# Übungsblatt 9: Sylowsatz und semidirekte Produkte

Die folgenden Lemmata könnten Ihnen bei einigen Aufgaben auf dem Blatt hilfreich sein. Sei im Folgenden $G$ stets eine endliche Gruppe und $p$ eine Primzahl.

**Lemma 1.** Sind $K,H < G$ Untergruppen mit $\mathrm{ggT}(|K|,|H|) = 1$. Dann ist $K \cap H = \{1\}$. Gilt andererseits $|K| = |H| = p$, so ist entweder $K \cap H = \{1\}$ oder $K = H$.

**Lösungshinweise: —** *$K \cap H$ ist eine Untergruppe von $K$ und von $H$, also muss deren Ordnung nach Lagrange ein Teiler der Ordnungen von $H$ und $K$ sein. Daraus folgt alles.* —

**Lemma 2.** Sind $K,H \lhd G$ Normalteiler mit $K \cap H = \{1\}$, dann ist $KH \cong K \times H$.

**Lösungshinweise: —** *Dies ist im Wesentlichen Aufgabe 2.3 auf Blatt 7.* —

## 1. Einfache Gruppen der Ordnung 60

**1.1.** Wenn $K < S_n$ eine Untergruppe vom Index 2 ist, dann gilt $K = A_n$.

**Lösungshinweise: —** *Eine Untergruppe vom Index 2 ist ein Normalteiler, also existiert ein nichttrivialer Homomorphismus $S_n \to S_n/K \cong \{\pm 1\}$. Wir wissen aus der Vorlesung (Satz 10C1), dass dieser gerade die Signatur sein muss. Also gilt $K = \ker(\mathrm{sign}) = A_n$.* —

**1.2.** Wenn es nur eine $p$-Sylowgruppe $P$ in einer Gruppe $G$ gibt, dann ist $P \lhd G$.

**Lösungshinweise: —** *Alle Sylowgruppen sind nach dem Sylowsatz zueinander konjugiert. Wenn es aber nur eine solche Gruppe gibt, so muss $g^{-1}Pg = P$ für alle $g \in G$ gelten. Das heißt $P$ ist ein Normalteiler.* —

**1.3.** (a) Sei $G$ eine endliche Gruppe und $r$ die Anzahl der $p$-Sylowgruppen. Dann gibt es einen Homomorphismus $\varphi : G \to S_r$.

(b) Ist $G$ einfach und $\varphi$ nicht trivial, so ist $\varphi$ sogar injektiv, also ist $|G|$ ein Teiler von $r! = |S_r|$.

**Lösungshinweise: —**

(a) *$G$ operiert durch Konjugation auf der Menge der Sylowgruppen. Eine Operation von $G$ auf einer Menge $X$ ist aber Äquivalent zu einem Homomorphismus $G \to \mathrm{Sym}(X)$. Die Aussage folgt.*

(b) *Der Kern $K$ des Homomorphismus $\varphi : G \to S_r$ ist ein Normalteiler in $G$. Da $G$ einfach ist, folgt $K = \{1\}$ oder $K = G$. Der zweite Fall kann nicht auftreten, da $\varphi$ nicht trivial ist und somit ist $\varphi$ injektiv. Damit ist nach Lagrange $|G| = |Im(G)|$ ein Teiler der Gruppenordnung $|S_r| = r!$.*

—

Sei $G$ eine einfache Gruppe der Ordnung $|G| = 60$. Wir wollen zeigen, dass $G \cong A_5$.

**S 1.4.** (5 Punkte)

(a) Zeigen Sie, dass es in $G$ genau zehn 3-Sylowgruppen gibt. *Hinweis:* Sylowsatz und Aufgaben 1.2 und 1.3.

(b) Zeigen Sie, dass es in $G$ genau sechs 5-Sylowgruppen gibt.

(c) Zeigen Sie, dass es in $G$ fünf 2-Sylowgruppen gibt. *Hinweis:* Wieviele Elemente von $G$ hätten wir schon gefunden, wenn es 15 2-Sylowgruppen gäbe?

(d) $G$ operiert auf der Menge der 2-Sylowgruppen und damit gibt es einen Homomorphismus $G \to S_5$. Folgern Sie aus 1.1, dass $G \cong A_5$.

**Lösungshinweise: —** *Zuerst beobachten wir für die Anwendung von Aufgabe 1.3, dass in einer einfachen Gruppe, deren Ordnung von mindestes zwei Primzahlen geteilt wird, die Operation von G auf den Sylowgruppen nicht trivial sein kann, da diese sonst normal in G wären.*
*Die Anzahl der p-Sylowgruppen ist kongruent zu* 1 *modulo p und ein Teiler der Gruppenordnung und damit auch von* $|G|/p^m$*, wenn* $p^m$ *die maximale Potenz von p ist, die in* $|G|$ *aufgeht. Damit ergeben sich nur wenige Möglichkeiten, die wir alle bis auf eine ausschließen werden, indem wir einen nichttrivialen Normalteiler angeben.*

(a) *Zahlen der Form* $1+3k$*, die Teiler von* 20 *sind, sind nur* $\{1,4,10\}$*. Der erste Fall wird durch Aufgabe 1.2 ausgeschlossen und der Fall von vier 3-Sylowgruppen durch 1.3 und obige Bemerkung.*

(b) *Es sind nur die Zahlen* $\{1,6\}$ *als Teiler von* 12 *der Form* $1+5k$ *möglich. Die eins wird wieder durch Aufgabe 1.2 ausgeschlossen.*

(c) *Auf der Menge X aller Elemente der Ordnung* 2 *operiert G durch Konjugation. Die Bahn eines Elementes* $\sigma$ *hat Länge* $1,3,5$ *oder* 15*, da nach Bahnengleichung diese ein Teiler von* 60 *sein muss und ungerade, da der Stabilisator eines Elementes eine 2-Sylowgruppe enthält und somit eine durch* 4 *teilbare Ordnung hat. Die ersten beiden Fälle sind nicht möglich, da wir dann einen Normalteiler der Ordnung* 2 *erhalten oder einen nichttrivialen Homomorphismus in die* $S_3$*. Bei Bahnen der Länge* 5 *erhalten wir die für Teil (d) notwendige Operation auf einer 5-elementigen Menge. Wenn die Bahn aber* 15 *Elemente hat, so hat nach Bahnenlemma der Stabilisator gerade* 4 *Elemente. Das Element* $\sigma$ *kann also nicht in zwei verschiedenen 2-Sylowgruppen enthalten sein, da wir sonst mehr als* 4 *Elemente im Stabilisator hätten (Gruppen der Ordnung* 4 *sind abelsch). Nach Lemma 1 enthalten alle 3-Sylowgruppen und 5-Sylowgruppen zusammen genau* $2\cdot 10+4\cdot 6=44$ *nichttriviale Elemente. Es bleiben also noch höchstens* 16 *Elemente für die 2-Sylowgruppen übrig. Die Anzahl der Sylowgruppen kann also höchstens fünf sein. Es kommen nur* $\{1,3,5\}$ *als Teiler von* 15 *der Form* $1+2k$ *in Frage. Die eins ist wieder wegen 1.2 und die* 3 *wegen 1.3 nicht möglich.*
*Insgesamt haben wir damit entweder genau* 5 *Sylowgruppen oder eine Bahn der Länge* 5 *und somit einen nichttrivialen Homomorphismus in die* $S_5$*.*

(d) *Der Homomorphismus ist injektiv, wie wir uns vorher überlegt haben. Also ist das Bild eine Untergruppe von* $S_5$ *der Ordnung* 60*. Nach Aufgabe 1.1 kann dies aber nur die* $A_5$ *sein, also* $G\cong A_5$*.*

—

## 2. Gruppen der Ordnung 8

Für jede endliche Gruppe $G$ existiert ein injektiver Gruppenhomomorphismus $G\hookrightarrow S_n$ für gewisse $n$. Man kann sich fragen, welches für $G$ das kleinste $n$ ist. Sicherlich ist $n=|G|$ immer möglich, aber meist zu groß:

**V 2.1.** Betrachten wir die Diedergruppe $D_4$ der Ordnung 8.

(a) Man zeige $D_4\hookrightarrow S_4$ indem man eine zu $D_4$ isomorphe Untergruppe $H<S_4$ angibt. Gibt es solche Gruppen auch in $S_n$ mit $n<4$?

Betrachten wir nun die Quaternionengruppe $Q$, ebenfalls der Ordnung 8.

(b) Man erläutere zunächst $Q\ncong D_4$.

(c) Ist $H$ eine 2-Sylowgruppe in $S_4$? in $S_5$?
Gibt es eine Untergruppe in $S_5$ isomorph zu $Q$?

(d) Man finde $K<S_6$ isomorph zu $D_4\times\mathbb{Z}/2\mathbb{Z}$. Ist $K$ eine 2-Sylowgruppe in $S_6$? in $S_7$? Gibt es eine Untergruppe in $S_7$ isomorph zu $Q$?

Welches ist demnach der minimale Grad $n$ für eine Einbettung $Q\hookrightarrow S_n$?

**Lösungshinweise: —**

(a) *Aus Aufgabe 2.2 von Blatt 8 gewinnen wir die Einbettung von* $D_4$ *als*
$H=\{\mathrm{id},(1,2,3,4),(1,3)(2,4),(1,4,3,2),(1,3),(2,4),(1,2)(3,4).(1,4)(2,3)\}<S_4$*. Die* $D_4$ *hat* 8 *Elemente, es kann also schon aus Kardinalitätsgründen nicht in* $S_n$ *für* $n\leq 3$ *eingebettet werden.*

(b) *In $Q$ gibt es sechs Elemente der Ordnung vier. In $D_4$ sind es nur zwei. Deswegen können die beiden Gruppen nicht isomorph sein.*
(c) *Die Ordnung von $S_4$ ist $4! = 24 = 2^3 \cdot 3$. Also sind alle Untergruppen der Ordnung acht 2-Sylowgruppen, insbesondere auch $H$. Dasselbe gilt für $S_5$, da $5! = 2^3 \cdot 3 \cdot 5$. Da alle Sylowgruppen zueinander konjugiert sind, kann es keine zu $Q$ isomorphe Untergruppe geben, denn sonst würde $Q \cong D_4$ folgen.*
(d) *Nimmt man in $S_6$ das Erzeugnis von $H$ und $(56)$, so ist die erzeugte Untergruppe $K$ von Ordnung $16$, da $(56)$ mit allen Elementen in $H$ kommutiert. Dies ist dann wegen $6! = 2^4 \cdot 3^2 \cdot 5$ eine 2-Sylowgruppe in $S_6$. $Q$ kann immer noch nicht als Untergruppe realisiert werden, da diese sonst zu einer Untergruppe von $K$ konjugiert sein müsste. In $K$ gibt es aber nur vier Elemente der Ordnung vier. Also ist das nicht möglich. Da in $S_7$ nur der Primfaktor $7$ hinzukommt, ändert sich wie vorher bei der $S_5$ nichts an den gemachten Aussagen.*

*Also lässt sich $Q$ nach Cayley in die $S_8$ einbetten, aber nicht in $S_n$ für $n < 8$.* —

**2.2.** Zeigen Sie, dass alle Untergruppen von $Q$ normal sind.

**Lösungshinweise: —** *Alle Untergruppen der Ordnung $1, 4$ und $8$ in $Q$ sind klarerweise normal. Für Ordnung $4$ gilt es, weil alle Untergruppen vom Index zwei normal sind. Es gibt aber nur eine Untergruppe von Ordnung $2$, die aus $\{\pm 1\}$ besteht. Diese ist aber offenbar sogar zentral, also auch normal.* —

**2.3.** Lässt sich $Q$ in nichttrivialer Weise als semidirektes Produkt schreiben?

**Lösungshinweise: —** *Dazu müsste $Q = K \rtimes H$ mit Untergruppen $K, H$ der Ordnungen zwei oder vier sein. Dies sind aber nach vorheriger Aufgabe normal in $Q$ und somit ist nach Lemma 2 dann $Q \cong K \times H$. Dies ist aber nicht möglich, da für $K$ und $H$ nur abelsche Gruppen in Frage kommen (da Ordnung $p$ und $p^2$) und somit $Q$ abelsch sein müsste.* —

*Bemerkung:* Es gibt bis auf Isomorphie genau fünf Gruppen der Ordnung acht: $\mathbb{Z}/_8, \mathbb{Z}/_2 \times \mathbb{Z}/_4, (\mathbb{Z}/_2)^3, D_4 = \mathbb{Z}/_4 \rtimes \mathbb{Z}/_2$ und $Q$.

## 3. Matrixgruppen über endlichen Körpern

**3.1.** Sei $p$ eine Primzahl. Zeigen Sie, dass $\mathrm{Aut}((\mathbb{Z}/_p)^n, +)$ isomorph zu $GL_n(\mathbb{Z}/_p)$ ist.

**Lösungshinweise: —** *$(\mathbb{Z}/_p)^n$ ist ein $\mathbb{Z}/_p$-Vektorraum. Wir zeigen, dass jeder Automorphismus $\varphi \in \mathrm{Aut}((\mathbb{Z}/_p)^n, +)$ nicht nur additiv, sondern sogar $\mathbb{Z}/_p$-linear ist. Die Aussage folgt dann aus der linearen Algebra. Es ist offenbar $\varphi(1v) = 1\varphi(v)$ und induktiv sieht man $\varphi((k+1)v) = \varphi(kv + v) = \varphi(kv) + \varphi(v) = k\varphi(v) + \varphi(v) = (k+1)\varphi(v)$. Wegen $\varphi(v) + \varphi(-v) = \varphi(v - v) = \varphi(0) = 0$ folgt $\varphi(-v) = -\varphi(v)$.*
*Umgekehrt definiert jede Matrix in $GL_n(\mathbb{Z}/_p)$ einen Automorphismus von $(\mathbb{Z}/_p)^n$, wie man direkt nachprüft.* —

Sei $\mathbb{F}_q$ ein Körper mit $q$ Elementen (z.B. $\mathbb{F}_p = \mathbb{Z}/_p$ für eine Primzahl $p$).

**V 3.2.** (a) Bestimmen Sie die Ordnung der Gruppe $GL_n(\mathbb{F}_q)$. *Hinweis:* Eine Matrix ist genau dann invertierbar, wenn ihre Spalten eine Basis von $\mathbb{F}_q^n$ bilden.
(b) Was ist dann die Ordnung von $SL_n(\mathbb{F}_q)$?

**Lösungshinweise: —**

(a) *Mit dem Hinweis reicht es alle Basen in $\mathbb{F}_q^n$ zu zählen. Wir können uns den ersten Basisvektor beliebig vorgeben, solange dieser ungleich null ist. Dies sind $q^n - 1$ Möglichkeiten. Der zweite Basisvektor darf nicht im Spann des ersten liegen. Dafür gibt es $q^n - q$ Möglichkeiten. Für den $k$-ten Basisvektor ergeben sich noch $q^n - q^{k-1}$ Wahlen, da dieser nicht in dem $(k-1)$-dimensionalen*

*Unterraum liegen darf, der von den ersten $k-1$ Vektoren aufgespannt wird. Insgesamt ergibt sich $|GL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.*

(b) *Die Gruppe $SL_n(\mathbb{F}_q)$ ist Kern des Determinantenhomomorphismus $\det : GL_n(\mathbb{F}_q) \to \mathbb{F}_q^\times$ und hat damit die Ordnung $|GL_n(\mathbb{F}_q)|/|F_q^\times| = \frac{1}{q-1}(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.*

—

**S 3.3.** (2 Punkte) Zeigen Sie, dass $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) \cong S_3$. Lassen Sie hierzu $GL_2(\mathbb{F}_2)$ auf den drei Geraden des $\mathbb{F}_2$-Vektorraums $\mathbb{F}_2^2$ operieren.

**Lösungshinweise: —** *Es ist $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2)$, weil alle invertierbaren Matrizen Determinante eins haben.*
*Weil $GL_2(\mathbb{F}_2)$ auf der Menge der drei Geraden $g_1 = \{(0,0),(1,0)\}$, $g_2 = \{(0,0),(0,1)\}$ und $g_3 = \{(0,0),(1,1)\}$ in $\mathbb{F}_2^2$ operiert, erhalten wir einen Homomorphismus $\varphi : GL_2(\mathbb{F}_2) \to S_3$. Die beiden Gruppen $S_3$ und $GL_2(\mathbb{F}_2)$ haben beide Ordnung sechs. Es reicht also Injektivität oder Surjektivität zu zeigen.*
*Man beobachtet dazu, dass die Matrizen $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ und $\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$ gerade den Traspositionen $(23),(12)$ und $(13)$ entsprechen. Also ist $\varphi$ surjektiv.*
*Alternativ: Sei $Ag_i = g_i$ für alle $g_i$, dann würde folgen, dass $A\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ und $A\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right) = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$ gilt, also $A = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$. Damit ist der Kern des Homomorphismus trivial und somit $\varphi$ injektiv* —

## 4. Gruppen der Ordnung 12

**S 4.1.** (2 Punkte) Zeigen Sie, dass es in einer Gruppe der Ordnung 12 stets einen nichttrivialen Normalteiler der Ordnung drei oder vier gibt. Damit ist jede Gruppe der Ordnung 12 ein semidirektes Produkt ihrer Sylowgruppen.
*Hinweis:* Sylowsatz und Abzählen der Elemente.

**Lösungshinweise: —** *Es gibt entweder eine oder vier 3-Sylowgruppen (Form $1+3k$, Teiler von vier). Im ersten Fall ist die 3-Sylowgruppe nach 1.2 normal. Im zweiten Fall gibt es nach Lemma 1 genau $2\cdot 4 = 8$ Elemente der Ordnung 3. Damit bleiben nur noch vier Elemente übrig und diese bilden damit die eindeutige 2-Sylowgruppe, die nun ihrerseits ein Normalteiler ist.*
*Nach Lemma 1 schneiden sich die beiden Sylowgruppen stets trivial und eine der beiden ist normal. Somit erhalten wir nach Vorlesung ein semidirektes Produkt der beiden Sylowgruppen.* —

Nun wollen wir alle möglichen semidirekten Produkte untersuchen, die man aus Gruppen der Ordnungen drei und vier erzeugen kann.

**V 4.2.** (a) Zeigen Sie, dass es jeweils genau ein nichttriviales semidirektes Produkt der Form $\mathbb{Z}/_3 \rtimes \mathbb{Z}/_4$ und $(\mathbb{Z}/_2)^2 \rtimes \mathbb{Z}/_3$ gibt.
(b) Warum sind alle nichttrivialen semidirekten Produkte der Form $\mathbb{Z}/_3 \rtimes (\mathbb{Z}/_2)^2$ untereinander isomorph?
(c) Gibt es ein nichtriviales semidirektes Produkt der Form $\mathbb{Z}/_4 \rtimes \mathbb{Z}/_3$?
(d) Zeigen Sie, dass die Gruppen aus (a) und (b) untereinander nicht isomorph sind. Wieviele Isomorphietypen von Gruppen der Ordnung 12 gibt es also?

**Lösungshinweise: —**

(a) *Die Automorphismengruppen von $\mathbb{Z}/_3$ und $(\mathbb{Z}/_2)^2$ sind nach den Aufgaben 3.1 und 3.3 isomorph zu $GL_1(\mathbb{Z}/_3) = \mathbb{Z}/_3^\times \cong \mathbb{Z}/_2$ und $GL_2(\mathbb{Z}/_2)$. Es gibt nur einen nichttrivialen Homomorphismus $\mathbb{Z}/_4 \to \mathbb{Z}/_2$, so dass das entstehende semidirekte Produkt eindeutig ist. Die Homomorphismen $\mathbb{Z}/_3 \to GL_2(\mathbb{Z}/_2) \cong S_3$ vertauschen gerade die drei Geraden in $(\mathbb{Z}/_2)^2$ zyklisch. Man kann durch anpassen der Basis diese Permutation eindeutig zu $(1,2,3)$ machen.*

(b) *Es gibt drei nichtriviale Homomorphismen* $(\mathbb{Z}/_2)^2 \to \mathbb{Z}/_2 \cong \mathrm{Aut}(\mathbb{Z}/_3,+)$ *nämlich die Matrizen* $(1\ 0)$, $(0\ 1)$ *und* $(1\ 1)$. *Diese sind aber alle äquivalent, da man die Matrizen durch Basiswechsel ineinander überführen kann.*

*Man kann es aber auch durch Nachrechnen prüfen: Seien* $\mathbb{Z}/_3 \overset{\varphi}{\rtimes} (\mathbb{Z}/_2)^2$ *und* $\mathbb{Z}/_3 \overset{\rho}{\rtimes} (\mathbb{Z}/_2)^2$ *zwei äußere semidirekte Produkte, dann gibt es ein* $A \in \mathrm{Aut}((\mathbb{Z}/_2)^2,+)$ *mit* $\varphi = \rho A$. *Dann ist* $\Psi : \mathbb{Z}/_3 \overset{\varphi}{\rtimes} (\mathbb{Z}/_2)^2 \to \mathbb{Z}/_3 \overset{\rho}{\rtimes} (\mathbb{Z}/_2)^2 : (x,y) \mapsto (x,Ay)$ *ein Isomorphismus der beiden semidirekten Produkte. Denn es ist* $\Psi((x_1,y_1)\cdot(x_2,y_2)) = \Psi((x_1\varphi(y_1)(x_2),y_1y_2) = (x_1\varphi(y_1)(x_2),A(y_1y_2)) = (x_1\rho(Ay_1)(x_2),A(y_1)A(y_2)) = (x_1,Ay_1)\cdot(x_2,Ay_2) = \Psi((x_1,y_1))\cdot\Psi((x_2,y_2))$. *Bijektivität ist auch klar und somit sind alle möglichen semidirekten Produkte isomorph.*

(c) *Nein, da es keinen nichttrivialen Homomorphismus von* $\mathbb{Z}/_3$ *nach* $\mathrm{Aut}(\mathbb{Z}/_4,+) \cong \mathbb{Z}/_4^\times \cong \mathbb{Z}/_2$ *gibt. Die Automorphismengruppe bestimmt man dabei ähnlich wie in Aufgabe 3.1.*

(d) *Die zweite Gruppe hat einen Normalteiler der Ordnung vier, während die beiden anderen einen Normalteiler der Ordnung drei besitzen. Da die Gruppen alle nichtkommutativ sind (nachrechnen!), kann das Komplement nach Lemma 2 nicht auch noch Normalteiler sein. Also bleibt noch zu zeigen, dass* $\mathbb{Z}/_3 \rtimes \mathbb{Z}/_4$ *und* $\mathbb{Z}/_3 \rtimes (\mathbb{Z}/_2)^2$ *nicht isomorph sind. In der ersten Gruppe gibt es aber ein Element der Ordnung vier, während es das in der zweiten Gruppe nicht gibt. Denn dort ist* $(a,b)^2 = (a\varphi(b)(a),b^2) = (a\varphi(b)(a),1)$. *und damit* $(a,b)^4 = ((a\varphi(b)(a))^2,1)$. *Es muss also* $a\varphi(b)a \neq 1$, *aber* $(a\varphi(b)a)^2 = 1$ *in* $\mathbb{Z}/_3$ *gelten. Dies ist aber nicht möglich.*

—

**4.3.** Die Gruppen $A_4$ und $D_6 \cong \mathbb{Z}/_6 \rtimes \mathbb{Z}/_2$ haben Ordnung 12. Zu welchen der obigen Gruppen sind diese isomorph?

**Lösungshinweise: —** *Sowohl* $A_4$, *als auch* $D_6$ *sind nicht abelsch, also bleiben noch die drei Kandidaten aus (a) und (b). Die* $A_4$ *enthält den Normalteiler* $V_4 = \{\mathrm{id},(12)(34),(13)(24),(14)(23)\}$ *der Ordnung vier und muss somit zu* $(\mathbb{Z}/_2)^2 \rtimes \mathbb{Z}/_3$ *isomorph sein. Die* $D_6$ *enthält einen Normalteiler der Ordnung drei, nämlich die Drehungen um* $0°, 120°$ *und* $240°$ *und keine Elemente der Ordnung vier. Sie muss also isomorph zu* $\mathbb{Z}/_3 \rtimes (\mathbb{Z}/_2)^2$ *sein.* —

## 5. Auflösbarkeit

Ziel dieser Aufgabe ist es zu zeigen, dass alle Gruppen der Ordnung $< 60$ auflösbar sind. Wir wissen schon aus der Vorlesung, dass Gruppen der Ordnung $p^n$ und $pq$ für Primzahlen $p,q$ auflösbar sind.

**5.1.** Zeigen Sie, dass Gruppen der Ordnung $pqr$ ($p < q < r$ Primzahlen) auflösbar sind, indem Sie zeigen, dass es entweder einen nichttrivialen Normalteiler geben muss (was folgt dann daraus?) oder die Anzahl der $p$-Sylowgruppen mindestens $q$, die Anzahl der $q$-Sylowgruppen mindestens $r$ und die Anzahl der $r$-Sylowgruppen mindestens $pq$ sein müsste. Damit ergeben sich dann zu viele Gruppenelemente.

**Lösungshinweise: —** *Die Anzahl der p-Sylowgruppen ist von der Form* $1+kp$. *Damit ist sie entweder* 1 *und wir hätten einen Normalteiler nach 1.2 oder sie ist größer als p. Da es ein Teiler von qr sein muss, ist die Anzahl insbesondere größer gleich q. Ebenso folgt, dass die Anzahl der q-Sylowgruppen* 1 *oder ein Teiler größer q von pr ist, also minderstens r. Im Fall r erhalten wir einen Teiler von pq, der größer als r sein soll. Der einzige solche Teiler ist pq selbst. Zählen wir nun alle Elemente in dem Fall zusammen, in dem wir stets mehr als eine Sylowgruppe haben, so erhalten wir nach Lemma 1 mindestens* $q(p-1)+r(q-1)+pq(r-1)+1 = pqr+(r-1)(q-1)$ *Elemente. Wegen* $r,q \geq 2$ *ist dies ein Widerspruch dazu, dass die Gruppenordnung pqr ist. Es gibt also stets einen nichttrivialen Normalteiler. Aus den schon* *bekannten Resultaten folgt, dass sowohl Normalteiler, als auch Faktorgruppe auflösbar sind. Nach dem Auflösbarkeitskriterium ist es somit auch jede Gruppe der Ordnung pqr.* —

**5.2.** Zeigen Sie, dass Gruppen der Ordnung $p^2q$ auflösbar sind. *Hinweis:* Im Fall $p < q$ beachte man, dass aus $p^2 \equiv 1 \mod q$ folgt, dass $q \mid p^2 - 1 = (p+1)(p-1)$.

**Lösungshinweise: —** *Im Fall $p > q$ ist die Anzahl der p-Sylowgruppen von der Form $1+kp$ und ein Teiler von q. Das ist aber nur für $k = 0$ möglich. Also haben wir nach 1.2 einen nichttrivialen Normalteiler gefunden.*
*Im Fall $p < q$ erhalten wir, dass die Anzahl der q-Sylowgruppen ein Teiler von $p^2$ von der Form $1+kq$ ist. Entweder dieser ist eins (dann sind wir wieder fertig) oder $1+kq = p^2$. Das führt auf $q \mid p^2 - 1 = (p+1)(p-1)$. Da q eine Primzahl ist, folgt $q \mid p+1$ oder $q \mid p-1$. Das zweite ist wegen der Größenbedingung (und $p \geq 2$) nicht möglich. Im ersten Fall ergibt sich $q = p+1$ und damit $p = 2, q = 3$. Damit hat unsere Gruppe die Ordnung 12 und wir erhalten aus Aufgabe 4.1 einen nichttrivialen Normalteiler.*
*Das weitere Argument funktioniert wie in 5.1.* —

**5.3.** Man zeige, dass Gruppen der Ordnung $24, 36, 40, 48, 54$ und $56$ auflösbar sind. *Hinweis:* Aufgabe 1.3 (und alle bisherigen Methoden)

**Lösungshinweise: —** *Es ist $24 = 2^3 \cdot 3$. Damit gibt es mit Aufgabe 1.3 einen Homomorphismus nach $S_3$. Wenn dieser nichttrivial ist, so erhalten wir aus Größengründen einen Kern und somit einen nichttrivialen Normalteiler. Wenn der Homomorphismus trivial ist, dann folgt, dass die 3-Sylowgruppen unter Konjugation invariant und somit Normalteiler sind. So oder so, wir erhalten einen nichttrivialen Normalteiler. Dasselbe funktioniert bei $48 = 2^4 \cdot 3$, $36 = 2^2 \cdot 3^3$ und $54 = 2 \cdot 3^3$ (in den beiden letzten Fällen mit vertauschten Rollen von zwei und drei).*
*Bei $40 = 2^3 \cdot 5$ betrachte man die 5-Sylowgruppen. Deren Anzahl ist von der Form $1+5k$ und Teiler von 8, also gibt es nur eine, die damit nach 1.2 ein Normalteiler ist.*
*Bei $56 = 2^3 \cdot 7$ erhält man entweder eine 7-Sylowgruppe oder acht. Im ersten Fall sind wir fertig, im zweiten Fall erhalten wir mit Lemma 1 genau $8 \cdot 6 = 48$ Elemente der Ordnung sieben. Damit bleiben noch acht Elemente übrig, die genau eine 2-Sylowgruppe bilden können, die dann wiederrum normal ist.*
*Wir erhalten also immer einen nichttrivialen Normalteiler und nach dem Auflösbarkeitskriterium dann die gewünschte Aussage.* —

*Bemerkung:* Burnside bewies 1904, dass alle Gruppen der Ordnung $p^n q^m$ auflösbar sind. Er vermutete zudem, dass alle Gruppen ungerader Ordnung auflösbar sind. Dieser Satz wurde schließlich 1962 von Feit und Thompson bewiesen und öffnete den Weg zur Klassifikation der endlichen einfachen Gruppen in den darauffolgenden Jahrzehnten.