A-6 Strukturerhaltende Abbildungen

Wir betrachten Abbildungen

$$\phi : \mathcal{M} \mapsto \mathcal{N}$$

zwischen Mengen $\mathcal{M}$ und $\mathcal{N}$, die gegebenenfalls deren algebraische Struktur erhalten. Mittels der Urbilder

$$\phi^{-1}(b) \;=\; \{a \in \mathcal{M} : \phi(a) = b\} \quad \text{für} \quad \mathrm{b} \in \mathcal{N}$$

lassen sich die Eindeutigkeitseigenschaften von Abbildungen wie folgt charakterisieren. ϕ ist

injektiv falls alle $\phi^{-1}(b)$ höchstens ein Element enthalten.
surjektiv falls alle $\phi^{-1}(b)$ mindestens ein Element enthalten.
bijektiv falls alle $\phi^{-1}(b)$ genau ein Element enthalten.

Im letzteren Falle heissen $\mathcal{M}$ und $\mathcal{N}$ gleichmächtig.

Die Elemente abzählbarer Mengen können durchnumeriert und dann mit ihrer Nummer identifiziert werden. Inbesondere kann man jede Menge von $n < \infty$ Elementen darstellen als

$$\mathcal{M} \;=\; \{1, 2, \ldots, n-1, n\}$$

Definition A.59 (Permutationen)

Eine bijektive Abbildung ϕ einer endlichen Menge in sich selbst heisst **Permutation** und lässt sich spezifizieren in der Tupelform

$$(\phi(1),\ \phi(2),\ \phi(3),\ \ldots,\ \phi(n)) \;\in\; \mathbb{N}^n$$

Lemma A.60

Es gibt auf $\mathcal{M}$ genau $n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$ unterschiedliche Permutationen, die bezüglich ihrer Hintereinanderausführung eine nichtkommutative Gruppe mit dem neutralen Element $(1, 2, \ldots, n)$ bilden.

Beispiel A.61

Die dreielementige Menge $\mathcal{M} \;=\; \{1, 2, 3\}$ hat die 6 Permutationen

$$\phi_1 = (1,2,3),\ \phi_2 = (2,1,3),\ \phi_3 = (1,3,2),$$

$$\phi_4 = (3,2,1),\ \phi_5 = (2,3,1),\ \phi_6 = (3,1,2)$$

Als neutrales Element erfüllt ϕ_1 für $i = 1 \ldots 6$

$$\phi_1 \circ \phi_i = \phi_i = \phi_i \circ \phi_1$$

Da ϕ_i für $i = 2, 3, 4$ jeweils ein Element von $\mathcal{M} = \{1, 2, 3\}$ festhält und die anderen beiden austauscht, ist es sein eigenes Inverses, so dass

$$\phi_i \circ \phi_i = \phi_1 \quad \text{für} \quad i = 2, 3, 4$$

Fortsetzung:

Die letzten beiden ϕ_5, ϕ_6 kann man interpretieren als Links- bzw. Rechtsverschiebung aller Elemente. Es gilt also

$$\phi_5 \circ \phi_6 = \phi_1 = \phi_6 \circ \phi_5 \quad \text{und} \quad \phi_5 \circ \phi_5 = \phi_6 \quad , \phi_6 \circ \phi_6 = \phi_5$$

Die Nichtkommutativität sieht man zum Beispiel bei

$$\phi_2 \circ \phi_3 = \phi_5 \;\neq\; \phi_6 = \phi_3 \circ \phi_2\ .$$

Definition A.62 (Homomorphismus und Endomorphismus)

(i) Falls auf $\mathcal{M}$ und $\mathcal{N}$ algebraische Verknüpfungen $+$ und/oder $*$ definiert sind, so dass für alle $a, b \in \mathcal{M}$

$$\phi(a+b) = \phi(a) + \phi(b) \quad \text{und} \quad \phi(a*b) = \phi(a) * \phi(b)$$

dann heisst ϕ ein **Homomorphismus** von $\mathcal{M}$ nach $\mathcal{N}$.

(ii) Falls $\mathcal{M} = \mathcal{N}$, die Struktur $\mathcal{M}$ also in sich selbst abgebildet wird, spricht man auch von einem **Endomorphismus**.

(iii) Je nachdem welche Struktur in $\mathcal{M}$ vorhanden und durch ϕ im obigen respektiert wird, nennt man ϕ einen Halbgruppenhomorphismus, Ringhomomorphismus usw.

Beispiel A.63

Für jede ganze Zahl $m > 1$ ist die Abbildung

$$\phi(a) \;=\; m*a \quad \text{für} \quad a \in \mathbb{Z}$$

ein injektiver Gruppenendomorphismus von $\mathbb{Z}$ in sich selbst. Obwohl $\mathbb{Z}$ und das Bild $\phi(\mathbb{Z})$ Ringe sind, ist ϕ kein Ringhomomorphismus, da z.B.

$$\phi(m*m) \;=\; m^3 \quad \neq \quad m^4 = \phi(m) * \phi(m)$$

Lemma A.64

Für jedes feste $0 \neq m \in \mathbb{Z}$ ist die Abbildung

$$\phi(a) \;=\; r_m(a) \;=\; a \bmod m$$

ein surjektiver Ringhomomorphismus von $\mathbb{Z}$ in den Restklassenring $\mathbb{Z}_m$.

Definition A.65

(i) Bijektive Homomorphismen heissen **Isomorphismen**. Gibt es einen Isomorphismus zwischen den algbraischen Strukturen $\mathcal{M}$ und $\mathcal{N}$, so nennt man diese **isomorph**.

(ii) Bei injektiven Homomorphismen spricht man auch von einer isomorphen Einbettung von $\mathcal{M}$ in $\mathcal{N}$.

Bemerkung:

Sind $\mathcal{M}$ und $\mathcal{N}$ isomorph, so haben sie genau diesselbe Struktur und unterscheiden sich eigentlich nur in der Bezeichnung ihrer Elemente.

Bei isomorphen Einbettungen gilt diese Beziehung (nur) für $\mathcal{M}$ und sein Bild $\phi(\mathcal{M}) \subset \mathcal{N}$.

Es kann aber sogar isomorphe Endomorphismen geben, die nicht unbedingt auf der Hand liegen und sich insbesondere von der Indentität unterscheiden.

Beispiel A.66

Auf dem Matrizenring $\mathbb{Z}^{2\times 2}$ kann man ϕ definieren so dass

$$\phi \quad : \quad \begin{bmatrix} a, b \\ c, d \end{bmatrix} \quad \mapsto \quad \begin{bmatrix} d, c \\ b, a \end{bmatrix}$$

Mit anderen Worten: Die Zeilen und Spalten der 2×2 Matrizen werden ausgetauscht.

Man kann überprüfen, dass ϕ den Ring $\mathbb{Z}^{2\times 2}$ isomorph in sich selbst abbildet und sogar sein eigenes Inverses ist, da $\phi(\,\phi(A)\,) = A$ für alle $A \in \mathbb{Z}^{2\times 2}$.

Beispiel A.67

Ordnet man jedem $a \in \mathbb{Z}$ das $A \in \mathbb{Z}^{2\times 2}$ zu, das a als erstes Diagonalelement hat und sonst nur aus Nullen besteht, so erhält man einen injektiven Ringhomomorphismus ϕ.

Man kann $\mathbb{Z}$ natürlich auch isomorph in $\mathbb{Z}^{2\times 2}$ einbetten, wenn man a durch ϕ in das zweite Diagonalelement von A bringen lässt.
Kopiert ϕ jedoch a in eines der beiden nichtdiagonalen Elemente, so geht die multiplikative Eigenschaft $\phi(a * b) = \phi(a) * \phi(b)$ verloren.

Mit anderen Worten: Das resultierende ϕ ist kein Ringhomomorphismus, sondern nur noch ein injektiver Gruppenhomomorphismus (Siehe Übung). Und das, obwohl dann das aus allen strikt dreiecksförmigen Matrizen bestehende Bild $\phi(\mathbb{Z})$ sogar wiederum ein Ring ist.

Lemma A.68

(i) *Jeder surjektive Homomorphismus ϕ bildet die neutralen und inversen Elemente von $\mathcal{M}$ in die entsprechenden neutralen und inversen Element von $\mathcal{N}$ ab.*

(ii) *Die homomorphen Bilder $\phi(\mathcal{U}) \subset \mathcal{N}$ von Unter(halb)gruppen, Unterringen usw. $\mathcal{U} \subset \mathcal{M}$ bilden dieselben Unterstrukturen von $\mathcal{N}$.*

(iii) *Das* **Kern** *von ϕ genannte Urbild*

$$Kern(\phi) \;=\; \phi^{-1}(0) \;=\; \{a \in \mathcal{M} : \phi(a) = 0 \in \mathcal{N}\}$$

ist bei Gruppenhomomorphismen eine Untergruppe und bei Ringhomomorphismen sogar ein Ideal. Die Quotientengruppe bzw. der Quotientenring von $\mathcal{M}$ bezüglich der durch den Kern definierten Äquivalenz ist isomorph zu dem Bild $\phi(\mathcal{M}) \subset \mathcal{N}$.

Satz A.69

(i) *Alle Endomorphismen einer Gruppe $\mathcal{M}$ in sich selbst bilden bezüglich der Hintereinanderausführung zunächst einen Monoid $Endo(\mathcal{M})$. Dessen neutrales Element ist die Indentitätsabbildung*

$$id_{\mathcal{M}} : \mathcal{M} \mapsto \mathcal{M} \quad mit \quad id_{\mathcal{M}}(a) = a \quad für \quad a \in \mathcal{M}$$

(ii) *Die bijektiven Abbildungen bilden einen Untermonoid $Iso(\mathcal{M}) \subset Endo(\mathcal{M})$ mit multiplikativer nichtkommutativer Gruppenstruktur.*

(iii) *Ist $\mathcal{M}$ selbst kommutative Gruppe, so kann man für jeweils zwei Elemente $\phi, \psi \in Endo(\mathcal{M})$ ihre Summe $\eta = \phi + \psi$ definieren durch*

$$\eta(a) \;=\; (\phi + \psi)(a) \;=\; \phi(a) + \psi(a) \quad für \quad a \in M$$

Bezüglich dieser Addition und der Hintereinanderausführung als Multiplikation bildet $Endo(\mathcal{M})$ einen nichtkommutativen Ring mit Eins.

Beispiel

Für $\mathcal{M} = \mathbb{Z} \times \mathbb{Z}$ erhält man einen Endomorphismenring, der zu dem von uns häufig betrachteten Matrixring $\mathbb{Z}^{2\times 2}$ isomorph ist. Beachte hier, dass algebraische Konzepte geschachtelt angewandt werden, da wir Isomorphie zwischen Ringen sprechen, von denen einer selbst aus Homomorphismen einer Gruppe besteht.

Bemerkung

Die letzte Isomorphieaussage im Lemma A.68 ist von eher theoretischer Bedeutung. Wir werden ihr später wiederbegegnen, wenn es um lineare Abbildungen als Homomorphismen zwischen sogenannten Vektorräumen geht. Nur in dem Zusammenhang muss diese Isomorphie wirklich verstanden werden.