Universität des Saarlandes
Fachbereich 9, Mathematik
Prof. Dr. R. Berger

Musterlösung zur 1. Übung der Linearen Algebra I, WS 1998/99

Lösung zur Aufgabe 5:

a) Sei n die Anzahl der Elemente von X und Y. Sei f surjektiv. Angenommen, f sei nicht injektiv. Dann gibt es $x_1 \neq x_2 \in X$ mit $f(x_1) = f(x_2)$. Dann ist die Anzahl der Elemente von $f(X)$ kleiner als n und f nicht surjektiv, was ein Widerspruch ist.

Sei f injektiv. Jedes Element von X hat unter f ein anderes Bild in Y, d.h. $|Y| \geq |f(X)| \geq n$. Also hat $f(X)$ genau n Elemente und f ist surjektiv.

b) Aus Teil a) sieht man, daß X unendlich viele Elemente enthalten muß.

(i) $f : \mathbb{N} \to \mathbb{N} : n \mapsto 2n$ (ii)$f : \mathbb{N} \to \mathbb{N} : n \mapsto \begin{cases} \frac{n}{2}, & n \text{ gerade} \\ \frac{n-1}{2}, & n \text{ ungerade} \end{cases}$

Lösung zur Aufgabe 6:

a) Sei $V := \bigcap\limits_{U \in \mathfrak{M}} U$. Wegen $\forall U \in \mathfrak{M} : e \in U$ ist $e \in V$, d.h. $V \neq \emptyset$. Seien $x, y \in V$ beliebig. Dann gilt $\forall U \in \mathfrak{M} : x, y \in U$, also $\forall U \in \mathfrak{M} : x \circ y^{-1} \in U$, und da alle U Untergruppen von G sind, gilt $x \circ y^{-1} \in V$. Also erfüllt V das Untergruppenkriterium (1.5.4), ist also Gruppe.

b) Was ist der leere Schnitt?? Wie kann man das sinnvoll definieren? Eine Möglichkeit ist $V := \bigcap\limits_{U \in \emptyset} U = \emptyset$ ist keine Gruppe, da V kein Einselement enthält. Also ist die kleinste Gruppe überhaupt $G = \{e\}$.

Man kann jedoch, was meistens gemacht wird, auch den leeren Schnitt als die gesamte Gruppe definieren $\bigcap\limits_{U \in \emptyset} U := G$, um diesem Problem zu entkommen.

c) $\mathfrak{M}$ kann überabzählbar unendlich viele Elemente enthalten.

d) Wegen $M \subset G$ ist G sicherlich eine Gruppe, welche die Menge M umfaßt, d.h. der Schnitt ist nicht leer und nach (a) eine Gruppe.

Lösung zur Aufgabe 7:

In 1.6.2 der Vorlesung wurde $a^{n+1} := a^n \circ a$ für alle $n \in \mathbb{N}_0$ und $a^0 := e$ definiert.

a) Der Beweis erfolgt in mehreren Schritten:

(i) Beh.: Sei $n \in \mathbb{N}_0$. Dann gilt $a \circ a^n = a^{n+1} = a^n \circ a$ (”*Kommutativität*”)

Beweis durch vollständige Induktion:

$\boldsymbol{n = 0}$: $a \circ e = a^1 = e \circ a$ klar!

$\boldsymbol{n \to n+1}$: $a^{(n+1)+1} \overset{Def.}{=} (a^{n+1}) \circ a \overset{IV}{=} (a \circ a^n) \circ a = a \circ (a^n \circ a) = a \circ a^{n+1}$

(ii)$\underline{\text{Fall } n, m \geq 0}$: Vollständige Induktion nach n

$\boldsymbol{n = 0}$: $a^{0+m} = a^m = e \circ a^m = a^0 \circ a^m$.

$\boldsymbol{n \to n+1}$: $a^{(n+1)+m} = a^{n+(1+m)} \overset{IV}{=} a^n \circ a^{m+1} \overset{(i)}{=} a^n \circ (a \circ a^m) = (a^n \circ a) \circ a^m = a^{n+1} \circ a^m$

(iii) Fall $n, m < 0$: $a^n \circ a^m = \underbrace{(a^{-1})^{-n}}_{a^{-n} \overset{\text{Teil } b)}{=} (a^{-1})^n} \circ (a^{-1})^{-m} \overset{(ii)}{=} (a^{-1})^{-n-m} = a^{n+m}$

(iv) Fall $n \geq 0, m < 0$: Vollständige Induktion nach n

$\boldsymbol{n = 0}$: $a^0 \circ a^m = a^{0+m}$ klar!

$\boldsymbol{n \to n+1}$: $a^{n+1} \circ a^m \overset{(i)}{=} a \circ a^n \circ a^m \overset{IV}{=} a \circ a^{n+m}$

$$= \begin{cases} a^{n+m+1}, & \text{falls } n+m \geq 0 \\ a \circ (a^{-1})^{-(n+m)} = a \circ a^{-1} \circ (a^{-1})^{-(n+m)-1} = (a^{-1})^{-(n+m+1)}, & \text{falls } n+m < 0 \end{cases} \Bigg\} = a^{n+m+1}$$

(v) Fall $n < 0, m \geq 0$: Analog zu (iv)

(vi) Beh.: $\forall\, m \in \mathbb{N}_0 : (a^n)^m = a^{nm}$. Der Beweis geht durch Induktion nach m ...

(vii) Beh.: $\forall\, m < 0 : (a^n)^m = a^{nm}$.
Bew.: Vorüberlegung: Wegen $a^n \circ (a^{-1})^n = a^n \circ a^{-n} = a^{n-n} = e$ und der Eindeutigkeit des Inversen ist $(a^n)^{-1} = (a^{-1})^n$. Deswegen gilt $(a^n)^m = ((a^n)^{-1})^{-m} = ((a^{-1})^n)^{-m} = (a^{-1})^{-nm} = a^{nm}$.

b) Es ist $(a \circ b) \circ (b^{-1} \circ a^{-1}) = a \circ (b \circ b^{-1}) \circ a^{-1} = a \circ a^{-1} = e$ und da das Inverse in einer Gruppe eindeutig definiert ist, muß $(b^{-1} \circ a^{-1}) = (a \circ b)^{-1}$ gelten.

c) Beh.: $(a \circ b)^n = a^n \circ b^n$
Bew.: $\boldsymbol{n = 0}$: klar!
$\boldsymbol{n \to n+1}$: $(a \circ b)^{n+1} \overset{Def}{=} (a \circ b)^n \circ (a \circ b) \overset{IV}{=} a^n \circ b^n \circ a \circ b \overset{komm.}{=} a^n \circ a \circ b^n \circ b = a^{n+1} \circ b^{n+1}$
$\boldsymbol{n < 0}$: $(a \circ b)^n = ((a \circ b)^{-1})^{-n} = (a^{-1} \circ b^{-1})^{-n} = (a^{-1})^{-n} \circ (b^{-1})^{-n} = a^n \circ b^n$

Lösung zur Aufgabe 8:

a) Die Anzahl der Bijektionen ist $|\mathfrak{S}_3| = 3! = 6$.

b) Die Elemente von $\mathfrak{S}_3$ sind

	123
e	123
τ_1	132
τ_2	321
τ_3	213
σ_1	312
σ_2	231

Die τ_i sind ***Transpositionen***, d.h. Permutationen, die genau zwei Elemente vertauschen.
Um die Gruppentafel zu berechnen ist es nicht nötig, alle Elemente miteinander zu multiplizieren. Bei endlichen Gruppen stehen in jeder Zeile und jeder Spalte immer alle Elemente genau einmal, d.h. es reicht hier fünf pro Spalte und Zeile zu berechnen. Aber durch Ergänzen kann man die Arbeit noch mehr vereinfachen - wie man gleich sehen wird.

Die erste Spalte und Zeile ist klar, da es sich dabei nur um Multiplikation mit dem Neutralelement handelt. Auch die $\sigma_i \circ \tau_j$ sind sofort klar, da τ_j einfach zwei Elemente vertauscht. Ebenfalls klar ist, daß doppelte Vertauschung nichts vertausch, d.h. $\tau_j^2 = e$ gilt. Somit sind die folgenden Einträge klar:

$\circ$	e	τ_1	τ_2	τ_3	σ_1	σ_2
e	e	τ_1	τ_2	τ_3	σ_1	σ_2
τ_1	τ_1	e				
τ_2	τ_2		e			
τ_3	τ_3			e		
σ_1	σ_1	τ_2	τ_3	τ_1		
σ_2	σ_2	τ_3	τ_1	τ_2		

Rechnen wir weiter: $\sigma_1^2 = \sigma_2$. Also kann in der fünften Zeile sofort das letzte fehlende Element $\sigma_1 \circ \sigma_2 = e$ eingetragen werden. Da das Inverse eindeutig ist, gilt auch $\sigma_2 \circ \sigma_1 = e$ und damit ist auch der Eintrag rechts unten in der Tabelle klar. Der Rest geht schnell:

- $\tau_2 \circ \tau_1 = \sigma_1 \Rightarrow \tau_3 \circ \tau_1 = \sigma_2$
- $\tau_3 \circ \tau_2 = \sigma_1 \Rightarrow \tau_1 \circ \tau_2 = \sigma_2$
- $\tau_1 \circ \tau_3 = \sigma_1 \Rightarrow \tau_2 \circ \tau_3 = \sigma_2$
- $\tau_1 \circ \sigma_1 = \tau_3 \Rightarrow \tau_1 \circ \sigma_2 = \tau_2$
- $\tau_2 \circ \sigma_1 = \tau_1$ und nun folgt der ganze Rest: $\tau_2 \circ \sigma_2 = \tau_3, \tau_3 \circ \sigma_1 = \tau_2, \tau_3 \circ \sigma_2 = \tau_1$

$\circ$	e	τ_1	τ_2	τ_3	σ_1	σ_2
e	e	τ_1	τ_2	τ_3	σ_1	σ_2
τ_1	τ_1	e	σ_2	σ_1	τ_3	τ_2
τ_2	τ_2	σ_1	e	σ_2	τ_1	τ_3
τ_3	τ_3	σ_2	σ_1	e	τ_2	τ_1
σ_1	σ_1	τ_2	τ_3	τ_1	σ_2	e
σ_2	σ_2	τ_3	τ_1	τ_2	e	σ_1

c) Die sechs Untergruppen sind $U_0 = \{e\}, U_1 = \{e, \tau_1\}, U_2 = \{e, \tau_2\}, U_3 = \{e, \tau_3\}, U_4 = \{e, \sigma_1, \sigma_2\}$ und $U_5 = \mathfrak{S}_3$.

U_0 und U_5 sind trivialerweise Untergruppen. Aus b) wissen wir $\tau_i^2 = e$, d.h. nach 1.5.4 sind $U_{1,2,3}$ Untergruppen.

Das einzige Problem ist U_4: Bei endlichen Gruppen reicht es (i) $e \in U$ und (ii) $\forall\, a, b \in U : a \circ b \in U$ nachzuweisen: Bedingung (i) gilt trivialerweise. Ferner gilt $\sigma_1^2 = \sigma_2 \in U_4$, $\sigma_2^2 = \sigma_1 \in U_4$, $\sigma_1 \circ \sigma_2 = e = \sigma_2 \circ \sigma_1 \in U_4$. Damit sind alle Produkte in U_4 und wir sind fertig.

Wer das Untergruppenkriterium 1.5.4 anwenden möchte, kann in der Gruppentafel jeweils das Inverse nachschlagen und sämtliche Produkte $a \circ b^{-1}$ ausrechnen.

Lösung zur Aufgabe 9:

Da $\mathbb{N}$ keine Gruppe ist, gibt es keine Gruppenhomomorphismen; jedoch ist $\mathbb{N}$ ein Monoid, so daß es Monoidhomomorphismen gibt. Die folgenden vier Homomorphismen zwischen den Monoiden sind leicht zu sehen:

(i) $f : \mathbb{N} \to G : n \mapsto \left\{ \begin{array}{cl} n, & \text{n gerade} \\ n-1, & \text{n ungerade} \end{array} \right\}$ surjektiv mit $\ker f = \{0, 1\}$ und Bild $f = G$.
(ii) $f : \mathbb{N} \to \mathbb{Z} : n \hookrightarrow n$ injektiv mit $\ker f = \{0\}$ und Bild $f = \mathbb{N}$.
(iii) $f : \mathbb{N} \to \mathbb{Q} : n \hookrightarrow n$ injektiv mit $\ker f = \{0\}$ und Bild $f = \mathbb{N}$.
(iv) $f : \mathbb{N} \to \mathbb{R} : n \hookrightarrow n$ injektiv mit $\ker f = \{0\}$ und Bild $f = \mathbb{N}$.

Man beachte daß die letzten drei Funktionen verschieden sind, da sie verschiedene Wertebereiche haben. In den Fällen (i)-(iii) gibt es aber sogar bijektive Abbildungen:

(i) $f : \mathbb{N} \to G : n \mapsto 2n$
(ii) $f : \mathbb{N} \to \mathbb{Z} : n \mapsto \left\{ \begin{array}{ll} -\frac{n}{2}, & \text{n gerade} \\ \frac{n+1}{2}, & \text{n ungerade} \end{array} \right.$

Bis hierher läßt es sich leicht nachrechnen, aber nun wird es schwer und ich verweise auf die Literatur (Forster, Analysis I §9). Kurz angedeutet gehen die Beweise folgendermaßen:

(iii) Zuerst werden alle Brüche zwischen 0 und 1 nach Größe sortiert aufgeschrieben. Hierdurch läßt sich jedem solchen Bruch eineindeutig eine natürliche Zahl zuordnen, d.h. es gibt eine Bijektion zwischen $\mathbb{N}$ und $\{b \in \mathbb{Q} | 0 \leq b < 1\}$.
Dies kann man für alle Intervalle machen, von denen es $\mathbb{N}$ viele gibt. Insgesamt haben wir also abzählbar unendlich viele abzählbar unendliche Mengen und wie man leicht zeigt, sind das wieder abzählbar viele Elemente.

(iv) Man benutze Cantors Diagonalverfahren.

Quintessenz: Es gibt mindestens zwei verschiedene Arten von Unendlichkeit, nämlich ***abzählbar*** (bijektiv zu $\mathbb{N}$) und ***überabzählbar*** unendlich (nicht bijektiv zu $\mathbb{N}$). Die Aufgabe 4 (b) ist also ungenau formuliert. Man benötigt eine Fallunterscheidung: Ob ein Bus mit abzählbar oder überabzählbar unendlich vielen Gästen kommt. Nur im ersten Fall kann man alle Gäste unterbringen!