Blatt 5, Aufgabe 2

Sei G eine Gruppe und für $g \in G$ die *Ordnung* $\operatorname{ord}(g)$ *von* g als die Anzahl der Elemente der Untergruppe $\langle g \rangle \subset G$ definiert.

Sei ein beliebiges $g \in G$ mit $\operatorname{ord}(g) < \infty$ gegeben.

Behauptung (a)**.** $\operatorname{ord}(g) = \min\{n \in \mathbb{N} \mid g^n = e\}$

Beweis. Da $\operatorname{ord}(g) < \infty$, kann die Liste

$$g^0, g^1, g^2, \ldots$$

nicht aus lauter verschiedenen Gruppenelementen bestehen. Also gibt es gewisse Exponenten i, j (oBdA $i > j$) mit $g^i = g^j$. Daraus folgt $g^{i-j} = e$. Damit existiert das Minimum der rechten Seite der Gleichung.

Sei nun n dieses Minimum, also die kleinste natürliche Zahl (≥ 1) mit $g^n = e$. Wir wollen zeigen, dass $n = \operatorname{ord}(g)$. Dazu erinnern wir uns an die Darstellung von $\langle g \rangle$ und vereinfachen diese:

$$\begin{aligned}\langle g \rangle &= \{\ldots, g^{-2}, g^{-1}, g^0, g^1, g^2, \ldots\} \\ &= \{g^0, g^1, g^2, \ldots\} \\ &= \{g^0, g^1, g^2, \ldots, g^{n-1}\}\end{aligned}$$

Dabei müssen wir die einzelnen Schritte begründen:

– Der erste Schritt folgt nach Blatt 4, Aufgabe 4(iii).

– Da $g^n = g\, g^{n-1} = e$, ist das Inverse von g das Gruppenelement g^{n-1}. Somit gilt $g^{-k} = g^{k(n-1)}$ für alle $k \geq 1$, womit wir die negativen g-Potenzen also nicht separat aufführen müssen, da sie jeweils gleich gewissen nichtnegativen g-Potenzen sind. Das begründet den zweiten Schritt.

– Da $g^n = e$, müssen wir g^n nicht separat aufführen. Da $g^{n+1} = g^n\, g = g$, müssen wir auch g^{n+1} nicht separat aufführen. Diese Argumentation können wir unbegrenzt fortführen, sodass wir also sehen, dass wir die Elemente g^k mit $k \geq n$ nicht aufführen müssen. Damit ist der dritte Schritt gezeigt.

Als Zwischenstand können wir festhalten: Die Anzahl der Elemente von $\langle g \rangle$ ist höchstens n. Um zu zeigen, dass sie genau n ist, müssen wir jetzt noch zeigen, dass in der Aufzählung $g^0, \ldots, g^{n-1}$ kein Element mehr als einmal vorkommt.

Sei dazu $g^i = g^j$ mit $i, j \in \{0, \ldots, n-1\}$, oBdA $i \geq j$. Dann folgt $g^{i-j} = e$. Wäre nun $i - j \neq 0$, so wäre $i - j$ eine natürliche Zahl, die kleiner als n ist, und trotzdem die Bedingung $g^{i-j} = e$ erfüllt. Das kann nicht sein, da n nach Definition die kleinste solcher Zahlen ist. $\square$

Behauptung (b)**.** $g^n = e \Leftrightarrow \operatorname{ord}(g) \mid n$

Beweis. Sei eine beliebige ganze Zahl n gegeben. Diese können wir durch die Ordnung von g mit Rest teilen:

$$n = k \cdot \operatorname{ord}(g) + r,$$

für gewisse $k \in \mathbb{Z}$, $r \in \{0, \ldots, \operatorname{ord}(g) - 1\}$. Dann sehen wir:

$$g^n = g^{k \cdot \operatorname{ord}(g) + r} = (g^{\operatorname{ord}(g)})^k \, g^r = e^k \, g^r = g^r$$

Also ist $g^n = e$ genau dann, wenn $g^r = e$. Das ist wiederum genau dann der Fall, wenn $r = 0$ ist (nach dem Argument im letzten Absatz des vorigen Beweises). Schließlich gilt das genau dann, wenn n durch $\operatorname{ord}(g)$ teilbar ist. □

Behauptung (c)**.** $\langle g \rangle = \{g^0, g^1, g^2, \ldots, g^{n-1}\}$

Beweis. Das haben wir bereits in (a) bewiesen. □

Behauptung (d)**.** $\operatorname{ord}(g^k) = \operatorname{ord}(g) \,/\, \operatorname{ggT}(k, \operatorname{ord}(g))$

Beweis. Nach (a) ist die Ordnung von g^k der kleinste Exponent n derart, dass $(g^k)^n = g^{kn} = e$ ist. Also ist kn das kleinste gemeinsame Vielfache von k und $\operatorname{ord}(g)$, womit nach einer Formel der fünften Klasse

$$kn = k \cdot \operatorname{ord}(g) \,/\, \operatorname{ggT}(k, \operatorname{ord}(g))$$

gilt. Durch Kürzen sehen wir, dass $n = \operatorname{ord}(g) \,/\, \operatorname{ggT}(k, \operatorname{ord}(g))$. □