Hausaufgaben zu Algebraische Strukturen / Linearen Algebra 2

Prof. Dr. P. Pickl
Kajetan Söhnen

Lösungsvorschlag zu Tutoriumsblatt 3a

Aufgabe 1: Wir betrachten die Gruppe der reellen invertirbaren 2×2 Matrizen.

(a) Geben Sie die Menge aller Matrizen an, die mit $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ kommutieren.

(b) Bestimmen Sie analog, die Menge der Matrizen die mit $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ kommutieren und schließen Sie auf die Menge der Matrizen die mit allen 2×2 Matrizen kommutieren.

Lösungsvorschlag. zu a) Sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ eine Matrix die mit $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ kommutiert. Dann gilt

$$\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix}.$$

Es folgt $c = 0$ und $a = d$. Durch unsere Rechnung wird auch klar, dass Matrizen in dieser Form tatsächlich mit $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ kommutieren, was (a) abschließt. Die Menge der gesuchten Matrizen, ist also

$$\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} | a, b \in \mathbb{R} \right\}.$$

zu b) Analog zu (a) zeigt man, dass die Menge der Matrizen die mit $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ kommutieren, durch

$$\left\{ \begin{pmatrix} a & 0 \\ c & a \end{pmatrix} | a, b \in \mathbb{R} \right\}$$

gegeben ist. Damit eine Matrix also sowohl mit $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ als auch mit $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ kommutiert, muss die Matrix die Form

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

haben. In dieser Form sieht man leicht, dass solche Matrizen tatsächlich mit allen Matrizen kommutieren.

$\square$

Aufgabe 2: (a) Zeige, dass die Menge der reellen 2×2 Diagonalmatrizen D, also Matrizen der Form $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ mit $a, b \neq 0$, eine Untergruppe der invertierbaren 2×2 Matrizen bildet.

(b) Zeigen Sie, dass es sich bei der Abbildung $f : D \to \mathbb{R}\backslash\{0\}$ gegeben durch $f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \frac{a}{d}$ um einen Gruppenhomomorphismus von $(D, \cdot)$ nach $(\mathbb{R} \setminus \{0\}, \cdot)$ handelt. Hier bezeichnet $\cdot$ die Matrixmultiplikation bzw. das Produkt reeller Zahlen.

($\star$) (c) Ist die Abbildung injektiv beziehungsweise surjektiv?

Lösungsvorschlag. zu a) Die Menge ist nicht leer, den sie enthält die Einheitsmatrix. Es gilt

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix},$$

die Menge ist also abgeschlossen bezüglich Multiplikation. Das Inverse der Matrix $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ ist durch $\begin{pmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{b} \end{pmatrix}$ gegeben, also sind auch die Inversen von Diagonalmatrizen in diagonal Form. Damit handelt es sich um eine Untergruppe

zu b) Es gilt $f\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = \frac{1}{1} = 1$, das neutrale Element der Matrixmultiplikation wird also auf das neutrale Element der Multiplikation in $\mathbb{R}$ abgebildet. Weiter gilt

$$f\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}\right) = \frac{ac}{bd} = \frac{a}{b} \cdot \frac{c}{d} = f\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right) \cdot f\left(\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}\right).$$

Damit ist die Abbildung auch verträglich mit den Gruppenoperationen, also ein Gruppenhomomorphismus.

zu c) Die Abbildung ist nicht Injektiv, da zum Beispiel $f\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right) = \frac{a}{a} = 1$ für alle $a \in \mathbb{R} \setminus \{0\}$. Die Menge ist surjektiv, da für alle $x \in \mathbb{R} \setminus \{0\}$ gilt, dass $f\left(\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}\right) = \frac{x}{1} = x$.

$\square$

Aufgabe 3: (a) Geben Sie einen Gruppenhomomorphismus von $f : (\mathbb{R}, +) \to (\mathbb{R} \setminus \{0\}, \cdot)$ an.

Lösungsvorschlag. Das typische Beispiel für so eine Abbildung ist die exp Funktion, also e^x. Es gilt $e^{x+y} = e^x \cdot e^y$, also ist es ein Gruppenhomomorphismus. $\square$

($\star$) (b) Geben Sie einen Gruppenisomorphismus $f : (\mathbb{R}, +) \to (\mathbb{R}, +)$ an, der eingeschränkt auf $(\mathbb{R} \setminus \{0\}, \cdot) \to (\mathbb{R} \setminus \{0\}, \cdot)$ kein Gruppenhomomorphismus ist.

Lösungsvorschlag. Eine mögliche Abbildung ist $f(x) = -x$. Es gilt $f(x + y) = -(x + y) = -x + (-y) = f(x) + f(y)$. Damit handelt es sich um ein Gruppenhomomorphismus bezüglich Addition. Gleichzeitig gilt $f(1) = -1$, das neutrale Element bezüglich Multiplikation wird also nicht "respektiert". Damit kann es sich nicht um einen Gruppenhomomorphismus bezüglich Multiplikation handeln. $\square$

Aufgabe 4: Sei G eine endliche Gruppe. Für $g \in G$ schreiben wir $o(g) := | < g > |$ für die Ordnung von g.

(a) Zeigen Sie, dass für jedes $g \in G$ ein $n \in \mathbb{N}$ existiert, sodass $g^n = e$, wobei e das neutrale Element ist.

($\star$)(b) Zeigen Sie, dass $o(g)$ die kleinste natürliche Zahl mit $g^{o(g)} = e$ ist.

Lösungsvorschlag.

zu a) Wir zeigen zunächst, dass es $n \neq m \in \mathbb{N}$ gibt, sodass $g^n = g^m$. Wäre das nicht so, wären g^k für alle k paarweise verschieden und wir hätten unendlich viele Elemente in G gefunden. Aber G war ja als endlich vorausgesetzt.

Damit gilt also $g^n = g^m$ wobei oBdA $n < m$ ist. In eine Gruppe dürfen wir kürzen und erhalten $e = g^0 = g^{m-n}$. Damit haben wir die gesuchte natürliche Zahl gefunden.

zu b) Sei $m = \min\{k \in \mathbb{N} \mid g^k = e\}$. Wir wollen zeigen, dass $m = o(g)$. Die Idee ist einfach, falls $m > o(g)$ hätte $< g >$ zu viele Elemente, falls $m < o(g)$ hätte $< g >$ zu wenig Elemente. Bei den sauberen Beweisen muss man allerdings etwas Fußarbeit leisten.

Angenommen $m > o(g)$. Dann enhält die Untergruppe $< g >$ die Elemente $g, g^2, \ldots, g^m$. Wenn all diese Elemente verschieden sind, haben wir $m > o(g)$ Elemente in $< g >$ gefunden, was im Widerspruch zur Definition von $o(g)$ steht. Wären zwei Elemente $g^l = g^k$ für $1 \leq l < k \leq m$ gleich, können wir wieder den Trick aus (a) verwenden und sehen dass $g^{k-l} = e$. Da $k - l < m$ steht das im Widerspruch zur Defintion von m als minimales Element mit dieser Eigenschaft.

Angenommen $m < o(g)$. Dann gibt es für alle $k \in \mathbb{Z}$ ein $0 \leq r \leq m - 1$ sodass $g^k = g^r$. Das folgt aus der Division mit Rest $k = qm + r$. Denn damit gilt

$$g^k = g^{qm+r} = (g^m)^q \circ g^r = e^q \circ g^r = g^r.$$

Damit gibt es in $< g >$ haben höchstens $m < o(g)$ Elemente, nämlich $g^0, g^1, g^2, \ldots, g^{m-1}$. Das steht wieder im Widerspruch zur Definition von $o(g)$.

Damit bleibt nur die Möglichkeit $m = o(g)$, was die Aufgabe beweist. $\square$