TU Chemnitz – Professur Numerische Mathematik
Prof. Dr. Fleurianne Bertrand
C. Bombach, T.-C. Riemer, Dr. M. Winkler

15. Januar 2024

Mathematik III (für IF, ET, Ph)

Wintersemester 2023/24

9. Übung: Algebraische Strukturen (Musterlösung)

Aufgabe 1

Zeigen Sie, dass $(\mathbb{Z}, \circ)$ mit der Operation $a \circ b := a+b-ab$ eine Halbgruppe ist. Gibt es ein neutrales Element? Falls ja, welche Elemente besitzen Inverse?

Lösung:

Wiederholung: Halbgruppe, neutrales Element, Inverse.

Wir verifizieren die Halbgruppeneigenschaften: Abgeschlossenheit und Assoziativgesetz.

- Abgeschlossenheit:
  Für $n, m \in \mathbb{Z}$ folgt $n \circ m = n + m - nm \in \mathbb{Z}$, da $n + m \in \mathbb{Z}$ und $nm \in \mathbb{Z}$.
- Assoziativgesetz:
  Es gilt für $a, b, c \in \mathbb{Z}$, dass

$$\begin{aligned}(a \circ b) \circ c &= (a + b - ab) \circ c = (a + b - ab) + c - c(a + b - ab)\\ &= a + b + c - ab - ac - bc + abc\\ &= a + (b + c - bc) - a(b + c - bc) = a \circ (b + c - bc) = a \circ (b \circ c).\end{aligned}$$

Damit ist $(\mathbb{Z}, \circ)$ eine Halbgruppe.

Das neutrale Element e, falls es existiert, muss folgendes erfüllen

$$a = a \circ e = e \circ a = a + e - ae \qquad \forall a \in \mathbb{Z}.$$

Dies ist äquivalent zu

$$0 = e - ae = (1 - a)e \qquad \forall a \in \mathbb{Z}.$$

Ergo, ist $e = 0$ das neutrale Element in $(\mathbb{Z}, \circ)$.

Es gilt nun, dass $a \in \mathbb{Z}$ ein Inverses $a^{-1} \in \mathbb{Z}$ bzgl. $\circ$ besitzt, falls

$$0 = e = a \circ a^{-1} = a^{-1} \circ a = a + a^{-1} - aa^{-1} = a + (1 - a)a^{-1}.$$

D.h., a besitzt ein Inverses, falls $a^{-1} = \frac{a}{a-1} \in \mathbb{Z}$. Ein Überprüfen für $a \in \{-2, -1, 0, 1, 2\}$ (andere a sind ausgeschlossen) liefert, dass nur $a = e = 0$ und $a = 2$ ein Inverses, nämlich 0 bzw. 2, haben.

Damit ist $(\mathbb{Z}, \circ)$ also keine Gruppe, aber ein Monoid.

Aufgabe 2

Welche der folgenden Beispiele sind Gruppen? Dabei bezeichnen $+$ und $\cdot$ die übliche Addition und Multiplikation reeller Zahlen.

a) $(G, +)$ mit $G = \{2n \mid n \in \mathbb{Z}\}$,

b) $(G, \cdot)$ mit $G = \{2n \mid n \in \mathbb{Z}\}$,

c) $(G, +)$ mit $G = \{2^n \mid n \in \mathbb{Z}\}$,

d) $(G, \cdot)$ mit $G = \{2^n \mid n \in \mathbb{Z}\}$.

Lösung:

Wiederholung: Gruppe, Gruppeneigenschaften.

Wir verifizieren nachfolgend für jedes der Beispiele die 4 Gruppeneigenschaften: Abgeschlossenheit, Assoziativgesetz, Neutrales Element, Inverses.

(a) $(G, +)$ mit $G = \{2n \mid n \in \mathbb{Z}\}$.

- Abgeschlossenheit:
  Für $n, m \in \mathbb{Z}$ folgt $(2n) + (2m) = 2(n + m) \in G$, da $n + m \in \mathbb{Z}$.
- Assoziativgesetz:
  Erfüllt, da Addition auf reellen Zahlen assoziativ. Bzw. da für $k, n, m \in \mathbb{Z}$ gilt $2n + [2m + 2k] = 2n + 2m + 2k = [2n + 2m] + 2k$.
- Neutrales Element:
  Für $n \in \mathbb{Z}$ gilt $2n + 2 \cdot 0 = 2n = 2 \cdot 0 + 2n$. Also $2 \cdot 0 \in G$ ist neutrales Element in G bzgl. $+$.
- Inverses Element:
  Für $n \in \mathbb{Z}$ folgt $2n + 2(-n) = 0 = 2(-n) + 2n$. Also ist $2(-n) \in G$ das Inverse zu $2n \in G$ bzgl. $+$.

$\Rightarrow G$ ist Gruppe.

(b) $(G, \cdot)$ mit $G = \{2n \mid n \in \mathbb{Z}\}$.

- Abgeschlossenheit:
  Für $n, m \in \mathbb{Z}$ folgt $(2n) \cdot (2m) = 2(2nm) \in G$, da $2nm \in \mathbb{Z}$.
- Assoziativgesetz:
  Erfüllt, da Multiplikation auf reellen Zahlen assoziativ. Bzw. da für $k, n, m \in \mathbb{Z}$ gilt $2n \cdot [2m \cdot 2k] = 2n \cdot 2m \cdot 2k = [2n \cdot 2m] \cdot 2k$.
- Neutrales Element:
  Angenommen, es sei $e = 2m$ mit $m \in \mathbb{Z}$ das neutrale Element in G und $0 \neq n \in \mathbb{Z}$. Dann folgt

  $$2n = 2n \cdot e = 2n \cdot 2m = 2(2nm) \quad \Longleftrightarrow \quad n = 2nm \quad \Longleftrightarrow \quad m = \frac{1}{2} \notin \mathbb{Z},$$

  was ein Widerspruch darstellt.

$\Rightarrow G$ ist keine Gruppe, da kein neutrales Element in G existiert. G ist damit eine Halbgruppe.

(c) $(G, +)$ mit $G = \{2^n \mid n \in \mathbb{Z}\}$.

- Abgeschlossenheit:
  Für $n, m \in \mathbb{Z}$ gilt nicht immer $2^n + 2^m \in G$. Z.B. mit $n = 1$ und $m = 0$ folgt $2^1 + 2^0 = 3$.

$\Rightarrow G$ ist keine Gruppe, da nicht abgeschlossen bzgl. $+$.

(d) $(G, \cdot)$ mit $G = \{2^n \mid n \in \mathbb{Z}\}$.

- Abgeschlossenheit:
  Für $n, m \in \mathbb{Z}$ folgt $2^n \cdot 2^m = 2^{n+m} \in G$, da $n + m \in \mathbb{Z}$.
- Assoziativgesetz:
  Erfüllt, da Multiplikation auf reellen Zahlen assoziativ.
- Neutrales Element:
  Für $n \in \mathbb{Z}$ gilt $2^n \cdot 2^0 = 2^n \cdot 1 = 2^n = 2^0 \cdot 2^0$. Also $2^0 \in G$ ist neutrales Element in G bzgl. $\cdot$.
- Inverses Element:
  Für $n \in \mathbb{Z}$ folgt $2^n \cdot 2^{-n} = 2^0 = 2^{-n} \cdot 2^n$. Also ist $2^{-n} \in G$ das Inverse zu $2^n \in G$ bzgl. $\cdot$.

$\Rightarrow G$ ist Gruppe.

Aufgabe 3

Bestimmen Sie alle Untergruppen der folgenden zyklischen Gruppe

$$G = \{e, a, a^2, a^3, a^4, a^5\}.$$

Welche dieser Untergruppen ist ein Normalteiler von G?

Lösung:

Wiederholung: Untergruppe, zyklische Gruppe, Normalteiler.

Wir erhalten sofort die trivialen Untergruppen

$$U_1 := \{e\}, \qquad U_6 := \{e, a, a^2, a^3, a^4, a^5\} = G,$$

siehe Vorlesung.

Zum Auffinden anderer Untergruppen gehen wir systematisch vor und untersuchen die von jedem Element erzeugte Untergruppe:

- Jede Untergruppe muss e enthalten.
- Die Untergruppe, die von a erzeugt wird ist wieder $\langle a \rangle = G = U_6$.
- Die Untergruppe, die von a^2 erzeugt wird ist

$$\langle a^2 \rangle = \{a^2, a^4, e\} =: U_3.$$

- Die Untergruppe, die von a^3 erzeugt wird ist

$$\langle a^3 \rangle = \{a^3, e\} =: U_2.$$

- Die Untergruppe, die von a^4 erzeugt wird ist wieder $\langle a^4 \rangle = U_3$.
- Die Untergruppe, die von a^5 erzeugt wird ist wieder $\langle a^5 \rangle = U_6$:

$$\langle a^5 \rangle = \{a^5, a^4, a^3, a^2, a^1, e\} = G.$$

Hinweis: Der *Satz von Lagrange* besagt, dass für jede Untergruppe U von G, die Mächtigkeit $|U|$ gerade $|G|$ teilt. Hier geht also nur $|U| \in \{1, 2, 3, 6\}$.

Ein Normalteiler ist eine Untergruppe U, für die gilt

$$a \circ U = U \circ a, \qquad \forall a \in G.$$

Aus der Vorlesung wissen wir, dass für abelsche Gruppen (kommutative Gruppen), alle Untergruppen Normalteiler sind (offensichtlich!) – Folie 294. Weiterhin wissen wir, dass zyklische Gruppen abelsch sind – Folie 291. Damit sind alle Untergruppen U_1, U_2, U_3, U_6 Normalteiler von G.

Aufgabe 4

Geben sei die Menge

$$\mathbb{Q}(\sqrt{5}) := \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$$

sowie folgende Addition und Multiplikation auf $\mathbb{Q}(\sqrt{5})$

$$\begin{aligned}(a + b\sqrt{5}) \oplus (c + d\sqrt{5}) &:= (a + c) + (b + d)\sqrt{5},\\ (a + b\sqrt{5}) \odot (c + d\sqrt{5}) &:= (a \cdot c + 5 \cdot b \cdot d) + (a \cdot d + b \cdot c)\sqrt{5}.\end{aligned}$$

Zeigen Sie, dass $(\mathbb{Q}(\sqrt{5}), \oplus, \odot)$ ein Körper ist.

Hinweis: Erinnert Sie die Definition der Operationen auf $\mathbb{Q}(\sqrt{5})$ an etwas? Z.B. an die Operationen auf einer ähnlich definierten Menge mit reellen Koeffizienten a, b aus Mathematik I?

Lösung:

Wiederholung: Körper, Körpereigenschaften.

Wir verifizieren die Körpereigenschaften für die Menge

$$\mathbb{Q}(\sqrt{5}) := \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$$

mit den Operationen

$$\begin{aligned}(a + b\sqrt{5}) \oplus (c + d\sqrt{5}) &:= (a + c) + (b + d)\sqrt{5},\\ (a + b\sqrt{5}) \odot (c + d\sqrt{5}) &:= (a \cdot c + 5 \cdot b \cdot d) + (a \cdot d + b \cdot c)\sqrt{5}.\end{aligned}$$

- $(\mathbb{Q}(\sqrt{5}), \oplus)$ ist eine abelsche Gruppe:
  - Seien $a, b, c, d \in \mathbb{Q}$ so ist $(a + b\sqrt{5}) \oplus (c + d\sqrt{5})$ wieder in $\mathbb{Q}(\sqrt{5})$, da $a + c, b + d \in \mathbb{Q}$.
  - Die Kommutativität folgt aus der Kommutativität der Addition in $\mathbb{Q}$: Seien $a, b, c, d \in \mathbb{Q}$ so ist

$$\begin{aligned}(a + b\sqrt{5}) \oplus (c + d\sqrt{5}) &= (a + c) + (b + d)\sqrt{5},\\ &= (c + d\sqrt{5}) \oplus (a + b\sqrt{5}).\end{aligned}$$

  - Die Assoziativität von $\oplus$ folgt direkt aus der Assoziativität der Addition in $\mathbb{R}$.
  - Neutrales Element ist $(0 + 0\sqrt{5})$, denn für $a + b\sqrt{5} \in \mathbb{Q}(\sqrt{5})$ folgt dann

$$(a + b\sqrt{5}) \oplus (0 + 0\sqrt{5}) = (a + 0) + (b + 0)\sqrt{5} = (a + b\sqrt{5})$$

    und analog von links.

– Das Inverse zu $a + b\sqrt{5} \in \mathbb{Q}(\sqrt{5})$ ist $(-a) + (-b)\sqrt{5} \in \mathbb{Q}(\sqrt{5})$:

$$(a + b\sqrt{5}) \oplus (-a + (-b)\sqrt{5}) = (a - a) + (b - b)\sqrt{5} = (0 + 0\sqrt{5})$$

und analog von links.

- Die Kommutativität von $\odot$ folgt aus der Kommutativität in $\mathbb{Q}$: Seien $a, b, c, d \in \mathbb{Q}$ so ist

$$\begin{aligned}(a + b\sqrt{5}) \odot (c + d\sqrt{5}) &= (ac + 5bd) + (bc + ad)\sqrt{5}, \\ &= (c + d\sqrt{5}) \odot (a + b\sqrt{5}).\end{aligned}$$

- Die Assoziativität von $\odot$ folgt ebenfalls aus der Assoziativität und Distributiviät der Multiplikation und Addition in $\mathbb{Q}$ – Hausaufgabe bzw. Fleißaufgabe.

- Sei $(e + f\sqrt{5})$ das neutrale Element bzgl. $\odot$, so müssen e, f folgendes erfüllen:

$$(a + b\sqrt{5}) \odot (e + f\sqrt{5}) = (ae + 5bf) + (af + be)\sqrt{5} = a + b\sqrt{5},$$

also $ae + 5bf = a$ und $af + be = b$. Dies führt auf $e = 1$ und $f = 0$, also $(1 + 0\sqrt{5})$ als neutrales Element.

- Das Inverse zu $a + b\sqrt{5} \in \mathbb{Q}(\sqrt{5})$ ist – analog zu den komplexen Zahlen – gegeben durch

$$\frac{a}{a^2 - 5b^2} + \frac{-b}{a^2 - 5b^2}\sqrt{5}$$

denn

$$\begin{aligned}&(a + b\sqrt{5}) \odot \left(\frac{a}{a^2 - 5b^2} + \frac{-b}{a^2 - 5b^2}\sqrt{5}\right) \\ &= \left(\frac{a^2}{a^2 - 5b^2} + \frac{-5b^2}{a^2 - 5b^2}\right) + \left(\frac{-ab}{a^2 - 5b^2} + \frac{ab}{a^2 - 5b^2}\right)\sqrt{5} = 1 + 0\sqrt{5}\end{aligned}$$

und analog von links.

- Distributivgesetz: Es seien $a, b, c, d, x, y \in \mathbb{Q}$. Dann folgt

$$\begin{aligned}(a + b\sqrt{5}) \odot \Big[(c + d\sqrt{5}) \oplus (x + y\sqrt{5})\Big] &= (a + b\sqrt{5}) \odot \Big((c + x) + (d + y)\sqrt{5}\Big) \\ &= [a(c + x) + 5b(d + y)] + [a(d + y) + b(c + x)]\sqrt{5}\end{aligned}$$

sowie

$$\begin{aligned}&\Big[(a + b\sqrt{5}) \odot (c + d\sqrt{5})\Big] \oplus \Big[(a + b\sqrt{5}) \odot (x + y\sqrt{5})\Big] \\ &= \Big[(ac + 5bd) + (ad + bd)\sqrt{5}\Big] \oplus \Big[(ax + 5by) + (ay + bx)\sqrt{5}\Big] \\ &= [a(c + x) + 5b(d + y)] + [a(d + y) + b(c + x)]\sqrt{5}.\end{aligned}$$

Aufgabe 5

(a) Es sei $\mathcal{P}(\mathbb{N})$ die Potenzmenge der natürlichen Zahlen. Untersuchen Sie die Relationen $\subseteq$ und $\not\subseteq$ auf Reflexivität, Symmetrie und Transitivität.

(b) Es sei $M = \{1, 2, 3\}$. Zeigen Sie, dass

$$(a, b)\, R\, (c, d) \iff (a, b) = (c, d) \text{ oder } (a, b) = (d, c)$$

eine Äquivalenzrelation auf $M \times M$ ist. In wie viele Äquivalenzklassen teilt R die Menge $M \times M$?

Lösung:

Wiederholung: Äquivalenzrelation, Äquivalenklassen.

(a) Wir betrachten die Potenzmenge $\mathcal{P}(\mathbb{N})$ mit den Relationen $\subseteq$ und $\not\subseteq$. Die Relation $\subseteq$ ist

- reflexiv: $A \subseteq A$ für $A \in \mathcal{P}(\mathbb{N})$.
- nicht symmetrisch: $A := \{1\} \subseteq \{1, 2\} =: B$ aber $B \not\subseteq A$.
- transitiv: Sei $A \subseteq B$ und $B \subseteq C$, dann folgt $A \subseteq B \subseteq C$ also $A \subseteq C$ für $A, B, C \in \mathcal{P}(\mathbb{N})$.

Die Relation $\not\subseteq$ ist auf $\mathcal{P}(\mathbb{N})$, wobei $A \not\subseteq B$ falls $\exists n \in \mathbb{N} : n \in A \ \wedge \ n \notin B$, ist

- nicht reflexiv: $A \subseteq A$ für $A \in \mathcal{P}(\mathbb{N})$.
- nicht symmetrisch: $A := \{1, 2\} \not\subseteq \{1\} =: B$ aber $B \subseteq A$.
- nicht transitiv: für $A = \{1, 2\} \not\subseteq \{3\} = B$ und $B \not\subseteq \{1, 2, 4\} = C$ gilt $A \subseteq C$.

(b) Die Relation $(a, b)\, R\, (c, d) \iff (a, b) = (c, d) \vee (a, b) = (d, c)$ auf $\{1, 2, 3\} \times \{1, 2, 3\}$ ist

- reflexiv: $(a, b)R(a, b)$, da $(a, b) = (a, b)$.
- symmetrisch: Wenn $(a, b)R(c, d)$, also $(a, b) = (c, d) \vee (a, b) = (d, c)$, dann auch $(c, d) = (a, b) \vee (c, d) = (b, a)$, also $(c, d)R(a, b)$.
- transitiv: Ist $(a, b)R(c, d)$ und $(c, d)R(e, f)$, dann ist

$$(a, b) = (c, d) = (e, f) \quad \text{oder} \quad (a, b) = (c, d) = (f, e)$$

oder

$$(a, b) = (d, c) = (f, e) \quad \text{oder} \quad (a, b) = (d, c) = (e, f).$$

Aus allen 4 Fällen folgt $(a, b)R(e, f)$.

Die Restklassen sind mit $a, b \in \{1, 2, 3\}$, $a \neq b$,

$$[(a, a)]_R = \{(a, a)\}, \qquad [(a, b)]_R = \{(a, b), (b, a)\}.$$

Es gibt also $3 + 3 = 6$ Restklassen, nämlich $[(1, 1)]_R$, $[(2, 2)]_R$, $[(3, 3)]_R$, $[(1, 2)]_R$, $[(1, 3)]_R$ und $[(2, 3)]_R$.

Aufgabe 6

Stellen Sie die Additions- und Multiplikationstafeln für $\mathbb{Z}_3$ und $\mathbb{Z}_6$ auf.

Verifizieren Sie mittels dieser Tabellen, dass $(\mathbb{Z}_3, +)$, $(\mathbb{Z}_3 \setminus \{0\}, \cdot)$ sowie $(\mathbb{Z}_6, +)$ Gruppen sind, $(\mathbb{Z}_6 \setminus \{0\}, \cdot)$ allerdings keine Gruppe ist.

Lösung:

Wir schreiben die Restklassen ohne Klammern, z.B. 1 statt $[1]_3$.

(a) $\mathbb{Z}_3$, Additions- und Multiplikationstabelle

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

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

(b) $\mathbb{Z}_6$, Additions- und Multiplikationstabelle

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Aufgabe 7

Bestimmen Sie die folgenden additiven Inversen

a) zu 1 in $\mathbb{Z}_{20}$, b) zu 4 in $\mathbb{Z}_{12}$, c) zu 199 in $\mathbb{Z}_{200}$,

sowie die folgenden multiplikativen Inversen

d) zu 2 in $\mathbb{Z}_7$, e) zu 7 in $\mathbb{Z}_{23}$, f) zu 10 in $\mathbb{Z}_{51}$.

Lösung:

Um das additive Inverse zu $n \in \mathbb{Z}_p$, $0 \leq n < p$, zu finden, suchen wir diejenige Zahl $0 \leq m < p$ mit $p = n + m$.

(a) Es gilt $1 + 19 = 20$, also ist 19 das additive Inverse zu 1 in $\mathbb{Z}_{20}$.

(b) Es gilt $4 + 8 = 12$, also ist 8 das additive Inverse zu 4 in $\mathbb{Z}_{12}$.

(c) Es gilt $199 + 1 = 200$, also ist 1 das additive Inverse zu 199 in $\mathbb{Z}_{200}$.

Um das multiplikative Inverse zu $n \in \mathbb{Z}_p$, $0 \leq n < p$, zu finden, suchen wir diejenige Zahl $0 \leq m < p$ mit $1 = nm \mod p$, also $nm = 1 + kp$ mit $k \in \mathbb{N}$. Dazu bietet es sich an sukzessiv $1 + kp$ für $k = 1, \ldots$ auf Teilbarkeit mit n zu überprüfen

(a) $8 = 1 + 7$ ist durch 2 teilbar und es folgt, dass 4 das multiplikative Inverse zu 2 in $\mathbb{Z}_7$ ist: $2 \cdot 4 \mod 7 = 1$.

(b) $24 = 1 + 1 \cdot 23$ ist nicht durch 7 teilbar.
$47 = 1 + 2 \cdot 23$ ist nicht durch 7 teilbar.
$70 = 1 + 3 \cdot 23$ ist durch 7 teilbar und es folgt, dass 10 das multiplikative Inverse zu 7 in $\mathbb{Z}_{23}$ ist: $10 \cdot 7 \mod 23 = 1$.

(c) $52 = 1 + 1 \cdot 51$ ist nicht durch 10 teilbar.
$103 = 1 + 2 \cdot 51$ ist nicht durch 10 teilbar.
Wir erkennen das Muster, dass die letzte Ziffer von $k \cdot 51 + 1$ immer die letzte Ziffer von $k + 1$ ist. Damit $k \cdot 51 + 1$ durch 10 teilbar ist, muss diese 0 entsprechen. Also setzen wir $k = 9$ und erhalten $460 = 1 + 9 \cdot 51$ bzw. 46 als multiplikatives Inverses zu 10 in $\mathbb{Z}_{51}$: $46 \cdot 10 \mod 51 = 1$.

Aufgabe 8

Berechnen Sie die Inversen in der Gruppe $(\mathbb{Z}_{457}, \cdot)$ zu

a) 12, b) 200, c) 400

mittels des euklidischen Algorithmus.

Lösung:

(a) Wenden wir bereits einen Schritt des euklidischen Algorithmus an, so erhalten wir mit etwas Kopfrechnen:

$$457 = 38 \cdot 12 + 1.$$

Es folgt also, dass $1 = 457 + (-38) \cdot 12$ und somit ist $-38 + 457 = 419$ das multiplikative Inverse zu 12 in $\mathbb{Z}_{457}$.

(b) Wir wenden den euklidischen Algorithmus an:

$$\begin{aligned} 457 &= 2 \cdot 200 + 57 \\ 200 &= 3 \cdot 57 + 29 \\ 57 &= 1 \cdot 29 + 28 \\ 29 &= 1 \cdot 28 + 1. \end{aligned}$$

Gehen wir nun rückwärts und nutzen die Zeilen aus dem Algorithmus zum Ersetzen, so erhalten wir

$$\begin{aligned} 1 &= 29 - 1 \cdot 28 \\ &= 29 - 1 \cdot [57 - 1 \cdot 29] = 2 \cdot 29 - 57 \\ &= 2 \cdot [200 - 3 \cdot 57] - 57 = 2 \cdot 200 - 7 \cdot 57 \\ &= 2 \cdot 200 - 7 \cdot [457 - 2 \cdot 200] = (-7) \cdot 457 + 16 \cdot 200. \end{aligned}$$

Es folgt, dass 16 das multiplikative Inverse zu 200 in $\mathbb{Z}_{457}$ ist, da $16 \cdot 200 \mod 457 = 1$.

(c) Wir wenden den euklidischen Algorithmus an:

$$\begin{aligned} 457 &= 1 \cdot 400 + 57 \\ 400 &= 7 \cdot 57 + 1. \end{aligned}$$

Gehen wir wieder rückwärts , so erhalten wir

$$\begin{aligned} 1 &= 400 - 7 \cdot 57 \\ &= 400 - 7 \cdot [457 - 1 \cdot 400] = 8 \cdot 400 - 7 \cdot 457. \end{aligned}$$

Es folgt, dass 8 das multiplikative Inverse zu 400 in $\mathbb{Z}_{457}$ ist, da $8 \cdot 400 \mod 457 = 1$.

Einfacher wäre übrigens folgende Überlegung gewesen:

$$1 = 16 \cdot 200 \mod 457 = 8 \cdot 2 \cdot 200 \mod 457 = 8 \cdot 400 \mod 457.$$

Aufgabe 9

In welchem endlichen Körper gilt *"25 divided by 5 is 14"* ?

Tipp: Googeln Sie mal nach dieser englischen Aussage und genießen Sie das Video.

Lösung:

Wir betrachten den $\mathbb{Z}_3$, dies ist ein Körper (da 3 prim) mit $25 \equiv 1$, $5 \equiv 2 = 2^{-1}$ sowie $14 \equiv 2$. Ergo gilt

$$25 \cdot 5^{-1} = 25 \cdot 2 \equiv 1 \cdot 2 = 2 \equiv 14 \mod 3.$$

Als endliche Körper kommen hier nur $\mathbb{Z}_p$ mit einer Primzahl p infrage. In einem Körper ist die Gleichung $25/5 = 14$ durch Multiplikation mit $5 \neq 0$ äquivalent zu

$$[25]_p = [5]_p \cdot [14]_p = [5 \cdot 14]_p = [70]_p.$$

Subtraktion von $[25]_p$ liefert

$$[0]_p = [45]_p.$$

Diese Gleichung kann nur erfüllt sein, wenn p ein Teiler von $45 = 3^2 \cdot 5$ ist, weshalb nur die Primzahlen $p = 3$ und $p = 5$ infrage kommen. Für $p = 5$ ist die ursprüngliche Gleichung nicht erfüllt, da wir durch 5 teilen und $[5]_5 = [0]_5$ keine Inverse in $\mathbb{Z}_5$ besitzt. Somit ist $\mathbb{Z}_3$ der einzige Körper, in dem die Gleichung $25/5 = 14$ erfüllt ist.

Bemerkung: Unter den Restklassenringen $\mathbb{Z}_p$ mit $p \leq 10^6$ gilt diese Gleichung nur für $p \in \{1, 3, 9\}$. Allergings erhalten wir nur für $p = 3$ einen Körper. Dies wurde numerisch getestet, ein Beweis ist nicht klar. Die Fälle $p > 10^6$, sowie andere endliche Körper wurden hier nicht betrachtet.