Algebra I – Aufgabensammlung mit Lösungsskizzen

Sommersemester 2020
Tutor: Philipp Schläger

Achtung: Die folgenden Aufgaben dienen zur Prüfungsvorbereitung. Die dargestellten Lösungen sind als „Skizzen“ aufzufassen. Eine entsprechende Form (z.B.: „Vor., Beh. und Bew.“), sowie nicht aufgeführte Zwischenschritte – welche nicht notwendigerweise durch „(wie/wieso?)“ markiert sind – sind zu ergänzen! Außerdem besteht keine Garantie für die Richtigkeit der Lösungen. Die Notation für Ideale $\langle x, y, ... \rangle$ ist hier mit runden Klammern $(x, y, ...)$. In der Klausur sind die spitzen Klammern zu nutzen! Mit $\mathbb{F}_p$ ist der Körper $\mathbb{Z}/p\mathbb{Z}$ gemeint.
Viel Erfolg bei der Klausur!

Aufgabe 1 (Ringe und Ideale)

a) Geben Sie für folgende mathematischen Strukturen jeweils mindestens ein Beispiel:

   i) nichtabelsche/abelsche Gruppe

   ii) Ring, Körper

   iii) Ideal, Hauptideal

b) Sei $S \subsetneq R$ eine echte Teilmenge des kommutativen Rings R. In dieser Aufgabe sei ein Unterring immer ein Unterring mit 1. Zeigen Sie:

   i) Ist S ein Unterring von R, dann ist S kein Ideal von R.

   ii) Ist S ein Ideal von R, so ist S kein Unterring von R.

c) Zeigen Sie, dass $(2, t)$ in $\mathbb{Z}[t]$ kein Hauptideal ist.

d) Sei R ein kommutativer Ring (wie immer mit 1), $I \subseteq R$ ein Ideal von R. Zeigen Sie: $I = R \Leftrightarrow I \cap R^* \neq \varnothing$.

Lösung:

a) i) abelsche Gruppe: $(\mathbb{Z}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$
nichtabelsche Gruppe: $(\mathrm{Gl}(n, K), \cdot)$ Gruppe der invertierbaren Matrizen über dem Körper K

ii) Ring: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}[t], +, \cdot)$
Körper: $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$

iii) Ideal: In $\mathbb{Z}$: $I = 4\mathbb{Z}$, in $\mathbb{Z}[t]$: $J = (2, t)$
Hauptideal: In $\mathbb{Z}$: $I = 4\mathbb{Z} = (4)$

b) i) Sei $S \subsetneq R$ eine echte Teilmenge des kommutativen Rings R. Sei S ein Unterring von R.
ZZ: S ist kein Ideal von R.
Angenommen, S wäre ein Ideal von R. Weil S ein Unterring von R ist, ist $1_R \in S$. Aus der Schluckeigenschaft von S ist dann $r \cdot 1_R = r \in S$ für alle $r \in R$. Also $S = R$. Widerspruch zu $S \subsetneq R$. S kann also kein Ideal von R sein. □

ii) Sei $S \subsetneq R$ eine echte Teilmenge des kommutativen Rings R. Sei S ein Ideal von R.
ZZ: S ist kein Unterring von R.
Angenommen, S wäre ein Unterring von R. Genauso wie oben folgt dies durch Schluckeigenschaft zum Widerspruch $S = R$. □

c) Siehe Skript (2.6.14).

d) Sei R ein kommutativer Ring und sei $I \subseteq R$ ein Ideal.
ZZ: $I = R \Leftrightarrow I \cap R^* \neq \varnothing$.
„$\Rightarrow$“
Sei $I = R$. Nach Voraussetzung ist dann $1_R \in I \cap R^* \neq \varnothing$.
„$\Leftarrow$“
Sei $I \cap R^* \neq \varnothing$. Sei $a \in I \cap R^*$. Es existiert ein $a^{-1} \in R$. Nach Idealeigenschaften von I ist $a \cdot a^{-1} = 1_R \in I$ und damit auch $r \cdot 1_R = r \in I$ für alle $r \in R$. Also $I = R$. □

Aufgabe 2 (Ringhomomorphismen)

Seien R, S Ringe und sei K ein Körper. Zeigen Sie:

a) Ist $\varphi : R \to S$ ein Ringhomomorphismus, so gilt $\varphi(R^*) \subseteq (\text{Bild}(\varphi))^* \subseteq S^*$

b) Ist $\varphi : K \to R$ ein Ringhomomorphismus und $R \neq \{0\}$, so ist φ injektiv.

c) Sei $R \subseteq S$ und $\alpha \in S$. Wie ist $R[\alpha]$ definiert? Zeigen Sie dann, dass $\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{N}_0\right\}$.

Lösung:

Seien R, S Ringe und sei K ein Körper.

a) Sei $\varphi : R \to S$ ein Ringhomomorphismus.
ZZ: $\varphi(R^*) \subseteq (\text{Bild}(\varphi))^*$ und $(\text{Bild}(\varphi))^* \subseteq S^*$.
1. Inklusion:
Sei $\alpha \in R^*$. ZZ: $\varphi(\alpha) \in (\text{Bild}(\varphi))^*$.
Sei $\beta = \alpha^{-1}$. Dann gilt mit $\varphi(\alpha), \varphi(\beta) \in \text{Bild}(\varphi)$:
$\varphi(\alpha) \cdot \varphi(\beta) = \varphi(\alpha \cdot \beta) = \varphi(1_R) = 1_S$ und analog $\varphi(\beta) \cdot \varphi(\alpha) = 1_S$. Also $\varphi(\alpha) \in (\text{Bild}(\varphi))^*$.
2. Inklusion:
Sei $b \in (\text{Bild}(\varphi))^*$. ZZ: $b \in S^*$.
Da $\text{Bild}(\varphi) \subseteq S$, ist auch $b^{-1} \in (\text{Bild}(\varphi))^* \subseteq S$, also $b \in S^*$. □

b) Sei $\varphi : K \to R$ ein Ringhomomorphismus und sei $R \neq \{0\}$.
ZZ: φ ist injektiv.
Nach VL genügt zu zeigen: $\text{Kern}(\varphi) = \{0\}$.
Sei $x \in K$ mit $\varphi(x) = 0$. Wenn $x \neq 0$, so existiert ein Inverses $y = x^{-1}$. Damit gilt: $\varphi(x \cdot y) = 1_R \neq 0_R = 0_R \cdot \varphi(y) = \varphi(x) \cdot \varphi(y)$ Dies steht im Widerspruch dazu, dass φ ein Ringhomomorphismus ist. Es folgt also $x = 0$ und somit $\text{Kern}(\varphi) = \{0\}$. □

c) Sei $R \subseteq S$ und $\alpha \in S$. Per Definition ist $R[\alpha]$ das Bild des Einsetzungshomomorphismus $\Psi_\alpha : R[t] \to S$. Dafür definieren wir $\Psi_\alpha : R[t] \to S$ mit $f = \sum_{i=0}^n a_i \cdot t^i \mapsto f(\alpha) := \sum_{i=0}^n a_i \cdot \alpha^i$. Dabei ist n von f abhängig. Damit ergibt sich: $R[\alpha] = \text{Bild}\,(\Psi_\alpha) = \{f(\alpha) \mid f \in R[t]\} = \left\{\sum_{i=0}^n a_i \cdot \alpha^i \mid a_i \in R, n \in \mathbb{N}_0\right\}$.

ZZ: $\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{N}_0\right\}$.
Nach obiger Definition ergibt sich $\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\sum_{i=0}^n a_i \cdot \frac{1}{2^i} \mid a_i \in \mathbb{Z}, n \in \mathbb{N}_0\right\}$. Offensichtlich gilt $\left\{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{N}_0\right\} \subseteq \mathbb{Z}\left[\frac{1}{2}\right]$. (wieso?)
Wir zeigen also die andere Inklusion:
Sei $x \in \mathbb{Z}\left[\frac{1}{2}\right]$. Dann existieren $n \in \mathbb{N}_0$ und $a_0, \ldots, a_n \in \mathbb{Z}$ mit $x = \sum_{i=0}^n a_i \cdot \frac{1}{2^i}$.
Setze $a := \sum_{i=0}^n a_i \cdot 2^{n-i} \in \mathbb{Z}$, dann gilt: $\frac{a}{2^n} = x \in \left\{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{N}_0\right\}$.
Insgesamt also $\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{N}_0\right\}$. □

Aufgabe 3 (Teilbarkeit)

a) Definieren sie für einen Integritätsring R und zwei Elemente $a, b \in R$, welche Eigenschaften ein größter gemeinsamer Teiler (ggT) und ein kleinstes gemeinsames Vielfaches (kgV) erfüllen müssen.

b) Berechnen Sie mithilfe des euklidischen Algorithmus einen ggT von 3738 und 5208 im Ring $\mathbb{Z}$

c) Berechnen Sie in $\mathbb{Q}[t]$ einen ggT von $f = t^3 + 3t^2 - t - 3$ und $g = t^3 + 3t^2 + 4t + 2$.

d) Sei R ein Integritätsring und seien $a, b \in R$. Zeigen Sie direkt: $aR = bR \Leftrightarrow a \sim b$ (a und b sind in R zueinander assoziiert).

e) Definieren Sie „irreduzibel“ und „prim“ in einem kommutativen Ring R. Geben Sie ein Beispiel für einen nichtfaktoriellen Ring R und ein Element $p \in R$, sodass p irreduzibel, aber nicht prim in R ist.

f) Seien R ein Integritätsring und $p, q \in R$. Seiein p prim und q irreduzibel in R, und gelte $p \nsim q$. Zeigen Sie für $r \in R$: $p \mid r \wedge q \mid r \Rightarrow pq \mid r$.

g) Sei $R = \mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$ der Ring der Gauß'schen ganzen Zahlen. Untersuchen Sie, ob $p = 1 + i$ und $q = 4 - 3i$ irreduzibel und prim in R sind.

h) Berechnen sie einen ggT d von $a = 4 + 8i$ und $b = 5 + 3i$ in $\mathbb{Z}[i]$ und finden Sie eine Darstellung $ax + by = d$ mit $x, y \in \mathbb{Z}[i]$. Dies ist nicht klausurrelevant.

i) Bestimmen Sie im Ring R jeweils ein (möglichst kleines) Erzeugendensystem der Ideale I, $I + J$, $I \cdot J$ und $I \cap J$. Dabei sind I und J Ideale:

i) $R = \mathbb{Z}$, $I = (60, 105)$ und $J = (51)$.

ii) $R = \mathbb{Z}$, $I = (120, 15, 99)$ und $J = (63)$.

iii) $R = \mathbb{Q}[t]$, $I = (t+1)$ und $J = \left((t+1)^3\right)$.

j) Sei R ein Integritätsring und $p \in R$ ein Primelement von R.
Zeigen Sie: $pR = (p)$ ist ein Primideal von R.
Zeigen Sie mithilfe der Definitionen: Ist R zudem ein Hauptidealring, so ist pR ein maximales Ideal.

Lösung:

a) Sei R ein Integritätsring. Seien $a, b \in R$. Ein Element $d \in R$ heißt größter gemeinsamer Teiler von a und b, wenn $d|a$ und $d|b$ und wenn zusätzlich für jeden gemeinsamen Teiler $f \in R$ von a und b (also $f|a$ und $f|b$) gilt: $f|d$.
Ein Element $c \in R$ heißt kleinstes gemeinsames Vielfaches von a und b, wenn $a|c$ und $b|c$ und wenn zusätzlich für jedes gemeinsame Vielfache $e \in R$ von a und b (also $a|e$ und $b|e$) gilt: $c|e$.

b) $5208 = 1 \cdot 3738 + 1470$
$3738 = 2 \cdot 1470 + 798$
$1470 = 1 \cdot 798 + 672$
$798 = 1 \cdot 672 + 126$
$672 = 5 \cdot 126 + 42$
$126 = 3 \cdot 42 + 0$
Also ist 42 ein ggT von 5208 und 3738.

c) $t^3 + 3t^2 - t - 3 = 1 \cdot (t^3 + 3t^2 + 4t + 2) + (-5t - 5)$
$t^3 + 3t^2 + 4t + 2 = -\frac{1}{5}(t^2 + 2t + 2) \cdot (-5t - 5) + 0$
Also ist $-5t-5$ ein ggT von f und g. Da $(t+1) \sim (-5t-5)$ ist $t+1$ auch ein ggT von f und g. Der normierte ggT von f und g ist daher $\text{ggT}(f, g) = t + 1$.

d) Sei R ein Integritätsring und seien $a, b \in R$.
ZZ: $aR = bR \Leftrightarrow a \sim b$
„$\Rightarrow$“
Sei $aR = bR$. ZZ: $a \sim b$.
Es gilt $a \in bR$ und somit $b|a$ in R. Außerdem gilt $b \in aR$, also $a|b$ in R. Daraus folgt, dass $a \sim b$ in R.
„$\Leftarrow$“
Sei $a \sim b$. ZZ: $aR = bR$.
Da $a \sim b$ folgt direkt $a|b$ und $b|a$. Das ergibt: $bR \subseteq aR$ und $aR \subseteq bR$. Folglich gilt $aR = bR$. □

e) Sei R ein kommutativer Ring. Ein Element $p \in R \setminus (\{0\} \cup R^*)$ heißt irreduzibel, wenn für alle $q_1, q_2 \in R$ mit $p = q_1 \cdot q_2$ folgt, dass $q_1 \in R^*$ oder $q_2 \in R^*$.
Ein Element $p \in R \setminus (\{0\} \cup R^*)$ heißt Primelement von R (oder prim in R), wenn für alle $q_1, q_2 \in R$ mit $p|q_1q_2$ folgt, dass $p|q_1$ oder $p|q_2$.
$R = \mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell. Denn beispielsweise ist 2 irreduzibel in R, aber nicht prim. Denn $2|6 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$ aber die Faktoren werden in R nicht von 2 geteilt.

f) Sei R ein Integritätsring und sei $p \in R$ prim und $q \in R$ irreduzibel. Sei $r \in R$ mit $p|r$ und $q|r$.
ZZ: $pq|r$.
Es existiert wegen $q|r$ ein $c \in R$ mit $r = cq$. Weil p prim ist folgt $p|c$ oder $p|q$. (wieso?)
Angenommen, $p|q$. Dann wäre $q = p \cdot \varepsilon$ mit $\varepsilon \in R$. Da q aber irreduzibel und $p \notin R^*$ folgt $\varepsilon \in R^*$ und somit $p \sim q$, was einen Widerspruch ergibt.
Also folgt $p|c$. Insgesamt folgt somit $pq|r$. (wieso?) □

g) Sei $R = \mathbb{Z}[i]$, $p = 1 + i$ und $q = 4 - 3i$.
ZZ: p ist irreduzibel und q ist reduzibel in R.
Zunächst wissen wir: $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$.
Betrachte zunächst p:
$p \neq 0$ und $p \notin R^*$ ist erfüllt. Angenommen $a, b \in R$ mit $p = ab$.
ZZ: $a \in R^*$ oder $b \in R^*$.
Zum Beweis benutzen wir das Quadrat des komplexen Betrags als Hilfsfunktion. Wir wissen, dass die Abbildung $|\cdot|^2 : R \to \mathbb{N}_0$ multiplikativ linear ist. Es gilt:
$2 = |p|^2 = |ab|^2 = |a|^2|b|^2$. Also folgt $|a|^2 = 1$ oder $|b|^2 = 1$. Da $R^* = \left\{z \in R : |z|^2 = 1\right\}$ folgt somit $a \in R^*$ oder $b \in R^*$. Demnach ist p irreduzibel in $R = \mathbb{Z}[i]$, also auch prim, da $\mathbb{Z}[i]$ faktoriell ist.
Nun betrachten wir q:
ZZ: q ist reduzibel in R.
Mit der gleichen Idee wie bei p kann man überlegen, weil $|q|^2 = 25 = 5 \cdot 5$, dass eine mögliche Zerlegung $q = ab$ höchstens mit $|a|^2 = |b|^2 = 5$ vorstellbar ist. Dadurch kommt man durch ausprobieren auf $q = 4 - 3i = (2 + i)(1 - 2i)$. Da weder $2 + i$ noch $1 - 2i$ Einheiten sind, ist eine nichttriviale Zerlegung von q gefunden und q ist reduzibel (und damit auch nicht prim) in $\mathbb{Z}[i]$. □

h) $\frac{a}{b} = \frac{4+8i}{5+3i} = \frac{(4+8i)(5-3i)}{5^2+3^2} = \frac{44}{34} + \frac{38}{34}i \approx 1 + i$
$(1 + i)(5 + 3i) = 2 + 8i$, also:
$4 + 8i = (5 + 3i)(1 + i) + 2$, und damit: $r_1 = 2$.

$\frac{b}{r_1} = \frac{5+3i}{2} = \frac{5}{2} + \frac{3}{2}i \approx 2 + i$
$(2 + i) \cdot 2 = 4 + 2i$, also:

$5+3i = 2\cdot(2+i)+(1+i)$, und damit: $r_2 = 1+i$

$\frac{r_1}{r_2} = \frac{2}{1+i} = \frac{2(1-i)}{2} = 1-i$
$(1-i)(1+i) = 2$, also:
$2 = (1+i)(1-i)+0$, und damit: $r_3 = 0$

Also ist $d := 1+i$ ein ggT von a und b.

Es gilt: $d = 1\cdot(5+3i)-(2+i)\cdot 2$
$= 1\cdot(5+3i)-(2+i)(1\cdot(4+8i)-(1+i)\cdot(5+3i))$
$= (1+(2+i)(1+i))\cdot b+(-(2+i)\cdot 1)\cdot a$
$= (-2-i)\cdot a+(2+3i)\cdot b$

i) Da R jeweils ein Hauptidealring ist, finden wir jeweils einen einzigen Erzeuger. Dabei helfen uns folgende Eigenschaften von Hauptidealen (Aufpassen bei allgemeinen Idealen! Siehe Lösung von Aufgabe 4.1 b):
$(a)+(b) = (a,b) = (d)$, wenn d ein ggT von a und b ist.
$(a)\cdot(b) = (a\cdot b)$.
$(a)\cap(b) = (c)$, wenn c ein kgV von a und b ist.

i) Sei $R = \mathbb{Z}$, $I = (60,105)$ und $J = (51)$.
- Wegen $60 = 2^2\cdot 3\cdot 5$ und $105 = 3\cdot 5\cdot 7$ ist $d_1 = 3\cdot 5 = 15$ ein ggT von 60 und 105. Also $I = (60,105) = (15) = 15\mathbb{Z}$.
- $I+J = (15)+(51) = (15,51)$. Wegen $51 = 3\cdot 17$ ist $d_2 = 3$ ein ggT von 15 und 51. Also $I+J = (3) = 3\mathbb{Z}$.
- $I\cdot J = (15)\cdot(51) = (15\cdot 51) = (765)$.
- $I\cap J = (15)\cap(51)$. Wegen $15 = 3\cdot 5$ und $51 = 3\cdot 17$ ist $c = 3\cdot 5\cdot 17$ ein kgV von 15 und 51. Also $I\cap J = (3\cdot 5\cdot 17) = (255)$

ii) Sei $R = \mathbb{Z}$, $I = (120,15,99)$ und $J = (63)$.
- Wegen $120 = 2^3\cdot 3\cdot 5$, $15 = 3\cdot 5$ und $99 = 3^2\cdot 11$ ist $d_1 = 3$ ein ggT von 120, 15 und 99. Also $I = (120,15,99) = (3)$.
- $I+J = (3)+(63) = (3,63)$. Wegen $63 = 3^2\cdot 7$ ist $d_2 = 3$ ein ggT von 3 und 63. Also $I+J = (3)$.
- $I\cdot J = (3)\cdot(63) = (3\cdot 63) = (189)$.
- $I\cap J = (3)\cap(63)$. Wegen $63 = 3^2\cdot 7$ ist $c = 3^2\cdot 7$ ein kgV von 3 und 63. Also $I\cap J = (3^2\cdot 7) = (63)$

iii) Sei $R = \mathbb{Q}[t]$, $I = (t+1)$ und $J = \left((t+1)^3\right)$.
- $I+J = (t+1)+\left((t+1)^3\right) = \left(t+1,(t+1)^3\right)$. Offensichtlich ist $t+1$ ein ggT von $t+1$ und $(t+1)^3$. Also $I+J = (t+1) = I$.
- $I\cdot J = (t+1)\cdot\left((t+1)^3\right) = \left((t+1)\cdot(t+1)^3\right) = \left((t+1)^4\right)$.
- $I\cap J = (t+1)\cap\left((t+1)^3\right)$. Offensichtlich ist $(t+1)^3$ ein kgV von $t+1$ und $(t+1)^3$. Also $I\cap J = \left((t+1)^3\right) = J$.

j) Sei $p\in R$ ein Primelement des Integritätsrings R.
1. Teil:
ZZ: pR ist ein Primideal von R, also für $a,b\in R$ mit $ab\in pR$ folgt $a\in pR$ oder $b\in pR$.
Seien $a,b\in R$ mit $ab\in pR$. Dann ist $p|ab$. Es gilt, da p prim ist: $p|a$ oder $p|b$. Also folgt $a\in pR$ oder $b\in pR$.
2. Teil:
ZZ: Ist R ein Hauptidealring, so ist pR ein maximales Ideal, also für ein Ideal J mit $pR\subsetneq J\subseteq R$ folgt $J = R$.
Sei J ein Ideal von R mit $pR\subsetneq J$. Sei $a\in J\backslash pR$. Da $p\in pR$, ist auch $p\in J$. Es folgt $pR+aR\subseteq J$. Da R ein Hauptidealring ist, existiert ein ggT d von p und a, sodass $pR+aR = dR$.
ZZ: $d\in R^*$
Angenommen $d\notin R^*$. Dann gäbe es einen nichttrivialen gemeinsamen Teiler von p und a. Durch die Eindeutigkeit der Primfaktorzerlegung folgt damit $p|a$. (wieso?) Damit wäre aber $a\in pR$, was einen Widerspruch ergibt.
Es gilt also $d\in R^*$ und somit $dR = R$, also folgt $J = R$. □

Aufgabe 4 (Restklassenringe)

a) Sei R ein Integritätsring und $a,b\in R$. Zeigen Sie: $b|a \Leftrightarrow \overline{a} = \overline{0}$ in R/bR.

b) Wie viele Elemente hat $\mathbb{F}_2[t]/\left(t^3+t+1\right)\mathbb{F}_2[t]$?

c) Sei R ein Integritätsring und I ein Ideal von R. Wann ist R/I ein Integritätsring und wann ist R/I ein Körper?

d) Konstruieren Sie einen Körper mit genau 16 (oder 4, 27, 125, etc.) Elementen.

e) Zeigen Sie: Existiert ein Ringhomomorphismus $\varphi:\mathbb{Z}/m\mathbb{Z}\to R$, so gilt $m\cdot 1_R = 0_R$ in R.

f) Zeigen Sie: Es existiert genau dann ein Ringhomomorphismus $\varphi:\mathbb{Z}/m\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$, wenn $n|m$ in $\mathbb{Z}$. Geben sie diesen Ringhomomorphismus explizit an.

g) Zeigen Sie: In $\mathbb{Z}/6\mathbb{Z}$ erfüllen alle Elemente α die Gleichung $\alpha^3 = \alpha$.
Also hat das Polynom $f = t^3 - t \in (\mathbb{Z}/6\mathbb{Z})[t]$ 6 Nullstellen. Überlegen Sie: Hat f dann 6 verschiedene Linearfaktoren?

h) Sei $\alpha = \sqrt{2}$. Zeigen Sie mithilfe des Homomorphiesatzes, dass $\mathbb{Z}[\alpha] \cong \mathbb{Z}[t]/\left(t^2-2\right)\mathbb{Z}[t]$.

Lösung:

a) Sei R ein Integritätsring und $a, b \in R$.
ZZ: $b|a \Leftrightarrow \overline{a} = \overline{0}$ in R/bR.
„$\Rightarrow$“
Gelte $b|a$ in R. Dann ist $a \in bR$ und somit $\overline{a} = a + bR = bR = \overline{0}$.
„$\Leftarrow$“
Gelte $\overline{a} = \overline{0}$ in R/bR. Dann ist $a + bR = 0 + bR = bR$. Also folgt $a \in bR$ (wieso?) und somit $b|a$ in R. □

b) $f := t^3+t+1$ ist ein Polynom dritten Grades. Folglich (ohne überprüfen zu müssen, ob f irreduzibel ist) bilden alle möglichen Polynome niedrigeren Grades ein Vertretersystem des Restklassenrings $R = \mathbb{F}_2[t]/(f)$. Also hat R 8 Elemente, da es für jeden der drei möglichen Koeffizienten eines Polynoms des Vertretersystems genau 2 Möglichkeiten gibt, insgesamt also $2^3 = 8$ mögliche Polynome.

c) Aus der Vorlesung ist bekannt: Ist R ein Integritätsring und $I \subseteq R$ ein Ideal von R, so ist

- R/I ein Integritätsring, genau dann, wenn I ein Primideal von R ist.
- R/I ein Körper, genau dann, wenn I ein maximales Ideal von R ist.

Im Fall, dass R ein Hauptidealring ist, sind beide Eigenschaften äquivalent.

d) Idee: Finde ein irreduzibles Polynom $f \in \mathbb{F}_p[t]$ vom Grad $\deg(f) = n$, sodass man einen Körper mit p^n Elementen konstruieren kann: $\mathbb{F}_p[t]/(f)$.
Zunächst stellt man sicher, dass es sich um einen Körper handelt:
Da$\mathbb{F}_p$ Körper, ist $\mathbb{F}_p[t]$ ein Hauptidealring. Also ist $\mathbb{F}_p[t]/I$ ein Körper, sobald I ein Primideal von $\mathbb{F}_p[t]$ ist. Da f irreduzibel ist, ist (f) ein Primideal von $\mathbb{F}_p[t]$. Damit ist $\mathbb{F}_p[t]/(f)$ ein Körper. Nach Vorlesung hat $\mathbb{F}_p[t]/(f)$ genau $p^{\deg(f)}$ Elemente.

- Für $16 = 2^4$ Elemente suchen wir uns ein irreduzibles Polynom $f_{16} \in \mathbb{F}_2[t]$ mit $\deg(f_{16}) = 4$. Zum Beispiel eignet sich da $f_{16} := t^4+t^3+t^2+t+1$. Dieses Polynom ist nach Übungsaufgaben irreduzibel und $K_{16} := \mathbb{F}_2[t]/(f_{16})$ ist ein Körper mit 16 Elementen.
- Für $4 = 2^2$ Elemente gehen wir ähnlich vor: $f_4 := t^2 + t + 1$ ist irreduzibel über $\mathbb{F}_2$ und es folgt $K_4 := \mathbb{F}_2[t]/(f)$ ist ein Körper mit 4 Elementen.
- Für $27 = 3^3$ Elemente suchen wir uns ein irreduzibles Polynom $f_{27} \in \mathbb{F}_3[t]$ mit $\deg(f_{27}) = 3$. $f_{27} := t^3+2t+2$ ist irreduzibel in $\mathbb{F}_3[t]$, da es keine Nullstellen in $\mathbb{F}_3$ hat. Polynome vom Grad 2 oder 3 über einem Körper sind genau dann reduzibel, wenn es eine Nullstelle gibt. Also ist $K_{27} := \mathbb{F}_3[t]/(f_{27})$ ein Körper mit 27 Elementen.
- Für $125 = 5^3$ Elemente suchen wir uns ein irreduzibles Polynom $f_{125} \in \mathbb{F}_5[t]$ mit $\deg(f_{125}) = 3$. $f_{125} := t^3 + t^2 + 1$ ist irreduzibel in $\mathbb{F}_5[t]$, da es keine Nullstellen in $\mathbb{F}_5$ hat. Polynome vom Grad 2 oder 3 über einem Körper sind genau dann reduzibel, wenn es eine Nullstelle gibt. Also ist $K_{125} := \mathbb{F}_5[t]/(f_{125})$ ein Körper mit 125 Elementen.

e) Sei R ein Ring. Sei $\varphi : \mathbb{Z}/m\mathbb{Z} \to R$ ein Ringhomomorphismus.
ZZ: $m \cdot 1_R = 0_R$.
Es gilt: $m \cdot 1_R = m \cdot \varphi(1_{\mathbb{Z}/m\mathbb{Z}}) = \varphi(m \cdot 1_{\mathbb{Z}/m\mathbb{Z}}) = \varphi(0_{\mathbb{Z}/m\mathbb{Z}}) = 0_R$. □

f) ZZ: Es existiert genau dann ein Ringhomomorphismus $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, wenn $n|m$ in $\mathbb{Z}$.
„$\Leftarrow$“
Gelte $n|m$. Dann ist für alle $x \in a + m\mathbb{Z}$: $x \in a + n\mathbb{Z}$. Damit ist $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ mit $a + m\mathbb{Z} \mapsto a + n\mathbb{Z}$ wohldefiniert. (wieso?)
φ ist der kanonische Ringhomomorphismus; die Homomorphismus-Eigenschaften lassen sich leicht nachprüfen. (wie?)
Bemerkung: Natürlich muss φ nicht injektiv sein, es kann also auch für $a, b \in \mathbb{Z}$ mit $a+m\mathbb{Z} \neq b+m\mathbb{Z}$ gelten: $\varphi(a+m\mathbb{Z}) = a+n\mathbb{Z} = b+n\mathbb{Z} = \varphi(b+m\mathbb{Z})$.
„$\Rightarrow$“
Sei $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ein Ringhomomorphismus. Wegen e) folgt somit $m \cdot 1_{\mathbb{Z}/n\mathbb{Z}} = 0_{\mathbb{Z}/n\mathbb{Z}}$. Mit anderen Worten: $\overline{m} = \overline{0}$ in $\mathbb{Z}/n\mathbb{Z}$, also $n|m$. □

g) Im Ring $\mathbb{Z}/6\mathbb{Z}$ betrachten wir:
$\overline{0}^3 = \overline{0^3} = \overline{0}$ ✓
$\overline{1}^3 = \overline{1^3} = \overline{1}$ ✓
$\overline{2}^3 = \overline{2^3} = \overline{8} = \overline{2}$ ✓
$\overline{3}^3 = \overline{3^3} = \overline{27} = \overline{3}$ ✓

$\overline{4}^3 = \overline{4^3} = \overline{64} = \overline{4}$ ✓
$\overline{5}^3 = \overline{5^3} = \overline{125} = \overline{5}$ ✓
Alternativ könnte man auch $\overline{4} = \overline{-2}$ und $\overline{5} = \overline{-1}$ benutzen.
Durch Polynomdivision erhält man in $(\mathbb{Z}/6\mathbb{Z})[t]$:
$t^3 - t = (t - \overline{0}) \cdot (t^2 - \overline{1})$
$t^3 - t = (t - \overline{1}) \cdot (t^2 + t)$
$t^3 - t = (t - \overline{2}) \cdot (t^2 + \overline{2}t + \overline{3})$
$t^3 - t = (t - \overline{3}) \cdot (t^2 + \overline{3}t + \overline{2})$
$t^3 - t = (t - \overline{4}) \cdot (t^2 + \overline{4}t + \overline{3})$
$t^3 - t = (t - \overline{5}) \cdot (t^2 + \overline{5}t)$
Auch hier kann man alternativ Addition durch Subtraktion und umgekehrt ersetzen, sodass gleiche Ergebnisse unterschiedlich aussehen können.
Also ja, man kann $t^3 - t$ als Produkt jedes der sechs Linearfaktoren und eines entsprechenden Faktors darstellen. Die Frage, warum nicht das Produkt aller Linearfaktoren $t^3 - t$ teilt, lässt sich dadurch beantworten, dass $(\mathbb{Z}/6\mathbb{Z})[t]$ nicht faktoriell ist. Da $\mathbb{Z}/6\mathbb{Z}$ nicht faktoriell ist, weil es insbesondere kein Integritätsring ist $(\overline{2} \cdot \overline{3} = \overline{0})$, ist auch $(\mathbb{Z}/6\mathbb{Z})[t]$ nicht faktoriell. Insbesondere muss es für einige Elemente keine bis auf Assoziiertheit eindeutige Faktorisierung in irreduzible Elemente geben. Insbesondere gibt es für $t^3 - t$ keine eindeutige „Primfaktorzerlegung“ und die Linearfaktoren, die aufgrund ihres Grades und ihrer Normiertheit irreduzibel sind, sind keine Primelemente, da sie allesamt $t^3 - t$ teilen, aber nicht unbedingt in unterschiedlichen Zerlegungen auftreten.

h) Sei $\alpha = \sqrt{2}$.
ZZ: $\mathbb{Z}[\alpha] \cong \mathbb{Z}[t]/(t^2 - 2)\mathbb{Z}[t]$
Um den Homomorphiesatz anzuwenden zeigen wir: Es gibt einen Ringhomomorphismus $\Psi : \mathbb{Z}[t] \to \mathbb{Z}[\alpha]$, sodass $\mathrm{im}(\Psi) = \mathbb{Z}[\alpha]$ und $\ker(\Psi) = (t^2 - 2)\mathbb{Z}[t]$.
Definiere $\Psi_\alpha : \mathbb{Z}[t] \to \mathbb{Z}[\alpha]$ den Einsetzungshomomorphismus. Dann ist $\mathrm{im}(\Psi_\alpha) = \mathbb{Z}[\alpha]$ nach Definition von $\mathbb{Z}[\alpha]$.
Um zu zeigen, dass $\ker(\Psi_\alpha) = (t^2 - 2)\mathbb{Z}[t]$, führen wir eine Mengeninklusion durch.
„$\supseteq$“ zeigt man leicht. (wie?)
„$\subseteq$“
Sei $g \in \ker(\Psi_\alpha)$. Dann ist $g(\alpha) = 0$. Da das Polynom $t^2 - 2$ normiert ist, können wir Division mit Rest durchführen, obwohl $\mathbb{Z}[t]$ kein euklidischer Ring ist. Wir bestimmen also $q, r \in \mathbb{Z}[t]$, sodass $g = q \cdot (t^2 - 2) + r$, wobei $r = 0$ oder $\deg(r) < \deg(t^2 - 2) = 2$.
Wegen $g(\alpha) = 0$ ist $r(\alpha) = 0$.
Angenommen $\deg(r) = 1$. Dann wäre $a_0 + a_1\alpha = 0$ für $a_0, a_1 \in \mathbb{Z}$ und $a_1 \neq 0$. Da $\sqrt{2} \notin \mathbb{Q}$, dem Quotientenkörper von $\mathbb{Z}$, ist $a_1\alpha \notin \mathbb{Z}$. (wieso?)
Also ist $\deg(r) < 1$.
Den Fall $\deg(r) = 0$ schließt man leicht aus (wie?) und somit ist $r = 0$.
Dadurch ergibt sich $(t^2 - 2) | g$, also $\ker(\Psi_\alpha) \subseteq (t^2 - 2)\mathbb{Z}[t]$. □

Aufgabe 5 (Chinesischer Restsatz)

a) Berechnen Sie alle ganzen Zahlen x, die die folgenden Kongruenzen lösen:

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 6 \mod 7 \\ x &\equiv 10 \mod 17 \end{aligned}$$

b) Berechnen Sie alle ganzen Zahlen x, die die folgenden Kongruenzen lösen. Vorsicht, hier sind nicht alle Moduln teilerfremd! Wie kann man dieses Problem lösen?

$$\begin{aligned} x &\equiv 5 \mod 15 \\ x &\equiv 2 \mod 3 \\ x &\equiv 15 \mod 23 \\ (*)\quad x &\equiv 11 \mod 21 \end{aligned}$$

Die letzte Kongruenz soll als Zusatzaufgabe hinzugenommen werden. Auch hier ist das Problem die fehlende Teilerfremdheit der Moduln. Ist das Kongruenzsystem dann überhaupt noch lösbar?

c) Berechnen Sie alle Polynome $f \in \mathbb{R}[t]$, die die folgenden Kongruenzen lösen:

$$\begin{aligned} f &\equiv 3t - 1 \mod (t^2 + 2t + 1) \\ f &\equiv -t + 1 \mod (t^2 - 3t - 2) \end{aligned}$$

d) (Nicht klausurrelevant!) Berechnen Sie alle Zahlen $z \in \mathbb{Z}[i]$, die die folgenden Kongruenzen lösen:

$$\begin{aligned} z &\equiv 2 - i \mod 2 + 4i \\ z &\equiv -1 - i \mod 2 + i \\ z &\equiv 2 + 3i \mod 5 + 4i \end{aligned}$$

Lösung: Die Lösungsskizze zu dieser Aufgabe ist mit einer anderen Notation aufgeschrieben, als sie in diesem Semester vorgestellt wurde.

a) Da $\mathrm{ggT}(3,7) = \mathrm{ggT}(7,17) = \mathrm{ggT}(3,17) = 1$ in $\mathbb{Z}$, ist der chinesische Restsatz anwendbar und das oben stehende Kongruenzsystem ist in $\mathbb{Z}$ lösbar.

1. Schritt:

i) Suche $y_1 \in \mathbb{Z}$, das die folgenden Kongruenzen löst:

$$\begin{aligned} y_1 &\equiv 1 \mod 3 \\ y_1 &\equiv 0 \mod 7 \\ y_1 &\equiv 0 \mod 17 \end{aligned}$$

Also $7 \cdot 17 | y_1$. Schreibe $y_1 = 7 \cdot 17 \cdot k_1$. Wir suchen also ein $k_1 \in \mathbb{Z}$, welches die folgende Kongruenz löst:

$$\begin{aligned} & 7 \cdot 17 \cdot k_1 \equiv 1 \mod 3 \\ \Leftrightarrow \quad & 1 \cdot 2 \cdot k_1 \equiv 1 \mod 3 \end{aligned}$$

Man erkennt: $k_1 = 2$ ist eine Lösung. Also ist $y_1 = 7 \cdot 17 \cdot 2 = 238$.

ii) Suche $y_2 \in \mathbb{Z}$, das die folgenden Kongruenzen löst:

$$\begin{aligned} y_2 &\equiv 0 \mod 3 \\ y_2 &\equiv 1 \mod 7 \\ y_2 &\equiv 0 \mod 17 \end{aligned}$$

Also $3 \cdot 17 | y_2$. Schreibe $y_2 = 3 \cdot 17 \cdot k_2$. Wir suchen also ein $k_2 \in \mathbb{Z}$, welches die folgende Kongruenz löst:

$$\begin{aligned} & 3 \cdot 17 \cdot k_2 \equiv 1 \mod 7 \\ \Leftrightarrow \quad & 2 \cdot k_2 \equiv 1 \mod 7 \end{aligned}$$

Man erkennt: $k_2 = 4$ ist eine Lösung. Also ist $y_2 = 3 \cdot 17 \cdot 4 = 204$.

iii) Suche $y_3 \in \mathbb{Z}$, das die folgenden Kongruenzen löst:

$$\begin{aligned} y_3 &\equiv 0 \mod 3 \\ y_3 &\equiv 0 \mod 7 \\ y_3 &\equiv 1 \mod 17 \end{aligned}$$

Also $3 \cdot 7 | y_3$. Schreibe $y_3 = 3 \cdot 7 \cdot k_3$. Wir suchen also ein $k_3 \in \mathbb{Z}$, welches die folgende Kongruenz löst:

$$\begin{aligned} & 3 \cdot 7 \cdot k_3 \equiv 1 \mod 17 \\ \Leftrightarrow \quad & 4 \cdot k_3 \equiv 1 \mod 17 \end{aligned}$$

Man erkennt: $k_3 = 13$ ist eine Lösung. Also ist $y_3 = 3 \cdot 7 \cdot 13 = 273$.

2. Schritt:
Setze $x_0 := 1 \cdot y_1 + 6 \cdot y_2 + 10 \cdot y_3 = 1 \cdot 238 + 6 \cdot 204 + 10 \cdot 273 = 4192$. Dann löst x_0 das in der Aufgabe stehende Kongruenzsystem.

3. Schritt:
Die gesamte Lösungsmenge L des Kongruenzsystems ist: $L = x_0 + \mathrm{kgV}(3,7,17)\mathbb{Z} = 4192 + (3 \cdot 7 \cdot 17)\mathbb{Z} = 4192 + 357\mathbb{Z}$. □

b) Der chinesische Restsatz ist nicht unmittelbar anwendbar, da die verschiedenen Moduln nicht paarweise teilerfremd sind. Um das System zu lösen bedienen wir uns eines Tricks für p und q teilerfremd: $a \equiv b \mod (pq) \Leftrightarrow a \equiv b \mod p$ und $a \equiv b \mod q$. (wieso?)

• Ohne $(*)$:
Wir können das Kongruenzsystem aus der Aufgabe wie folgt umschreiben:

$$\begin{aligned} x &\equiv 5 \equiv 2 \mod 3 \\ x &\equiv 5 \equiv 0 \mod 5 \\ x &\equiv 2 \mod 3 \\ x &\equiv 15 \mod 23 \end{aligned}$$

Da sich die nun entstandenen Kongruenzen nicht gegenseitig ausschließen, sondern zum Teil identisch sind, ist nun der chinesische Restsatz für das Kongruenzsystem

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 0 \mod 5 \\ x &\equiv 15 \mod 23 \end{aligned}$$

anwendbar, da dort alle Moduln paarweise teilerfremd sind: $\mathrm{ggT}(3,5) = \mathrm{ggT}(5,23) =$

$\mathrm{ggT}(3, 23) = 1$.

1. Schritt:

i) Suche $y_1 \in \mathbb{Z}$, das die folgenden Kongruenzen löst:

$$\begin{aligned} y_1 &\equiv 1 \mod 3 \\ y_1 &\equiv 0 \mod 5 \\ y_1 &\equiv 0 \mod 23 \end{aligned}$$

Also $5 \cdot 23 | y_1$. Schreibe $y_1 = 5 \cdot 23 \cdot k_1$. Wir suchen also ein $k_1 \in \mathbb{Z}$, welches die folgende Kongruenz löst:

$$\begin{aligned} & 5 \cdot 23 \cdot k_1 \equiv 1 \mod 3 \\ \Leftrightarrow \quad & 2 \cdot 2 \cdot k_1 \equiv 1 \mod 3 \end{aligned}$$

Man erkennt: $k_1 = 1$ ist eine Lösung. Also ist $y_1 = 5 \cdot 23 \cdot 1 = 115$.

ii) Suche $y_2 \in \mathbb{Z}$, das die folgenden Kongruenzen löst:

$$\begin{aligned} y_2 &\equiv 0 \mod 3 \\ y_2 &\equiv 1 \mod 5 \\ y_2 &\equiv 0 \mod 23 \end{aligned}$$

Also $3 \cdot 23 | y_2$. Schreibe $y_2 = 3 \cdot 23 \cdot k_2$. Wir suchen also ein $k_2 \in \mathbb{Z}$, welches die folgende Kongruenz löst:

$$\begin{aligned} & 3 \cdot 23 \cdot k_2 \equiv 1 \mod 5 \\ \Leftrightarrow \quad & 4 \cdot k_2 \equiv 1 \mod 5 \end{aligned}$$

Man erkennt: $k_2 = 4$ ist eine Lösung. Also ist $y_2 = 3 \cdot 23 \cdot 4 = 276$.

iii) Suche $y_3 \in \mathbb{Z}$, das die folgenden Kongruenzen löst:

$$\begin{aligned} y_3 &\equiv 0 \mod 3 \\ y_3 &\equiv 0 \mod 5 \\ y_3 &\equiv 1 \mod 23 \end{aligned}$$

Also $3 \cdot 5 | y_3$. Schreibe $y_3 = 3 \cdot 5 \cdot k_3$. Wir suchen also ein $k_3 \in \mathbb{Z}$, welches die folgende Kongruenz löst:

$$\begin{aligned} & 3 \cdot 5 \cdot k_3 \equiv 1 \mod 23 \\ \Leftrightarrow \quad & 15 \cdot k_3 \equiv 1 \mod 23 \end{aligned}$$

Da $\mathrm{ggT}(15, 23) = 1$ findet man mit dem erweiterten euklidischen Algorithmus $k_3, z_3 \in \mathbb{Z}$, sodass $k_3 \cdot 15 + z_3 \cdot 23 = 1$.
Es gilt:

$$\begin{aligned} 23 &= 1 \cdot 15 + 8 \\ 15 &= 1 \cdot 8 + 7 \\ 8 &= 1 \cdot 7 + 1 \text{ , also:} \\ 1 &= 8 - 7 = 8 - (15 - 8) = 2 \cdot 8 - 15 \\ &= 2 \cdot (23 - 15) - 15 = 2 \cdot 23 - 3 \cdot 15 \end{aligned}$$

Also ist $k_3 = -3$ und $z_3 = 2$, wobei z_3 uninteressant ist. Das gefundene k_3 löst die obenstehende Kongruenz und somit ist $y_3 = 3 \cdot 5 \cdot -3 = -45$.

2. Schritt:
Setze $x_0 := 2 \cdot y_1 + 0 \cdot y_2 + 15 \cdot y_3 = 2 \cdot 115 + 0 \cdot 276 + 15 \cdot -45 = -445$. Dann löst x_0 das in der Aufgabe stehende Kongruenzsystem.

3. Schritt:
Die gesamte Lösungsmenge L des Kongruenzsystems ist: $L = x_0 + \mathrm{kgV}(3, 5, 23)\mathbb{Z} = -445 + (3 \cdot 5 \cdot 23)\mathbb{Z} = -445 + 345\mathbb{Z}$.

• Mit $(*)$:
Wir können das Kongruenzsystem aus der Aufgabe wie folgt umschreiben:

$$\begin{aligned} x &\equiv 5 \equiv 2 \mod 3 \\ x &\equiv 5 \equiv 0 \mod 5 \\ x &\equiv 2 \mod 3 \\ x &\equiv 15 \mod 23 \\ x &\equiv 11 \equiv 2 \mod 3 \\ x &\equiv 11 \equiv 4 \mod 7 \end{aligned}$$

Da sich die nun entstandenen Kongruenzen nicht gegenseitig ausschließen, sondern zum Teil identisch sind, ist nun der chinesische Restsatz für das Kongruenzsystem

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 0 \mod 5 \\ x &\equiv 15 \mod 23 \\ x &\equiv 4 \mod 7 \end{aligned}$$

anwendbar, da dort alle Moduln paarweise teilerfremd sind: $\mathrm{ggT}(3, 5) = \mathrm{ggT}(5, 23) = \mathrm{ggT}(3, 23) = \mathrm{ggT}(3, 7) = \mathrm{ggT}(5, 7) = \mathrm{ggT}(7, 23) = 1$.

1. Schritt:

i) Suche $y_1 \in \mathbb{Z}$, das die folgenden Kongruenzen löst:

$$\begin{aligned} y_1 &\equiv 1 \mod 3 \\ y_1 &\equiv 0 \mod 5 \\ y_1 &\equiv 0 \mod 23 \\ y_1 &\equiv 0 \mod 7 \end{aligned}$$

Also $5 \cdot 23 \cdot 7 | y_1$. Schreibe $y_1 = 5 \cdot 23 \cdot 7 \cdot k_1$. Wir suchen also ein $k_1 \in \mathbb{Z}$, welches die folgende Kongruenz löst:

$$\begin{aligned} & 5 \cdot 23 \cdot 7 \cdot k_1 \equiv 1 \mod 3 \\ \Leftrightarrow \quad & 2 \cdot 2 \cdot 1 \cdot k_1 \equiv 1 \mod 3 \end{aligned}$$

Man erkennt: $k_1 = 1$ ist eine Lösung. Also ist $y_1 = 5 \cdot 23 \cdot 7 \cdot 1 = 805$.

ii) Suche $y_2 \in \mathbb{Z}$, das die folgenden Kongruenzen löst:

$$\begin{aligned} y_2 &\equiv 0 \mod 3 \\ y_2 &\equiv 1 \mod 5 \\ y_2 &\equiv 0 \mod 23 \\ y_2 &\equiv 0 \mod 7 \end{aligned}$$

Also $3 \cdot 23 \cdot 7 | y_2$. Schreibe $y_2 = 3 \cdot 23 \cdot 7 \cdot k_2$. Wir suchen also ein $k_2 \in \mathbb{Z}$, welches die folgende Kongruenz löst:

$$\begin{aligned} 3 \cdot 23 \cdot 7 \cdot k_2 &\equiv 1 \mod 5 \\ \Leftrightarrow \quad 3 \cdot k_2 &\equiv 1 \mod 5 \end{aligned}$$

Man erkennt: $k_2 = 2$ ist eine Lösung. Also ist $y_2 = 3 \cdot 23 \cdot 7 \cdot 2 = 966$.

iii) Suche $y_3 \in \mathbb{Z}$, das die folgenden Kongruenzen löst:

$$\begin{aligned} y_3 &\equiv 0 \mod 3 \\ y_3 &\equiv 0 \mod 5 \\ y_3 &\equiv 1 \mod 23 \\ y_3 &\equiv 0 \mod 7 \end{aligned}$$

Also $3 \cdot 5 \cdot 7 | y_3$. Schreibe $y_3 = 3 \cdot 5 \cdot 7 \cdot k_3$. Wir suchen also ein $k_3 \in \mathbb{Z}$, welches die folgende Kongruenz löst:

$$\begin{aligned} 3 \cdot 5 \cdot 7 \cdot k_3 &\equiv 1 \mod 23 \\ \Leftrightarrow \quad 13 \cdot k_3 &\equiv 1 \mod 23 \end{aligned}$$

Da $\mathrm{ggT}(13, 23) = 1$ findet man mit dem erweiterten euklidischen Algorithmus $k_3, z_3 \in \mathbb{Z}$, sodass $k_3 \cdot 15 + z_3 \cdot 23 = 1$.
Es gilt:

$$\begin{aligned} 23 &= 1 \cdot 13 + 10 \\ 13 &= 1 \cdot 10 + 3 \\ 10 &= 3 \cdot 3 + 1 \text{ , also:} \\ 1 &= 10 - 3 \cdot 3 = 10 - 3 \cdot (13 - 10) \\ &= 4 \cdot 10 - 3 \cdot 13 = 4 \cdot (23 - 13) - 3 \cdot 13 \\ &= 4 \cdot 23 - 7 \cdot 13 \end{aligned}$$

Also ist $k_3 = -7$ und $z_3 = 4$, wobei z_3 uninteressant ist. Das gefundene k_3 löst die obenstehende Kongruenz und somit ist $y_3 = 3 \cdot 5 \cdot 7 \cdot -7 = -735$.

iv) Suche $y_4 \in \mathbb{Z}$, das die folgenden Kongruenzen löst:

$$\begin{aligned} y_4 &\equiv 0 \mod 3 \\ y_4 &\equiv 0 \mod 5 \\ y_4 &\equiv 0 \mod 23 \\ y_4 &\equiv 1 \mod 7 \end{aligned}$$

Also $3 \cdot 5 \cdot 23 | y_4$. Schreibe $y_4 = 3 \cdot 5 \cdot 23 \cdot k_4$. Wir suchen also ein $k_4 \in \mathbb{Z}$, welches die folgende Kongruenz löst:

$$\begin{aligned} 3 \cdot 5 \cdot 23 \cdot k_4 &\equiv 1 \mod 7 \\ \Leftrightarrow \quad 2 \cdot k_4 &\equiv 1 \mod 7 \end{aligned}$$

Man erkennt: $k_4 = 4$ ist eine Lösung. Also ist $y_4 = 3 \cdot 5 \cdot 23 \cdot 4 = 1380$.

2. Schritt:
Setze $x_0 := 2 \cdot y_1 + 0 \cdot y_2 + 15 \cdot y_3 + 4 \cdot y_4 = 2 \cdot 805 + 0 \cdot 966 + 15 \cdot -735 + 4 \cdot 1380 = -3895$. Dann löst x_0 das in der Aufgabe stehende Kongruenzsystem.

3. Schritt:
Die gesamte Lösungsmenge L des Kongruenzsystems ist: $L = x_0 + \mathrm{kgV}(3, 5, 23, 7)\mathbb{Z} = -3895 + (3 \cdot 5 \cdot 23 \cdot 7)\mathbb{Z} = -3895 + 2415\mathbb{Z}$. □

c) Um zu sehen, ob der chinesische Restsatz unmittelbar anwendbar ist, müssen wir vorher die Teilerfremdheit der beiden Moduln überprüfen. Schaue also, ob 1 ein ggT von $t^2 + 2t + 1$ und $t^2 - 3t - 2$ ist. Dazu führe Polynomdivision durch:

$$\begin{aligned} t^2 - 3t - 2 &= (t^2 + 2t + 1) \cdot (1) + (-5t - 3) \\ t^2 + 2t + 1 &= (-5t - 3) \cdot \left(-\frac{1}{5}t - \frac{7}{25}\right) + \left(\frac{4}{25}\right) \end{aligned}$$

Weil $1 \sim \frac{4}{25}$ in $\mathbb{R}[t]$ ist 1 ein ggT der beiden Moduln. Also ist das Kongruenzsystem lösbar und der chinesische Restsatz anwendbar. Da wir das später noch brauchen, führen wir jetzt schon einmal den erweiterten euklidischen Algorithmus durch:

$$\begin{aligned} 1 &= \frac{25}{4} \cdot \left((t^2 + 2t + 1) + \left(\frac{1}{5}t + \frac{7}{25}\right)(-5t - 3)\right) \\ &= \frac{25}{4} \cdot \Bigg((t^2 + 2t + 1) + \\ &\quad \left(\frac{1}{5}t + \frac{7}{25}\right)\left((t^2 - 3t - 2) - (t^2 + 2t + 1)\right)\Bigg) \\ &= \frac{1}{4}\left((-5t + 18)(t^2 + 2t + 1) + \right. \\ &\quad \left.(5t + 7)(t^2 - 3t - 2)\right) \end{aligned}$$

1. Schritt:

i) Suche $g_1 \in \mathbb{R}[t]$, das die folgenden Kongruenzen löst:

$$\begin{aligned} g_1 &\equiv 1 \mod t^2 + 2t + 1 \\ g_1 &\equiv 0 \mod t^2 - 3t - 2 \end{aligned}$$

Also $(t^2-3t-2)|g_1$. Schreibe $g_1 = (t^2-3t-2)\cdot k_1$. Wir suchen also ein $k_1 \in \mathbb{R}[t]$, welches die folgende Kongruenz löst:

$$(t^2-3t-2)\cdot k_1 \equiv 1 \mod t^2+2t+1$$

Da $\mathrm{ggT}(t^2-3t-2, t^2+2t+1) = 1$ findet man mit dem erweiterten euklidischen Algorithmus $k_1, z_1 \in \mathbb{R}[t]$, sodass $k_1\cdot(t^2-3t-2)+z_1\cdot(t^2+2t+1)=1$.
Nach obiger Rechnung ist $k_1 = \frac{1}{4}(5t+7)$ und $z_1 = \frac{1}{4}(-5t+18)$, wobei z_1 uninteressant ist. Das gefundene k_1 löst die obenstehende Kongruenz und somit ist $g_1 = (t^2-3t-2)\cdot\frac{1}{4}(5t+7) = \frac{1}{4}(5t^3-8t^2-31t-14)$.

ii) Suche $g_2 \in \mathbb{R}[t]$, das die folgenden Kongruenzen löst:

$$g_2 \equiv 0 \mod t^2+2t+1$$
$$g_2 \equiv 1 \mod t^2-3t-2$$

Also $(t^2+2t+1)|g_2$. Schreibe $y_2 = (t^2+2t+1)\cdot k_2$. Wir suchen also ein $k_2 \in \mathbb{R}[t]$, welches die folgende Kongruenz löst:

$$(t^2+2t+1)\cdot k_2 \equiv 1 \mod t^2-3t-2$$

Da $\mathrm{ggT}(t^2+2t+1, t^2-3t-2) = 1$ findet man mit dem erweiterten euklidischen Algorithmus $k_2, z_2 \in \mathbb{R}[t]$, sodass $k_2\cdot(t^2+2t+1)+z_2\cdot(t^2-3t-2)=1$.
Nach obiger Rechnung ist $k_2 = \frac{1}{4}(-5t+18)$ und $z_2 = \frac{1}{4}(5t+7)$, wobei z_2 uninteressant ist. Das gefundene k_2 löst die obenstehende Kongruenz und somit ist $g_2 = (t^2+2t+1)\cdot\frac{1}{4}(-5t+18) = \frac{1}{4}(-5t^3+8t^2+31t+18)$.

2. Schritt:
Setze $f_0 := (3t-1)\cdot g_1 + (-t+1)\cdot g_2 = (3t-1)\cdot\frac{1}{4}(5t^3-8t^2-31t-14)+(-t+1)\cdot\frac{1}{4}(-5t^3+8t^2+31t+18) = \frac{1}{4}\left(20t^4-42t^3-108t^2+2t+32\right) = \left(5t^4-\frac{21}{2}t^3-27t^2+\frac{1}{2}t+8\right)$. Dann löst f_0 das in der Aufgabe stehende Kongruenzsystem.

3. Schritt:
Die gesamte Lösungsmenge L des Kongruenzsystems ist: $L = f_0 + \mathrm{kgV}(t^2+2t+1, t^2-3t-2)\mathbb{R}[t] = f_0 + ((t^2+2t+1)\cdot(t^2-3t-2))\mathbb{R}[t] = f_0 + (t^4-t^3-7t^2-7t-2)\mathbb{R}[t]$.

d) Zunächst überprüfen wir die drei Moduln auf paarweise Teilerfremdheit, um zu sehen, ob der chinesische Restsatz anwendbar ist. Es gilt:

- $\frac{2+4i}{2+i} = \frac{(2+4i)(2-i)}{5} = \frac{8}{5}+\frac{6}{5}i \approx 2+i$
  $(2+i)(2+i) = 3+4i$, also:
  $2+4i = (2+i)(2+i)+(-1)$ und damit $r_1 = -1$.

  $\frac{2+i}{-1} = -2-i$
  $(-1)(-2-i) = 2+i$, also:
  $2+i = (-2-i)(-1)+0$ und damit $r_2 = 0$.

  Also ist $r_1 = -1$ ein ggT von $(2+4i)$ und $(2+i)$. Weil $-1 \sim 1$ ist demnach auch 1 ein ggT und die beiden Moduln sind teilerfremd.
- $\frac{5+4i}{2+4i} = \frac{(5+4i)(2-4i)}{20} = \frac{26}{20}-\frac{12}{20}i \approx 1-i$
  $(2+4i)(1-i) = 6+2i$, also:
  $5+4i = (2+4i)(1-i)+(-1+2i)$ und damit $r_1 = -1+2i$.

  $\frac{2+4i}{-1+2i}\frac{(2+4i)(-1-2i)}{5} = \frac{6}{5}-\frac{8}{5}i \approx 1-2i$
  $(-1+2i)(1-2i) = 3+4i$, also:
  $2+4i = (-1+2i)(1-2i)+(-1)$ und damit $r_2 = -1$.

  $\frac{-1+2i}{-1} = 1-2i$
  $(-1)(1-2i) = -1+2i$, also:
  $-1+2i = (1-2i)(-1)+0$ und damit $r_3 = 0$.

  Also ist $r_2 = -1$ ein ggT von $(5+4i)$ und $(2+4i)$. Weil $-1 \sim 1$ ist demnach auch 1 ein ggT und die beiden Moduln sind teilerfremd.
- $\frac{5+4i}{2+i} = \frac{(5+4i)(2-i)}{5} = \frac{14}{5}+\frac{3}{5}i \approx 3+i$
  $(3+i)(2+i) = 5+5i$, also:
  $5+4i = (2+i)(3+i)+(-i)$ und damit $r_1 = -i$.

  $\frac{2+i}{-i} = (2+i)(i) = -1+2i$
  $(-i)(-1+2i) = 2+i$, also:
  $2+i = (-1+2i)(-i)+0$ und damit $r_2 = 0$.

  Also ist $r_1 = -i$ ein ggT von $(2+4i)$ und $(2+i)$. Weil $-i \sim 1$ ist demnach auch 1 ein ggT und die beiden Moduln sind teilerfremd.

Also ist der chinesische Restsatz anwendbar und das Kongruenzsystem ist lösbar.

1. Schritt:

i) Suche $y_1 \in \mathbb{Z}[i]$, das die folgenden Kongruenzen löst:

$$y_1 \equiv 1 \mod 2+4i$$
$$y_1 \equiv 0 \mod 2+i$$
$$y_1 \equiv 0 \mod 5+4i$$

Also $(2+i)\cdot(5+4i)|y_1$. Schreibe $y_1 = (2+i)\cdot(5+4i)\cdot k_1 = (6+13i)\cdot k_1$. Wir suchen also ein $k_1 \in \mathbb{Z}[i]$, welches die folgende Kongruenz löst:

$$(6+13i)\cdot k_1 \equiv 1 \mod 2+4i$$

Da $\mathrm{ggT}(6+13i, 2+4i) = 1$, findet man mit dem erweiterten euklidischen Algorithmus $k_1, x_1 \in \mathbb{Z}[i]$, sodass $k_1 \cdot (6+13i) + x_1 \cdot (2+4i) = 1$.
Es gilt:
$\frac{6+13i}{2+4i} = \frac{(6+13i)(2-4i)}{20} = \frac{64}{20} + \frac{2}{20}i \approx 3$
$(3)(2+4i) = 6+12i$, also:
$6+13i = (2+4i)(3) + i$ und damit $r_1 = i$.
Also folgt:
$1 = (-i)(i) = (-i)\cdot((6+13i) - 3(2+4i)) = (-i)(6+13i)+(3i)(2+4i)$. Also ist $k_1 = (-i)$ und $x_1 = 3i$. Das gefundene k_1 löst die Kongruenz und somit ist $y_1 = (6+13i)(-i) = 13-6i$

ii) Suche $y_2 \in \mathbb{Z}[i]$, das die folgenden Kongruenzen löst:

$$y_2 \equiv 0 \mod 2+4i$$
$$y_2 \equiv 1 \mod 2+i$$
$$y_2 \equiv 0 \mod 5+4i$$

Also $(2+4i)\cdot(5+4i) | y_2$. Schreibe $y_2 = (2+4i)\cdot(5+4i)\cdot k_2 = (-6+28i)\cdot k_2$. Wir suchen also ein $k_2 \in \mathbb{Z}[i]$, welches die folgende Kongruenz löst:

$$(-6+28i)\cdot k_2 \equiv 1 \mod 2+i$$

Da $\mathrm{ggT}(-6+28i, 2+i) = 1$, findet man mit dem erweiterten euklidischen Algorithmus $k_2, x_2 \in \mathbb{Z}[i]$, sodass $k_2\cdot(-6+28i) + x_2 \cdot (2+i) = 1$.
Es gilt:
$\frac{-6+28i}{2+i} = \frac{(-6+28i)(2-i)}{5} = \frac{16}{5} + \frac{62}{5}i \approx 3+12i$
$(3+12i)(2+i) = -6+27i$, also:
$-6+28i = (2+i)(3+12i) + i$ und damit $r_1 = i$.
Also folgt:
$1 = (-i)(i)$
$= (-i)\cdot((-6+28i) - (3+12i)(2+i))$
$= (-i)(-6+28i) + (-12+3i)(2+i)$. Also ist $k_2 = (-i)$ und $x_2 = (-12+3i)$. Das gefundene k_2 löst die Kongruenz und somit ist $y_2 = (-6+28i)(-i) = 28+6i$

iii) Suche $y_3 \in \mathbb{Z}[i]$, das die folgenden Kongruenzen löst:

$$y_3 \equiv 0 \mod 2+4i$$
$$y_3 \equiv 0 \mod 2+i$$
$$y_3 \equiv 1 \mod 5+4i$$

Also $(2+4i)\cdot(2+i) | y_3$. Schreibe $y_3 = (2+4i)\cdot(2+i)\cdot k_3 = (10i)\cdot k_3$. Wir suchen also ein $k_3 \in \mathbb{Z}[i]$, welches die folgende Kongruenz löst:

$$(10i)\cdot k_3 \equiv 1 \mod 5+4i$$

Da $\mathrm{ggT}(10i, 5+4i) = 1$, findet man mit dem erweiterten euklidischen Algorithmus $k_3, x_3 \in \mathbb{Z}[i]$, sodass $k_3\cdot(10i) + x_3\cdot(5+4i) = 1$.
Es gilt:
$\frac{10i}{5+4i} = \frac{(10i)(5-4i)}{41} = \frac{40}{41} + \frac{50}{41}i \approx 1+i$
$(1+i)(5+4i) = 1+9i$, also:
$10i = (5+4i)(1+i) + (-1+i)$ und damit $r_1 = -1+i$.

$\frac{5+4i}{-1+i} = \frac{(5+4i)(-1-i)}{2} = -\frac{1}{2} - \frac{9}{2}i \approx -1-4i$
$(-1-4i)(-1+i) = 5+3i$, also:
$5+4i = (-1+i)(-1-4i)+i$ und damit $r_2 = i$.

Also folgt:
$1 = (-i)(i)$
$= (-i)\cdot((5+4i) - (-1-4i)(-1+i))$
$= (-i)(5+4i) + (4-i)(-1+i)$
$= (-i)(5+4i)+(4-i)\,(10i - (1+i)(5+4i))$
$= (4-i)(10i) + ((4-i)(-1-i) - i)(5+4i)$
$= (4-i)(10i) + (-5-4i)(5+4i)$.
Also ist $k_3 = (4-i)$ und $x_3 = (-5-4i)$. Das gefundene k_3 löst die Kongruenz und somit ist $y_3 = (10i)(4-i) = 10+40i$

2.Schritt:
Setze $z_0 := (2-i)\cdot y_1 + (-1-i)\cdot y_2 + (2+3i)\cdot y_3$
$= (2-i)\cdot(13-6i) + (-1-i)\cdot(28+6i) + (2+3i)\cdot(10+40i)$
$= (20-25i) + (-22-34i) + (-100+110i)$
$= -102+51i$.
Dann löst z_0 das in der Aufgabe stehende Kongruenzsystem.

3.Schritt:
Die gesamte Lösungsmenge L des Kongruenzsystems ist: $L = z_0 + \mathrm{kgV}(2+4i, 2+i, 5+4i)\mathbb{Z}[i] = (-102+51i) + (2+4i)(2+i)(5+4i)\mathbb{Z}[i] = (-102+51i) + (-40+50i)\mathbb{Z}[i]$

Aufgabe 6 (Irreduzibilität)

a) Zeigen Sie, dass $f = t^6 + t^3 + 1$ in $\mathbb{Q}[t]$ irreduzibel ist.
Hinweis: Benutzen Sie das Transformationskriterium mit $c = 1$.

b) Zeigen Sie, dass $f = 12t^5 + 21t^3 + 28t^2 - 7t + 7$ in $\mathbb{Q}[t]$ irreduzibel ist.

c) Zeigen Sie per Gegenbeispiel, dass die Rückrichtung des Reduktionskriteriums nicht im Allgemeinen gilt. Geben Sie also ein Beispiel dafür an, dass über dem Integritätsring R ein Polynom $f \in R[t]$ irreduzibel ist, obwohl es ein Primelement $p \in R$ gibt, sodass $\overline{f} \in (R/pR)[t]$ reduzibel ist.

d) Zeigen Sie, dass $f = t^3 - 9t^2 + 27t - 34$ in $\mathbb{Q}[t]$ irreduzibel ist.
Hinweis: Benutzen Sie das Transformationskriterium mit $c = 3$.

e) Zeigen Sie, dass $f = t^4 + 2t^2 + 1$ reduzibel in $\mathbb{Z}[t]$ ist. Geben Sie eine nichttriviale Zerlegung von f an.

f) Zeigen Sie, dass $f = 27t^3 + 5t^2 - 10t - 3$ irreduzibel in $\mathbb{Q}[t]$ ist.

Lösung:

a) Sei $f = t^6 + t^3 + 1 \in \mathbb{Q}[t]$.
Nach dem Transformationskriterium ist f genau dann irreduzibel, wenn $f(t+1)$ irreduzibel in $\mathbb{Q}[t]$ ist. Betrachte $f(t+1)$ in $\mathbb{Z}[t]$.
Es gilt: $f(t+1) = t^6+6t^5+15t^4+21t^3+18t^2+9t+3$.
Da $3|3$, $3|9$, $3|18$, $3|21$, $3|15$, $3|6$ und $3 \nmid 1 = \mathrm{LK}(f(t+1))$ und $3^2 = 9 \nmid 3$ ist $f(t+1)$ nach dem Eisensteinkriterium mit $p = 3$ irreduzibel in $\mathbb{Z}[t]$, weil $f(t+1)$ normiert und damit auch primitiv ist. Weil $\mathbb{Q} = Q(\mathbb{Z})$ ist f demnach auch irreduzibel in $\mathbb{Q}[t]$. □

b) Sei $f = 12t^5 + 21t^3 + 28t^2 - 7t + 7 \in \mathbb{Q}[t]$.
Da $7|7$, $7|-7$, $7|28$, $7|21$, $7|0$, $7 \nmid 12$ und $7^2 = 49 \nmid 7$ ist f nach dem Eisensteinkriterium mit $p = 7$ ist f irreduzibel in $\mathbb{Z}[t]$, weil f in $\mathbb{Z}[t]$ primitiv ist aufgrund von $ggT(7, 12) = 1$. Weil $\mathbb{Q} = Q(\mathbb{Z})$ ist f demnach auch irreduzibel in $\mathbb{Q}[t]$. □

c) Sei $f = t^2 + 1 \in \mathbb{Z}[t]$. Dann ist f offensichtlich irreduzibel in $\mathbb{Z}[t]$. Betrachten wir das „reduzierte“ Polynom $\overline{f} = t^2 + \overline{1} \in (\mathbb{Z}/2\mathbb{Z})[t]$. Dann ist $\overline{f}$ reduzibel mit $\overline{f} = (t + \overline{1})^2$, und diese Zerlegung ist nicht trivial. Also ist die Rückrichtung des Reduktionskriteriums nicht gültig.
Dies ist auch dadurch offensichtlich, dass man nur ein Primelement zur Reduzierung finden muss, und es gibt oft unendlich viele.

d) Sei $f = t^3 - 9t^2 + 27t - 34 \in \mathbb{Q}[t]$.
Nach dem Transformationskriterium ist f genau dann irreduzibel, wenn $f(t+3)$ irreduzibel in $\mathbb{Q}[t]$ ist. Betrachte $f(t+3)$ in $\mathbb{Z}[t]$.
Es gilt: $f(t+3) = t^3-7$. Dieses Polynom ist in $\mathbb{Z}[t]$ irreduzibel nach Eisensteinkriterium mit $p = 7$, da $7|7$, $7|0$, $7^2 = 49 \nmid 7$ und $7 \nmid 1 = \mathrm{LK}(f(t+3))$, weil $f(t+3)$ normiert und damit auch primitiv ist,. Weil $\mathbb{Q} = Q(\mathbb{Z})$ ist f demnach auch irreduzibel in $\mathbb{Q}[t]$. □

e) Sei $f = t^4 + 2t^2 + 1 \in \mathbb{Z}[t]$.
Es gilt: $f = (t^2 + 1)^2$ mit den Faktoren $t^2 + 1 \in \mathbb{Z}[t] \setminus (\mathbb{Z}^* \cup \{0\})$. Also ist f reduzibel in $\mathbb{Z}[t]$. □

f) Sei $f = 27t^3 + 5t^2 - 10t - 3 \in \mathbb{Q}[t]$.
Wir betrachten f in $\mathbb{Z}[t]$ und wenden das Reduktionskriterium für $p = 2$ an: $\overline{f} = t^3 + t^2 + \overline{1} \in (\mathbb{Z}/2\mathbb{Z})[t]$ ist irreduzibel in $(\mathbb{Z}/2\mathbb{Z})[t]$, da es keine Nullstellen hat ($\deg(\overline{f}) = 3$). Nach Reduktionskriterium ist daher auch f irreduzibel in $\mathbb{Z}[t]$, weil f in $\mathbb{Z}[t]$ primitiv ist aufgrund von $ggT(3, 5) = 1$. Weil $\mathbb{Q} = Q(\mathbb{Z})$ ist f demnach auch irreduzibel in $\mathbb{Q}[t]$. □

Aufgabe 7 (Körpererweiterungen)

a) Definieren Sie den Grad einer Körpererweiterung.

b) Definieren Sie, was es für $\alpha \in L$ bedeutet, algebraisch über K zu sein, wenn $K \subseteq L$ eine Körpererweiterung ist.

c) Bestimmen Sie bei der Körpererweiterung $K \subseteq L$ die Minimalpolynome m_α für

i) $K = \mathbb{Q}$, $L = \mathbb{R}$ und $\alpha = 3\sqrt{5} - \frac{1}{3}$.

ii) $K = \mathbb{Q}$, $L = \mathbb{C}$ und $\alpha = e^{2\pi i/5}$.

iii) $K = \mathbb{Q}$, $L = \mathbb{R}$ und $\alpha = \sqrt[3]{5} - 1$.

iv) $K = \mathbb{Q}$, $L = \mathbb{R}$ und $\alpha = \sqrt{5} + \sqrt{7}$.

Geben Sie jeweils auch eine K-Basis des K-Vektorraums $K[\alpha]$ an.

d) Zeigen Sie, dass $[\mathbb{R} : \mathbb{Q}] = \infty$, indem Sie die Gradformel für Körpererweiterungen für geeignete Zwischenkörper verwenden.

e) Zeigen Sie, dass $L := \mathbb{F}_3[t]/(t^2+1)\mathbb{F}_3[t]$ ein Körper ist. Bestimmen Sie anschließend $[L : \mathbb{F}_3]$ und eine $\mathbb{F}_3$-Basis von L.

Lösung:

a) Sei $K \subseteq L$ eine Körpererweiterung. Dann kann man L als K-Vektorraum auffassen. Der Grad der Körpererweiterung $K \subseteq L$ ist definiert als: $[L : K] := \dim_K(L)$.
Bemerkung: Der Grad einer Körpererweiterung ist eine natürliche Zahl oder ∞.

b) Sei $K \subseteq L$ eine Körpererweiterung und $\alpha \in L$. Dann heißt α algebraisch über K, falls es ein Polynom $f \in K[t]$ gibt, mit $f(\alpha) = 0$. Ist α nicht algebraisch, so heißt α transzendent über K.

c) i) Für die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{R}$ ist das Minimalpolynom m_α für $\alpha = 3\sqrt{5} - \frac{1}{3}$ zu berechnen.
1. Schritt:
$\alpha^2 = 9 \cdot 5 - 2\sqrt{5} + \frac{1}{9}$.
2. Schritt:
$\alpha^2 + \frac{2}{3}\alpha = 45 - 2\sqrt{5} + \frac{1}{9} + 2\sqrt{5} - \frac{2}{9} = 45 - \frac{1}{9}$
$\alpha^2 + \frac{2}{3}\alpha - \frac{404}{9} = 0$
3. Schritt:
Sei $f := t^2 + \frac{2}{3}t - \frac{404}{9}$, dann ist $f(\alpha) = 0$.
4. Schritt:
Prüfe f auf Irreduzibilität in $\mathbb{Q}[t]$. Angenommen, f wäre reduzibel: $f = gh$ mit $g, h \in \mathbb{Q}[t] \backslash \mathbb{Q}^*$. Dann ist, weil $\mathbb{Q}[t]$ insbesondere ein Integritätsring ist, wegen $f(\alpha) = g(\alpha) \cdot h(\alpha) = 0$ auch o.B.d.A. $g(\alpha) = 0$. Weil $g, h \notin \mathbb{Q}[t]^* = \mathbb{Q}^*$ gilt $\deg(g), \deg(h) \geq 1$. Aufgrund $\deg(f) = 2 = \deg(g) + \deg(h)$ ist $\deg(g) = 1$. Also ist $g = a_0 + a_1 t$ mit $a_0, a_1 \in \mathbb{Q}$ und $a_1 \neq 0$ und es folgt $g(\alpha) = 0 = a_0 + a_1\alpha = a_1 \cdot (a_0 a_1^{-1} + \alpha)$. Damit ergibt sich $a_0 a_1^{-1} + \alpha = 0$, also $\alpha = -a_0 a_1^{-1} \in \mathbb{Q}$. Da aber $\alpha \notin \mathbb{Q}$ ergibt sich ein Widerspruch und f ist irreduzibel. Da f bereits normiert ist, ist $m_\alpha := f$ das Minimalpolynom von α.
5. Schritt:
Wegen $\deg(m_\alpha) = 2$ ist $\mathcal{B} = (1, \alpha)$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}[\alpha]$. □

ii) Für die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{C}$ ist das Minimalpolynom m_α für $\alpha = e^{2\pi i/5}$ zu berechnen.
1. Schritt:
$\alpha = e^{2\pi i/5} = \cos(2\pi/5) + i\sin(2\pi/5) = \frac{\sqrt{5}-1}{4} + \frac{\sqrt{2(\sqrt{5}+10)}}{4}i$
$\alpha^2 = \frac{-\sqrt{5}-1}{4} + \frac{(\sqrt{5}-1)\sqrt{2(\sqrt{5}+10)}}{8}i$
$\alpha^3 = \frac{-\sqrt{5}-1}{4} - \frac{(\sqrt{5}-1)\sqrt{2(\sqrt{5}+10)}}{8}i$
$\alpha^4 = \frac{\sqrt{5}-1}{4} - \frac{\sqrt{2(\sqrt{5}+10)}}{4}i$
2. Schritt:
$\alpha^2 + \alpha^3 = \frac{-2\sqrt{5}-2}{4}$
$\alpha + \alpha^4 = \frac{2\sqrt{5}-2}{4}$
$\alpha + \alpha^2 + \alpha^3 + \alpha^4 = -1$
$\alpha + \alpha^2 + \alpha^3 + \alpha^4 + 1 = 0$
3. Schritt:
Sei $f := t^4 + t^3 + t^2 + t + 1$, dann ist $f(\alpha) = 0$.
4. Schritt:
Prüfe f auf Irreduzibilität in $\mathbb{Q}[t]$. Wir betrachten f in $\mathbb{Z}[t]$. Da $2 \nmid 1 = \mathrm{LK}(f)$ kann man das Reduktionskriterium für $p = 2$ anwenden. $\overline{f} = t^4 + t^3 + t^2 + t + 1 \in (\mathbb{Z}/2\mathbb{Z})[t]$ ist irreduzibel nach Übungsaufgabe. Nach dem Reduktionskriterium ist f daher irreduzibel in $\mathbb{Z}[t]$, weil f normiert und damit auch primitiv ist, und wegen $\mathbb{Q} = Q(\mathbb{Z})$ ist f auch irreduzibel in $\mathbb{Q}[t]$. Weil f normiert und irreduzibel mit $f(\alpha) = 0$ ist $m_\alpha := f$ das Minimalpolynom von α.
5. Schritt:
Wegen $\deg(m_\alpha) = 4$ ist $\mathcal{B} = (1, \alpha, \alpha^2, \alpha^3)$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}[\alpha]$. □

iii) Für die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{R}$ ist das Minimalpolynom m_α für $\alpha = \sqrt[3]{5} - 1$ zu berechnen.
1. Schritt:
$\alpha^2 = \sqrt[3]{5}^2 - 2\sqrt[3]{5} + 1$
$\alpha^3 = 5 - 3\sqrt[3]{5}^2 + 3\sqrt[3]{5} - 1$
2. Schritt:
$\alpha^3 + 3\alpha^2 = 7 - 3\sqrt[3]{5}$
$\alpha^3 + 3\alpha^2 + 3\alpha = 4$
$\alpha^3 + 3\alpha^2 + 3\alpha - 4 = 0$
3. Schritt:
Sei $f := t^3 + 3t^2 + 3t - 4$, dann ist $f(\alpha) = 0$.
4. Schritt:
Prüfe f auf Irreduzibilität in $\mathbb{Q}[t]$. Wir betrachten f in $\mathbb{Z}[t]$. Da $7 \nmid 1 = \mathrm{LK}(f)$ kann man das Reduktionskriterium für $p = 7$ anwenden. $\overline{f} = t^3 + \overline{3}t^2 + \overline{3}t - \overline{4} \in (\mathbb{Z}/7\mathbb{Z})[t]$ ist irreduzibel, da $\overline{f}$ keine Nullstellen in $\mathbb{Z}/7\mathbb{Z}$ hat:
$\overline{f}(\overline{0}) = \overline{-4} = \overline{3}$
$\overline{f}(\overline{1}) = \overline{3}$
$\overline{f}(\overline{2}) = \overline{22} = \overline{1}$
$\overline{f}(\overline{3}) = \overline{59} = \overline{3}$

$\overline{f}(\overline{4}) = \overline{120} = \overline{1}$
$\overline{f}(\overline{5}) = \overline{211} = \overline{1}$
$\overline{f}(\overline{6}) = \overline{338} = \overline{2}$
Da Polynome vom Grad 2 oder 3 über einem Körper genau dann reduzibel sind, wenn sie eine Nullstelle haben, ist $\overline{f}$ irreduzibel in $(\mathbb{Z}/7\mathbb{Z})[t]$. Nach dem Reduktionskriterium ist f daher irreduzibel in $\mathbb{Z}[t]$, weil f normiert und damit auch primitiv ist, und wegen $\mathbb{Q} = Q(\mathbb{Z})$ ist f auch irreduzibel in $\mathbb{Q}[t]$. Weil f normiert und irreduzibel mit $f(\alpha) = 0$ ist $m_\alpha := f$ das Minimalpolynom von α.
5. Schritt:
Wegen $\deg(m_\alpha) = 3$ ist $\mathcal{B} = \left(1, \alpha, \alpha^2\right)$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}[\alpha]$. □

iv) Für die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{R}$ ist das Minimalpolynom m_α für $\alpha = \sqrt{5} + \sqrt{7}$ zu berechnen.
1. Schritt:
$\alpha^2 = 12 + 2\sqrt{35}$
$\alpha^3 = 26\sqrt{5} + 22\sqrt{7}$
$\alpha^4 = 284 + 48\sqrt{35}$
2. Schritt:
$\alpha^4 - 24\alpha^2 = -4$
$\alpha^4 - 24\alpha^2 + 4 = 0$
3. Schritt:
Sei $f := t^4 - 24t^2 + 4$, dann ist $f(\alpha) = 0$.
4. Schritt:
Prüfe f auf Irreduzibilität in $\mathbb{Q}[t]$. Wir betrachten f in $\mathbb{Z}[t]$. Angenommen, f wäre reduzibel in $\mathbb{Z}[t]$. Sei $f = g \cdot h$ mit $g, h \in \mathbb{Z}[t] \backslash \mathbb{Z}^*$. Da f normiert ist, kann man o.B.d.A. auch g und h als normiert annehmen (da die Leitkoeffizienten jeweils Einheiten sind, und man mit dem Inversen multiplizieren kann). Damit ist also $\deg(g), \deg(h) \geq 1$. Mit Gradformel ergeben sich somit zwei Möglichkeiten:
1. Möglichkeit:
o.B.d.A. $\deg(g) = 1$ und $\deg(h) = 3$.
Dann existieren $a_0, b_0, b_1, b_2 \in \mathbb{Z}$ mit $g = t + a_0$ und $h = t^3 + b_2t^2 + b_1t + b_0$. Es gilt: $g \cdot h = (t + a_0)(t^3 + b_2t^2 + b_1t + b_0) = t^4 + (a_0 + b_2)t^3 + (a_0b_2 + b_1)t^2 + (a_0b_1 + b_0)t + a_0b_0$.
Koeffizientenvergleich liefert:
$a_0 + b_2 = 0$, also $b_2 = -a_0$.
$a_0b_2 + b_1 = -a_0^2 + b_1 = -24$
$a_0b_1 + b_0 = 0$, also $b_0 = -a_0b_1$.
$a_0b_0 = -a_0^2b_1 = 4$, also $b_1 \in \{-1, -2\}$. Dann ist aber $-a_0^2 \in \{-22, -23\}$, also $a_0^2 \in \{22, 23\}$. Dies ist in $\mathbb{Z}$ nicht möglich. Somit ergibt sich ein Widerspruch. $\deg(g) = 1$ und $\deg(h) = 3$ ist keine mögliche Zerlegung.
2. Möglichkeit:
$\deg(g) = \deg(h) = 2$.
Dann existieren $a_0, a_1, b_0, b_1 \in \mathbb{Z}$ mit $g = t^2 + a_t + a_0$ und $h = t^2 + b_1t + b_0$. Es gilt: $g \cdot h = (t^2 + a_1t + a_0)(t^2 + b_1t + b_0) = t^4 + (a_1 + b_1)t^3 + (a_0 + b_0 + a_1b_1)t^2 + (a_0b_1 + a_1b_0)t + a_0b_0$.
Koeffizientenvergleich liefert:
$a_1 + b_1 = 0$, also $b_1 = -a_1$.
$a_0 + b_0 + a_1b_1 = a_0 + b_0 - a_1^2 = -24$
$a_0b_1 + a_1b_0 = -a_1a_0 + a_1b_0 = a_1(-a_0 + b_0) = 0$, also $a_1 = 0$ oder $a_0 = b_0$.
$a_0b_0 = 4$
Angenommen, $a_0 = b_0$. Dann ist $a_0 \in \{2, -2\}$ und somit $-a_1^2 \in \{-20, -28\}$, was in $\mathbb{Z}$ nicht möglich ist. Somit ergibt sich ein Widerspruch.
Angenommen, $a_1 = 0$. Dann ist $a_0 + b_0 = -24$, also $a_0 = -24 - b_0$ und somit $a_0b_0 = -24b_0 - b_0^2 = 4$ Dann ist aber $b_0^2 + 24b_0 = -4$ und somit $b_0 < 0$. Es ergeben sich 3 Möglichkeiten: $b_0 \in \{-1, -2, -4\}$. Es gilt aber:
$(-1)^2 + 24 \cdot (-1) = -23 \neq -4$
$(-2)^2 + 24 \cdot (-2) = -44 \neq -4$
$(-4)^2 + 24 \cdot (-4) = -80 \neq -4$
Also ergibt sich jeweils ein Widerspruch. Insgesamt ist also eine $\deg(g) = \deg(h) = 2$-Zerlegung nicht möglich.
Damit ist f in $\mathbb{Z}[t]$ irreduzibel.
Weil $\mathbb{Q} = Q(\mathbb{Z})$ ist damit auch f irreduzibel in $\mathbb{Q}[t]$. Weil f normiert und irreduzibel mit $f(\alpha) = 0$ ist $m_\alpha := f$ das Minimalpolynom von α.
5. Schritt:
Wegen $\deg(m_\alpha) = 4$ ist $\mathcal{B} = \left(1, \alpha, \alpha^2, \alpha^3\right)$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}[\alpha]$. □

d) Wir wissen, dass für jedes $n \in \mathbb{N}$ das Element $\sqrt[n]{2} \in \mathbb{R}$ algebraisch über $\mathbb{Q}$ ist. Das Minimalpolynom ist jeweils $m_{\sqrt[n]{2},\mathbb{Q}} = t^n - 2$ (irreduzibel nach Eisenstein). Da $\mathbb{Q} \subseteq \mathbb{R}$ und $\sqrt[n]{2} \in \mathbb{R}$, ist auch $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[n]{2}) \subseteq \mathbb{R}$ ein Zwischenkörper und nach Gradsatz gilt: $[\mathbb{R} : \mathbb{Q}] = [\mathbb{R} : \mathbb{Q}(\sqrt[n]{2})] \cdot \underbrace{[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}]}_{=n}$
Also gilt $n \mid [\mathbb{R} : \mathbb{Q}]$ für alle $n \in \mathbb{N}$. Dies ist nur für $[\mathbb{R} : \mathbb{Q}] = \infty$ möglich. □

e) Sei $L = \mathbb{F}_3[t]/(t^2 + 1)\mathbb{F}_3[t]$.
ZZ: L ist ein Körper.
Wir zeigen, dass $(t^2 + 1)$ in $\mathbb{F}_3[t]$ irreduzibel ist. Da $\mathbb{F}_3$ ein Körper ist, und $f = t^2 + 1$ den Grad 2 hat, ist f genau dann reduzibel, wenn f eine Nullstelle in $\mathbb{F}_3$ besitzt. Aber $f(0) = 1$, $f(1) = 2$ und $f(2) = 2$. Also ist f irreduzibel über $\mathbb{F}_3$. Mit der Begründung wie in Aufgabe 4 d) ist L ein Körper. Laut VL ist $\mathcal{B} = \left(\overline{1}, \overline{t}\right)$ eine $\mathbb{F}_3$-Basis von L. Außerdem gilt $\dim_{\mathbb{F}_3}(L) = 2 = \deg(f)$. □
Bemerkung: Man beachte, dass Restklassen in der Basis eines Restklassenrings sein müssen. Dies ist bei $R[\alpha]$ anders, da $R[\alpha]$ kein Restklassenring ist.

Aufgabe 8 (Moduln)

a) Sei $R = \mathbb{Z}_6$ und $M = R \times R$. Ist M ein freier R-Modul? Falls ja, geben Sie eine Basis an. Ist die Familie $((2,4))$ über R linear unabhängig?

b) Sei $\varphi : \mathbb{Z}^{3\times 1} \to \mathbb{Z}^{2\times 2}$ gegeben durch $(x,y,z)^T \mapsto \begin{pmatrix} x & x+y \\ z & x+z \end{pmatrix}$. Zeigen Sie dass φ ein $\mathbb{Z}$-Modulhomomorphismus ist und bestimmen Sie die darstellende Matrix $M_{\mathcal{C}}^{\mathcal{B}}(\varphi)$ für die Basen $\mathcal{B} = \left((-1,1,0)^T, (0,1,0)^T, (1,0,1)^T\right)$ von $\mathbb{Z}^{3\times 1}$ und $\mathcal{C} = \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right)$ von $\mathbb{Z}^{2\times 2}$.

c) Sei K ein Körper und V ein K-Vektorraum. Sei $F \in \mathrm{End}_K(V)$. Wie wird V zu einem $K[t]$-Modul (ohne Beweis)?

d) Sei $A := \begin{pmatrix} 0 & 3 & 0 & 0 \\ -24 & 5 & 1 & 0 \\ 6 & 6 & 0 & 0 \end{pmatrix} \in \mathbb{Z}^{3\times 4}$. Bestimmen Sie eine Smith-Normalform S von A, so dass alle Elementarteiler positiv sind. Ist S dadurch eindeutig bestimmt? Sei φ_A die Standardinterpretation von A. Bestimmen Sie Basen von $\ker(\varphi_A)$ und $\mathrm{im}(\varphi_A)$.

e) Sei $A \in \mathbb{Q}^{3\times 3}$ eine quadratische Matrix. Sei H die zugehörige charakteristische Matrix und sei das charakteristische Polynom $h_A = (t-1)(t-2)^2$. Geben Sie (bis auf Assoziiertheit der Elementarteiler) alle möglichen Smith-Normalformen von H an.

Lösung:

a) M ist ein freier R-Modul, denn $((1,0),(0,1))$ bildet eine Basis (einfach nachzurechnen). Die Familie $((2,4))$ ist nicht linear unabhängig, denn $3 \cdot (2,4) = (0,0) = 0_M$ liefert eine nicht-triviale Darstellung der 0_M.

b) Wir müssen zeigen, dass φ $\mathbb{Z}$-linear ist, d.h. $\varphi(v+w) = \varphi(v) + \varphi(w)$ und $\varphi(\alpha \cdot v) = \alpha \cdot \varphi(v)$ für alle $v, w \in \mathbb{Z}^{3\times 1}$ und $\alpha \in \mathbb{Z}$. Seien $v = (x,y,z)^T, w = (a,b,c)^T \in \mathbb{Z}^{3\times 1}$ und $\alpha \in \mathbb{Z}$. Dann gilt:
$\varphi(v+w) = \varphi((x+a, y+b, z+c)^T) = \begin{pmatrix} x+a & x+a+y+b \\ z+c & x+a+z+c \end{pmatrix} = \begin{pmatrix} x & x+y \\ z & x+z \end{pmatrix} + \begin{pmatrix} a & a+b \\ c & a+c \end{pmatrix} = \varphi(v) + \varphi(w)$. Außerdem gilt $\varphi(\alpha \cdot v) = \varphi((\alpha x, \alpha y, \alpha z)^T) = \begin{pmatrix} \alpha x & \alpha x + \alpha y \\ \alpha z & \alpha x + \alpha z \end{pmatrix} = \alpha \cdot \begin{pmatrix} x & x+y \\ z & x+z \end{pmatrix}$. Damit ist φ tatsächlich ein $\mathbb{Z}$-Modulhomomorphismus.
Für die darstellende Matrix berechnen wir: $\varphi((-1,1,0)^T) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = (-1) \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + (-1) \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Analog erhalten wir mit $\varphi((0,1,0)^T) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ und $\varphi((1,0,1)^T) = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ die darstellende Matrix

$$M_{\mathcal{C}}^{\mathcal{B}}(\varphi) = \begin{pmatrix} -1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ -1 & 0 & 2 \end{pmatrix}. \qquad \square$$

c) Da $(V,+)$ bereits eine abelsche Gruppe ist, muss für einen $K[t]$-Modul nur eine passende Skalarmultiplikation $\cdot_F : K[t] \times V \to V$ definiert werden: Für $p \in K[t]$ und $v \in V$ setzen wir dafür $p \cdot_F v := (p(F))(v)$, wobei F in das Polynom p eingesetzt wird. Heraus kommt eine Abbildung von V nach V, in die wir v einsetzen können. (Endomorphismen bilden einen Ring, wobei die Hintereinanderausführung (Verknüpfung) die Multiplikation ist. Dabei ist $F^0 = \mathrm{id}_V$.)

d) Durch elementare Zeilen- und Spaltenumformungen lässt sich A in Smith-Normalform überführen. Die Matrix $S = P \cdot A \cdot Q$ ist in Smith-Normalform, wobei $S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 6 & 0 \end{pmatrix}$, $P = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ und $Q = \begin{pmatrix} -1 & 1 & 1 & 0 \\ 1 & -1 & 0 & 0 \\ -28 & 29 & 24 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.
Die Elementarteiler von A sind 1, 3 und 6 (allesamt positiv). Die Smith-Normalform ist durch die Elementarteiler eindeutig bestimmt. Die Elementarteiler sind bis auf Assoziiertheit eindeutig, in $\mathbb{Z}$ bedeutet das „bis aufs Vorzeichen“, was durch die Forderung „positiv“ eindeutig ist. Somit ist S eindeutig bestimmt. Achtung: P und Q hängen

von den durchgeführten Zeilen- und Spaltenumformungen ab und sind nicht eindeutig! Die Basen von $\ker(\varphi_A)$ und $\mathrm{im}(\varphi_A)$ sind also auch nicht eindeutig!
Es ist $\varphi_A : \mathbb{Z}^{4\times 1} \to \mathbb{Z}^{3\times 1}$ und wir versehen gedanklich $\mathbb{Z}^{4\times 1}$ und $\mathbb{Z}^{3\times 1}$ mit den jeweiligen Standardbasen. Eine Basis $\mathcal{C}$ von $\mathrm{im}(\varphi_A)$ ist dann gegeben durch die Spalten von $P^{-1} = \begin{pmatrix} 3 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, multipliziert mit den Elementarteilern in den jeweiligen Spalten, also: $\mathcal{C} = \big((3,1,0)^T, (-3,0,0)^T, (0,0,6)^T\big)$. Für eine Basis $\mathcal{D}$ von $\ker(\varphi_A)$ benötigen wir die letzte Spalte von Q. Damit ist $\mathcal{D} = \big((0,0,0,1)^T\big)$ nach Vorlesung eine Basis von $\ker(\varphi_A)$. □

e) Nach Vorlesung sind die Elementarteiler einer charakteristischen Matrix alle ungleich 0. Damit muss es also drei Elementarteiler s_1, s_2, s_3 (von 0 verschieden) von H geben. Weiter wissen wir, dass diese sich aufsteigend teilen müssen (in $\mathbb{Q}[t]$) und dass deren Produkt das charakteristische Polynom ist. Es gilt also $s_1 \mid s_2 \mid s_3$ und $s_1 s_2 s_3 = (t-1)(t-2)^2$. Die einzigen Möglichkeiten (bis auf Assoziiertheit) dafür sind:

- $s_1 = 1$, $s_2 = (t-2)$ und $s_3 = (t-1)(t-2)$. In diesem Fall wäre die Smith-Normalform dann $\begin{pmatrix} 1 & 0 & 0 \\ 0 & (t-2) & 0 \\ 0 & 0 & (t-1)(t-2) \end{pmatrix}$.
- $s_1 = 1$, $s_2 = 1$ und $s_3 = (t-1)(t-2)^2 = h_A$. In diesem Fall wäre die Smith-Normalform dann $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & h_A \end{pmatrix}$. □

Aufgabe 9 (Normalformen)

a) Sei K ein Körper, $n \in \mathbb{N}$ und $A \in K^{n\times n}$ eine quadratische Matrix. Wann ...

i) ... ist diagonalisierbar?

ii) ... gibt es eine zu A ähnliche Matrix in Frobenius-Normalform?

iii) ... gibt es eine zu A ähnliche Matrix in Weierstraß-Normalform?

iv) ... gibt es eine zu A ähnliche Matrix in Jordan-Normalform?

b) Sei $A = \begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 3 & 4 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \in \mathbb{Q}^{4\times 4}$ und sei $F_A : \mathbb{Q}^{4\times 1} \to \mathbb{Q}^{4\times 1}$ die Standardinterpretation von A.

i) Bestimmen Sie eine zu A ähnliche Matrix $A_{\mathcal{F}}$ in Frobenius-Normalform sowie eine Basis $\mathcal{B}$ von $\mathbb{Q}^{4\times 1}$, so dass $M_{\mathcal{B}}^{\mathcal{B}}(F_A) = A_{\mathcal{F}}$.

ii) Bestimmen Sie eine zu A ähnliche Matrix $A_{\mathcal{W}}$ in Weierstraß-Normalform sowie eine Basis $\mathcal{C}$ von $\mathbb{Q}^{4\times 1}$, so dass $M_{\mathcal{C}}^{\mathcal{C}}(F_A) = A_{\mathcal{W}}$.

iii) Bestimmen Sie eine zu A ähnliche Matrix $A_{\mathcal{J}}$ in Jordan-Normalform sowie eine Basis $\mathcal{D}$ von $\mathbb{Q}^{4\times 1}$, so dass $M_{\mathcal{D}}^{\mathcal{D}}(F_A) = A_{\mathcal{J}}$.

c) Sei $A = \begin{pmatrix} 2 & 0 & 4 \\ 3 & 0 & 3 \\ 0 & 0 & 1 \end{pmatrix} \in \mathbb{Q}^{3\times 3}$ und sei $F_A : \mathbb{Q}^{3\times 1} \to \mathbb{Q}^{3\times 1}$ die Standardinterpretation von A.

i) Bestimmen Sie eine zu A ähnliche Matrix in Frobenius-Normalform.

ii) Bestimmen Sie eine zu A ähnliche Matrix in Weierstraß-Normalform.

iii) Bestimmen Sie eine zu A ähnliche Matrix in Jordan-Normalform.

d) Sei $A \in \mathbb{Q}^{4\times 4}$ eine Matrix mit dem charakteristischen Polynom $h_A = (t-1)(t-2)(t+1)^2$.

i) Geben Sie alle möglichen Frobenius-Normalformen von A an.

ii) Geben Sie alle möglichen Weierstraß-Normalformen von A (bis auf Reihenfolge der der Faktoren der Elementarteiler der charakteristischen Matrix) an.

iii) Geben Sie alle möglichen Jordan-Normalformen (bis auf Reihenfolge der Eigenwerte von A) an.

Lösung:

a) i) (LinA-Wiederholung) A ist diagonalisierbar, wenn das charakteristische Polynom von A in Linearfaktoren zerfällt und die algebraische Vielfachheit eines jeden Eigenwertes mit der geometrischen Vielfachheit übereinstimmt.

ii) Für jede quadratische Matrix über einem Körper gibt es eine ähnliche Matrix in Frobenius-Normalform.

iii) Für jede quadratische Matrix über einem Körper gibt es eine ähnliche Matrix in Weierstraß-Normalform. Ausschlaggebend ist, dass man die Elementarteiler (Elemente von $K[t]$) in irreduzible Faktoren zerlegen kann.

iv) Zu A gibt es eine ähnliche Matrix in Jordan-Normalform, wenn das charakteristische Polynom in Linearfaktoren zerfällt.

b) Die charakteristische Matrix von A ist durch $H = tE_4 - A = \begin{pmatrix} t-2 & 0 & -1 & 0 \\ 0 & t-1 & 0 & 0 \\ 0 & -3 & t-4 & 0 \\ 0 & -1 & 0 & t-1 \end{pmatrix}$ gegeben. Mittels elementarer Zeilen- und Spaltenumformungen erhalten wir eine Smith-Normalform S von H und Matrizen $P, Q \in \mathbb{Q}[t]^{4\times 4}$ mit $S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & (t-1)^2(t-2)(t-4) \end{pmatrix}$, wobei $S = P \cdot H \cdot Q$. Aus Layout-Gründen wird hier die berechnete Matrix P transponiert angegeben: $P^T = \begin{pmatrix} 1 & 0 & t-4 & -\frac{1}{9}t^4 + \frac{11}{9}t^3 - \frac{13}{3}t^2 + \frac{49}{9}t - \frac{20}{9} \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & -\frac{1}{9}t^3 + \frac{7}{9}t^2 - \frac{11}{9}t + \frac{5}{9} \\ 0 & -1 & -3 & \frac{1}{3}t^3 - \frac{7}{3}t^2 + \frac{14}{3}t - \frac{8}{3} \end{pmatrix}$. Für die zu berechnende Basis müssen wir später die Spalten von $P^{-}1$ kennen. Es gilt $P^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & t-1 & \frac{1}{9}t^3 - \frac{7}{9}t^2 + \frac{11}{9}t - \frac{5}{9} & 1 \\ -t+4 & -3 & 1 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$.

i) Der einzige nichttriviale Elementarteiler ist $g_1 := (t-1)^2(t-2)(t-4) = t^4 - 8t^3 + 21t^2 - 22t + 8$. Die Frobenius-Normalform von A besteht also aus nur einem Block, nämlich $A_{\mathcal{F}} = B(g_1) = \begin{pmatrix} 0 & 0 & 0 & -8 \\ 1 & 0 & 0 & 22 \\ 0 & 1 & 0 & -21 \\ 0 & 0 & 1 & 8 \end{pmatrix}$. Für die zugehörige Basis benötigen wir die letzte Spalte von P^{-1} (denn es gibt nur einen nichttrivialen Elementarteiler). Wir schreiben $F := F_A$ für die Standardinterpretation von A und $\mathcal{E} = (e_1, e_2, e_3, e_4)$ sei die Standardbasis. Sei $w_4 = ((0,1,0,0)^T)$. Dann ist $\mathcal{B} = \big(\psi_F(w_4), F(\psi_F(w_4)), F^2(\psi_F(w_4)), F^3(\psi_F(w_4))\big)$ die gesuchte Basis, wobei $\psi_F(w_4) = 0 \cdot_F e_1 + 1 \cdot_F e_2 + 0 \cdot_F e_3 + 0 \cdot_F e_4 = w_4 =: a_1$. Mit $F(e_2) = (0,1,3,1)^T$, $F^2(e_2) = (3,1,15,2)^T$ und $F^3(e_2) = (21,1,63,3)^T$ ist die gesuchte Basis $\mathcal{B} = \left(\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ 15 \\ 2 \end{pmatrix}, \begin{pmatrix} 21 \\ 1 \\ 63 \\ 3 \end{pmatrix} \right)$.

ii) Wir übernehmen die Bezeichnungen der letzten Teilaufgabe.
Der einzige nichttriviale Elementarteiler hat die Faktorisierung $g_1 := (t-1)^2(t-2)(t-4)$. Somit besteht die Weierstraß-Normalform $A_{\mathcal{W}}$ von A aus drei Begleitmatrix-Blöcken, $A_{\mathcal{W}} = \mathrm{Diag}(B(t-1)^2, B(t-2), B(t-4)) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$.
Für die zugehörige Basis $\mathcal{C}$ berechnen wir $g_{1,1} := \frac{g_1}{(t-1)^2} = (t-2)(t-4) = t^2 - 6t + 8$, $g_{1,2} := \frac{g_1}{(t-2)} = (t-1)^2(t-4) = t^3 - 6t^2 + 9t - 4$ und $g_{1,3} := \frac{g_1}{(t-4)} = (t-1)^2(t-2) = t^3 - 4t^2 + 5t - 2$. Wir setzen anschließend $a_1' := g_{1,1} \cdot_F a_1 = F^2(a_1) - 6F(a_1) + 8a_1 = (3,3,-3,-4)^T$, sowie $a_2' := g_{1,2} \cdot_F a_1 = F^3(a_1) - 6F^2(a_1) + 9F(a_1) - 4a_1 = (3,0,0,0)^T$ und $a_3' := g_{1,3} \cdot_F a_1 = F^3(a_1) - 4F^2(a_1) + 5F(a_1) - 2a_1 = (9,0,18,0)^T$.
Die Basis $\mathcal{C}$ ist dann gegeben durch $\mathcal{C} = (a_1', F(a_1'), a_2', a_3') = \left(\begin{pmatrix} 3 \\ 3 \\ -3 \\ -4 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \\ -3 \\ -1 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 9 \\ 0 \\ 18 \\ 0 \end{pmatrix} \right)$.

iii) Ausgehend von der Weierstraß-Normalform müssen wir für die Jordan-Normalform nicht mehr viel machen. Da das charakteristische Polynom in Linearfaktoren zerfällt, existiert eine zu A ähnliche Matrix in Jordan-Normalform. Die algebraischen Vielfachheiten der Eigenwerte $\lambda_2 = 2$ und $\lambda_3 = 4$ sind jeweils 1 und daher sind auch die geometrischen Vielfachheiten jeweils 1. Für den Eigenwert $\lambda_1 = 1$ berechnen wir die geometrische Vielfachheit. Betrachten wir die Matrix

$1 \cdot E_4 - A = \begin{pmatrix} -1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & -3 & -3 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$. Durch elementare Zeilenumformungen (Gauß) transformiert sich diese zu $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$, hat also Rang 3. Damit ist die geometrische Vielfachheit $4 - 3 = 1$ und es gibt also nur einen Jordan-Block zum Eigenwert λ_1 der Größe 2×2. Insgesamt ist die Jordan-Normalform von A also $A_{\mathcal{J}} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$.

Die gesuchte Basis ist (mit der Bezeichnung von ii)) gegeben durch $\mathcal{D} = ((F - 1 \cdot \mathrm{id})(a_1'), a_1', a_2', a_3')$. Das zweite Element ist $(F - 1 \cdot \mathrm{id})(a_1') = F(a_1') - a_1' = (0, 0, 0, 3)^T$ und es ergibt sich somit die gesuchte Basis $\mathcal{D} = \left(\begin{pmatrix} 0 \\ 0 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \\ -3 \\ -4 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 9 \\ 0 \\ 18 \\ 0 \end{pmatrix} \right)$.

c) Die charakteristische Matrix von A ist $H = \begin{pmatrix} t-2 & 0 & -4 \\ -3 & t & -3 \\ 0 & 0 & t-1 \end{pmatrix}$. Das charakteristische Polynom ist damit $h_A = t(t-1)(t-2) = t^3 - 3t^2 + 2t$, welches in paarweise verschiedene Linearfaktoren zerfällt. Die Smith-Normalform (bis auf Assoziiertheit der Elementarteiler) von H ist gegeben durch $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & h_A \end{pmatrix}$. Dies kann man berechnen, oder man nutzt den Umstand, dass h_A quadratfrei ist und somit der einzige nichttriviale Elementarteiler sein muss.

i) Da es nur einen nichttrivialen Elementarteiler von H gibt, hat die Frobenius-Normalform nur einen Block, nämlich $A_{\mathcal{F}} = B(h_A) = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -2 \\ 0 & 1 & 3 \end{pmatrix}$.

ii) Der einzige nichttriviale Elementarteiler zerfällt in die irreduziblen Faktoren t, $t-1$ und $t-2$. Daher ist die Weierstraß-Normalform von der Gestalt $A_{\mathcal{W}} = \mathrm{Diag}(B(t), B(t-1), B(t-2)) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$.

iii) Da h_A in paarweise verschiedene Linearfaktoren zerfällt, haben die drei Eigenwerte von A $(0, 1, 2)$ jeweils algebraische (und damit auch geometrische) Vielfachheit 1. Damit ist die Jordan-Normalform gegeben durch $A_{\mathcal{J}} = \mathrm{Diag}(J_1(0), J_1(1), J_1(2)) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. □

d) Für i) und ii) benötigen wir alle möglichen Smith-Normalformen S der charakteristischen Matrix. Da die Elementarteiler sich aufsteigend teilen müssen und das Produkt der Elementarteiler das charakteristische Polynom h_A sein muss, in welchem nur ein einziger Faktor mehrfach (doppelt) auftaucht, gibt es nur zwei Möglichkeiten:

- $S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & h_A \end{pmatrix}$
- $S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (t+1) & 0 \\ 0 & 0 & 0 & (t-1)(t-2)(t+1) \end{pmatrix}$

i) Falls die erste Smith-Normalform zutrifft, so gibt es nur einen Block in der Frobenius-Normalform, die Begleitmatrix zu $h_A = t^4 - t^3 - 3t^2 + t + 2$. Diese ist dann $A_{\mathcal{F}} = \begin{pmatrix} 0 & 0 & 0 & -2 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 1 \end{pmatrix}$.

Im anderen Fall (zweite Smith-Normalform) gibt es zwei Blöcke, die Begleitmatrizen $B(g_1) = B(t+1) = (-1)$ und $B(g_2) = B((t-1)(t-2)(t+1)) = B(t^3 - 2t^2 - t + 2) = \begin{pmatrix} 0 & 0 & -2 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}$. Damit ergibt sich $A_{\mathcal{F}} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$.

ii) Falls die erste Smith-Normalform zutrifft, so gibt es nur einen nichttrivialen Elementarteiler mit der Zerlegung in drei irreduzible Faktoren mit Vielfachheiten und es ergibt sich bis auf Reihenfolge die Weierstraß-Normalform $A_{\mathcal{W}} = \mathrm{Diag}\left(B(t-1), B(t-2), B((t+1)^2)\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & -2 \end{pmatrix}$.

Falls die zweite Smith-Normalform zutrifft, ist die Weierstraß-Normalform bereits eine

Diagonalmatrix, denn die beiden nichttrivialen Elementarteiler zerfallen jeweils in paarweise verschiedene Linearfaktoren. Damit ist $A_{\mathcal{W}} = \mathrm{Diag}(B(t+1), B(t-1), B(t-2), B(t+1)) = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$ die zugehörige Matrix in Weierstraß-Normalform.

iii) Für die Jordan-Normalformen vergessen wir kurz, wie die möglichen Smith-Normalformen der charakteristischen Matrix von A aussehen. Wir kennen die Faktorisierung des charakteristischen Polynoms $h_A = (t-1)(t-2)(t+1)^2$. Da h_A in Linearfaktoren zerfällt, gibt es eine Jordan-Normalform von A. Die Eigenwerte von A sind somit $\lambda_1 = 1$, $\lambda_2 = 2$ und $\lambda_3 = -1$. Die Eigenwerte λ_1 und λ_2 haben jeweils die algebraische Vielfachheit 1 (und deswegen zwingend auch geometrische Vielfachheit 1, denn $1 \leq$ geom. Vielf. $\leq$ alg. Vielf.). Einzig zum Eigenwert λ_3 fehlen uns Informationen. Daher gibt es zwei mögliche Jordan-Normalformen:
Falls die geometrische Vielfachheit von λ_3 1 ist, so gibt es zu λ_3 nur einen Jordan-Block der Größe 2×2. In diesem Fall wäre $A_{\mathcal{J}} = \mathrm{Diag}(J_1(\lambda_1), J_1(\lambda_2), J_2(\lambda_3)) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}$.
Falls die geometrische Vielfachheit von λ_3 2 ist, so gibt es zwei Jordan-Blöcke zum Eigenwert -1. Die Größen dieser Blöcke müssen sich zu 2 addieren, weshalb nur zwei 1×1-Blöcke infrage kommen. In diesem Fall ist $A_{\mathcal{J}} = \mathrm{Diag}(J_1(\lambda_1), J_1(\lambda_2), J_1(\lambda_3), J_1(\lambda_3)) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$ die Jordan-Normalform von A. □