Algebra, Theorie endlicher Gruppen $(G,\cdot)$, Einselement sei als 1 notiert.

Das Folgende gilt für alle endlichen Gruppen:

(1) Satz: $\forall a \in G\ \exists\, k \in \mathbb{N}:\ a^k = 1$ Für jedes Element a gibt einen Exponenten k, so dass die Potenz 1 ist.

Beweis: $\exists \bar{a}: a\bar{a} = 1$. Sei $a^i = a^j$ mit $i < j$. Dann folgt $1 = a^i\bar{a}^i = a^j\bar{a}^i = a^{j-i} = a^k$. q.e.d

(2) Def.: Sei $a \in G$. Die kleinste natürliche Zahl (>0) mit $a^k = 1$ heißt Ordnung von a, kurz $ord(a)$.

(3) Satz und Def.: $\langle a\rangle := \{1, a, a^2, \dots, a^{ord(a)-1}\}$ ist eine Gruppe.

$\langle a\rangle$ heißt „von a erzeugte Untergruppe“.

Beweis: Abgeschlossenheit: $a^i a^j = a^{i+j} = a^{ord(a)+r} = a^{ord(a)}a^r = a^r$, notiert für $i + j \geq ord(a)$, da sonst klar.

Inverses zu a^i ist $a^{ord(a)-i}$, denn $a^i a^{ord(a)-i} = a^{ord(a)} = 1$. q.e.d.

(4) Def.: Die Ordnung einer Gruppe ist die Anzahl ihrer Elemente, also $ord(G) = |G|$, damit auch $ord(\langle a\rangle) = ord(a)$.

(5) Def.: Sei $g \in G$. Die Menge $g\langle a\rangle := \{g, g\,a, g\,a^2, \dots, g\,a^{ord(a)-1}\}$ heißt Nebenklasse von a.

(6) Satz: a) Jede Nebenklasse $g\langle a\rangle$ hat genau $ord(a)$ Elemente.

b) Zwei Nebenklassen sind entweder gleich oder disjunkt.

Beweis a) Mehr Elemente können es ja nicht sein, aber evt. weniger. Sei Sei $\bar{g}\,g = 1$ und $g\,a^i = g\,a^j$, dann folgt $\bar{g}\,g\,a^i = \bar{g}\,g a^j$ also $a^i = a^j$. Letzteres ist in $\langle a\rangle$ für $i \neq j$ nicht möglich, also sind es auch $ord(a)$ Elemente.

b) Sei $g\,a^i = h\,a^j$ mit $i < j$ ein Element aus beiden Nebenklassen. Dann folgt $g = h\,a^{j-i} \in h\langle a\rangle$ also auch $\forall r \quad ga^r \in h\langle a\rangle$ und damit $g\langle a\rangle \subseteq h\langle a\rangle$. Weiter folgt $g\,a^i a^{ord(a)-j} = h\,a^j a^{ord(a)-j} = h$, damit wie oben $h\langle a\rangle \subseteq g\langle a\rangle$, also $g\langle a\rangle = h\langle a\rangle$. Ein gemeinsames Element erzwingt also schon, dass die Nebenklassen gleich sind. Kein gemeinsames Element heißt „disjunkt“ q.e.d

(7) Hauptsatz zur Ordnung von Gruppen und Elementen

a. $ord(a)\,|\,ord(G)$, jede Elementordnung teilt die Gruppenordnung

b. $\forall a:\ a^{ord(G)} = 1$, ein Element hoch Gruppenordnung ist immer 1.

c. $e = q \cdot ord + r$, dann gilt $a^e = a^r$. Dabei kann man als ord die Elementordnung oder die Gruppenordnung nehmen.

Beweis: a) Die Vereinigung aller Nebenklassen –es gebe z Stück- ist die ganze Gruppe und alle Nebenkassen haben gleich viele Elemente, nämlich $ord(a)$. Dann ist $z \cdot ord(a) = ord(G)$. b) $a^{ord(G)} = a^{z\cdot ord(a)} = \left(a^{ord(a)}\right)^z = 1^z = 1 = 1$ c) klar. qed