Prof. Dr. H. Brenner **Osnabrück SS 2011**

Körper- und Galoistheorie

Anhang 2

DEFINITION 2.1. Eine *Verknüpfung* $\circ$ auf einer Menge M ist eine Abbildung

$$\circ : M \times M \longrightarrow M,\ (x,y) \longmapsto \circ(x,y) = x \circ y.$$

Statt $\circ(x,y)$ schreibt man $x \circ y$ oder $x * y$ oder einfach xy.

Wenn X ein geometrisches Objekt ist, und $M = \mathrm{Bew}\,(X)$ die Menge der Bewegungen auf X (also die bijektiven Abbildungen von X nach X, die die geometrische Struktur von X respektieren), so ist die Hintereinanderschaltung von Bewegungen, also

$$\mathrm{Bew}\,(X) \times \mathrm{Bew}\,(X) \longrightarrow \mathrm{Bew}\,(X),\ (f,g) \longmapsto g \circ f,$$

eine Verknüpfung.

DEFINITION 2.2. Ein *Monoid* ist eine Menge M zusammen mit einer Verknüpfung

$$\circ : M \times M \to M$$

und einem ausgezeichneten Element $e \in M$ derart, dass folgende beiden Bedingungen erfüllt sind.

(1) Die Verknüpfung ist *assoziativ*, d.h. es gilt

$$(x \circ y) \circ z = x \circ (y \circ z)$$

für alle $x, y, z \in M$.

(2) e ist *neutrales Element* der Verknüpfung, d.h. es gilt

$$x \circ e = x = e \circ x$$

für alle $x \in M$.

Die Hintereinanderausführung von Bewegungen ist assoziativ, da es allgemeiner bei der Hintereinanderausführung von Abbildungen nicht auf die Klammerung ankommt. Die identische Bewegung ist die neutrale Bewegung. In einem Monoid ist das neutrale Element eindeutig bestimmt. Wenn es nämlich zwei Elemente e_1 und e_2 gibt mit der neutralen Eigenschaft, so folgt sofort

$$e_1 = e_1 e_2 = e_2.$$

DEFINITION 2.3. Ein Monoid $(G, \circ, e)$ heißt *Gruppe*, wenn jedes Element ein *inverses Element* besitzt, d.h. wenn es zu jedem $x \in G$ ein $y \in G$ gibt mit $x \circ y = e = y \circ x$.

Die Menge aller Abbildungen auf einer Menge X in sich selbst ist mit der Hintereinanderschaltung ein Monoid; die nicht bijektiven Abbildungen sind aber nicht umkehrbar, so dass sie kein Inverses besitzen und daher keine Gruppe vorliegt. Die Menge der bijektiven Selbstabbildungen einer Menge und die Menge der Bewegungen eines geometrischen Objektes sind hingegen eine Gruppe. In einer Gruppe ist das inverse Element zu einem Element $x \in G$ eindeutig bestimmt. Wenn nämlich y und z die Eigenschaft besitzen, zu x invers zu sein, so gilt

$$y = ye = y(xz) = (yx)z = ez = z.$$

Daher schreibt man das zu einem Gruppenelement $x \in G$ eindeutig bestimmte inverse Element als

$$x^{-1}.$$

DEFINITION 2.4. Eine Gruppe $(G, \circ, e)$ heißt *kommutativ* (oder *abelsch*), wenn die Verknüpfung kommutativ ist, wenn also $x \circ y = y \circ x$ für alle $x, y \in G$ gilt.

LEMMA 2.5. *Sei $(G, e, \circ)$ eine Gruppe. Dann besitzen zu je zwei Gruppenelementen $a, b \in G$ die beiden Gleichungen*

$$a \circ x = b \text{ und } y \circ a = b$$

eindeutige Lösungen $x, y \in G$.

Beweis. Wir betrachten die linke Gleichung. Aus beidseitiger Multiplikation mit a^{-1} (bzw. mit a) von links folgt, dass nur

$$x = a^{-1} \circ b$$

als Lösung in Frage kommt. Wenn man dies einsetzt, so sieht man, dass es sich in der Tat um eine Lösung handelt. □

DEFINITION 2.6. Sei $(G, e, \circ)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt *Untergruppe* von G wenn folgendes gilt.

(1) $e \in H$.
(2) Mit $g, h \in H$ ist auch $g \circ h \in H$.
(3) Mit $g \in H$ ist auch $g^{-1} \in H$.