$\mathbf{Aufgabe}\ \mathbf{1}$ : Es sei M eine endliche Menge und die Funktion

$$f: M \to M$$

sei surjektiv. Zeigen Sie, dass f dann auch injektiv ist.

**Lösung**: Um die obige Behauptung beweisen können, formulieren wir zunächst den folgenden Hilfssatz.

Hilfssatz: Ist M eine endliche Menge und ist die Funktion

$$f: M \to N$$

nicht injektiv, so gilt

$$card(f(M)) < card(M)$$
.

Beweis des Hilfssatzes: Es seien  $x_1, x_2, \dots, x_{n-1}, x_n$  die verschiedenen Elemente der Menge M, es gelte also

$$M = \{x_1, x_2, \dots, x_{n-1}, x_n\}$$
 und  $card(M) = n$ .

Da f nicht injektiv ist, gibt es  $i, j \in \{1, \dots, n\}$  mit

$$i \neq j$$
, aber  $f(x_i) = f(x_j)$ .

Dann haben wir

$$card(f(M))$$
=  $card(f(M))$ 
=  $card(f(x_1), \dots, f(x_i), \dots, f(x_{j-1}), f(x_j), f(x_{j+1}), \dots, f(x_n))$ 
=  $card(f(x_1), \dots, f(x_i), \dots, f(x_{j-1}), f(x_{j+1}), \dots, f(x_n))$ 
da  $f(x_j) = f(x_i)$ 
 $\leq n - 1$ 
 $< n$ 
=  $card(M)$ .

Also haben wir insgesamt card(f(M)) < card(M).

**Beweis**: Wir beweisen nun die in der Aufgabe gemachte Behauptung. Wir führen den Beweis indirekt und nehmen an, dass die Funktion

$$f:M\to M$$

nicht injektiv ist. Nach dem gerade bewiesenem Hilfssatz wissen wir, dass dann

ist. Da f nach Voraussetzung <u>surjektiv</u> ist, wissen wir andererseits, dass f(M) = M ist. Ersetzen wir also in der oberen Ungleichung f(M) durch M, so erhalten wir den Widerspruch

$$card(M) < card(M)$$
.

Folglich muss die Annahme, dass f nicht injektiv ist, falsch sein.

Bemerkung: Es ist häufig so, dass eine Behauptung nicht unmittelbar bewiesen werden kann. Statt dessen versuchen wir in so einem Fall, den wesentlichen Grund, aus dem die Behauptung gilt, als Hilfsatz zu formulieren und zu beweisen. Der eigentliche Beweis stützt sich dann auf diesen Hilfsatz. Oft ist dieser Hilfssatz eine geeignete Verallgemeinerung der Behauptung. Unter Umständen ist es nicht mit einem einzigen Hilfssatz getan. So wurde zum Nachweis der Fermat'schen Vermutung die algebraische Geometrie entwickelt, die aus Hunderten von Definitionen und Sätzen besteht, mit deren Hilfe die Vermutung bewiesen wurde.