Universität des Saarlandes
Fakultät für Mathematik und Informatik
Fachrichtung Mathematik
Prof. Dr. Roland Speicher
Dr. Tobias Mai

Präsenzübungen zur Vorlesung *Höhere Mathematik für Ingenieure I*
Wintersemester 2020/21

Blatt 3 A
Lösungshinweise

Aufgabe 1: Es seien A und B beliebige Mengen und $f\colon A \to B$ eine Abbildung. Beweisen oder widerlegen Sie die folgenden Aussagen.

(a) Ist A höchstens abzählbar, so ist $f(A)$ höchstens abzählbar.

(b) Ist B höchstens abzählbar, so ist $f^{-1}(B)$ höchstens abzählbar.

Definition: Eine Menge M heißt ***höchstens abzählbar***, falls sie endlich im Sinne von Aufgabe 2 auf Präsenzblatt 2 B oder abzählbar unendlich ist.

Lösung:

(a) Es sei A endlich, d.h. $\#A = n$ für ein $n \in \mathbb{N}$. Ist f injektiv, so ist $\#f(A) = n$. Ist f nicht injektiv, so ist $1 \leq \#f(A) < n$. In jedem Fall ist $f(A)$ eine endliche Menge. Nun sei A abzählbar unendlich, d. h. es gibt eine bijektive Abbildung $\Phi\colon \mathbb{N} \to A$. Ist f injektiv, so ist eine Abzählung für $f(A)$ gegeben durch die Bijektion

$$\Psi\colon \mathbb{N} \to f(A), \quad n \mapsto f(\Phi(n)).$$

Ist f nicht injektiv, so ist $f(A)$ entweder endlich oder $f(A)$ hat unendlich viele Elemente und wir müssen in der obigen Abzählung Schritt für Schritt alle Elemente streichen, die bereits gezählt wurden. Eine Abzählung $\Psi\colon \mathbb{N} \to f(A)$ ist in diesem Fall gegeben durch die Rekursion $\Psi(1) := f(\Phi(1))$ und

$$\Psi(n) := f\Big(\Phi\big(\min\{m \in \mathbb{N} \mid f(\Phi(m)) \neq \Psi(k) \text{ für alle } k < n\}\big)\Big)$$

für alle $n \in \mathbb{N}$ mit $n \geq 2$.

(b) Es seien $A = \mathbb{R}$, $B_1 = \{1\}$, $B_2 = \mathbb{N}$ und $f(x) = 1$. Dann gilt

$$f^{-1}(B_1) = f^{-1}(B_2) = \mathbb{R},$$

sodass weder das Urbild der endlichen Menge B_1 noch das Urbild der abzählbar unendlichen Menge B_2 abzählbar sind.

Aufgabe 2: Es seien $M = \{1,2,3\}$ und $\{P_i\}_{i=1}^k$ mit $1 \leq k \leq 3$ eine *Partition* von M, d. h. $P_1, \dots, P_k$ sind nicht-leere Teilmengen von M, sodass $\bigcup_{i=1}^k P_i = M$ und $P_i \cap P_j = \emptyset$ für alle $i,j \in \{1,\dots,k\}$ mit $i \neq j$ gilt. Zeigen Sie, dass durch

$$x \sim y \qquad :\Longleftrightarrow \qquad \exists i \in \{1,\dots,k\} \colon x,y \in P_i$$

eine Äquivalenzrelation auf M gegeben ist. Wie viele Äquivalenzrelationen gibt es insgesamt auf M?

Lösung: Wir rechnen für $\sim$ die definierenden Eigenschaften einer Äquivalenzrelation nach:

- **Reflexivität:** Es sei $x \in M$. Da $\bigcup_{i=1}^k P_i = M$, existiert $i \in \{1,\dots,k\}$ mit $x \in P_i$. Insbesondere gilt also $x \sim x$.
- **Symmetrie:** Es seien $x,y \in M$ mit $x \sim y$. Dann gibt es $i \in \{1,\dots,k\}$ mit $x,y \in P_i$, also gilt auch $y \sim x$.
- **Transitivität:** Es seien $x,y,z \in M$ mit $x \sim y$ und $y \sim z$. Dann gibt es $i,j \in \{1,\dots,k\}$ mit $x,y \in P_i$ und $y,z \in P_j$. Da nach Voraussetzung $P_l \cap P_m = \emptyset$ für $l \neq m$ und $y \in P_i \cap P_j$, folgt $i = j$, sodass $x,z \in P_i$, also $x \sim z$.

Wie oben gezeigt ist durch eine Partition eine Äquivalenzrelation auf M gegeben. Umgekehrt definiert eine Äquivalenzrelation eine Zerlegung von M in Äquivalenzklassen die wegen der Transitivität per Definition disjunkt sind. Also ist durch eine Äquivalenzrelation eine Partition gegeben. Das bedeutet es gibt genau so viele Äquivalenzrelationen auf M, wie es Partitionen von M gibt. Im Fall $M = \{1,2,3\}$ sind das 5 Stück; nämlich

$$\big\{\{1,2,3\}\big\}, \quad \big\{\{1,2\},\{3\}\big\}, \quad \big\{\{1,3\},\{2\}\big\}, \quad \big\{\{2,3\},\{1\}\big\} \quad \text{und} \quad \big\{\{1\},\{2\},\{3\}\big\}.$$

Aufgabe 3: In Aufgabe 1 auf Präsenzblatt 2 B haben wir für jedes $n \in \mathbb{N}$ auf der Menge $\mathbb{Z}_n := \{0,1,\dots,n-1\}$ eine Addition $+_n$ und eine Multiplikation $*_n$ durch die folgenden Vorschriften definiert: Für $a,b \in \mathbb{Z}_n$ ist $a +_n b \in \mathbb{Z}_n$ bzw. $a *_n b \in \mathbb{Z}_n$ der Rest, den die ganze Zahl $a+b$ bzw. ab bei der Division mit n lässt.

(a) Wir betrachten den wichtigen Spezialfall, dass $n = p$ eine Primzahl ist. Zeigen Sie, dass dann $(\mathbb{Z}_p, +_p, *_p)$ ein Körper ist.

  Hinweis: Der *euklidische Algorithmus* erlaubt die Berechnung des größten gemeinsamen Teilers $\mathrm{ggT}(m,n)$ zweier natürlicher Zahlen $m,n \in \mathbb{N}$. Mit dem *erweiterten euklidischen Algorithmus* kann man zudem noch zwei ganze Zahlen $s,t \in \mathbb{Z}$ bestimmen, für die $\mathrm{ggT}(m,n) = sm + tn$ gilt. Diese Aussage, die als *Lemma von Bézout* bekannt ist, dürfen Sie ohne Beweis verwenden.

(b) Erklären Sie am Beispiel $(\mathbb{Z}_4, +_4, *_4)$, warum die Einschränkung auf Primzahlen entscheidend ist, um einen Körper zu erhalten.

Lösung:

(a) Da die Verknüpfungen $+_n$ und $*_n$ auf $\mathbb{Z}_n$ über die entsprechenden Verknüpfungen auf $\mathbb{Z}$ definiert sind, folgt direkt, dass $(\mathbb{Z}_n, +_n)$ eine Abelsche Gruppe mit dem neutralen Element 0 ist und dass auf $\mathbb{Z}_n$ das Distributivgesetz für $+_n$ und $*_n$ gilt. Es bleibt also zu zeigen, dass $(\mathbb{Z}_n \setminus \{0\}, *_n)$ im Fall $n = p$ eine Abelsche Gruppe mit dem neutralen Element 1 ist.

Wir überlegen uns zunächst, dass es zu jedem Element $0 \neq a \in \mathbb{Z}_p$ ein $s \in \mathbb{Z}_p$ mit $s *_p a = 1$ gibt. Hierfür verwenden wir den Hinweis. Weil p eine Primzahl und $a \in \mathbb{Z}_p$ ist, muss $\mathrm{ggT}(a, p) = 1$ gelten. Nach dem Lemma von Bézout finden wir also $s, t \in \mathbb{Z}$, sodass $sa + tp = 1$. Gemäß unserer Definition der Verknüpfungen $+_p$ und $*_p$ ist also $s *_p a = 1$; wegen $1 \neq 0$, ist zudem klar, dass $s \neq 0$ gelten muss.
Damit sehen wir, dass für $a, b \in \mathbb{Z}_p \setminus \{0\}$ auch $a *_p b \in \mathbb{Z}_p \setminus \{0\}$ sein muss, weil sonst

$$0 = s *_p 0 = s *_p (a *_p b) = (s *_p a) *_p b = 1 *_p b = b$$

einen Widerspruch zur Annahme $b \neq 0$ liefern würde. (Man beachte, dass wir hierbei verwendet haben, dass $+_p$ auf $\mathbb{Z}_p$ assoziativ ist und dass $1 *_p b = b$ sowie $b *_p 0 = 0$ für alle $b \in \mathbb{Z}_p$ gilt; diese Eigenschaften ergeben sich direkt aus der Assoziativität der Multiplikation auf $\mathbb{Z}$ und der Tatsache, dass $1 \cdot b = b$ für alle $b \in \mathbb{Z}$ gilt.)
Also ist $*_p : (\mathbb{Z}_p \setminus \{0\}) \times (\mathbb{Z}_p \setminus \{0\}) \to \mathbb{Z}_p \setminus \{0\}$ eine wohldefinierte Verknüpfung. Diese Verknüpfung ist assoziativ und kommutativ, weil sie von der Multiplikation von $\mathbb{Z}$ induziert wird, die eben diese Eigenschaften hat. Ferner haben wir gesehen, dass es zu jedem Element $0 \neq a \in \mathbb{Z}_p$ ein $s \in \mathbb{Z}_p \setminus \{0\}$ gibt mit $s *_p a = 1 = a *_p s$, d. h. s ist das Inverse zu a bezüglich $*_p$. Damit stellt $(\mathbb{Z}_p \setminus \{0\}, *_p)$ eine Abelsche Gruppe mit dem neutralen Element 1 dar.

(b) Für $2 \in \mathbb{Z}_4$ gilt $2 *_4 2 = 0$. Somit ist $\mathbb{Z}_4 \setminus \{0\}$ nicht abgeschlossen unter $*_4$; insbesondere kann 2 kein Inverses bezüglich $*_4$ besitzen.