EIN SATZ ÜBER DIE ENDLICHEN EINFACHEN GRUPPEN.*

Von

L. RÉDEI

in SZEGED (UNGARN).

§ 1. Einleitung.

Eine Gruppe[1] mit lauter Abelschen maximalen Untergruppen ist stets auflösbar (s. unten) und somit nichteinfach. Umgekehrt folgt hieraus, dass eine (nichtzyklische) einfache Gruppe mindestens eine nichtabelsche maximale Untergruppe haben muss. Es liegt als nächster Schritt nahe diejenigen einfachen Gruppen zu untersuchen, die lauter Abelsche zweitmaximale[2] Untergruppen haben. Hierüber beweisen wir den folgenden:

Satz. 1°. *Eine Gruppe ist einfach, wenn alle maximalen Untergruppen nichtabelsch sind ohne Zentrum, mit lauter Abelschen maximalen Untergruppen.*

2°. *Es gilt die Umkehrung: Hat eine einfache Gruppe lauter Abelsche zweitmaximale Untergruppen, so sind alle maximalen Untergruppen ohne Zentrum (folglich nichtabelsch).*

3°. *Es gibt nur eine einfache Gruppe von gerader Ordnung mit lauter Abelschen zweitmaximalen Untergruppen, das ist die Ikosaedergruppe* $\mathfrak{G}_{60}$.

Bemerkung. Aus 3° folgt, dass eine einfache Gruppe von gerader Ordnung (> 60) mindestens eine nichtabelsche zweitmaximale Untergruppe enthält.

Bekanntlich vermutet man, dass es überhaupt keine (nichtzyklischen) einfachen

---

* Ein Vortrag des Verfassers gehalten am 26. April 1948 im Seminar von Prof. T. Nagell an der Universität in Uppsala.

[1] Von unendlichen Gruppen soll völlig abgesehen werden, »Gruppe« heisst »endliche Gruppe«.

[2] Wir nennen eine Untergruppe $\mathfrak{H}$ von einer Gruppe $\mathfrak{G}$ zweitmaximal, wenn es eine Untergruppe $\mathfrak{K}$ mit $\mathfrak{H} \subset \mathfrak{K} \subset \mathfrak{G}$ gibt, so dass $\mathfrak{H}$ maximal in $\mathfrak{K}$, letzteres wieder maximal in $\mathfrak{G}$ enthalten ist. Das schliesst selbstverständlich nicht aus, dass sich $\mathfrak{H}$ und $\mathfrak{G}$ auch durch längere Untergruppenketten $\mathfrak{H} \subset \mathfrak{K}_1 \subset \ldots \subset \mathfrak{K}_e \subset \mathfrak{G}$ ($e \geqq 2$) verbinden lassen. Wenn wir über die zweitmaximalen Untergruppen einer Gruppe $\mathfrak{G}$ eine Aussage machen, so soll stets mit einverstanden sein, dass sie auch existieren, d. h. $\mathfrak{G}$ weder eine zyklische Gruppe von Primzahlordnung noch $\mathfrak{G} = 1$ (Einheitsgruppe) ist; offenbar sind diese die einzigen Gruppen ohne zweitmaximale Untergruppen.

Gruppen von ungerader Ordnung gibt. Ist diese Vermutung richtig[3], so bleibt nur 3° als wesentlicher Inhalt des Satzes übrig. Es glückte mir nicht ein Analogon von 3° für ungerade Ordnungszahlen aufzustellen (weder verneinend noch bejahend), worin man eine neue Angabe erblicken kann, dass die einfachen Gruppen von ungerader Ordnung sich schwer erforschen lassen.

Wegen obiger Vermutung verdienen die Teile 1°, 2° des Satzes eine besondere Aufmerksamkeit. Trotz meines bisherigen Misserfolgs (s. unten) scheint nämlich eine verhältnismässig leichte Aufgabe zu sein, die Gruppen von ungerader Ordnung aufzusuchen, für die die Bedingungen von 1° erfüllt sind. Würde sich dabei Nichtexistenz herausstellen, so wäre dadurch nebenbei die gesagte Vermutung bedeutend bekräftigt, im anderen Falle selbstverständlich widerlegt.

Allerdings können wir sagen, dass nach 2° die einfachen Gruppen mit lauter Abelschen zweitmaximalen Untergruppen eine verblüffende Symmetrie in ihren maximalen Untergruppen aufzeigen[4]. Es ist erfreulich, dass es nach 3° mindestens eine Gruppe (nämlich $\mathfrak{G}_{60}$) mit dieser Symmetrie gibt[5], und so würde man sich weniger wundern, wenn noch weitere solche Gruppen (nämlich von ungerader Ordnung) existierten.

Der Beweis des Satzes — im wesentlichen der einzige Gegenstand unserer Arbeit — wird ziemlich mühsam. Dabei wird sich der Nachweis der in 3° behaupteten Einzigkeit von $\mathfrak{G}_{60}$ für eine besonders nette Aufgabe erweisen. Zum Erfolg haben uns die in unseren Gruppen im Falle gerader Ordnung enthaltenen Diedergruppen verholfen — bei ungerader Ordnung fehlten uns solche »Glücksterne«.

Den Satz werden wir noch in zwei Richtungen ergänzen. Erstens wird nämlich der Inhalt des Satzes erst dadurch in klares Licht gesetzt, dass wir alle nichtabelschen Gruppen ohne Zentrum mit lauter Abelschen maximalen Untergruppen

---

[3] Meines Erachtens ist obige Vermutung bisher nur sehr wenig »begründet« worden. Solche »Gründe« gibt es nämlich zwei. Erstens, man konnte bisher keine (nichtzyklische) einfache Gruppe von ungerader Ordnung auffinden, man bedenke aber hierzu, dass man an Möglichkeiten von Gruppenkonstruktionen (mit vorgegebenen Eigenschaften) überhaupt sehr arm ist, und so auch alle bisher gefundenen einfachen Gruppen weniger durch eine »Konstruktion« als durch einen glücklichen Zufall geliefert wurden, wobei (vielleicht als zweiter Zufall) die 2 unter den Primfaktoren der Gruppenordnung auftrat. Zweitens, man kennt einige einschränkende Bedingungen, damit eine zusammengesetzte Zahl die Ordnung einer einfachen Gruppe sein kann — die Anzahl der verschiedenen Primfaktoren ist grösser als der kleinste Primfaktor, dieser ist mindestens dreifach, die Anzahl aller Primfaktoren ist mindestens 8 — alle diese Bedingungen lassen aber immer noch eine weite Möglichkeit zur Existenz einer einfachen Gruppe von ungerader Ordnung zu.

[4] Eine Symmetrie von anderer Art steckt in den bekannten einfachen Gruppen im allgemeinen.

[5] Ich denke, dass eine volle Klarheit über die Struktur von $\mathfrak{G}_{60}$ ohne obigen Satz nunmehr nicht vorstellbar ist.

angeben. Eine solche Gruppe bezeichnen wir mit $\mathfrak{G}^\circ$, diese sind bekannt (s. unten), und haben eine sehr elegante Struktur. Zweitens stellen wir einen Zusatz auf, in dem wir die Eigenschaften der einfachen Gruppen des Satzes näher entwickeln, soweit wir es konnten. Dabei hat uns der Wunsch geleitet, den Weg für weitere Untersuchungen zu ebnen.

Beim Beweis (des Teils 2°) des Satzes werden wir allgemeiner alle nichtabelschen Gruppen benötigen, die lauter Abelsche maximale Untergruppen haben. Eine solche Gruppe bezeichnen wir mit $\mathfrak{G}^*$, so dass dann die $\mathfrak{G}^\circ$ nichts anderes sind als die $\mathfrak{G}^*$ ohne Zentrum. Mit den $\mathfrak{G}^*$ haben sich Miller und Moreno[6] ferner Schmidt[7] beschäftigt, genau hat sie dann Verfasser[8] bestimmt. Bequemlichkeitshalber werden wir die $\mathfrak{G}^*$ im § 3 voll aufzählen (teils mit veränderten einfacheren Bezeichnungen). Hier bemerken wir über die $\mathfrak{G}^*$ im allgemeinen nur, dass sie sich auf Grund ihrer Eigenschaften in drei Typen mit je unendlich vielen Gruppen — von denen wir eine beliebige bzw. mit $\mathfrak{G}_{\mathrm{I}}$, $\mathfrak{G}_{\mathrm{II}}$, $\mathfrak{G}_{\mathrm{III}}$ bezeichnen werden — einteilen lassen, denen noch (als vierter Typ bestehend aus einer einzigen Gruppe) die Quaternionengruppe hinzukommt, diese bezeichnen wir mit $\mathfrak{G}_8$. Selbst die $\mathfrak{G}^\circ$ machen dabei einen Teil aller $\mathfrak{G}_{\mathrm{I}}$ aus und sind überhaupt in mehrerer Hinsicht die bemerkenswertesten unter allen $\mathfrak{G}^*$[9].

Wir führen folgende Bezeichnungen ein:

p, q sind verschiedene Primzahlen;

$k(p^e)$ $(e \geqq 1)$ ist der (endliche kommutative) Körper von p^e Elementen;

$O(x)$ bezeichnet die Ordnung von x, wobei x eine Gruppe oder ein Gruppenelement ist; für $x \in k(p^e)$, $\neq 0$ wird $O(x)$ dadurch sinnvoll, dass man x als ein Element der multiplikativen Gruppe aller Elemente $(\neq 0)$ von $k(p^e)$ auffasst;

$O(p \pmod q)$ bezeichnet die »Ordnung von p mod q« d. h. die kleinste positive ganze Zahl e mit $p^e \equiv 1 \pmod q$.

---

[6] G. A. Miller and H. C. Moreno, Non-abelien groups in which every subgroup is abelian, Transactions Amer. Math. Soc. 4 (1903), 398—404.

[7] O. Schmidt, Über Gruppen, deren sämtliche Teiler spezielle Gruppen sind (russisch mit deutscher Zusammenfassung), Receuil Math. de la Soc. Math. d. Moscou 31 (1924), 367—372.

[8] L. Rédei, Das »schiefe Produkt« in der Gruppentheorie mit Anwendungen auf die endlichen nichtkommutativen Gruppen mit lauter kommutativen echten Untergruppen und die Ordnungszahlen, zu denen nur kommutative Gruppen gehören, Commentarii Mat. Helv. 20 (1947), 225—263.

[9] Nach diesem lässt sich der Inhalt der Teile 1°, 2° des Satzes folgenderweise näher besprechen. Wir legen uns alle Gruppen mit lauter Abelschen zweitmaximalen Untergruppen vor. Diese lassen sich anders so charakterisieren, dass als maximale Untergruppen nur Abelsche Gruppen und die $\mathfrak{G}_{\mathrm{I}}$, $\mathfrak{G}_{\mathrm{II}}$, $\mathfrak{G}_{\mathrm{III}}$, $\mathfrak{G}_8$ zugelassen wurden. Nun sprechen 1°, 2° aus, dass eine solche Gruppe dann und nur dann einfach ist, wenn unter allen, hier vorgezählten Gruppen keine Abelschen und keine $\mathfrak{G}_{\mathrm{II}}$, $\mathfrak{G}_{\mathrm{III}}$, $\mathfrak{G}_8$ sondern nur die $\mathfrak{G}_{\mathrm{I}}$ und auch unter diesen nur die $\mathfrak{G}^\circ$ als maximale Untergruppen wirklich auftreten. (Vgl. die oben anschliessend und in § 3 folgende Beschreibung von $\mathfrak{G}^\circ$ bzw. aller $\mathfrak{G}^*$.)

Aus § 3 nehmen wir folgende Angaben über die obigen Gruppen $\mathfrak{G}^\circ$ (Spezialfall $u = 1$ von $\mathfrak{G}_I$) vorweg. *Die $\mathfrak{G}^\circ$ stehen mit den (geordneten) Paaren p, q in eineindeutiger Zuordnung, weshalb wir $\mathfrak{G}^\circ = \mathfrak{G}^\circ(p, q)$ schreiben dürfen, wobei*

$$O\big(\mathfrak{G}^\circ(p,q)\big) = p^e q \qquad \big(e = O(p \pmod q)\big) \tag{1}$$

gilt[10]. *Und zwar lässt sich $\mathfrak{G}^\circ$ durch ein System erzeugender Elemente $P_\alpha\big(\alpha \in k(p^e)\big), Q$ angeben, wofür die »definierenden Gleichungen«*[11]

$$P_\alpha^p = Q^q = 1(\alpha \neq 0),\ P_\alpha P_\beta = P_{\alpha+\beta},\ QP_\alpha Q^{-1} = P_{\omega\alpha} \tag{2}$$

gelten mit einem beliebigen, festen ω von der Eigenschaft[12]:

$$O(\omega) = q \qquad \big(\omega \in k(p^e)\big)\,. \tag{3}$$

Um uns mit diesen Gruppen $\mathfrak{G}^\circ$ völlig bekannt zu machen, stellen wir hier ihre weiteren Eigenschaften zusammen, die sich nunmehr unmittelbar einsehen lassen. Alle verschiedenen Elemente von $\mathfrak{G}^\circ$ sind die $P_\alpha Q^i (\alpha \in k(p^e);\ i = 0, \ldots, q-1)$ mit der Produktregel

$$P_\alpha Q^i \cdot P_\beta Q^k = P_{\alpha+\omega^i\beta} Q^{i+k}\,. \tag{4}$$

Die Potenz berechnet sich (durch eine Induktion nach t) zu[13]

$$(P_\alpha Q^i)^t = P_{\alpha(1+\omega^i+\cdots+\omega^{i(t-1)})} Q^{it}\,. \tag{5}$$

Das Einselement ist $P_0 (= 1)$, alle übrigen Elemente sind von Primzahlordnung, und zwar die $P_\alpha (\alpha \neq 0)$ und die $P_\alpha Q^i (i = 1, \ldots, q-1)$ sind von p-ter bzw. q-ter Ordnung. Die Sylowgruppen stimmen mit den maximalen Untergruppen überein (sind Abelsch). Die p-Sylowgruppe umfasst alle P_α, ist elementar[14] von der Ordnung p^e, sie ist zugleich die einzige echte normale Untergruppe. Die q-Sylowgruppen sind (zyklisch) von der Ordnung q, ihre Anzahl ist p^e, keine von ihnen wird durch ein ausserhalb liegendes Element in sich transformiert.

Übrigens lässt sich $\mathfrak{G}^\circ$ selbstverständlich auch schon durch irgendzwei nichtvertauschbare Elemente erzeugen. Insbesondere mit P_1, Q geht das so. Vor allem gilt nach (4)

---

[10] Es ist klar, dass stets $O\big(\mathfrak{G}^\circ(p,q)\big) \neq O\big(\mathfrak{G}^\circ(q,p)\big)$ ist, und so sind die $\mathfrak{G}^\circ$ schon durch $O(\mathfrak{G}^\circ)$ eindeutig bestimmt.

[11] Die Eleganz von (2) haben wir so erreicht, dass wir die Elemente P_α mit den $\alpha\big(\in k(p^e)\big)$ (statt etwa mit $1, 2, \ldots$) »numeriert« haben.

[12] Die zu den $q-1$ verschiedenen ω in (3) gehörenden $\mathfrak{G}^\circ(p, q)$ sind isomorph.

[13] Das Einselement bezeichnen wir sowohl in Gruppen als auch in $k(p^e)$ mit 1, was aber zu keinem Missverständnis führen wird.

[14] Eine Abelsche Gruppe nennen wir üblicherweise elementar, wenn ihre Invarianten gleiche Primzahlen sind. Zyklisch ist eine solche nur dann, wenn sie von Primzahlordnung ist.

$$Q^i P_1 Q^{-i} = P_{\omega^i} . \tag{6}$$

Da ω bekanntlich ein primitives Element von $k(p^e)$ ist, so lassen sich alle Elemente von $k(p^e)$ eindeutig in der Form $\alpha = c_0 1 + c_1\omega + \cdots + c_{e-1}\omega^{e-1}$ schreiben mit Koeffizienten $c_i = 0, \ldots, p-1$. Dann liefern (6) und

$$P_\alpha Q^k = P_1^{c_0} \ldots P_{\omega^{e-1}}^{c_{e-1}} Q^k$$

die gewünschte Erzeugung. Diese Bemerkung wird weiter nicht verwendet.

Wir kommen auf unseren Satz zurück, den wir nunmehr (zugleich die beiden Teile 1°, 2° vereinigt) kurz auch so aussprechen:

Die Gruppen mit lauter maximalen Untergruppen $\mathfrak{G}^\circ$ sind die sämtlichen einfachen Gruppen mit lauter Abelschen zweitmaximalen Untergruppen, unter ihnen kommt nur $\mathfrak{G}_{60}$ mit gerader Ordnung vor.

Da wir nach obigem die $\mathfrak{G}^\circ$ genau kennen, so wurde uns erst hierdurch der Inhalt des Satzes klar. Hierzu kommt noch, wie oben angekündigt, der folgende:

Zusatz. *Eine im obigen Satz charakterisierte (daher einfache) Gruppe $\mathfrak{E}$ hat die folgenden Eigenschaften* 1—13[15]:

1. *Die maximalen Untergruppen sind lauter Gruppen $\mathfrak{G}^\circ$.*
2. *Die Sylowgruppen sind elementare Abelsche Gruppen.*
3. *Jede zwei verschiedenen Sylowgruppen sind fremd*[16].
4. *Alle verschiedenen echten Untergruppen sind die maximalen und die Untergruppen $(\neq 1)$ der Sylowgruppen.*
5. *Die Normalisatoren der Sylowgruppen sind die maximalen Untergruppen.*
6. *Der Index einer Sylowgruppe in ihrem Normalisator ist eine Primzahl.*
7. *Jede Sylowgruppe ist der Normalisator aller ihrer echten Untergruppen.*
8. *Die Elemente $(\neq 1)$ sind von Primzahlordnung.*
9. *Vertauschbar sind zwei Elemente dann und nur dann, wenn sie in eine Sylowgruppe gehören.*

Man setze $v = O(\mathfrak{E})$, $p|v$ und definiere $e = e(p)$ durch $p^e||v$[17], *bezeichne mit $\mathfrak{S}_p$ eine p-Sylowgruppe, mit $\mathfrak{N}_p = \mathfrak{G}^\circ(p, p')$ ihren Normalisator, wobei dann $p' = p'(p)$ ein durch p eindeutig bestimmter Primfaktor $(\neq p)$ von v ist und*

---

[15] Davon ist 1. nichts anderes, als die definierende Eigenschaft von $\mathfrak{E}$. Die 2.—13. haben wir in einer Reihenfolge zusammengestellt, in der sie sich auch leicht nacheinander beweisen lassen werden.

[16] Fremd sind zwei Gruppen, wenn sie ausser 1 kein gemeinsames Element haben.

[17] $a^b||c$ bezeichnet $a^b|c$, $a^{b+1} \nmid c$.

(7) $$O(\mathfrak{S}_p) = p^e,\ O(\mathfrak{N}_p) = p^e p' \qquad \left(e = O(p \pmod{p'})\right)$$

gilt. (*Die Abbildung* $p \to p'$ *braucht rückwärts nicht eindeutig zu sein*!).

10. *Die Anzahl der verschiedenen Konjugierten von* $\mathfrak{S}_p$ (*und auch von* $\mathfrak{N}_p$) *ist*

(8) $$\frac{\nu}{p^e p'},$$

gleich dem Index von $\mathfrak{N}_p$.

11. *Zwei verschiedene Konjugierte von* $\mathfrak{N}_p$ *sind entweder fremd oder ihre Durchschnittsgruppe ist von der Ordnung* p', *letzterer Fall tritt für jedes* $\mathfrak{N}_p$ *wirklich auf.*

12. *Die Anzahl der Elemente* p-*ter Ordnung ist*

(9) $$\frac{\nu(p^e-1)}{p^e p'},$$

sie zerfallen in

(10) $$\frac{p^e-1}{p'}$$

Klassen konjugierter Elemente. Folglich gilt die Gleichung

(11) $$1+\sum_{p|\nu}{}' \frac{\nu(p^e-1)}{p^e p'} = \nu$$

und die Ungleichung

(12) $$1 < \sum_{p|\nu}{}' \frac{1}{p'} < 1+\sum_{p|\nu}{}' \frac{1}{p^e p'}.$$

13. $\mathfrak{E}$ *lässt sich durch zwei Elemente erzeugen.*

Bemerkungen. Dieser Zusatz bezieht sich nach dem Satz insbesondere auf $\mathfrak{E} = \mathfrak{G}_{60}$ (mit $\nu = 60 = 2^2 \cdot 3 \cdot 5$, $2' = 3$, $3' = 5' = 2$), wie man das leicht auch direkt einsehen kann.

Damit es zu einer ungeraden ν ein $\mathfrak{E}$ gibt, muss nach 12. die Gleichung (11) erfüllt sein, die wir wegen grösserer Durchsichtigkeit auch in der Form

(13) $$\frac{\nu-1}{\nu} = \sum_{p|\nu}{}' \frac{1}{p^e}\frac{p^e-1}{p'}$$

schreiben. Der zweite Faktor im Summand ist nach (10) ganz, und so handelt es sich um eine Partialbruchzerlegung mit den Nebenbedingungen $p'|\nu$ (p' Primzahl), $e = O(p \pmod{p'})$. Diese rein zahlentheoretische Aufgabe ist offenbar keine leichte (die uns im Zusammenhang mit den $\mathfrak{E}$ nur für $2 \nmid \nu$ angeht). Wir konnten nicht beweisen, dass es nur endlich viele Lösungen gibt, was übrigens sehr wahrscheinlich

ist. Auch glückte es uns nicht ausser $\nu = 60$ weitere gerade Lösungen zu finden. Wir haben eine ungerade Lösung gefunden: $\nu = 1004913 = 3^3 \cdot 7 \cdot 13 \cdot 409$ (mit $3' = 13$, $7' = 13' = 409' = 3$). Hierzu kann es aber ein $\mathfrak{E}$ schon aus dem Grunde nicht geben, weil die Anzahl der Primfaktoren bloss 6 ist. Deshalb können wir aussprechen, dass die (zahlentheoretische) Bedingung (13) nicht hinreicht, damit es ein $\mathfrak{E}$ mit $O(\mathfrak{E}) = \nu$ gibt[18].

Uns scheint insbesondere 11. einen Ansatz zu bieten, um aus ihm weitere (notwendige) zahlentheoretische Bedingungen für ν zu gewinnen, das hat uns aber nicht geglückt.

Wir beweisen den Satz und Zusatz in der Reihenfolge: 1°, 2°, Zusatz, 3°. Die meiste Mühe werden wir dabei mit 2° haben.

Wir bemerken noch, dass wir alle nichteinfachen Gruppen mit lauter Abelschen zweitmaximalen Untergruppen bestimmen konnten, worauf wir in einer anderen Arbeit zurückkommen. Diese sind sämmtlich auflösbar.

§ 2. Beweis vom Teil 1° des Satzes.

Zur Vorbereitung beweisen wir den folgenden:

Hilfssatz. Haben $\mathfrak{G}^\circ(p, q)$, $\mathfrak{G}^\circ(p, r)$ $(q \neq r)$ die gemeinsame p-Sylowgruppe $\mathfrak{S}$, legt man dabei für $\mathfrak{G}^\circ(p, q)$ die Bezeichnungen (1)-(3) zu Grunde, so gibt es eine Permutation $S\alpha$ der Elemente α von $k(p^e)$ mit

$$S(\alpha+\beta) = S\alpha + S\beta\,, \quad RP_{S\alpha}R^{-1} = P_{S(\overline{\omega}\alpha)}\,, \tag{14}$$

wobei R und $\overline{\omega}$ je ein festes Element von $\mathfrak{G}^\circ(p, r)$ bzw. $k(p^e)$ bezeichnet mit $O(R) = O(\overline{\omega}) = r$.

Nach § 1 kann man nämlich die Elemente P_α von $\mathfrak{S}$ so mit $\overline{P}_\alpha$ bezeichnen, dass bei passenden $R, \overline{\omega}$ (vgl. (2))

$$\overline{P}_\alpha \overline{P}_\beta = \overline{P}_{\alpha+\beta}\,, \quad R\overline{P}_\alpha R^{-1} = \overline{P}_{\overline{\omega}\alpha}$$

gilt. Definiert man die Permutation S durch $\overline{P}_\alpha = P_{S\alpha}$, so folgt (wegen $P_{S\alpha}P_{S\beta} = P_{S\alpha+S\beta}$) die Richtigkeit des Hilfssatzes.

Um den Teil 1° des Satzes zu beweisen, nehmen wir an, dass eine Gruppe $\mathfrak{G}$ mit lauter maximalen Untergruppen $\mathfrak{G}^\circ$ eine echte normale Untergruppe $\mathfrak{N}$ habe, woraus wir einen Widerspruch ableiten. Wir dürfen $O(\mathfrak{N})$ möglichst gross annehmen,

---

[18] Dagegen folgen aus (13) für die $\mathfrak{E}$ sofort die ersten zwei von den am Ende der Fussnote [3] erwähnten drei notwendigen Bedingungen (insbesondere die erste hiervon in der verschärften Form (12)).

woraus folgt, dass die Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ einfach ist, und unterscheiden die folgenden Fälle 1), 2), wovon sich 1) in die weiteren Fälle 11), 12) spalten wird.

1) $\mathfrak{N}$ sei zugleich maximale Untergruppe von $\mathfrak{G}$. Dann ist $\mathfrak{N}$ ein $\mathfrak{G}^\circ$, wir setzen

$$\mathfrak{N} = \mathfrak{G}^\circ(p, q) \tag{15}$$

mit $O(\mathfrak{N}) = p^e q$. Da $\mathfrak{N}$ maximal und normal in $\mathfrak{G}$ ist, so kann $\mathfrak{G}/\mathfrak{N}$ keine echten Untergruppen haben, d. h. $O(\mathfrak{G}/\mathfrak{N})$ ist eine Primzahl r mit $O(\mathfrak{G}) = p^e qr$. Wäre $r = p$, so gilt $O(\mathfrak{G}) = p^{e+1}q$, woraus folgt, dass die p-Sylowgruppe von $\mathfrak{G}$ eine maximale Untergruppe d. h. ein $\mathfrak{G}^\circ$ ist. Diese sind aber keine p-Gruppen, und so folgt aus diesem Widerspruch $r \neq p$. Bezeichne $\mathfrak{S}_p$ die p-Sylowgruppe von $\mathfrak{N}$, die nunmehr wegen $p^e \| O(\mathfrak{G})$ auch eine Sylowgruppe von $\mathfrak{G}$ ist. Da ferner $\mathfrak{S}_p$ nach (15) normal in $\mathfrak{N}$ ist, so muss $\mathfrak{N}$ im Normalisator von $\mathfrak{S}_p$ enthalten sein. Dabei ist Gleichheit unmöglich, denn dann müsste nach bekanntem Satz $\mathfrak{N}$ sein eigener Normalisator sein, wobei doch $\mathfrak{N}$ normal in $\mathfrak{G}$ ist. Folglich ist $\mathfrak{N}$ echt enthalten im Normalisator von $\mathfrak{S}_p$, der also nur $\mathfrak{G}$ sein kann. Wir haben gewonnen, dass $\mathfrak{S}_p$ normal in $\mathfrak{G}$ ist mit $O(\mathfrak{G}/\mathfrak{S}_p) = qr$.

11) Es sei $r = q$. Dann gilt

$$O(\mathfrak{G}) = p^e q^2 . \tag{16}$$

Bezeichne $\mathfrak{S}_q$ eine q-Sylowgruppe von $\mathfrak{G}$. Für (15) übernehmen wir die Bezeichnungen in (2), (3), und dann dürfen wir $\mathfrak{S}_q$ (unter den Konjugierten) so wählen, dass eben $Q \in \mathfrak{S}_q$ gilt. Andererseits ist $\mathfrak{S}_q$ echt enthalten in einer maximalen Untergruppe von $\mathfrak{G}$, die wegen (16) und $O(\mathfrak{S}_q) = q^2$ offenbar nur ein $\mathfrak{G}^\circ(q, p)$ sein kann mit $O(\mathfrak{G}^\circ(q, p)) = q^2 p$. Da $\mathfrak{S}_p$ normal in $\mathfrak{G}$ ist, so liegen alle Elemente p-ter Ordnung von $\mathfrak{G}$ in ihm, noch mehr in (15). Es folgt, dass beide Gruppen (15), $\mathfrak{G}^\circ(q, p)$ ein gemeinsames Element $P_\alpha (\neq 1)$ haben. Nach (2) gilt $QP_\alpha Q^{-1} = P_{\omega\alpha}$. Weiter ist $\mathfrak{S}_q$ normal in $\mathfrak{G}^\circ(q, p)$, und so folgt für sein Element Q^{-1}, dass auch das Konjugierte (man beachte $P_\alpha^{-1} = P_{-\alpha}$)

$$P_\alpha Q^{-1} P_\alpha^{-1} = Q^{-1} P_{\omega\alpha} P_\alpha^{-1} = Q^{-1} P_{(\omega-1)\alpha}$$

in $\mathfrak{S}_q$ liegt. Offenbar ist dieses Element wegen $\omega \neq 1$ mit Q nicht vertauschbar, obwohl beide Elemente in der (wegen $O(\mathfrak{S}_q) = q^2$) Abelschen Gruppe $\mathfrak{S}_q$ liegen. Wegen dieses Widerspruchs ist der vorliegende Fall 11) unmöglich.

12) Es sei $r \neq q$. Da auch $r \neq p$ gilt, so sind jetzt p, q, r die verschiedenen Primfaktoren von

$$O(\mathfrak{G}) = p^e qr . \tag{17}$$

Da $\mathfrak{G}/\mathfrak{S}_p$ eine Untergruppe r-ter Ordnung hat, so hat $\mathfrak{G}$ eine (maximale) Unter-

gruppe $p^e r$-ter Ordnung, in der $\mathfrak{S}_p$ (nach obigem nämlich sogar in $\mathfrak{G}$) normal enthalten sein muss. Da andererseits nach der Voraussetzung diese Untergruppe ein $\mathfrak{G}^\circ$, und zwar ein $\mathfrak{G}^\circ(p, r)$ oder ein $\mathfrak{G}^\circ(r, p)$ ist, so bleibt hiervon nach § 1 nur die erste Möglichkeit übrig. Also enthält $\mathfrak{G}$ ein $\mathfrak{G}^\circ(p, r)$ mit

$$O\big(\mathfrak{G}^\circ(p, r)\big) = p^e r\,, \tag{18}$$

und dabei ist $\mathfrak{S}_p$ eine gemeinsame p-Sylowgruppe von dieser Gruppe und von (15). Der Hilfssatz kommt somit zur Geltung, aus dem wir auch die Bezeichnungen $S, R, \overline{\omega}$ übernehmen dürfen.

Da (15) in $\mathfrak{G}$ normal enthalten ist, so gilt

$$RQR^{-1} = P_\varrho Q^a \tag{19}$$

mit einem $\varrho \in k(p^e)$ und einer ganzen Zahl $a (q \nmid a)$. Bei passender Wahl von R darf $\varrho = 0 (P_\varrho = 1)$ gesetzt werden. Dem Hilfssatz gegenüber verhalten sich nämlich alle $R' = P_\xi R\big(\xi \in k(p^e)\big)$ als gleichberechtigte Elemente (sogar mit gemeinsamen $S, \overline{\omega}$, was uns nicht wichtig ist), weshalb wir R durch R' ersetzen dürfen. Man berechnet nach (19) und (2)

$$R'QR'^{-1} = P_\xi P_\varrho Q^a P_\xi^{-1} = P_{\varrho + \xi(1-\omega^a)} Q^a\,.$$

Wegen (3) und $q \nmid a$ ist $1-\omega^a \neq 0$, und so geht der erste Faktor rechts für ein passendes ξ in $P_0 = 1$ über. Das beweist die Behauptung über (19), wofür somit von vornherein

$$RQR^{-1} = Q^a \tag{20}$$

angenommen werden darf.

Wir betrachten die Elemente von $\mathfrak{G}$ von der Form

$$R_1 = P_{S1} Q^i R \tag{21}$$

und beweisen

$$R_1^t = P_\varkappa Q^{i(1+a+\cdots+a^{t-1})} R^t \qquad (t = 1, 2, \ldots)\,, \tag{22}$$

wobei zur Abkürzung

$$\varkappa = S1 + \omega^i S\overline{\omega} + \omega^{i(1+a)} S\overline{\omega}^2 + \cdots + \omega^{i(1+a+\cdots+a^{t-2})} S\overline{\omega}^{t-1} \tag{23}$$

gesetzt wurde. Vor allem ist (22) für $t = 1$ richtig, da dann $\varkappa = S1$ ist. Wir nehmen (22) für ein t an, und berechnen

$$R_1^{t+1} = R_1^t R_1\,.$$

Da nach (14)

$$R^t P_{S1} = P_{S\overline{\omega}^t} R^t$$

gilt, so folgt nach Einsetzung von (21), (22):

$$R_1^{t+1} = P_\varkappa Q^{i(1+a+\cdots+a^{t-1})} P_{S\overline{\omega}^t} R^t Q^i R\,.$$

Wendet man hier noch (2) und (20) an (nach letzterem ist $R^tQ^i = Q^{ia^t}R^t$), so entsteht nach (23) eben (22) mit $t+1$ statt t, und so ist die Richtigkeit dieser Formel allgemein bewiesen.

Da $\mathfrak{G}$ nichtzyklisch ist, so ist jedes Element ($\neq 1$) in einer maximalen Untergruppe enthalten. Diese sind lauter $\mathfrak{G}^\circ$, und so sind alle Elemente ($\neq 1$) von $\mathfrak{G}$ von Primzahlordnung. Ferner ist die Untergruppe (15) vom Index r in $\mathfrak{G}$, weshalb die ausserhalb (15) liegenden Elemente die Ordnung r haben müssen. Das bezieht sich auch auf die Elemente R_1 in (21), und so muss $\varkappa$ nach (22) für $t=r$ verschwinden. Das lautet nach (23):

$$S1+\omega^i S\overline{\omega}+\omega^{i(1+a)}S\overline{\omega}^2+\cdots+\omega^{i(1+a+\cdots+a^{r-2})}S\overline{\omega}^{r-1} = 0\,. \tag{24}$$

Hieraus leiten wir aber einen Widerspruch ab. Wegen (3) gilt $\omega^c-1 = 0$ dann und nur dann, wenn $q|c$ ist, und so folgt

$$\sum_{i=0}^{q-1}\omega^{ic} = \frac{\omega^{qc}-1}{\omega^c-1} = 0 \qquad (q \nmid c). \tag{25}$$

Andererseits kann nicht $QR = RQ$ sein, denn dann wäre QR ein Element von qr-ter Ordnung in $\mathfrak{G}$, was doch, wie gesagt, ausgeschlossen ist. Wegen (20) folgt hieraus $a \not\equiv 1 \pmod q$. Wieder wegen (20) und $O(R) = r$ muss offenbar $a^r \equiv 1 \pmod q$ gelten, und so gilt auch $a, a^2, \ldots, a^{r-1} \not\equiv 1 \pmod q$, d. h.

$$1,\ 1+a,\ \ldots,\quad 1+a+\cdots+a^{r-2} \not\equiv 0 \pmod q\,.$$

Addiert man also die Gleichungen (24) für $i = 0, \ldots, q-1$, so entsteht wegen (25) einfach $qS1 = 0$. Da q durch die Charakteristik p von $k(p^e)$ nicht teilbar ist, so folgt hieraus $S1 = 0$. Andererseits gilt nach (14) auch $S0 = 0$, beide ergeben: $S1 = S0$. Da aber S eine Permutation ist, so folgt hieraus die falsche Gleichung $1 = 0$ (im Körper $k(p^e)$). Dieser Widerspruch zeigt, dass Fall 1) unmöglich ist.

2) $\mathfrak{N}$ sei keine maximale Untergruppe von $\mathfrak{G}$. Wir wählen eine maximale Untergruppe $\mathfrak{G}^\circ$ fest, die $\mathfrak{N}$ (echt) enthält. Da $\mathfrak{G}^\circ$ nur eine echte normale Untergruppe enthält, nämlich eine (Sylowgruppe) vom Primzahlindex, so muss diese mit $\mathfrak{N}$ zusammenfallen, und so folgt, dass $O(\mathfrak{G}^\circ/\mathfrak{N})$ eine Primzahl ist. Andererseits ist $\mathfrak{G}^\circ/\mathfrak{N}$ eine maximale Untergruppe von $\mathfrak{G}/\mathfrak{N}$, hat also sich selbst oder $\mathfrak{G}/\mathfrak{N}$ zum Normalisator. Der zweite fall ist unmöglich, weil $\mathfrak{G}/\mathfrak{N}$ einfach ist. Wir haben also gewonnen, dass $\mathfrak{G}^\circ/\mathfrak{N}$ von Primzahlordnung und sein eigener Normalisator ist, auch müssen dann die Konjugierten paarweise fremd sein. Nach einem Satz von Fro-

benius[19] folgt hieraus, dass $\mathfrak{G}/\mathfrak{N}$ nicht einfach ist. Dieser Widerspruch beweist Teil 1° des Satzes.

§ 3. Die Gruppen mit lauter Abelschen maximalen Untergruppen.

Als Vorbereitung zum § 4 zählen wir hier auf Grund der Arbeit [8] alle nichtabelschen Gruppen auf, die lauter Abelsche maximale Untergruppen haben. Wie wir es im § 1 schon gesagt haben, bezeichnen wir diese Gruppen mit $\mathfrak{G}^*$ und teilen diese in die Gruppen $\mathfrak{G}_{\mathrm{I}}$, $\mathfrak{G}_{\mathrm{II}}$, $\mathfrak{G}_{\mathrm{III}}$ und $\mathfrak{G}_8$ ein. Die letztere ist (wie schon erwähnt) die Quaternionengruppe, die übrigen geben wir hier an (vgl. die Fussnote [22]). Das Zentrum und die Kommutatorgruppe bezeichnen wir bzw. mit $\mathfrak{Z}_{\mathrm{I}}$, $\mathfrak{Z}_{\mathrm{II}}$, $\mathfrak{Z}_{\mathrm{III}}$ und $\mathfrak{K}_{\mathrm{I}}$, $\mathfrak{K}_{\mathrm{II}}$, $\mathfrak{K}_{\mathrm{III}}$, die maximalen Untergruppen mit $\mathfrak{M}_{\mathrm{I}}$, $\mathfrak{M}_{\mathrm{II}}$, $\mathfrak{M}_{\mathrm{III}}$.

$\mathfrak{G}_{\mathrm{I}}$ ist definiert durch[20]

$$P_\alpha^p = Q^{q^u} = 1\,, \quad P_\alpha P_\beta = P_{\alpha+\beta}\,, \quad QP_\alpha Q^{-1} = P_{\omega\alpha} \qquad \left(\alpha, \beta \in k(p^e)\right), \tag{26}$$

wobei p, q und $u(\geqq 1)$ beliebig gegeben sind, $e = O\big(p \pmod q\big)$ ist, und ω ein festes (sonst beliebiges) Element von $k(p^e)$ mit $O(\omega) = q$ bezeichnet. $\mathfrak{G}_{\mathrm{I}}$ ist (bis auf Isomorphe) durch p, q, u eindeutig bestimmt, weshalb wir es nötigenfalls mit $\mathfrak{G}_{\mathrm{I}}(p, q, u)$ bezeichnen. Es gilt

$$O(\mathfrak{G}_{\mathrm{I}}) = p^e q^u\,. \tag{27}$$

Alle verschiedenen Elemente sind die $P_\alpha Q^i (\alpha \in k(p^e);\ i = 0, \ldots, q^u - 1)$, und es gilt:

$$P_\alpha Q^i \cdot P_\beta Q^j = P_{\alpha+\omega^i\beta} Q^{i+j}\,, \tag{28}$$

$$(P_\alpha Q^i)^t = P_{\alpha(1+\omega^i+\cdots+\omega^{i(t-1)})} Q^{it}\,. \tag{29}$$

Es ist

$$P_0 = 1\,, \quad O(P_\alpha) = p (\alpha \neq 0)\,, \quad O(Q) = q^u\,. \tag{30}$$

Die Ordnung aller Elemente lässt sich nach der Regel bestimmen:

$$O(P_\alpha Q^i) = \begin{cases} pO(Q^i)\,, & \text{wenn} \quad \alpha \neq 0\,,\ q \mid i\,, \\ O(Q^i)\,, & \text{wenn} \quad \alpha = 0 \quad \text{oder} \quad q \nmid i\,. \end{cases} \tag{31}$$

---

[19] Der Satz von Frobenius lautet: Ist eine Untergruppe einer Gruppe ihr eigener Normalisator und sind die konjugierten Untergruppen paarweise fremd, so bilden die ausserhalb dieser Untergruppen liegenden Elemente mit 1 zusammen eine (echte) normale Untergruppe der gegebenen Gruppe. (S. z.B.: Speiser, Theorie der Gruppen von endlicher Ordnung, 3. Aufl., 1937, Satz 180, S. 202.)

[20] Das wird selbstverständlich so gemeint, dass $\mathfrak{G}_{\mathrm{I}}$ durch die in (26) vorkommenden Elemente erzeugt wird.

Alle P_α bilden eine p-Sylowgruppe $\mathfrak{S}$, sie ist elementar, von der Ordnung p^e, und normal. Die q-Sylowgruppen sind die $\{P_\alpha Q\}$[21], zyklisch von der Ordnung q^u, ihre Zahl ist p^e. Es gilt

$$\mathfrak{Z}_{\mathrm{I}} = \{Q^q\}\,, \quad \mathfrak{K}_{\mathrm{I}} = \mathfrak{S}\,, \tag{32}$$

die $\mathfrak{M}_{\mathrm{I}}$ sind $\{\mathfrak{S}, Q^q\}$ und die q-Sylowgruppen.

$\mathfrak{G}_{\mathrm{II}}$ ist definiert durch

$$A^{p^{u+1}} = B^{p^v} = 1\,, \quad BAB^{-1} = A^{1+p^u} \qquad (u, v \geqq 1)\,. \tag{33}$$

Nötigenfalls schreiben wir genauer $\mathfrak{G}_{\mathrm{II}}(p, u, v)$. Es gilt

$$O(\mathfrak{G}_{\mathrm{II}}) = p^{u+v+1}\,. \tag{34}$$

Alle verschiedenen Elemente sind die $A^iB^k (i = 0, \ldots, p^{u+1}-1;\ k = 0, \ldots, p^v-1)$ und es gilt

$$O(A) = p^{u+1}, \quad O(B) = p^v, \tag{35}$$

$$A^iB^k \cdot A^jB^l = A^{i+j+jkp^u}B^{k+l}, \tag{36}$$

$$(A^iB^k)^t = A^{it+p^uik\binom{t}{2}}B^{kt}\,. \tag{37}$$

Es gilt

$$\mathfrak{Z}_{\mathrm{II}} = \{A^p, B^p\}\,, \quad \mathfrak{K}_{\mathrm{II}} = \{A^{p^u}\}\,, \tag{38}$$

die $\mathfrak{M}_{\mathrm{II}}$ sind die $\{AB^i, B^p\}$ $(i = 0, \ldots, p-1)$ und $\{A^p, B\}$.

$\mathfrak{G}_{\mathrm{III}}$ ist definiert durch

$$A^{p^u} = B^{p^v} = C^p = 1, \quad AC = CA, \quad BC = CB, \quad BAB^{-1} = AC (u \geqq v \geqq 1). \tag{39}$$

Nötingenfalls schreiben wir genauer $\mathfrak{G}_{\mathrm{III}}(p, u, v)$. Es gilt

$$O(\mathfrak{G}_{\mathrm{III}}) = p^{u+v+1}. \tag{40}$$

Alle verschiedenen Elemente sind die $A^iB^kC^m (i = 0, \ldots, p^u-1;\ k = 0, \ldots, p^v-1;$ $m = 0, \ldots, p-1)$, und es gilt

$$O(A) = p^u, \quad O(B) = p^v, \quad O(C) = p\,, \tag{41}$$

$$A^iB^kC^m \cdot A^jB^lC^n = A^{i+j}B^{k+l}C^{m+n+jk}, \tag{42}$$

$$(A^iB^kC^m)^t = A^{it}B^{kt}C^{ik\binom{t}{2}}\,. \tag{43}$$

Es gilt

$$\mathfrak{Z}_{\mathrm{III}} = \{A^p, B^p, C\}\,, \quad \mathfrak{K}_{\mathrm{III}} = \{C\}\,, \tag{44}$$

die $\mathfrak{M}_{\mathrm{III}}$ sind die $\{AB^i, B^p, C\}$ $(i = 0, \ldots, p-1)$ und $\{A^p, B, C\}$.

[21] »{ }« bezeichnet die durch die eingeklammerten Elemente erzeugte Gruppe.

Diese $\mathfrak{G}_{\mathrm{I}}(p, q, u)$, $\mathfrak{G}_{\mathrm{II}}(p, u, v)$, $\mathfrak{G}_{\mathrm{III}}(p, u, v)$ sind auch verschieden mit der einzigen Ausnahme, dass die Gruppen $\mathfrak{G}_{\mathrm{II}}(2, 1, 1)$, $\mathfrak{G}_{\mathrm{III}}(2, 1, 1)$ gleich sind. (Und zwar sind letztere gleich der Diedergruppe 8-ter Ordnung). Wir wiederholen nunmehr genauer, dass die $\mathfrak{G}_{\mathrm{I}}$, $\mathfrak{G}_{\mathrm{II}}$, $\mathfrak{G}_{\mathrm{III}}$ (wobei man z. B. von $\mathfrak{G}_{\mathrm{II}}(2, 1, 1)$ abzusehen hat) und $\mathfrak{G}_8$ alle verschiedenen $\mathfrak{G}^*$ sind. Wir haben auch zu bemerken, dass $\mathfrak{G}_8$ bekanntlich ein Zentrum 2-ter Ordnung hat, und so liest man von (32), (38), (44) ab, dass unter allen $\mathfrak{G}^*$ nur die $\mathfrak{G}_{\mathrm{I}}(p, q, 1)$ (d. h. Fall $u = 1$ von $\mathfrak{G}_{\mathrm{I}}$) ohne Zentrum sind; da (26) für $u = 1$ in (2) übergeht, so sehen wir, dass die $\mathfrak{G}^\circ$ in der Tat die sämtlichen $\mathfrak{G}^*$ ohne Zentrum sind, wie wir es im § 1 schon vorweggenommen haben[22].

§ 4. Beweis vom Teil 2° des Satzes.

Um Teil 2° vom Satz zu beweisen nehmen wir eine einfache Gruppe $\mathfrak{G}$ mit lauter Abelschen zweitmaximalen Untergruppen an, und dann haben wir zu zeigen, dass die maximalen Untergruppen lauter $\mathfrak{G}^\circ$ sind.

Bezeichne $\mathfrak{S}$ eine p-Sylowgruppe (mit $p|O(\mathfrak{G})$), $\mathfrak{M}$ eine maximale Untergruppe, X ein nicht in $\mathfrak{M}$ liegendes Element von $\mathfrak{G}$, $\mathfrak{N}$ eine echte normale Untergruppe von $\mathfrak{M}$ (deren Existenz erst nachher sichergestellt wird), $\mathfrak{Z}$ das Zentrum von $\mathfrak{M}$. (Wir haben eben zu beweisen, dass stets $\mathfrak{Z}=1$ ist.) Wir setzen im allgemeinen $a' = XaX^{-1}$, wobei a ein Element oder eine Untergruppe von $\mathfrak{G}$ sein darf. Im Beweis gehen wir so vor, dass wir nacheinander die folgenden **a**—**m** zeigen.

a. *Es gilt* $\mathfrak{M}' \neq \mathfrak{M}$. Sonst wäre nämlich $\mathfrak{M}$ normal in $\mathfrak{G} = \{\mathfrak{M}, X\}$, wobei doch $\mathfrak{G}$ einfach ist.

b. *Bei passender Wahl von* X *sind* $\mathfrak{M}$, $\mathfrak{M}'$ *nicht fremd, was wir fortan annehmen wollen.* Wären nämlich alle $\mathfrak{M}'$ fremd zu $\mathfrak{M}$, so würde wegen **a** aus dem Satz von

---

[22] In der Arbeit [8] habe ich die $\mathfrak{G}^*$ »1-stufig nichtkommutative Gruppen«, kurz »Gruppen 1-ter Stufe« genannt und sie dort im Satz 4 (S. 234) angegeben. Dabei habe ich eine etwas abweichende Bezeichnung verwendet, so dass ich für die dortigen $G_{\mathrm{I}}(p, q, u)$, $G_{\mathrm{II}}(p, u, v)$, $G_{\mathrm{III}}(p, u, v)$ in vorliegender Arbeit $\mathfrak{G}_{\mathrm{I}}(q, p, u)$, $\mathfrak{G}_{\mathrm{II}}(p, v-1, u)$, $\mathfrak{G}_{\mathrm{III}}(p, u, v)$ geschrieben habe. (Insbesondere sind also bei G_{I} bzw. $\mathfrak{G}_{\mathrm{I}}$ die p, q umgetauscht worden.) Es ist noch zu bemerken, dass ich in der Arbeit [8] die $\mathfrak{G}_{\mathrm{I}}$, $\mathfrak{G}_{\mathrm{II}}$, $\mathfrak{G}_{\mathrm{III}}$ in drei weiteren Formen (Sätze 5, 6, 7, S. 241—244) angegeben habe. Obige Form von $\mathfrak{G}_{\mathrm{I}}$ weicht nur unwesentlich von der Form ab, in der ich $\mathfrak{G}_{\mathrm{I}}$ im Satz 5 (S. 241 in der Arbeit [8]) angegeben habe, wie man das leicht einsehen kann. Dagegen entnehme man $\mathfrak{G}_{\mathrm{II}}$, $\mathfrak{G}_{\mathrm{III}}$ am besten aus Satz 7 (S. 244 in der Arbeit [8]). Vgl. noch Satz 8 (S. 257—259 in der Arbeit [8]). Es soll bemerkt werden, dass alle Gruppen $\mathfrak{G}^*$ sich mit grosser begrifflicher Einfachheit als schiefe Produkte angeben lassen (vgl. Satz 4 in der Arbeit [8]), oben wollten wir uns aber lieber einer »expliziten« Definition der Gruppen $\mathfrak{G}^*$ bedienen. Auch bemerke ich, dass ich bald an einer anderen Stelle den Begriff des schiefen Produktes verallgemeinern werde.

Frobenius[19] wieder ein dem vorigen ähnlicher Widerspruch folgen, dass $\mathfrak{G}$ eine echte normale Untergruppe hat.

c. $\mathfrak{M}$ *ist ein* $\mathfrak{G}^*$. (Hieraus folgt nach § 3 die Existenz von $\mathfrak{N}$.) Wegen der Annahme sind nämlich alle maximalen Untergruppen von $\mathfrak{M}$ Abelsch. Mit anderen Worten ist $\mathfrak{M}$ ein $\mathfrak{G}^*$ oder Abelsch. Im letzteren Fall wäre aber der Durchschnitt $\mathfrak{M} \cap \mathfrak{M}'$ wegen **b** eine echte normale Untergruppe von $\mathfrak{G} = \{\mathfrak{M}, \mathfrak{M}'\}$, und so ist die Behauptung richtig.

d. *Ist* $\mathfrak{S}$ *Abelsch, so ist es zyklisch oder elementar.* Wegen **c** ist nämlich $\mathfrak{S}$ kein $\mathfrak{M}$, muss also in einem $\mathfrak{M}$ echt enthalten sein. Dieses $\mathfrak{M}$ ist dann keine p-Gruppe mehr, und so folgt aus **c** und § 3, dass $\mathfrak{M}$ ein $\mathfrak{G}_{\mathrm{I}}$ ist. Da die Sylowgruppen von $\mathfrak{G}_{\mathrm{I}}$ zyklisch oder elementar sind, so bezieht sich dies auch auf (seine Untergruppe) $\mathfrak{S}$, womit die Behauptung bewiesen ist.

e. $\mathfrak{M} \cap \mathfrak{M}'$ *enthält keine Untergruppe* $(\neq 1)$, *die in* $\mathfrak{M}$ *und* $\mathfrak{M}'$ *normal ist.* Sonst würde nämlich wieder die Existenz einer echten normalen Untergruppe von $\mathfrak{G} = \{\mathfrak{M}, \mathfrak{M}'\}$ folgen, was falsch ist.

f. *Es gilt* $\mathfrak{N} \neq \mathfrak{N}'$. Da nämlich $\mathfrak{N}$ und $\mathfrak{N}'$ je eine echte normale Untergruppe von $\mathfrak{M}$ bzw. $\mathfrak{M}'$ ist, so folgt die Behauptung aus **e**.

g. *Es ist* $\mathfrak{M} \neq \mathfrak{G}_8$. Bekanntlich enthält $\mathfrak{G}_8$ alle Untergruppen normal, und so folgt die Behauptung aus **b** und **e**.

h. $\mathfrak{Z}$ *und* $\mathfrak{Z}'$ *sind fremd.* Da $\mathfrak{Z} \cap \mathfrak{Z}'$ normal in $\mathfrak{M}$ und $\mathfrak{M}'$ ist, so ist die Behauptung wegen **e** richtig.

i. *Alle Elemente* $(\neq 1)$ *von* $\mathfrak{M} \cap \mathfrak{M}'$ *sind von Primzahlordnung.* Nach **e** und **g** ist nämlich $\mathfrak{M}$ (und auch $\mathfrak{M}'$) ein $\mathfrak{G}_{\mathrm{I}}$, $\mathfrak{G}_{\mathrm{II}}$ oder $\mathfrak{G}_{\mathrm{III}}$. Die zwei letzteren sind p-Gruppen, für die nach (37), (38) und (43), (44) die p-te Potenz jedes Elementes in $\mathfrak{Z}_{\mathrm{II}}$ bzw. $\mathfrak{Z}_{\mathrm{III}}$ liegt. Wenn also $\mathfrak{M}$ ein $\mathfrak{G}_{\mathrm{II}}$ oder $\mathfrak{G}_{\mathrm{III}}$ ist, so liegt die p-te Potenz jedes Elementes von $\mathfrak{M} \cap \mathfrak{M}'$ in $\mathfrak{Z} \cap \mathfrak{Z}'$, woraus wegen **h** die Richtigkeit der Behauptung für diese Fälle folgt. Im übriggebliebenen Fall ist $\mathfrak{M}$ ein $\mathfrak{G}_{\mathrm{I}} = \mathfrak{G}_{\mathrm{I}}(p, q, u)$. Ist dabei $u = 1$, so ist $\mathfrak{M}$ ein $\mathfrak{G}^\circ$, und dann sind sogar alle Elemente von $\mathfrak{M}$ von der behaupteten Eigenschaft. Im Falle $u \geqq 2$ bezeichne U ein Element von $\mathfrak{G}_{\mathrm{I}}$ von zusammengesetzter Ordnung. Dann ist nach (31) entweder $pq \mid O(U)$ oder ist $O(U)$ eine Potenz $(\geqq q^2)$ von q. Entsprechend liegt U^p bzw. U^q nach (29), (32) leicht ersichtlich in $\mathfrak{Z}_{\mathrm{I}}$. Gibt es also ein solches Element U in $\mathfrak{M} \cap \mathfrak{M}'$, so liegt U^p bzw. U^q in $\mathfrak{Z} \cap \mathfrak{Z}'$. Das steht mit **h** in einem Widerspruch, woraus die Behuptung folgt.

j. $\mathfrak{M}$ ist kein $\mathfrak{G}_{\mathrm{II}} = \mathfrak{G}_{\mathrm{II}}(p, u, v)$ mit $O(\mathfrak{G}_{\mathrm{II}}) > 8$. Denn nehmen wir an, dass $\mathfrak{M} = \mathfrak{G}_{\mathrm{II}}$, $O(\mathfrak{G}_{\mathrm{II}}) > 8$ ist. Bezeichne $U(\neq 1)$ ein Element von $\mathfrak{M} \cap \mathfrak{M}'$. Nach **h**

gilt $U^p = 1$. Wir behalten für G_{II} die Bezeichnungen in (33) und zeigen, dass U von der Form

$$U = A^{p^u x} B^{p^{v-1} y} \tag{45}$$

ist. Denn setzen wir $U = A^i B^k$. Es ist $p^u | i$, $p^{v-1} | k$ zu zeigen. Wegen $U^p = 1$ und (37) gilt

$$A^{ip+p^u ik\binom{p}{2}} B^{kp} = 1 ,$$

d. h. wegen (35)

$$p^u | i\left(1+p^{u-1}k\binom{p}{2}\right), \quad p^{v-1} | k .$$

Hieraus folgt die behauptete Teilbarkeit für i und k, oder es muss

$$p | 1+p^{u-1}k\binom{p}{2}$$

gelten. Dann ist aber gewiss

$$p \nmid p^{u-1}k\binom{p}{2},$$

also $u = 1$, $p \nmid k$, $v = 1$, $p = 2$ und nach (34) $O(\mathfrak{M}) = 8$. Mit diesem Widerspruch haben wir (45) gezeigt.

Wir zeigen $v = 1$. Sonst liegt nämlich U wegen (45), (38) in $\mathfrak{Z}$ und aus Symmetriegründen auch in $\mathfrak{Z}'$. Das stösst in **h**, und so ist in der Tat $v = 1$.

Wir setzen $\mathfrak{N} = \{A^p, B\}$; es ist $\mathfrak{N}$ maximal also auch normal in (der p-Gruppe) $\mathfrak{M}$. Wegen (45) gilt $U \in \mathfrak{N}$, und so gilt aus Symmetriegründen auch $U \in \mathfrak{N}'$. Da $\mathfrak{N}$, $\mathfrak{N}'$ Abelsch sind, so ist $\{U\}$ normal in $\{\mathfrak{N}, \mathfrak{N}'\}$, folglich muss $\{\mathfrak{N}, \mathfrak{N}'\} \subset \mathfrak{G}$ gelten. Ausserdem gilt nach **f** $\mathfrak{N} \neq \mathfrak{N}'$.

Wir zeigen, dass $\{\mathfrak{N}, \mathfrak{N}'\}$ keine p-Gruppe ist. Denn nehmen wir das Gegenteil an. Da $\mathfrak{N}$ maximal in $\mathfrak{M}$ und $\neq \mathfrak{N}'$ ist, so folgt hieraus, dass $\{\mathfrak{N}, \mathfrak{N}'\}$ eine p-Sylowgruppe von $\mathfrak{G}$, also zu $\mathfrak{M}$ konjugiert ist. Nun sind aber alle Elemente von $\mathfrak{N}$ (wegen $v = 1$) offenbar von einer Ordnung $< O(A)$ $(= p^{u+1})$. Das gilt auch für $\mathfrak{N}'$, und so folgt aus dem obengesagten, dass sich $\mathfrak{M}(= \mathfrak{G}_{II}(p, u, 1))$ durch Elemente von der Ornung $< O(A)$ erzeugen lässt. Folglich muss es mindestens ein Element $A^i B^k (p \nmid i)$ mit $O(A^i B^k) \leqq \frac{1}{p} O(A) = p^u$ geben. Aus (37) (mit $t = p^u$) ergibt sich wegen (35)

$$p^{u+1} | ip^u + p^u ik\binom{p^u}{2},$$

also $p \nmid \binom{p^u}{2}$, $p = 2$, $u = 1$. Wegen $v = 1$ sind wir wieder auf den Widerspruch $O(\mathfrak{M}) = 8$ gestossen. Wir haben gezeigt, dass $\{\mathfrak{N}, \mathfrak{N}'\}$ keine p-Gruppe ist.

Hieraus folgt nach obigem auch, dass $\{\mathfrak{N}, \mathfrak{N}'\}$ nichtabelsch, also maximal in $\mathfrak{G}$ ist. Da $\{\mathfrak{N}, \mathfrak{N}'\}$ die Abelsche, nichtzyklische p-Untergruppe $\mathfrak{N}$ hat, so muss $\{\mathfrak{N}, \mathfrak{N}'\}$ nach § 3 ein $\mathfrak{G}_{\mathrm{I}}(p, q, u)$ sein und die (einzige) p-Sylowgruppe dieser Gruppe muss $\mathfrak{N}$, $\mathfrak{N}'$ enthalten. Diese p-Sylowgruppe ist aber Abelsch, und so folgt, dass auch $\{\mathfrak{N}, \mathfrak{N}'\}$ Abelsch ist. Dieser Widerspruch beweist die Behauptung.

k. *$\mathfrak{M}$ ist kein $\mathfrak{G}_{\mathrm{III}} = \mathfrak{G}_{\mathrm{III}}(p, u, v)$ mit $O(\mathfrak{G}_{\mathrm{III}}) > p^3$.* Der Beweis wird dem von **j** sehr ähnlich aber etwas leichter. Wir nehmen wieder an, dass die Behauptung falsch also $\mathfrak{M} = \mathfrak{G}_{\mathrm{III}}$, $O(\mathfrak{G}_{\mathrm{II}}) > p^3$ ist, und bezeichnen mit $U(\neq 1)$ ein Element von $\mathfrak{M} \cap \mathfrak{M}'$, wofür nach **h** wieder $U^p = 1$ gelten muss. Aus (43) folgt sofort

$$U = A^{p^{u-1}x} B^{p^{v-1}y} C^z . \tag{46}$$

Wieder zeigt sich $v = 1$, denn sonst liegt U wegen (44), (46) in $\mathfrak{Z}$, ebenfalls auch in $\mathfrak{Z}'$, ein Widerspruch mit **h**.

Aus $v = 1$, (40) und der Annahme $O(\mathfrak{M}) > p^3$ folgt $u \geqq 2$.

Wir setzen jetzt $\mathfrak{N} = \{A^p, B, C\}$; wieder ist $\mathfrak{N}$ maximal und normal in $\mathfrak{M}$. Nach (46) gilt $U \in \mathfrak{N}$ und aus Symmetriegründen $U \in \mathfrak{N}'$, und weiter folgt ebenso wie bei **j** $\{\mathfrak{N}, \mathfrak{N}'\} \subset \mathfrak{G}$, $\mathfrak{N} \neq \mathfrak{N}'$.

Wieder zeigen wir, dass $\{\mathfrak{N}, \mathfrak{N}'\}$ keine p-Gruppe ist. Sonst folgt, dass $\{\mathfrak{N}, \mathfrak{N}'\}$ eine p-Sylowgruppe mithin zu $\mathfrak{M}$ konjugiert ist. Anderseits sind wegen $v = 1$, $u \geqq 2$ und (43) die Elemente von $\mathfrak{N}$ von einer Ordnung $< O(A) (= p^u)$, desgleichen die von $\mathfrak{N}'$, und so lässt sich $\mathfrak{M}$ durch Elemente von der Ordnung $< O(A)$ erzeugen. Folglich muss es ein Element $A^i B^k C^m (p \nmid i)$ mit $O(A^i B^k C^m) \leqq \frac{1}{p} O(A) = p^{u-1}$ geben, ein offenbarer Widerspruch mit (43). In der Tat ist $\{\mathfrak{N}, \mathfrak{N}'\}$ keine p-Gruppe.

Von hier an gilt der Beweis wörtlich ebenso wie bei **j**, und so ist die Behauptung richtig.

l. *$\mathfrak{M}$ ist kein $\mathfrak{G}_{\mathrm{III}} = \mathfrak{G}_{\mathrm{III}}(p, u, v)$ mit $O(\mathfrak{G}_{\mathrm{III}}) = p^3$.* Denn nehmen wir an, dass $\mathfrak{M} = \mathfrak{G}_{\mathrm{III}}$, $O(\mathfrak{G}_{\mathrm{III}}) = p^3$ (also $u = v = 1$) ist. Wegen $O(\mathfrak{M}) = O(\mathfrak{M}')$ ist $O(\mathfrak{M} \cap \mathfrak{M}') < p^2$, denn sonst wäre $\mathfrak{M} \cap \mathfrak{M}'$ normal in $\mathfrak{M}$ und $\mathfrak{M}'$ im Gegensatz zu **f**. Wegen **b** lässt sich also $\mathfrak{M} \cap \mathfrak{M}' = \{U\}$ setzen mit $O(U) = p$.

Nach (44) ist jetzt $\mathfrak{Z} = \{C\}$, $\mathfrak{Z}' = \{C'\}$. Diese sind nach **h** verschieden, und so lässt sich aus Symmetriegründen annehmen, dass U kein Element von $\{C\}$ ist.

Wir setzen $\mathfrak{K} = \{U, C\}$ und

$$\mathfrak{L} = \begin{cases} \{U, C'\}, & \text{wenn} \quad \{U\} \neq \{C'\}, \\ \{U, A'\}, & \text{wenn} \quad \{U\} = \{C'\}. \end{cases}$$

Diese Gruppen $\mathfrak{K}$, $\mathfrak{L}$ sind Abelsch und elementar von der Ordnung p^2, und somit normal in $\mathfrak{M}$ bzw. $\mathfrak{M}'$ enthalten. Hieraus folgt nach **e** $\mathfrak{K} \neq \mathfrak{L}$. Andererseits ist $\{U\}$ normal in $\{\mathfrak{K}, \mathfrak{L}\}$, und so ist diese Gruppe echt enthalten in $\mathfrak{G}$. Auch ist sie nichtabelsch, denn sonst wäre sie Abelsch von der Ordnung p^3 und somit konjugiert zur Sylowgruppe $\mathfrak{M}$; das ist aber unmöglich, da $\mathfrak{M}$ nichtabelsch ist. Nach diesem ist $\{\mathfrak{K}, \mathfrak{L}\}$ nichtabelsch und maximal in $\mathfrak{G}$.

Zuerst nehmen wir an, dass $\{\mathfrak{K}, \mathfrak{L}\}$ ein $\mathfrak{G}_\mathrm{I}$ ist. Da aber $\{\mathfrak{K}, \mathfrak{L}\}$ die zwei verschiedenen nichtzyklischen Abelschen p-Untergruppen $\mathfrak{K}$, $\mathfrak{L}$ enthält, die elementenweise nicht miteinander vertauschbar sind, so ist diese Annahme falsch.

Es bleibt nur übrig, dass $\{\mathfrak{K}, \mathfrak{L}\}$ eine nichtabelsche p-Gruppe, somit konjugiert zu $\mathfrak{M}$ ist. Dabei sind diese Gruppen verschieden, denn sonst wäre $\mathfrak{L} \subset \mathfrak{M}$; ausserdem gilt $\mathfrak{L} \subset \mathfrak{M}'$ also $\mathfrak{L} \subseteq \mathfrak{M} \cap \mathfrak{M}'$, wobei doch die rechte Seite gleich $\{U\}$ ($\subset \mathfrak{L}$) ist. Dieser Widerspruch beweist $\{\mathfrak{K}, \mathfrak{L}\} \neq \mathfrak{M}$. Nun ist $\mathfrak{K}$ (maximal also) normal in $\{\mathfrak{K}, \mathfrak{L}\}$ und $\mathfrak{M}$, folglich auch normal in $\{\{\mathfrak{K}, \mathfrak{L}\}, \mathfrak{M}\} = \mathfrak{G}$. Dieser Widerspruch beweist die Behauptung.

m. $\mathfrak{M}$ ist ein $\mathfrak{G}^\circ$. Nach **c** ist nämlich $\mathfrak{M}$ ein $\mathfrak{G}^*$ und nach **g**, **j**, **k**, **l** keine p-Gruppe (man nehme in Rücksicht, dass der Ausnahmefall $\mathfrak{M} = \mathfrak{G}_\mathrm{II}$, $O(\mathfrak{G}_\mathrm{II}) = 8$ von **j** wegen $\mathfrak{G}_\mathrm{II}(2, 1, 1) = \mathfrak{G}_\mathrm{III}(2, 1, 1)$ in **l** erledigt wurde). Folglich ist $\mathfrak{M}$ ein $\mathfrak{G}_\mathrm{I} = \mathfrak{G}_\mathrm{I}(p, q, u)$. Wir haben also nur noch $u = 1$ zu zeigen. Nehmen wir deshalb $u \geqq 2$ an.

Da das obengesagte für alle maximalen Untergruppen von $\mathfrak{G}$ gilt, so können wir hieraus die Bemerkung voranschicken, dass alle Sylowgruppen von $\mathfrak{G}$ Abelsch und zwar zyklisch oder elementar sind.

Bezeichne $\mathfrak{S}_0$ die p-Sylowgruppe von $\mathfrak{M}$, die also elementar von der Ordnung p^e und normal in $\mathfrak{M}$ ist. Wir setzen $\mathfrak{N} = \{\mathfrak{S}_0, Q^q\}$. Dies ist die einzige (maximale) Untergruppe von der Ordnung $p^e q^{u-1}$ von $\mathfrak{G}_\mathrm{I}$, ist auch normal und Abelsch.

$\mathfrak{S}_0$ ist auch eine Sylowgruppe von $\mathfrak{G}$. Bezeichne nämlich $\mathfrak{S}$ eine Sylowgruppe von $\mathfrak{G}$ über $\mathfrak{S}_0$. Wäre $\mathfrak{S}_0 \subset \mathfrak{S}$, so wäre $\mathfrak{S}_0$ normal in $\mathfrak{S}$ und $\mathfrak{M}$, also auch in $\mathfrak{G} = \{\mathfrak{S}_0, \mathfrak{M}\}$. Dies ist unmöglich, und so ist in der Tat $\mathfrak{S}_0 = \mathfrak{S}$. Deshalb schreiben wir nachher $\mathfrak{S}$ statt $\mathfrak{S}_0$.

$\mathfrak{N}'$ ist nicht enthalten in $\mathfrak{M}$, denn nach **e** ist $\mathfrak{N}' \neq \mathfrak{N}$, und $\mathfrak{N}$ ist die einzige Untergruppe von $\mathfrak{M}$ von der Ordnung $p^e q^{u-1}$.

Wir zeigen, dass $\mathfrak{N}$, $\mathfrak{N}'$ fremd sind. Denn setzen wir $\mathfrak{N}_0 = \mathfrak{N} \cap \mathfrak{N}'$ und nehmen

$\mathfrak{N}_0 \neq 1$ an. $\mathfrak{N}_0$ ist normal in $\mathfrak{N}$ und $\mathfrak{N}'$, folglich auch in $\{\mathfrak{N}, \mathfrak{N}'\}$, und so ist letztere Gruppe echt enthalten in $\mathfrak{G}$. Auch ist sie nichtabelsch, denn sonst müssen die in den $\mathfrak{N}, \mathfrak{N}'$ enthaltenen Sylowgruppen $\mathfrak{S}, \mathfrak{S}'$ von $\mathfrak{G}$ gleich sein; dies bedeutet $\mathfrak{S} = X\mathfrak{S}X^{-1}$, woraus folgt, dass $\mathfrak{S}$ normal in $\mathfrak{G} = \{\mathfrak{M}, X\}$ ist. Wegen dieses Widerspruchs ist $\{\mathfrak{N}, \mathfrak{N}'\}$ in der Tat nichtabelsch, und so ist es nach obigem ein $\mathfrak{G}_I$. Dabei ist $\mathfrak{S}$ nicht normal in $\{\mathfrak{N}, \mathfrak{N}'\}$. Da nämlich $\mathfrak{N}'$ nicht in $\mathfrak{M}$ liegt, so ist $\mathfrak{G} = \{\mathfrak{M}, \mathfrak{N}'\}$; wäre nun $\mathfrak{S}$ normal in $\{\mathfrak{N}, \mathfrak{N}'\}$, so müsste es auch normal in $\mathfrak{G}$ sein, was nicht sein kann. Andererseits ist $\mathfrak{S}$ eine Sylowgruppe von $\{\mathfrak{N}, \mathfrak{N}'\}$, und so folgt aus beiden nach § 3, dass $\mathfrak{S}$ zyklisch ist. Es ist auch elementar von der Ordnung p^e, woraus folgt $e = 1\big(O(\mathfrak{S}) = p\big)$. Wegen $q|O(\mathfrak{N})$ gilt noch mehr $q|O(\{\mathfrak{N}, \mathfrak{N}'\})$. Andererseits folgt aus $O(\mathfrak{S}) = p$, dass $p||O(\mathfrak{G})$ und so ist auch $p||O(\{\mathfrak{N}, \mathfrak{N}'\})$. Beide ergeben, da $\{\mathfrak{N}, \mathfrak{N}'\}$ ein $\mathfrak{G}_I$ ist, dass $O(\{\mathfrak{N}, \mathfrak{N}'\}) = pq^t$ gilt mit einem $t \geqq 1$. Nun hat also $\{\mathfrak{N}, \mathfrak{N}'\}$ nach § 3 eine einzige normale Sylowgruppe $\overline{\mathfrak{S}}$. Diese ist auch elementar und von der Ordnung p oder q^t. Andererseits haben wir schon bemerkt, dass $\mathfrak{S}$ nicht normal in $\{\mathfrak{N}, \mathfrak{N}'\}$ ist, und so muss $O(\overline{\mathfrak{S}}) = q^t$ gelten. Da ferner $\{\mathfrak{N}, \mathfrak{N}'\}$ maximal in $\mathfrak{G}$ ist, so lässt sich das oben über $(\mathfrak{S}_0 =)\ \mathfrak{S}$ bewiesene auch auf $\overline{\mathfrak{S}}$ anwenden, nach dem also $\overline{\mathfrak{S}}$ eine q-Sylowgruppe von $\mathfrak{G}$ ist. Das hat zur Folge, dass es (wie in $\overline{\mathfrak{S}}$ auch) in $\mathfrak{G}$ keine Elemente von einer durch q^2 teilbaren Ordnung gibt. Das ist aber ein Widerspruch, da schon $\mathfrak{M}$ zyklische q-Sylowgruppen von der Ordnung $q^u (\geqq q^2)$ enthält. Wir haben gezeigt, dass $\mathfrak{N}, \mathfrak{N}'$ fremd sind.

Wegen $\mathfrak{N} = \{\mathfrak{S}, Q^q\}$ und (31) besteht $\mathfrak{N}$ aus allen Elementen von $\mathfrak{M}$, deren Ordnung $\neq q^u$ ist. Ähnlich besteht $\mathfrak{N}'$ aus allen Elementen von $\mathfrak{M}'$, deren Ordnung $\neq q^u$ ist. Hieraus folgt nach dem eben bewiesenen, dass alle Elemente $(\neq 1)$ von $\mathfrak{M} \cap \mathfrak{M}'$ von der Ordnung q^u sind. Wegen $u \geqq 2$ folgt hieraus offenbar, dass $\mathfrak{M} \cap \mathfrak{M}'$ überhaupt kein Element $\neq 1$ enthält. Dies steht mit **b** in einem Widerspruch, womit wir (**m** und auch) den Teil 2° des Satzes bewiesen haben.

§ 5. Beweis des Zusatzes.

Alle Behauptungen 1.-13. des Zusatzes beweisen wir der Reihe nach so:

ad 1: Dies ist nämlich eine Wiederholung der Definition von $\mathfrak{E}$[15].

ad 2: Bezeichne $\mathfrak{S}$ eine Sylowgruppe von $\mathfrak{E}$. Da $\mathfrak{S}$ kein $\mathfrak{G}^\circ$ ist, so ist es in einem $\mathfrak{G}^\circ \big(= \mathfrak{G}_I(p, q, 1)\big)$ echt enthalten. Hieraus folgt die Behauptung.

ad 3: Denn betrachten wir zwei verschiedene, nicht fremde Sylowgruppen $\mathfrak{S}, \mathfrak{S}_1$, die dann notwendig zu demselben p gehören, und setzen $\mathfrak{D} = \mathfrak{S} \cap \mathfrak{S}_1 (\neq 1)$. Dann ist $\mathfrak{D}$ normal in $\{\mathfrak{S}, \mathfrak{S}_1\}$, folglich ist diese Gruppe echt enthalten in $\mathfrak{E}$. Auch

muss sie nichtabelsch, d. h. ein $\mathfrak{G}^\circ(p, q)$ oder $\mathfrak{G}^\circ(q, p)$ sein. Von diesen Gruppen kann aber nur die erste die p-Gruppe $\mathfrak{D}$ normal enthalten, und dabei muss $\mathfrak{D}$ die p-Sylowgruppe von $\mathfrak{G}^\circ(p, q)$ $(= \{\mathfrak{S}, \mathfrak{S}_1\})$ sein. Hieraus folgt $O(\mathfrak{S})|O(\mathfrak{D})$. Da auch $O(\mathfrak{D})|O(\mathfrak{S})$ gilt, so ist $O(\mathfrak{D}) = O(\mathfrak{S})$ $(= O(\mathfrak{S}_1))$. Hiernach enthält $\mathfrak{G}^\circ(p, q)$ die verschiedenen normalen Sylowgruppen $\mathfrak{S}$, $\mathfrak{S}_1$. Dieser Widerspruch beweist die Behauptung.

ad 4: Die maximalen Untergruppen $\mathfrak{G}^\circ$ von $\mathfrak{E}$ enthalten nämlich nur solche echten Untergruppen, die von Primzahlpotenzordnung sind.

ad 5: Bezeichne $\mathfrak{S}$ eine Sylowgruppe von $\mathfrak{E}$ und $\mathfrak{N}$ ihren Normalisator. Wegen des schon bewiesenen 4. genügt es zu zeigen, dass $\mathfrak{S} \subset \mathfrak{N}$ gilt. Andernfalls wäre $\mathfrak{S}$ sein eigener Normalisator, und dann folgte aus 3. und dem Satz von Frobenius[19] der Widerspruch, dass $\mathfrak{E}$ nichteinfach ist.

ad 6: Folgt aus 5.

ad 7: Denn bezeichne $\mathfrak{S}$ eine Sylowgruppe von $\mathfrak{E}$, $\mathfrak{S}_0$ eine echte Untergruppe von ihr, $\mathfrak{N}_0$ den Normalisator von $\mathfrak{S}_0$. Wegen 2. ist $\mathfrak{S} \subsetneqq \mathfrak{N}_0$. Wenn also die Behauptung falsch ist, so ist $\mathfrak{S} \subset \mathfrak{N}_0$, also nach 4. $\mathfrak{N}_0$ ein $\mathfrak{G}^\circ$. Dies enthält aber nur die einzige echte normale Untergruppe $\mathfrak{S}$, dieser Widerspruch beweist die Behauptung.

ad 8: Nämlich ist jedes Element in einem $\mathfrak{G}^\circ$ enthalten.

ad 9: Es seien U, V zwei vertauschbare Elemente von $\mathfrak{E}$. Dann ist $\{U, V\}$ Abelsch, und so folgt die Behauptung aus 4.

ad 10: Da $\mathfrak{N}_p$ sein eigener Normalisator ist, so folgt die Richtigkeit von (8).

ad 11: Betrachten wir ein $\mathfrak{N}_p = \mathfrak{G}^\circ(p, p')$ und eine der Konjugierten $\overline{\mathfrak{N}}_p (\neq \mathfrak{N}_p)$. Wir setzen $\mathfrak{D} = \mathfrak{N}_p \cap \overline{\mathfrak{N}}_p$. Die p-Sylowgruppen von $\mathfrak{N}_p$, $\overline{\mathfrak{N}}_p$ sind verschieden, denn sie haben die verschiedenen Normalisatoren $\mathfrak{N}_p$, $\overline{\mathfrak{N}}_p$, folglich sind sie nach 3. auch fremd. Hieraus folgt $p \nmid O(\mathfrak{D})$, und so ist in der Tat nur $O(\mathfrak{D}) = 1$ oder p' möglich. Der zweite Fall hiervon muss nach § 4 **b** für mindestens ein $\mathfrak{N}_p$ wirklich vorkommen, und so ist die Behauptung richtig.

ad 12: Da jedes $\mathfrak{S}_p$ genau $p^e - 1$ Elemente p-ter Ordnung enthält, so folgt (9) aus (8) und 2. Wegen 8. ergibt sich dann (11) aus (9). Nach 9. hat jedes Element p-ter Ordnung genau $\frac{\nu}{p^e}$ Konjugierte, und so folgt hieraus und aus (9) die Richtigkeit von (10). Aus (11) ergibt sich auch (12).

ad 13: Es genügt zu zeigen, dass es in $\mathfrak{E}$ zwei Elemente X, $Y(\neq 1)$ gibt, die in keiner maximalen Untergruppe $\mathfrak{N}_p = \mathfrak{G}^\circ(p, p')$ liegen. Das trifft gewiss zu, wenn $O(X)$, $O(Y)$ ein Paar verschiedener Primzahlen ist, das mit keinem Paar p, p' (oder p', p) übereinstimmt. Bezeichne t die Anzahl aller verschiedenen Primfaktoren

von ν. Dann ist t zugleich die Anzahl der Paare p, p', andererseits lassen sich aus den verschiedenen Primfaktoren von ν genau $\binom{t}{2}$ Paare bilden. Wenn also $\binom{t}{2} > t$, d. h. $t > 3$ ist, so folgt aus dem obengesagten die Richtigkeit der Behauptung. Da wegen der Einfachheit von $\mathfrak{E}$ $t \geqq 3$ ist[23], so haben wir nur noch den Fall $t = 3$ zu untersuchen. Bezeichnen wir mit p, q, r die verschiedenen Primfaktoren von ν. Kommen nicht alle Paare p, q; p, r; q, r (in irgendeiner Reihenfolge der Elemente) unter den p, p'; q, q'; r, r' vor, so schliesst man ebenso wie vordem. Im übriggebliebenen Fall gilt mit geeigneter Bezeichnung

$$p' = q\,, \quad q' = r\,, \quad r' = p\,.$$

Aus (12) folgt noch $\frac{1}{p}+\frac{1}{q}+\frac{1}{r} > 1$, und so müssen p, q, r in irgendeiner Reihenfolge mit 2, 3, 5 übereinstimmen. Das lässt nur die zwei Möglichkeiten zu:

$$2' = 3\,, \quad 3' = 5\,, \quad 5' = 2$$

oder

$$2' = 5\,, \quad 5' = 3\,, \quad 3' = 2\,.$$

Da im allgemeinen $e = O(p \,(\mathrm{mod}\, p'))$ gilt, so muss entsprechend $\nu = 2^2 \cdot 3^4 \cdot 5$ bzw. $\nu = 2^4 \cdot 3 \cdot 5^2$ sein. Man rechnet aber leicht nach, dass (11) in keinem dieser zwei Fälle befriedigt ist, womit wir den Zusatz bewiesen haben.

§ 6. Beweis vom Teil 3° des Satzes.

Wir zeigen zuerst folgendes (übrigens bekanntes) Lemma, von dem wir im nachfolgenden Beweis von 3° wiederholt Gebrauch machen werden.

Irgendzwei verschiedene Elemente X, Y von 2-ter Ordnung einer Gruppe erzeugen stets eine Diedergruppe. Wird $Z = XY$ gesetzt, so gilt $XZX^{-1} = Z^{-1}$ und $O(\{X, Y\}) = 2O(Z)$. Alle verschiedenen Elemente von $\{X, Y\}$ sind Z^i und $XZ^i (i = 0, \ldots, O(Z)-1)$, die letzteren sind von 2-ter Ordnung.

Hiervon brauchen wir nur $XZX^{-1} = Z^{-1}$ zu zeigen. Diese Gleichung ist richtig, denn links und rechts stehen die gleichen Elemente YX^{-1}, $Y^{-1}X^{-1}$.

Bezeichne nunmehr $\mathfrak{E}$ eine (einfache) Gruppe mit lauter Abelschen zweitmaximalen Untergruppen und gerader Ordnung. Wir haben zu beweisen, dass $\mathfrak{E} = \mathfrak{G}_{60}$ ist.

---

[23] $t \geqq 3$ folgt auch aus (12).

Wir übernehmen für $\mathfrak{E}$ alle Bezeichnungen des Zusatzes, so dass dann jetzt $2|\nu$ gilt. Insbesondere setzen wir

$$2' = \pi\,, \quad 2^c||\nu\,, \quad \pi|2^c-1 \qquad\qquad c = O\big(2\,(\mathrm{mod}\ \pi)\big)\,, \tag{47}$$

wobei dann π ein ungerader Primfaktor von ν ist und notwendig $c \geqq 2$ gilt. Die Anzahl der 2-Sylowgruppen $\mathfrak{S}_2$ ist nach (8)

$$\mu = \frac{\nu}{2^c\pi}\,. \tag{48}$$

Wir wählen ein $\mathfrak{S}_2$ fest, das wir mit $\mathfrak{S}$ bezeichnen. Alle Elemente $(\neq 1)$ von $\mathfrak{S}$ und den übrigen $\mathfrak{S}_2$ bezeichnen wir bzw. mit (vgl. Zusatz 2., 3.):

$$A_1, \ldots, A_{2^c-1}\,, \tag{49}$$

$$B_1, \ldots, B_{(\mu-1)(2^c-1)}\,. \tag{50}$$

Wir bilden alle Produkte A_iB_j, ihre Zahl ist

$$(\mu-1)\,(2^c-1)^2\,, \tag{51}$$

und zeigen, dass sie alle verschieden sind. Wenn nämlich $A_iB_j = A_kB_l$ ist, so ist $B_j = (A_iA_k)B_l$ von der 2-ten Ordnung, d. h. $(A_iA_k)B_l = B_l(A_iA_k)$. Dies ist wegen Zusatz 9. nur mit $A_iA_k = 1$ möglich, und dann gilt $A_i = A_k$, $B_j = B_l$. In der Tat sind die A_iB_j verschieden.

Wir zeigen

$$\pi = 2^c-1\,. \tag{52}$$

Nach dem jetzt bewiesenen ist (51) die Mindestzahl der Elemente $(\neq 1)$ von $\mathfrak{E}$, und so folgt aus (48)

$$\nu = 2^c\pi\mu > (\mu-1)\,(2^c-1)^2\,.$$

Wäre nun (52) falsch, so ist wegen (47) $2^c-1 \geqq 3\pi$, und dann hat man aus vorigem

$$2^c\mu > 3(\mu-1)\,(2^c-1)\,.$$

Hieraus folgt

$$3(2^c-1) > \mu(2\cdot 2^c-3)\,.$$

Wegen (48) ist aber $\mu \geqq 3$, und so folgt weiter

$$2^c-1 > 2\cdot 2^c-3$$

d. h. $2 > 2^c$, $c < 1$. Dieser Widerspruch beweist (52).

Da wieder nach Zusatz 9. alle Paare A_i, B_j unvertauschbar sind, so sind die

$\{A_i, B_j\}$ nach dem Lemma nichtabelsche Diedergruppen, zugleich also maximale Untergruppen von $\mathfrak{E}$. Dann muss jedes $\{A_i, B_j\}$ ein $\mathfrak{G}^\circ(p, 2)$ sein[24].

Wir bezeichnen deshalb mit $p_1, \ldots, p_t (t \geqq 1)$ alle verschiedenen Primfaktoren von ν mit der Eigenschaft, dass es in $\mathfrak{E}$ Untergruppen $\mathfrak{G}^\circ(p_s, 2)$ gibt. (Mit anderen Worten sind die p_s sämtliche Lösungen von $p_s' = 2$)[25]. Wegen $p_s \neq 2$, $2|p_s-1$ ist $O\big(p_s \pmod 2\big) = 1$ und so enthält ν alle p_s nur einmal:

$$p_1, \ldots, p_t || \nu \,. \tag{53}$$

Auch gilt

$$O\big(\mathfrak{G}^\circ(p_s, 2)\big) = 2p_s \qquad (s = 1, \ldots, t) \,. \tag{54}$$

Es folgt noch, dass alle A_iB_j von einer Ordnung $p_1, \ldots, p_t$ sind[26].

Wir zeigen

$$t = 2 \,. \tag{55}$$

Mann summiere nämlich in (13) nur über die $p = p_1, \ldots, p_t$; jedesmal ist wegen (53) $e = 1$ zu setzen, und so folgt

$$1 > \sum_{i=1}^{t} \frac{p_i-1}{2p_i} = \frac{1}{2} \sum_{i=1}^{t} \left(1-\frac{1}{p_i}\right),$$

d. h.

$$\frac{1}{p_1} + \cdots + \frac{1}{p_t} > t-2 \,.$$

Die linke Seite ist im Fall $t \geqq 3$ nicht grösser als $\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+(t-3)\,(<t-2)$, und so muss $t \leqq 2$ gelten. Zum vollen Beweis von (55) nehmen wir $t = 1$ an. Dann sind alle A_iB_j von der Ordnung p_1. Wegen (9) (angewandt für $p = p_1$) und (51) folgt hieraus

$$\frac{\nu(p_1-1)}{2p_1} \geqq (\mu-1)(2^c-1)^2 \,.$$

Nach (52) gilt dann

$$\frac{\nu}{2} > \pi(\mu-1)(2^c-1) \,.$$

Man setze (48) ein:

---

[24] Die andere Möglichkeit $\{A_i, B_j\} = \mathfrak{G}^\circ(2, p)$ fällt aus, denn die einzige echte normale Untergruppe dieser Gruppe ist ein $\mathfrak{S}_2$ also (wegen $c \geqq 2$) nichtzyklisch, wobei doch alle Diedergruppen mindestens eine zyklische echte normale Untergruppe enthalten.

[25] Wir wollen bemerken, dass π sehr wohl unter den $p_1, \ldots, p_t$ vorkommen kann, denn $2' = \pi$, $\pi' = 2$ schliessen einander nicht aus.

[26] Weil nämlich $\{A_iB_j\}$ die einzige echte normale Untergruppe von $\{A_i, B_j\}$ ist.

$$2^{c-1}\mu > (\mu-1)(2^c-1)\,,$$

d. h.

$$2^c-1 > \mu(2^{c-1}-1)\,.$$

Es folgt

$$2^c-2 \geqq \mu(2^{c-1}-1)\,,$$

d. h. $2 \geqq \mu$. Wie schon erwähnt, muss aber $\mu \geqq 3$ sein. Dieser Widerspruch beweist (55).

Bemerken wir die Folgerung von (52), (10), dass alle Elemente 2-ter Ordnung von $\mathfrak{E}$ miteinander konjugiert sind.

Bezeichnen wir die p_s-Sylowgruppen von $\mathfrak{E}$ mit $\mathfrak{S}^s (s = 1, 2)$. Wegen $p_s' = 2$ hat jedes $\mathfrak{S}^s$ ein $\mathfrak{G}^\circ(p_s, 2)$ zum Normalisator (in $\mathfrak{E}$). Dies hat zur Folge, dass jedes $\mathfrak{S}^s$ mit einem Element 2-ter Ordnung von $\mathfrak{E}$ vertauschbar ist. Da alle Elemente 2-ter Ordnung von $\mathfrak{E}$ konjugiert sind, so gibt es umgekehrt zu jedem solchen Element ein mit ihm vertauschbares $\mathfrak{S}^1$ und $\mathfrak{S}^2$.

Wir wählen ein Element A in (49) fest[27], bezeichnen mit n_s die Anzahl der mit A vertauschbaren $\mathfrak{S}^s (s = 1, 2)$ und wollen n_s bestimmen. Hierzu halten wir $s (= 1, 2)$ fest, und bezeichnen ein festes, mit A vertauschbares $\mathfrak{S}^s$ mit $\mathfrak{S}_0$, wobei dann $O(\mathfrak{S}_0) = p_s$ gilt und $\{A, \mathfrak{S}_0\}$ eine Untergruppe $\mathfrak{G}^\circ(p_s, 2)$ von $\mathfrak{E}$ ist. Ein beliebiges $\mathfrak{S}^s$ können wir in der Form $X\mathfrak{S}_0X^{-1}$ annehmen mit $X \in \mathfrak{E}$. Hierfür lautet die Bedingung der Vertauschbarkeit mit A so: $AX\mathfrak{S}_0X^{-1}A^{-1} = X\mathfrak{S}_0X^{-1}$, d. h. $X^{-1}AX \cdot \mathfrak{S}_0 \cdot X^{-1}A^{-1}X = \mathfrak{S}_0$. Dies ist wieder äquivalent damit, dass $X^{-1}AX$ zum Normalisator $\{A, \mathfrak{S}_0\}$ von $\mathfrak{S}_0$ gehört, d. h. (wegen $O(A) = 2$) von der Form AS_0^i ist, wobei S_0 ein erzeugendes Element von $\mathfrak{S}_0$ bezeichnet. Da $O(S_0) = p_s$ ungerade ist, so dürfen wir uns auf gerade Zahlen $i = 2k$ beschränken, und dann sind die gesuchten X mit der Bedingung $X^{-1}AX = AS_0^{2k}$ charakterisiert. Wegen $AS_0A^{-1} = S_0^{-1}$ lässt sich hierfür $S_0^kX^{-1}AXS_0^{-k} = A$ schreiben, und dies bedeutet wegen Zusatz 9. dasselbe wie $XS_0^{-k} \in \mathfrak{S}$, d. h. wie $X \in \mathfrak{S}S_0^k (k = 0, \ldots, p_s-1)$. Solche Elemente X gibt es 2^cp_s.

Dies braucht aber noch nicht die gesuchte Anzahl n_s zu sein, denn es können für zwei Elemente X, Y von $\mathfrak{S}$, $\mathfrak{S}S_0, \ldots, \mathfrak{S}X_0^{p_s-1}$ die entsprechenden Konjugierten $X\mathfrak{S}_0X^{-1}$, $Y\mathfrak{S}_0Y^{-1}$ gleich sein. Das ist dann und nur dann der Fall, wenn $X^{-1}Y$ mit $\mathfrak{S}_0$ vertauschbar ist, d. h. in $\{A, \mathfrak{S}_0\}$ gehört, d. h. von der Form $A^jS_0^l$ ist $(j = 0, 1;\ l = 0, \ldots, p_s-1)$. Die Anzahl dieser Elemente ist $2p_s$. Da sich weiter die letzte Bedingung auch in der Form $Y = XA^jS_0^l$ schreiben lässt, so sieht man

[27] Selbstverständlich hat dieses A mit den Bezeichnungen im § 3 nichts zu tun.

wegen $AS_0A^{-1} = S_0^{-1}$ sofort, dass umgekehrt mit einem X zusammen auch jedes dieser Y in einem der $\mathfrak{S}$, $\mathfrak{S}S_0$, ..., $\mathfrak{S}S_0^{p_s-1}$ enthalten ist, und so führen je $2p_s$ der vorher gefundenen $2^c p_s$ Elemente X zu demselben $X\mathfrak{S}_0X^{-1}$. Hieraus folgt

$$n_s = 2^{c-1} \qquad (s = 1, 2)\,. \tag{56}$$

Dieses Resultat bezieht sich gleichsam für alle $A = A_1, \ldots, A_{2^{c-1}}$. Da andererseits klar ist, dass ein $\mathfrak{S}^s$ nicht mit zwei verschiedenen A_i, A_j vertauschbar sein kann, denn der Normalisator von $\mathfrak{S}^s$ ist von der (nicht durch 4 teilbaren) Ordnung $2p_s$, und so führt (56) sofort zum folgenden: Es gibt sowohl für $s = 1$ als auch für $s = 2$ insgesamt je

$$2^{c-1}(2^c-1) \tag{57}$$

p_s-Sylowgruppen $\mathfrak{S}^s$, die mit einem Element $(\neq 1)$ von $\mathfrak{S}$ vertauschbar sind.

Andererseits zeigen wir aber leicht, dass die hier gesagten $\mathfrak{S}^s$ mit den (verschiedenen) $\{A_iB_j\}$ übereinstimmen. Zunächst haben wir nämlich oben schon festgestellt, dass jedes $\{A_i, B_j\}$ eine maximale Untergruppe $\mathfrak{G}^\circ(p_s, 2)$ von $\mathfrak{E}$ ist, die dann $\{A_iB_j\}$ normal enthält, so dass also letztere Gruppe ein mit A_i vertauschbares $\mathfrak{S}^s$ ist. Folglich genügt es zu zeigen, dass jede, mit einem A_i vertauschbare zyklische Untergruppe $\{X\}(\neq 1)$ von $\mathfrak{E}$ von ungerader Ordnung notwendig ein $\{A_iB_j\}$ ist. Es muss nämlich $O(\{A_i, X\}) = 2O(X)$ gelten, wobei $\{A_i, X\}$ die Gruppe $\{X\}$ normal enthält, und so folgt aus Zusatz 4. und 5., dass $\{A_i, X\}$ (nichtabelsch d. h.) eine Diedergruppe ist mit $A_iXA_i^{-1} = X^{-1}$. Dann sind A_i, A_iX nichtvertauschbar und es gilt $(A_iX)^2 = 1$, beide besagen, dass A_iX ein B_j ist. Wegen $X = A_i \cdot A_iX = A_iB_j$ ist die Behauptung richtig.

Beachte man noch, dass alle $\mathfrak{S}^s$ paarweise fremd sind, und so enthalten die bei (57) genannten $\mathfrak{S}^s$ insgesamt $2^{c-1}(2^c-1)(p_1-1+p_2-1)$ Elemente $(\neq 1)$. Diese Elemente stimmen nach dem eben gewonnen Resultat mit den A_iB_j zusammen, deren Zahl gleich (51) ist, und so folgt aus beiden:

$$2^{c-1}(2^c-1)\,(p_1+p_2-2) = (\mu-1)\,(2^c-1)^2\,.$$

Nach (52) haben wir dann:

$$(\pi+1)\,(p_1+p_2-2) = 2\pi(\mu-1)$$

d. h.

$$\pi(2\mu-p_1-p_2) = p_1+p_2-2\,. \tag{58}$$

Hieraus folgern wir zunächst, dass π mit einem der p_1, p_2 übereinstimmt. Wenn nämlich $\pi \neq p_1, p_2$, so folgt aus (48), (53), (55) $\mu \geqq p_1p_2$. Dies mit (58) ergibt

$$\pi(2p_1p_2-p_1-p_2) \leqq p_1+p_2-2\,,$$

und so folgt wegen $\pi \geqq 3$

$$6p_1p_2 \leqq 4p_1+4p_2-2\,.$$

Noch mehr gilt dann $p_1p_2 < p_1+p_2$. Dies ist aber falsch, und so ist π das eine von p_1, p_2. Wir dürfen annehmen, dass

(59) $$\pi = p_1\,.$$

Betrachten wir nun rechts in (13) nur die Glieder mit $p = 2, p_1, p_2$, so folgt:

$$1 > \frac{1}{2^e}+\frac{p_1-1}{2p_1}+\frac{p_2-1}{2p_2}\,,$$

d. h.

$$\frac{1}{p_1}+\frac{1}{p_2} > \frac{1}{2^{e-1}}\,.$$

Wegen (52), (59) folgt hieraus

$$\frac{1}{p_1}+\frac{1}{p_2} > \frac{2}{p_1+1}\,.$$

Dies ergibt

$$p_2 < \frac{p_1(p_1+1)}{p_1-1} = p_1+2+\frac{2}{p_1-1} \leqq p_1+3$$

also

$$p_2 \leqq p_1+2\,.$$

Andererseits folgt aus (58), (59) $p_1 | p_2-2, p_1+2 \leqq p_2$, folglich gilt

(60) $$p_2 = p_1+2\,.$$

Wieder nach (58) folgt hieraus $\pi(\mu-p_1-1) = p_1$. Wegen (59) und (60) bedeutet dies $\mu = p_1+2 = p_2$. Nach (48), (59) haben wir dann:

(61) $$\nu = 2^e p_1p_2\,.$$

Nach (52), (59) sind $p_1 = 2^e-1, p_2 = 2^e+1$ Primzahlen, und dies geht nur mit $e = 2, p_1 = 3, p_2 = 5$. Folglich ist $\nu = 2^2 \cdot 3 \cdot 5$ und so kann $\mathfrak{E}$ in der Tat nur die Ikosaedergruppe $\mathfrak{G}_{60}$ sein. Andererseits ist klar, dass die zweitmaximalen Untergruppen von $\mathfrak{G}_{60}$ Abelsch sind, womit wir auch den noch übriggebliebenen Teil 3° des Satzes bewiesen haben.