1 | Millimeterarbeit II

Bestimmen Sie mit Hilfe des erweiterten euklidischen Algorithmus (Beweis zu Satz 13.13) zu den folgenden Paaren von Ringelementen a, b jeweils Ringelemente x, y, für die gilt: $xa + yb \sim \mathrm{ggT}(a, b)$.

(a) $17, 54 \in \mathbb{Z}$.
(b) $X^3 + X^2 + X + 1,\ X^3 + 1 \in \mathbb{R}[X]$

Einen größten gemeinsamen Teiler haben Sie jeweils bereits in Aufgabe 1 auf Blatt 5 berechnet.

Euklidischer Algorithmus (Blatt 5)		erweiterter Algorithmus
a: $54 = 3 \cdot 17 + 3$	$\Rightarrow$	$3 = 54 - 3 \cdot 17$
$17 = 5 \cdot 3 + 2$	$\Rightarrow$	$2 = 17 - 5 \cdot 3$
		$= 17 - 5 \cdot (54 - 3 \cdot 17)$
		$= 17 - 5 \cdot 54 + 15 \cdot 17$
		$= 16 \cdot 17 - 5 \cdot 54$
$3 = 1 \cdot 2 + 1$	$\Rightarrow$	$1 = 3 - 1 \cdot 2$
$2 = 2 \cdot 1$		$= 54 - 3 \cdot 17 - (16 \cdot 17 - 5 \cdot 54)$
$\mathrm{ggT}(54, 17) \sim 1$		$= \underline{\underline{6 \cdot 54 - 19 \cdot 17}}$

2,5

b: $A := X^3 + X^2 + X + 1$		
$B := X^3 + 1$		
$A = 1 \cdot B + (X^2 + X)$	$\Rightarrow$	$X^2 + X = A - B$
$B = (X-1) \cdot (X^2 + X) + (X+1)$	$\Rightarrow$	$X + 1 = B - (X-1)(X^2+X)$
		$= B - (X-1)(A - B)$
		$= \underline{\underline{X \cdot B - (X-1) \cdot A}}$
$X^2 + X = X \cdot (X+1)$		
$\mathrm{ggT}(A, B) \sim X + 1$		

2,5

2 | Begradigung

Bestimmen Sie charakteristisches Polynom, Minimalpolynom und eine Jordannormalform der folgenden Endomorphismen.

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 11 & 6 & -4 & -4 \\ 22 & 15 & -8 & -9 \\ -3 & -2 & 1 & 2 \end{pmatrix}$$

$$\chi_A = \det \begin{pmatrix} -X & 1 & 0 & 0 \\ 11 & 6-X & -4 & -4 \\ 22 & 15 & -8-X & -9 \\ -3 & -2 & 1 & 2-X \end{pmatrix}$$

$$= \det \begin{pmatrix} -X & 1 & 0 & 0 \\ 11 & 6-X & 0 & -4 \\ 22 & 15 & 1-X & -9 \\ -3 & -2 & X-1 & 2-X \end{pmatrix} \quad -2 \quad +$$

$$= \det \begin{pmatrix} -X & 1 & 0 & 0 \\ 11 & 6-X & 0 & -4 \\ -3 & 2X+1 & 0 & 1-X \\ -3 & -2 & X-1 & 2-X \end{pmatrix}$$

$$= -(X-1) \det \begin{pmatrix} -X & 1 & 0 \\ 11 & 6-X & -4 \\ -3 & 2X+1 & 1-X \end{pmatrix}$$

$$= -(X-1)\left[-X(6-X)(1-X) + 12 - 11(1-X) - 4X(2X+1)\right]$$

$$= -(X-1)\left[-X(X^2-7X+6) + 12 - 11 + 11X - 8X^2 - 4X\right]$$

$$= -(X-1)\left(-X^3 + 7X^2 - 6X + 1 + 11X - 8X^2 - 4X\right)$$

$$= -(X-1)\underbrace{\left(-X^3 - X^2 + X + 1\right)}_{\text{Nullstelle } 1}$$

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

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

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

$$= \underline{\underline{(X-1)^2(X+1)^2}}$$

1

$$\mu_A = \begin{cases} (X-1)(X+1) & \text{oder} \\ (X-1)^2(X+1) & \text{oder} \\ (X-1)(X+1)^2 & \text{oder} \\ (X-1)^2(X+1)^2 & \end{cases}$$

$$(A-\mathbb{1})(A+\mathbb{1}) = \begin{pmatrix} -1 & 1 & 0 & 0 \\ 11 & 5 & -4 & -4 \\ 22 & 15 & -9 & -9 \\ -3 & -2 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 11 & 7 & -4 & -4 \\ 22 & 15 & -7 & -9 \\ -3 & -2 & 1 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 10 & \dots & \\ & \dots & \end{pmatrix} \neq 0$$

$$(A-\mathbb{1})^2(A+\mathbb{1}) = \begin{pmatrix} -1 & 1 & 0 & 0 \\ 11 & 5 & -4 & -4 \\ 22 & 15 & -9 & -9 \\ -3 & -2 & 1 & 1 \end{pmatrix} \begin{pmatrix} -1 & 1 & 0 & 0 \\ 11 & 5 & -4 & -4 \\ 22 & 15 & -9 & -9 \\ -3 & -2 & 1 & 1 \end{pmatrix} \cdot (A+\mathbb{1})$$

$$= \begin{pmatrix} 12 & 4 & -4 & -4 \\ & \dots & & \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 11 & 7 & -4 & -4 \\ 22 & 15 & -7 & -9 \\ -3 & -2 & 1 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} -20 & \dots \\ \dots & \end{pmatrix} \neq 0$$

$$(A-\mathbb{1})(A+\mathbb{1})^2 = \begin{pmatrix} -1 & 1 & 0 & 0 \\ 11 & 5 & -4 & -4 \\ 22 & 15 & -9 & -9 \\ -3 & -2 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 11 & 7 & -4 & -4 \\ 22 & 15 & -7 & -9 \\ -3 & -2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 11 & 7 & -4 & -4 \\ 22 & 15 & -7 & -9 \\ -3 & -2 & 1 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} -1 & 1 & 0 & 0 \\ 11 & 5 & -4 & -4 \\ 22 & 15 & -9 & -9 \\ -3 & -2 & 1 & 1 \end{pmatrix} \begin{pmatrix} 12 & \\ 12 & \\ 60 & \dots \\ -12 & \end{pmatrix}$$

$$= \begin{pmatrix} \dots & \\ & \\ -12 & \dots \end{pmatrix} \neq 0$$

Also $\mu_A = \underline{\underline{(X-1)^2(X+1)^2}}$

JNF von A: $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ 1

$$B = \begin{pmatrix} 5 & 4 & 2 & 1 \\ 0 & 1 & -1 & -1 \\ -1 & -1 & 3 & 0 \\ 1 & 1 & -1 & 2 \end{pmatrix}$$

$$\chi_B = \ldots = \underline{\underline{(X-1)(X-2)(X-4)^2}}$$ 1

$$\mu_B = \begin{cases} (X-1)(X-2)(X-4) & \text{oder} \\ (X-1)(X-2)(X-4)^2 \end{cases}$$

$$(B-\mathbb{1})(B-2\cdot\mathbb{1})(B-4\cdot\mathbb{1})$$

$$= \underbrace{\begin{pmatrix} 4 & 4 & 2 & 1 \\ 0 & 0 & -1 & -1 \\ -1 & -1 & 2 & 0 \\ 1 & 1 & -1 & 1 \end{pmatrix}\begin{pmatrix} 3 & 4 & 2 & 1 \\ 0 & -1 & -1 & -1 \\ -1 & -1 & 1 & 0 \\ 1 & 1 & -1 & 0 \end{pmatrix}}\begin{pmatrix} 1 & 4 & 2 & 1 \\ 0 & -3 & -1 & -1 \\ -1 & -1 & -1 & 0 \\ 1 & 1 & -1 & -2 \end{pmatrix}$$

$$= \begin{pmatrix} 11 & 11 & 5 & 0 \\ & \ldots & & \\ & & & \end{pmatrix} \cdot \begin{pmatrix} 1 & 4 & 2 & 1 \\ 0 & -3 & -1 & -1 \\ -1 & -1 & -1 & 0 \\ 1 & 1 & -1 & -2 \end{pmatrix}$$

$$= \begin{pmatrix} 6 & & \\ & \ldots & \\ & & \end{pmatrix} \neq 0$$

Also $\mu_B = \underline{\underline{(X-1)(X-2)(X-4)^2}}$

JNF von B: $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 4 \end{pmatrix}$ 1

$$C = \begin{pmatrix} 4 & 1 & 2 \\ 0 & 4 & 3 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\chi_C = (4-x)^2(-x) = \underline{\underline{x(x-4)^2}}$$

$$\mu_C = \begin{cases} x(x-4) & \text{oder} \\ x(x-4)^2 \end{cases}.$$

$$C \cdot (C - 4 \cdot \mathbb{1}) = \begin{pmatrix} 4 & 1 & 2 \\ 0 & 4 & 3 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & -4 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 4 & \\ 0 & \cdots & \\ 0 & & \end{pmatrix} \neq 0.$$

Also $\mu_C \underline{\underline{= x(x-4)^2}}$. 0,5

JNF von C: $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 4 \end{pmatrix}$ 0,5

3 | **Schweres Element**

Zeigen Sie, dass das Polynom $X^n - 2$ in $\mathbb{Q}[X]$ für $n \geqslant 1$ irreduzibel ist.

Nach dem Fundamentalsatz der Algebra ist

$$X^n - 2 = (X - \varepsilon_1) \cdot \ldots\ldots\ldots\ldots \cdot (X - \varepsilon_n) \quad (*)$$

für gewisse komplexe Nullstellen $\varepsilon_i \in \mathbb{C}$. Für jedes ε_i gilt: $\varepsilon_i^n = 2$,

also insbesondere $|\varepsilon_i|^n = 2$,

also $|\varepsilon_i| = \sqrt[n]{2}$.

Vergleiche nun die konstanten Koeffizienten in $(*)$:

Angenommen, $X^n - 2 = A \cdot B$ für gewisse $A, B \in \mathbb{Q}[X]$. Wir können OE annehmen, dass A und B normiert sind. Jede NS von $X^n - 2$ muss eine NS von A oder B sein, und umgekehrt. Nach eventueller Umnummerierung der NS ε_i gilt also:

$$A = \prod_{i=1}^{k} (X - \varepsilon_i) \quad \text{für ein } k \in \{0, \ldots, n\}.$$

Der Koeffizient von A in Grad 0 ist dann

$$a_0 = (-1)^k \prod_{i=1}^{k} \varepsilon_i,$$

somit $|a_0| = (\sqrt[n]{2})^k$. Da $A \in \mathbb{Q}[X]$, muss andererseits gelten:

$$|a_0| \in \mathbb{Q}.$$

Aus dem folgenden Lemma ergibt sich daher:

$$k = 0 \quad \text{oder} \quad k = n.$$

Also ist $A = 1$ oder $A = X^n - 2$, und somit $X^n - 2$ irreduzibel über $\mathbb{Q}$.

3

Lemma: Für $k, n \in \mathbb{N}$ gilt:
$$(\sqrt[n]{2})^k \in \mathbb{Q} \iff n \mid k$$

Beweis:

($\Leftarrow$) ✓

($\Rightarrow$) Sei $(\sqrt[n]{2})^k = \frac{a}{b}$ für gewisse $a, b \in \mathbb{Z}$ mit $b \neq 0$.

Dann ist
$$2^k \cdot b^n = a^n$$

Schreibe $a = 2^\alpha \cdot \tilde{a}$ mit $\tilde{a}$ teilerfremd zu 2, $\alpha \in \mathbb{N}_0$

$b = 2^\beta \tilde{b}$ mit $\tilde{b}$ teilerfremd zu 2, $\beta \in \mathbb{N}_0$

Dann ergibt sich:
$$2^{k+n\beta} \cdot \tilde{b}^n = 2^{n\alpha} \cdot \tilde{a}^n$$

Wegen der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}$ ergibt sich also:
$$k + n\beta = n\alpha$$

bzw. $k = n(\alpha - \beta)$, also $n \mid k$. $\square$

2

(Für Nachweis, dass $X^n - 2$ über $\mathbb{Z}$ irreduzibel ist, maximal 3,5 Punkte.
Für Lösungen, die Eisenstein-Kriterium verwenden, ohne dieses Kriterium zu beweisen, maximal 1,5 Punkte, und auch nur, weil dieses Kriterium von einigen Übungsleitern fälschlicherweise als „Tipp" genannt wurde.)

4 | Hyperrotation

Sei $f\colon \mathbb{Q}^n \to \mathbb{Q}^n$ der bezüglich der Standardbasis durch folgende Matrix gegebene Endomorphismus ($n \geqslant 2$). Bestimmen Sie alle Unterräume von $\mathbb{Q}^n$, die f-stabil sind.

$$\begin{pmatrix} 0 & \cdots & 0 & 2 \\ 1 & & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & 1 & 0 \end{pmatrix}$$

Tipp: Benutzen Sie die vorherige Aufgabe.

$$\chi_f = \det \begin{pmatrix} -X & & 0 & 2 \\ 1 & -X & & 0 \\ & 1 & \ddots & \vdots \\ & & \ddots & -X & 0 \\ 0 & & & 1 & -X \end{pmatrix}$$

Entwicklung nach erster Zeile

Spalte n
Zeile 1
$n+1$

$$= -X \cdot \det \begin{pmatrix} -X & & 0 & 0 \\ 1 & \ddots & & \vdots \\ & \ddots & -X & 0 \\ 0 & & 1 & -X \end{pmatrix} + \overbrace{(-1)^{n+1}}\, 2 \cdot \det \begin{pmatrix} 1 & -X & & \\ & 1 & \ddots & \\ & & \ddots & -X \\ 0 & & & 1 \end{pmatrix}$$

$$= -X \cdot (-X)^{n-1} \qquad + (-1)^{n+1} 2$$

$$= (-1)^n (X^n - 2)$$ 2

Ist $W \subseteq \mathbb{Q}^n$ ein f-stabiler UVR, so folgt laut Lemma 14.15:

$$\chi_f = \chi_{f|W} \cdot \chi_{\bar{f}}$$ 1,5

Da hier χ_f laut Aufgabe 3 irreduzibel ist, folgt dann $\chi_{f|W} \sim 1$ oder $\chi_{f|W} \sim \chi_f$.
Somit folgt $\dim W = 0$ oder $\dim W = n$.

Also sind $\{0\}$ und $\mathbb{Q}^n$ die einzigen f-stabilen UVR.

1,5