Die unendliche Diedergruppe $G = \langle x, y \mid x^2 = 1, y^x = y^{-1} \rangle$. Wie können wir herausfinden, was für eine Gruppe G darstellt? Z. B. ist G endlich oder unendlich?

Eine Möglichkeit: scharfes Hinschauen! Betrachte die Gruppe D_∞ aus Kapitel I. Dann erfüllen die Matrizen a und b die Relationen von G in x und y. Also ist nach obigem Satz D_∞ ein epimorphes Bild von G, d.h. $G/N \cong D_\infty$. Aber wir wissen nicht, was N ist.

Andere Möglichkeit: versuche Worte in x, y zu normalisieren. Es gilt: $yx = xy^{-1}$. Daher kann durch wiederholtes Anwenden dieser Regel jedes Wort in x, y in die Form $x^e y^f$ für $e, f \in \mathbb{Z}$ gebracht werden. Da $x^2 = 1$ in G gilt, können wir $e \in \{0, 1\}$ verlangen. Damit können wir einsehen, dass $G \cong D_\infty$ gilt, denn kein Wort dieser Form wird trivial in D_∞.

2.3 Abelsche Invarianten

2.3.1 Definition. Sei G eine Gruppe.

- Für $g, h \in G$ heißt $[g, h] = g^{-1}h^{-1}gh$ der *Kommutator* von g und h.
- $G' = \langle [g, h] \mid g, h \in G \rangle$ ist die *Kommutatoruntergruppe* von G.

2.3.2 Lemma. *$G' \trianglelefteq G$ und G/G' ist die größte abelsche Faktorgruppe von G.*

Beweis. Sehr einfach. □

2.3.3 Lemma. *Sei $G = \langle X \mid R \rangle$ endlich präsentiert.*

a) G/G' ist eine endlich erzeugte abelsche Gruppe.
b) $G/G' \cong \langle X \mid R \cup C \rangle$ für $C = \{[x, y] \mid x, y \in X\}$.

Beweis. a) G ist endlich präsentiert und daher endlich erzeugt. Damit ist auch jede Faktorgruppe von G endlich erzeugt.
b) Sei H die von der gegebenen Präsentation erzeugte Gruppe. Dann ist H abelsch, da die Erzeuger von H kommutieren. Weiter erfüllt H die Relationen von G und damit ist H epimorphes Bild von G via $\pi : G \to H : x \mapsto x$. Nach Lemma gilt $G' \leq ker(\pi)$, denn G/G' ist maximal abelsche Faktorgruppe, und damit ist H epimorphes Bild von G/G'. Andererseits erfüllt G/G' die Relationen von H und ist daher epimorphes Bild von H. Die beiden zugehörigen Epimorphismen sind invers zueinander und daher gilt $H \cong G/G'$. □

Endlich erzeugte abelsche Gruppen sind aus der Algebra bekannt. Man kann diese Gruppen vollständig klassifizieren nach dem folgenden Satz.

2.3.4 Satz. *(Hauptsatz über endlich erzeugte abelsche Gruppen)*
Sei A eine endlich erzeugte abelsche Gruppe, dann gilt $A \cong \mathbb{Z}/k_1\mathbb{Z} \times \ldots \times \mathbb{Z}/k_r\mathbb{Z} \times \mathbb{Z}^s$ mit $k_1 \mid \ldots \mid k_s$.

2.3.5 Definition. Dann heißen $(k_1, \ldots, k_r; s)$ die *abelschen Invarianten* von A.

2.3.6 Beispiel. Jede abelsche Gruppe der Ordnung 8 ist isomorph zu einer der folgenden Gruppen: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/8\mathbb{Z}$.

2.3.7 Bemerkung. Die abelschen Invarianten einer abelschen Gruppe bestimmen ihren Isomorphietyp vollständig.

Sei $G = \langle X \mid R \rangle$ endlich präsentiert. Dann können wir eine endliche Präsentation von G/G' ableiten nach obigem Lemma. Außerdem können wir den Isomorphietyp von G/G' mit dem folgenden Algorithmus bestimmen.

2.3.1 Modifikation der Relatoren von G/G'

Sei $X = \{x_1, \ldots, x_n\}$ und $R = \{r_1, \ldots, r_l\}$. Dann ist $r_i = r_i(X)$ ein Wort in $X \cup X^{-1}$.
Wir nehmen jetzt an, dass wir in G/G' rechnen. Dann können wir die Erzeuger von G als vertauschbar betrachten. Damit können wir jedes r_i umschreiben zu einem Wort $r_i = x_1^{e_{i1}} \cdots x_n^{e_{in}}$, welches sortiert ist in den Variablen X. Da das Wort sortiert ist, hängt es nur von den Exponenten $e_{ij} \in \mathbb{Z}$ ab. Schreibe alle Exponenten in eine Matrix:

$$E = \begin{pmatrix} e_{11} & \ldots & e_{1n} \\ \vdots & & \vdots \\ e_{l1} & \ldots & e_{ln} \end{pmatrix} \in \mathbb{Z}^{l \times n}.$$

Für die Zeilen e_i von E gilt $e_i \in \mathbb{Z}^n$ und daher definiert $\mathbb{Z}^n/\langle E \rangle$ eine abelsche Gruppe. (Die additive Gruppe $\mathbb{Z}^n$ ist das n-fache direkte Produkt von $\mathbb{Z}$. Mit $\langle E \rangle$ ist der der Zeilenraum von E gemeint, also der Aufspann der Zeilen e_i von E.)

2.3.8 Satz. *$G/G' \cong \mathbb{Z}^n/\langle E \rangle$.*

Beweis. Sei $y_1, \ldots, y_n$ die Standardbasis von $\mathbb{Z}^n$ und sei $Y = \{y_1, \ldots, y_n\}$. Sei F frei auf X. Die Bijektion $X \to Y : x_i \mapsto y_i$ definiert einen Epimorphismus $\sigma : F \to \mathbb{Z}^n$. Sei $\alpha : \mathbb{Z}^n \to \mathbb{Z}^n/\langle E \rangle$ der natürliche Epimorphismus auf die Faktorgruppe. Dann ist $\beta = \sigma\alpha$ ein Epimorphismus $\beta : F \to \mathbb{Z}^n/\langle E \rangle$. Nach der Konstruktion von E sind die Relationen $R \cup C$ von G/G' in F gerade die Relationen, die auch $ker(\beta)$ erzeugen. Daher induziert β einen Isomorphismus von der Form $G/G' \to \mathbb{Z}^n/\langle E \rangle$. □

Damit haben wir die endlich präsentierte Gruppe G/G' in eine additiv geschriebene abelsche Faktorgruppe von $\mathbb{Z}^n$ umgeschrieben. Untersuche nun den Faktor von $\mathbb{Z}^n$ weiter.

2.3.2 Bestimmung der abelschen Invarianten von Faktoren von $\mathbb{Z}^n$

Sei $E \in \mathbb{Z}^{l \times n}$. Wir wollen den Zeilenraum von E untersuchen. Falls $l < n$, dann fülle E durch 0-Zeilen auf, so dass wir $n \leq l$ annehmen können. (0-Zeilen verändern den Zeilenraum von E nicht.)

2.3.9 Satz. *Sei $E \in \mathbb{Z}^{l \times n}$ mit $n \leq l$.*

a) Dann existieren $P \in GL(l, \mathbb{Z})$ und $Q \in GL(n, \mathbb{Z})$, so dass $D = PEQ$ eine Diagonalmatrix mit Diagonale $(d_1, \ldots, d_n)$ ist, wobei $d_i \in \mathbb{N}_0$ und $d_i \mid d_{i+1}$ gilt.

b) $\mathbb{Z}^n/\langle E \rangle \cong \mathbb{Z}^n/\langle D \rangle$.

c) $\mathbb{Z}^n/\langle D \rangle \cong C_{d_1} \times \ldots \times C_{d_n}$. (Mit $C_0 \cong \mathbb{Z}$ und $C_d = \mathbb{Z}/d\mathbb{Z}$ für $d \in \mathbb{N}$.)

Beweis. a) Konstruiere P, Q und D durch Zeilen- und Spaltenoperationen auf E. Erlaubte Operationen auf Zeilen sind:

- Multiplikation einer Zeile mit ± 1.
- Vertauschen von zwei Zeilen.
- Addition eines vielfachen einer Zeile zu einer anderen Zeile.

Jede dieser Operation lässt sich durch eine Multplikation PE für eine Matrix $P \in GL(l, \mathbb{Z})$ darstellen. Iterierte Anwendungen dieser Operationen sind durch Produkte solcher Matrizen darstellbar. $(P_2(P_1E) = (P_2P_1)E = PE.)$

Analog gehen wir für Spalten vor. Hier lässt sich jede der elementaren Operation auf Spalten durch Multiplikation EQ für eine Matrix $Q \in GL(n, \mathbb{Z})$ darstellen.
Nun ist zu zeigen, dass eine iterierte Anwendung solcher Zeilen- und Spaltenoperationen zu einer Diagonalmatrix führt. Falls $E = 0$, dann ist nichts zu tun. Also sei $E \neq 0$.
Modifiziere E nach den folgenden Schritten:

1. Vertausche Zeilen und Spalten bis $|e_{11}| = \min_{i,j}\{|e_{ij}| \mid e_{ij} \neq 0\}$.
2. Multipliziere e_1, so dass $e_{11} > 0$ gilt.
3. Falls $e_{11} \nmid e_{i1}$ für ein i (oder $e_{11} \nmid e_{1j}$) gilt, dann multipliziere e_i, so dass e_{i1} positiv wird, und bilde durch Division mit Rest $e_{i1} = ae_{11} + r$ für $0 \leq r < e_{11}$.
4. Addiere $-ae_1$ zu e_i. Damit wird $0 \neq e_{i1} = r < e_{11}$.
5. Nun iteriere das Verfahren (auch auf Spalten), solange bis alle e_{i1} und e_{1j} durch e_{11} teilbar sind.

Da e_{11} in jedem Durchlauf dieser Iteration vom Betrag kleiner wird, bricht diese Iteration irgendwann ab. Dann gilt $e_{11} \mid e_{i1}$ und $e_{11} \mid e_{1j}$. Nun können wir durch Zeilen- und Spaltenoperationen die erste Zeile und Spalte bis auf e_{11} ausräumen.
Durch Iteration dieses Verfahrens mit der unteren rechten $(l-1)\times(n-1)$ Matrix erhalten wir nach endlich vielen Schritten eine Diagonalmatrix D mit Diagonalelementen $d_1, \ldots, d_n \in \mathbb{N}_0$.

Nun muss noch die Teilbarkeitsbedingung hergestellt werden. Zunächst tausche Zeilen und Spalten, so dass alle Nullen am Ende stehen, und für die Nicht-Null-Einträge gilt $d_i \leq d_{i+1}$. Falls für all i gilt $d_i \mid d_{i+1}$ sind wir fertig. Andernfalls wähle das kleinste i, so dass es ein $j > i$ gibt mit $d_i \nmid d_j$. Setze $d := ggT(d_i, d_j)$. Nach dem erweiterten Euklidischen Algorithmus existieren dann $x, y \in \mathbb{Z}$ mit $d = xd_i + yd_j$. Für $a := \frac{d_i}{d}$ und $b := -\frac{d_j}{d}$ gilt dann $ax - by = 1$, und somit:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d_i & 0 \\ 0 & d_j \end{pmatrix} \begin{pmatrix} x & b \\ y & a \end{pmatrix} = \begin{pmatrix} d & 0 \\ yd_j & ad_j \end{pmatrix} \to \begin{pmatrix} d & 0 \\ 0 & ad_j \end{pmatrix}$$

Wir erhalten eine neue Diagonalmatrix, wobei $d \mid ad_j$. (Übrigens ist $ad_j = kgV(d_i, d_j)$.) Iteriere auch dieses Verfahren. Wiederrum ist gewährleistet, dass die Berechnung nach endlichen vielen Schritten abbricht, da in jedem Schritt das kleinste Diagonalelement, welches nicht alle folgenden Diagonalelemente teilt, durch ein kleineres ersetzt wird. Da die natürlichen Zahlen wohlgeordnet sind, kann dies nur endlich oft geschehen.

b) Es ist $D = PEQ$. Die Matrix P definiert eine iterierte Anwendung von Zeilenoperationen und ändert daher nur das gewählte Erzeugendensystem für den Zeilenraum. Damit gilt $\langle P(EQ)\rangle = \langle EQ\rangle$. Die Matrix Q ist invertierbar und definiert damit einen Isomorphismus von $\mathbb{Z}^n$ auf $\mathbb{Z}^n$. Dieser Isomorphismus bildet $\langle E\rangle$ auf $\langle D\rangle$ ab. Also induziert Q einen Isomorphismus der Faktoren $\mathbb{Z}^n/\langle E\rangle \to \mathbb{Z}^n/\langle D\rangle$.

c) Ist klar. □

2.3.10 Definition. Die Diagonalmatrix D heißt die *Smith-Normalform* von E.

Der Beweis des Satzes ist konstruktiv und zeigt einen Algorithmus, mit dem P, Q und D zu E bestimmt werden können. Die Schritte in dem Algorithmus können auch nach anderen Strategien als in dem Beweis gewählt werden. Damit kann versucht werden, die Einträge in allen entstehenden Matrizen klein zu halten. (Die „Explosion“ der Einträge in den Matrizen ist ein zentrales Problem.)

Bezüglich der Komplexität ist der hier vorgestellte Algorithmus ist schwer zu analysieren. Es gibt jedoch Algorithmen (z. B. von Kannan und Bachem), welche die Smith-Normalform in polynomieller Laufzeit bestimmen können.

2.3.3 Beispiele

2.3.11 Beispiel. Sei $G = \langle a, b, c, \mid a^2, b^3 \rangle$. Dann ist

$$E = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in \mathbb{Z}^{3\times 3}.$$

Damit ist

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in \mathbb{Z}^{3\times 3}.$$

Es folgt nun sofort, dass $G/G' \cong \mathbb{Z}/6\mathbb{Z} + \mathbb{Z} \cong C_6 \times C_\infty = C_2 \times C_3 \times C_\infty$ gilt. Ferner ist $|G| = \infty$.

2.3.12 Beispiel. Sei $G = \langle x, y \mid x^2 = 1, y^x = y^{-1} \rangle \cong D_\infty$. Dann ist

$$E = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \in \mathbb{Z}^{2\times 2}.$$

Also folgt $G/G' \cong C_2 \times C_2$.

2.3.4 Elementare Folgerungen

2.3.13 Lemma.
- *Sei F frei auf X mit $|X| = n$. Dann gilt $F/F' \cong \mathbb{Z}^n$. (Die Gruppe $\mathbb{Z}^n$ heißt auch frei abelsch.)*
- *Sei F_i frei auf X_i mit $|X_1| \neq |X_2|$. Dann gilt $F_1 \ncong F_2$. (Eindeutigkeit freier Gruppen.)*
- *Sei $G = \langle X \mid R \rangle$ endlich präsentiert mit $|R| < |X|$. Dann gilt $|G| = \infty$.*

Beweis. Sollte jetzt einfach sein. □