Übungsblatt 3 - Jovan Petrov - Übungsgruppe 3 - Kohlhaas

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 $p(x) = x - z \in \mathbb{C}[x]$ das Min.pol. von z über $\mathbb{C}$, da $p(z) = 0$ und $\operatorname{grad} p = 1 \rightarrow$ 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 $\operatorname{charpol}_z(t) = \det((z \cdot) - t\,\mathrm{Id})$ z als Nullstelle:

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

$$= t^2 - t\sqrt{2} + 1$$

Für $q(x) = x^2 - x\sqrt{2} + 1 \in \mathbb{R}[x]$ gilt $q(z) = 0$, also teilt 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.

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

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

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

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 $w(n) = n^4 + 1 > 1 > 0 \ \forall n \in \mathbb{Z}$ 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 $w(x)$ dann in $\mathbb{Z}$ eine Nullstelle hätte.

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

$$m(x) = x^4 + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$$
$$= x^4 + bx^3 + x^2 + ax^3 + abx^2 + ax + x^2 + bx + 1$$
$$= x^4 + (a+b)x^3 + (2+ab)x^2 + (a+b)x + 1$$

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

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

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

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

Aufgabe 3

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

Beweis.

Es gelte $[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-1}})] = 2$ 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 $\mathbb{Q}$ linear abhängig sind, d. h. es ex. $\lambda_1, \dots, \lambda_n \in \mathbb{Q}$ nicht alle 0 mit $\sum_{i=1}^{n} \lambda_i \sqrt{q_i} = 0$. O.B.d.A. sei $\lambda_n \neq 0$.
Dann gilt $\sqrt{q_n} = \sum_{i=1}^{n-1} \left(-\frac{\lambda_i}{\lambda_n} \sqrt{q_i}\right) \in \mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_{n-1}})$
Da $\mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_n})$ der kleinste Körper ist, der $\mathbb{Q}, \sqrt{q_1}, \dots, \sqrt{q_n}$ enthält aber $\sqrt{q_n} \in \mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_{n-1}})$ gilt
$\mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_n}) = \mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_{n-1}}) \Rightarrow [\mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_n}) : \mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_{n-1}})] = 1 \neq 2$
Widerspruch!

2. $K \subset L$, $[L:K] = 2$, $(0 \neq z \in K)$, $\exists \alpha \in L \setminus K : \alpha^2 \in K$. 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 1 linear unabhängig und somit eine Basis des K-Vektorraums L bilden.
Seien $\lambda_1, \lambda_2 \in K$, beide $\neq 0$, $\lambda_1 \alpha + \lambda_2 \cdot 1 = 0 \Rightarrow \lambda_2 + \lambda_1 \alpha = 0 \Rightarrow \alpha = -\lambda_1 \lambda_2^{-1} \in K$.
Widerspruch! Also bilden α und 1 sind im K-VR L lin. unab. und wegen $\dim_K L = 2$ eine Basis. Besitze $b \in L$ eine Wurzel $\beta \in L$.
Für $\beta \in L$ ex. $\lambda_1, \lambda_2 \in K$ mit $\beta = \lambda_1 \alpha + \lambda_2$
$\Rightarrow \beta^2 = \lambda_1^2 \alpha^2 + \lambda_2^2 + 2\lambda_1\lambda_2\alpha$

Angenommen seien λ_1, λ_2 beide nicht 0.

Dann gilt da $\beta^2, \lambda_1^2, \alpha^2, \lambda_2^2, 2, \lambda_1, \lambda_2 \in K$, $2\lambda_1\lambda_2 \neq 0$

$$\alpha = 2^{-1}\lambda_1^{-1}\lambda_2^{-1}\left(\beta^2 - \lambda_1^2\alpha^2 - \lambda_2^2\right) \in K$$

Widerspruch!

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

Fall 1: $\lambda_1 = 0 \Rightarrow \beta = \lambda_2 \Rightarrow \underline{\beta \in K}$

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

Widerspruch! Also gilt $\underline{\alpha\beta \notin K}$

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

$\alpha = (\lambda_1\alpha)\lambda_1^{-1} \in K$. Widerspruch! Also gilt $\underline{\beta \notin K}$.

$$\alpha\beta = \lambda_1\alpha^2 \overset{\lambda_1, \alpha^2 \in K}{\Rightarrow} \underline{\alpha\beta \in K}$$

* Für $\beta = 0 \in K \subset L$ gelten beide $\beta = 0 \in K$, $\alpha\beta = 0 \in K$. □

3. $a \in \mathbb{Q}$. Dann gilt $\left(\exists \alpha \in \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \alpha^2 = a\right) \Leftrightarrow \left(a = c^2 \prod_{i \in I} p_i,\ c \in \mathbb{Q},\ I \subseteq \{1, \dots, n\}\right)$

Beweis

"$\Leftarrow$": Diese Richtung ist offensichtlich, da falls $a = c^2 \prod_{i \in I} p_i \in \mathbb{Q}$

Dann ist a Quadratzahl in $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ mit $a = \left(c \prod_{i \in I} \sqrt{p_i}\right)^2$,

$c \prod_{i \in I} \sqrt{p_i} \in \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$.

"$\Rightarrow$": Wir beweisen diese Richtung per Induktion:

(IA): $n = 1$: Sei p_1 bel. Primzahl und sei $a \in \mathbb{Q}$ Quadrat in $\mathbb{Q}(\sqrt{p_1})$.

Da $\{1, \sqrt{p_1}\}$ Basis des $\mathbb{Q}$-VRs $\mathbb{Q}(\sqrt{p_1})$ ist gilt $\exists \alpha = \lambda_1 + \lambda_2\sqrt{p_1}$, $\lambda_1, \lambda_2 \in \mathbb{Q}$

mit $\alpha^2 = a$. $a = \alpha^2 = \lambda_1^2 + \lambda_2^2 p_1 + 2\lambda_1\lambda_2\sqrt{p_1} \in \mathbb{Q}$. $\Rightarrow \lambda_1 = 0 \vee \lambda_2 = 0$.

* $\lambda_1 = 0 \Rightarrow \alpha = \lambda_2\sqrt{p_1} \Rightarrow a = \lambda_2^2 p_1 = c^2 \prod_{i \in I} p_i$ mit $c = \lambda_2$, $I = \{1\}$

* $\lambda_2 = 0 \Rightarrow \alpha = \lambda_1 \Rightarrow a = \lambda_1^2 = c^2 \prod_{i \in I} p_i$ mit $c = \lambda_1$, $I = \emptyset$.

(IS): Es gelte die Aussage für ein $n \in \mathbb{N}$:

Seien $p_1, \dots, p_{n+1}$ bel. verschiedene Primzahlen. Wir bezeichnen noch

$K_m = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_m})$ für $m \leq n+1$.

$p_{n+1} \in \mathbb{Q} \subset K_n$ ist ein Quadrat in der Körpererweiterung $K_{n+1} \supset K_n$, da $p_{n+1} = (\sqrt{p_{n+1}})^2$, $\sqrt{p_{n+1}} \in K_{n+1}$. Sei $a \in \mathbb{Q} \subset K_n$ ein bel. Quadrat in K_{n+1}. Nach Aufgabe 3.2 gilt also entweder ist also entweder a oder $a p_{n+1}$ ein Quadrat in $K_n \subset K_{n+1}$.

* Ist a ein Quadrat in K_n, gilt $a = c^2 \prod_{i \in I} p_i$ $I \subset \{1, \dots, n\} \subset \{1, \dots, n+1\}$, $c \in \mathbb{Q}$ nach der IV.

* Ist $a p_{n+1}$ ein Quadrat in K_n, ist $\frac{a}{p_{n+1}} = (a p_{n+1}) \left(\frac{1}{p_{n+1}}\right)^2 \in \mathbb{Q} \subset K_n$ auch Quadratzahl in K_n. $\frac{a}{p_{n+1}} = c^2 \prod_{i \in I} p_i$ $I \subset \{1, \dots, n\}$, $c \in \mathbb{Q}$,

$\Rightarrow a = c^2 \prod_{i \in I} p_i$ $I \subset \{1, \dots, n+1\}$. □