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.

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

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

Bemerkung: Dies verallgemeinert die erste Aufgabe. Für einen K-Vektorraum V der Dimension n ist der Ring $(\operatorname{End}_K(V),+,\circ)$ 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 $(\operatorname{End}(A),+,\circ)$ 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 $\mathbb{C}^{2\times 2}$ betrachten wir die vier Matrizen

$$E=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad I=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\quad J=\begin{pmatrix}0&i\\i&0\end{pmatrix},\quad K=\begin{pmatrix}i&0\\0&-i\end{pmatrix}.$$

(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 $\mathbb{C}^{2\times 2}$ aufgespannte $\mathbb{R}$-Vektorraum

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

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

(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?

S 1.4. (4 Punkte) Seien $R_1,\dots,R_n$ Ringe. Zeigen Sie, dass $R=R_1\times\dots\times R_n$ 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 $R_1,\dots,R_n$.

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 $R/\mathfrak{a}\cong S/f(\mathfrak{a})$.

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?

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

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?

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.

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?

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.

Die Eulersche φ-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 φ 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, φ 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 $k\in\mathbb{N}$.

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?

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