

Formale Grundlagen

1. Übungsaufgaben

2008-04-01, Lösungen

1. Bekanntlich gibt es zu jeder Relation eine zugehörige inverse Relation, definiert durch

$$x \xrightarrow{R} y \iff y \xrightarrow{R^{-1}} x.$$

Warum ergibt sich dennoch keine Gruppe?

Lösung: Das neutrale Element ist die Diagonale, (i.e. die Gleichheitsrelation oder Identität). $(R; R^{-1})$ muß jedoch nicht die Diagonale sein, nämlich z.B. dann nicht, wenn es zu einem x überhaupt kein y mit $x \xrightarrow{R} y$ gibt, denn dann kann auch nicht $x \xrightarrow{R; R^{-1}} x$ gelten.

Aber auch wenn R zu groß ist (z.B. die Allrelation), ist $(R; R^{-1})$ nicht die Diagonale.

Tatsächlich kann man zeigen, daß die einzigen invertierbaren Relationen die bijektiven Funktionen sind (welche daher auch tatsächlich eine Gruppe bilden).

2. Zeigen Sie, daß in jeder Gruppe gilt: $a \cdot b = a \cdot c \implies b = c$.

Lösung: Es gelte $a \cdot b = a \cdot c$. Weil a in einer Gruppe liegt, können wir mit a^{-1} von links multiplizieren und erhalten $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$, und nach Anwendung des Assoziativgesetzes $(a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c$, somit gemäß der Definition für inverse Elemente $1 \cdot b = 1 \cdot c$, was mit der Definition für ein neutrales Element zu $b = c$ führt.

3. Betrachten Sie den Ring \mathbb{Z}_{15} (ganze Zahlen modulo 15). Warum ist dieser kein Körper? Welche Elemente darin sind invertierbar?

Lösung: Invertierbar sind jene Zahlen u , sodaß $\text{ggT}(u, 15) = 1$. Invertierbar sind somit nur 1, 2, 4, 7, 8, 11, 13, 14. Wir bemerken, daß diese eine multiplikative Gruppe bilden. Sie sind jedoch nicht gegenüber der Addition abgeschlossen.

4. Finden Sie $a, b \in \mathbb{Z}_{15}$ mit $a \neq 0 \neq b$, sodaß $a \cdot b = 0$. Kann es solche Elemente auch in einem Körper geben?

Lösung: $3 \cdot 5 \equiv 0$.

In einem Körper kann das nicht sein, weil in einem solchen folgt dann $(a \cdot b) \cdot b^{-1} \cdot a^{-1} = 0 \cdot b^{-1} \cdot a^{-1}$, was sich zu $1 = 0$ vereinfachen läßt.

5. Welche Elemente im Ring \mathbb{Z}_{17} sind invertierbar? Warum? Ist \mathbb{Z}_{17} ein Körper?

Lösung: Die Menge der invertierbaren Elemente erbt von der Gesamtmenge die Gruppenoperatoren mitsamt allen Rechengesetzen. Durch die Definition sind natürlich auch alle Elemente darin invertierbar. Das einzige, was tatsächlich noch nachgeprüft werden muß, ist, daß das Produkt zweier invertierbarer Elemente stets wieder invertierbar ist.

Diese Eigenschaft ist tatsächlich immer erfüllt, denn für invertierbare x, y gilt stets

$$(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = 1 = (x \cdot y) \cdot (y^{-1} \cdot x^{-1}),$$

weshalb auch $x \cdot y$ invertierbar ist, mit $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$. (Man beachte die Umkehrung der Reihenfolge, die in nichtkommutativen Monoiden wesentlich ist.)

6. Ist in den Körpern \mathbb{Z}_5 bzw. \mathbb{Z}_7 die Gleichung $x^2 = 2$ lösbar? Und wie sieht die Lösung gegebenenfalls aus?

Lösung: Eine einfache Tabellierung zeigt, daß es über \mathbb{Z}_5 keine Lösung gibt, über \mathbb{Z}_7 dagegen die beiden Lösungen $x = 3$ und $x = 4$. Man beachte, daß die zweite Lösung auch als $x = -3$ geschrieben werden kann.

7. Sei R ein beliebiger kommutativer Ring. Der Polynomring $R[x]$ besteht dann aus allen formalen Ausdrücken, welche aus Elementen von R und x gebildet werden können, wobei weiterhin alle Rechengesetze gelten sollten. Berechnen Sie Summe und Produkt der beiden Polynome $p := x^6 + x^3 - 1$ und $q := x^4 + x^3 + x$.

Lösung: Anwendung der bekannten Rechengesetze (vor allem des Distributivgesetzes) ergibt

$$\begin{aligned} p \cdot q &= (x^6 + x^3 - 1) \cdot (x^4 + x^3 + x) \\ &= (x^6 + x^3 - 1) \cdot x^4 + (x^6 + x^3 - 1) \cdot x^3 + (x^6 + x^3 - 1) \cdot x \\ &= (x^{10} + x^7 - 1 \cdot x^4) + (x^9 + x^6 - 1 \cdot x^3) + (x^7 + x^4 - 1 \cdot x) \\ &= x^{10} + x^9 + 2 \cdot x^7 + x^6 - x^3 - x. \end{aligned}$$

8. Verwenden Sie für die Berechnungen im vorigen Beispiel $R = \mathbb{Z}_2$ und $R = \mathbb{Z}_3$ statt $R = \mathbb{R}$.

Lösung: Über \mathbb{Z}_2 gelten $2 = 0$ und $+1 = -1$; somit vereinfacht sich das Ergebnis zu $x^{10} + x^9 + x^6 + x^3 + x$.

Über \mathbb{Z}_3 gilt $2 = -1$; somit vereinfacht sich das Ergebnis zu $x^{10} + x^9 - x^7 + x^6 - x^3 - x$.

9. Rechnen Sie nach, daß sich mit dem Relationenprodukt tatsächlich ein Monoid ergibt.

Lösung: Seien $R, S, T: X \rightarrow X \rightarrow \Omega$ Relationen auf einer Menge X . Wir müssen zeigen, daß $(R; S); T = R; (S; T)$. Dies ist per definitionem genau dann erfüllt, wenn

$$\bigwedge_{x: X} \bigwedge_{t: X} (x \xrightarrow{(R;S);T} t \iff x \xrightarrow{R;(S;T)} t)$$

Seien also $x, t: X$ beliebig gewählt. Und sei $x \xrightarrow{(R;S);T} t$. Dann gibt es ein $z: X$, sodaß $x \xrightarrow{(R;S)} z$ und $z \xrightarrow{T} t$; und weiters ein $y: X$, sodaß $x \xrightarrow{R} y$ und $y \xrightarrow{S} z$. Damit gilt aber auch $y \xrightarrow{(S;T)} t$ und somit auch $x \xrightarrow{R;(S;T)} t$, womit eine Richtung der Äquivalenz gezeigt ist. Die andere Richtung funktioniert analog.