Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Übungen zur Grundlagen der Mathematik im Wintersemester 2019/2020, Blatt 4
Fachbereich Mathematik, Stefan Geschke

A: Präsenzaufgaben am 4. November 2019

1. Eine *Partition* einer Menge M ist eine Menge nichtleerer Teilmengen von M, die paarweise disjunkt sind und deren Vereinigung ganz M ist. Für eine Partition P auf M definieren wir eine Relation $\sim_P$ indem dem wir für alle $a, b \in M$ definieren:

$$a \sim_P b \qquad \Leftrightarrow \qquad \exists A \in P(a \in A \wedge b \in A)$$

   Zeigen Sie, dass $\sim_P$ eine Äquivalenzrelation ist.

   Lösung. Sei M eine Menge und P eine Partition von M. **Behauptung**. $\sim_P$ ist eine Äquivalenzrelation auf M.

   Beweis. Wir zeigen als erstes die Reflexivität von $\sim_P$. Sei $a \in M$. Da P eine Partition von M ist, existiert ein $A \in P$ mit $a \in A$. Also gilt $a, a \in A$ und damit auch $a \sim_P a$. Das zeigt, dass $\sim_P$ reflexiv ist.

   Für die Symmetrie seien $a, b \in M$ und es gelte $a \sim_P b$. Dann existiert ein $A \in P$ mit $a \in A$ und $b \in A$. Damit gilt aber auch $b \sim_P a$.

   Schließlich beweisen wir die Transitivität. Seien $a, b, c \in M$ mit $a \sim_P b$ und $b \sim_P c$. Dann existieren $A, B \in P$ mit $a, b \in A$ und $b, c \in B$. Insbesondere ist $b \in A \cap B$. Da P eine Partition ist und A und B nichtleeren Durchschnitt haben, muss $A = B$ gelten. Damit gilt aber auch $c \in A$. Es folgt $a \sim_P c$. Damit ist $\sim_P$ transitiv. □

2. Wir wollen noch einmal die Relationen $\equiv \mod m$ auf den ganzen Zahlen vertiefen. Seien $a, b, c, d \in \mathbb{Z}$ und $m \in \mathbb{N}$. Angenommen, $a \equiv c \mod m$ und $b \equiv d \mod m$. In einer der Hausaufgaben wurde bereits gezeigt, dass in diesem Falle $a + b \equiv c + d \mod m$ gilt. Zeigen Sie nun

$$a \cdot b \equiv c \cdot d \mod m.$$

   Lösung. Seien a, b, c,d und m wie oben mit $a \equiv b \mod m$ und $c \equiv d \mod m$. **Behauptung.** $a \cdot b \equiv c \cdot d \mod m$

   Beweis. Nach Voraussetzung gilt $m|(c - a)$ und $m|(d - b)$. Wir wollen $m|(cd - ab)$ zeigen. Es gilt $cd - ab = cd - cb + cb - ab = c(d - b) + (c - a)b$. Der erste Summand der rechten Seite ist durch m teilbar, da $d - b$ durch m teilbar ist. Der zweite Summand der rechten Seite ist ebenfalls durch m teilbar, da $c - a$ durch m teilbar ist. Damit ist die Summe auf der rechten Seite der Gleichung durch m teilbar und damit auch $cd - ab$. □

3. Das Ergebnis aus Aufgabe 2 können wir wie folgt interpretieren: Für zwei ganze Zahlen a und b hängen die Äquivalenzklassen $[a + b]_m$ und $[a \cdot b]_m$ nur von den Äquivalenzklassen $[a]_m$ und $[b]_m$ ab, nicht aber von der Wahl der Repräsentanten a und b. Damit können wir auf dem Quotienten $\mathbb{Z}/\equiv \mod m$ die folgenden Operationen definieren: Für $a, b \in \mathbb{Z}$ seien $[a]_m + [b]_m = [a + b]_m$ und $[a]_m \cdot [b]_m = [ab]_m$.

Wenn die Kongruenz modulo m nicht so gutartig wäre, was könnte bei einer Definition der Form $[a] + [b] = [a + b]$ schief gehen? Dazu betrachten wir die Äquivalenzrelation $\sim$ auf $\mathbb{Z}$ mit den Äquivalenzklassen $A = \{\dots, -2, -1\}$, $B = \{0\}$ und $C = \{1, 2, \dots\}$. Auch hier wollen wir $[a]_\sim + [b]_\sim = [a + b]_\sim$ definieren. Was ist das Problem?

Lösung. Wir können die Äquivalenzklassen A und C durch verschiedene Repräsentanten hinschreiben. So gilt $A = [-1]_\sim = [-2]_\sim$ und $B = [2]_\sim = [1]_\sim$. Es ist aber $[(-1) + 2]_\sim = [1]_\sim = C$ und $[(-2) + 1]_\sim = [-1]_\sim$. Wir können also die Summe von A und C nicht definieren, indem wir $a \in A$ und $c \in C$ wählen und dann $A + C = [a + c]_\sim$ setzen, weil $[a + b]_\sim$ davon abhängt, welche Vertreter a und c wir für die Äquivalenzklassen A und C gewählt haben.

Bei der Relation $\equiv \mod m$ besteht dieses Problem nicht und wir können auf dem Quotientenraum $\mathbb{Z}/\equiv \mod m$ auf die naheliegende Weise $+$ und $\cdot$ definieren.

B: Hausaufgaben zum 11. November 2019

1. Sei $m \in \mathbb{Z}$. Den Quotientenraum $\mathbb{Z}/\equiv \mod m$ schreibt man meistens als $\mathbb{Z}_m$ oder als $\mathbb{Z}/m\mathbb{Z}$. Auf $\mathbb{Z}_m$ seien die Operationen $+$ und $\cdot$ definiert wie in der Präsenzaufgabe 2.

   Zeigen Sie, dass $(\mathbb{Z}_m, +, \cdot)$ die Assoziativ- und Kommutativgesetze sowie das Distributivgesetz erfüllt.

   Lösung. Einfachstes Nachrechnen. Beispiel: $[a]_m + [b]_m = [a + b]_m = [b + a]_m = [b]_m + [a]_m$.

2. (a) Gibt es in $(\mathbb{Z}_m, +, \cdot)$ neutrale Elemente bezüglich der Addition oder Multiplikation? Wenn ja, wie lauten diese?

   (b) Gibt es in $\mathbb{Z}_m$ Inverse bezüglich der Addition? Wie sehen diese aus?

   Lösung. (a) Für jedes $a \in \mathbb{Z}$ ist $[a]_m + [0]_m = [a + 0]_m = [a]_m$. Damit ist $[0]_m$ das neutrale Element bezüglich der Addition. Außerdem gilt $[1]_m \cdot [a]_m = [1 \cdot a]_m = [a]_m$. Damit ist $[1]_m$ das neutrale Element bezüglich der Multiplikation.

   (b) Für jedes $a \in \mathbb{Z}$ ist $[-a]_m + [a]_m = [-a + a]_m = [0]_m$. Jede Äquivalenzklasse $[a]_m$ hat also ein Inverses bezüglich $+$, nämlich $[-a]_m$.

3. Wir setzen $m = 8$. Welche $a \in \mathbb{Z}_m$ besitzen Inverse bezüglich der Multiplikation? Wie lauten diese?

   Lösung. Durch Ausprobieren sieht man, dass $[1]_8$, $[3]_8$, $[5]_8$ und $[7]_8$ Inverse bezüglich $\cdot$ haben. Diese vier Äquivalenzklassen sind nämlich alle zu sich selbst invers. Die anderen Elemente von $\mathbb{Z}_8$ sind nicht invertierbar.

4. Sei M eine nichtleere Menge. Wir definieren eine Operation $+$ auf $\mathrm{Pot}(M)$ mittels

   $$A + B = (A \setminus B) \cup (B \setminus A).$$

   Für $\cdot$ definieren wir einfach $A \cdot B = A \cap B$.

   Zeigen Sie, dass $(\mathrm{Pot}(M), +, \cdot)$ alle Körperaxiome bis auf die Existenz von Inversen bezüglich der Multiplikation erfüllt.

   Hinweis: Man erspart sich viele Rechnungen, wenn man benutzt, dass $A + B$ genau die Elemente von M enthält, die in genau einer der Mengen A und B vorkommen.

   Lösung. Wegen der Kommutativität von $\cup$ ist die Definition von $A + B$ symmetrisch in A und B. Damit ist auch $+$ kommutativ. Assoziativ- und Kommutativgesetz für $\cdot$ folgen sofort aus den Gesetzen für $\cap$. Wir zeigen das Assoziativgesetz für $+$.

   Seien $A, B, C \in \mathrm{Pot}(M)$. Für $m \in M$ ist $m \in A + B$ genau dann, wenn m in genau einer der Mengen A und B liegt. Damit ist $m \in (A + B) + C$ genau dann, wenn m in genau einer der Menge A und B liegt und nicht in C, oder wenn m in C liegt, aber nicht in genau einer der Mengen A und B. Damit ist $m \in (A + B) + C$, falls m in genau einer der Mengen A, B und C liegt. Völlig analog sieht man, dass m genau dann in $A + (B + C)$ liegt, wenn m in genau einer der Menge A, B und C liegt. Damit gilt $(A + B) + C = A + (B + C)$.

Das neutrale Element bezüglich der Addition ist die leere Menge $\emptyset$: Für alle $A \in \mathrm{Pot}(M)$ gilt

$$A + \emptyset = (A \setminus \emptyset) \cup (\emptyset \setminus A) = A.$$

Alle Elemente von $\mathrm{Pot}(M)$ sind bezüglich $+$ zu sich selbst invers. Für $A \in \mathrm{Pot}(M)$ gilt nämlich

$$A + A = (A \setminus A) \cup (A \setminus A) = \emptyset.$$

Das neutrale Element bezüglich der Multiplikation ist die Menge M selbst. Für alle $A \in \mathrm{Pot}(M)$ ist $A \cdot M = A \cap M = A$.

Wir zeigen noch das Distributivgesetz. Seien wieder $A, B, C \in \mathrm{Pot}(M)$. Für $m \in M$ gilt $m \in A \cdot (B + C)$ genau dann, wenn m ein Element von A ist und in genau einer der Mengen B und C vorkommt. Das ist aber genau dann der Fall, wenn m in genau einer der Mengen $A \cdot B$ und $A \cdot C$ vorkommt. Das zeigt

$$A \cdot (B + C) = A \cdot B + A \cdot C.$$

□

5. Sei $(\mathbb{K}, +, \cdot)$ ein Körper. Für jedes $x \in \mathbb{K}$ schreiben wir x^2 als Abkürzung für $x \cdot x$. Zeigen Sie, dass die bekannte binomische Formeln $(a + b)^2 = a^2 + 2ab + b^2$ gilt. Geben Sie in jedem Rechenschritt genau an, welches Körperaxiom Sie benutzen.

   Lösung. Leichtes Nachrechnen. Beachte: Dass man ausmultiplizieren kann, muss man erstmal zeigen.