Lineare Algebra I
Lösungsskizzen zum Tutoriumsblatt 4

Moritz Fleischmann

Zur Vorlesung von Prof. Dr. Fabien Morel, Dr. Andrei Lavrenov und Oliver Hendrichs im Wintersemester 2024-25

Disclaimer: Das sind keine offiziellen Lösungen, sondern nur eine getexte Version der Lösungen zu ausgewählten Aufgaben, die ich in meinem Tutorium bespreche. Fehler, Fragen oder Anmerkungen gerne an m.fleischmann@mnet-online.de .

Wie üblich, wen das Vorgeplänkel nicht interessiert, der kann die Lösungen in den grau hinterlegten Boxen finden.

Aufgabe 1

1. Sei $(G, \cdot)$ eine Gruppe. Wir definieren $\forall g, h \in G : g * h := h \cdot g$. Zeige, dass $(G, *)$ eine zu $(G, \cdot)$ isomorphe Gruppe ist.
2. Sei $(G, \cdot)$ eine Gruppe und sei $()^{-1} : G \to G$ ein Gruppenhomomorphismus. Zeige, dass G abelsch ist.

Lösung:

Bevor wir den Beweis selbst führen, wollen wir uns, wie üblich, klar machen, was wir zeigen wollen und was die verwendeten Begriffe sind. Gruppen hatten wir in der Lösung zum dritten Blatt definiert, hier kommt als neuer Begriff der Homomorphismus hinzu:

Seien $(G, *), (H, \cdot)$ Gruppen. Dann nennen wir eine Abbildung

$$\varphi : G \to H \tag{1}$$

einen *(Gruppen)homomorphismus*, falls gilt, dass

$$\forall g, g' \in G : \varphi(g * g') = \varphi(g) \cdot \varphi(g') \tag{2}$$

Ein Gruppenhomomorphismus erhält also die Struktur einer Gruppe indem es keinen Unterschied macht, ob wir erst den Homomorphismus und dann die Gruppenoperation, oder erst die Gruppenoperation und dann den Homomorphismus anwenden. Wir können also sozusagen, auf eine gewisse Art und Weise, die Struktur der ersten Gruppe G in der Gruppe H wiederfinden. Besonders offensichtlich ist das z.B. bei

$$\varphi : (\mathbb{Z}, +) \to (\mathbb{R}, +) \tag{3}$$
$$z \mapsto z \tag{4}$$

Da die Addition in den ganzen und den reellen Zahlen gleich funktioniert, ist das ein Homomorphismus. Und wir sehen, dass wir die Gruppe der ganzen Zahlen in den reellen Zahlen wiederfinden. Weniger offensichtlich ist das bei anderen Homomorphismen, z.B.

$$\varphi : (\mathbb{R}, +) \to (\mathbb{C} \backslash \{0\}, \cdot) \tag{5}$$
$$x \mapsto e^{ix} \tag{6}$$

Wir berechnen für beliebige Zahlen $x, y \in \mathbb{R}$:

$$\varphi(x+y) = e^{i(x+y)} = e^{ix} \cdot e^{iy} = \varphi(x) \cdot \varphi(y) \tag{7}$$

also ist auch das ein Gruppenhomomorphismus. Die Struktur der Addition auf reellen Zahlen lässt sich also in der Multiplikation auf dem Einheitskreis in der komplexen Ebene wiederfinden. Man sollte allerdings mit der Aussage "Man findet die Struktur der ersten Gruppe in der zweiten wieder" nur mit Vorsicht anwenden, denn zum Beispiel ist bei

$$\varphi : (\mathbb{R}, +) \to (\mathbb{Z}, +) \tag{8}$$
$$x \mapsto 0 \tag{9}$$

nicht mehr wirklich etwas von den reellen Zahlen in den ganzen Zahlen zu finden.
Eine Bemerkung zum Begriff Homomorphismus: Es gibt neben Gruppen noch weitere algebraische Strukturen (z.B. Ringe, Körper, Monoide, Moduln, Vektorräume), einige werden wir in der linearen Algebra noch kennen lernen. Zwischen all diesen Objekten gibt es jeweils auch Homomorphismen. Ob man nun Gruppenhomomorphismus, Vektorraumhomomorphismus, Körperhomomorphismus, etc. sagt, oder einfach nur Homomorphismus, hängt vom Kontext ab. Solange klar ist, welche Art von Homomorphismus gemeint ist, wird die genaue Bezeichnung üblicherweise weggelassen.
Es gibt eine Reihe von Begriffen für Homomorphismen mit speziellen Eigenschaften:

Seien G, H Gruppen und $\varphi : G \to H$ ein Gruppenhomomorphismus. Wir nennen φ einen

- *Monomorphismus*, wenn φ injektiv ist.
- *Epimorphismus*, wenn φ surjektiv ist.
- *Isomorphismus*, wenn φ bijektiv ist.
- *Endomorphismus*, wenn $G = H$ gilt, also φ eine Gruppe auf sich selbst abbildet.
- *Automorphismus*, wenn φ Isomorphismus und Endomorphismus gleichzeitig ist, also ein bijektiver Homomorphismus $\varphi : G \to G$.

Existiert zwischen zwei Gruppen G, H ein Isomorphismus, so nennen wir die Gruppen *isomorph*. Das ist deswegen ein besonderer Begriff, da die Strukturen der beiden Gruppen in diesem Fall wirklich gleich sind. Jedem Element aus G entspricht genau ein Element aus H und die Verknüpfungen zwischen zwei Elementen aus G und den entsprechenden Elementen aus H sind gleichförmig. In der (linearen) Algebra werden wir häufig folgende Situation haben: Wir möchten eine Eigenschaft P für eine algebraische Struktur X zeigen. Das direkt zu zeigen ist allerdings sehr aufwendig. Stattdessen finden wir eine Struktur Y, die zu X isomorph ist und für die wir die Eigenschaft P leichter nachweisen können. Wir betrachten das Problem also aus einem anderen Blickwinkel um es einfacher lösen zu können.

Wir definieren für Homomorphismen noch

Seien G, H Gruppen und $\varphi : G \to H$ ein Homomorphismus. Dann ist der *Kern von* φ die Menge aller Elemente aus G, die auf das neutrale Element in H abgebildet wird. In Formeln:

$$\ker(\varphi) = \{x \in G : \varphi(x) = e_H\} \tag{10}$$

wobei e_H das neutrale Element in H ist.

einige grundlegende Eigenschaften eines Gruppenhomomorphismus $\varphi : G \to H$ sind:

1. Das neutrale Element bleibt erhalten:
$$\varphi(e_G) = e_H \tag{11}$$

2. Inverse Elemente bleiben erhalten:
$$\forall g \in G : \varphi(g^{-1}) = \varphi(g)^{-1} \tag{12}$$
wobei das inverse auf der linken Seite natürlich in G, das inverse der rechten Seite in H liegt.

3. φ ist genau dann injektiv, wenn $\ker(\varphi) = \{e_G\}$ gilt.

Diese Eigenschaften sind leicht nachzuprüfen.

1. Oft ist es hilfreich, sich vor einem Beweis noch einmal genau zu überlegen, welche Informationen einem zur Verfügung stehen und welche Dinge man zeigen will.
Zur Verfügung steht uns hier zum einen, dass $(G, \cdot)$ eine Gruppe ist, also die Gruppenaxiome. In unserem Beweis können wir diese alle verwenden. Zum anderen wissen wir, dass die Abbildung $g * h = h \cdot g$ definiert ist.
Um zu zeigen, dass $(G, *)$ eine zu $(G, \cdot)$ isomorphe Gruppe ist, müssen wir zwei Dinge nachprüfen. Zum einen, dass $(G, *)$ eine Gruppe ist, zum anderen, dass es einen Isomorphismus zwischen den beiden Gruppen gibt. Die Gruppeneigenschaften kennen wir, diese können nacheinander geprüft werden. Um zu zeigen, dass ein Isomorphismus existiert, gibt es verschiedene Werkzeuge, wir kennen jedoch noch keins davon, müssen also auf die simpelste Methode zurückgreifen: Eine Abbildung definieren und prüfen, dass sie ein Isomorphismus ist.

Wir prüfen zuerst, dass $G(, *)$ eine Gruppe ist. Dafür weisen wir Abgeschlossenheit, Assoziativität, Existenz des neutralen und Existenz von inversen Elementen nach.

(a) *Abgeschlossenheit*: Seien $g, h \in G$. Dann gilt $g * h = h \cdot g$. Da $(G, \cdot)$ eine Gruppe ist, wissen wir, dass $h \cdot g$ in G liegt. Also liegt $g * h$ in G, die Operation ist also abgeschlossen.

(b) *Assoziativität*: Auch die Assoziativität der Operation $*$ werden wir auf die Assoziativität in $(G, \cdot)$ zurückführen. Dafür seien $g, h, k \in G$ beliebig:
$$(g * h) * k = k \cdot (g * h) = k \cdot (h \cdot g) = (k \cdot h) \cdot g = (h * k) \cdot g = g * (h * k) \tag{13}$$
also ist $*$ assoziativ auf G.

(c) *Neutrales Element*: Wir wollen zeigen, dass ein neutrales Element in $(G, *)$ existiert. Der einfachste Weg ist hier, eines zu finden und nachzuweisen, dass es wirklich ein neutrales Element ist. Da wir keine weiteren Anhaltspunkte haben, können wir uns anschauen, welche ausgezeichneten Elemente wir bisher kennen. Das sind aber nur das neutrale Element $e.$ von $(G, \cdot)$ und bezüglich eines Elements $g \in G$ das Element selbst und das inverse Element g^{-1} bezüglich $(G, \cdot)$. Das neutrale Element muss unabhängig von unserer Wahl von $g \in G$ sein, also testen wir, ob $e.$ ein neutrales Element bezüglich $*$ ist. Sei $g \in G$ beliebig:
$$e. * g = g \cdot e. = g \tag{14}$$

wobei wir die Eigenschaft von $e.$ verwendet haben, neutrales Element bezüglich $\cdot$ zu sein. Es gilt also $e_* = e.$ für das neutrale Element e_* bezüglich $*$.

(d) *Inverses Element*: Sei $g \in G$ beliebig. Wir wollen zeigen, dass ein inverses Element [a] $-g$ bezüglich $*$ existiert. Ähnlich wie gerade eben, haben wir nicht besonders viel zur Verfügung. Die einzigen ausgezeichneten Elemente sind g selbst, g^{-1} und e_*. Das neutrale Element ist im Allgemeinen nicht invers zu g. Testen wir also g^{-1}

$$g * g^{-1} = g^{-1} \cdot g = e. = e_* \tag{15}$$

wobei wir wieder die Eigenschaften der Gruppe $(G, \cdot)$ verwendet haben. Wir sehen, dass g^{-1} auch das inverse Element bezüglich $*$ ist, also gilt $-g = g^{-1}$.[b]

Wir haben nachgewiesen, dass $(G, *)$ eine Gruppe ist, nun brauchen wir also einen Homomorphismus. Es ist klar, dass der zukünftige Homomorphismus eine Abbildung $\varphi : (G, *) \to (G, \cdot)$ sein wird[c], die Frage ist nur, worauf ein Element $g \in G$ abgebildet wird. Da wir hier kreativ sein müssen, stellt sich wieder die Frage, was wir zur Verfügung haben und sehen, dass das wieder die Elemente g, g^{-1}, e sind. φ ist sicher keine Abbildung auf e, denn das ist im Allgemeinen nicht surjektiv. Testen wir also

$$\varphi : (G, *) \to (G, \cdot) \tag{16}$$
$$g \mapsto g^{-1} \tag{17}$$

Wir prüfen, ob das ein Isomorphismus ist:

(a) *Homomorphismus*: Hierfür müssen wir einfach die bedingende Gleichung nachweisen: Seien $g, h \in (G, *)$, dann gilt:

$$\varphi(g * h) = (g * h)^{-1} = (h \cdot g)^{-1} = g^{-1} \cdot h^{-1} = \varphi(g) \cdot \varphi(h) \tag{18}$$

wobei wir folgende Eigenschaft verwendet haben: Ist M eine beliebige Gruppe, dann gilt für $a, b \in M$, dass $b^{-1}a^{-1}ab = e_M$ gilt, also ist $(ab)^{-1} = b^{-1}a^{-1}$. Wir sehen also, dass φ ein Homomorphismus ist.

(b) *Injektivität*: Wir wenden die obige Äquivalenz an und zeigen, dass der Kern von φ nur das neutrale Element enthält. Sei $g \in \ker(\varphi)$, also $g \in G$, sodass $\varphi(g) = e.$ gilt. Dann gilt:

$$e. = \varphi(g) = g^{-1} \tag{19}$$

Daraus folgt allerdings direkt, dass $g = e. = e_*$ gilt. Da wir für ein beliebiges Element im Kern gezeigt haben, dass es das neutrale Element ist, enthält der Kern nur das neutrale Element (bezüglich $*$) und die Abbildung φ ist injektiv.

(c) *Surjektivität*: Sei $g \in G$ ein beliebiges Element, dann wollen wir zeigen, dass es ein Urbild hat. In diesem Fall ist das allerdings offensichtlich, denn jedes Element hat ein Inverses und Inversion ist involutiv, es gilt also

$$\varphi(g^{-1}) = (g^{-1})^{-1} = g \tag{20}$$

das heißt jedes Element wird von seinem eigenen Inversen getroffen, also ist φ surjektiv.

Da wir alle Eigenschaften geprüft haben, sehen wir, dass φ ein Isomorphismus ist. Folglich sind $(G, *)$ und $(G, \cdot)$ isomorph.

[a] Wir bezeichnen hier das inverse Element bezüglich $*$ mit $-g$ um es von dem inversen Element g^{-1} bezüglich $\cdot$ zu unterscheiden. Das dient nur der Übersicht.

[b] Hätten wir hier mit g angefangen, dann wäre unsere Rechnung $g * g = g \cdot g$ und darüber können wir weiter nichts aussagen. Im Allgemeinen wird es nicht e. sein.

[c] Man könnte hier auch $\psi : (G, \cdot) \to (G, *)$ wählen. Ist eine Gruppe G zu einer Gruppe H isomorph, so ist natürlich automatisch H zu G isomorph, da eine bijektive Abbildung immer ein bijektives Inverses hat. Die Frage ist hier lediglich, ob dieses Inverse auch ein Homomorphismus ist. Die Antwort ist ja, aber ich weiß nicht, ob das in der Vorlesung so gezeigt wurde. Es ist aber nicht schwer zu zeigen.

Natürlich ist ein Beweis in dieser Ausführlichkeit nicht erforderlich.

2. Hier wissen wir folgendes:
   G ist eine Gruppe mit der Gruppenoperation $\cdot$. Außerdem ist

$$\psi : G \to G \tag{21}$$
$$g \mapsto g^{-1} \tag{22}$$

ein Homomorphismus.
Wir wollen zeigen:
G als Gruppe ist abelsch, also gilt $\forall g, h \in G : g \cdot h = h \cdot g$.

Seien $g, h \in G$. Dann gilt:

$$g \cdot h = ((g \cdot h)^{-1})^{-1} = \psi((g \cdot h)^{-1}) = \psi(h^{-1} \cdot g^{-1}) = \psi(h^{-1}) \cdot \psi(g^{-1}) = h \cdot g \tag{23}$$

wobei wir wieder $(g^{-1})^{-1} = g$ und $(gh)^{-1} = h^{-1}g^{-1}$ verwendet haben. Die Gruppe ist also abelsch.

Man beachte hierbei, dass der Homomorphismus φ aus der ersten Teilaufgabe und der Homomorphismus ψ aus der zweiten Aufgabe *nicht* die gleiche Abbildung sind. Zwar bilden sie als Abbildung auf Mengen gleich ab, aber als Abbildung auf Gruppen unterscheiden sie sich, da die Definitionsmenge jeweils eine andere Gruppe ist.

Aufgabe 2
Sei U eine beliebige Menge. Zeige, dass $(\mathcal{P}(U), \Delta)$ eine Gruppe ist. Aufgabe 1 vom ersten Tutoriumsblatt darf verwendet werden.

Lösung:
Da wir die erste Aufgabe des ersten Blattes verwenden dürfen, wollen wir kurz wiederholen, was die (für Δ relevanten) Aussagen waren. Seien dafür $A, B, C \subseteq U$ beliebig:

$$A \Delta B = B \Delta A \tag{24}$$
$$(A \Delta B) \Delta C = A \Delta (B \Delta C) \tag{25}$$
$$A \Delta \varnothing = A \tag{26}$$
$$A \Delta A = \varnothing \tag{27}$$

Wir nennen diese Aussagen nun $(\Delta 1)$ bis $(\Delta 4)$.

Wir wollen zeigen, dass $(\mathcal{P}(U), \Delta)$ eine Gruppe ist. Also zeigen wir die Eigenschaften:

1. *Abgeschlossenheit*: Die symmetrische Differenz zweier Teilmengen von U ist offensichtlich wieder eine Teilmenge von U.

2. *Assoziativität*: Das ist Aussage $(\Delta 2)$.

3. *Neutrales Element*: Aussage $(\Delta 3)$ sagt uns direkt, dass $\varnothing$ das neutrale Element bezüglich Δ ist.

4. *Inverses Element*: Aussage $(\Delta 4)$ sagt uns direkt, dass A sein eigenes Inverses bezüglich Δ ist.

Da wir alle Eigenschaften gezeigt haben, ist $(\mathcal{P}(U), \Delta)$ eine Gruppe und wir sind fertig.

Man sieht also, dass der Beweis unter Verwendung bereits gezeigter Aussagen recht kurz werden kann. Mithilfe von $(\Delta 1)$ könnte man direkt sehen, dass wir sogar eine abelsche Gruppe haben.

Aufgabe 3
Sei X eine Menge. Zeige:

1. Die Menge der Bijektionen S_X ist eine Gruppe bezüglich Komposition.

2. Sei $Y \subseteq X$ eine Menge und sei für $g \in S_Y$ die folgende Abbildung $i(g) \in S_X$ definiert:

$$i(g)(x) := \begin{cases} g(x), & x \in Y \\ x, & x \in X \setminus Y \end{cases} \tag{28}$$

   Zeige, dass $i : S_Y \to S_X$ ein Monomorphismus von Gruppen ist.

3. Sei $f : X \to Y$ eine Bijektion. Zeige, dass f einen Gruppenisomorphismus zwischen S_X und S_Y induziert.

Lösung:
Nur als Bemerkung, weil man davon viel Gebrauch machen wird.

Sei X eine Menge. Dann ist

$$\mathsf{Bij}(X) := S_X := \mathfrak{S}_X := \{f : X \to X \mid f \text{ bijektiv}\} \tag{29}$$

die sogenannte *symmetrische Gruppe auf X*, bzw. die Menge der *Permutationen auf X*.

Die Schreibweise $\mathsf{Bij}(X)$ ist eher selten. Ist X eine Menge mit $n \in \mathbb{N}$ Elementen, schreibt man auch S_n.

1. Wir prüfen wie üblich die Gruppenaxiome:

   (a) *Abgeschlossenheit*: Seien $f, g \in S_X$. Dann müssen wir zeigen, dass $f \circ g$ ebenfalls in S_X liegt. Wir haben in Aufgabe 2, auf dem zweiten Tutoriumsblatt bereits gezeigt, dass die Verknüpfung zweier bijektiver Abbildungen wieder bijektiv ist, also ist $f \circ g \in S_X$ klar.

   (b) *Assoziativität*: Die Komposition von Abbildungen ist immer assoziativ, also gibt es nichts zu zeigen.

(c) *neutrales Element*: Wir wählen als neutrales Element die Identität

$$\mathbb{1}_X : X \to X \tag{30}$$
$$x \mapsto x \tag{31}$$

die jedes Element auf sich selbst abbildet. Offenbar liegt $\mathbb{1}_X$ in S_X. Sei $f \in S_X$. Um die Gleichheit von zwei Abbildungen zu zeigen, lassen wir sie auf ein beliebiges Element $x \in X$ wirken und zeigen, dass das Ergebnis das gleiche ist:

$$(f \circ \mathbb{1}_X)(x) = f(\mathbb{1}_X(x)) = f(x) \tag{32}$$

Also ist $f \circ \mathbb{1}_X = f$, das heißt $\mathbb{1}_X$ ist das neutrale Element bezüglich Komposition.

(d) *inverses Element*: Wie wir bereits auf Tutoriumsblatt 1, Aufgabe 2 gezeigt haben, ist eine Abbildung genau dann bijektiv, wenn eine inverse Abbildung existiert und diese inverse Abbildung ist wieder bijektiv. Eine inverse Abbildung erfüllt genau die Eigenschaften eines inversen Elements im Sinne der Gruppe, denn sei $f \in S_X$ mit inverser Abbildung $f^{-1} \in S_X$, dann gilt

$$f \circ f^{-1} = f^{-1} \circ f = \mathbb{1}_X \tag{33}$$

und wir hatten gezeigt, dass $\mathbb{1}_X$ das neutrale Element bezüglich Komposition ist.

Da wir gezeigt haben, dass alle Gruppenaxiome gelten, ist S_X eine Gruppe.

2. Wir müssen die beiden Eigenschaften prüfen, die einen Monomorphismus ausmachen: Injektivität und Linearität:

(a) *Homomorphismus*: Seien $f, g \in S_Y$, dann müssen wir zeigen, dass $i(f \circ g) = i(f) \circ i(g)$ gilt. Die Gleichheit zeigen wir durch die Wirkung auf Elemente $x \in X$. Hierbei ist nun wichtig ob $x \in Y$ oder $x \in X\backslash Y$ liegt, also machen wir eine Fallunterscheidung. Wir betrachten zuerst die linke Seite. Für $x \in Y$ gilt:

$$i(f \circ g)(x) = (f \circ g)(x) = f(g(x)) \tag{34}$$

Für $x \in X\backslash Y$ gilt:

$$i(f \circ g)(x) = x \tag{35}$$

Dann betrachten wir die rechte Seite. Für $x \in Y$ gilt:

$$(i(f) \circ i(g))(x) = i(f)(i(g)(x)) = i(f)(g(x)) = f(g(x)) \tag{36}$$

wobei wir in der dritten Gleichheit verwendet haben, dass g eine Bijektion auf Y ist. Da $x \in Y$ gilt, gilt also auch $g(x) \in Y$ und damit $i(f)(g(x)) = f(g(x))$ per Definition. Zuletzt noch die rechte Seite für $x \in X\backslash Y$

$$(i(f) \circ i(g))(x) = i(f)(i(g)(x)) = i(f)(x) = x \tag{37}$$

wobei wir jeweils nur die Definition von i verwendet haben. Vergleichen wir beide Fälle für die linke und rechte Seite sehen wir, dass die beiden Abbildungen auf allen Elementen übereinstimmen. Also sind sie die gleiche Abbildung und i ist ein Homomorphismus.

(b) *Injektivität*: Sei $f \in \ker(i)$, es gelte also $f \in S_Y$ mit $i(f) = \mathbb{1}_X$, da wir aus der ersten Teilaufgabe wissen, dass $\mathbb{1}_X$ das neutrale Element auf S_X bezüglich der Komposition ist. Dann wissen wir

$$\left.\begin{matrix} f(x), & x \in Y \\ x, & x \in X\backslash Y \end{matrix}\right\} = i(f) = \mathbb{1}_X = \begin{cases} x, & x \in Y \\ x, & x \in X\backslash Y \end{cases} \tag{38}$$

also gilt für alle Elemente $x \in Y$, dass $f(x) = x$ gilt, folglich ist f das neutrale Element $\mathbb{1}_Y$ von S_Y. Das ist äquivalent zur Injektivität von i.

Bei den beiden Teilaufgaben haben wir nun gesehen, dass die Objekte (Funktionen, bzw. Mengen von Funktionen sind auch Objekte) mit denen wir es zu tun haben, zwar komplizierter aussehen als vorher und ihre Elemente bestimmte Eigenschaften haben, die wir verwenden müssen, die grundlegenden Ideen bleiben allerdings genau gleich.

3. Wir müssen hier nun nachweisen, dass eine Abbildung einen Gruppenisomorphismus induziert. Dazu müssen wir uns überhaupt erst darüber klar werden, was denn diese induzierte Abbildung ist. Der Begriff "induziert" wird oft etwas schwammig verwendet, da muss man erst eine gewisse Intuition entwickeln, dann sieht man üblicherweise schnell, welches Objekt genau induziert wird. Gemeint ist damit grundsätzlich in etwa "Wir haben f mit den Eigenschaften $(P_i)_i$ und es gibt eine Methode, daraus ein Objekt g mit den Eigenschaften $(Q_i)_i$ zu erhalten."
   Man trifft in algebraischen Gebieten häufig auf sogenannte kommutative Diagramme. Diese dienen der Veranschaulichung von Situationen wie dieser und werden oft als Hilfsmittel verwendet um Beweise zu führen. Ohne präzise Definition verstehen wir das so: Haben wir eine Menge von Objekten und Abbildungen zwischen diesen Objekten, können wir diese aufmalen und egal in welcher Reihenfolge wir den Pfeilen folgen, das Ergebnis ist das Gleiche. Beispielsweise in gibt es die Mengen A, B, C, D und zwischen ihnen die vier Abbildungen

$$\begin{tikzcd} A \arrow[r, "\phi"] \arrow[d, "\psi"] & B \arrow[d, "f"] \\ C \arrow[r, "g"] & D \end{tikzcd}$$

   $\phi : A \to B, \psi : A \to C$ usw. Die Aussage des Diagramms ist nun, dass für ein Element in A beide Wege zum gleichen Ergebnis führen, die Komposition $g \circ \psi$ also mit der Komposition $f \circ \phi$ übereinstimmt.[1]

   Wir haben eine Abbildung $f : X \to Y$ und wollen einen Weg finden, eine Abbildung zu finden, die eine Bijektion aus S_X auf eine Bijektion aus S_Y abbildet. Um einen Überblick über diese Situation zu erhalten, ist es oftmals hilfreich, sich ein Diagramm zu malen: Da wir eine Abbildung von X nach Y haben und uns mit Bijektionen auf X, bzw. Y beschäftigen wollen, beginnen wir so:

[1] Nur um das klarzustellen: Dass $f \circ \phi = g \circ \psi$ gilt, muss vor dem Zeichnen des Diagramms überprüft werden. Das Diagramm dient dann lediglich als Hilfsmittel bei einer Weiterführung des Beweises.

$$\begin{tikzcd} X \arrow[r, "f"] & Y \\ X & Y \end{tikzcd}$$

Wir wollen, gegeben eine Bijektion $\psi : X \to X$ eine Bijektion $f_*(\psi) : Y \to Y$ finden, zeichnen also ψ ein. Wir zeichnen auch $f_*(\psi)$ ein, allerdings nur mit einer gestrichelten Linie, da wir die Existenz zeigen wollen.

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\psi"] & Y \arrow[d, dotted, "f_*(\psi)"] \\ X & Y \end{tikzcd}$$

Wir sehen jetzt schon, worauf das ganze hinausläuft. Wir suchen einen Weg von Y nach Y, dieser muss f und ψ beinhalten, also bleibt eigentlich nur der Bogen über die linke Seite, also der Weg $Y \overset{f^{-1}}{\to} X \overset{\psi}{\to} X \overset{?}{\to} Y$, wobei wir verwendet haben, dass f bijektiv ist, also eine inverse Abbildung besitzt. Alles was uns fehlt ist die letzte Abbildung von X nach Y, aber hier können wir natürlich wieder f einsetzen. Wir passen das Diagramm an indem wir f durch f^{-1} ersetzen und in der unteren Zeile noch ein f eintragen:

$$\begin{tikzcd} X \arrow[d, "\psi"] & Y \arrow[l, "f^{-1}"'] \arrow[d, dotted, "f_*(\psi)"] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

Wir können also $f_*(\psi) = f \circ \psi \circ f^{-1} : Y \to Y$ definieren.[a] Die gesamte Abbildungsdefinition sähe so aus:

$$f_* : S_X \to S_Y \tag{39}$$
$$\psi \mapsto f \circ \psi \circ f^{-1} \tag{40}$$

Nun kommt der formale Teil des Beweises: Wir haben eine Abbildung definiert, also prüfen wir, ob sie auch ein Isomorphismus ist.

(a) *Homomorphismus*: Seien $\varphi, \psi \in S_X$, dann berechnen wir für ein beliebiges Element $y \in Y$:

$$f_*(\varphi \circ \psi)(y) = f \circ (\varphi \circ \psi) \circ f^{-1}(y) \tag{41}$$
$$= (f \circ \varphi \circ f^{-1}) \circ (f \circ \psi \circ f^{-1})(y) \tag{42}$$
$$= f_*(\varphi) \circ f_*(\psi)(y) \tag{43}$$

was zeigt, dass f_* ein Homomorphismus ist.

(b) *Bijektivität*: Wir könnten direkt zeigen, dass f_* bijektiv ist indem wir Injektivität und Surjektivität überprüfen, doch gerade letzteres ist ein bisschen unangenehm. Stattdessen

gehen wir wie folgt vor:
Es gilt für die bijektive Abbildung $\mathbb{1}_X : X \to X$, dass

$$\forall \psi \in S_X : \mathbb{1}_{X,*}(\psi)(x) = \mathbb{1}_X \circ \psi \circ \mathbb{1}_X^{-1}(x) = \psi(x) \tag{44}$$

die Identität auf Mengen induziert also die Identität auf Bijektionen. Weiter gilt für bijektive Abbildungen $f : X \to Y, g : Y \to X$, eine Abbildung $\psi \in S_Y$ und ein Element $y \in Y$, dass:

$$\begin{aligned}
(f \circ g)_*(\psi)(y) &= (f \circ g) \circ \psi \circ (f \circ g)^{-1}(y) && (45)\\
&= f \circ (g \circ \psi \circ g^{-1}) \circ f^{-1}(y) && (46)\\
&= f \circ g_*(\psi) \circ f^{-1}(y) && (47)\\
&= f_* \circ g_*(\psi)(y) && (48)
\end{aligned}$$

also ist die Verknüpfung auf der Menge der Bijektionen verträglich mit der Induktion von Abbildungen. Da f bijektiv ist und f^{-1} existiert, existiert also auch $(f^{-1})_*$ und die Rechnung gerade eben zeigt uns, dass

$$\mathbb{1}_{X,ast} = (f \circ f^{-1})_* \tag{49}$$

Das bedeutet, dass f_* als Abbildung von Bijektionen ein Inverses hat, nämlich $(f_*)^{-1} = (f^{-1})_*$. Damit ist f_* automatisch bijektiv.

Also induziert f einen Isomorphismus zwischen S_X und S_Y.

[a] Natürlich braucht man dieses Diagramm nicht um den Beweis zu führen, es dient lediglich der Veranschaulichung und kann helfen Dinge zu sehen, die man vorher nicht gesehen hat. Und man würde auch keine drei Diagramme zeichnen, sondern nur eines. Dass wir hier drei Diagramme haben soll nur helfen, den Gedankengang sichtbar zu machen. Das Diagramm hier ist nun übrigens kommutativ, weil wir $f_*(\psi)$ genau so definiert haben, dass es keinen Unterschied macht, welcher Reihe von Pfeilen man folgt.

Aufgabe 4

1. Seien S_n die Menge der Bijektionen auf der Menge $\{1, \ldots, n\}$. Zeige, dass S_n für $n \geq 3$ nicht kommutativ ist.

2. Konstruiere einen injektiven Gruppenhomomorphismus $S_n \times S_m \to S_{n+m}$.

Lösung:

1. Zur Vereinfachung definieren wir folgende Notation: $[[n]] = \{1, \ldots, n\}$. Wir hatten die symmetrische Gruppe in der dritten Aufgabe bereits definiert und insbesondere gezeigt, dass es eine Gruppe ist. Da wir dort nicht spezifiziert hatten, was X ist, gilt es selbstverständlich auch für S_n. Wir überlegen uns, dass eine Abbildung $\sigma \in S_n$ nur eine Vertauschung, der n ersten Zahlen ist. Wir definieren die Transpositionen $\tau_{i,j} \in S_n$ für $i \neq j \in [[n]]$:

$$\tau_{i,j} : [[n]] \to [[n]] \tag{50}$$

$$k \mapsto \begin{cases} j, & k = i \\ i, & k = j \\ k & \text{sonst} \end{cases} \tag{51}$$

diese Permutation bildet also i auf j und umgekehrt ab, lässt aber alle anderen Elemente gleich. Damit sehen wir:

Sei $n \geq 3$ gegeben. Wir suchen nun $\sigma_1, \sigma_2 \in S_n$, sodass $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$ ist. Wir wählen $\sigma_1 = \tau_{1,2}, \sigma_2 = \tau 2, 3$. Dann gilt:

$$\tau_{1,2} \circ \tau_{2,3}(3) = \tau_{1,2}(\tau_{2,3}(3)) = \tau_{1,2}(2) = 1 \tag{52}$$
$$\tau_{2,3} \circ \tau_{1,2}(3) = \tau_{2,3}(\tau_{1,2}(3)) = \tau_{2,3}(3) = 2 \tag{53}$$

bei unterschiedlicher Reihenfolge der Komposition, erhält man also unterschiedliche Ergebnisse. Es reicht hierbei, dass die Funktionen auf einem einzigen Element nicht übereinstimmen. Damit haben wir gezeigt, dass S_n nicht abelsch ist.

2. Wir wollen einen injektiven Gruppenhomomorphismus $S_n \times S_m \to S_{n+m}$. $S_n \times S_m$ verstehen wir dabei als Gruppe mit der Verknüpfung $(\circ, \circ)$, die koordinatenweise wirkt und die wir als $\circ$ schreiben. Es gilt also $(\sigma_1, \tau_1) \circ (\sigma_2, \tau_2) = (\sigma_1 \circ \sigma_2, \tau_1 \circ \tau_2)$ mit neutralem Element $(\mathbb{1}_n, \mathbb{1}_m)$ und das zu (σ, τ) inverse Element ist (σ^{-1}, τ^{-1}). Dafür überlegen wir uns folgendes: Ein Element $\sigma \in S_n$ vertauscht n Elemente untereinander, ein Element $\tau \in S_m$ vertauscht m Elemente. Der offensichtliche Weg, eine Permutation für $n + m$ Elemente zu konstruieren ist, dass wir die ersten n Elemente wie σ vertauschen und die anderen m Elemente wie τ. Diese Abbildung wird genau die notwendigen Eigenschaften haben. Formal:

Wir definieren:

$$\mathscr{S} : S_n \times S_m \to S_{n+m} \tag{54}$$
$$(\sigma, \tau) \mapsto \begin{pmatrix} [[n+m]] \to [[n+m]] \\ k \mapsto \begin{cases} \sigma(k), & k \in [[n]] \\ \tau(k-n) + n, & k \in \{n+1, \ldots, n+m\} \end{cases} \end{pmatrix} \tag{55}$$

Diese Abbildung ist wohldefiniert: Ist $k \in [[n + m]]$ eine Zahl zwischen 1 und n, wird sie auf $\sigma(k)$ abgebildet, also wieder im Bereich zwischen 1 und n. Ist k dagegen zwischen $n + 1$ und $n + m$, liegt $k - n$ zwischen 1 und m, also im Definitionsbereich von τ. $\tau(k - n)$ liegt wieder zwischen 1 und m, also liegt das Endergebnis in $\{n+1, \ldots, n+m\}$. Da σ und τ jeweils bijektiv sind, ist die neue Abbildung ebenfalls bijektiv. Unsere Abbildung ist also nicht nur wohldefiniert, sondern bildet auch so ab, wie wir es uns überlegt hatten. Wir zeigen, dass es ein Monomorphismus ist:

(a) *Homomorphismus*: Seien $(\sigma_1, \tau_1), (\sigma_2, \tau_2) \in S_n \times S_m$. Wir wollen zeigen, dass die Abbildung linear ist, dafür prüfen wir die linke und die rechte Seite jeweils auf einem Element im Bereich $\{1, \ldots, n\}$ und einem im Bereich $\{n+1, \ldots, n+m\}$, womit wir gezeigt hätten, dass die Abbildungen gleich sind.

$$\mathscr{S}(\sigma_1 \circ \sigma_2, \tau_1 \circ \tau_2)(k) = \begin{cases} \sigma_1(\sigma_2(k)), & k \in [[n]] \\ \tau_1(\tau_2(k-n)) + n, & k \in \{n+1, \ldots, n+m\} \end{cases} \tag{56}$$

Und

$$\mathscr{S}(\sigma_1,\tau_1)\circ\mathscr{S}(\sigma_2,\tau_2)(k) = \mathscr{S}(\sigma_1,\tau_1)(\mathscr{S}(\sigma_2,\tau_2)(k)) \tag{57}$$

$$= \begin{cases} \mathscr{S}(\sigma_1,\tau_1)(\sigma_2(k)), & k \in [[n]] \\ \mathscr{S}(\sigma_1,\tau_1)(\tau_2(k-n)+n), & k \in \{n+1,\dots,n+m\} \end{cases} \tag{58}$$

$$= \begin{cases} \sigma_1(\sigma_2(k)), & k \in [[n]] \\ \tau_1(\tau_2(k-n))+n, & k \in \{n+1,\dots,n+m\} \end{cases} \tag{59}$$

wobei wir in der dritten Gleichheit verwendet haben, dass σ und τ Permutationen sind, das heißt ihre Definitionsmengen auf sich selbst abbilden. Liegt $k \in [[n]]$, dann natürlich auch $\sigma(k)$. Wir sehen, dass die beiden Abbildungen auf allen Elementen gleich agieren, also sind sie die gleiche Abbildung und $\mathscr{S}$ ist ein Homomorphismus.

Injektivität: Da wir bereits gezeigt haben, dass $\mathscr{S}$ ein Homomorphismus ist, können wir die Injektivität nachweisen indem wir zeigen, dass der Kern trivial ist. Dafür sei $(\sigma,\tau) \in \ker(\mathscr{S})$, also $(\sigma,\tau) \in S_n \times S_m$ und $\mathscr{S}(\sigma,\tau) = \mathbb{1}_{S_{n+m}}$. Wir sehen

$$\left.\begin{matrix} k, & k \in \{1,\dots,n\} \\ k, & k \in \{n+1,\dots,n+m\} \end{matrix}\right\} = \mathbb{1}_{S_{n+m}}(k) \tag{60}$$

$$= \mathscr{S}(\sigma,\tau)(k) = \begin{cases} \sigma(k), & k \in [[n]] \\ \tau(k-n)+n, & k \in \{n+1,\dots,n+m\} \end{cases} \tag{61}$$

also gilt für alle $k \in [[n]]$, dass $\sigma(k) = k$ und für alle $k \in [[m]]$, dass $\tau(k) = k$ gelten muss. Damit ist aber $\sigma = \mathbb{1}_{S_n}$ und $\tau = \mathbb{1}_{S_m}$, das heißt (σ,τ) ist das neutrale Element von $S_n \times S_m$. Folglich ist der Kern trivial und $\mathscr{S}$ injektiv.

Insgesamt haben wir einen injektiven Homomorphismus von Gruppen zwischen $S_n \times S_m$ und S_{n+m} konstruiert und sind fertig.