Prof. Dr. H. Brenner **Osnabrück SS 2015**

Elemente der Algebra

Vorlesung 1

Der Gruppenbegriff

DEFINITION 1.1. Eine *Verknüpfung* $\circ$ auf einer Menge M ist eine Abbildung

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

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

DEFINITION 1.2. 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 $x \in M$.

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

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

Aus der Grundvorlesung sind schon viele kommutative Gruppen bekannt. Zunächst gibt es die additiven Zahlbereiche, also

$$(\mathbb{Z}, 0, +),\ (\mathbb{Q}, 0, +),\ (\mathbb{R}, 0, +),\ (\mathbb{C}, 0, +)\,,$$

wobei jeweils das Inverse durch das Negative einer Zahl gegeben ist. Diese Zahlbereiche haben allerdings über die additive Gruppenstruktur hinaus noch mehr Struktur, nämlich die Multiplikation, die mit der Addition durch die Distributivgesetze verbunden sind. Dies wird später mit dem Begriff des „Ringes“ bzw. des „Körpers“ präzisiert. Bei $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ gilt ferner, dass man durch jede von null verschiedene Zahl „dividieren darf“. Dies ist gleichbedeutend damit, dass multiplikative Gruppen

$$(\mathbb{Q} \setminus \{0\}, 1, \cdot),\ (\mathbb{R} \setminus \{0\}, 1, \cdot),\ (\mathbb{C} \setminus \{0\}, 1, \cdot)$$

vorliegen. Diese werden meistens mit $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$ bezeichnet. Innerhalb der ganzen Zahlen darf man nur durch 1 und -1 dividieren, und in der Tat ist die Menge $\{1, -1\}$ mit der Multiplikation eine Gruppe. Und wenn wir schon bei kleinen Gruppen sind: Es gibt im wesentlichen genau eine Gruppe mit nur einem Element, die man die triviale Gruppe nennt.

Ferner ist der Begriff des Vektorraums bekannt, also beispielsweise der $\mathbb{Q}^n$, $\mathbb{R}^n$, $\mathbb{C}^n$ mit komponentenweiser Addition. Das neutrale Element ist der Nullvektor $0 = (0, \ldots, 0)$, und das Inverse ist wieder das Negative eines Vektors, das wiederum komponentenweise gegeben ist. Diese Gruppen sind alle kommutativ.

Die Drehungen in der Ebene an einem regelmäßigen n-Eck bilden wiederum eine kommutative Gruppe, die aus n Elementen besteht (siehe unten). Die Menge aller ebenen Drehungen zu einem beliebigen Winkel α, $0 \leq \alpha < 2\pi$, ist ebenfalls eine Gruppe, die sogenannte *Kreisgruppe*. Sie ist die Symmetriegruppe des Kreises.

Lösbarkeit von Gleichungen

Häufig wird gesagt, dass es in der Algebra um die Lösbarkeit und die Lösungen von Gleichungen geht.

SATZ 1.5. *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. □

Im Aufbau des Zahlsystems spielt das Bestreben eine wichtige Rolle, Gleichungen eines bestimmten Typs lösbar zu machen. So erklärt sich der Übergang von $\mathbb{N}$ nach $\mathbb{Z}$ dadurch, Gleichungen der Form

$$a + x = b \text{ mit } a, b \in \mathbb{N}\,,$$

lösen zu können, und der Übergang von $\mathbb{Z}$ nach $\mathbb{Q}$ dadurch, Gleichungen der Form

$$ax = b \text{ mit } a, b \in \mathbb{Z},\ a \neq 0\,,$$

lösen zu können.

Potenzgesetze

Sei G eine (multiplikativ geschriebene) Gruppe und $g \in G$ ein Element. Dann definieren wir zu jeder ganzen Zahl $k \in \mathbb{Z}$ die k-te *Potenz* von g, geschrieben g^k, durch

$$g^k = \begin{cases} e_G, \text{ falls } k = 0\,, \\ gg\cdots g \quad k - \text{mal, falls } k \text{ positiv ist}\,, \\ g^{-1}g^{-1}\cdots g^{-1} \quad (-k) - \text{mal, falls } k \text{ negativ ist}\,. \end{cases}$$

Bei additiver Schreibweise schreibt man kg und spricht vom k-ten *Vielfachen* von g.

LEMMA 1.6. *Sei G eine Gruppe und $g \in G$ ein Element, und seien $m, n \in \mathbb{Z}$ ganze Zahlen. Dann gelten die folgenden Potenzgesetze.*

(1) *Es ist $g^0 = e_G$.*
(2) *Es ist $g^{m+n} = g^m g^n$.*

Beweis. Die erste Aussage folgt aus der Definition. Die zweite Aussage ist klar, wenn beide Zahlen ≥ 0 oder beide ≤ 0 sind. Sei also m positiv und n negativ. Bei $m \geq -n$ kann man in $g^m g^n$ „innen“ $-n$-mal g mit g^{-1} zu e_G kürzen, und übrig bleibt die $m - (-n) = (m + n)$-te Potenz von g, also

g^{m+n}. Bei $m < -n$ kann man m-mal g mit g^{-1} kürzen und übrig bleibt die $-n-m = -(m+n)$- te Potenz von g^{-1}. Das ist wieder g^{m+n}. □

Die vorstehende Aussage werden wir später so formulieren, dass ein Gruppenhomomorphismus von $\mathbb{Z}$ nach G vorliegt, siehe hierzu auch Lemma 10.7.

Gruppenordnung und Elementordnung

DEFINITION 1.7. Zu einer endlichen Gruppe G bezeichnet man die Anzahl ihrer Elemente als *Gruppenordnung* oder als die *Ordnung der Gruppe*, geschrieben

$$\operatorname{ord}(G) = \#(G).$$

DEFINITION 1.8. Sei G eine Gruppe und $g \in G$ ein Element. Dann nennt man die kleinste positive Zahl n mit $g^n = e_G$ die *Ordnung* von g. Man schreibt hierfür $\operatorname{ord}(g)$. Wenn alle positiven Potenzen von g vom neutralen Element verschieden sind, so setzt man $\operatorname{ord}(g) = \infty$.

LEMMA 1.9. *Sei G eine endliche Gruppe. Dann besitzt jedes Element $g \in G$ eine endliche Ordnung. Die Potenzen*

$$g^0 = e_G,\ g^1 = g,\ g^2, \ldots, g^{\operatorname{ord}(g)-1}$$

sind alle verschieden.

Beweis. Da G endlich ist, muss es unter den positiven Potenzen

$$g^1,\ g^2,\ g^3, \ldots$$

eine Wiederholung geben, sagen wir $g^m = g^n$ mit $m < n$. Wir multiplizieren diese Gleichung mit g^{-m} und erhalten

$$g^{n-m} = g^m g^{-m} = (g^1 g^{-1})^m = e_G^m = e_G.$$

Also ist die Ordnung von g maximal gleich $n-m$. Mit dem gleichen Argument kann man die Annahme, dass es unterhalb der Ordnung zu einer Wiederholung kommt, zum Widerspruch führen. □

Untergruppen

DEFINITION 1.10. 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 $g^{-1} \in H$.

Man hat beispielsweise die beiden Ketten von sukzessiven additiven Untergruppen,

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

und multiplikativen Gruppen

$$\{1, -1\} \subseteq \mathbb{Q}^\times \subseteq \mathbb{R}^\times \subseteq \mathbb{C}^\times.$$

Die triviale Gruppe $\{e\}$ ist Untergruppe von jeder Gruppe. Untervektorräume eines Vektorraums sind ebenfalls Untergruppen.

LEMMA 1.11. *Sei G eine Gruppe und $H_i \subseteq G$, $i \in I$, eine Familie von Untergruppen. Dann ist auch der Durchschnitt*

$$\bigcap_{i \in I} H_i$$

eine Untergruppe von G.

Beweis. Siehe Aufgabe 2.2. □

DEFINITION 1.12. Sei G eine Gruppe und $M \subseteq G$ eine Teilmenge. Dann nennt man

$$(M) = \bigcap_{M \subseteq H,\, H \text{Untergruppe}} H$$

die von M *erzeugte Untergruppe*.

Insbesondere spricht man zu einer endlichen Menge $g_1, \ldots, g_n \in G$ von der davon erzeugten Untergruppe

$$(g_1, \ldots, g_n)\,.$$

Sie besteht aus allen „Wörtern“ oder „Termen“ (Buchstabenkombinationen) in den g_i und g_i^{-1}. Zu einem einzigen Element g hat die davon erzeugte Gruppe eine besonders einfache Gestalt, sie besteht nämlich aus allen Potenzen

$$g^k,\ k \in \mathbb{Z}\,,$$

wobei diese Potenzen untereinander nicht verschieden sein müssen.

Zyklische Gruppen

DEFINITION 1.13. Eine Gruppe G heißt *zyklisch*, wenn sie von einem Element erzeugt wird.

Die Gruppe $\mathbb{Z}$ der ganzen Zahlen ist zyklisch, und zwar ist 1 aber auch -1 ein Erzeuger. Alle anderen ganzen Zahlen sind kein Erzeuger von $\mathbb{Z}$, da die 1 nur ein ganzzahliges Vielfaches von 1 und von -1 ist (allerdings ist die von einer ganzen Zahl $n \neq 0$ erzeugte Untergruppe „isomorph“ zu $\mathbb{Z}$). Ebenso sind die „Restklassengruppen“

$$\mathbb{Z}/(n) = \{0, 1, \ldots, n-1\}$$

zyklisch, und 1 und -1 sind ebenfalls Erzeuger. Allerdings gibt es dort in aller Regel noch viele weitere Erzeuger; mit deren genauer Charakterisierung werden wir uns bald beschäftigen.

Wie gesagt, in einer zyklischen Gruppe gibt es ein Element g derart, dass man jedes andere Element als g^k mit einer ganzen Zahl $k \in \mathbb{Z}$ schreiben kann, die im Allgemeinen nicht eindeutig bestimmt ist. Daraus folgt sofort die folgende Beobachtung.

LEMMA 1.14. *Eine zyklische Gruppe ist kommutativ.*

Beweis. Das ist trivial. □

Wir erwähnen zwei Modelle für die zyklische Gruppe der Ordnung n.

Eine zyklische Blüte der Ordnung fünf.

BEISPIEL 1.15. Sei $n \in \mathbb{N}$. Dann bilden die ebenen Drehungen um Vielfache des Winkels $360/n$ Grad eine zyklische Gruppe der Ordnung n.

BEISPIEL 1.16. Sei $n \in \mathbb{N}$. Bei Division durch n besitzt jede ganze Zahl k einen eindeutig bestimmten Rest aus

$$\mathbb{Z}/(n) = \{0, 1, \ldots, n-1\},$$

den man mit $k \mod n$ bezeichnet. Auf der Menge dieser Reste kann man addieren, und zwar setzt man

$$a + b := (a + b) \mod n.$$

D.h. man ersetzt die in $\mathbb{Z}$ durch die gewöhnliche Addition gewonnene Summe durch ihren Rest modulo n. Dies ist ebenfalls eine zyklische Gruppe, siehe Aufgabe 1.17, mit 1 als Erzeuger.

Abbildungsverzeichnis