Prof. Dr. Ellen Henke
Dr. Julian Kaspczyk
Edoardo Salati

Lösungsblatt 5

LA/LAAG
28. November 2021

Bezeichnungen

Sei M eine Menge. Dann ist $\mathrm{Sym}(M) := \{\phi : M \longrightarrow M \mid \phi \text{ ist eine Bijektion}\}$ die *symmetrische Gruppe* auf M. Wenn $M = \{1, 2, \dots n\}$ ist, schreibt man auch $\mathrm{Sym}(n)$ oder S_n.

Hausaufgaben zur Vorbereitung

Die folgende Aufgabe dient Ihnen zur Vorbereitung der fünften Präsenzübung. Der späteste Abgabetermin ist der 17.11.2021 um 23.59 Uhr. Bearbeiten Sie die Aufgabe aber möglichst vor Ihrem fünften Übungstermin!

Lösung der ersten Vorbereitungsaufgabe

In der ersten Vorbereitungsaufgaben war zu entscheiden, welche der folgenden Aussagen richtig sind.

(1) Sei $2\mathbb{Z}$ die Menge der geraden ganzen Zahlen. Dann ist $(2\mathbb{Z}, +)$ eine Untergruppe von $(\mathbb{Z}, +)$.

(2) Sei $3\mathbb{Z}$ die Menge der durch 3 teilbaren ganzen Zahlen. Dann ist $(3\mathbb{Z}, +)$ keine Untergruppe von $(\mathbb{Z}, +)$.

(3) Sei $2\mathbb{Z} + 1$ die Menge der ungeraden ganzen Zahlen. Dann ist $(2\mathbb{Z} + 1, +)$ eine Untergruppe von $(\mathbb{Z}, +)$.

(4) Es ist $\{-1, 1\}$ eine Untergruppe von $(\mathbb{R} \setminus \{0\}, \cdot)$.

Die Aussage in (1) ist richtig. Um dies zu sehen, zeigen wir, dass $2\mathbb{Z}$ in $(\mathbb{Z}, +)$ die Eigenschaften (U0), (U1) und (U2) aus Definition 2.5 erfüllt.

(U0) Es gilt $0 \in 2\mathbb{Z}$.

(U1) Seien $x, y \in 2\mathbb{Z}$. Dann existieren $r, s \in \mathbb{Z}$ mit $x = 2r$ und $y = 2s$. Nun gilt $x + y = 2r + 2s = 2(r + s) \in 2\mathbb{Z}$.

(U2) Sei $x \in 2\mathbb{Z}$ und $r \in \mathbb{Z}$ mit $x = 2r$ Dann gilt $-x = -2r = 2(-r) \in 2\mathbb{Z}$.

Die Aussage in (2) ist falsch. Man kann nämlich wie in (1) zeigen, dass $3\mathbb{Z}$ eine Untergruppe von $(\mathbb{Z}, +)$ ist.

Die Aussage in (3) ist falsch. Es gilt $0 \notin 2\mathbb{Z} + 1$, sodass (U0) aus Definition 2.5 nicht erfüllt ist. Außerdem ist auch (U1) nicht erfüllt, da die Summe zweier ungerader Zahlen stets gerade und damit nicht in $2\mathbb{Z} + 1$ ist (die Feststellung, dass (U0) nicht erfüllt ist, reicht aber schon, um zu begründen, dass es sich nicht um eine Untergruppe handelt).

Die Aussage in (4) ist richtig. Um dies zu sehen, zeigen wir, dass $E := \{-1, 1\}$ in $(\mathbb{R} \setminus \{0\}, \cdot)$ die Eigenschaften (U0), (U1) und (U2) aus Definition 2.5 erfüllt.

(U0) Es gilt $1 \in E$.

(U1) Für $x, y \in E$ gilt auch $xy \in E$, denn $1 \cdot 1 = 1 \in E$, $(-1) \cdot (-1) = 1 \in E$, $(-1) \cdot 1 = -1 \in E$ und $1 \cdot (-1) = -1 \in E$.

(U2) Für $x \in E$ gilt $x^{-1} \in E$, denn $1^{-1} = 1 \in E$ und $(-1)^{-1} = -1 \in E$.

Lösung der zweiten Vorbereitungsaufgabe

In der zweiten Vorbereitungsaufgabe war der folgende Lückentext zu ergänzen.

(1) Es sind $- \ldots$ und $\ldots$ die einzigen ganzen Zahlen, die ein multiplikatives Inverses in $\mathbb{Z}$ besitzen.

(2) Wenn $(K, +, \cdot)$ ein Körper ist und $a \in K$ invertierbar ist, dann gilt $a \neq \ldots_K$.

(3) Das Inverse von 2 in $\mathbb{Q}$ bezüglich der Addition ist $\ldots$. Das Inverse von $\frac{1}{5}$ in $\mathbb{Q}$ bezüglich der Multiplikation ist $\ldots$.

(4) Existiert ein $0 \neq a \in \mathbb{Q}$ mit $-a = a^{-1}$? (Ja/Nein) $\ldots$

Die Lücken sind wie folgt auszufüllen:

(1) 1, 1

(2) 0

(3) -2, 5

(4) Nein

Hier eine Begründung für das "Nein" in der letzten Lücke: Gäbe es ein $0 \neq a \in \mathbb{Q}$ mit $-a = a^{-1}$, so hätten wir $-a^2 = 1$, also $a^2 = -1$. Das ist in $\mathbb{Q}$ nicht möglich.

Präsenzaufgaben

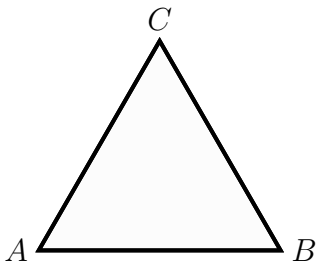
Die folgenden Aufgaben werden in den Übungen gemeinsam besprochen. Um Ihren Lernerfolg zu steigern, sollten Sie sich aber bereits im Vorfeld der Übungen mit den Aufgaben auseinandergesetzt haben.

Prof. Dr. Ellen Henke
Dr. Julian Kaspczyk
Edoardo Salati

Lösungsblatt 5

Aufgabe 2

Gegeben ist das folgende gleichseitige Dreieck:



Die Drehung des gegebenen Dreiecks um den Mittelpunkt um 120° (bzw. um 240°, bzw. um 360°) bezeichnen wir mit r_1 (bzw. mit r_2, bzw. mit id). Es werde dabei gegen den Uhrzeigersinn gedreht.

Die Spiegelung des gegebenen Dreiecks an der Höhe durch den Eckpunkt A bzw. B bzw. C bezeichnen wir mit s_1 bzw. s_2 bzw. s_3.

Machen Sie sich klar, dass man alle genannten Spiegelungen und Drehungen als Abbildungen auffassen kann, sodass es Sinn macht, von Kompositionen von Drehungen/Spiegelungen zu sprechen.

Sei $D_6 := \{\mathrm{id}, r_1, r_2, s_1, s_2, s_3\}$.

(a) Zeigen Sie, dass D_6 mit der Komposition von Abbildungen, $\circ$, eine nicht-abelsche Gruppe ist. Stellen Sie die Gruppe $(D_6, \circ)$ mithilfe einer Multiplikationstafel dar.

(b) Geben Sie das neutrale Element der Gruppe $(D_6, \circ)$ an.

(c) Geben Sie für jedes Element von D_6 sein Inverses an.

(d) Zeigen Sie, dass $\{id, r_1, r_2\}$ eine Untergruppe von D_6 ist.

(e) Machen Sie sich klar, dass die Elemente von D_6 bereits dadurch festgelegt sind, wie sie die mit A, B, C bezeichneten Ecken des Dreiecks permutieren. Identifizieren Sie jedes Element von D_6 auf diese Weise mit einem Element von S_3. Machen Sie sich klar, dass sie auf diese Weise eine Bijektion von D_6 nach S_3 bekommen.

Lösung

Jede Drehung und jede Spiegelung des Dreiecks lässt sich dadurch beschreiben, wie sie die Eckpunkte des Dreiecks bewegt. Deshalb können wir jede der Drehungen und Spiegelungen als eine Abbildung von $\{A, B, C\}$ nach $\{A, B, C\}$ auffassen.

Beispielsweise lässt s_1 den Eckpunkt A fest und vertauscht die beiden anderen Eckpunkte. Deshalb können wir s_1 auffassen als die Abbildung

$$\begin{aligned}&\{A, B, C\} \to \{A, B, C\},\\ &A \mapsto A,\\ &B \mapsto C,\\ &C \mapsto B.\end{aligned}$$

Wir bearbeiten nun die einzelnen Teilaufgaben.

(a) Um zu zeigen, dass D_6 zusammen mit der Komposition von Abbildungen eine Gruppe ist, beweisen zunächst, dass $\alpha \circ \beta \in D_6$ für alle $\alpha, \beta \in D_6$. Damit ist durch

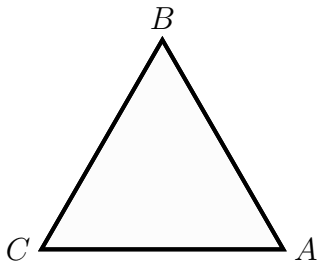
$$D_6 \times D_6 \to D_6, (\alpha, \beta) \mapsto \alpha \circ \beta$$

eine binäre Operation gegeben. Danach weisen wir die Eigenschaften (1), (2), (3) aus Definition 2.1 nach, also dass $\circ$ assoziativ ist, dass es ein neutrales Element bezüglich $\circ$ gibt und dass jedes Element von D_6 ein Inverses hat.

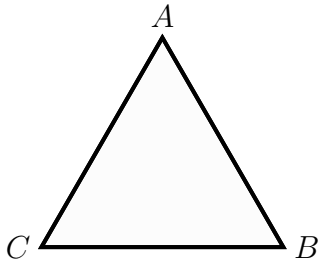
Wie angekündigt, beginnen wir damit, zu zeigen, dass $\alpha \circ \beta \in D_6$ für alle $\alpha, \beta \in D_6$ gilt. Um dies zu sehen, gibt es zwei Möglichkeiten. Die erste Möglichkeit besteht darin, alle möglichen Kompositionen zweier Elemente von D_6 zu bestimmen. Das liefert dann auch gleich die Multiplikationstafel. Man erhält:

$\circ$	id	r_1	r_2	s_1	s_2	s_3
id	id	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	id	s_3	s_1	s_2
r_2	r_2	id	r_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	id	r_1	r_2
s_2	s_2	s_3	s_1	r_2	id	r_1
s_3	s_3	s_1	s_2	r_1	r_2	id

Wir zeigen exemplarisch, wie sich die Kompositionen bestimmen lassen. Dazu schauen wir uns das Beispiel $s_1 \circ r_1$ an. Um $s_1 \circ r_1$ zu bestimmen, müssen wir uns anschauen, was passiert, wenn wir auf unser Dreieck zuerst die Drehung r_1 und anschließend die Spiegelung s_1 anwenden, denn $s_1 \circ r_1$ bedeutet "Wende erst r_1 und dann s_1 an". Wenn wir die Drehung r_1 auf unser Dreieck anwenden, drehen wir jeden Eckpunkt gegen den Uhrzeigersinn "um eine Position weiter". Nach Anwendung der Drehung r_1 erhalten wir also das folgende Dreieck:



Wenden wir jetzt die Spiegelung s_1 an, so heißt das, dass wir die Eckpunkte A und B vertauschen und den Eckpunkt C festlassen. Wir gelangen also zu folgendem Dreieck:



Wir sehen, dass wir, um von unserem Ausgangsdreieck zu obigem Dreieck zu kommen, die beiden Eckpunkte A und C vertauschen und den Eckpunkt B festlassen müssen, also die Spiegelung s_2 anwenden müssen. Folglich erhalten wir bei Anwendung von s_2 bzw. von $s_1 \circ r_1$ das gleiche Dreieck. Somit gilt $s_1 \circ r_1 = s_2$.

Völlig analog lassen sich alle Kompositionen von Elementen von D_6 bestimmen, was dann zur obigen Multiplikationstafel führt. Die Multiplikationstafel zeigt, dass $\alpha \circ \beta \in D_6$ für alle $\alpha, \beta \in D_6$.

Wie oben schon erwähnt, gibt es noch eine zweite Möglichkeit, zu zeigen, dass $\alpha \circ \beta \in D_6$ für alle $\alpha, \beta \in D_6$ gilt: Wir haben bereits beobachtet, dass wir jedes Element von D_6 als eine Abbildung von $\{A, B, C\}$ nach $\{A, B, C\}$ interpretieren können. Wie man sich leicht überlegen kann, ist jede solche Abbildung bijektiv (sie ist injektiv, da eine Drehung/Spiegelung zwei verschiedene Eckpunkte auf verschiedene Eckpunkte bewegt und surjektiv, da es zu jedem Eckpunkt einen Eckpunkt gibt, der auf ihn bewegt wird). Wir können also jedes Element von D_6 als eine Bijektion von $\{A, B, C\}$ nach $\{A, B, C\}$ auffassen. Außerdem werden je zwei verschiedene Elemente von D_6 auch durch verschiedene Bijektionen beschrieben. Mit den Elementen von D_6 sind also sechs paarweise verschiedene Bijektionen von $\{A, B, C\}$ nach $\{A, B, C\}$ gegeben. Nach Lemma 2.3 aus dem Vorlesungsskirpt gilt $|\mathrm{Sym}(\{A, B, C\})| = 3! = 6$. Es ist aber $\mathrm{Sym}(\{A, B, C\})$ die Menge der Bijektionen von $\{A, B, C\}$ nach $\{A, B, C\}$. Somit gibt es genau sechs Bijektionen von $\{A, B, C\}$ nach $\{A, B, C\}$. Und wegen $|D_6| = 6$ müssen alle sechs davon in D_6 liegen. Folglich können wir D_6 als die Menge aller Bijektionen von $\{A, B, C\}$ nach $\{A, B, C\}$ auffassen. Sind nun $\alpha, \beta \in D_6$, so ist $\alpha \circ \beta$ gemäß Lemma 1.10 (c) aus dem Skript eine Bijektion von $\{A, B, C\}$ nach $\{A, B, C\}$, nach den obigen Überlegungen also auch ein Element von D_6. Damit gilt $\alpha \circ \beta \in D_6$ für alle $\alpha, \beta \in D_6$.

Wir zeigen nun, dass D_6 zusammen mit $\circ$ die Eigenschaften (1), (2) und (3) aus Definition 2.1 hat.

(1) $\circ$ ist assoziativ nach Lemma 1.9.

(2) Es ist id neutral bezüglich $\circ$. Dies lässt sich an der Multiplikationstafel ablesen, folgt aber auch aus Lemma 1.11.

(3) Zu jedem Element α von D_6 existiert ein Inverses, also ein $\alpha^* \in D_6$ mit $\alpha = \alpha^* = \mathrm{id} = \alpha^* \circ \alpha$. Das lässt sich aus der Multiplikationstafel ablesen, folgt aber auch aus Lemma 1.12.

Damit bildet D_6 zusammen mit $\circ$ eine Gruppe.

Man könnte dies auch noch etwas anders begründen: Oben haben wir ja gesehen, dass wir D_6 als die Menge aller Bijektionen von $\{A, B, C\}$ nach $\{A, B, C\}$ auffassen können. Und die Menge aller Bijektionen von $\{A, B, C\}$ nach $\{A, B, C\}$ bildet gemäß Lemma 2.2 zusammen mit $\circ$ eine Gruppe, nämlich die symmetrische Gruppe $\mathrm{Sym}(\{A, B, C, \})$.

Um Teil (a) zu beenden, bleibt noch zu begründen, dass $(D_6, \circ)$ nicht abelsch ist. Das können wir an der Multiplikationstafel ablesen, denn z. B. sehen wir, dass $r_1 \circ s_1 = s_3 \neq s_2 = s_1 \circ r_1$. Dass $(D_6, \circ)$ nicht-abelsch ist, gilt aber wegen $|\{A, B, C\}| = 3$ auch schon nach Lemma 2.2.

(b) id ist das neutrale Element. Das haben wir in (a) gesehen beim Nachweis, dass $(D_6, \circ)$ die Eigenschaften (1), (2), (3) aus Definition 2.1 erfüllt.

(c) Die Inversen können wir aus der Multiplikationstafel ablesen: Es gilt $(s_i)^{-1} = s_i$ für alle $i \in \{1, 2, 3\}$ und natürlich $\mathrm{id}^{-1} = \mathrm{id}$. Außerdem $(r_1)^{-1} = r_2$, sodass $(r_2)^{-1} = r_1$.

(d) Wir zeigen, dass $\{r_1, r_2, \mathrm{id}\}$ in $(D_6, \circ)$ die Eigenschaften (U0), (U1) und (U2) aus Definition 2.5 erfüllt.

(U0) Es ist $\mathrm{id} \in \{r_1, r_2, \mathrm{id}\}$.

(U1) Wir zeigen, dass jedes Produkt zweier Elemente von $\{r_1, r_2, \mathrm{id}\}$ wieder in $\{r_1, r_2, \mathrm{id}\}$ liegt: Es ist $r_1 \circ r_1 = r_2$, $r_2 \circ r_2 = r_1$ und $r_1 \circ r_2 = \mathrm{id} = r_2 \circ r_1$. Für $\alpha \in \{r_1, r_2, \mathrm{id}\}$ gilt außerdem $\alpha \circ \mathrm{id} = \mathrm{id} \circ \alpha = \alpha \in \{r_1, r_2, \mathrm{id}\}$.

(U2) Nach (c) liegt das Inverse eines Elements von $\{r_1, r_2, \mathrm{id}\}$ wieder in $\{r_1, r_2, \mathrm{id}\}$.

(e) Wir haben bereits in Teil (a) gesehen, dass wir jedes Element von D_6 dadurch beschreiben können, wie es die Eckpunkte permutiert, d. h. bewegt. Wir haben auch gesehen, dass wir jedes Element von D_6 mit einer Bijektion von $\{A, B, C\}$ nach $\{A, B, C\}$ identifizieren können. Wenn wir nun die Eckpunkte mit 1, 2 und 3 statt mit A, B und C bezeichnen, so können wir uns analog klarmachen, dass wir jedes Element von D_6 mit einer Bijektion von $\{1, 2, 3\}$ nach $\{1, 2, 3\}$, also mit einem Element von $S_3 = \mathrm{Sym}(3)$, identifizieren können. Je zwei verschiedene Drehungen/Spiegelungen werden dabei durch

zwei verschiedene Bijektionen beschrieben. Ordnen wir jedem Element von D_6 nun "seine" Bijektion zu, bekommen wir also eine injektive Abbildung von D_6 nach S_3. Wegen $|D_6| = 6 = |S_3|$ ist diese auch surjektiv, insgesamt also bijektiv.

Hinweise:

(1) Manche Mathematikerinnen und Mathematiker bezeichnen die Gruppe, die wir hier als D_6 bezeichnet haben, mit D_3. Damit wollen sie unterstreichen, dass es sich um die Menge der Drehungen und Spiegelungen eines gleichseitigen *Drei*ecks handelt. Wir haben die Bezeichnung D_6 gewählt, um zu unterstreichen, dass die Gruppe 6 Elemente hat.

(2) Das in dieser Aufgabe vorgestellte Beispiel wird auf eine sehr schöne Art in Abschnitt 1.1 des Buchs "Elementar(st)e Gruppentheorie" von Tobias Glosauer behandelt. Wenn Sie Zeit haben, schauen Sie doch mal rein (es ist über Google Books zugänglich).

Aufgabe 3

Sei n eine natürliche Zahl und seien $k, h \in \{1, \dots, n\}$. Definiere

$$G_k := \{\varphi \in \mathrm{Sym}(n) \mid \varphi(k) = k\} \qquad \text{and} \qquad G_{k,h} := \{\varphi \in \mathrm{Sym}(n) \mid \varphi(k) = k, \varphi(h) = h\}$$

Zeigen Sie:

(a) dass G_k eine Untergruppe von $\mathrm{Sym}(n)$ ist,

(b) dass $G_{k,h}$ eine Untergruppe von $\mathrm{Sym}(n)$ ist. Wie kann man $G_{k,h}$ durch G_k und G_h beschreiben?

Lösung

Der Einfachheit halber schreiben wir im Folgenden id statt $\mathrm{id}_{\{1,\dots,n\}}$.

(a) Wir zeigen, dass die Eigenschaften (U0), (U1), (U2) aus Definition 2.5 erfüllt sind.

- (U0) Weil $\mathrm{id}(k) = k$ ist, gilt $\mathrm{id} \in G_k$.
- (U1) Wenn $\varphi, \eta \in G_k$ sind, dann $(\varphi \circ \eta)(k) = \varphi(\eta(k)) = \varphi(k) = k$. Also $\varphi \circ \eta \in G_k$.
- (U2) Wenn $\varphi \in G_k$ ist, dann $\varphi^{-1}(k) = \varphi^{-1}(\varphi(k)) = (\varphi^{-1} \circ \varphi)(k) = \mathrm{id}(k) = k$, sodass $\varphi^{-1} \in G_k$.

(b) Der Beweis, dass $G_{k,h}$ eine Untergruppe von $\mathrm{Sym}(n)$ ist, verläuft völlig analog zum Beweis von (a).

Für $\varphi \in \mathrm{Sym}(n)$ gilt

$$\begin{aligned}\varphi \in G_{k,h} &\Leftrightarrow \varphi(k) = k \wedge \varphi(h) = h \\ &\Leftrightarrow \varphi \in G_k \wedge \varphi \in G_h \\ &\Leftrightarrow \varphi \in G_k \cap G_h.\end{aligned}$$

Es folgt $G_{k,h} = G_k \cap G_h$.

Auf Blatt 7 wird in Aufgabe 6 gezeigt, dass der Schnitt zweier Untergruppen immer eine Untergruppe ist. Dass $G_{k,h} = G_k \cap G_h$ eine Untergruppe ist, kann man also auch aus (a) zusammen mit Aufgabe 6 von Blatt 7 folgern.

Aufgabe 4

Lemma 2.12 aus der Vorlesung besagt folgendes:
Sei $(G, +)$ eine abelsche Gruppe. Die folgenden Regeln gelten für alle $g, h \in G$ und $m, n \in \mathbb{Z}$:

(a) $(-n)g = -(ng) = n(-g)$.

(b) $(n + m)g = ng + mg$.

(c) $n(mg) = (nm)g$.

(d) $m(g + h) = mg + mh$.

Die Teile (a) und (b) wurden bereits in der Vorlesung bewiesen. Beweisen Sie nun (c) und (d).

Lösung

(c) Zunächst beweisen wir die Aussage für den Fall, dass $n \geq 0$ gilt. Dazu wenden wir das Prinzip der vollständigen Induktion an. Für jedes $n \in \mathbb{N}_0$ sei $P(n)$ die Aussage

Es gilt $n(mg) = (nm)g$ für alle $m \in \mathbb{Z}$ und alle $g \in G$.

1. Induktionsanfang: Wir zeigen zunächst, dass $P(0)$ wahr ist. Für $g \in G$ und $m \in \mathbb{Z}$ gilt $0(mg) = 0_G$ gemäß Notation 2.11 aus dem Vorlesungsskript. Ebenso gilt $(0m)g = 0g = 0_G$ gemäß Notation 2.11 aus dem Vorlesungsskript, also $0(mg) = (0m)g$. Damit ist $P(0)$ wahr.
2. Induktionsschritt: Sei ein $n \in \mathbb{N}_0$ gegeben, so dass $P(n)$ wahr ist (Induktionsvoraussetzung). Wir wollen folgern, dass auch $P(n + 1)$ wahr ist. Wir müssen also zeigen, dass
$$(n + 1)(mg) = ((n + 1)m)g$$

für alle $m \in \mathbb{Z}$ und alle $g \in G$. Seien also $m \in \mathbb{Z}$ und $g \in G$. Es gilt

$$\begin{aligned}(n+1)(mg) &= n(mg) + mg && \text{gemäß Notation 2.11}\\ &= (nm)g + mg && \text{nach Induktionsvoraussetzung}\\ &= (nm+m)g && \text{nach Lemma 2.12 (b)}\\ &= ((n+1)m)g. \end{aligned}$$

Damit gilt auch $P(n+1)$. Der Induktionsbeweis ist damit abgeschlossen.

Wir können nun also sagen, dass $(nm)g = n(mg)$ für alle $n \in \mathbb{N}_0$, alle $m \in \mathbb{Z}$ und alle $g \in G$ gilt. Darauf aufbauend betrachten wir nun den allgemeinen Fall. Dazu ist noch zu zeigen, dass $(nm)g = n(mg)$ auch dann gilt, wenn $n, m \in \mathbb{Z}$ mit $n < 0$ und $g \in G$ gilt. Seien also $n, m \in \mathbb{Z}$, $n < 0$ und $g \in G$. Dann gilt

$$\begin{aligned}(nm)g &= ((-|n|)m)g && \text{denn } n = -|n| \text{ wegen } n < 0\\ &= (|n|(-m))g\\ &= |n|((-m)g) && \text{da (c) für } n \geq 0 \text{ schon bewiesen}\\ &= |n|(-mg) && \text{nach Lemma 2.12 (a)}\\ &= (-|n|)(mg) && \text{nach Lemma 2.12 (a)}\\ &= n(mg) && \text{da } n = -|n|. \end{aligned}$$

Damit ist (c) bewiesen.

(d) Zunächst zeigen wir die Aussage für den Fall $m \geq 0$. Dazu wenden wir wieder das Prinzip der vollständigen Induktion an. Für jedes $m \in \mathbb{N}_0$ sei $P(m)$ die Aussage

Es gilt $m(g+h) = mg + mh$ für alle $g, h \in G$.

1. Induktionsanfang: Wir zeigen, dass $P(0)$ wahr ist. Für $g, h \in G$ gilt $0(g+h) = 0_G$ gemäß Notation 2.11 und $0g + 0h = 0_G + 0_G = 0_G$ gemäß Notation 2.11. Also $0(g+h) = 0g + 0h$. Damit ist $P(0)$ wahr.
2. Induktionsschritt: Sei ein $m \in \mathbb{N}_0$ gegeben, so dass $P(m)$ wahr ist (Induktionsvoraussetzung). Wir wollen folgern, dass auch $P(m+1)$ wahr ist. Wir müssen also zeigen, dass
$$(m+1)(g+h) = (m+1)g + (m+1)h$$
für alle $g, h \in G$ gilt. Es gilt
$$\begin{aligned}(m+1)(g+h) &= m(g+h) + (g+h) && \text{gemäß Notation 2.11}\\ &= mg + mh + g + h && \text{nach Induktionsvoraussetzung}\\ &= (mg+g) + (mh+h) && \text{da } (G,+) \text{ abelsch}\\ &= (m+1)g + (m+1)h && \text{gemäß Notation 2.11.}\end{aligned}$$
Damit ist $P(m+1)$ wahr. Der Induktionsbeweis ist damit abgeschlossen.

Wir haben (d) also für den Fall $m \geq 0$ bewiesen. Zu zeigen bleibt, dass (d) auch mit $m < 0$ gilt. Sei also $m \in \mathbb{Z}$, $m < 0$ und $g \in G$. Dann gilt

$$\begin{aligned}
m(g+h) &= (-|m|)(g+h) && \text{denn } m = -|m| \text{ wegen } m < 0 \\
&= -((|m|)(g+h)) && \text{nach Lemma 2.12 (a)} \\
&= -(|m|g + |m|h) && \text{da (d) für } m \geq 0 \text{ schon bewiesen} \\
&= (-|m|g) + (-|m|h) \\
&= (-|m|)g + (-|m|)h && \text{nach Lemma 2.12 (a)} \\
&= mg + mh.
\end{aligned}$$

Vielleicht noch ein Wort zur Begründung der vierten Gleichheit: Hier haben wir benutzt, dass in der abelschen Gruppe $(G, +)$ für alle $x, y \in G$ die Gleichung $-(x+y) = (-x) + (-y)$ erfüllt ist. Um dies zu sehen, beobachtet man einfach, dass $(x+y)+((-x)+(-y)) = (x+(-x))+(y+(-y)) = 0_G+0_G = 0_G$ gilt, wobei wir für die zweite Gleichheit benutzt haben, dass $(G, +)$ abelsch ist.

Wir haben (d) nun bewiesen.

Aufgabe 5

Sei $K := \mathbb{R} \times \mathbb{R}$.

(a) Für alle (a, b), $(a', b') \in K$ sei

$$(a, b) + (a', b') := (a + a', b + b'),$$

$$(a, b) \circ (a', b') := (aa' - bb', ab' + a'b).$$

Man zeige, dass $(K, +, \circ)$ ein Körper ist.

Bemerkung: Man nennt diesen Körper den *Körper der komplexen Zahlen* und bezeichnet ihn mit $\mathbb{C}$. Man schreibt i für das Element $(0, 1)$.

(b) Was ist i^2?

(c) Definieren Sie nun

$$(a, b) \cdot (a', b') := (aa', bb').$$

Beweisen Sie, dass $(K, +, \cdot)$ ein Ring ist. Handelt es sich auch um einen Körper? Und um einen Integritätsring?

(d) Was können Sie über $(K, +, \circ)$ sagen, wenn man den Körper $\mathbb{R}$ der reellen Zahlen durch einen beliebigen Körper oder einen kommutativen Ring ersetzt?

Lösung

(a) Wir beweisen zuerst, dass $(K,+)$ eine abelsche Gruppe ist.
Es ist $+$ assoziativ, weil

$$((a,b)+(a',b'))+(a'',b'') = (a+a',b+b')+(a'',b'') = (a+a'+a'',b+b'+b'')$$

und

$$(a,b)+((a',b')+(a'',b'')) = (a,b)+(a'+a'',b'+b'') = (a+a'+a'',b+b'+b'')$$

gleich sind.
Für $(a,b) \in K$ gilt

$$(0,0)+(a,b) = (0+a,0+b) = (a,b) = (a+0,b+0) = (a,b)+(0,0).$$

Somit ist $(0,0)$ neutral bezüglich $+$. Für $(a,b) \in K$ gilt $(a,b)+(-a,-b) = (0,0)$, womit $(-a,-b)$ invers zu (a,b) ist. Es ist also $(K,+)$ eine Gruppe.
Für alle $(a,b),(a',b') \in K$ gilt $(a,b)+(a',b') = (a+a',b+b') = (a'+a,b'+b) = (a',b')+(a,b)$, wobei wir für die zweite Gleichheit die Kommutativität der Addition in $\mathbb{R}$ benutzt haben. Somit ist $(K,+)$ sogar eine abelsche Gruppe.

Wir beweisen nun, dass $(K,+,\circ)$ ein Ring ist. Dazu weisen wir zunächst nach, dass $\circ$ assoziativ ist. Dies gilt, weil

$$\begin{aligned}((a,b)\circ(a',b'))\circ(a'',b'') &= (aa'-bb',ab'+a'b)\circ(a'',b'') = \\ &= ((aa'-bb')a''-(ab'+a'b)b'',(aa'-bb')b''+(ab'+a'b)a'') = \\ &= (aa'a''-a''bb'-ab'b''-a'bb'',aa'b''-bb'b''+aa''b'+a'a''b)\end{aligned}$$

und

$$\begin{aligned}(a,b)\circ((a',b')\circ(a'',b'')) &= (a,b)\circ(a'a''-b'b'',a'b''+a''b') = \\ &= (a(a'a''-b'b'')-b(a'b''+a''b'),a(a'b''+a''b')+b(a'a''-b'b'')) = \\ &= (aa'a''-ab'b''-a'bb''-a''bb',aa'b''+aa''b'+a'a''b-bb'b'')\end{aligned}$$

gleich sind.

Es ist $(1,0)$ neutral bezüglich $\circ$, weil $(1,0)\circ(a,b) = (1\cdot a-0\cdot b,1\cdot b+0\cdot a) = (a,b)$ und analog $(a,b)\circ(1,0) = (a,b)$ ist.

Wir beweisen nun die Distributivgesetze. Es gilt

$$\begin{aligned}(a,b)\circ((a',b')+(a'',b'')) &= (a,b)\circ(a'+a'',b'+b'') = \\ &= (aa'+aa''-bb'-bb'',ab'+ab''+a'b+a''b)\end{aligned}$$

und

$$((a,b)\circ(a',b'))+((a,b)\circ(a'',b'')) = (aa'-bb',ab'+a'b)+(aa''-bb'',ab''+a''b) = (aa-bb''+aa''-bb'',ab'+a'b+ab''+a''b).$$

Weil beides gleich ist, haben wir schon einmal eines der Distributivgesetze gezeigt. Um das andere zu zeigen, beweisen wir zunächst, dass $\circ$ kommutativ ist. Dies gilt wegen

$$(a,b)\circ(a',b') = (aa'-bb',ab'+a'b) = (a',b')\circ(a,b).$$

Das andere Distributivgesetz gilt nun wegen

$$\begin{aligned}((a,b)+(a',b'))\circ(a'',b'') &= (a'',b'')\circ((a,b)+(a',b'))\\ &= (a'',b'')\circ(a,b)+(a'',b'')\circ(a',b')\\ &= (a,b)\circ(a'',b'')+(a',b')\circ(a'',b'').\end{aligned}$$

Hierbei haben wir für die erste und die dritte Gleichheit die Kommutativität von $\circ$ und für die zweite Gleichheit das bereits bewiesene Distributivgesetz verwendet.

Bis hierhin haben wir gezeigt, dass $(K,+,\circ)$ ein kommutativer Ring ist. Um zu zeigen, dass es sich sogar um einen Körper handelt, müssen wir beweisen, dass jedes Element aus $K\setminus\{(0,0)\}$ ein Inverses hat.

Fur jedes $(0,0)\neq(a,b)\in K$ gilt $a^2+b^2\neq 0$ und $(a,b)\circ(a,-b)=(a^2+b^2,0)$. Nun gilt

$$(a,b)\circ\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)=(1,0).$$

Somit haben alle von $(0,0)$ verschiedenen Elemente von K ein Inverses. Folglich ist $(K,+,\circ)$ ein Körper.

(b) Es gilt $i^2=(0,1)\circ(0,1)=(0-1,0)=(-1,0)$.

Und was ist daran besonders? Nun ja, es gilt $(-1,0)=-(1,0)=-1_K$. Damit ist -1_K in K also ein Quadrat, nämlich das Quadrat von i. Das ist eine interessante Eigenschaft, die wir aus den uns vertrauten reellen Zahlen nicht kennen. Für eine reelle Zahl r gilt ja $r^2\geq 0$, womit es kein $r\in\mathbb{R}$ mit $r^2=-1$ gibt.

Es wird noch interessanter: Nämlich kann man $\mathbb{R}$ in K "einbetten". Damit ist folgendes gemeint: Wir identifizieren jede reelle Zahl r mit $(r,0)$. Für $r,s\in\mathbb{R}$ gilt nun $(r,0)+(s,0)=(r+s,0)$ und $(r,0)\circ(s,0)=(rs,0)$ gilt. Wir können also zwei "Zahlen" $(r,0),(s,0)$ so addieren bzw. multiplizieren, wie wir die entsprechenden reellen Zahlen r und s addieren bzw. multiplizieren würden. Man kann sich den Körper $\mathbb{R}$ deshalb als einen in K enthaltenen Körper vorstellen, dessen Addition und Multiplikation von K kommen.

Damit gibt es zwar in $\mathbb{R}$ kein Element r mit $r^2=-1$. Aber immerhin ist $\mathbb{R}$ in einem Körper K enthalten, der ein Element i mit $i^2=-1$ besitzt.

(c) In (a) haben wir bewiesen, dass $(K, +)$ eine abelsche Gruppe ist.
Es ist $\cdot$ assoziativ, weil

$$((a,b)\cdot(a',b'))\cdot(a'',b'') = (aa',bb')\cdot(a'',b'') = (aa'a'',bb'b'') = \\ = (a,b)\cdot(a'a'',b'b'') = (a,b)\cdot((a',b')\cdot(a'',b'')).$$

$\cdot$ ist auch kommutativ, weil $(a,b)\cdot(a',b') = (aa',bb') = (a'a,b'b) = (a',b')\cdot(a,b)$ ist.
Eines der Distributivgesetze lässt sich so beweisen:

$$(a,b)\cdot((a',b')+(a'',b'')) = (a,b)\cdot(a'+a'',b'+b'') = \\ = (aa'+aa'',bb'+bb'') = (aa',bb')+(aa'',bb'') = \\ = ((a,b)\cdot(a',b'))+((a,b)\cdot(a'',b''))$$

Das andere Distributivgesetz lässt sich daraus unter Verwendung der Kommutativität von $\cdot$ ableiten (ähnlich wie in (a)).

Das Element $(1,1)$ ist neutral bezüglich $\cdot$. Wir haben somit gezeigt, dass $(K,+,\cdot)$ ein kommutativer Ring ist.

Es bleibt die Frage zu beantworten, ob $(K,+,\cdot)$ ein Körper bzw. ein Integritätsring ist. Nehmen Sie die Elemente $(1,0) \neq (0,0) \neq (0,1)$. Sie sind beide nicht Null, aber es ist $(1,0)\cdot(0,1) = (0,0)$. Damit ist $(K,+,\cdot)$ kein Integritätsring, nach Beispiel 2.27 also auch kein Körper.

(d) Sei $K = R \times R$. Bis zur Existenz der multiplikativen Inversen hängt der Beweis in (a) nicht davon ab, davon $R = \mathbb{R}$ der Körper der reellen Zahlen ist. Der Beweis zeigt, dass K ein kommutativer Ring ist, sofern R ein kommutativer Ring ist (was insbesondere auch dann der Fall ist, wenn R ein Körper ist).

Für die Existenz der multiplikativen Inversen haben wir in (a) benutzt, dass für reelle Zahlen a, b mit $(a,b) \neq (0,0)$ stets $a^2 + b^2 \neq 0$ gilt. Wenn R ein Körper ist, der diese Eigenschaft nicht hat, dann können wir die Existenz der multiplikativen Inversen nicht mehr beweisen. Aber wenn R ein Körper ist und $a^2 + b^2 \neq 0_R$ für alle $(a,b) \in K$ mit $(a,b) \neq (0,0)$ gilt, dann können wir es, womit K in diesem Falle ein Körper ist.

Hausaufgaben zur Nachbereitung

Die folgenden Aufgaben sind abzugeben. Bitte laden Sie Ihre Abgabe bis zum 24.11.2021, 12:00 Uhr, in den dafür vorgesehenen Opal-Ordner hoch.

Aufgabe 7 (4 Punkte)

Seien X, Y Mengen und $\alpha : X \longrightarrow Y$ eine Bijektion. Zeigen Sie:

(a) Für $\pi \in \mathrm{Sym}(X)$ gilt $\hat{\pi} := \alpha \circ \pi \circ \alpha^{-1} \in \mathrm{Sym}(Y)$.

(b) Die Abbildung $\phi : \mathrm{Sym}(X) \longrightarrow \mathrm{Sym}(Y)$, $\pi \mapsto \hat{\pi}$ ist eine Bijektion.

(c) Für $\pi_1, \pi_2 \in \mathrm{Sym}(X)$ gilt

$$\phi(\pi_1 \circ \pi_2) = \phi(\pi_1) \circ \phi(\pi_2).$$

Lösung

(a) Sei $\pi \in \mathrm{Sym}(X)$. Dann ist $\pi \circ \alpha^{-1}$ eine Abbildung von Y nach X, weil α^{-1} eine Abbildung von Y nach X und π als Element von $\mathrm{Sym}(X)$ eine Abbildung von X nach X ist. Weil $\pi \circ \alpha^{-1}$ eine Abbildung von Y nach X und α eine Abbildung von X nach Y ist, ist $\hat{\pi} = \alpha \circ \pi \circ \alpha^{-1}$ also eine Abbildung von Y nach Y.

Nach Lemma 1.10 (c) ist jede Komposition von bijektiven Abbildungen eine Bijektion. Es ist α nach Voraussetzung eine Bijektion, α^{-1} ist nach Lemma 1.12 (b) ebenso eine Bijektion, und π ist als Element von $\mathrm{Sym}(X)$ ebenso eine Bijektion. Folglich ist $\hat{\pi} = \alpha \circ \pi \circ \alpha^{-1}$ eine Bijektion, und zwar (nach dem vorherigen Absatz) eine von Y nach Y. Es ist also $\hat{\pi} = \alpha \circ \pi \circ \alpha^{-1} \in \mathrm{Sym}(Y)$ nach Definition von $\mathrm{Sym}(Y)$.

(b) Nach Lemma 1.13 genügt es, eine Abbildung $\psi : \mathrm{Sym}(Y) \longrightarrow \mathrm{Sym}(X)$ finden, so dass $\psi \circ \phi = \mathrm{id}_{\mathrm{Sym}(X)}$ und $\phi \circ \psi = \mathrm{id}_{\mathrm{Sym}(Y)}$.

Für jedes $\tau \in \mathrm{Sym}(Y)$ definieren wir $\widetilde{\tau} := \alpha^{-1} \circ \tau \circ \alpha$. Analog zu (a) lässt sich einsehen, dass $\widetilde{\tau}$ für jedes $\tau \in \mathrm{Sym}(Y)$ eine Bijektion von X nach X, also ein Element von $\mathrm{Sym}(X)$, ist. Sei nun

$$\psi : \mathrm{Sym}(Y) \to \mathrm{Sym}(X), \tau \mapsto \widetilde{\tau}.$$

Für $\pi \in \mathrm{Sym}(X)$ gilt dann

$$(\psi \circ \phi)(\pi) = \psi(\alpha \circ \pi \circ \alpha^{-1}) = \alpha^{-1} \circ (\alpha \circ \pi \circ \alpha^{-1}) \circ \alpha = (\alpha^{-1} \circ \alpha) \circ \pi (\alpha^{-1} \circ \alpha) = \mathrm{id}_X \circ \pi \circ \mathrm{id}_X = \pi,$$

wobei die letzte Gleichheit nach Lemma 1.11 gilt. Für $\tau \in \mathrm{Sym}(Y)$ gilt

$$(\phi \circ \psi)(\tau) = \phi(\alpha^{-1} \circ \tau \circ \alpha) = \alpha \circ (\alpha^{-1} \circ \tau \circ \alpha) \circ \alpha^{-1} = (\alpha \circ \alpha^{-1}) \circ \tau \circ (\alpha \circ \alpha^{-1}) = \mathrm{id}_Y \circ \tau \circ \mathrm{id}_Y = \tau,$$

wobei die letzte Gleichheit wieder nach Lemma 1.11 gilt.

Damit haben wir gezeigt, dass $\psi \circ \phi = \mathrm{id}_{\mathrm{Sym}(X)}$ und $\phi \circ \psi = \mathrm{id}_{\mathrm{Sym}(Y)}$. Wie eingangs festgestellt, folgt daraus, dass ϕ bijektiv ist.

(c) Für $\pi_1, \pi_2 \in \mathrm{Sym}(X)$ gilt

$$\begin{aligned}
\phi(\pi_1 \circ \pi_2) &= \alpha \circ (\pi_1 \circ \pi_2) \circ \alpha^{-1} \\
&= \alpha \circ (\pi_1 \circ \mathrm{id}_X \circ \pi_2) \circ \alpha^{-1} && \text{nach Lemma 1.11} \\
&= \alpha \circ (\pi_1 \circ (\alpha^{-1} \circ \alpha) \circ \pi_2) \circ \alpha^{-1} && \text{da } \alpha^{-1} \circ \alpha = \mathrm{id}_X \\
&= (\alpha \circ \pi_1 \circ \alpha^{-1}) \circ (\alpha \circ \pi_2 \circ \alpha^{-1}) \\
&= \phi(\pi_1) \circ \phi(\pi_2).
\end{aligned}$$

Aufgabe 6 (6 Punkte)

Prüfen Sie, ob es sich um einen Körper handelt:

$$(\mathbb{Z}, \oplus, \odot) \quad \text{mit} \quad a \oplus b := a + b - 1, \quad a \odot b := a + b - ab.$$

Lösung

Natürlich sind sowohl $\oplus$ als auch $\odot$ Operationen.

Wir beweisen nun, dass $(\mathbb{Z}, \oplus)$ eine abelsche Gruppe ist.
$\oplus$ ist assoziativ:

$$(x \oplus y) \oplus z = (x + y - 1) \oplus z = x + y + z - 2 = x + (y + z - 1) - 1 = x \oplus (y \oplus z).$$

Es gilt $x \oplus y = x + y - 1 = y \oplus x$, sodass $\oplus$ kommutativ ist.

1 ist neutral bezüglich $\oplus$, weil $1 \oplus x = 1 + x - 1 = x$ ist. Für jedes $x \in \mathbb{Z}$, ist $x \oplus (-x + 2) = x - x + 2 - 1 = 1$, sodass $-x + 2 \in \mathbb{Z}$ invers zu x ist. Wir haben somit gezeigt, dass $(\mathbb{Z}, \oplus)$ eine abelsche Gruppe ist.

Wir machen uns nun klar, dass $(\mathbb{Z}, \oplus, \odot)$ ein kommutativer Ring ist.

$\odot$ ist assoziativ:

$$\begin{aligned}(x \odot y) \odot z &= (x + y - xy) \odot z = x + y - xy + z - xz - yz + xyz = \\ &= x - xy - xz + xyz + (y + z - yz) = x - x(y + z - yz) + (y + z - yz) = x \odot (y \odot z).\end{aligned}$$

Weiterhin ist $\odot$ kommutativ, weil $x \odot y = x + y - xy = y \odot x$ ist. Für alle $x \in \mathbb{Z}$ gilt $x \odot 0 = x + 0 - 0 = x = 0 \odot x$, sodass 0 neutral bezüglich $\odot$ ist.
Es gilt

$$\begin{aligned}x \odot (y \oplus z) = x \odot (y + z - 1) &= x + y + z - 1 - xy - xz + x = \\ &= (x + y - xy) + (x + z - xz) - 1 = (x \odot y) \oplus (x \odot z),\end{aligned}$$

womit eines der Distributivgesetze bewiesen ist. Das andere Distributivgesetz lässt sich nun mithilfe der Kommutativität aus dem bereits bewiesenen Distributivgesetz ableiten (das geht so ähnlich wie in Aufgabe 5 (a)).

Wir haben nun gezeigt, dass $(\mathbb{Z}, \oplus, \odot)$ ein kommutativ Ring ist. Um zu prüfen, ob $(\mathbb{Z}, \oplus, \odot)$ auch ein Körper ist, müssen wir überprüfen, ob jedes von 1 (= neutrales Element bezüglich $\oplus$) verschiedene Element von $\mathbb{Z}$ ein multiplikatives Inverses bezüglich $\odot$ hat.

Für alle $x \in \mathbb{Z}$ mit $x \neq 1$ suchen wir also ein $y \in \mathbb{Z}$, so dass $x \odot y = 0$ gilt (weil 0 das neutrale Element bezüglich $\odot$ ist). Es ist $x \odot y = x + y - xy = 0$ genau wenn, dann $y(x - 1) = x$ ist. Wenn z. B. $x = 3$ gilt, existiert kein $y \in \mathbb{Z}$, sodass $y(3 - 1) = 2y = 3$ ist. Damit hat also 3 kein multiplikatives Inverses. Folglich ist $(\mathbb{Z}, \oplus, \odot)$ kein Körper.

Prof. Dr. Ellen Henke
Dr. Julian Kaspczyk
Edoardo Salati

Lösungsblatt 5

Zusatzaufgabe

Die folgende Aufgabe stellt eine besondere Herausforderung dar. Die Aufgabe wird nicht bewertet. Wenn Sie meinen, eine vollständige Lösung zu haben, sind Sie eingeladen, diese (oder Teile davon) in Ihrer Präsenzübung präsentieren.

Aufgabe 8

Eine Gruppe G heißt *zyklisch* genau dann, wenn ein Element $x \in G$ existiert, so dass alle Elemente $g \in G$ eine Potenz von x sind, d.h. für jedes $g \in G$ existiert ein $n \in \mathbb{Z}$ mit $g = x^n$. Beweisen Sie die folgendene Aussagen.

(a) $(\mathbb{Z}, +)$ ist zyklisch.

(b) Die triviale Untergruppe $\{0\}$ ist die eindeutige endliche Untergruppe von $(\mathbb{Z}, +)$.

(c) Für jede Unterguppe $\{0\} \neq M \leq \mathbb{Z}$ existiert $n \in \mathbb{N}$, so dass $M = n\mathbb{Z}$ ist ($n\mathbb{Z}$ ist die Menge aller durch n teilbaren ganzen Zahlen). Insbesondere existiert eine Bijektion zwischen M und $\mathbb{Z}$.

(d) Alle Unterguppen von $(\mathbb{Z}, +)$ sind zyklisch.

(e) Sei $(R, +, \cdot)$ ein Ring (mit multiplikativem neutralen Element 1_R) und $S \subseteq R$ eine Teilmenge von R. S heißt Unterring von R falls:

1. $1_R \in S$;
2. $(S, +)$ ist eine Untergruppe von $(R, +)$;
3. für alle $a, b \in S$ gilt $a \cdot b \in S$.

Sei K ein Körper, so dass $\mathbb{Z}$ ein Unterring von K ist. Zeigen Sie, dass $\mathbb{Q} \subseteq K$ gilt. Damit ist $\mathbb{Q}$ der "kleinste" Körper, der $\mathbb{Z}$ als Unterring enthält.

Lösung

Zunächst eine Bemerkung zur Schreibweise. Für eine natürliche Zahl n und ein $g \in G$ meinen wir mit x^n das n-fache Produkt $x \cdots x$. Es ist $x^0 = 1_G$. Weiterhin ist x^{-n} das n-fache Produkt $x^{-1} \cdots x^{-1}$.

Im Falle einer additiv geschriebenen Gruppe schreiben wir nx statt x^n.

(a) Für $x \in \mathbb{Z}$ schreiben wir $\langle x \rangle$ für die Menge der Potenzen von x. Wir beweisen, dass $\mathbb{Z} = \langle 1 \rangle$ ist. Tatsächlich gilt für jedes $z \in \mathbb{Z}$, dass $z = n \cdot 1$ oder $z = (-n) \cdot 1$ für ein eindeutiges $n \in \mathbb{N}_0$. D.h, dass $(\mathbb{Z}.+)$ zyklisch ist.

(b) Sei $H \subseteq \mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$ mit $H \neq \{0\}$. Dann existiert $0 \neq z \in \mathbb{Z}$ sodass $z \in H$. Weil H eine Untergruppe ist, ist auch $-z \in H$. Daher können wir $z > 0$ annehmen. Für jedes $n \in \mathbb{N}$ sind die Zahlen nz alle vesrschieden und alle in H enthalten, sodass die Abbildung $j : \mathbb{N} \longrightarrow H$ definiert durch $j(n) = nz$ eine Injektion ist. Weil $\mathbb{N}$ unendlich ist, ist damit auch H unendlich.

(c) Nach dem Beweis von (b) existiert ein $z \in \mathbb{Z}$ mit $z > 0$ und $z \in M$. Sei $n := \min\{z \in M \mid z > 0\}$. Wir zeigen, dass $M = n\mathbb{Z}$ ist.
Es ist $n\mathbb{Z} \subseteq M$. In der Tat folgt dies leicht aus der Tatsache, dass $n \in M$ gilt und M eine Untergruppe ist.

Sei $m \in M$ mit $m > 0$. Dann gilt $m \geq n$ nach Definition von n. Wir können $m = nk + t$ mit $k, t \in \mathbb{N}$ und $0 \leq t < n$ schreiben (nach Lemma 1.29). Wenn $t \neq 0$ ist, dann gilt $t = m - nk \in M$, weil m und nk beide in M enthalten sind, ein Widerspruch zur Wahl von n. Damit ist $t = 0$ und $m = nk \in n\mathbb{Z}$. Folglich gilt auch $M \subseteq n\mathbb{Z}$.

Insgesamt gilt also $M = n\mathbb{Z}$.

(d) Nach (c) gilt für jede Untergruppe M von $(\mathbb{Z}, +)$, dass entweder $M = \{0\}$ (womit M zyklisch ist) oder $M = n\mathbb{Z}$ für ein $n \in \mathbb{N}$ gilt, womit alle Element von $M = n\mathbb{Z}$ eine Potenz von n sind und M also zyklisch ist.

(e) Weil $\mathbb{Z}$ ein Unterring von K ist und K ein Körper ist, existiert für jedes $0 \neq z \in \mathbb{Z}$ ein Inverses $z^{-1} \in K$, d.h. $zz^{-1} = 1$. Wir identifizieren jedes z^{-1} mit $\frac{1}{z}$. Dann gilt für alle $x, z \in \mathbb{Z}$ mit $z \neq 0$, dass $x\, z^{-1} = x\dfrac{1}{z} \in K$. D.h., dass jedes Element $\dfrac{x}{z} \in \mathbb{Q}$ in K enthalten ist, sodass $\mathbb{Q} \subseteq K$ gilt.