Westfälische Wilhelms-Universität Münster
Fachbereich 10 Mathematik und Informatik

Einführung in die Algebra

Tobias Wedemeier

22. Oktober 2014
gelesen von
Prof. Dr. Kramer

Inhaltsverzeichnis

1 Elementare Gruppentheorie

Erinnerung: eine **Verknüpfung** auf einer nicht leeren Menge X ist eine Abbildung

$$X \times X \to X, (x, y) \mapsto m(x, y).$$

Häufig schreibt man $m(x, y) = xy$ oder $m(x, y) = x + y$, je nach Kontext. Die Schreibweise $m(x, y) = x + y$ wird eigentlich nur für kommutative Verknüpfungen benutzt, d.h. wenn $\forall x, y \in X$ gilt $m(x, y) = m(y, x)$.

1.1 Def. Gruppe

Eine **Gruppe** $(G, \cdot)$ besteht aus einer Verknüpfung $\cdot$ auf einer nicht leeren Menge G, mit folgenden Eigenschaften:

(G1) Die Verknüpfung ist assoziativ, d.h. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ gilt $\forall x, y, z \in G$.
(Folglich darf man Klammern weglassen.)

(G2) Es gibt ein neutrales Element $e \in G$, d.h. es gilt $e \cdot x = x \cdot e = x \forall x \in G$

(G3) Zu jedem $x \in G$ gibt es ein Inverses $y \in G$, d.h. $xy = e = yx$.
man schreibt dann auch $y = x^{-1}$ für das Inverse zu x.

Fordert man von der Verknüpfung nur (G1) und (G2), so spricht man von einer Halbgruppe mit Eins oder einem **Monoid**. Fordert man nur (G1), so spricht man von einer Halbgruppe.

1.2 Beispiel 1

- $(\mathbb{Z}, +), (\mathbb{Q}, +)$ sind kommutative Gruppen.
- $(\mathbb{Z}, \cdot), (\mathbb{N}, \cdot), (\mathbb{N}, +)$ sind Monoide.

1.3 Beobachtungen

a) Das Neutraleelement (einer Verknüpfung) ist eindeutig bestimmt: sind e, e' beides Neutralelemente, so folgt: $e = ee' = e'$

b) Das Inverse zu x ist eindeutig bestimmt:
$xy = e = xy' = y'x \Rightarrow y' = y'e = y'xy = ey = y$

1.4 Lemma 1 (Sparsame Definition von Gruppen)

Sei $G \times G \to G$ eine assoziative Verknüpfung. Dann ist G schon eine Gruppe, wenn gilt:

(i) es gibt $e \in G$ so, dass $ex = x \ \forall x \in G$ gilt.

(ii) zu jedem $x \in G$ gibt es ein $y \in G$ mit $yx = e$

Beweis
Sei $yx = e$, es folgt $yxy = y$. Wähle z mit $zy = e$, es folgt $\underbrace{zy}_{=e} xy = zy = e \Rightarrow xy = e$

Weiter gilt $xe = xyx = ex = x$. □

1.5 Beispiel 2

Sei X eine nicht leere Menge, sei $X^X = \{f : X \to X\}$ die Menge aller Abbildungen von X nach X. Als Verknüpfung auf X nehmen wir die Komposition von Abbildungen. Dann gilt wegen $f = id_X \circ f = f \circ id_X$, dass id_X ein Neutralelement ist.
Damit haben wir ein Monoid $(X_X, \circ)$.
Sei $Sym(X) = \{f : X \to X | f \text{ bijektiv}\}$. Zu jedem $f \in Sym(X)$ gibt es also eine Umkehrabbildung $g : X \to X$ mit $f \circ g = g \circ f = id_X$. Folglich ist $(Sym(X), \circ)$ eine Gruppe, die **Symmetrische Gruppe**.
Wenn X endlich ist mit n Elementen, so gibt es genau $n! = n(n-1)(n-2) \cdot \dots \cdot 2 \cdot 1$ Permutationen, also hat $Sym(X)$ dann genau $n!$ Elemente.

Für $X = \{1, 2, 3, \dots, n\}$ schreibt man auch $Sym(X) = Sym(n)\left(= S_n\right)$.

1.6 Def. zentralisieren

Sei $G \times G \to G$ eine Verknüpfung. Wir sagen, $x, y \in G$ vertauschen oder kommutieren oder x **zentralisiert** y, wenn gilt $xy = yx$.
Eine Gruppe, in der alle Elemente vertauschen heißt kommutativ oder **abelsch**.

1.7 Beispiel 3

(a) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Q}^*, \cdots)$ sind abelsche Gruppen.

(b) K Körper, $G = Gl_2(K) = \{X \in K^{2\times 2} \mid det(X) \neq 0\}$ Gruppe der invertierbaren 2×2 Matrizen.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$\Rightarrow$ nicht abelsch, genauso $Gl_n(K)$ für $n \geq 2$.

(c) $Sym(2)$ ist abelsch, aber $Sym(3)$ nicht. Allgemein ist $Sym(X)$ nicht abelsch, falls $\#X \geq 3$ gilt.

1.8 Def. Untergruppe

Sei G eine Gruppe, sei $H \subseteq G$. Wir nennen H **Untergruppe** von G, wenn gilt:

(UG1) $e \in H$

(UG2) $x, y \in H \Rightarrow xy \in H$

(UG3) $x \in H \Rightarrow x^{-1} \in H$

Offensichtlich ist eine Untergruppe dann wieder eine Gruppe, mit der von G vererbten Verknüpfung.

Bsp

(a) $(\mathbb{Q}, +)$. $\mathbb{Z}$ ist Untergruppe, denn $0 \in \mathbb{Z}, m, n \in \mathbb{Z} \Rightarrow m + n \in \mathbb{Z}$ und $n \in \mathbb{Z} \Rightarrow -n \in \mathbb{Z}$

(b) $(\mathbb{Q}^*, \cdot)$. $\mathbb{Z}^*$ ist keine Untergruppe, kein Inverses.

1.9 Lemma 2

Sei G eine Gruppe und sei U eine nicht leere Menge von Untergruppen von G. Dann ist auch
$\bigcap U = \{g \in G | \forall H \in U \text{ gilt } g \in H\}$
eine Untergruppe von G.
Beweis
Für alle $H \in U$ gilt $e \in H$, also $e \in \bigcap U$. Angenommen $x, y \in \bigcap U$. Dann gilt für alle $H \in U$, dass $xy \in H$ sowie $x^{-1} \in H$. Es folgt $xy \in \bigcap U$ sowie $x^{-1} \in \bigcap U$. □

1.10 Def. $\langle X \rangle$

Sei G eine Gruppe und $X \subseteq G$ eine Teilmenge. Wir setzen:

$$\langle X \rangle = \bigcap \{H \subseteq G | H \text{ Untergruppe und } X \subseteq H\}$$

Ist nicht leer, da mindestens G enthalten ist.

- Es gilt z.B. $\langle \emptyset \rangle = \{e\}$, denn $\{e\}$ ist Untergruppe.
- Ist $H \subseteq G$ Untergruppe mit $X \subseteq H$, so folgt $X \subseteq \langle X \rangle \subseteq H$, insb. also $\langle H \rangle = H$.

Satz
Sei $X \subseteq G$ und sei $W = \{x_1 \cdot x_2, \cdots \cdot x_s | s \geq 1, x_i \in X \text{ oder } x_i^{-1} \in X \ \forall i = 1, \ldots, s\}$.
Dann gilt: $\langle X \rangle = \{e\} \cup W$.
Beweis
Wegen $X \subseteq \langle X \rangle$ und $e \in \langle X \rangle$ folgt $\{e\} \cup W \subseteq \langle X \rangle$. Ist $f, g \in W$, so folgt $fg \in W$ sowie $f^{-1} \in W$, also ist $H = \{e\} \cup W$ eine Untergruppe von G, mit $X \subseteq H$. Es folgt $\langle X \rangle \subseteq H = \{e\} \cup W$. □

1.11 Def. zyklische Gruppe

Sei G eine Gruppe und sei $g \in G$. Für $n \geq 1$ setze $g^n = \underbrace{g \cdot \cdots \cdot g}_{n-mal}$ sowie $g^{-n} = \underbrace{g^{-1} \cdot \cdots \cdot g^{-1}}_{n-mal}$ und $g^0 = e$.
Dann gilt $\forall k, l \in \mathbb{Z}$, dass $g^k \cdot g^l = g^{k+l}$.
Sei $\langle g \rangle = \langle \{g\} \rangle \overset{1.10}{=} \{g^n | n \in \mathbb{Z}\}$. Man nennt $\langle g \rangle$ die von g erzeugte **zyklische Gruppe**. Wenn für ein $n \geq 1$ gilt $g^n = e$, so heißt n ein **Eponent** von g. DIe **Ordnung** von g ist der kleinste Eponent von g,

$$o(g) = min\left(\{n \geq 1 | g^n = 1\} \cup \{\infty\}\right)$$

$o(g) = \infty$ bedeutet: $g^n \neq e \ \forall n \geq 1$
$o(g) = 1$ bedeutet: $g^n = g = e$

1.12 Zyklische Gruppen

Eine Gruppe G heißt **zyklisch**, wenn es ein $g \in G$ gibt mit $G = \langle g \rangle$. Wegen $g^k g^l = g^{k+l} = g^{l+k} = g^l g^k$ gilt: zyklische Gruppen sind abelsch.

Satz
Sei $G = \langle g \rangle$ zyklisch mit $o(g) = n < \infty$. Dann gilt $\#G = n$ und $G = \{g, g^1, g^2, g^3, \ldots, g^n\}$. **Beweis**
Jedes $m \in \mathbb{Z}$ lässt sich schreiben als $m = kn + l$ mit $0 \leq l < n$ (Teilen mit Rest), also $g^m = \underbrace{g^{kn}}_{=e} . g^l = g^l$.

Es folgt $G \subseteq \{g, g^2, \ldots, g^n\}, g^n = g^0$. Ist $g^k = g^l$ für $0 \leq k \leq l < n$, so gilt $e = g^0 = g^{l-k}$, also $l - k = 0$ (wegen$l < n$), also $\#\{g, g^2, \ldots, g^n = g^0\} = n$. □

Folgerung
Ist G endlich mit $\#G = n$ und ist $h \in G$ mit $O(h) = n$, so folgt $\langle h \rangle = G$. Insbesondere ist dann G eine zyklische Gruppe. $\square$

1.13 Nebenklassen

Sei G eine Gruppe und sei H eine Untergruppe. Sei $a \in G$. Wir definieren:

$$aH = \{ah | h \in H\} \subseteq G$$

$$Ha = \{ha | h \in H\} \subseteq G$$

Man nennt aH die **Linksnebenklassen** von a bzgl. H (und Ha die **Rechtsnebenklassen**). In nicht abelschen Gruppen gilt im allgemeinen $aH \neq Ha$.

Lemma
Sei $H \subseteq G$ Untergruppe der Gruppe G und $a, b \in G$.
Dann sind äquivalent:

(i) $b \in aH$

(ii) $bH = aH$

(iii) $bH \cap aH \neq \emptyset$

Beweis

$(i) \Rightarrow (ii):$ $b \in aH \Rightarrow b = ah$ für ein $h \in H \Rightarrow bH = \{ahh' | h' \in H\} \overset{H \text{ Untergruppe}}{=} \{ah'' | h'' \in H\} = aH$

$(ii) \Rightarrow (iii)$: klar

$(iii) \Rightarrow (i)$: Sei $g \in bH \cap aH,\ g = bh = ah' \Rightarrow b = ah'h^{-1} \in aH$, da H Untergruppe

$\square$

Folgerung
Jedes $g \in G$ liegt in genau einer Linksnebenklasse bzgl. H, nämlich $g \in gH$. Entsprechendes gilt natürlich für Rechtsnebenklassen. Man setzt:
$G/H = \{gH \mid g \in G\}$ Menge der Linksnebenklasse, Rechtsnebenklassen analog.

Lemma
Sei $H \subseteq G$ Untergruppe der Gruppe G, sei $a \in G$.
Dann ist die Abbildung $H \to gH, h \mapsto gH$ bijektiv.
Beweis
SSurjektivïst klar nach Definition von gH. Angenommen, $gh = gh' \Rightarrow h = g^{-1}gh' = h'$ $\square$

1.14 Satz von Lagrange

Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Wenn zwei der drei Mengen $G, H, G/H$ endlich sind, dann ist die dritte ebenfalls endlich und es gilt:

$$\#G = \#h \cdot \#G/H$$

Insbesondere ist dann $\#H$ eine **Teiler** von $\#G$.

Beweis
Wenn G endlich ist, dann sind auch H und ${}^G/_H$ endlich.
Angenommen, ${}^G/_H$ und H sind endlich. Dann ist auch $G = \bigcup {}^G/_H = \bigcup\{gH \mid gH \in {}^G/_H\}$ endlich, da $\#gH = \#H$ nach 1.13.
Jetzt zählen wir genauer: sei $\#{}^G/_H = m; \#H = n$ etwa ${}^G/_H = \{g_1H, g_2H, \dots g_mH\}$.
$g_iH \overset{1.13}{=} n \qquad g_iH \cap g_jH = \emptyset$ für $i \neq j$ nach 1.13.
$G = g_1 \cap \#g_2H \cap \dots \cap g_mH \Rightarrow \#G = m \cdot n$ ☐

Bem
(1) Eine entsprechende Aussage gilt für Rechtsnebenklassen.

(2) Die Abbildung $G \to G, \quad g \mapsto g^{-1}$ bildet die Linksnebenklassen bijektiv auf die Rechtsnebenklassen ab:

$$(gH)^{-1} = \{(gh)^{-1} \mid h \in H\} \overset{\text{Achtung!}}{=} \{h^{-1}g^{-1} \mid h \in H\} = \{hg^{-1} \mid h \in H\} = Hg^{-1} \qquad \text{(ÜA)}$$

Korollar A (Lagrange)
Sei G eine endliche Gruppe und sei $g \in G$. Dann teilt $o(g)$ die Zahl $\#G$.
Beweis
Da G endlich ist, folgt $o(g) < \infty$. Nach dem Satz von Lagrange ist $\#\langle g\rangle = o(g)$ ein Teiler von $\#G$. ☐

Korollar B
Sei G eine endliche Gruppe, sei p eine **Primzahl** (d.h. die einzigen Teiler von p sind 1 und p) und $p > 1$. Wenn gilt $\#G = p$, dann ist G zyklisch. Für jedes $g \in G\backslash\{e\}$ gilt $\langle g\rangle = G$.
Beweis
Sei $g \in G\backslash\{e\}$. Dann ist $o(g) > 1$ und $o(g)$ teilt p. Es folgt $o(g) = p$, also $G = \langle g\rangle$ vgl. 1.12. ☐
Für endliche Gruppen sind Teilbarkeitseigenschaften wichtig, wie wir sehen werden.
Die Zahl $\#{}^G/_H := [G : H]$ nennt man auch den **Index von H in G**.

Wichtige Rechenregeln in Gruppen
(a) Man darf kürzen

$$ax = ay \Rightarrow x = y$$
$$xa = ya \Rightarrow x = y$$

(multipliziere beide Seiten von links/rechts mit a^{-1})

(b) Es gilt $(x^{-1})^{-1} = x$ $(x^{-1}x = e = xx^{-1} \Rightarrow (x^{-1})^{-1} = x)$

(c) Beim Invertieren darf die Reihenfolge umgedreht werden:

$(ab)^{-1} = b^{-1}a^{-1}$ $\left(ab(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})ab \Rightarrow (ab)^{-1} = b^{-1}a^{-1}\right)$ (in abelschen Gruppen gilt natürlich damit$(ab)^{-}$

1.15 Homomorphismen

Seien G, K Gruppen. Eine Abbildung $\varphi : G \to K$ heißt **(Gruppen-)Homomorphismus**, wenn $\forall x, y \in G$ gilt

$$\varphi \underbrace{(x \cdot y)}_{\text{Verküpfung in G}} = \underbrace{\varphi(x)\varphi(y)}_{\text{Verknüpfung in K}}$$

Bsp
(a) $id_G : G \to G$ ist Homomorphismus

(b) $H \subseteq G$ Untergruppe $i : H \hookrightarrow G, \quad h \mapsto h$ Inklusion, ist Homomorphismus.

(c) $(G, \cdot) = (\mathbb{Z}, +)\quad m \in \mathbb{Z}\quad \varphi : \mathbb{Z} \to \mathbb{Z}, x \mapsto mx$ ist Homomorphismus, denn $\phi(x+y) = m(x+y) = mx + my = \varphi(x) + \varphi(y)$

(d) G Gruppe, $a \in G,\ a \neq e,\quad \lambda_a(x) = ax.$
$\lambda : G \to G$ ist kein Homomorphismus, denn $\lambda_a(e) = a, \lambda(ee) = a$, aber $\lambda_a(e)\lambda_a(e) = aa \neq a$

Lemma
Sei $\varphi : G \to K$ ein Homomorphismus von Gruppen. Dann gilt $\varphi(e_G) = e_K$ und $\varphi(x^{-1}) = \varphi(x)^{-1}\ \forall x \in G$. ($e_G$ Neutralelement in G und e_K Neutralelement in K)
<u>Beweis</u>

$$\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G) \overset{\text{kürzen}}{\Rightarrow} e_K = \varphi(e_G)$$
$$e_K = \varphi(e_G) = \varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x) \Rightarrow \varphi(x)^{-1} = \varphi(x^{-1})$$

□

<u>Achtung:</u> $\varphi(x)^{-1}$ ist das Inverse in K von $\varphi(x)$ <u>nicht</u> die Umkehrabbildung!

Das **<u>Bild</u>** eines Homomorphismus $\varphi : G \to K$ ist $\varphi(G) \subseteq K$,
der **<u>Kern</u>** ist $ker(\varphi) = \{x \in G \mid \varphi(x) = e_K\} \subseteq G$

1.16 Satz 1

Bild und Kern von Gruppenhomomorphismen sind Untergruppen.

<u>Beweis</u>
Setze $H = \varphi(G) \subseteq K$. Es folgt $e_K \in H$. Für $\varphi(x), \varphi(y) \in H$ gilt $\varphi(x)\varphi(y) = \varphi(xy) \in H$ sowie $\varphi(x)^{-1} = \varphi(x^{-1}) \in H$, also ist H Untergruppe.

Index

Die Seitenzahlen *sind mit Hyperlinks zu den entsprechenden Seiten versehen, also anklickbar!*

Abbildungsverzeichnis