Endlich erzeugte abelsche Gruppen

Alina Braun

1. Definitionen und Einführung
2. Endlich erzeugte Untergruppen von abelschen Gruppen
3. Zyklische Gruppen
4. Darstellung von endlich erzeugten abelschen Gruppen
5. Rückblickende Fragestellungen

Definitionen und Einführung

Ziel: Beweis, dass jede endlich erzeugte abelsche Gruppe ein direktes Produkt aus den additiven Gruppen $\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$ ist.

Def. 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 $\circ: G \times G \ni (g,h) \longmapsto g \circ h \in G$ 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:

$g \circ h = h \circ g$

Def. 1.2: Sei G eine Gruppe

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

$$\langle S \rangle := \bigcap_{H \subset G \, U G \atop S \subset H} H$$

  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

Beispiele:

- $(\mathbb{Z}, +)$ ist eine unendliche abelsche Gruppe, die endlich erzeugt ist mit 1
- $(\mathbb{Q}, +)$ ist abelsch aber nicht endlich erzeugt, dem wählt man $x_1, \ldots, x_s$ 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 $x_1, \ldots, x_s$ dargestellt werden

Endlich erzeugte Untergruppen von abelschen Gruppen

Sei S $\subseteq$ G, G sei eine Gruppe

- $\langle S \rangle$ ist allg. schwer zu beschreiben
- Bei abelschen Gruppen ist es allerdings einfach, da sie die Struktur eines $\mathbb{Z}$-Moduls haben

Sei G nun eine abelsche Gruppe und man schreibt "+" als ihre Verknüpfung, dann definiert man für $g \in G$ und $n \in \mathbb{N}$:

$$0 \cdot g = 0$$

$$(*) \quad n \cdot g = \underbrace{g + \ldots + g}_{n}$$

$$(-n) \cdot g = -(n \cdot g)$$

Lemma 2.1: 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 $R \times G \to G$, $(r, g) \mapsto r \cdot g$ (Skalarmultiplikation) existiert, die folgendes erfüllt:

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

$\to$ also ist zu zeigen, dass die Axiome für $z \in \mathbb{Z}$ und $g \in G$ gelten.

(*) impliziert: 1 g = g , m (ng) = (mn)g,
(m + n) g = m g + n g, m (g + g') = mg + mg'
für m,n ∈ $\mathbb{Z}$, $g, g' \in G$
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.
→ Behauptung □

Folgendes Lemma beschreibt nun das Aussehen von $\langle S \rangle$ für $S \subseteq G$ und G abelsch.

Lemma 2.2:

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

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

Beweis:

Bezeichne die rechte Seite der Gleichung mit H.

Man zeigt zuerst $H \subseteq \langle S \rangle$.

Nach Def. 1.2. ist $S \subseteq \langle S \rangle$.

Da jede UG abgeschlossen bezüglich Addition und Inversenbildung ist, muss es neben $g \in S$ auch $ng \in \langle S \rangle$ für $n \in \mathbb{Z}$ geben.

$\rightarrow \langle S \rangle$ muss endliche Summen $\sum_{g \in S'} n_g g$, $S' \subseteq S$ enthalten.

$\rightarrow H \subseteq \langle S \rangle$

Es bleibt noch zu zeigen, dass H eine UG ist.

Prüfe Abgeschlossenheit bezüglich Addition und Inversenbildung:

$h_1 = \sum_{g \in S'} n_g g$ *und* $h_2 = \sum_{g \in S''} m_g g$ mit endlichen S', S'' $\subseteq$ S seien zwei beliebige Elemente aus H.

Setze $n_g = 0$ für $g \in S'' \backslash S'$ und $m_g = 0$ für $g \in S' \backslash S''$.

Dann ist: $h_1 + h_2 = \sum_{g \in S' \cup S''} n_g g + \sum_{g \in S' \cup S''} m_g g$

$$= \sum_{g \in S' \cup S''} (n_g + m_g) \cdot g$$

$$-h_1 = -\sum_{g \in S'} n_g g = \sum_{g \in S'} (-n_g) g$$

$\rightarrow$ Behauptung $\square$

Zyklische Gruppen

Man betrachtet nun abelsche Gruppen, für die G = $\langle g \rangle$ mit g $\in$ G gilt,
Frage: Wie sieht $\langle g \rangle$ aus?

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

Beweis:
1. endlicher Fall
Sei G eine Gruppe mit $ord\ G = n$
Wenn $n = 1 \rightarrow \langle g \rangle = g \rightarrow \langle g \rangle = \{e\}$
Da $e = 1 \rightarrow \langle g \rangle = \{g^0\}$

Wenn $n > 1$, dann liegen folgende Elemente in $\langle g \rangle$:
$e = g^0, g^1, \ldots, g^n, g^{n+1}, \ldots$. 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 $g^m = e$
$\rightarrow \langle g \rangle = \left\{ g^0, g^1, \ldots, g^{m-1} \right\}$

$$= \left\{ g^n \mid n \in \mathbb{N} \right\}$$

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

2. unendlicher Fall:

G besteht aus folgenden Elementen:

$\langle g \rangle = \left\{ \ldots, g^{-n}, \ldots, g^{-1}, e, g^{1}, \ldots, g^{n}, \ldots \right\}$

Wenn $g^i = g^j$ für $i \neq j \rightarrow g^{i-j} = e$.

Für $i - j = n$ erhält man eine endliche UG, die von g erzeugt wurde ↯

Widerspruch zur Annahme, dass G unendlich ist

$\rightarrow \langle g \rangle = \left\{ g^n \mid n \in \mathbb{Z} \right\}$ □

Im nächsten Lemma wird das Verhältnis von zyklischen und abelschen Gruppen deutlich.

Lemma 3.1: Jede zyklische Gruppe ist abelsch

Beweis: Sei G eine zyklische Gruppe
Aus der vorherig. Beh. weiß man, dass $G = \langle g \rangle = \left\{ g^n \mid n \in \mathbb{Z} \right\}$.
Mit einer multiplikativen Verknüpfung folgt sofort für $n, m \in \mathbb{Z}$:
$g^n g^m = g^{n+m} = g^m g^n \rightarrow$ abelsch
$\rightarrow$ Behauptung □

Bem. 3.2: Bei einer additiven Verknüpfung sieht $\langle g \rangle$ wie folgt aus:
$\langle g \rangle = \left\{ m \cdot g \mid m \in \mathbb{Z} \right\}$

Beispiel:
$\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$ sind zyklische Gruppen mit Erzeuger 1 bzw. der Restklasse $\bar{1}$ bei einer additiven Verknüpfung.

$\rightarrow \mathbb{Z} = \langle 1 \rangle = \left\{ m \cdot 1 \mid m \in \mathbb{Z} \right\}$
$\rightarrow \mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$
Restklasse: $\bar{a} = a + n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle = \left\{ a + n\mathbb{Z} \mid a \in \mathbb{Z} \right\} =$
$\left\{ n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z} \right\}$

$\bar{1}$ ist immer ein Erzeuger von $\mathbb{Z}/n\mathbb{Z}$.
Für z. B. $\mathbb{Z}/10\mathbb{Z}$ ist aber auch $\bar{a} \in \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$ ein Erzeuger, denn für $\bar{3}$ gilt z.B.:
$\mathbb{Z}/10\mathbb{Z} = \langle\bar{3}\rangle = \{10\mathbb{Z}, 3 + 10\mathbb{Z}, 6 + 10\mathbb{Z}, 9 + 10\mathbb{Z}, 2 + 10\mathbb{Z}, 5 + 10\mathbb{Z}, 8 + 10\mathbb{Z}, 1 + 10\mathbb{Z}, 4 + 10\mathbb{Z}, 7 + 10\mathbb{Z}\}$

Merke: 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

Mit obigem Beispiel kommt man zu folgendem Satz:
Satz 3.3:
Jede zyklische Gruppe ist isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$ für ein $n \in \mathbb{N}$

Beweis:

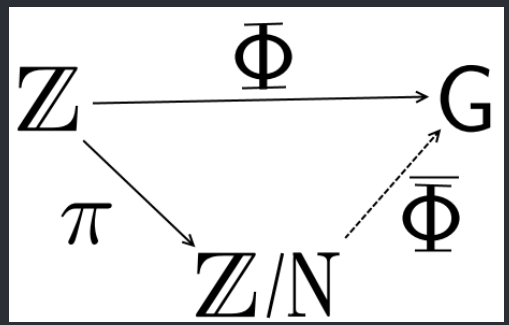
Sei G eine zyklische Gruppe mit Erzeuger $g \in G$ und additiver Verknüpfung, also $G = \langle g \rangle$. Da G zyklisch ist, ist der Gruppenhomomorphismus $\Phi : \mathbb{Z} \to G, m \mapsto m \cdot g$ surjektiv.

Für den Kern gilt: $\mathrm{Ker}\Phi = \{m \in \mathbb{Z} \mid \Phi(m) = e\} \subset \mathbb{Z}$, wobei e das neutrale Element von G ist.

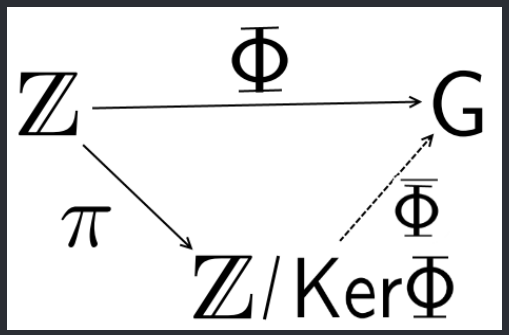
$\to$ Da $\mathrm{Ker}\Phi$ eine UG von $\mathbb{Z}$ ist und $\mathbb{Z}$ ein Hauptidealring ist, gilt:

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

Man erinnere sich an den Homomorphiesatz:



In der Algebra wurde gezeigt, dass KerΦ ein Normalteiler von $\mathbb{Z}$ ist.



Nach Kor. 2.2 aus dem Algebra Skript (Homomorphiesatz) gilt:
$\mathbb{Z}/Ker\Phi \cong Bild\Phi$

Betrachte $Ker\Phi = n\mathbb{Z}$
1. $n = 0$: $Ker\Phi = 0 \rightarrow$ neutrales Element von G ist 0.
$\rightarrow \Phi$ ist bijektiv, also muss $G \cong \mathbb{Z}$ sein.

2. $n \geq 1$: $Ker\Phi = n\mathbb{Z}$. Mit dem Homomorphiesatz folgt sofort, dass $\bar{\Phi} : \mathbb{Z}/n\mathbb{Z} \to G$ ein kanonischer Isomorphismus ist.

$\to G \cong \mathbb{Z}/n\mathbb{Z}$

$\to$ Beh. $\square$

Darstellung von endlich erzeugten abelschen Gruppen

- Man betrachtet nun die Darstellung von G als $\mathbb{Z}$-Modul, wobei G abelsch ist.
- G hat endlich viel Erzeuger $g_1, \ldots, g_k$
- Erzeuger können als k-Tupel geschrieben werden: $S = (g_1, \ldots, g_k) \to G = \langle S \rangle$

Sei $\varphi_S : \mathbb{Z}^k \to G, \quad (m_1, \ldots, m_k) \mapsto \sum_{i=1}^{k} m_i g_i$
ein surjektiver Homomorphismus

Def. 4.1:

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

Seien nun $r_1, \ldots, r_l$ Erzeuger des Kerns:

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

Wenn man $r_1, \ldots, r_l$ als Spalten schreibt, erhält man eine Matrix

$R = (r_1\, r_2 \ldots r_l)$

R hat k Zeilen und l Spalten und repräsentiert eine Abbildung:

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

$\to \mathbb{Z}^l \xrightarrow{R} \mathbb{Z}^k \xrightarrow{S} G$ bezeichnet eine Darstellung von G.

Beispiel:

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:

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

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

$\{2\mathbb{Z}\} \times \{2\mathbb{Z}\}\}$

$\to \langle (2, 0), (0, 2) \rangle = Ker\varphi_{S_1}$

Man erhält also folgende Darstellung von G:

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

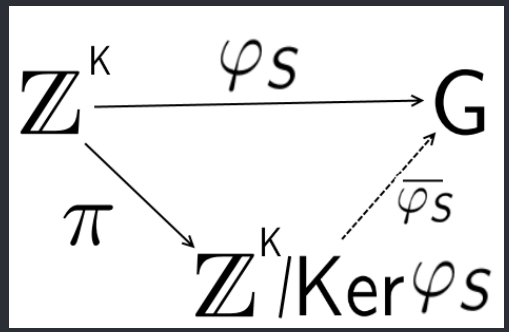
Wie sieht die Darstellung von G aus, wenn man S_2 bzw. S_3 betrachtet?

$$\varphi_{S_2} : \mathbb{Z}^3 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$
$$(m_1, m_2, m_3) \mapsto m_1 \cdot (\bar{1}, \bar{0}) + m_2 \cdot (\bar{0}, \bar{1}) + m_3 \cdot (\bar{1}, \bar{1})$$
$$\varphi_{S_3} : \mathbb{Z}^2 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$
$$(m_1, m_2) \mapsto m_1 \cdot (\bar{1}, \bar{0}) + m_2 \cdot (\bar{1}, \bar{1})$$
$$\mathbb{Z}^3 \xrightarrow{\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}} \mathbb{Z}^3 \xrightarrow{((\bar{1},\bar{0})\ (\bar{0},\bar{1})\ (\bar{1},\bar{1}))} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
$$\mathbb{Z}^2 \xrightarrow{\begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix}} \mathbb{Z}^2 \xrightarrow{((\bar{1},\bar{0})\ (\bar{1},\bar{1}))} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Folgende Behauptung zeigt, dass der Isomorphietyp allein an der Matrix R abzulesen ist:

Beh.: Es gilt: $G \cong \mathbb{Z}^k/Ker\varphi_S = \mathbb{Z}^k/Im\ R$

Beweis:
Homomorphiesatz:



Da $\bar{\varphi}_S$ 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 3.3)

$Ker\varphi_S$ wird von $r_1, \ldots, r_l$ erzeugt $\rightarrow$ $Ker\varphi_S$= Im R

$\rightarrow$ Beh. □

Wie sieht die Darstellung von $\mathbb{Z}$ bzw. $\mathbb{Z}/n\mathbb{Z}$ aus, wenn man als Erzeuger 1 bzw. $\bar{1}$ wählt?

$\rightarrow$ Diese Frage werden wir später zusammen beantworten.

Lemma 4.2:

Jede Untergruppe von $\mathbb{Z}^k$ ist endlich erzeugt.

Beweis:

Sei $H \subseteq \mathbb{Z}^k$.

Beweisführung per Induktion nach k.

$k = 0 \rightarrow$ trivial $\rightarrow \mathbb{Z}^0 = \{0\}$

$k > 0$: Betrachte die Projektion $\pi : \mathbb{Z}^k \rightarrow \mathbb{Z}, \quad (z_1, \ldots, z_k) \mapsto z_k$

auf die letzte Komponente.

$IA : k = 1 : H \subseteq \mathbb{Z}$. H ist dann ein Ideal

Da $\mathbb{Z}$ Hauptidealring ist $\rightarrow H = n\mathbb{Z}$ für ein $n \in \mathbb{N}$

Somit wird H endlich erzeugt.

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

$IS: k-1 \to k:$

$\pi(H) \subseteq \mathbb{Z}$, denn $\pi(\mathbb{Z}^k) = \mathbb{Z}$. Da $\mathbb{Z}$ Hauptidealring ist und $\pi(H)$ Ideal von $\mathbb{Z} \to \pi(H) = n\mathbb{Z}$ für ein $n \in \mathbb{N}$

Sei nun $\pi^{-1}(n) = g \in H \longleftrightarrow g \in \pi^{-1}(n) \cap H$ und

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

Also ist $H' \cong \{(z_1, \ldots, z_{k-1}) \in \mathbb{Z}^{k-1} \mid \exists z_k = 0 : (z_1, \ldots, z_{k-1}, z_k) \in H\} \subseteq \mathbb{Z}^{k-1}$

Nach IA ist H' endlich erzeugt. Stelle nun folgende Behauptung auf:

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

Beweis: zu zeigen: $\forall h \in H \; \exists \, l \in \mathbb{Z}$ mit $h - lg \in H'$

Es gilt $\pi(h) \in \pi(H) = n\mathbb{Z} \rightarrow \pi(h) = l \cdot n$

$= l \cdot \pi(g)$, für ein $l \in \mathbb{Z}$

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

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

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

$\rightarrow \pi(h) - l \cdot \pi(g) = m - l \cdot n = m - m/n \cdot n = 0$

$\rightarrow h - lg \in Ker\pi \cap H = H'$

$\rightarrow$ Beh. $\square$

Überlegung: Kann man R auf besonders einfache Form bringen?

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

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

Im folgenden werden die Elementarmatrizen definiert:

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

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

Beispiele für ein 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

$\rightarrow \pi^{-1}(1) = 2 \longleftrightarrow \pi(2) = 1, \pi^{-1}(2) = 3 \longleftrightarrow \pi(3) = 2,$

$\pi^{-1}(3) = 1 \longleftrightarrow \pi(1) = 3$

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

Wenn sich S zu SE ändert, müssen sich dadurch auch die Erzeuger des Kerns ändern.

Die Änderung kann durch $E^{-1}R$ beschrieben werden.

Es gilt: $(E_{ij}(\lambda))^{-1} = E_{ij}(-\lambda)$, $(E_i)^{-1} = E_i$

$(P(\pi))^{-1} = P(\pi^{-1})$

$\rightarrow$ Man erhält folgende Darstellung für G:

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

Zusammenfassend gilt:

Lemma 4.3:

Sei $\mathbb{Z}^l \xrightarrow{R} \mathbb{Z}^k \xrightarrow{S} G$ eine 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 $S = (g_1, \ldots, g_k)$ ein Erzeugendensystem von G. Wie oben gezeigt, ist dann auch SE^{-1} ein Erzeugendensystem von G.

Die Spalten $r_1, \ldots, r_l$ erzeugen $Ker\varphi_S$

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

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

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

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

Wenn wir zudem Elementaroperationen von rechts durführen, ändert sich das Erzeugnis von R nicht.

Bezeichnet man diese Matrix mit E', dann kann man R einfach zu RE' ändern. Es folgt:

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

$\rightarrow$ Beh. $\square$

Rückblickende Fragestellungen

Folgende Fragen sind eine Vertiefung buw. Verinnerlichung des vorangegangenen SToffs.
Das Handout dient als Gedächtnisstütze und enthält die zentralen Aussagen des Vortrags.

Frage 1:

Sei $\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, \bar{1}, \ldots, \overline{n-1}\}$ eine zyklische Gruppe der Ordnung n.

Zeigen Sie, dass die Erzeuger von $\mathbb{Z}/n\mathbb{Z}$ genau die Restklassen $\{m \cdot \bar{1} \mid m \in \mathbb{N}\}$ mit $ggT(m, n) = 1$ sind.

Hinweis: Sie dürfen verwenden, dass

$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \longleftrightarrow ggT(a, b) = d \; \forall a, b \in \mathbb{Z}$

Frage 2:

Sind die Gruppen $(\mathbb{Z}/5\mathbb{Z})^*$ bzw. $(\mathbb{Z}/8\mathbb{Z})^*$ zyklisch?

Frage 3:

Wie sieht die Darstellung der Gruppen $\mathbb{Z}$ bzw. $\mathbb{Z}/n\mathbb{Z}$ mit den Erzeugern 1 bzw. $\bar{1}$ aus?

Lösung 1:

„→“ Falls $\langle m \rangle = \mathbb{Z}/n\mathbb{Z}$ gilt, dann ist insbesondere $\bar{1} \in \langle m \rangle$, da $\bar{1}$ immer ein Erzeuger von $\mathbb{Z}/n\mathbb{Z}$ ist.

$\rightarrow \exists\, r, s \in \mathbb{Z} : rm = 1 + ns \leftrightarrow mr - ns = 1$

→ Also folgt $1 \in m\mathbb{Z} + n\mathbb{Z}$ und da 1 Erzeuger der zyklischen Gruppe $\mathbb{Z}$ ist, gilt $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$

Mit dem Hinweis folgt sofort $ggT(m, n) = 1$

„←“ Wenn wir nun umgekehrt annehmen, dass $ggT(m, n) = 1$, dann folgt mit dem Hinweis sofort: $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$

$\rightarrow \exists\, r, s \in \mathbb{Z} : mr + ns = 1$ bzw. $rm = 1 + ns$

$\rightarrow \overline{rm} = \bar{1}$ Da $\bar{1}$ ganz $\mathbb{Z}/n\mathbb{Z}$ erzeugt, tut dies auch $\overline{m}$

→ Beh. □

Lösung 2:

$(\mathbb{Z}/5\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

Die Gruppe ist zyklisch, da 5 eine Primzahl ist. Wählt man $g = \bar{2}$ als Erzeuger, so gilt:

$$\begin{aligned}\langle\bar{2}\rangle &= \{\bar{2}^n \mid n \in \{1, .., 4\}\} \\ &= \{\bar{2}, \bar{4}, \bar{3}, \bar{1}\} \\ &= \{g, g^2, g^3, g^4 = e\}\end{aligned}$$

$(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

Die Gruppe ist nicht zyklisch, da für jedes Element $g \in (\mathbb{Z}/8\mathbb{Z})^*$ gilt, dass $g^2 = \bar{1} = e$. Wenn g Erzeuger wäre, müsste $g^2 \neq e$ gelten.

Lösung 3:

Für $\mathbb{Z}$ gilt:

$\varphi_S : \mathbb{Z} \to \mathbb{Z}, \quad (m) \mapsto m \cdot 1$

$Ker\varphi_S = \{m \in \mathbb{Z} \mid m = 0\} \to Ker\varphi_S = 0$

Also kann man $\mathbb{Z}$ wie folgt darstellen:

$\{0\} \to \mathbb{Z} \xrightarrow{(1)} \mathbb{Z}$

Für $\mathbb{Z}/n\mathbb{Z}$ gilt:

$\varphi_S : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad (m) \mapsto m \cdot \bar{1}$

$Ker\varphi_S = \{m \in \mathbb{Z} \mid m \cdot \bar{1} = n\mathbb{Z}\}$

$\to \langle n \rangle = Ker\varphi = \{n\mathbb{Z}\}$

Also kann man $\mathbb{Z}/n\mathbb{Z}$ wie folgt darstellen:

$\mathbb{Z} \xrightarrow{(n)} \mathbb{Z} \xrightarrow{\bar{1}} \mathbb{Z}/n\mathbb{Z}$