Aufgabe 1 (Herbst 2015)**.** Betrachten Sie das Polynom $f = x^2 + x + 1 \in \mathbb{F}_5[x]$.

(a) Zeigen Sie, daß $K = \mathbb{F}_5[x]/(f)$ ein Körper mit 25 Elementen ist. (2 Punkte)

(b) Bestimmen Sie ein Element $w \in K$ mit $w^2 = 2$. (3 Punkte)

(c) Zeigen Sie, daß die Matrix

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in \mathcal{M}_{2\times 2,\mathbb{F}_5}$$

über K diagonalisierbar ist. (3 Punkte)

Lösung. **Zu (a):** Das Polynom f ist irreduzibel über $\mathbb{F}_5$, denn es hat Grad 2 und keine Nullstelle in $\mathbb{F}_5$, da

$$\begin{aligned} f(0) &= 1, \\ f(1) &= 3, \\ f(2) &= 7 = 2, \\ f(3) &= 13 = 3, \\ f(4) &= 21 = 1. \end{aligned}$$

Es folgt, daß (f) ein Primideal in $\mathbb{F}_5[x]$ ist, und damit schon ein maximales Ideal, da $\mathbb{F}_5[x]$ als Polynomring über einem Körper ein Hauptidealring ist. Dies zeigt, daß der Quotientenring $K = \mathbb{F}_5[x]/(f)$ ein Körper ist. Für eine Nullstelle a von f in einem Zerfällungskörper ist

$$K \to \mathbb{F}_5(a), x + (f) \mapsto a$$

ein Isomorphismus und $[K : \mathbb{F}_5] = \deg(f)$. Also ist K ein $\mathbb{F}_5$-Vektorraum der Dimension 2, und hat 25 Elemente.

Zu (b): Sei $\alpha = x + (f)$ die Klasse von x in K. Es folgt aus dem in (a) angegebenen Isomorphismus, daß $(1, \alpha)$ eine $\mathbb{F}_5$-Vektorraumbasis von K ist. Das heißt jedes Element $w \in K$ lässt sich schreiben als $w = w_1 + w_2\alpha$ mit $w_1, w_2 \in \mathbb{F}_5$. Um ein Element mit $w^2 = 2$ zu finden gengüt es also w_1 und w_2 zu bestimmen.

$$\begin{aligned} & w^2 = 2 \quad \Leftrightarrow \quad (w_1 + w_2\alpha)^2 = 2 \quad \Leftrightarrow \quad w_1^2 + 2w_1w_2\alpha + w_2^2\alpha^2 = 2 \\ \Leftrightarrow \quad & w_1^2 + 2w_1w_2\alpha - w_2^2(\alpha + 1) = 2 \quad \Leftrightarrow \quad (w_1^2 - w_2^2) + (2w_1w_2 - w_2^2)\alpha = 2 \\ \Leftrightarrow \quad & (w_1^2 - w_2^2) = 2 \text{ und } 2w_1w_2 - w_2^2 = 0 \quad \Leftrightarrow \quad w_1^2 - w_2^2 = 2 \text{ und } w_2(2w_1 - w_2) = 0 \end{aligned}$$

Die zweite Gleichung liefert $w_2 = 0$ oder $w_2 = 2w_1$. Im ersten Fall wäre nach der ersten Gleichung $w_1^2 = 2$, doch 2 ist in $\mathbb{F}_5$ kein Quadrat. Also muß $w_2 = 2w_1$ gelten. Eingesetzt in die erste Gleichung ergibt sich

$$-3w_1^2 = w_1^2 - 4w_1^2 = 2$$

also $w_1^2 = 1$ in $\mathbb{F}_5$, das heißt $w_1 \in \{1, 4\}$. Für $w_1 = 1$ ist $w_2 = 2$ und für $w = w_1 + w_2\alpha = 1 + 2\alpha$ gilt tatsächlich

$$w^2 = (1 + 2\alpha)^2 = 1 + 4\alpha + 4\alpha^2 = 1 + 4\alpha - 4(1 + \alpha) = 1 - 4 = -3 = 2,$$

wie gewünscht.

Zu (c): Das charakteristische Polynom der Matrix A ist

$$\begin{aligned} \chi_A &= \det(xE_2 - A) \\ &= \det \begin{pmatrix} x - 1 & -2 \\ -3 & x - 4 \end{pmatrix} \\ &= (x - 1)(x_4) - (-2)(-3) \\ &= x^2 - 5x + 4 - 6 = x^2 - 2. \end{aligned}$$

Das Element w aus (b) ist eine Nullstelle von χ_A, die zweite Nullstelle ist gegeben durch $-w$, und da $2 \neq 0$ in $\mathbb{F}_5$, sind dies verschiedene Nullstellen. Die Matrix A hat also die beiden verschiedenen Eigenwerte $\pm w$ mit algebraischer Vielfachheit jeweils 1, die geometrische Vielfachheit muß jeweils auch (mindestens) 1 sein. Das charakteristische Polynom χ_A zerfällt über K also in Linearfaktoren und die Matrix ist über K diagonalisierbar.

Aufgabe 2 (Herbst 2014)**.** Sei $K \subset L$ eine Körpererweiterung, seien $\alpha, \beta \in L$ gegeben, so daß $\alpha + \beta$ und $\alpha\beta$ algebraisch über K sind. Man zeige, daß α und β algebraisch über K sind. (5 Punkte)

Lösung. Da $\alpha + \beta$ und $\alpha\beta$ algebraisch über K sind, ist $M = K[\alpha + \beta, \alpha\beta] = K(\alpha + \beta, \alpha\beta)$ endliche und damit algebraische Erweiterung von K. Betrachte das Polynom

$$f = (X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta \in M[X].$$

Es gilt $f(\alpha) = f(\beta) = 0$. Also sind α und β algebraisch über M. Also ist $M[\alpha, \beta] = M(\alpha, \beta)$ endliche und damit algebraische Erweiterung von M. Nach der Transitivität algebraischer Erweiterungen ist also auch $M[\alpha, \beta]/K$ algebraische Körpererweiterung. Also sind α und β algebraisch über K.

Aufgabe 3 (Herbst 2017)**.** Es seien K ein Teilkörper von $\mathbb{R}$ und $f \in K[X]$ ein Polynom. Weiter sei $Z \subset \mathbb{C}$ ein Zerfällungskörper von f über K. Der Grad $[Z : K]$ sei ungerade. Zeigen Sie, daß dann auch Z ein Teilkörper von $\mathbb{R}$ ist. (6 Punkte)

Lösung. Da $\mathbb{C}$ algebraisch abgeschlossen ist, zwerfällt f über $\mathbb{C}$ in Linearfaktoren. Seien $\{a_1, \ldots, a_n\}$ die komplexen Nullstellen von f. Da Z Zefällungskörper von f ist, gilt nach Definition

$$Z = K(a_1, \ldots, a_n).$$

Wir führen einen Widerspruchsbeweis. Angenommen $Z \not\subseteq \mathbb{R}$. Dann muß die Nullstellenmenge ein nichtreelles Element a enthalten. Sei $\overline{a} \neq a$ das komplex Konjugierte.
Wir bemerken zunächst, daß $\overline{a}$ ebenfalls eine Nullstele von f sein muß also $\overline{a} \in \{a_1, \ldots, a_n\}$: das Minimalpolynom von a über $\mathbb{R}$ ist $(x-a)(x-\overline{a}) = x^2 - (a+\overline{a})x + a\overline{a}$ (denn $a + \overline{a} = 2\Re(a) \in \mathbb{R}$ und $a\overline{a} = |a|^2 \in \mathbb{R}$) und es muß f teilen.

Die Idee ist nun, mit Hilfe dieses Elements eine Zwischenerweiterung zwischen Z und K zu konstruieren, die Grad 2 hat. Setze $M = K(a, \overline{a})$ und $M_0 = M \cap \mathbb{R}$. Wir berechnen den Grad der Erweiterung $M_0 \subset M_0(a)$. Da

$$a + \overline{a} = 2\Re(a) \in M \cap \mathbb{R} = M_0$$
$$a\overline{a} = |a|^2 \in M \cap \mathbb{R} = M_0$$

ist das Polynom $x^2 - (a + \overline{a})x + a\overline{a} \in M_0[x]$. Seine Nullstellen sind wie oben gesehen a und $\overline{a}$. Es ist irreduzibel, denn sonst wäre $a \in \mathbb{R}$, ein Widerspruch zu Annahme. Also ist dies auch das Minimalpolynom von a über M_0, $M_0(a)$ ist sein Zerfällungskörper und es gilt

$$[M_0(a) : M_0] = \deg(x^2 - (a + \overline{a})x + a\overline{a}) = 2.$$

Da $a, \overline{a} \in \{a_1, \ldots, a_n\}$ Nullstellen von f sind, ist $K \subset M = K(a, \overline{a}) \subset Z$ ein Zwischenkörper. Da $K \subset \mathbb{R}$ gilt dies auch für $M_0 = M \cap \mathbb{R}$, und da $a \in Z$ haben wir insgesamt

$$K \subset M_0 \subset M_0(a) \subset Z.$$

Nun gilt mit der Gradformel (zweimal angewendet)

$$\begin{aligned}[Z : K] &= [Z : M_0] \cdot [M_0 : K] \\ &= [Z : M_0(a)] \cdot [M_0(a) : M_0] \cdot [M_0 : K] \\ &= [Z : M_0(a)] \cdot 2 \cdot [M_0 : K].\end{aligned}$$

Somit wäre der $[Z : K]$ gerade, ein Widerspruch zur Annahme.

Zusatzaufgabe (Herbst 1987)**.** Man entscheide, ob die folgenden Aussagen richtig oder falsch sind , und gebe eine kurze Begründung.

(a) Der Körper $\mathbb{Q}$ der rationalen Zahlen besitzt echte Teilkörper. (2 Punkte)

(b) Jedes nicht konstante irreduzible Polynom über $\mathbb{Q}$ hat nur einfache Nullstellen. (2 Punkte)

(c) Ist $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom mit den Nullstellen $\alpha, \beta \in \mathbb{C}$, so gilt $\beta \in \mathbb{Q}(\alpha)$. (2 Punkte)

(d) Das direkte Produkt $\mathbb{R} \times \mathbb{R}$ des Körpers $\mathbb{R}$ mit sich selbst ist ein zu $\mathbb{C}$ isomorpher Körper. (2 Punkte)

Lösung. **Zu (a):** Falsch.
Jeder Teilkörper $F \subset \mathbb{Q}$ enthält 0 und 1. Da F additiv abgeschlossen ist, enthält F dann die ganzen Zahlen $\mathbb{Z}$. Da jedes Element in $x \in F\backslash 0$ invertierbar ist, gilt $\frac{1}{x} \in F$, also $\{\frac{1}{n} \mid n \in \mathbb{N}\} \subset F$. Da F multiplikativ abgeschlossen ist, folgt $m \cdot \frac{1}{n} = \frac{m}{n} \in F$ für alle $m \in \mathbb{Z}$, $n \in \mathbb{N}$. Also $\mathbb{Q} \subset F$ und damit folgt Gleichheit.

Zu (b): Richtig.
Der Körper $\mathbb{Q}$ hat Charakteristik 0 und solche Körper sind vollkommen, das heißt jedes irreduzible nicht konstante Polynom ist separabel, in anderen Worten, es hat (in jedem Zerfällungskörper) nur einfache Nullstellen.

Zu (c): 2 mägliche Interpretationen der Fragestellung: Nimmt man an, daß die Anzahl der Nullstellen umspezifiziert ist, so ist die Aussage im Allgemeinen falsch:
Gegenbeispiel: das Polynom $f = X^3 - 2 \in \mathbb{Q}[X]$ ist irreduzibel nach Eisenstein. Die komplexen Nullstellen sind

$$\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2},$$

wobei $\omega = e^{\frac{2\pi i}{3}} \in \mathbb{C} \setminus \mathbb{R}$ eine primitive dritte Einheitswurzel ist und $\sqrt[3]{2} \in \mathbb{R}$. Also gilt für $\alpha = \sqrt[3]{2}$ und $\beta = \omega\sqrt[3]{2}$, daß $\beta \notin \mathbb{Q}(\alpha) \subset \mathbb{R}$.
Nimmt man dagegen an, daß es genau zwei Nullstellen α und β gibt, also $\deg(f) = 2$, so ist die Aussage richtig, da $f = (X - \alpha)(X - \beta)$ in einem Oberkörper, und da f und $(X - \alpha) \in \mathbb{Q}(\alpha)[X]$, ist auch $(X - \beta) \in \mathbb{Q}(\alpha)[X]$, also $\beta \in \mathbb{Q}(\alpha)$.
Zu (d): Falsch.
Das direkte Produkt $\mathbb{R} \times \mathbb{R}$ (mit komponentenweiser Addition und Multiplikation) ist nicht einmal ein Integritätsbereich, denn es enthält zum Beispiel die Nullteiler

$$(0, 1) \cdot (1, 0) = (0 \cdot 1, 1 \cdot 0) = (0, 0).$$