Algebra I, WiSe 2011\2012 – Lösung Blatt 11

11.1. • Zeigen zunächst: R ist Integritätsbereich.

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

$\Rightarrow \quad a \cdot b \in (0)$.

Da 0 keine Einheit ist, ist (0) Primideal.

$\Rightarrow \quad a \in (0) \quad$ oder $\quad b \in (0)$

$\Rightarrow \quad a = 0 \quad$ oder $\quad b = 0$

$\Rightarrow$ R ist nullteilerfrei also ein Integritätsbereich.

• Sei nun $a \in R \setminus \{0\}$. Wir zeigen: a ist Einheit.

$\nearrow$ a ist keine Einheit $\Rightarrow$ a^2 ist keine Einheit

(sonst $\exists\, b \in R$ mit $a^2 b = 1$, d.h. $a(ab) = 1$, d.h. a wäre Einheit)

$\overset{\text{Vor.}}{\Rightarrow}$ (a^2) ist Primideal

Wegen $a \cdot a = a^2 \in (a^2)$ folgt also $a \in (a^2)$.

$\Rightarrow \exists\, b \in R$ mit $a = ba^2$, also $(ba - 1)a = 0$.

Da $a \neq 0$ und R nullteilerfrei ist, folgt $ba - 1 = 0$, also $ba = 1$

$\Rightarrow$ a ist Einheit $\lightning$ a keine Einheit.

Also: Jedes $a \in R \setminus \{0\}$ ist Einheit $\Rightarrow$ R Körper. $\blacksquare$

11.2. (i) Es gelte

$$v_1 = \mathrm{KgV}(a_1, \ldots, a_n)$$

$$v_2 = \mathrm{KgV}(a_1, \ldots, a_n)$$

$\overset{(\beta)}{\Longrightarrow}$ $v_1 \mid v_2$ und $v_2 \mid v_1$

Nach Vorlesung ist das aber äquivalent dazu, dass v_1 und v_2 assoziiert zueinander sind, d.h.

$\exists\ \varepsilon \in R$ Einheit mit $v_2 = \varepsilon v_1$.

(ii) „$\Leftarrow$": Sei $v \in R$ gegeben mit $(v) = \bigcap_{i=1}^{n} (a_i)$.

Zeigen: $v = \mathrm{KgV}(a_1, \ldots, a_n)$.

- Es ist $(v) \subset \bigcap_{i=1}^{n} (a_i) \iff \forall i\ (1 \leq i \leq n)$ ist $(v) \subset (a_i)$

$\iff \forall i\ (1 \leq i \leq n)$ gilt $a_i \mid v$

$\Rightarrow$ v erfüllt Bedingung (α).

- Sei nun $v' \in R$ gegeben mit $a_i \mid v'$ $\forall i\ (1 \leq i \leq n)$

$\overset{\text{siehe oben}}{\Longrightarrow}$ $(v') \subset \bigcap_{i=1}^{n} (a_i) = (v)$

$\Rightarrow$ $v \mid v'$

$\Rightarrow$ v erfüllt auch Bedingung (β).

$\Rightarrow$ $v = \mathrm{KgV}(a_1, \ldots, a_n)$.

„$\Rightarrow$": Gelte nun $v = \mathrm{KgV}(a_1, \ldots, a_n)$.

Zeigen: $(v) = \bigcap_{i=1}^{n} (a_i)$.

- Nach (α) gilt: $a_i \mid v \quad \forall i \ (1 \leq i \leq n)$

$$\xrightarrow[\text{von oben}]{\text{Argument}} (v) \subset \bigcap_{i=1}^{n} (a_i)$$

- Sei nun $w \in \bigcap_{i=1}^{n} (a_i)$.

$\Rightarrow \forall i \ (1 \leq i \leq n)$ ist $w \in (a_i)$ d.h. $\exists\, b_i \in R$ mit $w = b_i a_i$

$\Rightarrow \forall i \ (1 \leq i \leq n)$ gilt $a_i \mid w$.

$\overset{(\beta)}{\Rightarrow} v \mid w$

$\Rightarrow w \in (v)$.

Also gilt auch $\bigcap_{i=1}^{n} (a_i) \subset (v)$ und die Gleichheit ist insgesamt gezeigt.

(iii) Es gibt ein Kleinstes gemeinsames Vielfaches in R,

$$v = \mathrm{KgV}(9, 3(2+\sqrt{-5})).$$

Schreibe $v = a + b\sqrt{-5}$ mit $a, b \in \mathbb{Z}$.

Aus (α) folgt dann

$$9 \mid a+b\sqrt{-5} \quad \text{und} \quad 3(2+\sqrt{-5}) \mid a+b\sqrt{-5} \qquad (*)$$

- Es ist

$$9 \cdot 3 = 27 \quad \text{und} \quad 3(2+\sqrt{-5})(2-\sqrt{-5}) = 3 \cdot 9 = 27$$

$\Rightarrow$ 27 ist ein gemeinsames Vielfaches von 9 und $3(2+\sqrt{-5})$

$\overset{(B)}{\Rightarrow} \quad v \mid 27$

- Außerdem ist

$$9 \cdot (2+\sqrt{-5}) = 9(2+\sqrt{-5}) \quad \text{und} \quad 3(2+\sqrt{-5}) \cdot 3 = 9(2+\sqrt{-5})$$

$\Rightarrow$ $9(2+\sqrt{-5})$ ist ein gemeinsames Vielfaches von 9 und $3(2+\sqrt{-5})$

$\overset{(B)}{\Rightarrow} \quad v \mid 9(2+\sqrt{-5})$

Also erhalten wir:

$$a+b\sqrt{-5} \mid 27 \quad \text{und} \quad a+b\sqrt{-5} \mid 9(2+\sqrt{-5}) \qquad (**)$$

- $(*) \Rightarrow \quad 9 \mid a+b\sqrt{-5}$ d.h. $9(c+d\sqrt{-5}) = a+b\sqrt{-5}$ für gewisse $c,d \in \mathbb{Z}$

$$\Rightarrow 9c + 9d\sqrt{-5} = a + b\sqrt{-5}$$

Also: $9(c-d\sqrt{-5}) = a - b\sqrt{-5}$

und damit: $9 \mid a - b\sqrt{-5}$

- $(**) \Rightarrow \quad a+b\sqrt{-5} \mid 27$

$\Rightarrow \quad (a+b\sqrt{-5})(c+d\sqrt{-5}) = 27$ für gewisse $c,d \in \mathbb{Z}$

$$\Rightarrow \underbrace{ac - 5bd}_{\text{muss } 27 \text{ sein!}} + \underbrace{(ad+bc)}_{\text{muss } 0 \text{ sein!}}\sqrt{-5} = 27$$

Damit berechnen wir:

$$(a-b\sqrt{-5})(c-d\sqrt{-5}) = ac - 5bd - (ad+bc)\sqrt{-5}$$

$$= ac - 5bd$$

$$= 27$$

(Dieses Argument nennen wir (*))

$$\Rightarrow \quad a-b\sqrt{-5} \mid 27$$

Also erhalten wir:

$$9 \mid a-b\sqrt{-5} \quad \text{und} \quad a-b\sqrt{-5} \mid 27 \qquad (***)$$

Mit dieser Vorarbeit nun zur Aufgabe:

(*), (***) $\Rightarrow$ $81 \mid (a+b\sqrt{-5})(a-b\sqrt{-5})$ d.h. $81 \mid a^2+5b^2$

(**), (***) $\Rightarrow$ $(a+b\sqrt{-5})(a-b\sqrt{-5}) \mid 27^2$ d.h. $a^2+5b^2 \mid 729$

Es ist $81 = 3^4$ und $729 = 3^6$ also haben wir:

deshalb!

$$3^4 \cdot x = a^2+5b^2 \quad \text{und} \quad (a^2+5b^2)\,y = 3^6 \quad \text{für gewisse } x,y \in \mathbb{Z}$$

$\Rightarrow$ $3^4 \cdot x \cdot y = 3^6$ $\Rightarrow$ $x,y \in \mathbb{Z}$ und es gibt nur die Möglichkeiten

$x = 1 \quad y = 3^2$

oder $x = 3 \quad y = 3$

oder $x = 3^2 \quad y = 1$

Wegen $a^2+5b^2 = 3^4 \cdot x$ folgt also:

$$a^2+5b^2 \in \{3^4, 3^5, 3^6\} = \{81, 243, 729\}$$

Fallunterscheidung:

(1) Gelte $a^2 + 5b^2 = 243$.

Es ist $a^2 + 5b^2 \equiv a^2 + b^2 \mod 4$ (da $5 = 1$).

Die Multiplikation in $\mathbb{Z}/4\mathbb{Z}$ ist gegeben durch

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\Rightarrow \forall\, x \in \mathbb{Z}/4\mathbb{Z}$ ist $x^2 \in \{0, 1\}$

$$\Rightarrow a^2 + 5b^2 \equiv a^2 + b^2 \mod 4$$
$$\equiv 0, 1 \text{ oder } 2 \mod 4.$$

Aber: $a^2 + 5b^2 = 243 \equiv 3 \mod 4$ ↯

(2) Gelte $a^2 + 5b^2 = 81$.

$(*) \Rightarrow 9 \mid a + b\sqrt{-5}$, d.h.

$$9(c + d\sqrt{-5}) = a + b\sqrt{-5}$$

Das erste Argument für $(**)$ zeigt:

$$9(c - d\sqrt{-5}) = a - b\sqrt{-5}$$

$$\Rightarrow 81(c + d\sqrt{-5})(c - d\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5})$$

$$\Rightarrow 81(c^2 + 5d^2) = a^2 + 5b^2 = 81$$

$$\Rightarrow c^2 + 5d^2 = 1 \quad \Rightarrow c = \pm 1 \text{ und } d = 0$$

$$\Rightarrow v = a + b\sqrt{-5} = 9(c + d\sqrt{-5}) = \pm 9.$$

(!)

Andererseits folgt aus (*): $3(2+\sqrt{-5}) \mid a+b\sqrt{-5}$

und damit (Vorzeichen von v irrelevant!):

$$3(2+\sqrt{-5}) \mid 9$$

$\Rightarrow$ $3(2+\sqrt{-5})(e+f\sqrt{-5}) = 9$ für gewisse $e, f \in \mathbb{Z}$.

und mit einem Argument wie in (#):

$$3(2-\sqrt{-5})(e-f\sqrt{-5}) = 9$$

$\Rightarrow$ $9(4+5)(e^2+5f^2) = 9 \cdot 9$

$\Rightarrow$ $e^2+5f^2 = 1$

$\Rightarrow$ $e = \pm 1$, $f = 0$.

Also erhalten wir:

$$\pm 3(2+\sqrt{-5}) = 9 \quad \text{d.h.} \quad \pm(2+\sqrt{-5}) = 3 \quad \text{f.} \quad ↯$$

(3) Gelte nun $a^2+5b^2 = 729$

(**) $\Rightarrow$ $a+b\sqrt{-5} \mid 27$

$\Rightarrow$ $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 27$ für gewisse $c, d \in \mathbb{Z}$

Mit dem Argument (#) aus (***) folgt:

$$(a-b\sqrt{-5})(c-d\sqrt{-5}) = 27$$

$\Rightarrow$ $(a^2+5b^2)(c^2+5d^2) = 729$ d.h. $729(c^2+5d^2) = 729$

$\Rightarrow$ $c^2+5d^2 = 1$

$\Rightarrow$ $c = \pm 1$ und $d = 0$. $\Rightarrow$ $v = a+b\sqrt{-5} = \pm 27$.

Aus (**) folgt wieder

$$a + b\sqrt{-5} \mid 9(2+\sqrt{-5}) \quad \text{d.h.} \quad 27 \mid 9(2+\sqrt{-5})$$

$$\Rightarrow \quad 27(e+f\sqrt{-5}) = 9(2+\sqrt{-5}) \qquad \text{für gewisse } e,f \in \mathbb{Z}$$

$$\Rightarrow \quad (27e - 18) + (27f - 9)\sqrt{-5} = 0$$

$$\Rightarrow \quad \left[\begin{array}{l} 27e - 18 = 0 \\ 27f - 9 = 0 \end{array}\right. \qquad \text{in } \mathbb{Z} \text{ nicht lösbar, d.h. } e,f \notin \mathbb{Z} \qquad \lightning$$

Also: In jedem Fall ergibt sich ein Widerspruch, d.h. es gibt doch kein kleinstes gemeinsames Vielfaches.

$\blacksquare$

11.3. Der euklidische Algorithmus liefert folgendes Schema:

$$a_0 = q_1 a_1 + a_2 \qquad q_1 \in R, \quad \tau(a_2) < \tau(a_1)$$

$$a_1 = q_2 a_2 + a_3 \qquad q_2 \in R, \quad \tau(a_3) < \tau(a_2)$$

$$\vdots \qquad\qquad \vdots$$

$$(*) \quad a_{i-1} = q_i a_i + a_{i+1} \qquad q_i \in R \quad \tau(a_{i+1}) < \tau(a_i)$$

$$\vdots \qquad\qquad \vdots$$

$$a_{N-2} = q_{N-1} a_{N-1} + a_N \qquad q_{N-1} \in R \quad \tau(a_N) < \tau(a_{N-1})$$

$$a_{N-1} = q_N a_N + 0 \qquad q_N \in R$$

(i) • Letzte Gleichung in (*):

$$a_N \mid a_{N-1} \xRightarrow[\text{Gleichung}]{\text{zweitletzte}} a_N \mid a_{N-2}$$

Gilt für $i \in \mathbb{N}$: $a_N \mid a_{i+1}$ und $a_N \mid a_i$

$\Rightarrow$ Wegen $a_{i-1} = q_i a_i + a_{i+1}$ folgt auch $a_N \mid a_{i-1}$

Mit Induktion folgt also

$$a_N \mid a_1 \text{ und } a_N \mid a_0. \qquad \|$$

(„Schema von unten nach oben gelesen")

• Ist nun a ein beliebiger Teiler von a_0 und a_1, dann folgt:

$a \mid a_2$ wegen $a_2 = a_0 - q_1 a_1$

Gilt nun für $i \in \mathbb{N}, i < N$ $a \mid a_{i-1}$ und $a \mid a_i$,

dann folgt wegen $a_{i+1} = a_{i-1} - q_i a_i$ auch $a \mid a_{i+1}$.

Mit Induktion erhalten wir also

$$a \mid a_N .$$

(„Schema von oben nach unten gelesen").

Also: a_N ist ein gemeinsamer Teiler von a_0 und a_1 und für jeden anderen gemeinsamen Teiler a folgt $a \mid a_N$.

$\Rightarrow$ $a_N = \operatorname{ggT}(a_0, a_1)$.

(ii) Die zweitletzte Relation in (*) liefert

$$a_N = -q_{N-1} a_{N-1} + a_{N-2} \qquad (-q_{N-1} \in R).$$

Gilt für ein $i \in \mathbb{N}, i \leq N-2$

$$a_N = r_i^{(i)} a_i + r_{i+1}^{(i)} a_{i+1}$$

mit $r_i^{(i)}, r_{i+1}^{(i)} \in R$

dann liefert (*)

$$a_{i+1} = -q_i a_i + a_{i-1}$$

Einsetzen ergibt:

$$a_N = r_i^{(i)} a_i + r_{i+1}^{(i)} (-q_i a_i + a_{i-1})$$

$$= (r_i^{(i)} a_i - r_{i+1}^{(i)} q_i) a_i + r_{i+1}^{(i)} a_{i-1}$$

$$= r_{i-1}^{(i-1)} a_{i-1} + r_i^{(i-1)} a_i$$

mit $r_{i-1}^{(i-1)} := r_{i+1}^{(i)} \in R$

$r_i^{(i-1)} := r_i^{(i)} - r_{i+1}^{(i)} q_i \in R$

Also erhalten wir durch Induktion

$$a_N = r_0^{(0)} a_0 + r_1^{(0)} a_1$$

mit $r_0^{(0)}, r_1^{(0)} \in R$ d.h. die gesuchte Darstellung.

(iii) $f(X) = X^5 + X^4 + X^3 + X^2 + X + 1$

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

- $a_0 := f(X)$, $a_1 := g(X)$

Division mit Rest:

$$a_0(X) : a_1(X) = X \quad \text{Rest} \quad (-X^3+1)$$

$$\Rightarrow \quad a_0(X) = X \cdot a_1(X) + \underbrace{(-X^3+1)}_{= a_2(X)}$$

Division mit Rest:

$$a_1(X) : a_2(X) = -X - 1 \quad \text{Rest} \quad 2X^2 + 2X + 2$$

$$\Rightarrow \quad a_1(X) = (-X-1)\,a_2(X) + \underbrace{2X^2+2X+2}_{=a_3(X)}$$

Division mit Rest:

$$a_2(X) : a_3(X) = -\frac{1}{2}X + \frac{1}{2} \qquad \text{Rest: } 0 \qquad (\checkmark)$$

$$\Rightarrow \quad a_2(X) = \left(-\frac{1}{2}X + \frac{1}{2}\right) a_3(X)$$

$$\Rightarrow \quad a_3(X) = 2X^2+2X+2 = \operatorname{ggT}(f(X), g(X))$$

(gesuchtes $d(X)$).

- Berechne gesuchte Darstellung:

$$a_3(X) = a_1(X) + (X+1)\,a_2(X)$$

und $a_2(X) = a_0(X) - X\,a_1(X)$

Einsetzen liefert:

$$a_3(X) = a_1(X) + (X+1)\left(a_0(X) - X\,a_1(X)\right)$$

$$= (X+1)\,a_0(X) + (-X^2-X+1)\,a_1(X).$$

Also erhalten wir als Darstellung

$$\operatorname{ggT}(f(X), g(X)) = 2X^2+2X+2 = \underbrace{(X+1)}_{=:r(X)} f(X) + \underbrace{(-X^2-X+1)}_{=:s(X)} g(X)$$

$\blacksquare$

11.4. Aus Vorlesung bekannt:

$$\mathbb{Z}[\sqrt{-5}]^* = \{-1, 1\}.$$

Vorarbeit: Wir zeigen, dass $3 \in \mathbb{Z}[\sqrt{-5}]$ irreduzibel ist.

Dazu:

Schreibe $3 = \alpha \cdot \beta$ mit $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ und

$$\alpha = a_1 + a_2\sqrt{-5}$$
$$\beta = b_1 + b_2\sqrt{-5} \qquad a_1, a_2, b_1, b_2 \in \mathbb{Z}.$$

$$\Rightarrow \quad (a_1 + a_2\sqrt{-5})(b_1 + b_2\sqrt{-5}) = 3$$

$$\overset{\text{„Konjugation"}}{\Rightarrow} \quad (a_1 - a_2\sqrt{-5})(b_1 - b_2\sqrt{-5}) = 3$$

Zusammen folgt:

$$(a_1^2 + 5a_2^2)(b_1^2 + 5b_2^2) = 9$$

Wegen $a_1^2 + 5a_2^2 \geq 0$ treten also folgende Fälle auf:

$$a_1^2 + 5a_2^2 = 1$$
oder $a_1^2 + 5a_2^2 = 3$
oder $a_1^2 + 5a_2^2 = 9$

- Falls $a_1^2 + 5a_2^2 = 1$ gilt:

$\Rightarrow a_1 = \pm 1,\ a_2 = 0 \Rightarrow \alpha \in \mathbb{Z}[\sqrt{-5}]^*$ also Einheit

(liefert triviale Zerlegung).

- Falls $a_1^2 + 5a_2^2 = 3$ gilt:

  Es müsste $a_2 = 0$ und $a_1^2 = 3$ gelten.

  $\Rightarrow$ Es gibt keine Lösung in $\mathbb{Z} \times \mathbb{Z}$, der Fall kann also nicht auftreten

- Falls $a_1^2 + 5a_2^2 = 9$ gilt:

  $\Rightarrow b_1^2 + 5b_2^2 = 1$

  Also folgt mit dem Argument aus dem ersten Fall:

  $\beta \in \mathbb{Z}[\sqrt{-5}]^*$ d.h. β ist Einheit (triviale Zerlegung).

$\Rightarrow$ 3 ist irreduzibel.

Damit zur eigentlichen Aufgabe:

(i) Mögliche Zerlegungen von $f(X)$ sind:

(a) $\alpha(\beta X^2 + \gamma X + \delta) = f(X)$

mit $\alpha, \beta, \gamma, \delta \in \mathbb{Z}[\sqrt{-5}]$

(b) $(\alpha X + \beta)(\gamma X + \delta) = f(X)$

mit $\alpha, \beta, \gamma, \delta \in \mathbb{Z}[\sqrt{-5}]$ (Zerlegungen in 2 Faktoren!)

Möglichkeit (a):

$\Rightarrow \alpha \cdot \beta = 3.$

$\beta \in \mathbb{Z}[\sqrt{-5}]^* = \{-1, +1\}$ d.h. $\alpha = \pm 3$

$$\Rightarrow \quad f(X) = \alpha\,(\beta X^2 + \gamma X + \delta)$$

$$= \alpha \cdot \frac{1}{\alpha} f(X) \qquad \text{(Rechne in } K\text{!)}$$

$$\Rightarrow \quad \mathbb{Z}[\sqrt{-5}][X] \ni \beta X^2 + \gamma X + \delta = \frac{1}{\alpha} f(X).$$

Aber:

$$\frac{1}{\alpha} f(X) = \pm X^2 \pm \frac{4}{3} X \pm 1 \quad \notin \mathbb{Z}[\sqrt{-5}][X] \qquad ↯$$

β ist also keine Einheit $\overset{3 \text{ irred.}}{\Longrightarrow}$ α ist eine Einheit

$\Rightarrow$ Zerlegung (a) ist trivial.

Möglichkeit (b):

Wegen $\alpha \cdot \gamma = 3$ und da 3 in $\mathbb{Z}[\sqrt{-5}]$ irreduzibel ist, können wir OE annehmen, dass

$$\alpha = \pm 3 \quad \text{und} \quad \gamma = \pm 1$$

gilt. Außerdem gilt (analog):

$$\beta\,\delta = 3 \quad \text{und} \quad \beta, \delta \in \{-1, 1, -3, 3\}$$

$\Rightarrow$ In K gelesen muss f eine Nullstelle besitzen in der Menge

$\delta = \pm 1$ $\quad$ $\delta = \pm 3$ d.h. $\beta = \pm 1$.

$$\left\{\pm 1, \pm \frac{1}{3}\right\}$$

Aber: $f(1) = 10$, $f(-1) = 2$, $f(\frac{1}{3}) = \frac{16}{3}$, $f(-\frac{1}{3}) = \frac{8}{3}$ $\quad$ ↯

Zerlegungen des Typs (b) gibt es also nicht.

Insgesamt: $f(X)$ in $\mathbb{Z}[\sqrt{-5}][X]$ irreduzibel.

(ii) In $K[X]$ rechnen wir:

$$\frac{1}{3}(3X+2-\sqrt{-5})(3X+2+\sqrt{-5})$$

$$= \frac{1}{3}\Big(9X^2 + 6X + \cancel{3\sqrt{-5}X} + 6X + 4 + \cancel{2\sqrt{-5}} - \cancel{3\sqrt{-5}X}$$
$$- \cancel{2\sqrt{-5}} + 5\Big)$$

$$= \frac{1}{3}(9X^2 + 12X + 9)$$

$$= 3X^2 + 4X + 3$$

$$= f(X)$$

Da die „Klammerfaktoren" zu Beginn wegen $K[X]^* = K^*$ Keine Einheiten in $K[X]$ sind, ist dies eine nichttriviale Zerlegung und $f(X)$ ist in $K[X]$ reduzibel. $\blacksquare$

(Bemerkung: Die Zerlegung wurde heuristisch unter Verwendung der Lösungsformel in $\mathbb{C}$ gefunden, Motivation war $K \subset \mathbb{C}$.)