Universität zu Köln

Universität zu Köln

Mathematisches Institut

Endlich erzeugte abelsche Gruppen

Autoren
Alina Braun und
Bianca Kusserow

Seminarleitung:
Dr. Stephan Ehlen

Handout zum Vortrag im Seminar

Elementare Zahlentheorie und Algebra, SS 19

02. April und 09. April 2019

Zusammenfassung

Das Seminar *Elementare Zahlentheorie und Algebra* wird im Sommersemester 2019 unter der Leitung von Dr. Stephan Ehlen gehalten. Im Seminar werden Themen der elementaren Zahlentheorie sowie hierzu hilfreiche Grundlagen der Algebra behandelt.
Die beiden Vorträge *Endlich erzeugte abelsche Gruppen I und II* stützen sich auf dem 6. Kapitel des Buches *Elementare und algebraische Zahlentheorie*, S. Müller-Stach, J. Piontkowski, Vieweg und Teubner, 2011

Inhaltsverzeichnis

Kapitel 1

Endlich erzeugte abelsche Gruppen I

Im ersten Teil dieser Vortragsreihe wird die Struktur und der Aufbau endlich erzeugter abelscher Gruppen analysiert. Zudem werden erste mögliche Darstellungsformen einer solchen Gruppe vorgestellt, mit denen dann später der Hauptsatz über endlich erzeugte abelsche Gruppen hergeleitet werden kann.
Das Ziel dieser Vortragsreihe ist es, zu beweisen, dass jede endlich erzeugte abelsche Gruppe ein direktes Produkt aus den additiven Gruppen $\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$ ist.

1.1 Grundlagen

Definition 1.1: *Sei G ein nicht-leere Menge. Man ordne jedem Paar $(g,h) \in G \times G$ genau ein Element $g \circ h \in G$ zu. $(G, \circ)$ heißt abelsche Gruppe, wenn die Verknüpfung*
$\circ : G \times G \ni (g,h) \mapsto g \circ h \in G$ folgende Eigenschaften erfüllt:

1. Assoziativität: $\forall g,h,f \in G$ gilt:
$(g \circ h) \circ f = g \circ (h \circ f)$

2. Neutrales Element: $\exists e \in G$, sodass $\forall g \in G$ gilt:
$g \circ e = e \circ g = g$

3. Inverses Element: Zu jedem $g \in G$ $\exists g^{-1} \in G$, sodass gilt:
$g \circ g^{-1} = g^{-1} \circ g = e$

4. Kommutativität: $\forall g,h \in G$ gilt:
$g \circ h = h \circ g$

Sind die Eigenschaften 1. - 3. erfüllt, so ist G eine Gruppe. Ist zusätzlich die 4. Eigenschaft erfüllt, ist die Gruppe abelsch.

Definition 1.2: *Sei G eine Gruppe*

- *wenn $S \subseteq G$, dann bezeichnet $\langle S \rangle$ die von S erzeugte Untergruppe von G*

$$\langle S \rangle := \bigcap_{\substack{H \subset G \; UG \\ S \subset H}} H$$

  $\langle S \rangle$ ist die kleinste Untergruppe von G, die S enthält
  Die Elemente von S heißen Erzeuger von $\langle S \rangle$

- *G heißt zyklisch, falls $G = \langle g \rangle$ für ein $g \in G$ gilt. G wird also von einem Element erzeugt*

- *G heißt endlich erzeugt, wenn G von endlich vielen Elementen erzeugt wird, d.h. wenn $\exists S \subseteq G$ mit $G = \langle S \rangle$ und S endlich*

Beispiel 1.1:

- *($\mathbb{Z}$, +) ist eine unendliche abelsche Gruppe, die endlich erzeugt ist mit 1*[1]
- *($\mathbb{Q}$, +) ist abelsch aber nicht endlich erzeugt, dem wählt man $x_1, ..., x_s$ und $w \in \mathbb{N}$, sodass w teilerfremd zu den Nennern aller x_i ist, dann kann $\frac{1}{w}$ nicht als ganzzahlige Linearkombination von $x_1, ..., x_s$ dargestellt werden*

1.2 Endlich erzeugte Untergruppen von abelschen Gruppen

Sei S $\subseteq G$ eine Untergruppe der Gruppe G. Im Allgemeinen ist es schwer zu verstehen, wie die von S erzeugte Untergruppe, $\langle S \rangle$, aussieht. Im Falle von abelschen Gruppen ist die Beschreibung ihrer Gestalt jedoch recht einfach, da abelsche Gruppen die Struktur eines $\mathbb{Z}$-Moduls tragen.
Wir nehmen also nun an, dass G eine abelsche Gruppe ist und schreiben ihre Verknüpfung mit "+". Dann definiert man für $g \in G$ und $n \in \mathbb{N}$:

$$\begin{aligned} 0 \cdot g &= g \\ n \cdot g &= \underbrace{g + ... + g}_{\text{n-mal}} \\ (-n) \cdot g &= -(n \cdot g) \end{aligned} \tag{1.1}$$

Lemma 1.1: *Jede abelsche Gruppe wird mit der additiven Verknüpfung zu einem $\mathbb{Z}$-Modul*

Beweis: Man nennt G ein R-Modul, wobei R ein kommutativer Ring ist, wenn eine Operation (Skalarmultiplikation)

$$R \times G \to G, \quad (r, g) \mapsto r \cdot g$$

existiert, die folgendes erfüllt:

1. $r_1\ (r_2\ g) = (r_1\ r_2)\ g$	$r_1, r_2 \in R, \quad g \in G$
2. $(r_1 + r_2)\ g = r_1\ g + r_2\ g$	$r_1, r_2 \in R, \quad g \in G$
3. $r\ (g_1 + g_2) = r\ g_1 + r\ g_2$	$r \in R, \quad g_1, g_2 \in G$

Also ist zu zeigen, dass die Axiome für $z \in \mathbb{Z}$ und g $\in$ G gelten.
(1.1) impliziert:
$1 \cdot g = g$,

$m \cdot (n \cdot g) = (m \cdot n) \cdot g$	für $m, n \in \mathbb{Z}, \quad g \in G$
$(m + n) \cdot g = m \cdot g + n \cdot g$	für $m, n \in \mathbb{Z}, \quad g \in G$
$m \cdot (g + g') = m \cdot g + m \cdot g'$	für $m \in \mathbb{Z}, \quad g, g' \in G$

Betrachtet man die Axiome des R-Moduls, sieht man, dass sie äquivalent zu denen eines Vektorraums sind. Ein R-Modul kann also als Vektorraum über einem Ring aufgefasst werden.
Da die abelsche Gruppe G die Axiome erfüllt, wird sie zu einem $\mathbb{Z}$-Modul. □

Im folgenden Lemma wird nun die Gestalt einer endlich erzeugten Untergruppe einer abelschen Gruppe präsentiert, welche sofort aus der $\mathbb{Z}$-Modul Struktur folgt:

Lemma 1.2: *Sei G abelsch und $S \subseteq G$. Dann gilt:*

$$\langle S \rangle = \left\{ \sum\nolimits_{g \in S'} n_g g \mid S' \subseteq S \text{ endlich}, n_g \in \mathbb{Z} \right\}$$

Beweis: Bezeichne die rechte Seite der Gleichung mit H: H:= $\left\{ \sum_{g \in S'} n_g g \mid S' \subseteq S \text{ endlich}, n_g \in \mathbb{Z} \right\}$

[1] Der Beweis hierfür folgt im Abschnitt 1.3 Zyklische Gruppen

Man zeigt zuerst H $\subseteq \langle S \rangle$.
Nach Def. 1.2. ist S $\subseteq \langle S \rangle$, denn $\langle S \rangle$ ist die kleinste Untergruppe von G, die S enthält.
Da jede Untergruppe abgeschlossen bezüglich Addition und Inversenbildung ist, muss es neben g $\in$ S auch ng $\in \langle S \rangle$ für n $\in \mathbb{Z}$ geben.
Aus dem selben Grund muss $\langle S \rangle$ endliche Summen $\sum_{g \in S'} n_g g, S' \subseteq S$ enthalten. Da S endlich ist, gibt es auch nur endliche Summen. Das Element g taucht immer nur einmal auf.
Also folgt, dass H $\subseteq \langle S \rangle$
Da $\langle S \rangle$ allerdings die kleinste Gruppe ist, die S enthält, kann H nicht kleiner sein als die von S erzeugte Untergruppe von G. Es muss also gelten, dass H = $\langle S \rangle$

Es bleibt noch zu zeigen, dass H eine Untergruppe ist.
Prüfe Abgeschlossenheit bezüglich Addition und Inversenbildung:
Seien

$$h_1 = \sum\nolimits_{g \in S'}, n_g g \text{ und } h_2 = \sum\nolimits_{g \in S''} m_g g$$

zwei beliebige Elemente aus H, wobei S', S" $\subseteq$ S endlich sind.
Setze

$$n_g = 0 \text{ für } g \in S'' \backslash S' \text{ und } m_g = 0 \text{ für } g \in S' \backslash S''.$$

Dann ist:

$$h_1 + h_2 = \sum\nolimits_{g \in S' \cup S''} n_g \cdot g + \sum\nolimits_{g \in S' \cup S''} m_g \cdot g = \sum\nolimits_{g \in S' \cup S''} (n_g + m_g) \cdot g$$

$$-h_1 = -\sum\nolimits_{g \in S'} n_g \cdot g = \sum\nolimits_{g \in S'} (-n_g) \cdot g$$

Die obigen Gleichheiten folgen sofort aus der $\mathbb{Z}$-Modul Struktur der abelschen Gruppe G. Da $h_1 + h_2$ und $-h_1$ in H liegen, ist H eine Untergruppe. □

1.3 Zyklische Gruppen

Man betrachtet nun abelsche Gruppen, für die G = $\langle g \rangle$ mit g $\in$ G gilt, Die Gruppen werden also nur von einem Element erzeugt.

Aus Lemma 1.2 wissen wir, wie eine endlich erzeugte Untergruppe aussieht. Nun stellt sich die Frage, aus welchen Elementen eine zyklische Gruppe besteht.
Hierzu folgendes Lemma:

Lemma 1.3: $\langle g \rangle = \left\{ g^n | n \in \mathbb{Z} \right\}$, *wobei* $(G, *)$ *eine Gruppe ist und* $g \in G$ *gilt.*

Beweis: Man unterscheidet zwei Fälle:
1. endlicher Fall:
Sei G eine Gruppe mit *ord* $G = n$
Für n = 1 ist $\langle g \rangle = g \rightarrow \langle g \rangle = \{e\}$. Aufgrund der multiplikativen Verknüpfung ist $e = 1$
$\rightarrow \langle g \rangle = \{g^0\}$
Wenn $n > 1$, dann liegen folgende Elemente in $\langle g \rangle$:

$$e = g^0, g^1, ..., g^n, g^{n+1}, ...$$

Da G endlich ist, muss $g^k = g^l$ für bestimmte $k, l \in \mathbb{N}$ gelten.
Sei o. B. d. A. $k > l \rightarrow g^{k-l} = e$

Sei m die kleinste Zahl, für die $g^m = e$ gilt.
Wenn $i, j < m$ und $i \neq j \rightarrow g^i \neq g^j$, denn sonst wäre $g^{i-j} = g^0 = e$ ↯ Widerspruch zu $g^m = e$
Also folgt:

$$\langle g \rangle = \left\{ g^0, g^1, ..., g^{m-1} \right\} = \left\{ g^n \mid n \in \mathbb{N} \right\}$$

Andererseits ist G also die kleinste von g erzeugte Untergruppe, die G enthält.
Also ist $G = \langle g \rangle$ und $g^m = g^n = e$

2. unendlicher Fall:
G besteht in diesem Fall aus folgenden Elementen:

$$\langle g \rangle = \{..., g^{-n}, ..., g^{-1}, e, g^1, ..., g^n, ...\}$$

Wenn $g^i = g^j$ für $i \neq j$ folgt $g^{i-j} = e$.
Für $i - j = n$ erhält man eine endliche Untergruppe, die von g erzeugt wurde.
↯ Widerspruch zur Annahme, dass G unendlich ist
$\rightarrow \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ □

Lemma 1.4: *Jede zyklische Gruppe ist abelsch*

Bemerkung 1.4.1: *Die Umkehrung dieses Lemmas gilt nicht. Wir haben bereits gesehen, dass nicht jede abelsche Gruppe zyklisch ist.*

Beweis von Lemma 1.4: Sei G eine zyklische Gruppe
Aus Lemma 1.3 weiß man, dass

$$G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

Mit einer multiplikativen Verknüpfung folgt sofort für $n, m \in \mathbb{Z}$:

$$g^n g^m = g^{n+m} = g^m g^n$$

Somit ist die Gruppe G abelsch. □

Wir können also festhalten, dass endlich erzeugte Gruppen nicht abelsch sein müssen. Da mussten wir die Bedingung voraussetzen. Bei zyklischen Gruppen hingegen folgt die Kommutativität aber sofort.

In der folgenden Bemerkung wird die Darstellung der Gruppenelemente für eine zyklische Gruppe mit der additiven Verknüpfung vorgestellt.

Bemerkung 1.4.2: *Bei einer additiven Verknüpfung sieht $\langle g \rangle$ wie folgt aus:*
$\langle g \rangle = \{m \cdot g \mid m \in \mathbb{Z}\}$

Beispiel 1.2: *$\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$ sind zyklische Gruppen mit Erzeuger 1 bzw. der Restklasse $\bar{1}$ bei einer additiven Verknüpfung.*
Es ist offensichtlich, dass

$$\mathbb{Z} = \langle 1 \rangle = \{m \cdot 1 \mid m \in \mathbb{Z}\}$$

Betrachte für $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$ die Restklassen.
Restklasse: $\bar{a} = a + n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, ..., (n-1) + n\mathbb{Z}\}$

Man sieht leicht, dass $\bar{1}$ immer ein Erzeuger von $\mathbb{Z}/n\mathbb{Z}$ ist. An folgendem Zahlenbeispiel wird nun deutlich, dass es aber noch weitere Erzeuger geben kann.
Für $\mathbb{Z}/10\mathbb{Z}$ ist auch $\bar{a} \in \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$ ein Erzeuger, denn für $\bar{3}$ gilt z.B.:
$\mathbb{Z}/10\mathbb{Z} = \langle \bar{3} \rangle = \{10\mathbb{Z}, 3+10\mathbb{Z}, 6+10\mathbb{Z}, 9+10\mathbb{Z}, 2+10\mathbb{Z}, 5+10\mathbb{Z}, 8+10\mathbb{Z}, 1+10\mathbb{Z}, 4+10\mathbb{Z}, 7+10\mathbb{Z}\}$

Dieses Beispiel führt uns zu folgendem Satz:

Satz 1.1: *Erzeuger von der Gruppe $\mathbb{Z}/n\mathbb{Z}$ mit additiver Verknüpfung sind alle Restklassen, die teilerfremd zu n sind.*

Der Beweis ist eine Übung [2]

Satz 1.2: *Jede zyklische Gruppe ist isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$ für ein $n \in \mathbb{N}$*

Beweis: Sei G eine zyklische Gruppe mit Erzeuger $g \in G$ und additiver Verknüpfung, also $G = \langle g \rangle$.
Da G zyklisch ist, ist der Gruppenhomomorphismus

$$\Phi : \mathbb{Z} \rightarrow G, m \mapsto m \cdot g$$

[2] Die Lösung ist auf den Folien der Präsentation dieses Kapitels zu finden

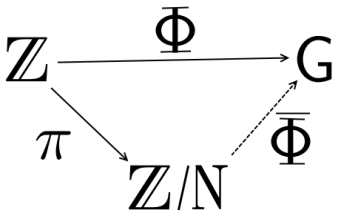
surjektiv.
Für den Kern gilt:

$$Ker\Phi = \{m \in \mathbb{Z} \mid \Phi(m) = e\} \subset \mathbb{Z},$$

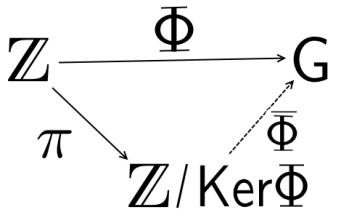
wobei e das neutrale Element von G ist.
Da KerΦ eine Untergruppe von $\mathbb{Z}$ ist und $\mathbb{Z}$ ein Hauptidealring ist[3], gilt:

$$Ker\Phi = n\mathbb{Z} \text{ für ein } n \in \mathbb{N} \quad Ker\Phi \text{ ist ein Ideal}$$

Man erinnere sich an den Homomorphiesatz:



KerΦ ist ein Normalteiler von $\mathbb{Z}$.[4] Somit kann der Normalteiler im Homomorphiesatz, wie folgt, durch KerΦ ersetzt werden:



Der Homomorphiesatz besagt, dass $\mathbb{Z}/Ker\Phi \cong Bild\Phi$[5]
Betrachte im Folgenden also den Kern:

$Ker\Phi = n\mathbb{Z}$
1. $n = 0 : Ker\Phi = 0 \rightarrow$ neutrales Element von G ist 0.
Da der Kern trivial ist, ist Φ bijektiv, also muss $G \cong \mathbb{Z}$ sein.
2. $n \geq 1 : Ker\Phi = n\mathbb{Z}$. Mit dem Homomorphiesatz folgt sofort, dass $\bar{\Phi} : \mathbb{Z}/n\mathbb{Z} \rightarrow G$ ein kanonischer Isomorphismus ist.
$\rightarrow G \cong \mathbb{Z}/n\mathbb{Z}$ □

Übung 1.1: *Sind die Gruppen* $(\mathbb{Z}/5\mathbb{Z})^*$ *bzw.* $(\mathbb{Z}/8\mathbb{Z})^*$ *zyklisch?* [6]

1.4 Darstellung von endlich erzeugten abelschen Gruppen

In diesem Abschnitt werden endlich erzeugte abelsche Gruppen betrachtet. Wir verwenden nun die Darstellung von G als $\mathbb{Z}$-Modul, wobei G abelsch ist, damit wir besser mit der Gruppe arbeiten können.
G hat im Folgenden also endlich viel Erzeuger $g_1, ..., g_k$, welche als k-Tupel geschrieben werden können:

$$S = (g_1, ..., g_k) \rightarrow G = \langle S \rangle$$

1.4.1 Erste einfache Darstellungsmöglichkeit einer endlich erzeugten abelschen Gruppe

Anhand der $\mathbb{Z}$-Modul Struktur definieren wir folgenden surjektiven Gruppenhomomorphismus:

$$\varphi_S : \mathbb{Z}^k \rightarrow G, \quad (m_1, ..., m_k) \mapsto \sum_{i=1}^{k} m_i g_i$$

[3] beide Aussagen wurden bereits in der Algebra Vorlesung bewiesen
[4] den Beweis findet man im Algebra Skript
[5] vgl. Korollar 2.2 aus dem Algebra Skript
[6] die Lösung ist auf den Folien der Präsentation dieses Kapitels zu finden

Definition 1.3: *Die Elemente des Kerns von φ_S heißen* ***Relationen*** *der Erzeuger S.*

Der Kern der oben definierten Abbildung ist immer endlich erzeugt[7], weshalb wir annehmen können, dass nun $r_1, ..., r_l$ Erzeuger des Kerns seien:

$$\langle r_1, ..., r_l \rangle = Ker\varphi_S = \{(m_1, ..., m_k) \in \mathbb{Z}^k \mid \varphi_S(m) = e_G\} \subset \mathbb{Z}^k$$

Wenn man $r_1, ..., r_l$ als Spalten schreibt, erhält man eine Matrix $R = (r_1\ r_2 ... r_l)$
R hat k Zeilen und l Spalten und repräsentiert eine Abbildung:

$$R : \mathbb{Z}^l \to \mathbb{Z}^k$$

Hieraus ergibt sich nun folgende Darstellungsmöglichkeit der Gruppe G:

$$\mathbb{Z}^l \xrightarrow{\mathrm{R}} \mathbb{Z}^k \xrightarrow{\mathrm{S}} G$$

Beispiel 1.3: *Betrachte* $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{1})\}$

$$S_1 = ((\bar{1}, \bar{0})\ (\bar{0}, \bar{1}))$$
$$S_2 = ((\bar{1}, \bar{0})\ (\bar{0}, \bar{1})\ (\bar{1}, \bar{1}))$$
$$S_3 = ((\bar{1}, \bar{0})\ (\bar{1}, \bar{1}))$$

sind 3 verschiedene Erzeugendensysteme von G.
Wir betrachten nun jeweils die Kerne:
Für S_1 gilt:

$$\varphi_{S_1} : \mathbb{Z}^2 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad (m_1, m_2) \mapsto m_1 \cdot (\bar{1}, \bar{0}) + m_2 \cdot (\bar{0}, \bar{1})$$

Für den Kern gilt dann:

$$Ker\varphi_{S_1} = \{(m_1, m_2) \in \mathbb{Z}^2 \mid m_1 \cdot (\bar{1}, \bar{0}) + m_2 \cdot (\bar{0}, \bar{1}) = \{2\mathbb{Z}\} \times \{2\mathbb{Z}\}\} = \langle (2, 0), (0, 2) \rangle$$

Man erhält also folgende Darstellung von G:

$$\mathbb{Z}^2 \xrightarrow{\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}} \mathbb{Z}^2 \xrightarrow{((\bar{1},\bar{0})\ (\bar{0},\bar{1}))} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Im Folgenden wird die Darstellung von G präsentiert, wenn man S_2 bzw. S_3 betrachtet.
Für S_2 gilt:

$$\varphi_{S_2} : \mathbb{Z}^3 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad (m_1, m_2, m_3) \mapsto m_1 \cdot (\bar{1}, \bar{0}) + m_2 \cdot (\bar{0}, \bar{1}) + m_3 \cdot (\bar{1}, \bar{1})$$

und für S_3 gilt:

$$\varphi_{S_3} : \mathbb{Z}^2 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad (m_1, m_2) \mapsto m_1 \cdot (\bar{1}, \bar{0}) + m_2 \cdot (\bar{1}, \bar{1})$$

Wählt man passende Erzeuger der Kerne dieser Abbildungen, so ergeben sich folgende Darstellungen der Gruppe G:

$$\mathbb{Z}^3 \xrightarrow{\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}} \mathbb{Z}^3 \xrightarrow{((\bar{1},\bar{0})\ (\bar{0},\bar{1})\ (\bar{1},\bar{1}))} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}^2 \xrightarrow{\begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix}} \mathbb{Z}^2 \xrightarrow{((\bar{1},\bar{0})\ (\bar{1},\bar{1}))} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Wir können anhand dieses Beispiels gut sehen, dass die Darstellung einer endlich erzeugten abelschen Gruppe nicht eindeutig ist. Sie ist abhängig von der Wahl des Erzeugendensystems.

[7] Der Beweis hierfür folgt in Lemma 1.5

Satz 1.3: *Es gilt:* $G \cong \mathbb{Z}^k/Ker\varphi_S = \mathbb{Z}^k/Im\ R$

Beweis: Für den Beweis verwendet man die Aussage des Homomorphiesatzes:
Da

$$\bar{\varphi_S} : \mathbb{Z}^k/Ker\varphi_S \to G$$

ein kanonischer Isomorphismus ist und $Ker\varphi_S$ ein Normalteiler, gibt es folgende Isomorphie:
$\mathbb{Z}^k/Ker\varphi_S \cong G$ (vgl. Bew. von Satz 1.2)
$Ker\varphi_S$ wird von $r_1, ..., r_l$ erzeugt $\to Ker\varphi_S$= Im R □

Übung 1.2: *Wie sieht die Darstellung von* $\mathbb{Z}$ *bzw.* $\mathbb{Z}/n\mathbb{Z}$ *aus, wenn man als Erzeuger 1 bzw.* $\bar{1}$ *wählt?* [8]

Lemma 1.5: *Jede Untergruppe von* $\mathbb{Z}^k$ *ist endlich erzeugt.*

Beweis: Sei $H \subseteq \mathbb{Z}^k$.
Beweisführung per Induktion nach k.
$k = 0 \to$ trivial $\to \mathbb{Z}^0 = \{0\}$
$k > 0$: Betrachte folgende Projektion auf die letzte Komponente:

$$\pi : \mathbb{Z}^k \to \mathbb{Z}, \quad (z_1, ..., z_k) \mapsto z_k$$

IA: $k = 1 : H \subseteq \mathbb{Z}$. H ist dann ein Ideal
Da $\mathbb{Z}$ Hauptidealring ist $\to H = n\mathbb{Z}$ für ein $n \in \mathbb{N}$
Somit wird H endlich erzeugt und ist sogar zyklisch, denn mit additiver Schreibweise gilt: H=$\langle n \rangle$

Induktionsannahme: Jede Untergruppe von $\mathbb{Z}^{k-1}$ ist endlich erzeugt.

IS: $k - 1 \to k$:
Es gilt $\pi(H) \subseteq \mathbb{Z}$, denn $\pi(\mathbb{Z}^k) = \mathbb{Z}$. Da $\mathbb{Z}$ Hauptidealring ist und $\pi(H)$ Ideal von $\mathbb{Z}$, folgt:
$\pi(H) = n\mathbb{Z}$ für ein $n \in \mathbb{N}$
Sei nun

$$\pi^{-1}(n) = g \in H \leftrightarrow g \in \pi^{-1}(n) \cap H$$

und

$$H' = H \cap \mathbb{Z}^{k-1} \times \{0\} = \{(z_1, ..., z_k) \in H \mid z_k = 0\}$$

Also ist $H' \cong \{(z_1, ..., z_{k-1}) \in \mathbb{Z}^{k-1} \mid \exists z_k = 0 : (z_1, ..., z_{k-1}, z_k) \in H\} \subseteq \mathbb{Z}^{k-1}$
Nach IA ist H' endlich erzeugt. Stelle nun folgende Behauptung auf:

Beh.: g erzeugt zusammen mit den Erzeugern von H' die Untergruppe $H \subseteq \mathbb{Z}^k$

Beweis: Es ist zu zeigen, dass $\forall h \in H\ \exists\ l \in \mathbb{Z}$ mit $h - lg \in H'$
Wenn das bewiesen ist, wird H von g zusammen mit den Erzeugern von H' erzeugt.
Es gilt $\pi(h) \in \pi(H) = n\mathbb{Z} \to \pi(h) = l \cdot n = l \cdot \pi(g)$, für ein $l \in \mathbb{Z}$
$n = \pi(g)$ gilt wegen $g \in \pi^{-1}(n) \cap H$
Betrachte nun

$$\pi(h - lg) = \pi(h) - l \cdot \pi(g)$$

und setze

$$m := \pi(h) \in n\mathbb{Z}, \quad l = m/n$$

Das liefert: $\pi(h) - l \cdot \pi(g) = m - l \cdot n = m - m/n \cdot n = 0$
Also muss $h - lg \in Ker\pi \cap H = H'$ gelten. □

1.4.2 Vereinfachte Darstellung einer endlich erzeugten abelschen Gruppe durch Transformation des Erzeugendensystems

In diesem Abschnitt wird die eben eingeführte Relationenmatrix etwas genauer betrachtet. Man kann sich überlegen, R auf besonders einfach Form, durch geschickte Wahl der Erzeuger von G, zu

[8] die Lösungen stehen auf den Folien der Präsentation dieses Kapitels

bringen.

Wenn $(g_1, ..., g_k) = S$ Erzeuger von G sind, sind auch

- $(g_1, ..., g_i + \lambda g_j, ..., g_k)$ für $\lambda \in \mathbb{Z}, i \neq j$
- $(g_1, ..., -g_i, ..., g_k)$
- $(g_{\pi(1)}, ..., g_{\pi(k)})$ für eine Permutation $\pi \in Perm(k)$

Erzeuger von G.

Diese Operationen heißen Elementaroperationen. Sie werden durch die Rechtsmultiplikation von Matrizen an den Zeilenvektor S beschrieben. Die drei Elementarmatrizen lassen sich wie folgt definieren:

- $E_{ij}(\lambda) = (a_{v\mu})$ mit $a_{ij} = \lambda$ und $a_{v\mu} = \delta_{v\mu}$ sonst
  = Einheitsmatrix mit zusätzlichen λ auf (i, j) mit $i \neq j$
- $E_i = (b_{v\mu})$ mit $b_{ii} = -1$ und $b_{v\mu} = \delta_{v\mu}$ sonst
  = Einheitsmatrix mit -1 als i-tes Diagonalelement
- $P(\pi) = (b_{v\mu})$ mit $b_{v\mu} = \delta_{\pi(v)\mu}$
  = Matrix, bei der in v-ter Zeile an $\pi(v)$-ter Stelle eine 1 steht und sonst nur 0

Die obigen drei transformierten Erzeugendensyteme können also durch Rechtsmultiplikation von $E_{ji}(\lambda), E_i$ und $P(\pi^{-1})$ an S beschreiben werden.

Beispiel 1.4: *Betrachte ein allgemeines Erzeugendensytem aus 3 Elementen:*
$S = (g_1, g_2, g_3)$
1. $SE_{ji}(\lambda)$*, wobei* $i = 2, j = 3$

$$\rightarrow (g_1, g_2, g_3) \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \lambda & 1 \end{pmatrix} = (g_1, g_2 + \lambda g_3, g_3)$$

2. SE_i*, wobei* $i = 3$

$$\rightarrow (g_1, g_2, g_3) \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = (g_1, g_2, -g_3)$$

3. Setze $\pi(1) = 2, \pi(2) = 3, \pi(3) = 1$
Da wir mit Spalten multiplizieren, wird π^{-1} *benutzt*
$\rightarrow \pi^{-1}(1) = 2 \leftrightarrow \pi(2) = 1, \pi^{-1}(2) = 3 \leftrightarrow \pi(3) = 2,$
$\pi^{-1}(3) = 1 \leftrightarrow \pi(1) = 3$

$$\rightarrow (g_1, g_2, g_3) \cdot \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = (g_2, g_3, g_1) = (g_{\pi(1)}, g_{\pi(2)}, g_{\pi(3)})$$

Wenn sich S zu SE ändert, müssen sich dadurch auch die Erzeuger des Kerns ändern.
Die Änderung kann durch $E^{-1}R$ beschrieben werden.

Bemerkung 1.4.3: *Es gilt:* $(E_{ij}(\lambda))^{-1} = E_{ij}(-\lambda), (E_i)^{-1} = E_i$
$(P(\pi))^{-1} = P(\pi^{-1})$

Man erhält folgende Darstellung für G:

$$\mathbb{Z}^l \xrightarrow{E^{-1}R} \mathbb{Z}^k \xrightarrow{SE} G$$

Diese Darstellung führt uns zu folgendem abschließenden Lemma:

Lemma 1.6: *Sei* $\mathbb{Z}^l \xrightarrow{R} \mathbb{Z}^k \xrightarrow{S} G$ *eine beliebige Darstellung einer endlich erzeugten abelschen Gruppe G.*
Falls E, E' Elementarmatrizen der Größe k bzw. l sind, dann ist auch

$$\mathbb{Z}^l \xrightarrow{ERE'} \mathbb{Z}^k \xrightarrow{SE^{-1}} G$$

eine Darstellung von G.

Beweis: Sei $S = (g_1, ..., g_k)$ ein Erzeugendensystem von G. Wie oben gezeigt, ist dann auch SE^{-1} ein Erzeugendensystem von G.
Die Spalten $r_1, ..., r_l$ erzeugen $Ker\varphi_S$. Also:

$$\varphi_S(r_j) = \sum\nolimits_{i=1}^{k} r_{ij} g_i = 0 \text{ für } 0 \leq j \leq l$$

Man kann dies als inneres Produkt von S und r_j auffassen:

$$S \cdot r_j = 0 = S \cdot \underbrace{E^{-1} \cdot E}_{\text{I}} \cdot r_j$$

$\rightarrow$ Der Wechsel von S zu SE^{-1} erfordert einen Wechsel von R zu ER

Wenn wir zudem Elementaroperationen von rechts durchführen, ändert sich das Erzeugnis von R nicht. Bezeichnet man diese Matrix mit E', dann kann man R einfach zu RE' ändern. Es folgt:

$$\mathbb{Z}^l \xrightarrow{ERE'} \mathbb{Z}^k \xrightarrow{SE^{-1}} G$$

Die Behauptung folgt. □

Kapitel 2

Endlich erzeugte abelsche Gruppen II

Im zweiten Teil dieser Vortragsreihe wird sich detaillierter mit der, im ersten Teil eingeführten, Darstellung einer endlich erzeugten abelschen Gruppe befasst. Das Augenmerk richtet sich hierbei auf die bereits definierte Relationenmatrix und mögliche Vereinfachungen auf Diagonalform mithilfe eines Diagonalisierungsalgorithmus.
Ziel ist es, mithilfe des Hauptsatzes über endlich erzeugte abelsche Gruppen, und daraus folgender Korollare, den Isomorphietyp der jeweiligen endlich erzeugten abelschen Gruppe zu bestimmen. Dieser ist ein direktes Produkt aus den additiven Gruppen $\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$.

2.1 Transformation der Relationenmatrix in Diagonalform

Dies ist die bereits bekannte Darstellung einer endlich erzeugten abelschen Gruppe:

$$\mathbb{Z}^l \xrightarrow{\mathrm{R}} \mathbb{Z}^k \xrightarrow{\mathrm{S}} G$$

Lemma 1.6 (Kapitel 1.4.2) besagt, dass ein Umformung von R durch Rechts- und Linksmultiplikationen von Elementarmatrizen zwar die Relationenmatrix sowie die Erzeuger von G ändert, sich jedoch wieder eine Darstellung von G ergibt:

$$\mathbb{Z}^l \xrightarrow{ERE'} \mathbb{Z}^k \xrightarrow{SE^{-1}} G$$

Diese Aussage wird sich im Folgenden zu Nutze gemacht, um das Ablesen des jeweiligen Isomorphietyps zu ermöglichen. Hierzu wird die Relationenmatrix R in Diagonalform transformiert.
Diese Transformation ist hierbei ausreichend, da aus Satz 1.3 (Kapitel 1.4.1) folgt, dass sich der Isomorphietyp alleine aus R ablesen lässt.

2.1.1 Der Diagonalisierungsalgorithmus

Man möchte die Relationenmatrix R in möglichst einfacher Form vorliegen haben.
Die naheliegendste einfache Form ist in diesem Fall die Diagonalform.
Man sucht also nach einem universellen 'Kochrezept' um R umzuformen.
Im Folgenden betrachten wir deshalb einen Algorithmus, der aus R durch Links- und Rechtsmultiplikation mit Elementarmatrizen (siehe Kapitel 1.4.2) eine Diagonalmatrix macht.

R hat also nach Anwendung des Algorithmus folgende Form:

$$R = \left(\begin{array}{ccc|c} n_1 & & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & n_r & 0 \\ \hline 0 & \cdots & 0 & 0 \end{array}\right)$$

Zur Erinnerung:

R hat k Zeilen und l Spalten
$\rightarrow$ R muss nicht symmetrisch sein
$\rightarrow$ Anzahl der Nullzeilen $\neq$ Anzahl der Nullspalten ist möglich.

Algorithmus 2.1:

Wichtig: Während des Algorithmus werden immer wieder schon fertige Zeilen und Spalten an den Rand getauscht und in den weiteren Durchläufen des Algorithmus nicht mehr betrachtet. Die jeweils verbleibende Matrix wird als Restmatrix bezeichnet
Zu Beginn: Ganz R ist die Restmatrix, d.h. die komplette Matrix R wird im 1. Durchlauf betrachtet.

Schritt 1:
Prüfe die Restmatrix auf Nullzeilen bzw. Nullspalten. Wenn es welche gibt, tausche diese an den unteren bzw. rechten Rand der Matrix.

Schritt 2:
Prüfe die Restmatrix auf eine Position (i_o, j_o) *in der Restmatrix mit* $r_{i_o j_0} \neq 0$, *aber* $r_{i_o j} = 0$ $\forall j \neq j_0$ *und* $r_{i j_0} = 0$ $\forall i \neq i_0$.
Wenn es eine solche Position gibt, dann tausche die i_0*-te Zeile mit der ersten Zeile der Restmatrix und die* j_0*-te Spalte mit der ersten Spalte der Restmatrix.*
Vergesse diese neue erste Zeile und Spalte der Restmatrix und wiederhole diesen Schritt so oft wie möglich.

Schritt 3:
Prüfe ob nach Schritt 2 *noch eine Restmatrix übrig ist.*
Wenn nicht, dann ist der Algorithmus beendet und R ist in Diagonalform umgeformt.
Wenn es noch eine Restmatrix gibt, gehe weiter zu Schritt 4.

Schritt 4:
Suche in der Restmatrix das Element $r_{i_o j_0}$ *mit dem kleinsten Betrag ungleich Null.*
Führe dann folgende Berechnungen durch:

1. *Für jede Zeile* $i \neq i_0$ *der Restmatrix berechne* q_i *durch Division mit Rest* $r_{i j_0} = q_i r_{i_o j_0} + r'_{i j_o}$ *mit* $0 \leq r'_{i j_0} < r_{i_o j_0}$, *und subtrahiere das* q_i*-fache der* i_0*-ten Zeile von der* i*-ten Zeile.*

2. *Für jede Spalte* $j \neq j_0$ *der Restmatrix berechne* q_j *durch Division mit Rest* $r_{i_o j} = q_j r_{i_o j_0} + r'_{i_o j}$ *mit* $0 \leq r'_{i_o j} < r_{i_o j_0}$, *und subtrahiere das* q_j*-fache der* j_0*-ten Spalte von der* j*-ten Spalte.*

Schritt 5:
Beginne erneut bei Schritt 1.

zu beweisen:

1. Algorithmus liefert eine Diagonalmatrix.
2. Algorithmus terminiert.

Beweis:

zu 1.: Ist klar nach Definition des Algorithmus.
zu 2.: Um zu beweisen, dass der Algorithmus terminiert, nehmen wir an, dass bei jedem Erreichen von Schritt 3 (ab dem 2. Durchlauf) entweder:

- Verkleinerung der Restmatrix oder

- Minimierung des Minimums der Beträge ($\neq 0$) der Restmatrix.

Beides wird durch natürliche Zahlen beschrieben, deshalb muss der Algorithmus zwangsläufig terminieren.
Wir müssen also nur noch zeigen, dass unsere Annahme stimmt:
Betrachte hierzu Schritt 4.
Vor der Ausführung des Schrittes ist das Minimum der Beträge ($\neq 0$) $|r_{i_0 j_0}|$. Nun führen wir Divisionen mit Rest bezüglich $r_{i_0 j_0}$ durch. Die einzige Möglichkeit, wie das Minimum der Beträge ($\neq 0$) dabei nicht sinken kann, ist, dass alle Einträge in r_{ij_0} und $r_{i_0 j}$ glatt durch $r_{i_0 j_0}$ teilbar sind, also r'_{ij_0} und $r'_{i_0 j}$ Null sind. Dann erfüllt die Position (i_0, j_0) aber die Voraussetzungen für Schritt 2 und nach Ausführung dessen hat sich die Restmatrix um eine Zeile und eine Spalte verkleinert.
$\Rightarrow$ Beh. $\square$

Beispiel:

Wende den Algorithmus auf folgende Matrix an. Schritte, bei denen sich nichts ändert sind nicht aufgeschrieben und die jeweilige Schrittnummer ist vermerkt. Zudem ist das wichtigste Element unterstrichen.

$$\begin{pmatrix} 8 & 15 & 23 \\ -16 & 18 & -4 \\ 0 & 15 & 15 \\ 16 & -30 & -14 \end{pmatrix}$$

$$\begin{pmatrix} 8 & 15 & 23 \\ -16 & 18 & \underline{-4} \\ 0 & 15 & 15 \\ 16 & -30 & -14 \end{pmatrix} \xrightarrow{4.1} \begin{pmatrix} -72 & 105 & 3 \\ -16 & 18 & \underline{-4} \\ -48 & 69 & 3 \\ 80 & -102 & 2 \end{pmatrix} \xrightarrow{4.2} \begin{pmatrix} -84 & 117 & 3 \\ 0 & \underline{2} & -4 \\ -60 & 81 & 3 \\ 72 & -94 & 2 \end{pmatrix} \xrightarrow{4.1} \begin{pmatrix} -84 & 1 & 235 \\ 0 & \underline{2} & -4 \\ -60 & 1 & 163 \\ 72 & 0 & -186 \end{pmatrix}$$

$$\xrightarrow{4.2} \begin{pmatrix} -84 & \underline{1} & 237 \\ 0 & 2 & 0 \\ -60 & 1 & 165 \\ 72 & 0 & -186 \end{pmatrix} \xrightarrow{4.1} \begin{pmatrix} -84 & \underline{1} & 237 \\ 168 & 0 & -474 \\ 24 & 0 & -72 \\ 72 & 0 & -186 \end{pmatrix} \xrightarrow{4.2} \begin{pmatrix} 0 & \underline{1} & 0 \\ 168 & 0 & -474 \\ 24 & 0 & -72 \\ 72 & 0 & -186 \end{pmatrix} \xrightarrow{2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 168 & -474 \\ 0 & \underline{24} & -72 \\ 0 & 72 & -186 \end{pmatrix}$$

$$\xrightarrow{4.1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 30 \\ 0 & \underline{24} & -72 \\ 0 & 0 & 30 \end{pmatrix} \xrightarrow{4.2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 30 \\ 0 & \underline{24} & 0 \\ 0 & 0 & 30 \end{pmatrix} \xrightarrow{2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 24 & 0 \\ 0 & 0 & \underline{30} \\ 0 & 0 & 30 \end{pmatrix} \xrightarrow{4.1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 24 & 0 \\ 0 & 0 & 30 \\ 0 & 0 & 0 \end{pmatrix}$$

Unsere Matrix liegt nun in Diagonalform vor.

Wir werden dieses Beispiel später erneut aufgreifen und die weiteren Erkenntnisse des Kapitels daran verdeutlichen.

2.2 Hauptsatz über endlich erzeugte abelsche Gruppen

Nachdem wir uns mit der Umformung von R in Diagonalform beschäftigt haben und einen universellen Weg kennen, kommen wir nun zurück zum Isomorphietyp der dargestellten Matrix und wie sich dieser anhand der Diagonalmatrix ablesen lässt.
Hierzu greifen wir nun Satz 1.3 aus Kapitel 1 wieder auf.

Dieser sagt uns, dass $G \cong \mathbb{Z}^k/Ker\varphi_S = \mathbb{Z}^k/Im\ R$.
Die Berechnung dieses Kokerns ist trivial und direkt aus der Diagonalmatrix ablesbar.
Dies verdeutlicht der nächste Hilfssatz:

Hilfssatz 2.2:

Falls $\mathbb{Z}^l \xrightarrow{R} \mathbb{Z}^k \xrightarrow{S} G$ *eine Darstellung einer endlich erzeugten ablschen Gruppe* G *ist und*

$$R = \left(\begin{array}{ccc|c} n_1 & & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & n_r & 0 \\ \hline 0 & \cdots & 0 & 0 \end{array}\right)$$

dann ist G isomorph zu

$$\mathbb{Z}^{k-r} \times \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$$

.

Nehmen wir jetzt diesen Hilfssatz und kombinieren ihn mit unserem Diagonalisierungsalgorithmus erhalten wir den angestrebten Hauptsatz:

Satz 2.3 (Hauptsatz über endlich erzeugte abelsche Gruppen):

Jede endlich erzeugte abelsche Gruppe ist isomorph zu einem endlichen Produkt von zyklischen Gruppen.

weiter Beispiel:

In unserem zuvor betrachteten Beispiel führt dies dazu das:

$$G \cong \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}$$

$\mathbb{Z}/1\mathbb{Z}$ *wird hierbei nicht aufgeschrieben da dies die triviale Gruppe ist.*

2.3 Weitere Varianten des Hauptsatzes

Im folgenden Abschnitt werden wir uns mit zwei Korollaren beschäftigen, bei denen es sich um Umformulierungen des Hauptsatzes handelt.
Für das erste Korollar benöten wir den Chinesischen Restsatz, deshalb wiederholend:

Chinesischer Restsatz (in $\mathbb{Z}$):

Seien $m, n \in \mathbb{Z}\backslash\{0\}$ *teilerfremd. Dann gilt* $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Korollar 2.4:

Jede endlich erzeugte abelsche Gruppe G *ist isomorph zu*

$$\mathbb{Z}^r \times \prod_{j=1}^{s} \prod_{i=1}^{s_j} \mathbb{Z}/p_j^{r_{ji}}\mathbb{Z}$$

für geeignete Primzahlen $p_j \in \mathbb{P}$ *und natürliche Zahlen* $r, s \in \mathbb{N}_0; s_j, r_{ji} \in \mathbb{N}$.
Die Zahl r *(der* Rang *der abelschen Gruppe* G*), sowie die Gruppen* $\mathbb{Z}/p_j^{r_{ji}}\mathbb{Z}$ *sind bis auf Reihenfolge eindeutig.*

Beweis:

Nach dem Hauptsatz (Satz 2.3) ist $G \cong \mathbb{Z}^r \times \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$
(r Anzahl der Nullzeilen (im Hilfssatz 2.2 $k - r$)).
Falls $n_i = \prod_{j=1}^{l_i} p_j^{r_{ji}}$ (Primfaktorzerlegung der n_i), dann ist nach dem Chinesischen Restsatz

$$\mathbb{Z}/n_i\mathbb{Z} \cong \prod_{j=1}^{l_i} \mathbb{Z}/p_j^{r_{ji}}\mathbb{Z}$$

Nach Umsortieren der Faktoren ist die Existenz der Zerlegung offensichtlich.

Noch zu zeigen: Eindeutigkeit.

Dazu: Nehme eine Primzahl p, die nicht in der Menge $\{p_1, ..., p_s\}$ vorkommt, dann ist die Multiplikation mit p ein Isomorphismus auf den Gruppen $\mathbb{Z}/p_j^{r_{ji}}\mathbb{Z}$.
Daraus folgt:

$$G/pG \cong (\mathbb{Z}/p\mathbb{Z})^r$$

und damit ist r festgelegt.
Nun beobachte, dass für jedes j gilt

$$G_j := \{g \in G \mid \exists n \in \mathbb{N}_0 : ord g = p_j^n\} \cong \prod_{i=1}^{s_j} \mathbb{Z}/p_j^{r_{ji}}\mathbb{Z}$$

.
Seien die r_{ji} durch $r_{j1} \geq r_{j2} \geq ... \geq r_{r_j s_j}$ geordnet.
Nun führe Induktionsbeweis nach r_{j1} durch:
$r_{j1} = 1$:
G_j ist ein $(\mathbb{Z}/p_j\mathbb{Z})$-Vektorraum der Dimension s_j und muss daher aus s_j Kopien von $\mathbb{Z}/p_j\mathbb{Z}$ bestehen.
Für $r_j 1 > 1$ betrachten wir

$$p_j G_j \cong \prod_{i=1}^{s_j} p_j\mathbb{Z}/p_j^{r_{ji}}\mathbb{Z} \cong \prod_{i=1}^{s_j} \mathbb{Z}/p_j^{r_{ji}-1}\mathbb{Z}$$

($\mathbb{Z}/p^0\mathbb{Z} = \mathbb{Z}/\mathbb{Z} = 0$ die triviale Gruppe)
Wende nun die Induktionsvoraussetzung auf $p_j G_j$ an, daraus folgt dann direkt die Eindeutigkeit der Faktoren $\mathbb{Z}/p_j^{r_{ji}-1}\mathbb{Z}$ in $p_j G_j$ und damit auch die Eindeutigkeit der Faktoren $\mathbb{Z}/p_j^{r_{ji}}\mathbb{Z}$ in G_j sowie G. □

Korollar 2.5:

Jede endlich erzeugt abelsche Gruppe G ist isomorph zu

$$\mathbb{Z}^r \times \prod_{i=1}^{l} \mathbb{Z}/n_i\mathbb{Z}$$

für geeignete natürliche Zahlen $n_i \geq 2$ mit $n_{i+1} \mid n_i$ für $i = 1, ..., l-1$ und $r \in \mathbb{N}_0$.
Die Zahlen n_i sind eindeutig bestimmt und heißen Elementarteiler.
Diese Form nennt man Smith-Normalform.

Beweis:

Annahme: G ist ein Produkt wie in Korollar 2.4.
OBdA nehme an, dass die r_{ji} für festes j absteigend sortiert sind (d.h. $r_{j1} \geq r_{j2} \geq r_{j3} \geq ...$).
Setze $n_i = \prod_{j=1}^{s} p_j^{r_{ji}}$, wobei $r_{ji} = 0$ für $i > s_j$.

Dann gilt $n_{i+1} \mid n_i$ offensichtlich aufgrund der Sortierung der r_{ji}.
Dass G isomorph zu $\mathbb{Z}^r \times \prod_{i=1}^{l} \mathbb{Z}/n_i\mathbb{Z}$ ist, folgt erneut aus dem chinesischen Restsatz.
Die Eindeutigkeit der n_i wird ähnlich gezeigt wie im Beweis zu Korollar 2.4 (mit Induktion über n_l) und wird deshalb hier nicht genauer erläutert. □

weiter Beispiel:

Kommen wir erneut zurück auf unser Beispiel.
Wir hatten gefunden, dass

$$G \cong \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}$$

.
Nun müssen wir die Primfaktorzerlegungen von 24 und 30 bestimmen.

$$24 = 2^3 \cdot 3 \qquad 30 = 2 \cdot 3 \cdot 5$$

Mit Korollar 2.4 folgt dann:

$$G \cong \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

Möchte man nun die Darstellung wie in Korollar 2.5 haben, dann fasst man die Faktoren analog zum Vorgehen im Beweis des Korollars zusammen:

$n_1 = 2^3 \cdot 3 \cdot 5 = 120$ *und* $n_2 = 2 \cdot 3 = 6$

Daraus folgt dann, dass

$$G \cong \mathbb{Z}/120\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

Nun ist unser Beispiel abgeschlossen und wir haben drei verschiedene Darstellungen des Isomorphietyps einer endlichen abelschen Gruppe gesehen, zu welcher die anfangs diagonalisierte Matrix gehört.

Wir haben nun also in diesem Kapitel bewiesen, dass jede endlich erzeugte abelsche Gruppe ein direktes Produkt aus den additiven Gruppen $\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$ ist und unser Ziel damit erreicht.
Mithilfe der beiden Korollare haben wir zudem verschiedene Möglichkeiten gesehen, dieses Produkt darzustellen.

2.4 Beispielaufgaben

Aufgabe 1

Sei G eine endlich erzeugte abelsche Gruppe mit einer Darstellung der Form $\mathbb{Z}^5 \xrightarrow{R} \mathbb{Z}^5 \xrightarrow{S} G$,wobei

$$R = \begin{pmatrix} 2 & 2 & -8 & -6 & 10 \\ 2 & 8 & -2 & -6 & 22 \\ 2 & 26 & 1756 & -126 & 688 \\ -6 & -6 & -96 & 48 & -30 \\ 10 & 22 & 392 & -30 & 284 \end{pmatrix}$$

1. *Bestimme $r, l \in \mathbb{N}_0$ und $n_1, ..., n_l \in \mathbb{N}$ mit $n_{i+1} \mid n_i$ für $1 \leq i \leq l-1$,*
   so dass $G \cong \mathbb{Z}^r \times \prod_{i=1}^{l} \mathbb{Z}/n_i\mathbb{Z}$.
   (wende Korollar 2.5 an)

2. *Bestimme $r, s \in \mathbb{N}_0$, $s_j, r_{ji} \in \mathbb{Z}$ und Primzahlen p_j,*
   so dass $G \cong \mathbb{Z}^r \times \prod_{j=1}^{s} \prod_{i=1}^{s_j} \mathbb{Z}/p_j^{r_{ji}}\mathbb{Z}$.
   (wende Korollar 2.4 an)

Hinweis:

Bearbeite zuerst 2. und forme dann mithilfe des Beweises von Korollar 2.5 zu 1. um.

Lösung:

Wir diagonalisieren zuerst die Matrix R:
(Schritte, bei denen sich nichts ändert sind nicht aufgeschrieben und die jeweilige Schrittnummer ist vermerkt. Zudem ist das wichtigste Element unterstrichen.)

$$R = \begin{pmatrix} \underline{2} & 2 & -8 & -6 & 10 \\ 2 & 8 & -2 & -6 & 22 \\ 2 & 26 & 1756 & -126 & 688 \\ -6 & -6 & -96 & 48 & -30 \\ 10 & 22 & 392 & -30 & 284 \end{pmatrix} \xrightarrow{4.1} \begin{pmatrix} \underline{2} & 2 & -8 & -6 & 10 \\ 0 & 6 & 6 & 0 & 12 \\ 0 & 24 & 1764 & -120 & 678 \\ 0 & 0 & -120 & 30 & 0 \\ 0 & 12 & 432 & 0 & 234 \end{pmatrix} \xrightarrow{4.2} \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & \underline{6} & 6 & 0 & 12 \\ 0 & 24 & 1764 & -120 & 678 \\ 0 & 0 & -120 & 30 & 0 \\ 0 & 12 & 432 & 0 & 234 \end{pmatrix}$$

$$\xrightarrow{4.1} \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & \underline{6} & 6 & 0 & 12 \\ 0 & 0 & 1740 & -120 & 630 \\ 0 & 0 & -120 & 30 & 0 \\ 0 & 0 & 420 & 0 & 210 \end{pmatrix} \xrightarrow{4.2} \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 1740 & -120 & 630 \\ 0 & 0 & -120 & \underline{30} & 0 \\ 0 & 0 & 420 & 0 & 210 \end{pmatrix} \xrightarrow{4.1} \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 1260 & 0 & 630 \\ 0 & 0 & -120 & \underline{30} & 0 \\ 0 & 0 & 420 & 0 & 210 \end{pmatrix}$$

$$\xrightarrow{4.2} \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 1260 & 0 & 630 \\ 0 & 0 & 0 & \underline{30} & 0 \\ 0 & 0 & 420 & 0 & 210 \end{pmatrix} \xrightarrow{2} \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 30 & 0 & 0 \\ 0 & 0 & 0 & 1260 & 630 \\ 0 & 0 & 0 & 420 & \underline{210} \end{pmatrix} \xrightarrow{4.1} \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 30 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 420 & \underline{210} \end{pmatrix}$$

$$\xrightarrow{4.2} \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 30 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \underline{210} \end{pmatrix} \xrightarrow{2} \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 30 & 0 & 0 \\ 0 & 0 & 0 & 210 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Der Isomorphietyp lässt sich nun aus R ablesen:

$$G \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/210\mathbb{Z}$$

Für 2. bestimme nun die Primfaktorzerlegungen:

$2 = 2$
$6 = 2 \cdot 3$
$30 = 2 \cdot 3 \cdot 5$
$210 = 2 \cdot 3 \cdot 5 \cdot 7$

Daraus folgt:

$$G \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$

Für 1. sortiere die Primfaktoren und fasse sie nach dem Muster im Beweis Korollar 2.5 zusammen:

$$G \cong \mathbb{Z} \times \mathbb{Z}/2 \cdot 3 \cdot 5 \cdot 7\mathbb{Z} \times \mathbb{Z}/2 \cdot 3 \cdot 5\mathbb{Z} \times \mathbb{Z}/2 \cdot 3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Also:

$$G \cong \mathbb{Z} \times \mathbb{Z}/210\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Dies ist zufällig identisch zu dem, was wir zuerst aus der Relationenmatrix ablesen konnten.
Fertig.

Aufgabe 2

Sei G eine endlich erzeugte abelsche Gruppe mit einer Darstellung der Form $\mathbb{Z}^4 \xrightarrow{R} \mathbb{Z}^4 \xrightarrow{S} G$,wobei

$$R = \begin{pmatrix} -13 & -16 & 3 & -14 \\ 1 & 0 & 3 & 0 \\ 22 & 24 & 4 & 22 \\ -15 & -16 & -5 & -16 \end{pmatrix}$$

Bestimme wieder 1. und 2. aus Aufgabe 1.

Lösung:

Diagonalisieren:

$$R = \begin{pmatrix} -13 & -16 & 3 & -14 \\ \underline{1} & 0 & 3 & 0 \\ 22 & 24 & 4 & 22 \\ -15 & -16 & -5 & -16 \end{pmatrix} \xrightarrow{4.1} \begin{pmatrix} 0 & -16 & 42 & -14 \\ \underline{1} & 0 & 3 & 0 \\ 0 & 24 & -62 & 22 \\ 0 & -16 & 40 & -16 \end{pmatrix} \xrightarrow{4.2} \begin{pmatrix} 0 & -16 & 42 & -14 \\ \underline{1} & 0 & 0 & 0 \\ 0 & 24 & -62 & 22 \\ 0 & -16 & 40 & -16 \end{pmatrix}$$

$$\xrightarrow{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -16 & 42 & \underline{-14} \\ 0 & 24 & -62 & 22 \\ 0 & -16 & 40 & -16 \end{pmatrix} \xrightarrow{4.1} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -16 & 42 & \underline{-14} \\ 0 & 8 & -20 & 8 \\ 0 & -16 & -44 & 12 \end{pmatrix} \xrightarrow{4.2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 12 & 0 & -14 \\ 0 & -8 & \underline{4} & 8 \\ 0 & -8 & -8 & 12 \end{pmatrix}$$

$$\xrightarrow{4.1} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 12 & 0 & -14 \\ 0 & -8 & \underline{4} & 8 \\ 0 & -24 & 0 & 28 \end{pmatrix} \xrightarrow{4.2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 12 & 0 & -14 \\ 0 & 0 & \underline{4} & 0 \\ 0 & -24 & 0 & 28 \end{pmatrix} \xrightarrow{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & \underline{12} & -14 \\ 0 & 0 & -24 & 28 \end{pmatrix}$$

$$\xrightarrow{4.1} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & \underline{12} & -14 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{4.2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 12 & \underline{2} \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{4.1} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & \underline{2} \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Der Isomorphietyp lässt sich nun aus R ablesen:

$$G \cong \mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Für 2. bestimme nun die Primfaktorzerlegungen:

$2 = 2$
$4 = 2^2 = 2 \cdot 2$

Daraus folgt:

$$G \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Für 1. sortiere die Primfaktoren und fasse sie nach dem Muster aus Beweis Korollar 2.5 zusammen:

$$G \cong \mathbb{Z} \times \mathbb{Z}/2 \cdot 2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Also:

$$G \cong \mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Dies ist zufällig identisch zu dem, was wir zuerst aus der Relationenmatrix ablesen konnten.
Fertig.

Literaturverzeichnis

Die Hauptquelle dieser Vortragsreihe war folgendes Buch:

- *Elementare und algebraische Zahlentheorie*, S. Müller-Stach, J. Piontkowski, Vieweg und Teubner, 2011

Es wurden folgende weitere Quellen zur Erarbeitung verwendet:

- Sript *Algebra I* der TU Dortmund, Autor: Rudolf Scharlau
- Skript *Algebra* der Uni Köln, Autor: Dr. Stephan Ehlen
- Skript *Endliche Gruppen* der Uni Tübingen, Autor: Thomas Keilen