D-MATH Algebra I HS 2024
Prof. Dr. Lorenz Halbeisen

Musterlösung Serie 10

IDEALE, ENDLICHE KÖRPER, 2. ISOMORPHIESATZ

---

53. Sei R ein Ring und sei $\mathrm{Mat}(n, R)$ der Ring der $n \times n$-Matrizen mit Koeffizienten in R mit der üblichen Addition und Multiplikation.

(a) Zeige: Ist $\mathfrak{a} \subseteq R$ ein Ideal, so ist $\mathrm{Mat}(n, \mathfrak{a})$ ein Ideal in $\mathrm{Mat}(n, R)$.

(b) Zeige: Jedes Ideal in $\mathrm{Mat}(n, R)$ ist von der Form $\mathrm{Mat}(n, \mathfrak{a})$ für ein geeignetes Ideal $\mathfrak{a} \subseteq R$.

(c) Sei $\mathfrak{a} \subseteq R$ ein Ideal in R.
Zeige:

$$\mathrm{Mat}(n, R/\mathfrak{a}) \;\cong\; \mathrm{Mat}(n, R)/\mathrm{Mat}(n, \mathfrak{a})\,.$$

Lösung: (a) Seien $A = (A_{ij})_{1\leqslant i,j\leqslant n}$ und $B = (B_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{Mat}(n, \mathfrak{a})$. Dann gilt

$$A + B = (A_{ij} + B_{ij})_{1\leqslant i,j\leqslant n}.$$

Da $\mathfrak{a}$ ein Ideal ist, liegt für alle i, j das Element $A_{ij} + B_{ij}$ in $\mathfrak{a}$. Somit ist $A + B \in \mathrm{Mat}(n, \mathfrak{a})$. Sei nun $R = (R_{ij})_{1\leqslant i,j\leqslant n} \in \mathrm{Mat}(n, \mathfrak{a})$. Dann gilt

$$(RA)_{ij} = \sum_{k=1}^{n} R_{ik}A_{ki}.$$

Da $\mathfrak{a}$ ein Ideal ist, gilt $R_{ik}A_{ki} \in \mathfrak{a}$ für alle $1 \leqslant i, j, k \leqslant n$. Somit liegt auch die Summe $\sum_{k=1}^{n} R_{ik}A_{ki}$ in $\mathfrak{a}$. Also ist $RA \in \mathrm{Mat}(n, \mathfrak{a})$.

(b) Sei $\mathfrak{A} \subseteq \mathrm{Mat}(n, R)$ ein Ideal. Betrachte die Menge

$$\mathfrak{a} := \{a \in R : \exists A \in \mathfrak{A}\, \exists i, j \in \{1, \ldots, n\}\colon\; A_{ij} = a\}.$$

Wir wollen zeigen, dass $\mathfrak{a} \subseteq R$ ein Ideal ist und dass $\mathfrak{A} = \mathrm{Mat}(n, \mathfrak{a})$ gilt.

Wir weisen zuerst nach, dass $\mathfrak{a}$ ein Ideal ist. Seien also $A, B \in \mathfrak{A}$ und seien $1 \leqslant i, j, k, l \leqslant n$. Wir müssen $A_{ij} + B_{kl} \in \mathfrak{a}$ zeigen. Wähle $\pi, \tau \in S_n$ mit $\pi(k) = i$ und $\tau(l) = j$. Seien P_π und P_τ die zugehörigen Permutationsmatrizen. Da $\mathfrak{A}$ ein Ideal ist, wissen wir $P_\pi B P_\tau^t \in \mathfrak{A}$. Ausserdem gilt $(P_\pi B P_\tau^t)_{ij} = B_{kl}$ und somit ist $(A + P_\pi B P_\tau^t)_{ij} = A_{ij} + B_{kl} \in \mathfrak{a}$. Sei ausserdem $r \in R$. Sei D die Diagonalmatrix, deren Diagonaleinträge alle gleich r sind. Dann ist $DA \in \mathfrak{A}$ und es gilt $(DA)_{ij} = rA_{ij}$. Daraus folgt $rA_{ij} \in \mathfrak{a}$. Somit ist $\mathfrak{a}$ ein Ideal.

Offensichtlich gilt $\mathfrak{A} \subseteq \mathrm{Mat}(n, \mathfrak{a})$. Für die umgekehrte Inklusion sei $A \in \mathrm{Mat}(n, \mathfrak{a})$. Sei $1 \leqslant i, j \leqslant n$ und betrachte die Matrix M, für die $M_{ij} = A_{ij}$ ist und deren andere Einträge alle 0 sind. Da A die Summe über alle solchen M ist, genügt es $M \in \mathfrak{A}$ zu zeigen. Laut Definition gibt es ein $B \in \mathfrak{A}$ und k, l mit $B_{kl} = A_{ij}$. Durch geeignete Multiplikation mit Permutationsmatrizen, wie oben, können wir annehmen, dass $(k, l) = (i, j)$ gilt. Sei nun N

die Matrix, für die $N_{ij} = 1$ ist und deren andere Einträge alle 0 sind. Dann gilt $NBN^t = M$ und somit $M \in \mathfrak{A}$.

(c) Sei $\varphi\colon \mathrm{Mat}(n, R) \to \mathrm{Mat}(n, R/\mathfrak{a})$ gegeben durch $\varphi(A)_{ij} = A_{ij} + \mathfrak{a}$. Wir prüfen nach, dass φ ein Ringhomomorphismus ist. Offensichtlich gilt $\varphi(1) = 1$. Seien $A, B \in \mathrm{Mat}(n, R)$. Dann ist

$$(\varphi(A) + \varphi(B))_{ij} = (A_{ij} + \mathfrak{a}) + (B_{ij} + \mathfrak{a}) = (A_{ij} + B_{ij}) + \mathfrak{a} = \varphi(A + B)_{ij}$$

und

$$\begin{aligned}(\varphi(A) \cdot \varphi(B))_{ij} &= \sum_{k=1}^{n} (A_{ik} + \mathfrak{a}) \cdot (B_{kj} + \mathfrak{a}) \\ &= \sum_{k=1}^{n} (A_{ik}B_{kj} + A_{ik}\mathfrak{a} + \mathfrak{a}B_{kj} + \mathfrak{a}\mathfrak{a}) \\ &= \sum_{k=1}^{n} (A_{ik}B_{kj} + \mathfrak{a}) \\ &= \Big(\sum_{k=1}^{n} A_{ik}B_{kj} \Big) + \mathfrak{a} \\ &= \varphi(AB)_{ij}.\end{aligned}$$

Weiter ist offensichtlich $\ker(\varphi) = \mathrm{Mat}(n, \mathfrak{a})$. Somit folgt die Aussage aus dem 1. Isomorphiesatz.

54. Zeige: Ist $\mathbb{F}$ ein endlicher Köper, so ist die multiplikative Einheitengruppe $\mathbb{F}^*$ zyklisch.

Hinweis: Verwende den Hauptsatz über endlich erzeugte abelsche Gruppen und betrachte die Nullstellen des Polynoms $X^n - 1$ (für ein geeignetes n).

Lösung: Nach dem Hauptsatz für endlich erzeugte abelsche Gruppen gibt es positive natürliche Zahlen $m_1, \ldots, m_r$ mit $m_i | m_{i+1}$ und $\mathbb{F}^* \cong \prod_{i=1}^{r} C_{m_i}$. Diese Gruppe ist genau dann zyklisch, wenn $r = 1$ ist. Das ist genau dann der Fall, wenn $m_r = |\mathbb{F}^*|$ gilt. Für alle $a \in \mathbb{F}^*$ muss $a^{m_r} = 1$ sein. Das bedeutet, dass jedes Element aus $\mathbb{F}^*$ eine Nullstelle des Polynoms $X^{m_r} - 1$ ist. Da dieses Polynom aber höchstens m_r verschiedene Nullstellen haben kann, folgt $m_r \geqslant |\mathbb{F}^*|$, also $m_r = |\mathbb{F}^*|$. Somit ist $\mathbb{F}^*$ zyklisch.

55. Zeige: $\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Körper, wenn m prim ist.

Lösung: Nimm zuerst an, dass m keine Primzahl ist. Das bedeutet, dass natürliche Zahlen $1 < k, l < m$ mit $kl = m$ existieren. Dann ist aber $\bar{k}\bar{l} = \bar{m} = \bar{0}$ und somit ist $\mathbb{Z}/m\mathbb{Z}$ nicht nullteilerfrei und a forteriori auch kein Körper.

Sei nun m eine Primzahl. Dann gilt nach Aufgabe 51, dass

$$|\mathbb{Z}/m\mathbb{Z}^*| = \varphi(m) = m - 1 = |\mathbb{Z}/m\mathbb{Z}| - 1$$

ist. Somit ist jedes Element aus $\mathbb{Z}/m\mathbb{Z}\backslash\{\bar{0}\}$ in $\mathbb{Z}/m\mathbb{Z}^*$ und $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper.

56. (a) Zeige: Ist $\varphi : R \to S$ ein Ringhomomorphismus und $\mathfrak{a} \subseteq S$ ein Ideal, dann ist $\varphi^{-1}[\mathfrak{a}]$ ein Ideal in R.

(b) Zeige: Ist $\varphi : R \to S$ ein surjektiver Ringhomomorphismus und $\mathfrak{a} \subseteq R$ ein Ideal, dann ist $\varphi[\mathfrak{a}]$ ein Ideal in S.

Lösung: (a) Aus der Gruppentheorie wissen wir bereits, dass $(\varphi^{-1}[\mathfrak{a}], +)$ eine Untergruppe von $(R, +)$ ist. Sei nun $a \in \varphi^{-1}[\mathfrak{a}]$, d.h. $\varphi(a) \in \mathfrak{a}$, und sei $r \in R$. Weil $\mathfrak{a}$ ein Ideal ist, gilt $\varphi(ra) = \varphi(r)\varphi(a) \in \mathfrak{a}$. Also ist auch $ra \in \varphi^{-1}[\mathfrak{a}]$. Somit ist $\varphi^{-1}[\mathfrak{a}]$ ein Ideal in R.

(b) Aus der Gruppentheorie wissen wir bereits, dass $(\varphi[\mathfrak{a}], +)$ eine Untergruppe von $(S, +)$ ist. Sei nun $a \in \varphi[\mathfrak{a}]$, d.h. es existiert ein $b \in \mathfrak{a}$ mit $a = \varphi(b)$, und sei $s \in S$. Da φ surjektiv ist, existiert ein $r \in R$ mit $\varphi(r) = s$. Daher gilt $sa = \varphi(r)\varphi(b) = \varphi(rb) \in \varphi[\mathfrak{a}]$. Somit ist $\varphi[\mathfrak{a}]$ ein Ideal in R.

57. *2. Isomorphiesatz*: Seien R, S Ringe und $\varphi\colon R \to S$ ein surjektiver Ringhomomorphismus. Sei $\mathfrak{a} \subseteq R$ ein Ideal mit $\ker(\varphi) \subseteq \mathfrak{a}$, und sei ψ wie folgt definiert:

$$\begin{array}{rccc} \psi\colon & R/\mathfrak{a} & \to & S/\varphi[\mathfrak{a}] \\ & r+\mathfrak{a} & \mapsto & \varphi(r)+\varphi[\mathfrak{a}] \end{array}$$

(a) Zeige, dass ψ wohldefiniert ist.

(b) Zeige, dass ψ ein Ringhomomorphismus ist.

(c) Zeige, dass ψ surjektiv und injektiv ist.

Lösung:

(a) Aus Aufgabe 56.(b) folgt, dass $\varphi[\mathfrak{a}]$ ein ideal von S ist, also ist $S/\varphi[\mathfrak{a}]$ ein wohldefinierter Ring. Für $r, r' \in R$ mit $r + \mathfrak{a} = r' + \mathfrak{a}$ gilt $r - r' \in \mathfrak{a}$, also $\varphi(r - r') \in \varphi[\mathfrak{a}]$. Daher ist

$$\varphi(r') + \varphi[\mathfrak{a}] = \varphi(r') + \varphi(r - r') + \varphi[\mathfrak{a}] = \varphi(r) + \varphi[\mathfrak{a}].$$

Wir folgern daraus, dass ψ eine wohldefinierte Abbildung ist.

(b) Für $r, r' \in R$ gilt

$$\psi((r+\mathfrak{a})+(r'+\mathfrak{a})) = \psi(r+r'+\mathfrak{a}) = \varphi(r+r')+\varphi[\mathfrak{a}] = (\varphi(r)+\varphi[\mathfrak{a}])+(\varphi(r')+\varphi[\mathfrak{a}])$$

und

$$\psi((r+\mathfrak{a})\cdot(r'+\mathfrak{a})) = \psi(r\cdot r'+\mathfrak{a}) = \varphi(r\cdot r')+\varphi[\mathfrak{a}] = (\varphi(r)+\varphi[\mathfrak{a}])\cdot(\varphi(r')+\varphi[\mathfrak{a}]).$$

Des weiteren gilt

$$\psi(1+\mathfrak{a}) = \varphi(1)+\varphi[\mathfrak{a}] = 1+\varphi[\mathfrak{a}].$$

Also ist ψ ein Ringhomomorphismus.

(c) Sei $r \in R$ mit $\psi(r + \mathfrak{a}) = 0 + \varphi[\mathfrak{a}]$. Dann folgt $\varphi(r) \in \varphi[\mathfrak{a}]$, also ist $r \in \mathfrak{a}$ und daher $r + \mathfrak{a} = 0 + \mathfrak{a}$. Somit ist ψ injektiv. Sei nun $s \in S$. Dann existiert wegen der Surjektivität von φ ein $r \in R$ mit $\varphi(r) = s$. Dann folgt

$$\psi(r+\mathfrak{a}) = s+\varphi[\mathfrak{a}],$$

also ist ψ surjektiv.