Lineare Algebra I
Übungsblatt 3

① Wir zeigen die Aussage:

$A(n)$: $a-1$ teilt $a^n - 1$

durch vollständige Induktion über $n \in \mathbb{N} - \{0\}$.

<u>Induktionsanfang</u>: $a-1 = (a-1) \cdot 1$, also $a-1$ teilt $a-1$, und die Aussage $A(1)$ gilt.

<u>$A(n) \Rightarrow A(n+1)$</u>: Sei $n \in \mathbb{N} - \{0\}$. Wir nehmen an, daß die Aussage "$a-1$ teilt $a^n - 1$" gilt, und zeigen, daß die Aussage "$a-1$ teilt $a^{n+1} - 1$" gilt.

$$a^{n+1} - 1 = a^{n+1} - a^n + a^n - 1$$
$$= \underbrace{a^n (a-1)}_{\text{durch } a-1 \text{ teilbar}} + \underbrace{a^n - 1}_{\text{durch } a-1 \text{ teilbar (nach Induktionsvoraussetzung)}}.$$

Also ist $a^{n+1} - 1$ durch $a-1$ teilbar (die Summe zweier durch $a-1$ teilbaren Zahlen ist durch $a-1$ teilbar).

Die Aussage $A(n)$ für $n \in \mathbb{N} - \{0\}$ ist daher per Induktion bewiesen

(2) Wir zeigen die Formel

$$F(n):\ a^n - 1 = (a-1)(1 + \dots + a^{n-1})$$

durch vollständige Induktion über $n \in \mathbb{N} - \{0\}$.

<u>F(1)</u> (Induktionsanfang): $a^1 - 1 = (a-1)(1 + \dots + a^0)$
$= (a-1)\,1$,

also ist die Formel $F(1)$ richtig.

<u>$F(n) \Rightarrow F(n+1)$</u>: Sei $n \in \mathbb{N} - \{0\}$, sodaß $F(n)$ gilt.

Wir zeigen, daß $F(n+1)$ gilt.

$$\begin{aligned} a^{n+1} - 1 &= a^{n+1} - a^n + a^n - 1 \\ &= (a-1)a^n + a^n - 1 \\ &= (a-1)a^n + (a-1)(1 + \dots + a^{n-1}) \\ &\quad \text{(nach der Induktionsvoraussetzung)} \\ &= (a-1)(1 + \dots + a^{n-1} + a^n) \end{aligned}$$

Also ist die Formel $F(n+1)$ richtig.

Die Formel $F(n)$ für $n \in \mathbb{N} - \{0\}$ ist daher per Induktion bewiesen.

③ (i) Wir zeigen, daß die Relation $\sim$ die 3 Eigenschaften einer Äquivalenzrelation erfüllt:

Reflexivität: Sei $a \in \mathbb{Z}$. Dann gilt: $a = a + n \cdot 0$, also $a \sim a$ ($k = 0$ funktioniert).

Symmetrie: Seien $a, b \in \mathbb{Z}$ sodaß $a \sim b$.
Dann $\exists k \in \mathbb{Z}$ sodaß $a = b + nk$, also

$$b = a + n(-k)$$

und $b \sim a$.

Transitivität: Seien $a, b, c \in \mathbb{Z}$ sodaß $a \sim b$ und $b \sim c$.
Dann existieren $k, l \in \mathbb{Z}$ sodaß

$$a = b + nk \quad \text{und} \quad b = c + nl.$$

Also $a = (c + nl) + nk = c + n(k+l)$
und damit $a \sim c$.

(ii) Erinnerung (Division mit Rest):
Sei $a \in \mathbb{Z}$. Dann gibt es eindeutig bestimmte $q, r \in \mathbb{Z}$ für die $a = nq + r$ und $0 \leq r < n$ gilt.

- Insbesondere $[a] = [r]$ wobei $r \in \{0, \dots, n-1\}$.
  Also $\mathbb{Z}/_{n\mathbb{Z}} \subset \{[0], \dots, [n-1]\}$.
  Die andere Inklusion $\{[0], \dots, [n-1]\}$ ist klar.
- Es ist ausreichend zu zeigen, daß die Klasse $[0], \dots, [n-1]$ paarweise verschieden sind. Sei $i, j \in \{0, \dots, n-1\}$ sodaß $[i] = [j]$.
  Dann gibt es $k \in \mathbb{Z}$ sodaß $i = j + nk$.
  Also $i = nk + j$ und $i = 0 \cdot n + i$ sind zwei Divisionen von i durch n.
  Nach Eindeutigkeit des Restes gilt $i = j$.

(4) Sei $x, y \in \mathbb{Z}/n\mathbb{Z}$. Wir zeigen, daß die Klasse $[a+b] \in \mathbb{Z}/n\mathbb{Z}$ unabhängig der Wahl der Repräsentanten $a \in \mathbb{Z}$ von x und $b \in \mathbb{Z}$ von y.

Seien $a', b' \in \mathbb{Z}$ sodaß $[a'] = [a] = x$ und $[b'] = [b] = y$.

Dann $a' \sim a$ und $b' \sim b$, also existiert es $k, l \in \mathbb{Z}$ sodaß

$a' = a + nk$ und $b' = b + nl$.

Dann $a' + b' = (a + nk) + (b + nl)$
$= a + b + n(k + l)$

und damit gilt $a' + b' \sim a + b$, also $[a'+b'] = [a+b]$

Es gilt auch $a'b' = (a + nk)(b + nl)$
$= ab + n(kb + al + nkl)$

und damit gilt $a'b' \sim ab$.
Die Klasse des Produktes $[ab]$ ist auch unabhängig der Wahl der Repräsentanten $a, b \in \mathbb{Z}$.

Also sind die Abbildungen $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$
$([a],[b]) \mapsto [a+b]$ und $([a],[b]) \mapsto [ab]$
wohldefiniert.

⑤ zu (i): Seien $a, a' \in \mathbb{Z}$ sodaß $[a]_m = [a']_m \in \mathbb{Z}/m\mathbb{Z}$

Wir zeigen, daß $[a]_n = [a']_n \in \mathbb{Z}/n\mathbb{Z}$.

Es existiert $k \in \mathbb{Z}$ sodaß $a = a' + mk$.

Nach Voraussetzung ist m durch n teilbar, also existiert es $q \in \mathbb{N}$ sodaß $m = nq$.

Also $a = a' + mk = a' + n(qk)$, und damit $[a]_n = [a']_n$.

zu (ii): Sei $a \in \mathbb{Z}$.

$$[a]_m \in f^{-1}\{[0]_n\} \iff [a]_n = [0]_n$$
$$\iff \exists k \in \mathbb{Z},\ a = nk$$

Also $f^{-1}\{[0]_n\} = \{[nk]_m \mid k \in \mathbb{Z}\}$.

Wir betrachten die Abbildung:

$$\varphi: \mathbb{Z}/q\mathbb{Z} \longrightarrow f^{-1}\{[0]_n\}$$
$$[k]_q \longmapsto [nk]_m$$

<u>φ ist wohldefiniert:</u> Seien $k, k' \in \mathbb{Z}$ sodaß $[k]_q = [k']_q$.
Dann $\exists l \in \mathbb{Z}$ sodaß $k = k' + ql$, also
$$nk = nk' + nql = nk' + ml$$
und damit $[nk]_m = [nk']_m$.

Wir haben schon gesehen, daß φ surjektiv ist.

<u>φ ist injektiv:</u> Seien $k, k' \in \mathbb{Z}$ sodaß $[nk]_m = [nk']_m$. Dann $\exists p \in \mathbb{Z}$ sodaß $nk = nk' + mp = n(k' + qp)$, also $k = k' + qp$, und damit $[k]_q = [k']_q$

Die Abbildung Ψ ist bijektiv, also

$$|f^{-1}\{[0]_n\}| = |\mathbb{Z}/9\mathbb{Z}| = 9 \quad \text{(nach 3 (ii))}$$