Übung zum Lehrerweiterbildungskurs Mathematik
'Lineare Algebra/Analytische Geometrie I'

Aufgabe B2 (Körper, modulares Rechnen)

(i) Stellen Sie die Verknüpfungstafeln von $\mathbb{Z}_2, \mathbb{Z}_3$ und $\mathbb{Z}_4$ auf!
Erinnerung:
$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ ist ein Ring mit den Elementen $\{0, 1, 2, \dots, m-1\}$ und Addition und Multiplikation modulo m.

(ii) Welche der drei Ringe $\mathbb{Z}_2, \mathbb{Z}_3$ und $\mathbb{Z}_4$ sind Körper?
Hinweis: Die Ringeigenschaften der drei Ringe dürfen Sie hier ohne Beweis voraussetzen!

Lösungsskizze

(i) (a) $\mathbb{Z}_2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

(b) $\mathbb{Z}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

(c) $\mathbb{Z}_4$:

$+$	0	1	2	3
0	0	1	3	2
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(ii) $\mathbb{Z}_2$ und $\mathbb{Z}_3$ sind Körper: Sie sind Ringe mit 1, und jedes Element ungleich 0 besitzt eine multiplikative Inverse; außerdem gilt

$$a \cdot b = 0 \Longrightarrow a = 0 \vee b = 0,$$

also die Abgeschlossenheit von $\mathbb{Z}_i^*$ (für $i = 1$ und $i = 2$) bei Multiplikation.
$\mathbb{Z}_4$ ist kein Köper, denn das Element 2 besitzt keine Inverse (und es gibt "Nullteiler": $2 \cdot 2 = 0$, obwohl $2 \neq 0$).