Algebra I

Musterlösung 8

Ringe, Ideale, Einheitengruppe

---

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

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

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 $R = (R_{ij})_{1\leq i,j\leq n} \in \mathrm{Mat}(n,\mathfrak{a})$. 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 $1 \leq i,j,k \leq n$. 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 $1 \leq i,j,k,l \leq n$. 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 $1 \leq i,j \leq n$ 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.

51. Sei n eine positive natürliche Zahl. Definiere die **Eulersche φ-Funktion** durch

$$\varphi(n) := \left|(\mathbb{Z}/n\mathbb{Z})^*\right|.$$

(a) Zeige: Für jede ganze Zahl a, die teilerfremd ist zu n, gilt

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad \textit{d.h.}\ n \mid (a^{\varphi(n)} - 1).$$

(b) Zeige: Existiert eine Zerlegung $n = q_1 \cdot \ldots \cdot q_r$ mit paarweise teilerfremden positiven Zahlen q_i, so ist $\varphi(n) = \prod_{i=1}^{r} \varphi(q_i)$.

(c) Zeige: Ist $n = p_1^{l_1} \cdot \ldots \cdot p_r^{l_r}$ mit paarweise verschiedenen Primzahlen p_i und $l_i > 0$ (für alle i), so gilt

$$\varphi(n) = n \cdot \prod_{i=1}^{r} \Big(1 - \frac{1}{p_i}\Big).$$

Lösung: Aus der Vorlesung wissen wir $(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} : 0 < a \leq n, \mathrm{ggT}(a,n) = 1\}$.

(a) Da $(\mathbb{Z}/n\mathbb{Z})^*$ eine Gruppe ist, folgt

$$\bar{a}^{\varphi(n)} = \bar{a}^{|(\mathbb{Z}/n\mathbb{Z})^*|} = \bar{1} \in (\mathbb{Z}/n\mathbb{Z})^*.$$

Das ist äquivalent zu $n \mid (a^{\varphi(n)} - 1)$.

(b) Wenn $q_1, \ldots, q_r$ teilerfremd sind, dann gilt $\mathbb{Z}/n\mathbb{Z} \cong \bigoplus_{i=1}^{r} \mathbb{Z}/q_i\mathbb{Z}$. Für die Einheitengruppe folgt $(\mathbb{Z}/n\mathbb{Z})^* \cong \prod_{i=1}^{r} (\mathbb{Z}/q_i\mathbb{Z})^*$ und damit

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| = \prod_{i=1}^{r} |(\mathbb{Z}/q_i\mathbb{Z})^*| = \prod_{i=1}^{r} \varphi(q_i).$$

(c) Zuerst berechnen wir

$$n \cdot \prod_{i=1}^{r}\Big(1-\frac{1}{p_i}\Big) = \prod_{i=1}^{r} p_i^{l_i}\Big(1-\frac{1}{p_i}\Big) = \prod_{i=1}^{r} p_i^{l_i-1}(p_i-1).$$

Mit Aufgabe (b) genügt es nun zu zeigen, dass $\varphi(p_i^{l_i}) = p_i^{l_i-1}(p_i-1) = p_i^{l_i} - p_i^{l_i-1}$ ist. Offensichtlich gilt

$$\{a \in \mathbb{N} : 0 < a \leq p_i^{l_i},\ \mathrm{ggT}(a, p_i^{l_i}) = 1\} = \{1, 2, \ldots, p^{l_i}\} \setminus \{p_i, 2p_i, 3p_i, \ldots, (p_i^{l_i-1})p_i\}.$$

Daraus folgt die Behauptung.

52. Sei $R = \mathbb{Z}/201\mathbb{Z} \oplus \mathbb{Z}/102\mathbb{Z} \oplus \mathbb{Z}/96\mathbb{Z}$.

(a) Bestimme die Ordnung $|R^*|$ der Einheitengruppe von R.

(b) Finde das multiplikativ Inverse von $(\overline{13}, \overline{13}, \overline{13})$ in R.

Lösung: (a) Es gilt

$$(\mathbb{Z}/201\mathbb{Z} \oplus \mathbb{Z}/102\mathbb{Z} \oplus \mathbb{Z}/96\mathbb{Z})^* \cong (\mathbb{Z}/201\mathbb{Z})^* \times (\mathbb{Z}/102\mathbb{Z})^* \times (\mathbb{Z}/96\mathbb{Z})^*.$$

Mit Aufgabe 51 berechnen wir

$$\begin{aligned} |(\mathbb{Z}/201\mathbb{Z})^*| &= \varphi(201) = \varphi(3)\cdot\varphi(67) = 2 \cdot 66 = 132 \\ |(\mathbb{Z}/102\mathbb{Z})^*| &= \varphi(102) = \varphi(3)\cdot\varphi(51) = 2 \cdot 50 = 100 \\ |(\mathbb{Z}/96\mathbb{Z})^*| &= \varphi(96) = \varphi(3)\cdot\varphi(2^5) = 2 \cdot 2^4(2-1) = 32. \end{aligned}$$

Daraus ergibt sich $|R^*| = 132 \cdot 32 \cdot 100 = 422400$.

(b) Wir wenden den Euklidischen Algorithmus an. Nämlich

$$\begin{aligned} 201 &= 15 \cdot 13 + 6 \\ 13 &= 2 \cdot 6 + 1 \\ \hline 1 &= 13 - 2 \cdot 6 = 13 - 2 \cdot (201 - 15 \cdot 13) \end{aligned}$$

Daraus ergibt sich

$$\overline{13}^{-1} = \overline{1 + 2 \cdot 15} = 31.$$

Genauso

$$\begin{aligned} 102 &= 7 \cdot 13 + 11 \\ 13 &= 1 \cdot 11 + 2 \\ 11 &= 5 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Wie in der Vorlesung berechnen wir nun

		7	1	5	2
0	1	7	8	47	102

und daher gilt $\overline{13}^{-1} = \overline{(-1)^3 \cdot 47} = \overline{55}$.

Genauso berechnen wir

$$\begin{aligned} 96 &= 7 \cdot 13 + 5 \\ 13 &= 2 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0, \end{aligned}$$

also

		7	2	1	1	2
0	1	7	15	22	37	96

und daher $\overline{13}^{-1} = \overline{(-1)^4 \cdot 37} = \overline{37}$. Insgesamt ist also $(\overline{13}, \overline{13}, \overline{13})^{-1} = (\overline{31}, \overline{55}, \overline{37})$.

53. Sei $\mathbb{F}$ ein Körper und sei $P(X) = a_n X^n + \ldots a_1 X^1 + a_0$ ein Polynom in X mit Koeffizienten in $\mathbb{F}$ vom Grad $n \geq 1$ (*d.h.* $a_n \neq 0$).

(a) Zeige: Gibt es ein $q \in \mathbb{F}$ mit $P(q) = 0$, so existiert ein Polynom $Q(X)$ vom Grad $n-1$ mit $P(X) = (X - q) \cdot Q(X)$.

(b) Zeige: $P(X)$ hat höchstens n verschiedene Nullstellen in $\mathbb{F}$.

Lösung: (a) Nach dem Euklidischen Algorithmus existieren Polynome $Q, R \in \mathbb{F}[X]$ mit $\deg(R) < \deg(X - q) = 1$ und $P(X) = (X - q)Q(X) + R(X)$. In diese Gleichung können wir nun q einsetzen und wir folgern $R(q) = 0$. Da R aber aus Gradgründen ein konstantes Polynom sein muss, ist es somit das Nullpolynom und die Aussage ist bewiesen.

(b) Seien $q_1, \ldots, q_k$ verschiedene Nullstellen von $P(X)$ in $\mathbb{F}$. Sei $Q(X) \in \mathbb{F}[X]$ so, dass $P(X) = (X - q_1)Q(X)$ ist. Wegen $q_2 \neq q_1$ muss $Q(q_2) = 0$ sein. Nun können wir Teil (a) auf $Q(X)$ anwenden. Induktiv finden wir ein Polynom $\tilde{Q}(X)$ mit

$$P(X) = \tilde{Q}(X) \cdot \prod_{i=1}^{k} (X - q_i).$$

Die linke Seite dieser Gleichung ist ein Polynom vom Grad n, die rechte Seite ist ein Polynom vom Grad $\geq k$. Daher gilt $k \leq n$.

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 laut Aufgabe 35 aber höchstens m_r verschiedene Nullstellen haben kann, folgt $m_r \geq |\mathbb{F}^*|$, 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 $\mathbb{Z}/m\mathbb{Z} \setminus \{\bar{0}\}$ in $\mathbb{Z}/m\mathbb{Z}^*$ und $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper.

56. (a) Seien $m, n \in \mathbb{N}$ zwei positive Zahlen und seien $\mathfrak{a} := (m)$ und $\mathfrak{b} := (n)$ die von m *bzw.* n erzeugten Ideale.
Zeige: $\mathfrak{a} + \mathfrak{b} = \mathbb{Z} \iff (m, n) = 1$.

(b) Finde die kleinste positive Zahl $a \in \mathbb{N}$ mit

$$\begin{aligned} a &\equiv 5 \pmod{9}, \\ a &\equiv 8 \pmod{11}, \\ a &\equiv 2 \pmod{14}. \end{aligned}$$

Lösung: (a) Es gilt $\mathfrak{a} + \mathfrak{b} = \{rm + sn : r, s \in \mathbb{Z}\}$. Jedes Element dieser Menge ist durch $\mathrm{ggT}(m, n)$ teilbar, daher ist $\mathrm{ggT}(m, n) = 1$ eine notwendige Bedingung für $\mathfrak{a} + \mathfrak{b} = \mathbb{Z}$. Sei nun $\mathrm{ggT}(m, n) = 1$. Dann ist nach dem Satz von Bézout $1 \in \{rm + sn : r, s \in \mathbb{Z}\}$, also gilt auch $\mathfrak{a} + \mathfrak{b} = \mathbb{Z}$.

(b) Es existieren ganze Zahlen k, l mit

$$k \cdot 9 + 5 = l \cdot 11 + 8,$$

also

$$k \cdot 9 - l \cdot 11 = 3.$$

Wie in Aufgabe 52 finden wir $\tilde{k}, \tilde{l}$ mit $\tilde{k} \cdot 9 - \tilde{l} \cdot 11 = 1$, nämlich $\tilde{k} = 5$ und $\tilde{l} = 4$. Somit ist eine Lösung $k = 3 \cdot \tilde{k} = 15$ und $l = 3 \cdot \tilde{l} = 12$, für diese ist $k \cdot 9 + 5 = 140$. Modulo $9 \cdot 11$ ist das dasselbe wie 41. Jetzt wiederholen wir das Prozedere. Es existieren ganze Zahlen k, l mit

$$k \cdot 99 + 41 = l \cdot 14 + 2,$$

also

$$k \cdot 99 - l \cdot 14 = -39.$$

Wieder gilt $\tilde{k} \cdot 99 - \tilde{l} \cdot 14 = 1$ für $\tilde{k} = 1$ und $\tilde{l} = 7$ und somit ist eine mögliche Lösung $k = -39$ und $l = -273$. Damit gilt $k \cdot 99 + 41 = -3820$. Die kleinste positive Zahl in $\overline{-3820}$ ist $-3820 + 3 \cdot 9 \cdot 11 \cdot 14 = 338$ und somit ist $a = 338$.