Lösungsvorschlag zu Blatt 6

Aufgabe 6.1

Sei $n \in \mathbb{N}$ und K ein Körper.

(a) **Behauptung:** Es existiert eine Matrix $A \in M_{n\times n}(K)$, so dass

$$\forall \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in M_{n\times 1} : \quad A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_n \\ \vdots \\ x_1 \end{pmatrix}.$$

Beweis: Definiere die Einträge A_{ij} der gesuchten Matrix A wie folgt für alle $i, j \in \{1, \dots, n\}$:

$$A_{ij} = \begin{cases} 1, & \text{falls } i + j = n + 1 \\ 0, & \text{sonst} \end{cases}$$

d.h. die Einträge von A sind 1 auf der Diagonalen von A_{1n} nach A_{n1} und sonst überall 0. Dann gilt

$$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{n} A_{1j}x_j \\ \vdots \\ \sum_{j=1}^{n} A_{nj}x_j \end{pmatrix} = \begin{pmatrix} x_n \\ \vdots \\ x_1 \end{pmatrix}.$$

(b) **Voraussetzung:** Sei $A \in M_{n\times n}$ beliebig.

Behauptung: Für alle $i, j \in \{1, \dots, n\}$ existiert eine $n \times n$-Matrix B, so dass $(BA)_{ij} = A_{ij}$ und $(BA)_{lm} = 0$ für alle Tupel $(l, m) \neq (i, j)$.

Beweis: Für $p, q \in \{1, \dots, n\}$ beliebig bezeichne im Folgenden E_{pq} die Matrix mit 1 an der Stelle (p, q) und 0 überall sonst.

Wähle $B = E_{ii}$. Nach Aufgabe 5.3(c) gilt $Z^k_{BA} = Z^k_B A$ für alle $k \in \{1, \dots, n\}$, wobei Z^k_{BA} die k-te Zeile von BA bezeichne und entsprechend Z^k_B die k-te Zeile von B (Vgl. Aufgabe 5.3). Nun ist $Z^k_B = 0$ für alle $k \neq i$, also $Z^k_{BA} = 0$ für alle $k \neq i$, d.h. bis auf die i-te Zeile sind alle Zeilen von BA gleich 0.

Berechnen wir also noch Z^i_{BA}. In der i-ten Zeile von B ist der i-te Eintrag 1 und alle anderen Einträge sind 0. Es gilt daher $Z^i_{BA} = Z^i_B A = Z^i_A$. Somit sind die Einträge der Matrix BA für alle $k, l \in \{1, \dots, n\}$ gegeben durch

$$(BA)_{kl} = \begin{cases} A_{kl}, & \text{falls } k = i \\ 0, & \text{sonst} \end{cases},$$

d.h. die i-te Zeile von BA ist identisch mit der von A und alle sonstigen Zeilen von BA sind überall 0.

Nun wählen wir $C = E_{jj}$. Nach Aufgabe 5.3(a) is $S^k_{(AB)C} = (AB)S^k_C$. Für $k \neq j$ gilt $S^k_C = 0$, somit sind alle Zeilen von $(AB)C$ außer die j-te Nullzeilen. Zu guter letzt bekommen wir über $S^j_{(AB)C} = (AB)S^j_C$, dass CAB in der i-ten Zeile überall 0 stehen hat, außer an der j-ten Stelle, wo A_{ij} steht.

(Alternativ von Hand nachrechnen statt Aufgabe 5.3 zu verwenden)

(c) **Voraussetzung:** Sei $J \subseteq M_{n\times n}(K)$ eine Menge von $n \times n$-Matrizen über einem Körper K mit den folgenden Eigenschaften:

(i) J enthält eine Matrix $A \neq 0$;
(ii) J ist additivabgeschlossen, d.h., $A, B \in J \Rightarrow A + B \in J$;
(iii) J ist abgeschlossen bezüglich Links- und Rechtsmultiplikation mit Elementen aus $M_{n\times n}(K)$, d.h., für alle $A \in J$ und alle $X \in M_{n\times n}(K)$ es gilt $AX \in J$ und $XA \in J$.

Behauptung: $J = M_{n\times n}(K)$.

Beweis: Nach Voraussetzung (i) existiert eine Matrix $A \in J$ mit $A \neq 0$, d.h. es existieren $i, j \in \{1, \dots, n\}$, so dass $A_{ij} \neq 0$. Nach Aufgabenteil (b) finden wir Matrizen $B, C \in M_{n\times n}(K)$, so dass die Matrix $A' := BAC$ gegeben ist durch

$$A'_{kl} = \begin{cases} a_j, & \text{falls } k = i \text{ and } j = l \\ 0, & \text{sonst} \end{cases},$$

Nach Voraussetzung (iii) gilt $BA \in J$ (Abgeschlossenheit unter Linksmultiplikation) und damit auch $A' = (BA)C \in J$ (Abgeschlossenheit unter Rechtsmultiplikation). Hieraus folgt, abermals nach (iii),

dass auch $E_{ij} = (\frac{1}{A_{ij}} E_{ii})A' \in J$. Aus der Vorlesung (Satz 8.3), wissen wir, dass wir elementare Zeilenumformungen über Multiplikation von Elementarmatrizen von links durchführen können, d.h. nach (iii) J stabil unter Zeilenumformungen ist. Zur Lösung der Aufgabe muss man sich noch überlegen, dass Spaltenumformungen über Multiplikation von den selben Elementarmatrizen von rechts durchgeführt werden können (d.h. ein entsprechendes Resultat von Satz 8.3 für Spaltenumformungen beweisen). Auf diese Weise bekommen wir durch Zeilen- und Spaltenvertauschen aus $E_{ij} \in J$ auch $E_{kk} \in J$ für alle $k \in \{1, \ldots, n\}$. In der Tat erhalten wir E_{kk} aus E_{ij} für alle $k \in \{1, \ldots, n\}$, in dem wir die i-te mit der k-ten Zeile und die j-te Spalte mit der k-ten Spalte vertauschen. Nach (ii) ist damit auch $I_n = \sum_{i=1}^{n} E_{ii} \in J$. Sei nun $A \in M_{n\times n}(K)$ beliebig. Dann ist $A = I_n A \in J$ nach (iii).

Aufgabe 6.2

Voraussetzung: Seien K ein Körper und V ein K-Vektorraum. Seien U, W zwei Unterräume mit

(i) $U + W = V$
(ii) $U \cap W = \{0\}$

Behauptung: Zu jedem $v \in V$ existieren eindeutig bestimmte Elemente $u \in U$ und $w \in W$, so dass $v = u + w$.

Beweis: Sei $v \in V$ beliebig. Nach Voraussetzung (i) gilt $V = U + W$. Somit existieren Vektoren $u \in U$ und $w \in W$ mit $v = u+w$. Wir müssen nun noch deren Eindeutigkeit nachweisen. Seien hierzu $u, u' \in U$ und $w, w' \in W$, so dass $u + w = v$ und $u' + w' = v$ gilt. Wir zeigen, dass hieraus bereits $u = u'$ und $w = w'$ folgt.

Aus $u + w = v = u' + w'$ folgt $u - u' = w' - w$. Da $u, u' \in U$ und U ein Vektorraum ist, gilt auch $u - u' \in U$. Analog erhalten wir aus $w', w \in W$, dass $u - u' = w' - w \in W$ gilt. Somit $u - u' \in U \cap W$. Nach Voraussetzung (ii) gilt $U \cap W = \{0\}$. Damit also $u - u' = 0$, bzw. $u = u'$. Doch wenn $u+w = u'+w'$ und $u = u'$ gilt, dann natürlich auch $w = w'$.

Somit existieren eindeutig bestimmte $u \in U$ und $w \in W$ mit $v = u + w$.

Aufgabe 6.3

(a) **Voraussetzung:** Sei K ein Körper und seien V, W zwei K-Vektorräume.

Behauptung: $U := V \times W$ ist ein K-Vektorraum bezüglich komponentenweiseer Addition und Skalarmultiplikation.

Beweis: Für den Beweis nutzen wir aus, dass die jeweiligen Vektorraum-Axiome stets in den einzelnen Komponenten gelten, da V und W nach Voraussetzung Vektorräume sind.

- Als erstes beweisen wir, dass $(U, +_U)$ eine abelsche Gruppe ist.

  Zunächst zeigen wir, dass $+_U$ wohldefiniert ist. Seien $u_1 := (v_1, w_1), u_2 := (v_2, w_2) \in U = V \times W$. Dann gilt $u_1 +_U u_2 := (v_1 +_V v_2, w_1 +_W w_2)$ nach Definition von $+_U$. Da sowohl V als auch W abgeschlossen unter (Vektor-)Addition sind, ist $v_1 +_V v_2 \in V$ und $w_1 +_W w_2 \in W$. Daher $u_1 +_U u_2 = (v_1 +_V v_2, w_1 +_W w_2) \in V \times W = U$.

  Nun zeigen wir, dass $+_U$ kommutativ ist. Seien $u_1 := (v_1, w_1), u_2 := (v_2, w_2) \in V \times W = U$ beliebig aber fest. Dann gilt

  $$\begin{aligned} u_1 +_U u_2 &= (v_1, w_1) +_U (v_2, w_2) = (v_1 +_V v_2, w_1 +_W w_2) \underset{(\star)}{=} (v_2 +_V v_1, w_2 +_W w_1) \\ &= (v_2, w_2) +_U (v_1, w_1) = u_2 +_U u_1, \end{aligned}$$

  wobei die Gleichheit $(\star)$ aus der Kommutativität von $+_V$ und $+_W$ folgt.

  Für die Assoziativität seien $u_1 = (v_1, w_1), u_2 = (v_2, w_2), u_3 = (v_3, w_3) \in V \times W = U$ beliebig aber fest. Dann gilt

  $$\begin{aligned} (u_1 +_U u_2) +_U u_3 &= ((v_1, w_1) +_U (v_2, w_2)) +_U (v_3, w_3) \\ &= ((v_1 +_V v_2) +_V v_3, (w_1 +_W w_2) +_W w_3) \\ &\underset{(\star)}{=} (v_1 +_V (v_2 +_V v_3), w_1 +_W (w_2 +_W w_3)) \\ &= (v_1, w_1) +_U ((v_2, w_2) +_U (v_3, w_3)) = u_1 +_U (u_2 +_U u_3) \end{aligned}$$

  wobei die Gleichung in $(\star)$ aus der Assoziativität von $+_V$ bzw. $+_W$ folgt.

Wir beweisen nun, dass $0_U := (0_V, 0_W)$ das neutrale Element von U bezüglich $+_U$ ist, wobei 0_V jenes von V und 0_W jenes von W bezeichnet. Da $0_V \in V$ und $0_W \in W$ gilt, ist $0_U \in U$. Sei nun $u = (v, w) \in V \times W = U$ beliebig. Dann

$$u +_U 0_U = (v, w) +_U (0_V, 0_W) = (v +_V 0_V, w +_W 0_W) = (v, w) = u,$$

wobei die letzte Gleichung komponentenweise aus der (additiven) Neutralität von 0_V bzw. 0_W in V bzw. W folgt. Da $+_U$ kommutativ ist, gilt außerdem auch $0_U +_U u = u$. Somit ist 0_U das neutrale Element von U bezüglich $+_U$.

Zum Schluss müssen wir noch die Existenz von additiv inversen Elementen nachweisen. Sei hierzu $u = (v, w) \in V \times W = U$ beliebig. Definiere $u' := (-v, -w)$, wobei $-v$ dass additiv Inverse von v in V und entsprechend $-w$ das additiv Inverse von w in W bezeichnet. Wir erhalten

$$\begin{aligned} u +_U u' &= (v, w) +_U (-v, -w) = (v +_V (-v), w +_W (-w)) = (0_V, 0_W) \\ &= 0_U, \end{aligned}$$

und wegen der Kommutativität von $+_U$ ebenfalls $u' +_U u = 0$. Somit ist u' das additiv Inverse zu U.

Somit ist $(U, +_u, 0_U)$ eine abelsche Gruppe.

- Nun zeigen wir noch, dass $(U, +_U, \cdot_U)$ auch die restlichen Vektorraumaxiome erfüllt.

  Zunächst ist die Skalarmultiplikation wohldefiniert. Seien hierfür $\lambda \in K$ und $u = (v, w) \in U$ beliebig. Da V und W K-Vektorräume sind gilt $\lambda \cdot_V v \in V$ und $\lambda \cdot_W w \in W$. Daher

  $$\lambda \cdot_U u = \lambda \cdot_U (v, w) = (\lambda \cdot_V v, \lambda \cdot_W w) \in V \times W = U$$

  .

  Als nächstes zeigen wir, dass sich $1 \in K$gegeben bezüglich $\cdot_U$ neutral verhält. Sei also wieder $u = (v, w) \in V \times W = U$ beliebig. Dann gilt

  $$1 \cdot_U u = 1 \cdot_U (v, w) = (1 \cdot_V v, 1 \cdot_W w) = (v, w),$$

  weil in den Vektorräumen V bzw. W stets $1 \cdot_V v = v$ und $1 \cdot_W w = w$ gilt.

  Nun weisen wir die Assoziativität der Skalarmultiplikation nach. Seien hierzu also $\lambda, \mu \in K$ und $u = (v, w) \in V \times W = U$ beliebig. Dann ist

  $$\begin{aligned} (\lambda\mu) \cdot_U u &= (\lambda\mu) \cdot_U (v, w) \\ &\underset{(\star)}{=} ((\lambda\mu) \cdot_V v, (\lambda\mu) \cdot_W w) \\ &= (\lambda \cdot_V (\mu \cdot_V v), \lambda \cdot_W (\mu \cdot_W w)) \\ &= \lambda \cdot_U (\mu \cdot_V v, \mu \cdot_W w) \\ &= \lambda \cdot_U (\mu \cdot_U (v, w)) \\ &= \lambda \cdot_U (\mu \cdot_U u) \end{aligned}$$

  wobei in $(\star)$ die Assoziativität der Skalarmultiplikation über V bzw. W ausgenutzt wurde.

  Als nächstes zeigen wir die Distributivität der Skalarmultiplikation bzgl. einer **Vektorsumme**. Hierfür seien zwei beliebige **Vektoren** $u_1 = (v_1, w_1), u_2 = (v_2, w_2) \in V \times W = U$ und ein beliebiger Skalar $\lambda \in K$ gegeben. Es gilt

  $$\begin{aligned} \lambda \cdot_U (u_1 +_U u_2) &= \lambda \cdot_U ((v_1, w_1) +_U (v_2 + w_2) \\ &= \lambda \cdot_U (v_1 +_V v_2, w_1 +_W w_2) \\ &= (\lambda \cdot_V (v_1 +_V v_2), \lambda \cdot_W (w_1 +_W w_2)) \\ &\underset{(\star)}{=} (\lambda \cdot_V v_1 +_V \lambda \cdot_V v_2, \lambda \cdot_W w_1 +_W \lambda \cdot_W w_2) \\ &= (\lambda \cdot_V v_1, \lambda \cdot_W w_1) +_U (\lambda \cdot_V v_2, \lambda \cdot_W w_2) \\ &= \lambda \cdot_U (v_1, w_1) +_U \lambda \cdot_U (v_2, w_2) \\ &= \lambda \cdot_U u_1 +_U \lambda \cdot_U u_2. \end{aligned}$$

  Dabei nutzt $(\star)$ die Distributivität bzgl. Vektorsummen komponentenweise in V bzw. W aus.

Zum Schluss zeigen wir noch die Distributivität einer **Skalarsumme** bzgl. der Skalarmultiplikation. Seien hierfür beliebige **Skalare** $\lambda, \mu \in K$ und ein beliebiger Vektor $u = (v, w) \in V \times W = U$ gegeben. Beobachte

$$\begin{aligned}(\lambda+\mu) \cdot_U u &= (\lambda+\mu) \cdot_U (v,w) \\ &\underset{(\star)}{=} ((\lambda+\mu) \cdot_V v, (\lambda+\mu) \cdot_W w) \\ &= (\lambda \cdot_V v +_V \mu \cdot_V v, \lambda \cdot_W w +_W \mu \cdot_W w) \\ &= (\lambda \cdot_V v, \lambda \cdot_W w) +_U (\mu \cdot_V v, \mu \cdot_W w) \\ &= \lambda \cdot_U (v,w) +_U \mu \cdot_U (v,w) \\ &= \lambda \cdot_U u +_U \mu \cdot_U u\end{aligned}$$

erneut ergibt sich die Gleichheit $(\star)$ aus der Distributivität der Summer in K bzgl. Skalarmultiplikation in V bzw. W. Es wurden somit alle Vektorraumaxiome geprüft. $(U, +_U, *_U, 0_U)$ ist also ein $K-$Vektorraum.

(b) **Voraussetzung:** Sei F die Menge aller Abbildungen $f : \mathbb{R} \to \mathbb{R}$ versehen mit punktweiser Addition und Skalarmultiplikation $(\lambda f)(x) := \lambda f(x)$ für $f, g \in F$ und $\lambda \in \mathbb{R}$. Seien ferner
$F_1 := \{f \in F | \forall x \in R\colon f(x) = f(-x)\}$ und $F_2 := \{f \in F | \forall x \in R\colon f(x) = -f(-x)\}$.

Behauptung: F ist ein $\mathbb{R}$-Vektorraum und F_1 und F_2 sind Unterräume von F.

Beweis: Aus Aufgabe 1.1a wissen wir bereits, dass $(F, +)$ abelsche Gruppe ist.

Seien nun $\lambda, \mu \in \mathbb{R}$ sowie $f, g \in F$ beliebig. Dann gilt für alle $x \in \mathbb{R}$:

- *Distributivität (I):* $((\lambda+\mu)f)(x) = (\lambda+\mu) \cdot f(x) = \lambda f(x) + \mu f(x) = (\lambda f + \mu f)(x)$
- *Distributivität (II):* $(\lambda(f+g))(x) = \lambda((f+g)(x)) = \lambda(f(x)+g(x)) = \lambda f(x)+\lambda g(x) = (\lambda f+\lambda g)(x)$
- *Assoziativität:* $((\lambda\mu)f)(x) = (\lambda\mu) \cdot f(x) = \lambda \cdot (\mu \cdot f(x)) = (\lambda(\mu f))(x)$
- Letztlich ist wegen $1 \in \mathbb{R}$ und $f(x) \in \mathbb{R}$ auch $(1 \cdot f)(x) = 1 \cdot f(x) = f(x)$ die Eins neutral bezüglich Skalarmultiplikation.

  Damit ist $(F, +, \cdot)$ ein $\mathbb{R}$- Vektorraum.

Offensichtlich gelten $F_1 \subseteq F$ und $F_2 \subseteq F$ aufgrund der Definition der Mengen. Zudem ist für $h \in F$ mit $h(x) = 0\ \forall x \in \mathbb{R}$ auch $h \in F_1$ und $h \in F_2$ (Bemerke, dass somit $0 \in F_1 \cap F_2$). Seien also $\mu \in \mathbb{R}$ sowie $f, g \in F_1$ und $u, v \in F_2$. Wir zeigen Abgeschlossenheit bezüglich der Operationen in F_1 und F_2.

- $(f + \mu g)(x) = f(x) + \mu \cdot g(x) = f(-x) + \mu g(-x) = (f + \mu g)(-x) \in F_1$.
- $(u+\mu v)(x) = u(x)+\mu \cdot v(x) = -u(-x)+\mu \cdot (-v(-x)) = -u(-x)-\mu \cdot v(-x) = (-(u+\mu v))(-x) \in F_2$

Damit sind F_1 und F_2 Untervektorräume von $(F, +, \cdot)$.

(c) **Behauptung:** $F_1 \cap F_2 = \{0\}$ und $F_1 + F_2 = F$.

Beweis: Sei $g \in F_1 \cap F_2$. Dann gilt für alle $x \in \mathbb{R}$, dass $g(x) = g(-x) = -g(x)$, d.h. $g(x) = -g(x)$ für alle $x \in \mathbb{R}$, beziehungsweise $2g(x) = 0$ für alle $x \in \mathbb{R}$. Wegen $2 \neq 0$ also $g(x) = 0$ für alle $x \in \mathbb{R}$. Damit gilt $g = 0$. Umgekehrt hatten wir oben bereits gesehen, dass $0 \in F_1 \cap F_2$. Somit $F_1 \cap F_2 = \{0\}$.

Sei nun $f \in F$ beliebig. Definiere die Abbildungen f_1 und f_2 in F durch $f_1(x) := \frac{f(x)+f(-x)}{2}$ und $f_2(x) := \frac{f(x)-f(-x)}{2}$ für alle $x \in \mathbb{R}$. Dann gilt

$$f_1(x) + f_2(x) = \frac{f(x)+f(-x)}{2} + \frac{f(x)-f(-x)}{2} = \frac{2f(x)+f(-x)-f(-x)}{2} = f(x).$$

Es bleibt zu zeigen, dass $f_1 \in F_1$ und $f_2 \in F_2$. Hierzu rechnen wir nach:

$$f_1(-x) = \frac{f(-x)+f(-(-x))}{2} = \frac{f(-x)+f(x)}{2} = \frac{f(x)+f(-x)}{2} = f_1(x)$$

$$-f_2(-x) = -\frac{f(-x)-f(-(-x))}{2} = -\frac{f(-x)-f(x)}{2} = \frac{f(x)-f(-x)}{2} = f_2(x)$$

Also $f_1 \in F_1$ und $f_2 \in F_2$. Damit ist die Behauptung bewiesen.

Aufgabe 6.4

Voraussetzung: Sei $n \in \mathbb{N}$ beliebig.

Behauptung: $\mathbb{Z}_n \setminus \mathbb{Z}_n^\times$ ist genau genau dann ein kommutativer Ring (ohne 1), wenn $n = p^k$ für eine Primzahl p und ein $k \in \mathbb{N}_0$.

Beweis: Für den folgenden Beweis benötigen wir 3 Hilfsaussagen.

Hilfsaussage 1: Für jede natürliche Zahl m existiert ein $l \in \mathbb{N}$ mit $m < 2^l$.
Beweis: Nach Induktion über m.
Induktionsanfang: Für $m = 1$ gilt $m < 2 = 2^1$.
Induktionsschritt: Sei $m > 1$ und gelte $m < 2^l$ für ein $l \in \mathbb{N}$. Dann gilt

$$m + 1 < m + m = 2m < 2 \cdot 2^l = 2^{l+1},$$

wobei im vorletzten Schritt die Induktionsvoraussetzung benutzt wurde.

Hilfsaussage 2: Jede natürliche Zahl m mit $m > 1$ kann als ein Produkt endlich vieler Primzahlen geschrieben werden.
Beweis: Ist m bereits prim, so sind wir fertig. Ist m nicht prim, so existieren nach Definition einer Primzahl Elemente $a, b \in \mathbb{N}$ mit $1 < a, b < m$, so dass $ab = m$. Sind a und b prim, so ist m ein endliches Produkt von Primzahlen. Andernfalls zerlegen wir a und/oder b (und damit m) weiter. Haben wir m in k solche Faktoren zerlegt für ein $k \in \mathbb{N}$, so gilt $m \geq 2^k$, da jeder dieser Faktoren in $\{2, \dots, m-1\}$ liegt. Nach Hilfsaussage 1 gibt es aber ein $l \in \mathbb{N}$ mit $m < 2^l$. Dementsprechend zerfällt m auf diese Weise in endlich vielen Schritten in Primfaktoren und zwar in höchstens $l - 1$ viele.

Hilfsaussage 3: Sei p eine Primzahl. Die Teiler von p^k sind genau $\{p^i : i \in \{0, \dots, k\}\}$.
Beweis: Ist a ein Teiler von p^k mit $a \neq 1$, so können wir a als endliches Produkt von Primzahlen schreiben (Hilfsaussage 2). Sei nun p' ein Primteiler von a. Dann teilt p' auch p^k. Nach iterativer Anwendung von Aufgabe 3.2 erhalten wir, dass p' ein Teiler von p ist, woraus bereits $p' = p$ folgt. Damit ist p der einzige Primteiler von a, womit wir $a = p^i$ für ein $i \in \{0, \dots, k\}$ gezeigt haben.

Zurück zur Aufgabe. Sei $R := \mathbb{Z}_n \setminus \mathbb{Z}_n^\times$. Wir zeigen beide Richtungen der Äquivalenz

$$R \text{ komm. Ring ohne } 1 \iff \exists p \in \mathbb{P}, k \in \mathbb{N}_0 : n = p^k$$

Dabei steht $\mathbb{P}$ für die Menge der Primzahlen.

$\Rightarrow$: Sei R ein kommutativer Ring ohne 1. Ist $n = 1$, so gilt $n = 2^0$ mit $2 \in \mathbb{P}$ und $0 \in \mathbb{N}_0$, d.h. die Behauptung ist wahr.

Sei nun $n > 1$. Für einen Widerspruchsbeweis nehmen wir nun an, dass n keine Primpotenz (also $\forall p \in \mathbb{P}, k \in \mathbb{N}_0 : p^k \neq n$) sei. Da n als Produkt endlich vieler Primzahlen geschrieben werden kann (Hilfsaussage 2), gibt es also mindestens zwei verschiedene Primzahlen, die n teilen. Wähle also $p, q \in \mathbb{P}$ mit $p|n$, $q|n$ und $p \neq q$. Da p ein gemeinsamer Teiler von p und n ist, folgt $\mathrm{ggT}(p, n) \geq p > 1$, also $\mathrm{ggT}(p, n) \neq 1$ und analog $\mathrm{ggT}(q, n) \neq 1$. Nach Aufgabe 3.4 ist $\mathbb{Z}_n^\times = \{x \in \mathbb{Z}_n : \mathrm{ggT}(x, n) = 1\}$, also sind $p, q \notin \mathbb{Z}_n^\times$ und damit $p, q \in R$ (denn $p, q < n$ ist offensichtlich, also $p, q \in \mathbb{Z}_n$).
Da p und q verschiedene Primzahlen sind, gilt $\mathrm{ggT}(p, q) = 1$. Mit dem euklidischen Algorithmus finden wir $a, b \in \mathbb{Z}$ mit $ap + bq = 1$, also

$$1 = \overline{ap + bq} = \overline{ap} +_n \overline{bq} = \underbrace{p +_n \dots +_n p}_{a\text{-mal}} + \underbrace{q +_n \dots +_n q}_{b\text{-mal}} \in R$$

Andererseits ist $1 \cdot 1 = 1$, also $1 \in \mathbb{Z}_n^\times$ und damit $1 \notin R$, ein Widerspruch. Somit gibt es ein $p \in \mathbb{P}$ und ein $k \in \mathbb{N}_0$ mit $n = p^k$.

$\Leftarrow$: Sei $p \in \mathbb{P}$ und $k \in \mathbb{N}_0$ mit $n = p^k$. Wir bestimmen zunächst, wie R aussieht. Wir wissen aus Aufgabe 3.4, dass $R = \{x \in \mathbb{Z}_n : ggT(x, n) \neq 1\}$.

Sei $x \in \mathbb{Z}_n$ mit $\mathrm{ggT}(x, n) \neq 1$, dann ist $q := \mathrm{ggT}(x, n)$ ein Teiler von $n = p^k$. Die Teiler von p^k sind $\{p^i : i \in \{0, \dots, k\}\}$ (Hilfsaussage 3). Es gilt somit $p|q$, und wegen $q|x$ auch $p|x$. Damit ist $R \subseteq \{x \in \mathbb{Z}_n : p|x\}$. Sei umgekehrt $x \in \mathbb{Z}_n$ mit $p|x$, dann ist p gemeinsamer Teiler von x und n, also $\mathrm{ggT}(x, n) \geq p > 1$. Damit ist $R = \{x \in \mathbb{Z}_n : p|x\}$. Wir zeigen: Das ist ein Ring ohne 1.

Zeige zunächst: $(R, +)$ ist eine Untergruppe von $(\mathbb{Z}_n, +)$. Es gilt $0 \in R$ wegen $p|0$. Für $x, y \in R$ gilt $p|x, p|y$. Sei $m \in \mathbb{Z}$ mit $\overline{x + y} = x + y - mn$, dann gilt wegen $p|n$ auch $p|x + y - mn = \overline{x + y}$,

also $\overline{x+y} \in R$. Außerdem ist $\overline{-x} = n - x$, aus $p|n$ und $p|x$ folgt also $p|\overline{-x}$ und damit $\overline{-x} \in R$. Damit ist $(R, +)$ eine Untergruppe von $(\mathbb{Z}_n, +)$ und damit insbesondere eine abelsche Gruppe.

Die Assoziativität und Kommutativität von $\cdot_n$ sowie die Distributivität sind $\forall$-Aussagen und übertragen sich somit von $\mathbb{Z}_n$ auf R, da $R \subseteq \mathbb{Z}_n$.

R ist abgeschlossen unter Multiplikation: Seien $x, y \in R$, etwa $x = ap$, $y = bp$. Sei $m \in \mathbb{Z}$ mit $\overline{xy} = xy - mn$, dann ist $xy - mn = abp^2 - mp^k = p(abp - mp^{k-1})$ und damit $p|\overline{xy}$, also $\overline{xy} \in R$.

Somit ist R ein kommutativer Ring. Es bleibt zu zeigen, dass R kein Einselement hat. Für $k = 0$ und $k = 1$ ist dies klar, da dann $R = \{0\}$. Sei also $k \geq 2$. Angenommen, es gäbe ein $r \in R$ mit $x \cdot_n r = x$ für alle $x \in R$. Wegen $r \in R$ wissen wir, dass $p|r$. Also $pa = r$ für ein $a \in \mathbb{Z}$. Multiplizieren auf beiden Seiten mit p^{k-1} liefert, dass $p^k a = p^{k-1} r$ in $\mathbb{Z}$. Da $p|r$ und $p|p^{k-1}$ (da $k \geq 2$), erhalten wir $r \in R$ und $p^{k-1} \in R$ und damit auch $p^{k-1} \cdot_n r \in R$. Hieraus folgt über R, dass

$$p^{k-1} \cdot_n r = \overline{p^{k-1} r} = \overline{p^k a} = \underbrace{p^k +_n \ldots +_n p^k}_{a \text{ mal}} = 0.$$

Nach Definition von r gilt aber auch $p^{k-1} \cdot_n r = p^{k-1} \neq 0$ in R, ein Widerspruch. Somit hat R kein Einselement.