8. Lösung zu algebraischen Strukturen: Grundbegriffe der Ringtheorie

Lösung (8.1) Wir haben $ab+(-a)b = \big(a+(-a)\big)\cdot b = 0\cdot b = 0$; also erfüllt $(-a)b$ die das Element $-(ab)$ definierende Gleichung, so daß $(-a)b = -(ab)$ gilt. Analog gilt $a(-b) = -(ab)$. Schließlich haben wir $(-a)(-b) = -\big((-a)b\big) = -(-ab) = ab$.

Lösung (8.2) (a) Zunächst seien $m, n \in \mathbb{N}$. Dann gilt

$$\begin{aligned}(m+n)\cdot r \;&=\; \underbrace{r+r+\cdots+r}_{m+n \text{ Summanden}}\\ &=\; \underbrace{r+\cdots+r}_{m \text{ Summanden}} \;+\; \underbrace{r+\cdots+r}_{n \text{ Summanden}} \;= m\cdot r + n\cdot r.\end{aligned}$$

Ferner gilt $(-m-n)r = -(m+n)r = -(mr+nr) = -mr-nr = (-m)r+(-n)r$. Die erste Behauptung gilt daher jedenfalls dann, wenn m und n das gleiche Vorzeichen haben. Wegen $0\cdot r = 0$ gilt die Behauptung auch dann, wenn $m = 0$ oder $n = 0$ gilt. Es bleibt der Fall, daß m und n unterschiedliches Vorzeichen haben, sagen wir $m > 0$ und $n < 0$. (Der Fall $m < 0$ und $n > 0$ wird vollkommen analog behandelt.) Im Fall $m \geq |n|$ gilt aufgrund der bereits gezeigten Fälle die Gleichung $(m-|n|)r+|n|r = mr$, also $(m+n)r-nr = mr$ und damit $(m+n)r = mr+nr$. Im Fall $m \leq |n|$ gilt aufgrund der bereits gezeigten Fälle $(|n|-m)r+mr = |n|r$, also $(-m-n)r+mr = -nr$ und damit auch hier $mr+nr = (m+n)r$.

(b) Ist $m > 0$, so gilt

$$\begin{aligned}m\cdot(r+s) \;&=\; \underbrace{(r+s)+\cdots+(r+s)}_{m \text{ Klammern}}\\ &=\; \underbrace{r+\cdots+r}_{m \text{ Summanden}} \;+\; \underbrace{s+\cdots+s}_{m \text{ Summanden}} \;=\; m\cdot r \,+\, m\cdot s.\end{aligned}$$

Für $m = -n < 0$ folgt die Behauptung dann wegen $m\cdot(r+s) = (-n)\cdot(r+s) = -\big(n\cdot(r+s)\big) = -(n\cdot r+n\cdot s) = (-n)\cdot r+(-n)\cdot s = m\cdot r+m\cdot s$, und für $m = 0$ gilt sie trivialerweise.

(c) Für $m, n \in \mathbb{N}$ erhalten wir

$$\begin{aligned}m\cdot(n\cdot r) \;&=\; \underbrace{(n\cdot r)+\cdots+(n\cdot r)}_{m \text{ Klammern}}\\ &=\; \underbrace{(r+\cdots+r)+\cdots+(r+\cdots+r)}_{m \text{ Klammern mit jeweils } n \text{ Summanden}}\\ &=\; \underbrace{r+\cdots+r}_{mn \text{ Summanden}} \;=\; (mn)\cdot r.\end{aligned}$$

Für $m = 0$ oder $n = 0$ gilt die Behauptung trivialerweise. ist schließlich $m = um'$ und $n = vn'$ mit $m', n' \in \mathbb{N}$ und $u, v \in \{\pm 1\}$, so haben wir $m\cdot(n\cdot r) = (um')\cdot\big((vn')\cdot r\big) = uv\,m'\cdot(n'\cdot r) = uv\,(m'n')\cdot r = (uvm'n')\cdot r = (mn)\cdot r$.

(d) Für $m \in \mathbb{N}$ haben wir einerseits $m\cdot(rs) = rs+\cdots+rs = (r+\cdots+r)s = (m\cdot r)s$, andererseits auch $m\cdot(rs) = rs+\cdots+rs = r(s+\cdots+s) = r(m\cdot s)$. Für $m = 0$ gilt die Behauptung trivialerweise. Für $m = -n < 0$ gilt sie dann wegen $m\cdot(rs) = (-n)\cdot(rs) = -\big(n\cdot(rs)\big) = -\big((n\cdot r)s\big) = \big((-n)\cdot r\big)s = (m\cdot r)s$ und analog $m\cdot(rs) = (-n)\cdot(rs) = -\big(n\cdot(rs)\big) = -\big(r(n\cdot s)\big) = r\big((-n)\cdot s\big) = r(m\cdot s)$.

Besitzt R ein Einselement 1, so gilt für alle $n \in \mathbb{N}$ und alle $r \in R$ einerseits $n\cdot r = r+\cdots+r = (1+\cdots+1)r = (n\cdot 1)r$, andererseits auch $n\cdot r = r+\cdots+r = r(1+\cdots+1) = r(n\cdot 1)$. Hieraus folgt dann leicht $(m\cdot 1)r = m\cdot r = r(m\cdot 1)$ für alle $m \in \mathbb{Z}$.

Lösung (8.3) (a) Es sei 1 das Einselement von R. Für alle $a, b \in R$ haben wir dann einerseits $(a+b)(1+1) = (a+b)\cdot 1+(a+b)\cdot 1 = a+b+a+b$, andererseits $(a+b)(1+1) = a(1+1)+b(1+1) = a+a+b+b$, insgesamt also $a+b+a+b = a+a+b+b$, und hieraus folgt $b+a = a+b$.

(b) Es gelte (6). Für alle $a, b, c \in R$ gilt dann $(a+b)c = c(a+b) = ca+cb = ac+bc$ und damit Axiom (7). Vollkommen analog sieht man, daß aus (7) schon (6) folgt.

Lösung (8.4) Daß $R_\star$ wieder ein Ring ist, rechnet man sofort nach; ebenso, daß $R_\star$ genau dann kommutativ ist, wenn R kommutativ ist. Das Element $(1,0)$ ist ein Einselement in $R_\star$, denn für alle $m \in \mathbb{Z}$ und alle $r \in R$ gilt

$$(1,0)\cdot(m,r) \;=\; (m,r) \;=\; (m,r)\cdot(1,0).$$

Für alle $r, s \in R$ erhalten wir ferner $(0,r)+(0,s) = (0,r+s)$ und $(0,r)\cdot(0,s) = (0,rs)$, so daß man mit den Elementen $r \in R$ genauso rechnet wie mit den Elementen $(0,r) \in R_\star$; die Abbildung $r \mapsto (0,r)$ ist also ein Isomorphismus von R auf $\{0\}\times R \subseteq R_\star$.

Lösung (8.5) Wir erhalten $a^2 = aa = (ab)(ab) = a(ba)b = abb = (ab)b = ab = a$ und $b^2 = bb = (ba)(ba) = b(ab)a = baa = (ba)a = ba = b$.

Lösung (8.6) (a) Wir können $R = 2\mathbb{Z}$ (Menge aller geraden ganzen Zahlen) und $U = 4\mathbb{Z}$ (Menge aller durch 4 teilbaren ganzen Zahlen) wählen.

(b) Wähle etwa $R = \mathbb{Z}$ und $U = 2\mathbb{Z}$.

(c) Wähle etwa $R = \mathbb{Z}\times(2\mathbb{Z})$ und $U = \mathbb{Z}\times\{0\}$.

(d) Wähle etwa $R = \mathbb{Q}$ und $U = \mathbb{Z}$.

(e) Wähle etwa $R = \mathbb{R}^{2\times 2}$ und

$$U \;=\; \{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \mid a \in \mathbb{R}\}\,.$$

Lösung (8.7) Es sei $U := \mathbb{Z}n$ mit $n \in \mathbb{N}_0$; wir wollen zeigen, daß U ein Unterring von $\mathbb{Z}$ ist. Zunächst gilt $0 = 0\cdot n \in U$. Wegen $-(xn) = (-x)n \in U$ gilt $-U \subseteq U$. Wegen $xn+yn = (x+y)n \in U$ gilt $U+U \subseteq U$. Wegen $(xn)\cdot(yn) = (xyn)n \in U$ gilt schließlich $UU \subseteq U$. Umgekehrt sei U ein Unterring von $\mathbb{Z}$. Ist $U = \{0\}$, so gilt $U = \mathbb{Z}\cdot 0$. Ist $U \neq \{0\}$, so enthält U ein Element $u_0 \neq 0$,

damit die beiden Elemente $\pm u_0$ und folglich auch die positive Zahl $|u_0|$. Dann gibt es aber auch eine kleinste positive Zahl n in U. Dann liegen auch alle Zahlen $kn = n+\cdots+n$ mit $k \in \mathbb{N}$ und alle Zahlen $(-k)n = -(kn)$ in U, so daß $\mathbb{Z}n \subseteq U$ gilt. Umgekehrt sei m irgendein Element in U. Polynomdivision mit Rest liefert eine Darstellung $m = kn+r$ mit $0 \leq r < n$ (und zwar sowohl für $m \geq 0$ als auch für $m < 0$). Es gilt dann $r = m - kn \in U - U \subseteq U$, was nur für $r = 0$ möglich ist (denn n war ja als *kleinstes* positives Element in U gewählt worden). Also gilt $m = kn \in \mathbb{Z}n$. Da $m \in U$ beliebig war, ist damit auch die Inklusion $U \subseteq \mathbb{Z}n$ gezeigt, so daß insgesamt $U = \mathbb{Z}n$ gilt.

Lösung (8.8) (a) Wir schreiben kurz $0, 2, 4$ statt $[0], [2], [4]$, sind uns aber bewußt, daß wir immer modulo 6 rechnen. Offensichtlich ist U abgeschlossen bezüglich der Addition und der Multiplikation und auch bezüglich der Bildung additiver Inverser (denn $-0 = 0$, $-2 = 4$ und $-4 = 2$). Also ist U ein Unterring von $\mathbb{Z}_6$. Wegen $4 \cdot 0 = 0$, $4 \cdot 2 = 2$ und $4 \cdot 4 = 4$ ist 4 ein Einselement in U. Dieses ist aber verschieden von dem Einselement 1 in $\mathbb{Z}_6$ (also der Restklasse [1] modulo 6).

(b) Ist u_0 ein Einselement in U, so gilt jedenfalls $u_0^2 = u_0 \cdot u_0 = u_0$. Ist $u \in U$ beliebig und schreiben wir $u_0 = [m_0]$ und $u = [m]$ mit $m, m_0 \in \mathbb{N}$, so haben wir $u = uu_0 = [m][m_0] = [mm_0] = [m_0 + m_0 + \cdots + m_0] = [m_0] + [m_0] + \cdots + [m_0] = u_0 + u_0 + \cdots + u_0 = m \cdot u_0$, so daß $U = \mathbb{Z} \cdot u_0$ gilt. Umgekehrt mögen die Bedingungen $U = \mathbb{Z} \cdot u_0$ und $u_0^2 = u_0$ gelten. Für alle Elemente $u = mu_0 \in U$ gilt dann $uu_0 = (mu_0)u_0 = mu_0^2 = mu_0 = u$, so daß u_0 tatsächlich ein Einselement von U ist.

Lösung (8.9) (a) Es sei $[x]$ eine Restklasse modulo n. Dann gelten die folgenden Aussagen:

- Sind x und n teilerfremd, so gibt es ganze Zahlen a und b mit $ax + bn = 1$ (lineare Darstellung des ggT), und hieraus folgt $[1] = [ax + bn] = [a][x]$, so daß $[x]$ eine Einheit ist.
- Haben x und n einen gemeinsamen Teiler $g > 1$, sagen wir $x = ga$ und $n = gb$ mit $[b] \neq [0]$, so gilt $[x] \cdot [b] = [gab] = [0]$, so daß $[x]$ ein Nullteiler ist.

Da ein Nullteiler niemals eine Einheit sein kann, folgt aus diesen beiden Beobachtungen, daß die Einheiten von $\mathbb{Z}_n$ genau die zu n teilerfremden Restklassen sind, während die Nullteiler die zu n nicht teilerfremden Restklassen sind. (Insbesondere ist also jedes Element von $\mathbb{Z}_n$ entweder eine Einheit oder ein Nullteiler.)

(b) Es sei $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ die Primfaktorzerlegung von n. Eine Restklasse $[x]$ ist genau dann nilpotent, wenn es eine Potenz m derart gibt, daß x^m durch $p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ teilbar ist, was genau dann der Fall ist, wenn x durch $p_1 p_2 \cdots p_k$ teilbar ist.

(c) Ist x idempotent in $\mathbb{Z}_n$, so ist $x^2 - x = x(x-1)$ durch n teilbar. Da x und $x-1$ keinen gemeinsamen Teiler haben können, heißt das, daß es teilerfremde Zahlen n_1 und n_2 mit $n = n_1 n_2$ derart geben muß, daß x durch n_1 und $x-1$ durch n_2 teilbar ist, sagen wir $x = an_1$ und $x - 1 = bn_2$. Dann gilt $an_1 - bn_2 = 1$; d.h., a und b müssen so gewählt werden, daß $an_1 - bn_2 = 1$ eine lineare Darstellung des ggT von n_1 und n_2 liefert. Nichttriviale idempotente Elemente gibt es in $\mathbb{Z}_n$ also nur, wenn n keine Primzahlpotenz ist, sondern mindestens zwei verschiedene Primteiler hat. Die idempotenten Elemente entsprechen dann genau den Paaren teilerfremder Zahlen (n_1, n_2) mit $n = n_1 n_2$. (Das werden wir in einer späteren Aufgabe noch präzisieren.)

Lösung (8.10) (a) Genau dann ist f eine Einheit in $C(I)$, wenn es eine stetige Funktion g gibt mit $fg = 1$, was genau dann der Fall ist, wenn f keine Nullstelle hat (denn dann ist mit f automatisch auch $g := 1/f$ stetig).

(b) Genau dann ist f ein Nullteiler in $C(I)$, wenn es eine stetige Funktion $g \neq 0$ gibt mit $fg \equiv 0$. Wegen $g \neq 0$ gibt es ein Teilintervall $J \subseteq I$, auf dem g keine Nullstelle hat; auf diesem Teilintervall muß dann f identisch verschwinden. Gibt es umgekehrt ein Teilintervall $J \subseteq I$, auf dem f identisch verschwindet, so wählen wir eine Funktion $g \neq 0$ in $C(I)$, die außerhalb von J identisch Null ist; wir haben dann $fg = 0$, aber $g \neq 0$, so daß f ein Nullteiler ist. Also ist die Funktion $f \in C(I)$ genau dann ein Nullteiler, wenn sie auf einem Teilintervall von I verschwindet.

(c) Genau dann ist $f \in C(I)$ nilpotent, wenn es eine Zahl $n \in \mathbb{N}$ gibt mit $f(x)^n = 0$ für alle $x \in I$, was genau dann erfüllt ist, wenn sogar $f(x) = 0$ für alle $x \in I$ gilt. Das einzige nilpotente Element von $C(I)$ ist also die Nullfunktion.

(d) Gilt $f^2 = f$, also $f(x)^2 = f(x)$ für alle $x \in I$, so haben wir $f(x) = 0$ oder $f(x) = 1$ für jeden Wert $x \in I$. Da eine stetige Funktion auf einem Intervall I nicht den Wert 0 und den Wert 1, aber keinen Wert dazwischen annehmen kann, bedeutet dies, daß die konstante Funktion $f \equiv 0$ und die konstante Funktion $f \equiv 1$ die einzigen nilpotenten Elemente von $C(I)$ sind.

Lösung (8.11) Die Einheiten von $K^{\times n}$ sind genau die invertierbaren Matrizen. Ein Nullteiler kann nicht invertierbar sein; umgekehrt ist jede nicht invertierbare Matrix ein Nullteiler, wie wir nun zeigen wollen. Ist A nicht invertierbar, so gibt es einen Vektor $v \neq 0$ mit $Av = 0$. Für die Matrix $B := (v \mid \cdots \mid v) \neq \mathbf{0}$ gilt dann $AB = \mathbf{0}$. (Es gibt auch eine Matrix $C \neq \mathbf{0}$ mit $CA = \mathbf{0}$. Mit A ist nämlich auch A^T nicht invertierbar, so daß es einen Vektor $w \neq 0$ gibt mit $A^T w = 0$. Für die Matrix C, die in jeder Zeile den Vektor w^T stehen hat, gilt dann $A^T C^T = \mathbf{0}$ und damit $CA = \mathbf{0}$. Eine nicht invertierbare Matrix ist damit sowohl Links- als auch Rechtsnullteiler.) Eine Matrix $A \in K^{n \times n}$ ist genau dann nilpotent, wenn $A^n = \mathbf{0}$ gilt, was genau dann der Fall ist, wenn 0 ein n-facher Eigenwert von A ist. Dies ist genau dann der Fall, wenn A durch einen Basiswechsel in die Form

$$\begin{bmatrix} 0 & & \star \\ & \ddots & \\ 0 & & 0 \end{bmatrix}$$

überführt werden kann. Eine Matrix A ist idempotent, wenn sie die Gleichung $A^2 = A$ erfüllt. Es gilt dann $K^n = \mathrm{Bild}(A) \oplus \mathrm{Kern}(A)$, und bezüglich einer Basis, die sich aus einer Basis des Bildes von A und einer Basis des Kerns von A zusammensetzt, nimmt A die Form

$$A \;=\; \begin{bmatrix} \mathbf{1} & 0 \\ 0 & \mathbf{0} \end{bmatrix}$$

an. Die idempotenten Elemente in $K^{n\times n}$ sind also genau diejenigen Matrizen, die Projektionen darstellen.

Lösung (8.12) (a) Es gibt $m, n \in \mathbb{N}$ mit $a^m = 0$ und $b^n = 0$. Wir behaupten, daß dann auch $(a+b)^{m+n-1} = 0$ gilt (so daß auch $a+b$ nilpotent ist). Nach der binomischen Formel (die anwendbar ist, weil a und b kommutieren) haben wir mit $N := m+n-1$ nämlich

$$(a+b)^N = \sum_{k=0}^{m-1} \binom{N}{k} a^k \underbrace{b^{N-k}}_{=0} + \sum_{k=m}^{N} \binom{N}{k} \underbrace{a^k}_{=0} b^{N-k} = 0,$$

denn für $k \geq m-1$ gilt $N-k \geq N-(m-1) = n$ und damit $b^{N-k} = 0$, und für $k \geq m$ gilt $a^k = 0$. Setzen wir $\ell := \min(m,n)$, so erhalten wir $(ab)^\ell = a^\ell b^\ell = 0$. Hierbei gilt die erste Gleichung, weil a und b kommutieren, die zweite, weil nach Wahl von ℓ mindestens eine der Bedingungen $a^\ell = 0$ und $b^\ell = 0$ gilt. Also ist auch ab nilpotent.

(b) Wegen $A^2 = B^2 = \mathbf{0}$ sind A und B nilpotent. Für die Summe

$$S \;:=\; A+B \;=\; \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \;=\; \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

erghalten wir $S^{2k-1} = S$ und $S^{2k} = \mathbf{1}$ für alle $k \in \mathbb{N}$, und für das Produkt

$$P \;:=\; AB \;=\; \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \;=\; \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

ergibt sich $P^n = P$ für alle $n \in \mathbb{N}$. Für alle $n \in \mathbb{N}$ haben wir also $S^n \neq \mathbf{0}$ und $P^n \neq \mathbf{0}$, so daß S und P nicht nilpotent sind.

Lösung (8.13) Es möge $b^n = 0$ gelten. Dann gilt auch $(ab)^n = a^n b^n = a^n \cdot 0 = 0$ für alle $a \in R$ (egal, ob a eine Einheit ist oder nicht); mit b ist also auch ab nilpotent. Nun sei a eine Einheit; wir wollen zeigen, daß $a+b$ eine Einheit ist. Wegen $a^{-1}(a+b) = 1 + a^{-1}b$ genügt es zu zeigen, daß $1+a^{-1}b$ invertierbar ist. Setzen wir $x := a^{-1}b$, so haben wir $x^n = 0$ und damit $(1+x)(1-x+x^2-x^3+\cdots+(-1)^{n-1}x^{n-1}) = 1$. Diese letzte Gleichung zeigt, daß $1+x$ invertierbar ist.

Lösung (8.14) Wir müssen zeigen, daß aus $(ab)y = 0$ schon $y = 0$ folgt. Es sei also $0 = (ab)y = a(by)$. Da a kein Nullteiler ist, folgt hieraus $by = 0$. Da b kein Nullteiler ist, folgt hieraus $y = 0$.

Lösung (8.15) Ist 0 das einzige nilpotente Element, so ist offensichtlich $x = 0$ die einzige Lösung der Gleichung $x^2 = 0$. Umgekehrt besitze die Gleichung $x^2 = 0$ nur die Lösung $x = 0$. Es sei $y \neq 0$ nilpotent; es gibt dann eine kleinste Zahl $n \geq 2$ mit $y^n = 0$. Für $x := y^{n-1}$ gilt dann $x^2 = y^{2n-2} = y^n \cdot y^{n-2} = 0 \cdot y^{n-2} = 0$, nach Voraussetzung also $x = 0$ und damit $y^{n-1} = 0$ im Widerspruch zur Wahl von n. Dieser Widerspruch zeigt, daß es außer 0 kein nilpotentes Element in dem betrachteten Ring gibt.

Lösung (8.16) Es gilt $a+b = (a+b)^2 = a^2+ab+ba+b^2 = a+ab+ba+b$ und damit $0 = ab+ba$, also $ba = -ab$. Hieraus folgt $ab = a^2b^2 = a(ab)b = -a(ba)b = -abab = -(-ba)(-ba) = -(ba)(ba) = b(-ab)a = b(ba)a = b^2a^2 = ba$.

Lösung (8.17) Gilt $R = R_1 \times R_2$, so sind $e := (1,0)$ und $1-e = (1,1)-(1,0) = (0,1)$ von $(0,0)$ und $(1,1)$ verschiedene idempotente Elemente. Gibt es umgekehrt ein idempotentes Element $e \notin \{0,1\}$, so gilt $R = Re \oplus R(1-e)$. Zunächst gilt $R = Re + R(1-e)$, denn jedes Element $r \in R$ läßt sich schreiben als $r = re + r(1-e)$. Andererseits gilt $Re \cap R(1-e) = \{0\}$, denn aus $xe = y(1-e)$ folgt durch Multiplikation mit e einerseits $xe = xe^2 = y(e-e^2) = y \cdot 0 = 0$, durch Multiplikation mit $1-e$ andererseits auch $0 = x \cdot 0 = x(e-e^2) = xe(1-e) = y(1-e)^2 = y(1-e)$; wir erhalten also $xe = y(1-e) = 0$. Mit $R_1 := Re$ und $R_2 := R(1-e)$ gilt also $R = R_1 \times R_2$.

Lösung (8.18) Es sei $x = (x_i)_{i\in I}$.

(a) Genau dann ist x eine Einheit in R, wenn es ein Element $y = (y_i)_{i\in I}$ gibt mit $1 = xy = (x_iy_i)_{i\in I}$, also $x_iy_i = 1_i$ für alle $i \in I$. Das ist genau dann der Fall, wenn für jeden Index i die i-te Komponente x_i eine Einheit in R_i ist. Es gilt also

$$R^\times \;=\; \{(x_i)_{i\in I} \mid x_i \in R_i^\times\}.$$

(b) Genau dann ist x ein Nullteiler in R, wenn es ein Element $y = (y_i)_{i\in I} \neq 0$ gibt mit $0 = xy = (x_iy_i)_{i\in I}$, also $x_iy_i = 0_i$ für alle $i \in I$. Das ist genau dann der Fall, wenn es mindestens einen Index i_0 derart gibt, daß x_{i_0} ein Nullteiler in R_{i_0} ist. Gilt nämlich einerseits $y_{i_0} \neq 0$, so haben wir $x_{i_0}y_{i_0} = (xy)_{i_0} = 0_{i_0}$, so daß x_{i_0} ein Nullteiler in R_{i_0} ist. Ist umgekehrt x_{i_0} ein Nullteiler in R_{i_0}, so gibt es ein Element $y_{i_0} \neq 0$ mit $x_{i_0}y_{i_0} = 0$. Setzen wir nun $y_i := 0$ für $i \neq i_0$, so ist $y \neq 0$ mit $xy = 0$, so daß x ein Nullteiler in R ist.

(c) Genau dann ist x nilpotent, wenn es einen Exponenten m gibt mit $0 = x^m = (x_i^m)_{i\in I}$, also $x_i^m = 0_i$ für alle $i \in I$. Dies ist genau dann der Fall, wenn jede einzelne Komponente $x_i \in R_i$ nilpotent ist und wenn es eine obere Schranke für die Nilpotenzgrade dieser Elemente x_i gilt. (Das ist automatisch der Fall, wenn die Indexmenge I endlich ist.)

(d) Genau dann ist x idempotent, wenn $(x_i^2)_{i\in I} = x^2 = x = (x_i)_{i\in I}$ gilt, wenn also $x_i^2 = x_i$ für jeden Index i gilt, wenn also jede einzelne Komponente $x_i \in R_i$ idempotent ist.

Lösung (8.19) Für alle $x \in R$ gilt $2x = (2x)^3 = 8x^3 = 8x$ und damit $6x = 0$. Zum Nachweis der Kommutativität von R führen wir die angegebenen Schritte durch.

(a) Aus $x^n = 0$ mit $n \geq 4$ folgt $0 = x^n = x^{n-3} \cdot x^3 = x^{n-3} \cdot x = x^{n-2}$ und damit auch $x^{n-2} = 0$. Ist also $x \in R$ nilpotent, so gilt schon $x^3 = 0$, wegen $x^3 = x$ also $x = 0$.

(b) Es gelte $x^2 = x$. Für alle $y \in R$ erhalten wir dann

$$\begin{aligned}(xy - xyx)^2 &= xyxy - xyxyx - xyxxy + xyxxyx \\ &= xyxy - xyxyx - xyxy + xyxyx = 0\end{aligned}$$

sowie

$$\begin{aligned}(yx - xyx)^2 &= yxyx - yxxyx - xyxyx + xyxxyx \\ &= yxyx - yxyx - xyxyx + xyxyx = 0.\end{aligned}$$

(c) Es gelte $x^2 = x$. Ist $y \in R$ beliebig, so sind die Elemente $xy - xyx$ und $yx - xyx$ nach (b) beide nilpotent, nach (a) also beide gleich dem Nullement; das bedeutet $xy = xyx = yx$. Es gilt also $xy = yx$ für alle $y \in R$, und das bedeutet genau, daß x im Zentrum von R liegt.

(d) Es sei $x = r^2$ ein Quadrat in R. Dann gilt $x^2 = r^4 = r^2 = x$. Nach (c) liegt dann x im Zentrum von R.

(e) Es sei $x \in R$ beliebig. Dann erhalten wir einerseits $(x^2 + x)^2 = x^4 + 2x^3 + x^2 = x^4 + 2x + x^2$ und damit

$$2x = (x^2 + x)^2 - (x^2)^2 - x^2 \in Z,$$

wenn Z das Zentrum von R bezeichnet. Andererseits haben wir

$$\begin{aligned}x^2 + x &= (x^2 + x)^3 = x^6 + 3x^5 + 3x^4 + x^3 \\ &= x^2 + 2x + 3x^2 + x = 4x^2 + 3x,\end{aligned}$$

folglich $0 = 3x^2 + 3x$ und damit $3x = -x^2 - x^2 - x^2 \in Z$. Mit $3x$ und $2x$ liegt aber auch $x = (3x) - (2x)$ in Z. Da $x \in R$ beliebig war, liegt also jedes Element von R im Zentrum von R, und das bedeutet genau, daß R kommutativ ist.

Lösung (8.20) Wegen $x = x^4 = (-x)^4 = -x$ gilt $2 \cdot x = 0$ für alle $x \in R$. Gilt $x^n = 0$ mit $n \geq 5$, so gilt $0 = x^{n-4} \cdot x^4 = x^{n-4} \cdot x = x^{n-3}$. Ist also $x \in R$ nilpotent, so gilt schon $x^4 = 0$, wegen $x^4 = x$ also $x = 0$. Der Nachweis von (b) und (c) erfolgt wortwörtlich wie in der vorigen Aufgabe. Wir beweisen nun die restlichen Aussagen.

(d) Wegen (c) genügt es zu zeigen, daß jedes Element der Form $x^2 + x$ idempotent ist. Das trifft aber zu, denn $(x^2 + x)^2 = x^4 + 2x^3 + x^2 = x^4 + x^2 = x + x^2$.

(e) Diese Aussage folgt sofort aus (d), angewandt auf $x^2 + y$ statt auf x.

(f) Für alle $x, y \in R$ gilt

$$\begin{aligned}\underbrace{(x^2 + y)^2 + (x^2 + y)}_{\in Z} &= \underbrace{x^4}_{=x} + x^2y + yx^2 + y^2 + x^2 + y \\ &= \underbrace{x^2 + x}_{\in Z} + \underbrace{y^2 + y}_{\in Z} + x^2y + yx^2\end{aligned}$$

und damit $x^2y + yx^2 \in Z$, wenn Z das Zentrum des Rings R bezeichnet.

(g) Wegen (f) gilt $(x^2y + yx^2)x^2 = x^2(x^2y + yx^2)$. Ausmultipliziert bedeutet dies $x^2yx^2 + yx^4 = x^4y + x^2yx^2$, also $x^4y = yx^4$ und damit $xy = yx$.

Lösung (8.21) (1)⇒(2): Aus $ax = ay$ folgt $a(x - y) = 0$; wegen $a \neq 0$ nach (1) daher $x - y = 0$, also $x = y$.

(2)⇒(3): Sind x_1, x_2 Lösungen der Gleichung $ax = b$, so gilt $0 = b - b = ax_1 - ax_2 = a(x_1 - x_2)$ und wegen (2) dann $x_1 = x_2$.

(3)⇒(1): Es sei $a \neq 0$. Dann hat die Gleichung $ax = 0$ wegen (3) nur die Lösung $x = 0$; also ist a kein Nullteiler.

Lösung (8.22) (1)⇒(2). Wir beweisen die Aussage zunächst für den Fall einer endlichen Indexmenge I, also für einen Polynomring $R[X_1, \ldots, X_n]$ in einer endlichen Zahl n von Variablen, und benutzen dazu Induktion über n. Beim Induktionsanfang $n = 1$ argumentieren wir so: Sind $p, q \in R[X]$ von Null verschiedene Polynome, so ist der Grad von pq sie Summe der Grade von p und q, folglich ≥ 0, so daß pq nicht das Nullpolynom sein kann. Aus $p \neq 0$ und $q \neq 0$ folgt also $pq \neq 0$, und dies bedeutet, daß $R[X]$ nullteilerfrei ist. Nach Induktionsannahme sei $R[X_1, \ldots, X_n]$ nullteilerfrei; wenden wir erneut den Induktionsanfang an, so sehen wir, daß auch $R[X_1, \ldots, X_n][X_{n+1}] = R[X_1, \ldots, X_n, X_{n+1}]$ nullteilerfrei ist. Damit ist der Induktionsbeweis beendet. Nun sei $R[(X_i)_{i \in I}]$ ein Polynomring in einer beliebigen (möglicherweise unendlichen) Zahl von Variablen. Es seien $p, q \neq 0$ Elemente von $R[(X_i)_{i \in I}]$. Da in den endlich vielen Termen, die für p und q auftreten, nur endlich viele Variablen vorkommen, können wir p und q auch als Elemente eines Polynomrings in endlich vielen Variablen auffassen; nach dem bereits gezeigten Ergebnis gilt dann $pq \neq 0$. Damit sind wir fertig.

(2)⇒(3). Es seien $f, g \in R[[(X_i)_{i \in I}]]$ von Null verschiedene formale Potenzreihen, sagen wir $f = h_r + \text{Terme}$ der Ordnung größer als r und $g = k_s + \text{Terme}$ der Ordnung größer als s, wobei h_r homogen vom Grad r und k_s homogen vom Grad s ist und wobei h_r und k_s von Null verschieden sind. Dann sind h_r und k_s von Null verschiedene Polynome; wegen (2) gilt dann $h_r k_s \neq 0$, und hieraus folgt $fg \neq 0$. Damit ist (3) bewiesen.

(3)⇒(2). Es seien $p, q \neq 0$ Polynome in $R[(X_i)_{i \in I}]$. Da wir p und q als endliche formale Potenzreihen und damit als Elemente von $R[[(X_i)_{i \in I}]]$ auffassen können, gilt dann $pq \neq 0$ wegen (3), also auch $pq \neq 0$ in $R[(X_i)_{i \in I}]$. Damit ist (2) gezeigt.

(2)⇒(1). Es seien $r, s \neq 0$ Elemente von R. Da wir r und s als "konstante Polynome" und damit als Elemente von $R[(X_i)_{i \in I}]$ auffassen können, gilt dann $rs \neq 0$ wegen (2), also auch $rs \neq 0$ in R. Damit ist (1) gezeigt.

Lösung (8.23) (a) Wir gehen davon aus, einen Körper K mit genau drei verschiedenen Elementen 0, 1 und a vorgelegt zu haben. Dann sind die folgenden Teile der Additions- und der Multiplikationstafel von vornherein festgelegt.

$+$	0	1	a
0	0	1	a
1	1	$\star$	$\star$
a	a	$\star$	$\star$

$\cdot$	0	1	a
0	0	0	0
1	0	1	a
a	0	a	$\star$

Um die Multiplikationstafel zu komplettieren, bleibt nur die Wahl $a^2 = 1$, wegen $a \neq 1$ also $a = -1$. Damit haben wir auch die Gleichungen $a + 1 = 1 + a = 0$ in der Additionstafel. Um diese zu komplettieren, bleiben dann nur noch die Gleichungen $1 + 1 = a$ und $a + a = 1$. Es ist dann $1 + 1 = -1$ und damit $3 = 0$ in K. Die Addition und Multiplikation sind damit vollständig festgelegt:

$+$	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

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

Wir erkennen, daß dies (mit $a = 1 + 1 = 2$) genau die Rechenregeln im Körper $\mathbb{Z}_3$ sind; damit ist gezeigt, daß $K = \mathbb{Z}_3$ gilt.

(b) Wir gehen davon aus, einen Körper K mit genau vier verschiedenen Elementen 0, 1, a und b vorgelegt zu haben. Dann sind die folgenden Teile der Additions- und der Multiplikationstafel von vornherein festgelegt.

$+$	0	1	a	b
0	0	1	a	b
1	1	$\star$	$\star$	$\star$
a	a	$\star$	$\star$	$\star$
b	b	$\star$	$\star$	$\star$

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	$\star$	$\star$
b	0	b	$\star$	$\star$

Um die Multiplikationstafel zu komplettieren, gibt es nur zwei Möglichkeiten: entweder $a^2 = 1$ und $ab = b$ oder aber $a^2 = b$ und $ab = 1$. Wegen $a \neq 1$ und $b \neq 0$ ist $ab = b$ unmöglich; also haben wir $a^2 = b$ und $ab = 1$, folglich auch $ba = 1$ und damit $b^2 = a$. Damit ist die Multiplikationstafel vollständig festgelegt.

Wir erhalten nun $(a - b)(a + b) = a^2 - b^2 = b - a$, nach Division durch $a - b \neq 0$ also $a + b = -1$. Hieraus erhalten wir $1 + a = -b \neq 0$ sowie $1 + b = -a \neq 0$; das additive Inverse zu 1 kann also nur 1 selbst sein. Also gilt $1 + 1 = 0$, damit aber auch $a + a = a(1 + 1) = a \cdot 0 = 0$ und $b + b = b(1 + 1) = b \cdot 0 = 0$. Wegen $-1 = 1$ haben wir also $a + b = 1$, $a + 1 = b$ und $b + a = 1$. Die Addition und Multiplikation sind damit vollständig festgelegt:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Es kann also höchstens einen Körper mit vier Elementen geben. Daß die durch die obigen Verknüpfungstafeln definierte Struktur $(K, +, \cdot)$ tatsächlich ein Körper ist, bleibt nachzurechnen, was (insbesondere beim Überprüfen der Assoziativ- und Distributivgesetze) etwas mühselig, aber vollkommen komplikationslos ist.

Lösung (8.24) (a) Ja. (Die Bedingungen $0 \in G$, $-G \subseteq G$, $G + G \subseteq G$ und $GG \subseteq G$ rechnet man sofort nach.)

(b) Nein, denn $X^2 \in G$, aber $X \cdot X^2 = X^3 \notin G$.

(c) Nein, denn $X \in U$, aber $X \cdot X = X^2 \notin U$, so daß $UU \not\subseteq U$ gilt.

(d) Nein, denn aus $UU \not\subseteq U$ folgt erst recht $K[X]U \not\subseteq U$.

Lösung (8.25) (a) Es sei $g := \mathrm{ggT}(m, n)$. Es gibt dann $x, y \in \mathbb{Z}$ mit $xm + yn = g$ (lineare Darstellung des ggT). Hieraus folgt $g\mathbb{Z} = (xm + yn)\mathbb{Z} \subseteq m\mathbb{Z} + n\mathbb{Z}$. Umgekehrt gibt es (teilerfremde) Zahlen $a, b \in \mathbb{Z}$ mit $m = ga$ und $n = gb$. Es gilt dann $\mathbb{Z}m + \mathbb{Z}n = \mathbb{Z}ga + \mathbb{Z}gb \subseteq \mathbb{Z}g + \mathbb{Z}g = \mathbb{Z}g$. Insgesamt gilt $\mathbb{Z}m + \mathbb{Z}n = \mathbb{Z}g$, und das war zu zeigen.

(b) Es sei $k := \mathrm{kgV}(m, n)$. Jedes Vielfache von k ist sowohl ein Vielfaches von m als auch von n; also gilt $\mathbb{Z}k \subseteq \mathbb{Z}m \cap \mathbb{Z}n$. Umgekehrt ist jedes gemeinsame Vielfache von m und n ein Vielfaches von k; also gilt $\mathbb{Z}m \cap \mathbb{Z}n \subseteq \mathbb{Z}k$. Insgesamt gilt $\mathbb{Z}m \cap \mathbb{Z}n = \mathbb{Z}k$, und das war zu zeigen.

(c) Es gilt

$$\begin{aligned}(\mathbb{Z}m)(\mathbb{Z}n) &= \{(am)(bn) \mid a, b \in \mathbb{Z}\} \\ &= \{abmn \mid ab \in \mathbb{Z}\} \\ &= \{\lambda mn \mid \lambda \in \mathbb{Z}\} \;=\; \mathbb{Z}mn.\end{aligned}$$

(d) Es sei $g := \mathrm{ggT}(m, n)$; wir haben dann $m = ga$ und $n = gb$ mit teilerfremden Zahlen $a, b \in \mathbb{Z}$. Nun gelten die folgenden Äquivalenzen:

$$\begin{aligned}&x \in (\mathbb{Z}m) : (\mathbb{Z}n) \Leftrightarrow x(\mathbb{Z}n) \subseteq \mathbb{Z}m \Leftrightarrow xn \in \mathbb{Z}m \\ &\Leftrightarrow xgb \in \mathbb{Z}ga \Leftrightarrow xb \in \mathbb{Z}a \\ &\Leftrightarrow xb \text{ ist durch } a \text{ teilbar} \\ &\Leftrightarrow x \text{ ist durch } a \text{ teilbar} \Leftrightarrow x \in \mathbb{Z}a,\end{aligned}$$

wobei die vorletzte Äquivalenz gilt, weil a und b teilerfremd sind. Wegen $a = m/g$ ist damit die Behauptung gezeigt.

Lösung (8.26) Offensichtlich besteht $\langle\langle 2, X\rangle\rangle$ genau aus denjenigen Polynomen $a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$, deren Leitkoeffizient a_0 gerade ist. Wäre $\langle\langle 2, X\rangle\rangle$

ein Hauptideal, so gäbe es ein Polynom $p \in \mathbb{Z}[X]$ mit $\langle\langle 2, X\rangle\rangle = \langle\langle p\rangle\rangle$. Weil dann 2 ein Vielfaches von p sein müßte, folgt zwangsläufig $p(X) = 2$; aber $\langle\langle 2\rangle\rangle$ ist das Ideal derjenigen Polynome, für die *alle* Koeffizienten gerade sind.

Lösung (8.27) Das Ideal $I = \langle\langle XYZ - X^2,\ XY^2 + X^2Z\rangle\rangle$ besteht aus allen Polynomen der Form

$$(\star)\ \ p(X,Y,Z)\cdot(XYZ-X^2) + q(X,Y,Z)\cdot(XY^2+X^2Z)$$

mit $p, q \in K[X,Y,Z]$. Wir müssen also für jedes der angegebenen Polynome entscheiden, ob es sich (mit geeignet gewählten Polynomen p und q) in der Form $(\star)$ darstellen läßt.

(a) Es gilt $X^2Z^2 - YX^2 \in I$, denn

$$X^2Z^2-YX^2 \ = \ Y\cdot(\underbrace{XYZ-X^2}_{\in I})+Z\cdot(\underbrace{XY^2+X^2Z}_{\in I}) \ \in \ I.$$

(b) Es gilt $XY + YZ^2 \notin I$, denn dieses Polynom ist nicht durch X teilbar, während offensichtlich alle Polynome der Form $(\star)$ durch X teilbar sind.

(c) Wir nehmen an, es gelte $XY^3 - X^3 \in I$. Dann läßt sich $XY^3 - X^3$ in der Form $(\star)$ darstellen; es gibt also Polynome $p, q \in K[X,Y,Z]$ derart, daß nach Kürzen durch X die Gleichung

$$Y^3-X^2 \ = \ p(X,Y,Z)\cdot(YZ-X) + q(X,Y,Z)\cdot(Y^2+XZ)$$

gilt. Diese Gleichung bleibt bestehen, wenn wir mit einer neuen Variablen T speziell $(X,Y,Z) = (T^2,T,T)$ einsetzen; sie geht bei diesen Einsetzen über in $T^3 - T^4 = q(T^2,T,T)\cdot(T^2+T^3)$, nach Kürzen mit T also

$$T - T^2 \ = \ q(T^2,T,T)\cdot(1+T),$$

was bedeuten würde, daß im Polynomring $K[T]$ das Polynom $T - T^2 = T(1-T)$ durch das Polynom $1+T$ teilbar wäre (was aber nicht der Fall ist). Dieser Widerspruch zeigt, daß $XY^3 - X^3 \notin I$ gilt.

Lösung (8.28) (a) Für alle $x \in I$ gilt $xJ \subseteq IJ \subseteq I$ und damit $x \in (I:J)$. Für alle $x \in (I:J)$ und alle $y \in J$ gilt $xy \in xJ \subseteq I$.

(b) Es gelten die folgenden Äquivalenzen:

$$\begin{aligned} &x \in (\textstyle\bigcap_\alpha I_\alpha) : J \ \Leftrightarrow\ xJ \in \bigcap_\alpha I_\alpha \\ &\Leftrightarrow\ xJ \subseteq I_\alpha \text{ für alle } \alpha \\ &\Leftrightarrow\ x \in (I_\alpha : J) \text{ für alle } \alpha \\ &\Leftrightarrow\ x \in \textstyle\bigcap_\alpha (I_\alpha : J). \end{aligned}$$

(c) Es gelten die folgenden Äquivalenzen:

$$\begin{aligned} &x \in I : (\textstyle\sum_\alpha J_\alpha) \ \Leftrightarrow\ x(\sum_\alpha J_\alpha) \subseteq I \\ &\Leftrightarrow\ xJ_\alpha \subseteq I \text{ für alle } \alpha \\ &\Leftrightarrow\ x \in (I : J_\alpha) \text{ für alle } \alpha \\ &\Leftrightarrow\ x \in \textstyle\bigcap_\alpha (I : J_\alpha). \end{aligned}$$

(d) Es gelten die folgenden Äquivalenzen:

$$\begin{aligned} &x \in (I:J):K \ \Leftrightarrow\ xK \subseteq (I:J) \ \Leftrightarrow\ (xK)J \subseteq I \\ &\Leftrightarrow x(JK) \subseteq I \ \Leftrightarrow\ x \in (I:JK). \end{aligned}$$

Also gilt $(I:J):K = I:(JK)$. Vertauschung der Rollen von J und K zeigt, daß dann auch $(I:K):J = I:(KJ) = I:(JK)$ gilt.

(e) Es gelten die Äquivalenzen $x \in I : (I+J) \Leftrightarrow x(I+J) \subseteq I \Leftrightarrow xJ \subseteq I \Leftrightarrow x \in (I:J)$.

Lösung (8.29) Ist J ein Ideal von R mit $I \subseteq J \subseteq R$, so ist offensichtlich $\widehat{J} := J/I = \{x + I \mid x \in J\}$ ein Ideal von $\widehat{R} := R/I$. Ist umgekehrt $\widehat{J}$ ein Ideal von $\widehat{R}$, so ist $J := \pi^{-1}(\widehat{J}) = \{x \in R \mid \pi(x) \in \widehat{J}\}$ ein Ideal von R, denn für alle $x, y \in J$ und alle $x \in R$ gelten die Bedingungen $\pi(x+y) = \pi(x) + \pi(y) \in \widehat{J} + \widehat{J} \subseteq \widehat{J}$ und damit $x + y \in \pi^{-1}(\widehat{J})$ sowie $\pi(rx) = \pi(r)\pi(x) \in \widehat{R}\widehat{J} \subseteq \widehat{J}$ und damit $rx \in \pi^{-1}(\widehat{J})$.

Für ein Ideal J von R mit $I \subseteq J \subseteq R$ gilt

$$\begin{aligned} \pi^{-1}\big(\pi(J)\big) \ &= \ \{x \in R \mid \pi(x) \in \pi(J)\} \\ &= \ \{x \in R \mid x + I = y + I \text{ für ein } y \in J\} \\ &= \ \{x \in R \mid x \in J + I\} \ = \ J, \end{aligned}$$

wobei im letzten Schritt die Bedingung $I \subseteq J$ eingeht. Umgekehrt gilt für jedes Ideal $\widehat{J}$ von $\widehat{R}$ die Beziehung $\pi\big(\pi^{-1}(\widehat{J})\big) = \widehat{J}$, denn für jede surjektive Abbildung $f : X \to Y$ zwischen beliebigen Mengen X und Y und für jede Teilmenge $B \subseteq Y$ gilt $f\big(f^{-1}(B)\big) = B$. Damit ist gezeigt, daß $J \mapsto \pi(J)$ und $\widehat{J} \mapsto \pi^{-1}\big(\widehat{J}\big)$ zueinander inverse Bijektionen sind.

Ist J ein Ideal von R mit $I \subseteq J \subseteq R$, so ist ein wohldefinierter Ringhomomorphismus $f : (R/I) \to (R/J)$ gegeben durch $x+I \mapsto x+J$. Nach dem Homomorphiesatz gilt dann $R/J = \text{Bild}(f) \cong (R/I)/\text{Kern}(f) = (R/I)/(J/I)$. Damit ist alles gezeigt.

Lösung (8.30) (1)⇒(2): Es sei I ein von $\{0\}$ verschiedenes Ideal von R. In I gibt es dann ein Element $x \neq 0$. Da R ein Körper ist, ist x invertierbar. Für ein beliebiges Element $a \in R$ gilt dann $a = (ax^{-1})x \in RI \subseteq I$; also gilt $I = R$.

(2)⇒(3): Es sei $f : R \to S$ ein Ringhomomorphismus mit $f \not\equiv 0$. Dann ist der Kern von f ein von R verschiedenes Ideal von R, nach Voraussetzung also $\{0\}$. Die Bedingung $\text{Kern}(f) = \{0\}$ bedeutet aber genau, daß f injektiv ist.

(3)⇒(1): Es sei $x \in R$ ein nichtinvertierbares Element. Dann ist $I := \langle\langle x\rangle\rangle = Rx$ ein echtes Ideal von R. Der kanonische Homomorphismus $f : R \to R/I$ ist daher nicht die Nullabbildung, nach Voraussetzung also injektiv; also ist $I = \text{Kern}(f) = \{0\}$, und das bedeutet $x = 0$. Also ist 0 das einzige nichtinvertierbare Element von R, und das heißt, daß R ein Körper ist.

Lösung (8.31) Es sei $R := K[X_1, \ldots, X_n]$; wir wollen zeigen, daß $I := \{p \in R \mid p(a_1, \ldots, a_n) = 0\}$ ein maximales Ideal von R ist.

Erster Beweis. Es sei $q \in R \backslash I$; dann gilt $q(X_1, \ldots, X_n) = q_0 + \sum_i q_i(X_i - a_i) + \sum_{i<j} q_{ij}(X_i - a_i)(X_j - a_j) + \cdots$ mit $q_0 \neq 0$. Dann liegt $q - q_0$ in I; folglich gilt $\langle\langle I, q\rangle\rangle = \langle\langle I, q_0\rangle\rangle = R$, wobei die letzte Gleichung gilt, weil ein Ideal, das eine Einheit enthält (in unserem Fall q_0) zwangsläufig der ganze Ring ist. Diese Überlegung zeigt, daß zwischen I und R kein weiteres Ideal mehr enthalten ist; also ist I ein maximales Ideal.

Zweiter Beweis. Wir betrachten den Auswertungshomomorphismus $f : R \to K$ mit $f(p) := p(a_1, \ldots, a_n)$. Da f surjektiv ist, gilt nach dem Homomorphiesatz die Isomorphie $K \cong R/\mathrm{Kern}(f) = R/I$. Also ist R/I ein Körper, I daher ein maximales Ideal.

Lösung (8.32) Es sei $f : \mathbb{Z} \to \mathbb{Z}$ ein Ringhomomorphismus. Dann ist f erst recht ein Endomorphismus der additiven Gruppe $(\mathbb{Z}, +)$ und damit nach Aufgabe (6.8) eine Abbildung der Form $f(x) = kx$ mit einer festen Zahl $k \in \mathbb{Z}$. Als Ringhomomorphismus muß f aber auch die Multiplikation respektieren, es muß also $f(xy) = f(x)f(y)$ und damit $kxy = (kx)(ky) = k^2xy$ für alle $x, y \in \mathbb{Z}$ gelten, und dies ist genau dann der Fall, wenn $k^2 = k$ gilt, also $k = 0$ oder $k = 1$. Die einzigen Ringhomomorphismen $f : \mathbb{Z} \to \mathbb{Z}$ sind also die Nullabbildung und die identische Abbildung.

Lösung (8.33) Die Abbildung f_a ist zunächst wohldefiniert, denn aus $[x] = [x']$ folgt $[ax] = [ax']$. (Ist $x - x'$ durch n teilbar, dann auch $ax - ax' = a(x - x')$.) Die Abbildung f_a respektiert ferner die Addition, denn $f_a([x] + [y]) = f_a([x + y]) = [a(x + y)] = [ax + ay] = [ax]+[ay] = f_a([x])+f_a([y])$. Für die Multiplikation erhalten wir einerseits $f_a([x]\cdot[y]) = f_a([x\cdot y]) = [axy]$, andererseits $f_a([x])\cdot f_a([y]) = [ax]\cdot[ay] = [a^2xy]$. Also ist f_a genau dann ein Ringhomomorphismus, wenn $[axy] = [a^2xy]$ für alle $x, y \in \mathbb{Z}$ und damit $[a] = [a^2]$ gilt. Dies ist genau der Fall für $[a] = 0$ und $[a] = 1$.

Lösung (8.34) (a) Ja, denn aus $xy = 1$ folgt $1 = f(1) = f(xy) = f(x)f(y)$.

(b) Nein. Ist beispielsweise x_0 eine beliebige reelle Zahl, so bildet der Auswertungshomomorphismus $f : C(\mathbb{R}) \to \mathbb{R}$ mit $f(\varphi) := \varphi(x_0)$ Nullteiler nicht zwangsläufig auf Nullteiler ab. (Ist φ eine stetige Funktion mit $f(x_0) \neq 0$, die auf einem Teilintervall $J \subseteq \mathbb{R}$ identisch Null ist, so ist φ ein Nullteiler in $C(\mathbb{R})$, aber $f(\varphi) = \varphi(x_0) \neq 0$ ist kein Nullteiler in $\mathbb{R}$.)

(c) Ja, denn aus $x^n = 0$ folgt $f(x)^n = f(x^n) = f(0) = 0$.

(d) Ja, denn aus $x^2 = x$ folgt $f(x)^2 = f(x^2) = f(x)$.

Lösung (8.35) (a) Wähle $R = \mathbb{Z}$, $S = 2\mathbb{Z}$ (Menge der geraden Zahlen) und $f \equiv 0$.

(b) Man kann etwa $R = S = \mathbb{Z}$ sowie $f \equiv 0$ wählen. Ein etwas interessanteres Beispiel erhalten wir mit $R = \mathbb{R}$ und $S = \mathbb{R}^{2\times 2}$, wenn $f : R \to S$ definiert ist durch

$$f(a) \;:=\; \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}.$$

(c) Wir setzen $e := f(1_R)$ und behaupten, daß e ein multiplikatives Neutralelement in S ist. Dazu sei $s \in S$ beliebig. Da f surjektiv ist, gibt es ein $r \in R$ mit $f(r) = s$. Wir erhalten dann $e\cdot s = f(1_R)f(r) = f(1_R\cdot r) = f(r) = s$ und $s \cdot e = f(r)f(1_R) = f(r \cdot 1_R) = f(r) = s$. Also gilt $e \cdot s = s \cdot e = s$ für alle $s \in S$, so daß e als multiplikatives Neutralelement für S nachgewiesen ist.

(d) Sind r_1, r_2 zueinander inverse Einheiten in R, so gilt $r_1r_2 = r_2r_1 = 1_R$. Es folgen dann die Gleichungen $f(r_1)f(r_2) = f(r_1r_2) = f(1_R) = 1_S$ und $f(r_2)f(r_1) = f(r_2r_1) = f(1_R) = 1_S$, so daß $f(r_1)$ und $f(r_2)$ zueinander inverse Einheiten in S sind.

Lösung (8.36) (a) Für $x, y \in I$ gilt $f(x) + f(y) = f(x + y) \in f(I)$; also gilt $f(I) + f(I) \subseteq f(I)$. Für $x \in I$ und $r \in R$ gilt $f(r)f(x) = f(rx) \in f(I)$; also gilt $f(R)f(I) \subseteq f(I)$. Damit ist gezeigt, daß $f(I)$ ein Ideal von $f(R)$ ist. Wählen wir $R := \mathbb{Z}$, $S := \mathbb{Q}$, $I := 2\mathbb{Z}$ und definieren wir $f : R \to S$ durch $f(x) = x$, so ist $F(I) = 2\mathbb{Z}$ kein Ideal von $S = \mathbb{Q}$.

(b) Für ein gegebenes Ideal J von S sei $I := f^{-1}(J)$. Für $x, y \in I$ gilt $f(x + y) = f(x) + f(y) \in J + J \subseteq J$ und damit $x + y \in I$; also gilt $I + I \subseteq I$. Für $x \in I$ und $r \in R$ gilt $f(rx) = f(r)f(x) \in SJ \subseteq J$ und damit $rx \in I$; also gilt $RI \subseteq I$. Damit ist gezeigt, daß I ein Ideal von R ist.

Ist J maximal, so muß I nicht zwangsläufig maximal sein. Betrachte etwa die Einbettungsabbildung $f : \mathbb{Z} \to \mathbb{Q}$ mit $f(x) = x$ für alle $x \in \mathbb{Z}$. Das Ideal $J := \{0\}$ ist ein maximales Ideal von $\mathbb{Q}$, aber $f^{-1}(J) = \{0\}$ ist kein maximales Ideal von $\mathbb{Z}$.

Lösung (8.37) Wir fragen zunächst allgemein, wie ein Ringisomorphismus $f : \mathbb{Z}_m \to \mathbb{Z}_n$ aussehen kann, und wählen dazu $a \in \mathbb{N}$ mit $f([1]_m) = [a]_n$. Für alle $x \in \mathbb{N}$ gilt dann

$$\begin{aligned} f([x]_m) &= f\big(\underbrace{[1]_m + \cdots + [1]_m}_{x \text{ mal}}\big) = \underbrace{f([1]_m) + \cdots + f([1]_m)}_{x \text{ mal}} \\ &= \underbrace{[a]_n + \cdots + [a]_n}_{x \text{ mal}} \;=\; x \cdot [a]_n \;=\; [ax]_n. \end{aligned}$$

Diese Abbildung ist genau dann wohldefiniert, wenn der Ausdruck $[ax]_n$ nur von $[x]_m$ und nicht von dem speziellen Repräsentanten x abhängt, was genau dann der Fall ist, wenn am durch n teilbar ist. Bisher haben wir nur ausgenutzt, daß $f : \mathbb{Z}_m \to \mathbb{Z}_n$ ein Homomorphismus abelscher Gruppen ist. Soll f sogar ein Ringhomomorphismus (also auch multiplikativ) sein, so muß für alle $x, y \in \mathbb{Z}$ die Bedingung $f([xy]_m) = f([x]_m[y]_m) = f([x]_m)f([y]_m)$ gelten, also $[axy]_n = [ax]_n[ay]_n = [a^2xy]_n$ und damit

$[0] = [(a^2 - a)xy]_n$. Dies ist genau dann der Fall, wenn $[a]_n^2 = [a]_n$ gilt, wenn also a modulo n idempotent ist. Damit haben wir das folgende Ergebnis: Die Ringhomomorphismen $f : \mathbb{Z}_m \to \mathbb{Z}_n$ sind genau die Abbildungen der Form $[x]_m \to [a]_n[x]_n$ mit einem idempotenten Element $[a]_n \in \mathbb{Z}_n$ derart, daß am durch n teilbar ist.

Wir machen eine weitere Vorbemerkung: Ist U ein Unterring des *endlichen* Rings R, so ist insbesondere U eine Untergruppe der endlichen additiven Gruppe $(R, +)$, nach dem Satz von Lagrange daher $|U|$ ein Teiler von $|R|$.

(a) Ist $f : \mathbb{Z}_m \to \mathbb{Z}_n$ surjektiv, so gilt $\mathbb{Z}_n \cong \mathbb{Z}_m/\mathrm{Kern}\ (\mathrm{f})$ nach dem Homomorphiesatz, folglich $|\mathbb{Z}_n| = |\mathbb{Z}_m/\mathrm{Kern}(f)| = |\mathbb{Z}_m|/|\mathrm{Kern}(f)|$, und das bedeutet $n \cdot |\mathrm{Kern}(f)| = m$. Also ist n ein Teiler von m. Ist dies umgekehrt der Fall, so ist durch $[x]_m \mapsto [x]_n$ eine Abbildung $f : \mathbb{Z}_m \to \mathbb{Z}_n$ wohldefiniert, die dann offensichtlich ein surjektiver Ringhomomorphismus ist, denn wir können $a = 1$ im der obigen Überlegung wählen.

(b) Ist $f : \mathbb{Z}_m \to \mathbb{Z}_n$ injektiv, so ist $f(\mathbb{Z}_m) \cong \mathbb{Z}_m$ ein Teilring von $\mathbb{Z}_n$, nach der Vorbemerkung folglich m ein Teiler von n, sagen wir $n = bm$. Nach der obigen Überlegung ist f von der Form $[x]_m \mapsto [ax]_n$, wobei am durch $n = bm$ teilbar ist, folglich a durch b teilbar, sagen wir $a = \lambda b$. Es gelten dann die folgenden Äquivalenzen:

$$\begin{aligned} f \text{ injektiv} &\Leftrightarrow \text{aus } n \mid ax \text{ folgt } m \mid x \\ &\Leftrightarrow \text{aus } bm \mid \lambda bx \text{ folgt } m \mid x \\ &\Leftrightarrow \text{aus } m \mid \lambda x \text{ folgt } m \mid x \\ &\Leftrightarrow m \text{ und } \lambda \text{ sind teilerfremd.} \end{aligned}$$

Da $[a]_n$ idempotent ist, ist $a^2 = a(a-1) = \lambda b(\lambda b - 1)$ durch $n = bm$ teilbar, also $\lambda(\lambda b - 1)$ durch m teilbar, folglich (da m und λ teilerfremd sind) auch $\lambda b - 1$ durch m teilbar, woraus folgt, daß b und m teilerfremd sind. Gibt es also einen surjektiven Ringhomomorphismus $f : \mathbb{Z}_m \to \mathbb{Z}_n$, so gilt $n = bm$ mit $\mathrm{ggT}(b, m) = 1$. Gilt umgekehrt $n = bm$ mit $\mathrm{ggT}(b, m) = 1$, so gehört zu der Faktorisierung $n = bm$ ein idempotentes Element $[a]_n$ (vergleiche Aufgabe (1.3)) derart, daß $[x]_m \mapsto [ax]_n$ ein (offensichtlich injektiver) Ringhomomorphismus ist.

Lösung (8.38) (a) Die Surjektivität von $f : \mathbb{Z} \to \prod_{k=1}^{N} \mathbb{Z}_{p_k}$ ist genau die Aussage des Chinesischen Restsatzes, daß für alle Zahlen $x_1, \ldots, x_N \in \mathbb{Z}$ die Kongruenzen $x \equiv x_k \bmod p_k$ für $1 \le k \le N$ simultan lösbar sind. Der Kern von f besteht aus allen Vielfachen von $p_1 p_2 \cdots p_N$, ist also nicht $\{0\}$; daher ist f nicht injektiv.

(b) Ein Zahl liegt genau dann im Kern von $f : \mathbb{Z} \to \prod_{k=1}^{\infty} \mathbb{Z}_{p_k}$, wenn sie durch sämtliche Primzahlen teilbar ist; diese Bedingung erfüllt nur die Zahl Null. Also ist f injektiv. Dagegen ist f nicht surjektiv, denn hat $x \in \mathbb{Z}$ die Primfaktorzerlegung $x = p_{i_1}^{m_1} \cdots p_{i_k}^{m_k}$, so sind die Komponenten $i_1, \ldots, i_k$ der Folge $f(x)$ gleich Null; insbesondere liegen also im Bild von f nur Folgen mit Nullen, woraus sich die Nichtsurjektivität ergibt.

Lösung (8.39) Zum Nachweis der Wohldefiniertheit von Φ müssen wir zeigen, daß die Definition von $\Phi([x]_{mn})$ nicht von der Wahl des Repräsentanten $x \in \mathbb{Z}$ abhängt. Gilt $[x]_{mn} = [y]_{mn}$, so ist $x - y$ durch mn teilbar. Dann ist $x - y$ aber sowohl durch m als auch durch n teilbar, so daß die Beziehungen $[x]_m = [y]_m$ und $[x]_n = [y]_n$ gelten. Damit ist die Wohldefiniertheit von Φ gezeigt. Daß Φ die Addition und die Multiplikation respektiert, ist offensichtlich; ebenso, daß Φ das multiplikative Neutralelement von $\mathbb{Z}_{mn}$ auf das multiplikative Neutralelement von $\mathbb{Z}_m \times \mathbb{Z}_n$ abbildet. Also ist Φ ein Homomorphismus unitärer Ringe.

Genau dann liegt $[x]_{mn}$ im Kern von f, wenn die Bedingungen $[x]_m = [0]_m$ und $[x]_n = [0]_n$ gelten, wenn also x sowohl durch m als auch durch n teilbar ist, wenn also x ein gemeinsames Vielfaches von m und n ist. Dies ist genau dann der Fall, wenn x durch das kgV von m und n teilbar ist. Der Kern von f ist also $\{[x]_{mn} \mid x \in \mathbb{Z} \cdot \mathrm{kgV}(m, n)\}$.

Wegen $|\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n| = |\mathbb{Z}_m \times \mathbb{Z}_n|$ ist die Abbildung f genau dann surjektiv, wenn sie injektiv ist. Dies ist genau dann der Fall, wenn der Kern von f nur aus $[0]_{mn}$ besteht, wenn also $\mathrm{kgV}(m, n) = mn$ gilt. Dies ist genau dann der Fall, wenn m und n teilerfremd sind.

Lösung (8.40) Wir müssen die vier Möglichkeiten $(a, b) = (\pm 1, \pm 1)$ durchgehen.

• Im Fall $(a, b) = (0, 0)$ haben wir $p(X) = X^2 = X \cdot X$. Da dieses Polynom reduzibel ist, ist von vornherein klar, daß R kein Körper sein kann. Dies folgt auch aus der Multiplikationstafel (bei der wir systematisch modulo $p(X)$ rechnen, aber der Bequemlichkeit halber keine Äquivalenzklassennotation verwenden, also etwa einfach $X + 1$ statt $[X + 1]$ schreiben).

$\cdot$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	0	X
$X+1$	0	$X+1$	X	1

• Im Fall $(a, b) = (0, 1)$ haben wir $p(X) = X^2 + 1 = (X + 1)^2$. Da dieses Polynom reduzibel ist, ist von vornherein klar, daß R kein Körper sein kann. Dies folgt auch wieder sofort aus der Multiplikationstafel.

$\cdot$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	1	$X+1$
$X+1$	0	$X+1$	$X+1$	0

• Im Fall $(a, b) = (1, 0)$ haben wir $p(X) = X^2 + X = X(X + 1)$. Da dieses Polynom reduzibel ist, ist von vornherein klar, daß R kein Körper sein kann. Dies folgt auch wieder sofort aus der Multiplikationstafel.

$\cdot$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	X	0
$X+1$	0	$X+1$	0	$X+1$

• Im Fall $(a, b) = (1, 1)$ haben wir $p(X) = X^2+X+1$. Dieses Polynom ist irreduzibel, so daß R ein Körper sein muß. Dies folgt auch aus der Multiplikationstafel.

$\cdot$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	$X+1$	1
$X+1$	0	$X+1$	1	X

Wir erkennen jetzt den Körper aus Aufgabe (8.23)(b) wieder. Es ist also nicht notwendig, in (8.23)(b) die Gültigkeit der Ringaxiome (insbesondere der Assoziativ- und Distributivgesetze) mühsam nachzurechnen. Diese ergibt sich jetzt vielmehr daraus, daß sich die Ringaxiome von einem Ring R (hier $\mathbb{Z}_2[X]$) unmittelbar auf einen Quotientenring R/I (hier mit $I = \langle\langle x^2 + ax + b\rangle\rangle$) übertragen.