1 Der Satz von Lagrange

Wir hatten soeben gesehen, dass bei endlichen zyklischen Gruppen ein direkter Zusammenhang zwischen der Untergruppenstruktur der Gruppe und der Primfaktorisierung der Gruppenordnung bestand. Zur Erinnerung:
Sei $(G, \cdot, e)$ eine zyklische Gruppe mit $|G| = n$, dann gilt:

1. $(U \leq G \Rightarrow |U|/|G|)$
2. $(\forall\, d \in \mathbb{N}$ mit $d/n\ \exists! U \leq G : |U| = d)$

Die Aussage 2) läßt sich im allgemeinen nicht auf nicht-zyklische Gruppen übertragen, weder in ihrer Existenz- noch in ihrer Eindeutigkeitsaussage, wie man an folgenden kleinen Gruppen bereits sehen kann.
$\mathbb{Z}_2 \times \mathbb{Z}_2$ hat drei Untergruppen der Ordnung 2.
A_4 hat keine Untergruppe der Ordnung 6.
Das Erstaunliche ist nun, dass die Aussage 1) sich sehr wohl auf endliche Gruppen ausdehnen läßt. Wir betrachten eine beliebige endliche Gruppe $(G, \cdot, e)$ und eine Untergruppe U von G. Durch U läßt sich eine Äquivalenzrelation auf G konstruieren:

$$\forall g, h \in G : (g \approx h \Leftrightarrow h \cdot g^{-1} \in U)\ ;\ [g] = Ug$$

Mit Hilfe der bijektiven Abbildung

$$f_{g,h} : \begin{cases} Ug & \rightarrow & Uh \\ ug & \mapsto & uh \end{cases}$$

sehen wir, dass alle Nebenklassen gleich groß sind und insbesondere so groß wie U selber. Dann gilt:

$$G = \dot{\bigcup_{g \in V}} Ug \quad \text{wobei } V \text{ ein Vertretersystem der Repräsentanten in } G \text{ ist.}$$

$$|G| = |\dot{\bigcup_{g \in V}} Ug| = \sum_{g \in V} |Ug| = \sum_{g \in V} |U| = [G : U] \cdot |U|$$

Die Anzahl der auftretenden Nebenklassen wird als der sogenannte Index der Untergruppe U in G bezeichnet und mit $[G : U]$ notiert. Wir haben also gezeigt:

$$|G| = [G : U] \cdot |U|$$

Damit ist sowohl die Untergruppenordnung als auch der Index immer ein Teiler der Gruppenordnung. Das ist der Satz von Lagrange.