Aufgabe 1 (5 Punkte)

Ist V ein Vektorraum über einem Körper K , $\varphi: V \rightarrow V$ K -linear und $U \subseteq V$ eine Teilmenge mit

1. $0 \notin U$
2. jedes $v \in U$ ist ein Eigenvektor von φ , und
3. zwei Elemente $v, v' \in U$ sind nur dann Eigenvektoren zum gleichen Eigenwert, wenn $v = v'$ gilt.

Zeigen Sie, dass U linear unabhängig ist.

Hinweis: Betrachten sie zunächst den Fall, dass U endlich ist, etwa per Induktion über $|U| \in \mathbb{N}$.

Lösungsskizze. Wir folgen dem Hinweis. Gilt $|U| = 0$, so ist $U = \emptyset$ und das ist per Definition linear unabhängig. Ist $|U| = n+1$, etwa $U = \{v_1, \dots, v_{n+1}\}$ mit $\varphi(v_i) = v_i \cdot \lambda_i$ für paarweise verschiedene $\lambda_i \in K$, so betrachte $r_1, \dots, r_{n+1} \in R$ mit

$$0 = \sum_{i=0}^{n+1} v_i \cdot r_i.$$

Zu zeigen ist $r_i = 0$ für alle $1 \leq i \leq n+1$; soweit ist das nur Definitionen ausschreiben. Wenden wir nun φ auf obige Gleichung an (was sonst könnten wir denn schon tun), so erhalten wir

$$0 = \varphi(0) = \varphi\left(\sum_{i=0}^{n+1} v_i \cdot r_i\right) = \sum_{i=0}^{n+1} \varphi(v_i) \cdot r_i = \sum_{i=0}^{n+1} v_i \cdot \lambda_i \cdot r_i.$$

Man muss nun beobachten, dass dies eine weitere Linearkombination der 0 ist, die man mit der ursprünglich gegebenen vergleichen kann: Multipliziert man nämlich die erste Gleichung mit λ_{n+1} und zieht die untere vom Ergebnis ab, erhält man

$$0 = \left(\sum_{i=0}^{n+1} v_i \cdot r_i\right) \cdot \lambda_{n+1} - \sum_{i=0}^{n+1} v_i \cdot \lambda_i \cdot r_i = \sum_{i=0}^{n+1} v_i \cdot (\lambda_{n+1} - \lambda_i) \cdot r_i = \sum_{i=0}^n v_i \cdot (\lambda_{n+1} - \lambda_i) \cdot r_i,$$

da der letzte Term in der mittleren Summe verschwindet. Aber $\{v_1, \dots, v_n\}$ erfüllt offensichtlich auch die Annahmen aus der Aufgabenstellung und ist daher per Induktionshypothese linear unabhängig, sodass

$$0 = (\lambda_{n+1} - \lambda_i) \cdot r_i$$

für alle $1 \leq i \leq n$ folgt. Aber da per Annahme $\lambda_i \neq \lambda_{n+1}$ für diese i folgt, da K als Körper nullteilerfrei ist, schon $r_i = 0$ für alle $1 \leq i \leq n$. Dann besagt aber die erste Gleichung einfach $0 = v_{n+1} \cdot r_{n+1}$ und damit $r_{n+1} = 0$ da v_{n+1} per Annahme. Das beendet also den Induktionsschritt, und damit das Argument für endliche U .

Für unendliches U erinnere ich daran, dass dann U linear unabhängig ist, genau dann, wenn alle seine endlichen Teilmengen das sind (in jeder Linearkombination tauchen ja per definitionem nur endlich viele nicht verschwindende Koeffizienten auf). Aber erfüllt U die Annahmen der Aufgabe, so auch jede Teilmenge von U (das haben wir oben ja schon für $\{v_1, \dots, v_n\} \subset \{v_1, \dots, v_{n+1}\}$ benutzt). Der schon bewiesene Fall endlicher Teilmengen impliziert also den allgemeinen. $\square$

Aufgabe 2 (5 Punkte)

Zeigen Sie, dass je zwei ähnliche quadratische Matrizen über einem Körper die selben Eigenwerte haben.

Lösungsskizze. Sei etwa $A' = B \cdot A \cdot B^{-1}$ für $A, A', B \in \text{Mat}(n, n, K)$ mit B invertierbar und $0 \neq v \in K^n$ ein Eigenwert von A zum Eigenwert λ . Dann ist $B \cdot v \neq 0$ da B invertierbar ist und

$$A' \cdot B \cdot v = B \cdot A \cdot B^{-1} \cdot B \cdot v = B \cdot A \cdot v = B \cdot \lambda \cdot v = \lambda \cdot B \cdot v$$

und damit λ ein Eigenwert von A' .

Wir haben also gezeigt, dass für $A \sim A'$, jeder Eigenwert von A auch einer von A' ist. Da Ähnlichkeit eine symmetrische Relation ist, folgt durch vertauschen von A und A' auch dass jeder Eigenwert von A' einer von A ist, und damit die Behauptung.

Der Beweis beschreibt natürlich auch den zu λ gehörigen Eigenraum: $\text{Eig}_\lambda(B \cdot A \cdot B^{-1})$ besteht aus dem Bild von $\text{Eig}_\lambda(A)$ unter $B \cdot -: K^n \rightarrow K^n$. $\square$

Aufgabe 3 (5 Punkte)

Entscheiden Sie, ob

$$\begin{pmatrix} 0 & 2 & 2 \\ 2 & -4 & -4 \\ -3 & 7 & 7 \end{pmatrix} \in \text{Mat}(3, 3, \mathbb{Q})$$

diagonalisierbar ist.

Lösungsskizze. Wir suchen zunächst die Eigenwerte. Laut Skript sind diese als genau diejenigen $\lambda \in \mathbb{Q}$ gegeben für die

$$\det \begin{pmatrix} \lambda & -2 & -2 \\ -2 & \lambda+4 & 4 \\ 3 & -7 & \lambda-7 \end{pmatrix} = 0.$$

Die linke Seite ist

$$\begin{aligned} & \lambda \cdot (\lambda + 4) \cdot (\lambda - 7) + (-2) \cdot 4 \cdot 3 + (-2) \cdot (-2) \cdot (-7) - (-2) \cdot (\lambda + 4) \cdot 3 - (-2) \cdot (-2) \cdot (\lambda - 7) - \lambda \cdot 4 \cdot (-7) \\ & = \lambda^3 - 3\lambda^2 - 28\lambda - 24 - 28 + 6\lambda + 24 - 4\lambda + 28 + 28\lambda = \lambda^3 - 3\lambda^2 + 2\lambda \end{aligned}$$

Scharfes Hinsehen zeigt, dass $\lambda = 0, 1, 2$ alles drei Nullstellen dieser polynomiellen Funktion sind, und damit Eigenwerte der Matrix. Wählen wir zu jedem der drei Werte einen nicht-trivialen Eigenvektor, etwa v_0, v_1, v_2 , so folgt aus der ersten Aufgabe, dass $\{v_1, v_2, v_3\}$ linear unabhängig ist und damit, weil $\dim_{\mathbb{Q}}(\mathbb{Q}^3) = 3$, eine Basis aus Eigenvektoren. Damit ist die Matrix diagonalisierbar und nach der zweiten Aufgabe ähnlich zu

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

□

Aufgabe 4 (5 Punkte)

- Zeigen Sie, dass für $p \in \mathbb{N}$ prim und $1 \leq k \leq p-1$ die Teilbarkeit $p \mid \binom{p}{k}$ gilt.
- Folgern Sie, dass für jeden Ring R mit $p \cdot 1 = 0 \in R$ (etwa R ein Körper der Charakteristik p), die Abbildung

$$\text{Frob}_p: R \longrightarrow R, \quad x \longmapsto x^p$$

ein Ringhomomorphismus ist; er heißt der *Frobenius-Endomorphismus* von R .

- Folgern Sie auch, dass für $R = \mathbb{Z}/p$ einfach $\text{Frob}_p = \text{id}$ gilt. Insbesondere ist die polynomielle Funktion

$$\mathbb{Z}/p \longrightarrow \mathbb{Z}/p, \quad t \longmapsto t^p - t$$

konstant mit Wert 0.

Zur Erinnerung: Es ist

$$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!} \in \mathbb{N}$$

die Anzahl der k -elementigen Teilmengen einer n -elementigen Menge und in jedem kommutativen Ring R gilt

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$$

für $x, y \in R$ und $n \in \mathbb{N}$ nach dem binomischen Lehrsatz aus der Analysis I.

Lösungsskizze. a) Nach Definition haben wir

$$(p-k)! \cdot k! \cdot \binom{p}{k} = p!$$

Sicherlich gilt $p \mid p!$. Aus dem Euklid'schen Lemma folgt dann, dass p einen der drei Faktoren auf der linken Seite teilen muss, und weiter gilt nach einer weiteren Anwendung vom Euklid'schen Lemma $p \mid i!$ genau dann, wenn $p \mid j$ für ein $1 \leq j \leq i$, was genau dann der Fall ist, wenn $p \leq i$. Das impliziert aber $p \nmid k!$ und $p \nmid (p-k)!$ aufgrund der Annahme $1 \leq k \leq p-1$. Es folgt also $p \mid \binom{p}{k}$ wie gewünscht.

b) Offenbar gelten $0^p = 0$, $1^p = 1$ und $(x \cdot y)^p = x^p \cdot y^p$ in jedem kommutativen Ring R . Es bleibt $(x+y)^p = x^p + y^p$ zu zeigen. Aber nach dem Hinweis gilt

$$(x+y)^p = \sum_{k=0}^p \binom{p}{k} x^k y^{p-k} = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k}$$

Aus a) wissen wir, dass für $1 \leq k \leq p$ ein $m_k \in \mathbb{N}$ existiert mit $\binom{p}{k} = p \cdot m_k$. Damit sehen wir in der Tat

$$(x+y)^p = x^p + y^p + p \cdot \left(\sum_{k=1}^{p-1} m_k x^k y^{p-k} \right) = x^p + y^p$$

falls $p=0$ in R gilt.

c) Offenbar gilt für $n \in \mathbb{Z}/p$ aufgrund von b)

$$n^p = \left(\sum_{i=1}^n 1 \right)^p = \sum_{i=1}^n 1^p = \sum_{i=1}^n 1 = n$$

was zu zeigen war.

Man beachte, dass die Behauptung äquivalent ist zu $p \mid n^p - n$ für alle $n \in \mathbb{N}$. Das kann man auch per Induktion über $n \in \mathbb{N}$ direkt aus a) folgern. $\square$