14. Übungsblatt

Musterlösungen

Aufgabe 59 a) $\alpha : R \longrightarrow S$ sei ein Ringhomomorphismus.

i) Sei $a \in R^\star$ beliebig. Dann existiert ein $b \in R$ mit $ab = 1_R = ba$. Da α ein Ringhom. ist, folgt

$$\alpha(a)\alpha(b) = \alpha(ab) = \underbrace{\alpha(1_R)}_{=1_S} = \alpha(ba) = \alpha(b)\alpha(a)$$

also $\alpha(a) \in S^\star$ und damit $\underline{\underline{\alpha(R^\star) \subseteq S^\star}}$.

ii) Wegen i) ist nur $\underline{S^\star \subseteq \alpha(R^\star)}$ zu zeigen.

Sei $c \in S^\star$ beliebig. Dann existiert ein $d \in S$ mit $cd = 1_S = dc$. Da α surjektiv ist, besitzen c und d Urbilder a bzw. b in R unter α, also $c = \alpha(a)$ und $d = \alpha(b)$, also

$$\alpha(ab) = \alpha(a)\alpha(b) = cd = \underbrace{1_S}_{=\alpha(1_R)} = dc = \alpha(b)\alpha(a) = \alpha(ba)$$

Da α injektiv ist, folgt $ab = 1_R = ba$, d.h. $a \in R^\star$ und $c = \alpha(a) \in \alpha(R^\star)$. Damit gilt $\underline{\underline{S^\star \subseteq \alpha(R^\star)}}$.

b) **"$\subseteq$"** Sei $(a,b) \in (R \times S)^\star$ beliebig. Dann gibt es ein $(c,d) \in R \times S$ mit

$$(ac, bd) = (a,b)(c,d) = (1_R, 1_S) = (c,d)(a,b) = (ca, db)\,.$$

also $ac = 1_R = ca$ und $bd = 1_S = db$, d.h. $a \in R^\star$ und $b \in S^\star$, woraus $(a,b) \in R^\star \times S^\star$ folgt. Damit ist $\underline{\underline{(R \times S)^\star \subseteq R^\star \times S^\star}}$ gezeigt.

"$\supseteq$" Sei $(a,b) \in R^\star \times S^\star$ beliebig. Dann folgt $a \in R^\star$ und $b \in S^\star$, so daß es Elemente $c \in R$ und $d \in S$ gibt mit $ac = 1_R = ca$ und $bd = 1_S = db$. Dann gilt für $(c,d) \in R \times S$

$$(a,b)(c,d) = (ac, bd) = (1_R, 1_S) = (ca, db) = (c,d)(a,b)\,,$$

d.h. $(a,b) \in (R \times S)^\star$. Folglich $\underline{\underline{R^\star \times S^\star \subseteq (R \times S)^\star}}$.

Insgesamt gilt die Gleichheit.

60. Aufgabe: Eine obere Dreiecksmatrix $A \in \mathrm{D}_n(\mathbb{R})$ ist von der Form $A = \begin{pmatrix} \star & \dots & \star \\ & \ddots & \vdots \\ 0 & & \star \end{pmatrix}$.

a) Seien $A = (a_{ik}), B = (b_{ik}) \in \mathrm{D}_n(\mathbb{R})$. Dann folgt

$$A - B = \begin{pmatrix} a_{11} - b_{11} & \dots & \star \\ & \ddots & \vdots \\ 0 & & a_{nn} - b_{nn} \end{pmatrix} \in \mathrm{D}_n(\mathbb{R}) \text{ und } AB = \begin{pmatrix} a_{11}b_{11} & \dots & \star \\ & \ddots & \vdots \\ 0 & & a_{nn}b_{nn} \end{pmatrix} \in \mathrm{D}_n(\mathbb{R}).$$

Ebenso gilt für die Einheitsmatrix $E \in \mathrm{D}_n(\mathbb{R})$. Also ist $\mathrm{D}_n(\mathbb{R})$ ein Unterring von $\mathrm{M}_n(\mathbb{R})$ und damit selbst ein Ring.

b) Die Abbildung $\alpha : \mathrm{D}_n(\mathbb{R}) \longrightarrow \mathbb{R}^n$ ist definiert durch

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ & \ddots & \vdots \\ 0 & & a_{nn} \end{pmatrix} \longmapsto \begin{pmatrix} a_{11} \\ \vdots \\ a_{nn} \end{pmatrix} .$$

$\mathbb{R}^n$ ist ein Ring bzgl. komponentenweise definierter Addition und Multiplikation. Mit a) folgt

$$\alpha(A+B) = \begin{pmatrix} a_{11}+b_{11} \\ \vdots \\ a_{nn}+b_{nn} \end{pmatrix} = \begin{pmatrix} a_{11} \\ \vdots \\ a_{nn} \end{pmatrix} + \begin{pmatrix} b_{11} \\ \vdots \\ b_{nn} \end{pmatrix} = \alpha(A) + \alpha(B)$$

$$\alpha(AB) = \begin{pmatrix} a_{11}b_{11} \\ \vdots \\ a_{nn}b_{nn} \end{pmatrix} = \begin{pmatrix} a_{11} \\ \vdots \\ a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} \\ \vdots \\ b_{nn} \end{pmatrix} = \alpha(A)\alpha(B)$$

$$\alpha(E) = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \quad \text{(Einselement in } \mathbb{R}^n) .$$

Damit ist α ein Ringhomomorphismus.

Ist $a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{R}^n$ beliebig, so ist die Diagonalmatrix $\begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \in \mathrm{D}_n(\mathbb{R})$ ein Urbild von a unter α. Damit ist α surjektiv.

Für $A = (a_{ik}) \in \mathrm{D}_n(\mathbb{R})$ gilt:

$$A \in \mathrm{Kern}(\alpha) \iff (0) = \alpha(A) = (a_{ii}) \iff A = \begin{pmatrix} 0 & & \star \\ & \ddots & \\ 0 & & 0 \end{pmatrix} ,$$

d.h. A ist eine strikt obere Dreiecksmatrix. Damit ist Kern(α) die Menge aller strikt oberen Dreiecksmatrizen in $\mathrm{D}_n(\mathbb{R})$.

c) Nach dem Ringhomomorphiesatz (13.14) gilt

$$\mathrm{D}_n(\mathbb{R})/\mathrm{Kern}(\alpha) \;\cong\; \mathbb{R}^n ,$$

da α ein surjektiver Ringhomomorphismus ist.

61. Aufgabe: a) "$\Longrightarrow$"

Sei $[a]_n \in \mathbb{Z}_n^\star$. Dann existiert $[b]_n \in \mathbb{Z}_n$ mit

$$[1]_n \;=\; [a]_n[b]_n \;=\; [ab]_n .$$

Dies ist gleichbedeutend mit

$$ab \equiv 1 \pmod{n} .$$

Wegen $n|1-ab$ gibt es ein $k \in \mathbb{Z}$ mit $nk = 1-ab$, d.h.

$$\underline{a}b + \underline{n}k \;=\; 1\,.$$

Da 1 eine ganzzahlige Linearkombination von a und n ist, folgt mit (3.9)

$$\mathrm{ggT}(a,n) \;=\; 1\,.$$

"$\Longleftarrow$"

Sind a und n teilerfremd, so gibt es nach (3.9) Zahlen $b, k \in \mathbb{Z}$ mit $ab + kn = 1$. Also

$$[1]_n = [ab+kn]_n = [ab]_n + [kn]_n = [ab]_n + [0]_n = [ab]_n = [a]_n[b]_n\,.$$

Folglich ist $[a]_n$ eine Einheit in $\mathbb{Z}_n$.

b) Es gilt $\mathbb{Z}_n \;=\; \{\,[0]_n, [1]_n, \ldots, [n-1]_n\,\}$. Sei $k \in \{0,1,2,\ldots,n-1\}$. Nach a) gilt

$$[k]_n \in \mathbb{Z}_n^\star \quad\Longleftrightarrow\quad \mathrm{ggT}(k,n) = 1\,.$$

Also mit (5.8) $\quad |\,\mathbb{Z}_n^\star\,| \;=\; |\{\,k \,|\, 0 \le k \le n-1\,,\, \mathrm{ggT}(k,n) = 1\,\}| \;=\; \varphi(n)\,.$

c) $(\mathbb{Z}_n^\star, \cdot)$ ist eine endliche Gruppe der Ordnung $\varphi(n)$. Sei $a \in \mathbb{Z}$ eine beliebige Zahl, die zu n teilerfremd ist. Dann ist $[a]_n$ nach a) ein Element aus $\mathbb{Z}_n^\star$, und es folgt

$$[a^{\varphi(n)}]_n \;=\; [a]_n^{\varphi(n)} \;=\; [1]_n\,.$$

Also gilt, falls $\mathrm{ggT}(a,n) = 1$

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Bemerkung: Dies ist ein wichtiges Ergebnis der Zahlentheorie. Es geht auf L.Euler und Fermat zurück.

62. Aufgabe: **a)** Nach (9.4) ist die angegebene Abbildung α ein Gruppenisomorphismus der zugrundeliegenden additiven Gruppen.

Noch zu zeigen: $\alpha(x \cdot y) = \alpha(x) \cdot \alpha(y) \quad$ und $\quad \alpha(1) = 1\,.$

Seien $a, b \in \mathbb{Z}$:

$$\begin{aligned}
\alpha([a]_{mn} \cdot [b]_{mn}) &= \alpha([a \cdot b]_{mn}) \\
&= ([a \cdot b]_m, [a \cdot b]_n) \\
&= ([a]_m \cdot [b]_m, [a]_n \cdot [b]_n) \\
&= ([a]_m, [a]_n) \cdot ([b]_m, [b]_n) \\
&= \alpha([a]_{mn}) \cdot \alpha([b]_{mn})
\end{aligned}$$

$\alpha([1]_{mn}) \;=\; ([1]_m, [1]_n) \quad$ (Einselement in $\mathbb{Z}_m \times \mathbb{Z}_n$).

Insgesamt ist $\alpha : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ ein Ringisomorphismus, falls m und n teilerfremd sind.

b) Nach a) und Aufgabe 59 gilt

$$\alpha(\mathbb{Z}_{mn}^\star) \;=\; (\mathbb{Z}_m \times \mathbb{Z}_n)^\star \;=\; \mathbb{Z}_m^\star \times \mathbb{Z}_n^\star$$

Da α bijektiv ist, folgt $|\,\alpha(\mathbb{Z}_{mn}^\star)\,| \;=\; |\,\mathbb{Z}_{mn}^\star\,|$. Also

$$\underline{\underline{|\,\mathbb{Z}_{mn}^\star\,|}} \;=\; |\,\alpha(\mathbb{Z}_{mn}^\star)\,| \;=\; |\,\mathbb{Z}_m^\star \times \mathbb{Z}_n^\star\,| \;=\; \underline{\underline{|\,\mathbb{Z}_m^\star\,| \cdot |\,\mathbb{Z}_n^\star\,|}}\,.$$

Mit Aufgabe 61b) kann man auch sagen: Für teilerfremde natürliche Zahlen m und n gilt

$$\varphi(m \cdot n) \;=\; \varphi(m) \cdot \varphi(n)\,.$$

Bemerkung: Diese Formel besagt, daß die Euler'sche Funktion φ **multiplikativ** ist. Sie ist in der Zahlentheorie ein wichtiges Hilfsmittel, um die Werte der Euler'schen Funktion zu berechnen (s. Aufgabe 63b).

***63. Aufgabe: a)** Es gibt genau p^k Zahlen in $\{1, 2, \ldots, p^k\}$. Wir zeigen im folgenden, daß davon genau p^{k-1} **nicht** teilerfremd zu p^k sind. Daraus folgt dann die Behauptung $\varphi(p^k) = p^k - p^{k-1}$.

Sei $l \in \{1, 2, \ldots, p^k\}$. Dann gilt

$$\mathrm{ggT}(l, p^k) = 1 \quad\Longleftrightarrow\quad \mathrm{ggT}(l, p) = 1 \quad\Longleftrightarrow\quad p \,|\, l \quad\Longleftrightarrow\quad l = mp \text{ mit } 1 \le m \le p^{k-1}\,.$$

Es gibt also genau p^{k-1} Vielfache von p, die $\le p^k$ sind. Dies sind genau die Zahlen aus $\{1, 2, \ldots, p^k\}$, die nicht teilerfremd zu p^k sind.

b) Sei $n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ die kanonische PFZ von $n \ge 2$. Dann sind die Primzahlen $p_1, \ldots, p_r$ paarweise verschieden, damit paarweise teilerfremd, so daß auch die auftretenden Primzahlpotenzen paarweise teilerfremd sind.

Die Aussage von Aufgabe 62b) läßt sich auf endlich viele paarweise teilerfremde Zahlen $n_1, \ldots, n_r$ ausdehnen (durch vollständige Induktion nach $r \ge 2$), d.h. es gilt für solche Zahlen

$$\varphi(n_1 \cdot n_2 \cdot \ldots \cdot n_r) \;=\; \varphi(n_1) \cdot \varphi(n_2) \cdot \ldots \cdot \varphi(n_r)\,.$$

Daraus folgt mit a)

$$\varphi(n) \;=\; \varphi(p_1^{k_1}) \cdot \ldots \cdot \varphi(p_r^{k_r}) \;=\; (p_1^{k_1} - p_1^{k_1-1}) \cdot \ldots \cdot (p_r^{k_r} - p_r^{k_r-1})\,.$$

Beispiel: $\varphi(1400) = \varphi(2^3 \cdot 5^2 \cdot 7) = \varphi(2^3) \cdot \varphi(5^2) \cdot \varphi(7) = (2^3 - 2^2)(5^2 - 5^1)(7-1) = 4 \cdot 20 \cdot 6 = 480$