-dimensionaler Tori. H_λ ist dann außerdem nicht leer, da

$$Rep(H'_\lambda,0) = \mathbb{R}^r.$$

Insbesondere ist H_λ eine r-dimensionale Untermannigfaltigkeit von $T(G)$.

Fall 2: λ ist unendlicher Ordnung. Setze

$$m_1 := \max_{n\in\{0,1\}^r}\sum_{j=1}^{r}\lambda_j n_j, \qquad m_2 := \min_{n\in\{0,1\}^r}\sum_{j=1}^{r}\lambda_j n_j.$$

Dann sind m_1 und $-m_2$ natürliche Zahlen mit

$$m := m_1 - m_2 \neq 0.$$

Wähle $k = (k_1,\dots,k_s) \in \prod_{j=1}^{s}\{1,\dots,p_j\}$ fest, das heißt wir betrachten eine beliebig ausgewählte Kopie eines r-dimensionalen Torus in $T(G)$. Setze

$$q := \sum_{j=1}^{s}\lambda_{r+j}\frac{k_j}{p_j}.$$

Dann ist $0 \le q - \lfloor q\rfloor \le 1$ und

$$Rep\,(H'_\lambda,k)\cap[0,1)^r = \dot{\bigcup_{n=m_2}^{m_1-1}}\left\{\varphi\in[0,1)^r \;\middle|\; \sum_{j=1}^{r}\lambda_j\varphi_j = q-\lfloor q\rfloor + n\right\}$$

eine Vereinigung von m affinen Hyperebenen mit Normalenvektor $(\lambda_1,\dots,\lambda_r)^T$ geschnitten mit $[0,1)^r$. Damit ist H_λ topologisch eine endliche Vereinigung von $(r-1)$-dimensionalen Untermannigfaltigkeiten der r Kopien das r-dimensionalen Torus $T(G_f)$.

Wir definieren allgemeiner:

Definition 4.1.9. Sei $A \subseteq X$. Dann setzen wir analog zu Bemerkung 4.1.8:

$$H'_A := \left\{([\varphi]_\sim,k)\in(\mathbb{R}^r/\sim)\times\prod_{j=1}^{s}\{1,\dots,p_j\} \;\middle|\; \forall\lambda\in A : \sum_{j=1}^{r}\lambda_j\varphi_j + \sum_{j=1}^{s}\lambda_{r+j}\frac{k_j}{p_j}\in\mathbb{Z}\right\}$$

und für jedes $k \in \prod_{j=1}^{s}\{1,\dots,p_j\}$:

$$Rep(H'_A,k) := \{\varphi\in\mathbb{R}^r \mid ([\varphi]/\sim,k)\in H'_A\}.$$

Bemerkung 4.1.10. Beachte, dass für je zwei Indizies $k, l \in \prod_{j=1}^{s}\{1, \ldots, p_j\}$ gilt: Sind die beiden Untermannigfaltigkeiten $Rep(H'_A, k)$ und $Rep(H'_A, l)$ der „Kopien" des r-dimensionalen Würfels nicht leer, so haben sie die gleiche Dimension.

Mit Bemerkung 4.1.8 hat außerdem jede Zusammenhangskomponente von H_A gleiche Dimension.

Satz 4.1.11. *Sei $A \subseteq X$. Dann hat H_A die Dimension $r - rk(A)$.*

Beweis. Es ist nach Bemerkung 4.1.8 für jedes $k \in \prod_{j=1}^{s}\{1, \ldots, p_j\}$ und jedes $\lambda \in A$ die Menge $Rep(H'_\lambda, k)$ eine (nach Definition abzählbare) Vereinigung affiner Hyperebenen mit Normalenvektor $(\lambda_1, \ldots, \lambda_r)^T$. Es gilt:

$$\begin{aligned} Rep(H'_A, k) &= \{\varphi \in \mathbb{R}^r \mid ([\varphi]/\sim, k) \in H'_A\} \\ &= \{\varphi \in \mathbb{R}^r \mid \forall \lambda \in A : ([\varphi]/\sim, k) \in H'_\lambda\} \\ &= \bigcap_{\lambda \in A} \{\varphi \in \mathbb{R}^r \mid ([\varphi]/\sim, k) \in H'_\lambda\} \\ &= \bigcap_{\lambda \in A} Rep(H'_\lambda, k). \end{aligned}$$

Sei $I \subseteq A$ maximal unabhängig, also $|I| = rk(A)$. Dann ist $\{(\lambda_1, \ldots, \lambda_r)^T \mid \lambda \in I\}$ linear unabhängig in $\mathbb{Q}^r$ nach Lemma 1.4.3 (i). Insbesondere besteht $\{(\lambda_1, \ldots, \lambda_r)^T \mid \lambda \in I\}$ aus $rk(A)$ linear unabhängigen Normalenvektoren von $Rep(H'_A, k)$, also

$$dim(Rep(H'_A, k)) \le r - rk(A).$$

Weiter ist der Unterraum

$$U := \left\{\varphi \in \mathbb{R}^r \;\middle|\; \sum_{j=1}^{r} \varphi_j \lambda_j = 0\right\}$$

mit Normalenvektoren $\{(\lambda_1, \ldots, \lambda_r)^T \mid \lambda \in A\}$ und Ortsvektor 0 Teilmenge von $Rep(H'_A, 0)$. Nach Lemma 1.4.3 ist $rk(A)$ die maximale Kardinalität linear unabhängiger Teilmengen von $\{(\lambda_1, \ldots, \lambda_r)^T \mid \lambda \in A\}$, also $dim(U) = r - rk(A)$. Mit obiger Ungleichung folgt die Behauptung. □

Lemma 4.1.12. *Sei (X, rk, m) ein durch G dargestelltes Tripel, $A \subseteq B \subseteq X$ und $rk(A) = rk(B)$, dann gilt:*

$$\mu_B(A) := \sum_{A \subseteq C \subseteq B} (-1)^{|C|-|A|} m(C)$$

ist gleich der Anzahl Zusammenhangskomponenten von

$$H_A \setminus \bigcup_{B \supseteq T \supsetneq A} H_T.$$

Insbesondere ist $\mu_B(A) \ge 0$.

Beweis. Sei $A \subseteq B$ mit $rk(A) = rk(B)$. Nach Lemma 4.1.11 ist dann $dim(H_A) = dim(H_B)$. Damit gilt für alle $A \subseteq T \subseteq T' \subseteq B$, dass $rk(T) = rk(T')$ und nach Definition außerdem $H_{T'} \subseteq H_T$. Es bezeichne jeweils $Zhk(Y)$ die Menge der Zusammenhangskomponenten von Y. Dann gilt für alle $A \subseteq T \subseteq T' \subseteq B$, dass

$$Zhk(H_{T'}) \subseteq Zhk(H_T),$$

denn: Sei $K' \in Zhk(H_{T'})$. Dann ist $K' \subseteq H_{T'} \subseteq H_T$ und K' zusammenhängend, also $K' \subseteq K$ für ein $K \in Zhk(H_T)$. Nach Bemerkung 4.1.10 ist außerdem

$$dim(K') = dim(H_{T'}) = dim(H_T) = dim(K).$$

Sei $l \in \prod_{j=1}^{s}\{1, \ldots, p_j\}$ der Index der entsprechenden „Kopie“ des r-dimensionalen Torus, in dem K' und K enthalten sind. Dann ist also

$$Rep(K') := \{\phi \in \mathbb{R}^r \mid ([\phi]_\sim, k) \in K'\} \subseteq \{\phi \in \mathbb{R}^r \mid ([\phi]_\sim, k) \in K\} =: Rep(K),$$

wobei $Rep(K')$ und $Rep(K)$ affine Unterräume gleicher Dimension sind, also $Rep(K') = Rep(K)$, also $K' = K$. Damit ist

$$\begin{aligned}\left|Zhk\left(H_A \backslash \bigcup_{B \supseteq T \supsetneq A} H_T\right)\right| &= \left|Zhk(H_A) \backslash Zhk\left(\bigcup_{B \supseteq T \supsetneq A} H_T\right)\right| \\ &= \left|Zhk(H_A) \backslash Zhk\left(\bigcup_{t \in B \backslash A} H_{A \cup \{t\}}\right)\right| \\ &= \left|Zhk(H_A) \backslash Zhk\left(\bigcup_{t \in B \backslash A} (H_A \cap H_t)\right)\right|\end{aligned}$$

und da für $t, s \in B \backslash A$ zwei Zusammenhangskomponenten von $H_A \cap H_t$ und $H_A \cap H_s$ entweder disjunkt oder gleich sind

$$\begin{aligned}\left|Zhk\left(H_A \backslash \bigcup_{B \supseteq T \supsetneq A} H_T\right)\right| &= \left|Zhk(H_A) \backslash \bigcup_{t \in B \backslash A} Zhk\left(H_{A \cup \{t\}}\right)\right| \\ &= \left|\bigcap_{t \in B \backslash A} Zhk(H_A) \backslash Zhk\left(H_{A \cup \{t\}}\right)\right| \\ &= \sum_{j=0}^{|B \backslash A|} \sum_{\substack{K \subseteq B \backslash A \\ |K| = j}} (-1)^j \left|Zhk(H_{A \cup K})\right| \qquad \text{siehe [9]} \\ &= \sum_{A \subseteq C \subseteq B} (-1)^{|C \backslash A|} m(C) \\ &= \mu_B(A).\end{aligned}$$

□

Damit ist der Beweis, dass dargestellte Tripel arithmetische Matroide sind, abgeschlossen.

5 Beispiele

In diesem Kapitel wollen wir unsere Resultate auf zwei dargestellte arithmetische Matroide anwenden. Betrachte dazu die beiden Mengen

$$X = \left\{\begin{pmatrix}2\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}\right\} \subseteq \mathbb{Z}^2,$$

$$Y = \left\{\begin{pmatrix}1\\-1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\-1\end{pmatrix}, \begin{pmatrix}0\\1\\-1\end{pmatrix}\right\} \subseteq \mathbb{Z}^3$$

als Untergruppen von $\mathbb{Z}^2$ beziehungsweise $\mathbb{Z}^3$.

5.1 Arithmetische Matroide

Wir betrachten die zu X und Y assoziierten dargestellten arithmetischen Matroide $\mathfrak{M}_X = (X, rk_X, m_X)$ durch $\mathbb{Z}^2$ und $\mathfrak{M}_Y = (Y, rk_Y, m_Y)$ durch $\mathbb{Z}^3$. Das heißt Rang und Vielfachheitsfunktionen sind gegeben durch:

$$
\begin{aligned}
rk_X \colon \mathbb{P}(X) &\to \mathbb{N} & \qquad m_X \colon \mathbb{P}(X) &\to \mathbb{N} \\
A &\mapsto Rang(\langle A \rangle), & A &\mapsto |G_A : \langle A \rangle|,
\end{aligned}
$$

$$
\begin{aligned}
rk_Y \colon \mathbb{P}(Y) &\to \mathbb{N} & \qquad m_Y \colon \mathbb{P}(Y) &\to \mathbb{N} \\
A &\mapsto Rang(\langle A \rangle), & A &\mapsto |G_A : \langle A \rangle|.
\end{aligned}
$$

Um die Rangfunktionen zu bestimmen, überprüfen wir die Vektoren entsprechend Lemma 1.4.3 auf lineare Unabhängigkeit bezüglich $\mathbb{Q}$. Damit erhalten wir für alle $A \subseteq X$ und $B \subseteq Y$:

$$rk_X(A) = \min\{2, |A|\}, \qquad rk_Y(B) = \min\{2, |B|\}.$$

Zur Berechnung der Vielfachheiten benutzen wir Lemma 2.3.12 und erhalten für alle Teilmengen B von Y die Vielfachheit $m_Y(B) = 1$ und für $\mathfrak{M}_X$ folgende Vielfachheiten:

$$
\begin{array}{c||c|c|c|c|c|c|c}
A & \emptyset & \left\{\begin{pmatrix}2\\0\end{pmatrix}\right\} & \left\{\begin{pmatrix}1\\1\end{pmatrix}\right\} & \left\{\begin{pmatrix}1\\-1\end{pmatrix}\right\} & \left\{\begin{pmatrix}0\\2\end{pmatrix}\right\} & \left\{\begin{pmatrix}2\\0\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix}\right\} & \left\{\begin{pmatrix}2\\0\end{pmatrix},\begin{pmatrix}1\\-1\end{pmatrix}\right\} \\
\hline
m_X(A) & 1 & 2 & 1 & 1 & 2 & 2 & 2
\end{array},
$$

$$
\begin{array}{c||c|c|c|c|c}
A & \left\{\begin{pmatrix}2\\0\end{pmatrix},\begin{pmatrix}0\\2\end{pmatrix}\right\} & \left\{\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}1\\-1\end{pmatrix}\right\} & \left\{\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}0\\2\end{pmatrix}\right\} & \left\{\begin{pmatrix}1\\-1\end{pmatrix},\begin{pmatrix}0\\2\end{pmatrix}\right\} & \left\{\begin{pmatrix}2\\0\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}1\\-1\end{pmatrix}\right\} \\
\hline
m_X(A) & 4 & 2 & 2 & 2 & 2
\end{array},
$$

$$
\begin{array}{c||c|c|c|c}
A & \left\{\begin{pmatrix}2\\0\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}1\\-1\end{pmatrix}\right\} & \left\{\begin{pmatrix}2\\0\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}0\\2\end{pmatrix}\right\} & \left\{\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}1\\-1\end{pmatrix},\begin{pmatrix}0\\2\end{pmatrix}\right\} & X \\
\hline
m_X(A) & 2 & 2 & 2 & 2
\end{array}.
$$

5.2 Darstellbarkeit der Duale

Die Rang- und Vielfachheitsfunktionen der Duale $\mathfrak{M}_X^* = (X, rk_X^*, m_X^*)$ und $\mathfrak{M}_Y^* = (Y, rk_Y^*, m_Y^*)$ lassen sich mit den Ergebnissen des letzten Abschnitts, Satz 1.2.3 und Definition 2.1.1 einfach bestimmen. Wir wollen in diesem Abschnitt entsprechend Theorem 2.3.11 dargestellte arithmetische Matroide $\mathfrak{M}_X' = (X', rk_{X'}, m_{X'})$ und $\mathfrak{M}_Y' = (Y', rk_{Y'}, m_{Y'})$ durch endlich erzeugte abelsche Gruppen $G_{X'} = G_X'$ und $G_{Y'} = G_Y'$ bestimmen, die $\mathfrak{M}_X^*$ und $\mathfrak{M}_Y^*$ darstellen.

Wir konstruieren zunächst X', Y' und $G_{X'}$, $G_{Y'}$ wie im Beweis zu Theorem 2.3.11 angegeben und suchen zur Veranschaulichung zu $G_{X'}$ und $G_{Y'}$ isomorphe Gruppen der Form $\mathbb{Z}^r \oplus \bigoplus_{i=1}^{s} \mathbb{Z}_{p_i}$ mit natürlichen Zahlen r, s und Primzahlen $p_1, \ldots, p_s$.

Betrachten wir zunächst Y'. Für $z \in \mathbb{Z}^3$ bezeichne $\overline{z}$ wie üblich die Nebenklasse der entsprechenden Untergruppe von $\mathbb{Z}^3$ mit Repräsentanten z und e_1, e_2, e_3 bezeichne die

Einheitsvektoren in $\mathbb{Z}^3$. Wir setzen

$$Y' := \{\overline{e_1}, \overline{e_2}, \overline{e_3}\} \subseteq \mathbb{Z}^3 / \left\langle \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}-1\\0\\1\end{pmatrix}, \begin{pmatrix}0\\-1\\-1\end{pmatrix} \right\rangle =: G_{Y'}.$$

$G_{Y'}$ wird durch $\overline{e_1}$ erzeugt, denn für alle ganzen Zahlen x,y,z gilt:

$$\overline{\begin{pmatrix}x\\y\\z\end{pmatrix}} = \overline{\begin{pmatrix}x\\y\\z\end{pmatrix} - y \cdot \begin{pmatrix}1\\1\\0\end{pmatrix} - z \cdot \begin{pmatrix}-1\\0\\1\end{pmatrix}} = \overline{\begin{pmatrix}x-y+z\\0\\0\end{pmatrix}}.$$

Da $G_{Y'} = \mathbb{Z}^3/\langle\{(1,1,0)^t, (-1,0,1)^t\}\rangle$, ist diese Darstellung von $\overline{(x,y,z)^t}$ offensichtlich eindeutig, insbesondere ist $\{\overline{e_1}\}$ Basis von $G_{Y'}$ und folgende Abbildung wohldefinierter Gruppenisomorphismus:

$$\begin{aligned} \psi\colon G_{Y'} &\to \mathbb{Z} \\ \overline{\begin{pmatrix}x\\y\\z\end{pmatrix}} &\mapsto x - y + z. \end{aligned}$$

Nach Bemerkung 2.3.3 (iii) stellt das zu $\psi(Y') = \{1, -1, 1\} \subseteq \mathbb{Z}$ assoziierte arithmetische Matroid $\mathfrak{M}_Y^*$ dar. Insbesondere ist die Vielfachheitsfunktion des Duals konstant eins und für alle Teilmengen B von Y ist

$$rk_Y^*(B) = \min\{1, |B|\}.$$

Dies stimmt mit den Berechnungen des letzten Abschnitts überein, wie man mit Satz 1.2.3 und Definition 2.1.1 nachrechnen kann.

Betrachte nun X' mit analogen Bezeichnungen. Wir setzen

$$X' = \left\{ e_i + \left\langle \begin{pmatrix}2\\1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\-1\\2\end{pmatrix} \right\rangle \;\middle|\; i = 1\dots4 \right\} \subseteq \mathbb{Z}^4 / \left\langle \begin{pmatrix}2\\1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\-1\\2\end{pmatrix} \right\rangle =: G_{X'},$$

Da

$$|(G_{X'})_t| = \left|(G_{X'}) : \left\{\overline{0}\right\}\right| = m^*(\emptyset) = m(X) = 2$$

suchen wir zwei verschiedene Elemente endlicher Ordnung aus $G_{X'}$ und erhalten

$$G_t' = \left\{ \overline{\begin{pmatrix}0\\0\\0\\0\end{pmatrix}}, \overline{\begin{pmatrix}1\\1\\0\\1\end{pmatrix}} \right\}.$$

Bemerkung. Beachte, dass $G_{X'}$ nicht isomorph zu $\mathbb{Z}^2$ sein kann. Wir haben aber eine bijektive Darstellung und da $\mathfrak{M}_X$ und $\mathfrak{M}_X'$ arithmetische Matroide sind sogar einen Arithmetische-Matroide-Isomorphismus. Diese sind also im Allgemeinen keine Gruppenisomorphismen.

Für alle ganzen Zahlen a, b, c, d gilt:

$$\begin{aligned}
\overline{\begin{pmatrix}a\\b\\c\\d\end{pmatrix}} &= \overline{\begin{pmatrix}a\\b\\c\\d\end{pmatrix} - \left\lfloor\frac{a}{2}\right\rfloor \cdot \begin{pmatrix}2\\1\\1\\0\end{pmatrix}} = \overline{\begin{pmatrix}a \bmod 2\\ b-\left\lfloor\frac{a}{2}\right\rfloor \\ c-\left\lfloor\frac{a}{2}\right\rfloor \\ d\end{pmatrix}} \\
&= \overline{\begin{pmatrix}a \bmod 2\\ b-\left\lfloor\frac{a}{2}\right\rfloor \\ c-\left\lfloor\frac{a}{2}\right\rfloor \\ d\end{pmatrix} + \left(c-\left\lfloor\frac{a}{2}\right\rfloor\right)\cdot\begin{pmatrix}0\\1\\-1\\2\end{pmatrix}} = \overline{\begin{pmatrix}a \bmod 2\\ b+c-2\cdot\left\lfloor\frac{a}{2}\right\rfloor \\ 0 \\ d+2c-2\cdot\left\lfloor\frac{a}{2}\right\rfloor\end{pmatrix}} \\
&= \overline{\begin{pmatrix}0\\ b+c-2\cdot\left\lfloor\frac{a}{2}\right\rfloor-(a \bmod 2) \\ 0 \\ d+2c-2\cdot\left\lfloor\frac{a}{2}\right\rfloor-(a \bmod 2)\end{pmatrix}} + (a \bmod 2)\cdot\overline{\begin{pmatrix}1\\1\\0\\1\end{pmatrix}} \\
&= \overline{\begin{pmatrix}0\\ b+c-a \\ 0 \\ d+2c-a\end{pmatrix}} + (a \bmod 2)\cdot\overline{\begin{pmatrix}1\\1\\0\\1\end{pmatrix}} \qquad \text{da } 2\cdot\left\lfloor\frac{a}{2}\right\rfloor = a-(a \bmod 2).
\end{aligned}$$

Insbesondere ist diese Darstellung eindeutig und

$$G_{X'} = \left\langle \overline{\begin{pmatrix}0\\1\\0\\0\end{pmatrix}}, \overline{\begin{pmatrix}0\\0\\0\\1\end{pmatrix}} \right\rangle \oplus \left\{ \overline{\begin{pmatrix}0\\0\\0\\0\end{pmatrix}}, \overline{\begin{pmatrix}1\\1\\0\\1\end{pmatrix}} \right\},$$

also haben wir einen Isomorphismus

$$\begin{aligned}
\phi\colon \qquad & G_{X'} \to \mathbb{Z}^2 \oplus \mathbb{Z}_2 \\
& \overline{\begin{pmatrix}0\\x\\0\\y\end{pmatrix}} + i\,\overline{\begin{pmatrix}1\\1\\0\\1\end{pmatrix}} \mapsto \begin{pmatrix}x\\y\end{pmatrix} \oplus (i + 2\cdot\mathbb{Z}) \qquad (i \in \{0,1\}).
\end{aligned}$$

Dann ist

$$\begin{aligned}
\phi(\overline{e_1}) &= \phi\left(\overline{\begin{pmatrix}0\\-1\\0\\-1\end{pmatrix}} + 1\cdot\overline{\begin{pmatrix}1\\1\\0\\1\end{pmatrix}}\right) = \begin{pmatrix}-1\\-1\end{pmatrix} \oplus (1 + 2\cdot\mathbb{Z}) \\
\phi(\overline{e_2}) &= \begin{pmatrix}1\\0\end{pmatrix} \oplus (0 + 2\cdot\mathbb{Z}) \\
\phi(\overline{e_3}) &= \phi\left(\overline{\begin{pmatrix}0\\0\\1\\0\end{pmatrix} + \begin{pmatrix}0\\1\\-1\\2\end{pmatrix}}\right) = \phi\left(\overline{\begin{pmatrix}0\\1\\0\\2\end{pmatrix}}\right) = \begin{pmatrix}1\\2\end{pmatrix} \oplus (0 + 2\cdot\mathbb{Z}) \\
\phi(\overline{e_4}) &= \begin{pmatrix}0\\1\end{pmatrix} \oplus (0 + 2\cdot\mathbb{Z}),
\end{aligned}$$

also

$$\phi(X') = \left\{ \begin{pmatrix} -1 \\ -1 \end{pmatrix} \oplus (1 + 2 \cdot \mathbb{Z}), \begin{pmatrix} 1 \\ 0 \end{pmatrix} \oplus (0 + 2 \cdot \mathbb{Z}), \begin{pmatrix} 1 \\ 2 \end{pmatrix} \oplus (0 + 2 \cdot \mathbb{Z}), \begin{pmatrix} 0 \\ 1 \end{pmatrix} \oplus (0 + 2 \cdot \mathbb{Z}) \right\}.$$

Betrachten wir nach Bemerkung 1.4.4 nur den „freien“ Teil der Elemente von $\phi(X')$, so haben wir wieder in $\mathbb{Q}^2$ paarweise linear unabhängige Vektoren, also nach Lemma 1.4.3 (1) für alle Teilmengen A von X:

$$rk^*_{X'}(A) = \min\{2, |A|\} = rk(A).$$

Dies stimmt, wie man wieder mit Satz 1.2.3 nachrechnen kann, mit den Ergebnissen des letzten Abschnitts überein. Zur Berechnung von $m^*_{X'}$ kann man Lemma 2.3.7 und Lemma 2.3.12 benutzen, um auf dieselben Ergebnisse zu kommen, die wir bei Betrachtung von Definition 2.1.1 aus den Ergebnissen des letzten Abschnitts erhalten.

6 Aussicht

Arithmetische Matroide wurden bisher kaum untersucht, sodass wir in diesem Abschlusskapitel ausschließlich Fragen aufzeigen werden, die sich während der Beschäftigung mit den neuen Definitionen dieser Arbeit ergaben.

Die Schwierigkeit all dieser Fragen ergibt sich aus möglicher Nicht-Injektivität einer surjektiven Abbildung ν von $\mathfrak{M} = (X, rk, m)$ nach $\mathfrak{M}' = (X', rk', m')$ mit $rk = rk' \circ \nu$ und $m = m' \circ \nu$, wobei entweder $\mathfrak{M}$ oder $\mathfrak{M}'$ ein arithmetisches Matroid sei. Ist ν jedoch bijektiv, so lässt sich jede dieser Fragen leicht mit „ja“ beantworten.

Rückwärtsvererbung von (m5):

Scholium 2.2.3 besagt, dass (m1) bis (m4) durch vielfachheitserhaltende Matroide-Homomorphismen „rückwärts vererbt“ werden. Es stellt sich die Frage, ob dies auch für (m5) gilt. In dem Fall wäre jede AM-Darstellung homomorph und jedes darstellbare Tripel wäre (darstellbares) arithmetisches Matroid.

Vorwärtsvererbung:

Andersherum ergibt sich die gleiche Fragestellung: Sei (X, rk, m) ein arithmetisches Matroid, X' eine Menge und rk', m' Abbildungen von der Potenzmenge von X' in die natürlichen Zahlen. Sei weiter ν eine surjektive Abbildung von X nach X' mit $rk = rk' \circ \nu$ und $m = m' \circ \nu$. Dann lassen sich im Allgemeinen leicht Beispiele finden, in denen nicht einmal (X', rk') ein Matroid ist. Wähle hierzu zum Beispiel für rk die Betragsfunktion und $m \equiv 1$. Dann rechnet man leicht nach, dass (X, rk, m) ein arithmetisches Matroid ist. Betrachte nun ein X' mit weniger als $|X|$ Elementen. Dann ist

$$rk'(X') = rk'(\nu(X)) = rk(X) = |X| > |X'|,$$

also ist bereits (rk1) nicht erfüllt. Dies funktioniert selbst noch unter der Bedingung, dass (X, rk, m) dargestellt sei, wähle dazu etwa X als die Menge der Einheitsvektoren in $\mathbb{Z}^{|X|}$.

Äquivalenz von arithmetischen Matroiden über Listen und über Mengen:

Offensichtlich lässt sich jedes arithmetische Matroid über einer Menge $X = \{x_1, \ldots, x_n\}$ als arithmetisches Matroid über einer Liste $X = \{(x_i, i) \mid 1 \leq i \leq n\}$ auffassen.

Man kann nun die Vorraussetzungen weiter einschränken, um vielleicht doch „vorwärts vererben" zu können. Es stellt sich die Frage, ob bei gegebenem arithmetischen Matroid $\mathfrak{M} = (X, m, rk)$ über einer liste $X = \{(x_i, i) \mid i \in I\}$ ($|I| < \infty$) auch (X', rk', m') ein arithmetisches Matroid ist, wobei $X' := \{x_i \mid i \in I\}$ und für alle $J \subseteq I$ gelte, dass

$$rk(\{(x_i, i) \mid i \in I\}) =: rk'(\{x_i \mid i \in I\})$$

und

$$m(\{(x_i, i) \mid i \in I\}) =: m'(\{x_i \mid i \in I\}).$$

Für beliebiges (X, m, rk) ist dies offensichtlich nicht der Fall, wähle etwa $X = \{(x, 1), (x, 2)\}$ mit $rk(X) = 2$, also

$$rk'(X') = rk(X) = 2 > |\{x\}| = |X'|.$$

Fordert man allerdings weiter, dass $\mathfrak{M}$ darstellbar entsprechend [1] sei, so ist die Antwort auf diese Frage nicht offensichtlich.

Darstellbarkeit des Duals eines darstellbaren arithmetischen Matroids:

Wir haben in Abschnitt 2.3 gezeigt, dass das Dual eines dargestellten arithmetischen Matroids darstellbar ist. Es bleibt offen, ob auch das Dual eines beliebigen darstellbaren arithmetischen Matroids wieder darstellbar ist.

7 Literatur

[1] D'Adderio, M. ; Moci, L.: Arithmetic matroids, Tutte polynomial and toric arrangements. In: *ArXiv e-prints* (2011), Mai

[2] Bosch, S.: *Algebra*. Springer-Verlag, 2009

[3] Wüstholz, G.: *Algebra*. Vieweg+Teubner, 2004

[4] Stanley, R. P.: A zonotope associated with graphical degree sequences. In: *Applied Geometry and Discrete Combinatorics* Bd. 4. American Mathematical Society, 1991, S. 555–570

[5] Bosch, S.: *Lineare Algebra*. Springer-Verlag, 2008

[6] Fischer, G.: *Lineare Algebra*. Vieweg+Teubner, 2010

[7] Tutte, W. T.: A contribution to the theory of chromatic polynomials. In: *Canadian Journal of Mathematics* 6 (1954), S. 80–91

[8] Moci, L.: A Tutte polynomial for toric arrangements. In: *ArXiv e-prints* (2009), November

[9] Stanley, R. P.: *Enumerative Combinatorics Vol. 1*. Cambridge University Press, 2000