Mathematisches Institut der Universität München
Wintersemester 2013/14

Daniel Rost
Lukas-Fabian Moser

Grundlagen der Mathematik I
Lösungsvorschlag zum 14. Tutoriumsblatt

Aufgabe 1.

a) Der Euklidische Algorithmus besteht in einer wiederholten Division mit Rest:

$$\begin{aligned} 6.706 &= 10 \cdot 623 + 476 \\ 623 &= 1 \cdot 476 + 147 \\ 476 &= 3 \cdot 147 + 35 \\ 147 &= 4 \cdot 35 + \boxed{7} \\ 35 &= 5 \cdot 7 + 0. \end{aligned}$$

b) Der letzte Rest > 0, der sich im Euklidischen Algorithmus ergibt, ist ein größter gemeinsamer Teiler von a und b, in diesem Fall also $d = 7$. Zur Bestimmung von x und y mit $7 = x \cdot a + y \cdot b$ kann man die Rechnung aus dem Algorithmus rückwärts lesen:

$$\begin{aligned} 7 &= 147 - 4 \cdot 35 = 147 - 4 \cdot (476 - 3 \cdot 147) \\ &= 13 \cdot 147 - 4 \cdot 476 = 13 \cdot (623 - 1 \cdot 476) - 4 \cdot 476 \\ &= 13 \cdot 623 - 17 \cdot 476 = 13 \cdot 623 - 17 \cdot (6.706 - 10 \cdot 623) \\ &= 183 \cdot \underbrace{623}_{=b} - 17 \cdot \underbrace{6.706}_{=a}, \end{aligned}$$

also können wir $x := -17$ und $y := 183$ nehmen.

c) Laut Vorlesung ist

$$v := \frac{ab}{d} = \frac{6.706 \cdot 623}{7} = 596.834$$

ein kleinstes gemeinsames Vielfaches von a und b.

Aufgabe 2. Laut Vorlesung gibt es Zahlen $x_1, y_1 \in \mathbb{Z}$ mit $d_1 = x_1 a + y_1 c$ und Zahlen $x_2, y_2 \in \mathbb{Z}$ mit $d_2 = x_2 b + y_2 c$. Dann ist

$$\begin{aligned} d_1 \cdot d_2 &= (x_1 a + y_1 c) \cdot (x_2 b + y_2 c) \\ &= x_1 x_2 \cdot ab + x_1 y_2 ac + x_2 y_1 bc + y_1 y_2 c^2. \end{aligned}$$

Da nach Voraussetzung c ein Teiler von ab ist, teilt c jeden Summanden im letzten Ausdruck, also ist c ein Teiler von $d_1 \cdot d_2$.

Aufgabe 3.

a) Der Hinweis lautet, die Werte $a^2 + k$ und $a^2 - k^2$ miteinander zu vergleichen: Letzterer läßt sich faktorisieren als $(a - k)(a + k)$, ist also stets durch $a + k$ teilbar. Andererseits ist

$$(a^2 + k) - (a^2 - k^2) = k^2 + k = k \cdot (k + 1),$$

also ist die Zahl $a + k$ genau dann ein Teiler von $a^2 + k$, wenn sie ein Teiler von $k \cdot (k + 1)$ ist.

(Der Kern dieses Arguments lautet: Ist $a + b = c$, und ist d ein Teiler von b, so gilt $d \mid a \iff d \mid c$.)

b) Nach a) (für $k = 6$) gilt für alle $a \neq -6$

$$\begin{aligned}
& (a+6) \mid (a^2+6) \\
\iff \quad & a+6 \in T(6 \cdot 7) = T(42) \\
\iff \quad & a+6 \in \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\} \\
\iff \quad & a \in \{-48, -27, -20, -13, -12, -9, -8, -7, -5, -4, -3, 0, 1, 8, 15, 36\}\,.
\end{aligned}$$

c) Wieder nach a) (für $k = -6$) gilt für alle $a \neq 6$

$$\begin{aligned}
& (a-6) \mid (a^2-6) \\
\iff \quad & a-6 \in T((-6)\cdot(-5)) = T(30) \\
\iff \quad & a-6 \in \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\} \\
\iff \quad & a \in \{-24, -9, -4, 0, 1, 3, 4, 5, 7, 8, 9, 11, 12, 16, 21, 36\}\,.
\end{aligned}$$

Aufgabe 4.

a) Es ist zum einen zu überprüfen, daß $x * y$ wirklich für alle $x, y \in G$ ein sinnvoller Ausdruck ist (in diesem Fall also: daß niemals durch 0 dividiert wird), und zum anderen, daß sein Wert tatsächlich wieder ein Element von G ist.

Für ersteres zeigen wir (wie im Hinweis vorgeschlagen) sogar, daß $1 + xy > 0$ für $x, y \in G$ ist: Wegen $|x|\,, |y| < 1$ folgt $|xy| = |x| \cdot |y| < 1$, also insbesondere $-1 < xy$ und damit $xy + 1 > 0$.

Zum Nachweis, daß für $x, y \in G$ auch $x * y \in G$ gilt, können wir nun (da wir wissen, daß der Nenner $xy + 1$ positiv ist), äquivalent umformen:

$$\begin{aligned}
& x * y \in G \\
\iff \quad & \frac{x+y}{1+xy} \in\,]-1, 1[\\
\iff \quad & -1 < \frac{x+y}{1+xy} < 1 \\
\iff \quad & -1 - xy < x + y < 1 + xy
\end{aligned}$$

Nun gilt aber

$$x + y < 1 + xy \iff x \cdot (1-y) < 1 - y,$$

und die letzte Aussage ist wahr wegen $1 - y > 0$ und $x < 1$; ebenso gilt

$$-1 - xy < x + y \iff -1 - y < (1+y)x \iff -(1+y) < (1+y) \cdot x,$$

und die letzte Aussage ist wahr wegen $1 + y > 0$ und $x > -1$.

b) Wir wissen schon, daß $*$ eine Verknüpfung auf G ist; ihre **Kommutativität** (für das Adjektiv „abelsch“) ist offensichtlich, weil

$$x * y = \frac{x+y}{1+xy} = \frac{y+x}{1+yx} = y * x$$

gilt.

Die **Assoziativität** von $*$ sieht man anhand der folgenden Rechnung: Für $x, y, z \in G$ gilt

$$\begin{aligned}
(x * y) * z &= \frac{x+y}{1+xy} * z = \frac{\frac{x+y}{1+xy} + z}{1 + \frac{x+y}{1+xy} \cdot z} \\
&= \frac{x + y + (1+xy) \cdot z}{1 + xy + (x+y) \cdot z} \\
&= \frac{x+y+z+xyz}{1+xy+yz+zx} \\
\text{sowie} \quad x * (y * z) &= x * \frac{y+z}{1+yz} = \frac{x + \frac{y+z}{1+yz}}{1 + x \cdot \frac{y+z}{1+yz}} \\
&= \frac{x \cdot (1+yz) + y + z}{1 + yz + x \cdot (y+z)} \\
&= \frac{x+y+z+xyz}{1+xy+yz+zx},
\end{aligned}$$

also ist tatsächlich $(x * y) * z = x * (y * z)$.

Ich behaupte, daß die Zahl $0 \in G$ **neutrales Element** von $(G, *)$ ist: Denn für alle $x \in G$ ist

$$\begin{aligned}
x * 0 &= \frac{x+0}{1+x \cdot 0} = \frac{x}{1} = x \\
\text{und} \quad 0 * x &= \frac{0+x}{1+0 \cdot x} = \frac{x}{1} = x,
\end{aligned}$$

wobei man sich die zweite Zeile aufgrund der Kommutatitivät von $*$ auch sparen könnte.

Für die Existenz von **Inversen** sei $x \in G$ gegeben; wir müssen ein $y \in G$ finden mit $x * y = 0 = y * x$. Ein offensichtlicher Kandidat (man betrachte den Zähler des Bruches, der $*$ definiert!) ist $y := -x$, und tatsächlich gilt mit dieser Festlegung sowohl $y \in G$ als auch

$$x * y = \frac{x + (-x)}{1 + x \cdot (-x)} = \frac{0}{1 - x^2} = 0$$

(und ebenso $y * x = 0$, schon wegen der Kommutativität von $*$).

Also ist $(G, *)$ eine Gruppe, genauer: eine abelsche Gruppe, weil die Verknüpfung $*$ ja kommutativ ist.

Für Interessierte: Wie kann man eine solche merkwürdige Gruppenstruktur finden?

Die Grundidee ist es, die Struktur einer schon bekannten Gruppe – in diesem Fall ist das die Gruppe $(\mathbb{R}, +)$ – mittels einer bijektiven Abbildung $f : \mathbb{R} \to G$ auf die Menge G zu „überspielen", und zwar durch die Festlegung, daß für $x, y \in G$ gelten soll

$$x * y := f(f^{-1}(x) + f^{-1}(y)),$$

also in Worten: Um $x, y \in G$ zu verknüpfen, ziehe man sie mittels f^{-1} in die Menge $\mathbb{R}$, addiere sie dort und schiebe das Resultat mittels f wieder in die Menge G zurück. Man kann sich relativ leicht überlegen, daß man auf diese Art automatisch eine Gruppenstruktur auf G erhält, deren neutrales Element $f(0)$ ist.

Die in unserer Aufgabe angegebene Gruppenstruktur entsteht nun durch die Wahl von $f(t) := \tanh(t)$, wobei $\tanh$ der sogenannte „Tangens hyperbolicus" ist, der definiert ist durch

$$\tanh : \mathbb{R} \to \,]-1, 1[\,, \quad t \mapsto \frac{e^t - e^{-t}}{e^t + e^{-t}}.$$

Diese Funktion ist bijektiv, und für sie gilt das sogenannte „Additionstheorem"

$$\tanh(s+t) = \frac{\tanh(s) + \tanh(t)}{1 + \tanh(s)\tanh(t)},$$

und damit ergibt sich

$$x * y = \tanh(\tanh^{-1}(x) + \tanh^{-1}(y)) = \frac{\tanh(\tanh^{-1}(x)) + \tanh(\tanh^{-1}(y))}{1 + \tanh(\tanh^{-1}(x))\tanh(\tanh^{-1}(y))} = \frac{x + y}{1 + xy}.$$