Lineare Algebra II
Lösungsvorschläge zum Tutoriumsblatt 4

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 $\mathbb{K} \subseteq \mathbb{C}$.

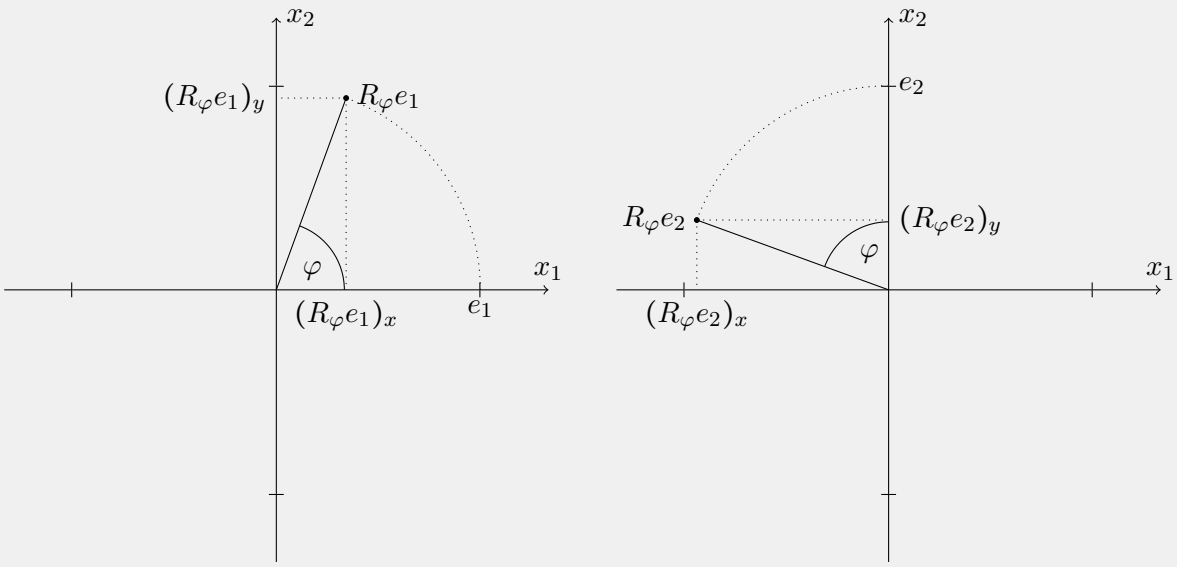
Aufgabe 1

Sei $V = \mathbb{R} \oplus \mathbb{R}$. Betrachte $R_\varphi : V \to V$, die Rotation um φ gegen den Uhrzeigersinn um den Ursprung.

1. Zeige, dass R_φ ein Homomorphismus ist. Bestimme die darstellende Matrix in der Standardbasis
2. Finde das Minimalpolynom von R_φ

Lösung:

1. Wir überlegen uns zuerst, wie eine Rotation aussieht. Dafür betrachten wir



Es ist ausreichend die Wirkung von R_φ auf Basisvektoren zu bestimmen. Wir sehen, dass die Rotation von e_1 um R_φ ein rechtwinkliges Dreieck erzeugt. Betrachten wir den Winkel φ, dann ist die x-Koordinate von $(R_\varphi e_1)$ die Ankathete des Winkels und die y-Koordinate bildet die Gegenkathete. Mithilfe von Sinus und Cosinus können wir also bestimmen (beachte, dass

$\mathsf{hyp} = 1$, da eine Drehung die Länge des Vektors unverändert lässt):

$$\cos(\varphi) = \frac{\mathsf{ank}(\varphi)}{\mathsf{hyp}} = \mathsf{ank}(\varphi) = (R_\varphi e_1)_x$$
$$\sin(\varphi) = \frac{\mathsf{geg}(\varphi)}{\mathsf{hyp}} = \mathsf{geg}(\varphi) = (R_\varphi e_1)_y$$

also gilt

$$R_\varphi \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos(\varphi) \\ \sin(\varphi) \end{pmatrix}$$

und analog bestimmen wir mithilfe des zweiten Bildes

$$R_\varphi \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin(\varphi) \\ \cos(\varphi) \end{pmatrix}$$

Insgesamt gilt also

$$R_\varphi \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a\cos(\varphi) - b\sin(\varphi) \\ a\sin(\varphi) + b\cos(\varphi) \end{pmatrix}$$

Man kann hier nun von Hand nachrechnen, dass die Abbildung $\mathbb{R}$-linear ist, oder man überlegt sich geometrisch, wieso das gelten muss.
Da R_φ linear ist, können wir eine darstellende Matrix aufschreiben. Die Spalten der darstellenden Matrix sind die Bilder der Basisvektoren, also gilt

$$A_\varphi = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}$$

2. Das Minimalpolynom μ_A ist das normierte Polynom kleinsten Grades, sodass $\mu_A(A_\varphi) = 0$. Das Minimalpolynom direkt zu bestimmen ist häufig schwer, also bestimmen wir zuerst das charakteristische Polynom, da dieses klar verwandt, aber direkt zu berechnen ist. Es gilt

$$\chi_A = \det(\lambda \mathbb{1}_2 - A_\varphi) = \lambda^2 - 2\lambda\cos(\varphi) + 1$$

wobei wir die Identität $\cos(\varphi)^2 + \sin(\varphi)^2 = 1$ verwendet haben. Mit der Mitternachtsformel erhalten wir

$$\begin{aligned} \lambda_{1,2} &= \frac{2\cos(\varphi) \pm \sqrt{4\cos(\varphi)^2 - 4}}{2} \\ &= \cos(\varphi) \pm \underbrace{\sqrt{\cos(\varphi)^2 - 1}}_{=\sqrt{-\sin(\varphi)} = i\sin(\varphi)} = \cos(\varphi) \pm i\sin(\varphi) \end{aligned}$$

also ist das charakteristische Polynom

$$\chi_A(\lambda) = (\lambda - (\cos(\varphi) + i\sin(\varphi)))(\lambda - (\cos(\varphi) - i\sin(\varphi)))$$

Das Minimalpolynom ist immer ein Teiler des charakteristischen Polynoms, da $\chi_A(A_\varphi) = 0$ gilt und gleichzeitig ist jede Nullstelle des charakteristischen Polynoms auch Nullstelle des Minimalpolynoms. Wir unterscheiden nun zwei Fälle:

(a) Gilt $\varphi = k\pi$ mit $k \in \mathbb{Z}$, dann ist $\sin(\varphi) = \sin(k\pi) = 0$ und damit gilt $\chi_A(\lambda) = (\lambda - \cos(\varphi))^2$. Das Minimalpolynom ist also entweder χ_A oder $(\lambda - \cos(\varphi))$ - setzen wir in letzteres Polynom A_φ ein, erhalten wir

$$(A_\varphi - \cos(\varphi)\mathbb{1}_2) = (\cos(\varphi)\mathbb{1}_2 - \cos(\varphi)\mathbb{1}_2) = 0$$

also gilt

$$\mu_A(\lambda) = (\lambda - \cos(\varphi))$$

da hier der Grad minimiert wird.

(b) Gilt $\varphi \neq k\pi$ für alle $k \in \mathbb{Z}$; dann gilt $\sin(\varphi) \neq 0$. In diesem Fall hat χ_A zwei verschiedene Nullstellen ersten Grades. Da jede Nullstelle von χ_A auch Nullstelle von μ_A sein muss, folgt daraus sofort

$$\mu_A = \chi_A$$

Aufgabe 2
Sei $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum mit $\dim(V) = n < \infty$ und $f : V \to V$ ein Homomorphismus. Seien $P, P_1, P_2 \in \mathbb{K}[X]$, sodass $P = P_1P_2$, P_1 und P_2 koprim und $P(f) = 0$. Wir betrachten die Zerlegung

$$V \simeq \underbrace{\ker(P_1(f))}_{=:U_1} \oplus \underbrace{\ker(P_2(f))}_{=:U_2}$$

1. Zeige $f(U_j) \subseteq U_j$
2. Seien $f_j := f\,|_{U_j} : U_j \to U_j$ mit Minimalpolynomen μ_j. Sei $Q \in \mathbb{K}[X]$, dann zeigen $Q(f)\,|_{U_j} = Q(f_j)$.
3. Zeige: $\mu_f(X) = \mathsf{kgV}(\mu_1, \mu_2)$

Lösung:
Wir überlegen uns vorher ein paar Sachen:
Ist $Q \in \mathbb{K}[X]$ und $g : V \to V$, was ist dann $Q(g)$? Wir erhalten die Abbildung $Q(g)$ indem wir das X in $Q(X)$ durch g ersetzen. Sei also

$$Q(X) = \alpha_k X^k + \ldots + \alpha_1 X + \alpha_0$$

dann ist

$$Q(g) = \alpha_k g^k + \ldots + \alpha_1 g + \alpha_0$$

wobei g^k hier als k-fache Komposition von g zu verstehen ist. Das heißt insgesamt erhalten wir eine Abbildung

$$\begin{aligned} Q(g) : V &\to V \\ v &\mapsto \alpha_k g^k(v) + \ldots + \alpha_1 g(v) + \alpha_0 v \end{aligned}$$

und da Summe, Komposition und skalares Vielfaches von Homomorphismen wieder ein Homomorphismus ist, ist $Q(g)$ ebenfalls ein Homomorphismus. Ein Beispiel:

Wir betrachten $V = \mathbb{R}$ und $g : V \to V$ wirkt als $v \mapsto 4v$. Weiter sei $Q(X) = X^3 + X - 1$. Dann gilt

$$Q(f) = f^3 + f - 1$$

und die Wirkung auf ein einzelnes Element ist

$$\begin{aligned} Q(f)(v) &= f^3(v) + f(v) - 1(v) \\ &= f^2(4v) + 4v - v \\ &= f(16v) + 4v - v \\ &= 64v + 4v - v = 67v \end{aligned}$$

Weiter können wir uns überlegen, was man aus $P(f) = 0$ direkt folgern kann. Die Naheliegende Vermutung, dass aus $P(f) = P_1P_2(f) = 0$ direkt folgt, dass $P_1(f) = 0$ oder $P_2(f) = 0$, ist jedoch falsch. In dieser Aufgabe wird gezeigt, wieso das falsch ist, bzw. wie die Situation tatsächlich aussieht. Als analoges[1] Beispiel überlegen wir uns folgendes:

Seien A_1, A_2 Ringe und sei $A := A_1 \times A_2$. Die Multiplikation von Elementen ist in diesem Fall komponentenweise definiert, das heißt für ein beliebiges $0 \neq a \in A_1, 0 \neq b \in A_2$ gilt

$$(a, 0) \cdot (0, b) = (0, 0)$$

Das Produkt ist also 0, aber weder $(a, 0)$ noch $(0, b)$ sind gleich 0. Das liegt daran, dass A kein Integritätsring ist.

In unserem Fall ist die Situation etwas anders. Wir werden aber zeigen, dass für jedes Element $v \in V$ entweder $P_1(f)(v) = 0$ oder $P_2(f)(v) = 0$ gilt - aber eben nicht notwendigerweise beides. Das heißt sowohl $P_1(f)$ als auch $P_2(f)$ sind nicht die Nullabbildung, aber ihr Produkt schon.

1. Es gilt zu zeigen, dass $f(U_j) \subseteq U_j$. Sei also $v \in U_j$, dann müssen wir zeigen, dass $f(v) \in U_j$ liegt. Da $v \in U_j$ gilt $P_j(f)(v) = 0$. Wir nehmen an, dass

   $$P_j(X) = \alpha_k X^k + \dots \alpha_1 X + \alpha_0$$

   dann gilt

   $$P_j(f) = \alpha_k f^k + \dots + \alpha_1 f + \alpha_0$$

   Setzen wir $f(v)$ ein erhalten wir

   $$\begin{aligned} P_j(f)(f(v)) &= \alpha_k f^k(f(v)) + \dots + \alpha_1 f(f(v)) + \alpha_0 f(v) \\ &= \alpha_k f(f^k(v)) + \dots + \alpha_1 f(f(v)) + \alpha_0 f(v) \\ &= f(\alpha_k f^k(v) + \dots + \alpha_1 f(v) + \alpha_0 v) \\ &= f(P_j(f)(v)) = 0 \end{aligned}$$

   wobei wir verwendet haben, dass f ein Homomorphismus und die Komposition von Abbildungen assoziativ ist.

   Das sagt uns nun folgendes: Sei $v \in V$, dann gibt es eindeutige $v_1 \in U_1$ und $v_2 \in U_2$, sodass $v = v_1 + v_2$. Wir haben gesehen, dass $f(v_j) \in U_j$ gilt. Da $P_2(f)$ eine Linearkombination aus

[1] Der Fokus liegt hier wirklich auf analog. Denn es ist natürlich nicht exakt die gleiche Situation.

Kompositionen von f ist, gilt auch $P_2(f)(v_1) \in U_1$. Lassen wir $P(f)$ auf v wirken, erhalten wir

$$\begin{aligned} P(f)(v) &= P_1(P_2(f))(v) \\ &= P_1(P_2(f)(v_1) + \underbrace{P_2(f)(v_2)}_{=0}) \\ &= P_1(\underbrace{P_2(f)(v_1)}_{\in U_1}) = 0 \end{aligned}$$

2. Sei $Q \in \mathbb{K}[X]$ beliebig mit Koeffizienten ρ_j. Wir wollen zeigen, dass $Q(f)$ als $Q(f)\mid_{U_1} + Q(f)\mid_{U_2} = Q(f_1) + Q(f_2)$ faktorisiert. Dazu überlegen wir uns folgendes: Da $V = U_1 \oplus U_2$ gilt, können wir eine Basis von V bilden, indem wir eine Basis von U_1 mit einer Basis von U_2 vereinigen. Sei also $v_1, \ldots, v_k$ eine Basis von U_1 und $w_1, \ldots, w_l$ eine Basis von U_2. Dann gilt für einen Vektor $v \in V$, dass mit geeigneten Koeffizienten:

$$v = \alpha_1 v_1 + \ldots + \alpha_k v_k + \beta_1 w_1 + \ldots \beta_l w_l$$

Es gilt außerdem

$$f(v_j) = \gamma_{1,j} v_1 + \gamma_{2,j} v_2 + \ldots + \gamma_{k,j} v_k$$

und die Koeffizienten für alle w_i sind 0, da laut erster Teilaufgabe $f(v_j) \in U_1$ gilt. Analog ist das Bild von w_j unter f wieder durch eine Linearkombination von w_i darstellbar, es gilt also

$$f(w_j) = \delta_{1,j} w_1 + \ldots + \delta_{l,j} w_l$$

Daraus folgt, dass $f_j : U_j \to U_j$ wohldefiniert ist (und wir nicht $f_j : U_j \to V$ schreiben müssen.) Nun können wir uns überlegen, wie die darstellende Matrix A_f in dieser Basis aussieht. Die Spalten der Matrix sind die Bilder der Basisvektoren, also können wir aus den beiden obigen Gleichungen direkt folgern, dass

$$A_f = \begin{pmatrix} \gamma_{1,1} & \gamma_{1,2} & \cdots & \gamma_{1,k} & 0 & 0 & 0 & 0 \\ \gamma_{2,1} & \gamma_{2,2} & \cdots & \gamma_{2,k} & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \gamma_{k,1} & \gamma_{k,1} & \cdots & \gamma_{k,k} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \delta_{1,1} & \delta_{1,2} & \cdots & \delta_{1,l} \\ 0 & 0 & 0 & 0 & \delta_{2,1} & \delta_{2,2} & \cdots & \delta_{2,l} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \delta_{l,1} & \delta_{l,2} & \cdots & \delta_{l,l} \end{pmatrix}$$

bzw, als Blockmatrix geschrieben

$$A_f = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

wobei A_j die darstellende Matrix von f_j in unserer Basis ist. Bei Blockmatrizen funktioniert die Multiplikation wie in normalen Matrizen, aber es werden nun Blöcke statt Zahlen

multipliziert. Das heißt also in Matrixschreibweise, dass

$$\begin{aligned}
Q(A_f) &= \rho_m A_f^m + \ldots \rho_1 A_f + \rho_0 \mathbb{1}_n \\
&= \rho_m \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}^m + \ldots + \rho_1 \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix} + \rho_0 \mathbb{1}_n \\
&= \rho_m \begin{pmatrix} A_1^m & 0 \\ 0 & A_2^m \end{pmatrix} + \ldots + \rho_1 \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix} + \rho_0 \mathbb{1}_n \\
&= \begin{pmatrix} \rho_m A_1^m + \rho_{m-1} A_1^{m-1} + \ldots + \rho_1 A_1 + \rho_0 \mathbb{1}_k & 0 \\ 0 & \rho_m A_2^m + \rho_{m-1} A_2^{m-1} + \ldots + \rho_1 A_2 + \rho_0 \mathbb{1}_l \end{pmatrix} \\
&= \begin{pmatrix} Q(A_1) & 0 \\ 0 & Q(A_2) \end{pmatrix}
\end{aligned}$$

Die Einschränkung $Q(f)\,|_{U_j}$ entspricht der Einschränkung von $Q(f)$ auf die Basisvektoren von U_j, also den ersten k bzw. letzten l Einträgen der Matrix $Q(A)$. Wie wir gesehen haben, sind das aber genau $Q(A_1)$, bzw. $Q(A_2)$, also gilt die zu zeigende Aussage.

3. Um zu zeigen, dass das Minimalpolynom das kleinste gemeinsame Vielfache ist, verwenden wir folgende Definition des kleinsten gemeinsamen Vielfachen: Für $a, b, v \in R$ in einem beliebigen Ring R gilt, dass

$$v = \mathsf{kgV}(a, b) \Leftrightarrow a|v, b|v \wedge \forall e \in R : (a|e \wedge b|e) \Rightarrow v|e$$

wir müssen also zeigen, dass μ_f genau diese beiden Eigenschaften erfüllt.

   (a) Wir zeigen $\mu_j|\mu_f$: Es gilt, dass $\mu_f(f_j) = \mu_f(f|_{U_j}) = 0$ - da $\mu_f(f) = 0$, gilt das natürlich auch für die Einschränkung $f|_{U_j}$. Da μ_j jeweils das Polynom kleinsten Grades ist, sodass $\mu_j(f_j) = 0$ gilt, folgt daraus $\mu_j \mid \mu_f$.

   (b) Wir zeigen, dass μ_f ein Teiler jedes gemeinsamen Vielfachen von μ_1, μ_2 sein muss. Dafür sei $Q \in \mathbb{K}[X]$ gegeben, sodass $\mu_1|Q$ und $\mu_2|Q$. Insbesondere ist also jede Nullstelle von μ_1 und μ_2 auch eine Nullstelle von Q. Das heißt aber, dass $Q(f_1) = Q(f_2) = 0$ gelten muss. Wir hatten oben gesehen, dass $Q(f|_{U_j}) = Q(f_j)$ gilt, also gilt

$$Q(f) = Q(f|_{U_1} + f|_{U_2}) = Q(f|_{U_1}) + Q(f|_{U_2}) = Q(f_1) + Q(f_2) = 0$$

   wobei wir verwendet haben, dass $Q(f)$ ein Homomorphismus ist. Da $Q(f) = 0$, gilt auch $\mu_f|Q$, also gilt die zweite Eigenschaft.

μ_f erfüllt die beiden charakterisierenden Eigenschaften des kleinstem gemeinsamen Vielfachen von μ_1, μ_2, also sind wir fertig.

Aufgabe 3

Sei $\mathbb{K}$ ein Körper, V ein n-dimensionaler $\mathbb{K}$-Vektorraum. Sei $f : V \to V$ ein Homomorphismus. Sei $\chi_f := \prod_{j=1}^{r} (X - \lambda_j)^{n_j}$, wobei die λ_j paarweise verschieden sind. Wir definieren $V_j := \ker(f - \lambda_j \mathbb{1}_V)^{n_j}$ und $f_j := f|_{V_j} : V_j \to V_j$. Zeige, dass $\chi_{f_j} = (x - \lambda_j)^{n_j}$ gilt.

Lösung:

Wir sind hier in einer ähnlichen Situation wie in Aufgabe 2.1. Nennen wir $P_j = (X - \lambda_j)^{n_j}$, dann gilt $\chi_f = P_1 \cdot \ldots \cdot P_r$ und alle P_j sind paarweise koprim. Außerdem gilt $V_j = \ker(P_j(f))$. Da die Polynome koprim sind, gilt

$$V = \bigoplus_{j=1}^{r} V_j$$

Weiter gilt für ein $v \in V_j$, dass

$$P_j(f)(f(v)) = (f - \lambda_j)^{n_j}(f(v)) = f\left((f - \lambda_j)^{n_j}(v)\right) = 0$$

also $f(V_j) \subseteq V_j$, insofern sind die $f_j : V_j \to V_j$ wieder wohldefiniert. Es gilt weiter

$$P_j(f_j) = (f_j - \lambda_j \mathbb{1}_V)^{n_j} = (f - \lambda_j \mathbb{1}_V)^{n_j}|_{V_j}$$

Sei $v = \sum_{j=1}^{r} v_j$ mit $v_j \in V_j \forall j \in [r]$, dann gilt:

$$P_j(f_j)(v) = (f_j - \lambda_j \mathbb{1}_V)^{n_j}(v) = (f - \lambda_j \mathbb{1}_V)^{n_j}|_{V_j}(v) = (f - \lambda_j \mathbb{1}_V)^{n_j}(v_j) = 0$$

da $V_j = \ker(f - \lambda_j \mathbb{1}_V)^{n_j}$ und $v_j \in V_j$. Da $P_j(f_j) = 0$ gilt, folgt also, dass $\mu_j | P_j$ - da $P_j = (X - \lambda_j)^{n_j}$ gilt, folgt daraus für ein $m_j \leq n_j$, dass

$$\mu_j = (X - \lambda_j)^{m_j}$$

Auf der anderen Seite können wir das charakteristische Polynom betrachten. Dieses enthält alle irreduziblen Faktoren von μ_j und ist ein Vielfaches von μ_j, also gilt $\chi_j = (X - \lambda_j)^{s_j}$ für ein $s_j \geq m_j$. Gleichzeitig gilt aber auch, dass $\dim(V_j) = \deg(\chi_j)$ gilt, da das charakteristische Polynom eines Homomorphismus $\mathbb{K}^l \to \mathbb{K}^l$ immer Grad l hat. Daraus folgt, dass $s_j = n_j$ gelten muss, also gilt

$$\chi_j = (X - \lambda_J)^{n_j}$$

Aufgabe 4
Sei $\mathbb{K}$ ein Körper und $P \in \mathbb{K}[X]$ irreduzibel. Sei $\mathbb{E} := \mathbb{K}[X]/P$. Zeige, dass $\mathbb{K} \subseteq \mathbb{E}$ ein Teilkörper ist. Zeige, dass P eine Nullstelle in $\mathbb{E}$ hat.

Lösung:
Wir verwenden folgenden Satz aus der Vorlesung:

Sei R ein euklidischer Ring und $f \in R$. Dann sind folgende Aussagen äquivalent:

1. f ist ein irreduzibles Element.
2. f ist ein Primelement.
3. Das von f erzeugte Ideal (f) ist ein Primideal.
4. Das von f erzeugte Ideal (f) ist ein maximales Ideal.
5. Der Faktorring $R/(f)$ ist ein Integritätsring.
6. Der Faktorring $R/(f)$ ist ein Körper.

Man kann sich hier noch merken, dass die Äquivalenzen

- (f) ist ein Primideal $\Leftrightarrow$ $R/(f)$ ist ein Integritätsring.

- (f) ist ein Maximales Ideal $\Leftrightarrow$ $R/(f)$ ist ein Körper.

in beliebigen Ringen gelten.
Die Aufgabenlösung:

Da P irreduzibel ist, ist $\mathbb{K}[X]/P$ ein Körper. Auf der anderen Seite hatten wir in einem früheren Blatt gezeigt, dass $\mathbb{K}[X]/P$ ein $\mathbb{K}$-Vektorraum mit Basis

$$\{\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}}\}$$

ist, wobei n der Grad von P sei. Die Abbildung

$$\begin{aligned} \varphi : \mathbb{K} &\to \mathbb{E} \\ a &\mapsto a\overline{1} \end{aligned}$$

ist ein Monomorphismus. Schränken wir die Operationen von $\mathbb{E} = \mathbb{K}[X]/P$ auf $\mathbb{K}$ ein, so erhalten wir genau die Operationen von $\mathbb{K}$ zurück, also ist $\mathbb{K}$ ein Unterkörper von $\mathbb{E}$.
Es sei $P = \alpha_n X^n + \ldots + \alpha_1 X + \alpha_0$ mit Koeffizienten in $\mathbb{K}$. Als nächstes betrachten wir P als Polynom mit Koeffizienten in $\mathbb{E}$, also $\hat{P} \in \mathbb{E}[Y]$. Es gilt dann also

$$\hat{P}(Y) = \alpha_n Y^n + \ldots + \alpha_1 Y + \alpha_0$$

wobei wir nun beliebige $v \in \mathbb{E}$ für Y einsetzen können. Setzen wir nun das Element $\overline{X}$ ein, erhalten wir

$$\hat{P}(\overline{X}) = \alpha_n \overline{X}^n + \ldots + \alpha_1 \overline{X} + \alpha_0$$

Da $\mathbb{E} \simeq \mathbb{K}[X]/P$ ist, gilt $\overline{X} \equiv X \mod P$, das heißt insgesamt also

$$\hat{P}(\overline{X}) \equiv \alpha_n X^n + \ldots + \alpha_1 X + \alpha_0 \mod P = 0 \mod P$$

also gilt $\hat{P}(\overline{X}) = 0$ in $\mathbb{E}$, das heißt $\overline{X}$ ist eine Nullstelle von $\hat{P}$ in $\mathbb{E}[Y]$. Da $\hat{P}$ aber genau P, nur mit einer größeren Variablenmenge ist, ist die zu zeigende Aussage gezeigt.