Lineare Algebra II
Lösungsvorschläge zum Tutoriumsblatt 6

Moritz Fleischmann

Zur Vorlesung von Prof. Dr. Fabien Morel, Dr. Andrei Lavrenov, Katharina Novikov und Oliver Hendrichs im Sommersemester 25

Disclaimer: Das sind keine offiziellen Lösungen, sondern nur eine getexte Version der Lösungen zu ausgewählten Aufgaben (Dank geht hierbei an Andrei Lavrenov für seine Lösungsskizzen), die ich in meinem Tutorium bespreche. Fehler, Fragen oder Anmerkungen gerne an m.fleischmann@mnet-online.de. Verteilung der Lösungen ist erlaubt und erwünscht.

Wie üblich, wen das Vorgeplänkel nicht interessiert, der kann die Lösungen in den grau hinterlegten Boxen finden. Es gilt grundsätzlich, dass $\mathbb{K} \subseteq \mathbb{C}$.

Aufgabe 1

Sei $(A, +)$ eine endliche abelsche Gruppe. Zeige:

1. Sei $n \in \mathbb{N}$, dann gilt
$$na = 0 \Leftrightarrow \mathsf{Ord}(a) | n$$
2. Sei $a \in A$, dann gilt:
$$\mathsf{Ord}(a) = \mathsf{Ord}(\langle a \rangle)$$
3. Sei $a \in A$ und $\mathsf{Ord}(A) = n$. Zeige, dass $na = 0$ gilt.
4. Zeige, dass $\exp(A) | \mathsf{Ord}(A)$.

Lösung:

Wir erinnern uns an die Begriffe, die hier verwendet werden:

Sei $(A, +)$ eine Gruppe. Wir definieren:

1. Sei $a \in A$. Dann ist die *Ordnung* von a das kleinste Vielfache von a, das gleich 0 ist, bzw. die Ordnung gibt an, wie oft ich das Element mindestens mit sich selbst aufsummieren muss, bis ich das neutrale Element erhalte.
$$\mathsf{Ord}(a) := \min\{n \in \mathbb{N} \mid an = 0\}$$
2. Die *Ordnung* von A ist die Kardinalität von A, also
$$\mathsf{Ord}(A) := |A|$$
3. Der *Exponent* von A ist die kleinste natürliche Zahl, die alle Elemente in A annihiliert. Das ist in folgendem Sinne gemeint:
$$\exp(A) := \min\{n \in \mathbb{N} \mid \forall a \in A : na = 0\}$$

Man beachte, dass die Notation für multiplikativ geschrieben Gruppen etwas anders aussieht. Dort würden wir schreiben:

$$\mathsf{Ord}(a) = \min\{n \in \mathbb{N} \mid a^n = 0\}$$
$$\exp(A) = \min\{n \in \mathbb{N} \mid \forall a \in A : a^n = 0\}$$

Wir fragen uns noch, wieso wir diese Dinge überhaupt anschauen. Die Begründung und Erläuterung dieser Aussagen ist Aufgabe der Vorlesung, hier aber ein kurzer Überblick: (Optional und für das Verständnis dieser Aufgabe nicht relevant!)

Es gibt eine Parallele zwischen endlichen abelschen Gruppen und endlichdimensionalen Vektorräumen mit Endomorphismus.

1. Jede endliche abelsche Gruppe kann eindeutig durch ihre Elementarteiler beschrieben werden. Sei $(A, +)$ eine solche Gruppe, dann gibt es die *Elementarteiler von* A, also Zahlen $d_1|\ldots|d_k \in \mathbb{N}$, sodass

   $$A \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_k\mathbb{Z}$$

   Analoges gilt für einen endlich dimensionalen $\mathbb{K}$-Vektorraum V mit Endomorphismus $f : V \to V$. Wie wir wissen gibt es ein Polynom χ_f, das *charakteristische Polynom* von f, sodass $\chi_f(f) = 0$ gilt und dass es eine Zerlegung von χ_f in Polynome $P_1|\ldots|P_k$ gibt, sodass

   $$V \simeq \mathbb{K}[X]/\chi_f \simeq \mathbb{K}[X]/P_1 \oplus \ldots \oplus \mathbb{K}[X]/P_k$$

   Wir sehen also, dass es sehr ähnliche Zerlegungen der beiden Strukturen gibt.

2. Es gilt, dass $d_k = \exp(A)$, also die kleinste Natürliche Zahl die alle Elemente aus A annihiliert. Analog gilt $P_k = \mu(f)$, also das normierte Polynom kleinsten Grades, das alle Elemente aus V in folgendem Sinne annihiliert: $\forall v \in V : \mu_f(f)(v) = 0$. Die beiden Objekte entsprechen einander also.

3. Weiterhin gilt, dass $d_1 \cdot \ldots \cdot d_k = \mathsf{Ord}(A)$, also die Anzahl der Elemente in A. Analog gilt $P_1 \cdot \ldots \cdot P_k = \chi_f$ und es gilt $\deg(\chi_f) = \dim_{\mathbb{K}}(V)$. Wir haben hier also durch die Darstellung einmal die Anzahl der Elemente und einmal die Dimension des Vektorraums.

Wir werden diese Parallelen in folgendem Sinne ausnutzen (Auch das werden wir hier nur kurz zusammenfassen, das sollte in den nächsten Wochen in der Vorlesung bewiesen werden.): Die einzelnen Summanden in unserer Darstellung als Moduln entsprechen f-Invarianten Unterräumen (also Räume $U \subseteq V$ mit $f(U) \subseteq U$) deren Dimension jeweils der Grad des Elementarteilers ist.
Bei der Jordanschen Normalform wird eine Basis gefunden, die diese einzelnen Räume jeweils separiert. Wird also eine Zerlegung $\chi_f = P_1 \cdot \ldots \cdot P_k$ gefunden, dann kann V durch diese Basis in k Unterräume zerlegt werden und wir können die Wirkung von J auf diese Unterräume jeweils separat betrachten. Das erlaubt es uns, f durch k kleinere Matrizen eindeutig zu beschreiben - diese kleineren Matrizen sind die Jordanblöcke, wobei die genaue Form eines Blocks J_l durch das Polynom P_l eindeutig beschrieben wird.
Wir werden zeigen, dass es eine Korrespondenz zwischen der Zerlegung von (V, f) und einer Gruppe A gibt, die es uns erlaubt, die gleichen Informationen auch durch Bestimmung der Elementarteiler $d_1, \ldots, d_k$ zu erhalten. Die Bestimmung der d_j ist im Allgemeinen aber einfacher als die Bestimmung der P_j, weswegen man die Jordansche Normalform üblicherweise bestimmt, ohne sich um die P_j konkret zu kümmern.

Eine Bemerkung noch: Man kann abelsche Gruppen immer als $\mathbb{Z}$-Modul ansehen. Ob man das hier explizit macht, oder einfach nur vom n-fachen Aufsummieren der Elemente spricht, macht in diesem Fall keinen Unterschied.

Nun zur Lösung:

1. "⇐" Es sei $a \in A$ und $n \in \mathbb{N}$ mit $\mathsf{Ord}(a)|n$. Die Teilbarkeit ist äquivalent zu $\exists k \in \mathbb{N} : n = \mathsf{Ord}(a) \cdot k$ und damit gilt:

$$an = \underbrace{a\mathsf{Ord}(a)}_{=0} k = 0$$

Was wir zeigen wollten.

"⇒" Es sei $an = 0$. Wir nehmen eine Fallunterscheidung vor:

- $0 < n < \mathsf{Ord}(a)$:
  In diesem Fall gilt $na = 0$, obwohl $\mathsf{Ord}(a)$ die kleinste, positive natürliche Zahl k ist, sodass $ka = 0$. Das ist ein Widerspruch!
- $n = \mathsf{Ord}(a)$:
  Offensichtlich gilt $\mathsf{Ord}(a)|\mathsf{Ord}(a)$, die Aussage ist also gezeigt.
- $n > \mathsf{Ord}(a)$:
  Da $\mathbb{Z}$ ein euklidischer Ring ist, können wir die Division mit Rest durchführen. Es gibt also eindeutige $p, r \in \mathbb{Z}$ mit

  $$n = p\mathsf{Ord}(a) + r$$

  und damit gilt:

  $$0 = na = p\underbrace{\mathsf{Ord}(a)a}_{=0} + ra$$

  also gilt $ra = 0$ mit $r < \mathsf{Ord}(a)$. Da $\mathsf{Ord}(a)$ die kleinste, positive natürliche Zahl mit dieser Eigenschaft ist, muss $r = 0$ gelten. Damit gilt $n = p\mathsf{Ord}(a)$, also $\mathsf{Ord}(a)|n$, was wir zeigen wollten.

"⇒" Wir wollen noch eine zweite Lösung präsentieren:
Weniger direkt, aber etwas eleganter ist die Lösung über Ideale. Wir betrachten die Menge

$$\alpha_a := \{n \in \mathbb{N} : an = 0\}$$

Sind $x, y \in \alpha_a, z \in \mathbb{Z}$, dann gilt: $(x + y)a = xa + ya = 0$ und $zxa = 0$, also $x + y \in \alpha_a$ und $zx \in \alpha_a$, das heißt α_a ist ein Ideal von $\mathbb{Z}$.
$\mathbb{Z}$ ist ein Hauptidealring, das heißt jedes Ideal ist Hauptideal und damit ist auch α_a ein Hauptideal, das heißt es existiert ein $d \in \mathbb{Z}$ mit $\alpha_a = d\mathbb{Z} = \{\ldots, -2d, -1d, 0, d, 2d, \ldots\}$. Da dies eine erschöpfende Auflistung aller Elemente ist, die a annihilieren, muss die Ordnung darin enthalten sein. Das kleinste positive Element in deser Menge ist d, also gilt $d = \mathsf{Ord}(a)$ per Definition von $\mathsf{Ord}(a)$. Insbesondere gilt, da $na = 0$ auch $n \in \alpha_a$, also gibt es ein $k \in \mathbb{Z}$ mit $n = k\mathsf{Ord}(a)$, das heißt $\mathsf{Ord}(a)|n$.

2. Wir listen die Elemente aus $\langle a \rangle$ auf. Durch abzählen sehen wir dann, dass die Ordnung der Gruppe gleich der Ordnung des Elements ist. Es gilt:

$$\langle a \rangle = \{ak \mid k \in \mathbb{Z}\} = \{a, 2a, \ldots, (\mathsf{Ord}(a) - 1)a, \underbrace{\mathsf{Ord}(a)a}_{=0}\}$$

Für $k > \mathsf{Ord}(a)$ gilt $k = p\mathsf{Ord}(a) + r$ mit $r \leq \mathsf{Ord}(a) - 1$ und $ka = ra$, also ist das Element bereits in dieser Auflistung enthalten.

Das sind aber genau $\mathsf{Ord}(a)$ Elemente, das heißt $\mathsf{Ord}(\langle a \rangle) = \mathsf{Ord}(a)$.

3. Sei $a \in A$ und $n = \mathsf{Ord}(A)$. Wir sollen zeigen, dass $na = 0$ gilt, insbesondere also, dass für alle $b \in A$ gilt, dass $b + na = b$ gilt. Da A eine Gruppe ist, reicht es aber tatsächlich aus zu zeigen, dass es ein einzelnes Element $b \in A$ gibt, sodass $b + na = b$. Wir betrachten dazu die Abbildung:

$$\begin{aligned} +a : A &\to A \\ b &\mapsto b + a \end{aligned}$$

Wir wollen zeigen, dass diese Abbildung bijektiv ist. Da A eine endliche Menge ist, reicht es aus, wenn wir Injektivität zeigen. Seien aber $b, c \in A$ mit $b + a = c + a$, dann gilt sofort $b = c$, also ist $+a$ injektiv. Wir summieren nun alle Elemente auf: (Da A endlich ist, können wir sie nummerieren, es gelte also $A = \{a_1, \ldots, a_n\}$)

$$z := \sum_{j=1}^{n} a_j$$

Es gilt

$$z + na = \sum_{j=1}^{n} a_j + a = \sum_{j=1}^{n} a_j = z$$

In der ersten Gleichheit verwenden wir die Distributivität der Addition. In der zweiten Gleichheit verwenden wir, dass auf der linken Seite und rechten Seite jeweils alle Elemente von A aufsummiert werden (Wir haben auf der linken Seite eine Summe von n Elementen. Jedes dieser Elemente ist die Summe aus a_j und a. Da $+a$ bijektiv ist, wird jedes Element aus A getroffen und kein Element zweimal getroffen, da dafür die Urbilder gleich sein müssten - das würde aber heißen, dass es $j, k \in [n]$ gäbe mit $a_j = a_k$. Wir haben aber jedes Element exakt einmal aufsummiert.) Da also $z + na = z$ gilt, ist $na = 0$, was wir zeigen sollten.

4. Wir betrachten die Abbildung

$$\begin{aligned} \Phi : \mathbb{Z} &\to \mathsf{Hom}(A, A) \\ n &\mapsto \begin{pmatrix} \varphi_n : A \to A \\ a \mapsto na \end{pmatrix} \end{aligned}$$

Da $\mathsf{Hom}(A, A)$ ein Ring ist, ist Φ ein Ringhomomorphismus. Die Kerne von Ringhomomorphismen sind immer Ideale des Definitionsrings, also gilt $\ker(\Phi) \trianglelefteq \mathbb{Z}$ und da $\mathbb{Z}$ ein Hauptidealring ist, gibt es damit ein $d \in \mathbb{Z}$ mit $\ker(\Phi) = d\mathbb{Z}$.
Da $\ker(\mathbb{Z}) = \{k \in \mathbb{Z} \mid \forall a \in A : ak = 0\}$, ist $\exp(A)$ auf jeden Fall Teil dieser Menge. Da $\exp(A)$ per Definition das kleinste Element ist, das diese Eigenschaft erfüllt, gilt $\ker(\mathbb{Z}) = \exp(A)\mathbb{Z}$. Auf der anderen Seite folgt mit Teilaufgabe 3, dass $\mathsf{Ord}(A)a = 0$ für alle $a \in A$ gilt, das heißt $\mathsf{Ord}(A) \in \ker(\Phi)$ und damit gibt es ein $k \in \mathbb{Z}$ mit $\mathsf{Ord}(A) = k \exp(A)$, also $\exp(A) | \mathsf{Ord}(A)$ - das war zu zeigen.

Aufgabe 2

1. *Kleiner Satz von Fermat* Sei p eine Primzahl und $a \not\equiv 0 \mod p$. Zeige, dass $a^{p-1} \equiv 1 \mod p$.

2. *Euler's Theorem* Sei $n \in \mathbb{N}$ und sei $a \in \mathbb{Z}$ koprim zu n. Zeige, dass $a^{\varphi(n)} \equiv 1 \mod n$.

Lösung:
Wir definieren die Eulersche Phi-Funktion als

$$\begin{aligned}\varphi : \mathbb{N} &\to \mathbb{N} \\ n &\mapsto |\{k \in \mathbb{N} \mid \mathsf{ggT}(k,n) = 1 \wedge k \leq n\}|\end{aligned}$$

1. Da p eine Primzahl ist, ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper, also sind alle Elemente außer $[p]$ invertierbar. Das heißt insbesondere, dass $[a] \in \mathbb{Z}/p\mathbb{Z}^\times$ liegt, da $[a] \neq [p]$ gilt.
Da $|\mathbb{Z}/p\mathbb{Z}| = p$ gilt, folgt $|\mathbb{Z}/p\mathbb{Z}^\times| = p-1$, das heißt die Einheiten bilden eine abelsche Gruppe mit $p-1$ Elementen. Da $a \in \mathbb{Z}/p\mathbb{Z}^\times$ liegt, gilt auch $\langle a \rangle \leq \mathbb{Z}/p\mathbb{Z}^\times$, die von a erzeugte Gruppe ist also Untergruppe von $\mathbb{Z}/p\mathbb{Z}^\times$ und wir können den Satz von Lagrange anwenden. Mit diesem gilt:
$$|\mathbb{Z}/p\mathbb{Z}^\times| = |\mathbb{Z}/p\mathbb{Z}^\times : \langle a \rangle| \cdot |\langle a \rangle|$$
Die für uns relevante Aussage ist, dass damit $\mathsf{Ord}(\langle a \rangle) | \mathsf{Ord}(\mathbb{Z}/p\mathbb{Z}^\times)$ gilt. Mit Aufgabe 1.2 gilt $\mathsf{Ord}(a) = \mathsf{Ord}(\langle a \rangle)$. Kombinieren wir diese beiden Aussagen erhalten wir
$$\mathsf{Ord}(a) | p-1$$
also gilt mit Aufgabe 1.1, dass (Man beachte hier, dass $\mathbb{Z}/p\mathbb{Z}^x$ eine Gruppe ist, die multiplikativ geschrieben wird, das neutrale Element ist also die 1 nicht 0.)
$$a^{p-1} \equiv 1 \mod p$$
das ist die zu zeigende Aussage.

2. Da wir eine Aussage $\mod n$ zeigen wollen, befinden wir uns in $\mathbb{Z}/n\mathbb{Z}$. Sei $k \in \mathbb{Z}$ eine Zahl, die zum Wert von $\varphi(n)$ beiträgt, d.h. eine Zahl die teilerfremd zu n ist. Dann existieren mit dem Lemma von Bézout $p, q \in \mathbb{Z}$ mit
$$pn + qk = 1 \Leftrightarrow qk \equiv 1 \mod n$$
also gilt $[k] \in \mathbb{Z}/n\mathbb{Z}^\times$. Insbesondere gilt also (beachte, dass das Lemma von Bézout eine Äquivalenz ist, die Aussage also in beide Richtungen gilt, d.h. aus $[k] \in \mathbb{Z}/n\mathbb{Z}^\times$ kann man umgekehrt $\mathsf{ggT}(k,n) = 1$ folgern.), dass
$$\varphi(n) = |\mathbb{Z}/n\mathbb{Z}^\times|$$
Da $\mathbb{Z}/n\mathbb{Z}^\times$ eine endliche abelsche Gruppe ist, können wir die erste Aufgabe anwenden. Mit Aufgabe 1.3 folgt, dass für alle Elemente $[a] \in \mathbb{Z}/n\mathbb{Z}^\times$ gilt
$$a^{\varphi(n)} = a^{|\mathbb{Z}/n\mathbb{Z}|} \equiv 1 \mod n$$
Das ist, was wir zeigen wollten.

Aufgabe 3
Seien A, B endliche abelsche Gruppen und sei $C := A \times B$.

1. Sei $(a,b) \in C$. Zeige $\mathsf{Ord}((a,b)) = \mathsf{kgV}(\mathsf{Ord}(a), \mathsf{Ord}(b))$.

2. Zeige $|C| = |A| \times |B|$ und $\exp(C) = \mathsf{kgV}(\exp(A), \exp(B))$.

Lösung:

1. Aus Aufgabe 1.1 gilt für $(a,b) \in C$ und $n \in \mathbb{N}$, dass

$$n \cdot (a,b) = 0 \Leftrightarrow \mathsf{Ord}(a,b) | n$$

Da Addition und Skalarmultiplikation in C komponentenweise durchgeführt werden, gilt $n \cdot (a,b) = (na, nb)$. Analog gilt

$$(na, nb) = 0 \Leftrightarrow na = 0 \wedge nb = 0 \Leftrightarrow \mathsf{Ord}(a) | n \wedge \mathsf{Ord}(b) | n$$

Wir wählen nun $n = \mathsf{Ord}(a,b)$, dann gilt $\mathsf{Ord}(a) | \mathsf{Ord}(a,b)$ und $\mathsf{Ord}(b) | \mathsf{Ord}(a,b)$, also ist die Ordnung von (a,b) auf jeden Fall ein Vielfaches der Ordnungen von a und b. Gäbe es ein kleineres Vielfaches k, dann gälte $\mathsf{Ord}(a) | k$ und $\mathsf{Ord}(b) | k$ also laut unser obigen Äquivalenzkette auch $\mathsf{Ord}(a,b) | k$. Da wir angenommen haben, dass $k < \mathsf{Ord}(a,b)$ ergibt das aber einen Widerspruch, also ist n bereits das kleinste gemeinsame Vielfache von $\mathsf{Ord}(a)$ und $\mathsf{Ord}(b)$. Das galt zu zeigen.

2. Die Anzahl der Elemente erhält man einfach durch abzählen, bzw. durch die Anzahl der Elemente des kartesischen Produkts von Mengen.
Wir zeigen, dass die linke Seite der Gleichung die rechte Seite teilt und umgekehrt.

- $\exp(C) | \mathsf{kgV}(\exp(A), \exp(B))$:
Wir schreiben $n := \mathsf{kgV}(\exp(A), \exp(B))$. Dann gilt $\exists x, y \in \mathbb{Z}$ mit $n = x \exp(A) = y \exp(B)$.
Sei nun $(a,b) \in C$ beliebig, dann gilt

$$n(a,b) = (na, nb) = (\underbrace{x \exp(A) a}_{=0}, \underbrace{y \exp(B) b}_{=0}) = (0,0)$$

Wir betrachten weiter

$$\Phi_C : \mathbb{Z} \to \mathsf{Hom}(C, C)$$
$$n \mapsto \begin{pmatrix} \varphi_n : C \to C \\ (a,b) \mapsto (na, nb) \end{pmatrix}$$

Da die Endomorphismen von C einen Ring bilden ist dies ein Ringhomomorphismus und damit gilt $\ker(\Phi_C) \trianglelefteq \mathbb{Z}$ und damit ist der Kern ein Hauptideal, also von der Form $\ker(\Phi_C) = k\mathbb{Z}$ für ein $k \in \mathbb{Z}$. Da der Exponent einer Gruppe die kleinste Zahl mit $\forall (a,b) \in C : (na, nb) = 0$ ist, gilt $k = \exp(C)$. Und da unser n diese Eigenschaft ebenfalls erfüllt, also im Kern der Abbildung Φ_C liegen muss, folgt damit $k | n$, also $\exp(C) | \mathsf{kgV}(\exp(A), \exp(B))$.

- $\mathsf{kgV}(\exp(A), \exp(B)) | \exp(C)$:
Es sei nun $n = \exp(C)$, dann gilt:

$$\forall (a,b) \in C : n(a,b) = (na, nb) = 0$$

also insbesondere gilt $\forall a \in A : na = 0$ und $\forall b \in B : nb = 0$. Wir führen hier das Argument mit dem Kern von Φ_A und Φ_B analog durch und erhalten $\exp(A)|n$ und $\exp(B)|n$. Daraus folgt aber bereits direkt, dass

$$\mathsf{kgV}(\exp(A), \exp(B))|\exp(C)$$

Da die beiden Zahlen sich gegenseitig teilen, müssen sie die gleiche Zahl sein, was wir zeigen wollten.

Aufgabe 4

1. Sei $(A, +)$ eine endliche abelsche Gruppe. Zeige, dass

$$\exp(A) = \mathsf{kgV}\{\mathsf{Ord}(a) \mid a \in A\}$$

2. Sei V ein n-dimensionaler $\mathbb{K}$-Vektorraum mit Endomorphismus $f : V \to V$. Es sei

$$U_v := \langle v \rangle_f = \langle v, f(v), f^2(v), \ldots \rangle$$

und $\mu_v := \mu_{f|_{U_v}}$. Zeige, dass

$$\mu_f = \mathsf{kgV}\{\mu_v \mid v \in V\}$$

Lösung:
Wir erinnern uns an die Analogien aus dem Kommentar zur ersten Teilaufgabe. Dies wird hier fortgesetzt.

1. Die Lösung dieser Aufgabe ist analog zur Lösung der Aufgabe 3.2.
Sei $n = \exp(A)$, dann gilt für alle $a \in A$, dass $na = 0$ und damit $\mathsf{Ord}(a)|n$. Das heißt aber, dass $\mathsf{kgV}\{\mathsf{Ord}(a) \mid a \in A\}|\exp(A)$ gilt.
Auf der anderen Seite sei $k = \mathsf{kgV}\{\mathsf{Ord}(a) \mid a \in A\}$, dann gilt für alle $a \in A$, dass $k = \mathsf{Ord}(a) \cdot k_a$, also $ka = 0$ und damit gilt $k|\exp(A)$.
Da beide Seiten sich gegenseitig teilen, sind sie gleich.

2. Da μ_f das normierte Polynom kleinsten Grades mit $\mu_f(f) = 0$ ist, gilt:

$$\forall v \in V : \mu_f(f|_{U_v}) = 0$$

denn falls $\mu_f(f) = 0$ ist, dann gilt das auch für jede Einschränkung von f. Da $\mu_f(f|_{U_v}) = 0$ gilt, muss μ_v ein Teiler von μ_f sein. Da alle μ_v Teiler von μ_f sind, gilt das auch für das kleinste gemeinsame Vielfache. Es gilt also bereits

$$\mathsf{kgV}\{\mu_v \mid v \in V\}|\mu_f$$

Umgekehrt sei $\mu = \mathsf{kgV}\{\mu_v \mid v \in V\}$, dann gibt es für jedes $v \in V$ ein P_v mit $\mu = \mu_v P_v$ und damit gilt:

$$\forall v \in V : \mu(f)(v) = P_v \mu_v(f|_{U_v})(v) = 0$$

Da aber die Nullabbildung die einzige Abbildung ist, die alle $v \in V$ auf 0 abbildet, folgt damit, dass $\mu(f)$ bereits diese Nullabbildung ist, also muss $\mu_f|\mu$ gelten, da μ_f das Polynom

kleinsten Grades mit dieser Eigenschaft ist.
Wir haben die Teilbarkeit in beide Richtungen gezeigt, also sind beide Polynome gleich.