

Übungsblatt 3 - Jovan Petrov - Übungsgruppe 3 - Kohlheim

Aufgabe 2

Zu bestimmen: Minimalpolynom von $z = \frac{1+i}{\sqrt{2}} \in \mathbb{C}$ über \mathbb{C} , \mathbb{R} und \mathbb{Q}

Da $z \in \mathbb{C}$ ist das Polynom $p(x) = \underline{x - z} \in \mathbb{C}[x]$ das Min-pol. von z über \mathbb{C} , da $p(z) = 0$ und $\text{grad } p = 1 \rightarrow$ irreduzibel.

Wir betrachten die Matrix $(z \cdot) = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$.

Nach Cayley-Hamilton hat $\text{charpol}_z(t) = \det((z \cdot) - t \cdot \text{Id})$

z als Nullstelle:

$$\begin{aligned} \text{charpol}_z(t) &= \det \begin{pmatrix} \frac{1}{\sqrt{2}} - t & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} - t \end{pmatrix} = \left(\frac{1}{\sqrt{2}} - t\right)^2 + \frac{1}{2} = \frac{1}{2} + t^2 - t\sqrt{2} + \frac{1}{2} \\ &= t^2 - t\sqrt{2} + 1 \end{aligned}$$

Für $q(x) = x^2 - x\sqrt{2} + 1 \in \mathbb{R}[x]$ gilt $q(z) = 0$, also ist das Min-pol. von z über \mathbb{R} $q(x)$. Wir beweisen, dass $q(x)$ irred. in \mathbb{R} und damit das Min-pol. von z über \mathbb{R} ist.

$$\Delta_q = (-\sqrt{2})^2 - 4 \cdot 1 \cdot 1 = 2 - 4 = -2 < 0.$$

Daher hat $q(x) \in \mathbb{R}[x]$ keine Nullstellen in \mathbb{R} ist wegen $\text{grad } q = 2$ also irreduzibel.

Dann ist folglich $q(x) = \underline{x^2 - x\sqrt{2} + 1} \in \mathbb{R}[x]$ das Min-pol. von z über \mathbb{R}

$$\text{Wir haben } z^2 - z\sqrt{2} + 1 = 0 \Leftrightarrow z^2 + 1 = z\sqrt{2} \Rightarrow (z^2 + 1)^2 - 2z^2 = 0$$

Daher ist $z \in \mathbb{C}$ Nullstelle des Polynoms

$$w(x) = (x^2 + 1)^2 - 2x^2 = x^4 + 2x^2 + 1 - 2x^2 = x^4 + 1 \in \mathbb{Q}[x]$$

Sei $w(x) = x^4 + 1$ in \mathbb{Z} reduzibel. Da $w(n) = n^4 + 1 > 1 > 0 \quad \forall n \in \mathbb{Z}$

hat w offensichtlich keine Nullstellen in \mathbb{Z} . Daher kann

w also nicht als ein Produkt zweier Polynome mit Grad

1 und 3 geschrieben werden, da $w(n)$ dann in \mathbb{Z} eine Nullstelle hätte.

$\Rightarrow w(x)$ kann als Produkt zweier Polynome in $\mathbb{Z}[x]$ mit Grad 2 geschrieben werden. Da $w(x) = 1 \cdot x^4 + 1$, sind die zwei Polynome der Form $x^2 + ax + 1$ und $x^2 + bx + 1$, $a, b \in \mathbb{Z}$

$$\begin{aligned} w(x) = x^4 + 1 &= (x^2 + ax + 1)(x^2 + bx + 1) \\ &= x^4 + bx^3 + x^2 + ax^3 + abx^2 + ax + x^2 + bx + 1 \\ &= x^4 + (a+b)x^3 + (2+ab)x^2 + (a+b)x + 1 \end{aligned}$$

$$\Rightarrow a+b = 2+ab = 0 \text{ für } a, b \in \mathbb{Z} \quad a+b=0 \Rightarrow b=-a$$

$$\Rightarrow 0 = 2+ab = 2-a^2 - \text{keine Lösung für } a \in \mathbb{Z} \text{ . Widerspruch!}$$

Daher ist $w(x) = x^4 + 1$ in $\mathbb{Z}[x]$ und damit auch nach Aufgabe 3 des letzten Blatts in $\mathbb{Q}[x]$ irreduzibel.

Daher ist also $w(x) = x^4 + 1$ das Min.pol von \mathbb{Z} über $\mathbb{Q}[x]$ (und $\mathbb{Z}[x]$).

Aufgabe 3

1. Seien p_1, \dots, p_n paarweise verschiedene Primzahlen.

$$[Q(\sqrt{p_1}, \dots, \sqrt{p_n}) : Q(\sqrt{p_1}, \dots, \sqrt{p_{n-1}})] = 2 \Rightarrow \sqrt{p_1}, \dots, \sqrt{p_n} \text{ lin. un.}$$

Beweis.

Es gelte $[Q(\sqrt{p_1}, \dots, \sqrt{p_n}) : Q(\sqrt{p_1}, \dots, \sqrt{p_{n-1}})] = 2$ für bel. verschiedene Primzahlen p_1, \dots, p_n , $n \in \mathbb{N}$ bel.

Seien q_1, \dots, q_n verschiedene Primzahlen, so dass $\sqrt{q_1}, \dots, \sqrt{q_n}$ über Q linear abhängig sind, d. h. es ex. $\lambda_1, \dots, \lambda_n \in Q$ nicht alle 0 mit $\sum_{i=1}^n \lambda_i \sqrt{q_i} = 0$. O.B.d.A. sei $\lambda_n \neq 0$.

$$\text{Dann gilt } \sqrt{q_n} = \sum_{i=1}^{n-1} \left(-\frac{\lambda_i}{\lambda_n} \sqrt{q_i} \right) \in Q(\sqrt{q_1}, \dots, \sqrt{q_{n-1}})$$

Da $Q(\sqrt{q_1}, \dots, \sqrt{q_n})$ der kleinste Körper ist, der

$Q, \sqrt{q_1}, \dots, \sqrt{q_n}$ enthält aber $\sqrt{q_n} \in Q(\sqrt{q_1}, \dots, \sqrt{q_{n-1}})$ gilt

$$Q(\sqrt{q_1}, \dots, \sqrt{q_n}) = Q(\sqrt{q_1}, \dots, \sqrt{q_{n-1}}) \Rightarrow [Q(\sqrt{q_1}, \dots, \sqrt{q_n}) : Q(\sqrt{q_1}, \dots, \sqrt{q_{n-1}})] = 1 \neq 2$$

Widerspruch!

2. $K \subset L$, $[L:K] = 2$, $(0 \neq \alpha \in L)$, $\exists x \in L \setminus K: x^2 \in K$. Dann gilt für $\beta \in L: \beta^2 \in K$ entweder $\beta \in K$ oder $\alpha\beta \in K$.

Beweis.

Da $\alpha \in L \setminus K$ und $0 \notin L \setminus K$ gilt also $\alpha \neq 0 \neq \alpha^2$.

Wir beweisen zunächst, dass α und α^2 linear unabhängig und somit eine Basis des K -Vektorraums L bilden.

$$\text{Seien } \lambda_1, \lambda_2 \in K, \text{ beide } \neq 0, \lambda_1 \alpha + \lambda_2 \alpha^2 \stackrel{\alpha^2 \in K}{=} 0 \Rightarrow \lambda_1 + \lambda_2 \alpha = 0 \Rightarrow \alpha = -\lambda_1 \lambda_2^{-1} \in K.$$

Widerspruch! Also bilden α und α^2 sind im K -VR L lin. unabh. und wegen $\dim_K L = 2$ eine Basis.

$$\text{Für } \beta \in L \text{ ex. } \lambda_1, \lambda_2 \in K \text{ mit } \beta = \lambda_1 \alpha + \lambda_2 \alpha^2$$

$$\Rightarrow \beta^2 = \lambda_1^2 \alpha^2 + \lambda_2^2 \alpha^4 + 2\lambda_1 \lambda_2 \alpha^3$$

Angenommen seien λ_1, λ_2 beide nicht 0.

Dann gilt da $B^2, \lambda_1^2, \kappa^2, \lambda_2^2 \kappa^4, \lambda_1, \lambda_2, 2 \in K$

$$\kappa^3 = 2^{-1} \lambda_1^{-1} \lambda_2^{-1} (B^2 - \lambda_1^2 \kappa^2 - \lambda_2^2 \kappa^4) \in K$$

$\kappa^2 \in K \wedge \kappa^2 \neq 0 \Rightarrow (\kappa^2)^{-1} \in K$, also ist $\kappa = \kappa^3 \cdot (\kappa^2)^{-1} \in K$. Widerspruch!

* Somit gilt hier $B \neq 0$ entweder $\lambda_1 = 0$ oder $\lambda_2 = 0$

Fall 1: $\lambda_1 = 0 \Rightarrow B = \lambda_2 \kappa^2 \stackrel{\lambda_2, \kappa^2 \in K}{\Rightarrow} \underline{B \in K}$

Angenommen gelte $\kappa B = \lambda_2 \kappa^3 \in K$. Da $\lambda_2 \neq 0, \lambda_2^{-1} \in K$: $\kappa^3 = \lambda_2^{-1} (\lambda_2 \kappa^3) \in K$

Widerspruch! Also gilt $\kappa B \notin K$

Fall 2: $\lambda_2 = 0 \Rightarrow B = \lambda_1 \kappa$. Angenommen sei $B = \lambda_1 \kappa \in K$. Da $\lambda_1 \neq 0, \lambda_1^{-1} \in K$

$\kappa = (\lambda_1 \kappa) \lambda_1^{-1} \in K$. Widerspruch! Also gilt $B \notin K$.

$$\kappa B = \lambda_1 \kappa^2 \stackrel{\lambda_1, \kappa^2 \in K}{\Rightarrow} \underline{\kappa B \in K}$$

* Für $B = 0 \in K \subset L$ gelten beide $B = 0 \in K, \kappa B = 0 \in K$. \square