Der Homomorphiesatz für Gruppen

Satz (4.29)

Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Dann induziert ϕ einen Isomorphismus

$$\bar{\phi} : G/\ker(\phi) \xrightarrow{\sim} \mathrm{im}(\phi).$$

Ist der Homomorphismus ϕ surjektiv, dann erhält man also einen Isomorphismus $G/\ker(\phi) \cong H$.

Die Isomorphiesätze

Satz (4.32)

Sei G eine Gruppe, $N \trianglelefteq G$ und U eine Untergruppe von G.

(i) Dann ist $N \cap U$ ein Normalteiler von U, und es gilt $U/(N \cap U) \cong (UN)/N$.

(ii) Ist auch $U \trianglelefteq G$ und gilt $U \supseteq N$, dann folgt $G/U \cong (G/N)/(U/N)$.

Anwendungsbeispiel zu Satz 4.32 (ii)

$G = (\mathbb{Z}, +)$, $N = \langle 6 \rangle = 6\mathbb{Z} \Rightarrow G/N \cong (\mathbb{Z}/6\mathbb{Z}, +)$

Sei außerdem $U = \langle 2 \rangle = 2\mathbb{Z}$. Dann gilt $U \trianglelefteq G$ (da $U \leq G$ und G abelsch ist) und $U \supseteq N$, denn

$6 = 3 \cdot 2 \in \langle 2 \rangle \Rightarrow N = \langle 6 \rangle \subseteq \langle 2 \rangle = U$

Auf Grund des Satzes gilt also $(G/N)/(U/N) \cong G/U \cong \mathbb{Z}/2\mathbb{Z}$

Frage: Wie sehen die Elemente von $(G/N)/(U/N) = (\mathbb{Z}/6\mathbb{Z})/(U/N)$ aus? Die Gruppe U/N ist das Bild von U in $G/N = \mathbb{Z}/6\mathbb{Z}$, dieses besteht aus den

Bild von U in $G/N = \mathbb{Z}/6\mathbb{Z}$, dieses besteht aus den

- Vielfachen von $\bar{2} = 2 + 6\mathbb{Z}$. also: $U/N = \{\bar{0}, \bar{2}, \bar{4}\}$
$= \langle \bar{2} \rangle \Rightarrow (\mathbb{Z}/6\mathbb{Z}) / (U/N) = (\mathbb{Z}/6\mathbb{Z}) / \langle \bar{2} \rangle =$
$\{\bar{a} + \langle \bar{2} \rangle \mid 0 \le a < 6\} = \{\langle \bar{2} \rangle, \bar{1} + \langle \bar{2} \rangle\}$
$\langle \bar{2} \rangle = \bar{2} + \langle \bar{2} \rangle = \bar{4} + \langle \bar{2} \rangle$
$\bar{1} + \langle \bar{2} \rangle = \bar{3} + \langle \bar{2} \rangle = \bar{5} + \langle \bar{2} \rangle$

Beweis von Satz 4.32, Teil (ii)

Es gilt $U/N \trianglelefteq G/N$, denn U/N ist das Bild des Normalteilers $U \trianglelefteq G$ unter dem kanonischen Epimorphismus $\pi_N : G \to G/N$. Dies zeigt, dass $(G/N)/(U/N)$ eine Gruppe ist.

Um $G/U \cong (G/N)/(U/N)$ nachzuweisen, wenden wir den Homomorphiesatz an auf die Abbildung $\phi : G \to (G/N)/(U/N)$, $g \mapsto (gN)(U/N)$ zu überprüfen:

(1) ϕ ist ein Homomorphismus
(2) ϕ ist surjektiv

(3) $\ker(\phi) = U$

zu (1) Dies folgt daraus, dass ϕ die Komposition der beiden kanonischen Epimorphismen $\pi_N : G \to G/N$, $g \mapsto gN$ und $\pi_{U/N} : G/N \to (G/N)/(U/N)$, $\bar{g} \mapsto \bar{g}(U/N)$ ist.

zu (2) klar, weil die Komposition von zwei surjektiven Abbildungen surjektiv ist

zu (3) Sei $g \in G$. z.z.: $g \in \ker(\phi) \iff g \in U$

Es gilt: $g \in \ker(\phi) \iff \phi(g) = e_{(G/N)/(U/N)}$

$\iff gN(U/N) = U/N \iff gN \in U/N$

$\iff \exists u \in U : gN = uN \iff$

$\exists u \in \mathcal{U} : g \in u\,N \iff \exists u \in \mathcal{U}, n \in N :$

$g = un \iff g \in uN \underset{uN = u}{\overset{u \supseteq N}{\iff}} g \in u$ $\square$

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 $p_1, \ldots, p_r$.

Surjektive Bilder endlich erzeugter Gruppen

Lemma (5.1)

Seien G, H beliebige Gruppen. Ist G endlich erzeugt und existiert ein surjektiver Homomorphismus $\phi : G \to H$, dann ist auch H endlich erzeugt.

additive Notation:

Sei $(G, +)$ eine abelsche Gruppe, und seien $U, V \leq G$. Von nun an bedeutet die Schreibweise $G = U \oplus V$, dass G ein inneres direktes Produkt von U und V ist.

Beweis von Lemma 5.1:

G endlich erzeugt $\Rightarrow$ $\exists$ endliche Menge $S = \{g_1, \dots, g_r\}$ ($r \in \mathbb{N}_0$) mit $G = \langle S \rangle$

Sei $\bar{S} = \phi(S) = \{\phi(g_j) \mid 1 \le j \le r\}$ die Bildmenge

Es genügt z.zg.: $H = \langle \bar{S} \rangle$ Dafür genügt es z.zg.:

Ist $U \le H$ mit $U \supseteq \bar{S}$, dann folgt $U = H$.

Sei U also eine solche Untergp. $U \supseteq \bar{S} \Rightarrow \phi^{-1}(U) \supseteq \phi^{-1}(\bar{S}) \supseteq S$ Da $\phi^{-1}(U)$ eine Untergruppe von G ist, folgt $\phi^{-1}(U) \supseteq \langle S \rangle = G \Rightarrow G = \phi^{-1}(U)$

Weil ϕ surjektiv ist, folgt $H = \phi(G) = \phi(\phi^{-1}(U)) = U$

↳ surjektiv

□

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.

Bem: In einer abelschen Gruppe $(G,+)$ ist $G[m]$ für jedes $m \in \mathbb{N}$ eine Untergruppe, und ebenso $Tor(G)$.

(1) Untergruppeneigenschaft von $G[m]$:

$0_G \in G[m]$, da $m \cdot 0_G = 0_G$

Für bel. $g, h \in G[m]$ gilt $m \cdot g = 0_G$, $m \cdot h = 0_G$, damit auch $m \cdot (g+h) = m \cdot g + m \cdot h = 0_G + 0_G = 0_G$, und $m \cdot (-g) = -(m \cdot g) = -0_G = 0_G$, also: $g+h \in G[m]$ und $-g \in G[m]$.

(Hinweis: In einer bel. Gruppe $(G, \circ)$ ist $\{g \in G \mid g^n = e\}$ im Allgemeinen keine Untergruppe von G siehe Globalübungsblatt 3, Aufgabe 1.)

(2) Untergruppeneigenschaft von $\mathrm{Tor}(G) = \bigcup_{n \in \mathbb{N}} G[n]$

$0_G \in \mathrm{Tor}(G)$ da $0_G \in G[1]$

Seien $g, h \in \mathrm{Tor}(G) \Rightarrow \exists m, n \in \mathbb{N}$:

$m \cdot g = 0_G, \; n \cdot h = 0_G \Rightarrow mn(g+h) =$

$mn\,g + mn\,h = n \cdot (m \cdot g) + m \cdot (n\,h) = n \cdot 0_G + m \cdot 0_G = 0_G$,

$m \cdot (-g) = -(m \cdot g) = -0_G = 0_G$

also: $g + h \in \mathrm{Tor}(G)$, $-g \in \mathrm{Tor}(G)$ □

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.

Freie und torsionsfreie endliche abelsche Gruppen

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.

Beweis von Proposition 5.4

zu (i) Es genügt, durch vollständige Induktion über n zu zeigen: Für jedes $n \in \mathbb{N}_0$ ist jede Untergruppe von $(\mathbb{Z}^n, +)$ eine freie abelsche Gruppe. Wir zeigen genauer: Jede Untergr. $U \leq \mathbb{Z}^n$ $(n \in \mathbb{N})$ ist isomorph zu $\mathbb{Z}^m$ für ein $m \in \mathbb{N}_0$ mit $m \leq n$.

Ind.-Anf.: $n = 0$ Sei U eine Untergruppe von $\mathbb{Z}^0 = \{0\}$

$\Rightarrow U = \{0\} \Rightarrow U \leq \mathbb{Z}^0$.

$n = 1$ Sei U eine Untergruppe von $(\mathbb{Z}, +)$. §3 $\Rightarrow$

$\Rightarrow U = \{0\} \Rightarrow U \cong \mathbb{Z}^0$.

$\underline{n=1}$ Sei U eine Untergruppe von $(\mathbb{Z}, +)$. §3 $\Rightarrow$

$U = r\mathbb{Z}$ für ein $r \in \mathbb{N}_0$. 1. $\underline{\text{Fall}}$: $r = 0 \Rightarrow U = \{0\} \cong \mathbb{Z}^0$

2 $\underline{\text{Fall}}$: $r \in \mathbb{N}$ Dann gilt $U \cong \mathbb{Z}$, denn $x \mapsto rx$ ist offenbar ein Isomorphismus zwischen $\mathbb{Z}$ und $U = r\mathbb{Z}$.

$\underline{\text{Ind-schritt}}$: Sei $n \in \mathbb{N}$, setze die Aussage für n voraus.

Sei $U \leq \mathbb{Z}^{n+1}$ z.zg. $U \cong \mathbb{Z}^m$ für ein $m \in \mathbb{N}_0$ mit $m \leq n+1$.

Sei $\pi : \mathbb{Z}^{n+1} \to \mathbb{Z}$ gegeben durch $a = (a_1, \dots, a_{n+1}) \mapsto a_{n+1}$

Dann ist $\ker(\pi) = \mathbb{Z}^n \times \{0\}$ und $\ker(\pi|_U) = U \cap \mathbb{Z}^n \times \{0\}$

Wegen $\mathbb{Z}^n \times \{0\} \cong \mathbb{Z}^n$ ist $\ker(\pi|_U)$ isomorph zu einer Untergruppe von $\mathbb{Z}^n$. Ind.-V. $\Rightarrow \ker(\pi|_U) \cong \mathbb{Z}^p$ für ein $p \in \mathbb{N}_0$ mit $p \leq n$.

Das Bild $\pi(U)$ ist eine Untergruppe von $(\mathbb{Z}, +)$.

§3 $\Rightarrow \exists\, r \in \mathbb{N}_0$ mit $\pi(U) = r\mathbb{Z} = \langle r \rangle$.

1. Fall: $r = 0 \Rightarrow \pi(U) = 0 \Rightarrow a_{n+1} = 0 \;\forall\, a \in U$

$\rightarrow U \leq \mathbb{Z}^n \times \{0\} \rightarrow U = \ker(\pi|_U) \cong \mathbb{Z}^p$

Wegen $p \leq n \leq n+1$ ist der Beweis in diesem Fall abgeschlossen.

2. Fall: $r > 0$ Sei $v \in U$ mit $\pi(v) = r$

Beh: U ist inneres direktes Produkt von $\ker(\pi|_U)$ und $\langle v \rangle$, d.h. $U = \ker(\pi|_U) \oplus \langle v \rangle$

klar: $\langle v \rangle$, $\ker(\pi|_U)$ sind Normalteiler von U (weil $\mathbb{Z}^{n+1}$ eine abelsche Gruppe ist)

Zu überprüfen: (1) $\ker(\pi|_U) \cap \langle v \rangle = \{0_{\mathbb{Z}^{n+1}}\}$

(2) $U = \ker(\pi|_U) + \langle v \rangle$

zu (1) Es genügt „$\subseteq$" zu überprüfen.

Sei also $u = (u_1, \dots, u_{n+1}) \in \ker(\pi|_U) \cap \langle v \rangle$.

$u \in \langle v \rangle \Rightarrow \exists k \in \mathbb{Z}$ mit $u = kv$

$u \in \ker(\pi|_U) \Rightarrow u_{n+1} = 0 \Rightarrow kv_{n+1} = 0 \Rightarrow kr = 0$

$\overset{r>0}{\Rightarrow} k = 0 \Rightarrow u = 0_{\mathbb{Z}^{n+1}}$

zu (2) „$\supseteq$" ist offensichtlich, da $\ker(\pi|_U)$ und $\langle v \rangle$ beides Untergp. von U sind

„$\subseteq$" Sei $u \in U$. zzg. $u \in \ker(\pi|_U) + \langle v \rangle$

$\pi(u) \in \pi(U) \overset{\pi(U) = \langle r \rangle}{\Rightarrow} \exists k \in \mathbb{Z}$ mit $\pi(u) = kr$

$\Rightarrow \pi(u - kv) = \pi(u) - k\,\pi(v) = kv - kv$

$= 0 \Rightarrow u - kv \in \ker(\pi|_U) \Rightarrow$

$u = (u - kv) + kv \in \ker(\pi|_U) + \langle v \rangle$

($\Rightarrow$ Beh.) Aus der Beh. folgt

$U \subseteq \ker(\pi|_U) \times \langle v \rangle \overset{\text{s.o.}}{\cong} \mathbb{Z}^p \times \mathbb{Z} = \mathbb{Z}^{p+1}$

Wegen $p+1 \leq n+1$ ist der Ind.-schritt damit abgeschlossen.

zu (ii) Sei $(G,+)$ eine torsionsfreie endl. erz. abelsche Gruppe. z.zg:
G ist frei, d.h. $G \cong (\mathbb{Z}^n,+)$ für ein $n \in \mathbb{N}_0$.
Sei $S \subseteq G$ ein endliches Erz.-system von G. Sei $T = \{g_1,\dots,g_n\} \subseteq S$ eine maximale Teilmenge mit der Eigenschaft, dass
$\mathbb{Z}^n \to G, (a_1,\dots,a_n) \mapsto \sum_{i=1}^{n} a_i g_i$
injektiv ist.

Beh.: Für jedes $g \in S$ gibt es ein $a_g \in \mathbb{N}$ mit $a_g g \in \langle T \rangle$. Sei also $g \in S$

1. Fall: $g \in T$ Dann gilt $1 \cdot g \in \langle T \rangle$, d.h. wir können $a_g = 1$ setzen.

2. Fall: $g \in S \setminus T$ Die Abb. $\mathbb{Z}^{n+1} \to G$,

$(a_1, \ldots, a_{n+1}) \mapsto \sum_{i=1}^{n} a_i g_i + a_{n+1} g$ ist nicht injektiv

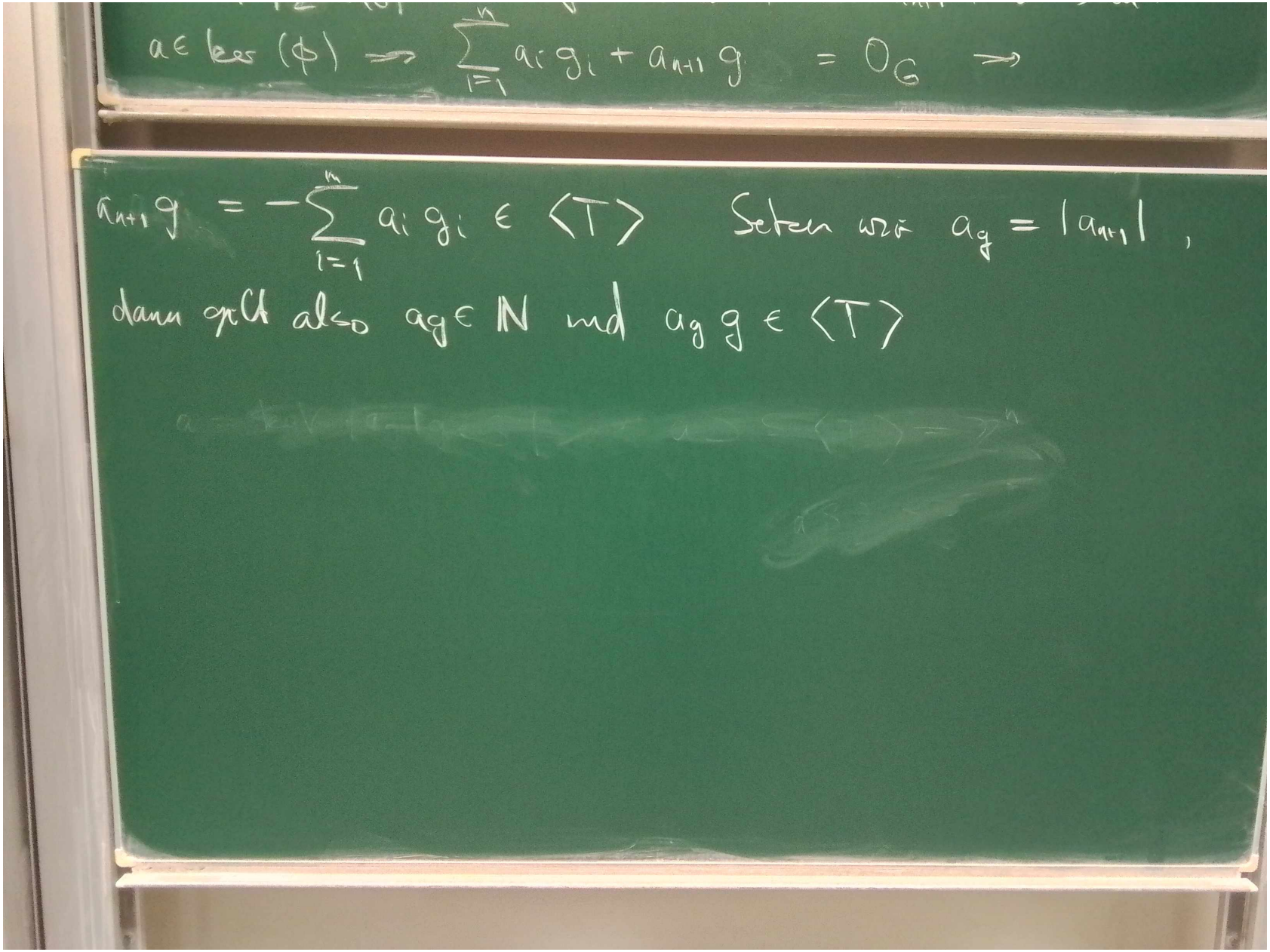
wegen $T \cup \{g\} \supsetneq T$ und aufgrund der Maximalität von T.

Diese Abb. ϕ ist ein Hom., und auf Grund der

Nicht-Inj. gibt ein $a \in \mathbb{Z}^{n+1} \setminus \{0\}$ in $\ker(\phi)$.

Da $\phi|_{\mathbb{Z}^n \times \{0\}}$ aber injektiv ist, muss $a_{n+1} \neq 0$ sein.

$a \in \ker(\phi) \to \sum_{i=1}^{n} a_i g_i + a_{n+1} g = 0_G \to$



(Abschluss des Beweises von (ii) auf den nächsten beiden Seiten)

Einige ergänzende Hinweise:

- Dass die Abbildung $\phi : \mathbb{Z}^{n+1} \to G$ ein Homomorphismus ist, kann einfach nachgerechnet werden: Für beliebige $a, b \in \mathbb{Z}^{n+1}$ gilt $\phi(a+b) = \sum_{i=1}^{n}(a_i + b_i)g_i + (a_{n+1} + b_{n+1})g$

$$= \left(\sum_{i=1}^{n} a_i g_i + a_{n+1} g\right) + \left(\sum_{i=1}^{n} b_i g_i + b_{n+1} g\right) = \phi(a) + \phi(b).$$

- Ausführung des Arguments Ende vorletzte Tafel:
  Sei $\phi_0 : \mathbb{Z}^n \to G$ definiert durch $\phi_0(b) = \sum_{i=1}^{n} b_i g_i$ für alle $b \in \mathbb{Z}^n$, dann gilt für alle $a \in \mathbb{Z}^{n+1}$ jeweils

$$\phi(a) = \phi_0(a_1, ..., a_n) + a_{n+1} g.$$

  Die Abbildung ϕ_0 ist laut Angabe injektiv. Ist nun $a \in \mathbb{Z}^{n+1}$ mit $\phi(a) = 0$ und $a_{n+1} = 0$, dann folgt $\phi_0(a_1, ..., a_n) = 0$ und somit $(a_1, ..., a_n) = 0$, insgesamt also $a = 0$.

Abschluss des Beweises von Proposition 5.4 (ii)

- Sei $a \in \mathbb{N}$ das kgV der Elemente a_g mit $g \in S$. Wegen $a_g g \in \langle T \rangle$ für alle $g \in S$ gilt dann $aS \subseteq \langle T \rangle$ und somit auch $\langle aS \rangle \subseteq \langle T \rangle$.
- Der Homomorphismus ϕ ist injektiv und offenbar nach Definition von $\langle T \rangle$ auch surjektiv, insgesamt also ein Isomorphismus. Es gilt also $\langle T \rangle \cong \mathbb{Z}^n$, d.h. die Untergruppe $\langle T \rangle$ ist eine freie abelsche Gruppe.
- Durch $g \mapsto ag$ ist somit ein Homomorphismus von $\psi : G \to T$ definiert, und auf Grund der Torsionsfreiheit von G ist dieser injektiv.
- Dies zeigt, dass G isomorph zu einer Untergruppe der endlich erzeugten freien abelsche Gruppe $\langle T \rangle$ ist. Nach Teil (i) ist G damit selbst eine endlich erzeugte freie abelsche Gruppe.