EXTRABLATT

Aufgabe 1. Sei $(G, \circ)$ eine beliebige endliche Gruppe mit Ordnung n und H eine Untergruppe von G mit Ordnung m. Gibt es immer ein $k \in \mathbb{N}$ mit $m \cdot k = n$?

Ja, solch ein k gibt es immer. Zunächst wissen wir aus der Vorlesung, dass $\sim_H$ definiert durch $a \sim_H b \Leftrightarrow a \circ b^{-1} \in H$ eine Äquivalenzrelation auf G ist und von Blatt 5 Aufgabe 2, dass die Äquivalenzklassen gerade die Nebenklassen sind, also für $a \in G$,

$$[a]_{\sim_H} = a \circ H = \{a \circ g \mid g \in H\}.$$

Daran sieht man, dass jede Äquivalenzklasse genau die Größe m hat, denn für verschiedene $g, h \in H$ ist auch $a \circ g \neq a \circ h$, sonst wäre

$$g = a^{-1} \circ a \circ g = a^{-1} \circ a \circ h = h.$$

Da G endlich ist, existieren auch nur endlich viele Äquivalenzklassen von $\sim_H$. Sei $k \in \mathbb{N}$ die Anzahl der Äquivalenzklassen.
Außerdem wissen wir aus der Vorlesung, dass alle Äquivalenzklassen disjunkt sind und G somit eine *disjunkte* Vereinigung der Äquivalenzklassen ist. Nun besteht G also aus k Äquivalenzklassen und jede Äquivalenzklasse aus m Elementen. Damit besteht G aus $k \cdot m = n$ Elementen.

Bemerkung: Die Anzahl k der Äquivalenzklassen von $\sim_H$ wird auch als der *Index von H in G* bezeichnet und als $[G : H]$ geschrieben. Der hier bewiesene Sachverhalt

$$|G| = [G : H] \cdot |H|$$

ist auch bekannt als der *Satz von Lagrange*.

Aufgabe 2. Wir betrachten die folgende Matrix in $M_{3,3}(\mathbb{Z}_2)$:

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

a) Zeigen Sie, dass $A \in \mathrm{GL}_3(\mathbb{Z}_2)$ ist und bestimmen Sie die Ordnung von A.

b) Sei $K = \{A^k \mid k \in \mathbb{Z}\} \cup \{0_{M_{3,3}(\mathbb{Z}_2)}\}$. Ist K zusammen mit der Matrixaddition und -multiplikation ein Körper?

a) Wir können die Determinante von A leicht mit der Regel von Sarrus für 3×3-Matrizen ausrechnen und erhalten $\det(A) = 1 \neq 0$, also ist $A \in \mathrm{GL}_3(\mathbb{Z}_2)$.
Nun zur Ordnung von A. Zur Erinnerung: A ist von endlicher Ordnung, falls ein $n \in \mathbb{N}$ existiert, sodass $A^n = 1_{M_{3,3}(\mathbb{Z}_2)}$ gilt, und hat Ordnung n, falls es keine kleinere natürliche Zahl mit dieser Eigenschaft gibt; andernfalls ist A von unendlicher Ordnung. Da $\mathbb{Z}_2$ aber endlich ist, ist auch $M_{3,3}(\mathbb{Z}_2)$ endlich und A kann nicht von unendlicher Ordnung sein.
Um die Ordnung von A zu bestimmen, können wir A als lineare Abbildung von ${\mathbb{Z}_2}^3$ nach ${\mathbb{Z}_2}^3$ mit $v \mapsto A \cdot v$ betrachten und da ${\mathbb{Z}_2}^3$ endlich ist, können wir die ganze Abbildung als Tabelle aufschreiben. Man beachte dabei, dass $e_i + e_i = 0$ für jedes $i \leq 3$ gilt.

$v:$	0	e_1	e_2	e_3	e_1+e_2	e_2+e_3	$e_1+e_2+e_3$	e_1+e_3
$Av:$	0	e_2	e_3	e_1+e_2	e_2+e_3	$e_1+e_2+e_3$	e_1+e_3	e_1

Außerdem haben wir $A^n = 1_{M_{3,3}(\mathbb{Z}_2)}$ genau dann wenn $v \mapsto A^n \cdot v$ die Identitätsabbildung auf ${\mathbb{Z}_2}^3$ ist. Man kann nun in der Tabelle gut nachvollziehen, dass $A^7 \cdot v = v$ für alle $v \in {\mathbb{Z}_2}^3$ ist und dass gleichzeitig $A^i \cdot e_1 \neq e_1$ für $i \leq 6$ gilt, also dass $A^i \cdot v$ nicht die Identität ist. Damit hat A die Ordnung 7.
Alternativ kann man an der Tabelle auch ablesen, dass die Abbildung eine Permutation auf ${\mathbb{Z}_2}^3$ ist, genauer ein Zykel der Länge 7, womit A auch Ordnung 7 haben muss.

b) Ja, $(K, +, \cdot)$ ist ein Körper. Da die Ordnung von A wie in a) gezeigt 7 ist, gilt

$$K = \{0_{M_{3,3}(\mathbb{Z}_2)}, 1_{M_{3,3}(\mathbb{Z}_2)}, A, A^2, A^3, A^4, A^5, A^6\}.$$

Damit $(K, +, \cdot)$ überhaupt eine Chance hat ein Körper zu sein, muss die Menge K unter der Matrizenaddition und -multiplikation abgeschlossen sein.
Für die Multiplikation ist dies recht leicht zu sehen: Jede Multiplikation mit der Nullmatrix ergibt ebendiese und mit $A^0 = 1_{M_{3,3}(\mathbb{Z}_2)}$ ist jede andere Multiplikation von Elementen aus K von der Form $A^i \cdot A^j = A^{i+j}$ für $i, j \leq 6$. Ist $i + j < 7$ so ist $A^{i+j} \in K \setminus \{0_{M_{3,3}(\mathbb{Z}_2)}\}$, ansonsten ist $A^{i+j} = A^7 \cdot A^{i+j-7} = A^{i+j-7} \in K \setminus \{0_{M_{3,3}(\mathbb{Z}_2)}\}$, da $A^7 = 1_{M_{3,3}(\mathbb{Z}_2)}$.

Schwieriger ist die Abgeschlossenheit von K unter der Matrizenaddition. Da die Nullmatrix das neutrale Element der Matrixaddition ist, ergibt jede Summe eines Elements aus K mit der Nullmatrix natürlich auch ein Element aus K. Außerdem ist jedes Element in $M_{3,3}(\mathbb{Z}_2)$ zu sich selbst invers, da $1+1=0$ in $\mathbb{Z}_2$ gilt. Also ist die Summe von einem Element aus K mit sich selbst ebenfalls in K.
Natürlich könnte man jetzt einfach jede mögliche Kombination von verschiedenen Elementen aus $K \setminus \{0_{M_{3,3}(\mathbb{Z}_2)}\}$ durchrechnen, wir begnügen uns aber mit den folgenden drei Rechnungen und argumentieren danach weiter:

$$A^0 + A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} = A^3 \in K$$

$$A^0 + A^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = A^6 \in K$$

$$A^0 + A^3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = A \in K$$

Sei nun allgemeiner $0 \leq i < j \leq 6$. Dann ist $A^i + A^j = A^i \cdot (A^0 + A^{j-i})$ und da K unter der Matrixmultiplikation abgeschlossen ist, reicht es nachzuprüfen, ob $A^0 + A^{j-i} \in K$ ist. Für den Fall, dass $j - i < 4$ gilt, haben wir das gerade nachgerechnet. Andernfalls ist $4 \leq j - 1 \leq 6$ und wir betrachten nun $A^i + A^j = A^j \cdot (A^{7-j+i} + A^0)$. Nun ist $7 - j + 1 < 4$ und somit haben wir schon nachgerechnet, dass $A^{7-j+i} + A^0 \in K$ gilt und somit auch $A^i + A^j$ in K ist.

Mit der Abgeschlossenheit von K unter der Matrixaddition können wir nun leicht das Untergruppenkriterium anwenden um zu sehen, dass K eine Untergruppe von $(M_{3,3}(\mathbb{Z}_2), +)$ ist: Offensichtlich ist $K \neq \emptyset$ und für $B, C \in K$ ist auch $B + (-C) = B + C \in K$. Da die Matrixaddition kommutativ ist, ist $(K, +)$ auch eine abelsche Gruppe.

Genauso können wir nachrechnen, dass $K \setminus \{0_{M_{3,3}(\mathbb{Z}_2)}\}$ eine Untergruppe von $(\mathrm{GL}_3(\mathbb{Z}_2), \cdot)$ ist: Es gilt $K \setminus \{0_{M_{3,3}(\mathbb{Z}_2)}\} \neq \emptyset$ und für $A^i, A^j \in K \setminus \{0_{M_{3,3}(\mathbb{Z}_2)}\}$ ist $A^i \cdot A^{-j} = A^i \cdot A^{7-j} \in K \setminus \{0_{M_{3,3}(\mathbb{Z}_2)}\}$ aufgrund der Abgeschlossenheit der Multiplikation. Da außerdem $A^i \cdot A^j = A^j \cdot A^i$ für alle i und j gilt, ist $(K \setminus \{0_{M_{3,3}(\mathbb{Z}_2)}\}, \cdot)$ also auch eine abelsche Gruppe.

Da das Distributivgesetz für alle Matrizen gilt, gilt es auch für K. Damit ist $(K, +, \cdot)$ also tatsächlich ein Körper.

Aufgabe 3. Wir betrachten die unendlichen Gruppen $(\mathbb{Z}, +)$ und $(\mathbb{Q}, +)$. Sei G eine echte Untergruppe von $(\mathbb{Z}, +)$ und H eine echte Untergruppe von $(\mathbb{Q}, +)$, d.h. es existieren mindestens ein $z \in \mathbb{Z}$ und ein $q \in \mathbb{Q}$ mit $z \notin G$ und $q \notin H$.

a) Welche Ordnungen kann G besitzen? Kann der Quotientenraum $\mathbb{Z}/G$ unendlich groß sein?

b) Kann der Quotientenraum $\mathbb{Q}/H$ endlich sein?

a) G ist entweder von unendlicher Ordnung oder hat Ordnung 1.
Die triviale Untergruppe $G = \{0\}$ ist eine "echte" Untergruppe von $(\mathbb{Z}, +)$ und hat Ordnung 1. Existiert allerdings ein $a \in G \setminus \{0\}$ so ist auch $a + a \in G$, $a + a + a \in G$ und generell

$$n \cdot a = \underbrace{a + \cdots + a}_{n-mal} \in G,$$

$$-n \cdot a = \underbrace{-a + \cdots + -a}_{n-mal} \in G.$$

Also ist $\{k \cdot a \mid k \in \mathbb{Z}\} \subseteq G$ womit G schon unendlich viele Elemente besitzt.

Der Quotientenraum $\mathbb{Z}/G$ ist genau dann unendlich, falls G Ordnung 1 hat.
Falls G Ordnung 1 hat, so ist $G = \{0\}$ und $\mathbb{Z}/G = \{\{n\} \mid n \in \mathbb{Z}\}$ ist unendlich groß. Falls G nicht Ordnung 1 hat, so existiert ein $n \in \mathbb{N} \cap G$. Für ein beliebiges $a \in \mathbb{Z}$ existieren dann ein $k \in \mathbb{Z}$ und ein $r \in \{0, 1, \ldots n-1\}$ mit $a = k \cdot n + r$. Also ist $a - r \in \{k \cdot n \mid k \in \mathbb{Z}\} \subseteq G$ und damit $a \in r + G$. Nun ist der Quotientenraum aber endlich, denn da a beliebig war haben wir gezeigt:

$$\mathbb{Z}/G = \{r + G \mid r \in \{0, 1, \ldots, n-1\}\}.$$

b) Der Quotientenraum $\mathbb{Q}/H$ ist immer unendlich.
Für einen Widerspruch machen wir folgende Annahme: $H \subsetneq \mathbb{Q}$ sei eine Untergruppe von $(\mathbb{Q}, +)$ so dass $\mathbb{Q}/H$ endlich ist. Dann existieren ein $n \in \mathbb{N}$ und $q_1, \ldots, q_n \in \mathbb{Q}$ mit

$$\mathbb{Q}/H = \{q_i + H \mid i \leq n\}.$$

Da $\mathbb{Q}$ gerade die (endliche) Vereinigung der Mengen $q_i + H$ ist, muss H also unendlich sein (siehe auch Aufgabe 1 diese Blattes). Insbesondere existiert ein $q \in H \setminus \{0\}$ und da H unter additiven Inversen abgeschlossen ist können wir annehmen, dass $q \in \mathbb{Q}^+$ ist. Dann existieren $r \in \mathbb{N}$ sowie $r_1, \ldots, r_n \in \mathbb{Z}$ und $s, s_1, \ldots, s_n \in \mathbb{N}$ mit

$$q = \frac{r}{s} \quad \text{und} \quad q_i = \frac{r_i}{s_i} \text{ für alle } i \leq n.$$

Da $q \in H$ ist, gilt auch

$$r = s \cdot q = \underbrace{\frac{r}{s} + \cdots + \frac{r}{s}}_{s-mal} \in H.$$

Wir definieren schließlich noch $m := r \cdot s_1 \cdot \cdots \cdot s_n \in \mathbb{N}$.
Sei nun $p \in \mathbb{Q}$ beliebig und $p' = \frac{p}{m} \in \mathbb{Q}$. Da p' in einer unserer endlich vielen Äquivalenzklassen liegt existieren ein $i \leq n$ und ein $h \in H$ so dass $p' = q_i + h$. Somit haben wir

$$\begin{aligned} p = p' \cdot m = m \cdot (q_i + h) = m \cdot q_i + m \cdot h = m \cdot \frac{r_i}{s_i} + m \cdot h \\ = r \cdot \underbrace{s_1 \cdot \cdots \cdot s_{i-1} \cdot s_{i+1} \cdot \cdots \cdot s_n}_{=:\pi_i \in \mathbb{N}} + m \cdot h = \underbrace{\pi_i \cdot r}_{\in H} + \underbrace{m \cdot h}_{\in H} \in H. \end{aligned}$$

Da p beliebig war haben wir also $\mathbb{Q} = H$ gezeigt und das ist ein Widerspruch zu unserer Annahme, dass H eine echte Untergruppe ist.

Aufgabe 4. Sei V ein K-Vektorraum und $F : V \to V$ eine lineare Abbildung. Gibt es dann immer eine *bijektive* lineare Abbildung $G : V \to V$, sodass $F \circ G \circ F = F$ ist?

Solch ein G gibt es immer genau dann wenn V endlich-dimensional ist.

Sei V also endlich-dimensional, sagen wir $\dim(V) = n$. Um einen Automorphismus der gesuchten Art zu finden, betrachten wir nun verschiedene Basen von V, mit deren Hilfe wir G definieren können.
Sei W ein Komplementärraum des Bildes $F[V]$ in V und sei $\dim(F[V]) = m \leq n$, dann ist also $\dim(W) = n - m$. Sei nun also $\{b_1, \ldots, b_m\}$ eine Basis von $F[V]$ und $\{b_{m+1}, \ldots, b_n\}$ eine Basis von W womit $B = \{b_1, \ldots, b_n\}$ eine Basis von V ist. Außerdem gilt die Dimensionsformel:

$$\dim V = \dim(\mathrm{Kern}(F)) + \dim(F[V]).$$

Also ist auch $\dim(\mathrm{Kern}(F)) = n-m$. Seien nun U ein Komplementärraum von $\mathrm{Kern}(F)$, $\{c_1, \ldots, c_m\}$ eine Basis von U und $\{c_{m+1}, \ldots, c_n\}$ eine Basis von $\mathrm{Kern}(F)$ womit wir mit $C = \{c_1, \ldots, c_n\}$ eine zweite Basis von V haben.
Nun wollen wir die Abbildung G auf der Basis B definieren und die Bilder mit Hilfe der Basis C so darstellen, dass gerade $F \circ G \circ F = F$ gilt. Dazu erinnern wir uns zunächst, dass für $v_1, v_2 \in V$ mit $F(v_1) = F(v_2)$ ein $a \in \mathrm{Kern}(F)$ existiert mit $v_1 + a = v_2$, also ist das Urbild $F^{-1}[\{w\}]$ eines Elements $w \in F[V]$ von der Form $v + \mathrm{Kern}(F)$ (siehe Blatt 2 Aufgabe 1b). Sei also $w \in F[V]$ beliebig. Da U ein Komplementärraum von $\mathrm{Kern}(F)$ ist, existiert genau ein $d \in V$, sodass $F^{-1}[\{w\}] \cap U = \{d\}$ ist. Zur Vollständigkeit ein Beweis davon:

Zuerst zeigen wir, dass der Schnitt nicht leer ist. Sei dazu $v \in F^{-1}[\{w\}]$. Dann können wir v als Linearkombination der Basis C schreiben, also

$$v = \sum_{i=1}^{n} \alpha_i c_i.$$

Aufgrund der Definition von C ist dann gerade $v = v_U + v_0$, wobei

$$v_U = \sum_{i=1}^{m} \alpha_i c_i \in U \quad \text{und}$$

$$v_0 = \sum_{i=m+1}^{n} \alpha_i c_i \in \mathrm{Kern}(F).$$

Damit ist aber auch $v_U \in F^{-1}[\{w\}] \cap U$, denn

$$F(v_U) = F(v_U) + F(v_0) = F(v_U + v_0) = F(v) = w.$$

Seien nun $v, d \in F^{-1}[\{w\}] \cap U$ zwei Elemente aus dem Schnitt. Dann ist einerseits $v - d \in K$ da $v, d \in U$; andererseits ist aber auch $v - d \in \mathrm{Kern}(F)$, denn $F(v) = F(d)$. Also ist $v - d \in U \cap \mathrm{Kern}(F) = \{0_V\}$, da U und $\mathrm{Kern}(F)$ Komplementärräume sind. Somit ist $v = d$.

Seien nun also $d_i \in V$ für $i \leq m$ so, dass $F^{-1}[\{b_i\}] \cap U = \{d_i\}$ gilt. Da die Bilder $F(d_1), \ldots, F(d_m)$ als Basis von $F[V]$ linear unabhängig sind, sind auch $d_1, \ldots, d_m$ linear unabhängig. Das bedeutet aber auch, dass $\{d_1, \ldots, d_m\}$ eine weitere Basis von U und $\{d_1, \ldots, d_m, c_{m+1}, \ldots, c_n\}$ eine Basis von V ist.

Schließlich definieren wir G als die lineare Fortsetzung von

$$G(b_i) = \begin{cases} d_i & \text{falls } 1 \leq i \leq m, \\ c_i & \text{falls } m < i \leq n. \end{cases}$$

Da G zwei Basen von V injektiv aufeinander abbildet, ist auch ganz G injektiv. Da V endlich-dimensional ist, ist G dann direkt surjektiv und somit auch bijektiv (siehe auch Blatt 6 Aufgabe 2).
Außerdem gilt $F \circ G \circ F = F$: Sei $v \in V$ beliebig. Wir schreiben das Bild von v als Linearkombination aus $\{b_1, \ldots, b_m\}$, also

$$F(v) = \sum_{i=1}^{m} \alpha_i b_i.$$

Wendet man G darauf an, erhält man

$$G(F(v)) = G\left(\sum_{i=1}^{m} \alpha_i b_i\right) = \sum_{i=1}^{m} \alpha_i G(b_i) = \sum_{i=1}^{m} \alpha_i d_i.$$

Da $d_i \in F^{-1}[\{b_i\}]$ ist erhält man mit erneutem Anwenden von F schließlich

$$(F \circ G \circ F)(v) = F(G(F(v))) = F\left(\sum_{i=1}^{m} \alpha_i d_i\right) = \sum_{i=1}^{m} \alpha_i F(d_i) = \sum_{i=1}^{m} \alpha_i b_i = F(v).$$

Sei V nun unendlich-dimensional. Dann existiert eine linear unabhängige Menge $B = \{b_i \mid i \in \mathbb{N}\}$, ohne Einschränkung der Allgemeinheit sei B auch eine Basis. Dann können wir eine lineare Abbildung $F : V \to V$ definieren durch

$$F(b_1) = b_1 \quad \text{und} \quad F(b_{i+1}) = b_i \text{ für alle } i \in \mathbb{N}.$$

Angenommen, es gäbe einen Automorphismus $G : V \to V$ mit $F \circ G \circ F = F$. Dann wäre aber $G(b_i) = b_{i+1}$ für $i \geq 2$ und somit $b_1 \notin G[V]$ oder $b_2 \notin G[V]$, ein Widerspruch zur Surjektivität von G.

Aufgabe 5. Sei $A \in M_{n,n}(K)$ *nilpotent*, das bedeutet es existiert ein $m \in \mathbb{N}$, sodass $A^m = 0_{M_{n,n}(K)}$. Ist dann auch immer $A^n = 0_{M_{n,n}(K)}$?

Ja, falls $A \in M_{n,n}(K)$ nilpotent ist ist auch $A^n = 0_{M_{n,n}(K)}$.
Wir betrachten für $k \in \mathbb{N}$ die lineare Abbildung

$$f_{A^k} : K^n \to K^n, \quad v \mapsto A^k \cdot v.$$

Da $f_{A^{k+i}} = f_{A^k} \circ f_{A^i}$ für alle $i, k \in \mathbb{N}$ gilt, haben wir

$$\text{Kern}(f_{A^k}) \subseteq \text{Kern}(f_{A^{k+1}}).$$

Außerdem gilt folgendes:

$$\text{Kern}(f_{A^{k+1}}) = \text{Kern}(f_{A^k}) \Rightarrow \text{Kern}(f_{A^{k+2}}) = \text{Kern}(f_{A^{k+1}}) \tag{$*$}$$

Um das zu sehen, sei $v \in \text{Kern}(f_{A^{k+2}})$ bliebig. Dann ist $f_A(v) \in \text{Kern}(f_{A^{k+1}}) = \text{Kern}(f_A)$, denn $f_{A^{k+1}}(f_A(v)) = f_{A^{k+2}}(v) = 0$. Schließlich gilt damit auch $f_{A^{k+1}}(v) = f_{A^k}(f_A(v)) = 0$ und somit $v \in \text{Kern}(f_{A^{k+1}})$.
Induktiv folgt aus $\text{Kern}(f_{A^{k+1}}) = \text{Kern}(f_{A^k})$ mit $(*)$ auch $\text{Kern}(f_{A^{k'}}) = \text{Kern}(f_{A^k})$ für alle $k' > k$.
Diese Tatsache, dass der Kern bis zu einem gewissen Punkt immer größer wird und ab dann konstant bleibt, wollen wir nun für unsere Behauptung nutzen:
Sei m_0 die kleinste natürliche Zahl mit $A^{m_0} = 0_{M_{n,n}(K)}$, das bedeutet auch $\text{Kern}(f_{A^{m_0}}) = K^n$. Da m_0 minimal mit dieser Eigenschaft ist, gilt $\text{Kern}(f_{A^{m_0-1}}) \subsetneq \text{Kern}(f_{A^{m_0}})$ und allgemeiner $\text{Kern}(f_{A^i}) \subsetneq \text{Kern}(f_A^{i+1})$ für alle $i < m_0$ aufgrund von $(*)$. Das heißt, wir haben

$$\text{Kern}(f_{A^0}) \subsetneq \text{Kern}(f_{A^1}) \subsetneq \cdots \subsetneq \text{Kern}(f_{A^{m_0}})$$

und, da jeder Kern ein Unterraum von K^n ist, auch

$$\dim(\text{Kern}(f_{A^0})) < \dim(\text{Kern}(f_{A^1})) < \cdots < \text{Kern}(f_{A^{m_0}}).$$

Daraus folgt aber auch $i \leq \dim(\text{Kern}(f_{A^i}))$ für alle $i \leq m_0$ und somit $n = \dim(\text{Kern}_(f_{A^{m_0}})) \geq m_0$.
Damit gilt also $\text{Kern}(f_{A^n}) = K^n$, d.h. $A^n = 0_{M_{n,n}(K)}$.