Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Fachbereich Mathematik
Algebra und Zahlentheorie
Christian Curilla

Grundlagen der Mathematik (LPSI/LS-M1)

Lösungen Blatt 9 WiSe 2010/11 - Curilla/Koch/Ziegenhagen

Präsenzaufgaben

(P29) (a) Es gilt

$$e_H \cdot \phi(e_G) = \phi(e_G) = \phi(e_G * e_G) = \phi(e_G) \cdot \phi(e_G)\,.$$

Hierbei hat man vor dem ersten und nach dem zweiten Gleichheitszeichen einfach geschickt das neutrale Element der jeweiligen Gruppe ergänzt. Die Kürzungsregel liefert uns nun $e_H = \phi(e_G)$.

(b) Sei $a \in G$ gegeben. Wir haben

$$\phi(a) \cdot \phi(a^{-1}) = \phi(a * a^{-1}) = \phi(e_G) = e_H = \phi(a) \cdot \phi(a)^{-1}\,.$$

Hierbei haben wir für das dritte Gleichheitszeichen die Aussage (a) benutzt. Ebenfalls liefert uns die Kürzungsregel nun das Gewünschte.

(P30) Wir nehmen zunächst an, dass das zweite Kriterium erfüllt ist und zeigen, dass dann auch die erste Bedingung gilt. Seien beliebige $x, y \in U$ gegeben, wir wollen zeigen, dass dann $x \cdot y^{-1} \in U$ ist. Nach Voraussetzung ist die zweite Bedingung zutreffend. Wir wenden den zweiten Teil der zweiten Bedingung auf y an und erhalten, dass $y^{-1} \in U$ ist. Deswegen können wir den ersten Teil der zweiten Bedingung auf $a = x$ und $b = y^{-1}$ anwenden und erhalten $x \cdot y^{-1} \in U$, das erste Kriterium ist also erfüllt.

Nun nehmen wir umgekehrt an, das erste Kriterium sei erfüllt. Dann muss insbesondere das neutrale Element e_G von G in U enthalten sein, denn wir können ein beliebiges $x \in U$ wählen (U ist nichtleer!) und das erste Kriterium auf $a = x$ und $b = x$ anwenden: Dies liefert $e_G = x \cdot x^{-1} \in U$. Ist nun ein beliebiges $x \in U$ vorgegeben, so wenden wir das erste Kriterium auf $a = e_G$ und $b = x$ an und erhalten $x^{-1} = e_G \cdot x^{-1} \in U$. Also ist der zweite Teil des zweiten Kriteriums erfüllt. Um nachzuweisen, dass auch der erste Teil gilt, setzen wir für beliebige $x, y \in U$ im ersten Kriterium $a = x$ und $b = y^{-1}$ ein - da wir uns eben überlegt haben, dass mit y auch y^{-1} in U liegt, dürfen wir das - und erhalten $x \cdot y = x \cdot (y^{-1})^{-1} \in U$. Damit ist gezeigt, dass das zweite Kriterium erfüllt ist, falls das erste gilt.

(P31) (a) Wir rechnen nach, dass χ die Addition respektiert: Für beliebige $x, y \in \mathbb{Z}$ ist

$$\chi(x+y) = [x+y] \quad \text{und} \quad \chi(x) \oplus \chi(y) = [x] \oplus [y] = [x+y].$$

Also ist $\chi(x+y) = \chi(x) \oplus \chi(y)$, die Abbildung χ ist ein Homomorphismus.

(b) Sei $x \in \mathbb{Z}$. Nach Definition liegt x genau dann im Kern von χ, wenn $\chi(x) = e_{\mathbb{Z}/m\mathbb{Z}}$ ist. Da das neutrale Element in $(\mathbb{Z}/m\mathbb{Z}, \oplus)$ die Äquivalenzklasse $[0]$ ist, bedeutet die Bedingung gerade $[x] = [0]$. Dies gilt bekanntlich genau dann, wenn $x \in [0]$ ist. Der Kern von χ ist also gleich der Äquivalenzklasse $[0] \subseteq \mathbb{Z}$.

(c) Sei $x \in \mathbb{Z}$. Dann ist wie bei der Berechnung des Kerns $\chi(x) = [1]$ genau dann, wenn $x \in [1]$ ist. Analoges gilt für $[2], ..., [m-1]$. Das Urbild einer Äquivalenzklasse ist also die Äquivalenzklasse selber.

Hausaufgaben

(H34) (a) Ausrechnen liefert

$\odot$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

(b) An der obigen Verknüpfungstafel lesen wir ab, dass $\odot$ zwei Element aus $\mathbb{Z}/5\mathbb{Z} \setminus \{[0]\}$ wieder auf ein Element in $\mathbb{Z}/5\mathbb{Z} \setminus \{[0]\}$ abbildet.
Wir haben bereits in der Vorlesung gesehen, dass $(\mathbb{Z}/5\mathbb{Z}, \oplus, \odot)$ ein Ring ist. Isbesondere ist $\odot$ auf $\mathbb{Z}/5\mathbb{Z} \setminus \{[0]\}$ assoziativ; wir wiederholen das Argument hier noch einmal: Für $a, b, c \in \mathbb{Z}$ ist

$$[a] \odot ([b] \odot [c]) = [a] \odot [b \cdot c] = [a \cdot (b \cdot c)] = [(a \cdot b) \cdot c] = [a \cdot b] \odot [c] = ([a] \odot [b]) \odot [c].$$

Damit ist $\odot$ natürlich auch eingeschränkt auf $\mathbb{Z}/5\mathbb{Z} \setminus \{[0]\}$ assoziativ.
Ebenfalls in der Vorlesung hatten wir überlegt, dass die Äquivalenzklasse [1] das neutrale Element in $\mathbb{Z}/5\mathbb{Z}$ bezüglich $\odot$ ist, auch dies wiederholen wir: Für beliebiges $a \in \mathbb{Z}$ ist

$$[a] \odot [1] = [a \cdot 1] = [a] = [1 \cdot a] = [1] \odot [a].$$

Da [1] in $\mathbb{Z}/5\mathbb{Z} \setminus \{[0]\}$ enthalten ist, besitzt $\mathbb{Z}/5\mathbb{Z} \setminus \{[0]\}$ ein neutrales Element. Es bleibt zu zeigen, dass jedes Element in $\mathbb{Z}/5\mathbb{Z} \setminus \{[0]\}$ ein Inverses bezüglich $\odot$ besitzt. Dies liest man leicht an der Verknüpfungstafel ab: [1] ist invers zu sich selbst, [2] und [3] sind invers zueinander und [4] ist ebenfalls invers zu sich selbst.
Insgesamt ergibt sich, dass $(\mathbb{Z}/5\mathbb{Z} \setminus \{[0]\}, \odot)$ eine Gruppe ist.

(c) Zwei Gruppen heißen isomorph, wenn es einen Isomorphismus, also einen bijektiven Homomorphismus zwischen ihnen gibt. Wir hatten in den Präsenzaufgaben auf Blatt 8 die folgende Verknüpfungstafel von $(\mathbb{Z}/4\mathbb{Z}, \oplus)$ errechnet:

$\oplus$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Wir wollen einen Isomorphismus $f\colon (\mathbb{Z}/5\mathbb{Z} \setminus \{[0]\}, \odot) \to (\mathbb{Z}/4\mathbb{Z}, \oplus)$ konstruieren. Zur besseren Lesbarkeit kennzeichnen wir Äquivalenzklassen in $\mathbb{Z}/5\mathbb{Z}\setminus\{[0]\}$ durch $[...]_5$, die in $\mathbb{Z}/4\mathbb{Z}$ durch $[...]_4$. Nach Aufgabe (P29a) muss das neutrale Element auf das neutrale Element, also die $[1]_5$ auf die $[0]_4$ abgebildet werden. Nach (P29b) werden selbstinverse Elemente auf selbstinverse Elemente

abgebildet, also muss die $[4]_5$ auf die $[2]_4$ gehen. Da die gesuchte Abbildung bijektiv sein soll, gibt es nur zwei Möglichkeiten, nun noch $[2]_5$ bzw. $[3]_5$ auf $[1]_4$ oder $[3]_4$ abzubilden. Tatsächlich liefern beide Wahlen einen Isomorphismus, wir entscheiden uns für die folgende Abbildung:

$$f([1]_5) := [0]_4, \quad f([2]_5) := [3]_4, \quad f([3]_5) := [1]_4, \quad f([4]_5) := [2]_4.$$

Die Abbildung f ist offensichtlich bijektiv. Wendet man f auf die Einträge der Verknüpfungstafel aus (a) an und ordnet die Einträge wieder einer Verknüpfungstafel entsprechend, so erhält man die Verknüpfungstafel von $(\mathbb{Z}/4\mathbb{Z}, \oplus)$. Dies besagt gerade, dass f die Verknüpfung der ersten Gruppe in die der zweiten Gruppe überführt, also ein Homomorphismus ist.

(d) Die Assoziativität und die Existenz eines neutralen Elementes ergeben sich genau wie in (c); insbesondere ist auch in $(\mathbb{Z}/p\mathbb{Z}\setminus\{[0]\}, \odot)$ die Äquivalenzklasse $[1]$ das neutrale Element.
Die Existenz von Inversen zeigt man wie folgt: Sei dazu $a \in \mathbb{Z}$ mit $[a] \neq [0]$, die Zahl a sei also nicht durch p teilbar. Wir benutzen nun den Hinweis: Weil p eine Primzahl ist, sind 1 und p die einzigen natürlichen Teiler von p. Da p nicht a teilt, muss $\mathrm{ggT}(p, a) = 1$ sein. Laut Hinweis gibt es also $s, t \in \mathbb{Z}$ mit $1 = sp+ta$. Wir zeigen, dass $[t]$ das Inverse zu $[a]$ ist: Zunächst einmal ist $[t] \neq [0]$, denn sonst wäre t und damit auch $1 = sp + ta$ durch p teilbar, was offenbar falsch ist. Folglich ist $[t]$ ein Element in $\mathbb{Z}/p\mathbb{Z} \setminus \{[0]\}$. Schließlich rechnen wir

$$[a] \odot [t] = [a \cdot t] = [1 - s \cdot p] = [1],$$

und da $\odot$ kommutativ ist, ist auch $[t] \odot [a] = [1]$. Folglich besitzt a ein Inverses, und $(\mathbb{Z}/p\mathbb{Z} \setminus \{[0]\}, \odot)$ erfüllt alle Gruppenaxiome.
Stillschweigend haben wir die ganze Zeit benutzt, dass $\odot$ eine Verknüpfung auf $\mathbb{Z}/p\mathbb{Z}\setminus\{[0]\}$ liefert, also dass für $[a], [b] \in \mathbb{Z}/p\mathbb{Z}\setminus\{[0]\}$ auch $[a]\odot[b] \in \mathbb{Z}/p\mathbb{Z}\setminus\{[0]\}$ ist. Dies können wir nun relativ leicht begründen: Wäre $[a] \odot [b] = [0]$, so wären $[a]$ und $[b]$ Nullteiler. Dies kann aber nicht sein, weil Nullteiler keine Inversen haben (vgl. Zusatzbemerkung in (H29b)).
Bemerkung: Mit dieser Aussage können wir jetzt folgendes zeigen:

$$\mathbb{Z}/m\mathbb{Z} \text{ ist ein Körper } \Leftrightarrow \text{ m ist eine Primzahl.}$$

Weil $\mathbb{Z}/m\mathbb{Z}$ ein kommutativer Ring ist, müssen wir nur zeigen, dass $(\mathbb{Z}/m\mathbb{Z} \setminus \{[0]\}, \odot)$ eine Gruppe ist, genau dann, wenn m eine Primzahl ist. Dass $(\mathbb{Z}/m\mathbb{Z}\setminus \{[0]\}, \odot)$ eine Gruppe ist, wenn m eine Primzahl ist, haben wir oben gezeigt. Wir müssen also noch zeigen, dass m eine Primzahl ist, wenn $(\mathbb{Z}/m\mathbb{Z}\setminus\{[0]\}, \odot)$ eine Gruppe ist. Wir können dies am leichtesten beweisen, indem wir die Kontraposition zeigen: Wenn m keine Primzahl ist, so gibt es $a, b \in \mathbb{N}$ mit $1 < a, b < m$ und $m = a \cdot b$. Es folgt dann $[a] \odot [b] = [m] = [0]$, $[a]$ und $[b]$ sind somit Nullteiler. Sie können daher keine Inversen bzgl. der Multiplikation haben (siehe oben) und $(\mathbb{Z}/m\mathbb{Z} \setminus \{[0]\}, \odot)$ kann somit keine Gruppe sein.

(H35) (a) Seien $x, y \in \mathbb{Z}$ beliebig. $[a] \odot [x] = [a] \odot [y]$ bedeutet (nach Definition) $[a \cdot x] = [a \cdot y]$. Es gilt folgendes

$$\begin{aligned} [a \cdot x] = [a \cdot y] &\Rightarrow [a \cdot x] \oplus [-a \cdot y] = [a \cdot y] \oplus [-a \cdot y] \\ &\Rightarrow [a \cdot x - a \cdot y] = [0] \\ &\Rightarrow [a \cdot (x - y)] = [0] \\ &\Rightarrow [a] \odot [x - y] = [0]. \end{aligned}$$

Weil $[a]$ nach Voraussetzung kein Nullteiler ist, gilt $[x-y] = [0]$. Damit erhalten wir

$$\begin{aligned} [x - y] = [0] &\Rightarrow [x] \oplus [-y] = [0] \\ &\Rightarrow ([x] \oplus [-y]) \oplus [y] = [0] \oplus [y] \\ &\Rightarrow [x] \oplus ([-y] \oplus [y]) = [y] \\ &\Rightarrow [x] \oplus [0] = [y] \\ &\Rightarrow [x] = [y]\,. \end{aligned}$$

Bemerkung: Man kann sich überlegen, dass dieser Sachverhalt ganz allgemein für Ringe gilt: Sei R ein Ring und $a \in R$ mit $a \neq 0$. Wir haben dann $ax = ay \Leftrightarrow ax + (-ay) = 0 \Leftrightarrow a(x + (-y)) = 0$. Ist a kein Nullteiler, so folgt somit $x + (-y) = 0$, und dass ist äquivalent zu $x = y$.

(b) Wir zeigen zunächst, dass τ injektiv ist. Seien dazu $x, y \in \mathbb{Z}$ gegeben mit $\tau([x]) = \tau([y])$. Dies bedeutet gerade, dass $[a] \odot [x] = [a] \odot [y]$ ist. Nach (a) muss also $[x] = [y]$ sein, also ist τ injektiv.
Da τ von $\mathbb{Z}/m\mathbb{Z}$ auf $\mathbb{Z}/m\mathbb{Z}$, also eine m-elementige Menge auf eine m-elementige Menge abbildet, folgt aus der Injektivität von τ auch die Surjektivität: Hätte ein Element kein Urbild, so würden m Elemente auf $m-1$ Element oder weniger durch τ abgebildet werden, eine solche Abbildung wäre aber nicht injektiv. Folglich ist τ bijektiv.

(c) Da τ surjektiv ist, gibt es ein $[x] \in \mathbb{Z}$ mit $\tau([x]) = [1]$. Dies bedeutet aber gerade, dass $[a] \odot [x] = [1]$ ist. Wegen der Kommutativität von $\odot$ ist dann auch $[x] \odot [a] = [1]$, und $[x]$ ist invers zu $[a]$ bezüglich $\odot$.

(H36) Wir benutzen das zweite Kriterium aus Aufgabe (P30): Seien $a, b \in \ker \phi$, also $\phi(a) = e_H$ und $\phi(b) = e_H$. Wir wollen zeigen, dass auch $a * b$ und a^{-1} in $\ker \phi$ liegen. Es ist also zu zeigen, dass $\phi(a * b) = e_H$ und $\phi(a^{-1}) = e_H$ ist. Da ϕ ein Homomorphismus ist, ist $\phi(a * b) = \phi(a) \cdot \phi(b) = e_H \cdot e_H = e_H$. Mit (P29b) folgt weiter $\phi(a^{-1}) = \phi(a)^{-1} = e_H^{-1} = e_H$. Damit ist das Kriterium erfüllt, und $\ker \phi$ ist eine Untergruppe von $(G, *)$.

(H37) (a) Das Ergebnis der Verkettung zweier Abbildungen ist klar, wenn eine der Abbildungen die Identität ist. Drei Drehungen um 120° entsprechen der Identitätsabbildung. Es bleiben die Verkettungen mit Spiegelungen zu berechnen. Spiegelt man zweimal an derselben Achse, so ist dies wieder die Identität. Den Rest der Verknüpfungstafel muss man per Hand ausrechnen, wir überlegen uns

exemplarisch ein Beispiel:
Wie benutzen die Nummerierung des Dreiecks, wie sie in der Aufgabenstellung beschrieben ist. Wollen wir nun $s_1 \circ s_2$ berechnen, so spiegeln wir zuerst an der Achse durch den Mittelpunkt und die linke Ecke. Dabei wird die Ecke 2 fixiert, die Ecke 1 und die Ecke 3 werden vertauscht. Spiegeln wir nun an der Achse durch Dreiecksmittelpunkt und Spitze, so wird die Nummerierung der oberen Ecke fixiert, bleibt also 3. Die anderen beiden Nummern werden vertauscht, die linke Ecke trägt nun die Nummer 1, die rechte Ecke die Nummer 2. Dies entspricht aber gerade dem Ergebnis, das wir bei Drehung des Dreiecks um 120° gegen den Uhrzeigersinn erhalten hätten, also bei Anwendung von δ. Folglich ist $s_1 \circ s_2 = \delta$.
Analoge Berechnungen liefern die folgende Verknüpfungstafel:

$\circ$	id	δ	δ^2	s_1	s_2	s_3
id	id	δ	δ^2	s_1	s_2	s_3
δ	δ	δ^2	id	s_3	s_1	s_2
δ^2	δ^2	id	δ	s_2	s_3	s_1
s_1	s_1	s_2	s_3	id	δ	δ^2
s_2	s_2	s_3	s_1	δ^2	id	δ
s_3	s_3	s_1	s_2	δ	δ^2	id

(b) Wäre D_3 kommutativ, so müsste beispielsweise $s_1 \circ \delta = \delta \circ s_1$ sein. Laut Verknüpfungstafel trifft dies nicht zu, D_3 ist also nicht kommutativ.

(c) Die Drehungen $\{\mathrm{id}, \delta, \delta^2\}$ bilden eine Untergruppe, wie man an der Verknüpfungstafel ablesen kann. Eine zweite Untergruppe ist beispielsweise $\{\mathrm{id}, s_1\}$.