1 | Rein in die Kartoffeln

Bestimmen Sie mit Hilfe des euklidischen Algorithmus jeweils einen größten gemeinsamen Teiler der folgenden Paare:

(a) $17, 54 \in \mathbb{Z}$.

(b) $X^3 + X^2 + X + 1,\ X^3 + 1 \in \mathbb{R}[X]$

(c) $X^3 + 6X + 7,\ X^2 + 3X + 2 \in \mathbb{R}[X]$

(d) $X^6 + X^5 + X + 2,\ 3X^3 + X^2 + 2X + 1 \in \mathbb{F}_5[X]$

a:

$$54 = 3 \cdot 17 + 3$$
$$17 = 5 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1$$

$$\mathrm{ggT}(54, 17) \sim 1$$ 1

b:

$$(X^3 + X^2 + X + 1) : (X^3 + 1) = 1$$
$$-(X^3 + 1)$$

Rest: $X^2 + X$

$$(X^3 + 1) : (X^2 + X) = X - 1$$
$$-(X^3 + X^2)$$
$$-X^2 + 1$$
$$-(-X^2 - X)$$

Rest: $X + 1$

$$(X^2 + X) : (X + 1) = X$$
$$-(X^2 + X)$$

Rest: 0

$$\mathrm{ggT}(X^3 + X^2 + X + 1,\ X^3 + 1) \sim X + 1$$ 1

c: ...

$$\mathrm{ggT}(\ldots, \ldots) \sim 13X + 13$$ 1

$(\sim X + 1$ in $\mathbb{R}[X])$

$3^{-1} = 2$ in $\mathbb{F}_5$

d: $(X^6 + X^5 + X + 2) : (3X^3 + X^2 + 2X + 1) = 2X^3 + 3X^2 + X + 2$

$$
\begin{aligned}
&-(X^6 + 2X^5 + 4X^4 + 2X^3) \\
&\quad -X^5 - 4X^4 - 2X^3 + X + 2 \\
&= 4X^5 + X^4 + 3X^3 + X + 2 \\
&-(4X^5 + 3X^4 + X^3 + 3X^2) \\
&\quad 3X^4 + 2X^3 + 2X^2 + X + 2 \\
&-(3X^4 + X^3 + 2X^2 + X) \\
&\quad X^3 + 2 \\
&-(X^3 + 2X^2 + 4X + 2)
\end{aligned}
$$

Rest: $3X^2 + X$

$(3X^3 + X^2 + 2X + 1) : (3X^2 + X) = X$

$-(3X^3 + X^2)$

Rest: $2X + 1$

$(3X^2 + X) : (2X + 1) = 4X + 1$

$$
\begin{aligned}
&-(3X^2 + 4X) \\
&\quad 2X \\
&-(2X + 1)
\end{aligned}
$$

Rest: 4

$(2X + 1) : 4 = 3X + 4$

Rest: 0

$\mathrm{ggT}(\ldots,\ldots) \sim 4$ 2

$(\sim 1$ in $\mathbb{F}_5[X])$

(Wie immer -0,5 je Rechenfehler.)

2 | Integritätstest

Welche der folgenden kommutativen Ringe sind Integritätsringe?

(a) $K \times K$ für einen Körper K *(mit komponentenweiser Addition und Multiplikation)*

(b) $(\mathbb{Z}/6\mathbb{Z})[X]$

(c) $\mathbb{R}[X^2, X^3] = \{\sum_{i=0}^{n} a_i X^i \mid n \in \mathbb{N}_0, a_i \in \mathbb{R} \text{ und } a_1 = 0\}$ *(Unterring von $\mathbb{R}[X]$)*

(d) $\mathbb{Z}[\mathbf{i}] = \{a + \mathbf{i}b \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ *(siehe Lineare Algebra I, Blatt 5, Aufgabe 3)*

(e) $\mathrm{Abb}(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R}\}$ *(mit punktweiser Addition und Multiplikation)*

Begründen Sie wie immer Ihre Antwort mit einem Beweis oder einen Gegenbeweis!

a: Kein Integritätsring, denn z.B.

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$ 1

b: Kein Integritätsring, denn z.B.

$[0] = [2] \cdot [3]$ in $\mathbb{Z}/6\mathbb{Z}[X]$ 1

e: Kein Integritätsring, denn z.B.

$f \cdot g = 0$ für $f : \mathbb{R}^2 \to \mathbb{R}^2$

$$x \mapsto \begin{cases} 1 & \text{falls } x = 0 \\ 0 & \text{sonst} \end{cases}$$

und $g : \mathbb{R}^2 \to \mathbb{R}^2$

$$x \mapsto \begin{cases} 1 & \text{falls } x = 1 \\ 0 & \text{sonst} \end{cases}$$ 1

Lemma: Ist $S \subseteq R$ Unterring und ist R Integritätsring, so ist auch S ein Integritätsring.

Beweis:

Seien $a, b \in S$ mit $a \cdot b = 0$ in S.

Dann ist auch $a \cdot b = 0$ in R,

also $a = 0$ oder $b = 0$ da R Integr.-Ring.

$\square$

c: Integritätsring nach Lemma, denn
$\mathbb{R}[x]$ Integritätsring nach Vorlesung. 1

d: Integritätsring nach Lemma, denn 1
Unterring von $\mathbb{C}$.

3 | Subprime

Sei $R := \mathbb{Z}[\sqrt{-5}] = \{a + \mathbf{i}\sqrt{5}b \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$, ein Unterring von $\mathbb{C}$.

(a) Berechnen Sie die Einheitengruppe von R: $R^\times = \{\pm 1\}$.

(b) Zeigen Sie, dass das Element $2 \in R$ irreduzibel, aber nicht prim ist.

(c) Ist R ein euklidischer Ring?

Tipp: In R gilt $2 \cdot 3 = (1 + \mathbf{i}\sqrt{5})(1 - \mathbf{i}\sqrt{5})$.

a: Für $z = a + \sqrt{-5}b$ mit $a, b \in \mathbb{Z}$

ist $|z|^2 = a^2 + 5b^2 \in \mathbb{N}_0$.

Falls $z \in R^\times$, $\exists\, w = c + \sqrt{-5}d \in R$ mit

$z \cdot w = 1$, also $|z|^2 \cdot |w|^2 = 1$.

Da $|z|^2, |w|^2 \in \mathbb{N}_0$ folgt $|z|^2 = 1$.

Daher $b = 0$ und $a = \pm 1$.

Also $R^\times \subseteq \{\pm 1\}$.

Andererseits $\pm 1 \in R$ mit $(\pm 1)^{-1} = \pm 1 \in R$.

Also $R^\times = \{\pm 1\}$.

1,5

b: 2 irreduzibel:

Sei $2 = (a + \sqrt{-5}b) \cdot (c + \sqrt{-5}d)$ mit $a, b, c, d \in \mathbb{Z}$.

Dann ist

① $2 = ac - 5bd$ (Realteil)

und ② $0 = ad + bc$ ($(\sqrt{5})^{-1} \cdot$ Imaginärteil)

und außerdem

③ $4 = \underbrace{(a^2 + 5b^2)}_{\in \mathbb{N}_0} \underbrace{(c^2 + 5d^2)}_{\in \mathbb{N}_0.}$ (Norm^2)

Falls $b \neq 0$ ist $a^2 + 5b^2 \geq 5$. $\lightning$ zu ③.

Falls $d \neq 0$ analog $\lightning$ zu ③.

Also $b = d = 0$ und wegen ① $2 = a \cdot c$.

Es folgt $a = \pm 1$ oder $c = \pm 1$, somit

$$a + \sqrt{-5}\,b = \pm 1 \in R^+$$

oder $c + \sqrt{-5}\,d = \pm 1 \in R^+$.

2

2 nicht prim:

$$2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

aber $2 \nmid (1 \pm \sqrt{-5})$ denn $\left(\underbrace{|2|^2}_{4} \nmid \underbrace{|(1\pm\sqrt{-5})|}_{6} \right)$.

1

c: R ist nicht euklidisch, denn in eukl. Ringen sind laut Vorlesung irreduzible Elemente prim.

0,5

4 | Überlegung

In dieser Aufgabe konstruieren wir einen nicht-trivialen Gruppenhomomorphismus $\mathrm{SU}(2) \to \mathrm{SO}(3)$.

Sei dazu $V \subset \mathrm{Mat}_{\mathbb{C}}(2 \times 2)$ der $\mathbb{R}$-Untervektorraum aus Aufgabe 4 auf Blatt 4, und sei $\langle \cdot, \cdot \rangle$ das dort definierte Skalarprodukt. Sei $\mathrm{SO}(V, \langle \cdot, \cdot \rangle)$ die Gruppe aller Isometrien von $(V, \langle \cdot, \cdot \rangle)$ mit Determinante 1.

$\boxed{\langle M, N \rangle := -\frac{1}{2}\mathrm{tr}(M \cdot N)}$

(a) Zeigen Sie, dass $\mathrm{SO}(V, \langle \cdot, \cdot \rangle)$ isomorph zu $\mathrm{SO}(3) = \mathrm{SO}(\mathbb{R}^3, \text{Standardskalarprodukt})$ ist.

(b) Zeigen Sie, dass für jede Matrix $A \in \mathrm{SU}(2)$ die folgende Abbildung eine wohldefinierte Isometrie von $(V, \langle \cdot, \cdot \rangle)$ ist.

$$\begin{aligned} \varphi_A \colon V &\to V \\ M &\mapsto AM\bar{A}^T \end{aligned}$$

(c) Zeigen Sie, dass die folgende Abbildung ein wohldefinierter Gruppenhomomorphismus ist.

$$\begin{aligned} \pi \colon \mathrm{SU}(2) &\to \mathrm{SO}(V, \langle \cdot, \cdot \rangle) \\ A &\mapsto \varphi_A \end{aligned}$$

(d) Zeigen Sie, dass π nicht trivial (das heißt hier: nicht konstant) ist und berechnen Sie den Kern von π.

Tatsächlich ist π sogar surjektiv! Es ist aber nicht so einfach, das explizit zu zeigen.

a: Aus Blatt 4, Aufgabe 4 (b) haben wir einen Isomorphismus

$$\left(V, \langle \cdot, \cdot \rangle\right) \xleftarrow{\cong} \left(\mathbb{R}^3, \langle \cdot, \cdot \rangle_{\text{Standard}}\right) : \tau,$$

$$\begin{aligned} A &\mapsfrom e_1 \\ B &\mapsfrom e_2 \\ C &\mapsfrom e_3 \end{aligned}$$

für den gilt:

(*) $\langle \tau(\underline{v}), \tau(\underline{w}) \rangle = \langle \underline{v}, \underline{w} \rangle_{\text{Standard}} \quad \forall \underline{v}, \underline{w} \in \mathbb{R}^3.$

Es folgt:

(**) $\langle M, N \rangle = \langle \tau^{-1}(M), \tau^{-1}(N) \rangle \quad \forall M, N \in V.$

Definiere

$$\begin{aligned} \Psi : \mathrm{SO}(V, \langle \cdot, \cdot \rangle) &\longrightarrow \mathrm{SO}(\mathbb{R}^3, \langle \cdot, \cdot \rangle_{\text{Standard}}) \\ \varphi &\longmapsto \tau^{-1} \circ \varphi \circ \tau \end{aligned}$$

Wegen (*) & (**) ist für jede Isometrie φ auch $z^{-1}\circ\varphi\circ z$ ein Isometrie. Also ist Ψ wohldefiniert.

Ψ ist Gruppenhomo:

$$\Psi(\varphi_1\circ\varphi_2) = z^{-1}\varphi_1\varphi_2 z = z^{-1}\varphi_1 z z^{-1}\varphi_2 z$$
$$= \Psi(\varphi_1)\circ\Psi(\varphi_2).$$

Ψ ist Iso, denn wir haben Inverses

$$z\varphi z^{-1} \circlearrowleft V \qquad \leftarrow\!\shortmid \qquad \varphi \circlearrowleft \mathbb{R}^3 .$$ 1

b: Für $M\in V$ und $A\in SU(2)$ ist auch $\varphi_A(M) = AM\bar{A}^T \in V$, denn:

① $$\overline{\varphi_A(M)}^T = (\overline{AM\bar{A}^T})^T = (\bar{A}\,\bar{M}\,A^T)^T$$
$$= A^{TT}\,\bar{M}^T\,\bar{A}^T$$
$$\underset{M\in V\checkmark}{=} -AM\bar{A}^T = -\varphi_A(M).$$ 1

② $$tr(\varphi_A(M)) = tr(AM\bar{A}^T) \quad \begin{array}{c} tr(AB) \\ \shortparallel \\ tr(BA) \end{array}$$
$$= tr(\underbrace{A\cdot\bar{A}^T}_{\mathbb{1},\ \text{da } A\in SU(2)}\cdot M)$$
$$= tr(M) = 0$$ 1

Ferner gilt:

$$\langle\varphi_A(M), \varphi_A(N)\rangle = -\tfrac{1}{2}tr(AM\bar{A}^TAN\bar{A}^T)$$
$$= -\tfrac{1}{2}\Big(tr(\underbrace{A\bar{A}^T}_{\mathbb{1}}\underbrace{A\bar{A}^T}_{\mathbb{1}}MN)\Big) = \langle M,N\rangle$$
da $A\in U(2)$ 1

c: $\varphi_{AB} = \varphi_A\circ\varphi_B$, denn

$$(\varphi_A\circ\varphi_B)(M) = A\cdot B\cdot M\cdot\bar{B}^T\cdot\bar{A}^T$$
$$= AB\cdot M\cdot\overline{AB}^T = \varphi_{AB}(M).$$ 1

Bis hier bereits volle Punktzahl.

---

d: $A \in \ker(\pi)$

$\Leftrightarrow \quad \pi(A) = \mathrm{id}$

$\Leftrightarrow \quad \varphi_A(M) = M \quad \forall M \in V$

$\Leftrightarrow \quad A M \bar{A}^T = M$ für $M \in \{ \underbrace{\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}}_{\text{Basis von } V.} \}$

Bevor wir weiterrechnen, zeigen wir zunächst:

Lemma: Jede Matrix aus $SU(2)$ hat die Form $\begin{pmatrix} u & -\bar{v} \\ v & \bar{u} \end{pmatrix}$ für gewisse $u, v \in \mathbb{C}$ mit $|u|^2 + |v|^2 = 1$.

Beweis:

Ansatz: Matrix hat die Form

$\begin{pmatrix} u & w \\ v & x \end{pmatrix}$ für gewisse $u, v, w, x \in \mathbb{C}$

mit (1) $\left\| \begin{pmatrix} u \\ v \end{pmatrix} \right\|^2 = \left\| \begin{pmatrix} w \\ x \end{pmatrix} \right\|^2 = \left\| \begin{pmatrix} u \\ w \end{pmatrix} \right\|^2 = \left\| \begin{pmatrix} v \\ x \end{pmatrix} \right\|^2 = 1$

und (2) $\begin{pmatrix} u \\ v \end{pmatrix} \perp \begin{pmatrix} w \\ x \end{pmatrix}$ und (3) $\begin{pmatrix} u \\ w \end{pmatrix} \perp \begin{pmatrix} v \\ x \end{pmatrix}$.

und (4) $ux - vw = 1$.

Falls $u = 0$ oder $x = 0$, folgt $u = x = 0$, und kurze Rechnung zeigt $w = -\bar{v}$.

Falls $u \neq 0$ und $x \neq 0$:

Betrachte zunächst $\begin{pmatrix} u' & w' \\ v' & x' \end{pmatrix}$ mit

$$\hat{u} := \frac{u}{|u|} \qquad u' := \hat{u}^{-1} \cdot u = |u| \in \mathbb{R}_{\geq 0}$$
$$v' := \hat{u}^{-1} \cdot$$
$$\hat{x} := \frac{x}{|x|} \qquad w' := \hat{x}^{-1} \cdot w$$
$$x' := \hat{x}^{-1} \cdot x = |x| \in \mathbb{R}_{\geq 0}.$$

Dann ist immer noch $\begin{pmatrix} u' & w' \\ v' & x' \end{pmatrix} \in \mathcal{U}(2)$,

d.h., 1, 2, 3 gelten auch für die gestrichenen Größen, und aus 4 wird

4' $\hat{u} \cdot \hat{w} \cdot (u'x' - w'v') = 1$

Wegen 1 ist $|u'|^2 = 1 - |v'|^2 = |x'|^2$, und da $u', x' \in \mathbb{R}_{\geq 0}$ folgt $\boxed{u' = x'.}$

Aus 2 folgt: $u'\bar{w}' + v'\bar{x}' = 0$,

also $u'(\bar{w}' + v') = 0$,

also $\boxed{w' = -\bar{v}'!}$

Eingesetzt in 4' erhalten wir:

$$\underset{\text{Norm } 1}{\hat{u} \cdot \hat{w}} \cdot \underbrace{(u'^2 - |v'|^2)}_{\in \mathbb{R}} = 1$$

Daraus folgt $\hat{u} \cdot \hat{w} = 1$, also $\boxed{\hat{u} = \bar{\hat{w}}.}$

Nun ergibt sich die Behauptung [...] $\square$

Zurück zur Aufgabe:

Ansatz: $A = \begin{pmatrix} u & -\bar{v} \\ v & \bar{u} \end{pmatrix}$ mit $|u|^2+|v|^2=1$

derart, dass

$$A \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \bar{A}^T = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

und $$A \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \bar{A}^T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

und $$A \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \bar{A}^T = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Nach endlicher Rechnung [...] folgt:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ oder } A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Man sieht leicht, dass diese beiden Matrizen tatsächlich in $\ker(\pi)$ liegen. Also folgt:

$$\ker(\pi) = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

Insbesondere folgt: π ist nicht trivial, denn es gibt auch Matrizen in

$$SU(2) \setminus \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

(z.B. $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$).

Bis zu 5 Bonuspunkte für Teil (a).