Lösungen 2

1. Es ei $p > 2$ eine Primzahl. Zeigen Sie, dass in $\mathbb{F}_p$ folgendes gilt:

$$1 \cdot 2 \cdot \cdots \cdot (p-1) = p - 1.$$

Solution: Um diese Aufgabe zu lösen betrachten wir zunächst die quadratische Gleichung

$$x^2 = 1 \tag{1}$$

in $\mathbb{F}_p$. Diese Gleichung hat offensichtlich die Lösung $y = 1$ und damit auch $-y = -1 = p - 1$. Es kann ausserdem keine Weiteren Lösungen geben, da wir die Gleichung umschreiben können als

$$0 = x^2 - 1 = (x-1)(x+1),$$

also in ein Produkt von zwei linearen Faktoren. Mehr als zwei Nullstellen hat dieses Polynom also sicherlich nicht.
Multiplizieren wir (1) mit dem multiplikativen Inversen von x (unter Annhame, dass x nicht null ist), erhalten wir, dass die Gleichung

$$x = x^{-1}$$

also nur 2 Lösungen in $\mathbb{F}_p$ besitzt. Mit anderen Worten, das multiplikative Inverse einer Zahl $x \in \mathbb{F}_p$, die nicht 1 oder -1 ist, ist verschieden von x.
Nun können wir das Produkt

$$1 \cdot 2 \cdot \cdots \cdot (p-1)$$

betrachten. Da in diesem Produkt für alle Zahlen $x \in \{2, \ldots, p-2\}$ auch das multiplikative inverse von x vorkommt, können wir die Faktoren passend vertauschen und erhalten das gewünschte Resultat

$$1 \cdot (2 \cdot 2^{-1}) \cdot (3 \cdot 3^{-1}) \cdot \cdots \cdot (p-1) = 1 \cdot (p-1) = p - 1. \tag{2}$$

Wichtig ist hier zu betonen, dass nur $\frac{p-3}{2}$ Produkte der Form $(x \cdot x^{-1})$ in dem obigen Produkt vorkommen. Denn insgesamt gibt es $p-3$ Zahlen zwischen 2 und $p-2$, jedoch stecken in jedem solchen Produkt $(x \cdot x^{-1})$ ja schon 2 dieser Elemente. Im Fall $p = 5$ ist zum Beispiel 3 das multiplikaitve inverse von 2. Trotzdem sind im Produkt (2) beide Faktoren $(2 \cdot 2^{-1})$ und $(3 \cdot 3^{-1})$ vorhanden - das ist formal nicht ganz korrekt, sondern soll nur die Idee des umschreibens der Faktoren im Produkt

$$1 \cdot 2 \cdot \cdots \cdot (p-1)$$

symbolisieren.

2. Sei K ein Körper. Zeigen Sie, dass die multiplikative Identität eindeutig ist, das heisst wenn 1 und $1'$ beide neutrale Elemente bezüglich der Multiplikation sind, dann $1 = 1'$. Leiten Sie daraus ab, dass jedes $0 \neq x \in K$ genau ein multiplikatives inverses Element hat.

   Solution: Seien $1, 1' \in K$ neutrale Elemnte bezüglich der Multiplikation. Dann ist $1' = 1 \cdot 1'$, weil 1 ein neutrales Element ist. Aus der Kommutativität der Multiplikation folgt $1 \cdot 1' = 1' \cdot 1$. Schliesslich ist auch $1'$ ein neutrales Element, also ist $1' \cdot 1 = 1$. Sodann erhalten wir

$$1' = 1 \cdot 1' = 1' \cdot 1 = 1,$$

   also ist die multiplikative Identität eindeutig. Sei nun $0 \neq x \in K$ uns seien y, z multiplikative Inverse von x. Dann ist $x \cdot y = 1$ und $x \cdot z = 1$. Multiplikation der ersten Gleichung mit z liefert $z \cdot x \cdot y = z$. Da Multiplikation kommutativ ist, erhalten wir $z \cdot x \cdot y = (x \cdot z) \cdot y = 1 \cdot y = y$. Also ist $y = z \cdot x \cdot y = z$ und somit ist das inverse Element ebenfalls eindeutig.

3. Es seien K ein Körper und $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(K)$. Finden Sie ein Kriterium, wann A invertierbar ist, und geben Sie eine Formel für A^{-1}.

   Solution: Wir nehmen an, dass A invertierbar ist und schreibe $A^{-1} = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$. Dann ist

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

   Wir erhalten also die Gleichung $cx + dz = 0$. Wir nehmen zunächst an, dass d nicht 0 ist. Dann folgt $z = -cx/d$. Dies setzen wir in die $ax + bz = 1$ ein und erhalten $ax + b(-cx/d) = 1$. Multiplikation beider Seiten mit d liefert $dx(ad - bc) = d$. Da $d \neq 0$ ist, erhalten wir, dass $(ad - bc) \neq 0$.

   Wir kehren zur Gleichung $cx + dz = 0$ zurück und nehmen jetzt an, dass $d = 0$ ist. Daraus folgt nun, dass $x = 0$ oder $c = 0$. Aus der Gleichung $cy + 0 \cdot w = cy + dw = 1$ folgt ausserdem, dass $cy = 1$ ist, somit ist $c \neq 0$ und deswegen $x = 0$. Aus der Gleichung $ax + bz = 1$ folgt nun $bz = 1$, also ist $b \neq 0$. Zusammen erhalten wir, dass $ad - bc = a \cdot 0 - bc = bc \neq 0$.

   In beiden Fällen ist also $(ad - bc) \neq 0$ eine notwendige Bedingung, damit die Matrix A eine Inverse besitzt. In diesem Fall gilt

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

   also ist dann

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

4. Es seien $A, B \in M_{n\times n}(\mathbb{R})$. Entscheiden Sie fuer jede der folgenden Aussagen, ob sie wahr oder falsch ist, und geben Sie einen Beweis oder Gegenbeispiel.

   (a) $A^2 - B^2 = (A + B)(A - B)$;

   (b) if $AB = 0$, dann gilt $A = 0$ oder $B = 0$.

   (c) wenn $AB = 0$, dann koennen A und B nicht beide invertierbar sein.

   (d) wenn A und B invertierbar sind, dann gilt das Gleiche fuer $A - B$.

   Hinweis: Gegenbeispiele lassen sich oft schon für $n = 2$ finden.

   Solution:

   (a) Diese Aussage ist im Allgemeinen falsch. Beachten Sie, dass

   $$(A + B)(A - B) = A^2 - AB + BA - B^2$$

   gilt. Dementsprechend ist die Gleichung nur dann erfüllt, falls

   $$AB = BA$$

   für die Matrizen A und B gilt. Also genau dann, wenn A und B kommutieren. Ein Gegenbeispiel wäre $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ und $B = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Wir sehen

   $$A^2 - B^2 = \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}$$

   und

   $$(A + B)(A - B) = \begin{pmatrix} -1 & 2 \\ -2 & 1 \end{pmatrix}.$$

   (b) Auch diese Aussage ist nicht wahr. Wir beachten, dass zum Beispiel für $A = B = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ gilt, dass

   $$AB = A^2 = 0.$$

   Insbesondere gibt es also Matrizen, die nicht die Nullmatrix sind, deren Quadrat 0 ist - im Gegensatz zu den rellen Zahlen, in denen jedes Quadrat einer Zahl ungleich 0 positiv ist.

   (c) Diese Aussage ist wahr. Angenommen A sei invertierbar. Dann gibt es eine Matrix A^{-1}, sodass

   $$AA^{-1} = A^{-1}A = \mathbf{1}_n$$

   gilt. Wir erhalten

   $$B = \mathbf{1}_n B = A^{-1}AB = A^{-1} \cdot 0 = 0.$$

   Die Nullmatrix ist aber sicherlich nicht invertierbar, daher folgt

   $$A \text{ invertierbar} \Rightarrow B \text{ nicht invertierbar.}$$

   Eine ähnliche Argumentation liefert

   $$B \text{ invertierbar} \Rightarrow A \text{ nicht invertierbar.}$$

(d) Nein, diese Aussage ist auch falsch. Angenommen A sei eine invertierbare Matrix. Dann ist für $A = B$ die Differenz

$$A - B = 0$$

sicher nicht invertierbar. Das liefert also schon eine unendliche Anzahl an Gegenbeispielen.
Für ein konkretes (und zudem anderes) Beispiel betrachten wir die Matrizen $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ und $B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Die Differenz ist

$$A - B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Nun folgt aus Teil (b) und (c), dass $A - B$ nicht invertierbar sein kann. (Warum?)

5. Finden Sie für jedes $n \in \mathbb{N}$ eine Matrix $A \in M_{n\times n}(\mathbb{R})$ so dass A^n die Nullmatrix ist und A^{n-1} nicht die Nullmatrix ist.

Solution: Die Matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

hat die gewünschte Eigenschaft.