Einfürung in die Algebra Hausaufgaben Blatt Nr. 7

Jun Wei Tan*

Julius-Maximilians-Universität Würzburg

(Dated: December 7, 2023)

Problem 1. Sei G eine Gruppe.

(a) Zeigen Sie, dass die Menge aller Automorphismen von G zusammen mit der Verkettung von Funktionen als Verknüpfung eine Gruppe bildet.

Man nennt diese Gruppe die *Automorphismengruppe* von G und schreibt $\mathrm{Aut}(G)$ für sie.

(b) Zeigen Sie, dass für jedes $g \in G$ durch

$$k_g : G \to G \qquad x \to gxg^{-1}$$

ein Automorphismus von G gegeben ist.

Dies zeigt, dass die Konjugation mit einem beliebigen Gruppenelement g einen Automorphismus von G liefert.

Proof. (a) Wir beweisen die Eigenschaften

(i) Neutrales Element:

Sei $1 : G \to G,\ 1(x) = x\ \forall x \in G$. Es ist klar, dass 1 bijektiv ist. Außerdem ist

$$1(xy) = xy = 1(x)1(y),$$

also 1 ist ein Automorphismus. Außerdem gilt für alle $f \in \mathrm{Aut}(G)$:

$$f1(x) = f(x)\ \forall x \in G,$$

also 1 ist das neutrale Element.

* jun-wei.tan@stud-mail.uni-wuerzburg.de

(ii) Existenz des Inverses: Sei $f \in \mathrm{Aut}(G)$. Weil f bijektiv ist, gibt es auch eine bijektive inverse Abbildung f^{-1}. Es bleibt zu zeigen, dass f^{-1} eine Homomorphismus ist. Sei $x, y \in G$ beliebig. Weil f bijektiv ist, gibt es Elemente $a, b \in G$, so dass $x = f(a)$ und $y = f(b)$ gilt. Per Definition eine inverse Abbildung ist $f^{-1}(x) = a,\ f^{-1}(y) = b$.

Es folgt:

$$\begin{aligned} f^{-1}(xy) &= f^{-1}(f(a)f(b)) \\ &= f^{-1}(f(ab)) && f \text{ ist ein Homomorphismus} \\ &= ab = f^{-1}(x)f^{-1}(y) \end{aligned}$$

also $f^{-1} \in \mathrm{Aut}(G)$.

(iii) Assoziatiativität

Folgt sofort aus der Assoziativität von Funktionverknüpfungen.

(iv) Abgeschlossenheit

Die Verkettung bijektive Abbildungen ist noch einmal bijektiv. Die Verkettung ist auch ein Homomorphismus (Definition 2.58), also $\mathrm{Aut}(G)$ ist abgeschlossen.

(b) Noch einmal zeigen wir alle Eigenschaften. Sei $g \in G$ beliebig. Wir betrachten k_g.

(i) Sie ist ein Homomorphismus.

Sei $x, y \in G$. Es gilt $k_g(x) = gxg^{-1}$ und $k_g(y) = gyg^{-1}$. Daraus folgt:

$$k_g(x)k_g(y) = gxg^{-1}gyg^{-1} = gxyg^{-1} = k_g(xy).$$

(ii) Sie ist injektiv.

Wir zeigen, dass $\mathrm{Ker}(k_g) = \{1\}$. Wir nehmen an, dass es $1 \neq x \in G$ gibt, so dass $k_g(x) = 1$. Dann ist

$$gxg^{-1} = 1 \implies gx = g.$$

Aus der Kurzungsregel folgt $x = 1$, ein Widerspruch.

(iii) Sie ist surjektiv. Sei $y \in G$ und $x = g^{-1}yg$. Dann gilt

$$k_g(x) = gxg^{-1} = gg^{-1}ygg^{-1} = y,$$

also sie ist surjektiv.

$\square$

Problem 2. Unter dem *Zentrum* $Z(G)$ einer Gruppe G versteht man die Menge aller Elemente von G, die mit allen Elementen von G vertauschen, also die Menge $Z(G) = \{g \in G | \text{es gilt } gxg^{-1} = x \text{ für alle } x \in G\}$. Wir definieren die Menge der *inneren Automorphismen von* G durch

$$\text{Inn}(G) := \{k_g | g \in G\} \qquad \text{mit } k_g \text{ wie in 1(b).}$$

Zeigen Sie, dass $Z(G) \trianglelefteq G, \text{Inn}(G) \leq \text{Aut}(G)$ und $G/Z(G) \cong \text{Inn}(G)$ gelten.

Proof. Wir schreiben zuerst einen alternativen Definition:

$$Z(G) = \{g \in G | \text{ es gilt } gx = xg \text{ für alle } x \in G\}.$$

Dann ist auch $1 \in Z(G)$, weil $1x = x1 = x$ für alle $x \in G$ gilt.

(a) $Z(G) \leq G$.

Sei $g, h \in Z(G)$. Dann gilt, für alle $x \in G$:

$$\begin{aligned} ghx(gh)^{-1} &= ghxh^{-1}g^{-1} \\ &= gxg^{-1} && h \in Z(G) \\ &= x && g \in Z(G), \end{aligned}$$

also $Z(G)$ ist abgeschlossen.

Sei jetzt $g \in Z(G)$ mit Inverse g^{-1} (momentan nicht angenommen, dass es in $Z(G)$ ist). Das Ziel ist:

$$g^{-1}xg = x \ \forall x \in G.$$

Weil G eine Gruppe ist, können wir x als y^{-1} schreiben für ein $y \in G$. Es gilt

$$\begin{aligned} g^{-1}y^{-1}g &= (g^{-1}yg)^{-1} \\ &= y^{-1} && g \in Z(G). \end{aligned}$$

Das heißt: $g^{-1}xg = x$ für alle $x \in G$, und alle Elemente in $Z(G)$ sind invertierbar.

(b) $Z(G) \trianglelefteq G$.

Folgt fast sofort per Definition: Wir betrachten die Nebenklassen. Sei $x \in G$. Es gilt

$$
\begin{aligned}
xZ(G) &= \{xg|g \in Z(G)\} \\
&= \{gx|g \in Z(G)\} \\
&= Z(G)x
\end{aligned}
$$

(c) $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$

Sei $f_1, f_2 \in \mathrm{Inn}(G)$, also es gibt $g_1, g_2 \in Z(G)$, so dass

$$
\begin{aligned}
f_1(x) &= g_1 x g_1^{-1} \\
f_2(x) &= g_2 x g^{-1}
\end{aligned}
$$

Dann ist $(f_1 \circ f_2)(x) = g_1 g_2 x g_2^{-1} g_1^{-1} = g_1 g_2 x (g_1 g_2)^{-1}$, also $f_1 \circ f_2 \in \mathrm{Inn}(G)$.

Die Abbildung $f : G \to G,\ f(x) = x = 1x1^{-1}$ ist auch ein Element von $\mathrm{Inn}(G)$. Es ist klar, dass es das neutrale Element ist.

Sei jetzt

$$
\begin{aligned}
f_1(x) &= g_1 x g_1^{-1} \\
f_1^{-1}(x) &= g_1^{-1} x g
\end{aligned}
$$

$f_1^{-1} \in \mathrm{Inn}(G)$, weil $g_1^{-1} \in G$ und $f_1 = k_{g_1^{-1}}$. Es gilt für alle $x \in X$, dass

$$
(f_1 \circ f_1^{-1})(x) = g_1 g_1^{-1} x g_1 g_1^{-1} = x
$$

Also $\mathrm{Inn}(G)$ ist eine Gruppe.

$G/Z(G) \cong \mathrm{Inn}(G)$.

Per Definition ist $\Lambda : g \to k_g$ eine surjektive Abbildung. Weiter ist Λ ein Homomorphismus: Sei $g, h \in G$. Dann ist $\Lambda(gh) = k_{gh}$, wobei $k_{gh}(x) = (gh)x(gh)^{-1}$ für alle $x \in G$. Es gilt

$$
\begin{aligned}
k_{gh}(x) &= (gh)x(gh)^{-1} \\
&= (gh)xh^{-1}g^{-1} \\
&= g(hxh^{-1})g^{-1} \\
&= (k_g \circ k_h)(x)
\end{aligned}
$$

Was ist der Kern des Homomorphismus? $k_g = 1$ genau dann, wenn

$$k_g(x) = gxg^{-1} = x \ \forall x \in G.$$

Der Kern ist per Definition genau das Zentrum. Dann folgt $G/Z(G) \cong \operatorname{Inn}(G)$ aus dem Homomorphiesatz.

$$\begin{tikzcd} G \arrow[r, "g\to k_g"] \arrow[d] & \operatorname{Inn}(G) \\ G/Z(G) \arrow[ur, "\cong"] & \end{tikzcd}$$

□

Problem 3. (a) Nach Beispiel 2.71 operiert S_n auf sich selbst per Konjugation. Beschreiben Sie die Bahnen dieser Operation.

(b) Wir nennen eine Transposition der S_3 *schön*, wen Sie von der Form $(1x)$ mit $x \in \{2,3\}$ ist. Sei das Neutrale von S_3 als Produkt schöner Transpositionen dargestellt. Kommen in diesem Produkt die einzelnen schönen Transpositionen dann stets in gerader Anzahl vor?

Proof. (a) Wir brauchen hier

> **Satz 2.52**
>
> Sei $\varphi = (a_1a_2\dots)(b_1b_2\dots)\dots \in S_n$ in Zykelnotation und $\psi \in S_n$. Dann
>
> $$\psi\varphi\psi^{-1} = (\psi(a_1)\psi(a_2)\dots)(\psi(b_1)\psi(b_2)\dots)\dots.$$

Per Definition sind die Bahnen definiert durch

$$\left\{\sigma'\sigma\sigma'^{-1} | \sigma' \in S_n\right\}.$$

Zu jedem $\sigma \in S_n$ gehört eine (vielleicht nicht eindeutige) Bahn. Wir schreiben σ als Produkt disjunkte Zykeln (im Sinne von Satz 2.41)

Dann zeigen wir zwei Richtungen

(i) Wenn zwei Permutationen die gleichen Zykellänge haben, sind sie konjugiert (Satz 2.53)

Dies zeigt, dass sie in der gleichen Bahn sind.

(ii) Wenn zwei Permutationen bzw. Elemente in S_n unterschiedliche Darstellungen als Produkt disjunkte Zykeln haben, wobei unterschiedliche heißt *nicht* bis auf die Reihenfolge der Faktoren), sind die Permutation nicht konjugiert. Dies folgt aus die Eindeutigkeit der Darstellung von σ als Produkt von disjunkte Zykeln.

Insgesamt gilt: Zwei Elemente liegen in der gleichen Bahn genau dann, wenn die Elemente die gleiche Darstellung als Produkt disjunkte Zykeln haben. Dann gibt es, für jede endliche monoton wachsende Folge

$$(a_1, a_2, \ldots, a_p),\ a_i \in \mathbb{N},\ \sum_{i=1}^{p} a_i \leq n,\ a_1 \leq a_2 \leq \cdots \leq a_p$$

eine Bahn.

(b) Nein. Es gilt $(12)(23) = (123)$, ein Zyklus der Länge 3. Also gilt $[(12)(23)]^3 = (123)^3 = 1$, aber die einzelnen Transpositionen kommen in ungerade Zahlen (3) vor. $\square$

Problem 4. Die Gruppe G operiere auf der Menge M. Weiter sei U eine Untergruppe von G, so dass die auf U eingeschränkte Operation transitiv auf M sei.

Zeigen Sie, dass dann $G = U \cdot G_m$ für alle $m \in M$ gilt.

Proof. Sei $m \in M$ fest, aber beliebig. Sei $U' \subseteq U$ eine minimale Teilmenge von U, so dass $\{xm | x \in U'\} = M$ (möglich weil die Operation transitiv ist). Wir können eine solche Teilmenge konstruieren, indem wir das Ergebnis der Operation xm betrachten und alle andere Elemente mit dem gleichen Ergebnis wegwerfen.

(i) Sei $a, b \in G_m,\ a \neq b$ und $x \in U'$. Dann gilt $xa \neq xb$ (Kürzungsregel)

(ii) Sei $x, y \in U',\ x \neq y$ und $a, b \in G_m$. Dann gilt $xa \neq yb$, weil $xam = xm$ und $ybm = ym$, aber $xm \neq ym$ per Definition von U' als minimale Teilmenge.

(iii) Dann betrachten wir alle Elemente von der Form $xa, x \in U', a \in G_m$. Wir haben schon gezeigt, dass alle solche Elemente unterschiedlich sind. Wie viele Elemente gibt es? $|U'| = |M|$ per Konstruktion und $|G_m| = |G|/|M|$ (Satz 2.71). Daraus folgt, dass

$$|U \cdot G_m| \geq |M|(|G|/|M|) = |G|,$$

also $G \subseteq U \cdot G_M$. Weil wir offenbar per Definition keine Elemente außerhalb G erreichen können, haben wir also $U \cdot G_m \subseteq G$ und daher Gleichheit.

$\square$