§ 5. Endlich erzeugte abelsche Gruppen

Ziele:

- Jede endlich erzeugte abelsche Gruppe ist ein direktes Produkt zyklischer Gruppen, genauer:
- Jede endliche abelsche Gruppe hat bis auf Isomorphie die Form

  $$\mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$$

  mit $r \in \mathbb{N}_0$, $e_1, \ldots, e_r \in \mathbb{N}$ und Primzahlen $p_1, \ldots, p_r$.
- Jede endliche erzeugte abelsche Gruppe hat bis auf Isomorphie die Form

  $$\mathbb{Z}^s \times \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$$

  mit $r, s \in \mathbb{N}_0$, $e_1, \ldots, e_r \in \mathbb{N}$ und Primzahlen $p_1, \ldots, p_r$.

Definition der Torsionsuntergruppen

Definition (5.2)

Sei G eine abelsche Gruppe und $m \in \mathbb{N}$.

(i) Man nennt $G[m] = \{g \in G \mid mg = 0_G\}$ die *m-Torsionsuntergruppe* von G.

(ii) Die Teilmenge $\mathrm{Tor}(G) = \bigcup_{n \in \mathbb{N}} G[n]$ wird die *Torsionsuntergruppe* von G genannt.

Definition der Torsionsfreiheit

Definition (5.3)

Sei G eine endlich erzeugte abelsche Gruppe.

(i) Wir bezeichnen G als torsionsfrei, wenn $\mathrm{Tor}(G) = \{0_G\}$ gilt.

(ii) Die Gruppe G ist frei, wenn für ein $r \in \mathbb{N}_0$ ein Isomorphismus zwischen G und $(\mathbb{Z}^r, +)$ existiert, wobei $\mathbb{Z}^0 = \{0\}$ gesetzt wird.

Proposition (5.4)

(i) Jede Untergruppe einer freien endlich erzeugten abelschen Gruppe ist eine freie endlich erzeugte abelsche Gruppe.

(ii) Jede torsionsfreie endlich erzeugte abelsche Grupe ist frei.

Zerlegung in Torsionsanteil und freien Anteil

Satz (5.5)

Ist G eine endlich erzeugte abelsche Gruppe, dann gibt es ein $r \in \mathbb{N}_0$ mit $G \cong \mathbb{Z}^r \times \mathrm{Tor}(G)$. Darüber hinaus ist $\mathrm{Tor}(G)$ eine endliche abelsche Gruppe.

Beweisskizze zu Satz 5.5

- Zeige, dass die Faktorgruppe $G/\mathrm{Tor}(G)$ torsionsfrei und somit nach Proposition 5.4 (ii) isomorph zu $\mathbb{Z}^r$ ist, für ein $r \in \mathbb{N}_0$.
- Stelle G als inneres direktes Produkt von $\mathrm{Tor}(G)$ und einer Untergruppe U von G isomorph zu $\mathbb{Z}^r$ dar. (Die Untergruppe U wird erzeugt durch die Urbilder der Einheitsvektoren $e_1, ..., e_r \in \mathbb{Z}^r$ unter dem Homomorphismus $G \to \mathbb{Z}^r$, den man durch den Isomorphismus $G/\mathrm{Tor}(G) \cong \mathbb{Z}^r$ enthält.)
- Die Gruppe $\mathrm{Tor}(G)$ ist als surjektives Bild einer endlich erzeugten Gruppe nach Lemma 5.1 ebenfalls endlich erzeugt.
- Da alle Elemente in $\mathrm{Tor}(G)$ endliche Ordnung haben, folgt daraus, dass $\mathrm{Tor}(G)$ endlich ist.

zum Beweis von Satz 5.5:

- zeige: Für jede abelsche Gruppe G ist die Faktorgruppe $\bar{G} = G/\mathrm{Tor}(G)$ torsionsfrei, d.h. es gilt $\mathrm{Tor}(\bar{G}) = \{0_{\bar{G}}\}$.

Sei $\bar{g} \in \mathrm{Tor}(\bar{G}) \Rightarrow \exists m \in \mathbb{N}$ mit $m \cdot \bar{g} = 0_{\bar{G}}$

$\bar{g} \in \bar{G} \Rightarrow \exists g \in G$ mit $\bar{g} = g + \mathrm{Tor}(G) \Rightarrow$

$m \cdot (g + \mathrm{Tor}(G)) = \mathrm{Tor}(G) \Rightarrow mg + \mathrm{Tor}(G) = \mathrm{Tor}(G)$

$\Rightarrow mg \in \mathrm{Tor}(G) \Rightarrow \exists n \in \mathbb{N}$ mit $n(mg) = 0_G$

$\Rightarrow (mn)g = 0_G \Rightarrow g \in \mathrm{Tor}(G) \Rightarrow$

$g + \mathrm{Tor}(G) = \mathrm{Tor}(G) \Rightarrow \bar{g} = \bar{0}_G$

$m \cdot (g + \mathrm{Tor}(G)) = \mathrm{Tor}(G) \Rightarrow mg + \mathrm{Tor}(G) = \mathrm{Tor}(G)$

$\Rightarrow mg \in \mathrm{Tor}(G) \Rightarrow \exists n \in \mathbb{N}$ mit $n(mg) = 0_G$

- Darstellung von G als direktes Produkt

bereits bekannt: Es gibt einen Isom. $\bar{\Phi} : G/_{\mathrm{Tor}(G)} \to \mathbb{Z}^r$, für ein $r \in \mathbb{N}_0$. Durch Komposition mit $\pi_{\mathrm{Tor}(G)} : G \to \bar{G}$, $\bar{G} = G/\mathrm{Tor}(G)$ erhalten wir einen surj. Hom $\phi : G \to \mathbb{Z}^r$ mit $\ker(\phi) = \mathrm{Tor}(G)$. Für $1 \le j \le r$ wählen wir jeweils ein Element $u_j \in G$ mit $\phi(u_j) = e_j$, wobei $e_j \in \mathbb{Z}^r$ den j-ten Einheitsvektor bezeichnet. Setze $U = \langle u_1, \dots, u_r \rangle$.

Beh.: $G = \mathrm{Tor}(G) \oplus U$

klar: Da G abelsch ist, gilt $\mathrm{Tor}(G) \trianglelefteq G$ und $U \trianglelefteq G$.

überprüfe noch (1) $\mathrm{Tor}(G) \cap U = \{0_G\}$ (2) $G = \mathrm{Tor}(G) + U$

zu (1) Sei $g \in \mathrm{Tor}(G) \cap U$. $g \in \mathrm{Tor}(G) \Rightarrow \exists m \in \mathbb{N} : mg = 0_G$

$g \in U \Rightarrow \exists\, k_1, \dots, k_r \in \mathbb{Z}$ mit $g = k_1 u_1 + \dots + k_r u_r$

$\Rightarrow m k_1 u_1 + \dots + m k_r u_r = 0_G$

$\overset{\phi}{\Longrightarrow} m k_1 e_1 + \dots + m k_r e_r = 0_{\mathbb{Z}^r}$

$\xRightarrow[\mathbb{R}^r \text{ linear unabh.}]{e_1, \dots, e_r \text{ in}} m k_j = 0$ für $1 \le j \le r \Rightarrow k_j = 0$

für $1 \le j \le r \Rightarrow g = 0_G$

<u>zu (2)</u> Sei $g \in G \Rightarrow \phi(g) = (k_1, \dots, k_r) \in \mathbb{Z}^r$

für geeignet $k_j \in \mathbb{Z}$, $1 \le j \le r$. Definiere

$u = k_1 v_1 + \dots + k_r v_r$ und $h = g - u$.

$\Rightarrow \phi(h) = \phi(g) - \phi(u) = (k_1, \dots, k_r)$

$- \sum_{j=1}^{r} k_j \phi(u_j) = (k_1, \dots, k_r) - \sum_{j=1}^{r} k_j e_j = 0_{\mathbb{Z}^r}$

g

m

Se

ϕ :

ϕ(a

für

Aus d

(*) a

Es läss

Die $\mathbb{F}_p$-Vektorraumstruktur auf p-Torsionsgruppen

Lemma (5.6)

(i) Sei G eine abelsche Gruppe, seien $s \in \mathbb{N}_0$, $m_1, ..., m_s \in \mathbb{N}$ und $g_1, ..., g_s \in G$ mit $\mathrm{ord}(g_i) \mid m_i$ für $1 \leq i \leq s$. Sei $U = \langle g_1, ..., g_s \rangle$. Dann gibt es einen surjektiven Gruppenhomomorphismus $\phi : \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_s\mathbb{Z} \to U$ mit

$$\phi(\bar{a}_1, ..., \bar{a}_s) = a_1 g_1 + ... + a_s g_s \qquad \text{für alle } a_1, ..., a_s \in \mathbb{Z}.$$

(ii) Ist G eine abelsche Gruppe mit $G[p] = G$, dann gibt es eine Abbildung $\cdot : \mathbb{F}_p \times G \to G$ mit $\bar{a} \cdot g = ag$ für alle $a \in \mathbb{Z}$ und $g \in G$. Mit dieser Abbildung wird auf G die Struktur eines $\mathbb{F}_p$-Vektorraums definiert.

Beweis von Lemma 5.6: <u>zu (i)</u>

geg: abelsche Gruppe G, $s \in \mathbb{N}_0$, $g_1, \dots, g_s \in G$, $m_1, \dots, m_s \in \mathbb{N}_0$ mit $\operatorname{ord}(g_i) \mid m_i$ für $1 \le i \le s$

Sei $U = \langle g_1, \dots, g_s \rangle$. Betrachte die Abb.

$\phi : \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_s\mathbb{Z} \to U$ geg. durch

$$\phi(a_1 + m_1\mathbb{Z}, \dots, a_s + m_s\mathbb{Z}) \overset{(*)}{=} a_1 g_1 + \dots + a_s g_s$$

für $a_1, \dots, a_s \in \mathbb{Z}$ mit $0 \le a_i < m_i$ für $1 \le i \le s$.

Aus $\operatorname{ord}(g_i) \mid m_i$ für $1 \le i \le s$ folgt, dass $(*)$ auch für beliebige $a_1, \dots, a_s \in \mathbb{Z}$ erfüllt ist.

Es lässt sich nun leicht überprüfen, dass

$/m_1\mathbb{Z}$ … $/m_s\mathbb{Z}$ (*)

Gruppe
t ein
von
$\dots h_r \mid k_1, \dots$
von $\mathrm{Tor}(G)$
gt
$1 \leq i \leq r \}$

$\square$

ϕ ein Gruppenhom. ist. Außerdem liegen $g_1, \dots, g_s$ im Bild. Daraus folgt $\mathrm{im}(\phi) = \langle g_1, \dots, g_s \rangle = U$, d.h. ϕ ist surjektiv.

<u>zu (ii)</u> Sei nun p eine Primzahl und G eine abelsche Gruppe mit $G[p] = G$. Für jedes $g \in G$ existiert nach Teil (i) eine Abb. $\phi_g : \mathbb{F}_p \to G$ mit $\phi_g(a + p\mathbb{Z}) = ag$ für alle $a \in \mathbb{Z}$. Definiere nun

$$\cdot : \mathbb{F}_p \times G \to G, \quad (a + p\mathbb{Z}, g) \mapsto \phi_g(a + p\mathbb{Z})$$

leicht zu überprüfen: Für alle $a, b \in \mathbb{Z}$ und $g, h \in G$ gilt $(a+p\mathbb{Z}) \cdot (g+h) = (a+p\mathbb{Z}) \cdot g + (a+p\mathbb{Z}) \cdot h$, $((a+p\mathbb{Z}) + (b+p\mathbb{Z})) \cdot g \overset{(**)}{=}$

$(a+p\mathbb{Z})\cdot g + (b+p\mathbb{Z})\cdot g$, $((a+p\mathbb{Z})(b+p\mathbb{Z}))\cdot g =$

$(a+p\mathbb{Z})\cdot((b+p\mathbb{Z})\cdot g)$, $(1+p\mathbb{Z})\cdot g = g$.

Zeige nur $(**)$: $((a+p\mathbb{Z})+(b+p\mathbb{Z}))\cdot g = (a+b+p\mathbb{Z})\cdot g$

$= \phi_g(a+b+p\mathbb{Z}) = (a+b)g = ag + bg =$

$\phi_g(a+p\mathbb{Z}) + \phi_g(b+p\mathbb{Z}) = (a+p\mathbb{Z})\cdot g + (b+p\mathbb{Z})\cdot g$.

Insgesamt ist damit gezeigt, dass $(G,+,\cdot)$ ein $\mathbb{F}_p$-Vektorraum ist. $\square$

Satz (5.7)

Sei G eine abelsche Gruppe.

(i) Sind $m, n \in \mathbb{N}$ teilerfremd, dann gilt $G[mn] \cong G[m] \times G[n]$.

(ii) Sei $n \in \mathbb{N}$ mit $G[n] = G$, und sei $n = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung von n, mit $r \in \mathbb{N}_0$, Primzahlen $p_1, ..., p_r$ und Exponenten $e_1, ..., e_r \in \mathbb{N}$. Dann besteht ein Isomorphismus $G \cong G[p_1^{e_1}] \times ... \times G[p_r^{e_r}]$.

Als Chinesischer Restsatz bekannt ist die Aussage

Satz (5.8)

Sind $m, n \in \mathbb{N}$ teilerfremd, dann existiert ein Isomorphismus $\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ abelscher Gruppen.

Beweis von Satz 5.7, nur Teil (i)

geg: abelsche Gruppe G, $m, n \in \mathbb{N}$ teilerfremd

zeige: $G[mn] = G[m] \oplus G[n]$

klar: $G[m] \subseteq G[mn]$, denn: Sei $g \in G[m]$. $\Rightarrow m \cdot g = 0_G$

$\Rightarrow (mn) \cdot g = n \cdot (mg) = n \cdot 0_G = 0_G \Rightarrow g \in G[mn]$

ebenso: $G[n] \subseteq G[mn]$ Daraus folgt, dass $G[m], G[n]$ Untergruppen von $G[mn]$ sind, sogar Normalteiler, da G abelsch. noch zu überprüfen:

(1) $G[m] \cap G[n] = \{0_G\}$ (2) $G[mn] = G[m] + G[n]$

(1) $G[m] \cap G[n] = \{0_G\}$ (2) $G[mn] = G[m] + G[n]$

zu (1) Sei $g \in G[m] \cap G[n] \Rightarrow mg = 0_G,\ n \cdot g = 0_G$

Lemma von Bézout $\Rightarrow \exists\, k, l \in \mathbb{Z}$ mit $km + ln = 1$

$\Rightarrow g = 1 \cdot g = (km + ln) \cdot g = k(mg) + l(n \cdot g) =$

$k \cdot 0_G + l \cdot 0_G = 0_G$

zu (2) Sei $g \in G[mn] \Rightarrow mn \cdot g = 0_G$ Verwende die

$k, l \in \mathbb{Z}$ von oben $\Rightarrow g = lng + kmg$

$m \cdot (lng) = l\, mng = l \cdot 0_G = 0_G \Rightarrow lng \in G[m]$

$n \cdot (kmg) = k\, mng = k \cdot 0_G = 0_G \Rightarrow kmg \in G[n]$

$\Rightarrow g = lng + kmg \in G[m] + G[n]$. $\square$

Zerlegung einer abelschen p^e-Torsionsgruppe

Satz (5.9)

Sei $e \in \mathbb{N}_0$, p eine Primzahl und G eine endliche abelsche Gruppe mit $G[p^e] = G$. Dann gibt es ein $r \in \mathbb{N}_0$ und $n_1, ..., n_r \in \mathbb{N}$, so dass

$$G \quad \cong \quad \mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r}\mathbb{Z} \qquad \text{gilt.}$$

Beweis:

- Der Beweis erfolgt durch vollständige Induktion über e. Im Fall $e = 0$ ist $G = \{0_G\}$ und die Aussage offensichtlich.
- Im Induktionsschritt betrachten wir die Gruppe $H = pG$ mit $H[p^{e-1}] = H$. Nach Induktionsvoraussetzung existiert ein Isomorphismus

$$\phi : \mathbb{Z}/p^{n_1}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r}\mathbb{Z} \to H.$$

Beweis von Satz 5.9 (Forts.)

- Es seien $h_1, \ldots, h_r \in H$ die Bilder der „Einheitsvektoren“ $(\bar{1}, \bar{0}, \ldots)$, $(\bar{0}, \bar{1}, \ldots)$ usw. in H. Wegen $pG = H$ existiert jeweils ein $g_j \in G$ mit $pg_j = h_j$.
- Zeige mit Hilfe von Lemma 5.6 (i), dass $U = \langle g_1, \ldots, g_r \rangle$ isomorph zur Gruppe

$$\mathbb{Z}/p^{n_1+1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{n_r+1}\mathbb{Z} \quad \text{ist.}$$

- Nach Lemma 5.6 (ii) ist $G[p]$ ein $\mathbb{F}_p$-Vektorraum, und $G[p] \cap U$ ist ein Untervektorraum. Wähle eine Basis $\{v_1, \ldots, v_s\}$ von $G[p] \cap U$ und erweitere diese durch $v_{s+1}, \ldots, v_t$ zu einer Basis von $G[p]$.
- Setze $V = \langle v_{s+1}, \ldots, v_t \rangle$. Überprüfe nun, dass $G = U \oplus V$ gilt. Daraus folgt dann

$$G \cong U \times V \cong \mathbb{Z}/p^{n_1+1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{n_r+1}\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^{t-s}.$$

Beweis von Satz 5.9 (Forts.)

- Für den Nachweis von $U \cap V = \{0_G\}$ beachte zunächst, dass die Menge links wegen $V \subseteq G[p]$ mit $(U \cap G[p]) \cap V$ übereinstimmt. Die Aussage folgt nun aus der Tatsache, dass $G[p]$ als $\mathbb{F}_[p]$-Vektorraum gleich der direkten Summe $(U \cap G[p]) \oplus V$ ist, auf Grund der Definition von V durch Basisergänzung.
- Zum Nachweis von $U + V = G$ sei $g \in G$ vorgegeben. Stelle pg durch die Erzeuger h_j von pG dar. Definiere damit ein $g' \in U$ mit $pg' = pg$, und setze $g'' = g - g'$. Überprüfe, dass $g'' \in G[p]$ liegt. Daraus folgt $g'' \in U + V$, denn die Basis von $G[p]$ als $\mathbb{F}_p$-Vektorraum setzt sich aus Elementen von U und V zusammen.

- genauere Ausführung des letzten Punkts:

  Das Element pg hat die Form $\sum_{j=1}^{r} a_j h_j$ mit $a_1, \ldots, a_r \in \mathbb{Z}$. Setzen wir $g' = \sum_{j=1}^{r} a_j g_j$, dann folgt aus $pg_j = h_j$ für $1 \leq j \leq r$ die Gleichung $pg' = pg$. Für das Element g'' folgt damit

$$pg'' = pg - pg' = \left(\sum_{j=1}^{r} a_j h_j\right) - p\left(\sum_{j=1}^{r} a_j g_j\right) = \left(\sum_{j=1}^{r} a_j h_j\right) - \left(\sum_{j=1}^{r} a_j p g_j\right) = \left(\sum_{j=1}^{r} a_j h_j\right) - \left(\sum_{j=1}^{r} a_j h_j\right) = 0_G .$$

  Also liegt g'' in $G[p]$.

Hauptsatz über endlich erzeugte abelsche Gruppe

Satz (5.10)

Sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es $r, s \in \mathbb{N}_0$ und $d_1, ..., d_s \in \mathbb{N}$ mit

$$G \quad \cong \quad \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_s\mathbb{Z}.$$

Dabei können die Zahlen d_i so gewählt werden, dass sie entweder

(i) alle Primzahlpotenzen sind oder

(ii) $d_i \mid d_{i+1}$ für $1 \leq i < s$ erfüllt ist.

Im Fall (ii) gezeichnet man die Zahlen d_i als Elementarteiler der abelschen Gruppe.

Anwendungsbeispiel zu Satz 5.10:

Die Zahl 100 lässt sich (bis auf Reihenfolge) auf folgende Weise in Primzahlpotenzen zerlegen: $4 \cdot 25$, $2 \cdot 2 \cdot 25$, $4 \cdot 5 \cdot 5$ und $2 \cdot 2 \cdot 5 \cdot 5$

Teil (i) besagt also, dass jede abelsche Gruppe der Ordnung 100 zu einer der folgenden Gruppen isomorph ist:

$$G_1 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}, \quad G_2 = (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/25\mathbb{Z}$$

$$G_3 = \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^2, \quad G_4 = (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/5\mathbb{Z})^2$$

Ebenso zeigt Teil (ii), dass jede abelsche Gruppe der Ordnung 100 zu einer der folgenden Gruppen isomorph ist:

$$H_1 = \mathbb{Z}/100\mathbb{Z}, \quad H_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z},$$

$$H_3 = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}, \quad H_4 = \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$$