# Übungsblatt 2: Ringe und Körper

## 1. RINGE

**1.1.** Zeigen Sie, dass die Menge $R^{n\times n}$ der $n\times n$-Matrizen über einem Ring $R$ mit den üblichen Operationen einen Ring bildet.

**Lösungshinweise: —** *Man kopiert die Beweise zur Assoziativität, Distributivität und (bei +) Kommutativität der Matrixaddition und -multiplikation aus der linearen Algebra. Das neutrale Element ist die Null- bzw- die Einheitsmatrix, usw...* **—**

Sei $(A,+)$ eine abelsche Gruppe und $\mathrm{End}(A)$ die Menge der Endomorphismen von $A$. Hierauf sei $\circ$ wie üblich die Komposition von Abbildungen. Wir definieren zu $f,g\in\mathrm{End}(A)$ die Summe $f+g\in\mathrm{End}(A)$ durch $(f+g)(a):=f(a)+g(a)$ für alle $a\in A$.

**1.2.** Zeigen Sie, dass $(\mathrm{End}(A),+,\circ)$ ein Ring ist.

**Lösungshinweise: —** *Man prüft die Ringaxiome direkt durch Rechnung nach...* **—**

*Bemerkung:* Dies verallgemeinert die erste Aufgabe. Für einen $K$-Vektorraum $V$ der Dimension $n$ ist der Ring $(\mathrm{End}_K(V),+,\circ)$ isormorph zum obigen Matrizenring $K^{n\times n}$.

Analog zum Satz von Cayley für Gruppen erhält man:

**Satz 1.1.** *Jeder Ring $(R,+,\cdot)$ ist isomorph zu einem Unterring des Endomorphismenrings $(\mathrm{End}(A),+,\circ)$ einer geeigneten abelschen Gruppe $(A,+)$. Hierbei kann $(A,+)=(R,+)$ gewählt werden.*

Dies ermöglicht oft die bequeme Konstruktion von Ringen als Unterringe.

**V 1.3.** In $\mathbb{C}^{2\times2}$ betrachten wir die vier Matrizen

$$E=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\quad I=\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right),\quad J=\left(\begin{smallmatrix}0&i\\i&0\end{smallmatrix}\right),\quad K=\left(\begin{smallmatrix}i&0\\0&-i\end{smallmatrix}\right).$$

(a) Zeigen Sie, dass diese bezüglich der Matrixmultiplikation eine endliche Gruppe $Q$ erzeugen, die *Quaternionengruppe*. Bestimmen Sie die Anzahl der Elemente von $Q$ und stellen Sie die Gruppentafel auf. Ist $Q$ kommutativ?

(b) Warum ist der von $Q$ in $\mathbb{C}^{2\times2}$ aufgespannte $\mathbb{R}$-Vektorraum

$$\mathbb{H}=\{\,aE+bI+cJ+dK : a,b,c,d\in\mathbb{R}\,\}$$

ein Unterring des Matrizenrings $\mathbb{C}^{2\times2}$?

(c) Welche Elemente in $\mathbb{H}$ sind invertierbar? Ist $\mathbb{H}$ ein Divisionsring (= Schiefkörper)? Ist $\mathbb{H}$ sogar ein Körper?

(d) Ist $S^3=\{\,aE+bI+cJ+dK : a^2+b^2+c^2+d^2=1;\ a,b,c,d\in\mathbb{R}\,\}$ eine Untergruppe von $\mathbb{H}^\times$?

(e) Wie sehen die Lösungen der Gleichung $x^2+1=0$ in $\mathbb{H}$ aus?

**Lösungshinweise: —**

(a) *Multipliziert man die Elemente paarweise zusammen, erhält man neben $E,I,J,K$ noch die vier Elemente $-E,-I,-J,-K$ und damit auch schon die ganze Gruppentafel. Die Formeln $IJ=K, JK=I, KI=J, I^2=J^2=K^2=-E$ reichen auch schon aus und sind "einfach" zu merken. Da $IJ=K$, aber $JI=-K$, ist $Q$ nicht kommutativ.*

(b) *Betrachtet man $\mathbb{H}$ als Vektorraum, so ist dieser offenbar eine additive Gruppe. Bei der Multiplikation der Elemente $E,I,J,K$ entstehen bis auf ihre additiven Inversen keine neuen Elemente, so dass man auch beim Multiplizieren nicht aus $\mathbb{H}$ herausfällt. Da das neutrale Element $E\in\mathbb{H}$ enthalten ist, ist $\mathbb{H}$ ein Unterring von $\mathbb{C}^{2\times2}$.*

(c) *Die Linearkombination* $aE+bI+cJ+dK$ *lässt sich auch in der Form* $\left(\begin{smallmatrix} a+di & b+ci \\ -b+ci & a-di \end{smallmatrix}\right)$ *schreiben. Bildet man hier die Determinante, so ergibt sich die Zahl* $a^2+b^2+c^2+d^2$*. Dies ist aber nicht* 0*, es sei denn es gilt* $a=b=c=d=0$*. Die Inverse ist gegeben durch* $\frac{1}{a^2+b^2+c^2+d^2}\left(\begin{smallmatrix} a-di & -b-ci \\ b-ci & a+di \end{smallmatrix}\right)$ *und ist damit wieder ein Element in* $\mathbb{H}$*. Damit ist* $\mathbb{H}$ *ein Divisionsring, aber offenbar kein Körper, da die Multiplikation nicht kommutativ ist.*

(d) $S^3$ *sind nach (c) genau die Matrizen mit Determinante* 1*. Diese bilden nach dem Multiplikationssatz für Determinanten eine Untergruppe. Damit hat man gezeigt, dass man die 3-Sphäre* $S^3$ *mit einer Gruppenstruktur ausstatten kann, so wie es auch für die* $S^1$ *möglich ist.*

(e) *Quadrieren der Matrix aus Teil (c) ergibt* $\left(\begin{smallmatrix} a^2-d^2+2adi-b^2-c^2 & 2ab+2aci \\ -2ab+2aci & a^2-d^2-2adi-b^2-c^2 \end{smallmatrix}\right)$*. Dies soll gleich* $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ *sein, so dass aus den Nebendiagonaleinträgen folgt:* $a=0$ *oder* $b=c=0, a\neq 0$*. Der zweite Fall führt sofort zu* $2ad=0$*, also* $d=0$ *und damit auf einen Widerspruch. Im Fall* $a=0$*, muss* $b^2+c^2+d^2=1$ *sein, um die Gleichung zu erfüllen. Damit lösen alle "rein imaginären" Elemente mit Betrag* 1 *die Gleichung* $x^2+1=0$*.*

—

**S 1.4.** (4 Punkte) Seien $R_1,\dots,R_n$ Ringe. Zeigen Sie, dass $R=R_1\times\cdots\times R_n$ mit der komponentenweisen Addition und Multiplikation ein Ring ist. Bestimmen Sie die Gruppe $R^\times$ der invertierbaren Elemente ausgehend von den Gruppen $R_1^\times,\dots,R_n^\times$. Bestimmen Sie die Nullteiler in $R$ ausgehend von den Nullteilern in $R_1,\dots,R_n$.

**Lösungshinweise: —** *Dass R einen Ring bildet, rechnet man direkt nach.*
*Damit ein Element* $r=(r_1,\dots,r_n)\in R$ *linksseitig invertierbar ist, muss es ein* $s=(s_1,\dots,s_n)\in R$ *geben, so dass* $sr=(s_1r_1,\dots,s_nr_n)=(1,\dots,1)$ *ist. Damit sind aber alle Einträge jeweils linksseitig invertierbar. Sind andererseits alle Einträge linksseitig invertierbar, so findet man auf diese Weise auch ein Linksinverses in R. Dies prüft man ebenso für die Rechtsinvertierbarkeit. Damit folgt* $R^\times=R_1^\times\times\cdots\times R_n^\times$*.*
*Sei* $N_i$ *die Menge aller Linksnullteiler in* $R_i$ *vereinigt mit* 0*. Sei* $a=(a_1,\dots,a_n)\in R$*, so dass es ein* $i\leq n$ *mit* $a_i\in N_i$ *gibt, dann gibt es* $b_i\in R_i\backslash\{0\}$ *mit* $a_ib_i=0$*. Damit ist* $a(0,\dots,0,b_i,0,\dots,0)=(0,\dots,0)$*, also a ein Linksnullteiler oder* $a=(0,\dots,0)$*. Ist andererseits* $a\in R$ *ein Linksnullteiler, gibt es also ein* $b\in R\backslash\{(0,\dots,0)\}$ *mit* $ab=(0,\dots,0)$*, so muss es ein* $i\leq n$ *mit* $b_i\neq 0$ *geben und damit folgt aus* $a_ib_i=0$*, dass* $a_i\in N_i$ *liegt. Damit ist also die Menge aller Nullteiler in R gegeben durch die Elemente* $(a_1,\dots,a_n)\neq(0,\dots,0)$*, so dass eines der Elemente* $a_i$ *in* $N_i$ *liegt. Für Rechtsnullteiler gilt ein analoges Ergebnis.*
*Insbesondere hat es in Produktringen immer Nullteiler der Form* $(a,0,\dots,0)$*, selbst wenn R selbst keine Nullteiler besitzt.* —

## 2. IDEALE

**V 2.1.** Sei $f\colon R\to S$ ein Epimorphismus von Ringen. Zeigen Sie:

(a) Das Bild eines Ideals $\mathfrak{a}\subset R$ ist wieder ein Ideal $f(\mathfrak{a})\subset S$.

(b) Das Urbild eines Ideal $\mathfrak{b}\subset S$ ist wieder ein Ideal $f^{-1}(\mathfrak{b})\subset R$.

Diese Zuordnung stiftet eine Bijektion zwischen den Idealen $\mathfrak{a}\subset R$, die $\ker(f)$ enthalten, und den Idealen $\mathfrak{b}\subset S$.

(c) Für jedes Ideal $\mathfrak{a}\lhd R$ mit $\mathfrak{a}\supset\ker(f)$ gilt $R/\mathfrak{a}\cong S/f(\mathfrak{a})$.

**Lösungshinweise: —**

(a) *Sei* $s\in S$*. Wegen der Surjektivität von f gibt es ein* $r\in R$ *mit* $f(r)=s$*. Sei* $a\in\mathfrak{a}$*, dann ist* $sf(a)=f(r)f(a)=f(ra)\in f(\mathfrak{a})$*, da* $\mathfrak{a}$ *ein Ideal ist. Der Rest der Eigenschaften folgt sofort aus den Homomorphieeigenschaften von f.*

(b) *Seien* $b_1,b_2\in f^{-1}(\mathfrak{b})$*, d.h.* $f(b_i)\in\mathfrak{b}$*. Dann ist* $f(b_1-b_2)=f(b_1)-f(b_2)\in\mathfrak{b}-\mathfrak{b}=\mathfrak{b}$*. Also ist* $b_1-b_2\in f^{-1}(\mathfrak{b})$*. Sei nun* $r\in R, b\in f^{-1}(\mathfrak{b})$*, dann ist* $f(rb)=f(r)f(b)\in S\cdot\mathfrak{b}\subset\mathfrak{b}$*, also* $rb\in f^{-1}(\mathfrak{b})$*.*

(c) *Schalten wir hinter die Abbildung $f$ die Quotientenabbildung $\rho : S \to S/f(\mathfrak{a})$, so erhalten wir eine Abbildung $g = \rho \circ f$, die $\mathfrak{a}$ als Kern besitz. Denn offenbar ist $\mathfrak{a} \subset \ker(g)$ und aus $g(r) = 0$ folgt $f(r) \in \ker(\rho) = f(\mathfrak{a})$, also $f(r) = f(a)$ für ein $a \in \mathfrak{a}$. Das liefert $f(r-a) = 0$, bzw. $r-a \in \ker(f)$. Wegen $\ker(f) \subset \mathfrak{a}$ folgt $r \in \mathfrak{a}$.*
*Damit ist aber nach dem Homomorphiesatz der Ring $R/\mathfrak{a}$ isomorph zu $S/f(\mathfrak{a})$.*

—

**S 2.2.** (3 Punkte) Sei $R$ ein Ring und $I, J$ Ideale in $R$. Zeigen Sie, dass $I \cap J$ und $I + J$ wieder Ideale sind. Ist $I \cup J$ im Allgemeinen wieder ein Ideal?

**Lösungshinweise: —** *Man rechnet direkt nach, dass $I \cap J$ und $I + J$ abelsche Gruppen bezüglich der Addition sind. Für $I \cup J$ geht schon diese Eigenschaft verloren, wie man z.B. im Fall $I = 2\mathbb{Z}, J = 3\mathbb{Z}$ sieht, da $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$ gilt.*
*Seien nun $i \in I$, $j \in J$ und $r \in R$. Dann ist $r(i + j) = ri + rj \in RI + RJ \subset I + J$, nach Definition der Idealeigenschaft. Ebenso gilt für $a \in I \cap J$, dass $ra \in RI \subset I$ und $ra \in RJ \subset J$, also $ra \in I \cap J$ erfüllt ist. Damit sind die beiden ersten Mengen Ideale.* —

**V 2.3.** Sei $R$ ein Ring und $R^{2\times 2}$ der $2 \times 2$-Matrizenring über $R$. Sei weiter $I$ ein Ideal in $R$. Zeigen Sie, dass $J = \left(\begin{smallmatrix} I & I \\ I & I \end{smallmatrix}\right) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : a, b, c, d \in I \right\}$ ein Ideal von $R^{2\times 2}$ ist. Ist der Quotientenring $R^{2\times 2}/J$ ebenfalls ein Matrizenring?

**Lösungshinweise: —** *Wir verwenden die Komplexnotation. Es gilt $\left(\begin{smallmatrix} R & R \\ R & R \end{smallmatrix}\right)\left(\begin{smallmatrix} I & I \\ I & I \end{smallmatrix}\right) = \left(\begin{smallmatrix} RI+RI & RI+RI \\ RI+RI & RI+RI \end{smallmatrix}\right) \subset \left(\begin{smallmatrix} I & I \\ I & I \end{smallmatrix}\right)$ und ebenso $\left(\begin{smallmatrix} I & I \\ I & I \end{smallmatrix}\right)\left(\begin{smallmatrix} R & R \\ R & R \end{smallmatrix}\right) \subset \left(\begin{smallmatrix} I & I \\ I & I \end{smallmatrix}\right)$, also ist $J$ ein Ideal. Die Elemente in $R^{2\times 2}/J$ sind Restklassen der Form $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) + \left(\begin{smallmatrix} I & I \\ I & I \end{smallmatrix}\right) = \left(\begin{smallmatrix} a+I & b+I \\ c+I & d+I \end{smallmatrix}\right) \in \left(\begin{smallmatrix} R/I & R/I \\ R/I & R/I \end{smallmatrix}\right)$, sind also Elemente des Matrizenrings $(R/I)^{2\times 2}$.* —

**V 2.4.** Zeigen Sie, dass alle Ideale in $R^{2\times 2}$ von der obigen Form sind. *Zusatz:* Gilt das auch in $R^{n\times n}$? Was kann man zu Links- bzw. Rechtsidealen in $R^{n\times n}$ sagen?

**Lösungshinweise: —** *Sei $E_{ij}$ die Matrix mit einer $1$ an der Stelle $(i, j)$ und $0$ sonst.*
*Sei nun $J \lhd R^{2\times 2}$ ein Ideal. Dann ist für $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in J$ auch $E_{ij}AE_{kl} \in J$ für alle $i, j, k, l \in \{1, 2\}$. Damit sieht man aber schon, dass $J = \left(\begin{smallmatrix} I & I \\ I & I \end{smallmatrix}\right)$ für eine Menge $I \subset R$, da jedes Element von einer beliebigen Stelle zu einer anderen Stelle verschoben werden kann. Wir müssen noch zeigen, dass $I$ ein Ideal ist. Da $J$ eine abelsche Gruppe bezüglich komponentenweiser Addition bildet, überträgt sich das direkt auf $I$. Und wegen $\left(\begin{smallmatrix} R & 0 \\ 0 & 0 \end{smallmatrix}\right) J = \left(\begin{smallmatrix} RI & RI \\ 0 & 0 \end{smallmatrix}\right) \subset J$ folgt auch, dass $RI \subset I$ gilt.*
*Dieser Beweis überträgt sich nahezu identisch in höhere Dimensionen.*
*Wenn man nur Linksideale (oder Rechtsideale) ansieht, so kann man im allerersten Schritt nur von links (rechts) mit Matrizen der Form $E_{ij}$ multiplizieren und erhält damit nur, dass die Einträge in gleichen Spalten (Zeilen) gleich sind. Die Linksideale sind also von der Form $\left(\begin{smallmatrix} I & K \\ I & K \end{smallmatrix}\right)$ für $I, K \lhd R$ und Rechtsideale von der Form $\left(\begin{smallmatrix} I & I \\ K & K \end{smallmatrix}\right)$* —

**S 2.5.** (4 Punkte) Zeigen Sie:
(a) Jeder Divisionsring $R$ hat nur die trivialen Ideale $\{0\}$ und $R$.
(b) Hat ein kommutativer Ring $R$ genau zwei Ideale (nämlich $\{0\}$ und $R$) dann ist $R$ ein Körper. *Hinweis:* für $a \neq 0$ in $R$ betrachte man das Ideal $(a)$.
(c) Geben Sie ein Gegenbeispiel im nicht-kommutativen Fall: ein Ring mit nur den beiden trivialen Idealen muss kein Divisionsring sein.

**Lösungshinweise: —**

(a) *Sei $I \neq \{0\}$ ein Ideal. Dann gibt ein $0 \neq a \in I$ und dieses besitzt im Divisionsring $R$ ein Linksinverses $b$. Für beliebiges $r \in R$, ist also $r = (rb)a \in I$. Damit ist $I = R$, was zu zeigen war.*

(b) *Wenn $a \neq 0$, dann ist das von $a$ erzeugte Hauptideal $(a) = Ra \neq \{0\}$. Also folgt aus der Voraussetzung $(a) = R$. Damit ist $1 \in (a)$ oder anders gesagt $1 = ra = ar$ für ein $r \in R$. Damit ist $a$ invertierbar, also $R$ ein Körper. (Im nicht-kommutativen Fall wäre $Ra$ kein Ideal...)*

(c) *Die Aufgaben 2.3 und 2.4 zeigen, dass für einen Körper $K$ der Ring $K^{2\times 2}$ nur die trivialen Ideale besitzt. Es ist aber kein Divisionsring, da er Nullteiler besitzt (z.B. $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$).*

—

## 3. Der Chinesische Restsatz

Für $n \in \mathbb{N}$ ist $n\mathbb{Z}$ ein Ideal in $\mathbb{Z}$ (nachprüfen!) und wir bilden den Quotientenring $\mathbb{Z}/n\mathbb{Z}$. Wenn Sie im Umgang mit Quotienten unsicher sind, prüfen Sie es am besten direkt:

**3.1.** Zeigen Sie, dass $\mathbb{Z}/n\mathbb{Z}$ tatsächlich ein Ring ist, indem Sie direkt die Wohldefiniertheit der Addition und Multiplikation von Restklassen nachweisen. Wo genau geht ein, dass $n\mathbb{Z}$ ein Ideal ist?

**Lösungshinweise: —** *Die Operationen $(a+n\mathbb{Z})+(b+n\mathbb{Z}) = (a+b)+n\mathbb{Z}$ und $(a+n\mathbb{Z})\cdot(b+n\mathbb{Z}) = (a\cdot b)+n\mathbb{Z}$ sind wegen der Idealeigenschaft von $n\mathbb{Z}$ wohldefiniert, wie man sofort nachrechnet und die Assoziativität und alle anderen Eigenschaften vererben sich von $\mathbb{Z}$.* —

**V 3.2.** Zeigen Sie, dass $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper ist, wenn $n$ eine Primzahl ist. Benutzen Sie folgende nützliche Regel: Wenn eine Primzahl $p$ das Produkt $ab$ von zwei ganzen Zahlen $a, b \in \mathbb{Z}$ teilt, dann teilt sie einen der beiden Faktoren.

**Lösungshinweise: —** *Wenn $n$ nicht prim ist, dann hat es einen echten Teiler $m$ mit $km = n$. In $\mathbb{Z}/n\mathbb{Z}$ geht diese Gleichung dann in $km = 0$ über, was bedeutet, dass es Nullteiler gibt. Diese können aber damit nicht invertierbar sein und $\mathbb{Z}/n\mathbb{Z}$ ist kein Körper.*

*Um zu zeigen, dass $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl $p$ ein Körper ist, müssen wir zeigen, dass jedes Nichtnullelement $a$ ein Inverses besitzt. Das zeigen wir, indem wir zeigen, dass die Linksmultiplikation $\lambda_a(x) = ax$ auf $\mathbb{Z}/p\mathbb{Z}$ surjektiv ist (Damit gibt es dann ein $b$ mit $ab = 1$). Da $\mathbb{Z}/p\mathbb{Z}$ endlich ist, ist dies Äquivalent zur Injektivität der Abbildung. Sei also $ax = ay$. Dann ist $a(x-y) = 0$ in $\mathbb{Z}/p\mathbb{Z}$, oder anders gesagt, $p$ teilt $a(x-y)$. Da $a$ nicht durch $p$ teilbar ist, folgt, dass $p$ den anderen Faktor $x-y$ teilt und damit $x = y$ in $\mathbb{Z}/p\mathbb{Z}$, was zu zeigen war.* —

Die Eulersche $\varphi$-Funktion $\varphi\colon \mathbb{N} \to \mathbb{N}$ ist definiert durch $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$. Anders gesagt, ist $\varphi(n)$ die Anzahl der invertierbaren Elemente in $\mathbb{Z}/n\mathbb{Z}$.

**V 3.3.** (a) Zeigen Sie mit Hilfe des Chinesischen Restsatzes, dass $\varphi$ multiplikativ ist, dass also $\varphi(nm) = \varphi(n)\varphi(m)$ gilt, wenn $(n)$ und $(m)$ teilerfremd sind.

Jede ganze Zahl lässt sich eindeutig in ein Produkt aus Primzahlpotenzen zerlegen, die untereinander teilerfremd sind. Daher reicht es, $\varphi$ auf Primzahlpotenzen zu kennen.

(b) Bestimmen Sie die Nullteiler in $\mathbb{Z}/p^k\mathbb{Z}$.

(c) Jeder Nicht-Nullteiler $a \neq 0$ in $\mathbb{Z}/p^k\mathbb{Z}$ ist invertierbar.
*Hinweis:* Man betrachte $x \mapsto ax$ auf der endlichen Menge $\mathbb{Z}/p^k\mathbb{Z}$.

(d) Schließen Sie, dass $\varphi(p^k) = p^{k-1}(p-1)$ für $k \in \mathbb{N}$.

**Lösungshinweise: —**

(a) *Wenn $(n)$ und $(m)$ teilerfremd sind, dann ist $n\mathbb{Z}+m\mathbb{Z} = \mathbb{Z}$ und der chinesische Restsatz liefert $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Ein Ringisomorphismus bildet aber auch die invertierbaren Elemente aufeinander ab, so dass deren Anzahl links und rechts übereinstimmt. Es folgt mit Aufgabe 1.4 $\varphi(nm) = \varphi(n)\varphi(m)$.*

(b) *Damit eine Restklasse zu $a \in \mathbb{Z}$ ein Nullteiler in $\mathbb{Z}/p^k\mathbb{Z}$ ist, muss es ein $b \in \mathbb{Z} \setminus p^k\mathbb{Z}$ und $l \in \mathbb{Z}$ geben, so dass $ab = lp^k$ gilt. Da $b$ nicht durch $p^k$ teilbar ist, folgt, dass $p$ $a$ teilt. Ist auf der anderen Seite $a$ durch $p^f$ $(1 \leq f < k)$ teilbar, so lässt sich $b = p^{k-f}$ setzen und man sieht, dass $a$ ein Nullteiler ist. Die Nullteiler sind also genau die durch $p$ teilbaren Elemente ungleich* 0.

(c) *Ist $a \neq 0$ nun ein Nicht-Nullteiler, d.h. teilerfremd zu $p$, so zeigt man ähnlich wie in Aufgabe 3.2, dass die Abbildung $\lambda_a(x) = ax$ auf $\mathbb{Z}/p^k\mathbb{Z}$ injektiv ist und somit $a$ ein Inverses besitzt.*

(d) *Wir müssen, um die Anzahl $\varphi(p^k) = |(\mathbb{Z}/p^k\mathbb{Z})^\times|$ zu bestimmen, die invertierbaren Elemente zählen, bzw. wir zählen die nichtinvertierbaren Elemente und ziehen diese Anzahl von der Gesamtzahl ab. Nach $(b)$ brauchen wir also die Zahlen $1 \leq a \leq p^k$, die durch $p$ teilbar sind. Dies sind aber genau $p^{k-1}$ Stück so dass sich $\varphi(p^k) = p^k - p^{k-1}$ ergibt.*

—

Die Eieraufgabe von Brahmagupta:

**V 3.4.** Eine alte Frau geht über den Marktplatz. Ein Pferd tritt auf ihre Tasche und zerbricht die gekauften Eier. Der Besitzer des Pferdes möchte den Schaden ersetzen und fragt die alte Frau, wie viele Eier in ihrer Tasche waren. Sie weiß die exakte Zahl nicht mehr, aber sie erinnert sich, dass genau ein Ei übrig bleibt, wenn sie beim Auspacken die Eier immer zu zweit aus der Tasche nimmt. Das Gleiche geschieht, wenn sie die Eier immer zu dritt, zu viert, zu fünft und zu sechst aus der Tasche nimmt. Nur wenn sie die Eier zu siebt aus der Tasche nimmt, bliebt kein Ei übrig. Was ist die kleinste Zahl an Eiern, welche die alte Frau in ihrer Tasche haben kann?

**Lösungshinweise: —** *Wenn die Anzahl der Eier $n$ kongruent* 1 *modulo* $2,3,4,5$ *und* 6 *ist, dann ist $n-1$ durch $kgV(2,3,4,5,6) = 60$ teilbar, also $n = 1+60k$. Damit diese Zahl noch minimal und durch* 7 *teilbar ist, muss $k = 5$ gewählt werden. Also hatte die Frau mindestens* 301 *Eier.* —

**3.5.** Berechnen Sie die letze Ziffer von $7^{103}$ und die letzten zwei Ziffern von $7^{2010}$.

**Lösungshinweise: —** *Es ist $7^2 = 49 \equiv -1$ modulo* 10*. Damit lassen sich die letzte Stelle bestimmen, indem man $7^{103} \equiv 7 \cdot (7^2)^{51} \equiv 7 \cdot (-1)^{51} \equiv -7 \equiv 3 \mod 10$ rechnet.*
*Will man aber die letzten beiden Ziffern, so muss man schon modulo* 100 *rechnen, was nicht ganz so einfach ist. Nach dem Chinesischen Restsatz reicht es aber auch dies modulo* 25 *und* 4 *zu betrachten. Es ist $7^2 = 49 \equiv -1 \mod 25$ und $7 \equiv -1 \mod 4$. Damit ist $7^{2010} \equiv -1^{1005} \equiv -1$ modulo* 25 *und $7^{2010} = 1 \mod 4$. Aus der ersten Kongruenz folgt, dass $7^{2010} = -1 + 25k$ und die zweite Kongruenz liefert $-1+25k \equiv 1 \mod 4$, woraus $k = 2$ folgt (die Zahl soll zwischen* 0 *und* 99 *liegen..). Dies liefert dann $7^{2010} \equiv 49 \mod 100$.*
—