# Musterlösung Serie 13

DREI AUFGABEN ZU ALGEBRA I

---

**80**. Finde die kleinste positive ganze Zahl $n$ für die gilt:

$$\begin{aligned} n &\equiv 5 \pmod 7 \\ n &\equiv 7 \pmod{10} \\ n &\equiv 10 \pmod{13} \end{aligned}$$

*Lösung*: Wir betrachten zuerst die ersten beiden Bedingungen. Für $n$ muss gelten: $n = k \cdot 7 + 5$ und $n = l \cdot 10 + 7$, d.h.

$$k \cdot 7 + 5 = l \cdot 10 + 7 \quad \Longleftrightarrow \quad k \cdot 7 = l \cdot 10 + 2 \quad \Longleftrightarrow \quad k \cdot 7 - l \cdot 10 = 2$$

Wir suchen zuerst Zahlen $k'$ und $l'$ mit $k' \cdot 7 - l' \cdot 10 = 1$. Mit dem Algorithmus aus der Vorlesung erhalten wir:

$$\begin{aligned} 10 &= 1 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

| | | 1 | 2 | 3 |
|---|---|---|---|---|
| **0** | **1** | 1 | 3 | 10 |
| **1** | **0** | 1 | 2 | 7 |

Somit ist $k' = 3$ und $l' = 2$, also $k = 2 \cdot k' = 6$ und $l = 2 \cdot l' = 4$, und wir erhalten $n = 6 \cdot 7 + 5 = 47$. Für jede Zahl $n = s \cdot 70 + 47$ ist $n \equiv 5 \pmod 7$ und $n \equiv 7 \pmod{10}$. Damit die dritte Bedingung erfüllt ist, muss gelten $n = t \cdot 13 + 10$, d.h.

$$s \cdot 70 + 47 = t \cdot 13 + 10 \quad \Longleftrightarrow \quad s \cdot 70 + 37 = t \cdot 13 \quad \Longleftrightarrow \quad t \cdot 13 - s \cdot 70 = 37.$$

Wir suchen wieder zuerst Zahlen $s'$ und $t'$ mit $t' \cdot 13 - s' \cdot 70 = 1$, welche wir wieder mit dem Algorithmus aus der Vorlesung erhalten:

$$\begin{aligned} 70 &= 5 \cdot 13 + 5 \\ 13 &= 2 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

| | | 5 | 2 | 1 | 1 | 2 |
|---|---|---|---|---|---|---|
| **0** | **1** | 5 | 11 | 16 | 27 | 70 |
| **1** | **0** | 1 | 2 | 3 | 5 | 13 |

Somit ist $t' = 27$ und $s' = 5$, also $t = 37 \cdot t' = 999$ und $s = 37 \cdot s' = 185$, und wir erhalten, dass die Zahl $t \cdot 13 + 10 = 12\,997$ alle drei Bedingungen erfüllt. Da nun jede Zahl $12\,997 - m \cdot (7 \cdot 10 \cdot 13) = 12\,997 - m \cdot 910$ ebenfalls alle drei Bedingungen erfüllt, ist die kleinste positive Zahl, welche alle drei Bedingungen erfüllt: $n = 257$.

**81**. Bestimme bis auf Isomorphie alle Gruppen der Ordnung $20$.

*Lösung* (vgl. mit Aufgabe 54): Sei $G$ eine Gruppe der Ordnung $20$. Zuerst berechnen wir $|G| = 20 = 4 \cdot 5$. Die Anzahl aller Sylow $5$-Untergruppen muss kongruent $1$ modulo $5$ sein und $4$ teilen, ist also gleich $1$. Es gibt also nur eine, sie ist normal und isomorph zu $C_5 = \langle a \rangle$. Sei $H \leqslant G$ eine Untergruppe der Ordnung $4$. Da $C_5 \trianglelefteq G$ ist gilt $C_5H = HC_5$ und somit ist $C_5H$ nach Aufgabe 17.(b) eine Untergruppe von $G$. Wegen $C_5 \leqslant C_5H$ und $H \leqslant C_5H$, wird $|C_5H|$ nach dem Satz von Lagrange von $4$ und $5$ geteilt. Deshalb gilt $|C_5H| = 20$ und somit ist $C_5H = G$. Weiter muss $C_5 \cap H = \{e\}$ sein, denn die Ordnung jedes Elements im Schnitt muss die beiden teilerfremden Zahlen $4$ und $5$ teilen, also gleich $1$ sein. Somit sind alle Eigenschaften des semidirekten Produktes erfüllt.

Es gibt also einen Homomorphismus $\varphi\colon H \to \mathrm{Aut}(C_5)$ mit $G \cong H \ltimes_\varphi C_5$. In Aufgabe 37 haben wir $\mathrm{Aut}(C_5)$ bestimmt. Es ist

$$\mathrm{Aut}(C_5) := \{\psi_k : 1 \leqslant k \leqslant 4\},$$

wobei $\psi_k$ der Automorphismus ist, der $a \in C_5$ auf $a^k$ sendet. Weil $5$ eine Primzahl ist gilt $\mathrm{Aut}(C_5) \cong C_4$ (für Primzahlen $p$ gilt immer $\mathrm{Aut}(C_p) \cong C_{p-1}$). Wir machen nun eine Fallunterscheidung, nämlich $H = C_4 = \langle g \rangle$ und $H = C_2 \times C_2 = \langle h \rangle \times \langle h \rangle$.

Sei zuerst $H = C_4$. Dann ist $\varphi\colon H \to \mathrm{Aut}(C_5)$, also $\varphi\colon C_4 \to C_4$, eindeutig durch das Bild eines Erzeugers von $C_4$ gegeben. Wegen $\mathrm{ord}(\varphi(g)) \,|\, \mathrm{ord}(g)$ gibt es bis auf Isomorphie nur drei Möglichkeiten für $\varphi(g)$, nämlich $\varphi_1(g) = \psi_1$, $\varphi_2(g) = \psi_2$ und $\varphi_4(g) = \psi_4$. Beachte, dass gilt:

$$\psi_4\big(\psi_4(g)\big) = \psi_4(a^4) = (a^4)^4 = a^{16} = a^1 = a$$

d.h. $\psi_4^2$ ist die Identität und $\mathrm{ord}(\psi_4) = 2$. Im ersten Fall ist $G = C_4 \times C_5 \cong C_{20}$, und im zweiten und dritten Fall ist $G = C_4 \ltimes_{\varphi_2} C_5$ bzw. $G = C_4 \ltimes_{\varphi_4} C_5$ ein nichttriviales semidirektes Produkt.

Sei nun $H = C_2 \times C_2$. Weil die Elemente $(h, e)$ und $(e, h)$ Ordnung $2$ haben, kommt für $\varphi(h, e)$ und $\varphi(e, h)$ jeweils auch nur $\psi_1$ oder $\psi_4$ infrage. Bis auf Isomorphie gibt es somit nur zwei Möglichkeiten für $\varphi$, nämlich:

- $\varphi_1(e,e) = \psi_1,\ \varphi_1(h,e) = \psi_1,\ \varphi_1(e,h) = \psi_1,\ \varphi_1(h,h) = \psi_1$
- $\varphi_4(e,e) = \psi_1,\ \varphi_4(h,e) = \psi_4,\ \varphi_4(e,h) = \psi_4,\ \varphi_4(h,h) = \psi_1$

Im ersten Fall ist $G = C_2 \times C_2 \times C_5$, und im zweiten Fall ist $G = (C_2 \times C_2) \ltimes_{\varphi_4} C_5$ ein nichttriviales semidirektes Produkt. Da letzteres die einzige nichtabelsche Gruppe ist, die kein Element der Ordnung $4$ enthält, gilt $(C_2 \times C_2) \ltimes_{\varphi_4} C_5 \cong D_{10}$.

**82**. Im Ring $R := \mathbb{Z}[i\sqrt{5}] \subset \mathbb{C}$ gilt die Gleichheit

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Zeige:

(a) Die Funktion $N\colon R \to \mathbb{N}, z = a + bi\sqrt{5} \mapsto |z|^2 = a^2 + 5b^2$ ist multiplikativ (das heisst, $\forall \alpha, \beta \in R : N(\alpha\beta) = N(\alpha)N(\beta)$).

(b) $R^* = \{u \in R \mid N(u) = 1\} = \{\pm 1\}$.

(c) Die Elemente $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ sind unzerlegbar in $R$.

(d) Die Elemente $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ sind keine Primelemente in $R$.

(e) Für das Ideal $I = (2, 1 + i\sqrt{5})$ gilt $I \cdot I = (2)$.

(f) $I$ ist kein Hauptideal von $R$.

(g) $I$ ist ein maximales Ideal von $R$.

(h) Kein anderes Primideal enthält die Zahl $2$.

(i) $R$ ist nicht faktoriell.

*Lösung*: (a) F"ur alle $\alpha \in R$ gilt $N(\alpha) = |\alpha|^2$, wobei $|\cdot|$ den gewöhnlichen komplexen Absolutbetrag bezeichnet. Für alle $\alpha, \beta \in R$ folgt daraus

$$N(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2|\beta|^2 = N(\alpha)N(\beta),$$

wie gewünscht.

*Variante:* Seien $\alpha = a_1 + a_2 i\sqrt{5}$ und $\beta = b_1 + b_2 i\sqrt{5} \in R$. Dann ist

$$\begin{aligned} N(\alpha\beta) &= N(a_1b_1 - 5a_2b_2 + (a_1b_2 + a_2b_1)i\sqrt{5}) \\ &= (a_1b_1 - 5a_2b_2)^2 + 5(a_1b_2 + a_2b_1)^2 \\ &= a_1^2b_1^2 + 25a_2^2b_2^2 + 5a_1^2b_2^2 + 5a_2^2b_1^2 \\ &= (a_1^2 + 5b_1^2)(b_1^2 + 5b_2^2) \\ &= N(a_1 + a_2 i\sqrt{5})N(b_1 + b_2 i\sqrt{5}) = N(\alpha)N(\beta). \end{aligned}$$

(b) Betrachte eine Einheit $u = a + bi\sqrt{5} \in R$. Da $N$ multiplikativ ist, gilt $N(u^{-1}) \cdot N(u) = N(u^{-1}u) = N(1) = 1$. Wegen $N(u^{-1}), N(u) \in \mathbb{N}$ muss daher $N(u) = a^2 + 5b^2 = 1$ sein. Daraus folgt sofort $b = 0$ und $a^2 = 1$, also $u = a = \pm 1$. Umgekehrt gilt für jedes Element $u = a + bi\sqrt{5} \in R$ mit $a^2 + 5b^2 = 1$ auch $(a + bi\sqrt{5})(a - bi\sqrt{5}) = 1$, also ist $u$ eine Einheit in $R$.

(c) Falls $2 = \alpha\beta$ mit $\alpha, \beta \in R$ ist, folgt $4 = N(2) = N(\alpha)N(\beta)$. Wenn $\alpha$ und $\beta$ keine Einheiten sind, ist $N(\alpha), N(\beta) > 1$ nach (b). Es gibt dann nur die Möglichkeit $N(\alpha) = N(\beta) = 2$. Diese kann aber nicht auftreten, da 2 wegen $a^2 + 5b^2 \neq 2$ für alle $a, b \in \mathbb{Z}$ nicht im Bild von $N$ liegt. Somit ist 2 unzerlegbar in $R$.

Wegen $a^2 + 5b^2 \neq 3$ für alle $a, b \in \mathbb{Z}$ liegt auch 3 nicht im Bild von $N$. Wegen $N(3) = 9 = 3 \cdot 3$ folgt darum analog, dass 3 unzerlegbar in $R$ ist.

Falls $1 + i\sqrt{5} = \alpha\beta$ mit $\alpha, \beta \in R$ ist, folgt $6 = N(1 + i\sqrt{5}) = N(\alpha)N(\beta)$. Wenn $\alpha$ und $\beta$ keine Einheiten sind, dann müssen $N(\alpha), N(\beta) \in \{2, 3\}$ sein. Dies ist wiederum nicht

möglich, da 2 und 3 nicht im Bild von $N$ liegen. Daher ist $1 + i\sqrt{5}$ unzerlegbar. Mit der gleichen Argumentation folgt auch die Unzerlegbarkeit von $1 - i\sqrt{5}$.

(d) Wegen der Gleichheit $6 = 2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$ sind 2 und 3 Teiler von $(1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$ und $1 + i\sqrt{5}$ und $1 - i\sqrt{5}$ Teiler von $2 \cdot 3$. Keines der vier Elemente ist aber ein Teiler eines anderen, weil sie nach (c) unzerlegbar sind, sich aber nach (b) nicht um Einheiten unterscheiden, da sie vershiedene Bilder unter $N$ haben.

(e) Durch Multiplikation der Erzeuger erhalten wir

$$I \cdot I = (2, 1 + i\sqrt{5})(2, 1 + i\sqrt{5}) = (4, 2 + 2i\sqrt{5}, -4 + 2i\sqrt{5}).$$

Da $(2) = \{2a + 2bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ ist, haben wir $4, 2 + 2i\sqrt{5}, -4 + 2i\sqrt{5} \in (2)$ und daher $I \cdot I \subset (2)$. Umgekehrt ist

$$2 = (2 + 2i\sqrt{5}) - (-4 + 2i\sqrt{5}) - 4 \in I \cdot I.$$

Somit gilt $(2) = I \cdot I$.

(f) Wir nehmen an, dass $I$ ein Hauptideal ist, d.h. $I = (2, 1 + i\sqrt{5}) = (\alpha)$ für ein $\alpha \in R$. Dann ist $2 = x\alpha$ für ein $x \in R$. Wegen der Unzerlegbarkeit von 2 ist entweder $x \in R^\times$ oder $\alpha \in R^\times$. Im ersten Fall ist 2 assoziiert zu $\alpha$, also $(2) = (\alpha) = (2, 1 + i\sqrt{5})$. Dies ist ein Widerspruch, da $1 + i\sqrt{5}$ nicht in $(2)$ liegt.

Es bleibt nur der Fall $\alpha \in R^\times$ übrig, in dem $I = (\alpha) = R$ ist. Auch dieser Fall kann nach (e) wegen des Widerspruchs

$$R = R \cdot R = I \cdot I = (2) \neq R$$

nicht auftreten. Somit ist $I$ kein Hauptideal.

(g) Aus (f) folgt bereits, dass $I \neq (1)$, also ein echtes Ideal ist. Betrachte ein echt grösseres Ideal $I \subsetneq I' \subset R$ und wähle ein Element $a + bi\sqrt{5} \in I' \backslash I$. Die Rechnung $a + bi\sqrt{5} = (a - b) + b \cdot (1 + i\sqrt{5})$ zeigt dann, dass $a - b \notin I$ ist. Wegen $\mathbb{Z} \cap I = 2\mathbb{Z}$ bedeutet dies, dass $a - b$ ungerade ist. Also ist

$$1 = (a + bi\sqrt{5}) - \tfrac{a-b-1}{2} \cdot 2 - b \cdot (1 + i\sqrt{5}) \in (a + bi\sqrt{5}) + I \subset I'.$$

Somit ist $I' = (1)$; und deshalb ist $I$ maximal.

(h) Sei $\mathfrak{p}$ ein Primideal, das 2 enthält. Dann ist auch $2 + 2 + 2 = 6 \in \mathfrak{p}$. Somit muss das Ideal $1 + i\sqrt{5}$ oder $1 - i\sqrt{5}$ enthalten. Wegen $1 + i\sqrt{5} = 2 - (1 - i\sqrt{5})$ enthält $\mathfrak{p}$ dann sowohl $1 + i\sqrt{5}$ als auch $1 - i\sqrt{5}$ und es folgt $I \subseteq \mathfrak{p}$. Da $I$ maximal ist, folgt $I = \mathfrak{p}$.

(i) Mögliche Lösungen sind:

- Aus (c) und (d) folgt, dass in $R$ unzerlegbare Elemente existieren, die nicht prim sind. Daher ist $R$ nicht faktoriell.
- Die Gleichung $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ ergibt nach (c) zwei Zerlegungen von 6 in unzerlegbare Elemente. Bei (d) haben wir festgestellt, dass $2, 3 \nmid 1 \pm i\sqrt{5}$ und $1 \pm i\sqrt{5} \nmid 2, 3$ gilt. Daher sind $2, 3$ nicht zu $1 \pm i\sqrt{5}$ assoziiert und die beiden obigen Zerlegungen sind nicht zueinander assoziiert. Deshalb kann $R$ nicht faktoriell sein.