Prof. Dr. Ellen Henke
Dr. Julian Kaspczyk
Edoardo Salati

Lösungsblatt 6

LA/LAAG
4. Dezember 2021

Hausaufgaben zur Vorbereitung

Die folgende Aufgabe dient Ihnen zur Vorbereitung der sechsten Übung. Der späteste Abgabetermin ist der 24.11.2021 um 23.59 Uhr. Bearbeiten Sie die Aufgabe aber möglichst vor Ihrem sechsten Übungstermin!

Aufgabe 1 (5 Punkte)

Bearbeiten Sie die Aufgaben, die Sie auf der Opal-Kursseite im Ordner *Hausaufgaben* unter der Überschrift *Vorbereitungsaufgaben für Übung 6* finden.

Lösung der ersten Vorbereitungsaufgabe

In der ersten Vorbereitungsaufgabe sollten die Additions- und die Multiplikationstafel von $\mathbb{Z}/7$ angegeben werden. Hierbei sollte jedes Element von $\mathbb{Z}/7$ in der Form $[k]$ mit $k \in \{0,1,2,3,4,5,6\}$ angegeben werden. Außerdem waren das additive und das multiplikative Inverse von $[5]$ in $\mathbb{Z}/7$ anzugeben, und zwar ebenfalls in der Form $[k]$ mit $k \in \{0,1,2,3,4,5,6\}$.
Additionstafel von $\mathbb{Z}/7$:

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[6]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[6]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[6]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[6]$	$[6]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$

Multiplikationstafel von $\mathbb{Z}/7$:

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[2]$	$[0]$	$[2]$	$[4]$	$[6]$	$[1]$	$[3]$	$[5]$
$[3]$	$[0]$	$[3]$	$[6]$	$[2]$	$[5]$	$[1]$	$[4]$
$[4]$	$[0]$	$[4]$	$[1]$	$[5]$	$[2]$	$[6]$	$[3]$
$[5]$	$[0]$	$[5]$	$[3]$	$[1]$	$[6]$	$[4]$	$[2]$
$[6]$	$[0]$	$[6]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

Lösungsblatt 6

Das additive Inverse von [5] in $\mathbb{Z}/7$ ist [2], denn $[5] + [2] = [2] + [5] = [7] = [0]$.

Das multiplikative Inverse von [5] in $\mathbb{Z}/7$ ist [3], denn wie wir aus der obigen Multiplikationstafel ablesen, gilt $[5] \cdot [3] = [3] \cdot [5] = [1]$.

Lösung der zweiten Vorbereitungsaufgabe

In der zweiten Vorbereitungsaufgabe sollte für zwei Restklassenringe die Anzahl ihrer invertierbaren Elemente angegeben werden.

Der erste Restklassenring war einer der folgenden (welchen Sie bei der Bearbeitung der Aufgabe zu sehen bekamen, war vom Zufall abhängig):

$$\mathbb{Z}/11, \mathbb{Z}/13, \mathbb{Z}/17, \mathbb{Z}/19, \mathbb{Z}/23, \mathbb{Z}/29, \mathbb{Z}/31, \mathbb{Z}/37, \mathbb{Z}/39, \mathbb{Z}/41, \mathbb{Z}/47, \mathbb{Z}/51.$$

Diese Restklassenringe sind alle von der Form $\mathbb{Z}/p$ für eine Primzahl p. Nach Lemma 2.34 ist jeder solche Restklassenring ein Körper. Per Definition sind in einem Körper alle vom Nullelement verschiedenen Elemente invertierbar. Das Nullelement selbst ist niemals invertierbar, denn wenn wir das Nullelement mit einem Körperelement multiplizieren, erhalten wir Lemma 2.19 zufolge immer das Nullelement, insbesondere also niemals das Einselement, womit das Nullelement kein multiplikatives Inverses haben kann. Die invertierbaren Elemente eines Körpers sind also genau die Elemente des Körpers, die vom Nullelement verschieden sind. Der Körper $\mathbb{Z}/p$ hat nach Lemma 2.29 genau p Elemente. Damit hat $\mathbb{Z}/p$ genau $p-1$ invertierbare Elemente.

Der zweite in der Aufgabe gegebene Restklassenring war einer der folgenden (welchen Sie bei der Bearbeitung der Aufgabe zu sehen bekamen, war vom Zufall abhängig):

$$\mathbb{Z}/4, \mathbb{Z}/8, \mathbb{Z}/16, \mathbb{Z}/32, \mathbb{Z}/64.$$

Jeder dieser Restklassenringe hat die Form $\mathbb{Z}/2^n$ für eine natürliche Zahl $n \geq 2$. Nach Lemma 2.29 hat der Ring $\mathbb{Z}/2^n$ genau die Elemente $[0], [1], [2], \ldots, [2^n-1]$. Sei $k \in \{0, 1, 2, \ldots, 2^n-1\}$. Nach Lemma 2.35 ist $[k]$ genau dann invertierbar in $\mathbb{Z}/2^n$, wenn $\mathrm{ggT}(2^n, k) = 1$ gilt. Falls k ungerade ist, ist die Bedingung $\mathrm{ggT}(2^n, k) = 1$ erfüllt. Falls k gerade ist, haben 2^n und k den gemeinsamen Teiler 2, womit $\mathrm{ggT}(2^n, k) \geq 2$ gilt, sodass die Bedingung $\mathrm{ggT}(2^n, k) = 1$ nicht erfüllt ist. Die Bedingung $\mathrm{ggT}(2^n, k) = 1$ ist folglich genau dann erfüllt, wenn k ungerade ist. Die invertierbaren Elemente von $\mathbb{Z}/2^n\mathbb{Z}$ sind damit genau die Elemente $[k]$, wobei $k \in \{0, 1, 2, \ldots, 2^n - 1\}$ ungerade ist. Da es genau $\frac{1}{2} \cdot 2^n = 2^{n-1}$ ungerade Elemente in $\{0, 1, 2, \ldots, 2^n - 1\}$ gibt, folgt, dass der Ring $\mathbb{Z}/2^n$ genau 2^{n-1} invertierbare Elemente hat.

Präsenzaufgaben

Die folgenden Aufgaben werden in den Übungen gemeinsam besprochen. Um Ihren Lernerfolg zu steigern, sollten Sie sich aber bereits im Vorfeld der Übungen mit den Aufgaben auseinandergesetzt haben.

Prof. Dr. Ellen Henke
Dr. Julian Kaspczyk
Edoardo Salati

Lösungsblatt 6

Aufgabe 2

Stellen Sie die Additions- und Multiplikationstafel für $\mathbb{Z}/6$ auf. Geben Sie alle invertierbaren Elemente von $\mathbb{Z}/6$ und deren Inverse an.

Lösung

Additionstafel von $\mathbb{Z}/6$:

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

Multiplikationstafel von $\mathbb{Z}/6$:

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[2]$	$[0]$	$[2]$	$[4]$	$[0]$	$[2]$	$[4]$
$[3]$	$[0]$	$[3]$	$[0]$	$[3]$	$[0]$	$[3]$
$[4]$	$[0]$	$[4]$	$[2]$	$[0]$	$[4]$	$[2]$
$[5]$	$[0]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

Die invertierbaren Elemente von $\mathbb{Z}/6$ sind genau die Elemente von $\mathbb{Z}/6$, so dass in der zugehörigen Zeile der Multiplikationstafel das Element $[1]$ auftaucht. Die invertierbaren Elemente von $\mathbb{Z}/6$ sind also $[1]$ und $[5]$. Dies lässt sich auch ohne einen Blick auf die Multiplikationstafel mithilfe von Lemma 2.35 begründen.

Es gilt $[1]^{-1} = [1]$, denn $[1] \cdot [1] = [1]$. Außerdem gilt $[5]^{-1} = [5]$, denn nach der Multiplikationstafel gilt $[5] \cdot [5] = [1]$.

Aufgabe 3

Geben Sie die folgenden Brüche in $\mathbb{Z}/5$ in der Form $[i]$ mit $i \in \{0, 1, 2, 3, 4\}$ an:

$$\frac{[1]}{[2]}, \quad \frac{[2]}{[3]}, \quad \frac{[3]}{[4]}, \quad \frac{[3] + [4]}{[2]}.$$

Lösung

Es gilt $[1]^{-1} = [1], [2]^{-1} = [3], [3]^{-1} = [2], [4]^{-1} = [4]$. Somit $\frac{[1]}{[2]} = [1]\cdot[2]^{-1} = [1]\cdot[3] = [3]$, $\frac{[2]}{[3]} = [2]\cdot[3]^{-1} = [2]\cdot[2] = [4]$, $\frac{[3]}{[4]} = [3]\cdot[4]^{-1} = [3]\cdot[4] = [12] = [2]$, $\frac{[3]+[4]}{[2]} = \frac{[7]}{[2]} = \frac{[2]}{[2]} = [2]\cdot[2]^{-1} = [1]$.

Aufgabe 4

Beweisen Sie Lemma 2.25 (b), (c), (d): Sei K ein Körper und seien $a, b, c, d \in K$ mit $b \neq 0 \neq d$. Dann gilt:

(1) $\frac{a}{b} - \frac{c}{d} = \frac{ad-cb}{bd}$ und $\frac{a}{b} - \frac{c}{b} = \frac{a-c}{b}$.

(2) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

(3) Falls $c \neq 0_K$, dann gilt $\frac{c}{d} \neq 0_K$ und

$$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}.$$

Lösung

Nach Lemma 2.25 (a) gilt folgendes:

(i) $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$,

(ii) $\frac{a}{b} + \frac{c}{b} = \frac{a+c}{b}$.

Nach (ii) gilt $\frac{a}{b} + \frac{-a}{b} = \frac{a+(-a)}{b} = \frac{0}{b} = 0 \cdot b^{-1} = 0$. Daher gilt $-\frac{a}{b} = \frac{-a}{b}$. Ebenso erhalten wir $-\frac{c}{b} = \frac{-c}{b}$ und $-\frac{c}{d} = \frac{-c}{d}$. Unter Nutzung der Definition $x - y := x + (-y)$ für alle $x, y \in K$ erhalten wir

$$\frac{a}{b} - \frac{c}{b} = \frac{a}{b} + (-\frac{c}{b}) = \frac{a}{b} + \frac{-c}{b} = \frac{a+(-c)}{b} = \frac{a-c}{b}.$$

Die dritte Gleichheit gilt dabei nach (ii). Damit ist der zweite Teil von (1) gezeigt.

Es gilt

$$\frac{a}{b} - \frac{c}{d} = \frac{a}{b} + (-\frac{c}{d}) = \frac{a}{b} + \frac{-c}{d} = \frac{ad+(-c)b}{bd} = \frac{ad+(-cb)}{bd} = \frac{ad-cb}{bd},$$

wobei die dritte Gleichheit nach (i) und die vierte Gleichheit nach Lemma 2.22 gilt. Der erste Teil von (1) ist damit auch gezeigt.

Um (2) und (3) zu beweisen, machen wir eine kleine Vorüberlegung:

Vorüberlegung: Für $x, y \in K \setminus \{0_K\}$ gilt $(xy)^{-1} = y^{-1}x^{-1}$.

Beweis: Wegen der Assoziativität und Kommutativität der Multiplikation in K gilt

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x1_Kx^{-1} = xx^{-1} = 1_K$$

und

$$(y^{-1}x^{-1})(xy) = (xy)(y^{-1}x^{-1}) \overset{s.o.}{=} 1_K.$$

Also $(xy)^{-1} = y^{-1}x^{-1}$. □

Um (2) zu erhalten, berechnen wir

$$\frac{a}{b} \cdot \frac{c}{d} = (ab^{-1})(cd^{-1}) = (ac)(d^{-1}b^{-1}) = (ac)(bd)^{-1} = \frac{ac}{bd},$$

wobei die zweite Gleichheit von der Assoziativität und Kommutativität der Multiplikation in K folgt und die dritte Gleichheit aus der obigen Vorüberlegung folgt.

Sei nun angenommen, dass $c \neq 0_K$. Nach Korollar 2.20 gilt $d^{-1} \neq 0_K$. Nun impliziert Lemma 2.23, dass $\frac{c}{d} = cd^{-1} \neq 0_K$. Insbesondere ist der Ausdruck $\frac{\frac{a}{b}}{\frac{c}{d}}$ definiert. Wir berechnen nun

$$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a}{b}\left(\frac{c}{d}\right)^{-1} = (ab^{-1})(cd^{-1})^{-1} = (ab^{-1})(dc^{-1}) = (ad)(c^{-1}b^{-1}) = (ad)(bc)^{-1} = \frac{ad}{bc},$$

wobei die dritte und die fünfte Gleichheit nach der obigen Vorüberlegung gelten und die dritte Gleichheit ebenfalls benutzt, dass d das Inverse von d^{-1} ist. Für die vierte Gleichheit haben wir des Weiteren die Kommutativität und Assoziativität der Multiplikation in K benutzt. Damit ist (3) bewiesen.

Aufgabe 5

(a) Beweisen Sie das Lemma von Bézout: Seien $a, b \in \mathbb{Z}$. Dann existieren $s, t \in \mathbb{Z}$, so dass $sa + tb = \mathrm{ggT}(a, b)$.

(b) Sei $n \geq 2$ eine natürliche Zahl und sei $k \in \mathbb{Z}$, so dass $[k]$ invertierbar in $\mathbb{Z}/n$ ist. Diskutieren Sie, wie das Lemma Bézout helfen könnte, das multiplikative Inverse von $[k]$ in $\mathbb{Z}/n$ zu finden.

Lösung

(a) Wir beweisen das Lemma von Bézout zunächst für den Spezialfall, dass $a, b \in \mathbb{N}_0$ gilt. Um das Lemma von Bézout für diesen Spezialfall zu beweisen, nutzen wir das Prinzip der vollständigen Induktion, genauer das Prinzip der *Abschnittsinduktion*, so wie es auf S. 14 im Vorlesungsskript beschrieben ist. Für jedes $n \in \mathbb{N}_0$ sei $P(n)$ die folgende Aussage:

Für jede Wahl von Elementen $a, b \in \mathbb{N}_0$ mit $a + b = n$ existieren $s, t \in \mathbb{Z}$, so dass

$sa + tb = \mathrm{ggT}(a, b)$.

Wir zeigen, dass $P(n)$ für jedes $n \in \mathbb{N}_0$ richtig ist (damit ist das Lemma Bézout für den Spezialfall $a, b \in \mathbb{N}_0$ bewiesen, denn für alle $a, b \in \mathbb{N}_0$ gibt es ein $n \in \mathbb{N}_0$ mit $a + b = n$).

1. Induktionsanfang: Wir beweisen zunächst $P(0)$. In diesem Falle gilt $a+b = 0$. Wegen $a, b \in \mathbb{N}_0$ muss damit $a = b = 0$ gelten. Nun gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(0, 0) = 0 = 0 \cdot a + 0 \cdot b$. Die Aussage $P(0)$ ist also erfüllt mit $s = 0 = t$.

2. Induktionsschritt: Sei nun eine natürliche Zahl $n \in \mathbb{N}$ gegeben, so dass $P(n')$ für jedes $n' \in \mathbb{N}_0$ mit $n' < n$ wahr ist (Induktionsvoraussetzung). Wir wollen folgern, dass auch $P(n)$ wahr ist. Seien dazu $a, b \in \mathbb{N}_0$ mit $a + b = n$. Wir müssen zeigen, dass $s, t \in \mathbb{Z}$ existieren mit $sa + tb = \mathrm{ggT}(a, b)$. Dabei dürfen wir verwenden, dass $P(n')$ für alle $0 \leq n' < n$ wahr ist, d. h. für jede Wahl von Elementen $a_0, b_0 \in \mathbb{N}_0$ mit $0 \leq a_0 + b_0 < n$ existieren $s_0, t_0 \in \mathbb{Z}$ mit $\mathrm{ggT}(a_0, b_0) = s_0 a_0 + t_0 b_0$.

Wir können o. B. d. A. (ohne Beschränkung der Allgemeinheit) annehmen, dass $b \leq a$ (ist dies nicht der Fall, können wir einfach die Rollen von a und b vertauschen). Ist $b = 0$, so gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(a, 0) = a = 1 \cdot a + 1 \cdot 0 = 1 \cdot a + 1 \cdot b$, sodass die gewünschte Aussage mit $s = 1 = t$ erfüllt ist. Nehmen wir jetzt an, dass $b \geq 1$, also dass $b \in \mathbb{N}$ gilt. Nach Lemma 1.29 existieren ein $q \in \mathbb{Z}$ und ein $r \in \{0, 1, \ldots, b-1\}$ mit $a = qb + r$. Nun gilt $r < b \leq a$ und damit $r + b < a + b$. Nach Induktionsvoraussetzung existieren also $s_0, t_0 \in \mathbb{Z}$ mit $\mathrm{ggT}(r, b) = s_0 r + t_0 b$. Es lässt sich unschwer einsehen (und wird in Aufgabe 7 bewiesen), dass $\mathrm{ggT}(r, b) = \mathrm{ggT}(a, b)$. Folglich gilt $\mathrm{ggT}(a, b) = s_0 r + t_0 b = s_0(a - qb) + t_0 b = s_0 a + (t_0 - s_0 q)b$. Mit $s := s_0$ und $t := t_0 - s_0 q$ gilt nun $sa + tb = \mathrm{ggT}(a, b)$. Damit haben wir $P(n)$ gezeigt, womit der Induktionsbeweis abgeschlossen ist.

Wie oben erläutert, ist das Lemma von Bézout nun für den Spezialfall $a, b \in \mathbb{N}_0$ bewiesen. Wir werden diesen Spezialfall jetzt anwenden, um das Lemma allgemein zu beweisen.

Seien also $a, b \in \mathbb{Z}$ beliebig. Wir behaupten, dass $\mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|)$ gilt. Für $a = b = 0$ gilt $|a| = |0| = 0 = a$ und $|b| = |0| = 0 = b$ und damit $\mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|)$. Sei nun angenommen, dass a oder b ungleich 0 ist. Eine natürliche Zahl l teilt a genau dann, wenn sie $|a|$ teilt (überlegen Sie sich, warum das so ist). Analog teilt eine natürliche Zahl b genau dann, wenn sie $|b|$ teilt. Folglich ist eine natürliche Zahl l genau dann ein gemeinsamer Teiler von a und b, wenn sie ein gemeinsamer Teiler von $|a|$ und $|b|$ ist. Damit muss der größte gemeinsame Teiler von a und b mit dem größten gemeinsamen Teiler von $|a|$ und $|b|$ übereinstimmen. Es gilt also $\mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|)$, wie behauptet.

Da $|a|, |b| \in \mathbb{N}_0$ gilt, zeigt der oben bewiesene Spezialfall des Lemmas von Bézout, dass ganze Zahlen s und t existieren mit $s|a| + t|b| = \mathrm{ggT}(|a|, |b|) = \mathrm{ggT}(a, b)$. Falls $a \geq 0, b \geq 0$ gilt, so gilt $a = |a|$ und $b = |b|$, so dass $sa + tb = \mathrm{ggT}(a, b)$ folgt. Falls $a < 0$ und $b < 0$ gilt, so gilt $|a| = -a$ und $|b| = -b$, sodass $\mathrm{ggT}(a, b) = s|a| + t|b| = s(-a) +$

$t(-b) = (-s)a + (-t)b$ folgt. Falls $a < 0$ und $b \geq 0$ gilt, so gilt $|a| = -a$ und $|b| = b$, sodass $\mathrm{ggT}(a,b) = s|a| + t|b| = s(-a) + tb = (-s)a + tb$ folgt. Falls $a \geq 0$ und $b < 0$ gilt, so gilt $|a| = a$ und $|b| = -b$, sodass $\mathrm{ggT}(a,b) = s|a| + t|b| = sa + t(-b) = sa + (-t)b$ folgt. Das Lemma von Bézout ist also für alle möglichen Wahlen von $a, b \in \mathbb{Z}$ erfüllt. Der Beweis ist also abgeschlossen.

Hinweis: Dieser Beweis war die schwierigste Aufgabe auf dem Übungsblatt. Wenn Sie den Beweis nicht komplett verstehen, machen Sie sich nichts draus.

(b) Sei $n \geq 2$ eine natürliche Zahl und sei $k \in \mathbb{Z}$, so dass $[k]$ invertierbar in $\mathbb{Z}/n$ ist. Nach Lemma 2.35 gilt $\mathrm{ggT}(k,n) = 1$. Nach dem Lemma von Bézout existieren $s, t \in \mathbb{Z}$ mit $1 = \mathrm{ggT}(k,n) = sk + tn$. Nun gilt

$$[1] = [sk + tn] = [sk] + [tn] = [s] \cdot [k] + [t] \cdot [n] = [s] \cdot [k] + [t] \cdot [0] = [s] \cdot [k] + [0] = [s] \cdot [k].$$

Damit gilt $[k]^{-1} = [s]$.

Aufgabe 6

Sei K ein Körper und sei n eine natürliche Zahl. Beweisen Sie, dass K^n zusammen mit der in Beispiel 3.2 angegebenen Addition und Skalarmultiplikation ein Vektorraum ist.

Lösung

Wir zeigen, dass K^n zusammen mit der in Beispiel 3.2 definierten Addition und Skalarmultiplikation die Eigenschaften (i)-(iv) aus Definition 3.1 erfüllt. Im Folgenden seien $x_1, x_2, \ldots, x_n$, $y_1, y_2, \ldots, y_n, z_1, z_2, \ldots, z_n \in K$. Außerdem seien $\lambda, \mu \in K$.

(i) Wir zeigen, dass K^n zusammen mit der in Beispiel 3.2 definierten Addition eine abelsche Gruppe ist.

Assoziativität der Addition: Es gilt

$$\begin{aligned}\left(\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}+\begin{pmatrix}y_1\\y_2\\\vdots\\y_n\end{pmatrix}\right)+\begin{pmatrix}z_1\\z_2\\\vdots\\z_n\end{pmatrix} &= \begin{pmatrix}x_1+y_1\\x_2+y_2\\\vdots\\x_n+y_n\end{pmatrix}+\begin{pmatrix}z_1\\z_2\\\vdots\\z_n\end{pmatrix}\\ &= \begin{pmatrix}(x_1+y_1)+z_1\\(x_2+y_2)+z_2\\\vdots\\(x_n+y_n)+z_n\end{pmatrix}\\ &= \begin{pmatrix}x_1+(y_1+z_1)\\x_2+(y_2+z_2)\\\vdots\\x_n+(y_n+z_n)\end{pmatrix}\\ &= \begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}+\begin{pmatrix}y_1+z_1\\y_2+z_2\\\vdots\\y_n+z_n\end{pmatrix}\\ &= \begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}+\left(\begin{pmatrix}y_1\\y_2\\\vdots\\y_n\end{pmatrix}+\begin{pmatrix}z_1\\z_2\\\vdots\\z_n\end{pmatrix}\right).\end{aligned}$$

Die erste, vierte und fünfte Gleichheit gelten dabei nach der Definition der Addition in K^n. Die zweite und dritte Gleichheit gelten wegen der Assoziativität der Addition in K (was wiederum nach Definition eines Körpers gilt).

Existenz eines neutralen Elements: Es gilt

$$\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}+\begin{pmatrix}0_K\\0_K\\\vdots\\0_K\end{pmatrix}=\begin{pmatrix}x_1+0_K\\x_2+0_K\\\vdots\\x_n+0_K\end{pmatrix}=\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}=\begin{pmatrix}0_K+x_1\\0_K+x_2\\\vdots\\0_K+x_n\end{pmatrix}=\begin{pmatrix}0_K\\0_K\\\vdots\\0_K\end{pmatrix}+\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}.$$

Somit ist

$$\begin{pmatrix}0_K\\0_K\\\vdots\\0_K\end{pmatrix}$$

neutral bezüglich der Addition.

Existenz von Inversen: Es gilt

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} -x_1 \\ -x_2 \\ \vdots \\ -x_n \end{pmatrix} = \begin{pmatrix} x_1 + (-x_1) \\ x_2 + (-x_2) \\ \vdots \\ x_n + (-x_n) \end{pmatrix} = \begin{pmatrix} 0_K \\ 0_K \\ \vdots \\ 0_K \end{pmatrix} = \begin{pmatrix} (-x_1) + x_1 \\ (-x_2) + x_2 \\ \vdots \\ (-x_n) + x_n \end{pmatrix} = \begin{pmatrix} -x_1 \\ -x_2 \\ \vdots \\ -x_n \end{pmatrix} + \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Somit ist $\begin{pmatrix} -x_1 \\ -x_2 \\ \vdots \\ -x_n \end{pmatrix}$ invers zu $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$.

Bisher haben wir gezeigt, dass K^n mit der in Beispiel 3.2 definierten Addition eine Gruppe bildet. Wir zeigen nun, dass es sich um eine abelsche Gruppe handelt. Das sehen wir wie folgt:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix} = \begin{pmatrix} y_1 + x_1 \\ y_2 + x_2 \\ \vdots \\ y_n + x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} + \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Hierbei haben wir die Kommutativität der Addition in K verwendet, um die zweite Gleichheit zu erhalten.

(ii) Wir zeigen, dass die in Beispiel 3.2 definierte Skalarmultiplikation assoziativ ist. Es gilt

$$(\lambda\mu) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} (\lambda\mu)x_1 \\ (\lambda\mu)x_2 \\ \vdots \\ (\lambda\mu)x_n \end{pmatrix} = \begin{pmatrix} \lambda(\mu x_1) \\ \lambda(\mu x_2) \\ \vdots \\ \lambda(\mu x_n) \end{pmatrix} = \lambda \begin{pmatrix} \mu x_1 \\ \mu x_2 \\ \vdots \\ \mu x_n \end{pmatrix} = \lambda \left(\mu \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \right).$$

Hierbei gelten die erste, dritte und vierte Gleichheit nach der Definition der Skalarmultiplikation in K^n. Die zweite Gleichheit gilt aufgrund der Assoziativität der Multiplikation in K.

(iii) Wir zeigen nun, dass das Distributivgesetz für Vektoren und Skalare gilt. Erstens gilt

$$\begin{aligned}
\lambda\left(\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}\right) &= \lambda \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix} \\
&= \begin{pmatrix} \lambda(x_1 + y_1) \\ \lambda(x_2 + y_2) \\ \vdots \\ \lambda(x_n + y_n) \end{pmatrix} \\
&= \begin{pmatrix} \lambda x_1 + \lambda y_1 \\ \lambda x_2 + \lambda y_2 \\ \vdots \\ \lambda x_n + \lambda y_n \end{pmatrix} \\
&= \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{pmatrix} + \begin{pmatrix} \lambda y_1 \\ \lambda y_2 \\ \vdots \\ \lambda y_n \end{pmatrix} \\
&= \lambda \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \lambda \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}.
\end{aligned}$$

Dabei gilt die erste Gleichheit nach Definition der Addition in K^n, die zweite Gleichheit nach Definition der Skalarmultiplikation in K^n, die dritte nach den Distributivgesetzen in K, die vierte nach Definition der Addition in K^n und die fünfte nach Definition der Skalarmultiplikation in K^n.

Zweitens gilt

$$\begin{aligned}(\lambda+\mu)\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix} &= \begin{pmatrix}(\lambda+\mu)x_1\\(\lambda+\mu)x_2\\\vdots\\(\lambda+\mu)x_n\end{pmatrix}\\ &= \begin{pmatrix}\lambda x_1+\mu x_1\\\lambda x_2+\mu x_2\\\vdots\\\lambda x_n+\mu x_n\end{pmatrix}\\ &= \begin{pmatrix}\lambda x_1\\\lambda x_2\\\vdots\\\lambda x_n\end{pmatrix}+\begin{pmatrix}\mu x_1\\\mu x_2\\\vdots\\\mu x_n\end{pmatrix}\\ &= \lambda\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}+\mu\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}.\end{aligned}$$

Dabei gilt die erste Gleichheit nach Definition der Skalarmultiplikation in K^n, die zweite nach den Distributivgesetzen in K, die dritte nach Definition der Addition in K^n und die vierte nach Definition der Skalarmultiplikation in K^n.

(iv) Es gilt

$$1_K\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix} = \begin{pmatrix}1_K\cdot x_1\\1_K\cdot x_2\\\vdots\\1_K\cdot x_n\end{pmatrix} = \begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}.$$

Dabei gilt die erste Gleichheit nach Definition der Skalarmultiplikation in K^n und die zweite, weil 1_K neutral bezüglich der Multiplikation in K ist.

Hausaufgaben zur Nachbereitung

Die folgenden Aufgaben sind abzugeben. Bitte laden Sie Ihre Abgabe bis zum 1.12.2021, 12:00 Uhr, in den dafür vorgesehenen Opal-Ordner hoch.

Lösungsblatt 6

Aufgabe 7 (6 Punkte)

(a) Seien m und n natürliche Zahlen mit $m > n$. Seien außerdem k und r natürliche Zahlen mit $m = kn + r$ und $r \in \{0, 1, \ldots, n-1\}$. Zeigen Sie, dass $\mathrm{ggT}(m, n) = \mathrm{ggT}(n, r)$.

(b) Nutzen Sie (a), um $\mathrm{ggT}(1055, 1026)$ zu berechnen. Finden Sie außerdem $s, t \in \mathbb{Z}$ mit $\mathrm{ggT}(1055, 1026) = s \cdot 1055 + t \cdot 1026$.

Hinweis: Wenn Sie nicht wissen, in welcher Weise Sie (a) verwenden sollen und wie Sie die Darstellung $\mathrm{ggT}(1055, 1026) = s \cdot 1055 + t \cdot 1026$ *finden sollen, so machen Sie sich mit dem erweiterten Euklidischen Algorithmus vertraut.*

(c) Folgern Sie aus (b), dass $[1026]$ in $\mathbb{Z}/1055$ invertierbar ist und bestimmen Sie das multiplikative Inverse von $[1026]$ in $\mathbb{Z}/1055$.

Lösung

(a) Sei $l \in \mathbb{N}$. Wir behaupten:

$$l \text{ teilt sowohl } n \text{ als auch } r \Leftrightarrow l \text{ teilt sowohl } n \text{ als auch } m. \tag{1}$$

Dies beweisen wir wie folgt:

$\Rightarrow$: Angenommen, l teilt sowohl n als auch r. Dann existieren ganze Zahlen a und b mit $n = la$ und $r = lb$. Nun gilt $m = kn + r = k(la) + lb = l(ka) + lb = l(ka + b)$. Damit ist l ein Teiler von m. Nach Annahme teilt l auch n. Somit teilt l sowohl n als auch m.

$\Leftarrow$: Angenommen, l teilt sowohl n als auch m. Dann existieren ganze Zahlen c und d mit $n = lc$ und $m = ld$. Es gilt $r = m - kn = ld - k(lc) = ld - l(kc) = l(d - kc)$. Damit ist l ein Teiler von r. Nach Annahme teilt l auch n. Somit teilt l sowohl n als auch r.

Damit haben wir (1) bewiesen.

Nach (1) stimmen die gemeinsamen Teiler von m und n mit den gemeinsamen Teilern von r und n überein. Damit muss auch der größte gemeinsame Teiler von m und n mit dem größten gemeinsamen Teiler von r und n übereinstimmen. Folglich gilt $\mathrm{ggT}(m, n) = \mathrm{ggT}(n, r)$.

(b) Es gilt

$$1055 = 1 \cdot 1026 + 29.$$

Mit $m := 1055$, $n := 1026$, $k := 1$ und $r := 29$ sind die Voraussetzungen aus (a) erfüllt. Nach (a) gilt also $\mathrm{ggT}(1055, 1026) = \mathrm{ggT}(m, n) = \mathrm{ggT}(n, r) = \mathrm{ggT}(1026, 29)$.

Es gilt

$$1026 = 35 \cdot 29 + 11.$$

Mit $m := 1026$, $n := 29$, $k := 35$ und $r := 11$ sind die Voraussetzungen aus (a) erfüllt. Nach (a) gilt also $\mathrm{ggT}(1026, 29) = \mathrm{ggT}(m, n) = \mathrm{ggT}(n, r) = \mathrm{ggT}(29, 11)$.

Es gilt

$$29 = 2 \cdot 11 + 7.$$

Mit $m := 29$, $n := 11$, $k := 2$ und $r := 7$ sind die Voraussetzungen aus (a) erfüllt. Nach (a) gilt also $\mathrm{ggT}(29, 11) = \mathrm{ggT}(m, n) = \mathrm{ggT}(n, r) = \mathrm{ggT}(11, 7)$.

Es gilt

$$11 = 1 \cdot 7 + 4.$$

Mit $m := 11$, $n := 7$, $k := 1$ und $r := 4$ sind die Voraussetzungen aus (a) erfüllt. Nach (a) gilt also $\mathrm{ggT}(11, 7) = \mathrm{ggT}(m, n) = \mathrm{ggT}(n, r) = \mathrm{ggT}(7, 4)$.

Es gilt

$$7 = 1 \cdot 4 + 3.$$

Mit $m := 7$, $n := 4$, $k := 1$ und $r := 3$ sind die Voraussetzungen aus (a) erfüllt. Nach (a) gilt also $\mathrm{ggT}(7, 4) = \mathrm{ggT}(m, n) = \mathrm{ggT}(n, r) = \mathrm{ggT}(4, 3)$.

Es gilt

$$4 = 1 \cdot 3 + 1.$$

Mit $m := 4$, $n := 3$, $k := 1$ und $r := 1$ sind die Voraussetzungen aus (a) erfüllt. Nach (a) gilt also $\mathrm{ggT}(4, 3) = \mathrm{ggT}(m, n) = \mathrm{ggT}(n, r) = \mathrm{ggT}(3, 1)$.

Es gilt

$$3 = 3 \cdot 1 + 0.$$

Mit $m := 3$, $n := 1$, $k := 3$ und $r := 0$ sind die Voraussetzungen aus (a) erfüllt. Nach (a) gilt also $\mathrm{ggT}(3, 1) = \mathrm{ggT}(m, n) = \mathrm{ggT}(n, r) = \mathrm{ggT}(1, 0) = 1$.

Insgesamt erhalten wir

$$\begin{aligned}\mathrm{ggT}(1055, 1026) &= \mathrm{ggT}(1026, 29) = \mathrm{ggT}(29, 11) = \mathrm{ggT}(11, 7) = \mathrm{ggT}(7, 4) = \mathrm{ggT}(4, 3) \\ &= \mathrm{ggT}(3, 1) = \mathrm{ggT}(1, 0) = 1.\end{aligned}$$

Berechnet man den ggT zweier natürlicher Zahlen auf diese Weise, so lässt man die Erläuterungen zwischen den Schritten normalerweise weg. Kürzer könnte man die obigen Schritte also einfach wie folgt aufschreiben:

$$\begin{aligned}1055 &= 1 \cdot 1026 + 29 \\ 1026 &= 35 \cdot 29 + 11 \\ 29 &= 2 \cdot 11 + 7 \\ 11 &= 1 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + \underline{1} \\ 3 &= 3 \cdot 1 + 0.\end{aligned}$$

Dieses Berechnungsverfahren des größten gemeinsamen Teilers ist als *Euklidischer Algorithmus* bekannt. Der letzte Rest ungleich Null ist der größte gemeinsame Teiler, hier also die 1.

Um $s, t \in \mathbb{Z}$ mit $1 = \mathrm{ggT}(1055, 1026) = s \cdot 1055 + t \cdot 1026$ zu finden, rechnen wir von der vorletzten Zeile (Zeile 6) in unserer kurzen ggT-Berechnung ausgehend "rückwärts":

$$\begin{aligned}
1 &= 4 - 3 && \text{nach Zeile 6}\\
&= 4 - (7 - 4) && \text{nach Zeile 5}\\
&= 2 \cdot 4 - 7\\
&= 2 \cdot (11 - 7) - 7 && \text{nach Zeile 4}\\
&= 2 \cdot 11 - 3 \cdot 7\\
&= 2 \cdot 11 - 3 \cdot (29 - 2 \cdot 11) && \text{nach Zeile 3}\\
&= 8 \cdot 11 - 3 \cdot 29\\
&= 8 \cdot (1026 - 35 \cdot 29) - 3 \cdot 29 && \text{nach Zeile 2}\\
&= 8 \cdot 1026 - 283 \cdot 29\\
&= 8 \cdot 1026 - 283 \cdot (1055 - 1026) && \text{nach Zeile 1}\\
&= 291 \cdot 1026 - 283 \cdot 1055.
\end{aligned}$$

(c) Nach (b) gilt $\mathrm{ggT}(1055, 1026) = 1$. Nach Lemma 2.35 ist also $[1026]$ invertierbar in $\mathbb{Z}/1055$. Um das multiplikative Inverse zu bestimmen, gehen wir so vor, wie in Aufgabe 5 (b) besprochen. Nach (b) gilt $1 = 291 \cdot 1026 - 283 \cdot 1055$. Also

$$\begin{aligned}
[1] &= [291 \cdot 1026 - 283 \cdot 1055] = [291 \cdot 1026 + (-283 \cdot 1055)]\\
&= [291 \cdot 1026] + [-283 \cdot 1055] = [291] \cdot [1026] + [-283] \cdot [1055]\\
&= [291] \cdot [1026] + [-283] \cdot [0] = [291] \cdot [1026].
\end{aligned}$$

Somit gilt $[1026]^{-1} = [291]$.

Aufgabe 8 (4 Punkte)

Sei $(R, +, \cdot)$ ein Ring.

(i) Beweisen Sie Lemma 2.36 (a): Für jedes $z \in \mathbb{Z}$ und jedes $a \in R$ gilt $za = (z1_R)a$.

(ii) Beweisen Sie Lemma 2.40: Wenn R endlich ist, so ist $\mathrm{char}(R) \neq 0$. Insbesondere ist die Charaktersitik eines endlichen Körpers immer eine Primzahl.

Lösung

(i) Wir geben zwei Beweise an, wobei der erste ein bisschen strenger als der zweite ist (trotzdem würden die meisten Mathematikerinnen und Mathematiker den zweiten Beweis als Beweis akzeptieren).

1. Beweis

Wir beweisen das Lemma zunächst für den Fall $z \geq 0$, und zwar per vollständiger Induktion. Für jedes $z \in \mathbb{N}_0$ sei $P(z)$ die Aussage

Für jedes $a \in R$ gilt $za = (z1_R)a$.

1. Induktionsanfang: Wir zeigen, dass $P(0)$ wahr ist. Sei $a \in R$. Gemäß Notation 2.11 gilt dann $0 \cdot 1_R = 0_R$ und somit $(0 \cdot 1_R)a = 0_R \cdot a \overset{\text{Lemma 2.19}}{=} 0_R$. Gemäß Notation 2.11 gilt aber auch $0 \cdot a = 0_R$. Somit gilt $0 \cdot a = 0_R = (0 \cdot 1_R)a$. Dies zeigt, dass $P(0)$ wahr ist.

2. Induktionsschritt: Sei ein $z \in \mathbb{N}_0$ gegeben, so dass $P(z)$ wahr ist. Wir wollen folgern, dass auch $P(z+1)$ wahr ist. Sei dazu $a \in R$. Um $P(z+1)$ zu zeigen, haben wir nachzuweisen, dass

$$(z+1)a = ((z+1)1_R)a$$

gilt. Nach Notation 2.11 gilt $(z+1)1_R = z \cdot 1_R + 1_R$. Also $((z+1)1_R)a = (z \cdot 1_R + 1_R)a = (z \cdot 1_R)a + 1_R \cdot a = (z \cdot 1_R)a + a$, wobei die vorletzte Gleichheit nach den Distributivgesetzen in R gilt. Nach Induktionsvoraussetzung, d. h. da $P(z)$ wahr ist, gilt $(z \cdot 1_R)a = za$. Es folgt

$$((z+1)1_R)a = (z \cdot 1_R)a + a = za + a.$$

Gemäß Notation 2.11 gilt aber $za + a = (z+1)a$. Damit folgt $(z+1)a = ((z+1)1_R)a$, womit $P(z+1)$ bewiesen ist.

Nachdem wir den Fall $z \geq 0$ behandelt haben, gehen wir jetzt zum Fall $z < 0$ über. Sei also angenommen, dass $z < 0$ und sei $n := |z|$. Dann gilt $z = -n$. Wir erhalten

$$\begin{aligned}
za &= (-n)a \\
&= n(-a) && \text{gemäß Notation 2.11} \\
&= (n1_R)(-a) && \text{da Lemma schon bewiesen für } z > 0 \\
&= (-(n1_R))a && \text{nach Lemma 2.22 (a)} \\
&= ((-n)1_R)a && \text{nach Lemma 2.12 (a)} \\
&= (z1_R)a.
\end{aligned}$$

Damit haben wir das Lemma nun auch für den Fall $z < 0$ bewiesen.

2. Beweis

Sei $a \in R$. Für $z > 0$ gilt

$$za = \underbrace{a + \cdots + a}_{z-\text{mal}} = \underbrace{1_R a + \cdots + 1_R a}_{z-\text{mal}} = \underbrace{(1_R + \cdots + 1_R)}_{z-\text{mal}} a = (z1_R)a.$$

Die vorletzte Gleichheit gilt dabei wegen der Distributivgesetze in R.

Sei jetzt $z = 0$ angenommen. Dann gilt $z1_R = 0 \cdot 1_R = 0_R$ (siehe Notation 2.11 im Vorlesungsskript), und Lemma 2.19 impliziert $(z1_R)a = 0_R a = 0_R$. Es gilt weiterhin $za = 0a = 0_R$ (ebenfalls gemäß Notation 2.11), sodass $za = 0_R = (z1_R)a$ folgt.

Für $z < 0$ können wir die Aussage $za = (z1_R)a$ nun so beweisen wie am Ende des oben vorgestellten Beweises.

(ii) Sei R endlich. Wir müssen zeigen, dass $\text{char}(R) \neq 0$ gilt. Dazu führen wir einen Widerspruchsbeweis.

Annahme: $\text{char}(R) = 0$.

Wir werden aus dieser Annahme einen Widerspruch ableiten. Sei

$$M := \{n \in \mathbb{N} \ : \ n1_R = 0_R\}.$$

Gemäß Definition 2.37 ist $\text{char}(R)$ das kleinste Element von M, wenn $M \neq \emptyset$ gilt, und gleich 0, wenn $M = \emptyset$ gilt. Da nach unserer Annahme $\text{char}(R) = 0$ gilt, folgern wir, dass

$$M = \emptyset \tag{1}$$

gilt.

Sei

$$\varphi : \mathbb{N} \to R, n \mapsto n1_R.$$

Wäre φ injektiv, so wäre $|\mathbb{N}| \leq |R|$. Dies ist nicht möglich, weil R endlich ist. Folglich ist φ nicht injektiv. Es gibt also $n, m \in \mathbb{N}$, so dass $n1_R = \varphi(n) = \varphi(m) = m1_R$ und $n \neq m$. Wir können o.B.d.A. (ohne Beschränkung der Allgemeinheit) annehmen, dass $n < m$ gilt. Es gilt nun

$$\begin{aligned}
0_R &= n1_R - n1_R \\
&= m1_R - n1_R && \text{da } n1_R = m1_R \\
&= m1_R + (-n1_R) \\
&= m1_R + (-n)1_R && \text{nach Lemma 2.12 (a)} \\
&= (m + (-n))1_R && \text{nach Lemma 2.12 (b)} \\
&= (m - n)1_R.
\end{aligned}$$

Nach Definition von M gilt damit $m-n \in M$. Dies ist ein Widerspruch zu (1). Aufgrund dieses Widerspruchs muss unsere Annahme, dass $\text{char}(R) = 0$ gilt, falsch sein. Somit

ist $\mathrm{char}(R) \neq 0$.

Wir folgern nun, dass die Charaktersitik eines endlichen Körpers eine Primzahl ist. Sei also R ein endlicher Körper. Dann ist R auch ein endlicher Ring. Somit gilt $\mathrm{char}(R) \neq 0$. Lemma 2.39 (a) impliziert nun, dass $\mathrm{char}(R)$ eine Primzahl ist.

Zusatzaufgabe

Die folgende Aufgabe stellt eine besondere Herausforderung dar. Die Aufgabe wird nicht bewertet. Wenn Sie meinen, eine vollständige Lösung zu haben, sind Sie eingeladen, diese in Ihrer Übung zu präsentieren.

Aufgabe 9

Gibt es einen Körper mit genau sechs Elementen?

Lösung

Wir geben hier (etwas ausführlicher) die Lösung wieder, die auf S. 343 des (empfehlenswerten und sehr gut lesbaren) Buchs "Lineare Algebra" von Albrecht Beutelspacher zu finden ist.

Angenommen, K ist ein Körper mit genau 6 Elementen. Nach Aufgabe 7 ist $p := \mathrm{char}(K)$ eine Primzahl. Sei $F := \{0 \cdot 1_K, 1 \cdot 1_K, \ldots, (p-1) \cdot 1_K\} = \{0_K, 1_K, \ldots, (p-1) \cdot 1_K\}$.

- Es gilt $p \leq 5$: Nehmen wir an, dies sei nicht der Fall, sodass $p > 5$. Da p eine Primzahl ist, gilt damit $p \geq 7$. Da K genau 6 Elemente hat, können die Elemente $0 \cdot 1_K, 1 \cdot 1_K, \ldots, (p-1) \cdot 1_K$ nicht paarweise verschieden sein. Es gibt also $i, j \in \mathbb{N}_0$ mit $0 \leq i, j \leq p-1$ und $i \neq j$, so dass $i \cdot 1_K = j \cdot 1_K$. Wir können o.B.d.A. annehmen, dass $i < j$ gilt. Wäre $i = 0$, so wäre $0_K = i \cdot 1_K = j \cdot 1_K$, was ein Widerspruch zu $j < p = \mathrm{char}(K)$ ist. Somit gilt $1 \leq i < j \leq p-1$. Nun gilt $0_K = j \cdot 1_K - j \cdot 1_K = j \cdot 1_K - i \cdot 1_K = j \cdot 1_K + (-i \cdot 1_K) = j \cdot 1_K + ((-i) \cdot 1_K) = (j + (-i)) \cdot 1_K = (j - i) \cdot 1_K$, wobei die vierte und fünfte Gleichheit von Lemma 2.12 (a), (b) folgen. Wegen $1 \leq i < j \leq p-1$ gilt $j - i < p$. Mit $(j-i) \cdot 1_K = 0_K$ haben wir also einen Widerspruch, denn p ist wegen $p = \mathrm{char}(K)$ die kleinste natürliche Zahl mit $p \cdot 1_K = 0_K$.
- Es gilt $p \neq 5$: Sonst gäbe es genau ein $a \in K$, das nicht in F liegt. Es gilt $a \neq a + 1_K$, denn mit $a = a + 1_K$ wäre $1_K = 0_K$. Somit liegt $a + 1_K$ in F (denn a ist ja das einzige Element von K, das nicht in F liegt). Es gibt also ein $0 \leq i \leq p-1$ mit $a + 1_K = i \cdot 1_K$. Ist $i = 0$, so folgt $a + 1_K = 0 \cdot 1_K = 0_K$ und somit $a = -1_K = (p-1) \cdot 1_K \in F$ (es gilt $(p-1) \cdot 1_K = -1_K$, weil $1_K + (p-1)1_K = p1_K = 0_K$), ein Widerspruch. Ist $i > 1$, so folgt $a + 1_K = i \cdot 1_K$ und damit $a = i \cdot 1_K - 1_K = (i-1) \cdot 1_K \in F$, wieder ein Widerspruch.

- Es gilt $p \neq 3$: Sonst wäre $F = \{0_K, 1_K, 2_K\}$, wobei $2_K := 1_K + 1_K$. Sei a ein Element von K, welches nicht in F liegt. Es gilt $2_K \cdot a \neq 0_K$ wegen Lemma 2.23, $2_K \cdot a \neq 1_K$ wegen $a \neq 2_K = (2_K)^{-1}$, und $2_K \cdot a \neq 2_K$, denn sonst wäre $a = (2_K)^{-1} \cdot 2_K = 1_K$. Somit gilt $2_K \cdot a \notin F$. Außerdem gilt $2_K a \neq a$, denn sonst wäre $2_K = aa^{-1} = 1_K$ und damit $1_K + 1_K = 1_K$, was $1_K = 0_K$ implizieren würde. Da nun a und 2_K verschiedene Elemente von $K \setminus F$ sind und $K \setminus F$ genau drei Elemente hat, existiert ein Element b von $K \setminus F$, welches sowohl ungleich a als auch ungleich $2_K \cdot a$ ist. Analog zur obigen Begründung von $2_K \cdot a \notin F$ lässt sich zeigen, dass $2_K b \notin F$ gilt. Es muss also $2_K b$ gleich b, a oder $2_K a$ sein. Mit $2_K b = b$ hätten wir $2_K = 1_K + 1_K = 1_K$ und damit den Widerspruch $1_K = 0_K$. Mit $2_K b = a$ hätten wir $b = 1_K b = (2_K \cdot 2_K)b = 2_K \cdot (2_K \cdot b) = 2_K \cdot a$, ein Widerspruch. Mit $2_K b = 2_K a$ hätten wir $b = a$, wieder ein Widerspruch.

- Es gilt $p \neq 2$: Sonst wäre $F = \{0_K, 1_K\}$. Sei $a \in K \setminus F$. Ähnlich wie in der Begründung von $p \neq 3$ sieht man, dass $a \neq a + 1_K$ und dass $a + 1_K \notin F$. Sei nun b ein Element von K, das verschieden von 0_K, 1_K, a und $a + 1_K$ ist. Ähnlich wie in der Begründung von $p \neq 3$ sieht man, dass $b + 1_K$ verschieden von $0_K, 1_K, a, a + 1_K$ und b ist (z. B. gilt $b + 1_K \neq a$, denn mit $b + 1_K = a$ wäre $b = b + 0_K = b + 1_K + 1_K = a + 1_K$, was ein Widerspruch zur Wahl von b ist). Es gilt also $K = \{0_K, 1_K, a, b, a + 1_K, b + 1_K\}$. Mit ähnlichen Überlegungen wie oben macht man sich klar, dass sowohl $a + b$ wie auch $a + b + 1_K$ weder gleich a, noch gleich b, noch gleich $a + 1_K$, noch gleich $b + 1_K$ ist. Es gilt außerdem $a + b + 1_K \neq 0_K$, denn andernfalls wäre $b + 1_K = -a$, wohingegen andererseits $a + a = (1_K + 1_K)a = 0_K a = 0_K$, also $a = -a$ gilt. Es ist also $a + b + 1_K = 1_K$ und damit $a + b = 0_K$. Letzteres impliziert aber $b = -a = a$, ein Widerspruch.

Egal um welche Primzahl es sich bei p handelt: Wir gelangen immer zu einem Widerspruch. Deshalb kann es keinen Körper mit genau sechs Elementen geben.