§3 Abelsche Gruppen, symmetrische Gruppen, einfache Gruppen

Wir klassifizieren jetzt die endlichen abelschen Gruppen.

1. **Lemma 1** Sei G eine abelsche p-Gruppe.

Falls G genau eine Untergruppe $H \subseteq G$ der Ordnung p hat, so ist G zyklisch.

Beweis: Sei $|G| = p^m$, $m \geq 1$. Induktion nach m.

$m = 1$: ok fertig mit §1.16.

$m \geq 2$: Betrachte $f: G \to G$, $g \mapsto g^p$.

Da G abelsch ist, ist f ein Homomorphismus, denn $(gh)^p = g^p h^p$ gilt dann. Es ist $\ker(f) = \{ g \in G \mid g^p = e \} = \{ g \in G \mid o(g) = 1, p \}$. Ist $o(g) = p$, so ist $g \in H$ mit $|\langle g \rangle| = p$. Also $H = \ker(f)$.

Sei $K = f(G)$ so $K \cong G/H$ nach Homomorphiesatz, $|K| = p^{m-1}$. Nach Cauchys Satz gibt es ein $k \in K$ mit $o(k) = p$. Daher $H \subseteq K$.

Damit hat K genau eine Untergruppe der Ordnung p, ist also nach Induktionsannahme zyklisch, $K = \langle \tilde{k} \rangle$ für ein $\tilde{k} \in K$. Wähle $g \in G$ mit $g^p = \tilde{k}$. Schon $o(g) = p \cdot r$

$\Rightarrow o(g^r) = p \Rightarrow g^r \in H \Rightarrow H \leq \langle g \rangle$

(wegen Einfachheit) und $F(\langle g \rangle) = K \Rightarrow$

$\langle g \rangle / H \cong K \Rightarrow o(g) = |K| \cdot |H| = p^m$ □

$\Rightarrow \langle g \rangle = G$.

Lemma B Sei G zyklisch mit $|G| = k \cdot l$.
Dann hat G genau eine Untergruppe der Ordnung k.

Beweis Betrachte $f: G \to G$, $g \mapsto g^k$ mit
Kern $\ker(f) = \{ g \in G \mid g^k = e \}$.
Ist $H \leq G$ Untergruppe der Ordnung k, so folgt $H \leq \ker(f)$
(Lagrange). Schreibe $G = \langle u \rangle$, $o(u) = k \cdot l$. Dann
gilt $f(G) = \langle u^k \rangle$ und $o(u^k) = l$, insgesamt
also $\underbrace{|f(G)|}_{=l} \cdot \underbrace{|\ker(f)|}_{=k} = |G| = k \cdot l$ □

Lemma C Sei G eine endliche p-Gruppe,
sei $u \in G$ ein Element mit maximaler Ordnung,
sei $U = \langle u \rangle \leq G$. Dann gibt es eine Untergruppe
$H \leq G$ mit $H \cap U = \{e\}$ und $G = HU$,
insbesondere ist $G \cong H \times U$.

Beweis: Sei $|G| = p^m$. Induktion nach $m \geq 1$

$m = 1$: G ist zyklisch, also $G = \langle u \rangle$. Sei $H = \{e\}$
$\Rightarrow$ fertig.

$m \geq 2$: 1. Fall G zyklisch, $G = \langle u \rangle$. Sei wieder
$H = \{e\} \Rightarrow$ fertig

2. Fall: G nicht zyklisch. Nach Lemma D hat
U nur eine Untergruppe der Ordnung p. Da
G nicht zyklisch ist, gibt es nach Lemma A und
Cauchys Satz ein Element $w \in G$ mit $o(w) = p$
und $w \notin U$. Sei $W = \langle w \rangle \Rightarrow W \cap U = \{e\}$.

Betrachte $F: G \to G/W$ mit $\ker(F) = W$.
$g \mapsto gW$

Dann ist die Einschränkung $F|_U : U \to G/W$ injektiv
(wer $U \cap W = \{e\}$) $\Rightarrow$ $o(F(u)) = o(u)$.

Damit ist $f(u)$ ein Element maximaler Ordnung in $G/W = L$
und $|G/W| = p^{m-1}$. Nach Induktion annah gibt
es eine Untergruppe $\tilde{H} \subseteq L$ mit $\tilde{H} \cap f(U) = \{e_L\}$
und $\tilde{H} \cdot f(U) = L$. Betrachte $H = f^{-1}(\tilde{H}) \subseteq G$.

Beh: $H \cap U = \{e\}$. Denn: $h \in H \cap U$
$\Rightarrow f(h) \in f(U) \cap f(\tilde{H}) = \{e_L\} \Rightarrow h \in W$
$\Rightarrow h = e$, denn $W \cap U = \{e\}$.

Für $g \in G$ beliebig ist $f(g) = f(u^s) f(h)$

für ein $s \in \mathbb{N}$, $h \in H$ $\Rightarrow$ $g = \underbrace{u^s}_{\in U} \cdot \underbrace{h \cdot w}_{\in H}$ für

ein $w \in W \subseteq H$ $\Rightarrow$ $G = UH = HU$. □

Korollar Ist G eine abelsche p-Gruppe, so

gibt es eindeutig Zahlen $u_1 \geq u_2 \geq \dots \geq u_r \geq 1$

mit $n = u_1 + u_2 + \dots + u_r$, $|G| = p^n$ und

$$G \cong \mathbb{Z}/p^{u_1}\mathbb{Z} \times \mathbb{Z}/p^{u_2}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{u_r}\mathbb{Z}$$

Beweis Wähle $u_1 \in G$ mit maximaler Ordnung,

schreibe $p^{u_1} = o(u_1)$. Set $U_1 = \langle u_1 \rangle$

$\Rightarrow$ $U_1 \cong \mathbb{Z}/p^{u_1}\mathbb{Z}$. Mit Lemma G' gibt

$G = U_1 H_1$, $U_1 \cap H_1 = \{e\}$, $G \cong U_1 \times H_1$

Wähle jetzt $u_2 \in H_2$ mit maximaler Ordnung

$o(u_2) = p^{u_2}$ usw. Nach endlich vielen

Schritten $G = U_1 \cdots U_r$, $G \cong U_1 \times \dots \times U_r$

$U_k \cong \mathbb{Z}/p^{u_k}\mathbb{Z}$ und $u_1 \geq u_2 \geq \dots \geq u_r \geq 1$.

Zur Eindeutigkeit. Wir setzen $F_\ell(g) = g^{(p^\ell)}$, $\ell \geq 0$.

Dann ist $F_\ell(u_k) = \begin{cases} \{e\} & \text{für } \ell \geq u_k \\ \mathbb{Z}/p^{u_k-\ell}\mathbb{Z} & \text{für } \ell < u_k \end{cases}$

damit $|F_\ell(G)| = \prod_{u_k > \ell} p^{u_k-\ell} = p^{N_\ell}$ mit

$N_\ell = \sum_{u_k > \ell} (u_k - \ell) = \sum_{u_k \geq \ell} (u_k - \ell)$. Folglich

$N_\ell - N_{\ell+1} = \sum_{u_k \geq \ell} u_k - \sum_{u_k \geq \ell} \ell - \sum_{u_k > \ell} u_k + \sum_{u_k > \ell} (\ell+1)$

$= \underbrace{\sum_{u_k = \ell} u_k - \sum_{u_k = \ell} \ell}_{=0} + \sum_{u_k > \ell} 1$ und damit

$\underbrace{N_{\ell-1} - N_\ell - (N_\ell - N_{\ell+1})}_{N_{\ell-1} - 2N_\ell + N_{\ell+1}} = \sum_{u_k = \ell} 1 = |\{k \mid u_k = \ell\}|$ □

2. Theorem Die Klassifikation der endlich abelschen Gruppen

Sei G eine endlich abelsche Gruppe der Ordnung

$$|G| = p_1^{m_1} \cdots p_s^{m_s}, \quad p_1 < p_2 < \ldots < p_s \text{ Primzahl}$$
$$m_1, \ldots, m_s \geq 1$$

Dann gilt $G \cong G_1 \times \ldots \times G_s$

G_k Sylow-p_k-Gruppe in G und

$$G_k \cong \mathbb{Z}/p_k^{n_{k,1}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_k^{n_{k,r_k}}\mathbb{Z} \qquad n_{k,1} \geq \ldots \geq n_{k,r} \geq 1, \quad r_k \geq 1$$

Die Zahlen m_i, n_{ij} usw. sind eindeutig durch G bestimmt. r_k, s

Insbesondere: jede endliche abelsche Gruppe ist ein Produkt von zyklischen Gruppen.

Beweis Sei $G_i \leq G$ die Sylow-p_i-Gruppe.

Da G abelsch ist, gibt es für jedes p_i genau eine solche Gruppe ($\tau_a(g) = aga^{-1} = g$ für alle $a, g \in G$)

Nach dem vorigen Satz sind die G_i von der angegebenen Gestalt.

Wir setzen $\tilde{G} = G_1 \times \dots \times G_s$ und definieren

$f: \tilde{G} \to G$, $(g_1, \dots, g_s) \mapsto g_1 \cdots g_s \in G$. Da G abelsch ist, ist f ein Homomorphismus. Weil $|\tilde{G}| = |G|$, bleibt zu zeigen, dass f injektiv ist.

Sei $(g_1, \dots, g_s) \in \ker(f)$. Angenommen, $g_j \neq e$.

Setze $t = \frac{|G|}{|G_j|} = \prod_{i \neq j} p_i^{m_i} \Rightarrow g_j^t \neq e$, denn

$o(g_j)$ ist Vielfaches von p_j. Aber $g_i^t = e$ für alle $i \neq j$

$$\Rightarrow f(g_1, \dots, g_s)^t = e^t = e \quad \lightning$$

$$\text{"} \; g_j^t$$

Damit ist f injektiv, also ein Isomorphismus. □

Theorem 2 klärt vollständig, wie endliche abelsche Gruppen aussehen. Wir betrachten noch endlich erzeugte abelsche Gruppen.

3. Def Eine Gruppe G heißt endlich erzeugt, wenn es eine endliche Teilmenge $X \subseteq A$ gibt mit $\langle X \rangle = A$.

Bsp
- jede endliche Gruppe ist endlich erzeugt (setze $X = G$)
- $(\mathbb{Z}, +)$ ist endlich erzeugt, etwa $\langle 1 \rangle = \mathbb{Z}$.
- $(\mathbb{Q}, +)$ ist nicht endlich erzeugt. (ÜA)

4. Satz Sei $(A,+)$ endlich erzeugt mit m Erzeugern.

Dann wird auch jede Untergruppe $B \subseteq A$ von m Elementen erzeugt. Insbesondere: jede Untergruppe einer endlich erzeugten abelschen Gruppe ist wieder endlich erzeugt.

Beweis: Sei m die minimale Anzahl von Erzeugern.

Wir machen Induktion nach m. Für $m=0$ ist $A=\{0\}$ trivial. (V). OE $B \neq \{0\}$

$\underline{m=1}$: $A = \langle a \rangle$ zyklisch. Wähle $k>0$ minimal mit $k \cdot a \in B$ (wir schreiben A hier additiv!). Für $l \cdot a \in B$ beliebig schreibe $l = n \cdot k + r$, $0 \leq r < k$

$\Rightarrow ra = la - nka \in B \Rightarrow r = 0 \Rightarrow B = \langle ka \rangle$. □

$\underline{m \geq 2}$: $a_1, \dots, a_m$ Erzeugendensystem von A, m minimal. Sei $B_0 = B \cap \langle a_1 \rangle = \langle k a_1 \rangle$, $k \geq 0$. Sei $b_1 = k a_1 \in B_0$

Betrachte $f: A \to A/\langle a_1 \rangle = \tilde{A}$, $\tilde{A}$ erzeugt von $a_2 + \langle a_1 \rangle, \dots, a_m + \langle a_1 \rangle$, $f(B) = \tilde{B} \subseteq \tilde{A}$

$\Rightarrow \tilde{B}$ erzeugt von Elementen $\tilde{b}_2, \dots, \tilde{b}_n$, $n \leq m$. (nach Induktionsannahme). Wähle $b_j \in B$ mit $f(b_j) = \tilde{b}_j$, $j = 2, \dots, n$. Jedes $b \in B$ ist von der Form $b = \tilde{s}_1 a_1 + s_2 b_2 + \dots + s_n b_n$, $n \leq m$

Dabei ist $\tilde{s}_1 a_1 \in B \Rightarrow \tilde{s}_1 a_1 = s_1 b_1$ für ein $s_1 \in \mathbb{Z}$ □ #