1 Anmerkungen zu den Korrekturen

Bei folgenden Begriffen traten z.T. Schwierigkeiten auf:

1.1 Nebenklassen

1. Ist $(G, \cdot)$ eine Gruppe, so ist für Teilmengen $A, B \subset G$ die Menge $A \cdot B$ definiert als
$$A \cdot B := \{ab \mid a \in A, b \in B\}.$$
Ist $g \in G$ ein Gruppenelement und $A \subset G$ eine Teilmenge, so ist
$$g \cdot A := \{g\}\, A = \{ga \mid a \in A\}.$$
Im Fall der Gruppe $\mathbb{Z} = (\mathbb{Z}, +)$ und der Teilmenge $\mathbb{Z} \subset \mathbb{Z}$ gilt:
$$\mathbb{Z} + \mathbb{Z} = \mathbb{Z} \qquad \text{und} \qquad 2\,\mathbb{Z} = \{z \in \mathbb{Z} \mid z \text{ ist gerade}\}$$
insbesondere ist also $\mathbb{Z} + \mathbb{Z} \neq 2\,\mathbb{Z}$

2. Ist speziell U eine Untergruppe von G so gilt für alle $u \in U$
$$uU = U$$

3. Die Gruppe $\mathbb{Z}\,/m\,\mathbb{Z}$ hat die Teilmengen $a + m\,\mathbb{Z}$ mit $a \in \mathbb{Z}$ als Elemente. Diese Mengen sollten nicht mit der Zahl a identifiziert werden.
So werden auch unsinnige Gleichungen wie
$$a + m\,\mathbb{Z} = b$$
mit $a, b \in \mathbb{Z}$ vermieden.

1.2 Homomorphismen

1. Lineare Abbildungen sind Abbildungen zwischen k-Vektorräumen (k ein Körper). Die meisten Abbildungen zwischen Gruppen, die man betrachten möchte, sind Gruppenhomomorphismen. Diese nennt man auch kurz Homomorphismen, allerdings *nicht* lineare Abbildungen.

2. Für allgemeine Gruppen gibt es keinen Basis-Begriff, wie im Fall von Vektorräumen. Die sogenannten *freien Gruppen* werden so definiert, dass sie „Basen“ besitzen. Die definierende Eigenschaft unterscheidet sich aber konzeptionell von der aus der linearen Algebra bekannten Definition der Basis eines Vektorraums.

3. Sind G, H Gruppen, $S \subset G$ ein Erzeugendensystem und $\varphi : G \to H$ ein Homomorphismus, so ist φ eindeutig festgelegt durch $\varphi(s)$ mit $s \in S$.
   Warnung: **Nicht jede Zuordnung** $s \mapsto h$ mit $s \in S$ und $h \in H$ definiert einen Gruppenhomomorphismus. Im Regelfall wird so nicht einmal eine Abbildung definiert, wenn $\phi(st) = \phi(s) \cdot \phi(t)$ für alle $s, t \in S$ gelten soll.

4. Ein (Gruppen-)Isomorphismus ist nach Defnition ein bijektiver Gruppenhomomorphismus.
   Wenn man zeigen möchte, dass zwei Gruppen G, H isomorph sind, dann **muss** ein Isomorphismus angegeben werden.

5. Wenn man zeigen möchte, dass ein Gruppenhomomorphismus $\phi : G \to H$ bijektiv ist, dann gibt es zwei (konzeptionell verschiedene) Möglichkeiten:

   (a) Man zeigt, dass die Abbildung ϕ injektiv und surjektiv ist.
   (b) Man zeigt, dass es eine Abbildung $\psi : H \to G$ gibt, so dass $\psi\phi = \mathrm{id}_G$ und $\phi\psi = \mathrm{id}_H$ gilt.

6. Annmerkungen zu den obigen beiden Punkten

   (a) Dass ein Gruppenhomomorphismus $\phi : G \to H$ injektiv ist, ist äquivalent zu der Aussage $\ker \phi = \{1\}$.
   (b) Die Gleichung $\psi\phi = \mathrm{id}_G$ sagt, dass ψ ein Linksinverses zu ϕ ist. Dies sagt insbesondere, dass ϕ injektiv ist.
   Die Gleichung $\phi\psi = \mathrm{id}_H$ sagt, dass ψ ein Rechtsinverses zu ϕ ist. Dies sagt insbesondere, dass ϕ surjektiv ist.
   Dass ψ ein Gruppenhomomorphismus ist, muss **nicht** gezeigt werden, weil es die Umkehrabbildung zu ϕ ist. Die Umkehrabbildung eines Gruppenhomomorphismus ist immer ein Gruppenhomomorphismus.

1.3 Gruppenwirkungen

1. Es ist nicht sinnvoll davon zu sprechen, dass eine Gruppenwirkung „die Identität“ ist. Man sagt: Die Gruppenwirkung ist trivial.

2. Wenn man alle Gruppenoperationen von einer Gruppe G auf einer Menge A angeben möchte, dann genügt es die Linksoperationen anzugeben. Dies hat nichts damit zu tun, ob G kommutativ ist oder nicht. Ist G kommutativ, so ist durch Vertauschen der Argumente jede Linksoperation auch eine Rechtsoparation. Ist G nicht kommutiativ gilt folgendes: Jede Linksoperation

$$\phi : G \times A \to A$$

eine Rechtoperation definiert durch

$$\psi : A \times G \to A, \psi(a, g) := \phi(g^{-1}, a).$$

Außerdem definiert jede Rechtsoperation

$$\psi : A \times G \to A$$

eine Linksoperation durch

$$\phi : G \times A \to A, \phi(g, a) = \psi(a, g^{-1}).$$

2 Lösungen

2.1 Aufgabe 1

Anstelle der geforderten Kombinatorik von Gruppentafeln sei der folgenden Standardbeweis von $G \cong \mathbb{Z}/5\,\mathbb{Z}$ erwähnt:

Sei G eine fünfelementige Gruppe und $a \in G$ mit $a \neq 1 \in G$. Wir betrachten $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ die von a erzeugte Untergruppe. Die Abbildung $\mathbb{N} \to G, n \to a^n$ ist offensichtlich nicht injektiv, d.h. es gibt natürliche Zahlen $n > m$ mit $a^n = a^m$. Daraus folgt, dass die Menge $N = \{n \in \mathbb{N} : a^n = 1\}$ nicht leer ist.
Da jede nichtleere Menge natürlicher Zahlen ein kleinestes Element besitzt (Wohlordnungsprinzip) gibt es ein kleinstes $n_0 \in N$ mit $a^{n_0} = 1$. Es gilt

$$\langle a \rangle = \left\{a^0, a^1, a^2, \ldots, a^{n_0-1}\right\} \qquad (*)$$

Dies sieht man nach Division mit Rest: Ist $n \in \mathbb{Z}$ so gibt es $q, r \in \mathbb{Z}$, so dass

$$n = qn_0 + r \qquad \text{mit } r \in \{0, 1, \ldots, n_0 - 1\} \qquad (**)$$

Also gilt

$$a^n = a^{qn_0+r} = (a^{n_0})^q \cdot a^r = a^r,$$

womit (*) gezeigt ist. Folglich induziert die Abbildung $\mathbb{Z} \to G, n \mapsto a^n$ einen Homomorphismus

$$\mathbb{Z}/n\,\mathbb{Z} \to \langle a \rangle,$$

der als inkektive Abbildung zwischen n_0-elementigen Mengen sogar ein Isomorphismus ist. Da jedes $g \in G$ zu genau einer Linksebenklasse von $G/\langle a \rangle$ gehört (nämlich $g\langle a \rangle$) und jede dieser Nebenklassen genau n_0 Elemente hat, folgt, dass die Ordnung n_0 von $\langle a \rangle$ die Ordnung von G teilt (*Satz von Lagrange*), ist also 1 oder 5. Der erste Fall ist ausgeschlossen, also ist

$$G = \langle a \rangle = \left\{1, a, a^2, a^3, a^4\right\}$$

2.2 Aufgabe 2

Wir definieren

$$\begin{aligned}\phi : \mathbb{Z}/mn\,\mathbb{Z} &\to \mathbb{Z}/m\,\mathbb{Z} \times \mathbb{Z}/n\,\mathbb{Z} \\ a + mn\,\mathbb{Z} &\mapsto (a + m\,\mathbb{Z}, a + n\,\mathbb{Z})\end{aligned}$$

Dies definiert einen Homomorphismus. Wir müssen zeigen, dass ϕ wohldefiniert ist, also

$$a + mn\,\mathbb{Z} = b + mn\,\mathbb{Z} \Longrightarrow a + m\,\mathbb{Z} = b + m\,\mathbb{Z} \text{ und } a + n\,\mathbb{Z} = b + n\,\mathbb{Z}$$

und, dass ϕ ein Homomorphismus ist.
Zum ersten Punkt: $a + mn\,\mathbb{Z} = b + mn\,\mathbb{Z}$ bedeutet: mn teilt $a - b$, also es gibt $z \in \mathbb{Z}$ mit $a - b = zmn$. Somit teilen auch m und n die Differenz $a - b$, womit $a + m\,\mathbb{Z} = b + m\,\mathbb{Z}$ und $a + n\,\mathbb{Z} = b + n\,\mathbb{Z}$. (Bemerkung: Erst jetzt wissen wir, dass ϕ eine Abbildung ist, es also sinnvoll ist, zu fragen, ob ϕ ein Homomorphismus ist.)
Dass ϕ ein Homomorphismus ist, folgt nun durch einfaches Nachrechnen (wir notieren $a_k := a + k\,\mathbb{Z}$):

$$\begin{aligned}\phi(a_{mn} + b_{mn}) &= \phi((a+b)_{mn}) = ((a+b)_m, (a+b)_n) \\ &= (a_m + b_m, a_n + b_n) = (a_m, a_n) + (b_m, b_n) \\ &= \phi(a_{mn}) + \phi(b_{mn})\end{aligned}$$

Sind m und n teilerfremd, so ist ϕ ein Isomorphimus. Wir geben eine Umkehrabbildung $\psi : \mathbb{Z}/m\,\mathbb{Z} \times \mathbb{Z}/n\,\mathbb{Z} \to \mathbb{Z}/mn\,\mathbb{Z}$ an. Da m und n teilerfremd sind, gibt es $x, y \in \mathbb{Z}$ mit $xm + yn = 1$. Wir definieren

$$\psi(a + m\,\mathbb{Z}, b + n\,\mathbb{Z}) := bmx + any + mn\,\mathbb{Z}$$

dies ist wohldefiniert (dies sieht man mit einer ähnlichen Argumentation wie bei ϕ).
Wir zeigen nun, dass ψ ein Links- und Rechtsinverses von ϕ ist:
Linksinvers

$$(\psi\phi)(a + mn\,\mathbb{Z}) = \psi(a + m\,\mathbb{Z}, a + n\,\mathbb{Z}) = \underbrace{amx + any}_{=a\cdot 1} + mn\,\mathbb{Z}$$

Rechtsinvers

$$\begin{aligned}(\phi\psi)(a + m\,\mathbb{Z}, b + n\,\mathbb{Z}) &= \phi(bmx + any + mn\,\mathbb{Z}) \\ &= (bmx + any + m\,\mathbb{Z}, bmx + any + n\,\mathbb{Z}) \\ &= (any + m\,\mathbb{Z}, bmx + \mathbb{Z}) \\ &= (\underbrace{any + amx}_{a} + m\,\mathbb{Z}, \underbrace{bmx + bny}_{b} + \mathbb{Z})\end{aligned}$$

Sind m und n nicht teilerfremd, so gibt es einen gemeinsamen Teiler $1 < d$. Definiere $k := \frac{mn}{d}$, dies ist ein ganzzahliges Vielfaches von m ($\frac{n}{d} \in \mathbb{Z}$) und ein ganzzahliges Vielfaches von n ($\frac{m}{d} \in \mathbb{Z}$). Es ist $k + mn\,\mathbb{Z} \neq mn\,\mathbb{Z}$, weil $d < mn$, allerdings ist

$$\phi(k + mn\,\mathbb{Z}) = (k + m\,\mathbb{Z}, k + n\,\mathbb{Z}) = (m\,\mathbb{Z}, n\,\mathbb{Z}) = \phi(0 + mn\,\mathbb{Z})$$

Also ist ϕ nicht injektiv.

2.3 Aufgabe 3

Eine Gruppenwirkung von $\mathbb{Z}$ bzw. $\mathbb{Z}/2\,\mathbb{Z}$ auf den Mengen $\{1, 2\}$ bzw. $\{1, 2, 3\}$ entspricht einem Gruppenhomomorphismus $\phi : \mathbb{Z} \to S_2$ bzw. $\psi : \mathbb{Z}/2\,\mathbb{Z} \to S_3$.

- Sei $\phi : \mathbb{Z} \to S_2$ ein Morphismus. Da $\mathbb{Z}$ zyklisch ist ($\mathbb{Z}$ wird von 1 erzeugt) wird jeder Homomorphismus von $\mathbb{Z}$ in eine Gruppe durch das Bild von 1 bereits festgelegt:
  Ist $\phi(1) = g \in G$, so gilt $\phi(-1)\phi(1) = \phi(0) = 1 \in G$, also ist $\phi(-1) = g^{-1}$ (Es ist ein Linksinverses zu g). Induktiv ergibt sich:

  $$\phi(n) = \begin{cases} g^n & \text{für } n \geq 0 \\ g^{-|n|} & \text{für } n < 0 \end{cases}$$

  Im vorliegenden Fall gibt es also höchstens zwei Homomorphismen definiert durch: $1 \mapsto \mathrm{id}$ bzw. $1 \mapsto (1\ 2)$. Die erste Zuordnung definiert den trivialen Homomorphismus. Für die zweite Zuordnung sieht man schnell, dass dies die Abbildung $\phi(n) = \begin{cases} \mathrm{id} & \text{für } n \text{ gerade} \\ (1\ 2) & \text{für } n \text{ ungerade} \end{cases}$ definiert. Sie ist ein Homorphismus, weil Summen von zwei geraden bzw. ungeraden Zahlen gerade sind und die Summe von einer ungeraden und einer geraden Zahl ungerade ist.

- Auch ein Homomorphismus ψ von $\mathbb{Z}/2\,\mathbb{Z}$ in eine Gruppe G ist durch das Bild ihres Erzeugers $[1]$ festgelegt. Ist nun $\psi([1]) = g$ so gilt:

  $$g^2 = \psi([1])\psi([1]) = \psi([1] + [1]) = \psi([0]) = 1$$

  Damit bleiben für ψ nur vier Möglichkeiten

  $$[1] \mapsto \mathrm{id}, \quad [1] \mapsto (1\ 2), \quad [1] \mapsto (1\ 3), \quad [1] \mapsto (2\ 3)$$

  Dass hierdurch Gruppenhomomorphismen definiert werden, ist unmittelbar klar.

2.4 Aufgabe 4

Die Elemente von $\mathrm{Sym}(E)$ erhalten Längen und Winkel (sie sind insbesondere orthogonal, erhalten also nach Definition das euklidische Skalarprodukt). Da $E^{[0]}$ auch als die Menge der Punkte in E gesehen werden kann, deren Abstand zum Ursprung $\sqrt{3}$ beträgt, wird $E^{[0]}$ wegen der Längenerhaltung auf sich abgebildet.
Die vierelementige Menge $M = \left\{[-1,1]\, v \mid v \in E^{[0]} \cap \{1\} \times \mathbb{R}^2\right\}$ wird wegen der Winkelerhaltung (zwischen den Endpunkten einer Strecke) auf sich abgebildet.
Wir definieren

$$m_1 := [-1,1]\,(1,1,1)\,, \qquad m_2 := [-1,1]\,(1,-1,1)\,,$$
$$m_3 := [-1,1]\,(1,-1,-1)\,, \qquad m_4 := [-1,1]\,(1,1,-1)$$

Weil M auf sich abgebildet wird, gibt es für $g \in \mathrm{Sym}(E)$ und $i = 1,2,3,4$ ein $\sigma_g(i) \in \{1,2,3,4\}$ mit

$$g.m_i = m_{\sigma_g(i)}$$

Es gilt für $g, h \in G$

$$m_{\sigma_{gh}(i)} = (gh).m_i = g.(h.m_i) = g.(m_{\sigma_h(i)}) = m_{\sigma_g(\sigma_h(i))} = m_{(\sigma_g \circ \sigma_h)(i)}$$

Wegen $\sigma_{\mathrm{id}} = \mathrm{id}_{\{1,2,3,4\}}$ ist also die Abbildung $i \mapsto \sigma_g(i)$ für jedes $g \in \mathrm{Sym}(E)$ invertierbar, also in S_4. Aus dem obigen folgt sofort, dass

$$h : \mathrm{Sym}(E) \to S_4$$

ein Gruppenhomomorphismus ist.
Da h ein Homomorphismus ist, müssen wir nur zeigen, dass es eine Erzeugermenge von S_4 im Bild von h gibt, zum Beispiel die Menge der Transpositionen $\{(1\,2), (1\,3), (1\,4), (2\,3), (2\,4), (3\,4)\}$. Diese Transpositionen sind Bilder der 180° Grad-Drehung um die Achsen

$$d_{12} := \mathbb{R}\,(1,0,1) \qquad d_{13} := \mathbb{R}\,(0,1,1) \qquad d_{14} := \mathbb{R}\,(1,1,0)$$
$$d_{23} := \mathbb{R}\,(1,-1,0) \qquad d_{24} := \mathbb{R}\,(0,-1,1) \qquad d_{34} := \mathbb{R}\,(1,0,-1)$$

Für die Injektivität machen wir uns folgenedes klar: Ist $h(g) = \mathrm{id}$, so gilt

$$\begin{array}{rcrl}
g.(1,1,1) = (1,1,1) & \text{oder} & g.(1,1,1) = (-1,-1,-1) & m_1 \text{ bleibt fix} \\
g.(1,-1,1) = (1,-1,1) & \text{oder} & g.(1,-1,1) = (-1,1,-1) & m_2 \text{ bleibt fix} \\
g.(-1,1,1) = (-1,1,1) & \text{oder} & g.(-1,1,1) = (1,1,-1) & m_1 \text{ bleibt fix} \\
g.(1,1,-1) = (1,1,-1) & \text{oder} & g.(1,1,-1) = (-1,-1,1) & m_1 \text{ bleibt fix}
\end{array}$$

Wegen $(1,1,1) = (-1,1,1) + (1,-1,1) + (1,1,-1)$ gilt auch $g.(1,1,1) = g.(-1,1,1) + g.(1,-1,1) + g.(1,1,-1)$.

Der Fall $g.(1,1,1) = (1,1,1)$ zieht nach sich, dass g auch auf die Vektoren $(-1,1,1), (1,-1,1), (1,1,-1)$ als Identität wirkt:
Eine Summe aus 1 und -1 mit drei Summanden ist genau dann 1, wenn zwei Summanden 1 sind und der dritte -1. Da diese Vektoren ein Erzeugendensystem von $\mathbb{R}^3$ bilden, ist g also die Identität.
Mit dem gleichen Argument sieht man, dass $g.(1,1,1) = (-1,-1,-1)$ nach sich zieht, dass g als Multiplikation mit -1 auf den anderen Vektoren wirkt. Da diese Vektoren $\mathbb{R}^3$ erzeugen, folgt: $g = -\mathrm{id}$, womit g nicht in $SO(3)$ wäre, ein Widerspruch.
Wir haben somit gefolgert, dass $\ker h = \{\mathrm{id}\}$, also h injektiv ist.

Alternativ kann man die Bahnformel verwenden, um $|\operatorname{Sym}(E)| = |S_4| = 24$ zu zeigen. Letzteres folgt aus der Bahnenformel, z.B. wirkt G transitiv auf der Menge der Seitenflächen (6 Elemente) mit Stabilisator die Drehungen um Vielfache von $\pi/2$ um die Seitennormale (4 Elemente), also $|\operatorname{Sym}(E)| = 4 \cdot 6 = |S_4|$ wie behauptet. Ebenso wirkt G tansitiv auf der Eckenmenge mit Stabilsator isomorph zu $\mathbb{Z}/3$, also $|\operatorname{Sym}(E)| = 3 \cdot 8 = |S_4|$.