**Beh.:** $(n,\varphi(n))=1 \iff (G \text{ Gruppe}, \#G=n \Rightarrow G \text{ zyklisch})$

**Notation:** Sei $C(n)$ die zyklische Gruppe der Ordnung $n$.

**Bew.:** Beide Bedingungen implizieren, daß $n$ quadratfrei ist:

Ist $p^k \| n$, $k\geq 2$, ist $p^{k-1} \mid \varphi(n)$, also $p \mid (n,\varphi(n))$,

und die Gruppe $C(\frac{n}{p^k}) \times C(p)^k$ ist nicht isomorph zu $C(n)$.

Sei also $n$ quadratfrei, etwa $n=p_1\cdots p_k$ und $\varphi(n)=(p_1-1)\cdots(p_k-1)$.

„$\Leftarrow$":

Ist $(n,\varphi(n))\neq 1$, so ist $n=pqm$ mit $p,q\in\mathbb{P}$, $p \mid q-1$, $m\in\mathbb{N}$.

Dann gibt es eine nichtabelsche Gruppe $H$ der Ordnung $pq$

(das semidirekte Produkt $H:=\mathbb{Z}_p \ltimes_f \mathbb{Z}_q$ mit der Operation

$b\cdot a := a\cdot f(a)(b)$, wo $f$ geg. ist durch

$$\begin{array}{ccccc} \mathrm{Aut}(\mathbb{Z}_q) & \supseteq & \mathbb{F}_q^\times & \cong & \mathbb{Z}/(q-1) \\ & & {\scriptstyle f}\nwarrow & & \uparrow \\ & & & \mathbb{Z}_p & \end{array}$$

)

also ist $H\times C(m)$ nichtabelsche Gruppe der Ordnung $n$.

„$\Rightarrow$": Sei $(n,\varphi(n))=1$ und $n$ minimal so, daß eine nichtzyklische Gruppe $G$ der Ordnung $n$ existiert. Werden einen $\lightning$ herleiten:

1) $m \mid n \Rightarrow (m,\varphi(m))=1$ $\ulcorner$aus $n=p_1\cdots p_k$ und $\varphi(n)=(p_1-1)\cdots(p_k-1)\lrcorner$

2) $n$ minimal $\Rightarrow$ jede echte UG und jede nichttriv. Faktorgruppe von $G$ ist zyklisch wegen 1)

3) $\underbrace{Z(G)}_{=\{a\in G;\, \forall g\in G:\, ga=ag\}}=\{1\}$ $\ulcorner$Sonst: $G/Z(G)$ zyklisch wegen 2), also $G$ abelsch

$\ulcorner$denn: $G/Z=\langle aZ\rangle$, dann ist $G=\langle a,Z\rangle$

$[g\in G \Rightarrow gZ=a^iZ \Rightarrow g=a^ib$ mit $b\in Z]$, für $u,v\in G$, etwa

$u=a^ib$, $v=a^jb'$ mit $b,b'\in Z \Rightarrow uv=a^iba^jb'=a^jb'a^ib=vu\lrcorner$,

damit ist $G$ zyklisch $\lightning\lrcorner$ (HS über endl. erz. ab. Gr.)

4) Sei $x \neq 1$ Element einer maximalen UG $U$ von $G$.
Dann ist $U$ der Zentralisator $C_G(x) := \{g \in G;\ gxg^{-1} = x\}$ von $x$ in $G$.
⌈ $C_G(x)$ ist echte UG von $G$ nach 3) ⌈sonst $x \in Z(G)$⌋, $U$ ist zyklisch nach 2), und deshalb $U \subseteq C_G(x)$. Da $U$ maximal, folgt $U = C_G(x)$. ⌋

5) Sind $U \neq V$ zwei maximale UG von $G$, ist $U \cap V = \{1\}$.
⌈ Sonst $1 \neq x \in U \cap V \underset{4)}{\Rightarrow} U = C_G(x) = V$, ↯ ⌋

6) $U$ maximale UG von $G \Rightarrow U = N_G(U) := \{g \in G;\ gUg^{-1} = U\}$, dem Normalisator von $U$ in $G$.
⌈ Sei $1 \neq x \in N_G(U)$. Betr. $\alpha: U \to U$, $u \mapsto \alpha(u) := xux^{-1}$, dann ist $\alpha \in \mathrm{Aut}(U)$. Ist $\#U = m$, gilt $\#\mathrm{Aut}(U) = \varphi(m) \mid \varphi(n)$.
Da $\mathrm{ord}\,x \mid n$, also $\mathrm{ord}\,\alpha \mid n$, ist $\mathrm{ord}\,\alpha = 1$ wegen $(\varphi(n), n) = 1$
$\Rightarrow x$ zentralisiert $U$, d.h. $U \subseteq C_G(x) \overset{3)}{=} U \Rightarrow x \in U$. ⌋

$\varphi(m)$ Automorphismen der zyklischen Gr. $U = C_m$

7) Sei $U$ maximale UG von $G$, $\#U = u$. Die Konjugierten von $U$ enthalten dann zusammen insg. $n - \frac{n}{u}$ viele Elemente $\neq 1$.
⌈ Die Anzahl der Konjugierten von $U$ ist der Index des Normalisators von $U$ in $G$, dieser ist $\frac{n}{u}$ nach 6). Nach 5) schneiden sich zwei Konjugierte von $U$ nur in $\{1\}$. Die Konjugierten enthalten also insg. $(u-1)n/u$ viele Elemente $\neq 1$. ⌋

Bahnen-gg. Gegl. Op. von $G$ auf $\{gUg^{-1}\} =: M$ durch Konjugation

8) Sei $U$ wie in 7), und $x$ in keinem Konjugierten von $U$.
Sei $V$ maximale UG mit $x \in V$, also nicht konjugiert zu $U$.
Jedes Konjugierte von $U$ schneidet jedes Konjugierte in $V$ nur in $\{1\}$. 7) auf $V$: die Konjugierten von $V$ enthalten $n - \frac{n}{v}$ Elemente $\neq 1$, also ist $n - \frac{n}{u} + n - \frac{n}{v} < n \Rightarrow uv < u + v$,

↯. □

Bemerkung/Zusatz:

Alternativer Beweis für

„$\Rightarrow$" im einfacheren Spezialfall $n = p_1 p_2$, $p_1 > p_2$:

Sei $S_1$ die Anzahl der $p_1$-Sylow UG von $G$, nach Sylow ist $S_1 \equiv 1\ (p_1)$.

Falls $S_1 \geq p_1 + 1$, wäre die Anzahl El. in $G \geq \underbrace{(p_1+1)(p_1-1)}_{\text{die } p_1\text{-Sylowgr. haben nur } e \text{ gemeinsam}} + \underbrace{1}_{\text{neutr. El. } e} = p_1^2 - 1 + 1 = p_1^2 > n$, ↯.

Also ex. genau eine $p_1$-Sylow-UG in $G$,

diese ist $C_{p_1}$ (zyklisch der Ordnung $p_1$).

Beh. $M = C_{p_1} \setminus \{1\} \subseteq C_{p_1} \trianglelefteq G$. Denn: Sei $g \in G$,

für $a \in M$ ist dann $gag^{-1} \in M$, da dies $\neq 1$ und auch wieder die Ordnung $p_1$ hat und nur eine $p_1$-Sylowgr. ex.

Somit operiert $G$ auf $M$ durch Konjugation.

Demnach können wir die Bahnengl. anwenden:

Nach dieser gilt $|\underbrace{a^G}_{\text{Bahn von } a \text{ bzgl. Konjugation, hat } \leq p_1 - 1 \text{ viele Elemente}}| \cdot |\underbrace{C_G(a)}_{\text{Zentralisator von } a = \text{Stabilisator von } a \text{, d.h. die } g \text{ mit } gag^{-1} = a}| = |G| = p_1 p_2$, es folgt: $|a^G| = 1$ oder $= p_2$.

Falls $|a^G| = p_2$: $M$ zerfällt in Bahnen der Ordnung $p_2$, es folgt $p_2 \mid p_1 - 1$. ↯.

Falls $|a^G| = 1$: $gag^{-1} = a$ für alle $g \Rightarrow C_{p_1} \subseteq Z(G)$.

Also ist $Z(G) = G$, d.h. $G$ abelsch, $G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2}$,

also $G \cong \mathbb{Z}_{p_1 p_2}$ und damit zyklisch. $\square$