**3.** Für eine endliche abelsche Gruppe $G$ und eine Primzahl $p$ sei

$$G(p) = \{\, a \in G \mid a^{p^k} = e \text{ für ein } k \geq 0 \,\}.$$

Zeigen Sie:

(i) $G(p)$ ist eine Untergruppe von $G$.

(ii) Ist $G = A \cdot B$ (dir), so ist $G(p) = A(p) \cdot B(p)$ (dir).

(iii) $G(p)$ ist die eindeutig bestimmte $p$-Sylowuntergruppe von $G$.

**Beweis:** (i) Wir benutzen das Untergruppenkriterium, und müssen zeigen: $G(p) \neq \emptyset$ und für alle $a, b \in G(p)$ ist auch $ab^{-1} \in G(p)$. Wegen $e = e^1 = e^{p^0}$ ist $e \in G(p)$, also $G(p)$ nicht leer. Es seien $a, b \in G(p)$. Nach Voraussetzung existieren $k, l \geq 0$ mit $a^{p^k} = e$ und $b^{p^l} = e$. Es sei $m = \max\{k, l\}$. Dann ist, wegen $p^k \mid p^m$ und $p^l \mid p^m$, auch $a^{p^m} = e$ und $b^{p^m} = e$. Außerdem ist $(b^{-1})^{p^m} = (b^{p^m})^{-1} = e$. Es folgt $(ab^{-1})^{p^m} = a^{p^m}(b^{-1})^{p^m} = e$, und das war zu zeigen. (In der Gleichheit $(ab^{-1})^{p^m} = a^{p^m}(b^{-1})^{p^m}$ haben wir benutzt, dass $G$ abelsch ist!)

(ii) Es sei $G = A \cdot B$ (dir). Wir erinnern uns an eine der äquivalenten Charakterisierungen des inneren Produkts: Jedes Element $g \in G$ kann in der Form $g = ab$ mit $a \in A$ und $b \in B$ dargestellt werden und es ist $A \cap B = \{e\}$. (Und $A$, $B$ sind Normalteiler von $G$, aber das ist hier trivialerweise der Fall, weil $G$ abelsch ist.) Wir zeigen: $G(p) = A(p) \cdot B(p)$. Die Direktheit des Produkts folgt dann wegen $A(p) \cap B(p) \subset A \cap B = \{e\}$.

$A(p) \cdot B(p) \subset G(p)$: Es seien $a \in A(p)$ und $b \in B(p)$. Nach Definition existieren $k, l \geq 0$, so dass gilt $a^{p^k} = e$ und $b^{p^l} = e$. Es sei $m = \max\{k, l\}$. Wie in (i) folgt $(ab)^{p^m} = a^{p^m} b^{p^m} = e$.

$G(p) \subset A(p) \cdot B(p)$: Es sei $g \in G(p)$. Dann existiert $k \geq 0$, so dass gilt $g^{p^k} = e$. Wegen $G = A \cdot B$ gibt es $a \in A$ und $b \in B$ mit $g = ab$. Dann ist $e = g^{p^k} = (ab)^{p^k} = a^{p^k} b^{p^k}$. Wegen $a^{p^k} = b^{-p^k} \in A \cap B = \{e\}$ folgt $a^{p^k} = e$ und $b^{-p^k} = e$ (und somit auch $b^{p^k} = e$). [1] Also ist $a \in A(p)$ und $b \in B(p)$.

(iii) Es genügt zu zeigen, dass $G(p)$ eine $p$-Sylowuntergruppe von $G$ ist. Weil $G$ abelsch ist, ist $x^{-1}G(p)x = x^{-1}xG(p) = G(p)$ für all $x \in G$, und somit, nach dem zweiten Sylowsatz, $G(p)$ dann schon die einzige $p$-Sylowuntergruppe von $G$.

Wir zeigen die Aussage zuerst für endliche zyklische Gruppen $G$. Es sei also $G = \langle a \rangle$ mit $a \in G$ und $|G| = \mathrm{ord}(a) = p^k m$ mit $k \geq 0$ und $p \nmid m$. Aus der

[1] *Alternative:* Eine weitere äquivalente Charakterisierung des inneren Produkts impliziert, dass die Darstellung von Elementen aus $G$ als Produkt von Elementen aus $A$ und $B$ eindeutig ist. Wegen $e = a^{p^k} b^{p^k} = ee$ mit $a^{p^k}$, $e \in A$ und $b^{p^k}$, $e \in B$ folgt also $a^{p^k} = e$ und $b^{p^k} = e$.

Einführung in die Algebra wissen wir: $\text{ord}(a^n) = \frac{p^k m}{\text{ggT}(n, p^k m)}$. Nach Definition ist $G(p)$ die Untergruppe jener Elemente, deren Ordnung eine Potenz von $p$ ist. Also ist $a^n \in G(p)$ genau dann, wenn $m \mid n$. Somit ist $G(p) = \langle a^m \rangle$, und das ist, wegen $\text{ord}(a^m) = p^k$, eine Untergruppe von $G$ der Ordnung $p^k$. Also ist $G(p)$ eine $p$-Sylowuntergruppe.

Es sei nun $G$ eine beliebige endliche abelsche Gruppe. Nach dem Struktursatz für endliche abelsche Gruppen ist $G = G_1 \cdot G_2 \cdot ... \cdot G_r$ (dir) mit zyklischen Gruppen $G_1, ..., G_r$. Wir beweisen die Aussage durch Induktion nach $r$. Den Fall $r = 1$ haben wir bereits behandelt. Es sei also $r > 1$ und wir nehmen an, die Aussage stimmt für $r - 1$. Wir setzen $H = G_2 \cdot ... \cdot G_r$. Es sei $|G_1| = p^k m$ und $|H| = p^l n$ mit $k, l \geq 0$ und $p \nmid m$, $p \nmid n$. Nach Induktionsvoraussetzung ist $G_1(p)$ die $p$-Sylowuntergruppe von $G_1$ und $H(p)$ die $p$-Sylowuntergruppe von $H$. Also ist $|G_1(p)| = p^k$ und $|H(p)| = p^l$. Dann ist aber

$$|G(p)| = |G_1(p) \cdot H(p)| = |G_1(p)||H(p)| = p^{k+l}.$$

Wegen $|G| = |G_1||H| = p^{k+l} mn$ mit $p \nmid mn$ ist also $G(p)$ die $p$-Sylowuntergruppe von $G$.