1 Anmerkungen zu Wohldefiniertheit

Wohldefiniertheit muss bewiesen werden, wenn von vornherin nicht klar ist, ob eine angegebene Zuordnungsvorschrift eine Abbildung definiert.
Hier gibt es zwei typische Fälle (Beispiele weiter unten). Erstens kann es sein, dass das Bild eines Elementes des Urbildbereichs von Wahlen abhängt, und zweitens kann es sein, dass das Bild kein Element des Bildbereichs ist. Wenn man dies ausschließt, dann hat man die Wohldefiniertheit einer Abbildung gezeigt (Verknüpfungen sind ein Spezialfall).
Ein Beispiel für eine nicht wohldefinierte Verknüpfung (wegen mehrdeutiger Bilder) ist folgendermaßen gegeben:
Sei $G = S_3$ und $H = \{\mathrm{id}, (1\,2\}$. Man kann versuchen auf $G/H = \{H, G_1, G_2\}$ mit $G_1 = \{(1\,3), (1\,2\,3)\}\,, G_2 = \{(2\,3), (1\,3\,2)\}$ eine Multiplikation zu definieren durch $(gH) \cdot (hH) = ghH$. Wenn man dies macht, dann erhält man

$$H = \mathrm{id}\, H = ((1\,2\,3)H) \cdot ((1\,3\,2)H) = ((1\,3)H) \cdot ((2\,3)H) = (1\,3\,2)H \neq H$$

Man kann dieses Beispiel so modifizieren, dass man eine "Abbildung" erhält, bei der das Bild nicht im Bildbereich liegt.
Definiere $(gH)(hH)$ als das Mengenprodukt $gHhH$, dann gilt (da das Mengenprodukt assoziativ ist):

$$\begin{aligned} G_1G_2 &= \{(1\,3), (1\,2\,3)\}\,\{(2\,3), (1\,3\,2)\} \\ &= \{(1\,3)(2\,3), (1\,3)(1\,3\,2), (1\,2\,3)(2\,3), (1\,2\,3)(1\,3\,2)\} \\ &= \{(1\,3\,2), (2\,3), (1\,2), \mathrm{id}\} \notin G/H \end{aligned}$$

Man beachte, dass die beide Alternativen aber eine Multiplikation auf G/H definieren, wenn H eine normale Untergruppe ist. In diesem Fall stimmen sie auch überein. Dies folgt dann aus $gH = Hg$ für alle $g \in G$.

2 Gruppenverknüpfung

Eine Gruppe ist laut Definition ein Paar $(G, \cdot)$, wobei G eine nicht-leere Menge ist und $\cdot : G \times G \to G$ eine Abbildung. Das Bild $\cdot(g, h)$ notiert man mit $g \cdot h$ oder gh.
Ist G eine abelsche Gruppe, so heißt die Verknüpfung oft $+$. Daher suggeriert die Verwendung von $+$, dass es sich um eine abelsche Gruppe handelt. Arbeitet man mit nicht-abelschen Gruppen, so ist die Verwendung des $+$-Zeichens irreführend.
Ebenso sei angemerkt, dass Potenzen bei einer Verknüpfung $+$ nicht mit Exponenten geschrieben werden, sondern mit Faktoren.
Damit ist gemeint, dass man für $m \in \mathbb{N}$ schreibt:

$$\underbrace{g + \ldots + g}_{m-\mathrm{mal}} =: m \cdot g$$

Für negatives $m \in \mathbb{Z}$
$$\underbrace{-(g + \ldots + g)}_{|m|-\text{mal}} =: m \cdot g$$

3 Gruppennachweis

Möchte man nachweisen, dass eine Menge G zusammen mit einer Verknüpfung $\cdot$ eine Gruppe ist, so reicht es neben des nachweises der Assoziativität zu zeigen, dass es ein Element $e \in G$ gibt, dass linksinvers ist und dass es zu jedem Element g ein linksinverses Element g^{-1} gibt.
Alternativ kann man sich auf rechtsneutral und rechtsinvers beschränken. Nicht ausreichend ist es die existenz von einem linksneutralen Element und die Existenz von rechtsinversen Elementen zu zeigen.

4 Lösungen

4.1 Aufgabe 1

Sei G eine Gruppe und H eine Untergruppe vom Index 2, d.h. es gibt genau zwei Links- bzw. Rechtsnebenklassen. Da die Nebenklassen eine Partition der Menge G liefern, ist die von H verschiedene Nebenklasse die Menge $G \setminus H$.
Es gilt nun $gH = H = Hg$ für $g \in H$ und $gH = G \setminus H = Hg$ für $g \in G \setminus H$, also
$$gH = Hg \qquad \forall g \in G.$$
Bemerkung: Man kann auch versuchen zu zeigen, dass G/H die von G induzierte Gruppenstruktur trägt. Dies führt aber im Endeffekt ebenso die Tatsache, dass die von H verschiedene Nebenklasse die Menge $G \setminus H$ ist.

4.2 Aufgabe 2

Die Aussage gilt sogar allgemeiner: Sei $n \geq 2$ und $N \subset S_n$ ein Normalteiler mit $(1\,2) \in N$, dann gilt $N = S_n$.

Beweis: Ist $\pi := (1\,2) \in N$, so ist auch $\gamma\pi\gamma^{-1} \in N$, da N normal ist. Seien nun $i, j \in \{1, 2, \ldots, n\}$ mit $i \neq j$. Definiere
$$\gamma = \gamma_{ij}(k) = \begin{cases} i & \text{für } k = 1 \\ j & \text{für } k = 2 \\ k & \text{sonst.} \end{cases}$$
Dann ist $\gamma\pi\gamma^{-1} = (i\ j)$, also enthält N jede Transposition. Die kleinste Untergruppe von S_n, die alle Transpositionen enthält, ist S_n selbst, da S_n von Transpositionen erzeugt wird. Folglich ist $N = S_n$.

4.3 Aufgabe 3

Sei $\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ein Gruppenhomomorphismus. Da $\mathbb{Z}/m\mathbb{Z}$ zyklisch ist mit Erzeuger $[1]_m$, ist ϕ durch das Bild $\phi([1]_m)$ festgelegt.

- Es gelte $m \mid n$, also ist $c := \frac{n}{m} \in \mathbb{Z}$. Definiere $\phi([x]_m) := [ckx]_n$ mit $k \in \mathbb{Z}$. Wir zeigen, dass dies wohldefiniert ist und dass jeder Homomorphismus von dieser Form ist. Die Homomorphismuseigenschaft folgt sofort aus der Distributivität in $\mathbb{Z}$.
  Wohldefiniertheit: Sei $[x]_m = [y]_m$, wir müssen zeigen, dass $[ckx]_n = [cky]_n$ gilt.
  Es ist nun aber
  $$ckx - cky = \frac{n}{m}k(x-y) = nk\frac{x-y}{m}$$
  und wegen $m \mid x-y$ ist dies in $\mathbb{Z}$, also ϕ wohldefiniert.
  Dies sind alle Homomorphismen: Wir müssen zeigen, dass $\phi([1]_m) = [ck]_n$ für ein $k \in \mathbb{Z}$ gilt. Es ist auf jeden Fall
  $$m\phi([1]_m) = \phi(m\,[1]_m) = \phi([m]_m) = \phi([0]_m) = [0]_n \qquad (*)$$
  Also gilt mit $[a]_n := \phi([1]_m)$:
  $n \mid ma$, also gibt es ein $k \in \mathbb{Z}$ mit $nk = ma$, woraus $a = \frac{n}{m}k = ck$ folgt.

- Es gelte $n \mid m$. Definiere $\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ durch $\phi([x]_m) := [kx]_n$ mit $k \in \mathbb{Z}$. Mehr Homomorphismen kann es offenbar nicht geben, es ist also nur noch die Wohldefiniertheit zu prüfen:
  Teil m die Differenz $x - y$. Weil n ein Teiler von m ist, ist n auch ein Teiler von $kx - ky = k(x-y)$.

- Seien m und n teilerfremd. Die Ordnung von $\phi([1]_m)$ ist offenbar ein Teiler von n (die Ordnung eines Gruppenelementes teilt die Gruppenordnung) und ein Teiler m wegen (*), also ist sie 1. Damit gilt $\phi([1]_m) = [0]_n$, also ist ϕ der triviale Homomorphismus.

4.4 Aufgabe 4

a) Seien $n, m, \ell \in N$ und $g, h, k \in G$ und $\phi_g := \phi(g)$

   – Wir zeigen, dass die Verknüpfung assoziativ ist
   $$\begin{aligned} ((g,n)(h,m))(k,\ell) &= (gh, n\phi_g(m))(k,\ell) \\ = (ghk, n\phi_g(m)\phi_{gh}(\ell)) &\overset{(1)}{=} (ghk, n\phi_g(m)\phi_g(\phi_h(\ell))) \\ \overset{(2)}{=} (ghk, n\phi_g(m\phi_h(\ell))) &= (g,n)(hk, m\phi_h(\ell)) \\ &= (g,n)((h,m)(k,\ell)) \end{aligned}$$

Das Gleichheitszeichen (1) benutzt, dass ϕ ein Homomorphismus ist und (2) benutzt, dass $\phi(g)$ ein Homomrphismus ist.

– (1,1) ist ein Linksneutrales Element

$$(1,1)(g,n) = (1g, 1\underbrace{\phi_1}_{=\mathrm{id}}(n)) = (g,n)$$

– $(g^{-1}, \phi_{g^{-1}}(n^{-1}))$ ist Linksinverses zu (g,n)

$$\begin{aligned}(g^{-1}, \phi_{g^{-1}}(n^{-1}))(g,n) &= (g^{-1}g, n\phi_{g^{-1}}(n^{-1})\phi_{g^{-1}}(n)) \\ &\overset{(3)}{=} (1, n\underbrace{(\phi_{g^{-1}}(n))^{-1}\phi_{g^{-1}}(n))}_{=1}\end{aligned}$$

Bei (3) wird benutzt, dass für einen Homomorphismus ψ gilt: $\psi(x^{-1}) = (\psi(x))^{-1}$

b) Zunächst die Eindeutigkeit: Sei $g \cdot n = h \cdot m$, dann gilt

$$G \ni h^{-1} \cdot g = m \cdot n^{-1} \in N$$

Also $h^{-1} \cdot g$ ist in $G \cap N = \{1\}$, woraus $g \cdot h^{-1} = 1$, also $g = h$ folgt. Genauso folgt $n = m$.
Zur Existenz: Es gilt $g \cdot \phi_{g^{-1}}(n) = (g,1) \cdot (1, \phi_{g^{-1}}(n)) = (g, \phi_g(\phi_{g^{-1}}(n)) = (g, \phi_1(n)) = (g,n)$.

c) Dass $\{1\} \times N$ eine Untergruppe von $G \ltimes N$ ist, ist offensichtlich, da das Produkt von zwei Elementen aus dieser Menge in der ersten Komponente eine 1 stehen hat. Ist nun $(1,m) \in \{1\} \times N$ so gilt:
$r := (g,n)(1,m)(g,n)^{-1}$ hat in der ersten Komponente den Eintrag $g1g^{-1} = 1$, also ist $r \in \{1\} \times N$.

Alternativ kann man sich klar machen, dass $(g,n) \mapsto g$ einen Gruppenhomorphismus von $G \ltimes N \to G$ definiert, dessen Kern gerade $\{1\} \times N$ ist. Kerne sind immer normale Untergruppen.

d) Die Elemente von $\mathrm{Aff}(\mathbb{R}^n)$ sind von der Form $v \mapsto Av + b$ mit $A \in \mathrm{GL}_n(\mathbb{R})$ und $b \in \mathbb{R}^n$. Wir definieren die Abbildung

$$\begin{aligned}\phi : \mathrm{Aff}(\mathbb{R}^n) &\to \mathrm{GL}_n(\mathbb{R}^n) \ltimes \mathbb{R}^n \\ (v \mapsto Av + b) &\mapsto (A,b)\end{aligned}$$

Sie hat offenbar die Abbildung

$$\begin{aligned}\psi : \mathrm{GL}_n(\mathbb{R}^n) \ltimes \mathbb{R}^n &\to \mathrm{Aff}(\mathbb{R}^n) \\ (A,b) &\mapsto (v \mapsto Av + b)\end{aligned}$$

als Inverses. Wir zeigen, dass ϕ ein Homomorphismus von Gruppen ist, also nach dem Vorausgehenden ein Isomorphismus:

$$\begin{aligned}\phi(v \mapsto Av + b)\phi(w \mapsto Bw + c) &= (A, b)(B, c) = (AB, b + Ac) \\ &= \phi(v \mapsto ABv + b + Ac) \\ &= \phi(v \mapsto A(Bv + c) + b)\end{aligned}$$

Es ist $v \mapsto A(Bv + c) + b$ offenbar die Verkettung von $v \mapsto Av + b$ und $w \mapsto Bw + c$.