Die einfache nicht-abelsche Gruppe mit 168 Elementen

Tobias Strubel & Merten Lampe
Vortrag zur Algebra I
TU Clausthal

letzte Änderung: 16. April 2003

Einleitung:
Nachdem in der Vorlesung [El2002] gezeigt worden ist, dass die kleinste einfache nicht-abelsche Gruppe die A_5 mit Ordnung 60 ist, wollen wir die Existenz der nächstgrößeren, der $GL(3, \mathbb{F}_2)$ mit 168 Elementen, beweisen.
Dazu werden wir in drei Schritten zeigen, dass

I) keine einfache nicht-abelsche Gruppe G mit $60 < |G| < 168$ existiert.

II) die Gruppe $GL(3, \mathbb{F}_2)$ einfach ist.

III) es keine weiteren einfachen nicht-abelschen Gruppen mit 168 Elementen gibt.

Schritt I

Es gibt keine einfache nicht-abelsche Untergruppe G mit $60 < |G| < 168$.

1.1 Wiederholung

Für die weiteren Schritte sind Kenntnisse des Argumentes von Poincaré, des Korrespondenzprinzips und der Eigenschaften des Normalisators nötig - wir werden sie hier noch einmal auffrischen.

Poincarés Argument

Sei $H \leq G$ eine Untergruppe mit Index $|G : H| = n$, dann gibt es eine Untergruppe $K \leq H$ mit $K \trianglelefteq G$ und

$$n \mid \ |G : K| \ \mid n!$$

Dieser Normalteiler kann auch trivial, also $\{e\}$ oder G sein.

- Falls man $H \neq G$ gewählt hat, so ist $n \geq 2$ und wegen $n \mid \ |G : K|$ muss gelten:
  $$|G : K| \neq 1, \text{ also } K \neq G.$$
- Nimmt man an, dass $K = \{e\}$ gilt, dann folgt $|G : K| = |G|$ und damit $|G| \ \mid n!$

Demnach reicht es also, nach einer großen Untergruppe $H < G$ zu suchen, deren "Index-Fakultät" nicht von der Gruppenordung geteilt wird. Existiert eine solche Untergruppe H, dann ist die Gruppe G nicht einfach.

Der Normalisator

Der Normalisator von P in G

$$N_G(P) := \{g \in G \mid gPg^{-1} = P\}$$

ist die größte Untergruppe von G mit

$$P \trianglelefteq N_G(P).$$

Es gelten folgende Aussagen:

- $|G : N_G(P)| =$ Anzahl Konjugierte von P

- $P \trianglelefteq H \Rightarrow N_G(P) \geq H$ [1]
- $N_G(P) = G \Rightarrow P \trianglelefteq G$ [2]
- $T := A \cap B \Rightarrow A, B \leq N_G(T)$ [3]

Das Korrespondenzprinzip

Sei $N \trianglelefteq G$, dann gilt
$$H^* \triangleleft G/N \longleftrightarrow N \leq H \triangleleft G.$$
Das heißt, dass man zu jeder Untergruppe einer Faktorgruppe von G einen korrespondierenden Normalteiler der Gruppe G findet, der zwischen G und dem herausfaktorisierten Normalteiler liegt.
Man kann so zB. aus nicht vorhandenen Untergruppen einer Faktorgruppe schließen, dass der herausfaktorisierte Normalteiler maximal in G war.
Weiterhin kann man zeigen, dass sich der Index dieser korrespondierenden Untergruppen nicht verändert.

1.2 Ausschluß einfacher Gruppenordnungen

Seien im Folgenden p und q Primzahlen.
Zu Gruppenordnungen $|G|$ mit folgender Primfaktorzerlegung existieren keine einfachen nicht-abelschen Gruppen:

- $|G| = p^n$.
  - Für $n = 1$ ist G eine abelsche Gruppe und wir suchen nicht-abelsche Gruppen.

  - Für $n > 1$ wurde gezeigt, dass das Zentrum von G
    $$Z(G) := \{g \in G \mid \forall\ h \in G: \ hgh^{-1} = g\}$$
    nicht trivial ist [4]:
    $$Z(G) - \{e\} \neq \emptyset.$$
    Da das Zentrum aber immer Normalteiler ist, folgt entweder,
    * dass wir mit diesem einen nicht-trivialen Normalteiler haben oder
    * dass $Z(G) = G$ gilt; womit G aber abelsch wäre.

- $|G| = p^n r$ mit $p > r \in \mathbb{N}$.
  Für *oBdA* $r > 1$ gilt nach den Sylow-Sätzen
  $$s_p \equiv 1 \mod p$$
  und
  $$s_p \mid r,$$
  woraus wegen $p > r$ nur $s_p = 1$ folgen kann.
  Dieses bedeutet aber, dass die p-Sylow-Gruppe Normalteiler ist [5]. □

[1] Da P Normalteiler in H ist, lassen mindestens alle $h \in H$ die Gruppe P invariant.
[2] Da alle Elemente $g \in G$ die Gruppe P invariant lassen.
[3] Die Elemente von A und B lassen die von T invariant, da es ja ihre eigenen sind...
[4] Beweis über die Bahnengleichung
[5] siehe Sylow-Sätze in der Vorlesung

1.3 Ausschluß weiterer Gruppenordnungen

Nach Anwendung des obigen Lemmas sind von den ursprünglichen 107 Gruppenordnungen noch folgende 20 übrig:

$$63, 70, 72, 80, 84, 90, 96, 105, 108, 112, 120$$

$$126, 132, 135, 140, 144, 150, 154, 160, 165$$

Anwendung von Poincaré

Folgende Gruppen können mit Poincarés Argument abgehandelt werden:

- $80 = 2^4 \cdot 5$
  Die 2-Sylow-Gruppe hat mit 16 Elementen Index 5 in G. Deshalb ist G wegen $80 \not| 5!$ nicht-einfach.
- $96 = 2^5 \cdot 3$
  Die 2-Sylow-Gruppe hat mit 32 Elementen Index 3 in G. Deshalb ist G wegen $96 \not| 3!$ nicht-einfach.
- $108 = 2^2 \cdot 3^3$
  Die 3-Sylow-Gruppe hat mit 27 Elementen Index 4 in G. Deshalb ist G wegen $108 \not| 4!$ nicht-einfach.
- $135 = 3^3 \cdot 5$
  Die 3-Sylow-Gruppe hat mit 27 Elementen Index 5 in G. Deshalb ist G wegen $135 \not| 5!$ nicht-einfach.
- $150 = 2 \cdot 3 \cdot 5^2$
  Die 5-Sylow-Gruppe hat mit 25 Elementen Index 6 in G. Deshalb ist G wegen $150 \not| 6!$ nicht-einfach.
- $160 = 2^5 \cdot 5$
  Die 2-Sylow-Gruppe hat mit 32 Elementen Index 5 in G. Deshalb ist G wegen $160 \not| 5!$ nicht-einfach.

Anwendung der Sylow-Sätze

Folgende Gruppen können nach Anwendung der Sylow-Sätze als nicht-einfach beiseite gelegt werden:

- $63 = 3^2 \cdot 7$
  $$s_7 \equiv 1 \mod 7 \ \wedge \ s_7 \mid 9 \ \Rightarrow \ s_7 = 1.$$
- $70 = 2 \cdot 5 \cdot 7$
  $$s_5 \equiv 1 \mod 5 \ \wedge \ s_5 \mid 14 \ \Rightarrow \ s_5 = 1.$$
- $84 = 2^2 \cdot 3 \cdot 7$
  $$s_7 \equiv 1 \mod 7 \ \wedge \ s_7 \mid 12 \ \Rightarrow \ s_7 = 1.$$
- $126 = 2 \cdot 3^2 \cdot 7$
  $$s_7 \equiv 1 \mod 7 \ \wedge \ s_7 \mid 18 \ \Rightarrow \ s_7 = 1.$$

- $140 = 2^2 \cdot 5 \cdot 7$

$$s_7 \equiv 1 \mod 7 \ \wedge \ s_7 \mid 20 \ \Rightarrow \ s_7 = 1.$$

- $154 = 2 \cdot 7 \cdot 11$

$$s_{11} \equiv 1 \mod 11 \ \wedge \ s_{11} \mid 14 \ \Rightarrow \ s_{11} = 1.$$

- $165 = 3 \cdot 5 \cdot 11$

$$s_{11} \equiv 1 \mod 11 \ \wedge \ s_{11} \mid 15 \ \Rightarrow \ s_{11} = 1.$$

1.4 Betrachtung der verbliebenen Gruppen

Mittlerweile sind von den ursprünglich 107 Gruppenordnungen nur noch folgende 7 übrig:

$$72, 90, 105, 112, 120, 132, 144$$

Diese werden wir nun einzeln betrachten und zeigen, dass sie allesamt nicht einfach sein können:

- $72 = 2^3 \cdot 3^2$

  $$s_3 \equiv 1 \mod 3 \ \wedge \ s_3 \mid 8 \ \Rightarrow \ s_3 \in \{1, 4\}$$

  Da für $s_3 = 1$ mit der 3-Sylow-Gruppe bereits ein Normalteiler gefunden wäre, sei *oBdA* $s_3 = 4$.
  Dann gibt es 4 konjugierte 3-Sylow-Gruppen. Wähle eine beliebige P davon aus und betrachte deren Normalisator $N_G(P)$. Es gilt

  $$|G : N_G(P)| = 4$$

  und deshalb [6] ex. nach Poincaré ein nicht-trivialer Normalteiler.

- $90 = 2 \cdot 3^2 \cdot 5$

  $$s_5 \equiv 1 \mod 5 \ \wedge \ s_5 \mid 18 \ \Rightarrow \ s_5 \in \{1, 6\}$$

  $$s_3 \equiv 1 \mod 3 \ \wedge \ s_3 \mid 10 \ \Rightarrow \ s_3 \in \{1, 10\}$$

  Mit *oBdA* $s_5 = 6$ gibt es $6 \cdot 4 = 24$ Elemente der Ordnung 5, demnach ist für 10 eins-disjunkte[7] konjugierte ($10 \cdot 8 = 80$ Elemente) 3-Sylow-Gruppen kein Platz.
  Also schneiden sich zwei dieser Konjugierten A, B zu einer neuen Gruppe [8] $T := A \cap B$ mit Ordnung 3 und $T < A, B$.

  Deren Normalisator $N_G(T)$ enthält A und B als Untergruppen, hat also eine Ordnung größer 9 und diese teilt $|G| = 90$. Es gilt $|N_G(T)| \in \{18, 45, 90\}$.

  - Falls $|N_G(T)| = 90$, dann ist $N_G(T) = G$ und damit T Normalteiler in G - wir sind fertig.

[6] wegen $N_G(P) \leq G$, Index 4 und $72 \nmid 4!$
[7] eins-disjunkt bedeutet disjunkt bis auf die Eins - gilt bei Primzahlordnung auf jeden Fall...
[8] Ordnung muss 9 teilen und ungleich 1 bzw. 9 sein...

  - Falls $|N_G(T)| = 45$, dann wäre $N_G(T)$ aus Indexgründen normal in G und wir sind fertig.
  - Falls $|N_G(T)| = 18$, dann wenden wir Poincaré an und erfahren, dass der index zur Fakultät 5!=120 von $|G|$ =90 geteilt werden muss. Da dieses nicht zutrifft, gibt es auch hier einen nicht-trivialen Normalteiler.

- $105 = 3 \cdot 5 \cdot 7$

$$s_7 \equiv 1 \mod 7 \ \wedge \ s_7 \mid 15 \ \Rightarrow \ s_7 \in \{1, 15\}$$
$$s_5 \equiv 1 \mod 5 \ \wedge \ s_5 \mid 21 \ \Rightarrow \ s_2 \in \{1, 21\}$$

  Nun kann es nicht gleichzeitig 15 Sylow-7-Gruppen und 21 Sylow-5-Gruppen geben, denn dafür sind nicht die nötigen $21 \cdot 4 + 15 \cdot 6 + 1 = 175$ Elemente vorhanden.
  Demnach gilt entweder $s_7 = 1$ oder $s_5 = 1$ und wir haben auf jeden Fall einen Normalteiler.

Die beiden folgenden Gruppenordnungen 112 und 120 gehen im Umfang weit über die anderen hinaus und werden hier deshalb nicht behandelt - die einzelnen Beweis-Schritte ähneln jedoch den gezeigten. Interessierte Leser können die Beweise in [ST2002, S. 134ff] nachlesen.

- $112 = 2^4 \cdot 7$
  Fakt!

- $120 = 2^3 \cdot 3 \cdot 5$
  Fakt!

- $132 = 2^2 \cdot 3 \cdot 11$

$$s_{11} \equiv 1 \mod 11 \ \wedge \ s_{11} \mid 12 \ \Rightarrow \ s_{11} \in \{1, 12\}$$

  Sei *oBdA* $s_{11} = 12$, dann haben die eins-disjunkten Konjugierten genau 120 Elemente der Ordnung 11 und die Eins.
  Betrachte nun

$$s_3 \equiv 1 \mod 3 \ \wedge \ s_3 \mid 44 \ \Rightarrow \ s_3 \in \{1, 4, 11\}$$

  Für $s_3 = 11$ haben wir nicht die erforderlichen 22 Elemente, also *oBdA* $s_3 = 4$.
  Betrachte nun die Sylow-2-Gruppen, für diese stehen dann wegen

$$132 - 120 - 8 - 1 = 3$$

  nur noch 3 Elemente der Ordnung 2^r zur Verfügung. Demnach kann es nur genau eine 2-Sylow-Gruppe geben, bestehend aus diesen 3 Elementen und der Eins.
  Wieder haben wir auf jeden Fall einen Normlateiler.

- $144 = 2^4 \cdot 3^2$

$$s_3 \equiv 1 \mod 3 \ \wedge \ s_3 \mid 16 \ \Rightarrow \ s_3 \in \{1, 4, 16\}$$

- Falls $s_3 = 4$, dann ist $|G : N_G(P)| = 4$ für eine beliebige 3-Sylow-Gruppe P und damit folgt nach Poincaré die Existenz eines nichttrivialen Normalteilers.
- Also ist *oBdA* $s_3 = 16$.
  * Angenommen die Konjugierten seien eins-disjunkt, dann verbrauchen sie $16 \cdot 8 + 1 = 129$ Elemente der Ordnungen 1, 3 und 9. Die verbleibenden 15 reichen für eine einzelne Sylow-2-Gruppe, diese ist Normalteiler.
  * Also schneiden sich *oBdA* zwei Sylow-3-Gruppen A, B in einer nichttrivialen Gruppe $T = A \cap B$ mit Ordnung 3.
    Nun ist wieder $A, B \leq N_G(T)$ und für die Ordnung bleibt nur $|N_G(T)| \in \{18, 36, 72, 144\}$
    · Für $|N_G(T)| = 144$ wäre ja $N_G(T) = G$ und damit T Normalteiler - wir sind fertig.
    · Für $|N_G(T)| = 72$ ist $|G : N_G(T)| = 2$ und damit wäre $N_G(T)$ normal in G - fertig.
    · $|N_G(T)| = 36$ scheitert nach Poincaré, da $4! = 24$ nicht von 144 geteilt wird.
    · $|N_G(T)| \neq 18$, denn dann hätte $N_G(T)$ als Gruppe mit 18 Elementen eine Sylow-3-Gruppe zum Normalteiler, was uns ein bißchen stört, da ja zumindest zwei (nämlich A und B) drin sein sollten.

Letztendlich ist nun gezeigt, dass es keine einfache nicht-abelsche Untergruppe G mit $60 < |G| < 168$ gibt. $\square$

Schritt II

Nachdem wir im ersten Schritt gezeigt haben, dass bei Gruppenordnungen zwischen 60 und 168 keine nicht-einfachen Gruppen existieren, wollen wir nun eine einfache Gruppe mit 168 Elementen vorstellen.

2.1 Die Gruppe $GL(3, \mathbb{F}_2)$

Diese Gruppe besteht aus den invertierbaren 3x3 Matrizen über dem zweielementigen Körper $\mathbb{F}_2$.

Anmerkungen zum Körper Ein Vektor b in $\mathbb{K}^d$ ist zu anderen a_i linear abhängig, wenn gilt:

$$b = \sum_{k=0}^{N} c_k a_k$$

wobei $c_i \in \mathbb{K}$. Demnach bleibt für linare Abhängigkeit in $\mathbb{F}_2^d$ nur über:

$$b = \sum_{k=0}^{N} e_k$$

mit e_k entweder Null oder a_k.

Berechnung der Mächtigkeit Für $A \in GL(3, \mathbb{F}_2)$ muss gelten: $\det A \neq 0$.

- Die erste Spalte darf den Nullvektor nicht enthalten, also gibt es hierfür $2^3 - 1$ Möglichkeiten für die Vektoren.
- Die zweite Spalte darf nicht linear abhängig von der ersten sein, das heißt nach obiger Bemerkung, dass sie weder Null, noch der erste Vektor sein darf. Also gibt es $2^3 - 1 - 1$ solche Vektoren.
- Die dritte Spalte darf zu den ersten beiden nicht linear abhängig sein, darf also nach obiger Bemerkung weder Null, noch eine der beiden anderen, noch deren Summe sein. Also gibt es $2^3 - 1 - 1 - 1 - 1$ solcher Vektoren.

Insgesamt ergibt sich damit eine Mächtigkeit von $(8 - 1)(8 - 2)(8 - 4) = 168$.

2.2 $GL(3, \mathbb{F}_2)$ ist einfach

Für $168 = 2^3 \cdot 3 \cdot 7$ nehmen wir an, dass es nicht-triviale Normalteiler $1 \neq N \triangleleft G$ gäbe und wählen den größten.
Dann ist G/N eine einfache Gruppe, da man sonst nach dem Korrespondenzsatz einen weiteren Normalteiler $N \leq K \triangleleft G$ finden könnte.
$|G/N| = |G : N|$ muss Teiler von 168 sein, also bleibt nur $G/N \in \{C_2, C_3, C_7\}$.
Wegen $|G/N| = |G : N| \in \{2, 3, 7\}$ muss also jeder mögliche Normalteiler Index 2, 3 oder 7 in G haben.

Betrachte $r := \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \in G$ und setze $s := r^T r = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$.

Es gilt $r^7 = 1$, $(r^T)^7 = 1$ und $s^3 = 1$. Demnach ist $r^T \notin \langle r \rangle$, denn sonst wäre auch $s \in \langle r \rangle$. Dann wäre aber mit s ein Element der Ordung 3 in der zyklischen Gruppe $\langle r \rangle$. Widerspruch!
Also gibt es mindestens 2 Sylow-7-Untergruppen, den Sylow-Sätzen nach sind es dann genau 8 eins-disjunkte.
Wir schließen nun nacheinander die einzelnen Indexe $2, 3, 7$ der Normalteiler aus:

- G kann keinen Normalteiler N mit Index 2 haben, denn dieser hätte dann nach den Sylow-Sätzen als Gruppe mit Ordnung 84 eine Sylow-7-Gruppe P als Normalteiler und demnach kann es keine anderen Sylow-7-Gruppen in G geben[9].
- Einen Normalteiler $N \triangleleft G$ mit Index 3 kann es auch nicht geben, da sonst mit r und $r^T \in N$ [10] auch $s \in N$ - was aber nicht sein kann, da dort wegen $56 = 2^3 \cdot 7$ keine Elemente der Ordnung 3 vorkommen.
- Also muss es einen Normalteiler mit Index 7 geben. Dieser enthält dann 1 oder 3 Sylow-2-Gruppen.
  - Falls es nur eine einzelne S gibt, dann gibt es auch nur eine in G, sie ist Normalteiler. Dann hat die Faktorgruppe G/S Ordnung 21 und eine einzelne Sylow-7-Gruppe als Normalteiler mit Index 3. Somit hat nach dem Korrespondenzprinzip auch G einen weiteren mit Index 3, was aber oben ausgeschlossen worden ist.
  - Also muss es 3 geben. Der Normalisator H einer beliebigen von ihnen hat also Index 3 und ist auf keinen Fall Normalteiler.

    Die natürliche Wirkung von G als Permutation auf den Rechtsnebenklassen $H\backslash G$
    $$\begin{cases} G \times H\backslash G & \rightarrow & H\backslash G \\ g \cdot Hx & \mapsto & Hxg \end{cases}$$

[9] Es bleiben einfach keine Elemente über, die die Konjugation der 8 Gruppen durchführen könnten. Jedes Element bildet durch Konjugation die Elemente von $P \subset N$ in N ab. Demnach sind alle Konjugierten von P in N, weshalb es dann nicht acht, sondern nur eine in G geben würde.

[10] Warum sind beide überhaupt drin? Für Ordnung 56 gilt: $S_7 \in \{1, 8\}$ und nach obiger Fußnote $s_7 \neq 1$. Daher sind alle Elemente der Ordnung 7 in N.

nutzen wir, um eine Permutation ξ_g mit

$$\begin{cases} \xi_g : & H\backslash G & \rightarrow & H\backslash G \\ \xi_g : & Hx & \mapsto & Hxg \end{cases}$$

zu definieren.
Jedes ξ_g wirkt also auf die 3 Elemente Hx, Hy, Hz von $H\backslash G$ und permutiert diese unter gewissen Voraussetzungen:
Falls $g \in H$, dann ist $\xi_g(Hx) = Hxg = Hx$ weder in der gleichen Nebenklasse, also ξ_g = id. Andere g 'schieben' Hx per Hxg in eine der beiden anderen Äquivalenzklassen Hy oder Hz.
Mit diesem Wissen definieren wir einen Homomorphismus η zwischen G und den Permutationen auf $H\backslash G$ (als Permutationen auf einer 3-elementigen Menge gerade S_3) wie folgt:

$$\begin{cases} \eta : & G & \rightarrow & \mathrm{Sym}(H\backslash G) = S_3 \\ \eta : & g & \mapsto & \xi_g. \end{cases}$$

Der Kern hat Index 3 in G, wie man mit obigen Überlegungen leicht sieht:

$$\ker\, \eta = \{g \in G \mid \eta(g) = id\} = \{g \in G \mid Hxg = Hx\}$$

Es gilt

$$G/\ker\, \eta \cong \mathrm{im}\ \eta = S_3$$

und da S_3 einen Normalteiler mit Index 2 hat, muß nach dem Korrenspondenzprinzip auch G einen Normalteiler N mit Index 2 haben, was nach unseren obigen Rechnungen aber ausgeschlossen ist - also gibt es keinen Normalteiler mit Index 7!

Damit hat $GL(3, \mathbb{F}_2)$ keine Normalteiler und ist somit einfach. $\square$

Schritt III

Für den letzten Schritt werden wir noch kurz ein Beispiel für eine zur $GL(3, \mathbb{F}_2)$ isomorphen Gruppe geben, die auf den ersten Blick völlig anders aussieht: die PSL(2,7).
Danach werden wir zeigen, dass alle einfachen nicht-abelschen Gruppen der Ordnung 168 isomorph zur $GL(3, \mathbb{F}_2)$ sind.

3.1 Die PSL(2,7)

Bevor wir die Eigenschaften der PSl(2,7) untersuchen, müssen wir die Gruppe erst definiren. Die GL(2,7) ist die Gruppe der invertierbaren 2×2 Matrizen mit Einträgen aus $\mathbb{Z}/7\mathbb{Z}$. Diese hat eine Untergruppe SL(2,7), die Untergruppe der Matrizen mit Determinate 1 (Kern der Determinantenabbildung!). Das Zentrum Z dieser Untergruppe besteht, wie man leicht erkennen kann aus den Vielfachen der Einheitsmatrix I mit Determinate 1 und ist ein nichttrivialer Normalteiler. Hier ist $Z = \{\pm I\}$. Die PSL(2,7) ist die Faktorgruppe SL(2,7)$/Z$. Sie hat $(7^2 - 1) \cdot 7/2 = 168$ Elemente.
Oben haben wir gezeigt, dass eine Gruppe mit Ordnung 168 einfach ist, wenn sie zwei Elemente der Ordnung 7 hat, die eine Untergruppe erzeugen, die ein Element der Ordnung 3 enthält. Damit zeigen wir auch, dass die PSL(2,7) einfach ist. Wir setzen

$$x := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} Z \text{ und } y := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} Z.$$

Beide haben die Ordnung 7 und

$$u := xyyx = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} Z$$

hat Ordnung 3. Also ist die PSL(2,7) einfach.

3.2 Alle einfachen Gruppen mit 168 Elementen sind isomorph

Zuerst haben natürlich alle diese einfachen Gruppen gemeinsam, dass sie nicht abelsch sind, denn $168 = 2^3 \cdot 3 \cdot 7$ ist nicht prim.
Nachfolgend ist $\mathrm{Syl}_p(G)$ die Menge der Sylow-p-Gruppen von G.
Nach den Sylow-Sätzen gilt

- $|\mathrm{Syl}_2(G)| \in \{1, 3, 7, 21\}$
- $|\mathrm{Syl}_3(G)| \in \{1, 4, 7, 28\}$
- $|\mathrm{Syl}_7(G)| \in \{1, 8\}$

$|\mathrm{Syl}_2(G)|, |\mathrm{Syl}_3(G)|$ und $|\mathrm{Syl}_7(G)|$ können nicht 1 sein, sonst wäre die entsprechende Sylowgruppe Normalteiler von G (Widerspruch zur Einfachheit). Nach Poincaré gilt für $|\mathrm{Syl}_2(G)| = 3$ dann für den Normalisator $N_G(P)$ eines $P \in \mathrm{Syl}_2(G)$:

$$168 = |G| \not| \, 3! = 6$$ [11]

Ebenso verfährt man für $|\mathrm{Syl}_3| = 4$.

Sei $|\mathrm{Syl}_3(G)| = 7$, dann wähle man $P \in \mathrm{Syl}_7(G)$. Wegen $|\mathrm{Syl}_7|(G) = 8$ gilt $|G : N_G(P)| = 8$ und damit $|N_G(P)| = 21$. Damit enthält dieser Normalisator entweder 1 oder 7 3-Sylowgruppen.

- Sei $Q \in \mathrm{Syl}_3(N_G(P))$ ein Normalteiler, dann ist $N_G(P) \leq$ [12] $N_G(Q)$, aber dann müsste $|N_G(P)| \big| |N_G(Q)|$ gelten im Widerspruch zu $|N_G(P)| = 21$ und $|N_G(Q)| \in \{6, 24\}$.
- Also gilt $|\mathrm{Syl}_3(G)| = 7$. Demnach sind alle Sylow-3-Gruppen von G in $N_G(P)$. Weiter ist $|N_G(P)| = 21$ und demnach $N_G(P) = \langle \mathrm{Syl}_3(G) \rangle$, weil $N_G(P)$ die kleinste[13] Untergruppe von G ist und alle Sylow-3-Gruppen von G enthält.
  Weil die Elemente von $N_G(P)$ aus Elementen der 3-Sylowgruppen zusammengesetzt sind und somit bei Konjugation auf Elemente abgebildet werden, die aus Elemente der 3-Sylowgruppen zusammengesetzt sind, ist aber $N_G(P) \lhd G$, was nicht sein kann.

Sei oBdA $|\mathrm{Syl}_2(G)| = 7$, dann hat der Normalisator eines $Q \in \mathrm{Syl}_2(G)$ die Ordnung 24, da $|G : N_G(Q)| = 7$. In $N_G(Q)$ gibt es nun eine oder 4 Sylow-3-Gruppen.

- Eine kann es nicht sein, denn sonst hätte deren Normalisator ebenfalls mindestens Ordnung 24, aber wir wissen seit kurzem, dass er gerade Ordnung 6 haben muss[14]!
- Damit sind es also 4 halbdisjunkte Untergruppen der Ordnung 3 in $N_G(Q)$. Durch die Konjugiertheit können wir schließen, dass jede dieser Untergruppen eine Sylow-2-Gruppe zum Normalisator haben muss.
  Da es 7 Sylow-2-Gruppen gibt, gibt es auch mindestens 7 konjugierte Normalisatoren, jeder enthält 4 Untergruppen der Ordnung 3. Da es genau 28 Untergruppen der Ordnung 3 gibt, sind diese Zahlen genau und es gibt diesbezüglich keine Überschneidungen. Demnach sind Normalisatoren für unterschiedliche Sylow-2-Gruppen ebenfalls unterschiedlich. Der Schnitt

[11] Der Normalisator hat Index 3

[12] Alle Elemente, die P normalisieren, normalisieren auch Q, da es ja für die ganze Gruppe, also auch Untergruppe gilt...

[13] Aus Teilergründen kann es zwischen 15 und 21 Elementen keine Untergruppe von G geben, also ist $N_G(P)$ die kleinste.

[14] da wir wissen, dass es 28 Sylow-3-Gruppen gibt und $168/28 = 6$

zweier solcher enthält gerade kein Element der Ordnung 3 mehr, also gilt für $R := N_G(Q_1) \cap N_G(Q_2)$: $|R| = 2^r$ und $R \,/\, 24$.
Es gilt

$$168 = |G| \geq |N_G(Q_1) \cdot N_G(Q_2)| = \frac{|N_G(Q_1)| \cdot |N_G(Q_2)|}{|R|} = \frac{24^2}{|R|}$$

Demnach hat R die Ordnung 4 oder 8.

- Falls R die Ordnung 8 hätte, wobei ja auch die Sylow-2-Gruppe die Ordnung 8 habe, müßte $R = Q_1 = Q_2$ gelten. Zwei Sylowgruppen sind ja verschieden, sodass $Q_1 \neq Q_2$ gilt.
- Also ist die Ordnung 4 und demnach ist R ein Normalteiler[15] von Q_1 und Q_2. Also enthält dessen Normalisator $N_G(R)$ auf jeden Fall die Untergruppen[16] Q_1 und Q_2. Dann teilt 8 die Normalisatorordnung und diese muss 168 teilen[17]. Da Q_1 und Q_2 unterschiedlich gilt $|N_G(R)| > 8$.
  Nach Poincaré gilt $|N_G(R)| \leq 24 = 168/7$ da diese Gruppe NT ist und damit die Gruppenordnung $|G|$ die Zahl $|G : N_G(R)|!$ teilt[18] und die 7 auch $|G|$ teilt.
  Also muss $|N_G(R)| = 24$ sein und damit enthält $N_G(R)$ mindestens 2, also genau 3 Sylow-2-Gruppen mit Ordnung 8.

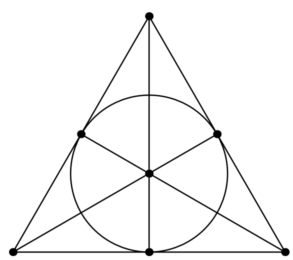
Für die p-Sylowgruppen gilt also:

p	$\|P\|$	$\mathrm{Syl}_p(G)$	$\|N_G(P)\|$
2	8	21	8
3	3	28	6
7	7	8	21

Man kann zeigen, dass es $S_1, S_2 \in \mathrm{Syl}_2(G)$, mit $|S_1 \cap S_2| = 4, \textit{gibt}$. Damit spannen wir die Untergruppe $Y := \langle S_1, S_2 \rangle$ auf, und es gilt $8 \big| |Y| \big| 168$ und damit $|Y| \in \{8, 24, 56, 168\}$. Wäre $|Y| = 8$, so wären die beiden 2-Sylowgruppen gleich. Nehmen wir also an, dass gilt: $|Y| = 56$. Dann wäre $|\mathrm{Syl}_2(Y)| \in \{1, 7\}$ und $|\mathrm{Syl}_7(Y)| \in \{1, 8\}$. Beide können aber nicht gleich 1 sein, weil die entsprechenden Normalisatoren echte Untergruppen von Y sind. Dies kann aber auch nicht sein, weil wir dann $8 \cdot 6 = 48$ Elemente der Ordnung 7 und $7 \cdot 7 = 49$ Elemente der Ordnugen 2,4 und 8 haben. $S_1 \cap S_2$ hat Index 2 in S_1 und S_2 und ist deswegen Normalteiler von S_1 bzw. S_2. Deswegen kann $|Y|$ auch nicht 168 sein. Also hat Y die Ordnung 24.
Es gilt: $|\mathrm{Syl}_2(Y)| \in \{1, 3\}$ und $|\mathrm{Syl}_3(Y)| \in \{1, 4\}$. Die 1 scheidet jeweils aus, weil beide dann Normalteiler von Y wären, der Normalisator dieser Sylowgruppen in G aber Ordnung 8 bzw. 6 hat und damit eine echte Teilmenge von Y wäre. $N_G(Y) = Y$, weil $N_G(Y)$ kein Normalteiler von G ist und es sonst keine Untergruppen von G gibt, die Y enthalten. Damit ist $|G : N_G(Y)| = |G : Y| = 7$ und das ist genau die Anzahl der Konjugierten von Y in G ($Y_i, i \in \{1 \dots 7\}$).

[15] Index 2
[16] Untergruppen in $N_G(R)$!
[17] weil der Normalisator ja Untergruppe ist
[18] deshalb mindestens 7!

Der Schnitt zwischen zwei solchen Konjugierten muss eine 2-Gruppe sein, denn wären Elemente der Ordnung 3 im Schnitt, so ergibt sich ein Widerspruch, da die 3-Sylowgruppen untereinander konjugiert sind, also nicht gleichzeitig in verschiedenen Konjugationklassen sein können. Jede der 21 2-Sylowgruppen kommt in genau einer Konjugationsklasse von Y vor, denn Y hat drei 2-Sylowgruppen, welche gleichzeitig auch 2-Sylowgruppen aus G sind. Also sind in jeder Konjugierten von Y 3 andere 2-Sylowgruppen. Jedes Paar von Konjugierten von Y (Y_1, Y_2) überschneidet sich in einer Untergruppe W_{12} mit $|W_{12}| = 4$, was man mit Hilfe von $\frac{|Y_1|\cdot|Y_2|}{|Y_1 \cap Y_2|} \leq 168$ leicht nachrechnen kann. Außerdem ist W_{12} in je einer einzelnen 2-Sylowgruppe von Y_1 bzw. Y_2 enthalten (Nachrechnen!). Diese 2-Sylowgruppen erzeugen ein $Z < G$ mit Ordnung 24, Z hat drei 2-Sylowgruppen. Zwei von diesen kennen wir bereits, die dritte muss in einer dritten Konjugiertenklasse von Y, nennen wir sie Y_3, sein. Denn hätte Z oBdA eine weitere 2-Sylowgruppe S_3 von Y_1, so wäre $Y_1 = \langle S_1, S_3 \rangle = Z$. Das kann aber nicht sein, weil Z damit keine 2-Sylowgruppe aus Y_2 enthält. Damit sind Y_1, Y_2 und Y_3 die einzigen Konjugierten von Y, die gemeinsame 2-Sylowgruppen mit Z haben. Z hat 7 Konjugierte (Beweis wie oben) $(Z_i, i \in \{1 \dots 7\})$.
Insgesamt haben wir also eine Menge $X = \left\{Z_i, Y_i : i \in \{1, \dots, 7\}\right\}$, wobei die Z_i, sowie die Y_i untereinander konjugiert sind. Außerdem gibt es für alle Z_j jeweils paarweise verschiedene l, m, n, so dass Y_l, Y_m und Y_n jeweils eine 2-Sylowgruppe mit Z_j gemeinsam haben. Die Abbildung $\varphi_g : X \to X,\ \varphi_g(M) \mapsto gMg^{-1}$ $(M \in X)$ ist ein Automorphismus auf X, wobei zwei verschiedene g auch zwei verschiedene Automorphismen induzieren.
Nun betrachten wir die Graphik[19].



Die Punkte sind die Konjugierten von Y, die Linien die Konjugierten von Z. Ein Punkt Y_i liegt auf einer Linie Z_j, genau dann wenn im Y_i und Z_j eine 2-Sylowgruppe gemeinsam haben. Jeder Punkt liegt also auf drei Linien und auf jeder Linie liegen drei Punkte. Die Gruppe der Automorphismen auf dieser Figur, die die gemeinsamen Punkte einer Linie auf einer Linie festhalten, hat gerade $7 \cdot 6 \cdot 4 \cdot 2 = 168$ Elemente. Damit ist jede einfache Gruppe der Ordnung 168 isomorph zu dieser Automorphismengruppe und somit auch zu jeder anderen einfachen Gruppe dieser Ordnung.

Zum Beispiel sind auch die GL(3,2) und die PSL(2,7) trotz ihren verschiedenen Formen isomorph.

[19] Ein herzliches Dankeschön an Benjamin Dumke, der die Grafik erstellt hat!

Literaturverzeichnis

[Bo2001] Siegfried Bosch
Algebra
Springer Verlag 2001 (4. Auflage)

[El2002] Christian Elsholtz
Algebra I Vorlesungsskript
TU Clausthal WS 2002/03

[ST2002] Geoff Smith and Olga Tabachnikova
Topics in Groups Theoriy
Springer Verlag 2002 (2. Auflage)