

Vortrag 5 — Endliche abelsche Gruppen

Seien $A_1, \dots, A_n$ abelsche Gruppen (additiv geschrieben). Definiere auf dem kartesischen Produkt $A_1 \times \dots \times A_n$ mittels eintragsweiser Addition eine abelsche Gruppenstruktur. Schreibe das Resultat $A_1 \oplus \dots \oplus A_n$, genannt *direkte Summe*.

Sei

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ s \downarrow & & \downarrow t \\ A' & \xrightarrow{f'} & B' \end{array}$$

ein kommutatives Viereck abelscher Gruppen und Gruppenmorphismen, d.h. sei $f' \circ s = t \circ f$.

Lemma 1. *Es gibt einen Gruppenmorphismus*

$$\begin{aligned} B/f(A) &\xrightarrow{u} B'/f(A') \\ b + f(A) &\mapsto t(b) + f(A') \end{aligned}$$

Lemma 2. *Sind s und t Isomorphismen, so auch u .*

Sind $k, \ell \geq 0$ und ist $S \in \mathbf{Z}^{k \times \ell}$ eine Matrix der Form $k \times \ell$ mit ganzzahligen Einträgen, so schreiben wir $\mathbf{Z}^{\ell \times 1} \xrightarrow{S} \mathbf{Z}^{k \times 1}$ für den Gruppenmorphismus, der einem ganzzahligen Vektor $x \in \mathbf{Z}^{\ell \times 1}$ den ganzzahligen Vektor $Sx \in \mathbf{Z}^{k \times 1}$ zuordnet. Komposition entspricht so der Matrixmultiplikation.

Bemerkung. Seien $m, n \geq 0$, und sei $M \in \mathbf{Z}^{m \times n}$ gegeben. Mit dem Elementarteilersatz gibt es invertierbare Matrizen $S \in \mathbf{Z}^{n \times n}$ und $T \in \mathbf{Z}^{m \times m}$ so, daß $D := TMS \in \mathbf{Z}^{m \times n}$ eine Diagonalmatrix ist (wenn auch keine quadratische, im allgemeinen), deren Diagonaleinträge sich sukzessive teilen. Dies gibt ein kommutatives Viereck

$$\begin{array}{ccc} \mathbf{Z}^{n \times 1} & \xrightarrow{M} & \mathbf{Z}^{m \times 1} \\ S^{-1} \downarrow \wr & & \wr \downarrow T \\ \mathbf{Z}^{n \times 1} & \xrightarrow{D} & \mathbf{Z}^{m \times 1} \end{array}$$

abelscher Gruppen mit vertikalen Isomorphismen. Mit Lemma 2 ist also

$$\mathbf{Z}^{m \times 1} / M\mathbf{Z}^{n \times 1} \simeq \mathbf{Z}^{m \times 1} / D\mathbf{Z}^{n \times 1}.$$

Lemma 3. *Habe die Diagonalmatrix $D \in \mathbf{Z}^{m \times n}$ die nichtverschwindenden Diagonaleinträge $d_1, \dots, d_s$ an den Positionen $(1, 1), \dots, (s, s)$, und ansonsten Nulleinträge. Dann ist*

$$\mathbf{Z}^{m \times 1} / D\mathbf{Z}^{n \times 1} \simeq \mathbf{Z}/d_1\mathbf{Z} \oplus \dots \oplus \mathbf{Z}/d_s\mathbf{Z} \oplus \mathbf{Z}^{\oplus(m-s)}.$$

Eine abelsche Gruppe A heißt *endlich erzeugt*, falls es ein $k \geq 0$ gibt und Elemente $a_1, \dots, a_k$ derart, daß jedes Element $a \in A$ sich schreiben läßt als

$$a = z_1 a_1 + \dots + z_k a_k$$

mit geeigneten $z_i \in \mathbf{Z}$. Das Tupel $(a_1, \dots, a_k)$ heißt auch *Erzeugendensystem* von A .

Lemma 4. Sei $A \xrightarrow{f} B$ ein surjektiver Gruppenmorphimus abelscher Gruppen. Seien B und $\text{Kern } f = \{a \in A : f(a) = 0\}$ endlich erzeugt. Dann ist auch A endlich erzeugt.

Sei $(b_1, \dots, b_s)$ ein Erzeugendensystem von B . Sei a_i ein Urbild von b_i unter f für $i \in [1, s]$. Sei $(x_1, \dots, x_t)$ ein Erzeugendensystem von $\text{Kern } f$. Dann ist

$$(x_1, \dots, x_t, a_1, \dots, a_s)$$

ein Erzeugendensystem von A .

Lemma 5. Jede Untergruppe ungleich $\{0\}$ von $\mathbf{Z}$ hat ein eindeutig bestimmtes Erzeugendensystem aus einem positiven Element. Insbesondere ist jede Untergruppe von $\mathbf{Z}$ endlich erzeugt.

Beweis. Sei $V \leq \mathbf{Z}$. Sei $v := \min(V \cap \mathbf{Z}_{\geq 1})$. Division mit Rest zeigt, daß (v) ein Erzeugendensystem von V ist. $\square$

Lemma 6. Sei $m \geq 0$. Sei $U \leq \mathbf{Z}^{m \times 1}$. Es ist U eine endlich erzeugte abelsche Gruppe.

Beweis. Induktion über m . Sei $\mathbf{Z}^{m \times 1} \xrightarrow{p} \mathbf{Z}^{(m-1) \times 1}$ die Projektion auf die Koordinaten 2 bis m . Es ist $\text{Kern } p \simeq \mathbf{Z}$. Werde nun Lemma 4 angewandt auf $A = U$, $B = p(U)$ und $f : A \rightarrow B, a \mapsto p(a)$. Es ist B endlich erzeugt nach Induktionsvoraussetzung. Es ist $\text{Kern } f$ endlich erzeugt, da Untergruppe von $\text{Kern } p$, und damit mit Lemma 5 sogar von einem Element erzeugt. $\square$

Satz. Sei A eine endliche abelsche Gruppe. Es gibt auf eindeutige Weise $d_1, \dots, d_s \in \mathbf{Z}_{\geq 2}$ mit $d_1 | d_2 | \dots | d_s$ so, daß

$$A \simeq \mathbf{Z}/d_1\mathbf{Z} \oplus \mathbf{Z}/d_2\mathbf{Z} \oplus \dots \oplus \mathbf{Z}/d_s\mathbf{Z}.$$

Beweis. Existenz. Sei $(a_1, \dots, a_m)$ ein Erzeugendensystem von A . Wir haben einen surjektiven Gruppenmorphimus $\mathbf{Z}^{m \times 1} \xrightarrow{f} A$, der den i -ten Standardbasisvektor auf a_i schickt für $i \in [1, m]$. Sei B der Kern von f . Nach vorigem Lemma ist B endlich erzeugt. Sei $(b_1, \dots, b_n)$ ein Erzeugendensystem von B . Wir haben einen surjektiven Gruppenmorphimus $\mathbf{Z}^{n \times 1} \rightarrow B$, der den i -ten Standardbasisvektor auf b_i schickt für $i \in [1, n]$. Insgesamt

$$\mathbf{Z}^{n \times 1} \rightarrow B = \text{Kern } f \rightarrow \mathbf{Z}^{m \times 1} \xrightarrow{f} A.$$

Mit dem Homomorphiesatz ist A isomorph zu $\mathbf{Z}^{m \times 1} / \text{Kern } f$. Sei M eine beschreibende Matrix des Kompositums $\mathbf{Z}^{n \times 1} \rightarrow \mathbf{Z}^{m \times 1}$ bezüglich der Standardbasen, i.e. sei das Kompositum gleich $\mathbf{Z}^{n \times 1} \xrightarrow{M} \mathbf{Z}^{m \times 1}$. Dann ist A isomorph zu $\mathbf{Z}^{m \times 1} / M\mathbf{Z}^{n \times 1}$. Eine Anwendung der Bemerkung und des Lemmas 3 zeigt nun die Existenz der d_i mit der verlangten Isomorphie.

Eindeutigkeit. Für $m \in \mathbf{Z}_{\geq 1}$ schreiben wir $A[m]$ für den Kern der Multiplikationsabbildung mit m auf A . Sei p eine Primzahl. Wir schreiben

$$v_p(m) := \max\{k \geq 0 : p^k | m\}$$

für die *Bewertung* (valuation) von m bei p . Für $k \in \mathbf{Z}_{\geq 0}$ schreiben wir

$$q_{A,p}(k) := v_p \left(\frac{|A[p^{k+1}]|}{|A[p^k]|} \right).$$

Es genügt, für gegebenes i die Bewertung $v_p(d_i)$ von d_i als invariant unter Isomorphie nachzuweisen.

Es ist $q_{A,p}(k)$ eine solche Invariante. Also ist auch s invariant unter Isomorphie, da s das Maximum der Werte $q_{A,p}(0)$ ist, wobei p die Primteiler von $|A|$ durchläuft.

Für $\ell \in [0, s-1]$ ist nun $v_p(d_{s-\ell}) = \min\{k \in \mathbf{Z}_{\geq 0} : q_{A,p}(k) \leq \ell\}$. □