5. Endlich erzeugte abelsche Gruppen

Erinnerung: • Eine Gruppe G heißt endlich erzeugt wenn es eine endliche Teilmenge $S = \{x_1, \dots, x_n\} \subseteq G$ gibt mit $G = \langle S \rangle = \langle x_1, \dots, x_n \rangle$.

• Ist $G = \langle x \rangle$ für ein $x \in G$, so nennen wir G zyklisch (für $\operatorname{ord}(x)$ endlich) bzw. ∞-zyklisch (für $\operatorname{ord}(x)$ unendlich).

Bem. • Ist G zyklisch und $|G| = n$, so ist $G \cong C_n$.

• Ist G ∞-zyklisch, so ist $G \cong (\mathbb{Z}, +)$.

• Endliche Gruppen sind immer endlich erzeugt, denn $G = \langle G \rangle$.

Faktum 5.1 Ist G endl. erzeugt, so existiert eine kleinste positive Zahl $r \in \mathbb{N}$ mit $G = \langle x_1, \dots, x_r \rangle$ für $x_i \in G$, und für alle $S \subseteq G$ mit $|S| < r$ gilt $\langle S \rangle \neq G$.

Beweis: Folgt aus der Tatsache, dass jede nicht-leere Teilmenge nat. Zahlen ein kl. Element besitzt. ⊣

Def. Ist $G = \langle x_1, \dots, x_r \rangle$ mit r minimal, so heißen $x_1, \dots, x_r$ Generatoren von G. [Manchmal wird die Minimalität weggelassen; eigentlich Basis] [analog: Erzeugendensystem vs. Basis]

Faktum 5.2 Sind $x_1, \dots, x_r$ Generatoren einer abelschen Gruppe G, so lässt sich jedes $x \in G$ schreiben als

$$x = \prod_{i=1}^{r} x_i^{n_i} = x_1^{n_1} \cdot \dots \cdot x_r^{n_r} \quad \text{mit } n_i \in \mathbb{Z} \text{ für } 1 \leq i \leq r.$$

Beweis: Folgt direkt aus der Definition von "endl. Erzeugt". ⊣

Folgerung: Ist G eine endl. erzeugte abelsche Gruppe und sind $x_1, \dots, x_r$ Generatoren von G, so ist

$$G = \left\{ \prod_{i=1}^{r} x_i^{n_i} : (n_1, \dots, n_r) \in \mathbb{Z}^r \right\}.$$

Lemma 5.3 Sei H eine endl. erzeugte abelsche Gruppe und $x_1, \dots, x_s$ Generatoren von H (für $s \geq 1$). Seien weiter $m_1, \dots, m_s \in \mathbb{N}$, nicht alle 0, mit $\underbrace{(m_1, \dots, m_s)}_{:= ggT(m_1, \dots, m_s)} = 1$.

Dann ex. Generatoren $y_1, \dots, y_s$ von H mit

$$y_1 = x_1^{m_1} \cdot \dots \cdot x_s^{m_s}.$$

Beweis: Sei $m := \sum_{i=1}^{s} m_i$, dann ist $m > 0$ (nach Voraussetzung). Der Beweis ist nun mit Induktion nach m.

- Ist $m = 1$, so ist $m_{i_0} = 1$ für genau ein i_0 (für alle anderen i's ist $m_i = 0$). Nach umnummerieren dürfen wir annehmen $i_0 = 1$. Setzen wir $y_i = x_i$ (für $1 \leq i \leq r$) so sind wir fertig.

- Sei nun $m > 1$ und sei der Satz bewiesen für alle m' mit $1 \leq m' < m$.
  Weil $(m_1, \dots, m_s) = 1$ ist $m_i \neq 0$ für mindestens zwei i. Nach umnummerieren dürfen wir annehmen $m_1 \geq m_2 > 0$. Dann sind $m_1 - m_2, m_2, \dots, m_s \in \mathbb{N}$ nicht alle 0 und $(m_1 - m_2, m_2, \dots, m_s) = 1$ (beachte dass gilt $(k \mid m_2 \wedge k \mid m_1 - m_2) \rightarrow k \mid m_1$).
  Weiter sind $x_1, x_1 \cdot x_2, x_3, \dots, x_s$ Generatoren von H, denn es gilt: $x_2 = x_1^{-1}(x_1 \cdot x_2)$, also $x_2 \in \langle x_1, x_1 x_2, \dots \rangle$.

Nun ist $m_1 - m_2 + \sum_{i=2}^{s} m_i = m - m_2 < m$ (weil $m_2 > 0$)
und mit der Induktionsvoraussetzung ex. Generatoren
$y_1, \dots, y_s$ von H mit

$$y_1 = x_1^{m_1-m_2} \cdot (x_1 \cdot x_2)^{m_2} \cdot x_3^{m_3} \cdot \dots \cdot x_s^{m_s}$$
$$= x_1^{m_1} \cdot \underbrace{x_1^{-m_2} \cdot x_1^{m_2}}_{= e_H} \cdot x_2^{m_2} \cdot \dots \cdot x_s^{m_s} = x_1^{m_1} \cdot x_2^{m_2} \cdot \dots \cdot x_s^{m_s}$$

(H abelsch)

was zu zeigen war. ⊣

Theorem 5.4 (Hauptsatz über endl. erzeugte abelsche Gruppen)
Sei G eine endl. erzeugte abelsche Gruppe. Dann
ex. Generatoren $x_1, \dots, x_r$ von G, so dass gilt:

$$G \cong \langle x_1 \rangle \times \langle x_2 \rangle \times \dots \times \langle x_r \rangle$$

Bem. $G \cong$ "Produkt von zykl. Gruppen C_n und von ∞-zykl. Gruppen $\mathbb{Z}$"

Beweis:
- Ist $r = 1$, so ist $G = \langle x_1 \rangle$ und wir sind fertig.
- Für $r > 1$ betrachten wir die Menge $\mathcal{R}$ aller r-Tupel $(\tilde{x}_1, \dots, \tilde{x}_r) \in G^r$ für die gilt $\langle \tilde{x}_1, \dots, \tilde{x}_r \rangle = G$ und $\operatorname{ord}(\tilde{x}_1) \le \operatorname{ord}(\tilde{x}_2) \le \dots \le \operatorname{ord}(\tilde{x}_r)$ wobei $n < \infty = \infty$ (für $n \in \mathbb{N}$). Es ist $\mathcal{R} \neq \emptyset$ (unmum.).

Sei $N_1 := \min \{ \operatorname{ord}(x_1) : x_1 \in G \wedge \exists (\tilde{x}_2, \dots, \tilde{x}_r) \in G^{r-1} ((x_1, \tilde{x}_2, \dots, \tilde{x}_r) \in \mathcal{R}) \}$

$N_2 := \min \{ \operatorname{ord}(x_2) : x_2 \in G \wedge \exists x_1 \in G (\operatorname{ord}(x_1) = N_1) \wedge \exists (\tilde{x}_3, \dots, \tilde{x}_r) \in G^{r-2} ((x_1, x_2, \tilde{x}_3, \dots, \tilde{x}_r) \in \mathcal{R}) \}$

$N_3 := \min \{ \operatorname{ord}(x_3) : x_3 \in G \wedge \exists x_1, x_2 \in G (\operatorname{ord}(x_1) = N_1 \wedge \dots$

Dann ist $0 < N_1 \le N_2 \le \dots \le N_r$ und für alle $(\tilde{x}_1, \dots, \tilde{x}_r) \in \mathcal{R}$ gilt: Ist $0 < j_0 \le r$ und für alle $0 < i < j_0$ gilt $\operatorname{ord}(\tilde{x}_i) = N_i$, dann ist $\operatorname{ord}(\tilde{x}_{j_0}) \ge N_{j_0}$. (*)
[folgt aus der Def. der N_i's]

Wir wählen nun $(x_1, \dots, x_r) \in R$ so, dass $\operatorname{ord}(x_i) = N_i$ für alle $1 \le i \le r$.

Wir wissen bereits $G = \left\{ \prod_{i=1}^{r} x_i^{n_i} : (n_1, \dots, n_r) \in \mathbb{Z}^r \right\}$

und zeigen nun $G \cong \prod_{i=1}^{r} \langle x_i \rangle \cong \prod_{i=1}^{r} C_{N_i}$. [Eindeutigkeit]

[Was ist der Unterschied? Vergleich Basen / Erzeugendensystem]

Dafür zeigen wir, dass aus $\prod_{i=1}^{r} x_i^{n_i} = 1$ (für $n_i \in \mathbb{Z}$) folgt:

$$N_i \mid n_i \quad \text{für} \quad N_i < \infty$$
$$n_i = 0 \quad \text{für} \quad N_i = \infty$$

D.h. das Produkt ist trivial. [Vergleich mit Basen in Vektorräumen]

Für einen Widerspruch nehmen wir an, es ex. $n_1, \dots, n_r$ mit

- $\prod_{i=1}^{r} x_i^{n_i} = 1$
- n_i nicht alle 0
- $n_i \ge 0$ (ersetze x_i durch x_i^{-1} falls $n_i < 0$ [und n_i durch $-n_i$])
- $0 \le n_i < N_i$

Sei weiter $d := (n_1, \dots, n_r) > 0$ und für $1 \le i \le r$ sei $m_i := \frac{n_i}{d}$.
Dann sind $m_1, \dots, m_r \in \mathbb{N}$ und $(m_1, \dots, m_r) = 1$.

Sei $1 \le j_0 \le r$ die kleinste Zahl mit $n_{j_0} \neq 0$ (d.h. $i < j_0 \to n_i = 0$).
Dann ist $m_{j_0} \neq 0$ und für $i < j_0$ ist $m_i = 0$. Somit ist

$$(m_{j_0}, m_{j_0+1}, \dots, m_r) = 1.$$

Sei $H := \langle x_{j_0}, \dots, x_r \rangle \le G$. Dann ex. mit Lem. 5.3 Generatoren $y_{j_0}, y_{j_0+1}, \dots, y_r$ von H mit $y_{j_0} = \prod_{i=j_0}^{r} x_i^{m_i}$.

Somit gilt $y_{j_0}^d = \prod_{i=j_0}^{r} x_i^{n_i}$ (weil $d \cdot m_i = n_i$ und H abelsch)

$= \prod_{i=1}^{r} x_i^{n_i}$ (weil $n_i = 0$ für $i < j_0$)

$= 1$ (nach unserer Annahme)

- Da $y_{j_0}, \dots, y_r$ Generatoren von H sind ist $y_{j_0} \neq 1$, denn sonst könnte y_{j_0} weggelassen werden.
- Da $d \mid n_{j_0}$ und $0 < n_{j_0}$ ist $d \leq n_{j_0}$ und weil $n_{j_0} < N_{j_0}$ ist $d < N_{j_0}$.
- Da $y_{j_0}^d = 1$ und $d > 0$ ist $\operatorname{ord}(y_{j_0}) \leq d$.

Wir erhalten somit

ord: N_1 N_{j_0-1} $< N_{j_0}$

$$G = \langle x_1, \dots, x_{j_0-1}, \underbrace{y_{j_0}, y_{j_0+1}, \dots, y_r}_{\text{Generatoren von } H} \rangle$$

mit $\operatorname{ord}(y_{j_0}) \leq d \leq n_{j_0} < N_{j_0} = \operatorname{ord}(x_{j_0})$ und $\operatorname{ord}(x_i) = N_i$ für alle $1 \leq i < j_0$. Das Widerspricht aber der Wahl von $x_1, \dots, x_r$ und somit gilt: $G \cong \prod_{i=1}^{r} \langle x_i \rangle$

(denn es gilt (*))

⊣

Korollar 5.5 Ist G eine endl. erzeugte abelsche Gruppe, so ist

$$G \cong C_{n_1} \times C_{n_2} \times \dots \times C_{n_s} \times \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_{\cong \mathbb{Z}^r \text{ (für } r \in \mathbb{N})}$$

mit $n_1 \mid n_2$, $n_2 \mid n_3$, $\dots$, $n_i \mid n_{i+1}, \dots$

Def. $C_{n_1} \times \dots \times C_{n_s}$ heißt Torsionsgruppe (von G) und r ist der Rang von G.

Beweis von Korollar 5.5 Mit Thm. 5.4 erhalten wir

[Algorithmus] $G \cong C_{m_1} \times \cdots \times C_{m_t} \times \mathbb{Z}^r$

mit $m_1 \mid \cdots \mid m_t$ (und $r \in \mathbb{N}$). Mit Aufgabe 8 ist

für $m, n \geq 1$: $C_m \times C_n \cong C_{n \cdot m} \iff \operatorname{ggT}(m,n) = 1$.

(insbesondere $C_n \cong C_{p_1^{k_1}} \times \cdots \times C_{p_s^{k_s}}$ für p_i prim und paarweise teilerfremd)

Daraus folgt direkt der folgende Algorithmus zur Berechnung der n_i's aus den m_j's:

- Für jede Primzahl p mit $p \mid \prod_{j=1}^{t} m_j$ schreiben wir in absteigender Reihenfolge die maximalen Potenzen p^k von p auf, welche jeweils m_j teilt (d.h. $p^k \mid m_j \wedge p^{k+1} \nmid m_j$).
- Die Produkte der Spalten (von rechts nach links) geben uns dann die n_i's. ⊣

Beispiel: $C_{12} \times C_9 \times C_{15} \times C_{15} \times C_{14}$

$C_4 \times C_3 \times C_9 \times C_3 \times C_5 \times C_3 \times C_5 \times C_2 \times C_7$

Primzahlen	Primzahlpotenzen welche 12, 9, ... teilen; absteigend				
2	4	2	1	1	1
3	9	3	3	3	1
5	5	5	1	1	1
7	7	1	1	1	1
Produkte der Spalten:	1260	30	3	3	1

Somit gilt: $C_{12} \times C_9 \times C_{15} \times C_{15} \times C_{14} \cong C_3 \times C_3 \times C_{30} \times C_{1260}$

Folgerungen:

- Sind $p_1, \ldots, p_s$ paarweise versch. Primzahlen, so gibt es (bis auf Isom.) nur eine abelsche Gruppe der Ordnung $\prod_{j=1}^{s} p_j$.
- Ist p prim, so gibt es (bis auf Isom.) nur zwei abelsche Gruppen der Ordnung p^2, nämlich $C_p \times C_p$ und C_{p^2}.
- Ist p prim, so gibt es (bis auf Isom.) $P(n)$ abelsche Gruppen der Ordnung p^n, wobei $P(n)$ die "Partitionsfunktion" bezeichnet.