



Prof. Dr. Fabien Morel

Dr. Andrei Lavrenov, Oliver Hendrichs, Katharina Novikov

Wintersemester 2024/25

20. Mai 2025

Lineare Algebra II – Lösungsskizzen zu Übungsblatt 3

Aufgabe 1.

Sei K ein Körper, V ein endlich dimensionaler K -Vektorraum und $f: V \rightarrow V$ ein Endomorphismus, so dass $f^2 = -\text{Id}_V$.

1. Nehmen wir an, dass $\dim V$ ungerade ist. Beweisen Sie, dass es $\lambda \in K$ gibt, so dass $\lambda^2 = -1$.
2. Sei K ein Unterkörper von $\mathbb{R}$. Beweisen Sie, dass $\dim V$ gerade ist.
3. Sei $K = \mathbb{C}$. Beweisen Sie, dass f diagonalisierbar ist.

Hinweis: Benutzen Sie $1 = \frac{i}{2}(X - i) - \frac{i}{2}(X + i)$, um zu beweisen, dass jedes Element $v \in V$ eine Summe der Eigenvektoren von f ist, die zu i oder $-i$ gehören.

Lösung.

1. Sei $n := \dim V$ ungerade. Da $f^2 = -\text{Id}_V$, schließen wir, dass $\det(f^2) = \det(-\text{Id}_V)$. Aber $\det(-\text{Id}_V) = (-1)^n = -1$, weil n ungerade ist und $\det(f^2) = \det(f)^2$. Deshalb haben wir für $\lambda := \det(f)$, dass $\lambda^2 = -1$.
2. Wenn $\dim V$ ungerade ist, gibt es $\lambda \in K$, so dass $\lambda^2 = -1$. Aber $K \subseteq \mathbb{R}$ und über den reellen Zahlen ist diese Gleichung unlösbar. Der Widerspruch zeigt, dass $\dim V$ gerade sein muss.
3. Da $1 = \frac{i}{2}(X - i) - \frac{i}{2}(X + i)$, haben wir auch $\text{Id}_V = \frac{i}{2}(f - i \cdot \text{Id}_V) - \frac{i}{2}(f + i \cdot \text{Id}_V)$. Dann für jedes $v \in V$ bezeichnen wir mit $v_1 := \frac{i}{2}(f - i \cdot \text{Id}_V)(v)$ und $v_2 := -\frac{i}{2}(f + i \cdot \text{Id}_V)(v)$. Es ist klar, dass

$$(f + i \cdot \text{Id}_V)(v_1) = \frac{i}{2}(f + i \cdot \text{Id}_V)(f - i \cdot \text{Id}_V)(v) = \frac{i}{2}(f^2 + \text{Id}_V)(v) = 0.$$

Mit anderen Worten v_1 ist entweder 0 oder ein Eigenvektor von f zum Eigenwert $-i$. Ähnlich ist v_2 entweder 0 oder ein Eigenvektor von f zum Eigenwert i . Da v beliebig war, haben wir bewiesen, dass

$$V = \text{Ker}(f - i \cdot \text{Id}_V) \oplus \text{Ker}(f + i \cdot \text{Id}_V).$$

Dann nehmen wir eine beliebige Basis $b_1, \dots, b_s$ von $\text{Ker}(f - i \cdot \text{Id}_V)$ und eine beliebige Basis $b_{s+1}, \dots, b_n$ von $\text{Ker}(f + i \cdot \text{Id}_V)$. Wir schließen, dass $b_1, \dots, b_s, b_{s+1}, \dots, b_n$ eine Basis von V ist und f die darstellende Matrix $\text{diag}(i, \dots, i, -i, \dots, -i)$ in dieser Basis hat.

Aufgabe 2.

Sei K ein Körper, V ein endlich dimensionaler K -Vektorraum, $f: V \rightarrow V$ ein diagonalisierbarer Endomorphismus und $\lambda_1, \dots, \lambda_r$ alle Eigenwerte von f , so dass $\lambda_i = \lambda_j \Rightarrow i = j$. Berechnen Sie das minimale Polynom $\mu_f(X)$ von f .

Lösung.

Beweisen wir zuerst, dass alle Eigenwerte λ_j Nullstelle von $\mu_f(X)$ sind. Betrachten wir ein Eigenvektor $v \neq 0$, der zu λ_j gehört. Dann $0 = \mu_f(f)v = \mu_f(\lambda_j)v$. Das ist nur möglich, wenn $\mu_f(\lambda_j) = 0$.

Setzen wir $P(X) = \prod_{i=1}^r (X - \lambda_r)$. Wir zeigen, dass $\mu_f(X) = P(X)$.

Da f diagonalisierbar ist, gibt es eine Basis $b_1, \dots, b_n$ von V , die aus Eigenvektoren von f besteht. Sei b_k zum Eigenwert λ_j gehörend. Dann

$$P(f)b_k = \left(\prod_{i \neq j} (f - \lambda_i \cdot \text{Id}_V) \right) (f - \lambda_j \cdot \text{Id}_V)b_k = 0.$$

Da k beliebig war, haben wir $P(f) = 0$. Daraus schließen wir, dass $\mu_f(X) \mid P(X)$.

Aufgabe 3.

Sei $p \in \mathbb{N}$ eine Primzahl, K ein Körper und $a \in K \setminus K^p = K \setminus \{x^p \mid x \in K\}$. Beweisen Sie, dass $X^p - a$ irreduzibel in $K[X]$ ist.

Hinweis: Betrachten Sie einen Faktor $Q(X)$ von $X^p - a$ und $V := K[X]/Q(X)$.

Lösung.

Nehmen wir an, dass $X^p - a = Q(X) \cdot R(X)$, $1 \leq \deg Q(X) =: d < p$, und definieren wir $V := K[X]/Q(X)$. Sei $f: V \rightarrow V$ der Endomorphismus von V , der durch Multiplikation mit X induziert wird.

Da $Q(f) = 0$, haben wir auch $f^p - a \cdot \text{Id}_V = Q(f) \cdot R(f) = 0$, d.h., $f^p = a \cdot \text{Id}_V$. Dann $\det(f)^p = a^d$ (insbesondere, $\det(f) \neq 0$). Da p eine Primzahl ist, gibt es $u, v \in \mathbb{Z}$, so dass $up + vd = 1$. Dann

$$(a^u \cdot \det(f)^v)^p = a^{up} (\det(f)^p)^v = a^{up} (a^d)^v = a^{up+vd} = a.$$

Aber dann $a \in K^p$ und der Widerspruch zeigt, dass $X^p - a$ irreduzibel ist.

Aufgabe 4.

Sei $p \in \mathbb{N}$ eine Primzahl, L ein Unterkörper von $\mathbb{C}$ und $\sigma: L \rightarrow L$ ein nicht-trivialer Körperautomorphismus, so dass $\sigma^p = \text{Id}_L$. Sei

$$K := \{x \in L \mid \sigma(x) = x\},$$

und nehmen Sie an, dass $\zeta := e^{2\pi i/p} \in \mathbb{C}$ zu K gehört.

1. Beweisen Sie, dass K ein Unterkörper von L ist.
2. Betrachten Sie σ als K -Endomorphismus von L und beweisen Sie, dass jedes $x \in L$ eine Summe der Eigenvektoren von σ ist, die zu ζ^i , $i = 0, \dots, p-1$ gehören.
Hinweis: Benutzen Sie Polynome $P_j(X) := \prod_{i \neq j} (X - \zeta^i)$ und argumentieren Sie ähnlich wie in Aufgabe 1 (3).
3. Beweisen Sie, dass $\dim_K L = p$.
Hinweis: Beweisen Sie, dass es einen Eigenvektor $v \in L \setminus K$ gibt und betrachten Sie die Multiplikation mit v .
4. Beweisen Sie, dass es $a \in K$ gibt, so dass $L \cong K[X]/(X^p - a)$ als Körper.

Lösung.

1. Da σ ein Körperautomorphismus ist, gilt für $x, y \in K$

$$\sigma(x + y) = \sigma(x) + \sigma(y) = x + y \quad \text{und} \quad \sigma(x \cdot y) = \sigma(x) \cdot \sigma(y) = x \cdot y.$$

Ähnlich gilt $\sigma(-x) = -\sigma(x) = -x$ und $\sigma(x^{-1}) = \sigma(x)^{-1} = x^{-1}$, $\sigma(0) = 0$, $\sigma(1) = 1$. Somit ist K ein echter Unterkörper.

2. Betrachten wir das Ideal $I \trianglelefteq K[X]$, das durch die Polynome $P_j(X)$, $0 \leq j < p$ erzeugt wird. Da jedes Ideal von $K[X]$ ein Hauptideal ist, gibt es $G(X) \in K[X]$, so dass $I = (G(X))$. Da $G(X) \mid P_j(X)$, muss es ein Produkt aus Konstanten und linearen Faktoren $(X - \zeta^i)$ sein für $i \neq j$. Aber, da j beliebig war, schließen wir, dass $G(X)$ konstant ist. Mit anderen Worten: $I = R$ insbesondere $1 \in I$, d.h. $\exists Q_j(X)$, so dass

$$1 = \sum_{i=1}^{p-1} P_j(X) Q_j(X).$$

Dann gilt auch $\text{Id}_L = \sum_{i=1}^{p-1} P_j(\sigma) Q_j(\sigma)$. Sei $x \in L$ und setzen wir $x_j := P_j(\sigma) Q_j(\sigma)(x)$. Es ist klar, dass

$$(\sigma - \lambda_j \cdot \text{Id}_L)(x_j) = (\sigma - \lambda_j \cdot \text{Id}_L) P_j(\sigma) Q_j(\sigma)(x) = (\sigma^p - \text{Id}_L) Q_j(\sigma)(x) = 0,$$

d.h., x_j ist entweder 0 oder ein Eigenvektor von σ , der zu λ_j gehört.

3. Sei $L_i := \text{Ker}(\sigma - \zeta^i \cdot \text{Id}_L)$. Dann $L_0 = K$ und $\sum_{i=0}^{p-1} L_i = L$ nach Teilaufgabe 2.

Da σ nicht die Identität ist, gilt $K \neq L$. Nehmen wir $x \in L \setminus K$ und zerlegen wir $x = \sum x_i$ für $x_i \in L_i$. Da $x \notin K$, gibt es mindestens ein $v := x_j \neq 0$ für $j > 0$ in dieser Zerlegung.

Es ist aber klar, dass für $y \in L_i$ gilt $v \cdot y \in L_{i+j}$:

$$\sigma(v \cdot y) = \sigma(v) \sigma(y) = \zeta^j v \cdot \zeta^i y,$$

d.h., Multiplikation mit v induziert einen Homomorphismus von L_i nach L_{i+j} . Ähnlich Multiplikation mit v^{-1} induziert einen Homomorphismus von L_{i+j} nach L_i .

Wir haben bewiesen, dass $L_i \cong L_{i+j}$ als K -Vektorräume für jedes i , insbesondere

$$L_0 \cong L_j \cong L_{2j} \cong \dots$$

Da $1 \leq j \leq p-1$ invertierbar mod p ist, schließen wir dass $K = L_0 \cong L_1 \cong \dots \cong L_{p-1}$. Aber da L_i Eigenräume sind, die zu verschiedenen Eigenwerten gehören, ist die Summe $L = \sum_{i=0}^{p-1} L_i$ direkt, d.h., $L \cong K^{\oplus p}$.

4. Wir haben in Teilaufgabe 3 insbesondere bewiesen, dass $a := v^p \in L_0 = K$. Betrachten wir jetzt den Ringhomomorphismus $K[X] \rightarrow L$, der X auf v abbildet. Dieser induziert einen Ringhomomorphismus $\varphi: K[X]/(X^p - a) \rightarrow L$. Wir haben auch in Teilaufgabe 3 gesehen, dass $v^i \in L_{ij}$ erzeugt. Deshalb ist φ surjektiv. Aber φ ist auch ein K -Homomorphismus und $K[X]/(X^p - a)$ und L haben die gleiche K -dimension p . Es folgt, φ ist ein Isomorphismus.