Prof. Dr. Helmut Wielandt

Tagebücher

D10

X

Dezember 1957 – Januar 1959

F übernommen in Heft: “Forschungsaufgaben”

$\lhd\lhd$

1. Kann man zwei vertauschbare subnormale Ugr in Teile zerlegen, die wechselseitig invariant sind? F

2. Nach Itô gilt der Satz: "Ist $\mathfrak{P}_1 \leq \Phi\mathfrak{P}$, $\mathfrak{P} \in \mathrm{Sy}\ \mathfrak{G}$, $\mathfrak{P}_1 \in s_{\mathfrak{G}}\mathfrak{P}$, so ist $\overline{\mathfrak{P}_1}$ p-nilpotent; dh. wenn noch $\mathfrak{G}$ frei von p freien Normalteilern vorausgesetzt wird: $\mathfrak{P}_1 \in s\mathfrak{G}$ " – vorausgesetzt, dass es keine einfache Gruppe $\mathfrak{F}$ von zusammengesetzter Ordnung mit folgenden Eigenschaften gibt: Eine volle p-Sylowgruppe von $\mathfrak{F}$ ist homomorphes Bild jedes q-Sylownormalisators von $\mathfrak{F}$ ($q \underset{\neq}{=} p$).
   Frage: Kann es solche $\mathfrak{F}$ geben?

Hallgruppen

3. Jede a-Hallgruppe $\mathfrak{H}$ ist vertauschbar mit jeder Untergr $\mathfrak{B}$ von $\mathfrak{G}$, deren Index in a^∞ aufgeht. $\mathfrak{A} \cap \mathfrak{B}$ ist a Hallgr v. $\mathfrak{B}$
   Denn $|\mathfrak{A} : \mathfrak{B}|$ ist durch $|\mathfrak{A}| = a$ und durch $|\mathfrak{B}|$, also durch $|\mathfrak{G} : \mathfrak{A}|$ teilbar, also durch $|\mathfrak{G}|$.
   Allg: $(|\mathfrak{G} : \mathfrak{A}|, |\mathfrak{G} : \mathfrak{B}|) = 1 \rightarrow \ \mathfrak{G} = \mathfrak{A}\mathfrak{B}$

1. Welche (auflösbaren) Gruppen enthalten nur Elemente von Primzahlpotenz-Ordnung?
   Wohl gelöst von Suzuki $\sim$ '55

2. Vererbt sich die Eigenschaft, eine nilpotente a-Hallgruppe zu besitzen, auf Untergruppen?
   F A: Nein (Itô)

3. Ist jede Gruppe zusammengesetzt, die auf zwei geeignete Ähnlichkeitsklassen simultan - transitiv ist?
   Sind die beiden Klassen elementweise vertauschbar?
   Führt auf Faktorisierung $\mathfrak{G} = NA$. $\mathcal{N}$B; Schur - Methode?

4. Man braucht nicht das Produkt aller Ähnlichkeitsklassen zu nehmen, um genau eine Nebenklasse der Kommutator - Gr zu bekommen; von jeder Familie von Klassen braucht man nur einen Vertreter.

5. Vermutung: Das Produkt von zwei komplementären zentrierten Hallgruppen ist nie einfach. Ist bei $\mathfrak{G} = \mathfrak{P} \cdot \mathfrak{H}$ richtig nach Bunsides p^α - Satz.

Automorphismen von p-Gruppen (p ungerade):

1. Ein p-freier Automorphismus α einer p Gruppe $\mathfrak{P}$ ist genau dann $= 1$, wenn er alle Elemente der Ord. p fest läßt ($p > 2$). Dazu IX 66 Veröff von Hu 1961 Acta Szeged (1.5)
   Bew: Indukt. $\mathfrak{P}/\Phi(\mathfrak{P})$ ist voll reduzibel unter a, also
   " " irreduzibel unter a (Indukt)
   Ist $\mathfrak{y} = \Phi\mathfrak{P}$, so ist $\mathfrak{y} \leq$ Ztr $\mathfrak{P}$. Denn es folgt aus $Y_1^P = Y_2 (Y_i \in \mathfrak{y})$ stets $Y_1^{P^\alpha} = Y_2$, also $\mathfrak{y}$ wird zentralisiert von $P^{\alpha-1}$. Die $P^{\alpha-1}$ liegen nicht alle in $\phi(\mathfrak{P})$, da dies bei a fest bleibt elementw., also erzeugen die $P^{\alpha-1}$ ganz $\mathfrak{P}$: $\mathfrak{y} \leq$ Ztr. $\mathfrak{P}$. Also ist Klasse $\mathfrak{P} \leqq 2$, $\Phi\mathfrak{P} \leq$ Ztr $\mathfrak{P}$. Sei nun $P^{p^2} = 1, \rightarrow P^p \in$ Ztr $\mathfrak{P}$. Dann $(P^p)^\alpha = P^p$, also $(P^\alpha)^p = P^p$, $(P^{\alpha-1})^p = 1$ wegen $[P, P^a]^p = 1$. Also $P^\alpha = CP$ mit $C^p = 1, \rightarrow C^a = C \rightarrow P^{\alpha^p} = P,\ \alpha = 1$.
   Frage: Genügt schon Betrachtung des Sockels von $\mathfrak{P}$? Nein

   $|\mathfrak{G}| = p^3$
2. Gilt ein allgemeinerer Satz über die p-fremden Autom. von $\mathfrak{G}$, die jeden durch p teilbaren Huf von g fest lassen?

3/4

2-tra Klassengruppen. Held? 30.12.7

Wann kann die Permutationsgruppe, die von den inneren Autom. von $\mathfrak{G}$ auf einer Klasse $\mathfrak{K}$ konjugierter Elemente von $\mathfrak{G}$ bewirkt wird, 2-fach transitiv sein? (Ohne dass je zwei Elemente $\mathfrak{K}$ vertauschbar sind). Man wird erst den Fall $\mathfrak{K} \ni P$, $|P| = p$ betrachten. Durch Untersuchen des (Normalisators) Zentralisators von $\{P^G, P^H\}$ kann man die Frage wohlreduzieren auf den Fall, daß je zwei Konjugierte von P dieselbe [eine] auf $\mathfrak{K}$ transitive Gruppe erzeugen. (Keine 2 Konj. sind vertauschbar). Dies führt auf die Frage: Welche scharf 2-tra Permgr. $\mathfrak{G}$ haben die Eigenschaft, daß $\mathfrak{G}_1$ ein Zentrumselementen P enthält, das mit jedem nicht auf P vertauschbaren Element von $\mathfrak{G}$ zusammen eine transitive Gruppe erzeugt?
$\mathfrak{G}$ hat Frobeniuskern $\mathfrak{F}$, $|\mathfrak{F}| = q^\mathfrak{f}$, elementar abelsch, da $\mathfrak{f}$ minim. NT von $\mathfrak{G}$; die Darstellung von $\mathfrak{G}$, durch Matritzen mod q (grad $= \mathfrak{f}$) stellt P durch eine Matrix $M(P)$ dar, die nat. irreduzibel und im Zentrum von $\mathfrak{G}_1$ ist. Dann ist aber $\mathfrak{G}_1 \leq$ Ring erzeugt von $M(P)$; wegen Ord $=$; es ist also $\mathfrak{G} = \left(\begin{smallmatrix} x \\ ax+b \end{smallmatrix}\right)$, $x \in$ GF(q^f).

4/5

1. Eine Klassen-Permutationsgruppe (d.h. die P Gr, die von den inneren Autom v $\mathfrak{G}$ auf einer Ähnlichkeitsklasse $\mathfrak{K}$ bewirkt wird) kann nie 3-tra sein, außer wenn $\{\mathfrak{K}\mathfrak{K}^{-1}\}$ abelsch
   Bew: die 2-tra Gr $\mathfrak{G}_1$ hat keinen Zentralisator.

2. Wenn die Frage von S. 4 nicht zu beantworten ist: Dann kann man vielleicht unter speziellen Vorauss. zum Ziel kommen, z.B. beweisen: $\mathfrak{G} = \mathfrak{A}\mathfrak{B}$ nicht einfach, wenn $\mathfrak{A}$ zyklisch ist und $\mathfrak{B}$ ein Zentrum hat.

3. Ist $\mathfrak{G}$ auf einer Klasse $\mathfrak{K}$ konj. Elem. von $\mathfrak{G}$ 2-pri oder $2\frac{1}{2}$-tra, so erzeugt $\mathfrak{K}$ einen abelschen Normalteiler.
Bew: $\mathfrak{G}_{12} = \mathfrak{G}_1 \cap \mathcal{N}\mathfrak{G}_{12} \to \{P_1, P_2\} \cap \mathfrak{K} = [\![P_1, P_2]\!]$. $\mathfrak{G}_{12} \neq \mathfrak{G}_{12x} \quad (x > 2)$
Scheint so nicht zu stimmen:
Achtung: Hierzu Miller-Blichfeldt-Dicks. S. 163, 165!
Fortsetzg S. 12

3′ Ist $\mathfrak{G}$ 2-pri auf $\mathfrak{N} = A^{\mathfrak{G}}$ und $\{A^{\mathfrak{G}}\}$ nicht abelsch, so ist die Darst. von $\mathfrak{G}$ auf $\mathfrak{K}$ eine 2-tra Frobeniusgr vom Grade $p+1$, p Primzahl (also $p = 2$ oder Fermat-Primzahl)

5/6

Reflexive Untergruppen.

1. Def: $\mathfrak{A} \leq \mathfrak{G}$ heisst [stark] reflexiv (oder selbst-konjugierend) in $\mathfrak{G}$, wenn $G \in \mathfrak{G} \to \exists_H \mathfrak{A}^G = \mathfrak{A}^H$, $H \in \{\mathfrak{A}, \mathfrak{A}^G\}$. [Wenn $\alpha \in$ Automgr $\mathfrak{G} \to \exists_H \mathfrak{A}^\alpha = \mathfrak{A}^H \ldots$]

2. Jede maximale Untergruppe von $\mathfrak{G}$ ist stark reflexiv.

3. Jede Hallgruppe mit Sylowturm ist stark reflexiv in $\mathfrak{G}$

4. Jede schwach abgeschlossene p-Gruppe ist reflexiv in $\mathfrak{G}$.

5. Ist $\mathfrak{A}$ refl., so sind je zwei in $\mathfrak{G}$ konj. Elemente des Zentralisators $\mathcal{C}\mathfrak{A}$ schon in $\mathcal{N}\mathfrak{A}$ konjugiert.

6. Ist $\mathfrak{A}$ refl und eine p-Sy von $\mathfrak{G}$ in $\mathcal{C}\mathfrak{A}$, so ist die max p-Faktorgr. von $\mathfrak{G}$ isomorph zu der von $\mathcal{N}\mathfrak{A}$

6/7

7. Der Begriff der Reflexivität ist vielleicht noch unnötig scharf für Verlagerungszwecke. Beispielsweise braucht man dort nur solche Konj. $\mathfrak{A}^G$ zu betrachten, die ein $P^G \in \mathfrak{P}$ zentralisieren (wo $[\mathfrak{P}, \mathfrak{A}] = 1$ vorausges. ist).

8. Gibt es zu der p-Gruppe P_1 nur eine maximale von Konjugierten von $\mathfrak{P}_1$ erzeugte p-Obergruppe $\overline{\mathfrak{P}_1}$ von $\mathfrak{P}$ (z.B. wenn $\mathfrak{P}_1$ schwach abg.), so sind je zwei Elem. von $\mathcal{C}\mathfrak{P}_1$, die in $\mathfrak{G}$ konj. sind, schon in $\mathcal{N}\overline{\mathfrak{P}_1}$ konj. Das gibt den Satz von Grün-Higman über p-reg Gruppen. und einen entsprechenden für q-Normalisator $\to$ p-Faktorgr.

9. Arbeit schreiben „Normalisatoren und p-Faktorgruppen“. siehe 1.2

10. Ist eine Sylowgr $\mathfrak{P}$ von $\mathfrak{G}$ direkter Faktor einer max Ugr $\mathfrak{M} < \mathfrak{G}$, so ist sie normal oder Faktorgruppe in $\mathfrak{G}$.

7/8

Noch Reflexive Untergr.

1. Sind $\mathfrak{A}, \mathfrak{B}$ stark refl. in $\mathfrak{G}$, so auch $\{\mathfrak{A}, \mathfrak{B}\}$ stark refl in $\mathfrak{G}$

2. Jede normale Hallgr mit Sylowturm einer max Untergr. von $\mathfrak{G}$ ist stark refl in $\mathfrak{G}$

3. $\mathfrak{P}$ p-Sy $\mathfrak{G}$, $[\mathfrak{P}, \mathfrak{A}] = 1$; $P_0 \in \mathfrak{P}$, $\mathfrak{A}$ refl in $\mathcal{Z}sP_0^\lambda$ $(P_0^\lambda \neq E) \to P_0^G \in \mathfrak{P} \to P_0^G = P_0^N$, $N \in \mathcal{N}\mathfrak{A} = \mathfrak{N}$. Daher $\underset{\mathfrak{G}\to\mathfrak{N}}{\text{Verl}}\ P_0 = P_0^{[\mathfrak{G}:\mathfrak{N}]}$

3a. wichtig ist: $\mathfrak{A} \leq \mathcal{C}\mathfrak{P}$; $\mathfrak{A}$ refl in jedem $\mathcal{C}P, 1 \neq P \in \mathfrak{P}$.

4. Nenne $\mathfrak{A}$ und $\mathfrak{A}^G$ benachbart, wenn aus $H \in \mathfrak{H} = \{\mathfrak{A}, \mathfrak{A}^G\}$ stets folgt: $\mathfrak{H} = \{\mathfrak{A}, \mathfrak{A}^{GH}\}$. Und nenne $\mathfrak{A}$ mit $\mathfrak{A}^G$ verkettet, wenn $\mathfrak{A}$ benachb. $\mathfrak{A}^{G_1}$ ben. $\cdots$ ben. $\mathfrak{A}^G$.
Def.: $\hat{\mathfrak{A}}$ = Erzeugnis aller mit $\mathfrak{A}$ verketteten $\mathfrak{A}^G$ $(G \in \mathfrak{G})$. $\mathfrak{A}$ verkettet $\mathfrak{A}^G$ $\to (\hat{\mathfrak{A}})^G = (\widehat{\mathfrak{A}^G})$.

5. $\mathfrak{P}$ = schwach abg p-Gr $\to \mathfrak{P} = \hat{\mathfrak{P}}$. $\mathfrak{G}$ p-regulär $\leftrightarrow \widehat{\mathfrak{Z}\mathfrak{P}} = p$-Gruppe

8/9

Sylow-Normalisator-Systeme (SNS)

1. Def: $p_1,\ p_2 \ldots$ verschiedene Primteiler von $\mathfrak{G} \to \Sigma = [\mathfrak{P}_1, \mathfrak{P}_2, \ldots]$ heisst ein SNS (vom Typ $p_1; p_2, \ldots$), wenn

$$\begin{array}{ll} \mathfrak{P}_1 & p_1\text{- Sy } \mathfrak{G} \\ \mathfrak{P}_2 & p_2\text{- Sy } N\mathfrak{P}_1 \\ \mathfrak{P}_3 & p_3\text{- Sy } N\mathfrak{P}_1 \cap N\mathfrak{P}_2 \ldots \end{array}$$

2. Je zwei SNS (vom gleichen Typ) sind konjugiert in $\mathfrak{G}$. Daher deckt $N\Sigma$ stets $\mathfrak{H}/\mathfrak{G}$, wenn $\mathfrak{G} \lhd \mathfrak{H}$. Dabei $N\Sigma = \bigcap_{\mathfrak{P}_\rho \in \Sigma} N\mathfrak{P}_\rho$.
Die Glieder eines SNS haben also grosse Normalisatoren bei normaler Einbettung von $\mathfrak{G}$.

2a. $\prod_{\mathfrak{P}_\rho \in \Sigma} \mathfrak{P}_\rho$ ist stark reflexiv.

3 Nicht zu verwechseln sind die SylowNormSyst mit den Untergr. $\mathfrak{H} \leq \mathfrak{G}$, die in $\mathfrak{G}$ zu jedem $\mathfrak{H}^\alpha$ $(\alpha \in A\mathfrak{G})$ konj. sind $(\mathfrak{H} \in \psi)$. Ist $\mathfrak{H} \in \psi$, so ist jede Sylowgr von $\mathfrak{G}$ in Ψ, ebenso jede mit $\mathfrak{H}$ invariant verknüpfte Gruppe wie $N\mathfrak{H}$, $Z\mathfrak{H}$; die subnormale Hülle von $\mathfrak{H}$ und der subn Kern; ferner $\mathfrak{H}^\Lambda$.

9/10

Sylow-Norm Systeme

1. Ψ enth. diejenigen Ugr von $\mathfrak{G}$, deren Fixgruppe die äussere Automgr von $\mathfrak{G}$ deckt.

2. Die Ψ- Gruppen von $\mathfrak{G}$, die bei <u>einer festen</u> Deckgr. der äuss. AutomGr $\ddot{A}$ von $\mathfrak{G}$ ungeändert bleiben, bilden einen Verband. Die größten Verbände bekommt man aus den kleinsten Deckgruppen: da die kleinsten auf $\ddot{A}$ abgeb. Untergr. von $A(\mathfrak{G})$. Ist $(|\ddot{A}\mathfrak{G}|, |g|) = 1$, so sind das die Vertretergr. von $\ddot{A}$. Den kleinsten Verband bilden die char. Untergr. von $\mathfrak{G}$, der ist in jedem anderen enthalten.

3. Man kann bei der Def von Ψ auch eine fest gewählte Untergr. $\ddot{\mathfrak{A}}$ von $\ddot{A}$ zu Grunde legen: $\Psi_{\ddot{\mathfrak{A}}}(\mathfrak{G}) \ni \mathfrak{H} \to \mathfrak{H}^{\ddot{a}} = \mathfrak{H}^G$ für jedes $\ddot{a} \in \ddot{\mathfrak{A}}$. Hier insbes. $|\ddot{\mathfrak{A}}|$ = Primzahl $q \nmid |\mathfrak{G}|$ untersuchen. Die Vollständigkeitseigenschaften von 9.3 bleiben auch für $\Psi_{\ddot{\mathfrak{A}}}$ gültig.

10/11

Aufgabe: $\mathfrak{G} = \mathfrak{P} \cdot \mathfrak{Q}$ mit simultaner monomialer Darstellung nach $\mathfrak{P}$ <u>und</u> $\mathfrak{Q}$ untersuchen.

11/12

2-tra Klassengruppen. F

1. Die Frage läuft daraus hinaus: Fortsetzg von S. 5 3.1.58
Welche 2-tra Permut.-Gruppen $\mathfrak{G}$ haben ein zentriertes $\mathfrak{G}_1$? (D.h. $\mathfrak{G}_1$ mit Zentrum $\mathfrak{Z} \neq 1$.) schreibe kurz $\mathfrak{G} \in 12{\cdot}1$,
NB: Man kann oBdA annehmen, daß $\mathfrak{G} = \mathfrak{G}^{(3)}$ der dritten Abschließung, ist. Denn es ist noch $Z_1 \in$ Ztr $\mathfrak{G}^{(3)}{}_1$.

2. Beispiele solcher $\mathfrak{G}$ sind diejenigen inhomog lin. Gruppen über
$K = \mathrm{GF}(p^f)$, die den Grad n haben und deren homogener Teil transitiv auf $\underbrace{K \oplus \cdots \oplus K}_{n}$ ist und zentriert ist (der Teil könnte also z.B. $\mathrm{GL}(n, p^f)$ oder $\mathrm{SL}(n, p^f)$ sein). Diese Gruppen enthalten alle einen elem. abelschen Normalteiler, gebildet von den Z_1^{G-1}. Diese Beispiele sind nicht alle scharf 2-tra.

2,5. $\langle Z\rangle\langle Z^{-1}\rangle = n\langle 1\rangle + c\langle C\rangle \to c|n$

3. Vermutung: Die Gruppen $12 \cdot 1$ haben el. ab. NT. $\{\langle c\rangle\}$.
Weiter sei $\mathfrak{G} \in 12 \cdot 1$, d.h. $\mathfrak{G}$ 2-tra, $\mathfrak{G}_1$ zentriert. Gr $\mathfrak{G} = n \quad 1 \neq Z_1 \in$ Ztr $\mathfrak{G}_1$, $Z_1^q = 1$, $Z_\nu = Z_1^G \in \mathfrak{G}_\nu$.

4. $\mathfrak{G}_{12}$ lasse genau m Ziffern fest, $m < n$; etwa $\{1, 2, \ldots, m\} = M$. Sei $\mathfrak{Z} = \{Z_1, \ldots, Z_m\}$. $[\mathfrak{Z}, \mathfrak{G}_{12}] = 1$. $\mathfrak{Z}_{12} \leq$ Ztr $\mathfrak{Z}$. Der Konst. von $\mathfrak{Z}$ auf M ist eine scharf 2-tra Gruppe, also $m = p^\mu$. Sei $\mathfrak{P}$ eine p-Sy von $\mathfrak{Z}$. Dann
$\begin{cases} \mathfrak{P} \lhd \mathfrak{P} \cdot \mathfrak{Z}_{12} \\ [\mathfrak{P}, \mathfrak{G}_{12}] = 1 \end{cases}$

Es ist $m > 2$, da $\mathfrak{G}_{12} \circ Z_1 = 1$.
Sogar $[\mathfrak{G}_{12}, \mathfrak{Z}] \equiv 1$

12/13

$\mathfrak{P}$ normale Sy $\mathfrak{P}\mathfrak{Z}_{12}$, also $\mathfrak{P}$ einzige p-Sy $\mathfrak{P}\mathfrak{Z}_{12}$. Ferner (Frob.)

1. ist $\mathfrak{P}\mathfrak{Z}_{12} \lhd \mathfrak{Z}$, also $\mathfrak{P}$ einzige p-Sy von $\mathfrak{Z}$. $\mathfrak{P}^{Z_1} = \mathfrak{P}$.
   $\mathfrak{Z}/\mathfrak{P}$ ist zyklisch, da erzeugt von Z_1 und $\mathfrak{Z}_{12}$. Es ist $\mathfrak{P}$ trans auf $1, \ldots, m$, also sind alle Z_μ $(\mu = 1, \ldots m)$ schon unter $\mathfrak{P}$ konjugiert, daher $\mathfrak{Z} = \{Z_1, \mathfrak{P}\} = \{Z_1\} \cdot \mathfrak{P}$. Also ist $\mathfrak{Z}' \leq \mathfrak{P}$. $\Phi\mathfrak{P} \leq \mathrm{Ztr}\mathfrak{P}$.
   Es ist $\mathfrak{P} \lhd \mathcal{N}\mathfrak{G}_{12}$, da $\mathfrak{P} \underset{\mathrm{Sy}}{\lhd} \mathfrak{Z} \lhd \mathcal{N}\mathfrak{G}_{12}$

2. Ist $p > 2$, so ist $\exp \mathfrak{Z}' = p$. dh $\begin{cases} Z_i Z_j^{-1} = \mathfrak{c} \to \mathfrak{c}^p = 1 \\ C \in \mathfrak{Z}' \to C^p = 1 \end{cases}$. Denn $\mathfrak{C}' = \{Z_2 Z_1^{-1}, \ldots, Z_m Z_1^{-1}\}$. Und ist $Z_2^{Z_1} = Z_3$,so ist $(Z_2 Z_1^{-1})^{Z_1} = Z_3 Z_1^{-1}$, also [wegen $C^n \in$ Ztr $\mathfrak{Z}$ wenn $C \in \mathfrak{Z}'$] $(Z_2 Z_1^{-1})^p = \{(Z_2 Z_1^{-1})^p\}^{Z_1} = (Z_3 Z_1)^p$, folglich, da $\mathfrak{P}$ Klasse 2 hat, $(Z_3 Z_2^{-1})^p = (Z_3 Z_1^{-1})^p : (Z_2 Z_1^{-1})^p = 1$ $\{c^p \in$ Ztr $\mathfrak{Z}$
   Aber alle $Z_i Z_k^{-1}$ sind konj in $\mathfrak{G}$, also ist $(Z_i Z_k^{-1})^p = 1$; $\exp \mathfrak{Z}' = p$
   Frage: Ist $\mathfrak{Z}'$ elementar abelsch?

3. Es ist $m = p^\mu \mid n$; $\mathfrak{P}$ versetzt alle n Ziffern. $\begin{cases} \text{Wenn } p^\mu \top n \text{ ist , ist} \\ \mathfrak{P} \text{ Sy } \mathfrak{G} \end{cases}$

   Bew:

   a) Ang.: $\mathfrak{P}$ läßt n fest; dann $Z_n \in \mathcal{Z}s\mathfrak{P}$, $Z_n^{Z_1} \in \mathcal{Z}s\mathfrak{P}$; aber da $\{Z_n, Z_n^{Z_1}\}$ $= \{Z_n, Z_1\} \ni Z_1$ (wegen $\mathrm{Ord}\{Z_i Z_j\} = \mathrm{Ord}\{Z_k Z_e\}$, wäre dann $Z_1 \in \mathcal{Z}s\mathfrak{P}$; Z_1 liesse $2, \ldots, m$ fest. Also ist $p \mid n$.
   [Anderer Beweis hierfür: $\langle Z \rangle \langle Z^{-1} \rangle = n\langle 1 \rangle + \mathfrak{c}\langle C \rangle$
   $c|n \;\; c|\mathfrak{G} : \mathfrak{H}| = n(n-1) = |\mathfrak{G} : \mathfrak{G}_{12}|$, dann $\mathfrak{H} = \mathcal{N}C$
   $C = \mathfrak{H} : \mathfrak{G}_{12} | n : p | \{C, \mathfrak{G}_{12}\} : \mathfrak{G}_{12} | n$]

13/14

Noch 2-tra Klassengr.: Sei $\mathfrak{G} \in 12 \cdot 1$

   b) [Ist $p^\rho \top g_{12}$, so ist $p^{\mu+\rho} \top \mathfrak{P}\mathfrak{G}_{12}$, $p^{\mu+\rho} | g$ Andererseits, $g = n(n-1)g_{12}$, also $p^\mu | n(n-1)$, $p^\mu | n$.] ausgestrichen
   $|\mathcal{N}\mathfrak{G}_{12} : \mathfrak{G}_{12}|$ teilt $|\mathfrak{G} : \mathfrak{G}_{12}| = n(n-1)$, also $m(m-1) | n(n-1)$ & da $m = p^\alpha$, $p | n$, $p \nmid n-1$ folgt $p^a | m$.

1') Ferner ist $m - 1 \big| n - 1$, denn $M - 1$ ist Block $\mathfrak{G}_1$.
   Gibt $n = n' p^a (p^a - 1) + p^a$

1. Lasse $\{Z_1, Z_2\}$ genau $1, \ldots, k$ fest. Dann ist $N\{Z_1, Z_2\}$ 2-tra auf $\{1...k\} = K$, also $\{Z, Z_\alpha\} = \{Z_\rho Z_\sigma\} (\rho, \sigma \leq k)$ und $\{Z_1, Z_2\}$ tra auf K. Der Konst von $N\{Z_1 Z_2\}$ auf K ist scharf 2-tra, und ist S. 4

unten $\binom{x}{ax+b}$ mod p'; Daher Ord $Z_2 Z_1^{-1}$ durch p' teilbar, also $p' = p$; d,h, es ist $k = p^\kappa | m = p^\mu$, und da $N\mathfrak{Z}$ auch scharf 2-tra auf M, ist $k-1 | m-1$. Hieraus folgt (mod $k-1$ rechnen)

$$\kappa | \mu, \text{ d.h. } m = k^\epsilon$$

2. Ist $\mathfrak{P}_{12}$ eine Sy $\mathfrak{G}_{12}$, $\mathfrak{P}_{12} \leq \mathfrak{P} =$ Sy $\mathfrak{G}$, so lässt $\mathfrak{P}_{12}$ p^λ Ziffern Λ fest, und es ist $p^\lambda | n$. $\mathfrak{P}_{12}$ ist tra auf Λ. Beweis wie 13.3
3. Aus $\langle Z \rangle \langle Z^{-1} \rangle = n\langle 1 \rangle + c\langle C \rangle$, $\operatorname{Ord} C = p$, $\operatorname{Ord} Z = q \neq p$ (Primz.) folgt: $|\chi(Z)|^2$ und $\chi(C)$ sind stets rational wenn χ irred (Aber $\chi(Z)$ ist nicht stets rat wenn $\operatorname{Ord} Z > 2$)

14/15

2-tra Klassengr F

1. Sei $\mathfrak{P}$ eine p-Sy von $\mathcal{N}\mathfrak{G}_{12}$. Jeder Autom von $\mathfrak{G}12$ unter $\mathfrak{P}$ kann auch durch ein Element P_1 von $\mathfrak{G}_1$ bewirkt werden [denn $\{Z_1\}$ ist eine stark abg. q-Gruppe und daher sind je zwei in $\mathfrak{G}$ konjugierte Komplexe, die 1 fest lassen, in g_1 konjugiert]. Aber $\mathfrak{G}_1 \cap \mathcal{N}\mathfrak{G}_{12}$ hat mod $\mathfrak{G}_{12}$ die $\operatorname{Ord} m - 1$, die zu p fremd ist, also kann man sogar $P_1 \in \mathfrak{G}_{12}$ wählen. Gibt nichts wesentlich Neues. Dahinter steckt nur:

2. Ist $\mathfrak{U} \leq \mathfrak{G}$, so ist $\mathcal{Z}s\mathfrak{U}$ transitiv auf den von $\mathfrak{U}$ festgelassenen Ziffern $\alpha\beta\ldots\rho$. Genauer: Schon die von $Z_\alpha, Z_\beta, \ldots, Z_\rho$ erzeugte Gruppe ist dort transitiv, denn i geht in k über unter $\{Z_i, Z_k\}$.

3. Nimmt man die Beh, daß jede Gr $\mathfrak{G} \in 12.1$ Primzahlpotenzgrad $p^{\cdot\cdot}$ hat mit $p = \operatorname{Ord} Z_2 Z_1^{-1}$, für kleinere Gr schon als richtig an, so folgt $p \neq r \big| n \rightarrow$ die r-Sy $\mathfrak{R}$ von $\mathfrak{G}$ sind halbregulär, dh. $r \nmid \frac{g}{n} = g_1$
Bew: sonst $N\mathfrak{R}_1$ 2-tra auf den bei $\mathfrak{R}_1$ festen Ziffern, also nach Indukt deren Anzahl $= p^{\cdot\cdot}$, aber $r \big|$ Anzahl.

15/16

Noch 2-tra Klassen Gr.: Sei $\mathfrak{G} \in 12 \cdot 1$

1. Zu jedem $\alpha \neq \beta$ gibt es genau ein $Z_\nu = (\alpha\beta\ldots)\ldots$. Denn es gibt $n(n-1)$ Paare $(\alpha\beta), n$ Z_ν, und jedes liefert nur $n-1$ Paare.

2. Lässt $\mathfrak{U} \leq \mathfrak{G}$ die Ziffern $\alpha, \beta, \ldots$ fest und ist $Z_\nu = (\alpha\beta_\nu)$ so zentralisiert Z_ν die Gr $\mathfrak{U}$. Bew: (1).

3. Lässt $\mathfrak{U} \leq \mathfrak{G}$ genau Λ Ziffernweise fest und ist $|\Lambda| > 1$, so ist $p \big| |\Lambda|$.
Bew: Sei $1, 2 \in \Lambda$. Dann wird $\mathfrak{U} \leq \mathfrak{G}_2$ von $\mathfrak{Z}$ zentralisiert, und jede Transitivitätslänge von $\mathfrak{Z}$ in $\Omega - M$ ist nach 13.3 durch p teilbar; dabei ist $\mathfrak{P}$ die p-Sy von $\mathfrak{Z}$.

3a. Es ist sogar jede Translge von $\mathfrak{Z}$ in $\Omega - M \geq \sqrt{p^M}$, also $|\Lambda| \equiv 0$ $(p^{[\frac{???+1}{2}]})$.

3b. Ferner ist $|\Lambda| \equiv 1 \;\; (p^m - 1)$.

16/17
3.1.58

4. Ist $n =$ Primzahl, so ist $\mathfrak{G} : \binom{x}{ax+b}$
Bew: Es ist dann $n = p$ nach 13.3, $\mathfrak{G}_{12} = 1$.

5. Um zu zeigen daß die „Quotienten“ $Z_\alpha Z_\beta^{-1}$ eine Gruppe der Ord n bilden, genügt:

   a) Es gibt nur n verschiedene unter ihnen; oder

   b) Zu $Z_1 Z_2^{-1}$ gibt es genau $n-1$ verschiedene Konjugierte; oder

   c) Zentralisator $Z_1 Z_2^{-1}$ ist transitiv.

6. Vielleicht kann man alle 2-tra Klassengr. vom Grad p^2 bestimmen; daher vielleicht alle Klagru des Grades p^2
Anfang 59 überlegt: Geht auch mit geometr. Überlegungen, enthalten alle Normalt. d Ord p^2 vom Typ (p,p): siehe XI, 42

7. Ist $2|n$, so ist $p = 2$. Beweis: Wähle $\mathfrak{G}_2' \leq \mathfrak{G}$ so daß $\mathfrak{G}_2'$ als kleinstes Transgebiet eins der Länge 2 hat, etwa $(\alpha\beta)$, $\{Z_\alpha, Z_\beta\}$ ist invariant bei $\mathfrak{G}_2'$ und hat genau ein Transgebiet der Länge p^μ. Wäre p^μ ungerade so lasse $\mathfrak{G}_2'$ dort eine Ziffer fest, kleinstes Tra-Gebiet hätte Länge 1.
Also $p = 2 \leftrightarrow 2|n$

[auf S. 16 geschrieben:]

7′ Ist $p > 2$, so ist $(\mathcal{N}\mathfrak{G}_{12} \cap \mathfrak{G}_1)/\mathfrak{G}_{12}$ zyklisch. Dann Ordnung ungerade, und dargestellt ohne Fixpunkt [auf Gr der Ord $m = 2^\mu$].

17/18

Zum p^a-Satz von Burnside:

1. Ist $|A^{\mathfrak{G}}| = p^\alpha \geq 1$, $A \neq 1$, so ist $\{A^{\mathfrak{G}}\}' \neq \{A^{\mathfrak{G}}\}$.
Bew: Es genügt zu zeigen, daß die subnormale Hülle $\overline{\{A\}}$ nicht perfekt ist. Da sie zugleich die normale Hülle von $\{A\}$ in $\overline{\{A\}}$ ist, kann man oBdA annehmen: $\overline{\{A\}} = \mathfrak{G}$, daher $\{A^{\mathfrak{G}}\} = \mathfrak{G}$. Dann fällt aber beim Bew von Burnside der Fall $f > 1$ aus: es gibt einen Char $\neq 1$ vom Grade 1
Anders ausgedrückt: Eine Ähnlichkeitsklasse $\neq 1$ der Länge p^α erzeugt einen imperfekten Normalteiler

2. Ist $\mathfrak{G}$ einfach und $|A^{\mathfrak{G}}| = p^\alpha q^\beta$, so ist für $\chi \neq \chi_1$

$$f_p \cdot f_q \cdot \chi(A) = 0$$

mit $f_p = 0$ wenn $p|f$ (z.B. $f_p =$ kleinster nicht neg Rest f mod p)

3. Burnside sagt: Zentriert · p-Gruppe $\neq$ einfach
Frage: Ist zentriert · nilpotent $\neq$ einfach?
Ist zentriert · zentriert $\neq$ einfach?
Forts. 19.4

18/19

Über 2-tra Gruppen $\mathfrak{G}$

1. Ist $\mathfrak{G}_1'$ intransitiv (in einer 2-tra Gr. $\mathfrak{G}$), so ist $\mathfrak{G}$ nicht einfach, sondern enth. einen nur 1-tra NT.
Bew: $\{\mathfrak{G}_{12}, \ldots, \mathfrak{G}_{1n}\}_{[2,..,n]}$ intra, also $\neq \mathfrak{G}_1$
Ausdehnung auf intra $\mathfrak{G}_1$?

2. Hat $\mathfrak{G}_1$ Zentrum, so hat $\mathfrak{G}$ vielleicht el ab. NT: siehe S.12ff.

3. Ist $\mathfrak{G}_1$ nilpotent, so ist $\mathfrak{G}$ nicht einfach. Denn $\mathfrak{G}_{12}^{\mathfrak{G}_1} \neq \mathfrak{G}_1$

3a Frage (Hupp.): Welche 3-tra Gruppen besitzen einen reg. Normalt.?

4. Der p^α-Satz von Burnside wäre in dem folgenden enthalten: Hat in einer primitiven Permgr $\mathfrak{G}$ die Gruppe $\mathfrak{G}_1$ einen Konstituenten vom Grad p^α, so ist $\mathfrak{G}_1$ nicht einfach. [$\mathfrak{G}$-Holomorph einer einfachen Gr wählen].

19/20

Faktorisierung

1. Ist $\mathfrak{G} = \mathfrak{AB}$, $\mathfrak{A}' \cap \mathfrak{B}' = 1$, so ist die zerfallende Hülle $\mathfrak{H}$ von $Z\mathfrak{G}$ abelsch.
Bew: $\mathfrak{H} \leq \mathfrak{ZB} \to \mathfrak{H}' \leq (\mathfrak{ZB})' = \mathfrak{B}'$, ebenso $\leq \mathfrak{A}'$, $= 1$.

2. Frage: Wie sieht die zerf. Hülle des Hyperzentrums von $\mathfrak{G}$ aus?

Methode von Schur

3. Verallgemeinerung der „symbolischen Potenzierung“ ist möglich, wenn ein Komplex $\mathfrak{K}$ normal unter der reg Untergr $\mathfrak{H}$ ist. Zu Vereinfachung nimm an, $\mathfrak{G}$ enthalte die reg Untergr $\mathfrak{H}$ und $Zs\mathfrak{H}$ sei transitiv, d.h. $\mathfrak{G} \geq \mathfrak{H}^*$. Ist dann α ein Autom. von $\mathfrak{H}$, dessen Wirkung auf die Charaktertafel von $\mathfrak{H}$ mit der einer Körperautomorphismus übereinstimmt, so ist neben $\mathfrak{K}$ auch stets $\mathfrak{K}^{(\alpha)}$ ein Hauptkomplex von $\mathfrak{G}$.
Bew: $\mathfrak{G}$ und $\mathfrak{H}$ ausreduzieren. $\mathfrak{K}^{(\alpha)}$ kann dann erhalten werden durch Anwend. eines alg. (Körper-)Automs und eine Ähnlichkeitstransf. mit $T \in$ Gruppenring von $\mathfrak{H}^*$, die aber die Matrix von π wegen Invarianz von π nicht ändern.

20/21

Meth v Schur.

1. Frage: Ist das direkte Produkt einer zykl. Gr. d. Ord p^α mit einer p-freien Gruppe stets eine B-Gruppe? F Ansatz: 2,3

2. Man sollte bei symbolischer Potenzierung stets die zentralen oder normalen Teile der Hauptkomplexe betrachten: $\zeta\mathfrak{K} = \mathfrak{K} \cap Z\mathfrak{H}$; $\nu\mathfrak{K} = \bigcap\limits_{H \in \mathfrak{H}} \mathfrak{K}^H$.

3. Es ist $\zeta(\mathfrak{K}^m) \equiv \zeta\mathfrak{K}^{(m)} \pmod{m}$ $m = 1, 2, ...$

4. Die Autom. von $\mathfrak{G}$, welche jedes Element in seiner Ähnl-Klasse belassen, sind diejenigen, die durch Transformation mit geeigneten Elementen des Gruppenrings von $\mathfrak{G}$ erzeugt werden können.

21/22

Satz von Wedderburn.

$\mathfrak{K}$ sei ein minimaler nicht komm. Körper, p^n Elemente $\mathfrak{G} = \mathfrak{K} - \{0\}$.

(1) Jede abelsche Untergr von $\mathfrak{G}$ ist zyklisch (erzeugt)**???**)

(2) Daher ist jede ungerade Sylowgr zyklisch.

(3) $\mathfrak{G}$ enthält nur 1 Element der Ord 2, nämlich -1

(4) $\mathfrak{G}$ enthält keine Quaternionengruppe. s. auch 26

a) $p = 2$ klar

b) $p > 3$: $p^2 + 1$ enthält einen ungeraden Primteiler q, dieser teilt $p^2 - 1$ nicht, daher erzeugt in $|\mathfrak{K}| = p$ jedes El der Ord q ganz $\mathfrak{K}$. Also gibt es keinen Quaternionenkörper über GF(p),daher in $\mathfrak{G}$ keine Quaternionengruppe (dieser würde einen Qukörper erzeugen).

c) $p = 3$: $a^2 + b^2 + c^2 + d^2 \equiv 0$ (p) hat Lösg 1110, also gibts wieder keinen Quatkörper, weiter wie b)

(5) Also ist jede Sylowgr von $\mathfrak{G}$ zyklisch.

(6) Ist $\mathfrak{Z}$ ein maximaler zykl Normalteiler von $\mathfrak{G}$, so ist $\mathfrak{Z} + \{0\}$ Teilkörper von $\mathfrak{K}$, da $\mathfrak{Z}$ eigener Zentralisator. Also

$$\left.\begin{array}{l|lll} |\mathfrak{G} : \mathfrak{Z}| & \text{Grad } \mathfrak{Z} + \{0\} = \alpha & Z = p^\alpha > \alpha & g = Z^\beta \\ Z = |\mathfrak{Z} + \{0\}| & & \frac{g}{2} \leq \alpha < Z & g < Z^2 \end{array}\right\} \text{ W!}$$

Forts. 26.

22/23

Klassenpermutationen

1. Die inneren Autom von $\mathfrak{G}$ können nicht auf einer Klasse 2-tra und simultan auf einer anderen tra sein

2. Können die inneren Autom auf 3 Klassen simultan transitiv sein?
   dh für 3 Zentralisatoren $\mathfrak{Z}_1, \mathfrak{Z}_2, \mathfrak{Z}_3$: $(\mathfrak{Z}_1 \cap \mathfrak{Z}_2)\mathfrak{Z}_3 = \mathfrak{G}$ usw.
   dh $\mathfrak{G} : \mathfrak{Z}_i \quad (i = 123)$ unabh.?

23/24

$\lhd\lhd$

1. Frage: Kann man meine Vertauschbarkeitstheorie dualisieren, also übertragen auf $\mathfrak{A}^{\frac{1}{\mathfrak{A}}}$? F

2. Man sollte einführen $s(\mathfrak{G}/\mathfrak{A})$, wenn $\mathfrak{A} \lhd \lhd \mathfrak{G}$, als Verband der $\mathfrak{B} \in s\mathfrak{G}$ mit $\mathfrak{A} \leq \mathfrak{B} \leq \mathfrak{G}$.

3. Was für Eigenschaft hat die (in die „Primär-Struktur von $\mathfrak{G}$"gehörende) Untergruppe $\bigcap \mathfrak{P}^{\mathfrak{G}}$ wo $\mathfrak{P}$ alle Sylowgr von $\mathfrak{G}$ durchläuft? oder $\bigcup_{\mathcal{P} \neq \mathfrak{Q}} (\mathfrak{P}^{\mathfrak{G}} \cap \mathfrak{Q}^{\mathfrak{G}})$?

24/25

Permutationsgruppen.

1. Der alte Satz, dass die symmetrische $\mathfrak{S}^n \quad (n > 6)$ keinen äusseren Autom besitzt kann so bewiesen werden:

   (a) $\{(12345)\}\{(67)\}\{(89)\}$.. ist eine max. abelsche Gr vom Typ $[5, 2, \ldots, 2]$, jede anders gebaute abelsche Gr vom Typ $[5, 2, \ldots, 2]$ hat kleinere Ordng.

   (b) Also geht bei Autom von $\mathfrak{S}^n$ jeder Fünferzyklus c in einen ebensolchen über.

   (c) Der Zentralisator $\mathfrak{Z}$ von c hat die Gestalt $\mathfrak{Z} = \{C\} \times \mathfrak{S}_{n-5}$, dabei ist $\mathfrak{S}_{n-5}$ der einzige Normalteiler von $\mathfrak{Z}$ vom Index 5.

   (d) also geht bei Autom von $\mathfrak{S}^n$ $\mathfrak{S}_{n-5}$ in $\mathfrak{S}'_{n-5}$ über

   (e) Daher geht auch ein minimaler Durchschnitt von verschiedenen $\mathfrak{S}^{n-5}$ in einen ebensolchen über, d.h. Transpositionen in Transpos.: daher auch $\mathfrak{S}^{n-1}$ in $\mathfrak{S}^{n-1}$.

NB (f) für $n = 5$ gehts ebenso mit Dreierzyklus statt 5.
   s. auch Hölder

25/26

Zum Satz von Wedderburn: Forts. von 22

(1) Ist K endl Schiefkörper mit Zentrum Z, so folgt aus $a^2 \in Z$ stets $a \in Z$ (und daher ist die 2-Sylowgr von $K_\times$ abelsch, daher zyklisch)
Bew: sonst gibt es x mit $x^a \neq x$. Dann hat $b = x^a - 1$ die Eig. $b^a = -b \neq 0$; $ab = -ba$. $L = Z + Za + Zb + Zab$ ist dann ein Körper der Ord $|Z|^4 = q^4$. (daher $q \equiv 1(2)$). Aber jeder solche Körper ist abelsch, da es einen ungeraden Primteiler r von $q^2 + 1$ gibt,(sonst $q^2 + 1 = 2^\alpha$, $q^2 \equiv -1(4)$, geht nicht), und jedes El der Ord r von L erzeugt ganz L.

(2) einen Zahlen-theorie-freien Beweis bekommt man vielleicht mit der Bemerkg: Ist K min. nichtablsch $a^2 \in Z, b^2 \in Z, ab \neq ba$, so ist $ab + ba \in Z$ da va und vb, daher $(a + b)^2 \in Z$.

3. Ist M komm. Teilkörper eines endl. (Schief) Körpers K, und ist $M_\times = \mathcal{N}\!s\, M_\times$, so ist $M = K$. Bew. mit Lagrange Resolvente:

26/27

Bilde $x \in K \to x^{(\alpha)} = \sum\limits_{m \neq 0} m^\alpha x^m \quad \alpha = 0, 1, 2, ..., m-1$
Es ist für $\mu \in M_\times \;\; x^{(\alpha)\mu} = \sum m^\alpha x^{\mu m} = \sum \left(\frac{m}{\mu}\right)^\alpha X^m = \mu^{-\alpha} x^{(\alpha)}$. Wäre für ein $\alpha \neq 0 \;\; x^{(\alpha)} \neq 0$, so wäre

$$\mu^{-1} x^{(\alpha)} \mu = \mu^{-\alpha} x^{(\alpha)}$$
$$\mu^{1-\alpha} = x^{(\alpha)} \mu x^{(\alpha)-1} \in M$$
$$x^{(\alpha)} \in \mathcal{N}\!s M$$

also $x^{(a)} \in M$ nach Vor.
Nach Vandermonde ist $\det(m^\alpha) \neq 0$, also nach Cramer

$$x = \frac{(\quad)}{(\quad)} \in M, \quad K \subseteq M.$$

3' Jeder echte Teilkörper eines endl. (schief) Körpers ist von seinem Normalisator verschieden. (3).

4. Ist M max Teilk. des endl wirklichen Schiefk. K, so wähle $t \in \mathcal{N}\!s M$, $\operatorname{Ord} t : M = r > 1$. Die Gl kleinsten Grades $\sum\limits_0^k m_\nu t^\nu = 0$, $m_k = 1$ $m_\nu \in M$ ist eindeutig bestimmt. Transf. mit $m \in M$ zeigt: t^ν zentralisiert m; also $t^k \in M$ wegen Maximalität von M. $t^k - Z_0 = 0$ ist die Gl kl. Grades, also $k = \operatorname{Ord}_M t = r$. Bei passender Wahl von t ist $t^{-1} m t = m^q$, $q = |Z|$; denn t^{-1} mit ist Autom $K : Z$, der genau Z elemw. fest lässt.

27/28

$m' = m^{1+t+\cdots+t^{k-1}} = m^{1+q+\cdots+q^{k-1}}$ Exponent teilt $q^k - 1 = |M| - 1$, also gibt es

$$\frac{q^k - 1}{1 + \cdots + q^{k-1}} = q - 1$$

Bilder m', diese bilden also gerade $Z_\times$. Wähle $m \in M$ $m^{1+\cdots+t^{k-1}} = Z_0$. Also kann man $t' = mt$ so wählen dass $t'^k = 1$. Dieses ist die Min Gl von t', aber reduzibel!

Bessere Anordnung des Beweises 3-4 für den Satz von Wedderburn:
$M \neq K$ sei maximaler komm Teilkörper des endl Schk. K.
Ann: $\exists t : \operatorname{Ord} t : M = r > 1$ r Primzahl.

a) $\{Mt\}/M$ zerfällt (weil jedes $z \in Z$ Norm aus $M : Z$ ist).Wenn $\mathfrak{N}s\ M : M$ zerfällt, ist $\mathfrak{N}sM = M$.

b) Also $t^{r-1} + \cdots + t + 1 = 0$ *[aber von einander verschiedene Körperautom. sind lin un. ausführl]* mit Basis $m_1, -, m_r$ von $K : Z$ multipl. und durch **???**gibt $\det(m_i^{t^q}) = 0$ entgegen Vorlesung

c) Wenn $M = \mathfrak{N}sM$, so folgt $M = K$ mit Lagrange.

6. Variante:

a) Ist für den Maximalkörper M $\mathfrak{N}sM \simeq \mathfrak{Z}sM$, dann K kommutativ nach 2.

b) Sonst wähle $t \in \mathfrak{N}sM - \mathfrak{Z}sM$, $t^r \in \mathfrak{Z}sM$, r Primzahl, man kann $t^r = 1$ machen, und $r = \operatorname{Gr} M$. Also: Jeder Max Kö hat Primzahlgrad $= r : Z$, und es gibt einen Zwischen kö des Grades $\leq r - 1$ nämlich $Z(t)$. Das ist unmöglich: Wähle M mit $M : Z = \min$

28/29

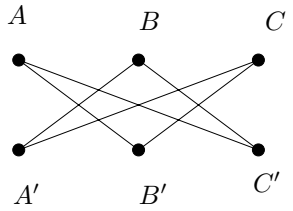
7. Vielleicht lässt sich der Beweis des Satzes von Wedderburn noch vereinfachen durch die Bemekg: Ist $\begin{cases} M \text{ Maximalkörper (komm.)} \\ b^{|M|-1} = 1 \end{cases}$, so lässt sich jedes $x \in K$ darstellen als Linear-Verbindung von solchen $t_\kappa \in K$, für die $b^{t_\kappa} \in M$ liegt Bew: $\sum\limits_{\lambda=0}^{|M|-1} m^{\kappa\lambda} x b^{-\lambda} = t_\kappa$.
macht $m^\kappa t x = t_\kappa b$ und $x = \sum a_\kappa t_\kappa,\ \ a_\kappa \in M$.

---

8. Andere Variante: $M : Z = r$ Primzahl. Zeige, dass $1, t, -, t^{r-1}$ lin un über M, dann $K : M = r$, also $K : Z = r^2$, also sind je zwei Zwischenkörper zwischen Z und K multiplikativ isomorph, daher nach 7. konjugiert unter Autom. Aber die Konjugierten einer Untergruppe können nicht die ganze Gruppe überdecken. Hier braucht man nicht den Normen-Satz.

---

1. Ein Isomorphie-Problem: Sind 3 Untergr und ihre Durchschnitte gegeben:



so gilt für die Indizes: $|A:B'||B:C'||C:A'| = |A:C'||C:B'||B:A'|$, dann $= \frac{|A||B||C|}{|A'||B'||C'|}$. Wenn nun die Durchschnitte stets normal sind, gilt dann etwa eine Isomorphie $\frac{A}{B'} \times \frac{B}{C'} \times \frac{C}{A'} \cong \frac{A}{C'} \times \frac{C}{B'} \times \frac{B}{A'}$ oder ähnlich?

29/30

Zur Theorie der Algebren

1. Das Gleiche, was auf 29.7 mittels $x \to \sum\limits_{M-0} mxm'^{-1}$ gemacht wurde, wo M eine zyklische Untergr. eines Schiefkörp. durchläuft, die auf einer Gr $\{m'\}$ homom abgebildet ist $(m \to m')$

– das Gleiche für beliebige Körper A endl. Ranges n über dem Zentrum Z einer einf. Algebra erreicht man durch die Bildung

$$x \to \sum_{1}^{n} \varphi(a_\nu) x b_\nu$$

wobei $a_1 \dots a_n$ eine Basis von $K : Z$, $b_1 \dots b_n$ die komplementäre Basis bzgl. der [irgend einer?] „Spur“ σ von $K : Z$ (dh. $\sigma(K) \in Z$; $\sigma(kl) = 0$ f. alle $l \in K \to l = 0$; $\sigma(zk) = z\sigma(k)$ für $z \in Z, k \in K$).
φ soll dabei einen Ringisomorphismus $:Z$ von A auf einen Teilkörper A' der Algebra bedeuten.

2. $t = \sum a_\nu x b_\nu \in Z$ für jedes x denn $t = \mathfrak{a}(xI)\mathfrak{b}$, und für alle $a \in A$ ist mit der reg Darstellung $R(a) : Z$:

$$at = a\mathfrak{a}(xI)\mathfrak{b} = \mathfrak{a}R(xI)\mathfrak{b} = \mathfrak{a}(xI)R\mathfrak{b} = \mathfrak{a}(xI)\mathfrak{b}a = ta$$

$$\begin{pmatrix} a & & & \\ & ??? & & \\ & & \vdots & \\ & & & a^{(n-1)} \end{pmatrix} \begin{pmatrix} \mathfrak{a} & & \\ & \ddots & \\ & & \ddots \\ & & \mathfrak{a}^{(n-1)} \end{pmatrix} (b)$$

$$= \begin{pmatrix} \mathfrak{a} \\ \vdots \end{pmatrix} R(\mathfrak{b} \cdots \mathfrak{b}^{(n-1)}) = \underbrace{\begin{pmatrix} \mathfrak{a} \\ \vdots \end{pmatrix} (\mathfrak{b})}_{I} \begin{pmatrix} \mathfrak{a} & & \\ & \ddots & \\ & & a^{(np)} \end{pmatrix}$$

also $R(\mathfrak{b}\ldots) = (\mathfrak{b}\ldots)\begin{pmatrix}\mathfrak{a} & & \\ & \ddots & \\ & & \end{pmatrix} \to R\cdot\mathfrak{b} = \mathfrak{b}\cdot a$

30/31

Algebren (Fortsetzg.)

1. Ist $\mathfrak{R}$ Ring, Ztr $\mathfrak{R} = \mathfrak{Z}$ ein Körper, $\mathfrak{Z} \leq a \leq \mathfrak{R}$ und $\mathfrak{A}$ habe 2 komplementäre Basen $\begin{pmatrix} a_i \\ b_i \end{pmatrix} : \mathfrak{Z}$. Dann folgt aus einem $\mathfrak{Z}$-Isom. $\mathfrak{A} \to \overline{\mathfrak{A}} \leq \mathfrak{R}$:

   $$\overline{a}t = ta \text{ für ein } t \neq 0 \text{ in } \mathfrak{R}.$$

   Bew: setze an $t = \sum_i \overline{a}_i x b_i$. Das kann nicht für alle $x \in \mathfrak{R} = 0$ sein, denn die Lösgsvektoren von $\sum \overline{a}_i x v_i = 0$ f. alle $x \in \mathfrak{R}$ bilden einen Modul ${}_{\mathfrak{R}}V_{\mathfrak{R}}$, aber enthält er $v = \{z_1 \; - \; z_n\}, \;\; z_\nu \in \mathfrak{Z}$. aber die $\overline{a}_i$ sind lin un : $\mathfrak{Z}$.
   Also gibts $\sum \overline{a}_i x b_i = t \neq 0$, und dann ist $\overline{a}t = ta$.

2. Um ähnlich zu beweisen daß bei normalen einf. Algebren $\mathfrak{R}[\mathfrak{V} : \mathfrak{Z}] = [\mathfrak{R} : \mathfrak{A}]$ ist, wobei $\mathfrak{V} = \mathcal{Z}s\mathfrak{A}$ muß man vielleicht 2 komplementäre Basen von $\mathfrak{R} : \mathfrak{V}$ heranziehen.

3. Dass $\mathfrak{A} : \mathfrak{Z}$ komplem. Basen hat, heißt: Die rechte und die linke reg Darst von $\mathfrak{A} : \mathfrak{Z}$ sind äquivalent (Frobenius Ring?) Das ist z.B. immer der Fall, wenn $\mathfrak{A} : \mathfrak{Z}$ einfach, dann gibts nur eine Darstellg. jeden Grades.

31/32

Algebren

1. Für $\mathfrak{A} : \mathfrak{Z}$ (Schief)körper kann man ohne Darstellgstheorie komplem. Basen angeben: Wähle irgend Basis $a_1 \cdots a_n$, setze für $x \in \mathfrak{A} \quad \sigma(x) = z_1$, wenn $x = \sum z_\nu a_\nu$. Dann gibts kein x mit $\sigma(a_i x) = 0$ für alle i, also ist $(\sigma(a_i a_j)) \neq 0$, und es gibt $\mathfrak{b}_1 \; \cdots \; \mathfrak{b}_n$ mit $\sigma(a_i \mathfrak{b}_j) = \delta_{ij}$. Dann sind $a_i, \; b_j$ kompl. Basen: Aus

   $$a_i x = \sum_\ell \xi_{i\ell} a_\ell, \quad x b_j = \sum_\ell b_\ell \eta_{\ell j}$$

   folgt

   $$\sigma(a_i x b_j) = \xi_{ij} = \eta_{ij}$$

32/33

P.-Gruppen vom Grade $p : \mathfrak{G}$. 22.2.58

1: Klassen konj. Ugruppen vom Index p (Fortsetzg. von VIII 167)
Ein Autom. der Ord. 2 von $\mathfrak{G}$ der eine Klasse fest lässt, lässt jede Klasse fest. Ebenso daher jeder Autom. gerader Ordnung
Bew: $\sigma^2 = 1$ Ist $\mathfrak{U}^\sigma = \mathfrak{U}, \; \mathfrak{V}^\sigma = \mathfrak{V}$, so folgt aus $\mathfrak{U}\mathfrak{K} = \mathfrak{K}\mathfrak{V} \quad \mathfrak{K}^\sigma = \mathfrak{K}$, also $\mathfrak{K} = \overline{\mathfrak{K}}$. [teilweise durchgestrichen; ersetzt durch: so $[\mathfrak{U}\mathfrak{V}] = [\mathfrak{U}\mathfrak{V}^\sigma] \quad \mathfrak{V} \approx \mathfrak{V}^\sigma$]
Rest folgt aus VIII 166(3): $|\mathfrak{K}| < \frac{p}{2} \to |\mathfrak{K}| = 1, \mathfrak{U}^p = \mathfrak{V}$.

2. Jeder Autom. ungerader Ord. lässt jede Klasse fest. VIII 170(14)

3. Hat $\mathfrak{G}$ einen Autom. der Ord. 2, der $\mathfrak{P}$ und ein $\mathfrak{U}$ *[eine Klasse]* fest lässt, so enthält $\mathfrak{G}$ nur eine Klasse.
$\mathfrak{U} = \mathfrak{U}^\sigma, \sigma^2 = 1$, $\mathfrak{U}\mathfrak{K} = \mathfrak{K}\mathfrak{V} \to \mathfrak{U}\overline{\mathfrak{K}} = \overline{\mathfrak{K}}\mathfrak{V}^\sigma$; $\mathfrak{V}\mathfrak{L} = \mathfrak{L}\mathfrak{W}^\sigma \to \mathfrak{U}\mathfrak{K}\mathfrak{L} = \mathfrak{K}\mathfrak{L}\mathfrak{W}^\sigma$
$\mathfrak{K}\mathfrak{L} = a\overline{\mathfrak{K}} + \overline{\mathfrak{b}}\mathfrak{P}$ $a, \mathfrak{b}$ rat
$\kappa\lambda = a\overline{\kappa}$ $|\lambda|$ rat $\to$ $\mathfrak{V}, \mathfrak{V}^\sigma$ in einer Klasse Rest 1. (VIII 166(2))

In belieb $\mathfrak{G}$ gilt: Zwei Untergruppen $\mathfrak{H}_1 \neq \mathfrak{H}_2$ vom Index p sind konjugiert genau wenn

$$k = |\mathfrak{H}_1 : \mathfrak{H}_1 \cap \mathfrak{H}_2| = p - 1 \qquad\qquad 34_2$$

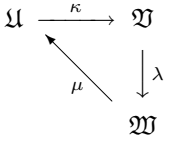
Grad p (Forts.) von 33 & VIII 166)

1. Sind $\mathfrak{U}, \mathfrak{V}$ Untergr. vom Index p, so setze die ganze Zahl $[\mathfrak{U}\mathfrak{V}] = \frac{k(p-k)}{p-1}$, wenn $|\mathfrak{U}\mathfrak{V}| = k|\mathfrak{U}|$.
dh. $|\mathfrak{V} : \mathfrak{U} \cap \mathfrak{V}| = k$. *Was ergibt das durch Betrachtung von* $\mathfrak{U} \cap \mathfrak{V} \cap \mathfrak{W}$*? (7→)* Dann gilt:

1a. $[\mathfrak{U}\mathfrak{V}] = [\mathfrak{V}\mathfrak{U}] = [\mathfrak{U}\mathfrak{V}^G]$ Deutung XI 354! $7 \to$

2. $\mathfrak{V} = \mathfrak{U}^G \leftrightarrow [\mathfrak{U}, \mathfrak{V}]$ eine Quadratzahl $\leftrightarrow [\mathfrak{U}, \mathfrak{V}] = 1$ denn das $|K|$ von VIII 166(2) ist $\sqrt{[\mathfrak{U}\mathfrak{V}]}$

3. $\circ\rho$ $[\mathfrak{U}\mathfrak{W}] = \frac{1}{r^2}[\mathfrak{U}\mathfrak{V}][\mathfrak{V}\mathfrak{W}]$ und r = ganz denn $\mathfrak{U}\mathfrak{K} = \mathfrak{K}\mathfrak{V}$, $\mathfrak{V}\mathfrak{L} = \mathfrak{L}\mathfrak{W} \to$
$\begin{cases} \mathfrak{U}\mathfrak{K}\mathfrak{L} = \mathfrak{K}\mathfrak{L}\mathfrak{W} \\ \mathfrak{U}\mathfrak{M} = \mathfrak{M}\mathfrak{W} \end{cases}$ und $\mathfrak{K}\mathfrak{L} = r\mathfrak{M} + s\mathfrak{P}$



$\to$ $\boxed{\kappa\lambda = r \cdot \overline{\mu}}$

$|\kappa|^2|\lambda|^2| = r^2|\mathfrak{p}|^2$ $[\mathfrak{U}\mathfrak{V}][\mathfrak{V}\mathfrak{W}] = r^2[\mathfrak{U}\mathfrak{W}]$
Also wenn von $\mathfrak{V}$ aus κ, λ vorkommen, so auch $\frac{\overline{\kappa}\lambda}{r}$ für das grösste $r > 0$ ganz mit $r|\overline{K}\lambda$, falls zu jedem $\mathfrak{V}$ die gleichen λ gehören.
Es kommt also auf $[\mathfrak{U}\mathfrak{V}]$ mod der mult. Gr der Quadrate an.
Stets ist $[\mathfrak{U}\mathfrak{V}][\mathfrak{V}\mathfrak{W}][\mathfrak{W}\mathfrak{U}] = \square$

4. $\mathfrak{V}_1 = \mathfrak{V}_2^G \leftrightarrow [\mathfrak{U}\mathfrak{V}_1] = m^2[\mathfrak{U}\mathfrak{V}_2]$ (23)

5. Es gibt höchstens so viele Klassen konj. Ugr vom Index p, als es mod rat^2 verschiedene ganze Zahlen der Form $\frac{k(p-k)}{p-1}$ gibt.

Grad p

6. Ist σ Automorphismus von $\mathfrak{G}$, so

$$[\mathfrak{UW}] = [\mathfrak{U}^\sigma \mathfrak{V}^\sigma]$$

6a. Jeder Autom σ von $\mathfrak{G}$, der P fest läßt, ist induziert von P^α. Zum Beweis zeige: $\operatorname{Ord}\sigma = q^\alpha \Rightarrow q = p$, $x^\sigma = x^R$ Folgere: Äussere Automorphismengr ist ord $\big|p-1$ 2-Gruppe.

7. Setze $(\mathfrak{UW}) = k$, wenn $|\mathfrak{UW}| = k|\mathfrak{U}|$. Dann gilt: Ist $(\mathfrak{UV}) = k$, $(\mathfrak{UW}) = l$, $(\mathfrak{VW}) = m$ und $(k,l) = 1$, so ist $m|kl$.

$$\begin{array}{rcl} \textit{Bew}: & & |\mathfrak{U} : \mathfrak{U} \cap \mathfrak{V}| = k, \quad |\mathfrak{U} : \mathfrak{U} \cap \mathfrak{W}| = l \\ [(k,l) = 1] & & |\mathfrak{U} : \mathfrak{U} \cap \mathfrak{V} \cap \mathfrak{W}| = kl \\ & = & |\mathfrak{V} : \mathfrak{U} \cap \mathfrak{V} \cap \mathfrak{W}| \\ m & = & |\mathfrak{V} : \mathfrak{V} \cap \mathfrak{VW}| \big| kl \end{array}$$

7'. Aus $(\mathfrak{UV}) = (\mathfrak{UW})$ folgt $\mathfrak{W} = \mathfrak{V}^G$ (4)

8. Ist $p - 1 = 2^\alpha \cdot q^\beta$, so gibt es höchstens zwei Klassen.
Bew: $k = 2^\alpha \cdot m$, $p - k = q^\beta \cdot n$; $2^\alpha m + q^\beta n = p$ hat genau eine Lösung m, n mit $1 \le m \le q\beta$, $1 \le n < 2^\alpha$. Also $[\mathfrak{UV}]$ eindeutig bestimmt.
[*Durchstreichung*
[*Es ist ja stets* $(\mathfrak{UV}) = 2$ *oder* q, *wenn* $\mathfrak{U} = \mathfrak{V}^G$.]
Nun wird nach 7 *mit* $m = (\mathfrak{UW})$ $\quad m \big| 2^\mu q^\lambda$, *also* $m = \begin{cases} 1 & \mathfrak{V} \sim \mathfrak{W}; \\ p-1 & \end{cases}$
oder $m = 2^\mu$; *dann* $(\mathfrak{UW}) = (\mathfrak{UV})$ *also* $\mathfrak{W} = \mathfrak{V}^G$ *dann* $2^\mu + q^\lambda = p - 1$, *dann hat jedes* $(\mathfrak{UW}_1^G)$ *von dr Form* $2^{\cdot\cdot}$ *den Wert* 2^μ, *also* $\mathfrak{W}_1 = \mathfrak{V}^G$; $\mathfrak{U}, \mathfrak{V}$ *sind die einzigen Klassen.*]

35/36

Noch Gruppen vom Gr. p

9. Die Klassen konj. Untergr in G vom Index p erleiden unter der Autom.-Gr. von $\mathfrak{G}$ eine zyklische halbreguläre Permutationsgr einer Ordnung 2^α *siehe X 286*
Bew: [**???**] Deck-2- Gruppe $\mathfrak{d} \le \mathcal{N}\mathfrak{P}$. $\exists \delta \in \mathfrak{d}$, permut Klasse $P^\delta = P \Rightarrow \mathfrak{K}^2 = \alpha\mathfrak{K} + \beta\mathfrak{P}$ W! Halbreg wegen 33_1

25.2.58 Hierzu XI 295 (7)

10. Ist $\mathfrak{G}$ eine maximale $\mathfrak{K} \neq$ trivial als konjugierenden Komplex besitzende Gruppe vom Grade p, so enthält $\mathfrak{G}$ genau ([Begründung]: denn $\mathfrak{U} \overset{\sigma}{=} \mathfrak{V}$, $\mathfrak{U} \overset{\tau}{=} \mathfrak{W}$, $\mathfrak{V}^{\sigma^{-1}\tau} = \mathfrak{W}$, aber $\sigma^{-1}\tau$ läßt p elem $W.$ fest, ist also ein innerer VIII 171) 2 Klassen $\mathfrak{U} = \mathfrak{G}_1$, $\mathfrak{V}$ und es gibt einen Autom. σ von $\mathfrak{G}$ mit $\mathfrak{U}^\sigma = \mathfrak{V}$, und jede solche σ hat die Ordnung 2. Wählt man $\mathfrak{U}$, $\mathfrak{V}$ so, dass $\mathfrak{U} \cap \mathfrak{N}\mathfrak{P} = \mathfrak{V} \cap \mathfrak{N}\mathfrak{P}$, so zentraliesiert σ diesen Durchschnitt!
Bew: $\mathfrak{G}$ nach $\mathfrak{U}$ darstellen: gebe $\overline{\mathfrak{G}}$ $\mathfrak{V}$ hat Transs. $\mathfrak{K}$
" $\mathfrak{V}$ $\mathfrak{F}$ $\mathfrak{U}$ " gebe $\overline{\overline{\mathfrak{G}}}$ $\overline{\mathfrak{K}}$
Transformiert man die zweite Darst. mit $\pi = \binom{P}{P^{-1}}$, so entsteht wieder eine Gr $\mathfrak{G}^*$, in der $\mathfrak{V}^*$ das Transs. $\mathfrak{K}$ hat. also $\{\overline{\mathfrak{G}}, \mathfrak{G}^*\} = \mathfrak{P} \cdot \{\overline{\mathfrak{U}}, \mathfrak{V}^*\} = \mathfrak{G}$
Wegen Max., daher $\overline{\mathfrak{U}} = \mathfrak{V}^*$; $\overline{\overline{\mathfrak{G}}}^\pi = \overline{\mathfrak{G}} \cdot \pi\overline{\overline{\sigma(G)}}\pi = \overline{G}$
Da $\sigma(P^\pi) = P^{-1}$, hat σ die Ord 2. Allgemeiner XI 284
Beispiel: $\mathfrak{G}_{168}$ ist maximal $|K| = 3$, hat also nur 2 Klassen, sind konj. in $\mathfrak{A}$.

11. Frage: Hat die max. Gruppe mit mehreren geg. konjugierenden Komplexen $\mathfrak{K}, \mathfrak{L} \ldots$ auch gewisse konjug. Automorphismen?
ja, wenn $\mathfrak{K}, \mathfrak{L} \ldots$ die gleichen Untergruppen verbinden.

36/37

$$\text{Grad } \mathfrak{G} = p$$

12. Allgemein kann man maximale intrans. Komplemente gegebener trans. Permgr. betrachten. [s.10]

13. Die max zu $\mathfrak{K}$ gehörige Obergr. von $\mathfrak{P}$ gestattet, wenn $\mathfrak{U} \underset{\mathfrak{K}}{\longrightarrow} \mathfrak{V}$, einen Autom σ d. Ord 2 mit

$$\mathfrak{K}^\sigma = \overline{\mathfrak{K}}, \quad \mathfrak{U}^\sigma = \mathfrak{V}, \quad \mathfrak{V}^\sigma = \mathfrak{U}.$$

Sie ist isomorph zu maximalen zu $\mathfrak{K}^{(\alpha)}$ gehör. Gruppe, wenn $\mathfrak{K}^{(\alpha)}$ konj. zu $\mathfrak{K}$.

NB zu 14: Die Tatsache $k = k_0 k'$, $k_0 \big| p-1$ legt die Vermutung nahe, dass das K mit $K\overline{K} = [\mathfrak{U}\mathfrak{W}]$ aus k' Perioden der Länge k_0 besteht.

14. Ist $p - 1 = \prod_i^r q_\rho^{\alpha_\rho}$ $(q_i \neq q_j)$, so gibt es genau 2^{r-1} verschiedene Werte $\frac{k(p-k)}{p-1}$ ganz. Daher gibt es $\leq 2^{r-1}$ verschiedene Klassen.
Bew. Sei stets k gerade, $l = p - k$, dann ist wegen $(k, l) = 1$ und $p - 1 \big| kl$ stets

$$q_1 = 2 \qquad k = \underbrace{2^\alpha \prod_{q_\rho > 2}{}' q_\rho^{\alpha_\rho}}_{= k_0 k'} \cdot k', \qquad l = \underbrace{\prod{}'' q\rho^{\alpha_\rho}}_{= l_0 l'} \cdot k',$$

und

$$k_0k' + l_0l' < p \text{ hat bei } k_0l_0 = p-1,\ (k_0, l_0) = 1$$

stets genau eine Lösung k', l' mit $1 \le k' < l_0,\ 1 \le l' < k_0$, nämlich $k' = [\frac{k_0^{-1}}{l_0}],\quad l' = [\frac{l_0^{-1}}{k_0}]$, wo $[\frac{a}{b}]$ = kleinster positiver Rest $a \mod b$.

Noch Grad $\mathfrak{G} = p$

Sei $p - 1 = 2^\alpha q^\beta$

15) Der für $[\mathfrak{U}\mathfrak{V}]$ in Betracht kommende Wert ist das Produkt xy mit $1 \le x < q^\beta,\ 1 \le y < 2^\alpha$ und $2^\alpha x + q^\beta y = p$
Es ist $x \equiv 2^{-\alpha} \quad (q^\beta)$, $y \equiv q^{-\beta} \quad (2^\alpha)$
jeweils der kleinste pos. Rest: $[\frac{a}{b}]$ = kl pos Rest $a \mod b$

$$[\mathfrak{U}, \mathfrak{V}] = [\frac{2^{-\alpha}}{q\beta}] - [\frac{q-\beta}{2^\alpha}] = [\frac{k_0^{-1}}{l_0}] \cdot [\frac{l_0^{-1}}{k_0}] \quad \text{allg.}$$

wo $p - 1 = k_0l_0$; k_0/k, l_0/l, $(k_0, l_0) = 1$
$p = 4^\nu \cdot 3 + 1 \to i = \frac{2p+1}{9}$, z.B.

$$\alpha = 1, \qquad p = 2q^\beta + 1 :\ [\mathfrak{U}, \mathfrak{V}] = \frac{q\beta + 1}{2} \cdot 1 = \frac{p+1}{4}$$

$$\alpha = 2, \qquad p = (2q^\beta)^2 + 1 :\ [\mathfrak{U}\mathfrak{V}] = \frac{3q^{2\beta}+1}{4} = \frac{3p+1}{16} = \frac{3q+1}{4}$$

$$\text{oder } \frac{q+1}{4} \cdot 3$$

$p - 1 = 2^\alpha q^\beta$: $\alpha = 2,\ p = 4q + 1$
Z.B.

p	$=$	7	11	13	19	23	29	37	47	49	59	83	101
$[\mathfrak{U}, \mathfrak{V}]$	$=$	2	3	3	5	6	6	7	12	11	15	21	19
h	$\le$				1		1			1			

$$\mathfrak{K} = 1 + P + P^3 + P^9 \qquad \text{Jordan}$$

$p - 1 = 2^\alpha q^\beta r^\gamma\ < 200$:

	$p-1$	k	l	$i = [\mathfrak{U}\mathfrak{V}]$	Klassenzahl $\leq$
$p = 43$	$2 \cdot 3 \cdot 7$	$3 \cdot 5$	$14 \cdot 2$	$[2 \cdot 5]$	
		$7 \cdot 1$	$6 \cdot 6$	$[2 \cdot 3]$	1
		$21 \cdot 1$	$2 \cdot 11$	[11] Jordan	
$p = 71$	$2 \cdot 5 \cdot 7$	$5 \cdot 3$	$14 \cdot 4$	$2^3 \cdot 3$	
		$7 \cdot 3$	$10 \cdot 5$	$3 \cdot 5$	2
		$35 \cdot 1$	$2 \cdot 18$	$2 \cdot 3^2$	
	Forts. 47_{12}				

38/39

$p = 67$	$2 \cdot 3 \cdot 11$	$3 \cdot 15$	$22 \cdot 1$	$[3 \cdot \underline{5}]$	
		$11 \cdot 5$	$6 \cdot 2$	$[2 \cdot \underline{5}]$	1
		$33 \cdot 1$	$2 \cdot 17$	$[1 \cdot 7]$	
$p = 79$	$2 \cdot 3 \cdot 13$	$3 \cdot 9$	$26 \cdot 2$	$[\underline{2} \cdot 3^2]$	
		$13 \cdot 1$	$6 \cdot 11$	11	2
		$39 \cdot 1$	$2 \cdot 20$	$[2^2 \cdot 5]$	
$p = 103$	$2 \cdot 3 \cdot 17$	$3 \cdot 23$	$34 \cdot 1$	[23]	
		$17 \cdot 5$	$6 \cdot 3$	$[3 \cdot \underline{5}]$	2
		$51 \cdot 1$	$2 \cdot 26$	$2 \cdot 13$	
$p = 131$	$2 \cdot 5 \cdot 13$	$5 \cdot 21$	$26 \cdot 1$	$3 \cdot 7$	
		$13 \cdot 7$	$10 \cdot 4$	$2^2 \cdot 7$	2
		$65 \cdot 1$	$2 \cdot 13$	$3 \cdot 11$	
$p = 171$	$2 \cdot 5 \cdot 17$	$5 \cdot 7$	$34 \cdot 4$	$2^2 \cdot 7$	
		$17 \cdot 3$	$10 \cdot 12$	$[2^2 \cdot 3^2]$	2
		$85 \cdot 1$	$2 \cdot 43$	[43]	
$p = 61$	$4 \cdot 3 \cdot 5$	$3 \cdot 7$	$20 \cdot 2$	$2 \cdot 7$	
		$5 \cdot 5$	$12 \cdot 3$	$3 \cdot 5$	2
		$15 \cdot 3$	$4 \cdot 4$	$2^2 \cdot 3$	
$p = 157$	$4 \cdot 3 \cdot 13$	$3 \cdot 35$	$52 \cdot 1$	$3 \cdot 5$	
$= 13^2 - 13 + 1$	$\rightarrow$	$13 \cdot 1$	$12 \cdot 12$	$2^2 \cdot 3$	2
$= 12^2 + 12 + 1$		$39 \cdot 3$	$4 \cdot 10$	$2 \cdot 3 \cdot 5$	

39/40

$p = 31$	$2 \cdot 3 \cdot 5$	$3 \cdot 7$	$10 \cdot 1$	7	
$5^2 + 5 + 1$	$\rightarrow$	$5 \cdot 5$	$6 \cdot 1$	5	2
		$15 \cdot 1$	$2 \cdot 8$	2^3	
$p = 151$	$2 \cdot 3 \cdot 5^2$	$3 \cdot 17$	$50 \cdot 2$	$2 \cdot 17$	
		$25 \cdot 1$	$6 \cdot 21$	$3 \cdot 7$	2
		$75 \cdot 1$	$2 \cdot 38$	$2 \cdot 19$	
$p = 181$	$2^2 \cdot 3^2 \cdot 5$	$9 \cdot 9$	$20 \cdot 5$	$3^2 \cdot 5$	
		$5 \cdot 29$	$36 \cdot 1$	29	2
		$45 \cdot 1$	$4 \cdot 34$	$2 \cdot 17$	
$p = 191$	$2 \cdot 5 \cdot 19$	$5 \cdot 23$	$38 \cdot 2$	$2 \cdot 23$	
		$19 \cdot 9$	$10 \cdot 2$	$2 \cdot 3^2$	2
		$95 \cdot 1$	$2 \cdot 48$	$2^4 \cdot 3$	
$p = 127$	$2 \cdot 3^2 \cdot 7$	$7 \cdot 13$	$18 \cdot 2$	$2 \cdot 13$	
		$9 \cdot 11$	$14 \cdot 2$	$2 \cdot 11$	2
		$63 \cdot 1$	$2 \cdot 32$	2^5	
$p = 139$	$2 \cdot 3 \cdot 23$	$3 \cdot 31$	$46 \cdot 1$	31	
		$23 \cdot 5$	$6 \cdot 4$	$2^2 \cdot 5$	2
		$69 \cdot 1$	$2 \cdot 35$	$5 \cdot 7$	
$p = 199$	$2 \cdot 3^2 \cdot 11$	$9 \cdot 5$	$22 \cdot 7$	$5 \cdot 7$	
		$11 \cdot 5$	$18 \cdot 8$	$2^3 \cdot 5$	2
		$99 \cdot 1$	$2 \cdot 50$	$2 \cdot 5^2$	

Verfahren, die Tabelle mit Rechenmaschine fortzusetzen: ziehe von p ab ν : $(a + b)$ wo $ab = p - 1$, bis Rest durch la oder b teilbar wird.

40/41

Gr $\mathfrak{G} = p$

1. Für $p < 200$ gibt es höchstens jeweils zwei Klassen konjugierter Untergruppen vom Index p. Denn soweit ist $p - 1 = 2^\alpha q^\beta r^\gamma$, also Anz. $h \leq 4$, und das Produkt der 3 mögl. $[\mathfrak{UV}] = i$ ist nie ein Quadrat, daher ist $h \neq 3$, $h \neq 4$. Gilt stets für $p - 1 = 2^\alpha q^\beta r^\gamma$ S.185
   $p < 200$ sind die ersten 43 Primzahlen. Für endliche Geometrien interessant.

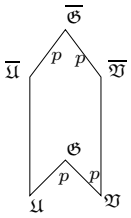
		k	l	$i = [\mathfrak{UV}]$	Klassenzahl
$p = 211$		$3 \cdot 47$	$70 \cdot 1$	[47]	
$p - 1 =$	$2 \cdot 3 \cdot 5 \cdot 7$	$5 \cdot 17$	$42 \cdot 3$	$3 \cdot 17$	
		$7 \cdot 13$	$30 \cdot 4$	$2^3 \cdot 13$	
		$15 \cdot 1$	$14 \cdot 14$	$2 \cdot 7$	2
		$21 \cdot 1$	$10 \cdot 19$	19	
		$35 \cdot 5$	$6 \cdot 6$	$2 \cdot 3 \cdot 5$	
		$105 \cdot 1$	$2 \cdot 53$	[53]	

NB: $p = 331 = 2\cdot3\cdot5\cdot11+1$ gibt $i = 83,\ 2\cdot37,\ 53,\ 7\cdot11,\ 2\cdot43,\ 3^2\cdot7,\ 3\cdot13$ also $h \le 2$ stimmt sogar für $p < 463 = 2\cdot3\cdot7\cdot11+1$.
Auch hier ist das Produkt von dreien nie ein Quadrat: $\to h \le 2$
Fortsetzung 184

2. Gibt es in $\mathfrak{G}$ zwei nicht konj. Ugr vom Index p, $(\mathfrak{U}, \mathfrak{V})$, so gibt es

   a) einen $\ddot{a}$-Autom σ der Ord 2 von $\mathfrak{G}$ mit $\mathfrak{U}^\sigma = \mathfrak{V}$, $P^\sigma = P^{-1}$, oder

   b) eine Vergrösserung $\overline{\mathfrak{G}}$.



mit $\overline{\mathfrak{U}} \cap \mathfrak{G} = \mathfrak{U}$, $\overline{\mathfrak{V}} \cap \mathfrak{G} = \mathfrak{V}$.

41/42

3. Vielleicht kann man eine projektive Ebene mit $43 = 6^2+6+1$ Punkten so konstruieren: Man wählt in der zykl. $\mathfrak{P}$ einen Komplex $\mathfrak{K}$ mit $|\mathfrak{K}| = 7$, $\mathfrak{K}\overline{\mathfrak{K}} = 6 + \mathfrak{P}$ und bezeichnet die 43 Mengen $\mathfrak{K}P^\alpha$ als Geraden. Geht nicht s. 5. Da je 2 Ger genau einen Pkt gemeinsam haben, steht da,

4a) $\mathfrak{q}\big|i \to \mathfrak{q} \ne \overline{\mathfrak{q}}$. Bew: sonst stets $q^{(v)} = \overline{q^{(v)}}$, $\pi q^{(v)}\big|\kappa, q\big|\kappa$.
$\operatorname{Ord}\sigma = 2^v \Rightarrow \mathfrak{q}^\sigma \ne \mathfrak{q}$; $\mathfrak{q} = \prod_1^e \mathfrak{q}^{(v)}$, $2^n\big|e_j$, $(p,i) = 1$ $f\big|\frac{p-1}{2^n}$, also q 2^n-Rest in jedem Fall, wenn $2^n\big|p-1$. Folgt $4\big|p-1 \quad\to\quad k\square R$.

4. Ist $\kappa\overline{\kappa} = i =$ ganzrat lösbar, $\kappa \in \operatorname{Rat}(\sqrt[p]{i})$ ganz, so ist bei $i = \prod q_\rho^{\alpha_\rho}$ stets ${q_\rho}^{\alpha_\rho}$ $\square$Rest mod p und $p\cdot4|p-1$. Denn wenn $q_\sigma = \mathfrak{q}_1 \dots \mathfrak{q}_s$, ist die Zahl der q_τ in i einerseits gerade, andererseits $q_\rho \cdot s$, also $2|\alpha_\rho s$. Ist also $\alpha_\rho \equiv 1(2)$, so $2|s$; dann ist $q^{p-1} = \prod N(\mathfrak{Q}_\sigma) = N(q_1)^s$. Aber $N(\mathfrak{Q}_1) \equiv 1\ (p)$ wegen $\varepsilon^n = 1$. Also $\mathcal{N}(\mathfrak{Q}_1) = q^{\frac{p-1}{s}} \equiv 1\ (p)$, wegen $2|s$ ist $q\square R$.
Genauer: Stets ist $q\square$Rest: ${q_\rho}^{\alpha_\rho} = q_1 q_2\ q_n$ mit $2|n = e\alpha_\rho$; also wenn $2 \nmid \alpha_\rho$ ist $2|e$, $f\big|\frac{p-1}{2}$, ${q_\rho}^{\frac{p-1}{2}} \equiv 1$

5. Im Fall $p > 43$ gibt es kein $\kappa\overline{\kappa} = 6$, denn (s.4a↑!) $2^{\frac{42}{2}} = 2^{21} \equiv (2^7)^3 \equiv (128)^3 \equiv (-1)^3 \equiv -1$.
Da auch $\left(\frac{5}{43}\right) = -1$, fällt sowohl $i = 2\cdot5$ wie $i = 2\cdot3$ aus: $h = 1$. Prüfen, ob Hilfsmittel von S. 178-81 nützen

42/43

Gr $p = 2q + 1$

6. *[Ist $p = 2q + 1 \equiv 1$, so ist Klassenzahl $= 1$*
   Bew: Es ist grad $\kappa = 2$ und daher κ reell wegen $p \equiv 1(4)$]
   NB: Stets ist $p = 2q + 1 \equiv 3 \pmod 4$

7. Bei $p = 11$ kommt $h = 2$ vor. Die einz. konj. Komplexe sind $\overline{\mathfrak{K}}$ mit $\mathfrak{K} = P^0 + \dots$ Die „Geraden“ sind

   $$\underbrace{\{1\ 3\ 4\ 5\ 9\}}_{\square \text{ Reste} \quad \text{mod } 11} \quad +\text{const.} \qquad T = (0)(3)(10)(19)(26)(45)(78)$$

   erzeugt mit $P = (012 \cdots 10)$ zusammen ein $\mathfrak{G}$.
   Je zwei Geraden haben 2 Pkt gemein un. jede Gerade hat 5 Pkte. Es ist $\mathfrak{G}_{1,3,4} = 1$, und da $T \neq 1$, ist $\mathfrak{G}$ nicht 3-tra.
   Hier bildet T $0 \to 0$, $r \to \frac{3}{r}$, $n \to \frac{1}{n}$ ab $r =$ Rest; $n =$ Nichtrest

   $$T = \begin{pmatrix} x \\ \varphi(m) \end{pmatrix} \qquad \varphi(X) = 5X^9 + 4X^4$$

   Man kann auch die Reste vermöge $r \to \frac{1}{r}$ abbilden, $0 \to 0$, hat die NR $\frac{\text{const.}}{r}$

8. Bei $p = 7$ gehts auch so: $v = \begin{pmatrix} 0 & r & n \\ 0 & \frac{4}{r} & \frac{1}{n} \end{pmatrix}$ bei Gerade $= \{124\} + \text{const.}$

9. $$\prod(r - d) = \begin{cases} 0 \\ 1 \\ 2 \end{cases}$$

10. $\mathfrak{K}\overline{\mathfrak{K}} = a + bi$ ergibt immer „Steinersysteme“ einer gewissn. Art
    Arbeitstitel: Die Geometrien mit p Punkten

43/44

$$p = 2q + 1$$

1. $\mathfrak{G}$ sei eine max Gruppe mit Gr $\mathfrak{G} = p = 2q + 1$, q Primzahl ≥ 3, $\mathfrak{G}$ zwei Klassen, also $\mathfrak{G}_1 = \mathfrak{U}$, $\mathfrak{G}_2 = \mathfrak{V}$ vom Index p. Sei σ ein Autom d. Ord 2 mit $\mathfrak{U}^\sigma = \mathfrak{V}$; sei $\mathfrak{D} = \mathfrak{U}_1\mathfrak{V}$. Dann ist $\mathfrak{D} = \mathfrak{D}^\sigma$, $\mathfrak{U}$ hat Translgr 1, $2q$; $\mathfrak{V}$ hat $q + 1$, q. σ zentralisiere $\mathfrak{N}_1$, wo $\mathfrak{N} = N\mathfrak{P}$, $P^\sigma = P^{-1}$.

2. Es ist sogar $D^\sigma = D$ f. jedes $D \in \mathfrak{D}$. Denn $\mathfrak{D}$ hat Translgen $1, q, q$; $\mathfrak{D}$ wird durch jeden q Konst. treu dargestellt, ist also $\simeq$ Gruppe des Grades q. σ macht einen Autom der Ord 1 oder 2 auf $\mathfrak{D}$, der eine q-Sylowgr elementwes fest lässt. Also Ord $\sigma = 1$ auf $\mathfrak{D}$.

3. $\mathfrak{D} \cap \mathfrak{D}^P = 1$; denn $(P^{-1}DP)^\sigma = P^1 DP^{-1} \neq P^{-1}DP$. Daher

$$\begin{aligned} |\mathfrak{D}|^2 &\leq |\mathfrak{G}| = |\mathfrak{D}| \cdot p(q+1) \\ |\mathfrak{D}| &\leq p(q+1) = (2q+1)(q+1) = 2q^2 + 3q + 1 \\ q \big| |\mathfrak{D}| \to |\mathfrak{D}| &\leq 2q^2 + 3q \\ |\mathfrak{D}| &= q \cdot m, \quad m \leq 2q+3 \end{aligned}$$

4. $\mathfrak{D}$ ist auflösbar, $|\mathfrak{D}| = qm$, $m \big| p-1$.
Bew: Sonst $q(q-1) \underset{\text{echt}}{\Big|} |\mathfrak{D}|$, $q-1 \underset{\text{echt}}{\Big|} m \underset{=}{\leq} 2q-2+5[; m] \ = 2(q-1)+\delta$

Wenn $q-1 \big| \delta$, $1 \leq \delta \leq 5$, so $q-1 = 1, 2$, $q = 3 \to$

$$\left.\begin{array}{ll} \text{Konst} & q \\ \text{Konst} & q+1 \end{array}\right\}$$

auflösb.
Wenn $\delta \leq 0$, ist $m = 2q-2$, da $q-1$ echt $\big| m$
$|\mathfrak{D}| = qm = q(q-1) \cdot 2$ Ind $\mathcal{N}\!sq$ in $\mathfrak{D}$ ist $\big| 2(q-1)$ und $\equiv 1 \mod q$ also $= 1, \underbrace{q+1, 2}_{\text{zu groß}} q+1, \ldots$
Also q-Sylowgr $\lhd \mathfrak{D}$, $\mathfrak{D}$ auflösbar; $|\mathfrak{D}| = qm$, $m | q-1$

5. Es ist $|\mathfrak{D}| = 2q$; $|\mathfrak{G}| = p(q+1)q \cdot 2 = p(p-1)\frac{p+1}{2}$. Denn $|\mathfrak{G}| = p(q+1) \cdot q \cdot m$, $m \big| q-1$
Die Ord des p-Syl- $\mathcal{N}\!s$ ist ungerade; da Klassenz $\mathfrak{G} > 1$, sonst ist sie pq. Daher

$$\text{Index } \mathcal{N}\!sp = \begin{cases} \equiv 1(p) \\ (q+1) \cdot m \end{cases}$$

$$\begin{aligned} (2q+2)m &\equiv 2(p) \\ 1 \cdot m &\equiv 2(p) \end{aligned}$$

mit $m \big| q-1$ folgt $m = 2$; $|\mathfrak{D}| = 2q$.

6. Ist der q-Konst. von $\mathfrak{V}$ nicht treu, so ist $p = 7$.
Bew: Dann enthält $\mathfrak{V}$ einen reg NT $\mathfrak{H}$ des $q+1$ Konst; dieser Konst. ist 2-trans, also [$\mathfrak{H}$ reg, da $\mathfrak{G}_0 \in \mathfrak{V} \cap \mathfrak{G}_1 = \mathfrak{D}$ und 2-Konst. $\mathfrak{D}$ treu]. $\mathfrak{H}$ elementar abels, $|\mathfrak{H}| = q+1 = r^\lambda = 2^\lambda$. Nun ist

$$\left.\begin{array}{l} q = 2^\lambda - 1 \\ p = 2q+1 = 2^{\lambda+1} - 1 \end{array}\right\} \text{ also } \begin{array}{c} \lambda \\ \lambda+1 \end{array} \text{ Primzahl}, \quad \lambda = 2, \ p = 7$$

7. Ist der q-Konst von $\mathfrak{V}$ treu, so ist er 2-tra, mit $p = 7, 11$. Denn sonst, wenn $\mathfrak{V}$ nicht 2-tra, ist $\mathfrak{Q} \lhd \mathfrak{V}$, $\mathfrak{W}$, so läßt 1 fest, $\mathfrak{V} < \mathfrak{G}_1$, $\mathfrak{V} = \mathfrak{G}_1$. Also $\mathfrak{V}$ 2-tra. Nun ist $q(q-1)\big||q$- Konst $\mathfrak{V}| = |\mathfrak{V}| = 2q(q+1)$, $q-1\big|2q+2$, $q-1\big|4 \quad q = 3, 5$ $p = 7, 11$.
Zusammenfassung S. 44-46:

8. Ist $\mathfrak{G}$ eine transitive Gr des Grades $p = 2q+1$, $q \geq 3$, mit 2 Klassen, so ist $\mathfrak{G}$ maximal und (*) $p = 7$ oder 11; $|\mathfrak{G}| = p(p-1)\frac{p+1}{2}$.
$[- - -]$ Maximalität ist entbehrlich: In jeder echten Untergr $\mathfrak{H}$ von $\mathfrak{G}$ wäre $|\mathfrak{H}| = pq(q+1)$ Index $\not\backslash p = (q+1) \not\equiv 1(p)$ Geht nicht. Der Beweis zeigt
(*) Es gibt <u>nur maximale</u> mit Klassenzahl 2 im Fall $p = 2q+1$

1958 p=2q+1

9. Da der konjugierende Komplex $\mathfrak{K}$ eindeutig bestimmt ist, liegen alle Gr. mit Grad $p = 2q+1$ mit $h \geq 2$ in einer und derselben maximalen. Da diese nach 8 keine Ugr mit $h \geq 2$ hat, folgt:

10. Hauptsatz über $p = 2q+1$: Es gibt nur 2 Gruppen vom Grad $p = 2q+1$, q Primzahl, die trans. sind und mehr als eine Klasse konj. Untergruppen vom Index p enthalten: $SL(3,2)$ und $PSL(2,11)$ mit der Ordnung $7 \cdot 6 \cdot 4 = 168, \quad 11 \cdot 10 \cdot 6 = 660$.
Denn $SL(3,2)$ enthält zwei nicht konj 7-Sylow-Komplemente der Ord 24 und $PSL(2,11)$ zwei 11-Sylowkompl. der Ord 60, nämlich $\mathfrak{A}_5$

11. Entsprechendes geht wohl bei $p = 2^\alpha q + 1$, $q \equiv 1(2^\alpha)$ [und vielleicht allgemeiner bei $p = mq+1$, $q \equiv 1(m)$; genau in diesem Fall ist $p = q + l$ mit $p-1\big|ql$ lösbar].

12. p beliebig: $i = \frac{kl}{p-1}$, $k + l = p \rightarrow$ genau eine der Zahlen k, l hat $\mod p$ ungerade Ordnung.
z.B. $k = \alpha a$, $l = \beta b$, $ab = p-1$, so haben α & β ung. ord. $\mod p$
Bew $42_{(4a)}$

Kernfreie Komplemente abelscher Gruppen

1. Ständige Vorauss. Sei $\mathfrak{R} < \mathfrak{G}$, $\mathfrak{U}$ und $\mathfrak{V}$ seien zwei nicht konjugierte, kernfreie* genaue Komplemente von $\mathfrak{R}$ in $\mathfrak{G}$; sei $\mathfrak{UV} \neq \mathfrak{G}$.
* dh. $\bigcap\limits_G \mathfrak{U}^G = \bigcap\limits_G \mathfrak{V}^G = 1$. Sei $\mathfrak{R}$ abelsch.

Sei $\left.\begin{matrix}\overline{\mathfrak{G}} \\ \overline{\overline{\mathfrak{G}}}\end{matrix}\right\}$ die Permut.-Darstellung (etwa rechts) von $\mathfrak{G}$ nach $\mathfrak{U}$ bezw $\mathfrak{V}$, beide mit $\mathfrak{R}$ als Vertretern.

Wegen $\mathfrak{U}\mathfrak{V} \neq \mathfrak{G}$ ist $\overline{\mathfrak{V}} \neq$ tra. Seien $\mathfrak{K}, \cdots \subset \mathfrak{R}$ die Transsyst. von $\overline{\mathfrak{V}}$. Dann ist $\mathfrak{U}\mathfrak{K} = \mathfrak{K}\mathfrak{V}, \ldots,$ und $\overline{\overline{\mathfrak{U}}}$ hat die Trans. $\mathfrak{K}^{(-1)}, \ldots.$ Sei $\overline{\mathfrak{V}}$ die maximale Untergr. von $\mathfrak{S}^{\mathfrak{R}}$, die die Trans. $\mathfrak{K}, ..$ hat und mit $\overline{\mathfrak{R}}$ vertauschbar ist; nenne $\overline{\mathfrak{G}}$ schlechthin maximal, wenn es nicht möglich ist, $\mathfrak{G}$ so zu $\mathfrak{G}^*$ zu vergrössern, dass es in $\mathfrak{G}^*$ noch kernfreie Komplemente $\mathfrak{U}^*, \mathfrak{V}^*$ gibt mit $\mathfrak{U}^*\mathfrak{V}^* \neq \mathfrak{G}^*$.

2. Dann ist mit $\pi = \binom{R}{R^{-1}}$: $\pi\overline{\overline{\mathfrak{U}}}\pi = \overline{\mathfrak{V}}$. Ferner ist $\overline{\mathfrak{R}} = \overline{\overline{\mathfrak{R}}}$ die reg Darst von $\mathfrak{R}$. Tritt ausserdem neben $\mathfrak{K}$ stets auch $\mathfrak{K}^{(-1)}$ als Trans von $\overline{\mathfrak{V}}$ auf, so ist $\overline{\overline{\mathfrak{U}}} = \overline{\mathfrak{V}}$, daher $\overline{\overline{\mathfrak{G}}} = \overline{\overline{\mathfrak{R}}}\,\overline{\overline{\mathfrak{U}}} = \overline{\mathfrak{R}}\,\overline{\mathfrak{U}} = \overline{\mathfrak{G}}$

Komplemente

3. Da $\mathfrak{R}$ abelsch, $\pi\mathfrak{R}\pi = \mathfrak{R}$, so ist $\pi\overline{\overline{\mathfrak{G}}}\pi = \mathfrak{R}\pi\overline{\overline{\mathfrak{U}}}\pi = \mathfrak{R}\overline{\mathfrak{V}} = \overline{\mathfrak{R}}$; σ bezeichne den Automorphismus von $\mathfrak{G}$ mit $\pi\overline{\overline{\sigma(G)}}\pi = \overline{G}$.

$$\text{Dann} \quad \begin{cases} \sigma(R) = R^{-1} & \text{für } R \in \mathfrak{R} \\ \sigma(\mathfrak{U}) = \mathfrak{V} \end{cases}$$

4. Ist $\mathfrak{R}$ abelsch und ist $\mathfrak{G}$ schlechthin maximal, so ist $\operatorname{Ord}\sigma \big| 4$ und σ^2 ein innerer Autom: $G^{\sigma^2} = G^S,\ S \in \mathfrak{R}$ mit $S^2 \in \mathrm{Ztr}\mathfrak{G}$, also wenn $|\mathrm{Ztr}\mathfrak{G}| \equiv 1(2)$, so $\sigma^2 = 1$. Es gibt genau zwei Klassen.
Bew: σ^2 lässt die Klasse $\mathfrak{U}$ fest, da es nur zwei Klassen gibt (das folgt so: $\pi\overline{\overline{\mathfrak{U}}}\pi = \overline{\mathfrak{V}}$
[*Abschnitt 4 ist mit einem großen Fragezeichen versehen und dem Kommentar:*]
Ist nicht ganz klar: Man muss wohl voraussetzen, dass $\overline{\mathfrak{V}}$ maximal in folgendem Sinn ist: $r\mathfrak{R}$ intransitiv, $\mathfrak{R}\overline{\mathfrak{V}}$ primitiv. Dann ist $\overline{\mathfrak{V}}$ von selbst kernfrei. Offen bleibt vor allem: Entsprechendes für $\mathfrak{R}$ nicht abelsch. Man kommt durch, wenn man voraussetzt, daß auch $\mathfrak{Z} \subset \mathfrak{G}$, wobei $\mathfrak{Z} = \mathcal{Z}s\overline{\mathfrak{R}}$ in $\mathfrak{S}^{\mathfrak{R}}$.

Lineare Abschliessung

1. Die trans. Permut-Darstellung von $\mathfrak{G}$ nach $\mathfrak{U}$ und nach $\mathfrak{V}$ sind genau dann fremd (bzglich der irred. Darstellgen $\neq 1$), wenn
$|\mathfrak{G} : \mathfrak{U} \cap \mathfrak{V}| = |\mathfrak{G} : \mathfrak{U}| \cdot |\mathfrak{G} : \mathfrak{V}|$, dh. $\mathfrak{U}\mathfrak{V} = \mathfrak{G}$, dh. $\mathfrak{U}$ noch trans. in der Darstellung nach $\mathfrak{V}$.
Bew: Dann ist das Kroneckerprod noch transitiv, dh: $\sum \chi(G)\psi(G) = g$.

2. Def: Eine Permgr. $\mathfrak{G}$ heißt linear vollstdg, wenn (nach Darstellung durch Permut-Matrizen) jede Permutation die sich als Linearverbdg von $G_1, \ldots, G_s \in \mathfrak{G}$ darstellen lässt, auch zu $\mathfrak{G}$ gehört.

3. Eine Permgr auf Ω heiße maximal, wenn jede umfassende Permgr. mit weniger Matrizen vertauschbar ist, d.h. z.B. ist $\mathfrak{G}$ maximal intra, oder maximal nur einfach tra.

4. Jede maximale PGr ist linear abgeschlossen.

50/51

5. Def: Ist $\mathfrak{G}$ eine Permgr, so sei die lineare Abschließung $\overline{\mathfrak{G}}$ von $\mathfrak{G}$ die Menge aller Linearverbdgen der Perm-Matr. von $\mathfrak{G}$, die selbst Perm Matr sind.

6. [Jede abgeschlossene oder maximale PGr enthält die lineare Abschl. jeder Untergr.] Maximal = linear abgeschlossen

7. Hat $\mathfrak{G}$ zwei Konstituenten $\mathfrak{G} = \mathfrak{A}\big|\mathfrak{B}$ derart, daß die Darst $\mathfrak{A}$ und $\mathfrak{B}$ fremd sind (dh. $\mathfrak{A}_i \cdot \mathfrak{B}_j = \mathfrak{G}$), so enthält $\overline{\mathfrak{G}}$ sowohl $\mathfrak{A}\big|1$ wie $1\big|\mathfrak{B}$ (also $\mathfrak{A} \times \mathfrak{B}$). Bew: Burnside's lineare Unabh. der irred Darstellungen.

8. Die lineare Abschliessung einer 2-tra Gruppe ist die symmetrische Gruppe. Die Abschl. einer halbreg Gruppe ist diese selbst.

51/52

Noch Lineare Abschließung $\mathfrak{G} \to \overline{\mathfrak{G}}$

9. $(\overline{\mathfrak{G}})_1$ hat die gleichen Transsysteme wie $\mathfrak{G}_1$ (wegen Vertauschbarkeit mit den V_i).

10. Ansatz zum Beweis des Satzes von der 2-Tra der Gr vom Grad p: Man braucht nur zu zeigen, dass die Gruppe $\mathfrak{G}_f$ der Ord pf, $f < p-1$ linear abgeschlossen ist.

11. Hat $\mathfrak{G}$ einen treuen regul. Konstituenten. so ist $\overline{\mathfrak{G}} = \mathfrak{G}$.

12. Man sollte auch die monomiale lin. Abschließung betrachten.

13. $\mathfrak{U}, \mathfrak{V}$ erzeugen genau dann äquivalente Perm.-Darstellungen von $\mathfrak{G}$, wenn für jede Ähnlichkeitsklasse $\mathfrak{K}$ von $\mathfrak{G}$ gilt: $|\mathfrak{U} \cap \mathfrak{K}| = |\mathfrak{V} \cap \mathfrak{K}|$

52/53

Lin Abschließung, Konjugiertheit

14. Notwendig für Konjugiertheit zweier Vertretergruppen $\mathfrak{U}, \mathfrak{V}$ nach einem Normalteiler $\mathfrak{N}$ ist: $U \equiv V(\ \mathfrak{N}) \to U$ zentralisiert ebenso viele Elemente von $\mathfrak{N}$ wie V. Es muss ja sogar $U = V^N$ sein.

15. Enthält eine tra Gr. $\mathfrak{G}$ auf Ω eine Untergr $\mathfrak{H}$ mit $\Gamma^{\mathfrak{H}} = \Gamma$, $\Delta^{\mathfrak{H}} = \Delta$, $\Gamma + \Delta = \Omega$ derart dass für $\gamma \in \Gamma$ stets $\mathfrak{H}_\gamma$ noch tra auf jedem tra Konst. von $\mathfrak{H}$ auf Δ ist, so kann man die Konstituenten von $\mathfrak{H}$ auf Γ zu $\mathfrak{G}$ hinzunehmen, ohne dass sich die Anzahl der Transs. von $\mathfrak{G}_1$ ändert.

16. z.B: Jeder Grad eines Trans von $\mathfrak{H}$ in Γ sei teilerfremd zu den Graden der Trans $\cdot \quad \cdot$ in Δ.

17. Ist $\mathfrak{G}$ tra und gibt es $\mathfrak{H} < \mathfrak{G}$ mit $\mathfrak{H}$: Insgesamt 2 Trasysteme Γ, Δ mit teilerfremden Graden und $\Gamma + \Delta = \Omega$, so ist $\mathfrak{G}$ 2-tra.

18. Ist die Abschließung einer $\begin{matrix} p\text{-Gruppe} \\ \text{Sylow "} \end{matrix}$ eine $\begin{matrix} p\text{-Gruppe} \\ \text{Sylow "} \end{matrix}$?

19. Klar ist: $|\mathfrak{G}^{(2)}|$ gerade $\iff$ $|\mathfrak{G}|$ gerade

Gruppen vom Gr. p
Carmichael
p.239

Grad $5p$

J.A. Todd, Proc Cambridge Ph. Soe. 48 (1952) gibt ein Beispiel einer pri Permgr. G des Grades $5 \cdot 11$, die 9 transitive Konstituenten von G_1 besitzt. $|G| = 660$.

Gr $\mathfrak{G} = p$

1. Hat $\mathfrak{G}$ zwei Klassen und ist daraus $\mathfrak{U}, \mathfrak{V}$ konsistent gewählt [dh. $\mathcal{N}\mathfrak{s}\mathfrak{P}$ gleichen Durchschnitt mit $\mathfrak{V}$ wie mit $\mathfrak{U}$, $= \mathfrak{F}$], so ist, wenn die Translängen k, l sind $(kl \equiv 0 \quad (p-1), k + l = p)$, der Index $|\mathfrak{U} : \underbrace{\mathfrak{U} \cap \mathfrak{V}}_{\mathfrak{d}}| = \begin{cases} k \\ l \end{cases}$, und zwar $\equiv 1 \mod |\mathfrak{F}|$.
NB: Über spezielle Gr. vom Grad p: Fryer (?), Canad, J.M. 7(1955), ∼30 [24-34]

2. Bei $p - 1 = 2^\alpha q^\beta$ ist, wenn $h > 1$, $f = q^{\cdot\cdot}$, also $|\mathfrak{U} : \mathfrak{d}| = \begin{cases} k \\ l \end{cases} \equiv 1 \mod q$, also $\not\equiv 0(q)$

3. Jede schlechthin maximale (bezgl $h > 1$) Gruppe $\mathfrak{G}$ hat nur noch eine äussere Autom-Gr. d. Ord. 2. Denn sonst könnte man $\mathfrak{G}^* = \mathfrak{G} \cdot \mathfrak{F}_1$ bilden, mit $\mathfrak{F}_1 =$ die Untergr. von $(\mathcal{N}\mathfrak{s}\mathfrak{P})_1$ in $\mathfrak{S}^p$, die die ungeraden äuss. Autom. von $\overline{\mathfrak{G}}$ liefert und $\mathfrak{U}\mathfrak{V}$ fest lässt, dh. den Durchschnitt $\mathcal{N}\mathfrak{s}\mathfrak{P}$. Es wäre $\mathfrak{U}^* = \mathfrak{U}\mathfrak{F}_1$, $\mathfrak{V}^* = \mathfrak{V}\mathfrak{F}_1$, also $\mathfrak{U}^*$ nicht konj zu $\mathfrak{V}^*$ in $\mathfrak{G}^*$. Neben $\mathfrak{K}$ ist auch $\mathfrak{K}^{\mathfrak{F}_1}$ ein konjug. Komplex für $\mathfrak{U}, \mathfrak{V}$; also ist $\mathfrak{K}^{\mathfrak{F}_1} = \mathfrak{K}$.

Gr $\mathfrak{G} = p$, $h > 1$

4. Ist $\mathfrak{G} = \mathfrak{G}(\mathfrak{K})$ die max Gruppe in der der konjug. Komplex $\mathfrak{K}$ auftritt: $\mathfrak{U}\mathfrak{K} = \mathfrak{K}\mathfrak{V}$, ($\mathfrak{U}$, $\mathfrak{V}$ konsistent), so hat $\mathfrak{G}$ keinen ungeraden äuss Autom. Denn ein solcher σ könnte gewählt werden, dass er $\mathfrak{F} = \mathfrak{U} \cap \mathcal{N}\mathfrak{P} = \ldots$ in sich überführt, also wird er $\mathfrak{U}$ in sich überf. (da Klasse und $\mathfrak{F}$ fest), ebenso $\mathfrak{V}$, es wäre also $\mathfrak{U}\mathfrak{K}^\sigma = \mathfrak{K}^\sigma\mathfrak{P}$, daher $\mathfrak{K}^\sigma = \mathfrak{K}$; dann aber gehört $\sigma = S$ schon zu $\mathfrak{G}(\mathfrak{K})$, da $S\mathfrak{K} = \mathfrak{K}S$.

5. In $\mathfrak{G}(\mathfrak{K})$ hat $\mathfrak{P}$ genau diejenigen unger. Autom., die $\mathfrak{K}$ in sich überführen. Denn $\mathfrak{G}(\mathfrak{K})$ $\mathfrak{P}$ grösste mit $\overline{\mathfrak{P}}$ vertauschbare Gruppe, die $\mathfrak{K}$ nur in sich permutiert.

6. Allgemeine Def: $\mathfrak{K} \subset \mathfrak{P} \to \mathfrak{G}(\mathfrak{K}) = \overline{\mathfrak{P}} \cdot \overline{\mathfrak{M}}$, wo $\overline{\mathfrak{M}}$ die grösste Permgruppe auf $\mathfrak{P}$ ist, die 1) mit $\overline{\mathfrak{P}}$ (= Reg. Darst von $\mathfrak{P}$) vertauschbar ist und 2) $\mathfrak{K}$ in sich überführt.

Grad p

Besser als 6:

7. Def: Sei K eine Menge * von $\overbrace{\text{Zahlen mod } p}^{\Omega}$; $1 < |K| < p-1$; $0 \notin K$, und zwar besitze K einen Multiplikator $\mu \neq 1$. Sei M die Menge der Multipl. Sei $\mathfrak{P}$ die Gruppe $\binom{\nu}{\nu+a}$ und $\mathfrak{V}(K)$ die größte Untergr von $\mathfrak{S}^\Omega$, die mit $\mathfrak{P}$ vertauschbar ist und K in sich überführt. Sei $\mathfrak{G}$(K)= $\mathfrak{P} \cdot \mathfrak{V}(\mathfrak{K})$
* Es interessiert nur der Fall $K \neq -K$

In $\mathfrak{G} = \mathfrak{G}(K)$ gilt:

8. $\mathcal{N}\mathfrak{P} \cap \mathfrak{V}$ enthält $\binom{\mu}{\mu\nu} = \binom{0\cdot\cdot}{0,\cdot\cdot}$ also lässt $\mathcal{N}\mathfrak{P} \cap \mathfrak{V}$ stets 0 fest: $\mathcal{N}\mathfrak{P} \cap \mathfrak{V} = \mathcal{N}\mathfrak{P} \cap \mathfrak{G}_0$; es ist $\mathfrak{G}_0\mathfrak{K} = \mathfrak{K}\mathfrak{V}$, wo $\mathfrak{K} = \{P^K\}$, $k \in K$

9. Ist $\mathfrak{V} = \mathfrak{V}_0$, so $\mathfrak{G}(K)$ auflösbar, $< \mathcal{N}\mathfrak{P}$.
Ist $\mathfrak{V} \neq \mathfrak{V}_0$, so $h[\mathfrak{G}(K)] \geq 2$, $\mathfrak{G} \neq \begin{matrix}\mathfrak{A}^\Omega \\ \mathfrak{S}^\Omega\end{matrix}$; (genauer $\mathfrak{M} = (\mathfrak{G}_0)^G$, sogar $\neq \mathfrak{G}_0^S$, $S \in \mathfrak{S}^\Omega$).

10. Stets ist $f[= |\mathfrak{F}|$, wo $\overbrace{\mathcal{N}\mathfrak{P}}^{\mathfrak{N}}$ in $\mathfrak{G} = \mathfrak{P} \cdot \mathfrak{F}]$ gleich der Anzahl der Multiplik. von K; genauer: $\mathfrak{N}_0 = \mathfrak{N} \cap \mathfrak{V} = \binom{\nu}{\mu\nu}$, alle $\mu \in M$.

11. Jeder Autom. von $\mathfrak{G}$, der die Klassen von $\mathfrak{G}_0$ und $\mathfrak{V}$ fest lässt, kann durch ein $S \in (\mathfrak{NP})_1$ dargestellt werden, das lässt $\mathfrak{G}_0$ und $\mathfrak{V}$ fest, also auch $\mathfrak{K} = \{P^K\}$; daher $S \in \mathfrak{V}$, also σ innerer Autom. Daher hat bei

$$\begin{cases} \mathfrak{V} \neq \mathfrak{G}_0 & \text{die äussere Autom Gr von } \mathfrak{G} \text{ die Ord 2.} \\ = & \text{die äussere Autom Gr von } \mathfrak{G} \text{ die Ord } \frac{p-1}{|M|} \end{cases}$$

12. $\mathfrak{G}$ vom Grad p beliebig $\rightarrow$ Jeder Komplex $\mathfrak{K}$, der in einer Vergrößerung $\mathfrak{G}^*$ von $\mathfrak{G}$ als konjugierender Komplex vorkommt: $\mathfrak{U}^*\mathfrak{K} = \mathfrak{K}\mathfrak{V}$, kommt schon in $\mathfrak{G}$ vor, und zwar ist $\mathfrak{U}\mathfrak{K} = \mathfrak{K}\mathfrak{V}$ mit $\mathfrak{U} = \mathfrak{U}^* \cap \mathfrak{G}$, $\mathfrak{V} = \mathfrak{V}^* \cap \mathfrak{G}$. [Dann $\mathfrak{U}^*\mathfrak{K} \cap \mathfrak{G} = \mathfrak{U}\mathfrak{K}$.]

13. $K_1 \neq K_2 \rightarrow \mathfrak{G}_1 \neq \mathfrak{G}_2$ oder auflösbar.
Denn $\mathfrak{G}_1 = \mathfrak{G}_2$ hat nur einen äuss. Autom σ der Ord 2, der müsste $\mathfrak{U}$ sowohl in $\mathfrak{V}_1$ wie in $\mathfrak{V}_2$ überführen, und die haben verschiedene Transitivitätssysteme.

14. $\mathfrak{G}(K_1) \leq \mathfrak{G}(K_2) \rightarrow M_1 \subseteq M_2$. Daher M = Multiplikator K. Bew. 10.

15. $K_1 = \rho K_2 \leftrightarrow \mathfrak{G}_1 = \binom{\nu}{\rho\nu}^{-1} \mathfrak{G}_2 \binom{\nu}{\rho\nu}$ wenn die $\mathfrak{G}_\rho$ nicht auflösb. Bew (13)

16. $\mathfrak{G}(K)$ hat Autom d. Ord 2, der $\mathfrak{G}_0$ mit $\mathfrak{V}$ vertauscht, = einziger äuss Automorphismus.

17. Bei der Gr $\mathfrak{G}$ ist mit $T = \sum_{K \in \mathfrak{K}} \overline{D}(K)$

    a) $T\overline{G} = \overline{\overline{G}}T$
    Bew mit $\overline{(K+V)} = K + \overline{\overline{V}}$, das mit $P^\nu G = V^{P\overline{\overline{V}}}$

    und daher bei maximalem $\mathfrak{G}$ zu $\mathfrak{K}$ auch mit $T\Pi = S$.

    b)

$$\begin{aligned} \overline{\mathfrak{G}} = \Pi\overline{\overline{G}}\Pi &= \Pi T\overline{G}T^{-1}\Pi^{-1} \qquad \Pi = \begin{pmatrix} \nu \\ -\nu \end{pmatrix} \\ &= S\overline{G}S^{-1} \end{aligned}$$

    $\Pi T = S$ ist hermitesch, jeder EW$=\begin{cases} k \\ \pm\sqrt{i} \end{cases}$ und macht den Autom σ von 16 auf $\mathfrak{G}$

18. Die Darstellungen $\overline{\mathfrak{G}}$, $\overline{\overline{\mathfrak{G}}}$ sind also stets äquivalent (17a)

19. Es ist

$$\begin{cases} S^{-1} = \frac{1}{i}S - \frac{j}{ik}E \quad k = |\mathfrak{K}| \quad E = (1); \\ S^2 = iI + jE, \end{cases} \qquad S = \begin{pmatrix} \overset{\text{stets } 0}{\downarrow} & \overbrace{\quad\quad\quad}^{K} & & & \\ 0 & 1 & 1 & 1 & 0 \\ 1 & \prime & \prime & & \\ & & & & \\ 1 & & & \vdots & \\ & & & & \end{pmatrix}$$

Also $S\overline{G}S = \overline{\overline{G}}S^2 = i\overline{\overline{G}} + jE$

59/60

20. Jede bei σ feste Perm aus $\mathfrak{G}(K)$ lässt $\frac{1}{2}K$ als Ganzes fest. s. auch 28
Denn $S = \Pi T$ hat Einsen in der Diag. genau an den Stellen $\frac{K}{2}$.

$$\text{Z.B.} \quad \underset{K=2}{P^2} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad ; \quad \Pi P^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{lässt 1 fest.}$$

20a. Die „Fixgruppe“ $\mathfrak{F} = \mathfrak{F}(K)$ bei $G = G^\sigma \in \mathfrak{G}(K)$ besteht genau aus allen Perm., die mit S vertauschbar sind.

21. Im Fall $K \neq -K$ ist genau dann $\mathfrak{G}(K)$ nicht auflösbar, wenn es eine Permutation Z der Ord zwei gibt mit $ZS = SZ$ oder wenn es eine Permut. v S gibt, die $\notin \mathcal{N}\mathfrak{P}$ ist. vgl 22.
Denn σ läßt ein El. d ord 2 in $\mathfrak{G}(K_1)$ fest, und umgekehrt ist $\{Z, \mathfrak{P}\}$ nicht auflösbar, da $K \neq -K$, also $2 \nmid \mathcal{N}\mathfrak{P}$ (10)
Ist $\mathfrak{d} = \mathfrak{U} \cap \mathfrak{V}$ gerade, so gibt es Z der Ord 2 fest bei S
schon in $\mathfrak{d}$.
Lässt σ in $\mathfrak{d}$ kein Element $\neq 1$ fest, so ist $\mathfrak{d}$ abelsch, $D^\sigma = D^{-1}$. – Auch $SZS^{-1} = Z^{-1}$ täte es.

60/61

6.3.58 Grad p

22. Es ist $\mathfrak{G}(K) = S\mathfrak{S}^\Omega S^{-1} \cap \mathfrak{S}^\Omega$.
Denn $\subset$, und $\cdots \cap \cdots \big|_1$ lässt K fest.

[*Abschn. 23. ist durchgestrichen und mit einem Fragezeichen versehen.*]

23. Aus $\mathfrak{G}(K_1) \subseteq \mathfrak{G}(K_2)$ folgt $K_1 = K_2$, wenn $\mathfrak{G}(K_1)$ nicht auflösbar.

24. Ist $\overline{G} = \left(\frac{\nu}{\nu}\right)$, $\overline{\overline{G}} = \left(\frac{\nu}{\overline{\nu}}\right)$, so ist $\overline{(K+\nu)} = K + \overline{\overline{\nu}}$, daher $\overline{\overline{\nu}} = \frac{1}{k}\sum\limits_{\kappa \in K} \overline{(\kappa+\nu)}$;
$k = |K|$. vgl. 46

25. Genau dann ist G fest bei σ, wenn $\overline{\nu} = \overline{\overline{\nu}}$ f. jedes ν, also $k\overline{\nu} = \sum_{\kappa \in K} \overline{(\kappa + \nu)}$ $(\nu = 0, \ldots, p-1)$; Vorausges: $G \in \mathfrak{G}$.
dh $\overline{(K+\rho)} = K + \overline{\rho} \Leftrightarrow G^\sigma = G$ [schreibe $G \in \mathfrak{F}(K) = \mathfrak{F}$]

26. Ist $Z^\sigma = \begin{cases} Z^{-1} \text{ oder} \\ Z, \end{cases}$ und $Z = (\ \rho)(\cdots) \cdot -$, so führt Z $(K - \rho)$ in sich über. Denn die ρ-te Zeile von S enthält $K - \rho$ Einsen.
Z.B. Wenn x beliebig, $Z = x^{1-\rho}$; dh x und x^σ sollen ρ ins selbe überführen:
$\rightarrow$ dann führen sie $K - \rho$ ins selbe über.

Grad p

27. Die Matrix $S = \Pi T$ hat 1 genau wo $\rho + r \in K$ ist. In der Zeile ρ sind also genau die $K - \rho$ mit Einsen besetzt

28. Genau dann gehört eine Permutation $\binom{\nu}{\nu'}$ zur Fixgruppe $\mathfrak{F} = \mathfrak{F}(K)$ von σ in $\mathfrak{G}(K)$, wenn gilt: aus $\lambda + \nu \in K$ folgt stets $\lambda' + \nu' \in K$. (17)

29. Def: $\mathfrak{F}(K) =$ Gruppe der mit $S = S(K)$ vertb. Permut.,
dh. $F = \binom{\nu}{\nu'} \in \mathfrak{F}(K) \leftrightarrow \quad \lambda + \nu \in K \rightarrow \lambda' + \nu' \in K$.

30. Genau dann ist $\mathfrak{G}(K)$ nicht auflösbar, wenn $\mathfrak{F}(K) \neq$ (dh. grösser als) Gruppe M der Multiplikationen $\binom{\nu}{\mu\nu}$; $M =$ Multipl. von K.
Dann liesse σ noch mehr als $(\mathfrak{N}\mathfrak{P})_1$ einzeln fest in auflösb. $\mathfrak{G}'$, so auch ein $P \in \mathfrak{P}$, geht nicht.

31. Ist eine Untergr $\mathfrak{H}$ von $\mathfrak{G}$ bei σ als Ganzes fest und läßt sie die Ziffer ρ fest, so führt sie $K - \rho$ in sich über. (27)

Grad p

32. $\mathfrak{F}(2K)$ macht höchstens solche Permutationen auf K (welches ja stets fest bleibt), die alle Strecken mit Mitten $\in K$ im Ganzen erhalten:
$\frac{K_1+K_2}{2} \in K \ \rightarrow \frac{K_1'+K_2'}{2} \in K$.

33. Setzt man $\delta_\nu = \begin{cases} 0 & \nu \notin K \\ 1 & \nu \in K \end{cases}$, so besteht $\mathfrak{F}(K)$ genau aus den Permutationen $\binom{\nu}{\nu'}$, die $\delta_{K+\lambda}$ ungeändert lassen.
[$\delta_{K+\lambda}$ ist das allg. Element von S].

34. $\mathfrak{F}(K)$ ist linear abgeschlossen (20a)

35. Die Eigenwerte $\tau \neq k$ von T (früher κ genannt) [mit der Eigenschaft $\tau\overline{\tau} = i$] sind insgesamt teilerfremd. Sonst wäre $\mathfrak{q}\big|\tau$, $\mathfrak{q}\big|\overline{\tau}$, daher durch Transform T mittels der Vandermonde-Matrix $V = (\ \varepsilon^{\rho\sigma})$, $|V|^2 = p^\alpha$, auch $\mathfrak{q}\big|$ jede zweireih. Unterdet von T und daher von S; diese nehmen aber u.a den Wert -1 an; $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ist Ausschnitt von S.

63/64

Grad p

36. Eine Permutationsmatrix A gehört genau dann zu $\mathfrak{G}(K)$, wenn $SAS - jE \geq 0$ ($S^2 = iI + jE$). Denn es ist $\mathrm{Sp}(SAS - jE)' \cdot (\quad)$ unabh. von A, also $= \mathrm{Sp}(S^2 - jE)'(\quad) = i^2 p$;

    α) Ist nun $SAS - jE \geq 0$, so sind in jeder Zeile einige Summanden $c \neq 0$ denn sie sind ≥ 0 und haben $\sum c = i$, $\sum c^2 = i^2 = (\sum c)^2$. Also ist in jeder Zeile genau 1 El. $\neq 0$, das ist $= i$
    Ebenso Spalte: $SAS - jE = iB$, B Permutation; $(SA - BS) \cdot S = 0$, $A \in \mathfrak{G}$

    β) Ist umgekehrt $A \in \mathfrak{G}$, so $SAS - jE = i \cdot A^\sigma \geq 0$. Stets ist $SAS^{-1} = \frac{1}{i} SAS - \frac{j}{i} E$.

37. Die Bedingg 36 heisst: $\big((K - \nu) \cap \overline{(K - \lambda)}\big) \geq j$ für alle λ, ν ist n & h für $\binom{\nu}{\nu} \in \mathfrak{G}(K)$.

38. Zusammenfassung: Sei K eine Menge von Zahlen $\mod p$, deren Multiplikator $M \neq 1$ ist und die 0 nicht enthält. Die Gr. $\mathfrak{G}(K) = \mathfrak{P} \cdot \mathfrak{V}$, wo $\mathfrak{V}$ maximal mit $\mathfrak{V}\mathrm{v}\mathfrak{P}$ und $K^{\mathfrak{V}} = K$, ist genau dann $\neq$ aufl., wenn $\mathfrak{F}(K) \neq \binom{\nu}{\mu\nu}$; $\mu \in M$. Dabei ist $\mathfrak{F}(K)$ die Gruppe der Permutationen, die jedes "gute" Paar (ρ, σ) in ein gutes Paar überführt; und (ρ, σ) "gut" heisst $\rho + \sigma \in K$.

64/65

Untergruppen vom Index p

39. Die Anzahl der Klassen konjugierter Untergr. in $\mathfrak{G}$ vom Index p ist gleich der Anzahl derjenigen Homomorphismen $\neq 1$ von $\mathfrak{G}$ in $\mathfrak{S}^p$, bei denen ein fest gewählter p-Sylow-Normalisator $\mathfrak{N}$ von $\mathfrak{G}$ eine fest gewählte Darstellung bekommt. Vor. $p \top |\mathfrak{G}|$.
    Bew: Die "normierten" p-Sylowkompl. $\mathfrak{U}, -$ betrachten, die das Urbild von $\mathfrak{N}_0$ enthalten.

40. Es gilt wohl:

    a) $K_1 \neq K_2 \to \mathfrak{F}(K_1) \cap \mathfrak{F}(K_2) \leq \mathfrak{N}\mathfrak{P}$

b) Jedes $\tilde{\mathfrak{F}} \subset \mathfrak{F}(K_1)$, $\tilde{\mathfrak{F}} \not\subset \mathcal{N}\mathfrak{P}$ ist in genau $h-1$ verschiedenen $\mathfrak{G}(K_\rho)$ enthalten, wenn $\{\mathfrak{P}, \tilde{\mathfrak{F}}\}$ $h+1$ Klassen von Untergr. vom Index p besitzt.

41. Stets ist $h(\mathfrak{G}(K)) \equiv 0(\mod (2))$, wenn $\mathfrak{G}'' \neq 1$.

42. $\mathfrak{U} \cap \mathfrak{V} = \mathfrak{V}_1$ lässt nur eine Ziffer fest, denn $(\mathcal{N}\mathfrak{P})_1 \subset \mathfrak{V}_1$

43. Die $G \in \mathfrak{G}$ mit $G^{-1}S = SG$ sind lin abgeschlossen, da $G^{-1} = G'$.

44. Die Paare $\{\mathfrak{U}_\alpha, \mathfrak{V}_\alpha\}$ mit $\mathfrak{U}_\alpha^\sigma = \mathfrak{V}_\alpha$ und gleichem $|\mathfrak{U}_\alpha \cap \mathfrak{V}_\alpha|$ sind konjugiert in $\mathfrak{G}$: Es gibt Sylowgr von $\mathfrak{G}$, die nur in <u>einem</u> $\mathfrak{U}_\alpha$ vorkommen (wähle geeigneten Teiler von $p-1$).

45. Es gibt genau $\begin{cases} k & \text{Paare } \mathfrak{U}_\alpha^\sigma = \mathfrak{V}_\alpha \text{ mit } |\mathfrak{U}_\alpha \cap \mathfrak{V}_\alpha| = \frac{g_1}{k} \\ \ell & \qquad\quad '' \qquad\qquad\quad = \frac{g_1}{\ell} \end{cases}$
Jede ein Fixelement besitzende Gr der Ord q^β liegt, wenn $q \nmid k$, in mindestens einem $\mathfrak{d}_\alpha = \mathfrak{U}_\alpha \cap \mathfrak{V}_\alpha$ der Ord $\frac{g_1}{k}$; entsprechend für l. Bew 44.

46. Seien $\mathfrak{H}$, $\mathfrak{H}^*$ 2 Untergr vom Index p in $\mathfrak{G}$ (beide $\neq \mathfrak{G}_1$), zugehörig $\mathfrak{K}, \mathfrak{L} \subseteq \mathfrak{P}$. Seien K, Λ die Exponentensätze zu $\mathfrak{K}, \mathfrak{L}$; nenne $i \sim j$, wenn $|i+K\cap\Lambda| = |j+K\cap\Lambda|$. Dann ist $i-j \sim i_G - {}_Gj$, wenn $\binom{i}{i_G}$ die $\mathfrak{H}$ erzeugte Perm, $\binom{j}{{}_Gj}$ die von $\mathfrak{H}^*$ erzeugte. Es ist $(i+K)^G \underset{\text{urspr. Darst.}}{=} i_G + K$, $(j+\Lambda)^G \underset{G}{=} j+1$.
Die Funktion $f(i) = |i+K\cap\Lambda|$ nimmt nur 2 Werte an, und keiner ist $= 0$. vgl. 24

Abgeschlossenen Permut- Gr

Sei $\mathfrak{A}$ abgeschlossen gegenüber Bildung von Linearverbindungen. Nenne $A \in \mathfrak{A}$ unzerlegbar wenn A nicht als Produkt von zwei ziffernfremden Permutationen aus $\mathfrak{A}$ geschrieben werden kann.

1. $\mathfrak{A}$ enthalte keine p-Gruppe mit einem trans Konst einer Länge $> p$. Dann sind je zwei unzerlegbare Elemente P_1, P_2 der Ord p entweder ziffernfremd oder konjugiert in $\{P_1, P_2\}$. Je zwei unzerlegbare Gruppen der Ordnung p sind konjugiert [sogar in $\mathcal{N}\mathfrak{P}$, (wo $\mathfrak{P}$ eine vorgeschriebene Sylow-Obergruppe von $\{P_1, P_2\}$ ist), falls letzteres eine p- Gruppe ist] Bew:

2. Jede p-Gruppe in $\mathfrak{A}$ ist das direkte Produkt der darin enthaltene unzerlegbaren Gr. d. Ord. p.; diese sind paarweise ziffernfremd.

3. $\mathfrak{P}$ [wo $\mathfrak{P}$ eine p-Sylowgr. von $\mathfrak{A}$ ist] ist abgeschlossen.

3. Sind P, Q zwei El der Ord p in $\mathfrak{A}$, sodaß $\{P, Q\}$ kein Transs. d. Lge p^2 hat, so enthält $\mathfrak{A}$ auch die Konstituenten $\{P$ auf Fixmenge von $Q\}$ und umgekehrt

Primitive Gruppen 9.3.58

1. $\mathfrak{G}$ sei eine primitive Gr. des Grades $n < p^2$; sei $|\mathfrak{G}| \equiv 0(p^2)$. Dann ist $\mathfrak{G}$ 2-tra. besser: XIII7
   Für $p \leq 7$**???** schon bei Manning 1919. Erweiterg:: 71(8a); $p \geq 11$ neu
   Bew: OBdA sei $\mathfrak{G}$ abgeschlossen. Sei $\mathfrak{P}$ eine p-Sylowgr. von $\mathfrak{G}$. Nach 67.3 ist der kleinste Grad q, p den ein El d Ord p hat, $\leq \frac{n}{2}$; $q \leq \frac{p}{2}$. $q = 1$ fertig. Nach Manning 1919 ist für eine prim Gruppe vom Grade $n = pq + k$, die ein El. der Ord p vom Grad qp enthält und $\neq \mathfrak{A}_n$, $\mathfrak{S}_n$ ist, für $q > 2$ und $p > 2(q-1)$ stets $k \leq 4(q-1)$. Also bei uns

$$qp \leqq k \leqq 4(q-1), \quad p \leq 4\frac{q-1}{q} < 4, \quad q < 2, \quad \text{geht n[icht]}$$

Fortsetzung 141

Folge:

2. $\mathfrak{G}$ enthalte eine Untergr. vom Index $n < p^2$ und habe eine durch p^2 teilbare ungerade Ord. Dann ist $\mathfrak{G}$ nicht einfach.
   NB:

3. Aus Manning 1919 folgt direkt: $\mathfrak{G}$ pri, $n \leq \frac{p(p+5)}{2}$, $p^3 | g \to \mathfrak{A}^\Omega \leq \mathfrak{G}$

Abgeschlossenen Gruppen.

1. Wenn man aus Voraussetzungen, die gegen Abschließung unempfindlich sind, Behauptungen über die Transitivitäts-Systeme von $\mathfrak{G}_1$ folgern will, so darf man beim Beweis $\mathfrak{G}$ als abgeschlossen annehmen.

9.3.58

2. $\mathfrak{U} \leq \mathfrak{G}$ auf Ω heisst zerlegbar, wenn $\Omega = \Gamma + \Delta$ mit $\mathfrak{U} \leq \mathfrak{U}^\Gamma \cdot \mathfrak{U}^\Delta \leq \mathfrak{G}$, $\mathfrak{U}^\Gamma \neq 1$, $\mathfrak{U}^\Delta \neq 1$.

3. Jede maximale in $\mathfrak{G}$ unzerlegbare Untergruppe $\mathfrak{M} \leq \mathfrak{H}$ einer bel. PGr $\mathfrak{H} \leq \mathfrak{G}$ ist normal in $\mathfrak{H}$. (trivial, wenn $\mathfrak{H}$ unzerlegbar.)
   Bew: Sei $\mathfrak{H}_\alpha \leqq \mathfrak{H}_\alpha^{\Gamma_1} \times \mathfrak{H}_\alpha^{\Gamma_2} \times \cdots \times \mathfrak{H}_\alpha^{\Gamma_S}$ eine möglichst feine Zerlgg von $\mathfrak{H}$ in ziffernfremde Untergr. in $\mathfrak{G}$. Dann ist $\mathfrak{M} \leq \overline{\mathfrak{M}^{\Gamma_1} \cdot \cdots \cdot \mathfrak{M}^{\Gamma_s}} \leq \mathfrak{G}$ also nur ein $\mathfrak{M}^{\Gamma_\sigma} \neq 1$ wegen Unzerlegbarkeit; $\mathfrak{M} \leq \mathfrak{H}^{\Gamma_\sigma}$, und da das unzerlegbar ist, ist $\mathfrak{M} = \mathfrak{H}^{\Gamma_\sigma} \lhd \mathfrak{H}$ [$\lhd$ hier: = „normal unter“].

4. Eine in $\mathfrak{G}$ unzerlegbare Gruppe $\mathfrak{M} \leq \mathfrak{H}$, die bei geg $\mathfrak{H}$, $\mathfrak{G}$ größtmögliche Ordnung hat, ist normal in jeder $\mathfrak{H}^S$, in der $\mathfrak{M}$ liegt
   Denn $\mathfrak{M}^{S^{-1}} \subset \mathfrak{H}$ unzerlegb. max.

5. Ist $\mathfrak{G}$ transitiv und $\overline{\mathfrak{G}_1}$ (lin Abschließung) zerlegbar, so ist $\mathfrak{G}$ imprimitiv. Dann sei $\mathfrak{M} \leq \overline{\mathfrak{G}_1}$ maximal-Ordnung unzerlegbar in $\mathfrak{G}$. Dann $\mathfrak{M} \lhd \overline{\mathfrak{G}_\alpha}$ für ein $\alpha > 1$ nach 4. $\mathfrak{M} \lhd \{\overline{\mathfrak{G}_1}, \overline{\mathfrak{G}_2}\}$. aber $\mathfrak{M}$ intra $\to \{\mathfrak{G}_1, \mathfrak{G}_2\}_\alpha$ intra
Anderer Bew 72.3

6. Ist $\Omega = \Gamma + \Delta$, $-\Gamma^{\mathfrak{G}} = \Gamma$, $\Delta^{\mathfrak{G}} = \Delta$ und sind alle Konstituenten von $\mathfrak{G}$ auf Γ primitiv, und ist $\mathfrak{G}^\Delta \neq 1$, so ist $\mathfrak{G}^\Delta$ treu, oder die Abschließg $\overline{\mathfrak{G}}$ von $\mathfrak{G}$ ist zerlegbar.
oder: Sonst wähle Γ so klein wie möglich. Dann ist der NT von $\mathfrak{G}$, der Δ ziffernweise fest läßt, auf jedem tra Konst von Γ noch transitiv, also zerfällt $\overline{\mathfrak{G}}$ wegen Abgeschlossenheit.

7. Ist $\mathfrak{G}$ uniprimitiv, so ist jeder tra Konstituent von $\mathfrak{G}_1$ treu, dessen komplementärer Konstituent nur primitive tra Konst enthält (Manning 1927).
Bew: (4)(5)(6) Anderer Beweis 72.2

7'. In einer uniprimitiven $\mathfrak{G}$ sind alle impri Konst von $\mathfrak{G}_1$ zusammengenommen treu. Sind keine da, so ist jeder primitive Konst. von $\mathfrak{G}_1$ treu. (Manning S 821)

8. Sind in einer Gr., deren Abschließung unzerlegbar ist, alle Konst primitiv, ausser evtl denen auf Δ, und ist $\mathfrak{G}^\Delta \neq 1$, so ist $\mathfrak{G}^\Delta$ treu.

8a. Damit 68.1 auf $n < 2p^2$ erweitern: $p^3 \big| |\mathfrak{G}| \to \mathfrak{G}$ 2-tra wenn pri. Hierzu Manning 1911, 1919
Beweis: Im tra Konst des Grades p^2 eine intra Ugr vom Index p betrachten. Ausdehnung auf $n < p^3$ mit ($\varphi(\mathfrak{P})$? (s. 11)

9. Besitzt $\mathfrak{G}$ einen NT, der auf mindestens einem trans Konst von $\mathfrak{G}$ transitiv ist und auf den übrigen $= 1$ ist, so zerfällt $\overline{\mathfrak{G}}$
Genauer:

10. Besitzt $\mathfrak{G}$ eine Ugr, die auf einigen tra Konst von $\mathfrak{G}$ tra ist und auf jedem anderen wenigstens eine Ziffer fest läßt, so ferfällt $\mathfrak{G}$ entsprechend.

11. Die Gruppe $\overset{(pppp)}{(ppp)}$ hat einen Konst vom Grad $3p^{2\,4p^2}$, in der jede Untergr. d. Ord p^2 einen trans. Konst. vom Grade p^2 besitzt.
Bew: Bei ppp suche 3 Pkte in der proj. Ebene über $K(p)$, die nicht auf einer Geraden liegen; bei $(pppp)$ 4 Geraden im Raum ohne gemeinsame Treffgerade.

Primitive Gr.

1. Ist $\mathfrak{G}$ primitiv, so hat jeder längste trans Konst. von $\mathfrak{G}_1$ mit jedem anderen eine Darstellg gemeinsam. Sonst wäre der Träger des ersten auch Trans von $\mathfrak{G}_\alpha$, wo α im Träger des zweiten.

2. Hieraus folgt unmittelbar der Satz von Manning 1927 (70.7) über die Entbehrlichkeit primitiver Konst. bezgl. treuer Darst.

3. Ebenso folgt der Satz 70.5: Zerfällt $\mathfrak{G}_1 = \mathfrak{A} \times \mathfrak{B}$, so kommt keine irred Darst $\neq 1$ v. $\mathfrak{G}_1$ auf Γ und Δ vor, in ihr müsste $\mathfrak{A} \to 1$ und $\mathfrak{B} \to 1$ sein, also $\mathfrak{G}_1 \to 1$. Also ist jeder Konst. von $\mathfrak{G}_1$ auf Γ zu jedem auf Δ fremd, insbesondere ist ein längster Konst vor $\mathfrak{G}_1$ zu einem anderen Konst. fremd; nun 72.1.

4. $\mathfrak{G}$ tra, $\geq j$ mit genau zwei Transsys; diese teilerfremde Länge, $\to \mathfrak{G}$ 2-tra. Bew: mit Abschliessung.

Abschließung von Perm-Gr.

1. Ist $\mathfrak{G}$ tra und $\overline{\mathfrak{G}}$ die abgeschlossene Hülle von $\mathfrak{G}$, so haben $\mathfrak{G}$ und $\overline{\mathfrak{G}}$ die gleichen Imprimitivitätssysteme.
   Vollständiger: 2 Also: Ist $\overline{\mathfrak{G}}$ pri, so auch $\mathfrak{G}$.
   Bew: Sei Δ Imprsyst von $\mathfrak{G}$; $\alpha \in \Delta$; $\overline{G} = \binom{\alpha \cdots}{\beta \ldots}, \beta \in \Delta$. Wähle $G = \binom{\alpha \ \cdots}{\beta \ \ldots} \in \mathfrak{G}$, dann $\overline{G} G^{-1} \in \overline{\mathfrak{G}_\alpha}$. Da $\mathfrak{G}_\alpha$ Δ fest lässt und $\overline{\mathfrak{G}_\alpha}$ die gleichen Transs. hat, ist auch ${}_\Delta\overline{\mathfrak{G}_1} = \Delta$, also $\Delta^{\overline{G} G^{-1}} = \Delta$, $\Delta^{\overline{G}} = \Delta^G = \Delta$.
   Anwendung der Abschließung: 140
   Ebenso beweist man:

2. Permutiert $\mathfrak{G}$ $\Delta_1, \Delta_2, \cdots, \Delta_S$ nur unter sich, und ist $\Delta_i \cap \Delta_j = \emptyset$, so permutiert $\overline{\mathfrak{G}}$ $\Delta_1, \Delta_2, \cdots, \Delta_S$ nur unter sich.
   Dh die Gruppen zwischen $\mathfrak{G}$ und $\mathfrak{G}_\alpha$ entsprechen (1,1) denen zwischen $\overline{\mathfrak{G}}$ und $\overline{\mathfrak{G}_\alpha}$.

3. $\overline{\mathfrak{G}}$ ist die größte PGr $\overline{\mathfrak{G}} \geq \mathfrak{G}$ mit den beiden Eigensch:

   a) Jedes Transs. von $\mathfrak{G}$ ist eins von $\overline{\mathfrak{G}}$

   b) Jedes Transs. von $\mathfrak{G}_\alpha$ ist eins von $(\overline{\mathfrak{G}})_\alpha$ f. jedes α.
      Beim Nachprüfen braucht man aus jedem Trans von $\mathfrak{G}$ nur ein α zu nehmen.

   Bew durch Betrachtung der vertauschbaren Matrizen V oder wohl auch durch Bestimmung von $\sum e_\rho^2$.

Ordnung primitiver Gruppen $\mathfrak{G}$ die $\neq$ 2-tra sind

1. $n = \text{Grad}\mathfrak{G}$, $p^a \| |\mathfrak{G}| \to a \leq \frac{2n}{p^2}$ $(p > 14)$ wohl unnötig. Aber $p = 2$?!
   Bew: Sei $[\frac{n}{p}] = k$, $p^\kappa \top k!$. Dann hat die p-Sylowgr von $\mathfrak{S}_n$ eine Untergr vom Index p^κ, die nur Transs d. Länge p hat. Also hat auch die p-Sy. $\mathfrak{P}$ von $\mathfrak{G}$ eine solche Untergruppe $\mathfrak{U}$ mit höchstens dem Index p^κ. $\mathfrak{U}$ hat noch mindestens $\alpha - \kappa$ Erzeugende. Da $\mathfrak{G}$ abgeschl ang. werden kann, haben die unzerlegbaren Elemente von $\mathfrak{U}$ im Mittel $\leq \frac{k}{\alpha-\kappa}$ p-Zyklen. Ist nun $\frac{k}{\alpha-\kappa} < p+3$, so ist nach Manning $n \leq 2(p+3)^2 - p^2$
   also umgekehrt:
   $n > 2(p+3)^2 - p^2 \to \frac{k}{\alpha-\kappa} \geq p+3 \to \alpha \leq \kappa + \frac{k}{p+3} < \frac{k}{p-1} + \frac{k}{p+3}$. Für $n \leq 2(p+3)^2 - p^2$ ist $n \leq p^2 + 12p + 18 < 2p^2$ $(p > 14)$ und daher nach 71.8a $\alpha \leq 2 < \frac{2n}{p^2}$

2. Asymptotisch kommt man mit Manning 1919 auf $\alpha < (1+\varepsilon)\frac{n}{p^2}$ herunter.

74/75

2. Die Ordnung einer einfach trans. prim Gr. vom Grade n ist $\leq e^{1,4n}$ (asymptotisch sogar $\leq e^{0,7n}$)
   Denn $\sum\limits_p \frac{\log p}{p^2} < 0,70$, $\log|\mathfrak{G}| = \sum \alpha \log p \leq \sum \frac{2n \log p}{p^2}$.
   Frage: Gehts ähnlich für Min Grad > 3 mittels Manning 1919, S. 382? Siehe 76.7

3. Eine einfache Gruppe $\mathfrak{G}$ ist genau dann alternierend, wenn sie eine Untergr. vom Index $< \log|\mathfrak{G}|$ enthält. (?)

4. Es gibt eine uniprimitive Gruppe vom Grad $n = \frac{kp(kp-1)}{2}$ deren Ordnung genau durch p^α teilbar ist, $\alpha = k + [\frac{k}{p}] + [\frac{k}{p^2}] + \cdots$. Nämlich die Darst. der $\mathfrak{S}_{kp}$ nach ungeordneten Paaren. Hier ist also $\alpha^2 \approx \frac{2n}{p^2}$

5. Man muss, um weiter zu kommen, zunächst die abgeschlossenen trans. p-Gruppen vom Grad p^2, p^3 ermitteln.

6. $\mathfrak{G}$ unipri, $n = 26 \quad \to \quad 5 \top |\mathfrak{G}|$.

75/76

Höhere Abschließungen

1. Sei $\mathfrak{G}$ eine Perm Gr auf Ω; $A \in \mathfrak{S}^\Omega$; $k = 1, 2, \ldots$
   Def: $A \in {}_k\mathfrak{G}$, wenn es zu jedem k-tupel $\alpha \ldots k$ ein $G \in \mathfrak{G}$ gibt, so dass $\alpha_A = \alpha_G, \cdots, k_A = k_G$.
   dh wenn $P_k(A) \leq \sum P_k(G)$.
   Man kann ${}_k\mathfrak{G}$ die k-te Annäherung an $\mathfrak{G}$ nennen.

2. $$ {}_k\mathfrak{G} = \bigcap_{a_1,\ldots,a_k \in \Omega} \mathfrak{S}^\Omega_{a_1 \ldots a_k} \cdot \mathfrak{G} $$

3. Mit $\mathfrak{G}$ ist auch ${}_k\mathfrak{G}$ eine Perm Gr auf Ω. Bew: 1
$\mathfrak{S} = \mathfrak{S}^\Omega \geq {}_1\mathfrak{G} \geq {}_2\mathfrak{G} \geq \cdots \geq {}_n\mathfrak{G} = \mathfrak{G}$ wenn $|\Omega| = n$

3a. ${}_k\mathfrak{G}$ ist die grösste Gruppe $\mathfrak{H}$ für welche stets $\mathfrak{H}_{\alpha_1 \cdots \alpha_{k-1}}$ die gleichen Transs. hat wie $\mathfrak{G}_{\alpha_1 \cdots \alpha_{k-1}}$.

4. Genau dann ist $\mathfrak{G}$ k-trans., wenn ${}_k\mathfrak{G} = \mathfrak{S}$.

5. $\mathfrak{H} \leq \mathfrak{G} \to {}_k\mathfrak{H} \leq {}_k\mathfrak{G}$

6. Ist $\mathfrak{H}$ eine transitive p-Gruppe des Grades p^2 und der Ordnung $p^{1+k} \cdot m$, so enthält ${}_k\mathfrak{H}$ alle "Diagonalelemente", dh. $|{}_k\mathfrak{H}| = p^{p+1} \cdot m'$. Bew 3a

7. Damit folgt: Ist $\mathfrak{G}$ primitiv vom Grade p^2 und ist $p^{1+k} \big| |\mathfrak{G}|$, so ist $\mathfrak{G}$ k-trans. Folge: $p^4 \big| |\mathfrak{G}| \to \mathfrak{G} \geq \mathfrak{A}^\Omega$ [nach] Jordan $n = (p-1)p + p$

8. Genau dann ist $\mathfrak{G}$ k-fach primitiv (oder $k + \frac{1}{2}$-fach tra), wenn ${}_{k+1}\mathfrak{G}$ diese Eigenschaft hat. (Dann heben sie auf ${}_{k+2}\mathfrak{G},\ {}_{k+3}\mathfrak{G}, \cdots$)

9. Kann man Ω so in $\Gamma + \Delta$ einteilen, daß Γ und Δ Transs. von $\mathfrak{G}$ sind und daß die Untergr. $\mathfrak{G}_{\gamma_1,\gamma_2}$ stets noch auf Δ die alten Transs. hat, ebenso $\mathfrak{G}_{\delta_1,\delta_2}$ auf Γ, dann "zerfällt" $\mathfrak{G}$ bezgl ${}_3\mathfrak{G}$, dh. wenn $\mathfrak{G} = \mathfrak{G}^\Gamma \mathfrak{G}^\Delta$, dann $\mathfrak{G}^\Gamma \leq {}_3\mathfrak{G}, \quad \mathfrak{G}^\Delta \leq {}_3\mathfrak{G}$.

10. Z.B. wenn $\mathfrak{G}$ nur 2 Transs. $\neq 1$ hat, mit Länge k, l derart, daß $(k(k-1), l) = 1$, $(l(l-1), k) = 1$, dann enthält ${}_3\mathfrak{G}$ die trans Konstituenten vom Grad k und l einzeln; Folge: ist $\mathfrak{G}$ pri, so ist $\mathfrak{G}$ 3-tra

11. N & h dafür, daß $\mathfrak{G}$ 2-tra, ist die Bedgg: $\mathfrak{G}$ pri & $\mathfrak{G} \ni \binom{1\ 2\ \cdots}{2\ 1\ \ldots}$, $\mathfrak{G} \ni \binom{1\ \cdots\ \nu\ \cdots}{2\quad\ \ \nu}$ zu jedem $\nu > 2$
Denn dann ist $(12) \in {}_2\mathfrak{G}$, also ${}_2\mathfrak{G} = \mathfrak{S}$.

1. Sei $\mathfrak{G}$ unipri; $\mathfrak{G}_1$ habe einen trans konst $\mathfrak{K}$, der sowohl $\frac{3}{2}$-tra ist (mit TraLgen $t \big| k-1$, $k = \operatorname{Grad} \mathfrak{K}$), als auch primitiv. Dann hat $\mathfrak{G}$ einen tra Konstit. $\mathfrak{L}$ von einem Grade l mit $t < l \big| kt$ und $k < l$?
Bew: Werde α von $\mathfrak{K}$ betroffen. $\mathfrak{G}_{\alpha 1}$ hat Transsysteme der Länge t, die aus $\mathfrak{K}$ entstehen. Wegen Primit. von $\mathfrak{K}$ entsteht kein Transs. d. Lge 1 aus irgend einem Konst. $\mathfrak{L}$ von $\mathfrak{G}_1$ mit Gr $\mathfrak{L} = l < k$; und aus $l > k$ sowieso nicht. Wenn also 1 aus $\mathfrak{L}$ entsteht, so $k = l$, diese sind gekoppelt und ähnlich; $\mathfrak{L}$ liefert dann nur 1 und t als Translgen von $\mathfrak{G}_{1\alpha}$. Ferner entsteht t nur aus $l \big| kt$ mit $t \leq l \leq kt$. Wenn kein l mit $l \big| kt,\ t < l$ vorhanden ist, dann entsteht t nur aus $l = t$. Dann bilden die sämtlichen Transs. Γ von $\mathfrak{G}_{1\alpha}$ mit $|\Gamma| = 1$ oder t zusammen einen Festblock von $\mathfrak{G}_1$. Ebenso von $\mathfrak{G}_2$, da $\mathfrak{G}_2 = \mathfrak{G}_1^\tau$, also von $\mathfrak{G}_1 \vee \mathfrak{G}_2 = \mathfrak{G}$. Aus Prim. von $\mathfrak{G}$ folgt nun, daß $\mathfrak{G}_{1\alpha}$ nur Transs. der Lgen 1 und t hat. Die $t's$ können nur entstehen

1. Eine primitive Gruppe unendlichen Grades, die endliche Permutationen $\neq 1$ umfasst, dürfte die alternierende Gruppe (endlicher Permu) enthalten. Vielleicht genügt: "Minimalgrad" kleinere Mächtigkeit als Grad

Dissertations-Thema: Perm.–Gruppen des Grades ∞. F
Aufgabe: die P Gr $\mathfrak{G}$ untersuchen, bei denen $\mathfrak{G}_1$

a) nur 2 Transs $\neq 1$ hat, oder

b) lauter gleich lange Transs. $\neq 1$ hat, und

c) auf diesen auch noch "ähnliche" Konstituenten,

d) die außerdem noch treu sind.

Verschiedene "Abschließungen" einer Gruppe

1. Man kann eine P Gr. $\mathfrak{G}$ ergänzen durch alle Permutationen, die auf den ungeordneten Paaren die Transsysteme von $\mathfrak{G}$ respektieren; nenne diese Abschliessg etwa ${}_{\frac{3}{2}}\mathfrak{G}$; ist $\geq {}_2\mathfrak{G} \geq \cdots$.

2. ${}_{\frac{3}{2}}\mathfrak{G}$ ist 2-tra genau wenn $\mathfrak{G}$ tra auf den ungeordneten Paaren, dh. $\mathfrak{G}_1$ nur $\frac{2}{2}$ Trans Konstit. $\neq 1$, und diese gepaart. Das sind nur die 2-tra $\mathfrak{G}$, wenn $|\mathfrak{G}| \equiv 0(2)$.

3. Enthält $\mathfrak{G}$ etwa ein Elem. P d. Ord $p = 2m + 1$ und ein $\{P\}$ normalisierendes Elem. Q d. Ord m, das alle von P fest gelassenen Ziffern fest läßt, so enthält ${}_{\frac{3}{2}}\mathfrak{G}$ die gekoppelten $\mathfrak{S}_p \cdot \mathfrak{S}_p \cdots$ der Ord $p!$

4. Geordnete Paare, Tripel, – bei $\mathfrak{S}_n$ entsprechen vd Waerdens "Flaggen" bei den projektiven od linearen Gruppen. Also sollte man mod. Gruppen erweitern durch

alle Matrizen M, zu denen es in $\mathfrak{G}$ zu jeder Flagge der Dim k ein G gibt mit demselben Flaggenbild. Oder durch Bildg von Lin. Verbdgen abschliessen.

5. Eine abstrakte Gruppe $\mathfrak{G}$ auf natürliche Weisen als P Gr $\mathfrak{G}^*$ darstellen und die Eigenschaften der ${}_k\mathfrak{G}^*$ untersuchen. ZB. $\mathfrak{G}^*$ = Holomorph von $\mathfrak{G}$. Dann $\binom{A}{A'} \in {}_2\mathfrak{G}^* \leftrightarrow$ für $A, B \in \mathfrak{G}$ stets ein Autom. σ von $\mathfrak{G}$, $S \in \mathfrak{G}$, existiert mit $A' = SA^\sigma,\ B' = SB^\sigma$.
Die $\frac{3}{2}$-Abschließung der Automgr von $\mathfrak{G}$ enthält nur Abbildungen von $\mathfrak{G}$ in sich, für die $\{A', B'\} \cong \{A; B\}$; diese Abb bilden aber vielleicht eine noch grössere "Abschliessung" als ${}_{\frac{3}{2}}\mathfrak{G}$.

6. Ist $\mathfrak{G}$ transitiv und $\mathfrak{G}_1$ k-fach abgeschlossen, $\mathfrak{G}_1 = \mathfrak{G}_1^{(k)}$, so ist $\mathfrak{G} = \mathfrak{G}^{(k+1)}$; aber nicht umgekehrt.
   Denn ${\mathfrak{G}^{(k+1)}}_1 \leq \mathfrak{G}_1^{(k)} = \mathfrak{G}_1$, daher wegen Trans. $|\mathfrak{G}^{(k+1)}| \leq |\mathfrak{G}|$.

Zum Satz von Frobenius

1. Ist $\mathfrak{G}$ transitiv, so ist $\mathfrak{G}_1 \cap \bigcup_{\alpha\neq\beta} \mathfrak{G}_{\alpha\beta} = \bigcup_{\beta\neq 1} \mathfrak{G}_{1\beta}$
   dh. wenn alle G_1 sich aus irgend welchen $G_{\alpha\beta}$ zusammensetzen läßt, so auch aus gewissen $G_{1\beta}$!
   Denn sei $\mathfrak{G}^*$ der trans NT mit $\mathfrak{G}^* \cap \mathfrak{G}_1 = \bigcup \mathfrak{G}_{1\beta}$, dann $\bigcup \mathfrak{G}_{1\beta} = \mathfrak{G}_1 \cap \mathfrak{G}^* \geq \bigcup \mathfrak{G}_{1\beta}$ nach meinem Satz.
   Frage: Gilt Entsprechendes auch für $\mathfrak{G}_{\alpha\beta\gamma}$? ... intransitive $\mathfrak{G}$?

2. $\mathfrak{G}$ k-tra, $\mathfrak{G}^* = \bigcup \mathfrak{G}_{\alpha_1\cdots\alpha_k\alpha_{k+1}} \to \mathfrak{G}^* \cap \mathfrak{G}_{1\cdots k} = \bigcup \mathfrak{G}_{1\cdots k\alpha_{k+1}}$
   Bew: 1 auf $\mathfrak{H} = \mathfrak{G}_{1\cdots k}$ anwenden.
   stimmt noch nicht, dh $\mathfrak{G}_{1\cdots k} \neq \mathfrak{G}_{1\cdots k}$. Ungeordnete Paare nehmen!

Aufgabe: "Gepaarte Konstituenten" bei Darstellung nach 2 verschiedenen Untergr. untersuchen: $\mathfrak{A}G\mathfrak{B} \leftrightarrow \mathfrak{B}G^{-1}\mathfrak{A}$.

Kompositionsfaktorgr. von Durchschnitten
Fortsetzg von Ausarb. PGr. §18& IX, 1-3

1. Seien $D \leq H_1, H_2, \cdots \leq G$; N die größte Untergr. von D, die in allen H_2 normal ist, N_i die größte Ugr von D, die in H_i normal ist. Dann treten in D/N keine anderen KFG auf als in den D/N_ν. (vorausgesetzt, dass D/N endl. K Reihe hat).
   Bew: $\Lambda = \sum K(D/N_i) \quad D^\Lambda = N_i^\Lambda \lhd H_i, \quad D^\Lambda \leq N$.

2. Ist H endl; Λ nach unten vollständig (dh. $\mathfrak{K} \in \Lambda \quad \to$ jeder einfache Ausschnitt von $\mathfrak{K}$ ist $\in \Lambda$), so ist H^Λ einzig in H, dh. $U \cong H^\Lambda$, $U \leq H \to U = H^\Lambda$. Dabei H^Λ min mit $K(H/H^\Lambda) \subset \Lambda$.
   Genauer:

3. H endl; Λ nach unten vollst, $H^\Lambda \leq B$, B hom. Bild von $H \to H^\Lambda = B^\Lambda$.

KFG von Durchschnitten

4. Seien $H_i \leq G$, $H_i \cap H_{i+1} = H_{i\ i+1}$, Kern $H_{i\ i+1}$ in H_i $(i = 1, i+1) = N_{i\ i+1}$. Ist dann $\overline{K}(H_{\underset{i+1}{\ i}} \big| N_{i\ i+1}) \subseteq \Lambda$, sonst $H_i^\Lambda = H_{i+1}^\Lambda$
   z.B.

4′. Ist $\left|H_{\substack{i\\i+1}} : H_i \cap H_{i+1}\right| \leq n$, so $H_i^{\overline{\mathfrak{S}_n}} = H_k^{\overline{\mathfrak{S}_n}}$. Dabei $\overline{\mathfrak{S}_n}$ = Menge einfacher Ausschnitte von $\mathfrak{S}_n$

5. Vor. 4. Ist $p \Big| |H_{\substack{1\\k}} : N|$, N = max gemein. NT von $H_1, H_2, \cdots$, so ist $p \leq$ max $|H_{\substack{i\\i+1}} : H_{i\ i+1}|$, und wenn =, so ist pT ….

6. Vor. 4. Ist $H_{\substack{i\\i+1}} \Big| N_{i\ i+1}$ auflösbar, so H_i/N auch

7. Ist Λ vollständig, $H_1 \cap H_i = H_{1i}$, $K(H_1/\cap H_{1i}^{h_1}) \subseteq \Lambda$, so ist $K(H_1/N) \subseteq \Lambda$, wo N = max NT aller $H_1, H_2, \cdots, H_i, \cdots$

84/85

8. Ist σ ein Autom d. Ord 2 von G, und $H_1 \leq G$, $H_1^\sigma = H_2$, $H_1 \cap H_2 = D$, $\cap D^{h_1} = N_1$, $\bigcap\limits_{h \in \{H_1 \cup H_2\}} D^h = N$, so ist $K(H_1/N) = K(H_1/N_1) + K(D/N_1)$.

85/86

DE Littlewoods (Buch) Vermutung (S. 147)

1. In einer primitiven Permutationsgruppe kommt jede irred. Darstellung höchstens einmal vor.
Burnside 1901 behauptet das ohne Beweis (S. 174) Todd

1. Im Normalisator N einer maximalen kovarianten Familie (von Komplexen in G) ist jede intravariante Untergr. von N normal, daher ist N nilpotent.

2. Statt “Aufspaltung” (so bei A. Scholz) könnte man “Verfeinerung” sagen.

3. Die Vertretergr. eines abelschen NTs bilden ein komm. Gruppoid (nach Festhaltg einer Vertretergr eine Gruppe)
Bew mit Verschiebungs-Systemen.

4. Sind in einer abelschen Aufspaltung $\mathfrak{G}/\mathfrak{A}$ vielleicht genau dann alle Komplemente konjugiert, wenn das mod allen Sylowkomplementen in $\mathfrak{A}$ gilt? Wie ist es mit Intravarianz ?

87/88

1. Ist $\mathfrak{A}$ abelsch, so bilden die Aufsp. von $\mathfrak{F}$ durch $\mathfrak{A}$ eine Gruppe. Was bilden sie, wenn $\mathfrak{A}$ nilpotent ist? (Wohl so eine Art “graded group”.)

2. $\mathfrak{A}$ abelsch, $\mathfrak{G} \rhd \mathfrak{A}$, Fakt Syst $\{C\} \to \mathrm{Ord}\{C\} = \mathrm{kgV}\,\mathrm{Ord}$ Einschränkung von $\{C\}$ auf die Sylowgruppe von $\mathfrak{G}/\mathfrak{A}$.
Bew: Gaschütz, Red.-Satz

3. Das Schreiersche Erweiterungsproblem lässt sich zu einem Einbettungsproblem verallgemeinern:
Geg: noch eine Untergr $\mathfrak{U}$ der Faktorgruppe. Für $\mathfrak{A} = 1$ kommt Schreier raus. Ausführlicher!

88/89

1. Eine abelsche Aufspaltg $\mathfrak{G} : \mathfrak{A}$ zerfalle sowohl mod $\mathfrak{M}$ wie mod $\mathfrak{N}$, wobei $\frac{\mathfrak{M}}{\mathfrak{N}} \lhd \mathfrak{G}$, und $< \mathfrak{A}$, & $\mathfrak{M} \cap \mathfrak{N} = 1$. Zerfällt dann $\mathfrak{G} : \mathfrak{A}$? oder wenigstens wenn $(|\mathfrak{M}|, |\mathfrak{N}|) = 1$?

2. Sei $\mathfrak{G} : \mathfrak{A}$ abelsche Aufsp., $|\mathfrak{A}| = p^\alpha$, $\mathfrak{P}$ p-Sy $\mathfrak{G}$, $\mathfrak{P} : \mathfrak{A}$ zerfalle.
Kann man dann jedes Kpl. $\mathfrak{P} : \mathfrak{A}$ fortsetzen zu einem von ganz $\mathfrak{G} : \mathfrak{A}$, oder wie hoch hinauf geht es?

89/90

1. Ist $\mathfrak{A} \lhd \lhd \mathfrak{G}$, $\mathfrak{B} \lhd \lhd \mathfrak{G}$, $\mathfrak{A} \cap \mathfrak{B} = 1$ und hat $\mathfrak{A}$ eine endl. Kompos.-Reihe, die nur nichtabelsche KFG enthält, so ist $\mathfrak{A} \circ \mathfrak{B} = 1$
Bew: Induktion nach $j(\mathfrak{A}, 1)$

2. Man sollte auf die "Verdichtungsstrecken" von $\mathfrak{G}$ für Kompreihen (oder Hauptreihen) achten: solche Gruppenpaare $1 < \mathfrak{A} \trianglelefteq \mathfrak{B} \trianglelefteq \mathfrak{G}$, für welche jede Kompositionsreihe von $\mathfrak{G}$ mindestens ein Glied $\mathfrak{G}_\nu$ mit $\mathfrak{A} \leq \mathfrak{G}_\nu \leq \mathfrak{B}$ enthält.

3. Index sagt mehr als Ordnung.

4. Die π-Länge einer π- auflösbaren Gruppe einführen.

90/91

4.5.58 Unendl. Gruppen: Hauptfaktoren.

1. Def: Ein Hauptfaktor von $\mathfrak{G}$ ist eine Faktorgr. $\mathfrak{A}/\mathfrak{B}$, wo $\mathfrak{A} \lhd \mathfrak{G}$ $\mathfrak{B} \lhd \mathfrak{G}$, $\mathfrak{B} < \mathfrak{A}$ und $\mathfrak{A}/\mathfrak{B}$ $\mathfrak{G}$-einfach.

2. Jede Gruppe $\mathfrak{G} \neq 1$ enthält einen Hauptfaktor.

   a) Sei nämlich $A \in \mathfrak{G}$ beliebig. $\mathfrak{A} = A^{\mathfrak{G}}$, und $\mathfrak{B}$ ein maximaler zu A fremder $\mathfrak{G}$-NT in $\mathfrak{A}$.

   b) Oder sei $\mathfrak{B}$ ein maximaler zu A fremder NT in $\mathfrak{G}$ und $\mathfrak{A}$ der Durchschnitt aller grösseren NT in $\mathfrak{G}$.

3. Def: $\mathfrak{G}$ heißt $\left\{ \begin{array}{l} \text{haupt kommutativ} \\ \text{oder haupt-zentral} \end{array} \right\}$, wenn jeder Hauptfaktor von $\mathfrak{G}$ $\left\{ \begin{array}{l} \text{komm.} \\ \text{zentral} \end{array} \right\}$ ist.

4. Faktorgruppen haben keine anderen Hauptfaktoren als die ganze Gruppe.

4a. Frage: Sind Hauptfaktoren von Hauptfaktoren einfach?

5. Frage: Ist jede Untergr. zu 3 von derselben Art? Hat jede haupt-zentrale Gr nur eine π-Sylowgr.? Wie verhält sich "haupt zentral" zu Baers Nilgruppen?

91/92

1. Einen Namen verdienen die $\mathfrak{A} \subset \mathfrak{G}$, für die aus $\mathfrak{A} \lhd \mathfrak{B} \lhd \mathfrak{C} \subseteq \mathfrak{G}$ folgt: $\mathfrak{A} \lhd \mathfrak{C}$. Z.B. die Sylowgr. von $\mathfrak{G}$ tun das. Es gilt dann stets $\mathcal{N}\mathcal{N}\mathfrak{A} = \mathcal{N}\mathfrak{A}$.

2. Frage von Baer (Lorenzenhof Pfingsten 58):
Man definiert einen "charakt" Operator $\mathfrak{G} \to T\mathfrak{G} \leqq \mathfrak{G}$ so, daß

   a) $T(\mathfrak{G}^\sigma) = (T\mathfrak{G})^\sigma$ für jeden Iso σ

   b) $\mathfrak{N} \trianglelefteq \mathfrak{G}$, $\mathfrak{N} \leq T\mathfrak{G} \to T(\mathfrak{G}/\mathfrak{N}) = (T\mathfrak{G})/\mathfrak{N}$

   Dann kann man zeigen:
   Wenn c) aus $\mathfrak{S} \leq \mathfrak{G}$, $(|\mathfrak{G} : \mathfrak{S}|, p) = 1$ für jeden Homo η folgt: $\mathfrak{S}^\eta$ ist p-normal, dann folgt für je zwei p-Sylowgr. $\mathfrak{P}_1, \mathfrak{P}_2$ und jeden T:

$$T\mathfrak{P}_1 \cap \mathfrak{P}_2 = \mathfrak{P}_1 \cap T\mathfrak{P}_2$$

   z.B. $T\mathfrak{P} = \overset{\circ}{\mathfrak{P}}{}^k$.

   Frage: Kann man die unschöne Bedgg b) abschwächen, und ebenso c)?

92/93

20.5.58 Intravarianz

1. Es gibt p-Gruppen $\mathfrak{P}$ mit und ohne eigentlich intravarianten Untergruppen.
Mit z.B. jede $\mathfrak{P}$, die nur $p+1$ Untergruppen der Ord p enthält und nicht alle im Zentrum.
Ohne z.B. die Gruppe der Ord p^3 $(p > 2)$ von Exp. p.

2. Nur Gruppen, die keine eigentlich intrav. Ugr. enthalten, können als Kerne bei "kleinsten" Aufspaltungen auftreten.

3. Aufgabe: Die p-Gruppen ohne eig. intrav. Ugr. untersuchen. Weichsel gesagt IV 62

4. Ist das System $\mathfrak{I}$ intrav in $\mathfrak{G}$ und ist $\mathfrak{N} = \mathcal{N}\mathfrak{I}$ und $\mathfrak{A}$ intrav in $\mathfrak{N}$, so ist auch das verlängerte System $\{\mathfrak{I}, \mathfrak{A}\}$ intrav in $\mathfrak{G}$.

5. Daher ist im $\mathcal{N}\mathfrak{N}$ eines max intrav Systems jede intrav. Ugr normal; z.B. ist $\mathfrak{N}$ nilpotent, keine Sy Gr ist nicht abelsch vom Exp p^2 und Ord p^3.

93/94

1. Wie liegen die Sylow-Turm-Normalisatoren zu Kompositions- und Hauptreihen von $\mathfrak{G}$?
   z.B. wenn $\mathfrak{G}$ auflösbar? 95_5

2. Man sollte die maximalen intravarianten π-Gruppen untersuchen. Die max. intrav π-π'-Gr. (dh. jeder $KF \in \pi$ oder π') sind ihre eigenen Normalisatoren. Aber es geht die Maximalität in Zwischengruppen verloren.

3. Beispiele von Gruppen suchen, die ein intravariantes System mit Normalisator 1 besitzen. Über ihnen zerfällt jede Erweiterung.

4. Der Satz von Gaschütz über p-Erweiterung von p-perfekten Gruppen $\mathfrak{G}$ mit abelscher p-Sylow-Gruppe beruht auf folgendem: In $\mathfrak{G}$ ist der p p'-Ketten-Normalisator eine p'-Gruppe.

1. Der Durchschnitt von zwei Intravarianz-System-Normalisatoren, die teilerfremde Indizes haben, ist wieder einer.
   Die Vereinigung von zwei Intrav-Systemen, deren $\mathcal{N}$s teilerfremde Indizes (oder Produk $\mathfrak{G}$) haben, ist wieder eins.

2. Ist $\mathfrak{I}$ ein Intrav-System und $\mathfrak{C}$ eine invariante Menge von Elementen von $\mathfrak{G}$, so ist $\mathfrak{I}^{\mathfrak{C}} = \sum \mathfrak{I}^C$ ein Intrav-System.

3. Ist jede Untergr. von $\mathfrak{G}$, auf die man jede Erweiterung von $\mathfrak{G}$ herabschieben kann, ein Intravarianz-Sy-Normalisator?

4. Enthält $\mathfrak{G}$ einen Intra-Sy-Normalisator $\in \mathfrak{f}_{\pi'}$, so zerfällt jede π-Erweiterung von $\mathfrak{G}$.

5. Jeder Sylow-Turm-Normalisator von $\mathfrak{G}$ deckt $\mathfrak{G}/\mathfrak{G}^{\nu}$. Forts.: 99

95/96

Verlagerung - Frobenius 22.6.58

Problem: Fortsetzung von Homom von Untergr.
Geg ein System Σ von Untergr. $\mathfrak{U} < \mathfrak{G}$, das gegen Durchschnittsbildung abgeschlossen ist und "ein" Homo η jedes $\mathfrak{U}$ in eine feste Gruppe $\mathfrak{H}$, der "verträglich" ist mit der Durchschnittsbildung in Σ. Wann ist η fortsetzbar auf $\mathfrak{G}$ (oder auf $\bigcup_{\Sigma} \mathfrak{U}$) ?
Vielleicht genügt es, wenn Σ normal in $\mathfrak{G}$, dh $\Sigma^G = \Sigma$?
Vielleicht genügt es, falls $|\mathfrak{H}| = p$, dass Σ alle p-Sy Gr enthält?

2. Aufgabe: Komplemente von subnormalen Untergruppen untersuchen.

3. Aufgabe: Funktionalgl. für die Verschiebgs. elemente bei zwei Supplementen des gleichen Normalteilers studieren.

4. Zerfalls-Sätze für abelsche $\mathcal{N}T$ übertragen auf $\mathcal{N}T$ mit abelschen Sylowgruppen

Zum Konjugiertheits-Problem von Zassenhaus:

1. Ist $\mathfrak{N} \lhd \mathfrak{G}$; $\mathfrak{K}, \mathfrak{C}$ Kpl. $\mathfrak{N}$ in $\mathfrak{G}$, $(|\mathfrak{N}|, |\mathfrak{K}|) = 1$, so kann man die größte kleinste elem. abelsche p-Aufspaltg von $\mathfrak{N}$ betrachten. Auf ihrem Kern $\mathfrak{A}$ bewirken $\mathfrak{K}$ und $\mathfrak{C}$ Darstellungen, die unter der vollen Autom Gr von $\mathfrak{A}$ vermutlich konjugiert sind, etwa $\eta,\ \tau$. Wenn man Zassenhaus für kleinere $(\mathfrak{G}/\mathfrak{N})$ als richtig annimmt: Entsprechende K und C sind konj. in $\mathfrak{G}_1$ also ihre darstellenden Autom von $\mathfrak{A}$, also wohl die ganzen Darstellungen von $\mathfrak{K}$ und $\mathfrak{L}$ konjugiert (dies ist eine Art Integrations-Verfahren). Zu zeigen bleibt, dass τ von einem El von $\mathfrak{N}$ erzeugt wird.

2. Man könnte Konjugiertheits-Kriterien nach der „österreichischen Methode“ (Monatshefte) aufstellen:
Z.B. wenn $\mathfrak{A}, \mathfrak{B} < \mathfrak{G}$, $T \in \mathfrak{G}$, so ist genau dann $T^{-1}\mathfrak{A}T = \mathfrak{B}$, wenn in jeder komplexen (oder rationalen) Darstellung von $\mathfrak{G}$ T den Fixraum von $\mathfrak{A}$ in den von $\mathfrak{B}$ überführt.
Bew: Reguläre Darst. von $\sum_{\mathfrak{A}} A$ betrachten: $T^{-1}\Sigma AT = \Sigma B$.
Verfeinerungen ansehen!

97/98

3. Sind $\mathfrak{K}$, $\mathfrak{K}'$ zwei Komplemente von $\mathfrak{N}$ in $\mathfrak{G}$, und ist jede <u>echte</u> Untergr. $\mathfrak{K}_\alpha < \mathfrak{K}$ unter $\mathfrak{N}$ konjug. zu der entspr. $\mathfrak{K}'_\alpha$, etwa $\mathfrak{K}_\alpha^{T_a} = \mathfrak{K}'_\alpha$, $T_a \in \mathfrak{N}$, so gilt:
Aus $\mathfrak{K}_\alpha^{K_\beta} = \mathfrak{K}_\gamma$ folgt $G_\beta^{-1} T_\alpha T_\beta^{-1} G_\beta T_\beta \in \mathfrak{T}_\gamma$.

4. Ähnlich folgt aus $K_\alpha K_\beta = K_\gamma$ und $K_\rho^{T_\rho} = K'_\rho$:

$$T_\alpha^{-K_\alpha+1} T_\beta^{-1+K_\beta^{-1}} = T_\gamma^{-K_\alpha+K_\beta^{-1}}$$

4′. Also aus $K_\alpha = K_\beta K_\gamma$ folgt

$$T_\alpha^{-K_\alpha+1} T_\beta^{-1+K_\beta} = T_\gamma^{-K_\alpha+K_\beta}$$

daher: Aus $K_\alpha K_\beta = K_\gamma$ folgt

$$T_\gamma^{-K_\gamma+1} T_\alpha^{-1+K_\alpha} = T_\beta^{-K_\gamma+K_\alpha}$$

Also:

$$T_\alpha^{-K_\alpha+1} T_\gamma^{-1+K_\gamma} = T_\beta^{-K_\alpha+K_\gamma}$$

1. Wenn $\mathfrak{G}^\nu$ $^{-\text{nilp.}}$ abelsche Sylowgruppen hat (nur), so enthält $\mathfrak{G}^\nu$ keinen zentralen Hauptfaktor von $\mathfrak{G}$.
   Bew: $\mathfrak{G}^\nu \cdot \mathfrak{G}_{p'} = \mathfrak{H}$ setzen: $\mathfrak{H}$ hat keinen p-Kopf mehr, und $\mathfrak{H} = \mathfrak{P} \cdot \mathfrak{G}_{p'}$, wo $\mathfrak{P}$ p-Sy Gr $\mathfrak{G}^\nu$, also $\mathfrak{P}$ abelsch. Verlagerung: $\mathfrak{P}$ enthält kein Zentrumselement von $\mathfrak{H}$. Das könnte man aber annehmen, wenn $\mathfrak{G}^\nu$ einen Zentr Fkt v. $\mathfrak{G}$ Bedeutng von „19V“?

2. Folge: Wenn $\begin{cases} \mathfrak{G} \text{ auflösbar ist und} \\ \mathfrak{G}^\nu \text{ abelsche Sylowgr. hat} \end{cases}$, dann ist jeder Sylowsystem-Normalisator von $\mathfrak{G}$ (und der $\mathcal{N}\mathfrak{s}$ jedes vollstd. Sylowturms ?) ein Komplement von $\mathfrak{G}^\nu$ in $\mathfrak{G}$.

3. Folge: Unter Vor. 2 zerfällt jede Erw. von $\mathfrak{G}$ über $\mathfrak{G}^\nu$, je zwei Kompl sind konjugiert.

4. Ebenso für $\mathfrak{G}^E$, definiert als $K(\mathfrak{G})$ von Higman (1956, S. 47).

99/100

1. Ist die p-Sylowgr. von $\mathfrak{G}$ abelsch und $\mathfrak{G}$ p-perfekt, so ist der p-p'- Normalisator von $\mathfrak{G}$ p-frei.
   Darauf beruhen Sätze von Gaschütz ’52 und Higman ’56

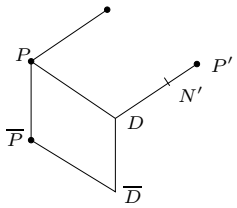
2. Zu Kriterien für p-Nilpotenz:
   In $\mathfrak{G}$ habe der Durchschnitt zweier verschiedener p-Sylowgruppen stets einen p-nilpotenten Normalisator. Dann sind je zwei p-Sylowgruppen von $\mathfrak{G}$ konjugiert unter dem Zentralisator ihres Durchschnitts. Folge mittels Verlagerung: Ist in $\mathfrak{G}$ der p- Sylow-$\mathcal{N}\mathfrak{s}$ sowie jeder $\mathcal{N}\mathfrak{s}$ eines Durchschnitts zweier p-Sylwgr p-nilpot., so ist $\mathfrak{G}$ nicht p-perfekt: $(\mathfrak{G}/\mathfrak{G}')_p \cong \mathfrak{G}_p/\mathfrak{G}'_p$,
   Folge: Ist der $\mathcal{N}\mathfrak{s}$ jeden von 1 verschiedenen p-Untergruppen von $\mathfrak{G}$ p-nilp, so ist $\mathfrak{G}$ p-nilpotent.

100/101

Verlagerung

1. Ist der Normalisator jedes echten Sylowdurchschnitts p-nilp., so sind je zwei Sylowgr konjugiert unter dem Zentralisator ihres Durchschnitts.

2. Eine $n + h$ Bedgg für Verlagerbarkeit ist:



$|D : \overline{D}_{N'}| < p^{|N':D|}$

3. Frage: Genügt es auch, wenn jedes p-freie Element im Normalisator von D auch $\overline{D}$ normalisiert? ja: XI, S69$_{19}$

4. Wenn $\mathcal{N}P \dot{<} G$, dann lassen sich je zwei p-Sylowgr durch eine Kette verbinden, in der je zwei benachbarte Glieder einen maximalen Durchschnitt haben. Man kann sogar feste Index $|P_i : P_i \cap P_{i+1}|$ vorschreiben
Denn sonst bilde die mit festen P "maximal Verbindung, gäben Block für die Darstellg von G auf den $P^g \cdots$

1. Ist P Sy Gr G und $\overline{P} < P$, $\overline{P} \lhd \mathcal{N}P$, so ist für jedes $P^g = Q$ definiert $\overline{Q} = \overline{P}^g$; und aus $R = Q^t$ folgt $\overline{R} = \overline{Q}^t$.

2. Genau wenn alle diese "Verjüngungen" $R \to \overline{R}$ "verträglich" sind in dem Sinne, daß $\overline{P} \cap R = P \cap \overline{R}$, ist $P/\overline{P}$ von G abschneidbar.

3. Nenne P vertr Q, wenn $\overline{P} \cap Q = P \cap \overline{Q}$. Dann gilt:

4. Ist P_1 vertr P_2 vertr $P_3 \cdots$ vertr P_n und $P_1 \cap P_2 \cap \cdots \cap P_n = P_1 \cap P_n$, so ist P_1 vertr P_n.
Denn $\overline{P}_1 \cap P_n = \overline{P}_1 \cap P_2 \cap \cdots \cap P_n = P_1 \cap \overline{P}_2 \cap P_3 \cap \cdots$

5. Wenn also in G je zwei Sylowg mit Durchschnitt D verbindbar sind durch eine "Maximal Kette", so genügen Vorauss. über Sylowgr mit Maximal-Durschnitt für Verlagerung.

1. Kann man ein "Tensorprodukt" zweier (additiv zu schreibenden) Gruppen einführen? Das könnte bei der Entwicklung einer Darstellungstheorie auf p-Gruppen nützlich sein.

2. Frage von Carter-Cambridge (Anf. 58):
Ist $G > H > N_G$, wo N ein SySy Normalisat. von G, so lässt sich zeigen $|N_H| \geq |N_G|$ mittels Deckmeide.
Frage: Gibt es sogar ein $N_H \geq N_G$?

3. Satz von R. Brauer (mitgeteilt Anf 1958):
Ist eine (verallg.) Quaternionengruppe eine Sylowgruppe von G, so ist G nicht einfach.

1. Satz von Thompson, Chicago (Aug 1958)
   Ist G eine Gruppe minimaler Ordnung mit der Eigenschaft, dass G nicht auflösbar ist, aber eine maximale Untergr. P enthält, die p-Sylowgr. von G ist, so enthält G keine "spezielle" Untergr. A.
   Dabei A speziell $\leftrightarrow$

   a) A abelsch (p,p)
   b) A in einem Sylowdurchschnitt
   c) Wenn $x \in \mathrm{Ztr}\ P^g$ ein Element $\neq 1$ von A zentralisiert, so zentralisiert x sogar A.
   d) $A \cap \mathrm{Ztr}(P^g) \neq 1$ für ein $g \in G$.

   Baer hofft, dass man sogar schliessen kann: P zyklisch.

2. Aufgabe: Verallgemeinerung des Satzes von Frobenius formulieren für subnormale statt normale Untergruppen.

$A \lhd \lhd G$ Gastein 1958

1. $A^\omega < B^\omega \to B^{\omega A} = B^\omega$
2. $A^{\nu\eta} = A^{\eta\nu}$, wenn η Homom G. ebenso für p statt ν.
3. Ist A^ν in einem anderen Sinn als $A^\nu \vee B$ fast normal?
4. P, Q verschiedene Hallgruppen: $s_G P \xrightarrow{\text{in}} sG \xrightarrow{\text{in}} s_G Q$. F
5. Gibt es "Anzahlsätze" in $s_G P$ oder in sG ?
6. Gruppen $\mathfrak{G}$ mit nilpotenten $p-q$-Hallgruppen $\mathfrak{H}$ untersuchen. Zerfällt $\mathcal{N}\mathfrak{H}$ subnormal, wenn $\mathfrak{G}$?

Gastein IX 58:

1. Notw. für Ex eines $G^* \lhd G$ mit $G^* \cap H_i = H_i^*$ gegeben ist: $H^t \cap H^* = H \cap H^{*t}$ falls $t \in G$. $\to$ 107.2
   Ist das auch hinreichend? Wohl ja wenn $H = G_p$ und $|H : H^*| = p$. Sollte durchführbar sein, wenn H/H^* auflösbar: Dazu kommt Zerfallsbedingung für $\mathcal{N}H$ oder $\mathcal{N}H^*/H^*$

2. Bei monomialer Darstellung mit p-ten Einheitswurzeln ist das Produkt Δ der Diagonalfaktoren

$$\Delta \equiv 1 + \chi \mod \mathfrak{p}^2 \quad (\mathfrak{p}^{p-1} = (p)).$$

   Zusammenhang mit Witt-Amsterdam?

3. $\exists$ ($G_{\{pq\}}$&$G_{p'}$ aufl & $G_{q'}$ aufl) $\to$ G aufl
   VI 59: Allgemeiner: Hat G 3 aufl Ugr mit paarweise teilerfremden Indizes, so ist G auflösbar. 2 reichen nicht: G_{168}, aber 2 reichen wenn beide nilpotent.

4. Sonderfall: existieren auflösbare Sylow Komplemente zu 3 verschiedenen Primzahlen, so ist G auflösbar
   Wenn i_1, i_2, i_3 paarw. fremd, G_1 aufl, so G nicht einfach: G_2 oder G_3 enthält einen NT $\neq 1$.

5. [*Durchgestrichen mit Vermerk „erl“:*
   Ist $G = AB$ und C “invariant verbunden” mit Normalteilern unter A und B (z.B. C vertauschbar mit $A_1 \lhd A$), so zerfällt $\mathcal{N}C$.]

106/107

1. Frage über Matrizen:
   Gilt mein Satz über lin. Scharen mit reellen EWen schon im wesentlichen unter der schwächeren Vorauss., daß eine komplexe Zahl von den EWen ausgelassen wird ?
   Zu 106.1:

2. Die Bedingung $H^t \cap H^* = H \cap H^{*t} \quad (t \in G)$ ist gleichwertig zur starken Abgeschlossenenheit (SA) von H^* in M:
   $SA \to H \cap H^{*t} \subseteq H^* \cap H^t \to H^s \cap H^* \leq H^{*s} \cap H$; s/t
   $\downarrow$
   $H \cap H^* = H \cap H^{*t} \to H^{*t} \cap H \subseteq H^* \leftrightarrow SA$

3. [*Durchstreichung*
   Zu Burnsides p^a-Satz: Sei $|\mathfrak{G} : \mathcal{N}A| = p^\rho$. Schon jede Perm. Darstellung von $\mathfrak{G}$, welche einen Grad $\equiv 0(p)$ hat, enthält eine irred Darstellung $\neq 1$ mit $|\chi(A)| = \chi(E)$]

4. Vermutung: Ist $\mathfrak{G}$ p-perfekt, so ist die p-Sylowgr. von $\mathfrak{G}$ nicht ihr eigener Normalisator. Stimmt jedenfalls für auflösbare $\mathfrak{G}$ (Indukt mit minim NT).

107/108

[Als Blatt lose eingelegt:]
X zu S. 108 $\quad n = 26$

Beispiele von Festblöcke: Länge Index in $\mathfrak{S}_\alpha$

	0	1	2	3	4						10			13					18		20		22	23		25
0		x		x	x					x	x		x	x				x						x		x
1	x		x		x	x					x	x		x	x				x						x	
2		x		x		x	x					x	x		x	x				x						x
3	x		x		x		x	x					x	x		x	x				x					
4	x	x		x		x		x	x						x		x	x				x				
5		x	x		x		x		x	x						x		x	x				x			
6			x	x		x		x		x	x						x		x	x				x		
7				x	x		x		x		x	x						x		x	x				x	
8					x	x		x		x		x	x						x		x	x				x
9	x					x	x		x		x		x	x						x		x	x			
10	x	x					x	x		x		x			x						x		x	x		
11	x	x	x					x	x		x		x			x						x		x	x	
12	x	x	x	x					x	x		x					x						x		x	x
13	x	x		x						x						x			x	x	x	x			x	
14		x	x		x						x						x			x	x	x	x			x
15			x	x		x						x		x				x			x	x	x	x		
16				x	x		x						x		x				x			x	x	x	x	
17	x				x	x		x								x				x			x	x	x	x
18		x				x	x		x					x			x				x			x	x	x
19			x				x	x		x				x	x			x				x			x	x
20				x				x	x		x			x	x	x			x				x			x
21					x				x	x		x		x	x	x	x			x				x		
22						x				x	x		x		x	x	x	x			x				x	
23	x						x				x	x				x	x	x	x			x				x
24		x						x				x	x	x			x	x	x	x			x			
25	x		x						x				x		x			x	x	x				x		

$\boxed{\text{Hieraus folgt, dass } \mathfrak{G}_{0+1} = 1 \text{ ist, und } |\mathfrak{G}| = 26 \cdot 10 \cdot 3\text{: Gibt } \mathfrak{G}_{13} \lhd \mathfrak{G}}$!

$\mathfrak{G}_{01}$	0	| 1	|6 7 8 15 16 19 20 21 22|	2 5 11 14 18 24|	3 9 12 17	23 25|	4 10 13
10	1	1	$\underline{9}$	6	6		$\underline{3}$
$\mathfrak{G}_{02}$	1	1	$\underline{8}$	6	6		$\underline{4}$
15							

[Ende des eingelegten Blatts]

1. Gruppen vom Grad $2p = m^2 + 1$.
   $2p = 26$: Es gibt eine Matrix $X = \begin{pmatrix} A & B \\ B' & C \end{pmatrix}$ wo jede Teilmatrix Polynom im Zyklus P der Ord $p = 13$ ist:

$$\begin{aligned} A &= \sum_6 P^r \quad r\square \text{ Rest} : A = P + P^{-1} + P^3 + P^{-3} + P^4 + P^{-4} \\ C &= \sum_6 P^n \quad n\square \text{ nicht Rest} : \\ B &= 1 + \sum_3 P^m \quad m \text{ biquadr. Rest: } B = 1 + P + P^3 + P^{-4} \end{aligned}$$

   Wenn es eine primitive, nicht zweif. tra Gruppe $\mathfrak{G}_{26}$ des Grades 26 gibt, so vermutlich die Gruppe der mit X vertb. Permutationen (die tut es aber nicht!) In ihr ist $|\mathcal{N}\{P\}/\{P\}| = 3^\Delta$ und sie läßt sich vermutlich als P Gr auf dem $GF(27)$ darstellen unter Festlassung der 0
   Anderenfalls gibt es noch eine andere Matrix außer diesem X mit den richtigen EWen $10^1 \quad 2^{13} \quad -3^{12}$ * von obiger Form $\left(\begin{smallmatrix} A & B \\ B' & C \end{smallmatrix}\right)$ und $\mathfrak{G}$ besteht aus den hiermit vtb. Oder es gibt keine $\mathfrak{G}_{26}$
   * dh. so def $C = F - 1 - A$ und $A^2 + A + BB' = 6 + UF$ mit $F = \begin{pmatrix} 1 & \cdots & 1 \\ & \ddots & \\ 1 & \cdots & 1 \end{pmatrix}$
   Hieraus folgt, dass A aus $6\,P^\rho$ $(\rho \neq 0)$ besteht, C auch, B aus 4 $(\rho \underset{\neq}{=} 0)$

2. Gruppen mit halbreg Untergruppen:
   Ist etwa $\mathfrak{H} = \left(\begin{smallmatrix} H & \\ & H \end{smallmatrix}\right) < \mathfrak{G}$ halbrg, dh die H reg, so hat jedes mit $\mathfrak{G}$ vtb V die Form $\left(\begin{smallmatrix} X & Y \\ Z & U \end{smallmatrix}\right)$ wo $X, \ldots$ mit jedem H vtb ist. Man arbeitet im Matrizenring des Grades 2 über dem Gruppenring von H. Muss auch direkt zu begründen sein, ohne Vertbarkeit zu betrachten. Fortsetzung: 176

108/109

Uniprimitive Perm.-Gruppen.

1. Die mit einer trans PGr einzeln vtbaren Matrizen V bilden einen Stammring $\mathfrak{V}$, wie bekannt.

2. Genau dann ist $\mathfrak{G}$ imprimitiv, wenn es ein $V \in \mathfrak{V}$ gibt mit $V^2 = V \geq 0,\ V \neq 0, 1, \frac{1}{n}F$. oder mit $0 \leq V^2 \leq V$ oder mit $V \geq 0$ und $V^\infty \neq F\cdot$

const.
Bew: die Stellen V der 1. Zeile wo $V \neq 0$ bilden ein Impr System, da aus $1 \to \nu$ folgt $\nu' \to \nu''$.

$2'$. dh wenn es ein primäres V gibt, dessen Maximalwurzel mehrfach ist.

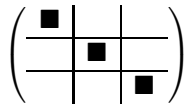
3. Genau dann ist $\mathfrak{G}$ 2-tra, wenn $\mathrm{Rg}\mathfrak{V} = 2$

4. Wenn in $\mathfrak{G}$ die Grade je zweier irred Bestandteile verschieden sind, dann hat jedes V mit rat Elementen auch rat EWe, also reelle EWe, und ist als normale Matrix dann symmetrisch. Dh jedes Transs von $\mathfrak{G}_1$ ist selbstgepaart.

109/110

Vertauschungsring $\mathfrak{V}$ einer Perm.-Gruppe

1. Kennt man $\mathfrak{V}$, so kann man den Obergruppenverbd von $\mathfrak{G}_1$ (einschl. Indizes) ermitteln: Die Idempotente ≥ 0 entsprechen eineind. den Obergruppen, die "Länge" ist der Index über $\mathfrak{G}_1$. ("Länge" = Zahl der El $\neq 0$ in einer Zeile)

2. Die Idempotente ≥ 0 sind symmetrisch
   Bew: Vertbarkeit mit $\mathfrak{G}$ benutzen, liefert $x =$ 

3. $\mathfrak{V}$ hat 3 Verknüpfungen:
   $\circ$ als Multipl entspr Elemente.
   Dazu eine Operation: $A \to \overline{A}'$
   " " $A \to \overline{A}$.

4. Die $\circ$-Idempotente sind die "primären" Größen.

Bemerkg über Matrizen der Ord p:
Haben zwei solche Matrizen gleichen Grad und die gleiche Spur, so haben sie dieselben Eigenwerte. Denn Darstellg durch p-te EWn ist **???**.

110/111

Perm - Gr mit 3 Tra Sy von $\mathfrak{G}_1$

$\mathfrak{V}$ hat EWe:

$V f \mathfrak{H}$	1	k	l
f	A	α	$-1-\alpha=\beta$
f'	A'	α'	$-1-\alpha'$

Es ergibt sich

$$k + f\alpha + f'\alpha' = 0 \quad \cdots$$
$$k^2 + f\alpha'^2 + f'^2\alpha'^2 = 0, \text{ wenn } f \neq f'$$

daraus

$$\alpha^2 f(n-1) + 2fk \cdot \alpha + k[f'(k-n)+k] = 0$$

und da α ganz ist: $f \mid nkl$, $f' \mid nkl$.
$f^2k^2 - f(n-1)k[f'(k-n)+k] = \square$ denn $= (af(n-1)+fk)^2$
Frame-Beweis zeigt $nkl = ff' \begin{vmatrix} 1 & 1 & 1 \\ 1 & \alpha & \beta \\ 1 & \alpha' & \beta' \end{vmatrix}^2 = ff'(\alpha'-\alpha)^2$
El. Teiler untersuchen insbes. für $p \nmid \alpha - \alpha'$.
Allgemein ist

$$n \begin{pmatrix} 1 & & \\ & k & \\ & & l \end{pmatrix} = \overline{\begin{pmatrix} & & \\ & & \\ & & \end{pmatrix}}' \begin{pmatrix} 1 & & \\ & f & \\ & & f' \end{pmatrix} \underbrace{\begin{pmatrix} 1 & k & l \\ 1 & \alpha & \beta \\ 1\alpha' & \beta' & \end{pmatrix}}_{\text{Det } = n(\alpha'-\alpha) = n\Delta}$$

Ferner ist:

$$\overline{\begin{pmatrix} & & \\ & & \\ & & \end{pmatrix}}' \begin{pmatrix} f^2+f & ff' \\ ff' & f'^2+f' \end{pmatrix} \begin{pmatrix} \alpha\beta \\ \alpha'\beta' \end{pmatrix} = n \begin{pmatrix} k & 0 \\ 0 & l \end{pmatrix}$$

NB: bei der pri Gr des Gr 21 ist $k = l = 10, \quad f = b \quad f' = 14$

In prim Gruppen ist $(k,l) \neq 1$ und $\sqrt{k} \leq l \leq k^2$
Stets ist $(f,f') \big| (k,l)$ nach 1. Elem-Teiler?
Daher $f = f' \to k = l$; also $k \neq l \to f \neq f' \to \alpha$ rat $\to \frac{n^2kl}{ff'} = \square$
NB: folgt auch direkt aus $ff'\Delta^2 = n^2kl$, da dann $(f,n) = 1$.

111/112

Satz: Ein trans. Konstit T von $\mathfrak{G}$ habe $|T| = p^\alpha$, $\alpha > 0$

Es gebe $P \in \mathfrak{G}$ so dass Ord $P = p^{\cdot\beta}$ und $\mathcal{Z}(P)$ transitiv und $P = \binom{1 \ \cdots}{\tau \ \cdots}$, $\tau \in T$.
Dann ist $\mathfrak{G}$ imprimitiv; genauer: $\mathfrak{G} \circ \{P\}$ ist ein intrans. NT von $\mathfrak{G}$; wenn dies $= 1$, so $\{P\} \lhd \mathfrak{G}$ intrans NT von $\mathfrak{G}$. Forts. 113
Bew: $\frac{p^\alpha}{g} \cdot \sum_{G \in \mathfrak{G}} P^G = V$, wo V primäre Größe.
Reduziere $\mathfrak{G}$ aus: in $\mathfrak{d}_\rho$ habe $P\chi_\rho$. Dann hat V in $\mathfrak{d}_\rho$ Charakter $p^\alpha\chi_\rho$ also ist $\frac{p^\alpha\chi_\rho}{f}$ ganz.
Sei $\mathfrak{d}_\rho \not\equiv 1$, sei $p \nmid f$. Dann ist $\chi_\rho \neq 0$; da $\chi_\rho \equiv f(\mathfrak{p})$.
also ist $P = \begin{pmatrix} \varepsilon_\rho & & \\ & \ddots & \\ & & \varepsilon_\rho \end{pmatrix}$ in $\mathfrak{d}_\rho$; $\mathfrak{G} \circ \{P\}$ hat $\begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix}$
also ist $\mathfrak{G} \circ \{P\} \lhd \mathfrak{G}$ intransitiv, andereseits $\neq 1$, da sonst $P \in Z(\mathfrak{G}) \cdots$, also $\mathfrak{G}$ imprimitiv.
Also aus $\mathfrak{d}_\rho \not\equiv 1$ folgt $p \mid f$, daher $n \equiv 1 \mod p$, aber dann lässt P eine Ziffer fest und ist $\equiv 1$ wegen $Z(P)$ tra.

112/113

Folge: Enthält $\mathfrak{G}$ eine reg abelsche p-Gruppe und hat $\mathfrak{G}_1$ ein Transs. T mit $|T| = p^\alpha > 1$, so $\mathfrak{G}$ imprim. (daher $\mathfrak{G}$ nicht einfach). Fortszg 115
Frage: kann man "abelsch" weglassen? Ja: S. 115

Aufgabe über Perm-Gr vom Grad $2p$; $p = 13$:
Es gibt eine Matrix $V = \begin{pmatrix} A & B \\ B' & C \end{pmatrix}$, wo $A \cdots C$ Polynome in P, $P'^3 = 1$ sind, Gr $N = 26$, derart, dass die EWe $10, 2^{13}, -3^{12}$ sind:

$$A = P + P^{-1} + P^3 + P^{-3} + P^4 + P^{-4} = \sum P^{\text{Rest}}$$
$$C = P^2 + P^{-2} + P^5 + P^{-5} + P^6 + P^{-6} = \sum P^{\text{Nichtrest}}$$
$$B = I + P + P^3 + P^{-4} = I + \sum P^{4.\ \text{Potenzrest} \quad \text{mod } 13}$$

Man suche Permutationen, die mit V vertauschbar sind. Vielleicht bilden sie eine tra (und dann unipri) Gruppe.

113/114

Monomiale Gruppen $\mathfrak{G}$

1. Der Satz von Frame gilt auch hier, wenn man nur diejenigen Transsysteme $(x_\alpha x_\beta \cdots) = T_\rho$ von $\mathfrak{G}_1 = (x_1) \cdots (x_\alpha \cdots x_{\beta_n} \cdots) \cdots$ berücksichtigt, die mit x_1 "gekoppelt" sind ($\varepsilon_1 = \varepsilon_\alpha$ f. alle $G \in \mathfrak{G}_{1\alpha}$):

$$\frac{n^r \prod_1^r n_\rho}{\prod_1^s f_\sigma^{e_\sigma^2}} = \frac{n^2}{d^2} \text{ ganz,}$$

wenn s = Anzahl der irred Bestandteile von $\mathfrak{G}$ $r = \sum e_\sigma^2$ und $d = \text{ggT}(f_1, f_2, \cdots, f_s)$.
Bew: denn wenn $\begin{pmatrix} w_{11} & \dots & w_{1s} \\ \vdots & & \\ w_{s1} & & w_{ss} \end{pmatrix} = W$ die Matrix der EWe der V_ρ mit $V_1 = I$, so ist

$$FW = \begin{pmatrix} f_1 & \dots & f_s \\ & & \\ & & \end{pmatrix} W = \begin{pmatrix} n & 0 \ \cdots \ 0 \\ & \\ & \end{pmatrix},$$

also $|W| = \frac{n}{d}$ = ganzalg
NB: f_σ steht e_σ^2-mal, und der Rest so gewählt, dass $|F| = d$

Genau dann sind alle Transs. mit x_1 gekoppelt (dh $\sum n_\rho = n$) wenn

aus $G_1^R = G_1'$ stets folgt $G_1 \equiv G_1' \mod \overline{\mathfrak{G}_1}$; dh wenn die Fokalgruppe $\mathfrak{G}_1 \square \mathfrak{G} \leq \overline{\mathfrak{G}_1}$

1. Satz: Sei $\mathfrak{G}$ Perm Gr des Grades $p^\alpha > p$, und $\mathfrak{G}_1$ habe ein Transs. T der Länge p^β. Dann ist $\mathfrak{G}$ imprimitiv. Einfacher Beweis 116 unten
   Kann vielleicht noch nach Muster von S. 112 ausgedehnt werden.
   Bew: Die zu T gehörige primäre Matrix V von $\mathfrak{G}$ ist auch primär für jede p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$.

2. Lemma: Für eine primäre Matrix V einer trans p-Gruppe ist nie $V^\infty > 0$; sogar $(E + V^p)^\infty = F$ ist nicht > 0.
   Bew: Die Transsysteme einer maximalen Obergruppe von $\mathfrak{P}_1$ betrachten.

   Bew 1: Also obiges V hat $(E + V^p)^\infty = F = F^2 \not> 0$, daher $\mathfrak{G}$ impr. oder $V^p = E$, dann aber $V =$ Permut., $p^\beta = 1$, $\mathfrak{G}$ impr

   Verschärfg: Es genügt: $\mathfrak{G}$ hat Gr $p^\alpha > 1$, $\mathfrak{G}_1$ hat ein Transgebiet, das ganz in einem Transgebiet einer maximalen Ugr von $\mathfrak{P}$ liegt. Dann ist schon $\mathfrak{G}$ impr. Verschfg 116

Trans-Systeme von $\mathfrak{G}_1$

Satz: Sei $\mathfrak{G}$ transitive Permgr; ein Transgebiet T von $\mathfrak{G}_1$ sei enthalten in einem Transsystem eines intra Normalteilers $\mathfrak{N}^*$ einer tra Ugr. $\mathfrak{U}$ von $\mathfrak{G}$. Dann $\mathfrak{G}$ imprimitiv
Bew. wie 115: Vergrössere die zu T gehör. primäre Matrix V von $\mathfrak{G}$ zu einer Vertauschmatrix von $\mathfrak{U}$ (die zu dem betrachteten Transs. des NT gehört). die neue Matrix ist eine "Permutationsmatrix mit Elementen der Gestalt $F = \left(\begin{smallmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{smallmatrix}\right)$, und keine Potenz von ihr ist > 0.
s. auch 115
Anwendung: Eine pri Gr des Grades 25 kann in $\mathfrak{G}_1$ nicht die Trans.-Längen $1, 4, 5, 5, 10$ haben.
klar, da [der Konst. von $\mathfrak{G}_1$ auf 4 Punkten] nicht eine durch 5 teilbare Ord hat.
Achtung: Das folgt unmittelbar aus meinem Impr-Kriterium in 46!

4. <u>Satz</u> Ist $\mathfrak{U} \leq \mathfrak{G}$ und sind B, Γ Festblöcke von $\mathfrak{U}$ bezw $\mathfrak{G}_1$, sodaß

   (a) $\Gamma \subseteq B$ und

   (b) $\frac{k_i}{b_i} \frac{|1^{\mathfrak{U}}|}{k} > \frac{2}{3}$ $(i = 1, \cdots s)$ wobei $B = B_1 \cup B_2 \cup \cdots \cup B_s$ (B_σ Tragebiet $\mathfrak{U}$) $b_i = |B_i|$, $k_i = |B_i \cap \Gamma|$, $k = \sum k_i = |\Gamma|$;
   so ist $\mathfrak{G}$ impri, B Block $\mathfrak{G}$.
   Bew wie 3 $\rightarrow$ Jede Spalte in B hat oben $> \frac{2}{3}k$ Einsen.

Über die Transit-Systeme von $\mathfrak{G}_1$ 8.10.58

1. Sei $\mathfrak{K} \subseteq \mathfrak{G}$ $1 \neq \alpha \in \Omega$, $|1^{\mathfrak{K}}| \geq |\alpha^{\mathfrak{K}}|$, $\alpha^{\mathfrak{G}_1} \subseteq \alpha^{\mathfrak{K}} < \Omega$. Dann $\mathfrak{G}$ imprim.
Bew: Sei V die zu $\alpha^{\mathfrak{G}_1}$ gehörige Vertauschmatrix
In den $|1^{\mathfrak{K}}|$ Zeilen von V mit den Nummern aus $1^{\mathfrak{K}}$ und den $|\alpha^{\mathfrak{G}_1}|$ Spalten mit Nummern aus $\alpha^{\mathfrak{G}_1}$ stehen nur Nullen ausser in Schnittpkten.
$V'V = \left(\begin{array}{c|c} //// & 0 \\ \hline & \end{array}\right)$ $1^{\mathfrak{K}}$.
$\alpha^{\mathfrak{G}_1}$
NB: Jede zerlegbare Matrix (≥ 0) in $\mathfrak{V}$ ist vollständig zerlegbar. Ist $\mathfrak{G}$ pri, so ist jedes zerlegbare V diagonal. Allgemeines Beweisprinzip; Grundlage:

2. Ist $\mathfrak{G}$ pri und ist $\mathfrak{S}$ irgend ein System von Spalten einer Matrix $V \in \mathfrak{V}$, so ist $\max\limits_{\alpha \in \mathfrak{S}, \beta \notin \mathfrak{S}} V'_\alpha V_\beta \geqq \max\limits_{\substack{\alpha,\beta \in \mathfrak{S} \\ \alpha \neq \beta}} V'_\alpha V_\beta =: \mu$ (V_β = Spalte von V)
Bew: sonst

$$V'V = \left(\begin{array}{c|c} \textbf{???} & \text{alle} \\ = \mu & < \mu \\ \hline & \end{array}\right) \quad \rightarrow \quad \left(\begin{array}{c|c} /// & 0 \\ \setminus\setminus\setminus & /// \end{array}\right) \neq \text{diag} \in \mathfrak{V} \Rightarrow \ \setminus\setminus\setminus > 0$$

Zussatz: Ist sogar max < min, sind die Nummern der Spalten in $\mathfrak{S}$ ein Block von $\mathfrak{G}$

3. Ist $\mathfrak{U} \leq \mathfrak{G}$, $\alpha \in \Omega$, $|1^{\mathfrak{U}}| > \frac{2}{3}|\alpha^{\mathfrak{U}}|$, $\alpha^{\mathfrak{G}_1} \leq \alpha^{\mathfrak{U}} \subset \Omega$, so $\mathfrak{G}$ impr., u. zwar ist $\alpha^{\mathfrak{U}}$ ein Block von $\mathfrak{G}$
Bew:

$$V = \left(\begin{array}{c|c|c} 0 & \mathfrak{S} & 0 \\ \hline & /// & \end{array}\right) \quad \Big\} 1^{\mathfrak{U}} \qquad \leftarrow$$
$\underbrace{\qquad}_{\alpha^{\mathfrak{U}}}$

zu $\alpha^{\mathfrak{G}_1}$ betrachten.
$\boxed{///}$ enth. insgesamt $k(|\alpha^U| - |1^U|)$ Einsen
NB: $\geqq$ wäre falsch: $\frac{2}{3}$ ist optimal: Stelle $\mathfrak{S}_5$ auf den 10 Paaren dar, $\mathfrak{U} = \mathfrak{S}_4$. Die Spalten aus $\mathfrak{S}$ enthalten im Mittel also wegen $VU = UV$ einzeln unten nur $< \frac{k}{3}$ Einsen ($k = |\alpha^{\mathfrak{G}_1}|$), daher

$$\left\{\begin{array}{lll} V'_\alpha V_\beta < \frac{k}{3} & \text{für} & V_\alpha \in \mathfrak{S},\ V_\beta \notin \mathfrak{S}. \\ V'_\alpha V_\beta > \frac{k}{3} & \text{für} & V_\alpha, V_\beta \in \mathfrak{S} \end{array}\right\} \quad \text{Nach 2 ist } \mathfrak{G} \text{ impr}$$

Wieso: wohl Trug Fortsetzung 4. auf S. 116
[Hierbei spielen die Vert Matrizen eigentlich keine Rolle!]

Maximale uniprimitive Untergruppen der $\mathfrak{S}^n$.

1. Sei $\mathfrak{G}$ max unipri, $S \in \mathfrak{S}^n$, $S \in \bigcap_{G \in \mathfrak{G}} G\mathfrak{S}^n_{12}\mathfrak{G}$. Dann ist $S \in \mathfrak{G}$.
   Bew: Sei V die Vertauschungs-Matrix von $\mathfrak{G}$ mit $V_{12} = \begin{pmatrix} 0 & 1 & \cdot & \cdot \\ \cdot & 0 & \cdot & \cdot \\ & & & \end{pmatrix}$.
   Dann führt S V in sich über, also $\{S, \mathfrak{G}\}$ mit V vertauschbar da $V \neq \left(\begin{array}{ccccc|c} 0 & 1 & 1 & 1 & 1 & \cdot \\ 1 & 0 & 1 & 1 & 1 & \cdot \\ 1 & 1 & 0 & 1 & 1 & \cdot \end{array}\right)$, ist $\{S, \mathfrak{G}\}$ nicht 2-tra, daher $S \in \mathfrak{G}$.

2. Sei $2^{\mathfrak{G}_1} = \Gamma$. $\mathfrak{G}$ enthalte Elemente $\binom{1\ 2\ \cdot}{2\ 1\ \cdot}$ und $\binom{1\ \gamma\ \cdots}{2\ \gamma\ \ldots}$ zu jedem $\gamma \in \Gamma$. Dann ist $\mathfrak{G}$ 2-tra oder imprimitiv. Besser: S. 121
   Bew: Zu jedem Paar α, β, zu dem es $G = \binom{1\ 2\ \cdots}{\alpha\ \beta\ \ldots} \in G$ gibt, gibt es ein $H \in \mathfrak{G}$ mit $(\alpha, \beta)_H = (\ \alpha\beta)_T$, wo $T = (12)$. (Bew. mit Fallunterscheidung $\alpha, \beta \geqq 2$)
   $\leqq$
   Ist $\mathfrak{G}$ pri, so lässt T die zu G gehörige Matrix V_{12} fest, das gleiche gälte für $\{G, T\} = \mathfrak{S}^n$, also ist $V_{12} = F - I$.

3.a) G pri, G_1 2-tra auf $2^{\mathfrak{G}_1} \ni 3$, $(12)\cdots \in \mathfrak{G}$, $(3)(12)\cdots \in G \to G$ 3-tra. Besser 121

1. Z.B.: $n \geq 4$, G_1 hat Trasyst $1|23|\cdots$,
   $\mathfrak{G}$ enthält $\binom{1\ 2\ \cdot}{2\ 1\ \cdot}$, $\binom{1\ 3\ \cdot}{2\ 3\ \cdot} \to \mathfrak{G}$ imprim

Über Vertauschungsringe:

Sei $\mathfrak{U} < \mathfrak{G}$; $\mathfrak{V}$ zu $\mathfrak{G}_1$.

2. Der Modul der n-Spalten, die auf jedem Transsyst. von $\mathfrak{U}$ konstant sind wird durch $\mathfrak{V}$ in sich übergeführt.

3. Sei m die kleinste Translänge von $\mathfrak{G}_1$ ausserhalb (1). Sind die Länge der Transsysteme von $\mathfrak{U}$ entweder "kurz" (dh $\leq$ ein l) oder "lang" ($> m\ l$), und gibt es beides, so ist das Produkt $V_m \cdot T_l = \sum$ kurz, daher G imprimitiv.

4. Schneidet man aus $V \in \mathfrak{V}$ eine Teilmatrix aus, deren Zeilen- und Spaltennummern je einem Transsystem von $\mathfrak{U}$ angehören, so hat diese Teilmatrix in jeder $\left\{\begin{array}{c}\text{Zeile}\\ \text{Spalte}\end{array}\right\}$ gleich viele Einsen. Damit: 5. "Kurz" mal "teilerfremd zum maximal" (beides für $\mathfrak{G}_1$) = Kurz: $\mathfrak{G}$ impr, wenn max teilerfremd zu etwas
   (beides für $\mathfrak{G}_1$)

5. $\mathfrak{G}$ ist primitiv genau wenn für $V \geq 0$, $V \neq I$ stets V^*V "primitiv" im Sinne von Perron-Frobenius

Transitivitäts-Systeme

1. Sei M = grösste Tra Länge von $\mathfrak{G}_1$ ausserhalb (1), $\mathfrak{G}$ tra.
   Sei $\mathfrak{U} < \mathfrak{G}$, $\mathfrak{U}$ habe zwei Tra-Längen k, l. Dann ist $M \geq \frac{l}{(k,l)}$, insbesondere $l \leq Mk$.
   Bew: $\mathfrak{U}_\kappa$ betrachten, $\kappa \in \{k\}$.

2. Sei $\mathfrak{U} < \mathfrak{G}$, Γ ein TraSy $\mathfrak{U}$. Dann ist in jedem $\mathcal{N} \in \mathfrak{V}_\mathfrak{G}$ der "Diagonalkasten" Γ, Γ in $\mathfrak{V}_\mathfrak{U}$. Wenn $\mathfrak{U}_\Gamma^\Gamma$ 2-Tra, $\mathfrak{G}$ pri, enthält der Kasten nur Nullen
   (da sonst $V = V'$ und $\begin{array}{c} \\ 1 \\ \vdots \\ 1 \end{array} \begin{array}{c} \begin{array}{ccc} 0 & 1 & 1 \end{array} \\ \left[\begin{array}{ccc} 0 & & 1 \\ & \diagdown & \\ 1 & & 0 \end{array}\right] \end{array}$ auf impr. $\mathfrak{G}$ führt).

2′. In einer pri $\mathfrak{G}$ mit einem 2-tra Konst $\mathfrak{G}_1^\Gamma$ gibt es kein El. das 1 und noch eine der Ziffern von Γ nach Γ bringt.

3. Sind Γ, Δ zwei Tra Sy von $\mathfrak{U} < \mathfrak{G}$, $V_\mathfrak{G} = \begin{array}{c} \\ \Delta \end{array} \overset{\Gamma}{\left(\begin{array}{|c|c|c|} \hline & & \\ \hline & W & \\ \hline & & \\ \hline \end{array}\right)}$,

   so ist $\begin{cases} W'W \text{ mit } \mathfrak{U}^\Gamma \text{ elementw vtb.} \\ WW' \text{ mit } \mathfrak{U}^\Delta \text{ elementw vtb.} \end{cases}$

Transit.-Systeme von $\mathfrak{G}_1$

1. Sei $\Delta = \{2, 3, \ldots, k\}$ ein Transs. von $\mathfrak{G}_1$. Zu jedem $\delta \in \Delta,\ \delta > 2$ gebe es $G \ni \mathfrak{G}$ mit $G = \left(\begin{smallmatrix} 1 & \delta' & \cdots \\ 2 & \delta & \ldots \end{smallmatrix}\right)$, $\delta' \in \Delta$. Dann bilden $1 \& \Delta$ einen Block von $\mathfrak{G}$; also $\mathfrak{G}$ impri, wenn $1 + \Delta \neq \Omega$
   NB: Die Forderung $G \ni (12)\cdots$ von S. 118 ist unnötig.
   Bew: Das V_Δ von $\mathfrak{G}$ ist

$$V_\Delta = \begin{array}{c} \\ \Delta \end{array} \overset{\Delta}{\left(\begin{array}{|c|c|c|} \hline & 1\,1\,1\,\cdots\,1 & \\ \hline & 1\,1\,\cdots\,1 & \\ \hline & & \\ \hline & & \\ \hline \end{array}\right)}$$

also, da W in der ersten Spalte soviel 1-Elemente hat wie in der ersten Zeile,

$$V_\Delta = \left(\begin{array}{c|cccccc} & 1&1&1&1&\cdots&1 \\ \hline & &1&1&1&\cdots&1 \\ & 1& & & & & \\ & 1& & & & & \\ & 1& & & & & \\ & 1& & & & & \\ \hline & & & & & & \end{array}\right)$$

Also $V_\Delta = V'_\Delta$, und wegen Transitivität von $\mathfrak{G}_1$ auf Δ hat jede Zeile von W ebensoviel 1-Elemente, daher

$$V_\Delta = \left(\begin{array}{c|ccccc|c} 0 & 1 & 1 & 1 & 1 & 1 & 0\ \cdots\ 0 \\ \hline 1 & 0 & 1 & 1 & 1 & 1 & \\ 1 & 1 & 0 & 1 & 1 & 1 & \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & & & & \ddots & & \\ 1 & 1 & 1 & 1 & & 0 & \\ \hline 0 & & & 0 & & & /\!/\!/ \end{array}\right), \text{ gibt } 1+\Delta = \overset{\text{Impri-}}{\text{system}}$$

1′. Sonderfall: G_1 2-tra auf Δ : $\mathfrak{G} \ni \left(\begin{smallmatrix} 1 & \delta' & \cdots \\ 2 & \delta & \cdots \end{smallmatrix}\right)$ für <u>ein</u> δ genügt für $1+\Delta$ Block $\mathfrak{G}$.

1″. Allgem. Formulierung: Sei $\beta \neq \alpha,\ \Delta = \beta^{\mathfrak{G}_\alpha}, \mathfrak{R} = \mathfrak{G}_*(\alpha\beta\ldots) \subset \mathfrak{G}$ und $|\Delta \cap \Delta^{\mathfrak{R}}| = n-1$. Dann $1+\Delta$ Block $\mathfrak{G}$.
NB: Die Vor besagt $|\Delta \cap \Delta^G| = n-1$ für $\underset{\text{ein}}{\text{jedes}}\ G = \left(\begin{smallmatrix} 1 & \cdots \\ 2 & \cdots \end{smallmatrix}\right) \in \mathfrak{G}$
gleichwertig: $\cdots \qquad \cdots$.

2. Genau dann ist $1+\Delta$ ein Block von $\mathfrak{G}$, wenn $|\Delta \cap \Delta^G| \geq |\Delta| - 1$ für jedes $G = \left(\begin{smallmatrix} 1 & \cdots \\ \delta & \cdots \end{smallmatrix}\right) \in \mathfrak{G}$. Denn V_Δ symmetrisch.

1. Bei Betrachtung von <u>Vertauschungsmatrizen</u> sollte folgender Satz über Matrizen nützlich sein:
Sei M quadratisch, $\mathfrak{e} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$; $|M\mathfrak{e}| = |M^*\mathfrak{e}|$, $M^*M = aI + bF$ $(F = (1))$;
MM^* hat auch alle Diag-Elemente $= a$. Dann ist auch $MM^* = aI + bF = M^*M$.
Bew: $MM^* = \begin{pmatrix} a & p & q & & \cdots \\ p & a & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix}$ hat dieselben EWe wie M^*M und

ist auch hermitesch, also $\vartheta^2(M^*M) = \vartheta^2(MM^*)$, daher $2(p^2+q^2+\dots) = m(m-1)b^2$, wenn Grad $M = m$. Ferner ist $2(p+q+\dots) = m(m-1)b$, wegen $\mathfrak{e}^*M^*M\mathfrak{e} = \mathfrak{e}^*MM^*\mathfrak{e}$. Da $p, q, \cdots$ dieselbe Summme und Quadratsumme wie die $m(m-1)$ übereinstimmenden Werte b haben, sind sie $= b$.

2. Zu Untersuchung von 2-tra Konstituenten T von $\mathfrak{G}_1$ scheint es (nach Mannings Beweis 1929) zweckmäßig die Matrix $V \in \mathfrak{V}_G$ zu betrachten, für die $V_{\Gamma\Gamma} = F - I$.

1. $\mathfrak{G}$ 2-tra, $\mathfrak{G}_1$ nilp $\rightarrow \mathfrak{G} \neq \mathfrak{G}'$
   Bew: "Existenz von NT... .

2. Vor: $\mathfrak{G}$ 2-tra; $\mathfrak{G}$ einfach $\rightarrow \mathfrak{G}_{12}^{\mathfrak{G}_1} = \mathfrak{G}_1$.

Aufgabe über Matrizen: Alle Matrizen M gegebenen Typs zu bestimmen mit $m/k = 0, 1$; $M^*M = a+bF$, sowie die mit ihnen vertauschbaren Permutationen. bei quadr. Matrizen, $n \times n$, gibt es stets die folgenden trivialen Lösungen:
a) $M = 0$ b) $M =$ Permutation
a′: $F-$ a) b′: $F-$ b) inbes. $M = M'$ untersuchen!
Bei $n \leq 5$ gibt es nur diese; warum noch? oBdA $M \geq E$. Für ein solches n gilt: Sind in einer PGr $\mathfrak{G}$ bei $\mathfrak{U} < \mathfrak{G}$ zwei trans Konstituenten des Grades n vorhanden u. einer davon 2-tra, so sind sie entweder bei geeigneter Bezifferung identisch, oder in i oder Vert-Matrix V von G ist der zugehörige Block $= 0$ oder F.

Jedenfalls sind alle $n \times n$ Matrizen mit dieser Eigenschaft normal nach 122.1

Aufgabe:

1) Minimalgrad $1\frac{1}{2}$-fach transitiver Gruppen $\geq$?

2) Zusammenhänge zwischen den transit. Konstituenten von $\mathfrak{G}_1$ der $\frac{3}{2}$-tra $\mathfrak{G}$?

3) Sind imprim. Normalteiler Frobenius'sch?

Frage: Kann man bei PGr mit reg Ugr $\mathfrak{R}$ vom Grad $3p$ Nutzen daraus ziehen, dass $\mathfrak{R}$ "Körperautomorphismen" besitzt, die $P \rightarrow P^\alpha$ überführen? "$K - A$" heißt: Es gibt eine Darstellung von $\mathfrak{R}$ (im Körper der p-ten EW) derart dass $P \rightarrow P^\alpha$, $D \rightarrow D$ ($D^3 = 1, D$ fest) durch $\varepsilon \rightarrow \varepsilon^\alpha$ bewirkt wird ($\varepsilon^p = 1$); nämlich irred. Darst. von $\mathfrak{R}$ tun das.

Aufgabe: Die (prim-)S-Ringe über den nichtabelschen Gruppen der Ordnungen $2p, 3p$ algebrentheoretisch aufstellen, insbesondere die kommutativen; darunter wieder die aus symmetrischen Matrizen bestehenden ($\kappa = \kappa^*$) s. S 125

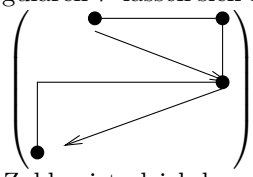
Sei $\mathfrak{V} = S.$-Ring über $\mathfrak{G}_{3p}$
$\mathfrak{V}_0 =$ Unterring mit Koeff-Summe 0; (rat Koeff.) $\mathfrak{V}_0$ wird durch jede irred Darst $\mathfrak{d}$ des Grades 3 von $\mathfrak{G}_{3p}$ treu dargestellt. Wenn $\mathfrak{V}$ durch Einbettung entsteht, enthält $\mathfrak{V}_0$ keine Diagonalmatrix ausser rat$\cdot$ I. Denn mit dieser wäre $1P \in \mathfrak{G}_{3p}$ elweis vtb, dh. oBdA: $\mathfrak{G}(=$ Einbettung) enthält $\mathfrak{G}_{3p} \times (\mathfrak{G}_{3p}^*)_p$, dann aber ist $p^2|g$, $\mathfrak{G}$ impr oder 2- tra. Hieraus folgt Rg $\mathfrak{V}_0$: Compl ≤ 9, bei Kommutativität von $\mathfrak{V}$ sogar ≤ 3. Durch Betrachtung der Körper, die in $\mathfrak{V}_0$ als direkte Summanden enthalten sind, sollte genaueres herauskommen; es sind lauter Kreiskörper, da wegen Erzegbarkeit des Vert Rings durch Ähnlklassen von $\mathfrak{G}$ alle EWe der Matrizen V im g-ten Kreisteilgskörper liegen. Wenn $\mathfrak{V}$ kleinen Rang hat, ergibt Betrachtung der reg Darst. von $\mathfrak{V}$ in $\Gamma(\mathfrak{H})$ Aussagen über Rationalität der Charaktere.
Falls kommutativ, aber $\mathfrak{V}_0$ nicht ein Körper, gibt es in $\mathfrak{d}$ eine Matrix

$$E = \begin{pmatrix} \alpha & \beta & \gamma \\ \gamma' & \alpha' & \beta' \\ \beta'' & \gamma'' & \alpha'' \end{pmatrix}$$

wo $\alpha, \alpha', \alpha''$ konj: $Z =$ Körper vom Grad $\frac{p-1}{3}$ in Rat$(\sqrt[p]{1})$
$E = \overline{E}' = \frac{1}{3}E^2$, Rg$E = 1 \to \alpha\alpha' = \beta\overline{\beta}$, $\alpha\alpha'\alpha'' = \beta\beta'\beta''$, $\alpha^{(i)} > 0$, $\sum \alpha^{(i)} = 1$
Die Anzahl der Körper im komm. $\mathfrak{V}$ ist gleich Anzahl der rat-irred. Bestandteile von $\mathfrak{G}$

Hat in einer pri $\mathfrak{G}$ die Gr. $\mathfrak{G}_1$ die Translängen $1, k, l, -, m$ mit $m =$ max, so ist $\frac{m}{(k,m)} \leq m'$, wo m' die zweitgrößte unter den verschiedenen Translängen von $\mathfrak{G}_1$ ist, denn sonst wähle $\alpha \in k$, dann sind die langen Transs. von G_1, auch solche von $\mathfrak{G}_\alpha$.
Z.B. können bei $\mathfrak{G}$ pri, Grad $= 39$ nie $1, 12, 26$ auftreten.

Den Satz über die prim Gr mit einer Translge 2 von $\mathfrak{G}_1$ kann man so beweisen: Zur regulären V lassen sich die auftretenden Paare in zykl. Reihenfolgen bringen

durch 

Jeder Zyklus ist gleich lang und $\mathfrak{G}$ transformiert jeden Zyklus in einen Zyklus. Aus Primitivität folgt daß jeder Zyklus alle n Zeilen (und Spalten) bewirkt, also gibt es 2 Zyklen der Lge n. Der Normalteiler, der jeden in sich überführt, hat Index 2 und ist zyklisch (also wegen Prim. von der Ord p). Frage: Ähnliches für Translge 3?

Zur "symbolischen Potenzierung" in rat-zahligen Vert-Ringen $\mathfrak{V}$ von $\mathfrak{G}$

1. Nenne eine Matrix $V \in \mathfrak{V}$ positiv, wenn ihre Elemente ≥ 0 sind; schwach positiv, wenn für jedes $G \in \mathfrak{G}$ Spur $GV \geq 0$ ist.

2. Sei $\mathfrak{V}$ abelsch und $\alpha \to \tilde{\alpha}$ ein Autom des EW-Körpers von $\mathfrak{V}$. Setze $\tilde{V} =$ die Matrix aus V, deren EWe aus den entsprechenden von V durch $\alpha \to \tilde{\alpha}$ hervorgehen.

3. Satz: Die Abb $V \to \overline{V}$ führt schwach positive V in ebensolche über. Denn
   $\mathrm{Spur}\langle\tilde{G}\rangle\overline{V} = \mathrm{Spur}\langle G\rangle V = g\mathrm{Spur}GV$
   Daher $\langle G\rangle = \sum\limits_{H\in\mathfrak{G}} H^{-1}GH$, $\langle\tilde{G}\rangle = \sum H^{-1}G^{\rho}H$, wo $\tilde{\varepsilon} = \varepsilon^{\rho}$ für ein prim g-te EW.

4. Wenn jedes primäre $V \in \mathfrak{V}$ eine "Klassenmatrix" const $\langle G\rangle$ ist, dann ist mit V auch stets $\overline{V}$ primär. Denn hier ist schwach pos $\equiv$ pos, also führt $\tilde{V}$ die Kanten des pos. Kegels in sich über, d sind die primären V_i.

5. Ein V_i zum Schur-Komplex $\mathfrak{K}_i$ ist sicher dann eine Klassenmatrix, wenn es ein $K \in \mathfrak{K}$ gibt, dessen Zentralisator in $\mathfrak{G}$ trans. ist (z.B. wenn $K \in$ Zentrum der reg. Ugr.)

6. Also wenn in jedem prim. Komplex $\mathfrak{K}_i$ ein K_i existiert, dessen Zentralisator in $\mathfrak{G}$ transitiv ist, dann gibt es zu jedem h mit $(h, g) = 1$ ein $\mathfrak{K}_i^{(h)} \ni K_i^h$, derart dass die Abb einen Autom des S-Rings bewirkt; es ist $|\mathfrak{K}_i^{(h)}| = |\mathfrak{K}_i|$ da der max EW und $\mathfrak{d}^2$ erhalten bleibt: Der Automorphismus kann durch Ähnlichkeitstransf. mit einer geeigneten unitären Matrix bewirkt werden, da man $\mathfrak{G}$ unitär und algebraisch ausreduzieren kann.

7. Überhaupt gibt es zu jedem primären $\mathfrak{K}_i$, das ein $Z = K_i$ und trans. Zentralisator enthält, so ein $\mathfrak{K}_i^{(h)}$, wie in (6) für jedes $(h, g) = 1$; $\mathfrak{K}_i^{(h)} = (Z^h)^{\mathfrak{G}} = (Z^h)^{\mathfrak{G}_1}$.
   ($\mathfrak{V}$ braucht nicht einmal abelsch zu sein) Bew wie 6.

8. Sei $\mathfrak{V}$ abelsch, jedem $V = \sum a_\nu G_\nu^{\mathfrak{G}}$ werde für $(h, g) = 1$ zugeordnet $V^{(n)} = \sum a_\nu G_\nu^{h\mathfrak{G}}$; ist eindeutg. Dann ist $V \to V^{(h)}$ ein Modulautom von $\mathfrak{V}$ über Ra. Wenn die Transformationsmatrix ganzzahlg, dann ist das sogar ein Modulautom von $\mathfrak{V}$ über ganzen Zahlen, es geht jedes primäre V_i in ein ebensolches über, **???**. (Induktion von dem kurzen V_i her).

8′. Wenn $V_1 = I$, $V_2, -, V_r$ alle primären V_{ij} und wenn der $(n-1)$-te Det Teiler der Matrix Spur $G_\alpha V_\beta$ $(\alpha = 1 - g;\ \beta = 2 - r)$ gleich d ist, so ist $d \cdot C$ ganzzahlig, wo C die Transform. Matrix $V_i \to V_i^{(h)}$ ist. Also:

8″. Wenn Spur$G_\alpha V_\beta$ $\alpha = 1$ hat, so ist für primäres V_i auch stets $V_i^{(h)}$ primär und ebenso lang wie V_i.
Ebenso wirds wohl gehen, wenn die ganzzahlige Matrix, vermöge der sich die Klassen durch die V ausdrücken, den ggT 1 der Unterdet hat.

Noch Vertauschungsringe $\mathfrak{V}$ von Matrizen

9. Sei $\mathfrak{V}$ abelsch, $V_0 = I$, $V_1 \cdots V_s$ die übrigen prim. Matr. $\in \mathfrak{v}$. $\mathfrak{v} = \begin{pmatrix} V_1 \\ \vdots \\ V_s \end{pmatrix}$;
$\mathfrak{c} = \begin{pmatrix} C_1 \\ \vdots \\ C_r \end{pmatrix}$ wo $C_0 = I$, $C_1 \cdots C_r$ die übrigen **???**-Summen der Klassen konj. Elemente in $\mathfrak{G}$ $(h, g) = 1$
Dann ist $\mathfrak{v}^{(h)} = Q\mathfrak{v}$, $\mathfrak{c}^{(h)} = P\mathfrak{c}$ und mit der (geg.) Matrix T aus $\mathfrak{c} = T\mathfrak{v}$ gilt dann

$$\boxed{PT = TQ}$$

Mit $N = \begin{pmatrix} n_1 & & \\ & \ddots & \\ & & n_s \end{pmatrix}$ n_σ = Grade der nichttriv. Transs von $\mathfrak{G}_1$ gilt

$$\boxed{QNQ' = N}.$$

Setzt man also $N^{-\frac{1}{2}} Q N^{\frac{1}{2}} = R$, so wird $RR' = I$. Sei $P_1 v P$, sonst beliebg, nur sei $U = PT$ ganzzahlg. Dann ist auch $PU = UQ$, wenn also der ggT der D_s von U d ist, ist $\boxed{dQ \text{ ganzzahlig}}$.

10. Wenn Q ganzzahlig oder ≥ 0, ist Q eine Permutation.
Denn $Q = N^{\frac{1}{2}} R N^{-\frac{1}{2}}$, R orthogonal, und $\mathfrak{e}Q = \mathfrak{e}$ mit $\mathfrak{e} = (1 \ \cdots \ 1)$

11. Wenn Q eine Perm, existiert in ganzz. $\mathfrak{V}$ die Abb $V \to V^{(n)}$ als Autom. und Fortsetzg von $\langle G \rangle \to \langle G^n \rangle$.
Praktisch rechnet man Q besser aus $P'S = SQ'$ aus, wo

$$S = (\mathrm{Sp}\, G_\rho V_\sigma) \qquad G_\rho \in C_\rho :$$

S hat im Mittel kleinere El als T.
Es ist $LS = nTN$, $L = \begin{pmatrix} e_1 & & \\ & \ddots & \\ & & e_r \end{pmatrix}$

1. Bei der Berechng der Matrix S ist die Kenntnis einer reg Ugr $\mathfrak{R}$ von G nützlich: $R_\rho^R = (1, \alpha_R \cdots)() \cdots \to S_{\rho\sigma}$ = Anzahl der α_R in Transs. $T_\sigma \cdots$.

2. Hat eine Gr des Grades $3p$ irred Bestandteile des Grades $1, 2p, p-1$, so hat eine der beiden primären Matrizen dazu die EWe k, $\frac{p-1-k}{2}$, $-p+k$ mit $k = p \pm \sqrt{\frac{12p-3}{9}}$
daher ist dann $3p = m^2 + m + 1$, $p = 3x^2 + 3x + 1 = 7, 19, 37, 61, \cdots$ und bei $p = 19$ kommen nur die Translängen $3 \cdot 19 = 1 + 24 + 32$ [vor].

3. Über irred. Bestandteile mit rationalen Charakteren.
Sei $\mathfrak{G}$ eine endl. Gr. linearer Substitutionen.

   a) Wenn für jede Matrix $\hat{H} = \sum_{G \in \mathfrak{G}} G^{-1}HG$ $(H \in \mathfrak{G})$ gilt
   Spur $G\hat{H}$ = Spur $G^h\hat{H}$ für jedes $(h, g) = 1$, $G \in \mathfrak{G}$, so haben alle Bestandteile von G rat Charaktere.

   b) Wenn $\cdots$ $\cdots$ haben, gilt sogar Spur GV = Spur G^hV für jedes $(h, g) = 1$, $G \in \mathfrak{G}$, und jede mit $\mathfrak{G}$ elementweise vertauschbare Matrix V.

4. Wenn G transitive PGr mit lauter rat-Char irr Bestandt, so gibt das Aussagen über die Transsysteme von $\mathfrak{G}_1$.

5. Entsprechendes gilt für andere Grdkörper, dann werden nur die h eingeschr.

131/132

1. Sei $P = \begin{pmatrix} 1 & & & \\ & \varepsilon & & \\ & & \ddots & \\ & & & \varepsilon^{p-1} \end{pmatrix}$, $\varepsilon^p = 1$, und es mögen nicht alle primit. p-ten EW auftreten. Ist dann Spur $P^\alpha G$ rational, dh. im Körper der p-fremden EWn. $(\alpha = 0 \cdots p-1)$, so ist $G = \begin{pmatrix} a & & & & \\ & 0 & & * & \\ & & 0 & & \\ & & * & \ddots & \\ & & & & 0 \end{pmatrix}$.
   Bew: $\begin{pmatrix} 1 & 1 & n \\ 1 & \varepsilon & n \\ \tau & \varepsilon^2 & \end{pmatrix} = W$; $G = \begin{pmatrix} x_1 & & \\ & \ddots & \\ & & x_n \end{pmatrix}$
   $W\mathfrak{x} = \mathfrak{e}$ rational $\rightarrow$ $\mathfrak{x} = W^{-1}\mathfrak{e}$, Die Zahlen nach der ersten in $W^{-1}\mathfrak{e}$ sind dann alg. konjugiert, aber eine ist 0. (zur fehlenden EWn).

2. Ebenso wenn

$$P = \left(\begin{array}{ccc|c|c} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ \hline & & & \varepsilon & \\ & & & \ddots & \\ & & & & \varepsilon \\ \hline & & & & \ddots \\ & & & & \end{array}\right),$$

hier ist $G = \begin{pmatrix} \Delta & & * \\ & B & \\ * & & C \end{pmatrix}$ mit $0 = \text{Spur } B = \text{Spur } C = \cdots$.

3. Die Vor ist erfüllt insbesondere wenn $G \in \mathfrak{N} - \mathfrak{P}$, wo $\mathfrak{P} \lhd \mathfrak{N}$ mit p-freiem Index; $\mathfrak{P} = \{P\}$.

Infrainvariante Untergruppen sind von Smirnov behandelt worden (Lit Kurosh, II)

Exponent einfacher Charaktere

1. Teilt man die Werte eines einfachen Char. von G irgend wie in 3 getrennte (auch leere) Häufchen
$\varphi \quad \chi \quad \psi$, und erzeugen diese die Körper
$K \quad L \quad M$,
so gibt es unter diesen Körpern zwei, deren Durchschnitt im dritten liegt.
Bew: Sonst wähle Autom
$-$ lässt M fest, aber $K \cap L$ nicht
$\sim$ lässt L fest, aber $M \cap K$ nicht
$*$ lässt K fest, aber $L \cap M$ nicht
und bilde $\simeq \overset{*}{\sim} \; -* \; \simeq *$, mit geeigneten (8) Vorzeichen ± 1 summiert gibt das 0, obwohl alle 8 Char. verschieden und daher lin un sind.

2. Ähnlich beweist man: Einteilg in 2 Häufchen gibt

K	L	
φ	χ	1
$\overline{\varphi}$	χ	-1
φ	$\tilde{\chi}$	-1
$\overline{\varphi}$	$\tilde{\chi}$	1
0	0	

Also $MK \subset L$ oder $L \subset K$.
Verschärfung von 1:

3. Es zeigt sich: Entweder ist $K \subseteq L$ oder $L \subseteq M$ oder $M \subseteq K$ oder $|KL : L| = |LM : M| = |MK : K| = 2$ mit $KL = LM = MK = KLM$, $K \cap L = L \cap M = M \cap K$.
   Aufgabe: Dann Existenz von $\exists \exp G = p^\alpha q^{\beta_r \gamma}$ wenn $p^\alpha q^{\beta_r \gamma} \Big| \exp x$?

133/134

Exponent eines einfachen Charakters

Sei $\chi(G)$ ein einfacher Char von $\mathfrak{G}$, X der von ihm erzeugte Körper.

1. Unter den $\chi(G)$ findet sich eine Basis von X.
   Denn $\chi(G)\chi(H) = \sum \cdots \chi(\mathfrak{J})$.

2. Es gibt keine zwei echten Teilkörper K, L von X, derart dasss alle $\chi(G) \in K \cup L$. Sonst wähle Basis X aus den $\chi(G)$, davon $\leq \frac{|X|}{2}$ in K, weitere $\leq \frac{|X|}{2} - |K \cap L|$ in L, Summe ist $< |X|$. W!

3. Nun seien $p^{\alpha+1}, \cdots, q^{\beta+1}, \cdots, r^{\gamma+1}, \cdots$ Exponenten von gewissen $\chi(G)$, und $\alpha\beta\gamma > 0$ maximal gewählt.
   Dann gibt es einen Exp $\chi(H) = p^{\alpha+1} q^{\beta+1} r^{\gamma+1} \cdots$.
   Bew: Sonst $X = X_{\frac{m}{p}} \oplus X_{\frac{m}{q}} \oplus X_{\frac{m}{r}} \oplus \cdots$ wo $X_k = X \cap K_k$· Aber es gilt:

4. Ist X ein Normal - Körper und sind $X_1, \ldots, X_n$ Teilkörper mit paarweise teilerfremden Graddefekten in X, so ist $X \neq \sum X_\nu$.
   Bew: Sonst wähle zu jedem X_ν ein Element P_ν der Ord p_ν der Galoisgr von X durch dass $p_\nu \big| \text{Defekt}\chi_\nu$. P_ν lässt X_ν elementweise fest, und auf X ist $\Pi' P_\nu \neq \Pi'' P_\nu$ wenn Menge$'\neq$ Menge$''$, wegen Ord $\Pi' P_\nu = \Pi' p_\nu$. Daher $\Pi(1 - P_\nu) \neq$ Nullop. auf X, aber auf $\sum X_\nu$.
   Schärfer: Ebenso beweist man:

5. Sei X ein Normalkörper, $X, \cdots, X_n \subset X$, $|X : X_\nu| = p_\nu^{\alpha_\nu}$, die Körper X_a zum gl. p_ν seien unabh., dh.

$$|X : \bigcap X_\alpha| = \prod |X : X_\alpha|.$$

   Dann $X \neq \sum X_\nu$. Das stimmt z.B. wenn jede Primzahl p höchstens in 2 der Defekte $|X : X_\nu|$ aufgeht.

135/136

19.10.1958

6. Ist $X = \sum_1^n X_\nu$, $X : X_\nu$ zykl mit erz. El. Q_ν, so ist $\prod_1^n (1 - Q_\nu) = 0$ im Gruppenring der Gal Gr $(X : P)$.

7. Daraus folgt weiter, wenn $\prod_1^r(\quad) = 0$ ein unverkürzbares Produkt, $|Q_1| \leqq 2^{r-1}$. Dann die in $\prod_2^r(1-Q_\nu)$ auftretenden Elemente der GG mit festem, etwa pos Zeilen ist $\leq 2^{r-1}$, und sie müssen aus vollen Nebenklassen nach $\{Q_1\}$ bestehen.

8. Weiter muss, wenn $\prod_1^n(1-Q_\nu) = 0$, jeder NT der GG mit zyklischer Faktorgr. wenigstens ein Q_ν enthalten.

9. Die Frage nach der möglichen Minimalzahl der durch p teilbaren Defekte kommt auf folgendes hinaus: Wieviel Untergr vom Index p braucht man, um die elementare Gr der Ord p^k zu überdecken? Das sind $p+1$ Stück, wenn $k \geq 2$. (weniger reichen nicht wegen Grössenordnung) $p+1$ reichen (man nehme alle, die eine feste Ugr vom Index p^2 enthalten).

136/137

10. Wenn $X = \sum^n X_\nu$, alle $X_\nu \subsetneqq X$, X normal abelsch, so geht jeder Primteiler p von $|X : Ra|$ in mindestens $p+1$ der Indizes $|X : X_\nu|$ auf. Die notwendige Gesamtzahl ist daher
$$n \geqq \sum_{p\,\big|\,|X:Ra|} (p+1)$$
Vermutung:

11. Hat der Charakterkörper X einer irred. Gr. den Grad n, so hat einer der Char. $\chi(G)$ die Höhe $\geq \sqrt{n}$. Genauer: Höhe $\geq \prod p^{\alpha+1} \cdot \prod_{k/2}{}' q$ wenn $n = \prod p^{\alpha+1} \prod q$

12. Entsprechendes geht für die verschiedenen irred. Charaktere einer festen Klasse konjugierter Elemente.

137/138

Vertauschungsringe von Matrizen

1. Kennt man eine rationale Basismenge von $\mathfrak{Z} = \mathrm{Zentr}\mathfrak{V}$ den Eigenwerten nach, so kann man u.U. den Index des von ihr erzeugten Moduls (ganzz.) in ganz $\mathfrak{Z}_{\text{ganz}}$ nach oben abschätzen: Mache einen unbekannten EW-Vektor $\mathfrak{v} \in \mathfrak{Z}$ durch Subtr. einer ganzz. Lin verbdg von $\mathfrak{b}_1 \cdots \mathfrak{b}_m$ zum Minimum, gibt obere Schranken für die Beträge gewisser Linearverbindungen der EW von $\mathfrak{v}$. Führt man diese Linverbdgen als Parameter ein, so sind die EWe des "Minimalvektors" zu $\mathfrak{v}$ durch kleine ganzzahlige Parameter dargestellt, gibt nur endl. viele Möglichkeiten. Die Ganzzahligkeit von $\frac{1}{n}\mathrm{Sp}\, M$ und $\frac{1}{n}\mathrm{Sp}\, M'M$ gibt weitere Einschränkungen.

2. Der Vert. Rg einer prim Gr. $\mathfrak{G}$ dürfte keinen S-Unterring enthalten ausser den triv. $\alpha I + \beta F$.

3. Die $V \in \mathfrak{V}$ mit $PV = V$ für eine feste Permutation $P \in \mathfrak{S}^n$ bilden einen S-Ring.
   Damit:

4. Enthält $\mathfrak{V}$ ein V vom Rang r, $\mathfrak{G}$ primitiv, so lässt jedes $G \in \mathfrak{G}$, welches r geeignete Ziffern fest lässt (nämlich zu lin un Spalten von V) sogar alle fest. Bew: 2, 3.
   Gibt vielleicht Anwendung auf Substgr gegebenen Grades, indem man diese in eine Permut.-Darst. einbettet.

5. Problem: Vertauschungsring und Minimalgrad einer primitiven Gruppe.

7. Aufgabe über PGr.:
   Es dürfte lohnen, die Gruppen vom Grade $kp + 1$, $k < p$ zu untersuchen, die ein El der Ord p vom Grad pk enthalten. Sie sind pri und vielleicht i.a. 2-tra (oder Frobeniussch?). Wäre nützlich für Untersuchung der Gruppen, die bei Studium prim Gr mit p-El. kleinen Grades auftreten bei der schrittweisen Verlängerung. Zu beginnen wäre mit $n = 2p + 1$.

139/140

Anwendung der Abschliessung

Sei $\mathfrak{G}$ pri, $\mathfrak{G}_1$ enthalte eine Untergruppe $\mathfrak{M}$, die nur 2 Transsysteme einer Länge > 1 hat. Dann hat auch $\mathfrak{G}_1$ höchstens 2 einer Länge > 1. [Genauer: $\mathfrak{G}$ unipri $\rightarrow$ schw. Abschl. von $\mathfrak{M}$ hat nur 2 Transs. $\neq (1)$] Ebenso für 3 statt 2 $*$
Bew:

a) oBdA ord$\mathfrak{M}$ maximal und $\mathfrak{G}$ abgeschl.

b) Ist $\mathfrak{M}' = \mathfrak{M}^G$ und $\mathrm{Gr}\{\mathfrak{M}, \mathfrak{M}'\} < 2\mathrm{Gr}\mathfrak{M} = 2m$ so hat $\{\mathfrak{M}, \mathfrak{M}'\} = \mathfrak{N} \leq 2$ Transsysteme der Lge > 1. Sonst wähle $\mathfrak{M}'' = \mathfrak{M}'^N$ so, daß $\mathrm{Gr}\{\mathfrak{M}, \mathfrak{M}''\} =$ min. Dann hätte auch $\{\mathfrak{M}, \mathfrak{M}''\}$ 3 Transs., und jedes besteht aus vollen Trans von $\mathfrak{M}$ oder $\mathfrak{M}''$. Gibt wegen Abgeschlossenheit eine trans. Ugr. von G_α, dann $\mathfrak{G}_1$ tra auf $\Omega - 1$.

c) $m \leq \frac{n}{2}$ gibt Wid.: wähle G so, daß $\mathfrak{M}^G$ mit $\mathfrak{M}$ eine Ziffer gemeinsam hat aber $\neq \mathfrak{M}$ ist. Dann ist $\{\mathfrak{M}, \mathfrak{M}^G\}$ Wid zu Max eig von $\mathfrak{M}$.

d) also $m > \frac{n}{2}$. Lässt $\mathfrak{M}$ α, β fest, und $G = \binom{\alpha \cdots}{\beta \cdots}$ so lässt $\mathfrak{M}^G$ β fest und hat eine Ziffer mit $\mathfrak{M}$ gemeinsam, also $\mathfrak{M}^G = \mathfrak{M}$ nach b). Daher, wenn $\Delta \ni 1$ die Fixmenge von $\mathfrak{M}$, ist $\mathcal{N}\mathfrak{M}$ tra auf Δ und $\mathcal{N}\mathfrak{M} \geq \mathfrak{G}_1$, daher $\mathcal{N}\mathfrak{M} = \mathfrak{G}_1$, $|\Delta| = 1$, dh. $\mathfrak{M} = \mathfrak{G}_1$.

$*$
Bew: — – – / – – — und — – – / — – – sind unmöglich

Fragen zur Verallg. d. Satzes von Frobenius:

Genügt es, wenn die in $\mathfrak{H}$ gelegenen Kommutatoren $[H, G]$, $G \notin \mathfrak{H}$, einen Normalteiler $\mathfrak{H}^* \neq \mathfrak{H}$ erzeugen?

Ordnung unipримitiver Gruppen. Forts. von 68

Man sollte den Satz 68.1 ohne Manning beweisen. Ansatz: $\mathfrak{G}$ sei unipri und 2-abgeschl. P, .. seien die unverkürzbaren p-Elemente, $p > \sqrt{n}$.

1. Haben P, P' eine Ziffer gemeinsam, so sind $\{P\}, \{P'\}$ konjugiert in $\{P, P'\}$. (als Sylowgr.)

2. Man kann in $\mathfrak{G}$ eine Reihe $\{P\}, \{P, P'\}, \cdots$ aufstellen, derart dass jedes neue $P^{(\nu)}$ eine Ziffer mit der vorigen Gruppe gemeinsam hat. Jedesmal kommen $< p$ Ziffern dazu, bis alle erschöpft sind:

3. $P, P' \in \mathfrak{G}_1 \to P$ konjugiert zu P' in $\mathfrak{G}_1$.
   Bew: Wähle $\mathfrak{H} = \{P_1, \cdots, P_m\}$ nach 2 maximal, dann haben P, P' Ziffern mit $\mathfrak{H}$ gemein, sind daher konj. zu P_1 im Erzeugnis.

Ordnung unipri Gr.

4. Je zwei unverkürzbare El. sind konj. in $\mathfrak{G}$.

5. Alle unverk. El. in $\mathfrak{G}$ erzeugen einen primitiven Normalteiler $\mathfrak{N}$. Sonst impr, aber 2-tra nach Induktion, $\mathfrak{N}_1$ hat also nur kurze Transsysteme in der Imp Zeile $\mathfrak{I}$, die 1 enthält, und alle anderen sind länger ($\geq p$); folglich werden die langen von $\mathfrak{G}_1$ in sich überführt, ebenso von $\mathfrak{G}_2$, wenn auch $\mathfrak{I} \ni 2$.

   Man muss die Annahme Grad $p < \frac{n}{2}$ oder $p^2 \big|$Grad ad absurdum führen ohne Manning.
   Fortsetzung 145

6. Frage: Folgt aus $p^\alpha \big| |\mathfrak{G}|$ stets $p^\alpha \leq n$?

Über Prim-Gruppen mit tra Untergr. kleineren Grades

[Einschub von S. 143:
Aufgabe: 2-tra Gr mit trans Ugr. $\mathfrak{H}$: Wichtig ist der Fall, dass je zwei Konj. zu $\mathfrak{H}$ in $\mathfrak{G}_1$ schon eine Ugr. des Gr. $n-1$ erzeugen: Affine Ebene, mit Gerade = Fixmenge von $G^{-1}\mathfrak{H}G$. → Ostrom & Wagner Thm.1 1958]

7. [*Die Abschnitte 7 bis 9 sind mit blauem Stift durchgestrichen; Abschnitt 8 ist von S. 143 eingeschoben*]
   Ist G 2 tra, G_a impri, $a, b \in \Delta$, G_Δ tra auf $\Omega - \Delta$, so ist $\Delta - a$ der einzige (Imprimitivitäts-)Block von G_a, welcher b enthält. Denn jede Konj von G_Δ muss volle Blöcke decken, andererseits kommen bei einem ev. 2. Verlängergsschritt weniger Ziffern hinzu als die Länge des Blocks. $\mathcal{N}G_\Delta$ 2-tra auf Δ; da $|\Delta| < \frac{1}{2}|\Omega|$ nach Marggraf, also je zwei Konj. zu G_Δ konj. in ihrem Erzeugnis.

8. *Folge: Verlängert man in einer pri G mit tra Untergr. H das H schrittweise möglichst langsam zu transitiven Gruppen von monoton steigendem Grad, so ist der Gradzuwachs höchstens beim ersten Schritt > 1.*
   Gibt grosse Verschärfung von Buch Manning S. 97 ff

9. *Folge: Ist $A < D < G$; G, A, B tra von verschiedenem Grad, G pri, so ist G mehrf tra bis herab zu B.*

142/143

Zur Darstellungstheorie bei $p \top g$.

Vor: $|\mathfrak{P}| = p$, sei $\mathfrak{P}$ eigener Zentralisator in $\mathfrak{G}$: $\mathfrak{P} = C\mathfrak{P}$.

1. Es gibt nur höchstens eine Familie von p-konj (dh. durch Autom. von $P(\sqrt[p]{1})$) Darstellungen.

2. Gibt es in dieser Familie e Darstellungen (also ist e der Grad des Charakters; $\frac{p-1}{e} = f$), so ist $|N\mathfrak{P} : \mathfrak{P}| = f$. Denn alle anderen Charaktere der Klasse von P sind rational, also (ist P zu f Potenzen konjugiert in G) die Untergruppe der Ord. f mod p lässt Klasse P fest.
   Bew geht kürzer direkt: Anzahl der Klassen mit p-Elementen ist, also zerfällt $\mathfrak{P}$ in e Klassen in $\mathfrak{G}$; also f Potenzen sind zueinander konjugiert.
   [Es folgen Einschübe zu S. 142, siehe oben.]

143/144

Beweis, dass p-reg Klassen $[X][Y]$ mit $\chi(X) \equiv \chi(Y) \bmod 1 - \varepsilon_{p^n}$ für alle X gleich sind: wie bei Brauer, Roquette?

a) Es ist $\{X\} = \{Y\}$
   Bew: den durch eine Darst. von $\mathfrak{H}$ induzierten Char. von $\mathfrak{G}$ betrachten, wo $\mathfrak{H} = \{X\}$ eine p-Sylow–Gruppe von $N\{X\}$.

b) Erleidet $\{X\}$ unter $\mathcal{N}\{X\}$ die Autom. $X \to X^\mu$, so betrachte die durch $X \to \eta = \text{prim } m\text{-te EWn}$ induzierte Darst. von $\mathfrak{H}^*$**???** $\chi(X) = \sum_\mu \eta^\mu \underset{(1-\varepsilon)}{\equiv} \sum \eta^{a\mu}\zeta$ $Y = X^a$. Das gleiche gilt, da mit $\chi(G)$ auch $\chi(G^\nu)$ ein Char ist, bei η^ν statt η: $\sum_\mu \eta^{\mu\nu} \equiv \sum_\mu \eta^{a\mu\nu}$ hieraus folgt, dass entsprechende Koeff mod p übereinstimmen, da $|\eta^{\nu\mu}| = m^{\frac{\varphi(m)}{2}}$, also kommt η^a unter den η^μ vor, dh, Y konj zu X in $\mathfrak{H}$.
   $*$ $\mathfrak{H} = \{X\}\times$ p-Sylowgr. von $C\{X\}$

Ordnung unipri Gruppen (Forts von 142)

1. Ist $\mathfrak{G}$ unipri, $P \in \mathfrak{G}$, Gr$P = qp$, P unverkürzbar und $p^2 \big| |\mathfrak{G}|$, so kommen beim ersten "Verlängerungsschritt genau q Ziffern zu P hinzu, und man kann es so machen, dass die verlängerte Gruppe $\mathfrak{H}$ q Transs. des Grades $p+1$ (festgekoppelte) hat, vorausgesetzt, dass nicht jede neue Ziffer in einem anderen Transs liegt.
Bew: Sei $P = - - -$
nimm
$H = | - || - || - | \in \mathcal{N}\{P\}$,
wo $| - || - | -$ in den neuen Ziffern, kommutiere mit P' in $| - || - || - |$
sodass $1 \neq H \circ P' = C$ dann hat C Grad $\leq 2q$, aber G enthält kein El des Grades $< 2q$, da ein konjugiertes D davon zu einer Verlängerung von $\{P\}$ um weniger Ziffern führen würde: $\{P, P^{\Delta}\}$. Also muss D oBdA von Primzahlord r jede seiner "alten" Ziffern durch eine der q neuen ersetzen, daher Ord$D = 2$; keine 2 neuen Ziffern sind im selben Transs von $\{P, D\}$, sonst wäre ein p-Zyklus von P fremd zu D, gäbe Verkürzung von P.

2. Nimmt man obiges P' hinzu: $\{PDP'\}$, so hat das q streng gekoppelte Konstituenten vom Grad $2p$, und zwar, falls $\mathfrak{G}$ 2-abgeschlossen, lauter symmetrische Gruppen $\mathfrak{S}_{2p}$. Weiter 148

Zu Knoche: Breite β von p-Gruppen $\mathfrak{G}$ 19.11.58

Arbeit für Acta Szeged:
Breite und Klasse von p-Gruppen [von S. 147]

1. Breite $\beta < p \rightarrow$ Klasse $c \leq \beta + 1$. Setze $\mathfrak{N} = \mathcal{N}A$, $A \in \mathfrak{G}$.
$\mathfrak{G} = \mathfrak{N}\mathfrak{G}^{[1]} \geq \mathfrak{N}\mathfrak{G}^{[2]} \geq \cdots \geq \mathfrak{N}\mathfrak{G}^{[\beta+2]}$, wo $\mathfrak{G}^{[\rho]}$ abst. Zentr. R.
einmal $= \mathfrak{N}\mathfrak{G}^{[i]} = \mathfrak{N}\mathfrak{G}^{[i+1]}$ $1 \leq i \leq \beta + 1$
$A \circ \mathfrak{G}^{[i]} \leq A \circ \mathfrak{N}\mathfrak{G}^{[i+1]} = A \circ \mathfrak{G}^{[i+1]} \leq \mathfrak{G}^{[i+2]}$
$\mathfrak{G} = \sum_{i=1}^{\beta+1} Z(\mathfrak{G}^{[i]}, \mathfrak{G}^{[i+2]}) \rightarrow \beta + 1 \geq p + 1 \rightarrow \beta \geq p.$
Ann: Seien alle $\mathfrak{G}^{[\rho]}$ verschieden.
NB: Knoche hat $c \leq \beta + 1$ für $\beta \leq 3$ und beliebiges p, ich nur für $p > 3$!

2. Obiger Beweis zeigt: Alle Elemente A mit $\beta_A \leq \beta_0 =$ fest werden überdeckt von $\beta_0 + 1$ festen echten Ugruppen von $\mathfrak{G}$, falls $c \geq \beta_0 + 2$

3. Der Beweis dürfte auch für unendliches $\mathfrak{G}$ gelten.

4. Wird $\mathfrak{G}$ von $p+1$ echten Untergr. überdeckt, so haben diese den Index p und den Durchschnitt $\Phi(\mathfrak{G})$. Denn jede von ihnen muss $p-1$ volle Nebenklassen von $\mathfrak{H}$ enth., wenn $\mathfrak{G}|\mathfrak{H} = (p, p)$; also enth. jede auch $\mathfrak{H}$, ihr Durchschnitt ist $\mathfrak{H}$, also gibt es nur eine Untergr. $\mathfrak{H}$ mit $\mathfrak{G}/\mathfrak{H} = (p, p)$.

5. Für $\beta = p$ gilt 1. auch noch: Sonst liegt 4. vor, insbesondere hat $Z(\mathfrak{G}/\mathfrak{G}^{[2]})$ den Index p, dann hat aber das Zentrum von $\mathfrak{G}/\mathfrak{G}^{[2]}$ zykl. Faktorgr.
Mir fehlt an Knoches Erg. also nur noch $\beta = 3,\ p \circ 2$ (**???**siehe 8)

6. Nachsehen, was Neumann-Schule für Resultat über FC-Gr hat.

7. Leicht zu zeigen: $p = 2,\ \beta(A_i) \leq 2 \to c\{A_i\} \leq 3$
Bew: Die Klasse einer 2-Gr vom Grad 4 ist ≤ 2.

8. $p = 2,\ \beta = 3\ \to\ c \leq 4$ Bew 7.

9. Frage: $p = 2, 3; \beta = 4 \to c \leq 5$?

10. Man müßte $\beta = p + 1$ erledigen, dann wäre K. voll überdeckt. Dazu außerd. Zentralisator betrachten, in der $\mathcal{N}A$ mit $\beta_A = p + 1$ deckt eine FGr $\mathfrak{Z}_{i+1}/\mathfrak{Z}_i$ und meidet alle anderen $(i = 1, \cdots, p + 1)$, daher (wegen $\mathfrak{G} : \mathfrak{N} = p^{p+1}$) $|\mathfrak{Z}_{i+1}/\mathfrak{Z}_i| = p$ $(i = 1 \cdots p + 1)$.

Ord unipri Gruppen

1. Hilfssatz: Ist $\mathfrak{G}$ 2- abgeschlossen und $\mathfrak{H} \leq \mathfrak{G}$, so "zerfällt" der Teil von $\mathcal{N}\mathfrak{H}$, der alle Transsysteme von $\mathfrak{H}$ einzeln fest lässt.

2. Bei P mit $\operatorname{Grad} pq$, $p^2 \mid |\mathfrak{G}|$ folgt aus 1:
Jedes El. des Grades $\leq 2p$, das den Träger $\mathfrak{T}$ von P in sich überführt, liegt ganz auf $\mathfrak{T}$ oder ganz außerhalb $\mathfrak{T}$.

3. Unter der Vor $\big|$ von S.145 gilt: G impr.
Bew:

   A. Ein El des Grades $2q$, das zwei Ziffern aus verschiedenen Zyklen von P vertauscht, enthält nur q Paare "gekoppelter" Ziffern. Bew mit Verlängerg. um q und $2q$ Ziffern, Betrachtg der gekoppelten symm Gruppen (abschliessen)

   B. Seien Λ, q gekoppelte Ziffern von P, T ein El des Grades $2q$, das sie enthält. Hat dann T^G <u>eine</u> Ziffer mit Λ gemeinsam, so jede Ziffer von Λ. (nach A). Daher ist dann $\Lambda = \Lambda^G$, wenn G eine Ziffer in Λ läßt.

Ordnung uniprim. Gruppen.

1. Zu jeder Primzahl p und zu $k = 1, 2, \cdots$ gibt es eine unipri Gruppe des Grades

$$n = \frac{kp(kp-1)}{2},$$

deren Ordnung genau durch

$$p^\omega = p^{k+[\frac{k}{p}]+[\frac{k}{p^2}]+\cdots}; \omega \leq \frac{k}{p-1}$$

teilbar ist, nämlich die Darst von $\mathfrak{S}_{kp}$ nach ungeord. Paaren, z.B.

$$\begin{aligned} k=2: &\qquad n=p(2p-1),\ p^\omega=p^2 &&< n \\ k=3: &\quad n=\tfrac{3p(3p-1)}{2},\ p^\omega=p^3 &&> n \text{ für } p>5 \\ k=p: &\qquad n=\tfrac{p^2(p^2-1)}{2},\ p^\omega=p^{p+1} \end{aligned}$$

2. Vermutung: Ist die Ord einer unipri Gruppe durch p^ω teilbar, so ist ihr Grad

$$n \gtrapprox \frac{\omega^2(p-1)^2}{2} \qquad (\text{ nämlich } k \gtrapprox (p-1)\omega)$$

Mehr kann jedenfalls nach 1 bestimmt nicht behauptet werden.
Auch das ist noch etwas zu viel behauptet mindestens für $\omega = 2$, da es unipri Gr des Grades p^2 gibt.
NB: Vermutlich ist eine irred. Untergruppe von $PSL(n,q) = \mathfrak{G}$ in der ein Element einen Fixpunktraum hoher Dimension hat, $= \mathfrak{G}$

[Die Seiten 150 bis 157 sind mit rotem Stift durchgestrichen]

13.12.58 *Fixgruppen von Automorphismen.*

1. *R. Brauer erwähnte im gestrigen Vortrag: Ist $|G|$ ungerade und erweitert man G durch eine Autom- Gruppe A vom Typ $(2,2)$ mit den Untergr. A_1, A_1', A_1'' und Einsel. A_0, und lässt A_i genau v_i Elemente von G fest usw, so ist*

$$g = \frac{v_1 v_1' v_1''}{v_0^2}.$$

Folgt aus seiner Theorie, lasse sich auch el. beweisen.
Verallgemeinerung:

2. *Sei q Primzahl, $q \nmid |G|$, und G sei erweitert eine q-Gruppe Q_0, welche eine nor. Untergr. Q_2 vom Index q^2 mit nicht zykl. Faktorgr. besitzt, und es seien $Q_1, Q_1', -, Q_q'$ die $q+1$ Zwischengruppen: $Q_2 < Q_1^{(\nu)} < Q_0$. Dann gilt*

$$(*) \qquad v_0^q \cdot v_2 = v_1 v_1' \cdots v_1^{(q)}.$$

Bew:

a) *Sei G eine elementar abelsche p-Gruppe, die minimal Q-invariant ist. Dann lässt jedes der $Q_\Delta^{(a)}$ entweder 1 oder g Elemente fest von G. ($g = |G|$). Nach Vor ist die Darst. von Q auf G irreduzibel, also*

zyklisch, falls Q_2 die ident Darst. macht. Also gibt es 3 Fälle:

NB: es genügt das für $|Q| = q^2$ zu beweisen, dann auf G_{Q_2} statt G anwd.

150/151

		v_0	v_1	$v_1' \cdots v^{(q)}$	v_2
I.	*Q_2 macht nicht ident Darst. auf G:*	1	1	$1 \cdots 1$	1
II.	*Genau ein $Q_1^{(v)}$ macht ident. Darst auf G:*	1	1	$g1 \cdots 1$	g
III.	*Ganz Q_0 macht ident Darst auf G:*	g	g	$g\,g \cdots g$	g

In jedem Fall gilt $(*)$

b) Ist G eine p-Gruppe (oder auch nur auflösbar), so Induktion nach G mit Hilfe des Hilfssatzes

3. Sei A eine Autom Gr. von G, $N \lhd G$, N fest bei A, $(|G|, |A|) = 1$. Sei G_A die Gruppe der Fixelemente von G unter A,usw. Dann ist $|G_A| = |N_A| \cdot |(G/N)_A|$.

c) Ist G nun beliebig, so folgt die Beh. aus dem

Hilfssatz 4: Sei A eine auflösbare (es genügt: Vermutung Zassh gilt für die Untergr von GA) Gruppe von Autom von G,
$(|A|, |G|) = 1$; G_p sei eine bei A feste Sylowgruppe G; Dann ist $G_p \cap G_A$ eine Sylowgr von G_A (= Fixgr von A in G)
Bew: Jede maximale bei A feste p-Gruppe P' oberhalb einer Sylowgr $(G_A)_p$ ist Sylowgr. von G: $P'^G = G_p$. A^g lässt, wie A, G_p fest, also A^g konj zu A in $\{A, A^g\}$, dh in $\mathcal{N}G_p = H$: $A^{gh} = A$, $P'^{gh} = G_p$ enth $|(G_A)_p|$ bei A feste Elemente: $G_p \cap G_A$ Sylowgr von G_A.

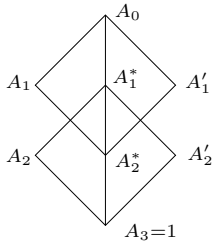
151/152

Fixgruppen von Autom.

5: Wenn Typ $A = (q^2, q)$ abelsch, so ist jede multipl. Relation zwischen den v_i abhängig von den beiden aus 2 folgenden

$$\oplus \quad \begin{cases} v_3 v_1^{*q} = v_2^* v_2^{(1)} v_2^{(2)} \cdots v_2^{(q)} \\ v_2^* v_0^q = v_1^* v_1' v_1^{(2)} \cdots v_1^{(q)} \end{cases}$$

Dabei bedeutet allg. A_i eine Untergr. vom Index q^i in A, v_i die Ord der Fixgr von A_i in G, und A_i^* sind die ausgezeichneten Gr ihrer Ord. A_1 vom Typ (q, q), und $A_2 = \phi A$.
ZB. $q = 2$: Bew mit dem Verbandsschema von A:



Als genaue Fixgruppen einer irred p-Gr. kommen nur Untergr. von A mit zykl Faktorgr in Frage, also $A_0 \;\; A_1 \;\; A_1^* \;\; (A_1') \;\; A_2^*$.
Aus diesem Schema entnimmt man die 4 *möglichen Verteilungen für die Ord der Fixgruppen (g oder* 1*) und findet, dass nur* 2 *unabh Beziehungen bestehen, nämlich* $\oplus$

152/153

6: Im Falle eines abelschen Typ $A = (q, q, q)$ *ergibt sich mit* $|A : A_i| = q^i$, $v_i = \operatorname{Ord} \mathcal{Z}sA$ *in G:*

$$\begin{cases} v_3 v_0^{p^2+p} = v_1^{(1)} \cdots v_1^{(p^2+p+1)} \\ v_2^{(1)} \cdots v_2^{(p^2+p+1)} v_0^{p^3+p^2+p} = [v_1^{(1)} \cdots v_1^{(p^2+p+1)}]^{p+1} \quad q \text{ statt } p! \end{cases}$$

Sind alle $v_2^{(\nu)} = g/j_1, \quad g_1^{(\nu)} = g/j_2$, *also* $j_\rho =$ *Index in G der Fixgruppe jeder Untergr der Ord* q^ρ *in A, dann wird mit passendem* $k \geq 1$*:*
$[j_0 = 1]$, $j_1 = k^{q^2}$, $j_2 = k^{q^2+q}$, $j_3 = k^{q^2+q+1} =$ *Index* $\mathcal{Z}sA$.
Überhaupt ist es besser Beziehungen zwischen Indizes als Ordnungen zu suchen. Direkte Faktoren, die von A zentralisiert werden, ändern die Indizes nicht; man hat einen Parameter weniger nötig, nämlich v_0.

7: Frage: Alle Relationen aufstellen bei gegebener q-Gruppe A. [Sie sind eine Invariante von A.]
Vermutlich folgen sie alle aus denen für Faktorgruppen vom Typ (q, q). *Wenigstens stimmt das für* 5 *und für die beiden Aussagen von* 6.

7′. Stets ist $v_A \cdot v_B \big| v_{A\cap B} \cdot v_{\{A,B\}}$, *wenn* A, B *in Automgr G Ord der "Darst mod" teilerfremd. Bew.* $172_1 \quad (|G|, |M|) = 1$

153/154

Fixgruppen von Autom.

8. Sei A dargestellt durch Autom einer p-Gruppe P, wo $(p, |A|) = 1$. *Sei* $N \lhd P$, $N^A = N$, *und A lasse eine Nebenkl Ny von N fest. Dann läßt A in ihr ein Element fest.*
Bew: Indukt nach $|P|$. *Wähle* $M \leq N$ *als minimal* $P - A$*-zulässig, dann* $M <$ *Ztr P. Nach Ind.* $[P/A]$ *lässt A eine Nebenklasse Mx fest,* $x \in N_y$.

x erzeugt also mit seinen Konjugierten unter A eine kommutative Gruppe. Setze $x_1 = \big(\prod_{a\in A} x^a\big)^\rho$, wo $\rho\cdot|A| \equiv 1(p)$, x fest bei A. Dann ist $x_1 \equiv x$ mod N *und x_1 fest bei A.*
Folge:

9. *Bedeutet unter der Vor von 8 P_A die Fixgr von A in P, so ist*

$$|P_A| = |N_A|\cdot|(P/N)_A|.$$

Folge:

10: *Ist $(|G|,|A|) = 1$, A dargestellt durch Autom von G, und ist G oder A auflösbar, so ist*

$$|G_A| = \prod_{p\,\big|\,|G|}\ \prod_i |P_A^{(i)}|$$

wo $P^{(i)}$ die verschiedenen Hauptfaktoren von P unter A durchläuft und P je eine bei A feste Sylowgr von G zu jeder Primzahl.

154/155

11: *Vor 10: Enthält die Darstellung von $U \le A$ auf (dem in Hauptfaktoren zerlegten) $P^{(i)}$ genau e_i mal die identische Darstellung, so lässt U genau $v = \prod p_i^{e_i}$ Elemente aus G fest.*

12. *Vor 10: Sind $U_1, U_2, \dots$ Untergruppen von A und besteht für jede auf den Sylowgr von G auftretende Darstellung v von A zwischen den Vielfachheiten $e, e, \cdots$ der Einsdarstellung von $U, U', \cdots$ in $\mathfrak{d}$ die Beziehung*

$$c_1e_1 + c_2e_2 + \cdots = 0,$$

so besteht für die $v_\alpha = |G \cap \mathfrak{Z}sU|$ die Gleichung $v_1^{c_1}v_2^{c_2}\cdots = 1$.
Bew: 10,11

13. *Ergänzung: Es genügt sicher, wenn $\sum c_\alpha e_\alpha = 0$ gilt für jede rat irreduzible Darstellung, oder für je eine aus jeder Familie absolut irred Darstellungen.*

155/156

Fixgruppen von Automorphismen

Beispiele: Bedeute stets U_α eine Untergr. der Ord α von A.

14: *A die Diedergr. d. Ord $2p$ (z.B. $p = 3:\ A = \mathfrak{S}_3$).*

Tafel der e:	U_1	U_2	U_p	U_{2p}	
rat irred Ch:	1	0	1	0	*alt. Ch.*
	2	1	0	0	
	1	1	1	1	
c_d	-1	2	1	-2	

also ist stets

$$v_1 \cdot v_{2p}^2 = v_2^2 v_p$$

Gleichwertig ist

$$|G : V_p| = |V_2 : V_{2p}|^2.$$

Ähnlich

15. *A Diedergr. d. Ord* $2p^3$ $(p > 2)$

$$\textit{Drei unabh Rel:} \quad \begin{cases} v_1 v_{2p^3}^2 & = v_{p^3} \cdot v_2^2 \\ v_p v_{2p^3}^2 & = v_{p^3} v_{2p} \\ v_{p^2} v_{2p^3}^2 & = v_{p^3} v_{2p^2} \end{cases}$$

156/157

16: *A die alternierende* $\mathfrak{A}_4$*:* $\begin{cases} v_1 v_{12}^3 & = v_4 v_3^3 \\ v_2 v_{12} & = v_3 v_4 \end{cases}$

Folge: $v_1 = \frac{v_2^3}{v_4^2}$ *schon bekannt.* $\quad v_1 v_{12}^2 = v_2 v_3^2$

17: $A = \mathfrak{S}_4$

$$\left.\begin{array}{rcl} v_1 v_{12}^3 & = & v_3^3 v_4 \\ v_2 v_{12} & = & v_3 v_4 \end{array}\right\} \textit{alt, folgt aus 14 } (p = 3), \textit{ 16}$$

$$\begin{array}{rcl} v_4 v_{24}^2 & = & v_8^2 v_{12} \\ v_3 \underline{v_2} \underline{v_4} & = & v_1 v_{24}^2 \end{array} \qquad \textit{neu}$$

mit $\underline{V_2}, \underline{V_4} =$ *<u>nicht</u> in* $\mathfrak{A}_4$ *enthaltene Gruppen der Ord* $2, 4$.

18: *Allgemein gilt, wenn* $\begin{cases} G \lhd AG \\ (|A|, |G|) = 1 \end{cases}$ *und A oder G aufl:*
$V_1, V_2 \leq A$, $V_i = G \cap \mathcal{Z}sU_i \;\rightarrow$
zu jedem $g, h \in G$ *gibt es* $k \in G$ *mit*

$$V_1^g \cap V_2^h \leq (V_1 \cap V_2)^k$$

Bew: $V_1^g \cap V_2^h$ *wird zentralisiert von* $\{U_1^g, U_2^h\}$*, und das hat ein* $\{U_1, U_2\}^k$ *als Untergruppe.*

19. *Folge:* $|V_1^g \cap V_2^h| \big| |V_1 \cap V_2|$
[*Ende der Durchstreichung mit rotem Stift*]

157/158

Fixgruppen v. Autom.

Sei $G \lhd GA$, $(|A|, |G|) = 1$, A od. G aufl., $U \leq A$. $V = G \cap \mathrm{Zs}\, U$.

20. V ist "massiv" in G, dh. aus $v_i \in V$, $v_i^g \in V$, $g \in G$ folgt $\exists v$ mit $v_i^g = v_i^v$.
Denn die v_i^g werden von U, U^g zentralisiert, und beide sind konjugiert unter $G \cap \{U, U^g\} \leq \cap \mathcal{Z}s\ v_i^g$ in G.
Und $G \cap \mathcal{N}U = G \cap \mathcal{Z}sU$.

20′. Je zwei in G konjugierte, unter U feste Objekte sind konjugiert unter V.

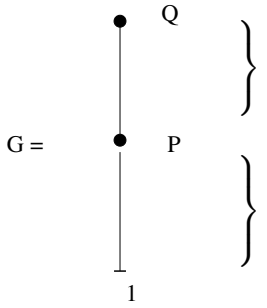
21.
$$V \cap V^g \begin{cases} = V^g \cap \mathcal{Z}s(U \circ \{g\}) \\ = V \cap \mathcal{Z}s(U \circ \{g\}) \end{cases} \qquad \circ \text{ Kommutatorgr}$$
Denn $\{V, Vg\} = V \cdot (V \circ \{g\})$.
Hängt vielleicht mit Kaloujnine, Berlin 1953 zusammen
Dabei zu beachten: $U \circ \{g\}$ ist normal bei U und g. Wenn also G einfach, ist $\{g^U\} < G$ oder $g \circ U = G$.

21′ Lässt A kein El von G fest, so lässt A nur eine p-Sylowgr **???**.

22. Vermutung: Eine nicht zykl. auflösbare Autom Gr A einer nicht auflösb Gruppe G mit $(|G|, |A|) = 1$ besitzt einen Fixpunkt $\neq 1$.
Bew. Skizze für $A =$ Vierergruppe U_4: Sei $V_4 = 1$. U_4 lässt zu jedem p genau eine p-Sylowgr. von G fest.

158/159

Durchstreichung [
[es ist $G = V_2 V_2' V_2''$] Die Sylowgr von G haben Klasse $\lessapprox 4$, ihre Normalisatoren sind nach Induktion nilpotent, also kann man die Sylowgruppen von G oben abspalten. Zu untersuchen ist nur der Fall



P & Q el. abelsch
Man braucht, dass jede irred. Darstellung von QU_4 entweder in Q oder in U_4 die identische Darstellung enthält; dh. dass jede irred. Darst. von QU_4 entweder in der durch U_4 oder durch Q erzeugten Perm-Darst. liegt, dh dass die Summe beider Permudarstellgen schon den vollen Rg. $4q$ hat
[Wielandts Kommentar zur Durchstreichung]
Stimmt so noch nicht mit $\rho^q = 1$ betr $\begin{pmatrix} \rho & \\ & \rho^{-1} \end{pmatrix}$, $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Hier hat weder Q noch U_4 eine identische Darstellung

23. Ist A = Vierergruppe ohne Fixpunkte, $|G|$ ung., so $\begin{cases} V_2 V_2' V_2'' = G \\ |V_2||V_2'||V_2''| = |G| \end{cases}$

jedes $V_2^{(i)}$ ist abelsch, lasse Index 2 weg.
Bew:

a) $V^{v'} \cap V'' = 1$, da $V \cap V'' = 1$ (21)
b) $vv' = v'v'' \to v = 1$ a)
c) $vv'v'' = v' \to v = v'' = 1$ b)
d) $vv'v'' = w' \to v = v^{\sigma'} \to v = 1;\ v'' = 1$ c)
e) $vv'v'' = ww'w'' \to v = w\ \ v'' = w''$ d)

wegen $|V||V'||V''| = |G|$ (1) ist Darstellung $g = vv'v''$ eindeutig **???**.

Abschließung, Fixgruppen: $G \lhd GA$, $(|G|, |A|) = 1$

24. Nach Nöbauer (?) gehört ein $a \in A$ genau dann zur Untergr. $U \leq A$, wenn a den Fixraum von U punktweise festlässt in jeder Darstellung von A. Daher sind die Untergruppen $U \leq A$ ($\subseteq$ Autom Gr G mit $(|A|, |G|) = 1$) sicher dann "abgeschlossen" im Sinn der Galoisverbindungen, wenn A auf G alle irred. Darstellungen bewirkt; allgemeiner: wenn RgA (insgesamt auf den Hauptfakt der festen Sylowgr.) $= |A|$: "A lin un auf G"
Letzteres ist direkt zu sehen: $B \leq A$, a lässt alles fest was B fest lässt $\to \underset{g}{\forall}\ g^{Ba} = g^B$, wegen lin Unabh. folgt $Ba = B$, $a \in B$.
Um Umkehrg zu beweisen, müßte man das "Erzeugnis" von F_B und F_C neu definieren, es muss alles enthalten, was von F_A und F_B durch Gleichungen in G bestimmt ist.

25. Ist $A = (a)$, $|A| = q$ Primzahlpotenz, und lässt a genau v Elemente von G fest, so enthält G genau $|G|/v$ Elemente der Norm 1 : $g^{1+a+\cdots+a^{q-1}} = 1$.
Denn Norm $g = 1 \leftrightarrow \operatorname{Ord} ga = q \underset{\text{Sylow}}{\longleftrightarrow} ga = h^{-1}ah$, $h \in G$;
Anz Norm $g = 1$ = Anz. d. q Sy Gr
Die Anzahl $\overline{v}$ der g mit Norm $g = 1$ ist also multiplikativ bzgl

$$\begin{cases} \text{Zerl. in Sylowgr.} \\ \text{Zerl. in Hauptfaktoren} \end{cases}$$

26. Allgemein, wenn $\begin{cases} A \text{ oder } G \text{ aufl.} \\ A \text{ genau } V \text{ fest lässt in } G, \end{cases}$ ist $|G/V|$ = Anzahl der „Verschiebungssysteme", die aus A eine Vertretergr. von GA/G machen.

27. Die Verschiebungssysteme bilden also i.a. keine Gruppe, sondern die Quotientengruppe G/V nach einer nicht normalen Untergruppe V.

28. Zyklenbild von G. ("Familienbild")
Stelle jede Klasse (Z) von konj. zyklischen Untergr. Z von G durch einen Punkt in der Höhe r dar, wo $|Z| = \prod_1^r p_\rho$. Schreibe $U \prec Z$ für $U \in Z^m$ für ein m, und verbinde zwei Punkte U, Z benachbarter Höhe durch einen Strich, wenn $U \prec Z$.
$|G : NZ|$ ist die Zahl d. ein (Z) gelegenen Gruppen. Schreibe $\delta(UZ) = \begin{cases} 1 \\ 0 \end{cases}$ wenn $\begin{matrix} U \prec Z \\ \text{sonst} \end{matrix}$. Dann gilt:
Für $H \leq G$ bedeute $A(UH)$ die Anzahl der verschiedenen $U^g \leq H (g \in G)$

29: Der Charakter des Elements u, welches U erzeuge, in der Permutationsdarstellung χ_H von G, die von der belieb. Untergr. $H \leq G$ induziert wird, ist

$$\chi_H(u) = \frac{|\mathcal{N}U|}{|H|} \cdot A(UH)$$

insbesondere für zykl. Z:

$$\chi_Z(u) = |\mathcal{N}U : Z| \cdot \delta(UZ)$$

[*Die Seiten 162 bis 164 sind mit rotem Stift durchgestrichen*

Fixgruppen s. auch IX 66

30. *Sei f_H die Dimension des Fixraumes von $H < G$ bei einer Darstellung $\mathfrak{d}(\mathfrak{G})$ mit Charakter $\chi(g)$. Ferner sei im Gruppenring von G (stets $H = \sum_{h \in H} h$ gesetzt) eine Darst. von G als Linverbdg von Untergruppen gegeben: Dann ist*

$$G = \sum c_H H \qquad c_H \in \text{ Körper mit Char. } 0$$

$$|G| \cdot f_G = \sum_H f_H \cdot |H| \cdot c_H; \qquad f_G = \sum_H \frac{c_H}{|G : H|} \cdot f_H$$

Bew: $|G| f_G = \sum_{g \in G} \chi(g) = \chi(G) = \sum c_H \chi(H)$

31. *Frage: Übersicht über alle Darstellungen von G als Lin Verbdg von Untergr. suchen*
R. Brauer am 7.1.59 geschrieben: $\sum_H c_H H = 0 \to \prod m_H^{h c_H}$ *wenn $H \leq G$, G dargest. durch Autom von M, $(g, m) = 1$ M und G aufl.*

32 *Die Darstellung von G als Linverbdg zykl. Gruppen Z ist eindeutig und lautet wegen*

$$\begin{cases} Z = \sum\limits_{d \mid |Z|} [Z_d] \quad [\ ] = \text{ Menge der Erzeugenden} \\ [Z] = \sum\limits_{U \le Z} \mu(|Z:U|)U \end{cases}$$

$$G = \sum_U U \cdot \mu(U < G)$$

wobei

$$\begin{aligned} \mu(U < G) &= \sum_{U \le Z \le G} \mu(Z:U) \qquad \mu = \text{ Möbius} \\ \mu(Z < G) &= \sum_{Z < V \text{ zykl} < G} \mu(V:Z) = \end{aligned}$$

162/163

33.

$$f_G = \sum_{Z \le G} \frac{\mu(Z<G)}{|G:Z|} f_Z = \sum_{(Z)} \frac{\mu(Z<G)}{|\mathcal{N}Z:Z|} f_Z$$

Also

$$f_G = \sum_{(Z)} d_Z f_Z, \quad d_Z = \frac{\mu(Z<G)}{|NZ:Z|} = \frac{1}{G:Z} \sum_{(V)>(Z)} \mu(V:Z) A(V<G)$$

und daher gilt für jede Darstellung von G durch Automorphismen einer Gruppe M, wenn $(|G|,|M|)=1$ und G oder M auflösbar ist, die Beziehung

33*

$$v_G = \prod_{(Z)} v_Z^{d_Z} \qquad \text{Bew 12}$$

Ganz allg.: $G = \sum c_H H \to v_G^{|G|} = \prod v_H^{c_H |H|}$ *Bew:* $p^{f_H} = |v_H|_p$ *& 30 s.u!*

34. *Entsprechend gilt für festes $H \le G$:*

$$f_H = \sum_{(U)} e_U f_U \text{ oder } \sum c_i H_i = 0 \to \prod |G_i|^{c_i |H_i|} = 1$$

mit

$$e_U = \frac{1}{|H:U|} \cdot \sum_{(U)<(Z)} \underset{\downarrow 32}{\mu(Z:U)} \cdot \underset{\downarrow \text{Erklärt 28}}{A(ZH)}$$

Alles steht in 30 + 32: Happy Birthday Theorem

35.

$$\mu(U_1 \times U_2 < G_1 \times G_2) = \mu(U_1 < G_2) \cdot \mu(U_2 \times G_2)$$

wenn $(|G_1|, |G_2|) = 1$
Bew: $G_i = \sum U_i \mu(U_i < G_i) \to G_1 \times G_2 = \sum (U_1 \times U_2) \ldots$ *und die zykl Gr von* $G_1 \times G_2$ *sind genau die* $U_1 U_2$.
Noch allgemeiner:

(33)

$$\sum c_H H = \sum e_K K \to \begin{cases} \prod v_H^{|H| c_H} = \prod v_K^{|K| e_K} \\ \sum c_H |H| f_H = \ldots \end{cases}$$

163/164

Fixgruppen

36.

$$\sum_{Z<G} |Z| \mu(Z < G) = |G|$$

Denn $G = \sum Z \mu(Z < G)$ *Hauptchar. einsetzen.*
Brauer: Relation 31.1 vielleicht gleich denen der Zetafunktionen in Brief 16.1.59

37.

$$\sum_{Z<G} \mu(Z < G) = 1$$

Bew:

$$\begin{aligned} = \sum_{Z<V<G} \mu(V : Z) &= \sum_{V} \sum_{Z<V} \mu(V : Z) \\ &= \sum_{V \neq 1} 0 + 1 \end{aligned}$$

38. $\mu(Z < G) = \mu(Z < H)$ *wenn* $H > C^* Z =$ *Erzeugnis der* $V < G$ *mit* $Z < V$, V *zykl..*
Es ist $C^* Z < CZ =$ *Zentralisator* Z, *also*

$$\mu(Z < G) = \mu(Z < CZ) = \mu(Z < C^* Z)$$

Das ist nützlich zur Berechnung von $\mu(Z < G)$ *in Verbindung mit 35: Wähle möglichst* H *so, dass* $H \geq C^* Z$ *und* H *direktes Produkt teilerfremder Gruppen.*
[*Ende der Durchstreichung mit rotem Stift*]

39. Isotopiegraph von G:
Jede Klasse $\langle Z\rangle$ von zyklischen Untergr. von G, die unter der (vollen) besser: inneren Autom Gr von G konjugiert sind, wird durch einen Punkt wie in Nr 28 dargestellt, der Primzahlindex "benachbarter" Pkte an den verbindenden Strich geschrieben, an den Punkt die Zahl der zyklischen Gruppen in der Klasse. Es ist natürlich $\mu(Z<G)=\mu(Z^\sigma<G)$ wenn σ Autom G, also

$$f_G=\sum_{\langle Z\rangle}\frac{\mu(Z<G)}{|G:Z|}\cdot|\langle Z\rangle|\cdot f_Z$$

Das Gleiche gilt für jede Eiteilung der zykl Ugr von G in isotope
und

$$|\langle Z\rangle|=\sum_{(Z)<\langle Z\rangle}|(Z)|=\sum A(ZG)$$

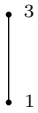
also

$$d_Z=\frac{\mu(Z<G)\cdot|\langle Z\rangle|}{|G:Z|}$$

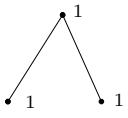
40. Unmittelbar "unter" einem Punkt U des Isotopiegr (oder des Familienbildes) liegen genau so viele Punkte, als $|U|$ Primteiler hat.

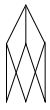
Fixgruppen

41. Beispiele zum Isotropiegraph: (unten die 1 weggelassen)
G Abelsch $|G|=p^\alpha$ Typ $(p\cdots p)$: •1 • $\frac{p^\alpha-1}{p-1}$

G Quaternionengruppe 

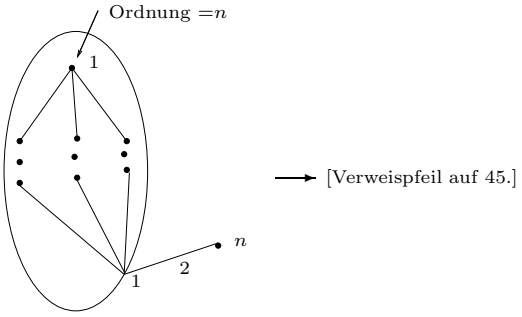
G Oktaedergruppe

G Zykl. Gr. d. Ord pq 

G Zykl Gr d Ord pqr  jede Primzahl eine Richtung

$|G| = p^3$, nicht abelsch, Exp $= p$ oder abelsch

Diedergr $|G| = 2n$ $n \equiv 0, 1 \mod 2$:



166/167

42. Ist $|G| = p^a$, Exp$G = p$, so $G = \sum\limits_{Z>1} (Z-1) + 1$ also

$$v_{p^d}^{p^\alpha} = \prod_{Z>1} \frac{v_p^p}{v_1} \cdot v_1$$

43 Quaternionengr: $G = V_4 + V_4' + V_4'' - 2V_2$

44: Allgemein ergibt jede Zerlegung von G/H, wenn $H \lhd G$, auch eine entsprechende Zerlgg von G in Linverbeg v. Untergr.

45 [Verweispfeil auf obige Skizze] Die Zerlegung $G = U_n + \sum\limits_1^n (V_2 - 1)$ ergibt

$v_G^{2n} = v_U^n \cdot \prod\limits_1^n \left(\frac{v_2^2}{v_1}\right)$

also $v_{2n}^2 v_1 = v_n \cdot v_2 v_2'$ mit $v_2 = v_2'$ wenn $2 \nmid n$.

167/168

Fixgruppen

46. Besitzt G eine Darstellung ohne Fixpkt (ausser 1), so ist in jeder Zerlegung

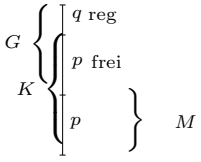
$$G - 1 = \sum_{1 \neq H \leq G} c_H (H - 1)$$

die folgende Bedgg erfüllt:

$$\sum c_H = 1.$$

Man sieht hieraus sofort, daß G selbst keinen NT $\neq 1$ enthalten kann, der unter einem Elementg $\notin N$ einen regulären Autom. erleidet.

47. Ist G eine Frobeniusgr: $N + \sum H = G + |N| \cdot 1$, mit Frobeniuskern N: und ist H in einer Darstellung von G fixpunktfrei, so hat N nur Fixpunkte, dh. ist auf die Matrix 1 abgebildet.
$f_H = f_G = 0$ ergibt mit der Vor.: $|N| f_N = |N| \cdot f_1$.
Hieraus folgt ein durchsichtiger Beweis für die
Nilpotenz einer aufl. Gruppe K mit regulärem Autom:
Nach Induktion kann man



annehmen: der p-freie Vertreter zentralisiert M.

168/169

48. Sei $G = H \cup \bigcup_{i=1}^{n} H_i$ mit $H_i \cap H = 1 = H_i \cap H_j$
G habe eine Darstellung, in der kein H_i einen Fixpunkt besitzt. Dann hat H nur Fixpunkte. [Rotes Fragezeichen]
Bew:

$$\begin{aligned} n \cdot 1 + G &= H + \sum_{1}^{n} H_i \\ (*) \quad n f_1 &= |H| f_H \end{aligned}$$

es ist $|H| \leqq n$, da wegen $H_i \cap H = 1$ $|H_i| \leq \frac{|G|}{|H|}$, also $|H_i - 1| \leq |G/H| - 1$, $(\cup(H_i - 1)) \leq n(|G/H| - 1)$
andererseits $= |G| - |H|$
also $n(\frac{|G|}{|H|} - 1) \geq |G| - |H|$, $n \geq |H|$. [Das letzte „$\geq$“ ist mit Bleistift korrigiert zu „$\leq$!“]
Hieraus folgt mit $(*)$ $f_H \geq f_1$, also läßt H alles fest.

49. Aufgaben: Analogon z. Familienbild u. Isotgraph bei Charakteren. Klassifikation von p-Gruppen mittels Isotopiegraph. Weitere Hilfsmittel zur Berechnung von $\mu(Z < G)$ entwickeln;
Sonderfälle betrachten: Jeder Elementzentralisator zyklisch; jedes Element habe Primzahlpotenzordnung; jede abelsche Gr. zyklisch; jedes $C^* Z$ nilpotent. (vgl 38). Im letzten Fall muss die Struktur der Sylowgr. von G alles bestimmen.

Fixgruppen

50. Für jedes System von Untergr. H, welche mit ihren Konjugierten zusammmen ganz $\mathfrak{G}$ überdecken (die also mit jeder Klasse konjugierter Elemente etwas gemeinsam haben) gilt eine Beziehg der Form $f_G = \sum_D c_D f_H$, wo D die minim. Durchschnitte der H durchläuft.
Bew: Schrittweise $\varphi + \psi - \varphi\psi$ bilden für die char. Fktionen.
1 wird erreicht $1 = f_n$, wo $f_1 = \varphi_1, , f_{n+1} - f_n + \psi_{n+1} - f_n\varphi_{n+1}$
Kürzer: sind $\varphi_1 - \varphi_n$ die geg Char Fkten so
$\prod(1 - \varphi_\nu) = 0$
$1 = \sum \varphi_\nu - \sum_{\alpha<\beta} \varphi_\alpha\varphi_\beta + \sum \varphi_\alpha\varphi_\beta\varphi_\gamma - +-.$
Untersuchen: Zerlegg von G in spezielle Untergr. hängt zusammen mit Überdeckung durch Normalisatoren s. 171 unten.

51. Fragen: Sind zwei Darstellungen von G auf M, $(|G|, |M|) = 1$, schon dann äquivalent (dh. durch Automorphismen von M ineinander überzuführen), wenn die Ordnungen oder Strukturen der Fixgruppen der zyklischen Untergr von G in beiden Fällen übereinstimmen?
Wenn ja, folgt daraus Zassenhaus' Vermutung.
Hat es Sinn, den von G auf M erzeugten Rechtsring zu betrachten?

52 Zassenhauss' Vermutung mit Schur Meth. angr.:
nach einer Vertretergr. darstellen, Transmodul der 2. betrachten

53 Die Anzahl der bei G fest bleibenden p-Sylowgr von M ist [bei $(|G|, |M|) = 1$ und wenn G oder M aufl]:

$$p_G = \frac{|M_G|}{|N_G|}$$

wo $N = \mathcal{N}P \cap M$, $P =$ eine Sylowgr.
Folglich befriedigt p_G die gleichen multipl. Relationen in Abh von G wie v_G !
Wenn man dies umgekehrt ohne Benutzung der Vor zeigen könnte, folgt $p_G \geq 1$ und damit die Richtigkeit der Vermutung von Zassenhaus.

NB: Über Darstellung von $\mathfrak{G}$ durch Autom von $\mathfrak{H}$ im Fall $(|\mathfrak{G}|, |\mathfrak{H}|) \neq 1$ steht was in Hall-Higman

Aufgaben:

a. Halls Verallg. d. Satzes von Frobenius mit Charakteren beweisen (vielleicht mit Hilfe von Brauers Kennzeichnung d. Ch.) und auf Summen von Charakteren $\sum_{G^n \in K} \chi(G)$ erweitern, wo $\chi \neq 1$ sein kann.

b. Ist der Mittelwert einer Klassenfunktion auf $\mathfrak{G}$ ganzzahlige Linearverbindung der Mittelwerte auf den "speziellen" Untergruppen von $\mathfrak{G}$?

171/172

Perm - Gruppen.

1. Haben U, V auf Ω t_U bezw t_V Transs., so ist

$$t_{U\cap V} + t_{\{U,V\}} \geq t_U + t_V$$

Bew: Sind $F_U, \cdots$ die Fixräume, so ist

$$\begin{array}{rcl} F_{U\cap V} & \geq & F_U + F_V \\ \dim \cdots & \geq & t_U + t_V - \dim(F_U \cap F_V) \\ & = & t_U + t_V - t_{\{U,V\}} \end{array}$$

1 Ist eigentlich ein Satz über Durchschnitt und Erzeugnis zweier Einteilungen einer Menge

2. Sei $\lambda =$ „Länge $G : H$" = Schrittzahl der längsten Kette $G > H > H_2 > \cdots > H_\lambda = 1$, wobei jedes H_λ Durchschnitt gewisser H^g ist.
Sei H max in G. Stellt man G nach H als prim. PGr. dar, so wird nach 1

$$t_{H_\lambda} \geq t_H + t_{M_{\lambda-1}} + 1, \text{ da } \{H_{\lambda-1}, M^g\} = G,$$

wenn $H_{\lambda-1} \cap M^g = H_\lambda$. Ist also G pri und hat G_1 $1 + m$ Transsysteme und hat $G : G_1$ die Länge λ, so

$$\text{Gr } G = n = t_{H_\lambda} \geq t_{H_0} + \lambda t_{H_1} = 1 + \lambda m$$

172/173

3. G pri $\rightarrow$ G treu in jeden irred. Bestandteil. Folge: Hat die pri Gr G einen irred Bestandteil vom Grade f und der Vielfachheit e, so ist $\lambda(G : G_1) \leq \frac{f}{e}$.

4. Ist G unipri, so haben die H_λ von 3. alle mindestens 2 Transgebiete der Lge > 1, also kann man die festzuhaltende Ziffer jeweils aus einem Gebiet der Länge $< \frac{n}{2}$ wählen; daher ist

$$|G_1| \leq (\frac{n-1}{2})^\lambda,$$

und nach 3 $\lambda \leq \frac{n-1}{2}$
also $|G| \leq n \cdot (\frac{n-1}{2})^{\frac{n-1}{2}}$ wenn G unipri.

5. Ebenso: hat G_1 mindestens 3 (≥ 4) Transgebiete der Lge > 1, so hat jedes H_λ mindestens 3 (≥ 4) Transgebiete der Lge > 1, daher dann, wenn G pri:

$$\begin{aligned} |G| &\leq n(\frac{n-1}{3})^{\frac{n-1}{3}} \\ \text{bzw.} &\leq n(\frac{n-1}{4})^{\frac{n-1}{4}}. \end{aligned}$$

Perm. - Gr.

6. In einer prim. PGr $\mathfrak{G}$ ist jeder irred Bestandteil $\neq 1$ treu, sein Zentrum ist 1.

7. Eine pri $\mathfrak{G}$ enthält keinen irred. Bestandteil $\neq 1$ vom Grad 1, ausser wenn $|\mathfrak{G}| = p$.
Bew 6: $\mathfrak{G}$ abelsch

8. Hat eine prim $\mathfrak{G}$ einen irred Bestandteil vom Grade 2, so ist $\mathfrak{G}$ eine Frobeniusgruppe. Denn $\mathfrak{G}_1$ lässt einen 1-dim VRaum von dem zwei-dim Darst Raum fest, $\mathfrak{G}_{12}$ also den ganzen Darst-R.
Allgemeiner:

9. Hat eine pri $\mathfrak{G}$ einen irred Bestandteil $\neq 1$ des Grades f der Vfh e, so ist die Länge von $\mathfrak{G} : \mathfrak{G}_1 \leq \frac{f}{e}$. Daher ist jedes $G \in \mathfrak{G}$ durch die Wirkung auf $\frac{f}{e}$ "unabhängige" Ziffern bestimmt.

10. Gilt für die Untergruppen H der Permgr G

$$\sum c_H H = 0,$$

so gilt für die Anzahl t_H der Trans-Systeme von H

$$\sum c_H \cdot |H| \cdot t_H = 0$$

Bew: oben Hauptcharakter einsetzen.

Meth v. Schur

1. Geg. sei reg Gruppe $\mathfrak{H} : \binom{x}{x_H}$ und $\mathfrak{K}$ sei ein Komplex in $\mathfrak{H}$. Dann gehören genau die Abb. $\binom{x}{x^\sigma}$ aus $\mathfrak{S}^{\mathfrak{H}}$ zur grössten Gruppe $\mathfrak{G}$, deren $\mathfrak{G}_1$, $\mathfrak{K}$ fest lässt, für welche gilt

$$(\mathfrak{K}X)^\sigma = \mathfrak{K} \cdot X^\sigma$$

also ein σ mit $\sigma = \binom{1\ \ -}{1\ \ -}$ ist in $\mathfrak{G}$. (dh in $\mathfrak{G}_1$) genau wenn

$$(\mathfrak{K}X)^\sigma = \mathfrak{K}^\sigma X^\sigma$$

insbesondere enthält $\mathfrak{G}_1$ alle Autom von $\mathfrak{H}$, welche $\mathfrak{K}$ in sich überführen.

Perm.-Gr vom Grad 26.

Fortsetz. v. 108

1. Enthält der 13-Sylow-$\mathfrak{Ns}$ ein El. d. Ord 2, so transformiert dieses jeden der beiden 13-Zyklen in sich, daher transformiert es sie oBdA konform und muss daher $B \to B'$, andererseits $\to B$ transformieren: $B = B'$. Für die nichttrivialen EWe a von A usw gilt dann:
$\beta = \varepsilon^m + \varepsilon^n + \varepsilon^{-m} + \varepsilon^{-n}$ ist Einheit.
Denn $= (\varepsilon^{m+n/2} + \varepsilon^{-\cdots})(\varepsilon^{m-n/2} + \varepsilon^{-\cdots})$
Es ist $\alpha = \overline{\alpha} = \Sigma$ von $6\,\varepsilon^i$, und entweder ist auch $\mathcal{N}\alpha = 1$, oder $\mathcal{N}\alpha = 25^2$, (α) Primideal des Grades 4 in $\mathrm{Ra}(\varepsilon)$

$$(\gamma) = (\alpha') \neq (\alpha),$$

wo $'$ ein Autom v. $K = \mathrm{Ra}(\varepsilon)$.
$\vartheta :\ 1 + \varepsilon + \varepsilon^{-1}$ dürfte Einheit sein: $\mathrm{Sp}\vartheta^2 = 30 \to \mathcal{N}\vartheta^2 \leq \left(\frac{30}{12}\right)^{12}$
$\mathcal{N}\vartheta \leq \left(\frac{3}{2}\right)^6 < 16^2$; Da ϑ reell, hat es einen geraden Grad, falls prim; da sonst $p^\nu \underset{13}{\equiv} 1$ und $p^\nu < 16$, und da $(\vartheta, 1-\varepsilon) = 1$, also $\mathcal{N}\vartheta \equiv 1$ (13), muss $\mathcal{N}\vartheta = 1$ sein. (jede $\mathcal{N}\vartheta$ ist Produkt von Primzahlpotenzen $\equiv 0, 1$ (13).

2. Es ist stets $\begin{cases} \alpha^2 + \alpha + \beta\overline{\beta} = 6 \\ (\alpha - \gamma)^2 + \beta\overline{\beta} = 5^2 \end{cases}$. Vielleicht kann man eine Cauchysche Parameterdarstellung verwenden, namentlich wenn $\beta = \overline{\beta}$.

3. Erledigung des Falls $\beta = \overline{\beta}$ (und damit $2 \mid (\mathcal{N}\mathfrak{P}_{12}|)$: $\beta = \overline{\beta}$ ergibt keine mögliche Matrix:
mit $\Delta = \varepsilon + \varepsilon^{-1} - 2$, $\Delta^{(a)} = \varepsilon^a + \varepsilon^{-a} - 2$ wird (Induktion) Kürzer: 181
$(*)$ vgl. 178 $\varepsilon^a + \varepsilon^{-a} \equiv 2 + a^2 \cdot \Delta - a^2(a^2-1) \cdot \Delta^2 (\mod \Delta^3)$
Ist nun $\begin{cases} \alpha = \varepsilon^a + \varepsilon^{-a} + \varepsilon^b + \varepsilon^{-b} + \varepsilon^c + \varepsilon^{-c} \quad (a^2 \not\equiv b^2 \not\equiv c^2) \\ \beta = \varepsilon + \varepsilon^{-1} + \varepsilon^d + \varepsilon^{-d} \end{cases}$ so wird jedenfalls mit ganzen Koeffizienten

$$\begin{aligned} \alpha &\equiv 6 + u\Delta + v\Delta^2 \quad (\Delta^3) \\ \beta &\equiv 4 + w\Delta + z\Delta^2 \quad (\Delta^3) \end{aligned}$$

und wegen $\alpha^2 + \alpha + \beta^2 - 6 = 0$ wird hiernach

$$\begin{cases} 6^2 + 6 + 16 - 6 \equiv 0 & (13) \\ \underline{12u} + 8w + \underline{u} \equiv 0 & (13) \\ \underline{12v} + u^2 + \underline{v} + 8z + w^2 \equiv 0 & (13) \end{cases} \begin{pmatrix} \text{Koeff} & 1 \\ & \Delta \\ & \Delta^2 \end{pmatrix}$$

daher $0 \equiv w$, $u^2 + 8z \equiv 0(13)$
Nun ist nach $(*)$

$$\left.\begin{array}{rcl} \alpha & \equiv & 6 + (a^2+b^2+c^2)\Delta - \{a^4+b^4+c^4-a^2-b^2-c^2\}\Delta^2 \\ \beta & \equiv & 4 + (1+d^2)\Delta - (d^4-d^2)\Delta^2 \end{array}\right\} \quad (\Delta^3)$$

Also

$$\begin{aligned} w &\equiv 1 + d^2 \equiv 0, d \equiv \pm 5 \\ z &\equiv -d^4 + d^2 \equiv -1 - 1 \equiv -2 \\ u^2 &\equiv -8z \equiv 16 \\ a^2 + b^2 + c^2 = u &\equiv \pm 4 \end{aligned}$$

176/177

Weiter ist nach (2)

$$(\alpha - \gamma)^2 = 25 - \beta^2$$

und

$$\beta = \varepsilon + \varepsilon^{-1} + \varepsilon^5 + \varepsilon^{-5},$$

also $\beta = \beta^{(5)}$. Daher $(\alpha - \gamma)^{(5)} = \pm(\alpha - \gamma)$ und daher $\alpha^{(5)} = \begin{cases} \alpha \\ \gamma \end{cases}$ da kein Koeff in $\alpha - \gamma$ verschwindet.
$a^2 + b^2 + c^2 = 4$ gibt nur die Summanden $1, 4, -1$, dann ist aber $a^{(5)} = \alpha$:
$\alpha^{(5)} = \alpha \to 6 =$ Gliederzahl $\alpha \equiv 0(4)$ W!
Hiermit ist $\beta = \overline{\beta}$ widerlegt.
Der $\mathcal{N}\mathfrak{P}_{13}$ enthält also ein El der Ord 3, daher ist

$$\beta = 1 + \varepsilon + \varepsilon^3 + \varepsilon^9$$

$$\beta\overline{\beta} = 3$$

$$\alpha^2 + \alpha - 3 = 0$$

$$\alpha = -\frac{1}{2} \pm \frac{1}{2}\sqrt{13} = \sum \varepsilon^{\square}$$

und es gibt also keine Matrix V für $n = 26$ als die von S. 108. Diese führt laut Rechnung nicht zu einer Gr $\mathfrak{G}$ des Gr 26, die unipri ist, also gibt es keine solche Gruppe.

177/178

1. Allg. ist

$$x^a + x^{-a} = 2 + \underbrace{a^2 \cdot (x+}_{\binom{a+1}{2}+\binom{a}{2}} x^{-1} - 2) + \underbrace{\left\{ \binom{a+2}{4} + \binom{a+1}{4} \right\}}_{\frac{a^2(a^2-1)}{12}} (x + x^{-1} - 2)^2 + \ldots$$
$$\text{Vermutl. } \binom{a+3}{6}+\binom{a+2}{6}$$

$a = 0, 1, 2, \cdots$
Es handelt sich um die Entwickelung von $\sin^2 a\varphi$ nach Potenzen von $\sin^2 \varphi$.
Verwandt mit $\cos n\varphi$ nach Potenzen von $\cos \varphi$

2. Das gibt Methode zur Untersuchung von Beziehungen zwischen Einheitswurzeln ε^a ($\operatorname{Ord}\varepsilon = p^\nu$): ε^a nach Potenzen von $1-\varepsilon$ (oder $\varepsilon - 2 + \varepsilon^{-1}$ und so weiter) entwickeln, dadurch kommen die Exponenten als Polynome "herunter", gibt g rat. Kongruenzen zwischen Polynomen der Exponenten. Speziell für lineare Kongruenzen **???**[Kurzschrift] ε^a:

3. Ist $g(x) = \sum a_\nu x^\nu$ ein Polynom mit ganzen rat Koeff und $\varepsilon^{p^m} = 1$ (siehe hierzu 180), so ist für jedes nat. $k < \varphi(p^m) =: M$:
$g(\varepsilon) \equiv 0$ und $(1-\varepsilon)^k \leftrightarrow \frac{g^{(\kappa)}(1)}{\kappa!} \equiv 0(p)$
$\leftrightarrow g(x) \equiv 0[\text{modd } p, (1-x)^M]$ $(\kappa = 0, 1, \ldots, k)$.
Bew: $g(x) = \sum \frac{g^{(K)}(1)}{\kappa!}(1-\zeta)^\kappa \quad (x = 1-\varepsilon)$

Bemerkg: 4: Genügt eine Matrix P der Gl $P^{p^m} = 1$, so folgt aus $g(P) = 0$ stets $\frac{g^{(\kappa)}(1)}{\kappa!} \equiv 0(p)$ $[\kappa = 0, 1, \ldots]$

5. Ähnlich für jedes ξ mit $1 - \xi \neq$ Einheit.

178/179

6. Insbesondere ergeben Beziehung zwischen m-gliedrigen Perioden η stets Kongruenzen für die m-ten Perioden der Exponenten a: $\eta = \varepsilon^a + \varepsilon^{as} + \cdots +$ mit $s^m = 1$
Das sollte zB. für Gaußsche Summen nützen.

7. In der Entwickelung einer Größe ξ (nach $(1-\vartheta)$), die bei der GaloisGr d. Ord m ungeändert bleibt, treten nur Polynome der a^m als Koeff. $\frac{g^{(\kappa)}(1)}{\kappa!}$ auf?

$$\begin{aligned}\xi = \sum_{s^m=1} \varepsilon^{as} &= \sum_s (1+\delta)^{as} \qquad \delta = \varepsilon - 1 \\ &= \sum_\nu \sum_s \binom{as}{\nu} \delta^\nu \\ &= m \sum_\nu \delta^\nu \cdot \text{ Summe der Glieder } a^k, \\ &\qquad\qquad \text{deren Exponenten } k \equiv 0(\mod m) \text{ sind.}\end{aligned}$$

Hieran wird man oft sehen können, in welchem Körper eine Grösse liegt. Anwenden auf Gr $= p$: VIII 166 (2) $\kappa\overline{\kappa} = \frac{k(p-k)}{p-1}$

8. Frage: Ist eine pri Gruppe des Grades n stets 2-tra, wenn

$$p \mid n, \quad n < \binom{p}{2}?$$

178/179

1. Man kann mit der Methode von S. 178 auch Einheitswurzeln beliebiger Ord. untersuchen, indem man einen Körper als Grdk. wählt, über den sie Ord p^m haben: Die p^m-ten EW sind unabh. über den k-ten, wenn $(k,p)=1$.

1a. Aufgabe: Alle Beziehungen zwischen n-ten EW angeben von der Form $\sum \varepsilon_\rho = 0$.

2. Kann man damit an meine Vermutung über die B-Eigenschaft der $\{P\}\times K$ mit $\operatorname{Ord} P = p^\alpha$, $(p,|K|)=1$?

4. Die Methode von S. 178 führt man wohl noch besser durch Entwicklung nach $\Delta = \log(1+\delta)$ durch:
$\varepsilon^n = 1, \varepsilon = 1+\delta, 0 \le a < p \to \varepsilon^a = e^{a\log(1+\delta)} = \sum\limits_0^\infty \frac{a^\nu}{\nu!}\Delta^\nu\big|_{<p}$; $\delta^1 \top \Delta$,

$$\text{d.h. } \boxed{\varepsilon^a \equiv \sum_{\nu=0}^{p-1} \frac{a^\nu}{\nu!}\Delta^\nu \mod \Delta^p}$$

5. Hiermit ergibt sich z.B: Aus $\kappa = \sum \varepsilon^a$, $\kappa\overline{\kappa} \equiv k^2 \mod p$ folgt für die $s_\nu = \sum a^u$:
$$\sum_{\lambda+\mu=n} \frac{s_\lambda}{\lambda!}\frac{s_\mu}{\mu!}(-1)^\lambda \equiv 0 \text{ für } 0 < n < p.$$
dh für $f(x) = \sum \frac{s_\lambda}{\lambda!}x^\lambda : f(-x) = \frac{1}{f(x)}$
$\frac{f(x)-k}{f(x)+k}$ ist eine ungerade Funktion |alles immer mod Δ^p|.
wenden!

180/182

[Im Tagebuch gibt es keine Seite 181]

6. Die Rechnung von S. 177 geht jetzt kurz: Ist
$$\begin{aligned} \alpha &= \varepsilon^a + \varepsilon^{-a} + \varepsilon^b + \varepsilon^{-b} + \varepsilon^c + \varepsilon^{-c} \\ \beta &= \varepsilon + \varepsilon^{-1} + \varepsilon^d + \varepsilon^{-d} \end{aligned}$$
und bezeichnet S_ν, t_ν die ν-te PotSumme von abc bzw $1d$ so ist (4)
$$\alpha \equiv 6 + s_2 X + \frac{s_4}{12}X^2$$
mit $\Delta^2 = X$
$$\beta \equiv 4 + t_2 X + \frac{t_4}{12}X^2,$$
also folgt durch Vergleich des Koeff von X in $\alpha^2 + \alpha + \beta^2 - 6 \equiv 0$:
$$12s_2 + s_2 + 8t_2 \equiv 0 \quad t_2 \equiv 0 \quad d \equiv 5 \quad t_4 = 2$$

daher X^2:

$$\cancel{S_4} + S_2^2 + \frac{\cancel{s_4}}{\cancel{12}} + \frac{16}{12} \equiv 0$$

$$S_2^2 \equiv 16 \qquad S_2 \equiv \pm 4$$

Allgemeine Fassung der Methode:

7. Setzt man

$$\left.\begin{array}{rcl} \exp x & = & 1 + \frac{x}{1!} + \cdots + \frac{x^{n-1}}{(n-1)!} \\ \log(1+x) & = & x - \frac{x^2}{2} + \cdots \pm \frac{x^{n-1}}{n} \end{array}\right| \quad \text{abgebrochen}$$

und ist $1, 2, \cdots, n-1$ teilerfremd zu der ganzen Zahl $\xi \in Ra[\vartheta]$, so existiert $\log(1+\xi) \mod \xi^n$ und $\exp\log(1+\xi) = \xi$ und man kann die Koeff in der Entwickelung nach Potenzen von ξ vergleichen mod ξ.
z.B.: $\varepsilon^p = 1, \xi = \varepsilon^2 - 2\varepsilon + 1$
Also: $\varepsilon^p - 1 \to \log\varepsilon$ existiert mod $(\varepsilon-1)^p = p(\varepsilon-1)$

182/183

8. Ein $\mathfrak{p}$-adischer Logarithmus λ in $K_8(\varepsilon)$ existiert <u>nicht</u> für ε in dem Sinn, dass eine hom Abb. der mlt. Gr in die add Gr möglich wäre: ε hat endl. Ord.
Also man kann Logarithmen von p-ten EW nur mod p einführen, $\mathfrak{p}$-adik nützt nichts beim Problem von S. 181.

9. In 182.7:
Die „Perioden“ der abgebroch. Expfkt sind die η mit $\frac{1}{1!} + \frac{\eta}{2!} + \cdots + \frac{\eta^{n-2}}{(n-1)!} = 0$

10. Allgemein kann man über jedem Ring R (durch Erweiterung) Logarithmen einführen: Im Ring $R(t)$ der formalen Potenzreihen rechne mod $\exp t - a$, wo $a \in R$ fest.

1 Hall & Ryser: Cyclic incidence matrices
Can. J. Math 3 495-502
zitiert u.a. Bruck & Ryser Can. J. Math. 188-93
S. Chowla Proc NAS 35(1949) 92-94
Chowla & Ryser Can. J. M. 2 93-99
M Hall Duke M. J. 14, 1079-1090 (1947)

183/184

$p - 1 = abc$ Gruppen vom Grad p (Forts. v. S. 40)

$ab\gamma + c\Gamma = p : i = \alpha A,\ \beta B,\ \gamma\Gamma \quad i = aA$ **???**βB
$\alpha = kl$: pos. Rest $(bc)^{-1} \mod a$: $\quad bc\alpha \equiv 1$ (a)
$\beta, \gamma \cdots$ I: $ab\gamma + \cdots$ $\quad$ II: $= 2p + 1$

p	$a\ b\ c$	α	β	γ		A	B	Γ
43	2·3·7	1	2	6	II	$11 \leftarrow$	5	1
61	4·3·5	3	2	3	II	2^2	$7 \leftarrow$	5
71	2·5·7	1	4	5	II	$2 \cdot 3^2$	3	3
67	2·3·11	1	1	2	II	17	$3 \cdot 5$	5
79	2·3·13	1	2	11	II	$2^2 \cdot 5$	3^2	1
103	2·3·17	1	1	3	I	$2 \cdot 13$	$23 \leftarrow$	5
31	2·3·5	1	1	1	I	2^3	7	5
131	2·5·13	1	1	4	I	$3 \cdot 11$	$3 \cdot 7$	7
151	$2{\cdot}3{\cdot}5^2$	1	2	21	II	$2 \cdot 19$	17	1

Faktorzerlegung von $AB\Gamma$ unwahrscheinlich: $\leftarrow$ grosse Primfaktoren der Invarianten. Setze

$$\Pi = AB\Gamma, \quad \pi = \alpha\beta\gamma$$

Es ist

$$\Pi \equiv \pi \mod p$$
$$\pi < abc = p - 1, \Pi < a^2b^2c^2 = (p-1)^2$$

18.1.1959 $\qquad$ Grad $\mathfrak{G} = p$ $\qquad$ Forts. von 40, 184

(1) Ist $p - 1 = 2^\alpha q^\beta r^\gamma$, so gibt es ≤ 2 Klassen von konjugierten Untergr. vom Index p.

Wenden!

Bew: Sonst mit Bez. v. S. 184

$$ii'i'' = \pi\Pi = j^2 \equiv \pi^2 (p)$$

$$j \equiv \pm\pi (p) \quad j = \pm\pi + mp = 0$$

Hier $a, b, c = 2^\alpha, q^\beta, r^\gamma$ bis auf Reihenfolge, die nachher passend gewählt wird.

$$\pi\Pi = \pi^2 \pm 2\pi mp + m^2p^2 \qquad \Pi = \pi \pm 2mp + \frac{m^2}{\pi}p^2$$

$$\pi \big| m^2 \quad m^2 \geq \pi \quad \Pi \geq \pi \pm 2mp + p^2$$

3 Fälle

1)

$$j = +\pi + mp \to (p-1)^2 \geq \Pi \geq \cdot + \cdot + p^2 \geq p^2 \quad \text{W!}$$

2)

$$\begin{aligned} j = -\pi + mp \;\; \& \;\; \frac{m^2}{\pi} \geq 2: \;\; 2mp &\geq \pi + 2p^2 - \Pi \geq 1 + 2p^2 \\ &\qquad -(p-1)^2 \\ &\geq p^2 + 2p \\ m &\geq \frac{p}{2} + 1 \\ j = -\pi + mp &\geqq (p - \pi) + \frac{p^2}{2} > \frac{p^2}{2} \\ p^3 > (p-1)^3 > \pi\Pi &> j^2 \frac{p^4}{4} \qquad p < 4 \quad \text{W!} \end{aligned}$$

3)

$$j = -\pi + mp, \;\; \pi = m^2, \;\; \Pi = m^2 - 2mp + p^2 = (p-m)^2$$
$$m = \sqrt{\pi} < \sqrt{p-1} \quad \Pi > (p - \sqrt{p-1})^2$$

Andererseits

$$(p-1)\Pi = abc\Pi = (p - ab\gamma)(p - bc\alpha)(p - ca\beta)$$

$$\begin{aligned} \Pi &< (p - ab\gamma)(p - ca\beta) \\ &= p^2 - p(ab\gamma + \cdot) + a \cdot (p-1)\beta\gamma \\ 2p\sqrt{p-1} - (p-1) &> p(ab\gamma + ca\beta) - a(p-1)\beta\gamma \\ 2p\sqrt{p-1} &> pab\gamma + ca\beta + (p-1)[a\beta(c-\gamma) + 1] \\ &> pab \end{aligned}$$

quadrieren:

$$4abc > a^2b^2, \quad 4c > ab \geq (c+2)(c+1),$$

wenn $a > b > c$, $c > c^2 \leq 3$ W!

185/186

1. B. Eckmann: Der Cohomologie-Ring einer beliebigen Gruppe: Comm. math Helv. 18(1945/6),232-282

2. Frobenius: Über Gruppen der Ordnung $p^\alpha q^\beta$ Acta Math 26 1902 Über die Kompos.reihe einer Gruppe. SB 1916.

3. Lit zur Beziehg zwischen Norm und Spektralnorm (zur Eckenfrage beim 3-dim Wertevorrat einer Matrix)
Lit-verz. in Mott-Schneider, Archiv 1958/9)

4. Schur: Über eine Klasse von Mittelbildungen mit Anwendungen auf die Determinantentheorie.
   Sitzber Berl math Ges 22(1923), 9-20

Fortsetzg von 185: Nach Hall & Ryser (Can. J. Math 3)
müssen, wenn j überhaupt in der Form $\beta\overline{\beta}$ dargestellt werden kann in $Ra(\sqrt[p]{1})$, die Gleichungen

$$x^2 = jy^2 + (-1)^{\frac{p-1}{2}} pz^2 \text{ und } \xi^2 = j\eta^2 + \zeta^2$$

nichttriviale ganzzahlige Lösungen haben.

Fortsetzg von 185: Gr. v. Gr. p = Primzahl

(1) Ansatz zum Beweis, dass stets ≤ 2 Klassen konj. Ugr vom Index p existieren:
Es genügt zu zeigen, dass für je drei Zerlegungen $p-1 = a_\lambda b_\lambda$ $(\lambda = 1,2,3)$ mit $(a_\lambda, b_\lambda) = 1$ $a_\lambda > 1, b_\lambda > 1$ gilt:

$$\prod_1^3 \left[\frac{a_\lambda^{-1}}{b_\lambda}\right]\left[\frac{b_\lambda^{-1}}{a_\lambda}\right] \neq \square$$

Dabei bezeichnet $\left[\frac{a}{b}\right]$ den kleinsten positiven Rest von $a \mod b$. Dazu können rekursive Formeln für $\left[\frac{a^{-1}}{b}\right]$ helfen, die die Argumente verkleinern. z.B.

$$\left[\frac{a^{-1}}{b}\right] = \left[\frac{a'^{-1}}{b}\right] \quad \text{wenn } a \equiv a'(b)$$

Anderer Ansatz 188

(2) Es ist

$$\underset{\alpha}{\left[\frac{a_1^{-1}}{b_1}\right]} \quad \underset{\beta}{\left[\frac{b_1^{-1}}{a_1}\right]} = \square \iff a_1 = 1 \text{ oder } b_1 = 1$$
$$\iff \square = 1 \quad (a_1 b_1 = p-1)$$

denn

$$\alpha a + \beta b = p$$
$$\alpha\beta ab = (p - \beta b)\beta b$$
$$x^2 = \alpha\beta \equiv (\beta b)^2 \to x \equiv \beta b \quad x = \beta b \text{ oder } \alpha a$$

Sei etwa $x = \beta b$, dann $\beta^2 b^2 = \alpha\beta$ $\alpha = \beta b^2, \beta b \mid p$

(3) Ist $p-1 = k_1 + l_1 = k_2 + l_2$ und $\frac{k_1 l_1 k_2 l_2}{(p-1)^2} = x^2$, x ganz, so ist bei passender Bezeichng. $k_1 = k_2,\ l_1 = l_2$.
Bew: Bezeichne so, dass $k_1 \equiv k_2(2), l_1 \equiv l_2(2)$ und $k_1 k_2 \leq l_1 l_2$. Dann ist

$0 < |x| < \frac{p+1}{4}$
$k_1 k_2 \equiv x^2 (p)$
Bei passender Wahl von Sign x ist $k_1 k_2 = mp + x, \quad 0 \leq m$ und wegen $k_1 k_2$ wird $m \leq |x|$.
Aus $(*)$ $k_1 k_2 (p - k_1)(p - k_2) = (p-1)^2 x^2$ folgt

$$(x + m) \equiv \frac{k_1 + k_2}{2} (p) \qquad \text{also}$$
$$\frac{k_1 + k_2}{2} = x + m + \varepsilon p, \quad \varepsilon = 0, 1$$

$k_1 k_2 = mp + x$ gibt nun

$$0 < (p-1)x = (\frac{k_1 + k_2}{2} - \varepsilon p)p - k_1 k_2 \text{ daher } \varepsilon = 0$$
$$\frac{k_1 + k_2}{2} = x + m \text{ gilt mit } (*)$$
$$mp + x = (m + x)^2$$
$$k_1 k_2 = \big(\frac{k_1 + k_2}{2}\big)^2, \quad k_1 = k_2$$

Ansatz: Ebenso zeigen, dass aus $\frac{\prod k_i l_i}{(p-2)^3} = x^2$ folgt ein $k_i = k_j$: Das genügt für Klassenzahl ≤ 2.
Forts. XI 38

Subnormale Untergruppen: 1, 24, 90, 92, 96, 105
Komposfaktorgruppen von Durchschnitten: 83-85
Hallgruppen, Sylowsätze: 1, 2
Primitive Permutationsgruppen: 74-75, 78-79, 109, 111-112, 115-118, 139-148, 148-57, 172-174
Abschliessung von Permutationsgr.: 50-54, 67-73, 76-77, 80, 140
Permutationen auf Ähnlichkeitsklassen: 2, 4-5, 12-17, 23
Perm: Gruppen vom Grad p, $2p$: $33\text{-}47_{p}$, $55\text{-}66_{p}$, 108_{2p}, 113_{2p}, 125_{3p}, 176_{26}, 184_{p}, 187_{p}
p-Gruppen (Automorphismen): 3, 103
Breite von: 146-148
Selbstkonjugierende Untergr.: 6-8
Erweiterungstheorie: 48, 88-89, 96-99
Intravarianz: 9-10, 87, 93-95
Monomiale Gruppen: 114
Schur-Methode: Faktorisierung: 19-21, 106, 110, 119-122, 126-132, 138, 175
Verlagerung: 96, 100-102, 107
p^a-Satz von Burnside: 18-19, 106 ← Gastein
Klasse $(n-1)$-Satz v. Frobenius: 82, 141
Ringe, Algebren: 22, 26-32 (auch endl. Schiefkörper)
Hauptfaktoren unendlicher Gr.: 91
Gruppencharaktere: 133-137, 143-44
Fixgruppen von Automorphismen: 158-170
Einheitswurzeln (Beziehungen zwischen): 178-183

M. Rev Cunihin Gol'berg
9; 492, 6 (p-Überauflösbarkeit)
10; 588, 678, 505
11; 495, 321
12; 156, 800
13; 818
14; 350, 139
15; 196 (w-Länge), 286
16; 10, 331, 898
17; 235
18; 110