Lösung 6

Zyklische und auflösbare Gruppen

1. Zeigen Sie, dass eine nicht-triviale endliche auflösbare Gruppe eine normale Untergruppe von Index p für eine Primzahl p hat.

2. Sei K ein Körper und $n \geqslant 1$. Zeigen Sie, dass die Gruppe (bzgl. Multiplikation) der oberen invertierbaren Dreiecksmatrizen

$$T(n,K) := \left\{ \begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & * \end{pmatrix} \right\} \leqslant \mathrm{GL}(n,K)$$

auflösbar ist.

3. Sei $f \in k[X]$ ein Polynom. Sei $K|k$ eine normale Körpererweiterung und $L|K$ ein Zerfällungskörper von f aufgefasst als Polynom in $K[X]$. Zeigen Sie, dass $L|k$ normal ist.

4. Sei C_d die zyklische Gruppe der Ordnung $d \geqslant 1$. Zeigen Sie, dass $\mathrm{Aut}(C_d)$ isomorph zur Gruppe $(\mathbb{Z}/d\mathbb{Z})^\times$ der Einheiten des Rings $\mathbb{Z}/d\mathbb{Z}$ ist.

   Lösung: Wir erinnern uns, dass $(\mathbb{Z}/d\mathbb{Z})^\times = \{k \in \mathbb{Z}/d\mathbb{Z} \mid \mathrm{ggT}(k,d) = 1\}$. Wir definieren die Abbildung

$$\Phi : (\mathbb{Z}/d\mathbb{Z})^\times \to \mathrm{Aut}(C_d),\ k \mapsto \varphi_k,\ \text{ wobei } \varphi_k(y) = y^k.$$

   Da $k \in (\mathbb{Z}/d\mathbb{Z})^\times$ ist φ_k ein Automorphismus. Man rechnet nach, dass Φ ein injektiver Gruppenhomomorphismus ist.

   Wir zeigen nun, dass Φ surjektiv ist. Sei $\varphi \in \mathrm{Aut}(C_d)$ und $c \in C_d$ ein Erzeuger der zyklischen Gruppe. Da φ ein Automorphismus ist, schickt es c auf einen Erzeuger von C_d. Nun erzeugt $\varphi(c) = c^k$ die Gruppe C_d genau dann, wenn $\mathrm{ggT}(k,d) = 1$. Daraus folgt direkt, dass $\varphi = \varphi_k = \Phi(k)$ mit $k \in (\mathbb{Z}/d\mathbb{Z})^\times$, und somit ist Φ surjektiv.

5. Sei $Q < \mathrm{GL}(2,\mathbb{C})$ die von

$$A := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ und } B := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

erzeugte Untergruppe von $\mathrm{GL}(2,\mathbb{C})$. Bestimmen Sie die Ordnung von Q. Ist Q auflösbar?

Lösung: Man berechnet, dass $A^2 = B^2 = -\mathrm{id}$ und somit haben A und B Ordnung 4 und A^2 und B^2 liegen im Zentrum von Q. Es ist

$$AB = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ BA = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix},\ A^3 = A^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ B^3 = B^{-1} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

Es ist leicht zu überprüfen, dass wir alle Elemente von Q aufgelistet haben und somit hat Q Ordnung 8. Die Gruppe Q heisst auch die *Quaternionengruppe*. Eine Gruppe der Ordnung p^3 mit p prim ist auflösbar. Dies kann man direkt nachrechnen oder man benutzt, dass jede endliche p-Gruppe nilpotent ist, was man zum Beispiel mit Induktion über die p-Potenz zeigen kann.

6. Zeigen Sie, dass eine Gruppe der Ordnung n zyklisch ist genau dann, wenn für jeden Teiler d von n höchstens eine zyklische Untergruppe der Ordnung d existiert. Schliessen Sie daraus, dass jede endliche Untergruppe der multiplikativen Gruppe eines Körpers zyklisch ist.

   Lösung: Sei $C_n = \langle c \rangle$ eine zyklische Gruppe der Ordnung n und d ein Teiler von n. Dann ist $\langle c^{n/d} \rangle$ eine Untergruppe von C_n der Ordnung d, da $c^{(n/d)d} = c^n = 1_{C_n}$ und c Ordnung n hat. Wir müssen nun zeigen, dass diese eindeutig ist. Sei $H \leqslant C_n$ eine Untergruppe der Ordnung d. Als Untergruppe einer zyklischen Gruppe ist H selbst zyklisch, das heisst $H = \langle c^m \rangle$ für ein m, das n teilt. Dann ist

$$d = |H| = |c^m| = n/m,$$

   woraus folgt, dass $m = n/d$ und damit $H = \langle c^{n/d} \rangle$.

   Für die andere Richtung sei G eine endliche Gruppe der Ordnung n mit der Eigenschaft, dass zu jedem Teiler d von n höchstens eine zyklische Untergruppe der Ordnung d existiert. Sei D die Menge aller Ordnungen von Elementen in G. Wir wollen zeigen, dass $n \in D$ (woraus folgt, dass G zyklisch ist). Falls $g \in G$ Ordnung d hat, so ist $\langle g \rangle$ die eindeutige Untergruppe von G der Ordnung d nach Annahme, das heisst alle Elemente der Ordnung d liegen in $\langle g \rangle$. Sei $\varphi(d)$ die Anzahl positiver ganzer Zahlen $a \leqslant d$ mit $\mathrm{ggT}(a,d) = 1$ (dies wird auch die *Eulersche Phi-Funktion* genannt). Dann gilt $\sum_{d|n} \varphi(d) = n$. (Ein Weg dies zu sehen ist, in dem wir bemerken, dass $\varphi(d)$ gerade die Anzahl der möglichen Erzeuger der zyklischen Gruppe C_d sind. Da jedes Element in C_n eine zyklische Untergruppe erzeugt, und alle Untergruppen $C_d \subseteq C_n$ von einem Element in C_n erzeugt werden, gilt die Formel.) Es gibt somit genau $\varphi(d)$ Elemente in G der Ordnung d, denn für jedes a koprim zu d ist $\langle g^a \rangle = \langle g \rangle$, und nach Eindeutigkeit der zyklischen Untergruppen kann es keine weiteren Elemente der Ordnung d geben. Wir erhalten somit

$$n = \sum_{d \in D} \varphi(d) \leqslant \sum_{d|n} \varphi(d) = n,$$

also gilt Gleichheit. Insbesondere ist $n \in D$ und damit gibt es ein Element der Ordnung n und G ist zyklisch.

Sei nun K ein Körper und $G \leqslant K^\times$ eine endliche Untergruppe der Ordnung n. Für alle $g \in G$ ist $g^n = 1$ in K, und da jedes Polynom vom Grad n höchstens n Nullstellen hat, folgt, dass die Elemente von G genau die Nullstellen des Polynoms $X^n - 1$ sind. Sei d ein Teiler von n. Falls kein Element der Ordnung d existiert, ist nichts zu zeigen. Sei also $g \in G$ ein Element der Ordnung d. Dann ist g Nullstelle des Polynoms $X^d - 1$ und alle anderen Elemente der Ordnung d in G sind ebenfalls Nullstellen dieses Polynoms. Es gibt aber höchstens d Nullstellen und diese sind somit genau die Elemente der zyklischen Gruppe der Ordnung d, die von g erzeugt wird. Damit gibt es höchstens eine zyklische Untergruppe der Ordnung d. Nach der obigen Aussage folgt, dass G zyklisch ist.