Karlsruher Institut für Technologie
Institut für Algebra und Geometrie
PD Dr. Stefan Kühnlein  Dipl.-Math. Jochen Schröder

# Einführung in Algebra und Zahlentheorie – Übungsblatt 13

**Aufgabe 1** (4 Punkte)
Gegeben sei die Matrix $A = \begin{pmatrix} 3 & 7 \\ 6 & 4 \end{pmatrix} \in \mathbb{Z}^{2\times 2}$.

a) Für den Parameter $\alpha \in \mathbb{Z}$ sei das LGS $Ax = \begin{pmatrix} 1 \\ \alpha \end{pmatrix}$ gegeben. Benutze den Gauß-Algorithmus, um das LGS zu vereinfachen, und bestimme, für welche $\alpha$ das LGS ganzzahlig lösbar ist.

b) Finde nun unimodulare Matrizen $S, T \in \mathrm{GL}_2(\mathbb{Z})$, so dass $SAT$ in Elementarteiler-Normalform ist. Gib die Elementarteiler $a_1 | a_2$ an.

c) Was müssen $\beta, \gamma \in \mathbb{Z}$ erfüllen, damit das LGS $Ax = \begin{pmatrix} \beta \\ \gamma \end{pmatrix}$ ganzzahlig lösbar ist? Verifiziere deine Aussage aus a).

Sei nun $H = \langle \begin{pmatrix} 3 \\ 6 \end{pmatrix}, \begin{pmatrix} 7 \\ 4 \end{pmatrix} \rangle$ eine freie Untergruppe von $\mathbb{Z}^2$ vom Rang 2.

d) Zeige, dass $H$ eine echte Untergruppe von $\mathbb{Z}^2$ ist.

e) Benutze $S, T$, um Basen $B_H = \{h_1, h_2\}$ von $H$ und $B_{\mathbb{Z}^2} = \{z_1, z_2\}$ von $\mathbb{Z}^2$ zu finden, so dass $h_1 = a_1 z_1, h_2 = a_2 z_2$ gilt. (*Hinweis: Basiswechsel, lineare Algebra*)

**Lösung Aufgabe 1**
Wir sehen $\det(A) = 30$. $A$ ist also nicht ganzzahlig invertierbar, aber rational und es ist $a_1 \cdot a_2 = 30$ wegen des Determinantenmultiplikationssatzes. Kennen wir dann nicht schon die Elementarteiler, wenn jeder Primfaktor in 30 einfach ist?

a) Das LGS ist eindeutig lösbar über $\mathbb{Q}$. Es ist also genau dann über $\mathbb{Z}$ lösbar, wenn die rationale Lösung bereits ganzzahlig ist. Wir wenden den Gaußalgorithmus an, um die Lösung zu bestimmen:

$$\left(\begin{array}{cc|c} 3 & 7 & 1 \\ 6 & 4 & \alpha \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 3 & 7 & 1 \\ 0 & -10 & \alpha - 2 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 3 & 7 & 1 \\ 0 & 1 & \frac{2-\alpha}{10} \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 3 & 0 & 1 - \frac{7}{10}(2-\alpha) \\ 0 & 1 & \frac{2-\alpha}{10} \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 1 & 0 & \frac{-4+7\alpha}{30} \\ 0 & 1 & \frac{2-\alpha}{10} \end{array}\right)$$

Wir haben also die beiden Bedingungen

$$-4 + 7\alpha \equiv 0(30) \text{ und } 2 - \alpha \equiv 0(10).$$

Wenn wir den Rest modulo 30 kennen, kennen wir auch den Rest modulo 10, wir betrachten deswegen die erste Bedingung. Wir benutzen $7^{-1} = 13$ modulo 30, was wir mit dem eukldischen Algorithmus finden (!) - oder eben gut raten:
$-4 + 7\alpha \equiv 0(30) \Leftrightarrow 7\alpha \equiv 4(30) \Leftrightarrow \alpha \equiv 4 \cdot 13(30) \equiv 22(30)$.
Jedes $\alpha$ dieser Form erfüllt auch die zweite Bedingung, also ist das LGS genau für die $\alpha \in 22 + 30\mathbb{Z}$ lösbar.

b) Wir finden die Elementarteiler-Normalform durch beidseitigen Gauß-Algorithmus, also Zeilen- und Spaltenoperationen. Dabei sind natürlich nur Skalierungen um Einheiten, also – da wir uns in $\mathbb{Z}$ bewegen – ausschließlich Skalierung mit $\pm 1$ erlaubt. Vertauschungsmatrizen und Additionsmatrizen haben Determinante $\pm 1$, sind also erlaubt.
Wir beginnen mit $A$, $I_2$, $I_2$ und protokollieren die Zeilenumformungen an der ersten Einheitsmatrix

(gibt $S$), die Spaltenumformungen an der zweiten Einheitsmatrix (gibt $T$).
Aus Gründen meiner beschränkten Fähigkeit mit LaTeX schreibe ich die Umformungsschritte zur Berechnung von $S$ und $T$ unter die Umformung von $A$.

(**Bemerkung:** Die Vorgehenweise ist dabei wie folgt, das funktioniert auch mit größeren Matrizen: Durch euklidischen Algorithmus (benötigt keine Skalierung) mit allen Einträgen können wir den ggT finden – dies ist der erste Elementarteiler. Dieser wird durch Vertauschung an die erste Komponente gebracht, danach werden die restlichen Einträge der ersten Zeile und Spalte zu 0 gemacht – das geht, da alle betroffenen Einträge Vielfache des ggTs sind.
Anschließend wiederholen wir den Algorithmus mit der unteren Matrix kleineren Formats, der zweite Elementarteiler ist also der ggT der restlichen Einträge und sofort.
Es kann nicht schaden, das mal an größeren Matrizen auszuprobieren.)

$$\begin{pmatrix} 3 & 7 \\ 6 & 4 \end{pmatrix} \overset{S1}{\rightsquigarrow} \begin{pmatrix} 3 & 1 \\ 6 & -8 \end{pmatrix} \overset{S2}{\rightsquigarrow} \begin{pmatrix} 1 & 3 \\ -8 & 6 \end{pmatrix} \overset{S3}{\rightsquigarrow} \begin{pmatrix} 1 & 0 \\ -8 & 30 \end{pmatrix} \overset{S4}{\rightsquigarrow} \begin{pmatrix} 1 & 0 \\ 0 & 30 \end{pmatrix}.$$

Dabei machen wir folgende Umformungen, die wir in $S$ und $T$ festhalten:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \overset{S1}{\rightsquigarrow} \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \overset{S2}{\rightsquigarrow} \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \overset{S3}{\rightsquigarrow} \begin{pmatrix} -2 & 7 \\ 1 & -3 \end{pmatrix} = T.$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \overset{S4}{\rightsquigarrow} \begin{pmatrix} 1 & 0 \\ 8 & 1 \end{pmatrix} = S.$$

Die Elementarteiler sind 1 und 30, was man auch schneller hätte ablesen können: Der erste Elementarteiler ist stets der ggT aller Matrixeinträge, den zweiten erhalten wir dann aus der Determinante unter Zuhilfenahme des Determinantenmultiplikationssatzes. Das geht so direkt natürlich nur bei $(2 \times 2)$-Matrizen.
Aber auch dann bekommen wir die Elementarteiler oft ohne Rechnen. Ist wie hier die Determinante quadratfrei (mit $d =\mid \det \mid$), so sind die Elementarteiler wegen der Teilbarkeitsbedingung stets $1|1|...|1|d$, nicht wahr?

c) Sicher ist $Ax = b$ genau dann lösbar, wenn $SAx = Sb$ lösbar ist, denn $S$ ist ja invertierbar. Wie bekommen wir $T$ in die Gleichung hinein?
Es ist $SAx = b$ genau dann lösbar, wenn $SATy = b$ lösbar ist, denn löst $x$ das LGS $SAx = b$, so löst $y = T^{-1}x$ das LGS $SATy = b$ und umgekehrt finden wir $x = Ty$ als Lösung von $SAx = b$, wenn $y$ das LGS $SATy = Sb$ löst.

(**Anmerkung:** Hier geht es nicht nur um die Lösbarkeit, wir sehen ja auch direkt ein, wie wir $x$ finden, das $Ax = b$ löst, wenn wir das einfache LGS $SATy = Sb$ lösen, dessen Koeffizientenmatrix diagonal ist! Das sollte man sich klar machen und hiermit auch mal konkret ein LGS ohne Gauß-Algorithmus lösen, vielleicht ein LGS aus a) mit passendem $\alpha$?)

Also ist $Ax = b$ lösbar, wenn $SATy = Sb$ lösbar ist, was dem LGS $\begin{pmatrix} 1 & 0 & | & \alpha \\ 0 & 30 & | & 8\alpha + \beta \end{pmatrix}$ entspricht, das genau dann ganzzahlig lösbar ist, wenn $\alpha + 8\beta$ ein 30-Vielfaches ist.
Für $\beta = 1$ erhalten wir dann zum Beispiel genau unsere Bedingung aus Aufgabenteil a).

d) Die Elemente aus $H$ sind genau die ganzzahligen Linearkombinationen $a \cdot \begin{pmatrix} 3 \\ 6 \end{pmatrix} + b \cdot \begin{pmatrix} 7 \\ 4 \end{pmatrix}$, was nach Definition genau dem Bild von $A$ als $\mathbb{Z}$-lineare Abbildung entspricht und da haben wir doch in a) und c) Vektoren gesehen, die nicht im Bild liegen, zum Beispiel

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} \notin H.$$

e) Hier müssen wir uns an die lineare Algebra erinnern, an Abbildungsmatrizen und vor allem Basiswechsel, jeweils vor allem, wie man diese berechnet.
Sei $i : H \to \mathbb{Z}^2, h \mapsto h$ die kanonische Einbettung, so ist $A$ die Abbildungsmatrix $A = D_{CB}(i)$, wobei $C$ die Standardbasis $\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$ von $\mathbb{Z}^2$ und $B$ die Basis $\{\begin{pmatrix} 3 \\ 6 \end{pmatrix}, \begin{pmatrix} 7 \\ 4 \end{pmatrix}\}$ von $H$ ist.

Unsere Aufgabe ist es, die Basen $B_H = \{h_1, h_2\}, B_{\mathbb{Z}^2} = \{z_1, z_2\}$ so zu finden, dass die Abbildungsmatrix $D_{B_{\mathbb{Z}^2} B_H}(i)$ durch die Matrix $SAT$ gegeben ist, dann erfüllen die $h_i, z_i$ gerade die

geforderte Bedingung.
(Hierbei geht natürlich wieder ein, wie die Abbildungsmatrix berechnet wird. Insbesondere sehen wir auch, dass diese Bedingung tatsächlich äquivalent dazu ist, dass unsere Basen die geforderte Bedinung erfüllen.)

In der Linearen Algebra lernen wir, dass $D_{B_{\mathbb{Z}^2}B_H}(i) = D_{B_{\mathbb{Z}^2}C}(\mathrm{id}_{\mathbb{Z}^2}) \cdot D_{CB}(i) \cdot D_{BB_H}(\mathrm{id}_H)$ ist.
Wir sind also fertig, wenn $S$ die Basiswechselmatrix $D_{B_{\mathbb{Z}^2}C}(\mathrm{id}_{\mathbb{Z}^2})$ und $T$ die Basiswechselmatrix $D_{BB_h}(\mathrm{id}_H)$ ist.
(**Bemerkung:** Das ist jetzt aber ein hinreichendes, kein notwendiges Kriterium an unsere neuen Basen, damit sie die geforderte Bedinung erfüllen. $S, T$ sind mögliche Belegungen für die Basiswechselmatrizen, aber nicht eindeutig! Klar, wenn wir $B_H, B_{\mathbb{Z}^2}$ passend gefunden haben, können wir zum Beispiel alles mit $-1$ durchmultiplizieren, um andere passende Basen zu finden. $S$ und $T$ waren ja auch nicht eindeutig...
Tatsächlich finden wir ja eine Bijektion zwischen den Basen und Basiswechselmatrizen, wenn $B, C$ fest gegeben sind... Basen, die die geforderte Eigenschaft besitzen, gehören zu Matrizen, die die Matrix $A$ in Elementarteiler-Diagonalform bringen und umgekehrt...
Das ist alles lineare Algebra.)

Wir haben also jeweils Basiswechselmatrizen und eine Basis gegeben, die Aufgabe ist es, die jeweils passende Basis zu finden. Dabei müssen wir unterschiedlich vorgehen, je nachdem, ob die Ausgangs- oder Zielbasis gegeben ist.

- $S = D_{B_{\mathbb{Z}^2}C}(\mathrm{id}_{\mathbb{Z}^2}) = \begin{pmatrix} 1 & 0 \\ 8 & 1 \end{pmatrix}$, $C$ ist die Standardbasis.
  Wir finden $B_{\mathbb{Z}^2}$ als Spalten der Inversen zu $S$, denn das sind doch die Koordinatenvektoren zur Standardbasis (sieht man nicht!) der Bilder unter Id (sieht man nicht!) der Basisvektoren. (LA again!)
  Es ist $S^{-1} = \begin{pmatrix} 1 & 0 \\ -8 & 1 \end{pmatrix}$, also $z_1 = \begin{pmatrix} 1 \\ -8 \end{pmatrix}$, $z_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.
- $T = D_{BB_H}(\mathrm{id}_H)$, $B$ wie oben gegeben.
  Die Spalten sind doch einfach die Koordinatenvektoren von den Vektoren aus $B_H$ zur Zielbasis $B$ und wir berechnen
  $h_1 = -2\begin{pmatrix} 3 \\ 6 \end{pmatrix} + 1\begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 1 \\ -8 \end{pmatrix}$ und $h_2 = 7\begin{pmatrix} 3 \\ 6 \end{pmatrix} - 3\begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 \\ 30 \end{pmatrix}$.

**Nachtrag:** Da wir wissen, was unsere Basisvektoren erfüllen werden/erfüllen müssen, hätte einer der beiden Berechnungsschritte gereicht, nicht wahr? Aber es ist doch ganz schön, beides zu berechnen und zu sehen, dass wir uns nicht verrechnet haben!

**Aufgabe 2** (4 Punkte) *alte Klausuraufgaben, wo man hinschaut...*
Es sei $G$ eine endliche abelsche Gruppe von Ordnung $n \in \mathbb{N}$. Zeige die Äquivalenz der folgenden Aussagen:

i) $G$ ist zyklisch.

ii) Für alle Teiler $d$ von $n$ gibt es genau eine Untergruppe von $G$ mit Ordnung $d$.

iii) Für alle Teiler $d$ von $n$ gibt es höchstens eine Untergruppe von $G$ mit Ordnung $d$.

**Lösung Aufgabe 2**
„(ii) $\Rightarrow$ (iii)“ ist offensichtlich.

„(iii) $\Rightarrow$ (i)“: $G$ ist eine endlich erzeugte abelsche Gruppe (als endliche Gruppe ist $G$ sicher endlich erzeugt, nicht wahr?) und wir können den Struktursatz anwenden. Dabei treten wegen der Endlichkeit der Gruppe in der Darstellung von $G$ keine Faktoren $\mathbb{Z}$ auf. Also gibt es $e_1|e_2|...|e_r$ mit $G \simeq \bigoplus_{i=1}^r \mathbb{Z}/e_i\mathbb{Z}$.
Wäre für $i < r$ $e_i \neq 1$, so gäbe es wegen $e_i|e_{r-1}|e_r$ ein $p \in \mathbb{P}$ mit $p|e_{r-1}$ und $p|e_r$, insbesondere haben die Restklassen $a_1 = \overline{\frac{e_{r-1}}{p}}$ und $a_2 = \overline{\frac{e_r}{p}}$ Ordnung $p$ in $\mathbb{Z}/e_{r-1}\mathbb{Z}$ beziehungsweise $\mathbb{Z}/e_r\mathbb{Z}$.
Dann aber sind $(0, ..., 0, a_1, 0)$ und $(0, ..., 0, a_2)$ verschiedene Elemente der Ordnung $p$ in $\bigoplus_{i=1}^r \mathbb{Z}/e_i\mathbb{Z}$. Dies

ist ein Widerspruch zur Voraussetzung.
Es folgt, dass $G \simeq \mathbb{Z}/e_r\mathbb{Z}$ ist, also zyklisch. (Dann ist natürlich $e_r = n$.)

„(i) $\Rightarrow$ (ii)": Ohne Einschränkung ist $G = \mathbb{Z}/n\mathbb{Z}$. Sei $d$ ein beliebiger Teiler von $n$.
**Existenz:** Die Restklasse $\overline{\frac{n}{d}}$ erzeugt eine Untergruppe von Ordnung $d$. Dies zeigt die Existenz.
**Eindeutigkeit:** Für jedes Element $\overline{z}$ von $G$ sei $z$ als Vertreter aus $\{0, ..., n-1\}$ gewählt. Dies gibt eine $\leq$-Anordnung auf $G$.
Sei nun eine beliebige Untergruppe $U$ von $G$ mit $\#(U) = d$ gegeben. Dann gibt es bezüglich $\leq$ ein minimales Element $\overline{x}$ in $U$. Für alle $\overline{u} \in U$ können wir mithilfe des euklidischen Algorithmus den ggT $g$ von $x, u$ konstruieren, es ist $g \leq x$, $\overline{g} \in U$, also wegen der Minimalität von $\overline{x}$ muss $x = g$ gelten, was einfacher ausgedrückt besagt, dass $x$ alle $u$ mit $\overline{u} \in U$ teilt, insbesondere auch $n$. Außerdem zeigt das, dass $\overline{x}$ ein Erzeuger der Gruppe $U$ ist.
Dann aber ist $x = \frac{n}{d'}$ für einen Teiler $d'$ von $n$ und $\#U = d'$, woraus direkt $d' = d$ folgt. Es gibt also höchstens eine Gruppe mit Mächtigkeit $d$.

**Aufgabe 3** (4 Punkte)
Gegeben sei die symmetrische Gruppe $S_7$ und $H = \{h \subseteq S_7 : \#h = 7\}$ die Menge der 7-Sylowgruppen. $S_7$ operiert auf $H$ durch Konjugation.

a) Bestimme $\#H$.

b) Bestimme die Mächtigkeit des Stabilisators von $h$ für ein beliebiges $h \in H$.

c) Zeige, dass es keine Untergruppe der Ordnung 140 von $S_7$ gibt.

**Lösung Aufgabe 3:**

a) Wegen $\#S_7 = 7 \cdot 6!$ mit $7 \nmid 6!$ sind die 7-Sylow-Gruppen tatsächlich die Elemente aus $H$. Da jede Gruppe mit 7 Elementen zyklisch ist, sind die 7-Sylow-Gruppen genau die Untergruppen, die von Elementen der Ordnung 7 erzeugt werden.
Jede Permuation lässt sich als Produkt disjunkter Zykel darstellen, die Ordnung ist das Produkt der Einzelordnungen der Zykel. Dies zeigt, dass die Elemente der Ordnung 7 genau die 7-Zykel sind. Es stellt sich also die Frage, wieviele 7-Zykel es gibt. Ein 7-Zykel $\sigma$ ist gegeben durch
$$\sigma = (1\ \sigma(1)\ \sigma^2(1)\ ...\ \sigma^6(1)).$$
Der Rest ist simple Kombinatorik:
Für $\sigma(1)$ gibt es die 6 Möglichkeiten $2, 3, 4, 5, 6, 7$, für jede dieser Wahlen dann nur noch 5 Möglichkeiten für $\sigma^2(1)$ usf. Damit ehalten wit 6! 7-Zykel in $S_7$.

Wieviele 7-Gruppen gibt es also? Wir wissen, dass jeweils sechs 7-Zykel die selbe Untergruppe erzeugen (mit $\sigma$ nämlich noch die Potenzen $\sigma^2, ..., \sigma^6$, schließlich ist das in der zu $\langle\sigma\rangle$ isomorphen Gruppe $\mathbb{Z}/7\mathbb{Z}$ so), verschiedene 7-Gruppen haben bis auf die Identität trivialen Schnitt - hätten sie ein nichttriviales Element $\tau$ gemeinsam, so würde das ja beide Untergruppen erzeugen, diese wären also gleich. Es gibt also $6!/6 = 5!$ verschiedene 7-Gruppen, dies ist $\#H$.

*Hinweis:* Mit den Sylow-Sätzen kommen wir bei der Aufgabe nicht weiter, die Anzahl der 7-Sylow-Gruppen ist $\equiv 1(7)$ und teilt 6!, das ist nicht eindeutig.

b) Je zwei Elemente aus $H$ sind konjugiert nach Sylow. Das aber impliziert direkt, dass die Operation transitiv ist, dass $H$ also die einzige Bahn ist.
Wir erinnern uns an den Beweis der Bahnbilanzformel, in dem wir Stabilisator und Bahn eines Elementes in Verbindung gebracht haben.
Die Mächtigkeit der Bahn $S_7 h = H$ ist der Index $[S_7 : \mathrm{Stab}_h] = \frac{\#S_7}{\#\mathrm{Stab}_h}$ und Umstellen ergibt $\#\mathrm{Stab}_h = \frac{\#S_7}{\#H} = \frac{7!}{5!} = 42$.
(Fans des Anhalters durch die Galaxis hätten das natürlich vorher schon gewusst.)

c) Nehmen wir an, es gebe eine solche Untergruppe $U$. Wieviele 7-Sylow-Gruppen besitzt $U$? Jetzt können wir das machen, was in a) nicht geklappt hat - die Sylow-Sätze anwenden:
Wegen $140 = 7 \cdot 20$ und da 1 der einzige Teiler von 20 ist, der $\equiv 1(7)$ ist, gibt es genau eine 7-Sylow-Gruppe $h_0$, auf der $U$ wieder durch Konjugation operiert, offensichtlich nun trivial, was bleibt $U$

auch anderes übrig?
In der Operation von $S_7$ auf $H$ ist $U$ dann im Stabilisator von $h_0$ enthalten, aber das ist ein Widerspruch wegen $\#U > 42 = \#\mathrm{Stab}_{h_0}$.

**Aufgabe 4** (4 Punkte)
Eine nichttriviale Gruppe $G$ heißt einfach, wenn sie nur die trivialen Normalteiler $\{e_G\}, G$ besitzt. Sei nun $G$ eine Gruppe. Zeige die folgenden Aussagen:

a) Sei $H \subseteq G$ eine Untergruppe, so dass es keine weitere Untergruppe der gleichen Ordnung gibt. Dann ist $H$ ein Normalteiler von $G$.

b) Sei $\#G = 40$. Dann ist $G$ nicht einfach.

c) Sei $\#G = 24$. Dann ist $G$ nicht einfach. (*Hinweis:* Sollte der Trick aus Aufgabenteil b) nicht funktionieren, so könnte die Gruppenoperation aus Aufgabe 3 helfen.)

**Lösung Aufgabe 4**
In dieser Aufgabe bezeichnen wir mit $s_p$ stets die Anzahl der $P$-Sylow-Gruppen.

a) Es reicht zu zeigen, dass für ein $g \in G$ und eine beliebige Untergruppe $H \subseteq G$ $gHg^{-1}$ eine Untergruppe der gleichen Ordnung ist (**Behauptung**). Dann muss – unter der zusätzlichen Bedingung, dass $H$ die einzige Gruppe der Ordnung $\#H$ ist – $gHg^{-1} = H$ für alle $g \in G$ gelten, also ist $H$ ein Normalteiler.

   Der **Beweis der Behauptung** ist nicht schwer.
   $e_G \in H$, also ist $ge_Gg^{-1} = e_G \in gHg^{-1}$, letzteres also nicht leer.
   Seien $x, y \in gHg^{-1}$, dann gibt es $x', y' \in H$: $x = gx'g^{-1}, y = gy'g^{-1}$ und es ist
   $xy^{-1} = (gx'g^{-1})(gy'g^{-1})^{-1} = gx'g^{-1}gy'^{-1}g^{-1} = gx'x'^{-1}g^{-1} \in gHg^{-1}$.

   Die Zuordnung $H \mapsto gHg^{-1}$, $h \mapsto ghg^{-1}$ ist offensichtlich surjektiv und wegen der Kürzungsregel in Gruppen auch injektiv, also sind $H$ und $gHg^{-1}$ gleichmächtig.

   (**Bemerkung:** Diese Aussage haben wir indirekt schon in Aufgabe 3 verwendet, sie steckt in der dort unbewiesenen Behauptung, dass $S_7$ auf den 7-Sylow-Gruppen operiert...)

b) Es ist $\#G = 2^3 \cdot 5$ und wir finden $s_5|8, s_5 \equiv 1(5)$ nach den Sylowsätzen. Offensichtlich folgt $s_5 = 1$, was bedeutet, dass es genau eine Gruppe mit 5 Elementen gibt[1], die nach a) ein Normalteiler ist.

c) Es ist $\#G = 2^3 \cdot 3$ und wir finden folgende Bedingungen an $s_3, s_2$:
   $s_3|4, s_3 \equiv 1(3) \Rightarrow s_3 \in \{1, 4\}$
   $s_2|3, s_2 \equiv 1(2) \Rightarrow s_2 \in \{1, 3\}$.

   Wieder mit a) sind wir fertig, wenn $s_2 = 1$ oder $s_3 = 1$ ist. Ist dies nicht der Fall, so sei mit $K$ die Menge der 2-Sylow-Gruppen[2] bezeichnet. $G$ operiert auf $K$ durch Konjugation.
   Die Operation entspricht einem Gruppenhomomorphismus $\varphi : G \to \mathrm{Sym}(K) \cong S_3$.

   Da zwei 2-Sylow-Gruppen nach den Sylow-Sätzen konjugiert sind, ist die Operation transitiv, insbesondere also nichttrivial (an dieser Stelle brauchen wir natürlich, dass es mehr als eine 2-Sylow-Gruppe gibt, nicht wahr?), also ist $\mathrm{Kern}(\varphi) \neq G$.
   Aber wegen $\#G = 24 > 6 = \#\mathrm{Sym}(K)$ ist $\varphi$ nicht injektiv, also $\mathrm{Kern}(\varphi) \neq \{e_G\}$.

   Der Kern ist also ein nichttrivialer Normalteiler.

   (**Nachtrag:** Wieso würde der Beweis so nicht funktionieren, wenn wir $G$ auf der vierelementigen Menge der 3-Sylow-Gruppen operieren lassen?)

---

[1] Wir erinnern uns, dass die hochtrabende Bezeichnung $p$-Sylow-Gruppe ja nur mit der Mächtigkeit der Untergruppe zu tun hat.

[2] Auch wenn es an dieser Stelle unbedeutend ist, sei hier noch einmal erwähnt, dass die 2-Sylow-Gruppen acht Elemente haben, nicht zwei...