Mathematisches Institut
der Universität München
Prof. Dr. Peter Otte

WiSe 2013/14
Lösung 3
29.10.2013

Übungen zur Analysis 1
für Informatiker und Statistiker

Lösung zu Blatt 3

Aufgabe 3.1 [Gruppen; 8 Punkte] Eine Menge G ausgestattet mit einer Verknüpfung $*$ heißt *Gruppe*, $(G, *)$, falls gilt

(i) $a * (b * c) = (a * b) * c$, $\forall a, b, c \in G$ (*Assoziativität*)

(ii) $\exists e \in G$ (*links-neutrales Element*), sodass $e * a = a \; \forall a \in G$

(iii) $\forall a \in G \; \exists b \in G$ (*links-inverses Element zu* a), sodass $b * a = e$.

Eine Gruppe $(G, *)$ heißt *abelsch* (oder *kommutativ*), falls

(iv) $a * b = b * a$ für alle $a, b \in G$

Sei nun $(G, *)$ eine Gruppe. *Zeigen Sie:*

(a) Ist $a \in G$, b ein links-inverses Element zu a und e ein links-neutrales Element von G, dann gilt $a * b = e$, sowie $a * e = a$. [*Hinweis:* Machen Sie in jedem Schritt in ihrer Lösung deutlich, welche der Eigenschaften (i)-(iii) Sie jeweils benutzen.]

Beweis. [2 Punkte] Hier wie in den meisten folgenden Teilaufgaben gibt es viele Lösungsmöglichkeiten. Jeder einwandfreie Beweis ist akzeptabel.

b ist auch rechts-invers (Variante 1): Sei c ein links-inverses Element zu b, dann gilt $a * b \overset{(ii)}{=} (e * a) * b \overset{(iii)}{=} ((c * b) * a) * b \overset{(i)}{=} c * ((b * a) * b) \overset{(iii)}{=} c * (e * b) \overset{(ii)}{=} c * b \overset{(iii)}{=} e.$

b ist auch rechts-invers (Variante 2): Eine weitere Lösungsmöglichkeit bietet die Beobachtung, dass für $x \in G$, gilt: $x^2 = x \implies x = e$ (Multiplikation mit x^{-1} von links, Benutzung der linksinversen und Linksneutralen Eigenschaften). Wir haben dann $(a * b)^2 = a * b * a * b = a * (b * a) * b = a * e * b = a * b$ (mehrmalige Benutzung von Assoziativität, sowie Definition von links-neutralen und links-inversen Elementen), und daher $a * b = e$.

Schließlich haben wir noch $a * e = a * (a^{-1} * a) = (a * a^{-1}) * a = e * a = a$ (Benutzung des vorherigen Schritts, Assoziativität und Links-neutralität von e). □

(b) Es gibt nur ein links-neutrales Element. [*Hinweis:* Aus (a) folgt, dass dieses auch rechts-neutral ist; es wird deshalb *das neutrale Element der Gruppe* genannt].

Beweis. [1 Punkt] Sei e' ein weiteres links-neutrales Element. Dann gilt $e' = e' * e = e$, wobei die erste Gleichheit aus Rechts-neutralität von e (vorherige Teilaufgabe) und die zweite aus Links-neutralität von e' folgt. □

(c) Für jedes $a \in G$ gibt es nur ein links-inverses Element.

Beweis. [1 Punkt] Seien b_1, b_2 links-invers zu a. Dann gilt $b_2 * a = e$, sowie $a * b_1 = e$ (da b_2 wegen (a) auch rechts-invers ist). Somit $b_1 = e * b_1 = b_2 * a * b_1 = b_2 * e = b_2$. □

(d) Für $a, b \in G$ gilt $(a * b)^{-1} \ = b^{-1} * a^{-1}$ (*shoe-socks property*).

Beweis. [1 Punkt] Es gilt $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = b^{-1} * b = e$ (Assoziativität, a^{-1} links-invers, e links-neutral, b^{-1} links-invers). Somit ist $b^{-1} * a^{-1}$ (links-)invers zu $a * b$. Wegen der Eindeutigkeit aus Teilaufgabe (c) gilt deshalb $b^{-1} * a^{-1} = (a * b)^{-1}$. □

(e) Für $a \in G$ gilt: $(a^{-1})^{-1} = a$ (*Involutionseigenschaft*).

Beweis. [1 Punkt] $a * a^{-1} = e$ nach Teilaufgabe (a), somit ist a links-invers zu a^{-1} und daher $a = (a^{-1})^{-1}$ nach Teilaufgabe (c). □

(f) $(\mathbb{R}, +)$ und $(\mathbb{R}\backslash\{0\}, \cdot\,)$ sind abelsche Gruppen. Identifizieren Sie jeweils das neutrale und die inversen Elemente.

Beweis. [2 Punkte] In den Definitionen 1.32 und 1.35 werden Addition und Multiplikation auf $\mathbb{R}$ als Verknüpfungen definiert, die gerade die Gruppeneigenschaften zusammen mit der Kommutativität erfüllen. Das neutrale Element von $(\mathbb{R}, +)$ ist 0, das von $(\mathbb{R} \setminus \{0\}, \cdot)$ ist 1. Für $x \in \mathbb{R}$ ist $-x$ das Inverse in $(\mathbb{R}, +)$ und $1/x$ das Inverse in $(\mathbb{R} \setminus \{0\}, \cdot)$. □

Aufgabe 3.2 [Symmetrische Differenz; 8 Punkte] Wir definieren die logische Verknüpfung, die einem *ausschließenden oder* (d.h. einem *entweder-oder*) entspricht, genannt *Kontravalenz* oder *XOR-Verknüpfung*, durch

$$A \veebar B \ := \ (A \wedge \neg B) \vee (\neg A \wedge B)\,,$$

wobei A, B zwei Aussagen bezeichnen. Weiter, sei für zwei Mengen M, N die *symmetrische Differenz* $M \Delta N$ definiert durch

$$M \Delta N \ := \ \big\{x \,\big|\, (x \in M) \veebar (x \in N)\big\}\,.$$

(a) *Zeigen Sie:* $M \Delta N \ = \ (M \backslash N) \cup (N \backslash M)\,.$

Beweis. [Insg. 2 Punkte] Seien $A = (M \setminus N) \cup (N \setminus M)$ und $x \in M \triangle N$. Wenn $x \in M$, dann $x \notin N$ und somit $x \in (M \setminus N) \subset A$. Genauso, wenn $x \in N$. Daher $M \triangle N \subset A$. [1 Punkt]. Sei nun $x \in A$. Entweder $x \in M \setminus N$ oder $x \in N \setminus M$ (denn $(M \setminus N) \cap (N \setminus M) = \emptyset$). In jedem Fall gilt $x \in M \triangle N$, also $A \subset M \triangle N$ [1 Punkt]. Daher $M = N$. □

(b) Sei X eine Menge. *Zeigen Sie:* $(\mathcal{P}(X), \Delta)$ ist eine abelsche Gruppe.

Beweis. [Insg. 6 Punkte] Wenn $M, N \subset X$, dann $M \triangle N \subset X$, und somit ist

$$P(X) \times P(X) \to P(X), \quad (M, N) \mapsto M \Delta N$$

eine Verknüpfung [1 Punkt]. Offenbar ist $M \triangle N = N \triangle M$ (denn die Vereinigung ist kommutativ), und somit ist Δ abelsch [1 Punkt]. Ist $M \in \mathcal{P}(X)$, so gilt $\emptyset \triangle M = M$, d.h. $\emptyset$ ist das (eindeutige links-)neutrale Element [1 Punkt]. Außerdem gilt $M \triangle M = \emptyset$, links-inverse Elemente existieren also [1 Punkt].

Schließlich zeigt eine Wahrheitstabelle (oder Verwendung der Distributivgesetze und de Morgan'schen Regeln) leicht, dass für Aussagen A, B und C gilt

$$(A \veebar B) \veebar C \;\Leftrightarrow\; (A \wedge B \wedge C) \vee (\text{genau eines von } A,\ B,\ C \text{ wahr}).$$

Die rechte Seite ist offenbar symmetrisch in A, B und C. Somit ist $\veebar$ assoziativ (da es offenbar kommutativ ist), und daher ist auch $\triangle$ assoziativ [2 Punkte].

[*Alternativ:* Beweis der Assoziativität von $\veebar$ durch Wahrheitstabelle.] $\square$

Aufgabe 3.3 [Relationen; 8 Punkte] Sei M eine Menge. Eine Teilmenge $R \subset M \times M$ wird *Relation in* (oder *auf*) M genannt. In diesem Zusammenhang schreiben wir xRy für die Aussage $(x, y) \in R$.

(a) Machen Sie sich klar, dass eine Ordnungsrelation $\prec$ (siehe Def. 1.41) eine Relation ist und drücken Sie die Reflexivitäts-, Antisymmetrie- und Transitivitätsbedingungen in Elementschreibweise aus. [Beispiel: R ist *symmetrisch*, falls $(x, y) \in R \Rightarrow (y, x) \in R$.]

Beweis. [1 Punkt] Wie aus Definition 1.41 folgt, kann eine Ordnungsrelation $\prec$ mit einer Teilmenge $R \subset M^2 = M \times M$ identifiziert werden, die folgende Eigenschaften erfüllt:

$$\begin{aligned} x \in M \;&\Rightarrow\; (x, x) \in R && (\textit{Reflexivität}) \\ (x, y), (y, x) \in R \;&\Rightarrow\; x = y && (\textit{Antisymmetrie}) \\ (x, y), (y, z) \in R \;&\Rightarrow\; (x, z) \in R && (\textit{Transitivität}) \end{aligned}$$

$\square$

Eine Relation heißt *Äquivalenzrelation*, wenn sie reflexiv, symmetrisch und transitiv ist. Ist $\sim$ eine Äquivalenzrelation auf M, dann schreiben wir $[x] := \{y \in M \mid x \sim y\}$ (*Äquivalenzklasse von* x), sowie $M/\!\sim\; := \{[x] \mid x \in M\}$.

(b) Finden Sie eine Äquivalenzrelation, die auf jeder Menge M definiert werden kann, und geben Sie die zugehörigen Äquivalenzklassen an.

Beweis. [1 Punkt] Die gesuchte Relation ist $R := \{(x, y) \in M^2 \mid x = y\}$. Diese ist offensichtlich reflexiv, symmetrisch und transitiv, also eine Äquivalenzrelation. Die Äquivalenzklassen sind $[x] = \{x\}$. $\square$

(c) Sei $\sim$ eine Äquivalenzrelation auf einer Menge M. *Zeigen Sie:* $M = \bigsqcup_{[x]\in M/\sim}[x]$, wobei mit $\bigsqcup$ die Vereinigung über paarweise disjunkte Mengen bezeichnet wird.

Beweis. [Insg. 2 Punkte] Zunächst gilt für alle $x, y \in M$ mit $[x] \neq [y]$, dass $[x] \cap [y] = \emptyset$, denn gäbe es $z \in [x] \cap [y]$, dann wäre $x \sim z$ und $z \sim y$ (Symmetrie), also $x \sim y$ (Transitivität), was im Widerspruch steht zu $[x] \neq [y]$. In $\cup_{[x]\in M/\sim}[x]$ wird also über paarweise disjunkte Mengen vereinigt [1 Punkt].

Für die Gleichheit $M = \sqcup_{[x]\in M/\sim}[x]$, bemerken wir zunächst, dass $\sqcup_{[x]\in M/\sim}[x] \subset M$ klar ist, denn eine Vereinigung von Teilmengen $[x] \subset M$ ist immer Teilmenge von M. Sei nun $y \in M$, dann ist $y \in [y]$ (Reflexivität), und damit $y \in \sqcup_{[x]\in M/\sim}[x]$, also gilt $M \subset \sqcup_{[x]\in M/\sim}[x]$. Insgesamt $M = \sqcup_{[x]\in M/\sim}[x]$. [1 Punkt] □

(d) Seien M, N nichtleere Mengen und $f : M \to N$ eine surjektive Abbildung. *Zeigen Sie*, dass durch $x_1 \sim x_2 \;:\Leftrightarrow\; f(x_1) = f(x_2)$ eine Äquivalenzrelation auf M induziert wird, sowie, dass

$$\tilde{f} : M/\sim \;\to\; N, \quad \tilde{f}([x]) := f(x)$$

eine wohldefinierte Bijektion ist.

Beweis. [Insg. 4 Punkte] Wir zeigen zunächst, dass die obigen definierte Relation $\sim$ eine Äquivalenzrelation auf M ist. (i) Reflexivität: Für $x \in M$ gilt $f(x) = f(x)$, also $x \sim x$. (ii) Symmetrie: Ist $x \sim y$, dann gilt $f(y) = f(x)$, also auch $y \sim x$. (iii) Transit.: Ist $x \sim y$ und $y \sim z$, dann $f(x) = f(y) = f(z)$, also auch $x \sim z$. [1 Punkt]

Die obige Zuordnung $\tilde{f} : M/\sim \to N$ ist eine (wohldefinierte) Abbildung, denn für $[x] = [y]$ gilt $x \sim y$ und damit $f(x) = f(y)$. [1 Punkt]

$\tilde{f}$ ist surjektiv, denn ist $w \in N$, so gibt es $x \in M$ mit $f(x) = w$ (Surjektivität von f), also ist w das Bild von $[x] \in M/\sim$ unter $\tilde{f}$. [1 Punkt]

Zusätzlich ist $\tilde{f}$ auch injektiv, denn aus $\tilde{f}([x]) = \tilde{f}([y])$ folgt $f(x) = f(y)$ und damit $x \sim y$, d.h. $[x] = [y]$. [1 Punkt] □

Aufgabe 3.4 [Geometrische Reihe; 8 Punkte] Zeigen Sie, dass für jede reelle Zahl $x \neq 1$ und $n \in \mathbb{N}$ gilt

$$1 + x + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1}.$$

Beweis. [2 Punkte] Die Gleichheit wird durch vollständige Induktion bewiesen. Sie ist offenbar wahr für $n = 1$. Außerdem gilt

$$\frac{x^{n+2} - 1}{x - 1} - \frac{x^{n+1} - 1}{x - 1} = \frac{x^{n+2} - x^{n+1}}{x - 1} = x^{n+1}\frac{x - 1}{x - 1} = x^{n+1},$$

was den Induktionsschritt beweist. □

Folgern Sie:

(*i*) Für $0 \leqslant x < 1$ hat $\{1, 1+x, 1+x+x^2, \dots\}$ kleinste obere Schranke $\frac{1}{1-x}$.

Beweis. [Insg. 3 Punkte] Für $x = 0$ ist das Problem trivial. Wir nehmen daher an, dass $0 < x < 1$.

Sei $a_n = 1 + x + \cdots + x^n$. Dann gilt $a_n = \frac{1-x^{n+1}}{1-x}$ nach dem ersten Teil, und somit $a_n = \frac{1}{1-x} - \frac{x^n}{1-x} \leq \frac{1}{1-x}$ solange $\frac{x^n}{1-x} \geq 0$. Dies gilt offenbar für $0 \leq x < 1$, und somit ist $\frac{1}{1-x}$ eine obere Schranke für $\{a_n | n \in \mathbb{N}\}$ [1 Punkt].

Um zu zeigen, dass $\frac{1}{1-x}$ die kleinste obere Schranke ist, sei $y < \frac{1}{1-x}$. Wir müssen zeigen, dass es ein $n \in \mathbb{N}$ gibt mit

$$\left(\tfrac{1-x^{n+1}}{1-x} = \right) a_n \; > \; y \, .$$

Sei $\epsilon := \frac{1}{1-x} - y > 0$. Wir müssen also zeigen, dass $\exists n : \frac{x^{n+1}}{1-x} < \epsilon$. Da $1 - x > 0$ ist dies äquivalent zu $x^{n+1} < \epsilon(1-x)$. Dies wiederum ist äquivalent zu $(1/x)^n > (\epsilon(1-x)/x)^{-1} =: r$.

Es ist also hinreichend zu zeigen: für $r \in \mathbb{R}, s > 1$ gibt es $n \in \mathbb{N}$ mit $s^n > r$. Da $t := s-1 > 0$ gilt $1+nt \leq (1+t)^n = s^n$, nach der Bernoulli-Ungleichung von Blatt 2. Für n hinreichend groß gilt $nt > r$ $(*)$ und somit $s^n > r$, was den Beweis abschließt. [2 Punkte]

Kommentar: $(*)$ erfordert eine geringfügig subtile Anwendung der Vollständigkeit von $\mathbb{R}$. Studenten, die bemerken dass $(*)$ nicht trivial ist, erhalten [1 Punkt], unabhängig davon, ob sie einen korrekten Beweis liefern. □

(*ii*) Sind $m > 1, n > 1$ natürliche Zahlen, sodass $m^n - 1$ prim ist, dann gilt $m = 2$ und n ist prim. [Eine natürliche Zahl m heißt prim, wenn sie nur durch ± 1 und $\pm m$ restfrei teilbar ist.]

Beweis. [Insg. 3 Punkte] Wir haben $m^n - 1 = (m-1)(1 + m + \cdots + m^{n-1})$ und das ist nur prim, wenn $m - 1 = \pm 1$ oder $1 + m + \cdots + m^{n-1} = \pm 1$. [1 Punkt] Die Forderungen $m \geq 2, n \geq 2$ implizieren, dass $m - 1 = 1$ die einzige Möglichkeit ist, und daher $m = 2$ [1 Punkt].

Wir zeigen durch Widerspruch, dass n prim ist: Wenn n zusammengesetzt ist, können wir schreiben $n = ab$ mit $a, b > 1$. Daher gilt $m^n - 1 = (m^a)^b - 1$. Aber $m^a \neq 2$ und $m^a \neq 0$, und somit $m^a - 1 \neq \pm 1$. $m^n - 1$ kann also nicht prim sein (siehe voriger Absatz), was im Widerspruch zur Bedingung an m, n steht [1 Punkt]. □