Aufgabe 1. Alle Elefanten sind rosarot. Beweis durch Induktion über die Anzahl der Elefanten: Für 0 Elefanten ist die Behauptung korrekt. Nehmen wir induktiv an, dass in jeder Menge die aus n Elefanten besteht, alle Elefanten rosarot sind. Sei X eine Menge mit $n+1$ Elefanten und nehmen wir einen Elefanten E heraus. Die restlichen n Elefanten sind alle rosarot nach der Induktionsannahme. Wir können E so wählen dass er rosarot ist: Falls er nicht rosarot wäre, ersetzen wir ihn mit einem dieser n rosaroten Elefanten. Also sind alle $n+1$ Elefanten rosarot. Wo liegt der Fehler?

Lösung. Der Induktionsschritt von $n = 0$ nach $n = 1$ funktioniert nicht. Falls $n = 1$ ist, und wir den einzigen Elefanten rausnehmen, sind zwar logischerweise alle andern (es gibt keine anderen) Elefanten rosarot. Falls der einzige Elefant nicht rosarot wäre, können wir ihn nicht mit einem anderen Elefanten aus der Restmenge ersetzen, da diese leer ist. Kurz: Der Fehler liegt darin, dass wir ein Element in der leeren Menge wählen, was per Definition nicht möglich ist.

Aufgabe 2. Sei $n \in \mathbb{N} = \{1, 2, 3, \ldots\}$. Betrachte die Äquivalenzrelation $\sim_n$ auf den ganzen Zahlen $\mathbb{Z}$, welche für $a, b \in \mathbb{Z}$ gegeben ist durch

$$a \sim_n b \text{ genau dann wenn } a - b \text{ ein Vielfaches von } n \text{ ist.}$$

Sei C_n die Menge der Äquivalenzklassen, also die Quotientenmenge. [1]

a) Wie viele Elemente besitzt C_n?

b) Für jede Zahl $a \in \mathbb{Z}$ sei $[a]_n \in C_n$ die dazugehörige Äquivalenzklasse. Zeige, dass $(C_n, +)$ eine Gruppe bildet, wobei die Addition zweier Klassen $[a]_n, [b]_n \in C_n$ definiert ist als
$$[a]_n + [b]_n := [a + b]_n.$$

c) Sei $C_n^\times = C_n \setminus \{[0]_n\}$. Ist die Multiplikation $\cdot$ geerbt von der Multiplikation auf $\mathbb{Z}$
$$[a]_n \cdot [b]_n := [a \cdot b]_n$$
wohldefiniert?

d*) Definiert $(C_n^\times, \cdot)$ eine Gruppe? Die Existenz der multiplikativen Inversen ist nicht ganz einfach. Googlen Sie nach dem *erweiterten euklidischen Algorithmus.*

e) Seien $n, m \in \mathbb{N}$ und $k \in \mathbb{Z}$. Betrachten Sie die Vorschrift $g^k_{n,m} : C_n \to C_m$ gegeben durch $[a]_n \mapsto [k \cdot a]_m$. Wann definiert diese Vorschrift eine wohldefinierte Abbildung $g^k_{n,m}$?

Lösung.

[1] Siehe die Erklärungen auf dem Forum: `https://forum.math.ethz.ch/t/exercise-sheet-1/3011`.

a) Per Division mit Rest durch n kann jede Zahl $a \in \mathbb{Z}$ als $a = l \cdot n + a'$ mit $0 \leq a' \leq n-1$ und $l \in \mathbb{Z}$ geschrieben werden. Mit der Transitivität der Relation, gilt $a \sim_n a'$.

Andererseits ist für $a \neq b$ und $0 \leq a, b \leq n-1$ die Differenz $0 < |a-b| < n$ und darum $a \sim_n b$ nicht möglich. Wir können C_n also als $C_n = \{[0]_n, \ldots, [n-1]_n\}$ schreiben, wobei kein Element gleich ist. Also hat C_n genau n Elemente.

b) Wir zeigen zuerst, dass die Addition wohldefiniert ist: Falls $a \sim_n a'$ und $b \sim_n b'$, also $a - a' = l_a n$ und $b - b' = l_b n$ für $l_a, l_b \in \mathbb{Z}$, dann gilt

$$a + b = a' + b' + n(l_a + l_b)$$

und darum $(a+b) \sim_n (a'+b')$. Das neutrale Element der Gruppe ist $[0]_n \in C_n$ und das Inverse eines Elementes $[a]_n$ ist $[-a]_n$.

c) *Falls $n = 1$ ist* folgt $C_1 = \{[0]_n\}$ eine triviale Gruppe mit einem Element. Doch dann ist $C_n^\times$ leer.

Falls $n > 1$ keine Primzahl ist, können wir n als Produkt $n = ab$ zweier natürlichen Zahlen $0 < a, b \leq n-1$ schreiben. Dann ist die Multiplikation nicht wohldefiniert, da $[a]_n \cdot [b]_n = [n]_n = [0]_n$ gilt.

Falls $n > 1$ eine Primzahl ist, Nun ist $n = ab$ nicht möglich für $0 \leq a, b \leq n-1$ per Definition einer Primzahl. Dies zeigt die Wohldefiniertheit des Wertebereichs.

Wir zeigen noch, dass die Multiplikation nicht vom Repräsentanten abhängt: Falls $a \sim_n a'$ und $b \sim_n b'$, also $a - a' = l_a n$ und $b - b' = l_b n$ für $l_a, l_b \in \mathbb{Z}$, dann gilt

$$a \cdot b = a'b' + n(l_a b' + a' l_b + n l_a l_b)$$

und darum $(a \cdot b) \sim_n (a' \cdot b')$. Dies zeigt die Unabhängigkeit des Repräsentanten.

d) Das neutrale Element der Gruppe ist $[1]_n \in C_n$. Falls n eine Primzahl ist, finden wir für das Inverse eines Elementes $[a]_n$ das Element $[b]_n$, wobei b die Gleichung $ab + ny = 1$ erfüllt. Wir erhalten durch b, y durch Rücksubstitution im erweiterten euklidischen Algorithmus [2].

e) Wir wollen, dass für alle $a, a' \in \mathbb{Z}$, dass aus $a \sim_n a'$ auch $ka \sim_m ka'$ folgt. Sei $l \in \mathbb{Z}$, so dass $a = a' + ln$. Dann ist $ka - ka' = kln$. Weil dies für beliebig mögliche l ein Vielfaches von m sein soll, muss kn ein Vielfaches von m sein, dass die Abbildung wohldefiniert ist.

[2] Siehe `https://math.stackexchange.com/questions/747342/extended-euclidean-algorithm-for-modular-inverse`

Aufgabe 3. Versuchen Sie Ihren Schreibstil zu üben. Um zum Beispiel die Regel $-0 = 0$ zu beweisen, wird etwa folgendes Argument erwartet:
Das additive Inverse -0 von 0 muss nach Definition der Inversen die Eigenschaft $(-0) + 0 = 0 + (-0) = 0$ erfüllen. Da aber die Definition des neutralen Elementes besagt, dass $0 + 0 = 0 + 0 = 0$ gilt und weil die Inverse in einer Gruppe eindeutig ist, muss $-0 = 0$ gelten.
Seien $x, y, z \in \mathbb{R}$. Zeigen Sie die folgenden weiteren Rechenregeln:

1. $-(x + y) = (-x) + (-y)$ (wobei wir für letzteres auch $= -x - y$ schreiben),
2. $-(x - y) = -x + y$,
3. Zeigen Sie, dass das Distributivgesetz für die Subtraktion $x(y - z) = xy - xz$. gilt.

Lösung.

1. Wegen Assoziativität und Kommutativität der Addition ist $(x+y)+((-x)+(-y))$ das gleiche wie $(x + (-x)) + (y + (-y)) = 0 + 0 = 0$. Aus der Eindeutigkeit der Inversen folgern wir $-(x + y) = (-x) + (-y)$.
2. Das folgt direkt aus der vorherigen Teilaufgabe, wenn wir y durch $-y$ ersetzen, sowie der Gleichung (2.2) aus dem Skript, welche besagt dass $-(-y) = y$.
3. Dies folgt aus dem Distributivgesetz für die Addition indem wir $y-z$ als $y+(-z)$ schreiben:

   $$x(y-z) = x(y+(-z)) = xy+x\cdot(-z) = xy+x\cdot((-1)\cdot z) = xy+(-1)(xz) = xy-xz,$$

   wobei wir wieder Assoziativität und Kommutativität der Multiplikation verwendet haben.

Aufgabe 4. Sei $(K, \leq)$ ein angeordneter Körper. Zeigen Sie, dass

$$x \leq y \iff x^3 + x \leq y^3 + y$$

für alle $x, y \in K$ gilt.

Lösung. Wir werden 2.11(k) aus dem Skript benutzen. Also

$$0 \leq x \leq y, \qquad 0 \leq z \leq w \qquad \Rightarrow \qquad 0 \leq xz \leq yw.$$

Dies folgt aus dem im Skript gezeigten 2.11(h)

$$0 \leq x, \qquad y \leq z \qquad \Rightarrow \qquad xy \leq xz,$$

weil

1. aus $0 \leq z, x \leq y$ die Ungleichung $xz \leq yz$ folgt,
2. aus $0 \leq y, z \leq w$ die Ungleichung $yz \leq yw$ folgt und
3. wir dann die Transitivität der Ordnung $\leq$ benutzen können.

Nun zur eigentlichen Aufgabe:
$\Rightarrow$: Wir nehmen $x \leq y$ an und beweisen $x^3 + x \leq y^3 + y$.

$\underline{0 \leq x}$: Dann folgt aus $0 \leq x \leq y$ und mehrfachem Anwenden von 2.11(k) mit $x = z$ und $y = w$, dass $x^n \leq y^n$ für alle n. Mit 2.11(c) aus dem Skript können wir Ungleichungen addieren. Also $x \leq y$ und $x^3 \leq y^3$ implizieren zusammen $x^3 + x \leq y^3 + y$.

$\underline{y \leq 0}$: Wir führen diesen Fall auf den vorherigen zurück. Aus $x \leq y$ und $y \leq 0$ folgt $0 \leq -y \leq -x$. Der vorherige Fall impliziert $-y^3 - y = (-y)^3 - y \leq (-x)^3 - x = -x^3 - x$, also $x^3 + x \leq y^3 + y$.

$\underline{x \leq 0 \leq y}$: In diesem Fall ist $x^3 \leq 0$ und $0 \leq y^3$. Also bekommen wir die gewünschte Ungleichung, wenn wir die Ungleichungen $x^3 \leq y^3$ und $x \leq y$ addieren.

$\Leftarrow$: Wir nehmen $x^3 + x \leq y^3 + y$ an und beweisen $x \leq y$.
Falls $x > y$ wäre, könnten wir wie oben herleiten, dass $x^3 + x > y^3 + y$, was ein Widerspruch zur Annahme ist.

Aufgabe 5. Sei $(K, \leq)$ ein angeordneter Körper und seien $x, y, z \in K$ mit $xyz > 0$. Zeigen Sie, dass die folgende Ungleichung gilt

$$\frac{x}{yz} + \frac{y}{zx} + \frac{z}{xy} \geq \frac{1}{x} + \frac{1}{y} + \frac{1}{z}.$$

Lösung. Wir haben $(x - y)^2 \geq 0$, $(y - z)^2 \geq 0$ und $(z - x)^2 \geq 0$. Somit gilt

$$(x - y)^2 + (y - z)^2 + (z - x)^2 \geq 0.$$

Wir multiplizieren die Klammern aus und erhalten

$$x^2 - 2xy + y^2 + y^2 - 2yz + z^2 + z^2 - 2zx + x^2 \geq 0.$$

Umgeformt also

$$2(x^2 + y^2 + z^2) \geq 2(xy + yz + zx).$$

Mit $2 = 1 + 1 > 0$ und 2.11(m) aus dem Skript (ist eine einfache Konsequenz aus 2.11(h)), ist die Ungleichung

$$2(x^2 + y^2 + z^2) \geq 2(xy + yz + zx)$$

äquivalent zu

$$x^2 + y^2 + z^2 \geq xy + yz + zx.$$

Weil $xyz > 0$ ist, gilt auch $(xyz)^{-1} = \frac{1}{xyz} > 0$ aus 2.11(j) und somit

$$\frac{x}{yz} + \frac{y}{zx} + \frac{z}{xy} = \frac{x^2 + y^2 + z^2}{xyz} \geq \frac{xy + yz + zx}{xyz} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}.$$

Aufgabe 6. (*Umgekehrte Dreiecksungleichung*) Sei $(K, \leq)$ ein angeordneter Körper. Zeigen Sie, dass für alle $x, y \in K$ die Ungleichung

$$\big||x| - |y|\big| \leq |x - y|$$

gilt. In welchen Fällen gilt Gleichheit?

Lösung. Durch die Dreiecksungleichung haben wir

$$|x| = |x - y + y| \leq |x - y| + |y|,$$

was uns

$$|x| - |y| \leq |x - y|$$

liefert. Analog gibt uns die Dreiecksungleichung

$$|y| = |y - x + x| \leq |y - x| + |x| = |x - y| + |x|,$$

aus welchem wiederum

$$|y| - |x| \leq |x - y| \iff |x| - |y| \geq -|x - y|$$

folgt. Somit ist $-|x - y| \leq |x| - |y| \leq |x - y|$, also $\big||x| - |y|\big| \leq |x - y|$.

Gleichheit gilt genau dann, wenn $\operatorname{sgn}(x) \cdot \operatorname{sgn}(y) \in \{0, 1\}$*:* Wir prüfen drei Fälle nach:

1. $\operatorname{sgn}(x) \cdot \operatorname{sgn}(y) = 0$ (äquivalent zu $x = 0$ oder $y = 0$):
   In diesem Fall ist es direkt ersichtlich, dass die umgekehrte Dreiecksungleichung erfüllt ist.

2. $\text{sgn}(x) \cdot \text{sgn}(y) = 1$ (äquivalent zu $x, y > 0$ oder $x, y < 0$):
   Dann ist in der Tat
   $$||x| - |y|| = \begin{cases} |x-y|, \ x, y > 0, \\ |-x-(-y)| = |-(x-y)| = |x-y|, \ x, y < 0. \end{cases}$$

3. $\text{sgn}(x) \cdot \text{sgn}(y) = -1$ (äquivalent zu $x < 0, y > 0$ oder $x > 0, y < 0$):
   Wir betrachten den Fall $x > 0$ und $y < 0$. Dann ist
   $$||x| - |y|| = |x - (-y)| = |x + y| \qquad \text{und} \qquad |x - y| = x - y.$$
   Falls Gleichheit $|x+y| = x-y$ gelten würde, wäre $x+y = x-y$ oder $x+y = y-x$. Also $y = -y$ oder $x = -x$. Dies führt[3] aber zu $x = 0$ oder zu $y = 0$, einem Widerspruch. Der Fall $x > 0, y < 0$ folgt analog.

Aufgabe 7.

1. Sei K ein Körper mit endlich vielen Elementen, kurz gesagt ein endlicher Körper. Zeigen Sie, dass es keine Ordnungsrelation auf K gibt, die K zu einem angeordneten Körper machen würde.
2. Sei K ein Körper. Angenommen es gibt ein Element $u \in K$ mit der Eigenschaft $u^2 + 1 = 0$. Zeigen Sie, dass es keine Ordnungsrelation auf K gibt, die K zu einem angeordneten Körper machen würde.

Lösung.

1. Wir nehmen per Widerspruch an, dass es eine Ordnungsrelation $\leq$ auf K gibt die K zu einem angeordneten Körper macht. Wir schreiben 1 für das Einselement von K, und wissen dass $0 < 1$ gilt (Folgerung (g)). Sei n die Anzahl Elemente von K. Wir erhalten strikte Ungleichungen
   $$0 < 1 < 1 + 1 < 1 + 1 + 1 < \cdots < \underbrace{1 + \cdots + 1}_{n-\text{mal}}$$
   was einen Widerspruch erzeugt, da dies $n + 1$ verschiedene Elemente wären.

   Ein angeordneter Körper muss also undendlich viele Elemente haben.

[3]Für die, die es ganz genau haben wollen: Wir benutzen hier, dass K ein Körper mit Charakteristik grösser als zwei ist, also $1 + 1 \neq 0$. Man kann zeigen, dass in einem angeordneten Körper $1 + 1 \neq 0$ nicht passieren kann. Für die Details, verweisen wir auf die Algebra Vorlesungen.

2. Wir nehmen an, dass es eine Ordnungsrelation $\leq$ auf K gibt, welche K zu einem angeordneten Körper macht. Da $u^2 \neq 0$, ist $u \neq 0$ und darum entweder $u > 0$ oder $u < 0$.

   $\underline{u > 0}$: Falls $u > 0$ gilt, dann ist $0 < u^2 = -1$. Die Gleichung $0 < -1$ steht aber zum Widerspruch zu $0 < 1$.

   $\underline{u < 0}$: Falls $u < 0$ gilt, dann ist $0 < -u$ und somit $0 < (-u)^2 = u^2 = -1$. Wie oben erzwingt dies einen Widerspruch.

   Somit schliessen wir, dass es keine Ordnungsrelation auf K gibt, die K zu einem angeordneten Körper machen würde.

   Im Besonderen kann $\mathbb{C}$ kein angeordneter Körper sein (für $u = i$ ist $i^2 + 1 = 0$).