Fachbereich Mathematik
Prof. Dr. Nils Scheithauer
Walter Reußwig

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 08/09 14. Oktober 2008

Algebra

1. Übung mit Lösungshinweisen

Aufgabe 1 Es seien R, S Ringe und $\varphi : R \to S$ ein Ringhomomorphismus. Zeige, daß folgende Aussagen äquivalent sind:

(1) Der Ringhomomorphismus φ ist injektiv.

(2) Der Ringhomomorphismus φ besitzt trivialen Kern.

LÖSUNG: Wir zeigen beide Implikationen.
(1) $\Rightarrow$ (2) Sei $x \in \ker(\varphi)$, dann gilt $\varphi(x) = 0 = \varphi(0)$, also folgt $x = 0$.
(2) $\Rightarrow$ (1) Sei $\varphi(x) = \varphi(y)$, dann gilt $x - y \in \ker(\varphi)$, also $x - y = 0$, also $x = y$.

Aufgabe 2 Es sei A eine abelsche Gruppe. Zeige, daß die Menge $\mathrm{End}(A)$ der Endomorphismen von A mit punktweiser Addition und Verknüpfung als Multiplikation einen Ring bildet. Ist dieser Ring kommutativ? Besitzt $\mathrm{End}(A)$ eine Eins?

LÖSUNG: Wir rechnen die Ringaxiome nach:

(R1) Die Summe zweier Endomorphismen ist punktweise definiert, daher ist es leicht einzusehen, daß $\mathrm{End}(A)$ eine abelsche Gruppe bildet.

(R2) Für zwei Endomorphismen $\varphi, \psi \in \mathrm{End}(A)$ ist auch die Verknüpfung $\varphi \circ \psi \in \mathrm{End}(A)$. Für drei Endomorphismen $\varphi, \psi, \rho \in \mathrm{End}(A)$ gilt:

$$\varphi \cdot (\psi \cdot \rho) = \varphi \circ (\psi \circ \rho) = (\varphi \circ \psi) \circ \rho = (\varphi \cdot \psi) \cdot \rho.$$

Somit ist die Multiplikation assoziativ.

(R3) Seien $\varphi_1, \varphi_2, \psi_1, \psi_2 \in \mathrm{End}(A)$, dann gilt für jedes $a \in A$:

$$\begin{aligned}
\big((\varphi_1 + \varphi_2) \cdot (\psi_1 + \psi_2)\big)(x) &= \big(\varphi_1 + \varphi_2\big)\big((\psi_1 + \psi_2)(x)\big) \\
&= \varphi_1\big(\psi_1(x) + \psi_2(x)\big) + \varphi_2\big(\psi_1(x) + \psi_2(x)\big) \\
&= \varphi_1(\psi_1(x)) + \varphi_1(\psi_2(x)) + \varphi_2(\psi_1(x)) + \varphi_2(\psi_2(x)) \\
&= \varphi_1 \cdot \psi_1(x) + \varphi_1 \cdot \psi_2(x) + \varphi_2 \cdot \psi_1(x) + \varphi_2 \cdot \psi_2(x)
\end{aligned}$$

Also gilt wie gefordert

$$(\varphi_1 + \varphi_2) \cdot (\psi_1 + \psi_2) = \varphi_1 \cdot \psi_1 + \varphi_1 \cdot \psi_2 + \varphi_2 \cdot \psi_1 + \varphi_2 \cdot \psi_2.$$

Dieser Ring besitzt eine Eins, der Identitätsendomporphismus leistet das Gewünschte.
In der Regel ist $\mathrm{End}(A)$ nicht kommutativ. Ein Gegenbeispiel liefert die Gruppe $\mathbb{Z} \oplus \mathbb{Z}$. Ihr Endomorphismenring ist nicht kommutativ, da es Matrizen in $M_2(\mathbb{Z})$ gibt, die nicht miteinander kommutieren. Beispiele dafür solltet Ihr leicht angeben können.

Aufgabe 3 Es sei R ein Ring. Zeige, daß unter sehr schwachen Vorraussetzungen an R die $n \times n$-Matrizen mit R-Einträgen $M_n(R)$ für $n > 1$ einen nicht kommutativen Ring bilden.

LÖSUNG: Wir nehmen nur an, daß es Elemente $a, b \in R$ gibt mit $a \cdot b \neq 0$. Dann folgt aus der Rechnung

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & ba \end{pmatrix}.$$

die Behauptung für den Fall $n = 2$. Eine Verallgemeinerungen auf großere Matrizen sollte nun ebenfalls nicht mehr schwer sein.

Aufgabe 4 Es sei R ein Ring. Ein Element $a \in R$ heißt *nilpotent*, falls es eine natürliche Zahl n gibt mit $a^n = 0$. Zeige: Sind a und b nilpotente Elemente eines kommutativen Rings R, dann ist auch $(a + b)$ nilpotent.
Ist obige Aussage auch wahr, wenn wir auf die Vorraussetzung, daß R kommutativ ist, verzichten?

LÖSUNG: Es sei $a^m = 0$ und $b^n = 0$ für zwei natürliche Zahlen $m, n \in \mathbb{N}$. OBdA können wir $m = n$ annehmen (warum?). Somit gilt nach dem Satz der Vorlesung

$$(a+b)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} a^k \cdot b^{2n-k} = \sum_{k=0}^{n} \binom{2n}{k} a^k \cdot b^{2n-k} + \sum_{k=n+1}^{2n} \binom{2n}{k} a^k \cdot b^{2n-k}.$$

In dieser Zerlegung in zwei Summen sehen wir nun, daß in der ersten Summe alle Terme verschwinden, da $b^l = 0$ für $l \geq n$ und in der zweiten Summe alle Terme verschwinden, da $a^l = 0$ für $l \geq n$. Somit ist $(a + b)$ nilpotent.
In nicht kommutativen Ringen kann die Aussage falsch sein, wie wir in $M_2(\mathbb{C})$ leicht sehen:

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{und} \quad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

sind nilpotente Matrizen, aber ihre Summe ist nicht nilpotent, da $(A + B)^2 = \mathbb{1}$.

Aufgabe 5 Es sei R ein Ring und es seien $f, g : \mathbb{Q} \to R$ zwei Ringhomomorphismen. Zeige, daß die folgenden Aussagen äquivalent sind:

(1) Für jede ganze Zahl $n \in \mathbb{Q}$ gilt $f(n) = g(n)$.

(2) Für alle $x \in \mathbb{Q}$ gilt $f(x) = g(x)$.

LÖSUNG: Wir zeigen beide Inklusionen.
(1) $\Rightarrow$ (2) Angenommen, wir haben zwei Ringhomomorphismen f, g, welche die Bedingungen für (1) erfüllen. Dann folgt

$$\begin{aligned} f\left(\frac{1}{n}\right) \cdot g(n) &= f\left(\frac{1}{n}\right) \cdot f(n) \\ &= f(1) = g(1) \\ &= g\left(\frac{1}{n}\right) \cdot g(n). \end{aligned}$$

Multiplizieren wir beide Seiten von rechts mit $g\left(\frac{1}{n}\right)$, so erhalten wir

$$f\left(\frac{1}{n}\right) = g\left(\frac{1}{n}\right),$$

woraus die Behauptung folgt (warum?).
(2) $\Rightarrow$ (1) Hier ist nichts zu zeigen.

Aufgabe 6 (Quaternionen) Wir betrachten die Menge

$$\mathbb{H} := \{\lambda := \lambda_0 \cdot \mathbb{1} + \lambda_1 \cdot i + \lambda_2 \cdot j + \lambda_3 \cdot k : \lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}\},$$

als $\mathbb{R}$-Vektorraum mit Basis $\{\mathbb{1}, i, j, k\}$ und folgender Multiplikation:

$$\begin{aligned}
\lambda \cdot \mu &= (\lambda_0 \cdot \mathbb{1} + \lambda_1 \cdot i + \lambda_2 \cdot j + \lambda_3 \cdot k) \cdot (\mu_0 \cdot \mathbb{1} + \mu_1 \cdot i + \mu_2 \cdot j + \mu_3 \cdot k) \\
&:= (\lambda_0\mu_0 - \lambda_1\mu_1 - \lambda_2\mu_2 - \lambda_3\mu_3) \cdot \mathbb{1} + (\lambda_0\mu_1 + \lambda_1\mu_0 + \lambda_2\mu_3 - \lambda_3\mu_2) \cdot i \\
&+ (\lambda_0\mu_2 + \lambda_2\mu_0 + \lambda_3\mu_1 - \lambda_1\mu_3) \cdot j + (\lambda_0\mu_3 + \lambda_3\mu_0 + \lambda_1\mu_2 - \lambda_2\mu_1) \cdot k.
\end{aligned}$$

Wir wollen zeigen, daß $(\mathbb{H}, +, \cdot)$[1] ein Ring ist, welcherer *Ring der Quaternionen* heißt.

(a) Mache Dir klar, daß $(\mathbb{H}, +)$ eine abelsche Gruppe ist.

(b) Zeige, daß folgende $\mathbb{R}$-lineare Abbildung $\pi : \mathbb{H} \to M_2(\mathbb{C})$, welche wie folgt auf der Basis von $\mathbb{H}$ definiert ist, injektiv ist, wobei wir $M_2(\mathbb{C})$ als reellen Vektorraum auffassen.

$$E := \pi(\mathbb{1}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I := \pi(i) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

$$J := \pi(j) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K := \pi(k) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

(c) Zeige, daß π multiplikativ ist.

(d) Zeige, daß die $\mathbb{R}$-lineare Hülle Q von $\{E, I, J, K\}$ einen Unterring von $M_2(\mathbb{C})$ bildet.

(e) Folgere nun, daß $\mathbb{H}$ ein Ring (und damit eine $\mathbb{R}$-Algebra) mit Eins ist. Ist $\mathbb{H}$ kommutativ? Bildet π die Eins von $\mathbb{H}$ auf die Eins von Q ab?

(f) Zeige die Relationen

$$i^2 = j^2 = k^2 = ijk = -1, \quad ij = -ji, \quad jk = -kj, \quad ki = -ik.$$

Mit formaler Multiplikation, wird der $\mathbb{R}$-Vektorraum, der durch die Basis $\{\mathbb{1}, i, j, k\}$ erzeugt wird, mit obigen Relationen ebenfalls zum Ring der Quaternionen, wenn wir verlangen, daß $\mathbb{1}$ mit allen anderen Elementen kommutiert, vgl. z. B. [Jantzen, Algebra] p. 300ff.

(g) Zeige, daß jedes Element von $\mathbb{H} - \{0\}$ invertierbar ist. Überlege, wie das Inverse zu einem Quaternion aussieht.

(h) Überlege, warum Du in dieser Aufgabe gezeigt hast, daß es eine Gruppenstruktur auf der Einheitskugel des $(\mathbb{R}^4, \|\cdot\|_2)$ gibt.

LÖSUNG: (a) Ein Vektorraum ist per Definition bezüglich der Addition eine abelsche Gruppe.

(b) Die Aussage ist äquivalent dazu, zu zeigen, daß $\{E, I, J, K\}$ in $M_2(\mathbb{C})$ $\mathbb{R}$-linear unabhängig ist. Dies zu zeigen, ist leicht, da 1 und i über $\mathbb{R}$ linear unabhängig sind.

---

[1] Sir William Rowan Hamilton (1805 - 1865), irischer Mathematiker und Physiker) konstruierte 1843 obige Verallgemeinerung der komplexen Zahlen auf einen 4-dimensionalen reellen Raum. Ihm zu Ehren werden die Quaternionen mit $\mathbb{H}$ bezeichnet.

(c) Dies folgt leicht, wenn wir uns anschauen, wie das Produkt der Bilder zweier Quaternionen $\lambda, \mu \in \mathbb{H}$ in Q aussieht:

$$\begin{aligned}
\pi(\lambda) = \pi(\lambda_0 \cdot \mathbb{1} + \lambda_1 \cdot i + \lambda_2 \cdot j + \lambda_3 \cdot k) &= \begin{pmatrix} \lambda_0 + \lambda_1 \cdot i & \lambda_2 + \lambda_3 \cdot i \\ -\lambda_2 + \lambda_3 \cdot i & \lambda_0 - \lambda_1 \cdot i \end{pmatrix} \\
\pi(\mu) = \pi(\mu_0 \cdot \mathbb{1} + \mu_1 \cdot i + \mu_2 \cdot j + \mu_3 \cdot k) &= \begin{pmatrix} \mu_0 + \mu_1 \cdot i & \mu_2 + \mu_3 \cdot i \\ -\mu_2 + \mu_3 \cdot i & \mu_0 - \mu_1 \cdot i \end{pmatrix} \\
\pi(\lambda) \cdot \pi(\mu) &=: \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} =: A,
\end{aligned}$$

wobei die komplexen Zahlen $a_{11}, a_{12}, a_{21}, a_{22} \in \mathbb{C}$ via Matrixmultiplilation zu berechnen sind. Wir erhalten beispielsweise

$$a_{11} = (\lambda_0 \cdot \mu_0 - \lambda_1 \cdot \mu_1 - \lambda_2 \cdot \mu_2 - \lambda_3 \cdot \mu_3) + (\lambda_1 \cdot \mu_0 + \lambda_0 \cdot \mu_1 + \lambda_2 \cdot \mu_3 - \lambda_3 \cdot \mu_2) \cdot i.$$

Rechnen wir alle diese Zahlen aus, sehen wir, daß die Matrix A wieder in $\mathrm{im}(\pi)$ liegt, somit genau ein Urbild $\nu \in \mathbb{H}$ hat. Die Koeffizienten dieses Quaternions bestimmen sich eindeutig aus den Einträgen von A, z. B. gilt $\nu_0 = \frac{1}{2} \cdot (a_{11} + a_{22})$. Rechnen wir das konkret aus, stellen wir fest, daß $\nu = \lambda \cdot \mu$ gilt, also gilt $\pi(\lambda \cdot \mu) = \pi(\lambda) \cdot \pi(\mu)$ für alle Quaternionen $\lambda, \mu \in \mathbb{H}$.

(d) Aus (c) wird klar, daß das Produkt zweier Matrizen aus Q wieder in Q liegt, da das Produkt ebenfalls Bild eines Quaternions aus $\mathbb{H}$ ist.

(e) Da $\pi : \mathbb{H} \to Q$ bijektiv ist und Produkte erhält, ist π^{-1} ebenfalls bijektiv und erhält Produkte. Damit ist $(\mathbb{H}, +, \cdot)$ aber ein Ring, da Q ein Ring ist, und somit alle Ringaxiome, die in $M_2(\mathbb{C})$ gelten, auch in $\mathbb{H}$ gelten müssen.
Dieser ist nicht kommutativ, wie aus Nachrechnen der Relationen in (f) sofort folgt. Weiter bildet π die Eins in $\mathbb{H}$ auf die Eins in Q ab. Also ist $\mathbb{H}$ ein nichtkommutativer Ring mit Eins.

(f) Die Rechnungen sind leicht.

(g) Die Invertierbarkeit eines Quaternions $\lambda \in \mathbb{H}$ ist mit dem, was wir bereits bewiesen haben, äquivalent zur Invertierbarkeit von $\pi(\lambda) \in Q$. In $M_2(\mathbb{C})$ können wir aber leicht Invertierbarkeit mit der Determinante entscheiden:

$$\det(\pi(\lambda)) = \det\left(\begin{pmatrix} \lambda_0 + \lambda_1 \cdot i & \lambda_2 + \lambda_3 \cdot i \\ -\lambda_2 + \lambda_3 \cdot i & \lambda_0 - \lambda_1 \cdot i \end{pmatrix}\right) = \lambda_0^2 + \lambda_1^2 + \lambda_2^2 + \lambda_3^2.$$

Die Determinante ist also genau dann 0, wenn das Quaternion 0 ist. Somit folgt die Behauptung.
Weiter ist das Invertieren von 2×2-Matrizen leicht. Wir erhalten

$$\lambda^{-1} = \pi^{-1}(\pi(\lambda^{-1})) = \pi^{-1}(\pi(\lambda)^{-1}) = \pi^{-1}\left(\frac{1}{\lambda_0^2 + \lambda_1^2 + \lambda_2^2 + \lambda_3^2} \cdot \begin{pmatrix} \lambda_0 - \lambda_1 \cdot i & -\lambda_2 - \lambda_3 \cdot i \\ \lambda_2 - \lambda_3 \cdot i & \lambda_0 + \lambda_1 \cdot i \end{pmatrix}\right).$$

(h) Wir sehen, die Elemente aus $\mathbb{H}$ mit euklidischer Norm 1 werden genau auf die Matrizen in Q mit Determinante 1 abgebildet. Die Matrizen mit Determinante 1 bilden aber eine Untergruppe von Q. Da diese Identifikation injektiv ist, erhalten wir auf der Einheitskugel eine Gruppenstruktur. Man kann zeigen, daß diese Gruppe isomorph ist zur $SU_2(\mathbb{C})$.

Hausübungen

Aufgabe H1 (Frobenius-Homomorphismus) Es sei $p \in \mathbb{N}$ eine Primzahl und R ein kommutativer Ring mit Eins und Charakteristik p.

(a) Zeige die Aussage aus der Vorlesung: Für $a, b \in R$ mit $ab = ba$ gilt

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k}.$$

(b) Folgere, daß die Abbildung

$$\varphi : R \to R, \quad \varphi(x) := x^p$$

ein Ringhomomorphismus ist.

LÖSUNG: (a) Dies sollte ein einfacher Induktionsbeweis sein, ihn vorführen zu müssen, sollte jedoch nicht nötig sein. Nachzulesen ist dieser z. B. im [Forster, Analysis I, 3. Ed.], p.6, wenn man hier "reelle Zahl" durch "Zahl aus dem Ring R" ersetzt. Die Vorraussetzung $ab = ba$ ist hier entscheidend.

(b) Die Abbildung φ ist auf Grund der Kommuatativität von R multiplikativ, nur die Additivität ist noch nachzuweisen. Es seien $x, y \in R$, dann folgt

$$\begin{aligned}
\varphi(x+y) &= (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k \cdot y^{p-k} \\
&= x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k \cdot y^{p-k} + y^p \\
&= \varphi(x) + \sum_{k=1}^{p-1} \binom{p}{k} x^k \cdot y^{p-k} + \varphi(y)
\end{aligned}$$

Da aber alle Binomialkoeffizienten in der mittleren Summe natürliche durch p teilbare Zahlen sind, verschwindet dieser Term, da R Charakterisik p hat. Somit folgt die Behauptung.

Aufgabe H2 Es sei R ein endlicher Ring mit Eins, wobei $1 \neq 0$ gelte. Zeige, das folgende Aussagen äquivalent sind:

(1) Der Ring R ist ein Divisionsring.

(2) Es gibt in R keine Nullteiler.

LÖSUNG: Hier sind beide Inklusionen zu zeigen.
(1) $\Rightarrow$ (2) Sind $a, b \in R$ mit $a \neq 0$ und $ab = 0$, so folgt aus $b = (a^{-1}a)b = a^{-1}(ab) = 0$, daß b schon 0 ist, also kein Linksnullteiler sein kann. Damit existieren aber auch keine Rechtsnullteiler, woraus die Behauptung folgt.
(2) $\Rightarrow$ (1) Wir folgern, daß es in einem Divisionsring keine Linksnullteiler gibt. Daraus folgt bereits die Behauptung, da es genau dann Linksnullteiler gibt, wenn es Rechtsnullteiler gibt.
Wir nummerieren die Elemente von R via $R = \{0, r_1, ..., r_n\}$ und betrachten für ein $0 \neq r_i \in R$ die Menge

$$R_i := \{r_i \cdot 0, r_i \cdot r_1, ..., r_i \cdot r_n\}.$$

Es gilt nun $R_i = R$, denn sonst wäre die Abbildung $R \ni r \to r_i \cdot r \in R$ nicht surjektiv, und da R endlich ist, auch nicht injektiv. Es gäbe also entweder ein $j \in \{1, ..., n\}$ mit $r_i \cdot r_j = 0$ oder zwei verschiedene Zahlen $j, k \in \{1, ..., n\}$ mit $r_i \cdot r_j = r_i \cdot r_k$. Im ersten Fall existierten Nullteiler, was der Vorraussetzung widerspricht.
Im zweiten Fall erhielten wir

$$r_i \cdot (r_j - r_k) = 0,$$

woraus $r_j = r_k$ folgt, was ebenfalls der Vorraussetzung widerspricht. Also ist obige Abbildung surjektiv. Damit ist aber r_i rechtsinvertierbar, da $1 \in R_i$. Analog ist zu zeigen, daß r_i auch linksinvertierbar ist, also ist r_i eine Einheit, also ist R ein Divisionsring.
