3. Teil: Gruppen II

13. Direkte Produkte von Gruppen

Satz 93: Es sei $I \neq \varnothing$ eine (Index)Menge und G_i eine Gruppe $\forall i \in I$. Das kartesische Produkt $\prod_{i\in I} G_i$, versehen mit der Verknüpfung $(x_i)_{i\in I} \cdot (y_i)_{i\in I} = (x_i y_i)_{i\in I}$, ist eine Gruppe. Sind alle Gruppen G_i abelsch (für $i \in I$), so ist auch $\prod_{i\in I} G_i$ abelsch.

Beweis: Nach dem Auswahlaxiom ist $\prod_{i\in I} G_i \neq \varnothing$. Die Assoziativität gilt wegen

$$\big((x_i)_{i\in I} \cdot (y_i)_{i\in I}\big) \cdot (z_i)_{i\in I} = \big((x_i y_i) z_i\big)_{i\in I} = \big(x_i (y_i z_i)\big)_{i\in I} = (x_i)_{i\in I} \cdot \big((y_i)_{i\in I} \cdot (z_i)_{i\in I}\big).$$

Ist e_i das neutrale Element von G_i (für $i \in I$), so ist $(e_i)_{i\in I}$ neutrales Element von $\prod_{i\in I} G_i$, da

$$(x_i)_{i\in I} \cdot (e_i)_{i\in I} = (x_i e_i)_{i\in I} = (x_i)_{i\in I} = (e_i x_i)_{i\in I} = (e_i)_{i\in I} \cdot (x_i)_{i\in I}.$$

Ist $x_i^{-1} \in G_i$ inverses Element zu $x_i \in G_i$ (für $i \in I$), so ist $(x_i^{-1})_{i\in I}$ inverses Element von $(x_i)_{i\in I}$, da

$$(x_i)_{i\in I} \cdot (x_i^{-1})_{i\in I} = (x_i x_i^{-1})_{i\in I} = (e_i)_{i\in I} = (x_i^{-1} x_i)_{i\in I} = (x_i^{-1})_{i\in I} \cdot (x_i)_{i\in I}.$$

Ist G_i abelsch $\forall i \in I$, so folgt

$$(x_i)_{i\in I} \cdot (y_i)_{i\in I} = (x_i y_i)_{i\in I} = (y_i x_i)_{i\in I} = (y_i)_{i\in I} \cdot (x_i)_{i\in I}.$$

Definition: Ist $I \neq \varnothing$ eine (Index)Menge und G_i eine Gruppe $\forall i \in I$, so wird die in Satz 93 beschriebenen Gruppe $\prod_{i\in I} G_i$ das (äußere) direkte Produkt der Gruppen G_i (mit $i \in I$) genannt.

Bemerkung: Ist I endlich, also o.B.d.A. $I = \{1, \dots, n\}$, so schreibt man für das direkte Produkt der Gruppen $G_1, \dots, G_n$ auch $G_1 \times \cdots \times G_n$. Schreibt man die Verknüpfungen der Gruppen $G_1, \dots, G_n$ additiv, so schreibt man stattdessen auch $G_1 \oplus \cdots \oplus G_n$.

Definition: Es sei G eine Gruppe und $N_i \trianglelefteq G$ für $1 \leq i \leq k$. Man sagt, G sei das (innere) direkte Produkt seiner Normalteiler $N_1, \dots, N_k$ wenn

1) $G = N_1 \cdots N_k$, wobei es sich um ein Komplexprodukt handelt, d.h.

$$G = \{a_1 \cdots a_k \mid a_i \in N_i \text{ für } 1 \leq i \leq k\}.$$

2) Für alle $a \in G$ ist die nach 1) existierende Darstellung $a = a_1 \cdots a_k$ mit $a_i \in N_i$ für $1 \leq i \leq k$ eindeutig, d.h.

$$\forall a \in G \; \exists!\, a_1 \in N_1 \dots \exists!\, a_k \in N_k : a = a_1 \cdots a_k.$$

Lemma 94: Es sei G einen Gruppe und $N_i \trianglelefteq G$ für $1 \leq i \leq k$. Dann gilt

$$\big\langle N_1 \cup \cdots \cup N_k \big\rangle = N_1 \cdots N_k.$$

Beweis: Induktion nach k. Der Fall $k = 1$ ist trivial. Der Fall $k = 2$ folgt aus Satz 29 (iii). Aus

$$N_1 \cup \cdots \cup N_{k+1} \subseteq \big\langle N_1 \cup \cdots \cup N_k \big\rangle \cup N_{k+1} \subseteq \big\langle \langle N_1 \cup \cdots \cup N_k \rangle \cup N_{k+1} \big\rangle$$

folgt

$$\big\langle N_1 \cup \cdots \cup N_{k+1} \big\rangle \subseteq \big\langle \langle N_1 \cup \cdots \cup N_k \rangle \cup N_{k+1} \big\rangle$$

und aus

$$\langle N_1 \cup \cdots \cup N_k \rangle \cup N_{k+1} \subseteq \big\langle N_1 \cup \cdots \cup N_{k+1} \big\rangle$$

folgt

$$\big\langle \langle N_1 \cup \cdots \cup N_k \rangle \cup N_{k+1} \big\rangle \subseteq \big\langle N_1 \cup \cdots \cup N_{k+1} \big\rangle.$$

Daraus ergibt sich insgesamt

$$\begin{aligned} \big\langle N_1 \cup \cdots \cup N_{k+1} \big\rangle = \big\langle \langle N_1 \cup \cdots \cup N_k \rangle \cup N_{k+1} \big\rangle &\overset{\text{IV}}{=} \big\langle N_1 \cdots N_k \cup N_{k+1} \big\rangle \\ &\overset{\text{Satz 29 (iii)}}{=} (N_1 \cdots N_k) N_{k+1} = N_1 \cdots N_{k+1} \end{aligned}$$

Bemerkung: Wegen Lemma 94 könnte man Bedingung 1) in der Definition des inneren direkten Produkts durch $G = \big\langle N_1 \cup \cdots \cup N_k \big\rangle$ ersetzen.

Lemma 95: Es sei G eine Gruppe, $A \trianglelefteq G$ und $B \trianglelefteq G$. Ist $A \cap B = \{e\}$, so gilt $ab = ba \ \forall a \in A \ \forall b \in B$.

Beweis: Ist $a \in A$ und $b \in B$, so gilt $aba^{-1} \in B$ (da $B \trianglelefteq G$) und $ba^{-1}b^{-1} \in A$ (da $A \trianglelefteq G$). Folglich ist $\big(aba^{-1}\big)b^{-1} = a\big(ba^{-1}b^{-1}\big) \in A \cap B = \{e\}$ und daher $aba^{-1}b^{-1} = e$ und $ab = ba$.

Lemma 96: Ist die Gruppe G das innere direkte Produkt ihrer Normalteiler $N_1, \ldots, N_k$, so gelten

(i) $N_i \cap N_j = \{e\}$ für $1 \leq i, j \leq k$, $i \neq j$,
(ii) $\forall i, j \in \{1, \ldots, k\}$, $i \neq j \ \ \forall a \in N_i \ \forall b \in N_j : ab = ba$.

Beweis: (i) Ist $x \in N_i \cap N_j$, so hat x die beiden Darstellungen

$$x = e \cdots exe \cdots\cdots e = e \cdots\cdots exe \cdots e \in N_1 \cdots N_k,$$

wobei x einmal an der i-ten und einmal an der j-ten Stelle steht. Aus der Eindeutigkeit der Darstellung folgt $x = e$.
(ii) Folgt aus (i) und Lemma 95.

Satz 97: Es sei G eine Gruppe und $G_i \leq G$ für $1 \leq i \leq k$. Dann sind äquivalent:

(i) $G_i \trianglelefteq G$ für $1 \leq i \leq k$ und G ist inneres direktes Produkt von $G_1, \dots, G_k$,

(ii) Die folgenden drei Bedingungen sind erfüllt:

1) $G = G_1 \cdots G_k$,

2) $\forall i, j \in \{1, \dots, k\},\ i \neq j\ \ \forall a \in G_i\ \forall b \in G_j : ab = ba$,

3) $G_i \cap (G_1 \cdots G_{i-1} G_{i+1} \cdots G_k) = \{e\}\ \forall i \in \{1, \dots, k\}$.

Beweis: (i) $\Rightarrow$ (ii) Bedingung 1) ist nach Definition des inneren direkten Produkts und Bedingung 2) nach Lemma 96 (ii) erfüllt. Es sei nun $x \in G_i \cap (G_1 \cdots G_{i-1} G_{i+1} \cdots G_k)$. Dann ist $x \in G_i$ und

$$\exists a_1 \in G_1 \dots \exists a_{i-1} \in G_{i-1}\, \exists a_{i+1} \in G_{i+1} \dots \exists a_k \in G_k : x = a_1 \cdots a_{i-1} a_{i+1} \cdots a_k.$$

D.h. x besitzt die beiden Darstellungen

$$x = e \cdots e x e \cdots e = a_1 \cdots a_{i-1} e a_{i+1} \cdots a_k,$$

wobei x im ersten Produkt an der i-ten Stelle steht. Aus der Eindeutigkeit der Darstellung folgt $x = e$.

(ii) $\Rightarrow$ (i) Wir zeigen zunächst $G_i \trianglelefteq G$ (für $1 \leq i \leq k$). Es sei $a \in G$ und $b \in G_i$. Dann ist $a = a_1 \cdots a_k$ für gewisse $a_i \in G_i$. Wegen Bedingung 2) kommutiert b mit jedem der Elemente $a_k, \dots, a_{i+1}$ und daher (mit Induktion nach $k - i$)

$$\begin{aligned} aba^{-1} &= a_1 \cdots a_k b a_k^{-1} \cdots a_1^{-1} = a_1 \cdots a_{k-1} b a_k a_k^{-1} \cdots a_1^{-1} \\ &= a_1 \cdots a_{k-1} b a_{k-1}^{-1} \cdots a_1^{-1} = \cdots = a_1 \cdots a_i b a_i^{-1} \cdots a_1^{-1} \end{aligned}$$

Wieder wegen Bedingung 2) kommutiert $a_i b a_i^{-1} \in G_i$ mit jedem der Elemente $a_{i-1}, \dots, a_1$ und daher (mit Induktion nach i)

$$\begin{aligned} aba^{-1} &= a_1 \cdots a_{i-1} \big(a_i b a_i^{-1}\big) a_{i-1}^{-1} \cdots a_1^{-1} = a_1 \cdots a_{i-2} \big(a_i b a_i^{-1}\big) a_{i-1} a_{i-1}^{-1} \cdots a_1^{-1} \\ &= a_1 \cdots a_{i-2} \big(a_i b a_i^{-1}\big) a_{i-2}^{-1} \cdots a_1^{-1} = \cdots = a_i b a_i^{-1} \in G_i. \end{aligned}$$

Zu zeigen bleibt die Eindeutigkeit der Produktdarstellung aus Bedingung 1). Angenommen $e = a_1 \cdots a_k$ mit $a_i \in G_i$ für $1 \leq i \leq k$. Mit Hilfe von Bedingung 2) erhält man

$$(a_1 \cdots a_{i-1} a_{i+1} \cdots a_k) a_i = e$$

und daher

$$a_i^{-1} = a_1 \cdots a_{i-1} a_{i+1} \cdots a_k \in G_i \cap (G_1 \cdots G_{i-1} G_{i+1} \cdots G_k) = \{e\},$$

d.h. $a_i = e$ (für $1 \leq i \leq k$). Ist nun $a_1 \cdots a_k = b_1 \cdots b_k$ mit $a_i, b_i \in G_i$ für $1 \leq i \leq k$, so folgt wieder mit Hilfe von Bedingung 2)

$$\big(a_1 b_1^{-1}\big) \cdots \big(a_k b_k^{-1}\big) = e.$$

Da $a_i b_i^{-1} \in G_i$ für $1 \leq i \leq k$ folgt aus dem eben gezeigten Spezialfall $a_i b_i^{-1} = e$ und somit $a_i = b_i$ für $1 \leq i \leq k$.

Korollar 98: Es sei G eine Gruppe und $N_i \trianglelefteq G$ für $1 \leq i \leq k$. Dann sind äquivalent:

(i) G ist inneres direktes Produkt von $N_1, \dots, N_k$,

(ii) Die folgenden beiden Bedingungen sind erfüllt:
1) $G = N_1 \cdots N_k$,
2) $N_i \cap (N_1 \cdots N_{i-1} N_{i+1} \cdots N_k) = \{e\}$ für $1 \leq i \leq k$,

(iii) Die folgenden beiden Bedingungen sind erfüllt:
1) $G = \langle N_1 \cup \cdots \cup N_k \rangle$,
2) $N_i \cap \langle N_1 \cup \cdots \cup N_{i-1} \cup N_{i+1} \cup \cdots \cup N_k \rangle = \{e\}$ für $1 \leq i \leq k$.

Beweis: (i) $\Rightarrow$ (ii) Folgt aus Satz 97 (i) $\Rightarrow$ (ii).
(ii) $\Rightarrow$ (i) Aus Bedingung 2) folgt insbesondere $N_i \cap N_j = \{e\}$ für $1 \leq i, j \leq k$, $i \neq j$. Daher ist wegen Lemma 95 Bedingung 2) von Satz 97 erfüllt und die Behauptung folgt aus Satz 97 (ii) $\Rightarrow$ (i).
(ii) $\Leftrightarrow$ (iii) Folgt aus Lemma 94.

Korollar 99: Es sei G eine Gruppe und $N_i \trianglelefteq G$ für $1 \leq i \leq k$. Ist G inneres direktes Produkt von $N_1, \dots, N_k$, so ist $G \cong N_1 \times \cdots \times N_k$.

Beweis: Betrachte die Abbildung $\varphi : N_1 \times \cdots \times N_k \to G$, $\varphi(a_1, \dots, a_k) = a_1 \cdots a_k$. Sie ist ein Homomorphismus, da

$$\varphi(a_1 b_1, \dots, a_k b_k) = (a_1 b_1) \cdots (a_k b_k) = (a_1 \cdots a_k)(b_1 \cdots b_k) = \varphi(a_1, \dots, a_k)\varphi(b_1, \dots, b_k),$$

wobei bei der zweiten Gleichung verwendet wurde, dass $a_i b_j = b_j a_i$ für $1 \leq i, j \leq k$, $i \neq j$ wegen Lemma 96 (ii). Die Abbildung φ ist surjektiv weil $G = N_1 \cdots N_k$ und injektiv wegen der Eindeutigkeit der Produktdarstellung (d.h. Bedingung 2) in der Definition des inneren direkten Produkts).

Korollar 100: Es sei G eine endliche Gruppe und $N_i \trianglelefteq G$ für $1 \leq i \leq k$. Ist G inneres direktes Produkt von $N_1, \dots, N_k$, so gilt

$$|G| = \prod_{i=1}^{k} |N_i|.$$

Beweis: Folgt aus Korollar 99.

Beispiel: Es sei G die folgende Untergruppe der S_4:

$$G = \big\{\varepsilon, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\big\}$$

(Es ist $G \leq S_4$. Ist $G = \{\varepsilon, \alpha, \beta, \gamma\}$, so gilt $\alpha \circ \beta = \gamma \in G$ und $\alpha^{-1} = \alpha \in G\ \forall \alpha \in G$.) Bezeichnet $G_1 = \big\{\varepsilon, (1\ 2)(3\ 4)\big\}$ und $G_2 = \big\{\varepsilon, (1\ 3)(2\ 4)\big\}$, so erfüllen G_1 und G_2 alle Bedingungen von Satz 97 (ii) und G ist daher inneres direktes Produkt von G_1 und G_2. Insbesondere ist $G \cong G_1 \times G_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Satz 101: Es seien $m, n \in \mathbb{N} \setminus \{0, 1\}$ und $\mathrm{ggT}(m, n) = 1$. Dann ist $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

Beweis: Es sei $\varphi : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $\varphi(a) = (a + m\mathbb{Z}, a + n\mathbb{Z})$. Diese Abbildung ist ein Homomorphismus, denn

$$\begin{aligned}\varphi(a+b) &= (a+b+m\mathbb{Z}, a+b+n\mathbb{Z}) \\ &= (a+m\mathbb{Z}, a+n\mathbb{Z}) + (b+m\mathbb{Z}, b+n\mathbb{Z}) = \varphi(a) + \varphi(b).\end{aligned}$$

Aus dem chinesischen Restsatz aus der Zahlentheorie folgt

$$\forall a_1, a_2 \in \mathbb{Z}\ \exists x \in \mathbb{Z} : x \equiv a_1 \pmod{m} \text{ und } x \equiv a_2 \pmod{n}.$$

D.h. $x + m\mathbb{Z} = a_1 + m\mathbb{Z}$ und $x + n\mathbb{Z} = a_2 + n\mathbb{Z}$ und daher

$$\varphi(x) = (x + m\mathbb{Z}, x + n\mathbb{Z}) = (a_1 + m\mathbb{Z}, a_2 + n\mathbb{Z}).$$

Also handelt es sich bei φ um einen Epimorphismus. Schließlich ist $\ker \varphi = mn\mathbb{Z}$, denn

$$\begin{aligned}a \in \ker\varphi &\Leftrightarrow a + m\mathbb{Z} = m\mathbb{Z} \wedge a + n\mathbb{Z} = n\mathbb{Z} \Leftrightarrow a \in m\mathbb{Z} \wedge a \in n\mathbb{Z} \\ &\Leftrightarrow m \mid a \wedge n \mid a \Leftrightarrow \mathrm{kgV}(m, n) \mid a \Leftrightarrow (mn) \mid a \Leftrightarrow a \in mn\mathbb{Z},\end{aligned}$$

wobei in der zweiten Zeile wieder Resultate aus der Zahlentheorie verwendet wurden. Aus dem Homomorphiesatz (Korollar 28) folgt nun

$$\mathbb{Z}_{mn} = \mathbb{Z}/mn\mathbb{Z} = \mathbb{Z}/\ker\varphi \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

Korollar 102: Besitzt $m \in \mathbb{N} \setminus \{0, 1\}$ die Primfaktorzerlegung $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ (d.h. $p_1, \ldots, p_k$ sind paarweise verschiedene Primzahlen und $\alpha_1, \ldots, \alpha_k \in \mathbb{N} \setminus \{0\}$), so gilt

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}.$$

Beweis: Folgt aus Satz 101 mit Induktion nach k.

Satz 103: Es sei G eine endlich erzeugte abelsche Gruppe. Dann ist G das innere direkte Produkt (endlich vieler) zyklischer Gruppen. Insbesonder gibt es (nicht notwendig verschiedene) $s \geq 0$ Primzahlpotenzen $p_1^{\alpha_1}, \ldots, p_s^{\alpha_s}$ und $r \geq 0$, derart dass

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}} \times \mathbb{Z}^r.$$

Beweis: Es bezeichne n die minimale Zahl von Elementen eines Erzeugendensystems von G. (D.h. $\exists a_1, \ldots, a_n \in G : G = \langle a_1, \ldots, a_n\rangle$ aber $\langle x_1, \ldots, x_k\rangle \subsetneq G$ für $x_1, \ldots, x_k \in G$ mit $k < n$.) Wir führen den Beweis mit Induktion nach n. Für $n = 1$ gibt es ein $a_1 \in G$ mit der Eigenschaft $G = \langle a_1\rangle$ und G ist daher zyklisch. Es sei nun $n > 1$ und die Behauptung für abelsche Gruppen mit Erzeugendensystemen mit weniger als n Elementen bereits gezeigt.

1. Fall: Es gibt ein Erzeugendensystem $a_1, \dots, a_n \in G$ mit der Eigeschaft, dass die Gleichung $a_1^{\alpha_1} \cdots a_n^{\alpha_n} = e$ nur für $\alpha_1 = \cdots = \alpha_n = 0$ gilt. D.h. es gilt

$$a_1^{\alpha_1} \cdots a_n^{\alpha_n} \neq e \quad \forall (\alpha_1, \dots, \alpha_k) \in \mathbb{Z}^k \setminus \{(0, \dots, 0)\}.$$

Für $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \mathbb{Z}$ gilt dann $a_1^{\alpha_1} \cdots a_n^{\alpha_n} = a_1^{\beta_1} \cdots a_n^{\beta_n} \Rightarrow a_1^{\alpha_1 - \beta_1} \cdots a_n^{\alpha_n - \beta_n} = e$ $\Rightarrow \alpha_1 - \beta_1 = \cdots = \alpha_n - \beta_n = 0 \Rightarrow \alpha_i = \beta_i$ für $1 \leq i \leq n$ $(*)$. Setzt man $N_i := \langle a_i \rangle$ für $1 \leq i \leq n$, so ist N_i Normalteiler von G, da G abelsch ist und G ist inneres direktes Produkt der zyklischen Gruppen $N_1, \dots, N_n$. Aus $G = \langle a_1, \dots, a_n \rangle$ folgt nämlich

$$\forall x \in G \; \exists \alpha_1, \dots, \alpha_n \in \mathbb{Z} : x = a_1^{\alpha_1} \cdots a_n^{\alpha_n} \in N_1 \cdots N_n,$$

d.h. $G = N_1 \cdots N_n$ und die Eindeutigkeit der Darstellung folgt aus $(*)$.

2. Fall: Ist $a_1, \dots, a_n \in G$ ein Erzeugendensystem von G, so

$$\exists (\alpha_1, \dots, \alpha_k) \in \mathbb{Z}^k \setminus \{(0, \dots, 0)\} : a_1^{\alpha_1} \cdots a_n^{\alpha_n} = e.$$

Da dann auch $a_1^{-\alpha_1} \cdots a_n^{-\alpha_n} = e$, kann man o.B.d.A. voraussetzen, dass $\alpha_1, \dots, \alpha_n$ mindestens eine positive Zahl enthält. O.B.d.A. sei $\alpha_1 > 0$ minimal mit dieser Eigenschaft. (D.h. $\alpha_1 > 0$ ist minimal, wenn man $a_1, \dots, a_n$ über alle Erzeugendensysteme von G mit n Elementen und $\alpha_1, \dots, \alpha_n$ über alle ganzen Zahlen mit $a_1^{\alpha_1} \cdots a_n^{\alpha_n} = e$ variieren lässt.) Wir behaupten nun, dass $\alpha_1 \mid \alpha_i$ für $2 \leq i \leq n$. Wir dividieren $\alpha_2, \dots, \alpha_n$ mit Rest durch α_1, genauer sei $\alpha_i = \beta_i \alpha_1 + \rho_i$ mit $0 \leq \rho_i < \alpha_1$ für $2 \leq i \leq n$. Dann gilt

$$\left(a_1 a_i^{\beta_i}\right)^{\alpha_1} a_2^{\alpha_2} \cdots a_{i-1}^{\alpha_{i-1}} a_i^{\rho_i} a_{i+1}^{\alpha_{i+1}} \cdots a_n^{\alpha_n} = a_1^{\alpha_1} \cdots a_n^{\alpha_n} = e. \quad (**)$$

Nun ist $a_1 a_i^{\beta_i}, a_2, \dots, a_n$ ebenfalls ein Erzeugendensystem von G, da

$$a_1^{k_1} \cdots a_n^{k_n} = \left(a_1 a_i^{\beta_i}\right)^{k_1} a_2^{k_2} \cdots a_{i-1}^{k_{i-1}} a_i^{k_i - \beta_i k_1} a_{i+1}^{k_{i+1}} \cdots a_n^{k_n} \quad \forall k_1, \dots, k_n \in \mathbb{Z}.$$

Wäre $\rho_i \neq 0$, so wäre $0 < \rho_i < \alpha_1$ und $(**)$ würde der Minimalität von α_1 widersprechen. Also ist $\rho_i = 0$ und daher $\alpha_1 \mid \alpha_i$, genauer $\alpha_i = \beta_i \alpha_1$ (für $2 \leq i \leq n$). Bezeichnet $a := a_1 a_2^{\beta_2} \cdots a_n^{\beta_n}$, so gilt

$$a^{\alpha_1} = a_1^{\alpha_1} a_2^{\beta_2 \alpha_1} \cdots a_n^{\beta_n \alpha_1} = a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_n^{\alpha_n} = e.$$

Auch $a, a_2, \dots, a_n$ ist ein Erzeugendensystem von G, da

$$a_1^{k_1} \cdots a_n^{k_n} = \left(a_1 a_2^{\beta_2} \cdots a_n^{\beta_n}\right)^{k_1} a_2^{k_2 - k_1 \beta_2} \cdots a_n^{k_n - k_1 \beta_n} = a^{k_1} a_2^{k_2 - k_1 \beta_2} \cdots a_n^{k_n - k_1 \beta_n} \quad (***)$$

für alle $k_1, \dots, k_n \in \mathbb{Z}$. Es seien $A := \langle a \rangle$ und $B = \langle a_2, \dots, a_n \rangle$. Da G abelsch ist, sind A und B Normalteiler von G und aus $(***)$ folgt $G = A \cdot B$. Wir zeigen nun $A \cap B = \{e\}$. Angenommen, $x \in A \cap B$. Dann gibt es $\gamma, \gamma_2, \dots, \gamma_n \in \mathbb{Z}$, derart dass $x = a^\gamma = a_2^{\gamma_2} \cdots a_n^{\gamma_n}$. Wegen $a^{\alpha_1} = e$ kann man dabei $0 \leq \gamma < \operatorname{ord}(a) \leq \alpha_1$ verlangen. Nun ist

$$e = x \cdot x^{-1} = a^\gamma a_2^{-\gamma_2} \cdots a_n^{-\gamma_n} = \left(a_1 a_2^{\beta_2} \cdots a_n^{\beta_n}\right)^\gamma a_2^{-\gamma_2} \cdots a_n^{-\gamma_n} = a_1^\gamma a_2^{\gamma \beta_2 - \gamma_2} \cdots a_n^{\gamma \beta_n - \gamma_n}.$$

Wäre $\gamma > 0$, so würde diese Beziehung der Minimalität von α_1 widersprechen. Also ist $\gamma = 0$ und daher $x = e$.

Aus Satz 97 folgt, dass G inneres direktes Produkt von A und B ist. Dabei ist A eine (endliche) zyklische Gruppe und B wird von weniger als n Elementen erzeugt. Nach IV ist B inneres direktes Produkt (endlich vieler) zyklischer Gruppen, woraus die Behauptung folgt. Der Zusatz folgt aus Korollar 99, Satz 36 und Korollar 102.

Bemerkung: Man kann zeigen, dass die Größen r, s und $p_1^{\alpha_1}, \dots, p_s^{\alpha_s}$ eindeutig bestimmt sind.

Lemma 104: Es sei G eine endliche zyklische Gruppe und $n \in \mathbb{N}$ habe die Eigenschaft $n \,\big|\, |G|$. Dann gibt es eine Untergruppe $H \leq G$ mit der Eigenschaft $|H| = n$.

Beweis: Es sei $|G| = m$ und $G = \langle a \rangle$, d.h. $G = \{e, a, \dots, a^{m-1}\}$. Bezeichnet $H := \langle a^{m/n} \rangle$, so ist $H \leq G$ und

$$|H| = \operatorname{ord}\left(a^{m/n}\right) \overset{\text{Satz 15 (v)}}{=} \frac{m}{\operatorname{ggT}\left(m, \frac{m}{n}\right)} = \frac{m}{m/n} = n.$$

Satz 105: Es sei G eine endliche abelsche Gruppe und $n \in \mathbb{N}$ habe die Eigenschaft $n \,\big|\, |G|$. Dann gibt es eine Untergruppe $H \leq G$ mit der Eigenschaft $|H| = n$.

Beweis: Nach Satz 103 gibt es Primzahlpotenzen $p_1^{\alpha_1}, \dots, p_s^{\alpha_s}$ (die nicht notwendig verschieden sein müssen), derart dass $G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$. Man kann nun leicht zeigen, dass es $n_1, \dots, n_s \in \mathbb{N} \setminus \{0\}$ mit den Eigenschaften $n = n_1 \cdots n_s$ und $n_i \mid p_i^{\alpha_i}$ (für $1 \leq i \leq s$) geben muss. (Man beachte dabei, dass es sich bei $|G| = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ nicht unbedingt um die Primfaktorzerlegung von $|G|$ handeln muss!) Nach Lemma 104 gibt es für jedes $i \in \{1, \dots, s\}$ eine Untergruppe $H_i \leq \mathbb{Z}_{p_i^{\alpha_i}}$ mit der Ordnung $|H_i| = n_i$. Dann ist offensichtlich $H_1 \times \cdots \times H_s \leq \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$. Bezeichnet $\varphi : \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}} \to G$ einen Isomorphismus, so sei $H := \varphi(H_1 \times \cdots \times H_s)$. Dann ist $H \leq G$ nach Lemma 25 (i) und

$$|H| = |H_1 \times \cdots \times H_s| = |H_1| \cdots |H_s| = n_1 \cdots n_s = n.$$

Bemerkungen: 1) Man kann Satz 105 als Umkehrung von Korollar 19 (ii) (Satz von Lagrange) für (endliche) abelsche Gruppen auffassen.
2) Für nichtabelsche Gruppen ist Satz 105 falsch. Man kann z.B. zeigen, dass die alternierende Gruppe A_5 (mit Ordnung $|A_5| = 5!/2 = 60$) keine Untergruppe der Ordnung 15 besitzt.