Lösung 17:
Satz von Cayley-Hamilton & spezielle Endomorphismen

1. **a)**

- Es ist klar, dass $T(0) = 0 \in \{0\}$ und folglich ist $T\{0\} \subseteq \{0\}$, also ist $\{0\}$ ein T-invarianter Unterraum.
- Per definitionem gilt für $v \in V$, dass $T(v) \in V$, und folglich ist $T(V) \subseteq V$ und also V ein T-invarianter Unterraum.
- Sei $v \in \mathrm{Im}(T)$, dann ist per definitionem $v \in V$ und also $T(v) \in \mathrm{Im}(T)$, also ist $T\big(\mathrm{Im}(T)\big) \subseteq \mathrm{Im}(T)$. Folglich ist $\mathrm{Im}(T)$ ein T-invarianter Unterraum.
- Sei $v \in \mathrm{Ker}(T)$, dann ist $T(v) = 0$ in jedem Unterraum von V enthalten, also insbesondere in $\mathrm{Ker}(T)$. Das zeigt $T\big(\mathrm{Ker}(T)\big) \subseteq \mathrm{Ker}(T)$. Folglich ist $\mathrm{Ker}(T)$ ein T-invarianter Unterraum.
- Sei $\lambda \in \mathbb{K}$ beliebig und $E_\lambda := \{v \in V \mid T(v) = \lambda v\}$ (wir verallgemeinern die Aussage also leicht: Falls λ kein Eigenwert von T ist, dann gilt einfach $E_\lambda = \{0\}$). Sei $v \in E_\lambda$, dann ist $T(v) = \lambda v$ und also

$$T(T(v)) = T(\lambda v) = \lambda T(v),$$

sprich $T(v) \in E_\lambda$. Also ist $T(E_\lambda) \subseteq E_\lambda$ und somit E_λ ein T-invarianter Unterraum.

b) Da Ausdrücke mit zu vielen Klammern schnell unleserlich werden, schreiben wir hier häufig Tv für das Bild eines Vektors v unter einer linearen Abbildung T, sprich es ist $Tv := T(v)$.

"⇒": Sei $W \subseteq V$ ein S-invarianter Unterraum und sei $w \in \Phi(W)$. Sei $v \in W$ mit $w = \Phi(v)$. Dann ist

$$T(w) = T(\Phi v) = (\Phi S \Phi^{-1})(\Phi v) = \Phi \underbrace{S(v)}_{\in W} \in \Phi(W)$$

und da w beliebig war, folgt $T(\Phi(W)) \subseteq \Phi(W)$ und somit ist $\Phi(W)$ ein T-invarianter Unterraum von V.

Bitte wenden!

"⇐": Sei $W \subseteq V$ ein Unterraum, sodass $\Phi(W)$ ein T-invarianter Unterraum ist. Sei $v \in W$ beliebig. Dann ist

$$S(v) = S\Phi^{-1}(\Phi v) = \Phi^{-1}T(\Phi v).$$

Da $\Phi(W)$ ein T-invarianter Unterraum ist, existiert ein $w \in W$, sodass gilt $T(\Phi v) = \Phi w$. Es folgt

$$S(v) = \Phi^{-1}(\Phi w) = w \in W$$

und folglich ist W ein S-invarianter Unterraum.

2. Wir wissen dank Cayley-Hamilton, dass $A^n \in \operatorname{span}(I_n, A, \ldots, A^{n-1})$. Für den Beweis der Aussage machen wir eine Induktion nach $k \in \mathbb{N}$, d.h. wir zeigen mittels Induktion für alle $k \in \mathbb{N}$, dass gilt

$$\mathcal{T}_A(k) := \operatorname{span}(I_n, A, \ldots, A^k) \subseteq \operatorname{span}(I_n, A, \ldots, A^{n-1}).$$

Daraus folgt, dass $\bigcup_{k\in\mathbb{N}} \mathcal{T}_A(k) = \operatorname{span}(I_n, A, A^2, \ldots) \subseteq \operatorname{span}(I_n, A, \ldots, A^{n-1})$ (überzeugen Sie sich, dass die Definition der linearen Hülle impliziert, dass die Gleichheit gilt und fragen Sie nach, wenn dies unklar ist).

Sei $k \geq n$, sodass $A^k \in \operatorname{span}(I_n, A, \ldots, A^{n-1})$ ist. Wir zeigen nun, dass daraus folgt, dass A^{k+1} in $\operatorname{span}(I_n, A, \ldots, A^{n-1})$ enthalten ist. Gegeben seien Koeffizienten $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1} \in \mathbb{K}$ mit

$$A^k = \sum_{l=0}^{n-1} a_l A^l \text{ und } A^n = \sum_{l=0}^{n-1} b_l A^l, \tag{†}$$

dann ist auch

$$\begin{aligned} A^{k+1} =& A\sum_{l=0}^{n-1} a_l A^l = \sum_{l=1}^{n} a_{l-1}A^l \overset{(\dagger)}{=} a_{n-1}\sum_{l=0}^{n-1} b_l A^l + \sum_{l=1}^{n-1} a_{l-1}A^l \\ =& \sum_{l=1}^{n-1}(a_{n-1}b_l + a_{l-1})A^l + a_{n-1}b_0 I_n \end{aligned}$$

und somit ist $A^{k+1} \in \operatorname{span}(I_n, \ldots, A^{n-1})$.

3. a) "⇒": Angenommen T ist nilpotent mit $T^k = 0$ für ein $k \in \mathbb{N}$. Sei λ ein beliebiger Eigenwert von T, d.h. per definitionem: es existiert $v \in V \setminus \{0\}$, sodass $T(v) = \lambda v$. Dann ist $\lambda^k v = T^k(v) = 0$ und wegen $v \neq 0$ also $\lambda = 0$.

Siehe nächstes Blatt!

"⇐": Angenommen 0 ist der einzige Eigenwert von T in $\mathbb{C}$. Da über $\mathbb{C}$ jedes Polynom in Linearfaktoren zerfällt, ist $\mathrm{char}_T(X) = (-1)^n X^n$. Nach dem Satz von Cayley-Hamilton ist $T^n = (-1)^n \mathrm{char}_T(T) = 0$ und T somit nilpotent.

b) Für beliebige $A \in M_{n\times n}(\mathbb{K})$ gilt $Ae_l = \sum_{i=1}^n A_{il} e_i$ bzw. $L_A(e_l) = A^{(l)}$. Wenn nun A eine obere Dreieckmatrix mit Eintrag 0 auf der Diagonalen ist, dann ist $A^{(l)} \in \mathrm{span}(\{e_i \mid 1 \leq i < l\})$. Angenommen wir wissen, dass $L_A^k(\mathbb{K}^n) \subseteq \mathrm{span}(\{e_i \mid 1 \leq i < n-k\})$ für ein $0 \leq k \leq n$. Dann ist

$$\begin{aligned} L_A^{k+1}(\mathbb{K}^n) \subseteq & L_A\big(\mathrm{span}(\{e_i \mid 1 \leq i \leq n-k\})\big) = \mathrm{span}(\{A^{(i)} \mid 1 \leq i \leq n-k\}) \\ \subseteq & \mathrm{span}(\{e_i \mid 1 \leq i < n-(k+1)\}). \end{aligned}$$

Wir wissen aus dem Fall $k = 0$, dass $L_A^0(\mathbb{K}^n) \subseteq \mathrm{span}(\mathcal{E}_n)$, dass die Induktionsvoraussetzung wahr ist und somit folgt nach Induktion, dass

$$L_A^n(\mathbb{K}^n) \subseteq \mathrm{span}(\{e_i \mid 1 \leq i < n-n\}) = \mathrm{span}(\emptyset) = \{0\}$$

und folglich ist $L_A^n = 0$.

Alternativ dazu verwendet man im wesentlichen dasselbe Argument um zu zeigen, dass $A^n = 0$ ist, woraus dann ebenfalls $L_A^n = L_{A^n} = 0$ folgt.

c) Wir haben in der Vorlesung gezeigt, das für beliebige von 0 verschiedene $v \in V$ gilt: Sei $k \in \mathbb{N}$ minimal mit $T^k(v) = 0$, dann ist die Menge $\{T^l(v) \mid 0 \leq l < k\}$ linear unabhängig und enthält k Elemente. Da jede linear unabhängige Teilmenge von V wegen $\dim(V) = n < \infty$ maximal n paarweise verschiedene Elemente enthält, ist also $k \leq n$. Da T nilpotent ist, existiert zu jedem $v \in V \setminus \{0\}$ ein $k \in \mathbb{N}$ mit $T^k(v) = 0$ und beides kombiniert impliziert also, dass $T^n(v) = 0$ für alle $v \in V$ (da sicherlich $T(0) = 0$).

Beachte: Wir haben in der Vorlesung *nicht* gezeigt, dass $T^k = 0$ gilt, da k von v abhängen konnte. Angenommen $T(v) \neq 0$, dann liefert das Argument aus der Vorlesung angewandt auf den Startvektor $v' := T(v)$ ein minimales k mit $T^k(v') = 0$, für welches gilt $T^k(v) \neq 0$. Ein explizites Beispiel ist gegeben durch L_A mit

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

In diesem Falle gilt $T(e_2) = e_1$ und $T(e_1) = 0$. Das k zum Vektor e_1 ist also gleich 1, aber das k zum Vektor e_2 ist gleich 2.

4. a) "⇒": Angenommen $a_0 = 0$, dann ist das charakteristische Polynom von der Form $\mathrm{char}_A(X) = Xq(X)$. Also hat L_A den Eigenwert $0 \in \mathbb{K}$ und folglich existiert ein Eigenvektor $v \in \mathbb{K}^n \setminus \{0\}$, sodass $L_A(v) = 0 \cdot v = 0$. Insbesondere ist L_A nicht injektiv, somit nicht invertierbar und also ist A nicht invertierbar.

Bitte wenden!

"⇐": Angenommen $a_0 \neq 0$, dann ist nach dem Satz von Cayley-Hamilton

$$\begin{aligned} I_n &= -\frac{1}{a_0}\big((-1)^n A^n + a_{n-1}A^{n-1} + \cdots + a_1 A\big) \\ &= -\frac{1}{a_0} A\big((-1)^n A^{n-1} + a_{n-1}A^{n-2} + \cdots + a_1 I_n\big). \end{aligned}$$

Folglich hat A eine Rechtsinverse und ist somit invertierbar.

b) Dies folgt aus dem Argument in Teilaufgabe a), da jede Rechtsinverse eine Inverse und die Inverse eindeutig ist.

c) Wir berechnen das charakteristische Polynom einer 2×2-Matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$:

$$\begin{aligned} \mathrm{char}_A(X) &= (a - X)(d - X) - bc \\ &= X^2 - (a + d)X + ad - bc \\ &= X^2 - \mathrm{tr}(A)X + \det(A). \end{aligned}$$

Bemerkung: Diese Formel gilt allgemein in dem Sinne, als für $A \in M_{n\times n}(\mathbb{K})$ der konstante term des charakteristischen Polynoms gleich der Determinanten von A und der Koeffizient von X^{n-1} gleich $(-1)^{n-1}\mathrm{tr}(A)$ ist.

Für die Inverse einer 2×2-Matrix A gilt nach der Formel aus Teil a) also

$$A^{-1} = -\frac{1}{\det(A)}\left(A - \mathrm{tr}(A)I_2\right).$$

5. a) Die n-ten Einheitswurzeln sind die Nullstellen von $X^n - 1$. Wir wissen aus der Analysis, dass dieses Polynom höchstens n Nullstellen in $\mathbb{C}$ besitzt. Zudem wissen wir, dass die komplexen Zahlen $e^{2\pi \mathrm{i}\frac{k}{n}}$ für $0 \leq k < n$ paarweise verschieden sind, denn $e^{2\pi \mathrm{i}\frac{k}{n}} = e^{2\pi \mathrm{i}\frac{l}{n}}$ gilt genau dann, wenn $e^{2\pi \mathrm{i}\frac{k-l}{n}} = 1$, was, nach dem was in der Analysis gezeigt wurde, genau dann gilt, wenn $n|k - l$ und letzteres ist für $0 \leq k, l < n$ genau dann der Fall, wenn $k = l$.

Es gilt

$$(e^{2\pi \mathrm{i}\frac{k}{n}})^n - 1 = e^{2\pi \mathrm{i}k} - 1 = 0$$

und somit sind dies genau die maximal n paarweise verschiedenen Nullstellen von $X^n - 1$ in $\mathbb{C}$. Es bleibt zu zeigen, dass die Menge dieser Nullstellen eine Gruppe bezüglich komplexer Multiplikation ist. Tatsächlich ist die 1 als Nullstelle in μ_n enthalten und ein neutrales Element für die Nullstelle. Seien $0 \leq k, l < n$, dann gilt:

$$(e^{2\pi \mathrm{i}\frac{k}{n}} e^{2\pi \mathrm{i}\frac{l}{n}})^n - 1 = (e^{2\pi \mathrm{i}\frac{k}{n}})^n (e^{2\pi \mathrm{i}\frac{l}{n}})^n - 1 = 0,$$

sodass μ_n abgeschlossen ist unter komplexer Multiplikation. Des Weiteren wissen wir, dass $1 = e^{2\pi \mathrm{i}\frac{k}{n}} e^{-2\pi \mathrm{i}\frac{k}{n}}$ und $(e^{-2\pi \mathrm{i}\frac{k}{n}})^n = e^{-2\pi \mathrm{i}k} = 1$, so dass für $\omega \in \mu_n$

Siehe nächstes Blatt!

auch die Inverse bezüglich komplexer Multiplikation $\omega^{-1} = \overline{\omega}$ in μ_n liegt. Da die komplexe Multiplikation assoziativ ist, ist μ_n eine Gruppe.

Aus der oben gegebenen expliziten Beschreibung von μ_n folgt sofort, dass für $\omega_1 := e^{\frac{2\pi \mathrm{i}}{n}}$ gilt $\mu_n = \{\omega_1^k \mid k \in \mathbb{Z}\}$. Im Folgenden schreiben wir $\omega_k := \omega_1^k$ für $k \in \mathbb{Z}$.

b) Angenommen $\dim(V) = n$ und sei zur Motivation des Arguments vorausgesetzt, dass T diagonalisierbar ist – was zu zeigen ist –, dann existieren $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ und eine Basis $\mathcal{B}$ von V, sodass

$$[T]_{\mathcal{B}} = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}.$$

Aus $T^N = \mathrm{id}_V$ folgt

$$I_n = [\mathrm{id}_V]_{\mathcal{B}} = [T^N]_{\mathcal{B}} = \big([T]_{\mathcal{B}}\big)^N = \begin{pmatrix} \lambda_1^N & & \\ & \ddots & \\ & & \lambda_n^N \end{pmatrix}.$$

Also wären die Eigenwerte von T allesamt enthalten in μ_N. Diese Einsicht und die Beweismethode im Falle einer Involution verwenden wir nun, um V als direkte Summe von Eigenräumen von T zu schreiben, was nach dem in der Vorlesung gezeigten impliziert, dass T diagonalisierbar ist.

Für $k \in \mathbb{Z}$ sei $E_k := \{v \in V \mid T(v) = \omega_k v\}$, wobei $\omega_1 := e^{\frac{2\pi \mathrm{i}}{N}}$ und $\omega_k := \omega_1^k$ wie oben. Wir behaupten, dass $V = \bigoplus_{k=0}^{N-1} E_k$, und nach besagtem Theorem wären wir dann fertig. Wir wissen bereits, dass die Summe $\sum_{k=0}^{N-1} E_k$ eine direkte Summe ist. Somit brauchen wir nur zu zeigen, dass sich ein beliebiges $v \in V$ als Summe von Elementen in E_k schreiben lässt. Gegeben $v \in V$ definiere

$$v_k := v + \omega_k T(v) + \cdots + \omega_k^{N-1} T^{N-1}(v) = \sum_{l=0}^{N-1} \omega_k^l T^l(v).$$

Zuerst bemerken wir, dass

$$T(v_k) = \sum_{l=0}^{N-1} \omega_k^l T^{l+1}(v) = \omega_k^{-1} \sum_{l=0}^{N-1} \omega_k^{l+1} T^{l+1}(v) = \omega_k^{-1} \sum_{l=0}^{N-1} \omega_k^l T^l(v),$$

da $\omega_k^N = 1$ und $T^N(v)$ nach Voraussetzung. Insbesondere ist also $v_k \in E_{N-k}$. Andererseits gilt

$$\sum_{k=0}^{N-1} v_k = \sum_{l=0}^{N-1} \left(\sum_{k=0}^{N-1} \omega_k^l \right) T^l(v) = Nv,$$

Bitte wenden!

denn für $l = 0$ ist $\sum_{k=0}^{N-1} \omega_k^l = N$ und andernfalls gilt unter Verwendung der Formel für geometrische Summen und der Tatsache, dass $\omega_l \in \mu_N$

$$\sum_{k=0}^{N-1} \omega_k^l = \sum_{k=0}^{N-1} \omega_l^k = \frac{\omega_l^N - 1}{\omega_l - 1} = 0.$$

Insbesondere ist also $v = \sum_{k=0}^{N-1} \frac{1}{N} v_k \in \sum_{k=1}^{N} E_k = \sum_{k=0}^{N-1} E_k$ und da v beliebig war, folgt die Behauptung.

6. **a)** Sei $A = \varphi(e) \in \mathrm{Gl}_N(\mathbb{C})$, dann ist nach Voraussetzung

$$A = \varphi(e) = \varphi(e)\varphi(e) = A^2.$$

Insbesondere ist also $I_N = A^{-1}A = A^{-1}A^2 = A$.

Sei $A = \varphi(g)$ und $B = \varphi(g^{-1})$, dann gilt

$$I_N = \varphi(e) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}) = AB$$

und folglich ist $B = A^{-1}$.

b) Seien $a, b \in \mathbb{F}_p^\times$ mit $a \sim b$, dann ist $a^2 = b^2$ bzw. $1 = a^2(b^2)^{-1} = (ab^{-1})^{-2}$. Insbesondere ist also ab^{-1} eine Nullstelle des Polynoms $X^2 - 1$ (mit den beiden Nullstellen ± 1) und somit ist $a = \pm b$. Da p ungerade ist, gilt für alle $a \in \mathbb{F}_p^\times$, dass $a \neq -a$. Andernfalls wäre $0 = a + (-a) = 2a$, aber da 2 und p koprim sind, ist $2 \in \mathbb{F}_p^\times$ und somit $2a \in \mathbb{F}_p^\times$ für alle $a \in \mathbb{F}_p^\times$. Das ist absurd. Also folgt $a \sim b$ genau dann, wenn $b = \pm a$ und somit ist für jedes $a \in \mathbb{F}_p^\times$ die Äquivalenzklasse $\varphi^{-1}(a^2) = [a] = \{a, -a\}$ eine Menge mit genau zwei Elementen.

Man berechnet nun

$$\mathbb{F}_p^\times = \varphi^{-1}\left(\mathbb{F}_q^\times\right) = \bigsqcup_{x \in \mathrm{sq}(\mathbb{F}_p^\times)} \varphi^{-1}(x),$$

und folglich

$$\mathbb{F}_p^\times = \sum_{x \in \mathrm{sq}(\mathbb{F}_p^\times)} |\varphi^{-1}(x)| = 2|\mathrm{sq}(\mathbb{F}_p^\times)|.$$

Es folgt:

$$|\{x \in \mathbb{F}_p^\times \mid \exists a \in \mathbb{F}_p^\times : x = a^2\}| = |\mathrm{sq}(\mathbb{F}_p^\times)| = \frac{|\mathbb{F}_p^\times|}{2} = \frac{p-1}{2}.$$

c) Es ist klar, dass $I_2 \in U \cap N$, so dass das neutrale Element in beiden enthalten ist. Man berechnet $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & a+b \\ 0 & 1 \end{smallmatrix}\right) \in U$ und $\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ b & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ a+b & 1 \end{smallmatrix}\right) \in N$.

Siehe nächstes Blatt!

Daraus folgt einerseits, dass U und N unter Matrixmultiplikation abgeschlossen sind, und dass $\left(\begin{smallmatrix}1 & a\\ 0 & 1\end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix}1 & -a\\ 0 & 1\end{smallmatrix}\right)$ sowie $\left(\begin{smallmatrix}1 & 0\\ a & 1\end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix}1 & 0\\ -a & 1\end{smallmatrix}\right)$. Also sind U und N auch abgeschlossen unter Inversion und somit sind U und N versehen mit der Matrixmultiplikation Gruppen. Aus der Rechnung folgt ebenfalls, dass U und N zyklisch sind mit Erzeugern $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ bzw. $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$.

Sei $g = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$. Da $\det(g) \neq 0$, wissen wir, dass $a \neq 0$ oder $c \neq 0$. Beachte, dass $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) = \left(\begin{smallmatrix}a & b\\ a+c & b+dd\end{smallmatrix}\right)$. Es reicht also, die Behauptung unter der Annahme $c \neq 0$ zu zeigen. Da $c \neq 0$, existiert ein $t \in \mathbb{F}_p^\times$, sodass $a + tc = 1$, und somit ist

$$\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}1 & b+td\\ c & d\end{pmatrix}.$$

Nun folgt wegen $1 = d - (b + td)c$, dass

$$\begin{pmatrix}1 & 0\\ c & 1\end{pmatrix}\begin{pmatrix}1 & b+td\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & b+td\\ c & c(b+td)+1\end{pmatrix} = \begin{pmatrix}1 & b+td\\ c & d\end{pmatrix}$$

Also gilt unter Verwendung von $\left(\begin{smallmatrix}1 & t\\ 0 & 1\end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix}1 & -t\\ 0 & 1\end{smallmatrix}\right)$, dass

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}1 & -t\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ c & 1\end{pmatrix}\begin{pmatrix}1 & b+td\\ 0 & 1\end{pmatrix}$$

und wegen $I_2 \in N$ haben wir also gezeigt, dass $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) = n_2u_2n_1u_1$ mit $u_1, u_2 \in U$ und $n_2, n_1 \in N$. Falls $c = 0$, dann wissen wir, dass $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) = n_2u_2n_1u_1$ mit $u_1, u_2 \in U$ und $n_2, n_1 \in N$. Da N eine Gruppe ist, ist also

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}^{-1} n_2u_2n_1u_1 = n_3u_2n_1u_1,$$

für ein $n_3 \in N$.

d) Wir haben in der Berechnung in c) gesehen, dass für $k \in \mathbb{Z}$ und $\overline{k}$ die Äquivalenzklasse von $k \mod p$ gilt

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^k = \begin{pmatrix}1 & \overline{k}\\ 0 & 1\end{pmatrix}.$$

(Dies verlangt streng genommen einen Induktionsbeweis: Für $k = 1$ ist die Aussage sicherlich wahr und der Induktionsschritt folgt aus der Berechnung mit $a = \overline{k}$ und $b = 1$.) Das analoge resultat gilt für $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$, was es uns erlaubt, für $a \in \mathbb{F}_p$ die Matrizen $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)^a$ und $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)^a$ zu definieren, indem wir a im Exponenten einfach mit einem Repräsentanten von a in $\mathbb{Z}$ identifizieren. Da sich zwei verschiedene Repräsentanten nur um ein Vielfaches von p unterscheiden und da $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)^p = \left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)^p = I_2$ gilt, ist die resultierende Matrix unabhängig von

Bitte wenden!

der Wahl des Repräsentanten von a. Ähnlich definieren wir ω^a für $a \in \mathbb{F}_p^\times$ und $\omega \in \mu_p = \{e^{2\pi \mathrm{i} \frac{k}{p}} \mid k \in \mathbb{Z}\}$.

Im Folgenden seien $u := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ und $n := \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Falls $\varphi(u) = \varphi(n) = I_N$, dann gelten

$$\varphi \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \varphi(u^a) = \varphi(u)^a = I_N$$
$$\varphi \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} = \varphi(u^a) = \varphi(u)^a = I_N$$

für alle $a \in \mathbb{F}_p$ und folglich ist $\varphi\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) = \varphi\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right) = I_N$ für alle $a \in \mathbb{F}_p$ und somit φ trivial, wegen a) und c).

Wir haben in der vorangehenden Aufgabe gezeigt, dass $\varphi(u)$ und $\varphi(n)$ beide diagonalisierbar sind über $\mathbb{C}$. Wenn beide nur Eigenwert 1 hätten, dann wären beide ähnlich zur Identität, und somit $\varphi(u) = \varphi(n) = I_N$ – da die Menge der zu I_N ähnlichen Matrizen nur I_N enthält –, was wiederum impliziert, dass φ trivial ist, im Widerspruch zur Voraussetzung.

Sei also $g \in \{u, n\}$, so dass $\varphi(g)$ einen nicht-trivalen Eigenwert besitzt. Sei ω eine nicht-triviale Einheitswurzel, so dass ω ein Eigenwert von $\varphi(g)$ ist. Wir berechnen für α wie im Hinweis:

$$\alpha^{-1} u \alpha = \begin{pmatrix} 1 & a^2 \\ 0 & 1 \end{pmatrix}$$
$$\alpha^{-1} n \alpha = \begin{pmatrix} 1 & 0 \\ (-a)^2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a^2 & 1 \end{pmatrix}.$$

Wenn also $v \in \mathbb{C}^N$ ein Eigenvektor von $\varphi(g)$ zum Eigenwert ω, dann ist also

$$\varphi(\alpha^{-1} g \alpha) v = \varphi(g^{a^2}) v = \varphi(g)^{a^2} v = \omega^{a^2} v$$

und folglich

$$\varphi(g)\big(\varphi(\alpha) v\big) = \omega^{a^2} \varphi(\alpha) v.$$

Es folgt, dass $\varphi(g)$ einen Eigenvektor zu ω^{a^2} besitzt für jedes $a \in \mathbb{F}_p^\times$. Da $g^p = I_2$, folgt $\omega^p = 1$ und folglich $\omega \in \mu_p$. Daraus folgt für $k \in \mathbb{Z}$, dass $\omega^k = 1$ genau dann, wenn $p \mid k$. Somit ist $\omega^{a^2} = \omega^{b^2}$ genau dann, wenn $a^2 = b^2$, so dass wir mindestens Anzahl der Quadrate in $\mathbb{F}_p^\times$ Eigenvektoren von $\varphi(u)$ zu paarweise verschiedenen Eigenwerten erhalten. Da Eigenvektoren zu verschiedenen Eigenwerten linear unabhängig sind, folgt $N \geq \frac{p-1}{2}$ aus Teilaufgabe b).