Prof. Dr. Helmut Wielandt

Tagebücher

D13

März 62 – Dezember 65

XIII
März 62 - Dezember 65

Reichardt: Vektor u Tensor R
Blaschke: 2. Aufl. 1960
Rudin: Fourier Analysis on groups
Vortrag 3.3.64: On the theory of permutation groups

Einband/ 0 = Inhaltsverzeichnis

0/1

Zentrale Automorphismen der Ord p gibt es für die Gruppe $\mathfrak{G}$ genau dann, wenn für den Kommutatorindex $i_{\mathfrak{G}}$ und die Zentrums Ord $z_{\mathfrak{G}}$ gilt: $p\big|(i_{\mathfrak{G}}, z_{\mathfrak{G}})$, und wenn nicht $\mathfrak{G} = \mathfrak{A} \times \mathfrak{B}$ und $|\mathfrak{A}| = 2 \qquad 2 \nmid i_{\mathfrak{B}}, \quad 2 \nmid z_{\mathfrak{G}}$

1/2

8.3.62

Vertauschbarkeit subnormaler Ugr.

Sei $\mathfrak{A} \lhd\lhd \mathfrak{G}$, $\mathfrak{B} \lhd\lhd \mathfrak{G}$, $\mathfrak{A}^*$ die größte mit $\mathfrak{B}$ vtb subnormale Ugr von $\mathfrak{A}$; dito $\mathfrak{B}^*$
Dann gilt:

(1) $\mathfrak{A}\big|$ Kern $\mathfrak{A}^*$ nilpot., $\mathfrak{B}\big|$ Kern $\mathfrak{B}^*$ nilp., genau gleiche Primteiler in $\big|\mathfrak{A}/\mathfrak{A}^*\big|, \big|\mathfrak{B}/\mathfrak{B}^*\big|$, alle "kritisch", d.h. es gibt nichtmod. Ausschnitte in $\mathfrak{G}$.
Bew.:

α) $\mathfrak{A}^\nu \leq \mathfrak{A}^*$, da $\mathfrak{A}^\nu \,\mathrm{v}\, \mathfrak{B}$

β) Ann. Sei p Primt. $\mathfrak{A}/\mathfrak{A}^*$, nicht $\mathfrak{B}/\mathfrak{B}^*$; dann $\mathfrak{A} \,\mathrm{v}\, \mathfrak{B}^*$, $\mathfrak{A}_{\overline{p}} \,\mathrm{v}\, \mathfrak{B}^*$, $\mathfrak{B} = \langle \mathfrak{B}^* \cdot \cdot \mathfrak{C}_S \rangle$ $\mathfrak{C}_S$ ein - $\overline{p}$-köpfig

$$\mathfrak{A}_{\overline{p}} \,\mathrm{v}\, \mathfrak{B} \qquad \mathfrak{A}_{\overline{p}} \leq \mathfrak{A}^* \qquad \text{W!}$$

γ) Sei p gemeins. Primt $\mathfrak{A}/\mathfrak{A}^*$, $\mathfrak{B}/\mathfrak{B}^*$ nicht kritisch: Dann $\mathfrak{A}_{\overline{p}}$ seminor, $\mathfrak{A}_{\overline{p}} \,\mathrm{v}\, \mathfrak{B}$ W!

(2) $\mathfrak{A}^*$ ist die maximale mit $\mathfrak{B}$ vtb. Untergruppe schlechthin! Diese ist also stets subnormal.
Bew: $\mathfrak{A}^* \leq \mathfrak{U} \leq \mathfrak{A} \to \mathfrak{U} \lhd\lhd \mathfrak{A}$, der Kern $\mathfrak{A}^* \leq \mathfrak{A} \leq \mathfrak{U}$ & $\mathfrak{A}/$ Kern nilp.
[Von S. 3 übernommen:]
Für beliebige Gr. bei Roseblade-Stonehewer, J. Alg. 8 (1968)!

2/3

(3) Sei $\mathfrak{P}$ p-Sylowgr $\mathfrak{G}$. Dann ist $\mathfrak{A}^*_{\mathfrak{P}}$ $(= \mathfrak{A} \cap \mathfrak{P})$ die größte mit $\mathfrak{B}_{\mathfrak{P}}$ vertb Ugr von $\mathfrak{A}_{\mathfrak{P}}$.
Bew.

α) $\mathfrak{A}^* \,\mathrm{v}\, \mathfrak{B} \to \mathfrak{A}^*_{\mathfrak{P}} \,\mathrm{v}\, \mathfrak{B}_{\mathfrak{P}}$

β) Sei $\mathfrak{A}^*_{\mathfrak{P}} \leq \mathfrak{Q} \leq \mathfrak{A}_{\mathfrak{P}}$, $\mathfrak{A} \,\mathrm{v}\, \mathfrak{G}_{\mathfrak{P}}$
$\mathfrak{Q}^{\cdot\cdot\mathfrak{G}} \,\mathrm{v}\, \mathfrak{B}_{\mathfrak{P}}^{\cdot\cdot\mathfrak{G}} = p^{\mathfrak{B}}$
$\downarrow = \mathfrak{R} \trianglelefteq\lhd \mathfrak{A}$
da $\mathfrak{R}$ $p\times$ einköpfig, folgt $\mathfrak{R} \,\mathrm{v}\, \mathfrak{B}, \mathfrak{R} \leq \mathfrak{A}^* \to \mathfrak{Q} \leq \mathfrak{A}^*_{\mathfrak{P}}$

3/4

Maximale nilpot. Untergruppen

(1) Seien $\mathfrak{P}_1 \times \mathfrak{Q}_1$, $\mathfrak{P}_2 \times \mathfrak{Q}_2$ maximale nilpotente pq-Untergr. von $\mathfrak{G}$.

a) Ist $\mathfrak{P}_1 \underset{c}{\leq} \mathfrak{P}_2$, so $\mathfrak{Q}_1 \underset{c}{\geq} \mathfrak{Q}_2$

b) Ist $\mathfrak{P}_1 \underset{c}{=} \mathfrak{P}_2$, so $\mathfrak{Q}_1 \underset{c}{=} \mathfrak{Q}_2$

c) Sogar $\mathfrak{P}_1\mathfrak{Q}_1 \underset{c}{=} \mathfrak{P}_2\mathfrak{Q}_2$

wobei c: bis auf Konjugiertheit in $\mathfrak{G}$
Bew:

(a) OBdA $\mathfrak{P}_1 \leq \mathfrak{P}_2$. $\exists g \in$ Zs $\mathfrak{P}_1$:
$\langle \mathfrak{Q}_1, \mathfrak{Q}_2^g \rangle q$ - Gp.; wegen $\mathfrak{R}_1 \times \mathfrak{Q}_1$ maximal
ist 〃 $= \mathfrak{Q}_1$; $\mathfrak{Q}_2^g \leq \mathfrak{Q}_1$

(b) Klar: Vertausche Rolle 1,2.

(c) Ist sogar $\mathfrak{P}_1 \underset{c}{=} \mathfrak{P}_2$, so oBdA $\mathfrak{P}_1 = \mathfrak{P}_2$, wie ob $\langle \mathfrak{Q}_1, \mathfrak{Q}_2^g \rangle = \mathfrak{Q}_1$, $\mathfrak{Q}_2^g = \mathfrak{Q}_1$, $g \in$ Zs $\mathfrak{P}_1$ $(\mathfrak{P}_2 \times \mathfrak{Q}_2)^g = \mathfrak{P}_2^g \times \mathfrak{Q}_2^g = \mathfrak{P}_1 \times \mathfrak{Q}_1$

(2) Verallg: Sei $\rho + (p) = \sigma$; $\mathfrak{A}_\rho \times \mathfrak{A}_p$. $\mathfrak{B}_\rho \times \mathfrak{B}_p$ seien max. nil σ- Gr in $\mathfrak{G}$

a) Sei $\mathfrak{A}_\rho \underset{c}{\leq} \mathfrak{B}_\rho$; dann $\mathfrak{A}_p \underset{c}{\geq} \mathfrak{B}_p$,

b) aus $\underset{c}{=}$ folgt $\underset{c}{=}$

c) und sogar $\mathfrak{A}_\rho \times \mathfrak{A}_p \underset{c}{=} \mathfrak{B}_\rho \times \mathfrak{B}_p$

4/5
Seite 5 ist leer
5/6

Permutationsgruppen; Zum verallg Satz von Frobenius

(1) Ist $\mathfrak{G}$ tra und hat $\mathfrak{G}_1$ auf $\Omega - 1$ einen intra Normalteiler $\mathfrak{N}_1$, dessen Tragebiete von $\mathfrak{G}_1$ halbregulär permutiert werden, so ex. $\mathfrak{N} \lhd \mathfrak{G}$, $\mathfrak{N}$ tra, $\mathfrak{N} \cap \mathfrak{G}_1 = \mathfrak{N}_1$.

(2) z.B: es genügt, daß $\mathfrak{N}_1 \lhd \mathfrak{G}_1$, $\mathfrak{G}$ 2-tra, $\mathfrak{G}_1/\mathfrak{N}_1$ nilpotent, $\mathfrak{N}_1$ intra ist, die Nicheinfachheit von $\mathfrak{G}$ zu zeigen.

(3) 2-Tra der PGr vom Grad p, die nicht $\leq \mathcal{N}\mathfrak{P}$ sind, folgt leicht so:
Ind.: primäre Komplexe konjugiert; die größte 1-tra Gruppe unter ihnen ist daher $\lhd \langle \mathfrak{G}, H \rangle = \mathfrak{K}$, wo $\mathcal{N}\mathfrak{P} = \langle H \rangle$; $\mathfrak{K}$ 3-tra, da $> \mathcal{N}\mathfrak{P}$, also $\mathfrak{G}$ 2-tra.

6/7

Ordnung prim. Gruppen

Satz: $\mathfrak{G}$ pri, $Gr = n$, $p^2 \big| |\mathfrak{G}|$, $p^2 > n \Rightarrow \mathfrak{A}_n \leq \mathfrak{G}$.

Ind. Bew: Sei $\mathfrak{P}$ eine p- Sy Gr $\mathfrak{G}$, $\begin{cases} \phi\mathfrak{P} = \{\text{Fixpkte}\} \\ f = |\phi\mathfrak{P}| \end{cases}$

1. $\mathfrak{G}$ 2-tra
2. Min-Grad $\mathfrak{G} \geq \frac{n}{3} - \frac{2\sqrt{n}}{3}$ $\quad n = kp, \quad k > 1$

2a siehe 25 (S. 16)

A. $f = 0$ besser $\mathfrak{P}^*$ statt $\mathfrak{P}_1$, ist später dann zu übernehmen

3. $\mathcal{N}\mathfrak{P}_1$ ist 2-tra auf $\phi\mathfrak{P}_1$ denn $\mathfrak{P}_1$ ist p-Sy Gr $\mathfrak{G}_{12}$
4. $\mathcal{N}\mathfrak{P}_1 \leq \mathcal{N}\mathfrak{P}$
Ind: Sonst $\mathfrak{P}_1 \leq \langle \mathfrak{P}, \mathfrak{P}' \rangle > \mathfrak{P}, \exists H \in \langle \mathfrak{P}, \mathfrak{P}' \rangle$ mit $(\mathrm{Ord} H, p) = 1$, das lässt jedes $\mathfrak{S} \in T\mathfrak{P}_1$ fest, $TH \leq \phi\mathfrak{P}_1 = \phi^*$ wergen 3 erzeugt H unter $\mathcal{N}\mathfrak{P}_1$ eine tra Gruppe $\mathfrak{H}$ mit $T\mathfrak{H} = \phi\mathfrak{P}_1$.

a) Falls $\phi\mathfrak{P}_1 \geq \frac{n}{2}$, enth. $\mathfrak{G}$ ein P mit $q \leq \frac{p-1}{2}$ Zyklen, da $n \leq p(p-1)$; $p \geq 2q+1 \geq 2q-1$ also nach Manning $\left|\phi\mathfrak{P}_1\right| \leq 4q-4 \leqq 2p-6$, $n \leq 4p-12$

7/8

$n = kp, \quad k \leq 4 - \frac{12}{p} \quad k \leq 3 \to q = 1 \;\to\; k = 2 \;\to\; \mathfrak{G}\ (p+1)$-tra $\to \mathfrak{G} \leq \mathfrak{A}_n$. Also 4 bewiesen.

5. $\left|\phi\mathfrak{P}_1\right| = p$ Denn auf $\phi^* = \phi\mathfrak{P}_1$ ist $\mathfrak{P}$ halbreg und $\lhd$ 2 tra

6. $\mathcal{N}\mathfrak{P}_1$ scharf 2-tra auf ϕ, da $\rhd$ Zykl Gr Grd p

7. Kein $G \in \mathfrak{G}$ läßt 1,2 $(\in \phi\mathfrak{P}_1 = \phi)$ fest und führt ein $\gamma > 1,2 \quad \gamma \in \phi$, in ein $\delta \in \phi$, $\delta \neq \gamma$ über. Denn sonst gäbe es $(1)(2)(\gamma\delta-) \in \mathcal{N}\mathfrak{P}_1$

unnötig [8. Kein $G \in \mathfrak{G}_{12}$ führt $\gamma, \delta \in \phi$ in das gleiche Transgebiet von $\mathfrak{P}_1$ über. sonst $\exists : GP^\nu, G^{-1} = (1)(2)(\gamma\delta\ldots)$ trotz 7]

9. $\mathfrak{G}_{12} \ni G$, $G \neq 1$ auf ϕ

8/9

sonst sind $2,\ldots,p = \phi - \{1\}$ ein Impr Block Δ für $\mathfrak{G}_1$. Wähle $\mathfrak{P}_1^{G_1}$ sodaß dies 2 nichts fest lässt. $\mathfrak{P}_1^{G_1}$ vertauscht dann jede Ziffer in $\phi - \{1\}$. G_1 bringt also lauter rechte Ziffern δ_r $(> p)$ nach $\phi - 1$. Ein Zyklus c in $\mathfrak{P}_1$, der so eine Ziff. enthält, enth keine zweite, da sonst $\Delta \cap \{$ Träg $C\}^{G_1}$ ein Block für C^{G_1} da $\neq$ Träg $C_1^{G_1}$ ist. Also jeder Zykel von $\mathfrak{P}_1$ enthlt höchstens <u>eine</u> δ_r, daher $k-1 \geq$ Aut $\delta_r = p-1 \quad k \geq p$ W!

10. Das G von 9 macht $\mathfrak{P}_1^{G^{-1}} \leq \mathfrak{G}_{12}$ und $\phi\langle\mathfrak{P}_1, \mathfrak{P}_1^{G^{-1}}\rangle < \phi\mathfrak{P}_1 = \phi^*$

11. Sei $\mathfrak{Q}$ das Erzeugnis aller $\mathfrak{P}_1^H \leq \mathfrak{G}_2$; Dann ist $\mathcal{N}\mathfrak{Q}$ 2-tra auf $\phi\mathfrak{Q}$
daher $\quad \mathcal{N}\mathfrak{P}_1$ 2-tra auf $\phi\mathfrak{Q}$
Die Gruppe der Ord. $p(p-1)$ von $\mathcal{N}\mathfrak{P}_1$ auf ϕ hat also eine intra Ugr mit einem 2-tra- Konstituenten auf $\phi\mathfrak{Q}$. Da die intra Ugr alle zyklisch sind, ist $\left|\phi\mathfrak{Q}\right| = 2$, dh $\mathfrak{Q}$ hat keinen Fixpunkt $\neq 1,2$. Also liegt jedes $\lambda = 2,-,p$ in einem Tragebiet von $\mathfrak{Q}$, das die Lge $\geq p$ hat und daher auch rechte Ziffern $(> p)$ enthält.

9/10

12. Kein Tragebiet von $\mathfrak{Q}$ enthält 2 der Ziffern $\ldots 3,-,p\ldots$. Denn der zugehör. tra Konstituent ergäbe in $\mathcal{N}\mathfrak{P}_1$ eine UGr mit tra Konst $\neq 1$ auf $\{3-p\}, \leq \mathfrak{G}_{12}$, trotz 7.

13. Also enthält $\mathfrak{Q} \geq p-2$ Tra Gebiete mit Längen

$$\begin{array}{rcl} & \geq & p+1 \\ p^2-p-2 & \geq & n-2 \geq (p+1)(p-2) \\ \text{daher} & = & \quad = \end{array}$$

14. $\mathfrak{Q}$ enthält $p-2$ Tra Geb d Lge $p+1$. $n=(p-2)(p+1)+2=p^2-p$

15. $\mathfrak{G}_1$ ist pri

    Sonst hat ein Block $\Delta \ni 2$ die Länge $1+x(p+1) \Big| p^2-p-1$

    Die Zahl der konj Blöcke ist $\frac{p^2-p-1}{1+x(p+1)} = y$ ganz; $y < \frac{p^2-p}{p-1} = p \quad y \equiv 1 \quad (p+1)$, $y=1$

16. $\mathfrak{G}_1$ 2-tra, $\mathfrak{G}$ 3 tra; 14,15 & Manning 17.7 S. 42

17. $\mathcal{N}\mathfrak{P}_1$ 3-tra ϕ trotz 6 W!.

10/11

Also: Es ist (gilt)

B. $\underline{f>0}$

18. $\underline{\text{Vor: } f=1}$ Sei jetzt $\mathfrak{P}$ eine p-Sy, die 2 fest läßt. $\mathfrak{P}_1$ ist p-Sy $\mathfrak{G}_{12}$, also $\mathcal{N}\mathfrak{P}_1$ 2-tra $\phi = \phi\mathfrak{P}_1$. $\mathfrak{P}_1$ (besser $\mathfrak{P}^*$ statt $\mathfrak{P}_1$) liegt in zwei versch p-Sy Gr; $\mathfrak{P}$, $\mathfrak{P}^G \leq \mathfrak{G}_1$ also $\exists H \in \langle \mathfrak{P}, \mathfrak{P}^G \rangle$, $(\mathrm{Ord}H, p) = 1$. H lässt jedes $t \in T\mathfrak{P}_1$ fest, wegen 2-Tra von $\mathcal{N}\mathfrak{P}_1$ gibt es tra Gr $\mathfrak{H} \leq (H)^{\mathcal{N}\mathfrak{P}_1}$ auf ϕ. Es ist $\left|\phi\right| < \frac{n}{2}$ wie in 4a also $\mathfrak{G} \geq \mathfrak{A}_n$ Marggraf[f].

18a. $f \geq 1 \rightarrow$ die Gruppe $\mathfrak{H}$ der $H \in g$ mit $T\mathfrak{P}^* \subseteq \phi\mathfrak{H}$ ist $\neq 1$, aber intransitiv auf $T\mathfrak{H}$.
`22 hierher`

C. $\underline{f \geqq 2}$ Sei wieder $\mathfrak{P}^*$ eine Ugr vom Index p in $\mathfrak{P}$, die kleineren Träger hat.

19. Zu $\alpha \neq \beta \in \phi^* = \phi\mathfrak{P}^*$ gibts $K \in \mathfrak{G}$: α^K, $\beta^K \in \phi$, K zentralisiert jeden in $\mathfrak{P}^*$ auftret. Zyklus.
Bew: Wähle $G \in \mathfrak{G}$, $\alpha \rightarrow 1 \quad \beta = 2$, $C\phi = \{1, 2, \ldots\}^C \quad \exists\, G_{12} : \quad \mathfrak{P}^{*G\,G_{12}} \leq \mathfrak{P}$
Das System der Zyklen $C_1 \ldots C_m$, die in $\mathfrak{P}^*$ auftreten, wird also durch GG_{12} in ein ebenfalls von $\mathfrak{P}$ zentralisiertes Zyklensystem überführt. Also gibt es $N \in \mathcal{N}\mathfrak{P}$: $C_r^{GG_{12}N} = C_\mu$ Setze $GG_{12}N = K$:
$\alpha^K = 1^N \in \phi \quad \beta^N = 2^N \in \phi, \quad C_\mu^K = C_\mu$

11/12

D. $\underline{f=2}$

20. Dann $\mathcal{N}\mathfrak{P}^*$ 2-tra $\phi^* \quad \mathcal{N}\mathfrak{P}^*$ pri ϕ^* also wie B folgt Wid!

E. $\underline{f=3}$

21. a) $|T\mathfrak{H} \cap \phi| \geq 2$ Genauer: Es gibt 2 Ziffern in ϕ, die im gleichen Transgebiet $\mathfrak{H}$ liegen. dann H-$(\alpha\beta\ldots) \in \mathfrak{H}$

$$19: \ \exists \ \ K = \begin{pmatrix} \alpha & \beta & \ldots \\ \rho & \sigma & \ldots \end{pmatrix} \qquad \rho, \sigma \in \phi$$

$\mathfrak{H}^K = \mathfrak{H} \quad \exists\, H_1 \in \mathfrak{H},\ \ H_1 = (\rho\,\sigma \quad)$ Sei etwa $1, 2$ im selben Tragebiet von $\mathfrak{H}$

b) Es gibt in ϕ zwei Ziffern, die in versch Tragebieten des Trägers von $\mathfrak{H}$ liegen.
Bew: $\mathfrak{H}$ ist intra auf $T\mathfrak{H}$ nach 18a. Seien α, β in verschiedenen Tragebieten
$19'$. $\exists\, M \in \mathfrak{H}$, $\alpha^H \in \mathfrak{H}$, $\ \alpha^H, \beta^H \in \phi$.

b′) also 3 nicht im selben Tragebiet von $\mathfrak{H}$ wie $1, 2$.

12/13

c) $\mathfrak{H}$ hat keinen Fixpunkt in ϕ^*. Wäre α einer, β keiner, so $\alpha^M\beta^M \in \phi \quad \alpha^H$ Fixpunkt $\mathfrak{H}$ in ϕ trotz b, a.

d) $\mathfrak{K}$ tra ϕ^* Es genügt zu zeigen: Sind $\alpha\beta \in \phi^*$, so $\exists\ K : \alpha^K \in \{1, 2\}$ denn $\beta, 2$ sind im selben Tragebiet sogar von $\mathfrak{H}$. Wähle $\beta = \alpha^H \neq \alpha$ das geht: 2; Wähle $K : \alpha^K, \beta^K \in \phi$. Da im selben Transgebiet von $\mathfrak{H}$, ist $\alpha^K \in \{1, 2\}$

22 Nie ist bei $f > 1$ $\mathfrak{K}$ tra, dh $\mathcal{N}\mathfrak{R}^*$ tra ϕ^*
Bew: $\mathfrak{K}$ hat auf $T\phi^*$ die Ordnung p^α, und $|\phi^*| \not\equiv 0$ $(\mathfrak{p})$, denn wegen $f > 1$ ist $p \nmid n$. Also ist $\mathfrak{H}$, da $|\mathfrak{K} : \mathfrak{H}| = p^\alpha$, tra auf ϕ^* wenn $\mathfrak{K}$ es ist, trotz 18a

13/14

23 Die Untergruppen $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$ vom Index p in $\mathfrak{P}_j$, die kleineren Grad als $\mathfrak{P}$ haben, werden von $\mathcal{N}\mathfrak{P}$ <u>transitiv</u> permutiert. (Wird vielleicht nicht gebraucht, Beweis lang, bis S.16.)
Bew. Unten

24. Sind $\alpha, \beta \in \phi\mathfrak{P}_2$, so $\exists\ K \in \mathfrak{K}_\vee$ ($= \cap$ Zentr der Zyklen von $\mathfrak{P}_\nu$) mit $\alpha^K, \beta^K \in \phi$. Bew wie 19

24a. Ferner gibts $K \in \mathfrak{K}_2 : K = (\rho\sigma\ldots) \quad \rho, \sigma \in \phi$

Bew 23: Ist Δ die Gesamtheit der Zyklen, die in jedem $\mathfrak{P}_1^N$ ($N \in \mathfrak{N} = \mathcal{N}\mathfrak{P}$) auftreten, so ist $\Delta \neq \varnothing$, wenn $\mathfrak{N}$ intra auf $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_t\}$, und $\mathfrak{V} = \mathfrak{K}_1^{\mathfrak{N}}$ zentralisiert jeden Zyklus in Δ und ist tra (nach 24) auf $\Omega - \Delta$, da jedes $\alpha \in \Omega - \Delta$

14/15

nach ϕ gebracht werden kann und die Durchschnitte der Tragebiete von $\mathfrak{V}$ mit ϕ ein unter der 2-tra Gruppe $\mathfrak{N}/\phi$ invariante System mit Lgen > 1 nach 24a bilden, also nur aus einem Tra System bestehen. Aus der Transitivität von $\mathfrak{V}$ auf $\Omega - \Delta$ folgt, da $\mathfrak{V}$ auf Δ Ord p^α hat und $(|\Omega - \Delta|, p) = 1$: $\mathfrak{V}$ tra $\Omega - \Delta$. $\mathfrak{V}$ hat eine Ugr, die auf ϕ^Δ tra ist, nämlich was vom $\mathcal{N}\mathfrak{P} \cap \mathfrak{V}.\mathfrak{P}$ übrig bleibt wenn man die Konstit. auf Δ wegdividiert. $\mathfrak{V}\mathfrak{P}$ enthält ein p- Element, P das $\lambda, 1 \leq \lambda \leq \ell$ ($\ell =$ Anz der Zyklen von $\mathfrak{P}$ auf $\Omega - \Delta$) Ziffern aus ϕ heraus nach $\Omega - \Delta$ bringt, denn kein p-Zyklus in $\mathfrak{V}\mathfrak{P}$ kann ganz in ϕ liegen, wegen $\mathcal{N}\mathfrak{P}$. $\mathfrak{V}$ enthält dann ein p-freies a. Ebenso wie $\mathfrak{V}$ gibts ein $\mathfrak{W}$ zu einem anderen Tra System von $\mathfrak{P}$ auf $\{\mathfrak{P}_1 \ldots, \mathfrak{P}_t\}$ mit derselben Eigenschaft. Auch $\mathfrak{W}$ enthält auf ϕ eine tra Ugr $\mathfrak{W}'$.
$\mathfrak{W}_0\langle\mathfrak{P}\rangle = \mathfrak{W}'_0\langle\mathfrak{P}\rangle$, $f > 1$ vom Grad $f + \ell$ und transitiv. Denn

genauer 26

24. Die Kommutatorgr zweier tra Gruppen, deren Träger etwas gemein haben, aber sich nicht enthalten ist tra auf der Vereinigg der Träger.

15/16

Forts. Bew 23.
OBdA ist $\ell \leq \frac{k}{2}$, daher $\ell \leq \frac{n-f}{2p}$
Ferner ist nach Marggraf[f] Gr $\mathfrak{W}'_0\mathfrak{W}'^p$ $\frac{n}{2} \leq$ Gr $\leqq \ell + f$. Also $f + \ell > \frac{n}{2} \to f + p > \frac{n}{2} \to f + kp > \frac{n}{2}$ wenn $\mathfrak{P}_1 k_1 p$ zusätzliche Fixpunkte hat, dh Gr $\mathfrak{P}_1 < \frac{n}{2}$. Geht nicht.

(25) $\mathfrak{G}$ enthält kein p-Element mit Grad $\leq \frac{n}{2}$ nach Manning, denn das gibt $q \leq \frac{n}{2p} < \frac{p}{2}$. [unnötig; siehe 27]

16/17

Hilfssatz über Kommutatoren in P Gr-

(26) Sei $\mathfrak{T}$ eine transitive Gruppe auf ihrem Träger T, und Q eine Permut, die eine Ziffer von T fest läßt, aber nicht T als Ganzes. Dann ist die Gruppe $\langle (T_1 \circ Q)^{T_n} \rangle_{T_i \in \mathfrak{T}}$ tra auf ihrem Träger $T \cup T^Q$.
Bew: Ist ν eine neue Ziffer, dh $\nu = \tau^Q$, $\tau \in T$, $\nu \neq T$, und $\alpha^Q = \alpha$, $\alpha \in T$, so exist $G \in \mathfrak{T}$: $G = (\alpha\tau \ldots)$

$$\begin{aligned} G \circ Q &= G^{-1}Q^{-1}GQ \\ &= (\tau\alpha \ldots)(\alpha\nu \ldots) \\ &= (\tau\nu \ldots) \\ (G \circ Q)^{T_2} &= (\tau^{T_2}\nu \cdots) \end{aligned}$$

also v mit allen $\tau \in T$ verbunden, daher alle τ miteinander verbunden, alles verbunden.
Frage: Verallgem auf $\mathfrak{T}$ und mehreren tra Konstituenten: S. 23

Fortsetzung D: $f \geq 2$

27. $\mathfrak{Z} = Zs\,\mathfrak{P} \ni Q : (|Q|, p) = 1,\ Q = 1$ auf $\Omega - \phi^*$.
Bew: $\mathfrak{P}^* = \mathfrak{P}_\alpha, \quad \alpha \notin \phi$.
Die Gr $\mathfrak{K}$, die jeden Zykl von $\mathfrak{P}^*$ zentral, enthält zu $\alpha, \beta \in \phi^*$ stets ein K mit $\alpha^K, \beta^K \in \phi$ (19)
Mit einem solchen K transformiere das El. $b_1 \notin \mathfrak{P}^*,\ h \in \mathfrak{P}$. Dann erhält man ein $P \in \mathfrak{K}$, $P = (\rho\sigma \ldots) \ldots\ \rho, \sigma \in \phi$
Also gibts in $\mathfrak{K} \cap \mathcal{N}\mathfrak{P}$ ein $Q = (\rho\sigma \ldots) \ldots$ und da Q keinen p-Zyklus auf ϕ enthält (er würde zu Vergröß. von $\mathcal{N}\mathfrak{P}$ führen), gilt durch Potenz. mit p:
$\exists\, R \in \mathfrak{K}, \quad R = (\rho'\sigma' \ldots) \ldots \rho', \sigma' \in \phi$ (Ord$R, p) = 1$. Dieses R zentalisiert $\mathfrak{P}$, sonst gäbe es p- El des Grades $\phi^* - \phi$, also auch des Grades $< \frac{n}{2}$ (notfalls durch wegdividieren des Stücks in $\phi^* - \phi$). Aus $(|R|, p) = 1$, $R \in \mathfrak{K}$ folgt $R\big|_{\Omega - \phi^*} = 1$

28. $\mathfrak{Z}$ ist tra auf ϕ denn $\phi\mathfrak{Z} = \phi$, $\mathfrak{Z} \lhd \mathcal{N}\mathfrak{P}$, $\mathcal{N}\mathfrak{P}$ 2-tra ϕ.

29. $\mathfrak{Z} \ni S$: $S = 1$ auf $\Omega - \phi^*$, S versetzt eine vorgeschriebene Ziffer $\alpha \in \phi$
Bew: R^Z tut das, wo R nach 27, Z passend in $\mathfrak{Z}$ nach 28.

30. Die Gruppe $\mathfrak{H}$, die auf $\Omega - \phi^* = 1$ ist, enthält ein H, das $\geq 1, \leq l$ Ziffern aus $\phi^* - \phi$ nach ϕ bringt; dabei $l = \frac{\phi^* - \phi}{p}$.
Bew: Wähle $K \in \mathfrak{K} : \phi^K \neq \phi$, K führt möglichst wenig Ziffern (μ) aus $\phi^* - \phi$ nach ϕ. Wähle $P \in \mathfrak{P} - \mathfrak{P}^*$; p^K versetzt ≥ 1, höchstens μ Ziffern aus ϕ, kein Zykl P^K liegt ganz in ϕ, also führt P^K genau μ Ziffern aus $\phi^* - \phi$ nach ϕ. Also $\mu \leq l$;P^K kann durch ein Produkt von p-freien Elementen von $P^K \in \mathfrak{K}$, dh durch ein $H \in \mathfrak{H}$, in $\mathfrak{P}$ zurück transformiert werden. H führt also μ Ziff. von $\phi^* - \phi$ nach ϕ.

31. $\mathfrak{G} \ni M \neq 1$, Gr $M \leq 3l$
Nimm nach 30 in $\mathfrak{H}$ ein El H, das in $\Omega - \phi^* = 1$ ist und nach 30 $\leq l$ Ziff aus $\phi^* - \phi$ nach ϕ bringt, eine darunter etwa ϕ erreicht. Nimm zu einem anderen $\mathfrak{P}_2$ ($\neq \mathfrak{P}^*$) nach 29 ein $S \in \mathfrak{Z} = Z\mathfrak{P}$, das φ bewegt und auf $\Omega - \phi_2 = 1$ ist (insb. auf $\phi^* - \phi$). S hat mit M höchstens l Ziffern gemein: $M = S \circ H \neq 1$ hat Grad $\leq 3l$. Allgemein gilt:

32. In 2-tra $\mathfrak{G} \not\geq \mathfrak{A}_n$ des Grades n ist Min Grad $\geq \frac{n}{6}$
Bew:

1: $n \leq 24$ klar

2: $n \geq 25$: $m \geq \frac{n}{3} - \frac{2\sqrt{n}}{3} \geq \frac{n}{3} - \frac{2n}{3\cdot 5} = \frac{n}{5} \geqq \frac{n}{6}$.

32′: NB: Wahrscheinlich sogar $m \geq \frac{n}{5}$
ja: Min Grad 4 $\quad\rightarrow\quad n \leq 7$ (Séguier S. 58)

20/21

33. $n \geq 3l_p$ wenn l minimimal gewählt nach 30
denn es gibt mind. 3 gekoppelte Ziffernsysteme in $\mathfrak{P}$, sonst gibts P' Gr $< \frac{n}{2}$

34. Endwiderspruch:

(33) $3l_p \leq n \underset{\rightarrow 32}{\leq} 6 \underset{\rightarrow \text{min Gr.}}{m} \leq 18l$
$p \leq 6 \quad p \leq 5 \quad k \leq 4 \quad l \leq \frac{4}{3} \quad l = 1$
Nach 31 $\exists\, M \in \mathfrak{G}$, Gr $M \leq 3$: $\mathfrak{G} \geq \mathfrak{A}_n$

21/22

Pri. Perm-Gr: Konstit von $\mathfrak{G}_1$

$\mathfrak{G}$ sei prim.

(1) Hat eine p-Sy-Gr. $\mathfrak{P}_1$ von $\mathfrak{G}_1$ k Konstituenten $\neq I$, so hat $\mathfrak{G}_1$ höchstens k Konstituenten $\mathfrak{T}_\nu$ ",
Denn jedes $\mathfrak{T}_\nu$ enthält einen Konst von $\mathfrak{P}_1$ = Korollar zum Satz: $p\big||\mathfrak{G}_1| \rightarrow p\big||\mathfrak{T}_\nu|$.
= Sonderfall der allg Vermutung über Anzahl der Tra Konst $\mathfrak{G}_1$ und von $\mathfrak{H} \subset \mathfrak{G}_1 \ldots$

22/23

Transitivität von Kommutatorgruppen

(i) $\mathfrak{A}$ habe die tra Konst $\mathfrak{A}_i$
$\mathfrak{B}$ 〃 $\mathfrak{B}_k$.
Jedes $\mathfrak{A}_i$ bewege eine Ziffer, die bei $\mathfrak{B}$ fest
〃 $\mathfrak{B}_k$ 〃 $\mathfrak{A}$.
Dann hat $\mathfrak{A} \circ \mathfrak{B}$ dieselben Transitivitätsgebiete wie $\langle \mathfrak{A}', \mathfrak{B}' \rangle$, wo $\mathfrak{A}'$ aus $\mathfrak{A}$ durch Fortlassen derjenigen Konstituenten besteht, die nur Fixpunkte von $\mathfrak{B}$ enthalten; entspr. $\mathfrak{B}$.
Bew: Sei $\{a_1, \ldots, a_m\}$ = Trä $\mathfrak{A}_1$, $a_1 \in \phi\mathfrak{B}$. Sei a_m ein Nichtfixpkt von $\mathfrak{B}$, a_m trete in $\mathfrak{B}_1$ auf; $\mathfrak{B}_1$ enthält b_1 fix bei a. $\mathfrak{A}B \ni (a_1 b_1)$ $a \ni (a_1 a_m \ldots)$; $\mathfrak{B} \ni (a_m b_1 \cdots)$. $\mathfrak{K} = \mathfrak{A} \circ \mathfrak{B}$ enthält $(b_1 a_m \cdots)$ $\mathfrak{A} \ni (a_m a_\mu \ldots)\mathfrak{K} \ni (b_1 a_\mu \ldots)$; $\mathfrak{K} \ni (b_1 a_\lambda \ldots) \quad \mathfrak{K} \ni (a_\lambda a_\mu)$
$\mathfrak{K}$ verbindet alle Ziffern im Träger $\mathfrak{A}_1$ miteinander, ebenso im Trä $\mathfrak{A}_i$, Trä $\mathfrak{B}_K$.

23/24

(1) Subnormale Ugr von pri Gruppen versetzen alle oder keine Ziffer.
Bew für einfaches $\mathfrak{A}$: $\mathfrak{A}' \neq 1 \to \mathfrak{A}^{\mathfrak{G}}$ tra $\quad \mathfrak{A}' = 1 \to \mathfrak{A}^{\mathfrak{G}} = \mathfrak{P}$, Ztr $\mathfrak{P}$ tra, $\mathcal{N}\mathfrak{A}$ tra
Unauflösbare intransitive Ugr von Perm Gr.

(2) $\mathfrak{H}$ unauflösbarer, $\mathfrak{H}_0$ perfekter Kern, $\mathfrak{H} \leq \mathfrak{G}_1$, $\mathfrak{H}$ hat $\leq k$ Transgebiete und ist mit diesen Eigensch maximal in $\mathfrak{G} \to$ Gr $\mathfrak{H} > \frac{n}{2}(n =$ Gr $\mathfrak{G})$
Bew: $\mathfrak{H}_0 \lhd\!\lhd \mathfrak{G}$ (1) also $\mathfrak{H}_0$ nicht vtb mit pass. $\mathfrak{H}_0^G$. Wähle das so, daß Gr $\mathfrak{K} =$ min; hätte $\mathfrak{K}\langle\mathfrak{H}, \mathfrak{H}^G\rangle$ mehr Tragebiete als $\mathfrak{H}$, so wäre $\mathfrak{H}_0$ mit jedem $\mathfrak{H}_0^K$ vtb, $\mathfrak{H}_0 \lhd\!\lhd \mathfrak{K}$, denn $\mathfrak{H}_0^G \lhd\!\lhd \mathfrak{K}$, also wegen Perfektheit $\mathfrak{H}_0 \,\mathrm{v}\, \mathfrak{H}_0^G$; Also $\mathfrak{K}$ hat $\leq k$ Tragebiete: also hat $\mathfrak{K}$ keinen Fixpkt, Gr $\mathfrak{H} > \frac{n}{2}$

24/25

(3) Sei $n \neq p^\alpha$, $\mathfrak{H}$ max mit $\phi\mathfrak{H} \neq \emptyset$, $\mathfrak{H}$ hat $\leq k$ Tragebiete, $\mathfrak{H}$ nicht nilpotent. Dann Gr $\mathfrak{H} \geq \frac{n}{2}$
Bew: $\mathfrak{H}$ ist auflösbar (2) $\mathfrak{K} = \mathfrak{H}^\nu$ $\mathfrak{K}$ ist nicht $\lhd\!\lhd \mathfrak{G}$ Wegen $n \neq p^\alpha$ (1) $\mathfrak{K}\psi\mathfrak{K}' = \mathfrak{K}^X$. $\mathfrak{H}$ nicht $\vee \mathfrak{H}' = \mathfrak{H}^x$
Wähle $\mathfrak{H}'$ so daß $\mathfrak{K}\psi\mathfrak{K}'$, Gr $\langle\mathfrak{H}, \mathfrak{H}'\rangle$ min
hätte $\mathfrak{H}$ neues Tra-Gebiet (fremd zu Trä $\mathfrak{H}$), so $\mathfrak{K}$ vtb mit allen $\mathfrak{K}\langle\mathfrak{H}, \mathfrak{H}'\rangle$
$\mathfrak{K} \lhd\!\lhd \langle\mathfrak{H}\mathfrak{H}'\rangle$

(Das ist der Satz (Deskins-Adney), der subnormale Kern einer max Ugr ist normal.)

25/26

Krit. für $\mathfrak{A} \lhd\!\lhd \mathfrak{G}$

(1) Sei $\mathfrak{A} \leq \mathfrak{B} \leq \mathfrak{G}$, $\forall X, Y \in \mathfrak{G}$ $\mathfrak{A}^X \,\mathrm{v}\, \mathfrak{B}^Y$ Dann ist $\mathfrak{A}^{\cdot\cdot\mathfrak{B}} = \mathfrak{A}^{\cdot\cdot\mathfrak{G}}$.

I. $\mathfrak{B} = \mathfrak{G}$ trivial

II $\mathfrak{B} < \mathfrak{G}$. Nach Kegel ist $\mathfrak{A}^{\mathfrak{G}} < \mathfrak{G}$ oder $\mathfrak{B}^{\mathfrak{G}} < \mathfrak{G}$, also $\mathfrak{A}^g = \mathfrak{G}' \lhd \mathfrak{G}$
$\mathfrak{B}' := \mathfrak{B} \cap \mathfrak{G}'$ $\quad \mathfrak{A}' \leq \mathfrak{B}' \leq \mathfrak{G}'$ $\quad \mathfrak{A}'^X \,\mathrm{v}\, \mathfrak{B}'^Y$ $\boxed{\to \text{ S.3}}$
$\mathfrak{A}' \leq \mathfrak{B}' \trianglelefteq \mathfrak{B}$, $\mathfrak{A}^{\cdot\cdot\mathfrak{G}} = \mathfrak{A}^{\cdot\cdot\mathfrak{G}'} \underset{\text{Ind.}}{=} \mathfrak{A}^{\cdot\cdot\mathfrak{B}'} = \mathfrak{A}^{\cdot\cdot\mathfrak{B}}$

Folge :

Satz (2) $\mathfrak{A} \lhd\!\lhd \mathfrak{B} \leq \mathfrak{G}$, $\quad \mathfrak{A}^X \,\mathrm{v}\, \mathfrak{B}^Y \Rightarrow \mathfrak{A} \lhd\!\lhd \mathfrak{G}$

(3) $\mathfrak{A} \,\mathrm{v}\, \mathfrak{B}$, $\mathfrak{B} \leq \mathfrak{G}' \to \mathfrak{A}' \,\mathrm{v}\, \mathfrak{B}$, wo $\mathfrak{A}' = \mathfrak{A} \cap \mathfrak{G}'$.

(4) $\mathfrak{A} \leq \mathfrak{B} \leq \mathfrak{G}$ $\underset{X}{\forall}$ $\mathfrak{A}^X \,\mathrm{v}\, \mathfrak{B} \to \underset{X}{\forall}$ $\mathfrak{A}^X \,\mathrm{v}\, \mathfrak{A}^{\cdot\cdot\mathfrak{B}}$ & ist $\mathfrak{A} \lhd\!\lhd \mathfrak{B}$, so $\mathfrak{A}^X \,\mathrm{v}\, \mathfrak{A}$.
Beweis 1

26/27

Fragen: $\mathfrak{A} \lhd\lhd \mathfrak{G}$ Vor $\mathfrak{A} \leq \mathfrak{G}$

(1) Wenn für alle $X \in \mathfrak{G}$ $\mathfrak{A} \lhd\lhd \langle \mathfrak{A}, \mathfrak{A}^X \rangle$ ist, ist dann $\mathfrak{A} \lhd\lhd \mathfrak{G}$?

(2) Es genügt, das für $|\mathfrak{A}| = p$ zu beweisen. Denn wenn $\mathfrak{A}$ einf, zusammengesetzte Ordng, so $\mathfrak{A} \,\mathrm{v}\, \mathfrak{A}^X \to \mathfrak{A} \lhd\lhd \mathfrak{G}$.
Und wenn $\mathfrak{A}$ zusammengesetzt, $\mathfrak{B} \lhd \mathfrak{A}$, min, so (Indukt) $\mathfrak{B} \lhd\lhd \mathfrak{G}$, $\mathfrak{B}^{\mathfrak{G}} = \mathfrak{N} \lhd \mathfrak{G}$. Ist $\mathfrak{B}$ nichtabelsch, so $\mathfrak{B} \lhd \mathfrak{N}$, und da jedes $\mathfrak{A}^X$ ein $\mathfrak{A}^N$ ist, ist das Erzeugnis $\mathfrak{F}$ aller zu $\mathfrak{B}$ isom. Füße von $\mathfrak{A}$ normal unter $\mathfrak{G}$ (Indukt: $\mathfrak{G}/\mathfrak{F}$) da oBdA $\mathfrak{G} = \mathfrak{A}\mathfrak{F}$. Ist $\mathfrak{B}$ abelsch, wieder $\mathfrak{G} = \mathfrak{A}\mathfrak{F}$ angenommen, so sei $\mathfrak{M}$ ein min $\mathcal{N}T$ von $\mathfrak{G}$ in $\mathfrak{F}$
$\mathfrak{M}' = 1$ oBdA $\mathfrak{A}\mathfrak{M} = \mathfrak{G}$. $\mathfrak{K} = \langle \mathfrak{A}, \mathfrak{A}^X \rangle > \mathfrak{A}$, also $\mathfrak{K} \cap \mathfrak{M} = \mathfrak{B} > 1$ $\mathfrak{B} \lhd \mathfrak{K}$, jedes $\mathfrak{K}^Y = \mathfrak{N}^M$, $\mathfrak{B} \leq \langle \mathfrak{A}^Y, \mathfrak{A}^{XY} \rangle = \mathfrak{G}$ X, Y OBdA also $\mathfrak{B} = \mathfrak{M}$, d.h. $\langle \mathfrak{A}, \mathfrak{A}^X \rangle \geq \langle \mathfrak{A}, \mathfrak{M} \rangle = \mathfrak{G}$. Nach Vor. $\mathfrak{A} \lhd\lhd (\mathfrak{A}\mathfrak{A}^X) = \mathfrak{G}$.

Also bleibt die Frage

(3) Erzeugt eine Klasse konj. El. schon dann eine p-Gruppe, wenn je zwei ihrer El. das tun?

27/28

[Die Seiten 28 und 29 sind rot durchgestrichen.]

Untergruppen mit wenig Tra-Gebieten

(1) $\mathfrak{A}^{\cdot\cdot\mathfrak{G}}$ hat höchstens so viele nichttriviale Transitivitätsgebiete wie $\mathfrak{A}$. Die nilpotenten Konstituenten von $\mathfrak{A}^{\cdot\cdot\mathfrak{G}}$ sind schon solche von $\mathfrak{A}$.
Bew: $\mathfrak{A}^{\cdot\cdot\mathfrak{G}} = \mathfrak{B}$ $\mathfrak{B} = \mathfrak{A}^{\mathfrak{B}}$ also hat $\mathfrak{B}$ kein Tragebiet in dem $\mathfrak{A} = 1$ und jedes Tragebiet von $\mathfrak{A}$ ist in einem von $\mathfrak{B}$ enthalten. Ist $\mathfrak{B}^\Gamma$ nilpot, or $(\mathfrak{A}^\Gamma)^{\mathfrak{B}^\Gamma} = \mathfrak{B}^\Gamma$, also $\mathfrak{A}^\Gamma = \mathfrak{B}^\Gamma$.
***???**die nilp Konst von $\mathfrak{A}$ werden nur weniger*

Satz (2) Sei $\mathfrak{G}$ pri; Gr= n; $\mathfrak{H} < \mathfrak{G}$; $\mathfrak{H}$ maximal so, daß $\mathfrak{H} \leq k$ Tragebiete hat und eine Ziffer fest läßt. Dann Grad $\mathfrak{H} > \frac{n}{2}$, oder $\mathfrak{H}$ ist p-Gr., $\mathfrak{H} \lhd\lhd \mathfrak{G}_\alpha$ für jedes $\mathfrak{G}_\alpha \geq \mathfrak{H}$.

A. Bew: Sei Gr $\mathfrak{H} \leq \frac{n}{2}$

(a) $\underline{\mathfrak{H} \trianglelefteq\trianglelefteq \langle \mathfrak{H}, \mathfrak{H}^G \rangle = \mathfrak{K}}$ (Bew: $\mathfrak{K} \leq \mathfrak{G}_\alpha$
$\underline{\text{Nach (i) ist } \mathfrak{H} \lhd\lhd \mathfrak{G}_\alpha;}$ $\mathfrak{H} \lhd\lhd \mathfrak{K}$, ebenso $\mathfrak{H}^X \lhd\lhd \mathfrak{K}$

(b) für jedes $G \in \mathfrak{G}$ und $\mathfrak{A} \lhd\lhd \mathfrak{H}$ ist $\mathfrak{A} \lhd\lhd \langle \mathfrak{A}, \mathfrak{a}^X \rangle$, denn $\mathfrak{A} \lhd\lhd \mathfrak{H} \lhd\lhd \langle \mathfrak{H}, \mathfrak{H}^X \rangle$.

28/29

(c) $\mathfrak{H}$ auflösbar! Bew 24(1) Sonst perfekter Kern $\mathfrak{A}$ mit allen $\mathfrak{A}^X$ vtb, also $\mathfrak{A} \lhd\lhd \mathfrak{G}$ trotz

(d) $\mathfrak{H}$ nilpotent.
Sonst $\mathfrak{A} = \mathfrak{H}^\nu$ mit allen Konj vtb., $\mathfrak{A} \lhd\lhd \mathfrak{G}$. Min subnormale Ugr $\mathfrak{M}$ von $\mathfrak{A}$ erzeugt p-Normalteiler $\mathfrak{P}$ von $\mathfrak{G}$, $\mathfrak{P}_1 \neq E$. $\mathfrak{Z} =$ Ztr $\mathfrak{P} \neq$ tra, da " $\to$ Wid zu $\mathfrak{G}$ pri

(e) $\mathfrak{H}$ *ist eine* p*-Gruppe*
Sonst $\sigma\mathfrak{P}$, $\mathfrak{A}$ *eine*
$\frac{n}{2}$*-Sy Gr* $\mathfrak{H}$. $\mathfrak{P}^Y$ *zentralisiert* q^X, *da* $\mathfrak{P}^Y \lhd \mathfrak{H}^Y \lhd\lhd \langle \mathfrak{H}^Y \mathfrak{H}^X \rangle$, *desgl* $\mathfrak{Q}^X \lhd\lhd \cdots$
$\mathfrak{P}^{\mathfrak{Q}}$ *zentral* $\mathfrak{Q}^{\mathfrak{G}}$ $\mathfrak{P}^{\mathfrak{G}}$ *tra,* $\mathfrak{Q}$ *hat Fixpkt* $\mathfrak{Q} = 1$.

B. *Sei jetzt* $\mathfrak{H}$ *nicht auflösbar (also Gr* $\mathfrak{H} > \frac{n}{2}$*)*

Forts: (f) *Versetzt* $\mathfrak{H}$ *eine Ziffer in Transgebiet* Γ *von* $g_{\mathfrak{G}}$, *so auch im gepaarten* Γ'. *Sonst* $\exists\, G = (\ldots \gamma, \gamma' \ldots) \ldots \in \mathfrak{G}$, *sodaß* $\mathfrak{H}^G$ *wie* $\mathfrak{H}\,\gamma'$ *fest lässt, also* $\mathfrak{H}$ *subnormal unter* $\mathfrak{H}^G$ *ist, aber* $1 \in$ *Tr* $\mathfrak{H}^G$.
$\mathcal{N}\mathfrak{H} = \mathfrak{G}_1 \geq \mathfrak{H}^G$. *W!*
Daher $\mathfrak{H} =$ *Norm Gr. in* $\mathfrak{G}_1$ *und* $\mathfrak{H}$ *eine größte perfekte subnormale einköpf. Ugr. von* $\mathfrak{H}$.

29/30

Zerschneidungs - Verfahren: Maximale 1-tra. Gr.

Vor. $\mathfrak{G}$ maximale nicht 2 tra Gr.

(1) Sei stets $\mathfrak{A}\,\dot{|}\,\mathfrak{B} \leq \mathfrak{G}$; $\{12\}^G = \{\xi\eta\}$, $\xi \in T\mathfrak{A}$, $\eta \in T\mathfrak{B} \Rightarrow \mathfrak{A}_\xi$ tra $\eta^{\mathfrak{B}}$. Dann ist $\mathfrak{A} \leq \mathfrak{G}$.
NB: Vielleicht allgemeiner zu formulieren:
$\mathfrak{G}$ beliebig, Vor..$\Rightarrow$ $\mathfrak{A} \leq \mathfrak{G}^V = V$-Abschl. $\mathfrak{G}$; $V = \{\{12\}^G\}_{\mathfrak{G}}$

(2) Sonderfall:
$\mathfrak{G}$ beliebig, $\mathfrak{A}|\mathfrak{B} \leq \mathfrak{G}$, aus $\alpha^G \in T\mathfrak{A}$ folgt $\beta^g \notin T\mathfrak{B}$, und aus $\beta^G \in T\mathfrak{A}$ folgt $\alpha^G \notin T\mathfrak{B}$. (dh $(\alpha\beta)$ werden von T in $T\mathfrak{B}$ nicht in $\mathfrak{G}$ getrennt). Dann ist $\mathfrak{A} \leq \mathfrak{G}^V \quad V = \{\alpha\beta\}^g$

(3) Folge: Sei $\mathfrak{A}|\mathfrak{B} \leq \mathfrak{G}$, $\alpha, \beta \in \Omega$, $\mathfrak{A} \not\leq \mathfrak{G}$. Dann $\exists\, G \in g : \alpha^G \in T\mathfrak{A}$, $\beta^G \in T\mathfrak{B}$ oder umgekehrt.

Beispiel:

(4) Das liefert verschmelzende Elemente für gegebene Konstituenten von Ugr von $\mathfrak{G}$.

30/31

Subnormale Ugren von pri Gr.

(1) Seien $\mathfrak{A}_1 \ldots \mathfrak{A}_R \lhd\lhd \mathfrak{G}$, jedes $\mathfrak{A}_i$ habe einen Fixpkt. Dann ist das Erzeugnis $\langle \mathfrak{A}_1 \ldots \mathfrak{A}_R \rangle$ intra denn im obersten pri Bestdteil sind alle $\mathfrak{A}_i = 1$.

(2) In einer transitiven Gruppe $\mathfrak{G}$ ist jede perfekte subnormale Ugr., die nicht im Rumpf liegt, fixpunktfrei.
Denn sie enthält eine einköpfige die nicht im Rumpf liegt, u. perfekt ist, und die ist $\lhd\, \mathfrak{G}$.

(3) Wenn eine perfekte tra Gr $\mathfrak{G}$ von subnormalen Ugr $\mathfrak{A}_i$ erzeugt wird, so erzeugen schon die fixpunktfreien $\mathfrak{A}|$ ganz $\mathfrak{G}$. (2)

31/32

(4) Wenn ein Homomorphismus φ eine wesentliche (nicht im Rumpf von $\mathfrak{G}$ erzeugte) einköpfige perfekte subnormale Ugr $\mathfrak{A}$ in den Rumpf von $\varphi(\mathfrak{G})$ abbildet, so ist $\varphi(\mathfrak{A}) = 1$.
denn sei $\mathfrak{K} = \text{Kern } \varphi$
$\mathfrak{A}_1$,-$\mathfrak{A}_k$ seien alle wesentl. mln. Ugr von $\mathfrak{G}$, die nicht in $\varphi\mathfrak{G}$ abgebildet werden. Dann $\mathfrak{A} \leq \mathfrak{K}$. $\langle \mathfrak{A}_1, , \mathfrak{A}_k \rangle = \mathfrak{G}$ also $\mathfrak{A} \leq \mathfrak{K}$.

(5) Wenn ein Erzeugnis $\mathfrak{G}$ perfekter $\mathfrak{A}_i \lhd\lhd \mathfrak{G}$ einen Fuß $= \mathfrak{F}$ hat, aber kein $\mathfrak{A}_i$ hat Fuß $= \mathfrak{F}$ so ist $|\mathfrak{F}| = p$ und der größte p-Normalteiler von $\mathfrak{G}$ liegt im Zentrum $Z(\mathfrak{G})$
Frage: Kann das vorkommen?

32/33

Subnormal-P einer Struktur

(1) Sei K eine Menge „abstrakter“ transitiver Permutationsgruppen, die mit $\mathfrak{K}$ auch jeden transitiven Konst. jedes Normalteilers von $\mathfrak{K}$ enthält.
Ist $\mathfrak{H}$ eine Permutgr, so „erlaubt“ K den Abstieg von $\mathfrak{H}$ zu $\mathfrak{H}^* < \mathfrak{H}$, wenn
a) $\mathfrak{H}^* \lhd \mathfrak{H}$ b) Es gibt einen trans. Konstituenten $\mathfrak{T}$ von $\mathfrak{H}$ und eine Ähnlichkeit $\sigma\mathfrak{T} = \mathfrak{K}$ „$= \sigma\mathfrak{H}$“ auf ein $\mathfrak{K} \in K$ und einen Normalteiler $\mathfrak{K}^* \lhd \mathfrak{K}$ derart, daß $\mathfrak{H}^* = \sigma^{-1}\mathfrak{K}^*$ in $\mathfrak{H}$.

(2) Kann man $\mathfrak{H}^{**}$ durch wiederholte Erlaubnis mit K erreicht, so $\mathfrak{H}^{**} \lhd\lhd \mathfrak{H}$

(3) Kann man sowohl $\mathfrak{H}_1^*$ wie $\mathfrak{H}_2^*$ jeweils durch einmalige Erlaubnis von K erreichen, so kann man $\vartheta = \mathfrak{H}_1^* \cap \mathfrak{H}_2^*$ sowohl von $\mathfrak{H}_1^*$ wie von $\mathfrak{H}_2^*$ aus durch (mehrmalige) Erlaubnis erreichen.
zum Beweis

(4) Hilfss.: Vor. 3 $\rightarrow$ man kann $\mathfrak{H}_1^*$ von $\mathfrak{N}$ aus erreichen, wenn $\mathfrak{H}_1^* \lhd \mathfrak{N} \lhd \mathfrak{H}$

33/34

Bew $\mathfrak{N} = \sigma^{-1}\mathfrak{L}$ $\quad \mathfrak{L} \lhd \mathfrak{K}$

α) Ist $\mathfrak{L}$ tra, so $\mathfrak{L} \in K$ $\quad \mathfrak{H}_1^*$ ist der größte $\mathcal{N}T$ von $\mathfrak{N}$, der durch σ auf $\mathfrak{K}^*$ abgebildet ist.

β) $\mathfrak{L}$ intra; $\mathfrak{L} = \mathfrak{L}_1\mathfrak{L}_2 \cdots \mathfrak{L}_m$, $\mathfrak{L}_\mu \in K$
σ_i = Einschr. σ $\mathfrak{N} = \mathfrak{N}_1\mathfrak{N}_2 \cdots \mathfrak{N}_m$ auf $\mathfrak{N}_i$
Ausführen! Lohnt.

Vermutungen:

(5) Sind $\mathfrak{H}_1, \mathfrak{H}_2 \lhd\lhd \mathfrak{H}$, so $\langle \mathfrak{H}_1^\wedge, \mathfrak{H}_2^\wedge \rangle = \langle \mathfrak{H}_1 \mathfrak{H}_2 \rangle^\wedge$
Es gilt sicher (XI 102)

(6) $\mathfrak{G}$ pri $\Rightarrow$ jeder tra Konst einer subnorm Ugr von $\mathfrak{G}_1$ ist ähnlich einem von $\mathfrak{K}$ oder $\mathfrak{K}_\alpha$ oder $\mathfrak{L}_\beta$, wenn $\mathfrak{K}, \mathfrak{L}$ gepaarte Konst. von $\mathfrak{G}$ sind.

34/35

Ugr. mit wenig Tragebieten.

Satz (1) Sei $\mathfrak{G}$ pri, $\mathfrak{H} \leq \mathfrak{G}_1$, $\mathfrak{H}$ nicht auflösbar, $\mathfrak{H}$ habe k nichttriv. Transgebiete. Dann hat $\mathfrak{G}_1$ höchstens k nichttr. Trgeb. Wähle $|\mathfrak{H}|$ maximal. Annahme: $\mathfrak{H} \neq \mathfrak{G}_1$. [bewiesen in [85] 7.5]

(a) $\mathfrak{H} \lhd\lhd \mathfrak{G}_\sigma$, wenn $\mathfrak{H} \leq \mathfrak{G}_\sigma$. Denn $\mathfrak{H}^{\cdot\cdot\mathfrak{G}_\sigma}$ hat $\leq k$ Transgebiete

(b) $\mathfrak{H}$ trifft nicht alle Transgebiete von $\mathfrak{G}_1$. Sonst Anz. n $\mathfrak{G}_1 \leq k$, aber $\mathfrak{H} = \mathfrak{G}_1$

(c) Sei $\mathfrak{M}$ ein Erzeugnis von in $\mathfrak{G}_1$ gelegenen konjugierten $\mathfrak{H}^G$, das nicht alle Tragebiete $\mathfrak{G}_2$ trifft, und $|\mathfrak{M}|$ max. Dann $\mathfrak{M} \lhd \mathfrak{G}_1$; $\mathfrak{G}_1 = \mathcal{N}\mathfrak{M}$.

(d) Sei $\mathfrak{A}$ eine einköpfige perfekte subnormale Ugr maximaler Ordnung von $\mathfrak{M}$ ($\mathfrak{M}$ ist nicht aufl.), und $\mathfrak{B} = \mathfrak{A}^{\mathfrak{G}_1}$. Dann $\mathfrak{G}_1 = \mathcal{N}\mathfrak{B}$.

(e) Trifft eine in $\mathfrak{G}_1$ gelegene konjugierte $\underline{\underline{\mathfrak{M}}} = \mathfrak{M}^H \quad \Gamma$ (also TraGeb $\mathfrak{G}_1$), so deckt $\underline{\underline{\mathfrak{M}}}$ das gepaarte P', hat dort keinen Fixpunkt. Sonst $\exists\ G = (\gamma_1\, \gamma' \cdots) \cdots$; $\mathfrak{M}^G$ läßt γ' fest, wie $\mathfrak{M}$, also $(\mathfrak{M}, \underline{\underline{\mathfrak{M}}}^G) \lhd\lhd \mathfrak{G}_{\gamma'}$.

35/36

Also $\mathfrak{M}^G \leq \mathcal{N}\mathfrak{B}$, $\underline{\underline{\mathfrak{M}}}^G \leq \mathfrak{G}_1$ aber $\mathfrak{M}$ trifft P, und $\mathfrak{M} \lhd \mathfrak{G}_1$, also versetzt von $\mathfrak{M}^\gamma$, und $\mathfrak{M}^G$ versetzt 1.

(f) Wähle γ, γ' zwei beliebige Fixpunkte vom $\mathfrak{M}$ in gespiegelten, von $\mathfrak{M}$ unberührten Trageb von $\mathfrak{G}$. (Exist. nach e)
$G = (\gamma \cap \gamma'\ )\ \mathfrak{M}^G$ lässt 1 und γ' fest, deshab Γ' also nicht, meidet (nach e) Γ, $\mathfrak{M}^G = \mathfrak{N}$ wegen Maximaleigensch. $\mathfrak{M}$
$G \leq \mathcal{N}\mathfrak{M} = \mathfrak{G}$. W!
Der Beweis zeigt sogar:

Satz (2) $\mathfrak{G}$ pri, $\mathfrak{H}$ perfekt, $\mathfrak{H} \leq \mathfrak{G}_1 \Rightarrow \exists \mathfrak{G}_\sigma \geq \mathfrak{H}$, so daß jedes Tra Gebiet von $\mathfrak{G}_\sigma$ eins von $\mathfrak{H}$ enthält; noch genauer: Bildet man von $\mathfrak{H}$ ausgehend die Subnormalen Hüllen in $\mathfrak{G}_\alpha, \mathfrak{G}_\beta, ..$ wobei $\alpha, \beta, ..$ jeweils ein Fixpunkt der schon erreichten Gruppe ist, so kommt man schliesslich zu einer Gr vom Grad $n-1$; die von 2 den enthaltenden $\mathfrak{G}_\sigma$ jedes Tra Gebiet trifft.

36/37

Andere Fassung:
(2′) In einer abstrakten Gr $\mathfrak{G}$ sei $\mathfrak{M}$ eine maximale Ugr, $\mathfrak{H} \leq \mathfrak{M}$, $\mathfrak{H}$ nicht auflösbar, und $\mathfrak{H} \lhd\lhd \mathfrak{M}^G$ immer wenn $\mathfrak{H} \leq \mathfrak{M}^G$. Dann gibts nur ein solches $\mathfrak{M}^G$.
Fortsetzg von (1f): Nun sei $\mathfrak{H}$ auflösbar
Bezeichnungen sonst wie in (1). Genügt: $\mathfrak{M} = \mathfrak{H}^{\mathfrak{G}_1}$.

(g) Sei $\underline{\mathfrak{M}}$ eine Konjug zu $\mathfrak{M}$, die 1 verschnt (1 im Konstit. $\mathfrak{T} \neq 1$) und ein $\delta \in \phi\mathfrak{M}$ fest lässt. Sei ω ein Subnormaloperator, der eine passende Ugr. $\underline{\mathfrak{U}} \unlhd\unlhd \underline{\mathfrak{M}}$, die auf $\mathfrak{T} \neq 1$ ist, annuliert $\underline{\mathfrak{U}}^\omega = 1$.
Dann ist $\mathfrak{M}^\omega = 1$. Sonst ist $\underline{\mathfrak{U}} \leq \mathcal{N}\langle \mathfrak{M}, \mathfrak{U}\rangle^\omega = \mathcal{N}\mathfrak{M}^\omega = \mathfrak{G}_1$

[besser gleich allgemeineren Satz?]

(h) Vor (g): $\underline{\mathfrak{T}}$ ist p- Gruppe.
Sei $\mathfrak{U}$ eine subn. Ugr kleinster Höhe in $\underline{\mathfrak{M}}$, die auf $\mathfrak{T} \neq 1$ ist; Höhe = min l: $\mathfrak{U}^{p, p_i \cdot\cdot p_l} = 1$. Gäbe es in $\mathfrak{T}$ eine q-köpfige subn Ugr $\mathfrak{V}$, $q \neq p_i$, so $\mathfrak{V}^{p_i \cdots p_r} = \mathfrak{V}^{p_i \cdot\cdot p_r} \neq 1$ trotz (g).

37/38

(i) Wenn $\mathfrak{M}$ in $\Gamma \neq 1$ ist und in Γ' einen Fixpunkt hat, so ist der Konstituent $\mathfrak{M}^\Gamma$ p-Gr.
[besser (l)]

(j) Das nach (e) <u>maximal</u> gewählte $\mathfrak{M}$ deckt jedes selbstgepaarte $\Gamma = \Gamma'$, sonst $G = (\gamma 1)..\in \mathfrak{G}$; $\mathfrak{M}^G = \mathfrak{M}$.
$\mathcal{N}\mathfrak{M} \geq \langle \mathfrak{G}_1, G\rangle$

(j′) Das max $\mathfrak{M}$ kann nicht Γ und Γ' meiden.

[(j) und (j′) sind umklammert mit der Anmerkung:]

= zusätzliche Vor.!

(k) Trifft ein Erzeugnis $\langle \mathfrak{H}^X \rangle \leq \mathfrak{G}_1$ ein Γ, aber nicht Γ', so ist es auf Γ eine p-Grp. ($\mathfrak{M} = \mathfrak{H}^{\mathfrak{G}_1}$) (i)

(l) Sei $\mathfrak{V}$, das Erzeugnis <u>aller</u> zu $\mathfrak{H}$ in $\mathfrak{G}$ konj. die in $\mathfrak{G}_1$ liegen. $\mathfrak{M}^{\mathfrak{q}_1} = \mathfrak{M}$ treffe Γ' nicht, dann ist sogar $\mathfrak{V}^\Gamma$ p-Gp.
Bew: auf $\mathfrak{V}^G$ wie geh. und p ist eindeutig bestimmt: $p = p_1$ wieder $p_1 - p_r$ miteinander gepaart, so $\mathfrak{H}$ (oder $\mathfrak{M}$ oder $\mathfrak{V}$) annulliert alle längsten einköpf Subnt. von $\mathfrak{H}$ haben Kopf $p = p_1$

38/39

(m) Hat $\mathfrak{M}$ q- Füße, $\mathfrak{F}$ so auch jede einköpfige subn. Ugr $\mathfrak{U}$ größter Länge. (Sonst zentralisieren sie sich, also $\mathfrak{U} \leq \mathcal{N}\mathfrak{F}$.)

(n) Hat der größte q-Normalteiler $\mathfrak{U}$ die Ord q^n der $\mathfrak{Q}$ von $\mathfrak{M}$ q^m, so zentralisiert ein gegebenes Element von $\mathfrak{U}$ mindestens q^{m-n} Elemente aus $\mathfrak{Q}$.

(o) Ist $\mathfrak{U} \lhd\lhd \mathfrak{G}$, $\mathfrak{U}_\Gamma \neq 1$, $\mathfrak{U}^\omega = 1$, so $\mathfrak{B}^\omega = 1$

(p) $\mathfrak{U} \leq \mathfrak{H}$ $\quad \mathfrak{U}^{\cdots \mathfrak{G}_\sigma \cdot \mathfrak{G}_\tau}$ .. nicht aufl $\Rightarrow$ Anz Tra Geb $\mathfrak{G}_1 \leq k$

(q) Sind $\overline{\mathfrak{U}}_1, \overline{\mathfrak{U}}_2$ zwei Endhüllen ($\mathfrak{U}_i \leq \mathfrak{H}$) und schneidet $\overline{\mathfrak{U}}_1$ nicht alle Trageb $\mathfrak{G}_1$, so folgt aus ${\overline{\mathfrak{U}}_2}^{\omega_2} = 1$ stets ${\overline{\mathfrak{U}}_1}^{\omega_1} = 1$

(r) $\mathfrak{H} \neq p^\alpha$; $\mathfrak{G}$ pri $\Rightarrow \underset{\alpha}{\exists}$ jeder Konst $\mathfrak{G}_\alpha$ enth einen von $\mathfrak{H}$ & $\mathfrak{H} \leq \mathfrak{G}_\alpha$

39/40

(s) $\mathfrak{G}_1$ hat keinen q-Sockel ($q \neq p$).
Bew sonst läge der q-Sockel von $\mathfrak{G}_\varphi$ ($\varphi \in$ **???**) in $\mathfrak{G}_1$

Fixpunkte von PGr.

(t) Ist das Erzeugnis zweier vertbaren P-Gr transitiv, so ist eine von ihnen fixpktfrei, genauer (w)
Bew genügt für pri $(\mathfrak{A}, \mathfrak{B})$ Indukt: $\overline{\Omega} =$ Trageb $\mathfrak{N}$.

(t′) Statt Vertauschbarkeit genügt Subnormalität + Auflösbarkeit.

a) $\underbrace{\langle \mathfrak{A}^p, \mathfrak{B}^p \rangle}_{\mathfrak{N}}$ treu: Indukt.

b) $\mathfrak{N}$ intra: $\overline{\Omega} =$ Tragebiete $\mathfrak{N}$
Faktorgruppe ist p-Gruppe also oBdA $|\langle \mathfrak{A}, \mathfrak{B} \rangle| = p$ und oBdA $\langle \mathfrak{A}, \mathfrak{B} \rangle$ pri, dort trivial.

(u) Entstehen. $\mathfrak{A}, \mathfrak{B}$ tra Gruppe $\mathfrak{G}$ und hat $\mathfrak{B}$ einen $\underset{\alpha}{\underset{\downarrow}{\text{FP}}}$, so ist $\mathfrak{A}^{\mathfrak{B}}$ tra. $\Gamma = \alpha^{\mathfrak{G}}$ fest bei $\mathfrak{A}, \mathfrak{B}$

40/41

(v) Vermutung: Haben sowohl $\mathfrak{A}$ wie $\mathfrak{B}$ Fixpunkte, so $\mathfrak{A} \circ \mathfrak{B}$ tra.
denn oBdA haben $\mathfrak{A}\mathfrak{B}$

(w) Ist ein Produkt zweier vertauschbarer Gruppen transitiv und hat eine einen Fixpkt, so ist die andere transitiv. $\alpha^{\mathfrak{A}} = \alpha \to \alpha^G = \alpha^B$.
Allgemeiner: Abschätzung für das Produkt der extremen Längen der Transgebiete

(w′) Produkt zweier vertauschbaren subn Ugr $\mathfrak{A}, \mathfrak{B}$ treu $\Rightarrow$ entweder: $\mathfrak{A}$ und $\mathfrak{B}$ fixpunktfrei, dh decken Tr $\mathfrak{A}\mathfrak{B}$ oder: die eine hat Fixpkt, die and ist tra
allg. gilt: größte mal kleinste Bahnlänge ist $\geqq n$ Bew $*$ s.o.

(x) Bei $k = 1, 2, 3$ ist wohl sogar Grad schwacher Abschl. $\mathfrak{H}$ in $\mathfrak{G}_\alpha = n - 1$. Die schw. Abschl. ist bis auf Ähnlk. Tr. das Erzeugnis aller „Endhüllen“ $\mathfrak{H}^{\cdot\cdot\mathfrak{G}_\alpha\cdot\cdot\mathfrak{G}_\beta\cdot\cdot}$. Die „Endhülle“ verfeinert die schw. Abschl.

(y) Auch für beliebige (nicht subn) Ausgangsgruppe $\mathfrak{A}$ ist $\mathfrak{V}$ die schw. Abschl.

41/42

$\mathfrak{G}$ pri Bahnenzahl $\sigma(\mathfrak{G}_\alpha)$

(1) Vor über $\mathfrak{G}_1$: Alle p-Sy Gr $\mathfrak{G}$ abelsch oder hamiltonsch, $\mathfrak{G}$ pri $\mathfrak{H} \leq \mathfrak{G}_\alpha$, $\mathfrak{H}$ rein $p\times$-köpfig $\to$
$\mathfrak{H}$ schneidet in einem passenden $\mathfrak{G}_\alpha \geq \mathfrak{H}$ jede Bahn.
Denn oBdA $\mathfrak{H} \lhd\lhd \mathfrak{G}_\alpha$ wenn $\mathfrak{H} \leq \mathfrak{G}_\alpha$, dann $\mathcal{N}\mathfrak{H} \geq \bigcup \mathfrak{P}_\alpha$
$\mathfrak{P}_\alpha =$ Erzeugnis der p-Sylow Gr $\mathfrak{G}_2$. $\mathfrak{P}_\alpha$ hat keinen weiteren Fixpkt.

(2) Alle Sy Gr $\mathfrak{G}_\alpha$ hamiltonsch, $\mathfrak{G}$ pri $\Rightarrow$ jedes $\mathfrak{H} \leq \mathfrak{G}_\alpha$ deckt für pass β jedes $\gamma^{\mathfrak{G}_\beta}$. Kurz: dann gilt der Decksatz
kürzer: $\mathfrak{H}$ deckt

(3) $\mathfrak{H}$ deckt, Tr $\mathfrak{H} =$ Tr $\mathfrak{K} \Rightarrow \mathfrak{K}$ deckt

(4) $\mathfrak{H}$ deckt nicht $\Rightarrow \exists p$: Ein Konst von $\mathfrak{H}$ hat ord $p^{\cdot\cdot}$ und die p- Sy Gr von $\mathfrak{G}_\alpha$ sind nicht hamiltonsch und ein Konst. von $\mathfrak{G}_\alpha$ hat einen p-Normalteiler und jeder Sylowkern ist auf diesen Konst. von $\mathfrak{G}_\alpha = 1$ (Baer)

41/42

Es ist sogar der Normalisator $\mathcal{N}_p s\mathfrak{G}_\alpha = \mathfrak{G}_\alpha \cap \bigcap \mathcal{N}\mathfrak{A}$, $\mathfrak{A} \lhd\lhd \mathfrak{G}_\alpha$, $\mathfrak{A}$ $p\times$-köpf. auf diesem Konst $\Gamma = 1$.

(5) Def: Ist $\mathfrak{E}$ eine abst. Gr, so sei $\mathcal{N}_{\mathfrak{E}} s\mathfrak{G}$ der gemeinsame Normalis. aller in $\mathfrak{G}$ subnorm Ugr, die zu $\mathfrak{E} \cong$ sind.

(6) Das Zentr in der Sy Gr $\mathfrak{P}$ von $\mathfrak{G}$ mit $\mathfrak{A}_p \leq \mathfrak{P}$

42/43

Vor: $\mathfrak{H} \leq \mathfrak{G}_\alpha$, $\mathfrak{G}$ pri, $\mathfrak{H}$ deckt nicht, $\mathfrak{H} \leq \mathfrak{G}_\sigma \Rightarrow \mathfrak{H} \lhd\lhd \mathfrak{G}_\sigma$. Dann gibt es:

(1) ein in gewissen Sinn* durch $\mathfrak{H}$ eind best. p: auf einer Bahn Γ von $\mathfrak{G}_\alpha$ ist (schwache Abschl $\mathfrak{H}\mathfrak{G}_\nu$)$= p^{???}$

Def$_{43}$ $\to (\mathcal{N}s_{\mathfrak{E}}\mathfrak{G}_\alpha)^\Gamma = 1$ für jedes $\mathfrak{E}$ das in $\mathfrak{H}$ als char. Ugr auftritt.

* jeder annull. kürzeste Operator fängt mit p an, dh jede kürzeste Primärreihe (= Kompreihe mit Primzahlpotenzindizes) fängt oben mit p an) zitiere Verstreutheit
Beisp.: $\mathcal{N}s\mathfrak{H}$ $\mathfrak{G}_\sigma$ reg p-Sy Gr $\mathfrak{G}_\sigma$

$A \lhd\lhd G$, $|G| = \infty$ ohne Normalketten

$|G| \leq \ \infty$ $A, B, \cdots \leq G$

1. $A \overset{B_i}{=} B_i \Rightarrow A^{\langle B_i \rangle_i} = \langle B_i \rangle_i$

2. Def: $\begin{cases} A^{\cdot\cdot G} = \langle B \rangle \\ A \lhd\lhd G \Leftrightarrow A^{\cdot\cdot G} = A \end{cases}$ kurz: $= \overline{A}$, Besser & gleichwertig: $B \leq A^B$

4. $A \leq A^{\cdot\cdot G}$

3. $A^{\cdot\cdot G} = A^{A^{\cdot\cdot G}}$ nach 1

5. $A^{\cdot\cdot G} = A^{\cdot\cdot A^{\cdot\cdot G}}$
   Bew: $A^B = B \Rightarrow B \leq A^{\cdot\cdot G} \Rightarrow \langle B \rangle = A^{\cdot\cdot A^{\cdot\cdot G}}$ nach 2

6. $A \leq B \Rightarrow A^{\cdot\cdot G} \leq B^G$ denn $\overline{A} = A^{\overline{A}} \leq A^{\overline{B}} \leq B^{\overline{B}} = \overline{B}$

6′ $\langle A_i^{\cdot\cdot G} \rangle_i \leq \langle A_i \rangle_i^{\cdot\cdot G}$

7. $A \leq B \lhd\lhd G \Rightarrow A^{\cdot\cdot G} = A^{\cdot\cdot B}$ 6
   A

8. $A \lhd\lhd B \lhd\lhd B \lhd\lhd G \rightarrow A \lhd\lhd G$ 7

9. $A \leq B \leq G$, $A \lhd\lhd G \Rightarrow A \lhd\lhd B$ $A \leq C \leq B_1 A^C = A \Rightarrow C \leq A^{\cdot\cdot G} = A$ $\langle C \rangle = A$

10. Def 2 ist äquivalent mit $A \lhd\lhd G \iff A = \bigcap A_i$ transfinite Normalreihe

Bew

a) Sei $A = \bigcap A_i$, $B = A^{\cdot\cdot G}$ im Sinn 2
   $B = A^B \leq$ jedes Gl der Normalkette A: $B \leq \bigcap A_i = A$
b) Sei $A = A^{\cdot\cdot G}$ im Sinn 2
   Sei $D = \bigcap$ klst Normenkette transfinit. $A \leq D$
   Wäre $A \leq D$, so $A^D < D$, Normenkette hätte nicht mit D abgebrochen

11. $A \lhd\lhd G \Rightarrow A_1 G_1 \lhd\lhd G_1$ 10

12. $B \leq G$, $B \leq A^B \Rightarrow B \leq A^{\cdot\cdot G}$
    Bew: $\langle A, B \rangle = C$ $B \leq A^B \leq A^C$ $A \leq A^C$ $C \leq A^C$ $C \leq A^{\cdot\cdot G}$

13. $A_\nu \lhd\lhd G$, $D = \bigcap A_\nu \Rightarrow D \lhd\lhd G$
Bew: $B \leq D^B \Rightarrow B \leq A_v^B \Rightarrow B \leq A_\nu. \Rightarrow B \leq D$

14. $G^\sigma =$ hom Bild $G = \overline{G}$, $\overline{B} = \overline{A}^{\cdot\cdot\overline{G}}$
$B, A = \overline{B}^{G^{-1}}, \overline{A}^{G^{-1}} \longrightarrow B = A^{\cdot\cdot G}$.

14 Aufgabe: Rechnen mit Ausschnitten - Kalkül entwickeln

15. $(A^{\cdot\cdot G})^\sigma \leq A^{\sigma\,\cdot\cdot G^\sigma}$.

46/47

Vertauschbarkeit u. Subnormalität

1. Ist $x_\nu \in G$, $A \leq G$, $x_n \in AA^{x_1} \cdots A^{x_n}$, so ist $x_n \in AA^{x_1} \cdots A^{x_{n-1}}$

$$\begin{aligned} x_n &= a_1 a_2^{x_1} \cdots a_n^{x_n} = a_1 a_2^{x_1} \cdots a_{n-1}^{x_{n-1}} x_n^{-1} a_n x_n \\ 1 &= \cdots \quad \cdots a_n \\ &= a_n a_1 a_2^{x_1} \cdots a_{n-1}^{x_{n-1}} \cdot x_n^{-1} \\ x_n &= (a_n a_1) a_2^{x_1} \cdots a_{n-1}^{x_{n-1}} \end{aligned}$$

Folge:

2. (i) Ist $AA^{x_1} \cdots A^{x_n} = G$, so $AA^{x_1} \cdots A^{x_{n-1}} = G$,
   (ii) Ist (i) & jeweils das Teilprodukt $AA^{x_1} \cdots A^{x_m}$ Gruppe, so $A = G$

   Man braucht also zum Nachweis von $A = G$ nur eine Folge von A^{x_n}, so daß A^{x_r} v $A^{1+\ldots+x_{r-1}}$ und $A^{1+x_1+\ldots+x_n} = G$

47/48

Anti- Monotonie von $\sum e_\rho^2$

(1) Sei $\mathfrak{G}$ eine endl. Gruppe linearer Subst. die Vielfachheiten seien e_ρ (der irred Darst v. $\mathfrak{G}$). Ist dann $\mathfrak{H} = \mathfrak{G}^* < \mathfrak{G}$, so ist $\sum {e_\rho^*}^2 \geq \sum e_\rho^2$ und = genau wenn $\mathfrak{G} \leq$ lin Abschliessg $\mathfrak{G}^*$. Denn $\sum {e_\rho^*}^2 = \mathrm{Rg}\mathfrak{V}^*$ (= Vert Ring von $\mathfrak{G}^*$)

$$\mathfrak{V}^* \geq \mathfrak{V}$$

Statt Endlichkeit von $\mathfrak{G}, \mathfrak{G}^*$ reicht auch vollstd. Reduzibilität
Folge

(2) $\mathfrak{G}^* \leq \mathfrak{G}$ endl: $\Rightarrow$ Mittelwert $|\chi|^2$ ist über $\mathfrak{G}$
$\leq$ " " " $\mathfrak{G}^*$

48/49

Zur Darstellungstheorie von p-Gruppen

(1) $|G| = p^a \Rightarrow \frac{k\chi}{f} \equiv k \mod \mathfrak{p}$
Bew: auf monomiale Gestalt bringen mit p^α- ten EW als Koeff: Zeilensumme $\equiv 1(\mathfrak{p})$. In $\sum\limits_{G \in \text{Klasse}} D(G)$ ist dann Zeilensumme $\frac{k\chi}{f} \equiv \sum 1 = k$

49/50

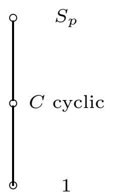
28/4/62 Projektion von $s\mathfrak{G}$

in $\mathfrak{H} \leq \mathfrak{G}$ ist genau dann möglich, wenn für jeden Subnormalfaktor $F = F_1 \times F_2$ gilt: $\mathfrak{H} \wedge F = \mathfrak{H} \wedge F_1 \times \mathfrak{H} \wedge F_2$ daher $F = A/B$, $\mathfrak{H} \wedge F = (\mathfrak{H} \cap A)B/B$
Bew: Ind bezgl $|\mathfrak{G}|$: $A, B \lhd\lhd \mathfrak{G}$ dann Ind bezgl $|\mathfrak{G} : A| + |\mathfrak{G} : B|$ Man kann auf $D = A \cap B \lhd \cdot\frac{A}{B}$ zurückkommen, dann auf $D = 1$, $\langle A, B \rangle = G$, $|A| = |B| = p$
Dann Fallunterscheidung: H deckt entweder G/N, $N = A^G \cap B^G$ oder meidet.
Fallunterscheidg ob ein $a^b \in H$ oder nicht.
Aufgabe: auf $|G| = \infty$, Max bedgg erweitern

50/51

Verlagerung. August 62

Suzuki ist an V.-Sätzen in folgender Situation interessiert:



$C \leq$ Center of $\mathcal{N}_G C$ even C is a direct factor of $\mathcal{N}_G C$.
Problem: What addit. cond. will give a hom σ of G with $\sigma C \neq 1$

51/52

Perm Gr vom Grad p. 12.9.62

1. Sind $A\,B\,C$ Matrizen aus dem Gruppenring der zykl. PGr des Grd p, und ist $\mathfrak{G}$ eine PGr des Grds p derart, dass (#) $\mathfrak{G}^A$, $\mathfrak{G}^{AB}$, $\mathfrak{G}^{ABC}$, $\mathfrak{G}^{ABCB}$, $\mathfrak{G}^{ABCBA} = \mathfrak{H} \leq \mathfrak{S}^p$, so hat auch $\mathfrak{H}^Q$ statt $\mathfrak{G}$ dieselben Eigenschaften, wo Q eine Permut. mit $A^Q = A^*$, $B^Q = B^*$, $\cdots$
   Wenn also $\mathfrak{G}$ maximal ist mit (#), so ist $\mathfrak{H} = \mathfrak{G}^Q$
2. Vermutung: Wenn $\mathfrak{G}^A$, $\mathfrak{G}^{AB}$, $\mathfrak{G}^{ABA} \leq \mathfrak{S}^p$, so teilt die Invariante zu A diejenige zu B. s. hierzu 6
3. Tatsächlich tritt in geeigneten Gruppen des Grades $p = \frac{q^n - 1}{q - 1}$ (q Primzahlpotenz) die Invariante q^{n-2} auf
   $\mathfrak{G} = PSL(n, q)$
   NB: Daher ist notwendig n ungerade, wenn dies p wirklich Primzahl.

52/53

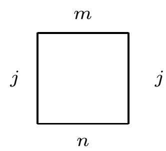
4. Die Invariante $j = \frac{p+1}{4}$ tritt, wenn $p \equiv 3\ (4)$, [vielleicht nicht in Gruppen aber] als Betragsquadrat einer Summe von $\frac{p-1}{2}$ p-ten Einheitswurzeln auf, nämlich wo die Exponenten die $\square$ Reste mod p sind (also $\kappa =$ Gaußsche Periode der Länge $\frac{p-1}{2}$).

5. Zwei Invarianten $j = \frac{t(p-t)}{p-1}$, $k = \frac{s(p-s)}{p-1}$, die sich nur um ein Quadrat einer rat Zahl unterscheiden, stimmen überein.
   Bew: Sei $a^2 j = b^2 k \quad (a,b) = 1$
   $a^2 | k \quad a^2 \leq k \leq \frac{p+1}{2p},\ b^2 \leq \cdots$
   $a, b \leq \sqrt{\frac{p+1}{4}} < \frac{p}{2}$. Wähle $s, t \leq \frac{p-1}{2}$
   (α) $a^2 t(p-t) = b^2 f(p-s)$ gibt $at \equiv bs$ bei pass. Wahl von sign b.
   $at = bs + xp + x = \frac{at-bs}{p}\ |x| < \frac{p}{4}$
   $|x| \leq \frac{p-1}{2p} \cdot (|a| + |b|) \leq \frac{(p-1)}{p} \cdot \sqrt{\frac{p+1}{4}}$
   $|x| \leq \frac{\sqrt{p-1}}{2} \sqrt{\frac{p^2-1}{p^2}} < \frac{1}{2}\sqrt{p-1} < \frac{1}{2}\sqrt{p} < \frac{p}{4}$

53/54

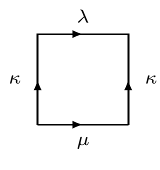
   $|a-b| \leq |a| + |b| \leq \sqrt{p+1} < \frac{p}{2}\ (p \geq 5)$
   $at = bs + xp$ in (α) eingesetzt gibt $a - b \equiv 2x \mod p$ und da beide Seiten $|\ | < \frac{p}{2}$, ist $0 = a - b - 2x$, $\underset{a}{\longrightarrow}$ $x^2 = ax \rightarrow \begin{cases} x = 0 \\ x = a \end{cases} \underset{a}{\longrightarrow}$
   $\begin{cases} a = b \ \ (= \pm 1) \\ a = -b \ \ (= \pm 1) \end{cases} \rightarrow j = k$

6. Folge:

   a) 

   $\Rightarrow$ $m{=}n$

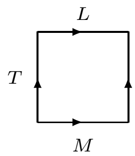
   3.72: Frage: Können dann auch die transformierenden Matrizen zuerst gleich gewählt werden? Dann könnte man die transf. Pgr als gleich annehmen (maximale nehmen)

   b) 

denn nach a) ist $|\lambda| = |\mu|$ und noch bei Wahl von sign μ.

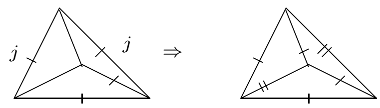
$$\begin{aligned} \kappa\overline{\kappa}\lambda &= a\mu \qquad a \in \mathbb{Z} \\ j\lambda &= a\mu \\ |\lambda| = |\mu| \Rightarrow j &= a \end{aligned}$$

c)



$\Rightarrow M{=}L$

d)



nach a)

54/55

7. Zwei Invarianten mit dem selben "A-freien Teil" w stimmen überein. Bew 5

8. Sind j_1, j_2, j_3 Invarianten mit $j_1 j_2 = a^2 j_3,\ a \in \mathbb{Z}, a^2 < j_1 < \frac{p+1}{4}$, so gibt es $b, c \in \mathbb{Z}$ mit
$$\begin{cases} at_3 &= t_1 t_2 + bp \\ at_3 &= t_1 + t_2 + 2b - a + cp \end{cases}$$
Dabei sind $|a|, |c|$ klein ($\lesssim \sqrt{p}$)

! Achtung: neue Bezeich.

9. Unter den Vor. von S. 56 oben ist
$$j_1 + j_2 + c^2 = j_3' + a^2 \text{ wenn } j_1 < j_2 < j_3 \text{ so } < j_3' + j_1$$
mit
$$j_3' = \frac{p^2 - s_3'^2}{4(p-1)} \in \mathbb{N} \text{ siehe S. 74, 80 } s_3' := 2c - b \text{ ungerade } \gtrless 0$$
$$s_3' \underset{p-1}{\equiv} s_1 s_2$$
$$b := \frac{s_1 s_2 - 2as_3}{p}\ (\in \mathbb{Z}), \quad c := \frac{b + as_3}{p} \in \mathbb{Z}$$
mod $p-2$ ist $\begin{cases} 4c \equiv s_1' s_2 \\ s_3' \equiv as_3 \end{cases}$, also ? $s_3' = kl$ pos Rest as_3 mod $p-2$ daher $s \neq s_3$, $j_4 \neq j_3$. $j_3' \equiv 1 + j_1 j_2 - \frac{j_1 j_2}{j_3}$ mod $p-2$. $j \equiv 1 - \frac{s^2}{p^2}$ mod $(p-2)^2$
$j_3' - 1 \equiv a^2(j_3 - 1)$

55/56

Sei
$$j_2 = \frac{(\frac{p}{2} + \frac{s_2}{2})(\frac{p}{2} - \frac{s_2}{2})}{p-1} = \frac{p^2 - s_2^2}{4(p-1)} \in \mathbb{N}$$
Dann ist $0 < s_2 < p$, s_2 ungerade. Sei $j_1 j_2' = a^2 j_3,\ a \in \mathbb{Z}$, dann
$$(p^2 - s_1^2)(p^2 - s_2^2) = 4(p-1)a^2(p^2 - s_3^2)$$

(α)
$$p^4 - (s_1^2 + s_2^2)p^2 + s_1^2 s_2^2 = 4p^2 a^2 (p-1) - 4pa^2 s_3^2 + 4s_3^2 a^2$$
wähle sgn a so, daß $s_1 s_2 \equiv 2as_3 (p)$

(β)
$$s_1 s_2 =: 2as_3 + bp \quad b \in \mathbb{Z}$$
Dann gibt (α) wegen $s_1^2 s_2^2 - 4a^2 s_3^2 = (4as_3 + bp)bp$
$$\begin{aligned} p^3 - (s_1^2 + s_2^2)p + (4as_3 + bp) \cdot b &= 4pa^2(p-1) - 4a^2 s_3^2 \\ 4as_3 b + 4a^2 s_3^2 &\equiv 0\ (p) \\ b + as_3 &\equiv 0\ (p) \end{aligned}$$

(γ) Setze
$$\frac{b + as_3}{p} = c \quad \in \mathbb{Z}$$
Dann folgt
$$p^2 - (s_1^2 + s_2^2) + 4as_3 c + b^2 p = 4a^2(p-1)$$
$$p^2 - s_1^2 + p^2 - s_2^2 - \{p^2 \qquad \underbrace{-4as_3 c - b^2}_{(-b^2+4bc-4c^2)-4(p-1)c^2} \qquad \} = 4a^2(p-1)$$
Durch $4(p-1)$ dividiert gibt das 9.

56/57

10. Ebenso gilt, falls $n^2 j_1 j_2 = a^2 j_3$ vorausgesetzt wird:
$$n^2(j_1 + j_2) + c^2 = j_3^* + a^2 + \frac{(n^2-1)p^2}{4p-4}$$
mit
$$\begin{cases} ns_1 s_2 & = 2as_3 + bp \\ b + as_3 & = p^c \\ j_3^* & = \frac{p^2 - (b-2c)^2}{4p-4}. \end{cases}$$
Wenn also $n^2 \equiv 1 \mod 4p-4$, so ist $j_3' \in \mathbb{Z}$.

11. Im Fall 9 wird

$$s_3' = \frac{(4p-4)as_3 - (p-2)s_1 s_2}{p^2}$$

$$j_3' \cdot p^4(4p-4) = p^6 - [(4p-4)as_3 - (p-2)s_1 s_2]^2$$

12. Für $p \geq 11$ ist jedes $j \geq 4$
Bew:

$$\begin{aligned} \frac{2(p-2)}{p-1} &\equiv 0(p-2) \text{ wenn ganz, } \Rightarrow \geqq p-2 \\ \frac{3(p-3)}{p-1} &\equiv 0(\frac{p-3}{2}) \ \ n \ \ \Rightarrow \geq \frac{p-3}{2} > 3 \text{ Gr.} \\ \frac{p}{2} > t \geq 4 \Rightarrow \frac{t(p-t)}{p-1} &\geq \frac{4(t-4)}{p-1} = \frac{4}{1+\frac{3}{p-1}} \geq (1 - \frac{3}{p-1})4 > 3, \end{aligned}$$

für

$p > 13$, nicht ganz für $p = 11$

12a. $j_1 j_2 j_3 = m^2, \ a = \frac{m}{j_3} \Rightarrow s_1 s_2 s_3 \equiv 8m \mod p$

13. Für $p \geq 11, \ j_1 j_2 = a^2 j_3$ ist

$$|a| < \frac{p}{8}; \quad |b| < \frac{5}{4}p \quad |c| < \frac{p}{8} + \frac{5}{4}$$

denn

$$a^2 \leq \frac{j_1 j_2}{4} \leq \frac{\frac{p+1}{4}\frac{p-1}{4}}{4} < \frac{p^2}{64}$$

$$|b| = \frac{c|s_1 s_2| + |2a_2 s_3|}{p} < \frac{p^2 + \frac{p}{4}p}{p}$$

14. Daher ist c der absolut kleinste Rest von $u_1 u_2 \mod p-2$
(wo $u_2 = \frac{1}{2}(p-2-s_2)$ denn es ist

15. Mod $p-2$: $j_\nu \equiv 1 - u_\nu^2 \qquad c \equiv u_1 u_2 \ u_\nu \equiv \frac{s_\nu}{2} \quad u_3' \equiv au_3$

15′: $2c - b = \left.\begin{matrix} s_3' \equiv s_1 s_2 \\ s_\nu' \equiv 1 \end{matrix}\right\} \mod (p-1)$

16.

$$p(2c+b) = 2b + s_1 s_2$$

gibt

$$|2c+b| \underset{\leq p+2}{\leq} \frac{5}{2} + \frac{|s_1 s_2|}{p} \leq p + \frac{5}{2}$$

also

$$|2c-b| \leq p + 2 + 4|c|$$

und

58/59

wenn $bc > 0$, so

$$\begin{aligned} |2c-b| &\leq p + \frac{5}{2} - 2 - 2 \\ |2c-b| &\leq p-2, \text{ also } j_3' > 0. \end{aligned}$$

17. Mit $u = \frac{p-2-s}{2}$ (wie bisher) gilt

$$\begin{aligned} j &= 1 - u^2 + \frac{u(u+1)}{p-1} \cdot (p-2) \\ &\equiv (1+u)^2 \quad \text{mod } p, \text{ also } 1+u = t \end{aligned}$$

also ist $u(u+1) \geq p-1$. Hiernach könnte es Zweck haben, statt i besser $k = \frac{u(u+1)}{p-1}$ zu betrachten ($0 < u < \frac{p}{2}$)

18. (a) läßt sich schreiben als

$$j_1 j_3 + j_2 j_3 + c^2 j_3 = j_3' j_3 + j_1 j_2$$

Frage: Ist $c^2 j_3 = j_1' j_2'$? Nachprüfen, ob wenigstens $\mod p-2$ $cj_3 = c_2 j_\nu$ wohl nicht: $cj \equiv u_1 u_2 (1 - u_3^2) \quad (p-2)$

59/60

19. Wenn nun j_1, j_2 also $u_1 u_2 (s_1 s_2)$ gegeben sind und man weiß, daß dazu ein a, j_3 gehört mit $j_1 j_2 = a^2 j_3$, so kann man j_3 so finden:
Bestimme $c = |u_1 u_2|_{p-2}$, dh. $c =$ (absolut kleinster Rest)

$$\begin{aligned} [b &= \frac{s_1 s_2 - 2cp}{p-2}] \\ as_3 &= \frac{p^2 c - s_1 s_2}{p-2} \end{aligned}$$

$$a^2 = \frac{4(p-1) j_1 j_2 + (as_3)^2}{p^2}$$

$$\operatorname{sgn} a = \operatorname{sgn}(as_3)$$

$$s_3^2 = \frac{p^2}{(p-2)^2} \cdot \frac{(p^2 c - s_1 s_2)^2}{4(p-1) j_1 j_2 + (as_3)^2}$$

$$j_3 = \frac{p^2 - s_3^2}{4(p-1)} = \frac{j_1 j_2}{a^2}$$

(Frage: $u_1 u_2 \Rightarrow u_3$?)
gibt

$$j_3 = \frac{p^2 j_1 j_2}{4(p-1)j_1 j_2 + \left(\frac{p^2 c - s_1 s_2}{p-2}\right)^2}$$

$$j_3' =$$

Forts. 74

60/61
Seite 61 ist leer!
61/62

Charaktere von p-Gruppen
4.11.62 Hilfss. f. Tamaschke

1. Ist $\mathfrak{G}$ eine p-Gp, D eine irred Darst mit Charakter χ, so gilt für jede Klasse konj. Elemente mit k Elementen

$$\frac{k\chi}{f} \equiv k \mod \mathfrak{p}$$

wo $\mathfrak{p}$ der Primteiler von p in $Q(\chi)$.
Allgemeiner:

62/63

Sei $\mathfrak{G}$ p-Gruppe, D eine Darstellg: $\mathbb{C}$, $g_1 \cdots g_k \in \mathfrak{G}$, $\sum_\kappa D(g_\kappa)$ habe den Eigenwert λ, $\sum g_\kappa \in$ Ztr Gr Rg $\mathfrak{G}$. Dann ist $\lambda \equiv k \mod \mathfrak{p}$
Bew: Ind $|\mathfrak{G}|$. oBdA D irreduzibel, & $g_1 \cdots g_\kappa$ eine Klasse konjugierter Elemente. Wähle D monomial, und sei $\mathfrak{G}'$ normale Untergr vom Index p, die intransitiv ist. (Gibt es die nicht, so ist $f = 1$ und die Beh trivial.)

a) $g_1 \notin \mathfrak{G}'$ Dann $\chi(g_\kappa) = 0$, $\lambda = \frac{k\chi}{f} = 0$ und $k \equiv 0 \mod p$, da sonst $k = 1$, $g_1 \in$ Ztr $\mathfrak{G}$, $D(g_1)$ diag., $g_1 \in \mathfrak{G}'$
b) $g_1 \in \mathfrak{G}'$ $\Rightarrow$ alle $g_\kappa \in \mathfrak{G}'$, $\sum g_\kappa$ ist auch Summe von Klassensummen in $\mathfrak{G}'$,
Ind: $|\mathfrak{G}'| < |\mathfrak{G}|$, also $\lambda \equiv k(\mathfrak{p})$

Verwandter Satz S. 105

63/64

25.1.63 Zerschneidung von Perm-Gruppen

(1) Sei $N \trianglelefteq G$, G pri, $N_\alpha \neq 1$. Dann läßt sich N_α auf $\Omega - \alpha$ nicht "zerschneiden"; Es gibt keine Einbettung $\Omega - \alpha = \Gamma + \Delta$ so, dass N_α Γ fest lässt und N_α^Γ enthält.
Bew:

(a) Alle Bahnen maximaler Länge von N_α trete in Γ auf. Ihre Vereinigung nenne $\Gamma' \subseteq \Gamma$. Da $N_\alpha^\Gamma \subseteq N_\delta$ $(\delta \in \Delta)$, ist Γ' Fixblock von N_δ, und für $g = (\alpha\delta\ldots)\ldots$ ist $\Gamma'^g = \Gamma'$, $G = \langle G_\alpha, g\rangle$ läßt Γ' fest, W!
NB: Hierfür genügt schon Transitivität von G; Primitivität unnötig.

(b) Sowohl Γ wie Δ mögen Bahnen $\Gamma', \ldots$ bzw $\Delta', \ldots$ maximaler Länge von N_α enthalten. Sei etwa $|\Gamma| \leq |\Delta|$, dann $2|\Gamma| < n = |\Omega|$, daher haben für $g \in G$ stets N_α^Γ und $(N_\alpha^\Gamma)^g$ einen Fixpunkt gemeinsam, also da $N_\beta \geq N_\alpha^\Gamma$ und daher Γ' Fixblock von N_β, ist Γ' Fixblock jedes $(N_\alpha^\Gamma)^g$, also von dem transitiven $(N_\alpha^\Gamma)^G$ W!

64/65

(2) Meine Verallgemeinerung des Satzes von Rietz gilt schon wenn $\mathcal{N}(G)$ (statt G) primitiv ist.

(3) Wenn $\mathcal{N}G$ pri ist, so hat jede subnormale Ugr von G lauter gleichlange Bahnen.

(4) Sei G pri, die voneinander verschiedenen Bahnlängen $\neq 1$ von G_α seien $l_1 < l_2 < \cdots l_k$. Dann hat jedes l_i mit mindestens einen der anderen einen ggT $\neq 1$ (z.B. mit dem längsten; trivial)

(5) Ist $A \lhd\lhd G$, $A_\alpha \neq 1$, G pri, so kann man A_α nicht auf $\Omega - \alpha$ zerschneiden, ausgenommen $\Omega = \alpha + \Gamma + \Delta$ mit $A^\Gamma = 1$.
Bew: Sei $S =$ Sockel G, $AS = N$.

65/66

Dann $A \lhd N \lhd\lhd G$, N tra.
Ann: A_α zerschneidbar:

$$\begin{array}{rcl} \Omega & = & \alpha + \Gamma + \Delta \\ & & \quad\;\downarrow \quad \downarrow \\ A_\alpha & = & \quad\; K \cdot L \end{array}$$

$L = A_\alpha^\Delta \leq A$.
Beh: $A^\Delta \neq 1 \rightarrow A^\Gamma = 1$.
Einige längsten Bahnen von A_α seien in Δ; etwa $\Delta', \Delta'', \ldots$. Dann Δ' Festblock von K^n für jedes $n \in N$, da K^n mindestens einen Fixpunkt β in $\alpha + \Gamma$ hat und die $\Delta', \cdots$ Bahnen von A_β sind. Also Δ' Bahn von K^N, das ΔN, daher $\lhd\lhd G$ ist. Daher haben alle Bahnen von K^N die gleiche Länge, und jeder tra Konst von K^N ist treu (der Normalteiler, der auf einer Bahn von K^N 1 hat, ist $\lhd\lhd G$ und daher $= 1$, da G pri). Hieraus folgt $K = 1$, denn $K^{\Delta'} = 1$. Also $A_\alpha = L$

5′ Mehr kann man wohl nicht sagen!
Setze auf $(3,3) = S$ die rational irred. (: Q_3) 2-Gruppe $\begin{pmatrix} \pm 1 & \\ & \pm 1 \end{pmatrix}$, $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$ der Ord 8; $|A| = 2 \cdot 3^2$, $a_1 = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$ mit 3 Fixpunkten in S. G ist pri, $A \lhd\lhd G$, $A_1 = \langle a_1 \rangle$ hat 3 Fixp.

66/67

6. Sei $1 \neq H \leq G_\alpha$, H tra auf Trä H, $G \lhd\lhd P$ P pri
Dann ist $H^{\cdot\cdot G}$ 2-tra.
Bew: $P \rhd P_1 \rhd\rhd G$
H^P 2 tra, P_1 2 tra pri; Ind: $|P|$.

7 Hat $H \neq 1$ $k \leq 3$ wesentliche Trasysteme, $H \leq G_\alpha$, G pri, so hat mit $S \circ H^{\cdot\cdot G}$ auch S_α höchstens k wesentliche Tra-systeme und nur den einen Fixpkt α
Bew mit

8. Die Fixpkte von N_α eines N-Teilers N von G bilden einen Block von G. Die zugehörige Äqn ist: $\alpha \sim \beta \iff N_\alpha = N_\beta$. Entsprechende Halbblöcke wird man kriegen durch $\alpha \prec \beta$ wenn $N_\alpha \leq N_\beta$.

67/68

9. Vermutlich folgt aus $A \trianglelefteq B$ nicht $\overline{A} \trianglelefteq \overline{B}$ (Abschliessungen).
Gegenbeispiel ?

68/69

Perm - Gr.

(1) G habe einen regulären Normalteiler N, und $U \leq G$ habe einen (od. mehrere) Fixpkt α. Dann ist $\mathcal{C}U$ tra auf den Fixpkten Φ von U; $|\Phi| \big| |\Omega|$
Bew: $H := NU$ $\;U = H_a$ $\;H \cap \mathcal{N}U$ tra Fix(U)
U zentralisiert die $n \in N$, die einen Punkt von Φ in α überführen.

Transfer

(2) Hilfssatz zur Verlagerung (Berechnung von det $D = \begin{pmatrix} \varepsilon_1 & & \\ & \ddots & \\ & & \varepsilon_n \end{pmatrix}$ mittels eines Produktes von Konjugierten D^x:
Ist P eine p-Gruppe und Δ das Ideal im Gr.Ring R mod p, das von den $x-1$ als Modul erzeugt wird, so erzeugt $\underline{P} = \sum\limits_P x$ das einzige minimale Ideal $\mathfrak{m}$ von R in Δ. Denn $\mathfrak{m} \cdot \Delta < \mathfrak{m}$ wegen $\Delta^\infty = 0$, also $\mathfrak{m}\Delta = 0$
$\mathfrak{m}(x-1) = 0$ $\mathfrak{m} = c \cdot \underline{P}$. Daher ist $\underline{P}$ als Produktsumme von $(x_i - 1)$ maximal vom Grad l darstellbar, wo l die Länge der Kette der Zassenhausschen p-Dimensions-Gruppen in P bedeutet (1937; Jennings) ∼1958

69/70

Notre Dame 22 3 63 Zum Satz v. Kegel: $A^x \,\mathrm{v}\, B^y$

(1) $A^x \,\mathrm{v}\, B^y$ (f alle $x, y \in G$): $\boxed{\overset{\text{unnötig}}{A^G B^G = G,}}$ $AB < G \Longrightarrow AB^G < G$ oder $A^G B < G$
Bew mit $A^x = \langle A^g \rangle, B^* = -$ maximal $A^* B^* \neq G$

(2) $A^x \,\mathrm{v}\, B^y$, $A^{\cdot\cdot G} B = AB^{\cdot\cdot G} = H \Rightarrow AB = H$
Bew: (1) auf $G' = (AB)^{\cdot\cdot G}$
Sonderfall:

(3) $A^x \,\mathrm{v}\, B^y$, $A^{\cdot\cdot G} = B^{\cdot\cdot G} \Rightarrow A^{\cdot\cdot G} = AB$

(4) FRAGE: Gilt $A^x \,\mathrm{v}\, B^y \Rightarrow AB = AB^{\cdot\cdot G} \cap A^{\cdot\cdot G} B$ oder Verwandtes?

70/71

Monomiale p-Gruppen

(1) Ist M eine trans.mon. p-Gr.: C_p, so erzeugt jede Diagonalmatrix $d \in M$ mit det $d \neq 1$ mit ihren Konjugierten schon alle Diag Matr.
Bew: Ind Grad $M = n$

(1) $n = p$ bekannt

(2) $n > p$: M ist impr. nimm Blöcke, konjugiert, aus je p Punkten; $M \to \overline{M} =$ auf ihnen hat $\overline{d}$ die Determinante $\delta_1, \cdots, \delta_{\frac{n}{p}}$ mit $\prod \neq 1$. Ind: Gr $\overline{M} = \frac{n}{p}$

$$d^M \ni \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_{\frac{n}{p}} \end{pmatrix} \text{ mit det } d_1, \neq 1, \text{ det } d_i = 1.\ (i > 1).$$

(3) Beh: Zu vorgegebenen k Stellen $(0 \leq k \leq \frac{n}{p} - 1) \cdot j_k$ gibt es $d_k^* \in d^M$ mit det $d_1^* \neq 1$, $d_{jk}^* = I =$ Einh.matr. des Grades p.
richtig für $k = 0$. Ind: sei $k > 0$, für $k - 1$ schon bewiesen. Geg $j_1, \cdots, j_k$. Wähle

$$\begin{cases} d^{**} \cdot & \text{det } {}^{x_1}_{1} \neq 1, \quad d_{j_1}^{**} = \cdots\cdots d_{j_{k-1}}^{**} = 1 \\ \widehat{d} : & \widehat{d}_k \neq 1,\ \widehat{d}_{j1} = \cdots = \widehat{d}_{k-1} = 1 \end{cases}$$

71/72

Wähle $q \in M$, das auf jedem der n' p Blöcke zyklische Perm, induziert (in einem passenden Zentrum). ein geeignetes Kommutatorprodukt $r = \prod[\widehat{d}, q^\kappa]$ hat an Stelle j_k gerade d_k^{-1} (nach (1)), also $rd^{**} = sd^* \in d^M$ mit $d_{j_1}^* = \cdots = d_{j_{k-1}}^* = 1$, det $d_1^* \neq 1$.

4) Nun $k = \frac{n}{p} + 1$ wählen < gibt $\widetilde{d}\, G_d M$, det $\widetilde{d}_1 \neq 1$, $\widetilde{d}_i = \cdots = \widetilde{d}_{\frac{n}{p}} = I$

geeignete Kommutrng mit q gibt $d_m^t = \begin{pmatrix} \varepsilon_1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \in d^M$

Eleganterer Beweis:

72/73

Beweis kürzer: Setze $D_1 = \{\text{diag det } = 1\}$. $D_1 M = \widehat{M}$. Dann $D \leq \widehat{M}$, daher $D_1 = [D, \widehat{M}] \leq \Phi(\widehat{M})$, $M = \widehat{M} \geq D$.

(2) Entsprechend gilt: Enthält eine monomiale p-Gruppe M mit Koeff $\in \mathfrak{C}$ $(= p\text{-Gp})$ eine Diagonalmatrix d mit Koeff $\in C_p$ $(\leq \text{Ztr } \mathfrak{C}, |C_p| = p)$ und det $\neq 1$, so enthält M alle Diagmatr. mit Koeff $\in C_p$.
Bew: $d^M = d^P$ wo P die zu M gehörige Permgp ist. Setze $\widetilde{M} = d^M \cdot P$, wende (1) an

73/74

Forts. von S. 60 $\quad$ P-Gr. vom Grad p. $\quad$ Notre Dame 26.4.63

Sei

(1)
$$j_1 j_2 = a^2 j_3,$$

mit

(2)
$$\begin{aligned} j &= \frac{k(p-k)}{p-1} = \frac{p^2 - s^2}{4(p-1)}, 0 < s < p; 1 < k < \frac{p}{2} \\ &= k - \frac{k(k-1)}{p-1} \end{aligned}$$

Dann

$$(p^2 - s_1^2)(p^2 - s_2^2) = (4p-4)a^2(p^2 - s_3^2)$$
$$s_1^2 s_2^2 \equiv 4a^2 s_3^2 \ (p)$$

(3)
$$\begin{cases} s_1 s_2 & = bp - 2as_3 \quad b \equiv 1(2),\ a \gtrless 0 \\ b & = \frac{s_1 s_2 + 2as_3}{p} \end{cases}$$

gibt eingesetzt

$$p^3 - p(s_1^2 + s_2^2) + b^2 p + 4as_3(as_3 - b) = 4a^2 p(p-1)$$
$$4as_3(as_3 - b) \equiv 0$$

(4)
$$as_3 - b = cp,\ c = \frac{as_3 - b}{p}$$

gibt eingesetzt

$$p^2 - s_1^2 + p^2 - s_2^2 + b^2 + 4as_3c = p^2 + 4a^2(p-1)$$

und mit der Abkürzung

$$s_3' = b + 2c \tag{5}$$

(gegenüber S. 56 hier $a \to -a$) gibt es

NB: In der Bezeichnung von XVI 69 ist $\begin{cases} a := & \delta z \\ b := & \delta(zs_3 - \nu p) \\ c := & \delta\nu \\ \delta s_3' = & zs_3 - \nu s_0 \\ s_3 := & p-2 \\ j_3' \equiv & 1\ (z) \end{cases}$

$$j_1 + j_2 + c^2 = a^2 + \frac{p^2 - s_3'^2}{4(p-1)} \tag{6}$$

$$= a^2 + j_3' \tag{7}$$

Wir zeigen durch Abschätzung, dass $j_3' > 0$, also wirklich eine Invariante ist (auf S. 80).

$$j_1j_3 + j_2j_3 + c^2j_3 = j_1j_2 + j_3j_3' \tag{7'}$$

74/75

Fortsetz: Kongruenzen

(8)	$j \equiv f_2^2\ (p)$		
(9)	$j \equiv \dfrac{s^2}{4}\ (p)$		
(10)	$b \equiv as_3\ (p)$	Bew(4)	
(11)	$s_1s_2 \equiv -2as_3\ (p)$	(3)	
(12)	$s^2 \equiv p^2 \quad \bmod 4p-4;$	$(s, 4p-4) = 1$	
(12′)	$s_1s_2 \equiv b - 2as_3$	$(p-1)$	(3)
(13)	$c \equiv -b + as_3$	$(p-1)$	
(13′)	$s_1s_2 \equiv -(b+2c) \equiv -s_3'$	$(p-1)$	
(14)	$s_1s_2 \equiv 2b - 2as_3$	$(p-2)$	
(15)	$2c \equiv -b + as_3$	$(p-2)$	
(16)	$s_1s_2 \equiv -4c$	$(p-2)$	
(16′)	$j \equiv 1 - \dfrac{s^2}{4}$	$(p-2)$	
(16″)	$s_3' \equiv as_3$	$(p-2)$	(15)

Forts.: Abschätzungen

Sei $p \geq 79$. wegen

(17) $$j = k - \frac{k(k-1)}{p-1}$$

(17′) $$s^2 \geq 2p-1$$

$$\begin{array}{rcl} s^2 & \equiv & p^2 \quad \bmod p-1 (12) \\ s^2 & \equiv & 1 \ (p-1) \\ s^2 & = & p,\ 2p-1,\ 3p-2, \cdots \\ s^2 & \neq & p,\ \text{da } 4p-4 \nmid p^2-p \\ & & \text{also } s^2 \geq 2p-1 \end{array}$$

ist stets

(18) $$p-1 \big| k(k-1)$$

also bei $p \geq 79$ $k(k-1) \geq 78$

(19) $$k \geq 10$$

Ferner

(20) $$k(k-1) \geq p-1$$

(21) $$k^2 \geq p-1+k \geq p+9$$

(22) $$j \geq \frac{\sqrt{p+9}(p-\sqrt{p+9})}{p-1} > \frac{\sqrt{p}(p-\sqrt{p})}{p-1} \geq \sqrt{p}-1$$
$$\geq 9$$

Ferner

(23) $$j \leq \frac{\frac{p-1}{2}(\frac{p+1}{2})}{p-1} = \frac{p+1}{4}$$

Daher aus (1) [mit $j_2 \leq \frac{\frac{p-3}{2}\frac{p+3}{2}}{p-1}$]:

(24) $$a^2 < \frac{1}{14}p^{\frac{3}{2}}$$

Sonst: aus (1) mit $i_2 \leq \frac{p+1}{4} - 1$ und $j_3 \geq 5$

(25) $$a^2 < \frac{p^2}{169}, \ |a| < \frac{p}{12} = \frac{p}{12}$$

(26) $$j_1 j_2 \leq \frac{p+1}{4} \cdot \frac{p-7}{4} = \frac{(p-3)^2}{16} - 1 \text{ (da } s_2 \leq s_1 - 2, \ s_1 \leq \frac{p+1}{4}\text{)}$$
$$j_1 j_2 \leq \frac{p^2}{16}$$

(26′) $|b| \leq \frac{7}{6}p$ (3, 25)

(26″) $|c| \leq |a| + 1$ (4, 26′)

76/77

[*Die ganze Seite 77 ist durchgestrichen*]

77/78

Fall I: $a > 0, b \geq 2a$

für $i = 1, 2$ ist

$$\begin{array}{rcl} s_i p & > & s_1 s_2 = bp - 2as_3 > bp - 2ap \\ s_i & > & b - 2a > 0 \\ s_i^2 & > & (b-2a)^2 \\ j_i & < & \dfrac{p^2 - (b-2a)^2}{4(p-1)} \end{array}$$

$$\begin{array}{rcl} a^2 & = & \dfrac{j_1 j_2}{j_3} < \dfrac{[p^2 - (b-2a)^2]^2}{16(p-1)^2 \cdot 9} \\ a & < & \dfrac{p^2 - (b-2a)^2}{12(p-1)} \end{array}$$

$$p^2 - b^2 + 4ab - 4a^2 - 12a(p-1) > 0$$
$$p^2 - b^2 - 4a \underbrace{[-b + a + 3p - 3]}_{\geq a+p, \text{ da } b \leq 2p-3} > 0 \qquad (26')$$
$$b^2 < p^2 - 4a(a+p) < p^2 - 4ap$$
$$0 < b < p - 2a$$

Nun ist aber, wenn $ba > 0$:

$$|c| = \left|\frac{as_3 - b}{p}\right| \leq \left\{ \begin{array}{ll} |a| & \text{od.} \\ \frac{|b|}{p} & \end{array} \right\} \leq |a| \tag{27}$$

also ist in Fall I

$$|s'_3| = |b + 2c| < |p - 2a| + 2|a| = p, \quad j'_3 > 0$$

78/79

Fall II: $a > 0, b \leq 2a$
Wegen

$$b = \frac{s_1 s_2 + 2as_3}{p}$$

ist $b > 0$,

$$\begin{aligned} |s'_3| &\leqq |b| + 2|c| \leq 2|a| + 2|a| \quad (27) \\ &\leq \frac{p}{3} \qquad (25) \end{aligned}$$

also $j'_3 > 0$ und sogar

$$j'_3 = \frac{p^2 - s'^2_3}{4(p-1)} > \frac{\frac{8}{9}p^2}{4(p-1)} = \frac{2p^2}{9(p-1)} > \frac{2}{9}(p+1)$$

also in Fall II: $\frac{2}{9}(p+1) < j'_3 \leq \frac{1}{4}(p+1)$

Fall III: $a < 0, b > 0$

Wegen

$$b = \frac{s_1 s_2 + 2as_3}{p} > 0$$

ist

$$|b| < \frac{s_1 s_2}{p} < p - 2$$

Ferner

$$c = \frac{aS_3 - b}{p} < 0, \quad |c| < |a| + \frac{|b|}{p} \leq |a| + \underset{(26')}{\frac{7}{6}}$$

$$|s'_3| = |b + 2c| \leq \begin{cases} |b| < p \text{ oder} \\ |2c| < \frac{p}{6} + \frac{7}{3} < p \end{cases}$$

also $j'_3 > 0$ in Fall III

79/80

Fall IV $a < 0, b < 0$

$$b = \frac{s_1 s_2 + 2as_3}{p} < 0 \text{ gibt } |b| \leq \begin{cases} (2|a|s_3 - s_1 s_2)/p \text{ oder} \\ \left|\frac{2as_3}{p}\right| < \frac{p}{6} \end{cases}$$

also

$$\begin{aligned} |b| &< \frac{p}{6} \\ |c| &\leqq |a| + 1 \leq \frac{p}{12} + 1 \\ |s_3'| &\leq \frac{p}{3} + 2 \leq p, \end{aligned}$$

$j_3' > 0$ in allen Fällen I - IV, noch prüfen!

Also weitere Ungl.

(28) $$s_3' < p$$

(29) $$ac > 0$$

sonst

$$\begin{aligned} s_3' &= as_3 - (p-2)c \\ |s_3'| &> (p-2)|c| \geq p - 2 \rightarrow\leftarrow (28), \text{ denn } |c| \geq 1 \end{aligned}$$

Bew. f. $c \neq 0$:
Wäre $c = 0$, so

$$s_3' = b = as_3 = \frac{s_1 s_2 + 2as_3}{p}$$

nach (12) ergibt sich

$$a^2 s_3^2 \equiv s_3^2 \ (4p-4)$$
$$4p - 4 \big| (a^2 - 1)s_3^2; \ 4p - 4 \big| a^2 - 1$$
$$a^2 - 1 \geq 4p - 4$$

widerspricht $j_1 + j_2 = a^2 + j_3'$, wonach $a^2 < \frac{p+1}{2}$

(30) $$|b| \leq p - 3$$

in

$$\begin{aligned} \text{I sogar} &< p - 2a \\ \text{II sogar} &< \frac{p}{6} \\ \text{III sogar} &< p - 2 \\ \text{IV sogar} &< \frac{p}{6} \end{aligned}$$

(31) $$|c| \leq |a|$$

Bew: $c = \frac{as_3 - b}{p}$, $|c| \leq |a|\left|\frac{sb}{p}\right| + \left|\frac{b}{p}\right| < |a| + 1$.

(32) $$j_3' \leq j_1 + j_2 \quad (17, 31)$$
$$p^2 + s_3' \geq s_1^2 + s_2^2$$

80/81

Forts: P-Gr vom Grad p

1. Sind die Bezeichnungen k und l für die Längen der Tra Systeme von $\mathfrak{H}$ in Darst $\mathfrak{G}_2$ so gewählt, daß $n = |\mathcal{N}P : P|$ Teiler von k ist, so ist $\mathfrak{H} \cap \mathfrak{K}$ vom Index pl in $\mathfrak{G}$.
   Bew: Index p^k geht nicht wegen 2:

2. Für jeden Primteiler q von n enthält $\mathfrak{H} \cap \mathfrak{K}$ jede q-Sylow Gruppe $\mathfrak{Q}$ von $\mathfrak{G}$, welche $\mathfrak{N}_1$ nichttrivial schneidet. Dabei ist angenommen, dass $\mathfrak{N}_1$ elementweise in sich übergeht bei $\mathfrak{G}_1 \to \mathfrak{G}_2$, denn $\mathfrak{Q}$ hat in Darst. $\mathfrak{G}_2$ einen Fixpunkt α, $\mathfrak{N}_1 \cap \mathfrak{Q}$ hat einen einzigen, 1, also ist $\alpha = 1$, und der bleibt bei $\mathfrak{G}_1 \to \mathfrak{G}_2$ fest wegen $\mathfrak{N}_1$ elementweise in sich übergeht.

3. Nicht jede q-Sy-Gr von $\mathfrak{G}_1$ zu $q \mid n$ kann im $\mathfrak{G}_2$ - Bild die Ziffer 1 fest lassen. Denn sonst $\mathfrak{G}_1$ als Normalisator ihres Erzeugnisses auch.

81/82

4. Wenn ein $\mathfrak{G}_1$ das unter UQ invariant ist (wo $P^Q = P^{-1}$) noch ein weiters V gestattet, so daß $g^V \in \mathfrak{S}^p$, so bleibt g^U invar. unter $V^*UQV = UV^{*2}Q$, also gestattet $\begin{cases} \mathfrak{G}^U & V^{*2}U \sim W \\ \mathfrak{G} & UV^* = aW + bP \end{cases}$
   Dann ist $V^*U = VW$ (bei passen. Normierg W) $\Rightarrow UU^* = WW^*$, (wobei $\mathfrak{G}^V$ W gestattet, $W = \sum{}' P^i$).

$$\begin{tikzcd} \mathfrak{G} \circ \arrow[r, "U"] \arrow[d, "V"'] & \circ\ \mathfrak{G}^U \\ \mathfrak{G}^V \circ \arrow[r, "W"'] & \circ\ \mathfrak{G}^{VW} = \mathfrak{G}^{V^*U} \arrow[u, "V"'] \end{tikzcd}$$

   Dann ist
$$V^*(U + W^*) \text{ hermitesch}$$
   Forts: 82 und XVI 51ff.

82/83

Forts: PGr vom Gr p

5. Man könnte die Permutationen, die mit UQ vertauschbar sind, nach Schurs Vorgang mittels Polynom - Darstellungen untersuchen; oder die $U = \sum{}' P^i$ darstellen durch $u(x) \mod p$ und $(1-x)^p$ (oder $(1-x)^{p-1}$), und so $UV = U^*W$ diskutieren
   Forts: 241, XVI 51

83/84

Aufgabe $\lhd\lhd$

Mit Hilfe von Tamaschkes Theorie den Verband derjenigen subnormalen Untergruppen von G untersuchen, die unter einer gegebenen Autom.-Gruppe A von G invariant sind.

Lit. Verlagerung:

Higman, Canad JM. 5 (1953) 477
Kochendörffer J Austral Math Soc <u>3</u>, 63-65
Zappa Mathematiche, Catania <u>13</u>, 61-64 (1959)

Frage: $\lhd\lhd$ $\qquad |\mathfrak{G}| \leq \infty$

Tritt jeder Kompfaktor von $\mathfrak{A}\mathfrak{B}$, wo $\mathfrak{A}, \mathfrak{B} \trianglelefteq \mathfrak{G}_1$ schon in $\mathfrak{A}$ oder $\mathfrak{B}$ auf? Dann wäre die Menge $\mathfrak{E}_\Lambda$ der Gruppen, die nur Komp f. aus Λ haben, wohl subnormal persistent. Wd!

84/85

1 Forts: ja. Man kann auch Hauptfakt unters.: genauer 3
  Aufgabe die subnormalen Ugruppen der charakteristisch einfachen Gruppen. Sind sie etwa normal?

2 Frage: Wenn A Erzeugnis subnormaler Ugr von $\mathfrak{G}$ ist, und nicht normal, gibts dann ein $g \in G$ mit $A \neq A^g \leq \mathcal{N}A$? Das wäre nützlich in Verbdg mit Zorn

21/6/63 3 Ist $G = \langle A_i \rangle$, $A_i \in \mathfrak{S}G$, so enthält jeder (subnormale, $\neq 1$) Ausschnitt von G einen von einem A_i. Dann die Eigenschaft $\mathfrak{E}(X)$: „Jeder Ausschnitt von X enthält einen Ausschnitt eines A_i“ ist persistent

4. NB: Eins der A_i braucht nicht $\lhd\lhd$ G zu sein, die anderen brauchen nur “schwach subnormal” zu sein, dh. Erzeugnisse subnormaler.

85/86

5. Zwei schwach subnormale Ugr, die keinen zyklischen Ausschnitt $\neq 1$ isomorph haben, sind elementweise vertauschbar.

6. Frage: Ist eine charakteristisch einfache Gruppe, die einen zyklischen Ausschnitt hat, abelsch?

7. Man könnte $\mathfrak{G}$ dann auflösbar nennen, wenn jeder (subn.) Ausschnitt von $\mathfrak{G}$ einen abelschen Ausschnitt enthält.
   Frage: Ist jede Untergruppe einer auflösbaren Gruppe auflösbar?
   Sind Bolkers "aufl Gruppen" in diesem Sinn auflösbar? vgl. Russe: AMS Transl. (2) 17

Def 8. $\mathfrak{A} \lhd \lhd \lhd \mathfrak{G} \mathrel{-\!\!\star\!\!-} \mathfrak{A} = \langle \mathfrak{A}_i \rangle,\ \mathfrak{A}_i \lhd\lhd \mathfrak{G}$

Frage: Gilt $\mathfrak{A} \lhd \lhd \lhd \mathfrak{B} \lhd \lhd \lhd \mathfrak{G} \succ \mathfrak{A} \lhd \lhd \lhd \mathfrak{G}$?
Gilt $\mathfrak{A} \lhd \lhd \lhd \mathfrak{G},\ \mathfrak{B} \lhd \lhd \lhd \mathfrak{G} \succ \mathfrak{A} \cap \mathfrak{B} \lhd \lhd \lhd \mathfrak{G}$?

86/87

26.6.63 Ausschnitte

(1) G Gruppe: $A \sqsubseteq G \mathrel{-\!\!\star\!\!-} A = Z/N,\ N \trianglelefteq Z \leq G$

(2) $A_i \sqsubseteq G \mathrel{-\!\!\star\!\!-} \bigcap A_i := \frac{Z}{N}$
$A_i = Z_i/N_i$; mit $Z = \bigcap Z_i,\ N = \prod (Z \underset{\substack{\uparrow \\ \text{mengen-} \\ \text{theor.}}}{\cap} N_i)$
NB: Für $A_i \leq G$ ist $\bigcap A_i =$ mengentheoret. Bedeutung
Für $A_i = G/N_i$ ist $\bigcap A_i = \prod G/N_i$ die $g \cdot g$ Faktorgruppe

(3) $A \cap B = B \cap A$

(4) $(A \cap B) \cap C \neq A \cap (B \cap C)$ i.a.
Bew: $|G| = 4$; $\exp 2$. $|A| = |B| = |C| = 2$.
$$\left.\begin{array}{lcl} G/A \cap [G/B \cap C] & = & G/A \cap C = C \\ [G/A \cap G/B] \cap C & = & G/G \cap C = C/C \end{array}\right\} \neq$$

(5) Def: $Z_1/N_1 \leq Z_2/N_2 \mathrel{-\!\!\star\!\!-} Z_1 \leq Z_2,\ N_1 \geq N_2 \cap Z_1$

(6) $\cdots \mathrel{-\!\!\star\!\!-} Z_1/N_1 \cap Z_2/N_2 = Z_1/N_1$

87/88

(7) $1 = \min \alpha$ (Ausschnitte von $\mathfrak{G}$), $G/1 = \max \alpha$.

(8) $Z_1/N_1 \leq Z_2/N_2 \leq Z_3/N_3 \succ Z_1/N_1 \leq Z_3/N_3$

(9) $\bigcap A_i/B_i \leq A/B \leq A_i/B_i \succ A/B = \bigcap A_i/B_i$.

(10) Verallg. der Projektion:
Sei $N \leq Z \leq G$ (nicht $N \trianglelefteq Z$!)
$H \leq G$
Setze $H \neg Z/N :=$ Gesamtzahl d N Kl zN, die El'e von H enth.
$:= (H \cap Z)N/N$

(11) Dann schon gilt: Sei $K \leq H$.
$H \neg Z/N = K \neg Z/N \Leftrightarrow Z \neg H/K = N \neg H/K$ nämlich $\Leftrightarrow H \cap Z \leq NK$.

88/89

$\triangleleft\triangleleft \quad \infty$

1) G perfekt, $\in$ Min sub, $G = \langle AB \rangle$, $A, B \triangleleft\triangleleft G \quad \succ \quad G = A_G B_G$
(Kerne) $= \bigcap A^g, \ldots$
Bew: Wähle B_0 bei festem A minimal mit $B_0 \trianglelefteq \triangleleft B$, $G = (A, B_0)$;

$$\begin{aligned} G &= A^G B_0 \\ G &\equiv B_0 \quad (A^G) \qquad B_0 \triangleleft B_1 \triangleleft \cdots \triangleleft G \\ G = (G,G) &\equiv (B_0, B_0^{b_2}) \;\; (A^G) \\ &\equiv (\underbrace{B_0 \cap B_0^{b_2}}_{=B_0 \text{ wegen Minimalität von } B_0}) \;\; (A^G) \end{aligned}$$

$$B_1 = B_0^{B_2} = B_0 \qquad B_0 \triangleleft B_2 \qquad B_0 \triangleleft G$$

$$\begin{aligned} G &\equiv A^G \;\; (B_0) \\ &\equiv A^{A^G} \;\; (B_0) \\ &\vdots \\ &\equiv A \;\; (B_0) \\ G &= AB_0 = AB_G \end{aligned}$$

ebenso weiter $= A_G B_G$

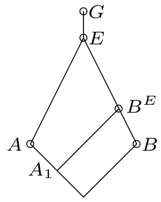
1′) Erzeugnis statt $G \in$ Min sub: $A \cap B \in$ min sub; nach Hall $\Rightarrow G \in \cdots$

89/90

Methode: 2) Allgemein sollte man mit dieser Methode perfekte (Sub-)Normalteiler von Produkten (sub-) normaler Ugr von $\mathfrak{G}$ untersuchen.

(3) Folgt aus $A_i \trianglelefteq\trianglelefteq G$, A_i perfekt $\langle A_i \rangle = \prod A_i$? Dabei kann Betrachtung des maximalen Normalteilers von $\langle A_i \rangle$ in $\prod A_i$ von Nutzen sein.

#4) Sei $A, B \trianglelefteq\trianglelefteq G$, $A \cap B = 1$; Beh $A^B \cap B^A$ enthält keine abelsche subnor
(Elementweise Vertauschbarkeit) Ugr $\neq 1$ von $\mathfrak{G} \;-\!\!\!\ast\!\!\!-\; (A, B) = 1$
Bew: $<$ klar
$>$ Indukt $n = [E : A] + [E : B]$, wo $[\ ]$ = Tiefe, $E = \langle AB \rangle$
$n = 0, 1, 2$ klar
$n > 2$, etwa $[E : B] > 1$, $B \ntrianglelefteq E$:



$A_i := A \cap B^E = A \cap B^A$
$[B^E : A_i] \leq [E : A]$, $[B^E : B] = [E : B] - 1$
$A_1 \lhd\lhd G$, da $\lhd A$.
abel $S \lhd\lhd G_1 A_1\ B_1 B^{A_1} \succ S \lhd\lhd G$, $S \lhd\lhd A^B \cap B^A \succ S = n$
Indukt: $(A_1, B) = 1 = (A_1, B^A) = (A_1, B^E)$
A_1 abelsch, $A \lhd E$, $G \leq A^B \cap B^A \succ A_1 = 1$
Hieraus folgt $\langle A, B^E \rangle = E\ A \cap B^E = 1$; $A^E \cap B^E$ hat keine abelsche subnor
Ugr von G, daher $(A, B^E) = 1$ (Indukt), $(A, B) = 1$

90/91

5) $A, B \trianglelefteq\trianglelefteq G$, $A \cap B = 1$, $\langle A, B \rangle = E$, $A^E \cap B^E$ enthält keine subnor abelsche Gr. $\neq 1 \Rightarrow (A, B) = 1$
Bew: in 4) wähle E für G.

7 Gedanke zur Behandlung von $\mathfrak{E}S\mathfrak{G}$ = Menge der Erzeugnisse subn Ugr von $\mathfrak{G}$:
$\mathfrak{E} \in \mathfrak{E}S\mathfrak{G} \succ [\mathfrak{G} : \mathfrak{E}] = \min \max{}_i [\mathfrak{G} : \mathfrak{A}_i]\ \langle \mathfrak{A}_i \rangle = \mathfrak{E}$
Es ist $[\mathfrak{G} : \mathfrak{E}] = 1 \;-\!\!\!\ast\!\!\!-\; \mathfrak{E} \trianglelefteq \mathfrak{G}$
Es ist $[\mathfrak{G} : \mathfrak{E}] \leq \infty$

8. Die richtige Verallgemeinerung der subnor. Ugr sind vielleicht die endlichen Durchschnitte von Erzeugnissen unendlich vieler Subnormaler Ugr.

91/92

9. Das Erzeugnis endlich vieler (n) endlicher subnormaler Ugr. ist subnor. und endlich.
Bew: Indukt. n.
Für $n = 2$: Ind min $[\mathfrak{G} : \mathfrak{A}_1]$, $[\mathfrak{G} : \mathfrak{A}_2]$

9′. Aufgabe: Schranke für Ord & Tiefe des Erzeugnisses angeben.

10. In einem Erzeugnis beliebig vieler endlicher subnormaler Ugr'en hat jede endliche Ugr eine endliche subnormale Hülle.

11. Ist $H \leq G$ und gibt es unter den in H gelegenen $A \trianglelefteq\trianglelefteq G$ eine maximale M, so ist $M \trianglelefteq H$, und M enthält jede subnor. Ugr von G in H.
Forts: 100

92/93

Arith. Str. zusg. Gruppen 13.7.63

1. Seien $\mathfrak{H}_1, \mathfrak{H}_2$ w-Untergruppen der endl. Gruppe $\mathfrak{G}$. Für eine Komp-Reihe $\mathfrak{G}_i$ von $\mathfrak{G}$ sei $\forall_i$ $\mathfrak{H}_1 \neg \mathfrak{G}^i$ konj zu $\mathfrak{H}_2 \neg \mathfrak{G}^i$ und dies eine maximale w-Ugr von $\mathfrak{G}^i$. $(i = 1, 2, \cdots)$
Damit gilt das Gleiche für jede K Reihe von $\mathfrak{G}$.
[NB: Analog für HauptR. und charakt. Reihen.]
Bew: Es genügt $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2$ zu betrachten
Der Witz ist: $\mathfrak{H}_i \neg \mathfrak{G}_2 = \mathfrak{H}_i \mathfrak{G}_1 \cap \mathfrak{G}_2$ das zeigt: Sind $\mathfrak{H}_i \neg \mathfrak{G}^1$ konj in $\mathfrak{G}^1$, so $\mathfrak{H}_i \mathfrak{G}_1$ konj in $\mathfrak{G}$, also unter $\mathfrak{G}_2$, daher $\mathfrak{H}_i \cap \mathfrak{G}_2$ konj in $\mathfrak{G}_2$.
Dass auch $\mathfrak{H}_i \neg \mathfrak{G}^2 = (\mathfrak{H}_i \cap \mathfrak{G}_1)\mathfrak{G}^2$ konj in $\mathfrak{G}_1$ ist klar.

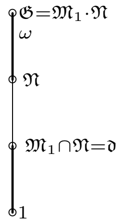
1'. Entsprechend für $\mathfrak{H}_1 \neg \mathfrak{G}^i = \mathfrak{H}_2 \neg \mathfrak{G}^i$ statt Konjug.

2. Wenn sogar die $\mathfrak{H}_{1,2} \neg \mathfrak{G}^i$ konjugiert in ihrem Erzeugnis sind $\mathfrak{H}_1$, $\mathfrak{H}_2$ konj. in ihrem Erzeugnis $\mathfrak{E}$.
Bew: oBdA $\mathfrak{G} = \mathfrak{E}$ $\mathfrak{G}^* \triangleleft \mathfrak{G}$; Ind: $\mathfrak{H}_i^* = \mathfrak{H} \cap \mathfrak{G}^*$ konj in $\mathfrak{G}^*$
oBdA $\mathfrak{H}_1^* = \mathfrak{H}_2^*$ $\quad \overline{\mathfrak{G}} = \mathcal{N}\mathfrak{H}_2^*$ in $\mathfrak{G}/\mathfrak{G}^* \neg \overline{\mathfrak{G}}$ sind $\overline{\mathfrak{H}}_1$, $\overline{\mathfrak{H}}_2$ konj.

93/94

3. Def: $\mathfrak{M} \in \underset{\substack{\uparrow \\ \text{extremal}}}{\mathfrak{E}_\omega} \mathfrak{G} \;-\!\!\star\!\!-\; \mathfrak{M}$ ist ω-Gr. v. $\mathfrak{G}$ und keine ω-Gr. $\overline{\overline{\mathfrak{M}}}$ von $\mathfrak{G}$ hat Ordng, die echtes Vielf. v. $|\mathfrak{M}|$
NB: Kann wohl weiter gefaßt werden: Es soll keine ω-Gp in $\mathfrak{G}$ geben, die die gleichen KFG wie $\mathfrak{M}$ hat und noch ein paar primzahllge dazu, dann wäre z.B. jede max aufl ω-Gp "extremal".

4. Sei $1 < \mathfrak{N} \triangleleft \mathfrak{G}$, $\mathfrak{M}_1 \in \mathfrak{E}_\omega \mathfrak{G}$ $(i = 1, 2)$ [$i = 1$ genügt, denn $i = 2$ **???**]
Sei $\mathfrak{M}_1 \cap \mathfrak{N} = \mathfrak{M}_2 \cap \mathfrak{N}$ & $\mathfrak{M}_1 \mathfrak{N} = \mathfrak{M}_2 \mathfrak{N}$
Dann $\mathfrak{M}_1 = \mathfrak{M}_2^G$ für ein $G \in \mathfrak{G}$.
Bew: $\overline{\mathfrak{G}} = \mathcal{N}(\mathfrak{M}_1 \cap \mathfrak{N}) \geq \mathfrak{M}_1, \mathfrak{M}_2$
oBdA $\overline{\mathfrak{G}} = \mathfrak{G}$: $\mathfrak{M}_1 \cap \mathfrak{N} \trianglelefteq \mathfrak{G}$ & $\mathfrak{M}_i \mathfrak{N} = \mathfrak{G}$



Nun ist $|\mathfrak{N} : \underbrace{\mathfrak{M}_1 \cap \mathfrak{N}}_{\mathfrak{d}}|_\omega = 1$ sonst könnte man mittels des Normalisators einer p-Sy $\mathfrak{N}/\mathfrak{d}$ noch größere ω-Ord erzielen, die ein Vielfaches der alten ist.

allgem: 10

Frage: Entsprechend für längere Normalketten?

94/95

5. Def: $\mathfrak{H} \in \omega$- Mi $\mathfrak{G}$ (w-minimal)
wenn $\mathfrak{H}$, aber keine echte Ugr von $\mathfrak{H}$, zu jedem $p \in \omega$ eine p-Sy $\mathfrak{G}$ enthält.

6. $\mathfrak{H} \in \omega$- Mi $\mathfrak{G}$ hat "Eigenschaft D", also $S\mathfrak{G} \to S\mathfrak{H}$ Homo.

Frage 7. Sei $\mathfrak{N} \lhd g$, und $\mathfrak{G}/\mathfrak{N} \in \mathfrak{E}_\omega(\mathfrak{G}/\mathfrak{N})$. Sei $|\mathfrak{N}|_\omega = 1$. Sind dann je zwei Komplemente von $\mathfrak{N}$ in $\mathfrak{G}$ konjugiert?
ObdA kann man $\mathfrak{N}$ als p-Gruppe annehmen beim Beweis.

Satz 8. Zwei ω-Hall-Gruppen, die dieselben Projektionen auf eine Normalkette $\{\mathfrak{G}_i\}$ von $\mathfrak{G}$ haben, sind konjugiert.
Bew: (4) $\mathfrak{H}_i \cap \mathfrak{G}_1$ ist ω-extremal in $\mathfrak{G}_1$.

Frage 9: Ist der Schnitt einer maxim. aufl. ω-Ugr $\mathfrak{H}$ von $\mathfrak{G}$ [kurz: $\mathfrak{H} \in \mathcal{MA}\omega\mathfrak{G}$] jeden Normalteiler von $\mathfrak{G}$ in einer Gruppe aus $\mathcal{MA}\omega\mathfrak{N}$?

95/96

9a Das wäre zu bejahen, wenn folgendes gilt: eine aufl. ω-Gr a von Autom von $\mathfrak{G}$ läßt stets eine ω-Gr $\neq 1$ von $\mathfrak{G}$ fest, wenn $|\mathfrak{G}|_\omega \neq 1$.

10. Sei $\mathfrak{H}_1 \neg \mathfrak{G}^i = \mathfrak{H}_2 \neg \mathfrak{G}^i$ eine ω-Gp $(i = 1, \cdots, 5)$ die in ihrem Normalisator in $\mathfrak{G}^i$ kurz: $\to$ einen Index hat, der zu ω fremd ist.
"große ω-Gp" Dann ist $\mathfrak{H}_1 = \mathfrak{H}_2^G$.
Bew für $s = 2$ wie 4, dann Indukt.

11. Die Vor von 10 ist für $s = 2$ und $\mathfrak{H}_1 \in \mathfrak{E}_\omega\mathfrak{G}$ (vgl 4) erfüllt.

12. Vorschlag zur Bezeichnung:

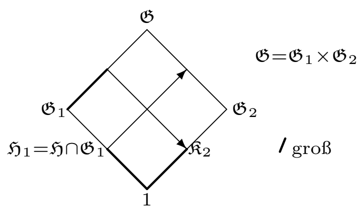
$$\begin{aligned}
\mathcal{J} &= \text{intravariant} \\
\mathcal{M} &= \text{"maximal"} \\
\mathcal{A} &= \text{"auflösbar"} \\
\omega &= \text{"}\omega\text{-Gp} \\
\mathcal{H} &= \text{"Hall"} \\
\text{"faktoriell"} = \mathcal{F} &= \text{"abelsch auf alle Faktoren von } \mathfrak{G}\text{"} \\
\mathcal{G} &= \text{"groß"}
\end{aligned}$$

z.B. $\mathfrak{H} \in \mathcal{F}\mathcal{G}\omega\mathfrak{G}$ heißt: jede Projektion von $\mathfrak{H}$ in Faktor $\mathfrak{F}$ von $\mathfrak{G}$ ist eine ω-Gp, die in Norm in $\mathfrak{F}$ einen Index prim zu ω hat.

96/97

13) $\mathfrak{H}\neg\mathfrak{G}^i \in \mathcal{H}\omega\mathfrak{G}^i \Rightarrow \mathfrak{H} \in \mathcal{H}\omega\mathfrak{G}$.

14) Ist für <u>eine</u> Kompreihe $\mathfrak{G}^i$ stets $\mathfrak{H}\neg\mathfrak{G}^i \in \mathcal{H}\omega\mathfrak{G}^i$ so gilt das für jede KR. von $\mathfrak{G}$.
genügt:



[Genügt zu zeigen: $\mathfrak{H} = (\mathfrak{H} \cap \mathfrak{G}_1) \times (\mathfrak{H} \cap \mathfrak{G}_2)$]
Beweis: $\mathfrak{K}_2 := \mathfrak{H}\mathfrak{G}_1 \cap \mathfrak{G}_2 \trianglelefteq \mathfrak{H}\mathfrak{G}_1$
$\mathfrak{K}_2$ ist $\in \mathfrak{H}\omega\mathfrak{G}_2$.
$\mathfrak{H} \leq \mathcal{N}\mathfrak{K}_2 : \mathfrak{H}\mathfrak{K}_2\omega$ Gp

$\mathfrak{C} := \mathfrak{H}_0\mathfrak{K}_2 \leq \mathcal{N}\mathfrak{H}_1,\ \mathfrak{C} \cap \mathfrak{G}_1 \leq \mathcal{N}\mathfrak{H}_1\ \ \mathfrak{C} \cap \mathfrak{G}_1\ \ \omega$-Gp
$\mathfrak{C} \cap \mathfrak{G}_1 = \mathfrak{H}_1$ wegen $\mathfrak{H}_1 \in \mathfrak{C}\omega\mathfrak{G}_1$
$\mathfrak{C}\neg\mathfrak{G}/\mathfrak{G}_1 = \mathfrak{H}_2\mathfrak{G}_1/\mathfrak{G}_1 \leq \mathfrak{H}\mathfrak{G}_1/\mathfrak{G}_1 \quad \mathfrak{H} \leq \mathfrak{C}$
$\mathfrak{C} = \mathfrak{H} \succ \mathfrak{K}_2 \leq \mathfrak{H}$
$|\mathfrak{H}_1 \times \mathfrak{K}| = |\mathfrak{H}|.\ \ \mathfrak{H} = \mathfrak{H}_1 \times \mathfrak{K}$ dann $\nearrow$

(14′) $\mathfrak{H} \in \mathcal{F}\mathfrak{H}\omega\mathfrak{G} \succ \mathfrak{H} \underset{D}{\leq} \mathfrak{G}$.

(15) Ist für eine K-Reihe $\mathfrak{G}^i$ stets $\mathfrak{H}\neg\mathfrak{G}^i \in \mathfrak{H}\omega\mathfrak{G}^i$, so $\mathfrak{H} \in \mathcal{F}\mathfrak{H}\omega\mathfrak{G}$; und wenn $\mathfrak{K}\neg\mathfrak{G}^i = \mathfrak{H}\neg\mathfrak{G}^i$, so $\mathfrak{K} \underset{\substack{\mathfrak{G} \\ \uparrow}}{=} \mathfrak{H}$
„konjug. in $\mathfrak{G}$“

97/98

(16) Insbes. ist $\mathcal{M}\mathcal{A}\omega \leq \mathcal{H}\omega$ daher gelten 14,15 auch für $\mathcal{F}\mathcal{M}\mathcal{A}\omega\mathfrak{G}$

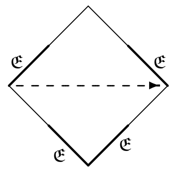
(17) Ordnet man die $p_i \in \omega$ in bestimmter Weise, ist jede $\{p, \cdots\}$ - Sylow-Normalisator Turmgruppe $\in \mathfrak{I} \cap \mathcal{H}\omega$; sie sind selbskonjugierend und man kann in jedem einfachen Faktor von $\mathfrak{G}$ eine solche beliebig wählen und dann zu einem $\mathfrak{H} \in \mathcal{F}\mathfrak{I}\mathcal{H}\omega\mathfrak{G}$ zusammensetzen und alle $\mathfrak{H}$ sind konjugiert.

(18) Wenn Vermutung 9a stimmt, ist $\mathcal{M}\mathcal{A}\omega \subseteq \mathcal{F}\mathcal{H}\omega$

(19) Nicht ist $\mathcal{MA}\omega \subseteq \mathfrak{I}$ z.B: $\mathfrak{G}_{168}$ $\quad \omega = \{2,3\}$
$\circledast$ Für unendliche Gruppen: Man könnte $0 \in \omega$ zulassen, so von Torsionsgruppen wegkommen

98/99

(20) Sei $\mathfrak{E}$ eine Klasse von Untergr. einer Gruppe $\mathfrak{G}$ ($\mathfrak{G}$ laufend) derart, daß
$\mathfrak{H} \neg (\mathfrak{A} \times \mathfrak{B})/\mathfrak{A} \in \mathcal{C}\ \mathfrak{A} \times \mathfrak{B}/\mathfrak{A}$
$\mathfrak{H} \cap \mathfrak{A} \in \mathcal{C}\mathfrak{A}$



folgt: dasselbe mit Vertauschung $\mathfrak{A} \leftrightarrow \mathfrak{B}$. Dann folgt aus $\mathfrak{H} \neg \mathfrak{G}^i \in \mathcal{C}\mathfrak{H}^i$ für eine Komposition$R$ (oder Haupt$R$:) dasselbe für jede.

(21) Wenn sogar gilt

$$\left.\begin{array}{ll} \mathfrak{H}\neg\{\mathfrak{A} \times \mathfrak{B}/\mathfrak{A}\} & \in \mathcal{C}\{\} \\ \mathfrak{H} \cap \mathfrak{A} & \in \mathcal{C}\mathfrak{A} \end{array}\right\} \mathfrak{H} = \mathfrak{H} \cap \mathfrak{A} \times \mathfrak{H} \cap \mathfrak{B}$$

so hat jede Gruppe $\mathfrak{H} \in \mathcal{F}\mathfrak{G}$ die Distributivitätseigenschaft

$$\mathfrak{H} \in \mathcal{D}\mathfrak{G} : \quad \mathfrak{H} \cap \langle \mathfrak{A}_i \rangle = \langle \mathfrak{H} \cap \mathfrak{A}_i \rangle$$

wenn $\mathfrak{A}_i \lhd\lhd \mathfrak{G}$

(22) Für unendliche Gruppen könnte nützlich sein der Begriff der
<u>lokalen Konjugiertheit:</u>
A zu B in G lok. konj. $\Leftrightarrow$ zu jeder endl. erzeugten (oder: endlichen) Ugr A' von A $\exists g \in G : A'^g \subseteq B$ und dasgl für $B' \leq B$.

99/100

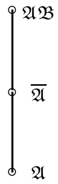
16.7.63 $\qquad \lhd\lhd$ Forts. von S. 92

(1) $\mathfrak{A}, \mathfrak{B} \lhd\lhd \mathfrak{G}$, $\mathfrak{AB} = \mathfrak{BA}$,
$\mathcal{S}\mathfrak{B}$ erfüllt die Max-Bedgg $\succ$ $\mathfrak{AB} \lhd\lhd \mathfrak{G}$ allgemeiner 2
Bew: sonst $\exists \mathfrak{C}_n \nearrow$, $\mathfrak{A} \leq \mathfrak{C}_n \lhd\lhd \mathfrak{G}$, $\mathfrak{C}_n \leq \mathfrak{AB}$ $\mathfrak{C}_n = \mathfrak{A} \cdot (\mathfrak{C}_n \cap \mathfrak{B})$; $\mathfrak{C}_n \cap \mathfrak{B} \nearrow$
W!

(1′) Es genügt: die { Subn Ugr von $\mathfrak{B} \geq \mathfrak{A} \cap \mathfrak{B}$} erfüllt die Max. Bedgg.

(2) Satz: $\mathfrak{A}, \mathfrak{B} \lhd\lhd \mathfrak{G}$, $\mathfrak{A}\mathfrak{B} = \mathfrak{B}\mathfrak{A} \succ \mathfrak{A}\mathfrak{B} \trianglelefteq\trianglelefteq \mathfrak{G}$
Bew: Indukt $t(\mathfrak{A}, \mathfrak{A}\mathfrak{B}) = n$

$n = 1:\ \mathfrak{A} \lhd \mathfrak{A}\mathfrak{B}$ bekannt
$n > 1:$



$$\begin{aligned}
\overline{\mathfrak{A}} &:= \mathfrak{A}^{\mathfrak{A}\mathfrak{B}} \\
&= \mathfrak{A} \cdot \underbrace{(\overline{\mathfrak{A}} \cap \mathfrak{B})}_{\substack{\overline{\mathfrak{B}} \lhd \mathfrak{B} \\ \overline{\mathfrak{B}} \lhd\lhd \mathfrak{G}}} = \mathfrak{A}\overline{\mathfrak{B}} \\
t(\mathfrak{A}, \mathfrak{A}\overline{\mathfrak{B}}) &= t(\mathfrak{A}, \mathfrak{A}\mathfrak{B}) = 1 \\
\succ \overline{\mathfrak{A}} \lhd\lhd \mathfrak{G} \succ\ & \mathfrak{A}\mathfrak{B} \lhd\lhd \mathfrak{G}
\end{aligned}$$

Noch allgemeiner: (7)

3) Frage: Erzeugen endlich viele A^g eine subn. Ugr wenn $A \lhd\lhd G$?

4) Frage: Welche $B \in \mathcal{S}G$ haben die Eigenschaft:

$$A \lhd\lhd G \succ \langle A, B\rangle \lhd\lhd G?$$

100/101

5) Sei $A, B \lhd\lhd G$ stets vorausg.

$$\langle A, B\rangle \lhd\lhd G \Leftrightarrow A^B \lhd\lhd G$$

6) $t(A, G) \leq 2 \succ \langle A, B\rangle \lhd\lhd G$

(7) Wenn $A, B \lhd\lhd G$ und $\langle A, B\rangle = ABA$, so $\langle A, B\rangle \lhd\lhd G$
Bew wie 4: $A^B =: \overline{A} = A\overline{B}A$ mit $\overline{B} = \overline{A} \cap B$

(8) Frage: Genügt auch $\langle A, B\rangle = (AB)^2$ oder sogar $= (AB)^n$?

(9) Seien $A, B \lhd\lhd G$. Beh:

$$\langle A, B\rangle \lhd\lhd G \Leftrightarrow A^B \lhd\lhd G \Leftrightarrow (A, B) \lhd\lhd G$$

(10) Def: A lokal subnormal in $G \Leftrightarrow$ Aus $E \leq A$, E endl erzeugt folgt $E \trianglelefteq\trianglelefteq G$
Frage: Eigenschaften?

101/102

(11) Wenn $G \in$ Min subn, so dürften meine Sätze über die Vertauschbarkeit von subn Ugr gelten. Jedenfalls ist dann, wenn $A \lhd\lhd G$, A/A' direktes Produkt endlich vieler p-Gruppen; A ist das Erzeugnis einköpfiger subnormaler. Tamaschkes Verbandstheorie übertragen.

(12) Frage: Was für eine Verbandsstruktur hat $\mathcal{S}\mathfrak{G}$ wenn $\mathfrak{G} \in$ Max sub?

(13) Frage: $\mathfrak{G} \in$ Min sub $\succ \mathcal{S}\mathfrak{G}$ Verband?
Gegenbeispiele wären wohl zunächst unter den p-Gruppen zu suchen. Stoff für Madison.

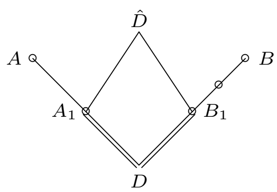
(14) Aufgabe: Subnormale Kerne und Hüllen unter der Vor $G \in M_{\text{in}}^{\text{ax}}$ sub untersuchen.

102/103

(15) $G \in$ Max sub; $D, A, B \lhd\lhd G$, $D \leq A \cap B \succ$ jeder Faktor von $\langle A, B\rangle$ über B enthält einen Faktor $\cong$ von A über D
Bew: Wähle Gegenbeispiele mit maximalem D

a) Wenn $D = A$ red. B, fertig
b) $D < \frac{A}{B}$

Wähle $A_1, B_1 \leq \mathcal{N} D \cap \frac{A}{B}$



Denn $B_1 \leq A$ fertig (Max alg D. Sei $B_1 \not\leq A \lhd\lhd G$. Ebenso $A_1 \not\leq B$ subnormal.
Denn $D < \widehat{D} := \langle A_1, B_1\rangle$
$\widehat{D} = A_1^{B_1} \cdot B_1$
$\{$Fakt $\widehat{D}$ bis $B_1\} \leq \{$ Fakt $A_1^{B_1}$ bis $D\}$, also

I: jeder Fakt $\widehat{D}$ bis B_1 enth Fakt A bis D. Nun bilde $\widehat{A} := \langle A, \widehat{D}\rangle$. Wegen $D < A_1 \leq A \cap \widehat{D}$ ist nach Max Eig D:

II Jeder Faktor von $\widehat{A}$ bis $\widehat{D}$ enth Fakt A bis A_1, also enth. Fakt A u D.
Nun $\langle A, B\rangle = \langle \widehat{A}, B\rangle$

III Jed Fakt $\langle A, B\rangle$ bis B enth Fakt $\widehat{A}$ bis B_1.

I+II+III genügt

103/104

Ansatz zum allg. Beweis von (15) ohne Max:
den Ausschnitt Z/N über B möglichst hoch schneiden. Man kann $N = B$ annehmen. Bei Annahme der Min Bedg für subn Ugr kann man annehmen $D = D_A$

(16) $A, B \trianglelefteq\trianglelefteq G$, $G = \langle A, B\rangle$. G/B^G perfekt, & $B \in \min \Rightarrow \exists$ minimal $A_1 \leq A \ni \langle A_1, B^G\rangle = G$ & $A_1 \trianglelefteq G$

104/105

Charaktere von p-Elementen in monomialen Darstellungen

(1) Sei $\mathfrak{G}$ endl Gruppe, $D(g)$ monomiale transitive Darst: $\mathbb{C}$ vom Grad n, h ein Element von p-Potenzordnung in $\mathfrak{G}$, k die Zahl seiner Konjugierten, $\chi =$ Sp $D(h)$, $\chi^0 =$ Sp $P(h)$ wo P die entsprechende tra. Permut-Darst von $\mathfrak{G}$ ist. Dann

$$\frac{k\chi}{n} \equiv \frac{k\chi^0}{n} \mod \mathfrak{p}$$

wo $\mathfrak{p}\big|p$ in $\mathbb{Q}(\chi)$.
Bew:

$$\begin{aligned} \frac{k\chi}{n} &= \text{Diagonalelement von } \sum_{h_1 \in \text{ Kl } h} D(h_1), \\ &\underset{\mathfrak{p}}{\equiv} \quad \cdot \quad \cdot \quad \sum P(h_1) = \frac{k\chi^0}{n} \end{aligned}$$

105/106

P-Gr mit reg Normalt.

In Diss Erber findet sich der Spezialfall $\mathfrak{G}$ aufl, $\mathfrak{U} = \mathfrak{G}_{12}$ des folgenden allgem. Satzes:
Enthält $\mathfrak{G}$ einen reg $\mathcal{N}T$ $\mathfrak{N}$, so sind je zwei Fixpkte α, β einer bel. Ugr $\mathfrak{H}$ von $\mathfrak{G}$ konjugiert unter $\mathfrak{N} \cap \mathcal{C}\mathfrak{H} = \mathcal{C}_{\mathfrak{N}}\mathfrak{H}$.
Bew: Sei $\alpha^N = \beta$, dann $\alpha^{NH} = \beta$, $\beta^{N^{-1}N^H} = \beta$; $N^{-1}N^H = 1$.
[$\mathfrak{G}^* = \mathfrak{H}\mathfrak{N}$ hat $\mathfrak{G}_1^* = \mathfrak{H}$ wenn $1 \in \phi\mathfrak{H}$. [Bew. durch Vergleich der Ord] in einer tra Gr $(\mathfrak{G}^*)$ sind daher je zwei $\alpha, \beta \in \phi\mathfrak{G}_1^*$ konjugiert unter $\mathcal{N}\mathfrak{G}_1^*$. Da $\mathcal{N}_{\mathfrak{G}^*}\mathfrak{G}_1^* = \mathfrak{G}_1^* \cdot \mathcal{N}_{\mathfrak{N}}\mathfrak{G}_1^*$ folgt der Satz.
Folge: In einer aufl pri Gr ist jede Gruppe mit ≥ 2 Fixp verschieden von ihrem Normalis. (in anderer Formulierung, allgemeiner aber gleichwertig, ="Satz von Taunt": $\mathfrak{G}$ endl, $\mathfrak{U} \leq \mathfrak{G}$, aus $\mathfrak{U} \leq \mathfrak{V} \leq \mathfrak{G}$ folgte $\mathcal{N}\mathfrak{V} = \mathfrak{V}$. Dann folgt aus $\mathfrak{U} \leq \mathfrak{V} \cap \mathfrak{W}^G$ auch $\mathfrak{V} = \mathfrak{V}^G$, $G \ni \mathfrak{V}$.

106/107

Selbstkonjugierende Untergruppen

(1) Df: $S \leq G$ $sC \iff \forall g \in G: \ S\text{cj}S^g$ in $\langle S, S^g\rangle$
$= \text{pronormal}$

(2) Thm: „Fixpunkte selbstkonjugierender Untergruppen“
Seien $S \le G, S$ sei in G, $T \le G$, $G = ST$, G acting on Ω
$\alpha, \beta \in \phi S$, $\beta \in \alpha^T$
Dann $\beta \in \alpha^{T \cap \mathcal{N}S}$
Bew: $\beta = \alpha^t$ $H := \langle S, S^t \rangle \le G_\beta =$ Fixgp
$\exists g' \in G' : S^{tg'} = S \quad tg' \le \mathcal{N}S$
$\alpha^{tg'} = \beta^{g'} = \beta$ aber $tg' \notin T$

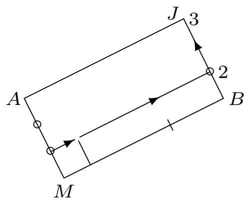
107/108

$S \le G' \le G = TS$
$g' = t_0 S$, $t_0 \in T \cap \langle S, S^g \rangle \le T_\beta$
besser
$t_1 := tt_0 \le T$
$S^{t'} = S^{tt_0} = S^{tg's^-} = S^{S^-} = S \quad t' \in \mathcal{N}S$
$\alpha^{t'} = \alpha^{tg'S^-} = \beta^{g'S^-} = \beta^{S^-} = \beta$
NB: Besonderer Beweis lohnt eigentlich nicht:
Bekannt ist $\exists n \in \mathcal{N}S : \alpha^n = \beta$. Nun $n = st$, $t \in \mathcal{N}S \cap N$, $\beta = \alpha^n = \alpha^{st} = \alpha^t$
(2) ist also nur Korallar zum allg. Satz über selfconj.

108/109

$\lhd\lhd \quad \infty$

(1) $A, B \trianglelefteq\trianglelefteq G$, $A \cap B = M$, von A bis M kein Faktor $p \Rightarrow AB = BA$ und jede Kette von A bis M entspricht einer Kette von AB bis B.
Indukt $d_A(M) + d_B(M) = s$
mit el'weise Vertb. bei $s = 2$



$\mathcal{Q}(A/M) \cong \mathcal{Q}(J/B)$

(2) Wenn keine subn-Reihe von G 3 mal denselben Primzahlindex hat, sind je zwei subn Ugr von G vtb.

(3) Vermutung: $A, B \lhd\lhd G$, $A \cap B = M$, $\langle A, B \rangle = J$

$$|A/M| = p^\alpha, \quad |B/M| = p^\beta \Rightarrow |J/M| = p^\gamma$$

Zum Beweis dürfte nützen

(4) $A, B \trianglelefteq\trianglelefteq G$, $|\langle A, B \rangle / A| < \infty \Rightarrow \langle A, B \rangle \trianglelefteq\trianglelefteq G$
(da $\langle A, B \rangle$ eine max in G subn Ugr oberhalb A enth.)

109/110

Fragen von D.G. Higman 20.10.63

Sei rk G = Anzahl der Bahnen von G_α, wo G eine primitive Gruppe.

(1) Ist die Struktur der minimalen Normalteiler N von G eingeschränkt durch Vorgabe von rk G?
z.B Anzahl der einfachen Faktoren, Primitivität von N

(2) Bahnlängen $1, k, k(k-1)$ sind für prim. G höchstens möglich, wenn $k = 5, 7, 57$.
Existieren Beispiele für $7, 57$?

(3) Wie verträgt sich rk $G = 3$ mit der Existenz von regulären Untergruppen? (Meth. von Schur)

110/111

$\lhd\lhd$ endlich (Frage: Auch ∞?)

$A \sim B$ bedeute: $A, B \trianglelefteq\trianglelefteq G$, perf. Kern A = perf Kern B

(1) $\langle (A \cap B), C\rangle \sim AC \cap BC$ Bew einköpf perf.

(2) $\langle A, B\rangle \cap C \sim \langle (A \cap C), (B \cap C)\rangle$

#(3) $\langle A, B\rangle = J \Rightarrow A^J \cap B^J \sim (A \cap B)^J$
Bew: Sei P einköpf perf, $P \leq A^J \cap B^J$. Diejenigen P^x, die $\not\leq A$ sind, werden von A fest gelassen (einzeln), und sie liegen in B. Wenn also kein $P^x \leq A \cap B$, so $\{P^x\} = Q + R$, wo $\substack{Q \text{ die in } A \\ R \text{ die in } B}$ gelegene P^x bezeichnet, $Q \neq \emptyset$, $R \neq \emptyset$ (wegen $P \in A^J \cap B^J$), mit R besteht aus den nicht in A gelegenen P^x, daher $R^A = R$. Aber nach Def von R ist auch $R^B = R$, daher $R^J = R$, also $R = R^J = \{P^x\}$, $Q = \emptyset \to\leftarrow$

#(4) $\langle A, B\rangle \sim \langle A_J, B_J\rangle$ mit $X_J = \bigcap X^j,\ J = \langle A, B\rangle$
Bew: P eink. perf., $P \leq J = \langle A, B\rangle$. Wäre $P \not\leq \langle A_J, B_J\rangle$, so $P \not\leq A^y$, $P \notin A^z$ für gewisse $y, z \in J$ also $P \not\leq \langle A^y, B^z\rangle = J_0$, $J_0 \trianglelefteq\trianglelefteq J$ aber $J_0^J = \langle A^{y^J}, B^{z^J}\rangle \geqq \langle A, B\rangle = J$ also $J_0 = J$

111/112

Allg:

(4′) $J = \langle A_1, \cdots, A_n\rangle \sim \langle A_{1_J}, \cdots, A_{n_J}\rangle$
Bew: Sei P eink perf $\leq J$. Wäre $P \not\leq$ rechte Seite, so $\exists x_i \in J \geq P \not\leq A_i^{x_i}$
$\Rightarrow P \not\leq J_0 = \langle A_1^{x_1} \cdots A_n^{x_n}\rangle$
$J_0 \lhd\lhd J$ aber $J_0^J \geqq \langle A_1 \cdots A_n\rangle = J$

(5) Wenn $J = \langle A_1, \cdots, A_n\rangle$, so $J = \langle A_1^{j_1}, \cdots, A_n^{j_n}\rangle \ \ \forall j_\nu \in J$

(5′) $\mathcal{S}G \in$ max, $\langle A_i \rangle_{i\in I} = J \Rightarrow \langle A_i^{j_i} \rangle = J$ denn r.S. $= J_0$ ist $\trianglelefteq\trianglelefteq J$, und $J_0^J = J$

(6) ohne alle Vor! A, B konj in $\underbrace{\langle A, B \rangle}_{J} \Rightarrow A = B$

Bew: $B = A^j \leq A^J$
$J = \langle A, B \rangle \leq A^J \quad J = A \quad B \leq A$ und umgek.

(7) Vertauschungssätze sollten erhältlich sein unter der Vor, dass die gemeinsamen p-Faktoren zentral sind in geeignetem Sinn.

112/113

$\lhd\lhd \quad \infty$

(1) $\langle A, B \rangle = J$; $A, B \trianglelefteq\trianglelefteq G$, $\mathcal{S}J$ lattice $A \dot\cap B$ loc imp (dh: $1 \neq F \leq A \cap B$, F fig $\Rightarrow F \neq F'$) $\Rightarrow A^J \cap B^J$ loc imp
Bew mit Induktion nach $d_J(A) + d_J(B)$ mittels

(2) „loc imp" is normally persistent

(3) Jede auflösb. Gr. im Sinn von Baer ist loc imp: dergl „lok aufl" ist loc imp

(4) Def: $\sum_0(G) = \{$ einfache Faktoren der endlich erzeugten Untergr. von $G\}$
(oder := { Köpfe der...}
Frage: Ist $\sum_0(A) \subseteq \mathcal{S}$ nor per?
NB: „loc imp" scheint nicht aufzutreten in Plotkins Bericht „Generalized soluble and generalized nilpotent groups", AMS Transl. (2)17, 29-116

(5) $\left.\begin{array}{l} B \trianglelefteq\trianglelefteq G, B = B', \langle a \rangle \trianglelefteq\trianglelefteq G \\ \text{rad } B = 1 \end{array}\right\} \Rightarrow a \in \mathcal{N}B$
Bew: Ind $d_G(B) : J = \langle a \rangle^J \cdot B$ mit $n = 1$, $B^J = R \cdot B \quad R = \text{rad } B^G$
nach Ind: $(B, R) = 1$, da $R \trianglelefteq B^J$
$B, B^g \leq ZsR$, clp R in B^G $B^g \leq B \cdot Z$ $Z = \mathcal{C}R$ $B^G = BZ \quad B = (B^G)' \lhd G$

113/114

endl. Perm.-Gr.
16.11.63

Satz 1: Sei G eine transitive Permgruppe des Grades n, und G_α habe die orbitlengths n_i, $\sum_{i=1}^{r} n_i = n$. (→ FPG Ex 3.13)
Sind alle $nn_i \equiv 1 \mod 2$ so ist $|G| \equiv 1(2)$.
Bew: Sei $|G| \equiv 0(2)$; zeige: $2 \big| n|\beta^{G_\alpha}|$ für pass $\beta \neq \alpha$.
Wähle $t = (\alpha\beta)\cdots \in G$. Setze $A = G_{\alpha\beta}$, $B = G_{\alpha\beta}\langle t \rangle$; $A \underset{2}{\lhd} B$, also $2 \big| |G/G_{\alpha\beta}| = nn_\beta$.

Allgemeiner:

Satz 2. Sei $p \Big| |G|$ und $p \nmid nn_1n_2\cdots n_r$. Dann $\exists G_p = p$-Sy G: $2\Big||\mathcal{N}G_p : G_p|$.
Bew: $t = (\alpha\beta)\cdots \in G$ $|\beta^{G_\alpha}| =: n_j$ Dann $\exists$ $G_p \leq G_{\alpha\beta} \underset{2}{\lhd} G\alpha\beta \cdot \langle t\rangle =: B$
$\mathcal{N}G_p/G_p$ deckt $B/G_{\alpha\beta}$. $\quad 2\Big||\mathcal{N}G_p/G_p|$

2′: Ist $|\mathcal{N}G_p : G_p|$ ($G_p = p$-Sy Gr S) ungerade für eine tra PGr G, und $2\Big||G|$, so $p \mid nn_j$ für ein j.

114/115

Satz 3: Sei T ein transitiver Konstituent einer Untergruppe U einer Perm Gr G, Träger $T = \Gamma \ni \alpha$. Seien $K, \cdots, L$ die tr-Konstituenten von G_α, die von Γ getroffen werden, und $K, \cdots, \Lambda$ ihre Träger. Dann $\langle G_\alpha, U\rangle \leq (G_{K\cup\cdots\cup\Lambda})_{\mathfrak{E}}$, wo $\mathfrak{E}$ die abstr. Komposfaktorgruppeen von $\Big(\underbrace{(G_{K\cup\cdots\cup\Lambda})^U}_{C}\Big)^{K\cup\cdots\cup L}$ bedeutet.
Bew: $C_{\mathfrak{E}} = (G_{K\cup\cdots\cup\Lambda})_{\mathfrak{E}}$

4. Ist G $(p-1)$-fach transitive (p Primzahl) und sind $n, n_1, n_2, \cdots$ die Grade von G und der tra Konst. von $G_{1,2,\cdots,p-1}$, so ist $p \mid n(n-1)\cdots(n-p+2)n_j$ für ein j.

115/116

Perm Gr & $\lhd\lhd$

Allg. Lemma:

(1) $C \overset{\Lambda}{\lhd\lhd} A_1 = A_1^A$
$C \overset{\Lambda}{\lhd\lhd} B_1 = B_1^B$
$\Rightarrow$ $C_\Lambda = C_\Lambda^A = C_\Lambda^B$
Bew: $C_\Lambda = A_{1\Lambda'} \trianglelefteq A$.

(1′) $C \overset{\Lambda}{\trianglelefteq\trianglelefteq} \begin{cases} A \\ B \end{cases} \Rightarrow \mathcal{N}(C_\Lambda) \geq \mathcal{N}A, \ \ \mathcal{N}B.$

116/117

Ordnung prim - P Gr.

(1) Ist G transitiv mit einem regulären Normalteiler R, vom Grade n, und läßt sich R durch r Elemente erzeugen, so gibt es $\Delta \subseteq \Omega$ mit $|\Delta| \leq r+1$ und $G_\Delta = 1$.
Bew: $R = \langle x_1, \cdots, x_r\rangle$, $\alpha \in R$; $\Delta := \{\alpha, \alpha^{x_1}, \cdots, \alpha^{x_r}\}$.

Folge:

(2) Hat die trans. Gr G einen regulären Normalteiler, so ist $|G| < n^{1+\log_2 n}$.

Aufgabe:

(3) Abschätzung für die Ordnung einer auflösbaren pri PGr des Grades n.

(4) G pri, $\delta \in \Delta =$ Träger eines längsten tra Konstituenten von $G_\alpha \Rightarrow G_{\alpha\delta}$ ist intransitiv in jedem tra Konst von G_α
Bew: Sonst $\exists \beta$: $G_{\alpha\beta}$ tra Δ', Δ invariant bei $\langle G_\alpha, G_\beta \rangle$.

117/118

Frage über monomiale Gruppen:

Wann gibt es eine Matrix M aus 0 und Einh.-Wu so, daß $g^{-1}Mg = \varepsilon(g) \cdot M$?
(mit $\varepsilon(g) \neq 1$)
höchstens wenn $\mathfrak{G}' \neq \mathfrak{G}$.
Genau wenn $\mathfrak{G} * \mathfrak{G}$ eine lineare Darst $\neq 1$ enthält.

Über 01-Matrizen

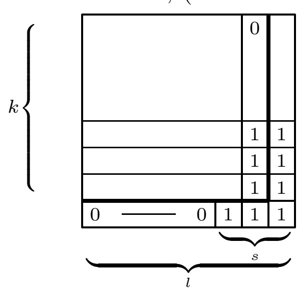
Beweis des Satzes von König: Bezeichnet r den termrank von A (= maximale Zahl von Einsen, keine zwei auf einer Reihe), so können die Einsen von A durch r Reihen überdeckt werden.
Bew:

(1) Man kann A maximal mit geg. $r(A) = r$ annehmen: $A \leq B$, $r(B) = r(A) \Rightarrow A = B$.

(2) Nach Streichen einer Zeile und Spalte mit Schnittel't 0 ist immer noch $r(A') = r$.

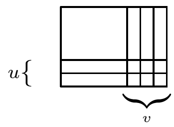
(3) A läßt sich (Induktion) durch $r+1$ Reihen überdecken, und zwar kann man von diesen eine beliebg. Zeile und eine bel. Spalte mit Schnitt 1 vorschreiben. Alle Schnitte sind 1.

(4) Sei $k \geq l$ (Typ $A = (k \times l)$) und eine Zeile minimaler Zeilensumme s sei die unterste, (und A maximal); etwa



Wähle Überdeckung mit $r+1$ Zeilen und Sp, davon unterste Zeile n rechteste Spalte. Wegen 3 sind die überdeckenden Spalten unter den letzten s, und wegen (oBdA) $r < k$ enthält jede von ihnen eine 0, und zwei außerhalb der gewählten überdeck. Zeilen. Das widerspricht der Min eig von s.

NB: jede maximale Matrix sieht so aus:



wo | und − mit Einsen voll besetzt, $u + v = r$

118/119

P-Gr. vom Rang 3

G tra, G_α habe 3 tra const. Eine der beiden Vert. matr. sei

$$V = [v \ \underbrace{s \cdots\cdot s}_{e} \ \underbrace{t \cdots t}_{f}] = V^*$$

Dann ist (bei trans. G):
(0) G pri $\Rightarrow |s|, |t| < v$ da $V \geq 0$ indecomposable & primitive,

(1abc)
$$\begin{cases} n = 1 + e + f \\ 0 = v + es + ft \\ nv = v^2 + es^2 + ft^2 \end{cases}$$

und (Beweis Frame)

$$\frac{nvw}{ef} = (s-t)^2$$

Ferner (aus $(V-s)(V-t) = cF$, $F = \binom{1\cdots 1}{1\cdots 1}$ (vgl el't $(1,1)$ und max EW))

(2)
$$(v-s)(v-t) = (v+st)n$$

und ähnlich Sp$\,(V-v)(V-t) =$ ↴

(3a)
$$nv(t+1) = e(s-v)(s-t)$$

und ebenso

(3b)
$$nv(s+1) = f(t-v)(t-s)$$

Daher aus $3a \cdot (t-v) - 3b \cdot (s-v)$:

(4)
$$nv(v-1-s-t) = (n-1)(v-s)(v-t)$$

und daraus mit (2)

(5)
$$v(v-1-s-t) = (n-1)(v+st)$$

und mit Frame und 3a, b:

(6)
$$\begin{cases} f(s-t)(t+1) = (s-v)w \\ e(t-s)(s+1) = (t-v)w \end{cases}$$

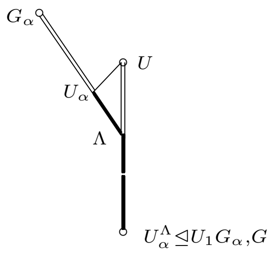
Das sollte Behandlung eines $\square$ freien n ermöglichen

Kompfakt Gr & Trans Konst von U_α

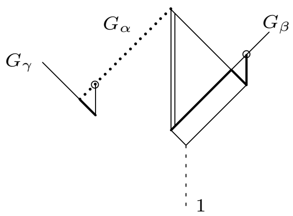
(1) Sei G pri, $U \leq G,\ U \neq U_\alpha \trianglelefteq G_\alpha$. Dann ist $\Sigma(U_\alpha) = \underbrace{\Sigma(U_\alpha^\Gamma)}_{\Lambda}$ mit $\Gamma = \alpha^U$

Σ Menge der Kompfaktgr.

Bew:



(2) Kompfakt von G_α:
G pri $\Rightarrow \sum(G_\alpha) \subseteqq \sum(K) + \sum(\Lambda)$ wo $K =$ Konst von $G_{\alpha\beta}$ auf β^{G_α}; $\Lambda =$ Konst von U auf γ^{G_α} wo $G_{\alpha\gamma} < U \leq G_\alpha$ und β, γ spiegel an α



Pri P-Gr G mit einem maximalen Sprung
in der Reihe der Bahnenlängen von G_α
27.11.63 nach Lektüre von MZ D G Higman

(1) Sei G tra, Bahnlgn $G_\alpha = n_1 = 1 < k \leq n_3 \cdots$
Dann $n_3 \geq k(k-1)$, und wenn $n_3 = k(k-1)$, so ist G_α 2-tra auf Γ mit $|\Gamma| = k$.
Bew: V sei Vertmatr zu Γ
$n_3 > k(k-1) \Rightarrow V^*V = kI + \beta V$ mit **???**, gibt Imprimitivität; siehe $(I+V)^\infty$

$n_3 = k(k-1) \Rightarrow V^*V = kI + W \quad W$ zu Δ Länge n_3.
$= V^2$

$$V = \begin{array}{c} \begin{array}{cccc} & \overbrace{\hphantom{1 \cdots 1}}^{R} & \overbrace{\hphantom{0}}^{n_3} & \overbrace{\hphantom{0}}^{n_4} \end{array} \\ \left(\begin{array}{c|c|c|c} 0 & 1 \cdots 1 & 0 & 0 \\ \hline 1 & & & \\ \vdots & M & N & 0 \\ 1 & & & \\ \hline 0 & N' & R & \end{array}\right) \\ \begin{array}{cccc} & \underbrace{\hphantom{1 \cdots 1}}_{\Gamma} & \underbrace{\hphantom{0}}_{\Delta} & \end{array} \end{array}$$

Wenn $M \neq 0$, so reichen die Einsen in den Zeilen Nr. $2, \cdots, k+1$ gerade aus um $N \neq 0$ zu machen für geeignetes $\Delta, |\Delta| = n_3$, also $M \neq 0 \Rightarrow M$ hat $k-1$ Einsen in jeder Zeile & Spalte,

$$I + V = \begin{pmatrix} 1 & \cdots & 1 & \\ \vdots & & & 0 \\ 1 & & 1 & \\ & 0 & & \boxed{} \end{pmatrix} \Rightarrow G \text{ impr.}$$

Also $M = 0$

121/122

Wäre G_α nicht 2-tra auf Γ, so gäbe es Vertmatrix R für G_α^Γ mit r Einsen je Zeile, $\operatorname{Sp} R = 0$, $0 < r < k-1$. Die Summe der n Konj. von R intr G gibt vert Matrix S für G mit rkn Einsen, also rk je Zeile; $rk < k(k-1)$, daher $S = r \cdot V$; das lieferte aber $M \neq 0$. Wid!

(1′.) Die $k(k-1)$ Einsen in N können so angeordnet werden:

$$N = \left.\begin{pmatrix} e & & & & \\ & e & & & \\ & & e & & \\ & & & \ddots & \\ & & & & e \end{pmatrix}\right\} k$$

$$e = (\underbrace{1 \cdots 1}_{k-1})$$

(1″) $G_{1,k+m}$ lässt auch 2 fest. $m = 1 \cdots k-1$
Denn die Spalte $k+1$ hat in dem Festblock $2 \cdots k+1$ von G_α nur eine 1 an der Stelle 2.

(1‴) Die Darstellung (1′) liefert eine Zerlegung von R in k^2 Blöcke der Grösse $(k-1)\times(k-1)$ (die mit Permutationsmatrizen besetzt sind, wenn $rk\ G = 3$). G_α^Δ ist impri, hat G_α^Γ also obersten pri Bestandteil.
$G_{1,2}$ hat einen <u>tra</u> Konst auf $k+2,\cdots,2k$ vom Grad $k-1$
Denn $|G_{1,2} : G_{1,2,k+2}| = k-1$.

Aufgabe: Fortsetzen bis

a) Bestimmung von V und der maximalen mit V vertb P Gr
b) Bestimmung der maximalen G mit maximalem Sprung hinter einem späteren n_k ⟨ **???** ⟩

122/123

Fortsetzg: Sei $n = k^2+1$

$N = G_{i,\cdots,k+1}$ ist auf Rest halbregulär und genau k Konjugierte N^x liegen in G_1, aber nicht in $G_{12\ldots k+1} = G_{1,\Gamma}$. Diese N^x müssen „hinten“ k Fixpunkte haben, sonst gibt N^{xg_1} zu viele Konj in G_1, also haben sie genau einen Fixpkt in Γ. Daher ist $N \cong$ einen halbregulären Normalteiler von K_2, wo $K = G_1^\Gamma$. Daher:

(1) entweder ist $K = G_1^\Gamma$ treu, oder K_2 hat halbreg. Normalteiler $\neq 1$.
Diese Überlegung muß einen allgemeinen Satz über die Kerne bei untreuen trans. Konst. geben.

(2) Nach (1) ist K_2 imprimitiv, wenn $k = \frac{7}{5}$, den es hat einen halbreg. auflösbaren NT, und sein Grad ist $\left\{ \begin{matrix} 6 \\ 56 \end{matrix} \right\} \neq p^{\alpha_1}$.

123/124

Higman-Gruppe

vom Grad 50 mit orbit lengths $1,7,42$:
Sei V die Vertmatrix mit Zeilensumme 7. Dann hat V die EWe $7,-3,2$ mit Vfh $1,21,28$, und genügt $V^2 = 7I + W$, $V = V'$, $V^2 = F + 6 - V$. V hat Gestalt

$$V = \left(\begin{array}{cc|cccc}
0 & e & 0 & 0 & \cdots & 0 \\
\hline
 & & f & 0 & \cdots & 0 \\
 & & 0 & f & & 0 \\
e & 0 & & 0 & & \vdots \\
 & & 0 & \vdots & & f \\
 & & \multicolumn{4}{c}{\begin{array}{|c|c|c|} \hline 0 & c & \quad S \quad \\ \hline & & \\ \hline \end{array}}
\end{array}\right)$$

$e = (1111111) \quad f = (111111) \quad S = S_{ik}$ Permut.

Die Matrix

$$S = \left(\begin{array}{ccccc} 0 & S_{12} & S_{13} & \cdots & S_{17} \\ \hline & 0 & & & \\ & & & \ddots & \\ S_{71} & S_{72} & S_{73} & & 0 \end{array}\right) = S'$$

genügt den Gleichungen (mit $F = \binom{1\cdots 1}{1\cdots 1}_{42} = F_{42}$, $\quad E = \begin{pmatrix} F_0 & & \\ & F_0 & \\ & & \ddots \end{pmatrix}$

$$\begin{aligned} SF =& FS = 6F \\ SE =& ES = F - E \\ S^2 =& F - E + 6 - S \\ \rightarrow \qquad S^3 =& 4F + 2E - 6 + 7S \\ S^4 =& 33F - 9E + 42 - 13S \\ S^5 =& 176F + 22E - 78 + 55S \end{aligned}$$

S hat die EWe $2, (-3), 6, -1$ mit Vfh $21, 14, 1, 6$.

$\left.\begin{array}{l} \text{Die Gl} \rightarrow \text{ zeigt } \operatorname{Sp} S^3 = 0 \\ \text{Für } I + S = T \text{ gilt } T^2 = F - E + G + T \end{array}\right\}$ gibt Beziehg zwischen S_{ik}

124/125

Abschliessg von P-Gr

(1) Die 2-Abschließung $G^{(2)}$ einer P Gr ungerader Ordnung hat ungerade Ordnung. Denn die Längen von G, G_α bleiben ungeändert.
Frage: Kann $|G^{(2)}|$ dann neue Primfaktoren enthalten?

(2) Die p-Abschließung einer PGr, deren Ordnung $\neq 0(p)$ ist, hat eine gleichartige Ordnung. Bew wie (1)

(3) Seien $A \leq B =$ tra zwei P Gr. Dann

$$B \leq A^{(2)} \quad \Longleftrightarrow \quad \begin{array}{l} A \text{ hat dieselben Orbits wie } B \\ A_\alpha \text{ hat dieselben Orbits wie } B_\alpha (\forall \alpha) \end{array}$$

Denn dann ist jede einfache VertMatrix von A auch eine von B, und umgekehrt ist trivial.

(3′) $A \leq B$ nicht notw. tra. $B \leq A^{(2)} \Longleftrightarrow$ jeder irred Bestandteil von B bleibt irred bei Einschränkung auf A, und verschiedene bleiben verschieden.

(4) Die 2-Abschließung einer tra p-Gruppe Perm Grad p^n ist die volle p-Sy der $S^{p^n} \Longleftrightarrow \underset{\substack{\uparrow \\ \text{Ableitung}}}{P^{(n-1)}} \neq 1$.

Denn genau dann bleibt jede in S^{p^n} enthaltene irred Darst bei Einschrkg auf P irreduzibel.

(5) G unipri vom Grad $p^3 \Rightarrow$ höchstens $p^{2p} \big| |G|$.
Bew:

a) $\widehat{P'}$ hat orblengths $p \Rightarrow$ je p gekoppelt $\Rightarrow |P'| \leq p^p, |P/P'| = p^2$ oder

b) orblength $\widehat{P'} = p^2 \Rightarrow |P'| \leq p^{2p-1}$, $|P/P'| = p$

$\widehat{N} :=$ größte Ugr mit orbits von N

125/126

10.12.63 Symbolische Potenzen im Vertauschungsring

(1) Sei $V = \begin{pmatrix} V_{11} & \cdots & V_{1k} \\ \vdots & & \\ V_{k1} & \cdots & V_{kk} \end{pmatrix}$ eine Vertauschungsmatrix von G, und je zwei $V_{\alpha\beta}$ seien vertauschbar. Für die „μ-te elementarsymmertische Funktion“ $e_\mu^{(V)}$, definiert durch $|\lambda I - \underset{\substack{\uparrow \\ x_{\alpha\beta}}}{\left(\begin{smallmatrix} x_{11}, \cdots \\ \cdots, xkk \end{smallmatrix}\right)}| = \sum (-1)^{k-\mu} f_\lambda (\underset{\substack{\uparrow \\ k^2 \text{ Variable!}}}{x_{11} \cdots x_{nn}})$

$$e_\lambda(V) = f_\lambda(V_{11}, \cdots, V_{nn})$$

gilt dann mit jeder Primzahl p:

$$\begin{aligned} e_\mu(V^p) &\equiv (e_\mu(V))^p \mod p \\ &\equiv e_\mu(V^{(p)}) \text{ mit } V^{(p)} := (V_{ik}^p) \end{aligned}$$

Bew: $(x_{\alpha\beta}) = x$

$$\sum_\mu (-1)^{k-\mu} e_\mu(X^p) \lambda^{p\mu} = |\lambda^p I - X^p|$$

$$\begin{aligned} &\equiv |(\lambda I - x)^p| = |\lambda I - X|^p \\ &\equiv \sum \lambda^{p\mu} e_\mu(X)^p (-1)^{k-\mu} \end{aligned}$$

$$\begin{aligned} e_\mu(X^p) \equiv e_\mu(X)^p = \big(\sum \overbrace{v_{\alpha\beta} v_{\gamma\delta} \cdots}^{\mu \text{ Faktoren}} \big)^p &\equiv \sum v_{\alpha\beta}^p v_{\gamma\delta}^p \cdots \\ &= e_\mu(v^{(p)}). \end{aligned}$$

(2) Insbesondere für den Spur-Block $SB(V) = \sum V_{ii}$ gilt $SB(V^p) \equiv \sum V_{ii}^p$

(3) Hiernach enthält der Vert-Ring von G unter Vor (1) stets eine Matrix W mit $SB(W) \equiv SB(V^{(p)})$ (p).

126/127

Vergrößerung von 2-tra Gruppen

Satz (1) Sei G 2-tra auf Ω ($|\Omega| \leq \infty$) und $G_\alpha = H$; sei $t = (\alpha\beta)\cdots \in G$. Sei $H \leq \widehat{H} \leq S_\alpha^\Omega$
Notwendig & hinreichend für Existenz eines $\widehat{G} \geq G$ mit $\widehat{G}_\alpha = \widehat{H}$ ist:

$$t^{-}\widehat{H}_\beta t = \widehat{H}_\beta.$$

Bew: notw klar, da $\widehat{H}_\beta = \widehat{G}_{\alpha\beta}$
hinreichend: bilde $\widehat{G} := \widehat{H} + \widehat{H}t\widehat{H}$
es genügt zu zeigen: $t\widehat{H}t \leq \widehat{G}$ (denn

$$\widehat{H}(t\widehat{H}t)\widehat{H} \leq \widehat{H}\widehat{G}\widehat{H} = \widehat{G},$$
$$\widehat{H}t\widehat{H} \cdot \widehat{H}t\widehat{H} \subseteq \widehat{G}$$
$$\widehat{G}\widehat{H}t\widehat{H} \leq \widehat{G}$$

da $\widehat{G}\widehat{H} \leq \widehat{G}$, folgt rechts Mult. $\widehat{G} \geq \widehat{G}$; $\widehat{G}$ Gp.
Es ist

$$\widehat{H} = H\widehat{H}_\beta, \text{ da } H \text{ tra } \Omega - \alpha$$
$$\text{also } t\widehat{H}t = tH\widehat{H}_\beta t$$
$$= tHt \cdot t^{-}\widehat{H}_\beta t \leq (\overbrace{H + HtH}^{\text{da } G \text{ 2-tra}}) \cdot \widehat{H}_\beta$$
$$\leq (\widehat{H} + \widehat{H}t\widehat{H})\widehat{H} = \widehat{G}$$

127/128

Aufgabe: Darstellungen faktorisierter Gruppen

(1) $G = AB$, $\chi_A(g)$ induz durch mon Darst ψ von A,
$\chi_B(g)$ induz durch mon Darst ω von B

$$\Rightarrow \frac{1}{g}\sum_G \overline{\chi_A}\chi_B = \begin{cases} 0 & \\ 1 & \text{wenn } \psi(x) = \omega(x) \text{ für } x \in A \cap B \end{cases}$$

Bew: Verkettende Matrix ist bestimmt durch ihr Element $(1,1)$, daher
Rg verk Modul ≤ 1, und $= 1$ genau wenn $\psi(x) = \omega(x)$ für $x \in A \cap B$

(1′) Im Fall $\frac{1}{g}\sum \overline{\chi}_A\chi_B = 1$ ist der Grad f des gemeinsamen irred. Bestandteils
$\rho = \binom{m_{11}\cdots}{\cdots m_{ff}}$ $\frac{|x|^2|y|^2}{|x^*y|^2} = f =$ Rg Verk. Matrix von χ_A, χ_B
wo $\rho(a)x = \psi(a) \cdot x \quad \rho(b)y = \psi(b)y$, unitär
Bew: oBdA $y = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

Da $y^*\rho^*(a)\rho(b)x = \psi^*(a)\omega(b)\cdot y^*x$

Wegen irred mon ρ ist $y^*x \neq 0$ oBdA $y^*x = 1$ also $y = \begin{pmatrix} 1 \\ 0 \\ | \\ 0 \end{pmatrix}$ $\quad x = \begin{pmatrix} 1 \\ \xi \\ 0 \\ 1 \\ 0 \end{pmatrix}$

gibt für $\rho(g) = \begin{pmatrix} m_{11} & m_{12} & \cdots \\ m_{21} & m_{22} & \cdots \end{pmatrix}_{f\times f}$ $g = a^- b : m_{11} + \xi m_{12} = \lambda(g) := \psi(a)\omega(b)$ für $g = ab$ Wid!

128/129

Daher $|m_{11} + \xi m_{1\nu}|^2 = 1$ für festes g also $|G| = \sum\limits_G |m_{11} + \xi m_{1\nu}|^2$, also

$$\begin{aligned} |G| &= \sum_G |m_{11}|^2 + |\xi|^2 \sum_G |m_{1\nu}|^2 + 2\mathrm{Re}\xi \sum_G \overline{m_{11}} m_{1\nu} \\ &= \frac{|G|}{f}(1 + |\xi|^2) \end{aligned}$$

$$f = 1 + |\xi|^2 = |x|^2 = \frac{|x|^2|y|^2}{|x^*y|^2}$$

also oBdA $\xi = \sqrt{f-1}$, ρ unitär.

Nun ist $\xi m_{12} = \lambda(g) - m_{11}$ also $|\xi||m_{1\nu}| \leq 2$
$|\xi^2| \cdot \frac{|G|}{f} = |\xi|^2 \sum\limits_G (m_{1\nu})^2 \leq 4|G|$
$f - 1 = |\xi|^2 \leq 4f$ klar, hilft nichts.
[Nun ... nichts: durchgestrichen]

129/130

Aufgabe

Untersuchung der genau 3-tra P Gr mit transitiven Untergruppen kleineren Grades (2-tra bei Hall 1962).

Aufgabe: Arithmetik der Gruppenringe
Jeder komm. Ring: **???**, der von „ganzen“ Größen erzeugt wird, ist endlicher $\mathfrak{o}$-Modul ($\mathfrak{o}$ = ganze Größen in alg. Zahlkörper)
Frage: <u>Welcher</u> Ring wird von allen Untergruppensummen einer abelschen endl. Gruppe erzeugt (reduzierte Form?)

130/131

S-Ringe von Matrizen

5.1.64 NB (25.10.76)
Siehe hierzu DG Higman: Geom. Dedicata 4, 1-32 (1975): Coherent configurations I

(1) Def: R ist ein S - Ring von Matrizen, wenn R aus $n \times n$-Matr. besteht, über $0 =$ ganze alg Zahl eine Basis aus „einf. Matrizen“ $\tau_1, \cdots .\tau_r$ besitze (nur $0, 1$ als Elemente) mit $\sum \tau_k = (1), \tau_1 = 1$
Higman fordert noch ein Diag. el’t $= 1 \Rightarrow$ alle El’te außerhalb Diag $= 0$, d.h. $\tau_k(1)_{(n\times n)} = n_k(1) = (1)\tau_k$
$\begin{pmatrix} 1 & & & & \\ & 1 & & 0 & \\ & & 1 & & \\ & 0 & & 1 & \\ & & & & 1 \end{pmatrix} \in R$ R halbeinfach. Also $n_1 + \cdots + n_r = n$.
Vollständig reduziert sei

$$\tau \sim \text{red}\ \tau = \begin{pmatrix} \overbrace{\begin{array}{|c|}\hline D^\delta(\tau) \\ \hline \end{array}}^{e_\delta \text{mal}} \end{pmatrix}; \quad \text{Gr } D^\delta = f_\delta$$

$r = \text{Rg}_{\mathfrak{o}} D$. Die Anzahl der inäqn. Darst in R sei d
Vorläufig kann R irgend ein halbeinfacher Ring von Matrizen sein.

(2) Setzt man für jede $f \times f$-Matrix $A = (a_{\kappa\nu})$
$A \downarrow = \begin{pmatrix} a_{11} \\ a_{12} \\ \vdots \\ a_{ff} \end{pmatrix}$ in fester, willkürl. Anwendung, und bezeichnet T_{f^2} die Permutationsmatrix des Grades f^2 mit

$$(A') \downarrow = T_{f^2} A \downarrow,$$

so ist

$$\det T_{f^2} = (-1)^{\frac{f(f-1)}{2}},$$

da soviel Paare von Stellen $(i, k), (k, i)$ vertauscht werden.
Es ist Sp$AB = \overline{A \downarrow}' T_{f^2} B \downarrow$. Setze

$$D(\tau) = \begin{pmatrix} D^1(\tau) \downarrow \\ D^2(\tau) \downarrow \\ \vdots \\ D^d(\tau) \downarrow \end{pmatrix} \quad \text{und } D = (D(\tau_1) \cdots D(\tau_r))$$

Wegen $r = \sum f_\delta^2$ ist D eine $r \times r$-Matrix

131/132

(3) Für S-Ringe ist

$$\begin{aligned}
&\mathrm{Sp}\ \tau_i\tau_k = n_k\delta_{ik^*}\\
&= \mathrm{Sp\ red}\ \tau_i\ \mathrm{red}\ \tau_k\\
&= \sum_j e_\delta\ \mathrm{Sp}\ D^\delta(\tau_i)D^\delta(\tau_k)\\
&= \sum e_\delta(D^\delta(\tau_i)\downarrow)'T_{f_\delta^2}(D^\delta(\tau_k)\downarrow)\\
&= D'ED\big|_{i,k}.
\end{aligned}$$

Mit

$$E := \begin{pmatrix} \ddots & & \\ & e_\delta T_{f_\delta^2} & \\ & & \ddots \end{pmatrix};\quad N := n(\delta_{ik^*})_{r\times r},$$

ist also

$$\#\quad D'ED = nN$$

(4) $\Delta := \det D$ ist ganz algebraisch, da

$$\begin{aligned}
\Delta^2 &= \pm\det D' \begin{pmatrix} \ddots & & \\ & T_{f_\delta^-} & \\ & & \ddots \end{pmatrix} D\\
&= (\mathrm{Sp}\ \tau_i\tau_k)
\end{aligned}$$

in der Darstellung von R, die jeden irred Bestandteil nur einmal enthält. Alle Spuren sind ganz alg. da $\sum \mathrm{EWe}(\tau_i\tau_k)$

(5) Ersetzg einer Darst in D durch eine äqu. ändert Δ nicht:

$$D^\delta(\tau) \Rightarrow (A'^- \times A)D^\delta(\tau),\ \det A'^- \times A = 1$$

132/133

6. Δ^2 ist rational.
Denn Körperautom. (eines Körpers, der alle Elem von D enthält) vertauschen die Darst. nur bis auf Äquivalenz, also $\Delta \to \pm\Delta$ (5)

7. Ist die Anzahl der Darstellungen D^δ mit

reellem Charakter		nichtreellem Char
geradem Grad f	r_0	c_0
ungeradem Grad f	r_1	c_1

so ist $\overline{\Delta} = (-1)^{c_1}\cdot\Delta$

denn Vertauschg zweier Darstellgen mit nichtreellen Char. vertauscht f Paare von Zeilen, gibt also $-$ wenn f ungerade, $+$ wenn f gerade. Die Darst. mit reellem Char geben nach 5 bei $x \to \overline{x}$ keinen Beitrag zu sgn Δ.

133/134

(8) Ist $\pi = \text{per } D$ die „Permanente" von $D = (d_{ik}), \pi = \sum d_{1d_1} \cdots d_{rd_r}$, so ist für $\alpha \in$ aut K

$$\Delta^\alpha \underset{2}{\equiv} \pi^\alpha = \text{per } D^\alpha = \text{per} \begin{pmatrix} \text{Darstellungen von} \\ D\text{; so vert,} \\ \text{daß} \sim \text{den alten} \end{pmatrix}$$

$$\underset{2}{\equiv} \det(\cdots) = \Delta$$

also $\Delta^\alpha \equiv \Delta \mod 2$ für jedes $\alpha \in$ aut K
Frage: Ist π rat?
Dann $\Delta^2 = (\pi + 2\gamma)^2 \equiv \pi^2 \mod 4 \equiv 0, 1 \mod 4$
Ja für „Determinanten-Permanente": 31.5.76 iterierte Laplace-Entwicklung

(9) Für jede Darstellung D^* eines halbeinfachen belieb. Ringes R, die die irred Darst. $D^{(\delta)}$ irgend eine Anzahl von Malen, e^*_δ-mal enthält, ist die Diskrim.

$$D(\tau_1, \cdots \tau_r) = \Delta^{*^2}_{(\tau_1 \cdots \tau_r)} = \prod_{\delta=1}^{d} e_\delta^{*f_\delta^2} \cdot \Delta^2(\tau_1 \cdots \tau_r)$$

Bew (3). Das gilt für <u>jede</u> Basis $(\tau_1 \cdots \tau_r)$ von R. Dabei

$$\Delta^{*^2} := \det(\text{Spur} D^*(\tau_i \tau_k))$$

(9′) Frage: Wenn $R, \widetilde{R}$ zwei S-Ringe mit $R \subseteq \widetilde{R}$, ist dann $\Delta(\tau_1, \cdots, \tau_r) \big| \Delta(\widetilde{\tau}_1, \cdots, \widetilde{\tau}_{\widetilde{r}})$? (Antwort (14)′) I.A. nicht!
Wenn ja, gilt für $R \subseteq$ Gruppenring von $\mathfrak{H}$: $\Delta(\tau_1 \cdots \tau_r) \big| h^h$
das gäbe gute Teilbarkeitsverschärfungen für Frame

134/135

(10) Δ ist rational genau wenn jedes $\alpha \in$ Aut K eine gerade Permutation der Charaktere von R bewirkt, für die f ungerade ist.
Wenn $R =$ Centralizer Rg dann e_ρ ungerade! Denn Vertauschg der geraden Darst ändert det Δ nicht.

(11) Wenn neben τ_k auch stets $\tau_k^* = \tau_{k^*}$ vorkommt.

→ S. 143 Sei $r = h + 2s$

wo $\left.\begin{array}{r}h \text{ die Anzahl der hermiteschen}\\ 2s \text{ die Anzahl der nicht hermiteschen}\end{array}\right\}\ \tau_k.$

Dann ist

$$s \equiv \sum_{\delta} \frac{f_\delta(f_\delta - 1)}{2} + c_1$$

denn

$$\begin{aligned}\operatorname{sgn}|N| &= (-1)^s\\ &= \operatorname{sgn}|E|\cdot \operatorname{sgn}\Delta^2\end{aligned}$$

Daher

(11′) $s \equiv \# f_\delta \equiv 2,3(4)$

wenn $2|c_1$, dh wenn jedes α die ungeraden Darst. mit nichtreell Char gerade permutiert und sonst $\equiv 1 + \# f_\delta \equiv 2,3(4)$

135/136

(12) Die Elementarteiler von $\{\cdots \underbrace{e_\delta}_{f_\delta^2 \text{ mal}} \cdots\}$ teilen die von $\{\cdots n_k \cdots\}$ denn die ersten sind die von E, die letzteren die von N, und D kann ganz alg gewählt werden;

$$\frac{\prod n n_k}{\prod e_\delta^{f_s^2}} = D(\tau_1 \cdots \tau_r) = \Delta^2(\tau_1 \cdots \tau_r) = \Delta^2.$$

Bew 3.

(12′) Ist R S-Ring $\tau_1 + \cdot + \tau_r = F = (1)_{r\times r}$

Bew: benutze $\begin{cases} D^{(1)}(\tau_k) = n_k \\ \widehat{\tau} = F,\ \widehat{\tau}_2 = \tau_2, \cdots, \widehat{\tau}_r = \tau_r \text{ als Basis } R\end{cases}$

$$\mathfrak{N}\begin{pmatrix} n & n_2 & \cdots & n_r \\ n_2 & & & \\ \vdots & & \boxed{n_k\delta_{ik^*}} & \\ n_r & & & \end{pmatrix} = (\operatorname{Sp}(\widehat{\tau}_i\widehat{\tau}_k)) = \widehat{D}' E \widehat{D}$$

$$\widehat{D} = \left(\begin{array}{c|c} n & \text{Rest wie} \\ 0 & D \\ | & \\ 0 & \end{array}\right)$$

$$E = \begin{pmatrix} 1 & & & \\ & e_2 T_{f_2^2} & & \\ & & \ddots & \\ & & & e_d T_{f_d^2}\end{pmatrix} = \begin{pmatrix} n & Z \\ 0 & \\ | & B \\ 0 & \end{pmatrix} =$$

$$\begin{pmatrix} n & Z \\ 0 & B \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \widetilde{E} \end{pmatrix}$$

mit $B_{(r-1)\times(n-1)}$
Daher $n|\Delta$, $(n_k\delta/_{k^*})_{2\cdots r} = B'EB - Z'Z$

$$\# \quad \frac{n^{r-2}\prod n_k}{\prod e_\delta^{f_\delta^2}}$$

ganz. Elem. Teiler von $(n\delta_{ik^*})_{2\cdots r} - Z'Z$ sind durch die von $\{ \underbrace{e_\delta \cdots}_{f_\delta^2 \text{ mal}} \}_{2\cdots r}$ teilbar.

136/137

(13) Achtung: Statt $\tau_i^* = \tau_{i^*} \in$ Basis zu verlangen, genügt, dass die Basis als Ganzes selbstdual ist bezüglich des inneren Produkts
Spur xy.

Antwort auf $9'$:

(14) Ist R ein Teil - S - Ring im Zentrum eines S - Rings R', so ist
$\Delta(\tau_1 \cdots \tau_r)\big|\Delta(\tau_1', \cdots, \tau_{r'}')$
Bew: Diskrim Matrix $D'(\tau_1', \cdots, \tau_{r'}') = D'(\tau_1 \cdots \tau_r \quad \tau_{r+1}' \cdots \tau_{r'}')$; für die treue Minimaldarst D' von R' ausschreiben. Die $r \times r$ Det $\neq 0$
für geeignete Wahl in den ersten r Spalten sind dann

$$\pm \det D(\tau_1 \cdots \tau_r). \quad \text{Laplace.}$$

(14′) Das Gleiche gilt wenn man die irred Darst von R' ganzzahlig machen kann derart daß R daher ausreduziert ist und äqu Darst daher gleich sind.
Aufgabe: Erweitern auf $m \times n$ S-Matrizen von XI 353
Man muß wohl von Paaren von Moduln reden: (M, N) mit MN Ring & NM Ring; das könnte für Ganzheit der EWe genügen
Vielleicht sollte man das als Def für halbeinfache Halbringe nehmen mit allgemeinerer Äq.def $M \sim PMQ$, $\det P \neq 0$ $\det Q \neq 0$
Das würde besser zu nichtunitären Darst. passen
z.B.: vtb mit $\left(\begin{smallmatrix} D_1 & 0 \\ 0 & D_2 \end{smallmatrix}\right)$ wenn D_r zwei Darst. eine Gr oder Moduln von Matrizen der Form $\left(\begin{array}{c|c} 0 & M \\ \hline N & 0 \end{array}\right)$

$$\begin{pmatrix} 0 & M \\ N & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & P^{-}MQ \\ Q^{-}NP & 0 \end{pmatrix}$$

F

137/138

Aufgabe: Halbringe von $(m \times n)$ - Matrizen

(16) Def ein Halbring M von $m \times n$ - Matrizen : $\mathbb{C}$ ist

a) ein Modul: $\mathbb{C}$, der

b) $MM^*M \leq M$ erfüllt $(M_1 M_2^* M_3 \in M)$.

(17) Ist M Halbring, so M^* und UMV mit U, V unitär auch Halbringe
Bew: $M^*MM^* \leq M^*$

$$\begin{aligned} UMV \cdot V^*M^*U^* \cdot UMV &= UMM^*MV \\ &\subseteq UMV \end{aligned}$$

(18) Def: $M \sim N$ wenn $M = UNV \quad U, V$ unitär

(19) Def: M halbeinfach wenn

$$M \sim \begin{array}{c} \begin{pmatrix} \mathbb{C}_{f_1 \times g_1} & & & \\ & C_{f_2 \times g_2} & & \\ & & \ddots & \\ & & & C_{f_d \times g_d} \end{pmatrix} \\ \begin{array}{ccc} | & | & | \\ e_1\text{-mal} & e_2\text{-mal} & e_d\text{-mal} \end{array} \end{array}$$

$$f_i, g_i \in \mathbb{N}.$$

(20) Der Verkettungsmodul zweier unitärer Darstellungen ist Halbring

(20′) Der Verkettungsmodul zweier transitiver Permgr ist ein halbeinfacher S-Halbring.

Vermutung: Ein Halbring M, der endlicher $\mathfrak{o}$-Modul ist, ist in einem mit Elementen $\in \mathfrak{o}$.

138/139

(21) Was man für diese Th. braucht, sind zwei Modul $\begin{array}{c} \mathrm{Rg} = m \\ | \\ \begin{cases} M = \{\mu\} \\ N = \{\nu\} \end{cases} \\ | \\ \mathrm{Rg} = n \end{array}$ so dass

MN ein he Ring R ist. Für jede $\left\{ \begin{array}{c} \text{Darst } D \text{ von } R \\ \text{Best } \mu_1 \cdots v_1 \cdots \end{array} \right\}$ kann man dann die $m \times n$ Matrix bilden:

$$D(\mu_1 \dots \ \mu_m; \ \ \nu_1 \cdots \nu_n) := \Big(\mathrm{Sp}\big(D(\mu_i \nu_k)\big)\Big); \quad \Delta = \det D$$

Transf auf andere Basen $\mu_1' \cdots \nu_1' \cdots$ ist klar: $\Delta \rightarrow \det A \cdot \det B \cdot D$
Abhängigkeit von D wie in 9.
Ist $m = n$ und $\left\{ \begin{matrix} D(\mu_1 \cdots v_m) \\ D'(\mu_1' \cdots v_m') \end{matrix} \right\}$ monomial, so ergeben sich Elementarteiler, falls geeignete $\mu\nu \in R$ ganz sind in dem Sinn, dass sie einen endl. $\mathfrak{o}$-Modul erzeugen.

(22) Um in einer Darstellung D eines Rings und endl. $\mathfrak{o}$-Moduls R einen ganzen Teilring R (dh endl $\mathfrak{o}$-Modul) auszureduzieren, bis zur Trenng der inäqn irr. Bestandteile, genügen die Nenner, die in $D(e_i)$ auftreten, wo e_i die zentralen prim Idempotenten von R durchläuft. Denn damit kann man die $D(e_\rho)$ auf Diagonalform bringen.

$$\begin{pmatrix} I & 0 \\ X & I \end{pmatrix} \begin{pmatrix} A & 0 \\ B & C \end{pmatrix} \begin{pmatrix} I & 0 \\ -X & I \end{pmatrix} = \begin{pmatrix} A & 0 \\ XA - CX + B & C \end{pmatrix} \text{ linear in } X.$$

z.B. um eine homogene volle Darst. D^δ in einem Matrizen- S-Ring trennen, genügen die Nenner der Koeffizienten des auf $\Box \sum \quad \sum e_\rho f_\rho$ normierten zentralen Idempotents zu D^δ

139/140

23. Allg Theorie: Gegeben Ring R mit 1, freier R-Modul M mit einer bilinearen nichtausgearteten Abbildung $\underbrace{(a_1, a_2)} \rightarrow \underline{a_1 a_2}$ geschrieben, $\in K =$ ein Körper.
$\mathrm{Rg}_R A = n$
Sind dann $b_1, \cdots, b_n$; $\widehat{b}_1, \cdots, \widehat{b}_n$ zwei Basen von M, so gilt für die Matrizen aus $K_{n\times n}$

$$B = (\underline{b_i b_k}), \quad \widehat{B} = (\widehat{b}_i \widehat{b}_k), \quad C = (b_i \widehat{b}_k)$$

(I)

$$\begin{cases} C' B^{-1} C & = \widehat{B} \\ C \widehat{B}^{-1} C' & = B \end{cases}$$

Bew: $\exists x : \widehat{b}_k = \xi_{lk} b_l$
$\underline{b_i \widehat{b}_k} = \underline{b_i b_l} \xi_{lk} \quad C = BX \ \Box$
$\underline{\widehat{b}_i \widehat{b}_k} = \widehat{b}_i b_l \xi_{lk} \quad \widehat{B} = C' X \ \circ$
Setze X aus $\Box$ in $\circ$ ein; dividiere erste Gl durch Zweite: $C\widehat{B}^{-1} = \ldots$

Wenn beide Basen "monomial" sind in dem Sinn dass B und $\widehat{B}$ monomiale Matrizen sind, so ergibt

Ia) Orthog rel für die Spalten von C

Ib) Orthog rel für die Zeilen von C

(II.) Ist z.B. M eine halbeinfache Algebra: K und K zerfällend und setzt man $a_1 a_2 = \text{Sp } D(a_1 a_{12})$ für eine beliebige treue Darstellg. $D(M) : K$, so ist jedes System von Matrixeinheiten e_i in M eine monomiale Basis. Und wenn $D \sim \sum e_\delta D^\delta$, D^δ irred H bel, ist

$$\text{Sp}(e^\alpha_{ik}\ e^\beta_{lm}) = \begin{cases} 0 & \alpha \neq \delta \text{ od } ik \neq ml \text{ oder } \beta' \neq \delta \\ 1 & ik = lm \text{ und } \alpha = \delta = \beta \end{cases}$$

daher

$$\underline{e^\alpha_{ik} \cdot e^\beta_{lm}} = \begin{cases} 0 & \alpha \neq \beta \text{ oder } ik \neq ml \\ e_\delta & \alpha = \beta,\ ik = ml \end{cases}$$

140/141

Also ist für ein System von Matr Einh. $\varepsilon_1 \cdots \varepsilon_n$:

$$E = \begin{pmatrix} e_1 Q_{f_1^2} & & & \\ & e_2 Q_{f_2^2} & & \\ & & \ddots & \\ & & & e_\delta Q_{f_\delta^2} \end{pmatrix} = E' \text{ wo } Q = (\delta_{ik,ml})$$

nur von der Darst D abhgig.

$$\det Q_{f_\delta^-} = (-1)\frac{f\delta(f_\delta - \ )}{2}$$

nicht von der Wahl der Matrixeinheiten.

III. Ist z.B. M ein S-Ring von Rg n in einer Gruppe H der Ord h, mit einfachen Basiselementen $\tau_1 \cdots \tau_n$; $\tau_2 = \underline{\mathfrak{T}_\nu}$, $|\mathfrak{T}_\nu| = t_\nu$, und wählt man für D die reg. Darst. von H, so wird die Matrix

$$T = (\underline{\tau_i \cdot \tau_k}) = \begin{pmatrix} t_1 & & & & \\ & t_2 & & & \\ & & & t_3 & \\ & & t_3 & & \\ & & & & \ddots \end{pmatrix} = (t_i \delta_{ik^*}) = T'$$

wenn zB. $\tau_3^* = \tau_4$.
Setzt man also

$$C = (\underline{\varepsilon_i \tau_k}) = (\text{Sp } D(\varepsilon_i \tau_k))$$

so wird nach I

$$\begin{cases} CT^- C' & = E \\ C' E^- C & = T \end{cases}$$

IV. Besonderer Fall: M kommutativer S-Ring: H. Die Darstellung ω_σ von M komme in der $D(M)$ e_σ mal vor. Dann ist ($e_\sigma = n_\sigma^{\#}$ bei T?)

$$E = \begin{pmatrix} e_1 & & \\ & \ddots & \\ & & e_n \end{pmatrix} = N^{\#}, \qquad T = \begin{pmatrix} t_1 & & & & \\ & \ddots & & & \\ & & & t_3 & \\ & & t_4 & & \\ & & & & \ddots \end{pmatrix}$$

141/142

Mit prim Idemp ε_ν von M wird

$$C = (\operatorname{Sp} D(\varepsilon_i \tau_k)) = E(\omega_{ik}) = EW$$

$\omega_{ik} = \chi_i(\tau_k)$ für M, $\omega_{ik} \in \Gamma$ ganz alg, gibt

$$\begin{cases} WT^- W' & = E^- \\ W'EW & = T \quad W'N^{\#}W = T \end{cases}$$

det $W = |\chi_i(\widetilde{\tau}_k)|$ mit $\overline{\tau}_1 = \underline{M}$; $\overline{\tau}_2 =$ **???**

$$= \begin{vmatrix} h & * & * & \cdots \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{vmatrix} \qquad h \big| \det W$$

Spezialfall: $M = \operatorname{Ztr} H$; H habe Darst Vfh e_σ; H habe Char Z_{ik} Grad f_σ

$$E = \begin{pmatrix} f_1^2 & & \\ & \ddots & \\ & & f_n^2 \end{pmatrix} \qquad T = \begin{pmatrix} n_1 & & & & \\ & \ddots & & & \\ & & & n_3 & \\ & & n_1 & & \\ & & & & \ddots \end{pmatrix} = (n_i \delta_{ik^*});$$

n_i Klassengl.

$$W = (\omega_{ik}) = \left(\frac{\overline{\chi_{ik}} n_k}{f_i} \right)$$

$$E^{\frac{1}{2}} W T^{-1} = (\overline{\chi_{ik}}) \qquad W = E^{-\frac{1}{2}} (\overline{\chi}) T$$

$$\begin{cases} \chi T \chi' & = I \\ \chi' \chi & = T^{-1} \end{cases}$$

V. Ist eine Ordnung in einer anderen enthalten, so ist ihre Diskrim-Matrix ein Vielfaches der anderen: $\Rightarrow$ ElTeiler Sätz
Anwendg auf ganzzahl. S-Ring in einer bel Max ord die letztere hat Diskr Matrix nach II.

142/143

Perm Gr G, tra, Char $= \chi$

Th: Die Anzahl der selbstgepaarten tra Konst. von G_a stimmt überein mit der Gesamtzahl der reellen einfachen Charaktere in $\chi(G)$ (mit Zählung der Vielfachheit)
Bew: ?

Achtung: Anders bei Higman, D. G.:
Coherent Configurations I; Geometriae Dedicata 4(1975), 1-32:
(7.4): Die Anzahl der symmetrischen Basismatrizen des Vertauschungsrings V einer primit. Perm. Gr. ist gleich der Anzahl der irreduziblen Bestandteile 1. Art minus Anzahl 2. Art, beide mit Vielfachheit gezählt. Dabei 1. Art: Darstellung auf reellen Matrizen transformierbar. 2. Art: Charakter reell, Char. Darst. nicht auf reellen Matrizen transformierbar
(well known for the group case, Frobenius-Schur)
Dort übrigens eine zusätzliche Bedingung (6.5) („Krein inequality") für die Basismatrizen von V.
Vorläufer bei L.L.Scott, AMS Notices, Jan. 1973, 701-20-45.

143/144
Die Seite 144 ist leer
144/145

Arithmet. Struktur bis S. 162: Januar 64

(Madison) 14.1.64, 20^{32} $\mathcal{M} = \max$; $\pi = \pi$-Untergr. $\widetilde{G}$ konjugiert in G, besser $\underset{G}{=}$
$Z =$ Centralizer

(1) Sei $N \trianglelefteq G$, $N \in \pi G$. Dann $A \in \mathcal{M}\pi G \iff N \leq A$, $A/N \in \mathcal{M}\pi G/N$.

(2) Sei $N \trianglelefteq G$, $|N|_\pi = 1$, $A \leq G$. Dann $A \in \mathcal{M}\pi G \iff A \in \pi G$, $AN/N \in \mathcal{M}\pi G/N$. Bew Thompson

(3) Folgende Klassen „großer" π-Gruppen haben Interesse: lage

$$\begin{aligned}
\mathfrak{L}\pi G : &= \{A \big| A \in \pi G;\ \ A \trianglelefteq B \in \pi G \Rightarrow A = B\} \\
\mathcal{M}\pi G : &= \qquad\qquad\qquad\ \leq \\
\mathcal{M}_1\pi G : &= \{A \big| A \in \pi G;\ \ |A|\big||B| = |B|_\pi \Rightarrow |A| = |B|\} \\
\mathcal{M}_2\pi G : &= \quad \cdots \qquad\qquad\qquad |A| \leq |B| = |B|_\pi \Rightarrow \cdots
\end{aligned}$$

$\hat{\mathcal{M}}$ siehe (7)(11). Es ist $\mathcal{M}_2 \subseteq \mathcal{M}_1 \subseteq \mathcal{M} \subseteq \mathfrak{L}$.
z.B.

(4) $A \in \mathcal{M}_1\pi G$, $N \trianglelefteq G$, $|N|_\pi \neq 1 \Rightarrow A \cap N \neq 1$.
Bew: sonst $B = \mathcal{N}_{NA}$ Sylowturm N.

Folge für $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_e = 1$, $G_{i-1}/G_i =: G^i$ gilt

(5) $A \in \mathcal{M}_1\pi G_1$ $B\neg G^\lambda = A \cap G^\lambda \Rightarrow A \underset{G}{\sim} B$
Bew mit Induktion mittels

(6) $A, B \in \mathcal{M}\pi G$, $B\neg G^\lambda = A\neg G^\lambda$, $N^{\min} \trianglelefteq G$
$\Rightarrow A \cap N = B \cap N = \prod_\times (A \cap N_\sigma)$; mit $N = N_1x + N_S$ ist $A \leq N_\sigma \in \hat{\mathcal{M}}\pi N_\sigma$
Def siehe (7)
Bew:

a) $|N| = p^\nu$, $p \in \pi$ $\quad N \cap A = B \cap N = N$

145/146

b) $|N| = p^\nu$, $p \notin \pi \Rightarrow A \cap N = 1 = B \cap N$
c) $N = N_1 \times \cdots \times N_s$, $N_\sigma = N'_\sigma$ einfach

Nun Benutze

Lemma (7) $N_1 \leq G$, $\mathcal{C}N_1 = 1$, $N_1 \cap K_1 = 1$, $K_1 \leq \mathcal{Z}_G N_1$, $K := N_1 \times K_1$, $A \in \mathcal{M}\pi G$, $a \in A - \mathcal{N}_A N_1 \Rightarrow [N_1^a, N_1] = 1$
$\Rightarrow A \cap (\overbrace{N_1 \times K_1}^{K}) = (A \cap N_1) \times (A \cap K_1)$, und $A \cap N_1 \in \widehat{\mathcal{M}}\pi N_1$, wo

Def: $\widehat{\mathcal{M}}\pi G = \{B \big| \exists c \in \pi \text{ aut } G \to B^c = B, \ \& \ x^c = x \in \pi G \Rightarrow x \in B\}$
Besser Def: (11): Bestimmg von $\hat{\mathcal{M}}$: (9)
Zum Beweis besser erst Lemma 8!
Bew: oBdA $K_1 = \mathcal{Z}_G N_1$; dann $N_1, K_1, N_1 \times K_1$ invariant unter $\mathcal{N}_A N_1$. Bilde die von $\mathcal{N}_A N_1$ auf N_1 induzierte Automgr C; $(A \cap N_1)^C = A \cap N_1$; Wähle ein beliebiges $B \in \mathcal{M}\{X \in \pi N_1, X^C = X\}$. Dann $B \in \widehat{\mathcal{M}}\pi N_1$, B invariant unter $\mathcal{N}_A N_1$, also

$$B^A = \langle B^1, B^{a_2}, \cdots, B^{a_s} \rangle \text{ wo } A = \sum_{r=1}^{s} (\mathcal{N}_A N_1) a_\sigma$$

Aber jedes B^{a_σ} liegt in einer anderen Konjugiert von N_1 unter A, und die zentralisieren sich nach Vorauss. gegenseitig. Also $B^A = B^1 \bullet B^{a_2} \bullet \cdots B^{a_\sigma} \in \pi G$ Wegen $A \in \mathcal{M}\pi G$ ist $B^A \leq A$, insbesondere $B \leq A$. Also $B \leq A \cap N_1$.

146/147

Nun enthält aber C insbesondere die von $A \cap N_1$ auf N_1 induzierten inneren Automorphismen, also $B^{A \cap N_1} = B$, daher $B \cdot (A \cap N_1) \in \pi N_1$ und fest unter $\mathcal{N}_A N_1$, also $B \cdot (A \cap N_1) = B$, d.h. $B \leq A \cap N_1$, also $B = A \cap N_1$

Schluß des Beweises von (6):

a) Wähle $K_1 = G_\lambda$ wo $\lambda = \min$ mit $N_1 \nleq G_\lambda$. Dann deckt N_1 das G^λ, $[N_1, G_\lambda] = 1$. Wähle in (7) $K_1 = G_\lambda$ gibt

$$A \cap G_{\lambda-1} = (A \cap N_1) \times (A \cap G_\lambda)$$

also

$$A \neg G^\lambda = (A \cap N_1) \underset{\substack{\uparrow \\ \text{dis-} \\ \text{junkt}}}{\cdot} G_\lambda / G_\lambda$$

ebenso

$$B \neg G^\lambda = (B \cap N_1) \cdot G_\lambda / G_\lambda$$
$$(A \cap N_1) G_\lambda = (B \cap N_1) G_\lambda$$
$$A \cap N_1 = B \cap N_1 \in \widehat{\mathcal{M}} \pi N_1$$

ebenso N_σ statt N_1.

b) Wähle in 7 $K_1 = N_2 \times \cdots \times N_S$, gibt

$$A \cap N = (A \cap N_1) \times (A_1 \cap N_2 \cdot N_S)$$

also kommen die 1. Komp von A invertiert vor, ebenso die σ-ten Komp:

$$A \cap N = \prod\nolimits_\times (A \cap N_\sigma) = \prod (B \cap N_\sigma) = B \cap N$$

147/148

Lemma (8) Verallg. des Gedankens von (7):
Vor: $A \in \mathcal{M} \pi G$, $B \in \pi G_1$ für jedes $a \in A$ ist $B \cdot B^a = B^a \cdot B$.
Beh: $B \leq A$
Bew: $B^A \in \pi G$, $A \cdot B^A \in \pi G$, $= A$.

(9) Ist $\mathcal{C} G = 1$, so ist $B \in \widehat{\mathcal{M}} \pi G \iff \exists M \in \mathcal{M} \pi \widehat{G} \ni B = G \cap M$.
$\neq s.$ (10)
Dabei $\widehat{G} := \operatorname{aut} G$, mit identif. G, inn G
Bew:

a) $B \in \widehat{\mathcal{M}} \pi G \Rightarrow \exists C \leq \operatorname{aut} G \quad \ni$

$$\begin{cases} B &= B^C \\ X &= x^C \in \pi G \Rightarrow X \leq B \end{cases}$$

$B^C = B$, also $BC \in \pi G$. Wähle $M \geq BC$, $M \in \mathcal{M} \pi \widehat{G}$. Dann $M \cap G \geq B$ und fest bei M, also bei C, daher $M \cap G = B$

b) Sei $M \in \mathcal{M} \pi \widehat{G}$, $B = G \cap M$. Dann $B^M = B$, und wenn $X \in \pi G$, $X^M = X$, so $XM \in \pi \widehat{G}$, also $XM = M$, $X \leq M$, $X \leq G \cap M = B$.

(10) Für jedes G ist $B \in \widehat{\mathcal{M}}\pi G \iff \exists M \in \mathcal{M}\pi$ hol (Holomorph) G mit $M \cap G = B$.
Bew wie (9). s. auch (11)

148/149

(11) $B \in \widehat{\mathcal{M}}\pi G \iff \exists H \trianglerighteq G,\ M \in \mathcal{M}\pi H,\ M \cap G = B$
Dies die beste Def von $\widehat{\mathcal{M}}$ aber wichtiger $\widehat{\widehat{\mathcal{M}}}$ (4)
Bew:

a) $\Rightarrow$ (10) $H = \operatorname{hol} G$

b) $\Leftarrow$ $C :=$ Aut von G, indduz von M; $B^C = B$;
$X^C = X \in \pi G \Rightarrow X^M = X,\ \langle X, M\rangle \in \pi H, = M$

(12) $B \in \widehat{\mathcal{M}}\pi G$, G_1 char in $G \Rightarrow B \cap G_1 \in \widehat{\mathcal{M}}\pi G_1$ Bew Def (7)

(13) Aufgabe: $C_\pi(S^k \text{ wr } S^\ell) =?$

(14) Aufgabe: Wann $\widehat{\mathcal{M}}\pi G = M\pi G = \mathfrak{L}\pi G$?

(15) Def: $\widehat{\widehat{\mathcal{M}}}\pi G = \{B \big| \exists_{H,M} G \trianglelefteq\trianglelefteq H, M \in \mathcal{M}\pi H, M \cap G = B\}$
$\widehat{c}$, $\widehat{\widehat{c}}\pi G =$ Aut. d. Klassen konjugierter $X \in \widehat{\widehat{\mathcal{M}}}\pi G, \widehat{\mathcal{M}}$

(16) Aufgabe: Untersuche die Familie der G mit $\widehat{\widehat{c}}_\pi G = 1$. Normal persistent?

149/150

(17) $N \trianglelefteq G,\ \widehat{c}_\pi N = 1 \Rightarrow c_\pi G = c_\pi G/N$.
Bew: Wenn $M_\pi = 1$, (24); Sonst (20). Sonderf 21

(18) $\widehat{c}_\pi G = 1 \forall \pi \iff G$ sol
Bew: $c_\pi \leq \widehat{c}_\pi \leq \widehat{\widehat{c}}_\pi$

(19) Frage: $\widehat{\mathcal{M}} = \widehat{\widehat{\mathcal{M}}}$?

(20) $\widehat{c}_\pi G = 1,\ B \in \widehat{\mathcal{M}}\pi G \Rightarrow B \in \underset{\substack{| \\ \text{Hall-} \\ \text{gp.}}}{\mathcal{H}} \pi G$
Bew: $\mathcal{M} \subseteq \widehat{\mathcal{M}}$, also $c_\pi G = 1$

(21) aufl $N \trianglelefteq G \Rightarrow c_\pi G = c_\pi G/N$
braucht nicht Th.– Feit

(22) Aufgabe: Nichtabelsche „Kohomologietheorie mit durchweg subnormaler“ Einbettung untersuchen $0 \to A \to B$

(23) Ist $a_\pi G$ die Zahl der Klassen unter aut G konjugierter max π- Untergruppen von G, so gilt:

$$C \text{ char in } G \Rightarrow a_\pi C \le a_\pi G$$

mit $\lhd\lhd$ char char statt $\trianglelefteq\trianglelefteq$.
Aufgabe: Weitere Sätze für: a_π statt c_π beweisen.

150/151

(24) Wenn $N \trianglelefteq G$, $|N|_\pi = 1$; $A, B \in \pi G$ so $A \underset{G}{\sim} B \iff AN \underset{G}{\sim} BN \iff$

$$AN/N \underset{G/N}{\sim} BN/N.$$

Bew: Th. Feit.

(24) Wenn $N \trianglelefteq G$; $N \le A, B \le G$ so $A \underset{G}{\sim} B \iff A/N \underset{G/N}{\sim} B/N$

(25) Ist jede komp Fakt Gr von G entw. π- oder π'- Gp, so ist $\widehat{\widehat{c}}_\pi G = 1$
Bew: $G \trianglelefteq\trianglelefteq H$, $M \in \mathcal{M}\pi M \Rightarrow$ mit (27)
M deckt die π-Char. fakt. von G, meidet die π'- Char. faktoren von G
Bew: Indukt $|G|$ mit (1), (2). Dann Konjugiertheit nach Satz für Layer Projections

(26) Frage: $\widehat{\widehat{c}}_n G = 1 \Rightarrow$ jeder Komp-Index $\begin{cases} \pi \text{ od} \\ \pi' \end{cases}$?

151/152

(27) $N \trianglelefteq\trianglelefteq G$, $N \in \pi G$, $A \in \widehat{\widehat{\mathcal{M}}}\pi G \Rightarrow N \le A$

(28) Aufgabe: wird die äußere Aut. Gr einer perfekten einfachen Gr. stets von Involutionen erzeugt?

(29) Große Aufgabe: Statt der Familie πG eine beliebige invariant definierte Klasse κG von Ugr von G betrachten, κ klassifizieren nach Verhalten bei Hom, $\times, \ldots$ Grundvor: σ iso $G \Rightarrow \kappa(G^\sigma) = (\kappa G)^\sigma$
z.B. $\kappa = \text{coc}$ $\quad A \in \text{ coc } G \iff \forall g \in G \exists h \in \langle A, A^g \rangle\ A^g = A^h$ also $A \in \text{ coc } G \iff A \underset{G}{\sim} B \Rightarrow A \underset{\langle A,B\rangle}{\sim} B$
oder

$$A \in \left\{ \begin{array}{c} \text{isc } G \\ \text{auc } G \end{array} \right\} \iff B \le G \left\{ \begin{array}{c} B \cong A \\ \exists \sigma \in \text{ aut } G \ni B = A^\sigma \end{array} \right\} \Rightarrow A \underset{\langle A,B\rangle}{\sim} B$$

(30) Zu jedem κ gehört $\hat{\kappa}, \hat{\hat{\kappa}}$,

$$A \in \hat{\kappa} G \iff \exists \hat{G} \trianglerighteq G,\ \hat{A} \in \kappa \hat{G},\ \hat{A} \cap G = A$$

$$A \in \hat{\hat{\kappa}} G \iff \exists \hat{\hat{G}} \trianglerighteq\trianglerighteq G, \ldots$$

Es ist $\kappa \subseteq \hat{\kappa} \subseteq \hat{\hat{\kappa}}$

152/153

Zu jedem κ gehört $\overleftarrow{\kappa}$:

$$A \in \overleftarrow{\kappa} G \iff \forall_\eta : H \twoheadrightarrow G, \exists B \in \kappa H \ni B^\eta \leq A.$$

z.B. $\overleftarrow{\pi} = \pi$, $\overleftarrow{\mathcal{M}\pi} = \mathcal{M}\pi$.
Komposition von Klassen.

$$A \in \kappa\lambda G \iff \exists H \in \lambda G,\ A \in \kappa H$$

$$A \in K\overline{\lambda} G \iff \exists \overline{G},\ \overline{A} \ni G \in \lambda \overline{G},\ \ \overline{A} \in K\overline{G},\ A = G \cap \overline{A}$$

z.B. $\mathcal{H}\pi = \mathcal{H}\overline{\pi}\,\overline{\nu}$; dabei
feste Bez:

$$\begin{array}{lcl} A \in \nu G & \iff & A \trianglelefteq G \\ A \in \sigma G & \iff & A \trianglelefteq\trianglelefteq G \\ A \in \delta G & \iff & A \text{ direkter Faktor von } G \end{array}$$

Man könnte schreiben $\sigma = \nu \ldots \nu$ oder $= \nu^a$
Aber vielleicht sollte man wie in Kohomol Th die Untergr als Abbildg abstrakter Gruppen festlegen. Vielleicht gibts das alles schon in Funktoren-Theorie.
Def: κ kovariant $\iff [\eta \in \text{ hom } G \Rightarrow (\kappa G)^\eta = \kappa(G^\eta)]$
z.B. π kov, $\mathcal{M}\pi$ nicht.

153/154

Def:

$$\kappa \left.\begin{array}{c} \text{super var} \\ \text{covar} \\ \text{subvar} \end{array}\right\} \iff \kappa(G^\eta) \left\{\begin{array}{c} \supseteq \\ = \\ \subseteq \end{array}\right. \quad (KG)^\eta$$

für $\forall \eta \in$ hom G
Besser: Schreibe

$$\kappa\eta \overset{\supseteq}{\underset{\subseteq}{=}} \eta\kappa$$

wenn für jeden Hom η von G gilt $\kappa(\eta(G)) \overset{\supseteq}{\underset{\subseteq}{=}} \eta(\kappa(G))$, z.B. $\mathcal{M}\pi$ subvar
κ direkt $\iff A, B \in \kappa G, \exists A \times B \Rightarrow A \times \overline{B} \in \kappa G$
Def:

$$\kappa \text{ distrib } \iff \left\{ \leftrightarrow \begin{array}{c} A \in \kappa(G_1 \times G_2) \\ A = A_1 \times A_2, \\ A_i \leq G_i, A_i \in \kappa G_i \end{array} \right\}$$

zB. π ist direkt; $\mathcal{M}\pi$ ist distr.
$\kappa =$ coc $\Rightarrow \kappa\eta = \eta\kappa,\ \kappa\delta \subseteq \kappa$
$\mathcal{M}$ coc distr. Allgemeiner:

(31) Satz: Sei $\left\{ \begin{array}{c} \kappa \text{ direkt} \\ \kappa\delta \subseteq \kappa, \eta\kappa \subseteq \kappa\eta \end{array} \right\}$; dann $\mathcal{M}\kappa$ distrib. („direkt“ wohl abzuschwächen ?)
Bew:

a) Sei $A \in \mathcal{M}\kappa(G_1 \times G_2)$, $A_i =$ Komp A in G_i; dann

$$A_i \in \kappa G_i \text{ da } \eta\kappa \subseteq \kappa\eta$$
$$A_i \in \kappa(G_1 \times G_2), \text{ da } \kappa\delta \subseteq \kappa$$
$$A \leq A_1 \times A_2 \in \kappa(G_1 \times G_2) \text{ da } \kappa \text{ direkt}$$
$$A = A_1 \times A_2 \text{ da } A \in \mathcal{M}\pi(G_1 \times G_2)$$

b) Sei $A = A_1 \times A_2$, $A_i \in \mathcal{M}\kappa G_i$; $G = G_1 \times G_2$.
Dann $A_i \in \kappa G$ da $\kappa\delta \leq \kappa$
$A = A_1 \times A_2 \in \kappa G$ da κ direkt; $|G| < \infty$!
Wähle $A \leq B \in \mathcal{M}\kappa G$, dann ist $B = B_1 \times B_2$ (a)
also mit $A_i \leq B_i \in \kappa G_i$, $A_i = B_i$

154/155

(32) Wenn $\hat{\pi}(C) \neq 1$ für jeden Kompfaktor jedes $M \leq G$ so gilt:

<u>Satz:</u> Ist $A, B \in \hat{\hat{\mathcal{M}}}\pi G$, $A \neg G^\lambda = B \neg G^\lambda$ für jeden nichtabelschen Faktor G^λ in einer $K.-R$, von G, so $A \underset{G}{\sim} B$.
Bew: Ind von unten

(33) Aufgabe: Projektionseigenschaft $\mathcal{S}G \to \mathcal{S}\hat{\mathcal{M}}$.

(34) Die Vor von (32) kann ersetzt werden durch
A, B sollen je eine 2-Sylowgr. von G enthalten. Vielleicht genügt auch: Ihre Projektionen in die nicht abelschen Faktoren G^λ sollen je eine 2-Sy von G^λ enthalten

(35) Hauptlemma: $M \in \mathcal{M}\pi G$, $S, T \leq G$; wenn $P_i \in \pi S_i$, so $\langle P_i \rangle \in \pi G$, wobei S_i die verschiedenen Konjugierten von S unter M sind; $S \leq \mathcal{N}T$, $S \cap T = 1$

$$\Rightarrow [M \neg ST/T] \neg S = M \neg S \qquad (*)$$

155/156

Vor schwächer: Wenn linke Seite von $(*) = P$ gesetzt wird, soll $P^M \in \pi G$ sein: d.h. für $P = (M \cap ST) \cdot T \cap S$ sei $P^M \in \pi G$.

(36) Vermutung $\begin{cases}\boxed{\text{V}}\\ \boxed{\text{V}'}\end{cases}$: In der äußeren Automgr. jeder einfachen Gr. S bilden die $|S|$- Elemente eine $\begin{cases}\text{nilpotente}\\ \text{auflösbare}\end{cases}$ Untergruppe.

$\Rightarrow \boxed{\text{V}''}$: S einfach, $|S|_\pi \neq 1$, $A \in \pi$ aut $G \Rightarrow \exists B \in \pi S$, $B \neq 1$, $B^A = B$

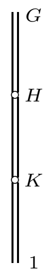
Th (37) $\boxed{\text{V}''}$ $\Rightarrow$ zwei max π- Ugr A, B von G s. auch sind $\underset{G}{=}$ genau wenn ihre Projektionen in die nichtabelschen Faktoren G^λ einer Normalreihe von G simultan-konjugiert in G sind
Bew mit 42

Th (38) $\boxed{\text{V}''}$ $\Rightarrow$ keine max π-Ugr von G meidet den π-Sockel S_π von G
($:= P/Q$ wo Q die max π-aufl nor Ugr von G und $P/Q =$ Sockel G/Q)
genügt V$''$ (S_π)! „für die einf. Fakt. von“
wohl gleichwertig:
$\boxed{\text{V}''}$ $\Rightarrow$ keine max π-Ugr von G meidet Kopf A wenn $A \trianglelefteq\trianglelefteq G$ und minimal in $\mathcal{S}G$ nicht - π - auflösbar (daher A einköpfig)
genügt V$''$ (Kopf A)

156/157

(39) Frage: Sind in einer einfachen Gruppe je zwei π-Untergr maximaler π-Ordnung konjugiert?
Antw: 15.11-77: NEIN! Bsp: $|G| = 168$, $\pi = \{2, 3\}$ aber dort wenigstens konjugiert in Aut G_1

(40) Methode: Erst die G untersuchen vom Bau



wo G/H und $K\pi$-sol, und H/K direktes Produkt einfacher nichtabelscher π-Gruppen.

Th (41) $\boxed{\text{V}''}$ $A, B \in \mathcal{M}\pi G$, $A\neg G^\lambda = B\neg G^\lambda$ für die nichtab G^λ
$\Rightarrow A \underset{\langle A,B\rangle}{=} B$
Bew: die Vor überträgt sich auf $G^* = \langle A, B\rangle$; auf G^* (37) anwenden

(42) Projektionen: $A \leq B \leq G$, $Q \in \mathcal{Q}G \Rightarrow$

i) $A\neg(Q\neg B) = (A\neg Q)\neg B$

ii) $A\neg Q = [A\neg(Q\neg B)]\neg Q$

also die beiden linken Seiten bestimmen sich gegenseitig

157/158

Bew:

i) $Q = U/N$; $Q\neg B = U \cap B\big/N \cap B$
$A\neg(Q\neg B) = (A \cap U \cap B)(N \cap B)/N \cap B = \mathfrak{L}/N \cap B$
$\underline{\mathfrak{L}} = A(N \cap B) \cap U \cap B = AN \cap B \cap U \cap B = AN \cap U \cap B$
andererseits $A\neg Q = (A \cap U)N/N = AN \cap U/N$
$(A\neg Q)\neg B = AN \cap U \cap B/N \cap B = \mathfrak{L}/N \cap B$

ii) $A\neg(Q\neg B) = AN \cap U \cap B/N \cap B$ s.o.

$$\begin{aligned} [A\neg(Q\neg B)]\neg Q &= (AN \cap U \cap B \cap U)N/N \\ &\ AN \cap U \geq N \\ &= (AN \cap U \cap BN)/N \\ &= AN \cap U/N \\ &= (A \cap U)N/N = A\neg Q \end{aligned}$$

(42′) $A \leq G' \leq G$, $Q \in \mathcal{Q}G$, $Q' = Q\neg G'$
$\overset{\text{äq. 42}}{\Rightarrow}$

i) $A\neg Q' = (A\neg Q)\neg Q'$

ii) $A\neg Q = (A\neg Q')\neg Q$

iii) $A\neg Q \cong A\neg Q'$

im endl Fall wegen Ord.

158/159

(43) Es ist $Q_1\neg(Q\neg Q_2) = (Q_1\neg Q) \cap Q_2$ genau wenn

a) $(U_1N \cap U)N_2 \cap U_2 = U_1(NN_2 \cap U_2) \cap UN_2 \cap U_2$

& b) $(N_1N \cap U)N_2 \cap U_2 = N_1(NN_2 \cap U_2) \cap UN_2 \cap U_2$

wobei die Reihenfolge der Faktoren geändert w. kann.

(44) Es ist $Q_1\neg Q_2 = Q_2\neg Q_1$ genau wenn $U_1N_2 \cap U_2 = N_1U_2 \cap U_1$ & $N_1N_2 \cap U_2 = N_1N_2 \cap U_1$ und das ist gleichwertig mit $N_1 \leq U_2$ & $N_2 \leq U_1$ dh mit $\langle N_1, N_2\rangle \leq U_1 \cap U_2$

(44′) Also $Q_1\neg Q_2 = Q_2\neg Q_1 \iff N_1, N_2 \leq U_1 \cap U_2 \iff N_i \leq U_j$
Frage: $\Rightarrow Q_1\neg(Q\neg Q_2) = (\quad).?$

(45) Aufgabe: π-Gr maximaler Ord in A^n, S^n

(46) Frage: Kann man eine Gruppe, in der die nichtabelschen Kompfakt. C^λ vorkommen, so vergrößern, dass jedes C^λ durch aut C^λ ersetzt wird und keine neuen nichtabelschen Faktoren auftreten ?

159/160

(47) Sei $c\mathcal{H}\pi G$ die Anzahl der Klassen konjugierter π-Hallgruppen in G_1 Dann gilt:
Ist $c\mathcal{H}\pi G^\lambda = 1 \overset{l}{\underset{1}{\forall}}\lambda$, so $c\mathcal{H}\pi G = 1$; und je zwei Hallgr. v. G sind schon in ihrem Erzeugnis konjugiert.
Steht das bei Hall? Bedeutet $G^\lambda \in C_\omega \Rightarrow G \in C_\omega$
Bew: Indukt λ.

(48) Vermutung: $A \in \hat{\hat{\mathcal{M}}}\pi G \Rightarrow A \neg G^\lambda \in \mathfrak{L}\pi G^\lambda$.
Das würde 37 in der Theorie der großen Proj. einordn.

(49) Vermutung: Ist $N \trianglelefteq G$ $|N|_\pi = \begin{cases} |N| \\ 1 \end{cases}$, $A \in \pi G$, so ist $A \in ccG \iff AN/N \in ccG/N$ dabei $A \in ccG \iff \forall x \in G \exists h \in \langle A, A^x\rangle \ni A^x = A^h$

(50) Sei $\mathfrak{L} \trianglelefteq G$, $\mathfrak{L} \in \pi' G$ (dh $|\mathfrak{L}|_\pi = 1$). Sei $A \in \pi G$, $U = U^{\mathfrak{L}} \leq G$; dann ist $A\mathfrak{L} \cap U\mathfrak{L} = (A \cap U)\mathfrak{L}$.
Bew: Sei $a \in A\mathfrak{L} \cap U\mathfrak{L}$ dann $a \equiv u(\mathfrak{L})$
Wähle $n \in \mathbb{N}, n \equiv 1(|G|_\pi); n \equiv 0(|G|_{\pi'})$
$a = a^n = u^n(\mathfrak{L})$ u^n ist π-El't in U.

160/161

Ersetze u durch u^n, dh oBdA kann man $\langle u\rangle \in \pi G$ annehmen. $\langle a\rangle, \langle u\rangle$ sind Kplte von $\mathfrak{L}$ in $\langle a\rangle\mathfrak{L} = \langle u\rangle\mathfrak{L}$; also nach Zasshs. $\exists \mathfrak{l} \in \mathfrak{L} \ni a = u^{\mathfrak{l}}$ wegen $U^{\mathfrak{L}} = U$ ist $u^{\mathfrak{l}} \in U$, also $a \in A \cap U$; $A\mathfrak{L} \cap U\mathfrak{L} \leq (A \cap U)\mathfrak{L} \geq$ triv.

(51) Man kann zu gegebenen $A_\lambda \in \pi K_\lambda$ nicht immer ein $A \in \pi G$ finden mit $A \neg K_\lambda \geqq A^\lambda$. ($K_\lambda$ nichtabelsche Kompfaktgr G)
zB. in A_5 wr A_5 schreibe $\pi = \{3, 5\}$ vor

$$\left\{ \begin{array}{ll} \text{unten} & 3 \times 5 \times 5 \times \times 5 \times 5 \\ \text{oben} & 5 \end{array} \right\} \text{geht nicht}$$

(52) Fragen:

a) G einfach: $c_\pi G = 1 \Rightarrow \hat{c}_\pi G = 1$?

b) $\boxed{G \succ Q \text{ einfach } \Rightarrow c_\pi Q = 1} \Rightarrow c_\pi G = 1$?

161/162

31.1.64 (Madison)

(53) Sind die Rümpfe aller ein-dick-köpfigen subnormalen Untergr von G auflösbar („G einschichtig"), und sind für ihre einfachen Köpfe S_i zwei verschiedene Untergruppen von $\hat{S}_i$ nie ineinander enthalten, so ist

$$c_\pi(G) = \text{ Anzahl der Klassen}$$

unter G konjugierter Funktionen f auf $\Sigma = \{S_1, \cdots, S_i, \cdots\}$ mit Werten $f(S_i) =$ eine Klasse in S_i konjugierter Gruppen $\in \hat{\mathcal{M}}\pi S_i$.

(54) z.B. Wenn noch alle $S_i \cong A^5$, und $|\pi \cap \{235\}| = 2$, so hat $f(S_i)$ stets 2 mögliche Werte, daher

$$c_\pi(G) = \text{ Anzahl der orbits}$$

von G auf der Potenzmenge von Σ

$$= \frac{1}{|G|} \cdot \sum_{g \in G} 2^{\zeta(g)}$$

wo $\zeta(g)$ die Anzahl der Zyklen = orbits von g auf Σ bezeichnet.

162/163

Tü, 15.7.64

(1) $A \trianglelefteq\trianglelefteq G$, $B \leq G$, $G = \langle A, B \rangle$,
$\underbrace{\exists g \in G : \quad B^g \leq \mathcal{N}A}$ $\Rightarrow A \trianglelefteq G$.

Statt dessen genügt: $\mathcal{N}_G(A)$ deckt G/A_1 (Nov 73)
z.B. $|G : A_1| < \infty$, $B \subseteq \bigcup (\mathcal{N}A)^g \quad (g \in G)$

Bew: Sonst $A \lhd \cdots \trianglelefteq A_2 \lhd A_1 \lhd G$ (kanonische Reihe)

$$G = B \cdot A_1 \quad g = ba_1.$$
$$B^{ba_1} \leq \mathcal{N}A \leq \mathcal{N}A_2$$
$$B^{a_1} \leq \mathcal{N}A_2 = \mathcal{N}A_2^{a_1}$$
$$B \leq \mathcal{N}A_2 \quad A_2 \trianglelefteq G \quad Wid!$$

Allgemeiner:

(2) $A \trianglelefteq\trianglelefteq G$, $B \leq G$, $\exists c \in \langle A, B \rangle; B^c \leq \mathcal{N}A \Rightarrow B \leq \mathcal{N}A.$ (1)

(3) Damit kommt wohl heraus: hat eine Ugr von $\mathfrak{G}_\alpha$ $t \leq 5$ wes. Bahnen und ist $\mathfrak{G}$ pri, so hat $\mathfrak{G}_\alpha \leq 4$ wes. Bahnen.

163/164

19.7.64 2-tra Gru: 3-Relationen

(1) Die Gruppe $\mathfrak{G}$ des Grades p der Ord $p(p-1)$ ist gekennzeichnet durch die Relation

$$R : x + y = 2z$$

Bew: $\mathfrak{G}$ läßt R invariant; wenn $s \in \mathfrak{S}^p R$ invar läßt so erhält S den Mittelpkt; läßt s 0 und 1 fest, so läßt S alle $\frac{x}{2^n}$ fest $0 \leq x \leq 2^n$. Wähle $2^n > p$, dann läßt S alle $\frac{0}{2^n}, \frac{1}{2^2}, \cdots, \frac{p-1}{2^n}$ fest, also alle x:

$$\mathfrak{H} = \text{ Gru } R \Rightarrow \mathfrak{H}_{12} = 1; \text{ da } \mathfrak{G} \leq \mathfrak{H}, \text{ ist } \mathfrak{G} = \mathfrak{H}$$

(2) Die Basis-3-Relationen von $\mathfrak{G}$ sind

$$\begin{array}{rcl} G & : & x = y = z \\ U_1 & : & x \neq y = z \\ U_2 & : & y \neq x = z \\ (1) & : & z \neq x = y \\ (a) & & \begin{cases} ax - y = (a-1)z \\ x \neq y \neq z \neq x \end{cases} \qquad \text{für } {}^1_0 \neq a \in K_p \end{array}$$

(3) Bezüglich der Verknüpfung zweier Rel R, S:

$$f_R \cdot f_S = \sum_t f_R(xtz) f_S(tyz)$$

haben die char Fkt der Basis rel von $\mathfrak{G}$ die

164/165

Multiplikationstafel:

	G	U_1	U_2	$(a) \neq 0$
G	G	0	U_2	0
U_1	U_1	0	$z \neq \begin{cases} x \\ y \end{cases}$	0
U_2	0	$(p-1)G$	0	U_2
(a) $a \neq 0$	0	U_1	0	(aa')

$\square + (1)$

trivial

Hiermit müßte sich zeigen lassen, daß jede echte Obergr. von $\mathfrak{G}$ 3-tra ist.
G, U_2 erzeugen Ideal
$G, U_1, U_2, \underbrace{\sum (a)}_{z \neq \begin{cases} x \\ y \end{cases}}$ erzeugen Ideal $\mathfrak{T}$

(4) Sei $\mathfrak{R}$ der Ring der invar Fkt mit rationalen Werten.
mod 7 haben wir als Elemente die (a) mit $a \neq 0$ und der Relation $\sum(a) \equiv 0$ und der Multipl. Tafel (Für Q als Koeff **???**)

	(a')
(a)	(aa')

$$a \equiv 1, 2, \cdots, p-1 \ (p)$$

Also

$$\mathfrak{R}/\mathfrak{T} \cong Q(Z_{p-1})/(\sum a^{\nu})$$

165/166

noch 2-tra P Gr

(5) Frage: Ist der 3-Relationenring einer 2-tra Gr $\mathfrak{G} \cong$ dann 2-Rel-Ring von $\mathfrak{G}_\alpha$?
Dann könnte man so die Frage der Erweiterung einer tra PGr untersuchen
Antwort: Ja, im Wesentlichen

(6) Sei $\mathfrak{G} \leq \mathfrak{S}^\Omega$ jeder 3-Rel. $f(xyz)$ von $\mathfrak{G}$ ordne zu

besser: 7 $\qquad \widetilde{f}(x,y) = f(xy\alpha) \quad \alpha \in \Omega$ fest

Dann

$$\begin{cases} \widetilde{c_1 f_1 + c_2 f_2} &= \qquad c_1 \widetilde{f_1} + c_2 \widetilde{f_2} \\ \widetilde{f_1 \circ f_2} &= \widetilde{f_1} \circ \widetilde{f_2} \ \ \& \ \ \widetilde{f_1 f_2} = \widetilde{f_1}\widetilde{f_2} \end{cases}$$

Also $\mathfrak{R} \to \widetilde{\mathfrak{R}}_\alpha$ ist Homomorphismus $(+ \circ \cdot)$
Dabei $\widetilde{f} = 0 \iff f(xy\alpha) \equiv 0$ in x, y
Ist $\mathfrak{G}$ transitiv, so folgt $f(xyz) \equiv 0 \quad xyz$
Also:
$f \to \widetilde{f}$ ist Isomorphismus wenn $\mathfrak{G}$ tra. Aber Achtung: hier $x, y = \alpha$ zugelassen

166/167

(7) Jeder invar. Fkt $f(xyz)$ von $\mathfrak{G} = 2$ tra ordne zu

$$f_\alpha(x,y) = f(xy\alpha) \text{ für } x, y \in \Omega - \alpha$$

Dann ist

$$(f \underset{\Omega}{\circ} g)_\alpha = f_\alpha \underset{\Omega-\alpha}{\circ} g_\alpha + f(\beta\alpha\alpha) g(\alpha\beta\alpha)$$

$\underbrace{\text{mit } \beta \neq \alpha}_{\text{const.}}$

Da die Konstanten $h(xy)$ auf $\Omega - \alpha + \Omega - \alpha$ ein Ideal $\mathfrak{C}_\alpha$ bilden, und

$f = c \Rightarrow f_\alpha = c$, ist $f \to f_\alpha$ ein Homom $\mathfrak{F}/\mathfrak{C}$ auf $\mathfrak{F}_\alpha/\mathfrak{C}_\alpha$. Der Kern dieses Hom besteht aus den $f(xyz)$ mit $f(xyz) = \text{const}$ auf

$$z \neq \begin{cases} x \\ y \end{cases} ,$$

d.h. auf $(x,y) \in \langle \Omega - \alpha, \Omega - \alpha)$. Das sind die
$f = \text{ const } f_{x \neq y = z} + \text{ const } f_{y \neq x = z} + \text{ const } f_{x=y=z}$; also sind sie trivial.
[NB das sind die G, U_1, U_2 im Bsp (3)]

167/168

(8) Satz: Die bei der 2-tra Gru $\mathfrak{G}$ invarianten Funktionen, die für $z = x$ und für $z = y$ stets verschwinden (deren Träger also zu den 3 trivialen Basis rel. $x \neq y = z$, $y \neq x = z$, $x = y = z$ fremd sind) bilden einen Ring $\mathfrak{R}_0$, der vermöge $f \to f_\alpha$ nach (6) isomorph auf dem vollen Ring aller Rel von G_α abgebildet ist. Das Einselement von $\mathfrak{R}$ ist

$$f_{x=y\neq z} = \begin{cases} 1 & x = y \neq z \\ 0 & \text{sonst} \end{cases}$$

(9) Satz: Sei $\mathfrak{G}$ tra Ordnet man jeder bei $\mathfrak{G}_\alpha$ inv. Fkt $f(xy) \quad (x, y \in \Omega - \alpha)$ zu die Fkt

$$\hat{f}(xyz) = \begin{cases} f(x^g y^g), \text{ wo } \begin{cases} z^g = \alpha \\ g \in \mathfrak{G} \end{cases} & \text{wenn } z \neq {}^x_y \\ 0 & \text{wenn } z = x \text{ oder } z = y \end{cases}$$

so ist $f \to \hat{f}$ ein Isomorphismus von $\mathfrak{R}(\mathfrak{G}_\alpha)$ auf den Ring $\mathfrak{R}_0$ der 3-Fkt von $\mathfrak{G}$, die für $z = \begin{cases} x \text{ od} \\ y \end{cases} = 0$ sind
Nun in $\hat{f}$ $x \to y \to z \to x$!

168/169

Primit. P-Gr.: Allgemeines

(1) Sei $\mathfrak{G}$ pri Ω, $\alpha \notin \Gamma = $ Bahn $\mathfrak{G}_\alpha$
Sei $0 \neq \Delta \subseteq \Omega$, $\Delta^{\mathfrak{G}_\alpha} \neq \Omega$; $1 \neq \mathfrak{U} \leq \mathfrak{G}_\rho, \exists \rho \in \Omega$.
Dann $\exists G \in \mathfrak{G}$, $\mathfrak{U}^G$ ändert Δ und hat einen Fixpunkt in Γ.
Bew: $\Delta^{\mathfrak{G}_\alpha}$ ist nur bei $\mathfrak{G}_\alpha$ invariant. Wählt man also H so, daß

$$\begin{cases} \mathfrak{U}^H \not\leq \mathfrak{G}_\alpha \\ \mathfrak{U}^H \leq \mathfrak{G}_{\gamma_1} & \text{für ein } \gamma_1 \in \Gamma \end{cases}$$

was wegen Primitivität von $\mathfrak{G}$ geht, so läßt $\mathfrak{U}^H$ $\Delta^{\mathfrak{G}_\alpha}$ nicht fest, daher $\exists G_\alpha$, $\mathfrak{U}$ läßt Δ^{G_α} nicht fest; $\mathfrak{U}^{G_\alpha^{-1}}$ läßt Δ nicht fest und hat Fixpunkt $\gamma_1^{G_\alpha} = \gamma \in \Gamma$.

169/170

Anders gesagt:

(1′) $\mathfrak{G}$ pri, $0 \neq \Delta \subset \Omega$ treffe nicht alle Bahnen von $\mathfrak{G}_\nu$, Γ ist eine Bahn $\neq \alpha$ von $\mathfrak{G}_\alpha$, $1 \neq \mathfrak{U}$ hat FP $\Rightarrow \exists G \in \mathfrak{G}$; $\mathfrak{U}^G$ ändert Δ und hat FP in Γ.

170/171

Allgem. Zerschneidungssatz

Satz (1) Wirke $\mathfrak{H}$ auf $\Omega = \Gamma + \Delta$, $\Gamma^{\mathfrak{H}} = \Gamma$. Sei $\Delta = U\Delta_i$ eine Überdeckg von Δ, $\forall i : \gamma \in \Gamma, \delta \in \Delta_i \Rightarrow \Delta_i \subseteq \delta^{\mathfrak{H}_\gamma}$ Sei $\mathfrak{N} = \{N \in \mathfrak{H} \big| \Delta_i^N = \Delta_i \forall i\}$. Dann gilt $\mathfrak{N}^\Gamma \times \mathfrak{N}^\Delta \subseteq \mathfrak{H}^{(2)}$
Zu zeigen ist: zu geg. $N \in \mathfrak{N}$, $\gamma \in \Gamma$, $\quad \delta \in \Delta$
$\exists H \in \mathfrak{H} : \delta^H = \gamma,\ \delta^H = \delta^N$.
Bew: Sei $\delta \in \Delta_i$. Dann $\delta^N \in \Delta_i \subseteq \delta^{\mathfrak{H}_\gamma}$
Wähle $G \in \mathfrak{H}_\gamma$: $\delta^N = \delta^G$.

(1′) Sonderfall $\Delta_i = \delta_i^{\mathfrak{H}}$ gibt die bisherige Zerschneidung

171/172

(2) Wirke $\mathfrak{H}$ auf $\Omega = \Gamma + \Delta_i$ $\Gamma^{\mathfrak{H}} = \Gamma$. Sei $\Delta = \cup\Delta_i$ eine bei $\mathfrak{H}$ invariante (im Ganzen) Überdeckung von Δ. Es gebe $\mathfrak{K} \leq \mathfrak{H}$ derart, daß
$\begin{cases} \text{i)} \quad \mathfrak{K} \text{ in jedem } \gamma^{\mathfrak{H}} \text{ einen Fixpunkt hat} \\ \text{ii)} \quad \text{für jedes } \delta \in \Delta_i \text{ gilt } \Delta_i \subseteq \delta^{\mathfrak{K}} \end{cases}$.
Sei $\mathfrak{N} = \{N \in \mathfrak{H} \big| \Delta_i^N = \Delta_i \forall i\}$. Dann ist

$$\begin{cases} \mathfrak{N}^\Gamma \times \mathfrak{N}^\Delta \leq \mathfrak{H}^{(2)} \\ \mathfrak{N} \trianglelefteq \mathfrak{H} \end{cases}$$

Bew: Geg $\begin{cases} \gamma \in \Gamma \\ \delta \in \Delta_i \end{cases}$. Wähle $\gamma_0 := \gamma^{H_0} =$ Fixpunkt $\mathfrak{K}$.
$\delta_0 := \delta^{H_0} \in \Delta_i^{H_0} = \Delta_0$. Nach Vor ist

$$\Delta_0 \subseteq \delta_0^{\mathfrak{K}} \subseteq \delta_0^{\mathfrak{H}_{\gamma_0}} = \delta^{H_0 \mathfrak{H}_{\gamma_0}}$$

also

$$\Delta_i \subseteq \delta^{H_0 \mathfrak{H}_{\gamma_0} \overline{H}_0} = \delta^{\mathfrak{H}_\gamma};\ (1)$$

Allgemeiner:

(3) $\Omega = \Gamma + \Delta$, $\mathfrak{H} \leq \mathfrak{G}$, $\Gamma^{\mathfrak{H}} = \Gamma$
$\mathfrak{H}$ habe in Γ die wes. Bahnen Γ_i, in Δ die Bahnen Δ_j
$\forall i, j \exists \gamma_i \in \Gamma_i$, $\delta_j \in \Delta_j : \Delta_j \leq \delta_j^{\mathfrak{G}_{\gamma_i}}$.
Dann ist $\mathfrak{H}^\Gamma$, $\mathfrak{H}^\Delta \leq \mathfrak{G}^{(2)}$

$\lhd\lhd$ Perm Gr.

(1) $\mathfrak{G}$ sei tra, $\mathcal{S}\mathfrak{G} \in$ max und werde von zwei subnorm. Ugr'en $\mathfrak{A}, \mathfrak{B}$ erzeugt; dann ist $\mathfrak{A}$ oder $\mathfrak{B}$ fixpunktfrei.
Bew: sonst hat $(\mathfrak{A}, \mathfrak{B}^g)$ Fixpkt, ist $\neq \mathfrak{G}$. aber:

(2) $\langle \mathfrak{A}, \mathfrak{B} \rangle = \mathfrak{G}$, $s\mathfrak{G} \in$ max, $\mathfrak{A}, \mathfrak{B} \trianglelefteq\trianglelefteq \mathfrak{G} \Rightarrow \langle \mathfrak{A}, \mathfrak{B}^g \rangle = \mathfrak{G}$.
denn sind $\langle \mathfrak{A}, \mathfrak{B}^g \rangle = \overline{\mathfrak{G}} \lhd\lhd \mathfrak{G}$
$\langle \mathfrak{A}, \mathfrak{B}^g \rangle^{\mathfrak{G}} < \mathfrak{G}$ aber $=$.

Frage:

(3) Welche unendlichen $\mathfrak{G}$ haben die Eigenschaft:

$$\mathfrak{A}, \mathfrak{B} \trianglelefteq\trianglelefteq \mathfrak{G}, \quad \langle \mathfrak{A}, \mathfrak{B} \rangle^{\mathfrak{G}} = \mathfrak{G} \Rightarrow \langle \mathfrak{A}, \mathfrak{B} \rangle = \mathfrak{G}?$$

anders geschrieben wird verlangt:

$$\mathfrak{A}, \mathfrak{B} \lhd\lhd \mathfrak{G}, \quad \mathfrak{A}^{\mathfrak{G}} \cdot \mathfrak{B}^{\mathfrak{G}} = \mathfrak{G} \Rightarrow \langle \mathfrak{A}, \mathfrak{B} \rangle = \mathfrak{G}$$

S-Ringe: Vollst.- Eig.

(1) Ist $\mathfrak{H} = \langle P \rangle \times \langle Q \rangle$ el abelsch Typ (p, p), so ist, mit $R = \langle PQ \rangle$, der von $1, \langle P \rangle, \langle Q \rangle, \langle PQ \rangle$, $\mathfrak{H}$ erzeugte Modul $\mathfrak{M}$, obwohl er S-Ring ist, deswegen nicht einbettbar, weil jeder einbettbare S-Ring, gedeutet als Gesamtheit $\mathfrak{F}$ invarianter Funktionen von 2 Variabl., die folgenden Eigenschaft hat (die $\mathfrak{M}$ nicht hat):

$$f(x\xi)g(\xi y)g(x\eta)f(\eta y)h(\xi\eta)$$

Aus $f, g, h \in \mathfrak{F}$ folgt

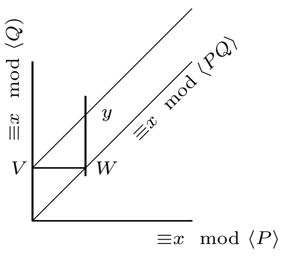
$$(*) \qquad \sum_{V,W} f(XV)g(VY)g(XW)f(WY)h(VW) \in \mathfrak{F}$$

Wähle bei $\mathfrak{M}$

$$\begin{aligned} f(X, Y) &= \chi_{\langle Q \rangle}(XY') \\ g(X, Y) &= \chi_{\langle PQ \rangle}(XY^{-1}) \\ h(X, Y) &= \chi_{\langle P \rangle}(XY^{-1}) \end{aligned}$$

$\chi_{\mathfrak{M}} =$ Charakt Fkt von $\mathfrak{M}$
Aus $(*)$ folgt nämlich dann:

$$\exists U, V \left\{ \begin{array}{c|c} Y \equiv W\langle Q \rangle & \text{wenn ein } \mathbf{???}SR \\ X \equiv W\langle R \rangle & \langle P \rangle \langle Q \rangle \\ X \equiv V\langle Q \rangle & \langle R \rangle \text{ enthält,} \\ V \equiv Y\langle R \rangle & \text{so auch } * \\ V \equiv W\langle P \rangle & \langle PQ^2 \rangle \end{array} \right.$$



174/175

Invariante Funktionen bei P Gr. 9.8.64

Hi Satz 1. Sei $\mathfrak{H} \leq \mathfrak{G}$, $\mathfrak{H}$ tra Ω, $0 \in \Omega$. Sei $\mathfrak{M}_0 \subseteq \Omega^{k-1}$ $(k \geq 2)$, $\mathfrak{M}_0$ inv bei $\mathfrak{H}_0$.
Definiere $\mathfrak{M} \subseteq \Omega^k : (\xi_1, \cdots, \xi_k) \in \mathfrak{M} \iff$ für jedes $N \in \mathfrak{H}$ mit $\xi_k^H = 0$ ist $(\xi_1^H, \cdots, \xi_{k-1}^H) \in \mathfrak{M}_0$ besser k durch $k+1$ ersetzen
Dann gilt: $\underline{\mathfrak{M} \text{ inv } \mathfrak{G} \iff \mathfrak{M}_0 \text{ inv } \mathfrak{G}_0}$
Bew: $\Rightarrow$ $(\xi_1 \cdots \xi_{k-1}) \in \mathfrak{M}_0$, $G_0 \in \mathfrak{G}_0 \Rightarrow (\xi_1, \cdots, \xi_{k-1}, 0) \in \mathfrak{M}$, da $\mathfrak{M}_0$ inv $\mathfrak{G}_0$ $(\xi_1^{G_0}, \cdots, \xi_{k-1}^{G_0}, 0) \in \mathfrak{M}$
$H = 1 : (\xi_1^{G_0} \cdots \xi_{k-1}^{G_0}) \in \mathfrak{M}_0 \Rightarrow \mathfrak{M}_0$ inv $\mathfrak{G}_0$
$\Leftarrow$ $\mathfrak{M}_0$ inv $\mathfrak{G}_0$
Nach Def. ist

$$\begin{aligned} \mathfrak{M} &= \{(\xi_1 \cdots \xi_{k-1} 0)^H \big|_{H \in \mathfrak{H}} \ (\xi_1 \cdots \xi_{k-1}) \in \mathfrak{M}_0\} \\ \text{also} \quad \mathfrak{M} &= (\mathfrak{M}_0, 0)^{\mathfrak{H}} \\ &= (\mathfrak{M}_0, 0)^{\mathfrak{G} \circ \mathfrak{H}} = (\mathfrak{M}_0, 0)^{\mathfrak{G}} \text{ inv. } \mathfrak{G} \end{aligned}$$

unnötig, siehe $2'$-$3'$

Satz 0 Ist $f(xy\cdots)$ inv. bei $\mathfrak{U} \leq \mathfrak{G}$ und $\mathfrak{G} = \sum\limits_1^n G_\nu \mathfrak{U}$, so ist $\sum\limits_{\nu=1}^n f(x^{G_\nu} y^{G_\nu} \cdots)$ inv. bei $\mathfrak{G}$.

175/176

Satz 2. $\mathfrak{H} \leq \mathfrak{G}$, $\mathfrak{H}$ tra Ω, $0 \in \Omega$; f eine Funktion von k Veränd. in Ω
Dann $f(\xi_1 \cdots \xi_k)$ inv $\mathfrak{G}$

$$\iff \quad \begin{array}{l} \exists g(\xi_1 \cdots \xi_{k-1}) \text{ inv. } \mathfrak{G}_0 \\ f(\xi_1 \cdots \xi_{k-1} \xi_k) = \\ g(\xi_1^H \cdots \xi_{k-1}^H) \text{ wenn } \xi_k^H = 0 \end{array}$$

Besser $2'$ S. 177.
Bew $\Rightarrow$ Sei $f(\xi_1 \cdots \xi_k)$ inv $\mathfrak{G}$. Setze $g(\xi_1 \cdots \xi_{k-1}) = f(\xi_1 \cdots \xi_{k-1} 0)$

a)

$$\begin{aligned} g(\xi_1^{G_0} \cdots \xi_{k-1}^{G_0}) &= f(\xi_1^{G_0} \cdots \xi_{k-1}^{G_0} 0^{G_0}) = f(\xi_1 \cdots \xi_{k-1} 0) \\ &= g(\xi_1 \cdots \xi_{k-1}) \Rightarrow g \text{ inv. } \mathfrak{G}_0 \end{aligned}$$

b)

$$\xi_k^H = 0 \Rightarrow f(\xi_1 \cdots \xi_{k-1} \xi_k) = f(\xi_1^H \cdots \xi_{k-1}^H 0) = g(\xi_1^H \cdots \xi_{k-1}^H)$$

$\Leftarrow$ Sei g inv $\mathfrak{G}_0$, $f(\xi_1 \cdots) = g(\xi_1^H \cdots)$ wenn $\xi_k^H = 0$. Für gegebenes $(\alpha_1 \cdots \alpha_k) \in \Omega^k$ setze

$$c_0 := f(\alpha_1 \cdots \alpha_k) \qquad \mathfrak{M} = \{(\xi_1 \cdots \xi_k) \big| f(\xi_1 \cdots \xi_k) = c_0\}$$
$$\mathfrak{M}_0 = \{(\xi_1 \cdots \xi_{k-1}) \big| g(\xi_1 \cdots \xi_{k-1}) = c_0\}$$

Dann gilt: $(\xi_1 \cdots \xi_k) \in \mathfrak{M} \iff$ für jedes H mit $\xi_k^H = 0$ ist $(\xi_1^H \cdots \xi_{k-1}^H) \in \mathfrak{M}_0$

$\mathfrak{M}_0$ inv $\begin{cases} \mathfrak{G}_0 \\ \mathfrak{H}_0 \end{cases}$; daher erfüllen $\mathfrak{M}$, $\mathfrak{M}_0$ die Vor von Hi Satz 1, also ist $\mathfrak{M}$ inv $\mathfrak{G}$ daher $(\alpha_1, \cdots, \alpha_k)^G \in \mathfrak{M}$ $\;f(\alpha_1^G \cdots \alpha_k^G) = f(\alpha_1 \cdots \alpha_k)$ f inv $\mathfrak{G}$

unnötig, siehe $2'$-$3'$

176/177

noch invar. Fkt

Nun Vor reg. Ugr:

Satz 3: Sei $\Omega = \mathfrak{H}$, $\mathfrak{G}$ wirke auf Ω, $K^H = KH \quad (H \in \mathfrak{H})$
Dann $f(x_1 \cdots x_k)$ inv $\mathfrak{G} \iff \underset{g}{\exists} f(x_1 \cdots x_k) = g(x_1\widetilde{x}_k, \cdots, x_{k-1}\overline{x}_k)$ mit $g(u_1 \cdots u_{k-1})$ inv $\mathfrak{G}_1$ (1=neutr El. $\mathfrak{H}$) und wenn es so ein g gibt, dann

$$g(u_1 \cdots u_{k-1}) \cdot f(u_1 \cdots u_{k-1} 1)$$

siehe $3'$
Bew: die $\mathfrak{G}$ der rechts angeg. Eig sind die mit der Eig. 2:

$x_k^H = 1 \iff H = x_k^{-1}$
Besser und direkter: Sei $\mathfrak{H}$ tra $\Omega, \mathfrak{H} \leq \mathfrak{G}$

Satz $2'$ $f(x_1 \cdots x_{k+1})$ inv $\mathfrak{G} \iff f(x_1 \cdots x_{k+1})$ inv $\mathfrak{H}$ & $f(x_1 \cdots x_k 0)$ inv $\mathfrak{G}_0$
Bew: $\Leftarrow G \in g \rightarrow$; wähle $K \in \mathfrak{H}$, $0^K = x_{k+1}$
$f(x_1^G \cdots x_{k+1}^G) = f(y_1^{KG} \cdots 0^{KG})$
$KG = G_0 H$ setze $y_i^K = x_i \quad (i = 1 \cdots k)$
Voller Bew S. 179

Satz 4: Vollstdigkeitseig der k- Invarianten von $\mathfrak{G}_1$:
Sei wie in 3 $\Omega = \mathfrak{H}$; Dann gilt:

a) Aus $f(x_1 \cdots x_\mu \cdots x_r \cdots x_k)$ inv $\mathfrak{G}_0$ folgt natürlich $f(x_1 \cdots x_r \cdots x_\mu \cdots x_k)$ inv $\mathfrak{G}_0$ (kurz: $\in \mathfrak{F}_0$)
b) $f(x_1 \cdots x_k) \in \mathfrak{F}_0 \rightarrow \sum_t f(x_1 \cdots t \cdots t \cdots x_k) \in \mathfrak{F}_0$
c) Aus $f(x_1 x_\nu x_k)$ inv $\mathfrak{G}_0$ folgt $f(x_1\overline{x}_\nu, \cdots, \overline{x}_\nu \cdots, x_k\overline{x}_\nu)$ inv $\mathfrak{G}_0$ $(\nu = 1 \cdots k)$

d) siehe 178

(e) $f(x_1 \cdots x_k)$, $g(u)$ inv $\mathfrak{G}_0 \Rightarrow$
FALTUNG
$\sum_{t \in \mathfrak{H}} f(x_1, \overline{t} \cdots x_k \overline{t}) g(t)$ inv $\mathfrak{G}_0$
NB: für $k = 1$ ist das Schurs Ring-Eig.

(e′) Man braucht die Summation in e nur über eine beliebige bei $\mathfrak{G}_1$ feste Teilmenge $\mathfrak{T}$ von $\mathfrak{H}$ zu erstrecken (ersetze g durch $g \cdot \chi_{\mathfrak{F}}$)

177/178

d) $f(u)$ inv $\mathfrak{G}_1 \rightarrow f(u^{-1})$ inv $\mathfrak{G}_0$

e″) $f(x_1 \cdots x_k)$, $g(u)$ inv $\mathfrak{G}_0 \rightarrow \sum_{t \in \alpha^{\mathfrak{G}_0}} f(x_1 t, \cdots, x_k t) g(t)$ inv $\mathfrak{G}_0$

f)

$$f(x_1 \cdots x_k) \in \mathfrak{F}_1 \Rightarrow \begin{cases} f(x_1 \overline{x_{k+1}}, \cdots, x_k \overline{x_{k+1}}) \in \mathfrak{F}, \text{ daher auch} \\ f(x_1 \overline{x_k}, \cdots, x_{k-1} \overline{x_k}, 1) \in \mathfrak{F}. \end{cases}$$

g) Ist $\mathfrak{U} \leq \mathfrak{G}$, $f(x \ldots)$ inv $\mathfrak{G}_0$, $h(x)$ inv $\mathfrak{U}$, so

$$f \circ h = \sum_t \hat{f}(x_1 t_{\cdot\cdot}^{-1}) h(t) \text{ inv } \mathfrak{U}.$$

Bew:

c) $k = 1$

$$\begin{aligned} & f(x_1, \overline{x}_{k+1} \cdots x_k \overline{x}_{k+1}) \text{ inv } \mathfrak{G} \quad x_1 \leftrightarrow x_{k+1} \\ \Rightarrow\ & f(x_{k+1}, \overline{x}_1 \cdots x_k \overline{x}_1) \text{ inv } \mathfrak{G} \quad x_{k+1} = 1 \\ \Rightarrow\ & f(\overline{x}_1 \ \ x_2 \overline{x}_1 \cdots x_k \overline{x}_1) \text{ inv } \mathfrak{G} \end{aligned}$$

d) folgt aus c ($k = 1$)

g) $f(xy^{-1}) h(y)$ inv $\mathfrak{U}$

h) $\mathfrak{H}$ add geschrieben:

$$\left.\begin{array}{r} f(x - y - y) f(y - x \ \ x) \\ f(xy) \in \mathfrak{F}_0 \rightarrow f(y, x), f(-x \ \ y - x)(-y \ \ x - y) \end{array}\right\} \in \mathfrak{F}_0$$

i) S. 179

Kurzer Beweis der Hauptsachen mit (Vor $\mathfrak{H}$ reg, $\Omega = \mathfrak{H}$)

Satz 3′

a) $f(x_1 \cdots x_{k+1}) \in \mathfrak{F} \rightarrow f(x_1 \cdots x_k \ 1) \in \mathfrak{F}_1$

b) $f(x_1 \cdots x_k) \in \mathfrak{F}_1 \rightarrow f(x_1 \overline{x}_{k+1}, \cdots, x_k \overline{x}_{k+1}) \in \mathfrak{F}$

c) $\cdots \rightarrow f(x_1 \overline{x}_k, \cdots, x_{k-1} \overline{x}_k, 1) \in \mathfrak{F}$
Bew

b): Satz $2'$.

c) b mit x_{k-1} ident x_k

178/179

Beweis von Satz $2'$: $\mathfrak{H}$ tra $\Omega \ni 0$

Beh: $f(x_1 \cdots x_k\ 0) \in \mathfrak{F}_0$, $f(x_1 \cdots x_k x_{k+1})$ inv $\mathfrak{H} \Rightarrow f(x_1 \cdots x_k x_{k+1}) \in \mathfrak{F}$

$$f(x_1^G \cdots x_{k+1}^G) = f(y_1^{HG} \cdots 0^{HG}) \text{ wo } \begin{cases} H : 0^H = x_{k+1}, \\ x_i = y_i^H, H \in \mathfrak{H} \\ y_{k+1} = 0 \end{cases}$$

$$\begin{aligned} &= f(y_1^{G_0 L} \cdots 0^{G_0 L}) \quad \text{wo } H = G_o L, L \in \mathfrak{H} \\ &= f(y_1^{G_0 L} \cdots 0^{L}) \\ &= f(y_1^{G_0} \cdots 0) \quad \text{da } f \text{ inv. } \mathfrak{H} \\ &= f(y_1 \cdots 0) \quad \text{da } f(x_1 \cdots 0) \in \mathfrak{F}_0 \\ &= f(y_1^H \cdots 0^H) = f(x_1 \cdots x_{k+1}) \end{aligned}$$

Wahrscheinlich ist 3 zu verallg. mittels $\Omega = \mathfrak{H}/\mathfrak{H}_1$

i) $f_0(xy\ldots)$ inv $\mathfrak{G}_0 \to \sum_{t\in\mathfrak{T}} f_0(x-t\ \ y-t\ \ \cdots)$ inv bei jeder Ugr von $\mathfrak{G}$, die $\mathfrak{T}$ als Ganzes fest läßt.

179/180

5. Beispiel: Gruppen vom Grad p

Sei $\Omega = K_p$ $\quad \mathfrak{H} : x^H = x + 1$ $\mathfrak{H} \leq \mathfrak{G} =$ einf. tra.

a) Bestimmung der $f(x) \in \mathfrak{F}_\Delta$

$$1, x^{p-1} \in \delta_0$$

Da $\mathfrak{G}_0$ nicht tra auf $\Omega - 0$, gibts 3 lin un inv Polynome
$\exists g \in \mathfrak{F}_0$, Gr $g < p-1$, $g(0) = 0$
hierunter wähle g so, daß g normiert und Grad $g = m =$ min
Ist $\mathfrak{T}$ Bahn von $\mathfrak{G}_0$ in $\Omega - 0$, so nach $4e'$ (mit 2. Fakt. $= 1$)

$$\mathfrak{F}_0 + \sum_{t\in\mathfrak{T}} g(x+t) - \sum_{t\in\mathfrak{T}} g(x) = \sum_{\substack{t_i \\ 1\leq\nu\leq m}} g_\nu(x) t^\nu = h(x)$$

$$g(x+t) = \sum_0^m g_\nu(x) t^\nu, \quad g_0 = g$$

da Gr $h < m$, ist $h = \text{const}$, also

$$\sum_{\mathfrak{T}} t^\nu = 0 \qquad \nu = 1, \cdots, m-1 \text{ wegen Gr } g_\nu = m - \nu$$

daher ist $|\mathfrak{T}| \geq m$
Ferner ist da $g \in \mathfrak{F}_0$ und $\mathfrak{G}_0$ tra $\mathfrak{T}$

$$\begin{aligned} g(t) - g(t_1) &= \text{const auf } \mathfrak{T} \ \ (t_1 \in \mathfrak{T} \text{ fest}) \\ &= 0 \end{aligned}$$

also $m \geq |\mathfrak{T}|$; $m = |\mathfrak{T}|$

$$g(t) = g(t_1) + \prod_{t \in \mathfrak{T}} (x - t)$$

wegen $\sum t^\nu = 0$, $\nu = 1, \cdots, m-1$ sind die ersten $m-1$ el sym Fkt der t auch 0, als $\prod (x-t) = x^m + \text{ const}$

$$g(x) = x^m + \text{ const } = x^m$$

wegen $g(0) = 0$

$$x^m \in \mathfrak{F}_0$$

180/181

hieraus folgt $m | p-1$ da für $x^{G_0} = x'$ $(x \neq 0)$ stets

$$\begin{aligned} x^{p-1} &= x'^{\,p-1} \\ x^m &= x'^{\,m} \qquad p - 1 = qm + r, \ r < n \\ x^\nu &= x'^{\,\nu} \qquad x^r \in \mathfrak{F}_0 \qquad r = 0 \end{aligned}$$

Nicht nötig fürs folgende:
NB: Hieraus folgt, dass $1, x^m, x^{2m} \cdots, x^{p-1}$ K-Basis von $\mathfrak{F}_0$ sind, denn ein m und richtige Anzahl $\frac{p-1}{m} + 1$ da festes Bahn $\mathfrak{T} \subseteq \Omega - \alpha$ die Länge m hat.

b) Einige 2-Invarianten. Mit x^m enthält $\mathfrak{F}_0$ (impr $\mathfrak{F}$) nach $4f$ auch $(x-y)^m$ und $\mathfrak{F}_0$ enthält mit jeder Form $\begin{cases} f(x) \\ g(x) \end{cases}$ vom Grade m auch

$$\sum_{t \in K} t^{p-1-m} \cdot f(xt) g(ty)$$

$$
\begin{aligned}
f \circ g &:= \sum_{t \in K} f(x,t) g(t,y) t^{(p-1-m)^{\checkmark \equiv 0 \mod m}} \\
& \quad f = \sum f_\mu x^\mu y^{m-\mu} \quad g = \sum g_\nu x^\nu y^{m-\nu} \quad \Rightarrow \\
-f \circ g &= \sum_{\mu,\nu} f_\mu (x)^\mu t^{m-\mu} g_\nu t^\nu y^{m-\nu} \Big|_{t^m} \text{ wegen } \sum t^\nu = 0 \\
& \qquad \qquad \qquad \qquad \qquad \begin{cases} p-1 \nmid \nu \\ \text{od. } \nu = 0 \end{cases} \\
&= \sum_{\mu=0}^{m} f_\mu g_\mu x^\mu y^{m-\mu}
\end{aligned}
$$

181/182

Da die Koeff in $f = (x-y)^m$ alle $\not\equiv 0$, ist

$$
\underbrace{f \circ \cdots \circ f}_{p-1} = x^m + x^{m-1} y + \cdots + y^m = \frac{x^{m+1} - y^{m+1}}{x - m}_{(x \neq y)}
$$

Daher

$$
h = \begin{cases} \frac{x^{m+1} - y^{m+1}}{x-y} & x \neq y \\ m x^m & x = y \end{cases} \to h \in \mathfrak{F}_0
$$

$x \neq 0$, $x' := x^{G_0} \Rightarrow$

$$
\frac{x^{m+1} - y^{m+1}}{x - y} = \frac{x'^{\, m+1} - y'^{\, m+1}}{x' - y'} \quad (x \neq y)
$$

subtrahiere $x^m = x'^{\, m}$:

$$
\frac{(x^m - y^m) y}{x - y} = \frac{(x'^{\, m} - y'^{\, m}) y'}{x' - y'} \text{ wegen } \quad x^m = x'^m
$$

$$
\frac{x'}{x} = \frac{y'}{y} \leftarrow y x' = x y' \quad \leftarrow \frac{y}{x-y} = \frac{y'}{x' - y'} \text{ wenn } \quad x^m \neq y^m
$$

das gilt aber auch für $x^m = y^m (\neq 0)$, da dann $\exists c$ mit $x^m \neq c^m$, also

$$
\frac{x'}{x} = \frac{c'}{c} = \frac{y'}{y}
$$

also zu G_0 $\exists a :\ \ x^{G_0} = ax$ für $x \neq 0$ auch für $x = 0$.
Zu G $\exists$ a, b; $x^G = ax + b$

182/183

Noch Gruppen vom Grad p

A. NB: Bei Ausnutzung der zykl Vert. C der Ord 3:

$$f(x\ y) \in \mathfrak{F}_1 \to f(y-x \quad -x) \quad \text{hat Ord 3}$$

Im Fall $\Omega = K_p$ wird es zweckmäßig sein, Funktionen auf $\Omega \times \Omega$ mit Werten aus K_{p^2} zu betrachten, damit die 3. Einh Wurzeln da sind.

B. NB: $\mathfrak{G}$ vom Grad p ist 3-tra genau wenn $\mathfrak{G}^*_{1-1}$ nur die beiden Bahnen $\{1-1\}$ und $\Omega - \{1-1\}$ hat. Will man also indirekt zeigen, daß $\mathfrak{G}$ 3-tra, so kann man annehmen $\mathfrak{G}^*_{1-1}$ hätte 3 Bahnen und damit drei lin un 2-Invarianten.

C. Die Gesamtheit $\mathfrak{F}$ der Vertauschungsmatrizen derjenigen Gruppen auf $1, 2, \cdots, (p-1)$, die zur Gruppe $\mathfrak{G}_0$ einer Gr des Grades p gehören, hat die Vollstd-Eig:

$$f(x\ y) \in \mathfrak{F} \Rightarrow f(x-y \quad -y) \in \mathfrak{F}$$

wo

$$f(0, y) = f(x, 0) = 0$$

gesetzt werden kann. Das bedeutet:

$$\begin{array}{c} {\scriptstyle i} \\ \downarrow \\ \begin{pmatrix} a \\ b \\ \vdots \\ c \\ 0 \\ d \\ \vdots \\ e \end{pmatrix} \end{array} \in \mathfrak{F} \Rightarrow \begin{array}{c} {\scriptstyle p-1} \\ \downarrow \\ \begin{pmatrix} d \\ \vdots \\ e \\ 0 \\ a \\ b \\ \vdots \\ e \end{pmatrix} \end{array} \in \mathfrak{F}.$$

Das ist wohl eine der 6 „Spiegelungen“ der Bahnen von $\mathfrak{G}_{01}$
Wenn $N \in \mathcal{N}\mathfrak{P}$ mit $N^2 = 1$, so gilt auch $f(y-x\ y) \in \mathfrak{F}$:

$$\begin{array}{c} \begin{pmatrix} a \\ \vdots \\ c \\ 0 \\ d \\ \vdots \\ e \end{pmatrix} \\ \uparrow \\ {\scriptstyle i} \end{array} \in \mathfrak{F} \Rightarrow \begin{array}{c} \begin{pmatrix} c \\ \vdots \\ a \\ 0 \\ e \\ \vdots \\ d \end{pmatrix} \\ \uparrow \\ {\scriptstyle i} \end{array} \in \mathfrak{F}.$$

183/184

Das muss nützlich für die Untersuchung der nicht 3-tra Gruppen $\mathfrak{G}$ vom Grad p sein. Ferner:

c$'$. Frage: Sei $\mathfrak{V}$ ein Ring von Matrizen mit dieser Symmetriebedgg, bestehend aus allen Matrizen, die mit einer geg tra 2-abg P Gr $\mathfrak{H}$ auf $\{12\cdots p-1\}$ vertauschbar sind; ist dann $\mathfrak{H}\mathfrak{P} \doteq \mathfrak{P}\mathfrak{H}$ mit $\mathfrak{P} = \langle P\rangle$, $P : x \to x+1$?

184/185

noch Gruppen vom Grad p.

d) Ist $\mathfrak{G}$ 2-tra, $f(xy) \in \mathfrak{F}_0$, so ist

$$\sum_t f(x-t, y-t) \text{ inv } \mathfrak{G}, \text{ also } = (x-y)^{p-1} \cdot c + d$$

$$\begin{aligned} f_{\kappa\lambda}(x,y) = \sum_t (x-t)^k (y-t)^l &= -\sum_{\kappa+\lambda=p-1} x^{k-\kappa} y^{l-\lambda} \binom{k}{\kappa}\binom{l}{\lambda} \\ &= \text{Form vom Grad } k+l-(p-1) \end{aligned}$$

Ist also $f(xy) \in \mathfrak{F}_0$, $f = \sum h_k$, h_k homogen vom Grade k, so ist

$$\sum h_k(x-t, y-t) = \begin{cases} 0 & k < 2p-2 \\ -(x-y)^{p-1} & k = l = p-1 \end{cases}$$

e) Die Faltung definiert man besser nicht durch $\sum f(x-t)g(t)$, sondern durch

$$f \circ g = -\sum_{t=0}^{p-1} f(x-t)g(t) = f(x-t)g(t)\big|_{t^{p-1}}$$

Dann gilt nämlich

$$x^{p-1} \circ x^k = \begin{cases} x^k & k = 0, 1 \cdots, p-2 \\ x^{p-1} + 1 & k = p-1 \end{cases}$$

daher $x^{p-1} \circ f(x) = f(x)$ wenn Grad $f < p-1$.

f) mit $(\Delta f)(x) = f(x+1) - f(x)$ gilt

$$\Delta(f \circ g) = (\Delta f) \circ g$$

Ferner

g)

$$f \circ g = g \circ f, \quad f \circ (g \circ h) = (f \circ g) \circ h$$

185/186

h)

$$\begin{cases} 1 \circ g = \begin{cases} 0 & \text{Gr } g < p-1 \\ +1 & g = t^{p-1} \end{cases} \\ 1 \circ g = g_{p-1}, \text{ wenn } g(t) = \sum\limits_{0}^{p-1} g_\nu t^\nu . \end{cases}$$

$n = p^\alpha$

i) Bei regulären Ugr vom Typ $(p, \cdots, p)$ ist Betrachtung des $\mathfrak{G}_0$-invarianten Polynoms $g(x)$ niedrigsten Grades und $g(G) = 0$ nützlich: es hat die Gestalt

$$g = x^k h(x^{p-1})$$

(Bew: $g(cx) = c^m g(x)$)
Wahrscheinlich ist $k \big| p-1$ (Bew: $x \to cx$) und $f(x) = f(x^{\frac{p-1}{p}})$ für jedes $f \in \mathfrak{F}$ wenigstens bei 2 abgeschlossenen $\mathfrak{G}$.

186/187

P-Gruppen $\mathfrak{G}$ vom Grad p^2 mit reg. elem Ugr.

(1) Wähle $K_{p^2} := \Omega =$ Wertevorrat der Funktionen. Die bei $\mathfrak{G}$ invar. Fkt. sind Polynome in $x, y, \cdots$ vom Grad $\leq q := p^2 - 1$ in jedem
<u>Azimutalen Fall:</u> Die primären Komplexe $\neq$ triv. sind konjugiert. In additiver Schreibweise: mit $f(x) \in \mathfrak{F}_0$ und $a \in K_p$ ist $f(ax) \in \mathfrak{F}_0$

(2) $\mathfrak{F}_0$ enthält, wenn n nichttriviale Bahnen von $\mathfrak{G}_0$ existieren, mit $e = \frac{p-1}{n}$ genau eine Fktion der Gestalt

$$\begin{cases} f_\lambda(x) - x^{\lambda e} h_\lambda(x^{p-1}) & (\lambda = 1 \cdots n) \\ f_\lambda(1) = 1 \end{cases}$$

Sie ist gekennzeichnet durch

$$f_\lambda(ax) = a^{e\lambda} f(x) \quad (\forall a \in K_p) \text{ Dabei } f_n = 1 - \delta_{x,0}$$

(3) NB: Dies kann auch ohne Anwendung von Polynomen zum Nachweis der Existenz und Eindtgkeit von f_λ direkt dienen, wobei „1“ dann irgend ein festes Element $\neq 0$ von Ω bezeichnet und über den Wertevorrat der Funktionen nur vorausgesetzt

187/188

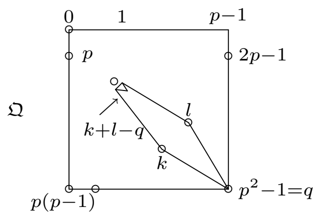
wird: Körper der n n-te Einheitswurzeln enthält).

(4)
$$\begin{cases} x^k \circ x^l = (-1)^{l+1}\binom{k}{k+l-q} x^{k+l-q} = c x^{k+l-q} \\ f(x+y) = \sum y^i f_i(x), \quad f_i = -f \circ x^{q-i} \end{cases}$$

wenn $2 \big| q = p^2 - 1$

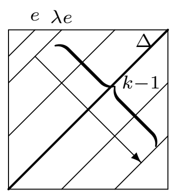
(5)
$$0 \leq a_i, b_i \leq p-1 \Rightarrow \left(\begin{array}{c} a_0 + a_1 p + \cdots + a_m p^m \\ b_0 + b_1 p + \cdots + b_m p^m \end{array} \right) = \prod \binom{a_i}{b_i}$$

(6) Nach (5) ist $x^k \circ x^l \neq 0$ genau wenn $k+l-q$ innerhalb od. auf Rand des Quadrates



bleibt:

(7) Die in f_λ auftretenden Potenzen liegen auf Schräglinien:



(8) Kein $f(x) \in \mathfrak{F}_0$ enthält eine Potenz aus $\Delta = \boldsymbol{/}$. Sonst wäre ein $f \neq$ const $\cdot x^q$ inv $\mathfrak{G}$ und in $x \to ax$, $a \in K_p$. Solche f sind aber $= \alpha + \beta x^2$.

188/189

9) f_1 hat gewisse Potenzen aus der 1. Schräglinie unter der Diagonalen $\boldsymbol{/} =: \Delta$ Denn sonst hätte f_1^n Potenzen auf Δ. $\rightarrow\leftarrow$ (7)

(10) f_{n-1} hat nur Potenzen über Δ. Sonst hätte nach (6) $\underbrace{f_{n-1} \circ \cdots \circ f_{n-1}}_{n}$ Potenzen auf Δ.

(11) Nicht $n = 2$: Bew (10), (9)
Nicht n gerade.

(12)

$$\begin{cases} (f_\lambda)^k = f_{k\lambda} & \lambda = 1, 2, \cdots \\ f_\lambda f_\mu = f_{\lambda+\mu} \end{cases}$$

Bew: 2

(13)

$$\begin{cases} f_\lambda \circ f_\mu = c_{\lambda\mu} \cdot f_{\lambda+\mu} & (\lambda + \mu \neq n) \text{ Bew: 2} \\ f_\lambda \circ f_{n-\lambda} = -1 \end{cases}$$

Bew: $\big|_{=0} = \sum{}' f_\lambda(t)^1 f_1(t) = q$

NB(13′) Bei Fkt mit Werten in bel Körper nach (3) gilt statt 13_2

$$f_\lambda \circ f_{n-\lambda} = q \cdot \delta_{x,0} - f_n = -1 + \gamma^2 \delta_{x,0}$$

189/190

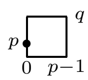
(14) Ist f^* das f_λ von kleinstem Grad, so ist $f^* \circ f =$ const für jedes $f \in \mathfrak{F}_0$ mit Grad $f < q$, das heißt $\sum f(t) = 0$.

Bew:

(15) Grad $f \circ g \leq$ Grad f (in normierter Schreibw, von Gr $\leq q$); und $<$ wenn Gr $g < q$ Bew (6)

(16) Für das f^* von (14) gilt ferner:

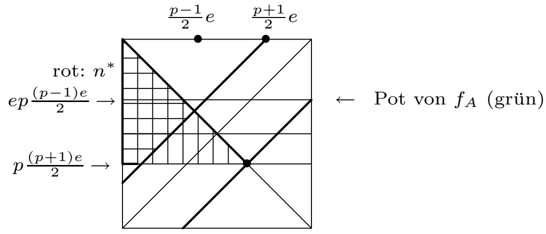
$$\begin{cases} n^* = \text{Gr } f^* \leq \frac{p+1}{2} \cdot p \\ f^* \text{ hat nur Potenzen über } \Delta. \end{cases}$$

[NB: Künftige Aufschreibung wäre besser mit q: 

, dann Δ $\backslash$, und die kleineren Exponenten liegen <u>unter</u> Δ.]
Zum Beweis: nach 11 ist n ungerade

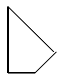
(17) Genau eins von f_λ und $f_{n-\lambda}$ $(0 < \lambda < n)$ hat Potenzen nur über der Diagonalen Δ.
Sonst $f_\lambda \circ f_{n-\lambda} \ni$ Potenzen auf Δ. $\rightarrow\leftarrow$ (8), oder $f_\lambda \circ f_{n-\lambda} = 0 \rightarrow\leftarrow$ (13)
Bew (16): Mindestens $f_{\frac{p-1}{2}}$ oder $f_{\frac{p+1}{2}}$ haben nur Potenzen über Δ $(\geq)$. Also mindestens $n^* =$ Gr $f^* \leq$ Gr $f_{\frac{p-1}{2}} \leq \frac{p-1}{2} \cdot p^e$ oder $n^* \leq$ Gr $f_{\frac{p+1}{2}} = \frac{p(p+1)}{2} p^e$ daher $n^* \leq \frac{p(p+1)}{2} e$. Also liegt n^* in dem rot schraffierten Bereich (da die Verteilg der Potenzen symmet. bezgl $\backslash$ ist; siehe 18):

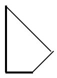
190/191



$\frac{(n+1)}{2}e(1+p) \equiv e(p-1)$
$\mathfrak{G}$ enthält unter Δ nur Pkte, die unter oder auf / (grün) liegen, darauf liegt aber kein roter Punkt.
Der Beweis zeigt zusätzlich:

(17′) Entweder Gr $f_{\frac{n-1}{2}} \leq \frac{(n-1)}{2}ep$ oder Gr $f_{\frac{n+1}{2}} \leq \frac{n+1}{2}ep$ oder beides.

Jedenfalls $n^* = \min \mathrm{Gr} \leq \frac{n+1}{2}ep$, $n^* \in$ $||| \cap \equiv$ = 

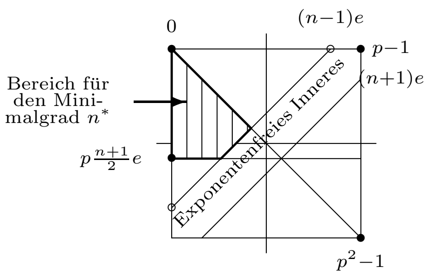
und  enthält den Grad jedes f_λ, der $\leq p^{\frac{n+1}{2}e}$ ist.

(18) Die Verteilg der Potenzen in f_λ ist symmetr. zu \, entsprechende Koeff c, d sind konjugiert: $c = d^p$.
Bew: $f_\lambda(x) = f_\lambda^p(x)$.

191/192

(19) Wenn f_2 Potenzen unter Δ besitzt, so haben $f_1, f_3, f_5 \cdots, f_{\frac{n+1}{2}}$ nur Potenzen über Δ
Bew: $f_2, f_4, \cdots, f_{\frac{n-1}{2}}$ haben Pot unter Δ, da $f_4 = f_2 \circ f_2, \cdots$ und sich die „äusseren“ Potenzen so lange nicht wegheben bei der Faltung, als man Δ nicht überschreitet.
Allgemeiner zeigt dieser Schluß mit (17):

(20) Wenn $f_\kappa, f_\lambda, \cdots, f_\mu$ Potenzen unter Δ enthalten, so $\kappa + \lambda + \cdots + \mu \neq n$, und wenn $\cdots < \cdot\cdot$, so hat $f_{n-(\kappa+\lambda+\cdots+\mu)}$ nur Potenzen über Δ.



Bessere Zeichnung zu 17

192/193

(21) Der Fall $n = 3$.
Fortzusetzen vielleicht mit Untersuchung von $\sum g(x-t)h(y-t)k(t)$
Benutzt man als Wertebereich der Funktionen irgend Integritätsbereich K mit 3 3-ten Einheitswurzeln $1, \delta, \delta^2$, so gelten bei Bahnen $0, \mathfrak{T}, \mathfrak{T}^{(\infty)} = \mathfrak{T}'$ $\mathfrak{T}^{(a^n)} = \mathfrak{T}^n$ a symbolische Potenzierung die Tafeln

	0	$\mathfrak{T}$	$\mathfrak{T}'$	$\mathfrak{T}''$
f_0	1	0	0	0
f_1	0	1	ρ	ρ^2
f_2	0	1	ρ^2	ρ
f_3	-1	-1	-1	-1

I: Festlegung der lin. un Funktionen aus $\mathfrak{F}_0$

	f_0	f_1	f_2	f_3
f_0	f_0	f_1	f_2	0
f_1	f_1	ζf_2	$p^2 f_0 + f_3$	0
f_2	f_2	$p^2 f_0 + f_3$	ηf_1	0
f_3	f_3	0	0	$-p^2 f_3$

II: Faltung $f_i \circ f_k$
Da z.B. die Charakt. Fkt χ_1 (von $\mathfrak{T}$) geg. durch

$$3\chi_1 = -f_0 + f_1 + f_2 - f_3,$$

wird

21_1

$$\begin{aligned} 9\chi \circ \chi &= \chi_0[3p^2 - 3] + \chi_1[p^2 - 8 + \eta + \zeta] \\ &\quad + \chi_2[p^2 - 2 + \eta\rho + \zeta\rho^2] + \chi_3[p^2 - 2 + \eta\rho^2 + \zeta\rho] \end{aligned}$$

Dabei ist $\zeta, \eta \in K$ mit $3\eta = p^2$.
Im Fall der kompl Zahlen K ist $|\zeta| = p$, $\overline{\zeta} = \eta$.
Also gibt 21_1 die Multipl Tafel des Schurrings bis auf „kleine“ Unsicherheit

193/194

Gruppen vom Grad p^a, azimutaler Fall

$\mathfrak{G}$ wirke auf K_+, $K =$ Körper GF(p^a) $\mathfrak{G}$ enthalte $\{x \to ax + b\} = \mathfrak{N}$ (= scharf 2-tra)
Aufgabe: Untersuche, ob $\mathfrak{G}$ 3-tra, wenn $\mathfrak{G} > \mathfrak{N}$!
Ansatz: Die bei $\mathfrak{N}$ invarianten Funktionen $f(xyz)$ mit Werten in K sind genau die homogenen der Grade $0, q, 2q, 3q$, $(q = |K| \cdot 1 = p^a \cdot 1)$ die nur von den Differenzen abhängen, sowie die Linearverbindungen von solchen. Trivial (dh

invar bei $\mathfrak{S}^K$), sind genau die Linearverbindgn (mit Teilgraden ≤ 1) von $1, (x-y)^q, (x-z)^q, (y-z)^q, [(x-z)(y-z)]^q \leftarrow$ was aber noch mod $x^{p^a} - x$ inv zu reduzieren ist, denn bei $\mathfrak{S}^0$ inv. sind genau die Linearverbdgn von

$$1, x^q, y^q, (x-y)^q, x^q y^q$$

invariant.
Ansatz: Die Annahme, $\mathfrak{G}$ liesse eine weitere Fkt. inv, widerlegen

194/195

Erweiterungen der scharf 2-tra Gruppe
$x \to ax + b$ über $GF(p^a) = \Omega = K$

kann man untersuchen mittels der (mindestens) auf $\Omega - \{0, 1\}$ (besser auf Ω definierten Funktionen $\Omega \to \Omega$, die bei $\mathfrak{G}_{01}$ invariant sind: $\mathfrak{F}_{01}$. Es gilt:

a)

$$\mathfrak{F}_{01} \ni f(x) \Rightarrow \mathfrak{F}_{01} \ni f(1-x), f(\frac{1}{x}), f(\frac{x-1}{x}), f(\frac{x}{x-1}), f(\frac{1}{1-x})$$

(Das sind die 6 gebrochenen lin Transform, die $0, 1, \infty$ vertauschen.) Ferner gilt:

(2)

$$\mathfrak{F}_{01} \ni f(x) \Rightarrow \mathfrak{F}_0 \ni f(\frac{x}{x-y}), f(\frac{x-y}{x}), f(\frac{x}{y})$$

denn allgemeiner gilt

(3)

$$\mathfrak{F}_{01} \ni f(x) \Rightarrow \mathfrak{F} \ni f(\frac{x-z}{y-z}).$$

Hieraus folgt:

(4)

$$f, g \in \mathfrak{F}_{01} \Rightarrow \mathfrak{F}_{01} \ni \sum{}' f(\frac{x}{y})\overset{f\odot g}{g}(t), \ \underbrace{\sum_{t \neq 0}{}' f(1-t) g(tx)}_{= f \odot g}$$

wo

$$\sum = \sum_{t \in K}, \qquad \sum{}' = \sum_{0 \neq t \in K}$$

NB: Es ist für $\widetilde{f} = \sum{}' f(t)$: $\widetilde{f \odot g} = \widetilde{f}_0 \circ \widetilde{g}_1$

(5) Ist

$$\mathfrak{F}_{01} \ni f = \sum_{0}^{p^\alpha - 1} a_\nu x_\nu \mathfrak{F}_{01} \ni g = \sum b_\nu x^2,$$

so ist

$$\sum{}' a_\nu b_\nu x^\nu \in \mathfrak{F}_{01}$$

195/196

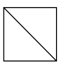
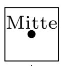
(6) Hieraus folgt ein Beweis für meinen Satz:

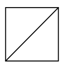
$$\mathfrak{G} > \mathfrak{N} \text{ (Gr. } = p) \Rightarrow \mathfrak{G} \text{ 3-tra},$$

wo $|\mathfrak{N}| = p(p-1)$.
Bew: Wähle $f \in \mathfrak{F}_{01}$, $f \neq$ const, Gr f minimal $= m$
Bei pass. Normierung wird $f = \sum_{1}^{p-1} a_\nu x^\nu$, $a_\nu = \begin{cases} 0 \\ 1 \end{cases}$.
Ferner ist $f(1-x) = (-1)^m f(x) + c$.
Wenn $m = 1$, so $f = x$ inv. unter $\mathfrak{G}_{01}, \mathfrak{G}_{01} = 1$, fertig.
Sei $m > 1$. Koeff. Vergl. bei x^{m-1} gibt

$$\begin{aligned} f(x) + c' &= (x-1)^m - a_{m-1}(x-1)^{m-1} + \cdots \\ a_{m-1} &= -m - a_{m-1} \end{aligned}$$

Da $m \not\equiv 0$, ist $a_{m-1} \not\equiv 0$, daher $\equiv 1$, also $m \equiv -2$, wegen $m \leq p-1$ ist $m = p-2$
[Nun ist $g = (x-1)^{p-1} - x^{p-1}$ ein Polynom vom Grad $p-2$, also $f =$ const g]
Also gibts nur ≤ 3 lin un Funktionen in $\mathfrak{F}_{01}$, zu kennzeichnen durch a_{p-1}, a_{p-2}, a_0 : $\mathfrak{G}$ ist 3-tra

(7) Mit $f \in \mathfrak{F}_{01}$ ist auch $f(x^p) \in \mathfrak{F}_{01}$. viel allgemeiner (8)
Bew: OBdA hat f nur Koeff $0, 1$ (5).
Dann ist $f(x^p) = [f(x)]^p \in \mathfrak{F}_{01}$.
Die in $\mathfrak{F}_{01}$ auftretenden Exponentenkonfigurationen gestalten also Spiegelungen an  

, daher auch an  .

$\downarrow$
???

196/197

(8) Wenn $(h, p^2 - 1) = 1$, so $f \in \mathfrak{F}_{01} \Rightarrow f(x^h) \in \mathfrak{F}_{01}$
Bew: OBdA $\begin{cases} f = \sum e_a(x) \\ \text{Werte ganzzahlig} \end{cases}$ $\quad e_a(x) = \delta_{xa}$
$h =$ Primzahl: $e_a \odot e_b = e_{ab}$

$$\underbrace{f \odot f \odot \cdots \odot f}_{???} = \sum e_{a^h} + h \cdot \ldots$$

kleinste Reste mod h: $\sum e_{a^h} = \overline{f} \in \mathfrak{F}_{01}$

$$\overline{f}(x^h) = \begin{cases} 1 \\ 0 \end{cases} \iff \begin{array}{ccc} x^h & = & a^h \\ & \neq & \end{array}$$

also $\overline{f}(x^h) = f(x)$ $\qquad\qquad\qquad\qquad \overline{f}(x) = f(x^{\frac{1}{h}})$.

(8′) $p > 2$ Insbesondere für ungerades $h \mid p^2+1$ ist stets

$$f(x) \in \mathfrak{F}_{01} \to f(x^h) \in \mathfrak{F}_{01}$$

also $x \to x^{\frac{p^2+1}{2}}$ erlaubt. Daher

$$\begin{array}{l} 2 \mid k \\ 2 \nmid k \end{array} \quad \Rightarrow \quad \begin{cases} x^k \to x^k \\ x^k \to x^{k+\frac{p^2-1}{2}} = x^{k-\frac{p^2-1}{2}} \end{cases}$$

(9) Wenn also das f mit minimalem Grad m (Siehe 6) $\underline{\text{eine}}$ gerade Potenz enthält, so enthält es stets $x^k + x^{k+\frac{p^2-1}{2}}$ für ungerade k mit demselben Koeffizienten.
Falls es $\underline{\text{nur}}$ gerade k enthält, so ist $f(x) = f(-x) = f(1-x)$, dabei $f(x) = f(x+1)$, d.h. $f(x) = g(x^p - x)$ $\;$ Gr $g \leq p-1$.
Mit der 0-1 - Bedingg folgt $\underline{\underline{\text{dann}}}$ $f = (x^p - x)^{p-1}$.

197/198

(10) Die f mit $f(x) = f(1-x)$ sind darstellbar als

$$\sum c_\nu (x^\nu + (1-x)^\nu)$$

(11) Wenn

$$(n, p^2-1) = (k, p^2-1),$$

so gibt es h mit

$$hn \equiv k \ (p^2-1) \text{ und } (h, p^2-1) = 1.$$

Also gilt dann

$$\mathfrak{F} \ni x^n \Rightarrow f \ni x^k$$

für das „minimale“ f.

(12) Aufgabe: Perm Gr mit regulärer zyklischer Ugr vom Grad $p-1$ untersuchen mit $\Omega = K_x$.
Man weiß:

$$f(x) \in \mathfrak{F}_1 \to \begin{cases} f(x^a) \in \mathfrak{F}_1, & (a, p-1) = 1 \\ \sum f(\frac{x}{t}) g(t); & \sum a_\nu b_\nu x^\nu \in \mathfrak{F}_1. \end{cases}$$

Vielleicht leichter
aus Schurs Satz von pri $\to$ 2-tra

Eine Klasse von Gruppen zu Ringen

Satz: Sei R ein Ring. Dann bilden diejenigen $1-1$ Abbildungen von R auf sich, die in der Form $x \to g(x) = \sum a_\nu \sigma_\nu(x)$ dargestellt werden können mit $a_\nu \in R$, σ_ν ein Ring-Endomorphismus von R, eine Gruppe $\mathfrak{E}_R$. Es ist $\mathfrak{E}_{GF(p^\alpha)} =$ Holomorph von $(\underbrace{p, p, \cdots, p}_{\alpha})$

198/199

Allg Theorie der Perm Gr mit reg Ugr

Sei (bei additiver Schreibg der reg Ugr)

$$f \wedge g := \sum f(x-t)g(x)$$

und

$$f \circ g(x) = f(g(x))$$

Dann gilt:
Ist f inv bei $\mathfrak{G}_0$ und $g : x \to g(x) \in \mathfrak{G}$ und $\varphi(x)$ eine beliebige Funktion, so ist

(1′)

$$(f \wedge \varphi) \circ g = f \wedge (\varphi \circ g)$$

Folgt das aus einer allg Formel mit belieb φ <u>und</u> f?
Beweis:

$$\begin{aligned}(f \wedge \varphi) \circ g \quad &= \quad \sum_t f(g(x)-t)\varphi(t) = \sum_s f(g(x)-g(s))\varphi(g(s)) \\ &\underset{f \text{ inv}}{=} \quad \sum f(x-s)\varphi(g(s)) = f \wedge (\varphi \circ g).\end{aligned}$$

199/200

1′ Für belieb lin $\mathfrak{l}(\mathfrak{l}(\mathfrak{x}+\mathfrak{y}) = \mathfrak{l}(\mathfrak{x}) + \mathfrak{l}(\mathfrak{y}))$ ist $(h \wedge k) \circ \mathfrak{l} = (h \circ \mathfrak{l}) \wedge (k \circ \mathfrak{l})$

(2) Hiermit Beweis des Satzes von Burnside über Gr $\mathfrak{G} = p$:
Sei $f \in \mathfrak{F}_0$, $0 <$ Gr $f < p-1$. Durch Faltung kann man erreichen

$$k := \text{Gr } f \leq \frac{p-1}{2}.$$

Dann ist $x^k = f \circ h_k \quad (k = 1, 2, \cdots, n)$ für geeignete Funktionen h_k. Also ist nach (1)

$$g \in \mathfrak{G} \Rightarrow g^k = f \wedge h_k(g),$$

daher Grad $g^k\big|_{\text{reduz}} \leq n$;

$$k = 1: \text{ Gr } g \leq n \leq \frac{p-1}{2};$$

also $k+2$: Gr $g^2\big|_{\text{red}} = 2$ Gr $g \leq n$, $\quad$ Gr $g \leq \frac{n}{2}$ usw: Gr $g = 1$.

(3) Diejenigen Permutationen g auf $\Omega = GF(p^2)$ die durch Polynome der Art

$$g(x) = \alpha + \beta x + \gamma x^p$$

dargestellt werden können, bilden eine Gruppe.
= Normalisator der Translationsgruppe. Man kann so ein El, nichttrivial in $\mathfrak{G}$ annehmen

(4) Allgemein ist mit $q = p^2 - 1$

$$\sum_{t \in K} f(x-t)g(y-t)h(z-t) = \underbrace{(-1)^{i+k+l}}_{\substack{=1 \text{ wenn} \\ p \text{ ungerade}}} \quad \bullet$$

$$\bullet \quad - \sum_{\substack{\frac{i+k+l}{q} \\ =1,2,\ldots}} f_i(x)g_k(y)h_l(z) = - \sum_{q \mid i+k+l}{}' f_i(x)g_k(y)h_l(z) \quad 1 < i,k,l \neq 0,0,0$$

wo

$$f(xyz) = \sum x_i f^i(y) \text{ usw.}$$

also

$$f_i(x) = -f(x) \wedge x^{p^2-1-i}$$

Dabei ist

(5)
$$(x^i)_k\big|_{x=0} = \delta_{ik}.$$

(6) In $x^i y^j\big|_k$ kommt $x^\alpha y^\beta$ genau dann vor, wenn $\alpha + \beta = i + j - k$ und $\alpha \prec i, \beta \prec k$;

dabei heißt $\alpha \prec i : \binom{i}{\alpha} \neq 0$, dh. x^α kommt in $(x+\alpha)^i$ vor.

(7) Ansatz: Wenn man eine $f(x,y) \in \mathfrak{F}_0$ finden könnte, für die $xy = \sum f(x-t, y-t)\varphi(t)$ eine Lösung $\varphi(t)$ hat, so wäre für $g \in \mathfrak{G}$ stets

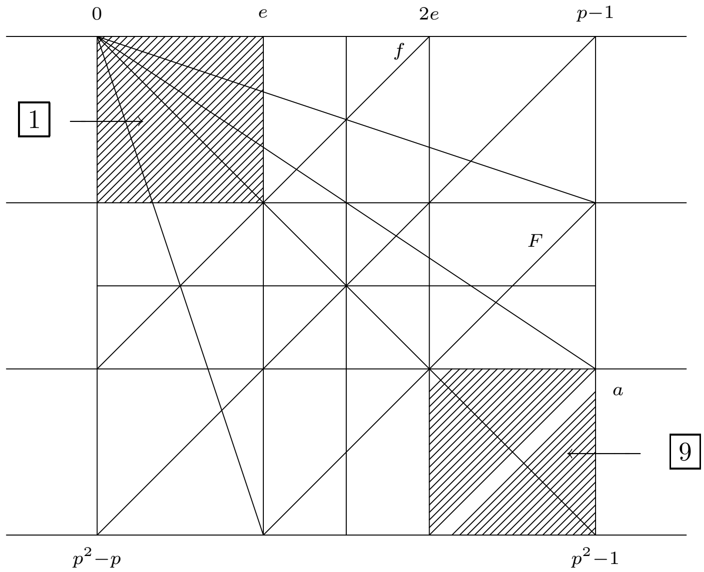
$$g(x) \cdot g(y) = \sum f(x-t\ y-t)\varphi(g(t)),$$

daher hätte $g(x)$ höchstens den Grad $\frac{1}{2} \cdot$ Gr f.
Nützlich ist dabei:

(8) Für $f(xy)$, $h(z)$ erkläre $f \wedge h = \sum f(x-t\ y-t)h(t)$.
Dann gilt mit $k(\lambda)$ bel:

$$(f \wedge h) \wedge k = f \wedge (h \wedge k).$$

(9) Der Fall $n = 3$ [Skizze ist eingelegt mit Vermerk "Zu S. 202 XIII"]



Ist F die invar Fkt zum Exp $2e$, so folgt aus $F \wedge \varphi = 0$ ($\wedge$ = Faltung), dass φ fremd zum Quadrat $\boxed{9}$ (abgeschl) ist. Also ist $\sum \varphi(t)t^\lambda = 0$ für $x \in \boxed{1}$, dh $\varphi \wedge x^\lambda = 0$, insb $\varphi \wedge x^{\frac{p^2-1}{3}} = 0$
Beweis: 10
Vermutung: Hieraus folgt $x^{\frac{p^2-1}{3}} = F \wedge h$ lösbar. (**???** $h \cap$ **???** Frobenius - Algebren jedes Hauptideal durch seinen Annulator bestimmt ist)

202/203

10. Satz von der Lösbarkeit
einer Faltungsgleichung auf endl. Abelschen Gruppen $\mathfrak{A}$.
Gegeben $f(x), g(x)$. Genau dann gibt es $u(x)$ mit $f \wedge u = g$, wenn aus $f \wedge v = 0$ stets $g \wedge v = 0$ folgt.
Bew: „Nur dann" klar:

$$g \wedge v = (u \wedge f)v = u \wedge (f \wedge v) = u \wedge 0 = 0$$

„Dann" Sei

$$F = (f(x-y))_{n\times n},\ G = (g(x-y))_{n\times n}$$

mit $n = |\mathfrak{a}|$. Aus $F_{\mathfrak{x}} = 0$ folgt $G_{\mathfrak{x}} = 0$, also (mit $F \sim \left(\begin{smallmatrix} I & 0 \\ 0 & 0 \end{smallmatrix}\right)$) $\exists$ Matrix $M_{n\times n}$:

$$G = MF$$

dh $\exists$ Fkt $m(x,y)$:

$$\begin{aligned} g(x-y) &= \sum_t m(x,t) f(t-y) \\ g(0-y) &= \sum m(0,t) f(t-y) \end{aligned}$$

$-y = z$

$$m(0,-t) =: v(t) \qquad\qquad g(z) = \sum v(t) f(z-t)$$
$$g = v \wedge f$$

203/204

11. Wieder $n = p^2$
Sei $\mathfrak{E}$ die Menge der Exponenten, die in der Darstellung mindestens eines $g \in \mathfrak{G}$ wirklich auftreten; Sei $\mathfrak{K}$ die Menge der Polynome $k(x)$ derart, daß für jedes $g \in \mathfrak{G}$ $k(g(x))$ nur Potenzen aus $\mathfrak{E}$ enthält. Dann gilt:

a) $\mathfrak{K}$ ist $\mathfrak{G} - K$- Modul: $\sum c_j k_j(g_i(x)) \in \mathfrak{K}$

b) $k \in \mathfrak{K} \to k(ax+b) \in \mathfrak{K}$ wenn $a \in$ Ugr der Ord e, $b \in K$

c) $k \in \mathfrak{K}, f$ beliebig $\Rightarrow k \wedge f \in \mathfrak{K}$

d) Vor $*$: Sei $\mathfrak{E} \leq 1$. Quadrant. Wenn $\mathfrak{E} \neq \{0,1,p\}$, so ist $x^2, x^{2p} \in \mathfrak{K}$, $x^{p+1} \notin \mathfrak{K}$

e) nach 10 gilt: Wenn ein $k \in \mathfrak{K}$ Potenzen einer Schrägreihe $\mathfrak{S}$ enthält, aber beide Enden nicht enthält, so $\mathfrak{E} = \{01p\}$, denn

f) Die $(p-1)$- homogenen Teile von $k \in \mathfrak{K}$ sind wieder in $\mathfrak{K}$, falls $\mathfrak{E}$ keine zwei Exponenten enthält, die sich um λe unterscheiden und in derselben Zeile liegen.
Denn $k(x) \in \mathfrak{K} \to k(ax) \in \mathfrak{K}$; das gibt e-homogene Teile $\in \mathfrak{K}$, so daß die Potenzen innerhalb k in Schritte von e fortschreiten. Aber wegen $x \in \mathfrak{G}$ gehören sie zu $\mathfrak{E}$, schreiten nur $p-1$ fort.

204/205

g) Die Potenzen, die in den $\mathfrak{K}$ auftreten (=: Exp $\mathfrak{K}$) sind <u>genau</u> die aus $\mathfrak{E}$: $\operatorname{Exp}\mathfrak{K} = \operatorname{Exp}\mathfrak{G}$.
Bew $\to$: $x \in \mathfrak{G}$, also $k(x)$ Exp $\in \mathfrak{E}$; $\operatorname{Exp}\mathfrak{K} \subseteq \mathfrak{E}$.
$\leftarrow$: $g \in \mathfrak{K}$, also $\mathfrak{E} \subseteq \operatorname{Exp}\mathfrak{K}$

h) $\mathfrak{E}$ ist abgeschlossen bezgl Verschiebung mit Vektoren ; Bew c)
d.h. mit $\underset{1}{\leftarrow}$ und $\uparrow 1$.

Vor $*$ i) $\begin{cases} \text{Sei } \mathfrak{E} \subseteq \text{ erster Quadrant: } a < \frac{p}{2},\ b < \frac{p}{2} \\ \text{Wenn } \mathfrak{E} \neq \{0\ 1\ p\}, \text{ so} \end{cases}$
enthält $\mathfrak{K}$ keine Funktion x^n, $n \notin \{0,1,p\}$
Bew: $n = a + bp$, $x^n \in \mathfrak{K} \to$

$g^a \cdot (g^p)^b$ hat Exp in $\mathfrak{E}$.
Wähle g so, dass es Exponenten auf der höchsten Schräglinie hat, die $\mathfrak{E}$ trifft. g^p hat dort auch Exponenten, und wegen
Gr $g+$ Gr $g^p \leq p^2 - 1$ ist Gr $gg^p =$ Gr $g+$ Gr g^p, nichts hebt sich, $\mathfrak{G}\mathfrak{G}^p$ enthält was auf der doppelt so hohen Schräglinie.

j) Unter Vor $*$ trägt jede Schräglinie höchstens 2 lin un Funktionen zu $\mathfrak{K}$ bei. (e)

205/206

k) Wenn ein $k \in \mathfrak{K}$ kein x^λ, $\lambda \leq p-1$ und kein $x^{p-\lambda}$, $\lambda \leq p-1$ enthält, so ist $k = 0$ (e)

l) Von 3 benachbarten inneren Exp auf einer Schräglinie in $\mathfrak{E}$ sind immer mindestens 2 in $\mathfrak{E}$ enthalten.
sonst verschiebe auf die 3 Schrägr h) d)

Vor $*$ m) Exp $\mathfrak{K}$ liegt symmetr. zur Diagonalen durch 0, denn Exp$\{g\}$ tut das, weil * Exp$\{g^p\} \subseteq \mathfrak{E} = \exp\{g\}$.
* das folgt aus

n) $x^p \in \mathfrak{K}$ außer wenn $\mathfrak{E} = \{0, 1\}$
(Vor: $*$!)
Bew: $x \in \mathfrak{K}$; man kann jedes $k \in \mathfrak{K}$ auf die Schräglinie $(1, p)$ schieben, das auf höherer Schräglinie liegt, kommt $x^p + cx$ heraus, so ist wegen $x \in \mathfrak{K}$ auch $x^p \in \mathfrak{K}$. Ausnahmen könnte es also nur geben, wenn x^p nur in $k \wedge \therefore$ auftrifft, d.h. jedes $k = a_0 + a_1 x + \ldots + a_m x^m$, $m \leq p-1$ ist. Dann ist, wenn $\mathfrak{E} \neq \{0, 1\}$, ein $k = x^2 + ax + b \in \mathfrak{K}$, $x^2 \in \mathfrak{K}$, Wid.

206/207

o) alle $g^p \in \mathfrak{K}$ $(g \in \mathfrak{G})$ (n) (a)

p) $k \in \mathfrak{K} \to k^p \in \mathfrak{K}$
Bew: Sei $k = \sum a_\nu x^\nu$
$\sum a_\nu g^\nu(x) = k(g(x))$ hat nur Potenzen in $\mathfrak{E} = \mathfrak{E}^p$
$(\quad)^p$ 〃 〃 〃 $\mathfrak{E}$
$\sum a_\nu^p g^p(x)$ 〃 〃 〃
$\sum a_\nu^p x^p = k(x)^p \in \mathfrak{K}$

q) Enthält $\mathfrak{K}$ in einer Schräglinie, die nicht durch $0, 1$ geht, zwei linear un hom Fkt, so auch in die vorangehenden.
Bew: $\leftarrow$ $0 \uparrow$ sind lin un wenn 0 einen inneren "Platz" hat; und einen solchen kann man stets machen wenn in der Schräglinie 2 lin un exist.

q′) Enthält ein Schräglinie eine Null, so hat die vorangehende den Rang 2.

207/208

r) Wenn $\mathfrak{E}$ im 1. Quadranten, so $\mathfrak{E} = \{0, 1, p+1\}$, $\mathfrak{G}$ läßt die reg Ugr. invariant
Bew: Enthält $\mathfrak{K}$ eink in der Schräglinie durch $2, 1+p, 2p$, so ist für

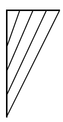
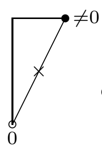
einen homogenen Teil h höchsten Schräggrades (etwa m), der in passendem g in $\mathfrak{G}$ auftritt, $k(h(\xi)) = 0$ für jedes $\xi \in K$.
Bew: Ist $\mathfrak{K} = ax^2 + bx^{p+1} + cx^{2p}$, so ist $0 \equiv ah^2 + bh^{p+1} + ch^{2p}$, aber nur mod $\underline{x^{p^2} - x}$, da sonst etwas in einer zu hohen Schräglinie, nämlich der zu $2m$, aufträte in $k(g(x))$.
Setzt man $h = \sum a_\nu x^\nu$ und dann $h^* := \sum a_\nu x^{\overline{p^\nu}}$
<u>wo der Exponent mod $p^2 - 1$ reduziert ist:</u>
$\overline{p^\nu} = \{$ kl positiver Rest von $p^\nu \mod p^2 - 1\}$ so ist
$ah^2 + bhh^* + ch^{*2} = 0$ <u>formal</u>
Durch Körpererweiterung $\overline{K}$ kann diese Form faktorisiert werden:
$0 = (\alpha h + \beta h^*)(\gamma h + \delta h^*)$
Da $\overline{K}[x]$ Integritätsbereich, folgt $\alpha h + \beta h^* = 0$ etwa.

208/209

also $\exists c : h^* = ch$ ($c \in K$ fest) für <u>jeden</u> homogenen Teil des Maximalschräggrades m in g, also ist $c \in K$. (nicht nur in $\overline{K}$). Also hat die Form k eine rat Nullstelle c, also ist die zweite auch rat. Bei passender Normierung ist $k = (x - cx^p)(x - dx^p)$
Falls $c \neq d$, sei wieder h ein höchster (Grad m) in g, und zwar etwa in g_1 mit $g_1(0) = 0$ auftretender homogener Teil. Dann ist $h - ch^* = 0$, daher hat $h - dh^* = (c - d)h^*$ <u>den vollen</u> Schräggrad, also hat $g_1 - dg_1^*$ den vollen Schräggrad.; $k(g) = (g_1 - cg_1^*)(g_1 - dg_1^*)$ hat nur Schräggrad m, also liegt $g - cg^*$ ganz auf der Schräglinie durch 0, d.h. $g_1 - cg_1^* =$ const
$g_1 - cg_1^p =$ const., wegen $g_1(0) = 0$ ist const $= 0$
$g_1(g_1^{-1}) - c[g_1(g_1^{-1})]^p = 0$
$x - cx^p = 0 \ \downarrow\uparrow$

209/210

Also ist $c = d : k = (x - cx^r)^2$, $c \neq 0$ wegen (d).
Wegen $k \in \mathfrak{K}$ hat dann $g - cg^p$ stets nur (für $\forall g \in \mathfrak{G}$) Exponenten im auf die Hälfte ähnlich verkleinerte Bereich $\frac{1}{2}\mathfrak{E}$. Übrigens ist $\mathfrak{E}$ ein

Dreieck  , denn sonst gäbe es $g =$ 

entgegen $g = cg^p$.

Satz I: Sei $\mathfrak{G}$ eine unter $x \to -x$ invariante, z.B. 2-abgeschlossene[1] Gruppe auf $\Omega = K_{p^2}$, $p > 2$, die alle Translationen $x \to x + t$, $t \in K$ enthält. In der reduzierten Darstellung jedes $g \in \mathfrak{G}$: $g(x) = \sum_0^{p^2-1} a_\nu x^\nu$ mögen nur Exponenten

[1] siehe 214

aus dem 1. Quadranten $\mathfrak{Q}_1$ auftreten[2](siehe 214 „g mager“): $\nu = a + bp$, mit $0 \leq a, b \leq \frac{p-1}{2}$. Dann ist entweder die Gruppe $\mathfrak{T}$ der Translationen normal in $\mathfrak{G}$, d.h. es treten höchstens $\nu = 0, 1, p$ auf, oder $\mathfrak{G}$ enthält einen intra Normalteiler mit auflösbarer Faktorgr; ist also imprim

210/211

Beweis: Wähle ein Polynom $m(x) \in K_{p^2}[x]$ nicht konstant derart, daß

a) für jedes $g \in \mathfrak{G}$ die in $m(g(x))_{\text{red}}$ auftretenden Exponenten in $\mathfrak{Q}_1$ liegen (z.B. $k = x$ tut das), und

b) der größte dabei auftretende „Schräggrad“ $\overline{\nu} = a + b$ (wenn $\nu = a + bp$) möglichst klein, etwa $= n$ ist.

A. Sei $\mathfrak{M}$ die Menge aller Polynome $f(x)$ über alg abg Erweit von K_{p^2} mit

$$\begin{cases} \text{Exp } f(g(x)) \subseteq \mathfrak{Q}_1 \\ (\text{Exponentenmenge} = \{\nu\}) \\ \underset{=\{\overline{\nu}\}}{\overline{\text{Exp}}} f(g(x)) \leq n \end{cases}$$

$m(x) \in \mathfrak{M}$, also $\mathfrak{M} \neq \emptyset$.
Da neben $g(x)$ stets $g(x) - t \in \mathfrak{G}$ wo $t \in K$ beliebig gewählt ist, folgt:

$$m(x) \in \mathfrak{M} = m(x - t) \in \mathfrak{M}$$

211/212

$\mathfrak{M}$ ist $\mathfrak{G}$-Modul:

$$f_1, f_2 \in \mathfrak{M} \to c_1 f_1 + c_2 f_2 \in \mathfrak{m}$$
$$f(x) \in \mathfrak{M} \to f(g(x)) \in \mathfrak{M}$$

Also $f \in \mathfrak{M} \to f \wedge h \in \mathfrak{M}, \quad \forall h.$
Ferner ist $1 \in \mathfrak{M}$, und

$$f(x) \in \mathfrak{M} \to f(x^p) \in \mathfrak{M}$$

Schließlich gilt

$$f(x) \in \mathfrak{M} \Rightarrow f(-x) \in \mathfrak{M}.$$

Bew:

$$\text{Exp } f(-g(x)) = \text{Exp } \underbrace{f(-g(-x))}_{=f(g(x))}$$

wegen $-g(-x) \in \mathfrak{G}$

[2]Es genügt vielleicht, dass die Potenzen in den Leitgliedern in $\mathfrak{Q}_1$ liegen (maximaler Schräggr.)

B. Wir zeigen: $\mathfrak{M}$ enthält kein k vom Schräggrad 2.
Annahme:

$$\mathfrak{M} \ni k = ax^2 + \beta x^{1+p} + \gamma x^{2p} + \delta x + \varepsilon x^p + \eta$$

oBdA $\eta = 0$. Ferner ist $\mathfrak{M} \ni \ell := k(x) + k(-x)$

$$\mathfrak{M} \ni \ell = \alpha x^2 + \beta x^{1+p} + \gamma x^{2p}$$

212/213

Notfalls in Erweiterungskörper $\widehat{K}$ zerlegt sich der quadrat. Teil ℓ:

$$\ell = (ax + bx^p)(cx + dx^p)$$

Da $ax + bx^p \neq \text{const}$, $\exists g \in \mathfrak{G}$: Grad $ag + bg^p \geq n$. Wegen der Quadrantenbedingg ist Exp $cg + bg^p \subseteq \mathfrak{G}_1$, Exp $cg + dg^p \in \mathfrak{Q}_1$, also $n \geq$ Grad $(ag + bg^p)(cg + dg^p) =$ Gr + Gr daher Gr $cg + dg^p \leqq 0$, $cg + dg^p =$ const, $x \to \overline{g}(x)$: $cx + dx^p = \text{const}$ $\overset{\downarrow}{\uparrow}$
Folglich gibts kein $k + \mathfrak{M}$: $\overline{\text{Gr}}\ k = 2$.

B. Es gibt kein $k \in \mathfrak{N}$ mit $\overline{\text{Gr}}\, k \geq 2$.
sonst $\exists k \wedge h \in \mathfrak{M}$ mit $\overline{\text{Gr}}\ k \wedge h = 2$.

C. Wähle $k \in \mathfrak{M}$, $k =$ const, oBdA $k(0) = 0$. Nach A,B ist $k = \alpha x + \beta x^p$, und da $k(g) \in \mathfrak{M}$ ist auch $k(g) = \alpha' x + \beta' x^p + \gamma'$

   I. $x \in \mathfrak{M}$. Dann $g \in \mathfrak{M}$, $\overline{\text{Grad}}\, g = 1$ fertig $(\forall g)$

   II. $x \notin \mathfrak{M}$. Dann enth. $\mathfrak{M}$ nur ein Elm mit El't mit $k(0) = 0$, also ist mit festem k

$$k(g) = c_g \cdot k(x) + d_g$$

   Die $g \in \mathfrak{G}$ mit $c_g = 1$, $d_g = 0$ bilden Normalteiler $\mathfrak{N}$ mit auflösbarer Faktorgr. Für $g \in \mathfrak{N}$ ist $k(g(x)) = k(x)$ und da $k(x) \neq \text{const}$, ist $\mathfrak{N}$ intransitiv QED
   ($\mathfrak{N} =$ Kern v. $g \to \left(\begin{smallmatrix} c_g & d_g \\ 0 & 1 \end{smallmatrix}\right)$)

213/214

Aufgabe
Satz I kann vielleicht auf Halbgruppen $\mathfrak{G}$ mit regulärer elementar-abelschen Untergruppe erweitert werden. Vermutlich ist $g(x) \in g \to -g(-x) \in \mathfrak{G}$. Siehe auch Satz II. 232
Bemerkung: Die Funktionen $f(x) = \alpha x + \beta x^p$ sind die sämtlichen additiven (dh Endomorphismen von K_+): $f(x+y) = f(x) + f(y)$
Der Schräggrad $\overline{\text{Gr}}\ \varphi(x)$ ist die kleinste Zahl k mit

$$\varphi(x) = \sum f_1 f_2 \cdots f_K \quad K \leq k, \quad f_i \text{ additiv}$$

Satz: Ist $\mathfrak{G}$ 2-abgeschlossen mit einer regulären Untergruppe $\mathfrak{H}$ dargestellt auf $\mathfrak{H}$, so gilt:

$$g(x) \in \mathfrak{G} \to -g(-x) \in \mathfrak{G}$$

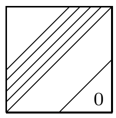
Bew: Ist $f(x)$ inv. bei $\mathfrak{G}_0$, so auch $f(-x)$; daher

$$f(-g(x)) = f(-x)$$
$$f(-g(-x)) = f(x), \qquad -g(-x) \in \mathfrak{G}$$

214/215

22.9.64

Satz I$'$: Ist $\mathfrak{G}$ eine nur einfache tra Gruppe des Grades p^2 mit el ab. Ugr $\mathfrak{H}$, die nicht in $\mathfrak{G}$ normal ist, so hat $\mathfrak{G}_0$ entweder eine Invariante $f(x^{p-1}) \neq \begin{cases} \text{const} \\ x^{p^2-1} \end{cases}$
oder die „homogenen" Invarianten f_i von S. 189 liegen für $i > \frac{n}{2}$ oberhalb der Diagonalen
haben die Faltungstafel auf S. 189 mit $c_{\lambda\mu} = 0$ für $n < i+j < \frac{3n}{2}$, d.h. $f_i \wedge f_j = 0$

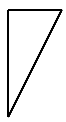


Beweis: oBdA sei $\mathfrak{G}$ 2-abgeschl. Wäre ein f_i unter $f_1, \cdots, f_{\frac{n-1}{2}}$ ganz oberhalb der Diagonalen, so ganz im 1. Quadranten $\mathfrak{Q}_1$, also hätte $f_i(\mathfrak{H})$ nur Exponenten oberhalb f, also in $\mathfrak{Q}_1$, falls $x = f \wedge h$ Lösung h hat. Nach Satz I, 210, geht das nicht. Also ist $x = f \wedge h$ unlösbar. Nun

Hilfssatz: Sei $\begin{cases} f \text{ homogen und} \\ \overline{\text{Gr}}\, f \geq 1 \text{ und } f \wedge h = x \end{cases}$ unlösbar, dann ist $f = (\alpha x + x^p)^n$
mit passenden α so dass $\alpha^{p+1} = 1$
Bew: je zwei Faltungen $f \wedge h$, die homogen vom $\overline{\text{Grad}}$ 1 sind, sind lin abhängig:

215/216

etwa $= \text{const}(\alpha x + \beta x^p)$. Nach Vor ist $\beta \neq 0$, oBdA $\beta = 1$. $f_0 = (\alpha x + x^p)^n$ ist eine Fktion dieser Eigenschaft
gäbe es ein davon lin un f $\;''\;\; ''$, so könnte man c finden, so daß $g = f - cf_0$

die Potenz x^{pn} nicht enthält: $g =$  Dann $\exists h : g \wedge h = x$ im Widerspruch zu $g \wedge h =$ const $(\alpha x + x^p)$.
Schluß des Beweises II.:
Wäre ein f_i ganz oberhalb der Diag, $i \leq \frac{n-1}{2}$, also f_i in $\mathfrak{Q}_1$, so wäre $f \wedge h$

unlösbar
also $f_i = c \cdot (x^p + dx)^{ie}$. Da $f_i = f_i^p = c^p(x + d^p x^p)^{ie}$, wäre $+cd = c^p$, $d = c^{p-1}$.

$$f_i = cx^{ie} \cdot (x^{p-1} + c^{p-1})^{ie}$$

Wähle $d_0 \in K : d_0^{p-1} = -1$; das geht da $\frac{p^2-1}{p+1}$ gerade. Dann ist $f_i(d_0 c) = 0$, trotz $d_0 c \neq 0$. Aber $f_i(x) \neq 0$ für $x \neq 0$. Wid.!

216/217

Noch Permgr mit reg Ugr. $\mathfrak{H}$

Normierung von $\mathfrak{G}$ durch Änderung der Einbettung von K_+ in $\mathfrak{G}$
Ist σ ein Automorphismus von $\mathfrak{H}$, so ist

a) σ vertauschbar mit Faltung und mit $\mathfrak{G}^\sigma = \sigma^{-1}\mathfrak{G}\sigma$.

b) $f \in \mathfrak{F}_0 \to f(x^\sigma) \in \mathfrak{F}_0^{(\sigma)}$

c) $f(x) \in \mathfrak{M}$ (im Sinn von S. 211) $\to f(x^\sigma) \in \mathfrak{M}^{(\sigma)}$
Damit kann man dann das $x^n + cx$ vom Beweis Satz II (S. 216) zu $x^p - x$ normieren durch Übergang von $\mathfrak{G}$ zu $\mathfrak{G}^\sigma$.

Partielle Summation:

$$x \cdot [f \wedge g] = (xf) \wedge g + f \wedge xg$$
$$x^2 \cdot [f \wedge g] = (x^2 f) \wedge g + 2xf \wedge xg + f \wedge x^2 g$$
$$x^{p+1} \cdot [f \wedge g] = (x^{p+1} f) \wedge g + xf \wedge x^p g + x^p f \wedge xg + f \wedge x^{p+1} g$$
$$x^p \cdot [f \wedge g] = x^p f \wedge g + f \wedge x^p g$$

217/218

Es gibt in K_{p^2} zwei Ableitungen:

$$f' = f(x+t)\big|_t, \quad f^* = f(x+t)_{t^p}$$

Rechenregeln aufstellen! siehe 221(1)

Partielle Summation funktioniert mit additiven Funktionen $l(x)$:
$l(x+y) = l(x) + l(y)$ also für $l(x) = \alpha x + \beta x^p$:

$$l[f \wedge g] = (lf) \wedge g + f \wedge lg$$

Bew:

$$= \sum l(x) f(x-t) g(t)$$
$$= \sum [l(x) - l(t)] f(x-t) g(t) + \sum l(t) f(x-t) g(t)$$

f, g sind beliebg.
Ist l additiv, so gilt

$$l^i \wedge l^k = [x^i \wedge x^k] \circ l$$

wenn $u \in K,\ l(u) < 0,\ \to u = 0$ und $f(h) \wedge \varphi(l) = 0 \quad \forall f, \varphi$ wenn l ausgeartet: $\exists u_0 \neq 0 : l(u_0) = 0$ denn dann tritt jeder Wert von l p-mal auf.

218/219

$n = 3$ Hier hat das f (zum Exp $2e$) einen 1-Annulator a homogen, auf der Schräglinie $5e$ oder tiefer. Denn auf der $5e - 1$ hat es sogar 2 lin un (alle diese $e+2$ Potenzen mit f gebildet, ergeben Linearverbindgen von e Potenzen auf der Linie $e-1$). Und wenn zwei Annullatoren eine Defektsumme (Defektschräglinie von $p^2 - 1$ aus gezählt mit 0 beginnend) $< p - 1$ haben, sonst ihre ggT auch Annullator (ggT der Formen in $x^{p^2-1}\ x^{p^2-p}$).
NB: $k < p, l$ additiv $\to$

$$l^k \wedge x^{p^2-2} = \alpha l^{k-1}$$
$$l^k \wedge x^{p^2-1-p} = \beta l^{k-1}$$

wenn $l = \alpha x + \beta x^p$

219/220

$$n = 3$$

Mit Hilfe des Annulators (Zerlegung von $a^{*)}$ Linearfaktoren) kann man zeigen

$$f = \sum_{i=1}^{l} \alpha_i l_i^{2e} \qquad a = \prod l_i$$

Ansatz: Man berechne dann z.B. $f \wedge x^{(p^2-1)-(2e-2)}$ oder allgemeiner $f \wedge x^k$ als $\sum \beta_i l_i^{\cdot\cdot}$ damit ist dann auch jedes $g \in \mathfrak{G}$ als $\sum \cdots l_i^{\overline{a}}$ dargestellt. Hieraus sollte man sehen können, daß g und g^2 nur dann Bereiche oberhalb der Linie $2e$ liegen, wenn g sogar oberhalb der Linie e liegt, d.h. in $\mathfrak{Q}_1$. Dann Satz I, S 210 anwenden.
$*)$ an der Gestalt als $\wedge$ Polynom in $x^{p^2-1-1},\ x^{p^2-1-p}$

$$= \frac{\partial}{\partial x} \text{ und } \frac{\partial}{\partial \overline{x}} \quad (\overline{x} = x^p)$$

Sind $l_1 \cdots l_e$ verschiedene Linearformen, so sind für festes $k \geq e$

$$l_1^k, \cdots, l_e^k$$

lin un (Vandermonde)
Sie müssen sich eignen zur Untersuchung der $f\wedge$ und damit der $g \in \mathfrak{G}$.
Vielleicht empfiehlt es sich, f als „symbolische Potenz“ zu schreiben!

noch Gruppen vom Grad p^2

(1) Die Untersuchung des Rings der $f(z,\overline{z})$ mit $z^p-\overline{z}=\overline{z}^p-z=0$ ist vermöge $z=x+iy$ gleichwertig zu $g(x,y)$ mit $x^p=x,\ y^p=y$.
Bew:

$$\underset{\substack{\uparrow\\ \text{„modulo“}}}{K[u]/}u^{p^2}-u\cong K[z,\overline{z}]/z^p-\overline{z},\ \overline{z}^p-z\cong K[x,y]/x^p-x,\ y^p-y$$

Wenn form $g^2\equiv r\ \ (u^p-\overline{u},\ \overline{u}^p-u)$, $g^2=r+a(u^p-\overline{u})+b\cdot(\overline{u}^p-u)$; oBdA a,b homogen; $=au^p+b\overline{u}^p$ wegen Homogenität; Gr a =Gr $b<2\hat{g}-p$

(2) Im Fall $n=3$ wäre es wohl nützlich, erst zu zeigen: Es gibt keine als Leitglied eines Gruppenelements auftretende Form $\ell^k\neq g(x,y)\in K[x,y]$ wo ℓ linear vom Grad $g=k\ \substack{\leq 2(\frac{p-1}{3})\\ >\frac{p-1}{2}}$ mit

$$g^2=ax^p+by\quad(*),$$

wo a,b Formen des Grades $2k-p$. stimmt im wes. siehe 223
(dass $k\neq\frac{p+1}{2}$ sein müsste, folgt so:
Wähle Diffop $\delta=\alpha\frac{\partial}{\partial x}+\beta\frac{\partial}{\partial y}$ mit $\partial b=v$, den gibts wegen Grad $b=1$; dann

$$2g-\delta g=\delta a-x^p+(\delta b)y^p=\delta a\cdot x^p$$

Wenn I. $a\neq cb$, so $\delta a\neq 0$, so also $g\big|x^p\quad g=x^k$ ebenso $g=y^k$ Wid!

Wenn II. $a=cb$:

Wenn aber $a=\text{const}\ b$, so $g\cdot\frac{\partial g}{\partial u}=c_1\cdot x^p+c_2y^p=(d_1x+d_2y)^p\quad g=(d_1x+d_2y)^k$

NB: für $g=l^k$, l linear reduziert sich g^2 tatsächlich auf „niedrige“ Potenzen:

$$g^2=l^p\cdot l^{2k-p}=(\therefore x^p+\therefore y^p)l^{2k-p}$$

$\leftarrow$ $(*)$ In $K(z\overline{z})$ gilt die entsprechende Bedgg für Graderniedrgg:
$g^2=\therefore z^p+\therefore\overline{z}^p$. [Verweis auf $(*)$ S. 221]
NB: Wenn $g=l^{\frac{p+1}{2}}\cdot g_1$, l linear, so ist

$$\begin{aligned} g^2 &= l^p\cdot(lg_1^2)\\ &= \therefore x^p+\therefore y^p\end{aligned}$$

Die Frage wäre, ob nur dann. Sonst invariant gegen $\substack{x\to ax+by\\ y\to cx+dy}$ mit $\begin{vmatrix} a & b\\ c & d\end{vmatrix}\neq 0$

Ja! 223 Daher kann $g^2=\therefore x^p+\therefore y^p$ nicht eintreten, wenn $g=l_1^k+l_2^k\quad l_1\neq\text{const}\ l_2$
NB: bei uns ist $g=\sum_1^n e_i^k,\quad n\leq e$
denn oBdA $l_1=x,\quad l_2=y$:
$(x^k+y^k)^2=\therefore\to x^k\cdot y^k=\therefore\ \ \substack{\downarrow\\ \uparrow}\ \text{Grad}_x$.

25.9.64 Noch P Gruppen vom Grad p^2

(1) Satz: Sei K ein Körper der Char p, $f \in K[x]$, $p > 2$, $f^2 = r + sx^{p^\lambda}$, $\frac{1}{2}p^\lambda \leq \hat{f} < p^\lambda$, $\lambda > 0$, $f \not\equiv 0$. $\hat{q} =$ Gr q
Dann ist entweder

$$\text{II} \qquad \text{Gr } f =: k \leq m+m'-\hat{q} \leq 2m-1 \begin{cases} q^2 T(r_1, S) \\ m = \max(\hat{r}, \hat{s}) \quad m' = \max(\widehat{r'}, \widehat{s'}) \end{cases}$$

oder

$$\text{I} \qquad \exists \ \alpha \text{ mit } \begin{cases} (x-\alpha)^p \big| f^2 \ \& \ \alpha^{p^\lambda} \in K \\ r = -\alpha^{p^\lambda} s \ \ \text{(also } \alpha \in K \text{ wenn } K \text{ vollkomm.)} \end{cases}$$

NB: sogar $2k - k^* < m + m' - \hat{q}$, wo $k^* = \#$ verschiedene Wu von f

Bew: Man kann annehmen, daß r und s keinen $\square \neq 1$ als gemeinsamen Faktor haben; damit ist $r' + ts' \not\equiv 0$. Bilde

$$\begin{aligned} R(t) &:= \text{Diskr}_x\,(\overbrace{r(x) + s(x)}^{h(x)}\,t) = \text{Diskr } h \\ &= \text{Res}_x(r + st\ ,\ r' + s't) = \text{Res}(h, h') \\ \text{Gr}_t R(t) &\leq m + m' \end{aligned}$$

mit $m = \max(\hat{r}, \hat{s})$, $m' = \max(\widehat{r'}, \widehat{s'})$
Frage: Gibt es Ähnliches wenn $f \cdot g$ „klein" statt f^2 klein?
Sei

$$(x-\xi)^n \big| f, n \geq 1;\ 0 < n \leq k$$
$$(x-\xi)^{n+1} \big| f^2 = r + sx^{p^\lambda}$$
$$x \to x + \xi: \quad x^{n+1} \big| r(x+\xi) + s(x+\xi) \cdot (x^{p^\lambda} + \xi^{p^\lambda})$$
$$= r(x+\xi) + \xi^{p^\lambda} s(x+\xi) + x^{p^\lambda} s(x+\xi)$$

wegen $n + 1 < p$ ist

$$x^{n+1} \big| r(x+\xi) + \xi^{p^\lambda} s(x+\xi) = a_0 + a_1 x + \cdots$$
$$a_0 = \cdots = a_n = 0$$

I. Wenn nun Gr $h < n$, so folgt

$$r(x+\xi) + \xi^{p^\lambda} s(x+\xi) \equiv 0$$
$$r(x) = -\xi^{p^\lambda} - s(x) \to \xi^{p^\lambda} \in K$$
$$f^2 = s(x) - (-\xi^{p^\lambda} + x^{p^\lambda}) = s(x)(x-\xi)^{p^\lambda}$$

fertig

Sei also weiter Gr $h \geq n = n_\xi$, für jede Wurzel ξ von f

$$\begin{aligned} R(t) &= \operatorname{Res}(r(x+\xi) + s(x+\xi)\cdot t \ , \ \frac{d}{dx}\cdots) \\ &= \operatorname{Res}(a_0 + a_1x + a_2x^2 + \cdots + \underset{\substack{\| \\ s_0+s_1x+s_2x^2+\cdots}}{s(x+\xi)}[t-\xi^p] \ , \ \frac{d}{dt}\ldots) \end{aligned}$$

$$= \underbrace{\begin{vmatrix} a_0 + s_0[t-\xi^{p^\lambda}] \\ a_1 + s_1[\ \ ] \\ \vdots \\ a_{n-1} + s_{n-1}[\ \ ] \end{vmatrix}}_{m' \text{ Spalten}} \underbrace{\begin{vmatrix} a_1 + s_1[\ \ ] \\ 2a_2 + 2s_s[\ \ ] \\ \vdots \\ na_n + ns_n \cdot [\ \ ] \end{vmatrix}}_{m \text{ Spalten}}$$

also wegen $a_0 = \cdots = a_n = 0$ haben wir

$$(t - \xi^{p^\lambda})^{2n-1} \big| R(t)$$

Aus $\xi \neq \eta$ folgt $\xi^{p^\lambda} \neq \eta^{p^\lambda}$ wegen Char p, also indem man ξ die Nullstellen von f durchlaufen läßt, folgt, wenn $R(t) \not\equiv 0$,

II: $k = \text{Gr } f \leq \text{Gr } R(t) \leq m + m'$.
Sei nun $R(t) \equiv 0$, dh.

$$h := r(x) + s(x) \cdot t \in K(t)[x]$$

hat einen quadratischen Faktor $\neq$ const $h = k^2 \cdot l$, $k, l \in K(t)[x]$Gr $k \geq 1$. Nach Wegschaffen der Nenner in t und Primitiv-machen von k, l wird $k_0^2 \cdot l_0 = h \cdot \varphi(t) =$ primitiv, also $\varphi =$ const, und wegen t- Grad auch $k_0 \in K[x]$ unabh. von t

$$l_0 = \therefore + t \therefore,$$

also $k_0^2 \big| r$ und $k_0^2 \big| s$ Wid!

Zusatz (1′) Unter den Vor von (1) ist in jeder Darstellg

$$f(x) = \sum_{\nu=1}^{n} c_\nu (x - \xi_\nu)^k \qquad n > \frac{p+1}{2} \text{ oder } n = 1$$

Denn $(x-\alpha)^{\frac{p+1}{2}} \big| f$, oBdA $\alpha = 0$ durch Translation, also

$$x^{\frac{p+1}{2}} \big| f \qquad 0 = \sum_{\substack{\nu=1 \\ \xi_\nu \neq 0}}^{n}{}' c_\nu \xi_\nu^{n-k}, \quad k = 0, \cdots, \frac{p+1}{2}$$

Sei $n > 1$, dann ist ein $\xi_\nu \neq 0$, die Anzahl der von Null verschiedenen ist $> \frac{p+1}{2}$.
Damit ist der Fall erledigt, dass der Annullator a von S. 219 quadratfrei ist.

NB (2) So könnte man im azimutalen Fall p^λ wohl mindestens für $n \geq 5$ direkt die Elemente $g \in \mathfrak{G}$ mod $x^{p^2} - x$ vermöge ihre Leitglieder, untersuchen, nachdem man durch eine Transl $x \to x + ax^p$ den Grad max gemacht hat.

NB (3) Man sollte die Untersuchung über die Einbettung regulärer Gruppen $\mathfrak{H}$ von vorn herein invariant führen (bezüglich Automorphismen von $\mathfrak{H}$).

225/226
[Die ganze Seite ist durchgestrichen.]

Siehe 227

226/227

Darstellung der Funktionen $K_{p^\alpha} \to K_{p^\alpha}$:

(1) Der Ring der Funktionen $K_{p^\alpha} \to K_{p^\alpha}$ ist isomorph $K_{p^\alpha}[x]/x^{p^\alpha} - x = R_{K_{p^\alpha}}$

(2)
$$R \cong K[u_1, \cdots, u_\alpha]/(u_1^p - u_1, \cdots, u_\alpha^p - u_\alpha)$$
wenn $K \geq K_{p^\alpha}$; dabei $K = K[x]/x^{p^\alpha} - x$
etwa $\alpha = 3$ Bew: Wähle $\alpha, \beta, \gamma \in K_{p^3}$ so, daß mit

$$\alpha' = \alpha^p, \quad \alpha'' = \alpha^{p^2} \text{ gilt } \begin{vmatrix} \alpha & \alpha' & \alpha'' \\ \beta & \beta' & \beta'' \\ \gamma & \gamma' & \gamma'' \end{vmatrix} \neq 0$$

In R_K setze

$$\begin{aligned} u_1 &:= \alpha x + \alpha' x^p + \alpha'' x^{p^2} \\ u_2 &:= \beta x + \beta' x^p + \beta'' x^{p^2} \\ u_3 &:= \gamma x + \gamma' x^p + \gamma'' x^{p^2} \end{aligned}$$

227/228

Dann ist in $u_i^p \equiv u_i \bmod x^{p^3} - x$.
Umgekehrt; definiert in $K[u_1 u_2 u_3]$ drei Polynome xyz von $u_1 u_2 u_3$ durch

$$\begin{aligned} u_1 &:= \alpha x + \alpha' y + \alpha'' z \\ u_2 &:= \beta x + \beta' y + \beta'' z \\ u_3 &:= \gamma x + \gamma' y + \gamma'' z \end{aligned}$$

Dann folgt aus $u_i^p = u_i$:

$$\begin{aligned} u_1 &:= \alpha z^p + \alpha' x^p + \alpha'' y^p \\ u_2 &:= \beta z^p + \beta' x^p + \beta'' y^p \\ u_3 &:= \gamma z^p + \gamma' x^p + \gamma'' y^p \end{aligned}$$

also

$$x = z^p \quad y = x^p \quad z = y^p$$

daher

$$x^{p^3} = x$$

RK_{p^α} sollte gut geeignet sein zur Untersuchung der Abb von K_{p^α} in sich. Alle diese u_i sind additive Funktionen auf K_{p^α}, wenn für $\xi \in K_{p^\alpha}$ gesetzt wird $u_i(\xi) = \alpha\xi + \alpha'\xi^p + \alpha''\xi^{p^2}$; Die Translationsgruppe (p, p, p) von K_{p^α} ist $x^\tau = x + d_i$.
$u_1 = u_1 + \alpha\xi + \alpha'\xi' + \alpha''\xi''$ usw., d.h.

228/229

die Translationen sind die p^α Transform

$$\mathfrak{T}: \quad u_i^\tau = u_i + \tau_i \text{ mit } \tau_i \in K_p$$
$$(\mathcal{N}\mathfrak{T})_0 \text{ ist } u_i' = \sum c_{ik} u_k, \quad \det c_{ik} \neq 0$$
$$\mathcal{N}\mathfrak{T} \text{ ist } u_i' = \sum c_{ik} n_k + d_i$$

Ist $\mathfrak{G}$ auf K_{p^3} 2-abgeschlossen und sind je zwei nichttriviale Bahnen von $\mathfrak{G}_0$ konjugiert (azimutaler Fall) so erhält $\mathfrak{G}$ mit $g(x)$ stets auch $g(ax)$ $a \in K_p$, und mit $f(x)$ ist (auch ohne 2-Abschließg) $f(ax)$ eine Invariante von $\mathfrak{G}$, $\forall a \in K_p$

$$\xi \in K_{p^\alpha} \iff (u_1, u_2, u_3) \in K,$$

wo $u_1 = \alpha\xi + \alpha'\xi^p + \alpha''\xi^{p^2}$ usw.

(2) NB: Zur Behandlung der P Gr mit reg $\mathfrak{H} \cong (\underbrace{p, p \cdots, p}_{\alpha})$ wird sich der Körper K_{p^α} nur dann empfehlen, wenn in $\mathfrak{H}$ eine Ugr der Ord p^β, $\beta \mid \alpha$ ausgezeichnet ist, oder eine Kette von solchen; die wird man dann mit Teilkörpern von K_{p^α} identifizieren, oder wenn bestimmte Autom. von $\mathfrak{H}$ interessieren, die man

229/230

besonders gut in K_{p^α} darstellen kann. In allen anderen Fällen wird man besser als Ω den Vektorraum $\mathfrak{V}$ der Dim α über K_p nehmen, etwa $\mathfrak{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_\alpha \end{pmatrix}$ $x_i \in K_p$. Invariante sind Funktionen $f(\mathfrak{x})$, Abbildungen von Ω in sich sind Funktionen n-Tupel:

$$f(\mathfrak{x}) = \begin{pmatrix} f_1(\mathfrak{x}) \\ \vdots \\ f_\alpha(\mathfrak{x}) \end{pmatrix},$$

Faltung ist

$$f \wedge g = \sum_{A \in \mathfrak{V}} f(\mathfrak{x} - A) g(A)$$

Vorteilhaft ist hier die Regel von den getrennten Veränderlichen: Wenn $f(x_1 \cdots x_\alpha) = f'(x_1 \cdots x_\beta)$, und ähnlich g, $f''(x_{\beta+1} \cdots x_\gamma)$ so ist

$$f \wedge g = (f_1' \wedge g') \cdot (f'' \wedge g'')$$

Insbesondere ist die Faltung von Monomen $x_1^{n_1}\ x_2^{n_2} \cdots x_\alpha^{n_\alpha}$ leicht, nämlich variablenweise auszuführen.
Dann braucht man die Binomialformel nicht:

$$\binom{n_0 + n_1 p + \cdots}{k_0 + k_1 p \cdots} \equiv \prod \binom{n_i}{k_i} \quad \text{mod } p.$$

Wieder gilt, wenn Exp $h(x_1 \cdots x_\alpha)$ die Menge der wirklich auftretenden Exponentenkombinationen bezeichnet:
Ist f Invariante von $\mathfrak{G}_0$ und $x_1 = f \wedge \therefore$, so ist für jedes $g \in \mathfrak{G}$
Exp $g_1 \subseteq$ Exp f.

230/231

(1) Der Ring aller Funktionen auf endlichem Ω mit Werten aus einem Körper K mit $|K| > 2$ ist ein Hauptidealring.
Der ggT von f und g ist die Funktion, die auf
Träger $f \cup$ Träger $g = 1$ ist, sonst $= 0$
Jedes Element von $K[x_1 \cdots x_\alpha]_{(x_i^p - x_i)_\alpha}$ ist Produkt von Faktoren $\sum c_\nu x_\nu + d$.
Bew:

$$\cong K K_{p^\alpha}[x]/xp^\alpha - x.$$

(2) Im Ring mit $\alpha = 2$ ist $l_1 \wedge l_2 = \begin{cases} 1 \\ 0 \end{cases}$ wenn l_1, l_2 lin $\genfrac{}{}{0pt}{}{\text{un}}{\text{ab}}$; daher $l_i = c_{i1} x_1 + c_{i2} x_2$

231/232

Gruppen vom Grad p^2

Satz II Wenn $\mathfrak{G}$ drei elementfremde rationale Komplexe $\neq \{1\}$ hat mit Längen $2 < n_1 \leq n_2 \leq n_3$, so ist $\mathfrak{G}$ linear oder $\mathfrak{G} \triangleright \mathfrak{N} \neq$ intra $\mathfrak{G}/\mathfrak{N}$ auflösbar.
Beweis: oBdA $\mathfrak{G}$ 2-abg. Besteht $\mathfrak{K}_1$ aus n_1 Ugr der Ord p, und ist die i-te von ihnen gekennzeichnet durch $l_i(x_1, x_2) = 0$, so ist (l_i linear),

$$\sum_{i=1}^{n_1} l_i^{p-1} =: f_1 \text{ inv. bei } \mathfrak{G}_0 = \begin{cases} n_1 - 1 & \alpha \in \mathfrak{K}_1 \\ n_1 & 0 \neq \alpha \notin \mathfrak{K}_1 \\ 0 & \alpha = 1 \end{cases}$$

ebenso

$$\sum_{j=1}^{n_2} m_j^{p-1} =: f_2.$$

Wegen $n_1 > 1$ sind $x_1, x_2 = f_1 \wedge \therefore$ also für $\forall g \in \mathfrak{G}$ $(g_1, g_2 = f_1 \wedge \therefore$
daher, wenn $\mathfrak{G}_1$ hom Leitglied $g_1 = h_1$; Gr $h_1 = k$:

$$\begin{aligned} h_1 &= \sum c_i l_i^k \\ \text{aber ebenso} \qquad &= \sum d_j m_j^k \end{aligned}$$

Für $k \geq n_1 + n_2 - 1$ sind $l_1^k \cdots m_{n_2}^k$ lin un, also ist $k \leq n_1 + n_2 - 2 \leq \frac{2(p+1)}{3} - 2 < \frac{2}{3}(p-1)$
Ebenso Leitglied g_2.
NB: Das Gleiche gilt für jede Funktion f mit $f = f_1 \wedge \therefore = f_2 \therefore$

232/233

Also ist Gesamtgrad $\frac{g_1}{g_2} < \frac{2(p-1)}{3}$; kurz: Exp $g_i \subseteq: \mathcal{E}$.
Nach Vor. ist $n_1 > 2$.
Dann ist x_1^2 und x_2^2 von der Form $f_1 \wedge \therefore$, also ist nach NB 232

$$\text{Exp} \begin{cases} g_1^2 \\ g_2^2 \end{cases} \subseteq \mathcal{E}.$$

Auf Leitglied h_1 wende (1) von S. 223 an:

$$h_1^2 = r x_1^p + s x_2^p \qquad \text{Gr}\, r, s = 2k - p = m$$

$\Rightarrow$ entw.

$$k := \text{Gr}\, h_1 \leq 2m - 1 = 4k - 2p - 1 \qquad k \geq \frac{2p-1}{3}\!\!\begin{smallmatrix}\downarrow\\\uparrow\end{smallmatrix}$$

oder

$$\exists l^{\frac{p+1}{2}} \big| h_1 = \sum^{n_1} c_i l_i^k = \sum^{n_2} d_j m_j^k$$

Differenziere mit n_1-1 lin Op, die alle l_i außer einem l_0, zum Verschwinden bringen. Wenn

$$n_1 - 1 \begin{cases} < & \frac{p+1}{2} \\ < & k \end{cases}, \text{ so bleibt } l \big| l_0^{\text{pos}}, l = l_0$$

Wenn sogar

$$n_2 - 1 < \begin{cases} \frac{p+1}{2} \\ k \end{cases} \qquad ,$$

so ebenso $l = m_0$; aber $l_i \neq m_j$. $\downarrow\!\uparrow$

233/234

Also ist

$$n_2 - 1 \geq \frac{p+1}{2} \text{ oder } \geq k.$$

Der erste Fall ist unmöglich wegen

$$\frac{p+1}{2} < n_2 \leq n_3 \Rightarrow n_2 + n_3 > p + 1,$$

also

$$\begin{aligned} k &\leq n_2 - 1 < \frac{p+1}{2} \\ k &\leq \frac{p-1}{2} \end{aligned}$$

Dann ist Exp g_1 im 1. Quadranten I von 210: $\mathfrak{G}$ linear oder $\trianglerighteq \mathfrak{N}$ intra, $\mathfrak{G}/\mathfrak{N}$ aufl.

Satz III. Sei $\mathfrak{G}$ pri, Grad p^2, mit reg Ugr. $\mathfrak{G}$ habe einen nichttrivialen rationalen Komplex; $\mathfrak{G}$ habe einen irrationalen Komplex. Dann ist $\mathfrak{G}$ linear.

Bew: Nach II hat $\mathfrak{G}$ nur einen nt rat Komplex, daher nur eine l.u. homogene Invariant f_0 vom Grad $p-1$. Wenn $\mathfrak{G}$ eine hom Inv vom Grad $< \frac{2}{3}(p-1)$ hat, so wohl fertig wie früher ($\sim$ 225)
Hat $\mathfrak{G}$ keine hom Inv., so kleinen Grades, so gibts $f_1, f_2 \in \mathfrak{F}_0$ mit $f_1(ax) = a^\alpha \cdot f_1(x)$

$$f_2(ax) = a^\beta f_2(x), \quad \alpha + \beta = p - 1, \ \ {}^{\alpha}_{\beta} \neq 0; \quad \alpha \leq \beta.$$

Dann

$$f_1 \wedge f_2 = cf_0 + d \Rightarrow f_0 \wedge f_1 \wedge f_2 = cf_0 \wedge f_0 = c \cdot e$$

234/235

$e \underset{p}{\not\equiv} 0$, da

$$\begin{aligned} e &= \sum f_0(-t) f_0(t) \\ &= (p-1)\cdot[k(k-1)^2 + (p+1-k)k^2] \end{aligned}$$

wenn der rat Komplex aus k Ugr besteht. Wegen $\mathfrak{G}$ pri ist $k > 1$, daher $e \not\equiv 0(p)$. Also ist $f_0 \wedge f_1 \neq 0$, das ist also homogen vom Grad $\alpha \leq \frac{p-1}{2}$.

HS $\mathfrak{G}$ 2-ab pri, reg el ab Ugr, Grad $p^2 \Rightarrow$ entweder Rang $g \leq 3$, jeder Komplex rational.
oder $\mathfrak{G} \underset{2}{\triangleright} \mathfrak{G}^* = \mathfrak{H}_1 \otimes \mathfrak{H}_2$ Kroneckerprod, $\mathfrak{G}_1 \cong \mathfrak{G}_2$ (von $k = 2$)
Einzelheiten bei Existenz einer vom Invariant oberhalb $\frac{2}{3}(p-1)$ noch nachzuprüfen.
Bew: I, II III $\in$ 234, tritt Rg $\mathfrak{G} = 3$ auf?
Kurz: $\mathfrak{G}$ unipri, Grad $\mathfrak{G} = p^2 \Rightarrow$ i.a. $\mathfrak{G}$ linear: $\mathfrak{H} \trianglelefteq \mathfrak{G}$.

235/236

$\lhd\lhd$

Unterhaltung mit Mr. Camina, QMC, London 22.10.64

(1) Def:

$$G \in \mathcal{Z} :\Longleftrightarrow \quad \text{If } G \trianglerighteq\trianglerighteq A \underset{\substack{|\\ \text{simple}}}{\triangleright} B. \text{ then } \mathcal{N}_G A \trianglelefteq\trianglelefteq G$$

$$G \in \mathcal{X} :\Longleftrightarrow \ A \trianglelefteq\trianglelefteq G \Rightarrow \mathcal{N} A \lhd\lhd G$$

clear: $\mathcal{X} \subseteq Z$.. Problem: $\mathcal{X} = Z$?

$$W(G) = \bigcap \mathcal{N}_G A, \quad A \lhd\lhd G.$$

(2)

result:	$G/W(G)$ nilp	$\Rightarrow G \in \mathcal{X}$
problem:		$\Leftarrow$?

3) Unterhaltung mit Barratt, Prof, Manchester:
Gilt

$$G_1 \times Z_\infty \cong G_2 \times Z_\infty \Rightarrow G_1 \cong G_2 \quad ?$$

4) Arbeit D. Robinson erschien Proc. Camb. PhSoc. 1964

236/237

31.1.65 nach Rektorfest
Erweiterung der Theorie max. π-Gruppen.

Sei $\mathcal{Q}G$ die Menge der In-Gruppen (Ausschnitte) von G.
Sei $\mathfrak{I}$ ein Ideal in $\mathcal{Q}$: $A \in \mathcal{Q},\ B \in \mathfrak{I}$
$\Rightarrow A\neg B \& B\neg A \in \mathfrak{I}$ (gleichwertig: $\Rightarrow B\neg A \in \mathfrak{I}$)
[NB: $\mathfrak{I}\mathcal{Q} \subseteq \mathfrak{I} \Rightarrow \mathcal{Q}\mathfrak{I} \subseteq \mathfrak{I}$]
Das Ideal habe die zusätzlichen Eigensch:

I. $G_1 \trianglelefteq G_3$, $G_1 \leq G_2 \trianglelefteq G_3$, $G_2/G_1 \in \mathfrak{I}$, $G_3/G_2 \in \mathfrak{I} \Rightarrow G_3/G_1 \in \mathfrak{I}$ („Integrabität") (od „Additivität")

II $G_0 \trianglerighteq G_1$, $G_0 \triangleright G_2$, $G_1 \cap G_2 = G_3$, $\exists I \in \mathfrak{I}$ mit $I\neg G_0/G_i = G_0/G_i \quad (i = 1, 2)$ $\Rightarrow G_0/G_3 \in \mathfrak{I}$.

III Ist $G_0 \trianglerighteq G_2$, $G_0 \trianglerighteq G_1 \trianglerighteq G_2$ und $G_0/G_1 \in \mathfrak{I}$, $I\neg G_1/G_2 = \{G_2/G_2\}$, so exist $H/G_2 \leq \mathfrak{I}:\ HG_1 = G_0$, $H \cap G_1 = G_2$, und je zwei solche H's sind konj in G_0.

Dann sind vermutlich je zwei Maximal Ausschnitte in $\mathfrak{I}$ die dieselben Projektionen in eine K_i-Reihe von G ergeben, konjugiert in G.

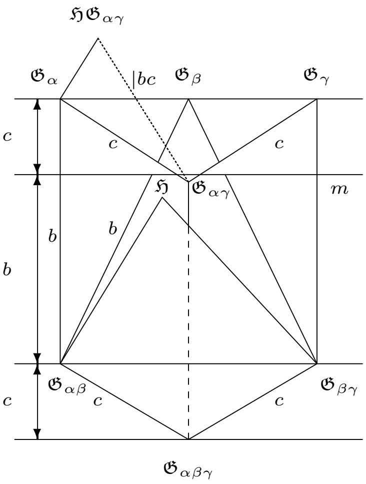
237/238

Teilkonstit. primitiver P. - Gruppen

(1) $\mathfrak{G}$ tra Ω, $\mathfrak{G}_\alpha$ simultan tra, auf $\beta^{G_\alpha} \neq \gamma^{G_\alpha}$ mit Längen $b \geq c$; $(|\Omega| = n)$. $\mathfrak{G}$ habe keinen Teilgrad m mit $m \geq b$ und $m \big| bc$.

$$\Rightarrow \mathfrak{K} := \langle \mathfrak{G}_\alpha, \mathfrak{G}_\gamma \rangle \subseteq \mathfrak{G}_{\alpha\gamma}\mathfrak{G}_\beta; \quad c \leq |\mathfrak{K} : \mathfrak{G}_a| \big| (b, n) \ ;$$

wenn $c > 1$, so $\mathfrak{G}$ impri
Zusatz $1'$ auf S. 239
Bew:



$$\begin{aligned}
\mathfrak{G}_{\alpha\beta} \cdot \mathfrak{G}_{\alpha\gamma} &= \mathfrak{G}_\alpha \\
|\mathfrak{G}_{\alpha\gamma} : \mathfrak{G}_{\alpha\beta\gamma}| &= b \\
|\mathfrak{G}_\alpha : \mathfrak{G}_{\alpha\beta\gamma}| &= bc \\
bc = |\mathfrak{G}_\gamma : \mathfrak{G}_{\alpha\beta\gamma}| &\leqq |\mathfrak{G}_\gamma : \mathfrak{G}_{\alpha\gamma}||\mathfrak{G}_\gamma : \mathfrak{G}_{\beta\gamma}| \\
&= cm
\end{aligned}$$

$$m \geq b \quad m|bc$$

$$m = b$$

Also steht hier: (Pfeil auf $\leqq$ oben) $=$

$$\mathfrak{G}_{\alpha\beta}\mathfrak{G}_{\beta\gamma} = \mathfrak{G}_\gamma$$

$$\begin{array}{lll}
\mathfrak{G}_{\alpha\gamma} & \text{vtb mit} & \mathfrak{G}_{\alpha\beta},\ \mathfrak{G}_{\beta\gamma} \\
\mathfrak{G}_{\alpha\gamma} & \text{vtb mit} & \langle\mathfrak{G}_{\alpha\beta},\ \mathfrak{G}_{\beta\gamma}\rangle =: \mathfrak{H}
\end{array}$$

also

$$\mathfrak{G}_\alpha,\ \mathfrak{G}_\gamma \leq \mathfrak{G}_{\alpha\gamma}\mathfrak{H} \subseteqq \mathfrak{G}_{\alpha\gamma}\mathfrak{G}_\beta$$

$$c \leqq |\langle\mathfrak{G}_\alpha, \mathfrak{G}_\gamma\rangle : \mathfrak{G}_\alpha| \text{ teilt } b;$$

Wenn $c > 1$ so $\mathfrak{G}$ impri
Bew:

$$\mathfrak{G}_\alpha\mathfrak{G}_\gamma \subseteq \mathfrak{K} \subseteq \mathfrak{G}_\alpha\mathfrak{G}_\beta$$

Wde!

238/239

Zusatz 1′: Wenn

$$(\mathfrak{K} : \mathfrak{G}_\alpha) = b,$$

so ist wegen $\mathfrak{K} \leq \mathfrak{G}_\alpha\mathfrak{G}_\beta$ sicher $\mathfrak{K} = \mathfrak{G}_\alpha\mathfrak{G}_\beta$ also $\mathfrak{G}_\alpha$ vertb $\mathfrak{G}_\beta$.
Frage: Gehts ebenso für Mannings Satz über 2-tra Konst von $\mathfrak{G}_\alpha$.

239/240

Frage von Dénes, J. Budapest 1965:

Gibt es eine Gruppe G, in der ein passendes Element $g' \in G'$ nicht ein Kommutator ist?

Gruppen $\mathfrak{G}$ vom Grad p.

(1) Zwei Untergr. vom Index p, die je eine Bahn gleicher Länge besitzen, sind konjugiert.
Denn von $\mathfrak{G}_1$ aus haben sie dieselbe Invariante.

(2) $\mathfrak{G}$ 3-tra $\Rightarrow$ Klassenzahl $c_p = 1$ (Ito)

(3) $a^2 j_1 = b^2 j_2 \Rightarrow j_1 = j_2$ oder $a^2 = b^2$
Bew: $a^2 k(p-k) = b^2 l(p-l)$ oBdA $ak \geq bl; a, b > 0$
$ak = \delta bl + xp \quad \delta = \pm 1 \ \frac{p}{4} > x \geq 0 \quad a^2, b^2 \leq \frac{p+1}{4}$

[1] $\delta a - b - 2\delta x = yp$

[2] $bly = x(a-x)$

[1] Zeigt: $y = 0$

[2] Zeigt:

$$\textbf{???} \begin{cases} x = 0 \to ak = bl & a(p-k) = b(p-l) \quad a = b \\ x = a \to ak = \delta bl + ap & a(p-k) = bl \quad ak = b(p-l) \quad a = b \end{cases}$$

240/241

Gruppen vom Grad p Forts. v. 83

Satz: Ist $j_1 j_2 = j_3 j_4$, so ist $j_1 = j_3$ oder $j_1 = j_4$.
Bew: Sei

$$j_1 = \frac{k(p-k)}{p-1}, \quad j_2 \cdots l, \ j_3 \cdots m, \ j_4 : \cdots m$$

oBdA sei $kl \geq mn$; $k, l, m, n < \frac{p}{2}$

$$k(p-k)l(p-l) = m(p-m)n(p-n)$$

$$\circledast \qquad kl = \delta mn + xp \qquad \delta = \pm 1$$

daher

$$0 \leq kl - mn \leq xp \leq kl + mn < 2 \cdot \frac{p}{2}\frac{p}{2} \qquad 0 \leq x < \frac{p}{2}$$

gibt eingesetzt in $kl(p^2 - p(k+l) + kl) = \cdots$

$$\begin{cases} m + n + \delta(2x - k - l) = py & \text{(I)} \quad \surd \\ mn(1-y) = (k-x)(l-x) & \text{(II)} \quad \surd \end{cases}$$

(I) zeigt, da $x \geq 0$, wegen $kl \geq mn$:

$$-p < py < 2p, \quad y = \begin{cases} 1 \\ 0 \end{cases} \qquad \surd$$

Fall $\underline{y = 1}$: $(k-x)(l-x) = 0$ etwa $x = k$ $\circledast$ gibt $k(p-l) = -\delta mn$, also $\delta = -1$.
$mn = k \cdot (p-l)$ & $m + n = k + (p-l)$ (aus I) geben $\{m, n\} = \{k, p-l\}$, etwa
$m = p - l > \frac{p}{2}$ W! $\surd$

Also ist
<u>$y = 0$:</u>

$$\left.\begin{array}{lccc} \mathrm{I} & m+n & = & \delta(k+l-2x) \\ \mathrm{II} & mn & = & \delta(k-x)\cdot\delta(l-x) \end{array}\right\} \{m,n\} = \{\delta(k-x), \delta(l-x)\} \qquad \surd$$

etwa $m = \delta(k-x)$, $n = \delta(l-x)$; $x = k - \delta m = [= l - \delta_n]$

$\circledast \quad kl = \delta mn + kp - \delta mp = k(p-l) = \delta m(p-n)$ also $\delta > 0,\ \delta = +1 \quad \surd$
$\circledast \qquad kl = +(k-x)(l-x) + xp$ gibt $0 = x(p-k-l+x) \quad \surd$

Ist $x = 0$, so $m = k$, $j_1 = j_3$. Ist $(\ \ ) = 0$, so $m = k - x = p - l > \frac{p}{2}$ W!

241/242

Gruppen vom Grad p

Aus der Vorauss.

$$k(p-k)l(p-l) = m(p-m)a^2(p-1), \quad a \neq 1, a > 0,\ k,l,m < \frac{p}{2}$$

wenn das aus $\kappa\lambda = a\mu$ entstand, gilt
$q|a \Rightarrow q|k$, $q|l$ bei passend. Normg.

folgt:

(1) $kl = \delta ma + xp$

(1′) $a^2m^2 < pj_1j_2$

(1′) $am < \frac{1}{4}p^{\frac{3}{2}}$

(1″) $|\lambda| < \frac{1}{4}(p + \sqrt{p})$

(2) $\delta(2x-k-l) + a(m+1) = yp$

(3) $(a-y)am = (k-x)(l-x)$

(3′) s.u. Frage: verfeinerbar in $Q(\sqrt[p]{1})$? Frage: ac |?

(4) Für $j = \frac{k(p-k)}{p-1} \neq 1$ ist $\frac{k}{2} < j < k$; $\sqrt{p} - 1 < j \leq \frac{p+1}{4}$
y, a, m bestimmen $k-x, l-x$
Unter der Voraussetzung $k < m < l$, also $j_1 < j_3 < j_2$, folgt:

(5) $\frac{kl}{4m} < a^2 < \frac{2kl}{m}$; stets $x \leq k, l \quad |y| \leq |c|$

(5′) $j_1 < a^2 < j_2$

(6) $x < l \qquad (1)$

(3′) $x(p+x-k-l) = am(a-y-\delta)$

(7) $y < a$ (2)

(8) $x < k$ (1)(5)

(9) $x > 0$ (1)(5)

(10) $(k-1)(l-1) + 2x + \delta a - 1 = p(x + \delta y)$

(11) $x + \delta y \geq 0$ (10)

242/243

26.9.65 (12) Ist $j_1 j_2 = a^2 j_3$ wegen $k\lambda = a\mu$, so ist $a|j_1$, $a|j_2$
Bew: Sei $q^\alpha|a$, wähle $\mathfrak{q}|q$, $\mathfrak{q} \nmid \kappa$.
Dann $\mathfrak{q}^\alpha|\kappa\lambda \quad \mathfrak{q}^\alpha|\lambda \quad \mathfrak{q}^\alpha|\lambda\overline{\lambda} = j_2 \quad q^\alpha|j_2$.
Anderer, einfacher Bew. 1. unten auf dieser Seite $*$

allg Zahlentheorie:

(13) Sind a, b, c, d paarweise teilerfremd, so ist

$$1 = a_1 bcd + ab_1 cd + abc_1 d + abcd_1$$

mit

$$|a_1| < |a|, \ |b_1| < b \quad \text{usw.}$$

Bew:

$$\frac{1}{abcd} = \frac{x_1}{a} + \frac{x_2}{b} + \frac{x_3}{c} + \frac{x_4}{d}$$

reduziere x_1 mod a, **???** y_1 und $0 \leq y_1$ ca **???**

$$n + \frac{1}{abcd} = \frac{y_1}{a} + \cdots + \frac{y_n}{d} \qquad n \in \mathbb{Z},\ 1 \leq n \leq \ \textbf{???}$$

ändert zwei oder 3 ein y_2 ab $\to y_2 - 1$.

Aus (12) folgt:

$\overset{?}{1978}$ (14)

$$\kappa\lambda = p^\alpha \mu \text{ kommt nicht vor}$$

$$a = p^\alpha \Rightarrow \begin{cases} a|k \ \ a|l \\ a|y \text{ oder } |y| < a \ y = 0 \end{cases}$$

$*$ Anderer Bew (12):

$$\kappa\lambda = a\mu \Rightarrow \lambda\overline{\mu} = \frac{j_2}{a} \cdot \overline{\kappa} \Rightarrow \overline{\kappa}\mu = \frac{\kappa\overline{\kappa}\lambda}{a} = \frac{j_1}{a}\lambda$$

$$* \quad \kappa\lambda = a\mu \Rightarrow \lambda\overline{\mu} = \frac{a\mu\overline{\mu}}{\kappa} = \frac{j_1 j_2}{a\kappa} = \frac{j_2}{a} \cdot \overline{\kappa}$$

15. Gilt $j_1 j_2 = a^2 j_3$ wegen $\kappa\lambda = a\mu$, so ist $j_1 j_2 j_3 = r^2$ mit $j_\alpha \big| r \big| j_\alpha j_\beta$
$j_1 = a_2 a_3, \cdots, \quad r = a_1 a_2 a_3$

16 Sei

$$K_1 K_2 = a_3 K_3^* + x_3 F \text{ und zykl.}$$

dann ist

$$\begin{gathered} K_1 K_1^* = a_2 a_3 I + c_1 F \text{ und zykl.} \\ k_1^2 = a_2 a_3 + c_1 p \text{ und zykl.} \\ k_1 = a_2 a_3 + c_1 \text{ und zykl.} \\ j_1 = a_2 a_3 \\ k_1(a_1 + x_1) = \text{ zykl } = t = \text{ const}_R \\ a_1 c_1 + k_1 x_1 = \text{ const} \\ k_1 k_2 = a_3 k_3 + x_3 p \end{gathered}$$

wenn $a_1 \leq a_2 \leq a_3$, so $a_2 a_3 < \frac{p}{4}$, daher $a_1, a_2 < \frac{\sqrt{p}}{2}$

17 Jeder Primteiler von $a_1 a_2 a_3$ ist 2^r-ter Rest mod p wenn $2^r \big| p - 1$.
denn kein $\mathfrak{q} | a_1 a_2 a_3$ ist $= \overline{\mathfrak{q}}$, so ist jeder Konjugierter $\mathfrak{q}_i$ reell, $\mathfrak{q}_i \big| \kappa \iff \mathfrak{q}_i \big| \overline{\kappa}$, $\forall q_i \big| \kappa$; $q \big| \kappa$ Wid!

$$0 \leq x_3 \leq \begin{cases} k_1 \\ k_2 \end{cases}$$

$$k_1(p - k_1) = a_2 a_3 (p - 1)$$

Ersetzg von k durch $p - k_2$ oder zyklische Vertauschung ergibt entweder $\{a_1, a_2, a_3\} \to \{a_1 a_2 a_3\}$ oder $\{a_1, a_2, a_3\} \to \{-a_1, -a_2, -a_3\}$

18.

$$kl - am = xp \Rightarrow |a| < \begin{cases} k^{\frac{2}{3}} \\ e^{\frac{2}{3}} \end{cases} \qquad \text{oder} \prod_{\substack{|| \\ x()()()}} = 0$$

also $x \approx \frac{kl}{p}$, $x_3 \approx \frac{k_1 k_2}{p}$

$$\begin{gathered} k(p - l) + am = (k - x)p \\ (p - k)l + am = (l - x)p \\ (p - k)(p - l) - am = (p - k - l + x)p \\ x(k - x)(p - l)(p - k - l + x) \equiv 0 \mod a^3 m^2 \end{gathered}$$

wenn $\prod :=\downarrow\neq 0$, so

$$|a^3m^2| \leq k^2 l(p-l) \text{ wenn } k < l$$

da $m \to p-m$ nichts an $|a|$ ändert, folgt

$$|a^3|(\frac{p+1}{2})^2 \leq k^2 \frac{p-1}{2}\frac{p+1}{2}$$

$$|a^3| \leq k^2 \quad \begin{array}{ccc} |a| & \leq & k^{\frac{2}{3}}, \text{ also auch} \\ |a| & \leq & l^{\frac{2}{3}} \end{array}$$

$$|a_1| \leq |a_2| \leq |a_3| \Rightarrow |a_1| \geq p^{\frac{1}{4}},\ |a_2| \leq \frac{1}{2}\sqrt{p},\ |a_3| \leq \left(\frac{p}{2}\right)^{\frac{2}{3}}$$

$$|a_1a_2a_3|^2 = j_1j_2j_3 < \frac{p^3}{4^3}$$

$$|a_1a_2a_3| < \frac{p^{\frac{3}{2}}}{8}$$

19. Der Automorphismus $g \to g^{KT}$ der Ordnung 2 von $\langle \mathfrak{G}, \mathfrak{G}^{KT}\rangle$ läßt ein Element i aus einem 2-Sylow - Zentrum fest. i untersuchen ?!

245/246

Perm Gr vom Grad p^2 Forts. von 235

(1) Ist $l(\mathfrak{x}) = \alpha_1x_1 + \alpha_2x_2$, so ist für $0 \leq i \leq q = p-1$

$$l^i(\mathfrak{x}) \wedge (x_1^q x_2^q(\frac{\gamma_1}{x_1} + \frac{\gamma_2}{x_2})) = -il^{i-1}(\mathfrak{x}) \cdot l(\gamma_1, \gamma_2)$$

Ähnlich zu Differentiation

(2)

$$f := \sum_\rho{}' l_\rho(\mathfrak{x})^q, \quad h := f \wedge (x_1^q x_2^q(\frac{\gamma_1}{x_1} + \frac{\gamma_2}{x_2})) \Rightarrow$$

$$h^2\big|_{x_1^{q-2}x_2^q} = 2 \cdot \sum_{\rho,\sigma} \underline{\beta_\rho\beta_\sigma l_\rho(\mathfrak{c}) \cdot l_\gamma(\mathfrak{c})} \cdot \Delta_{\rho\sigma}^{q-2}$$

$$\Delta_{\rho\sigma} = \begin{vmatrix} \alpha_\rho & \beta_\rho \\ \alpha_\sigma & \beta_\sigma \end{vmatrix}$$

$$l_\rho = \alpha_\rho x_1 + \beta_\rho x_2 \qquad \mathfrak{c} := (\gamma_1\gamma_2)$$

(3) Wenn $f(\mathfrak{x}) \in$ inv G_0, dann

$$\sum_{\mathfrak{t}} f(\mathfrak{x}-\mathfrak{t})f(\mathfrak{y}-\mathfrak{t})f(\mathfrak{z}-\mathfrak{t}) =: {}^3f \quad \in \text{ inv } G.$$

Das sollte man auf $f = \sum' l_\rho^2$ anwend. Es wird ${}^3f \neq 0$

(4)

$$\sum_{\mathfrak{t}} t_1^{\alpha} t_2^{\beta} = \begin{cases} 1 & \alpha \text{ und } \beta \text{ pos-Vielfache von } q \\ 0 & \text{sonst} \end{cases}$$

(5) Ist

$$f = \sum_{\rho=1}^{\mathfrak{r}} l_\rho(\mathfrak{x})^q, \text{ so ist } r(r-1) \geq p-2; G \text{ nichtlinear}$$

Bew. Schätze Anzahl der Pkte ab, die von zweien sichtbar.

246/247

Perm Gr vom Grad p : Burnside-Beweis.

B: $\sum tg(t) = 0$ wenn $\mathfrak{G}$ 1-tra

(1) $\exists$ invariante

$$f(x) = \sum_0^n a_\nu x^\nu \quad 0 < n < p-1, a_n \neq 0$$

wenn $\mathfrak{G} \neq$ 2- tra

(2)

$$\begin{aligned} \sum t \big| f(x^{g^{-1}} - t) &= f(x - t^g) = a_n(x-t^g)^n + a_{n-1}(x-t^g)^{n-1} + \cdots \\ &= a_n(-t)^n + \mathbf{???}(t) \\ c &= \sum t f(x - g(t)) \\ &= x^n \cdot \therefore + x^{n-1}[a_{n-1} \sum_t \overline{m} a_n n \sum tg(t)] \end{aligned}$$

[Anmerkung mit Verweispfeil auf das erste Gleichheitszeichen in (2):
Koeff von $x^{n-1}t^n$ ist links 0, rechts = Koeff t^n in $g(t) + na_n$
also Grad $g < n$]
also

$$\sum_t tg(t) = 0 \quad x \perp g, \forall g$$

A: Lemma: Gr $\mathfrak{G} = p$, $\sum tg(t) = 0 \forall g \in \mathfrak{G} \iff g = ax + b, \forall g$
Bew:

(3) Aus

$$\mathcal{F}(x) \perp g(x), \quad \forall g \in G$$

folgt

$$\begin{cases} \mathcal{F}(h(x)) \perp g(x) \\ \mathcal{F}'(x) \perp g(x) \\ k(x) \perp g(x) \\ \forall \text{ Gr } k \leq \text{ Gr } \mathcal{F} \end{cases}$$

(3)
$$h(x) \perp g(x) \quad \forall g, h \in \mathfrak{G}$$

(4)
$$m = \max \operatorname{Grad} g \Rightarrow 2m < p - 1$$

(5)
$$1, x, x^2, \cdots, x^{\frac{p-1}{2}} \perp g(x) \forall g$$

(6)
$$h^\kappa \perp g \quad \forall g, h \qquad \kappa = 0, 1, \cdots, \frac{p-1}{2}$$
$$\text{red Gr}\, h^\kappa < p - 1 - m \qquad 0 < \kappa \leq \frac{p-1}{2}$$

also
$$\kappa m < p - 1 - m \text{ wenn } \kappa m \leq p - 1,\ 0 < \kappa \leq \frac{p-1}{2}$$

(7) Wäre $m \geq 2$, so $\exists \kappa : 0 \leq \kappa \leq \frac{p-1}{2}$ $\quad p - 1 = \kappa m + r \quad \delta \leq r \leq m\ \kappa m \leq p - 1$ $\kappa m < p - 1 - m \qquad r = p - 1 - \kappa m > m$ Wid.
folgt B

247/248

$$\bigcap H^x H^y$$

(1) Für $H \leq G$ defin.
$$_G H = \bigcap_{\substack{x,y \in G \\ H^x \neq H^y}} H^x H^y$$

(2) $(_G H)^g = {_G H}, \ \forall g \in G$

(3) $_G H \leq G$. $u, v \in {_G H} \quad u = h_1^x h_2^y,\ v = h_3^y h_4^x\ uv = h_1^x (h_2 h_3)^y h_4^x$ konj zu $(h_4 h_1)^x (h_2 h_3)^v$

(4) $x \in {_G H} \Rightarrow H^x = H$ sonst $x \in H H^x$, Wid.

(6) $x \in {_G H} \Rightarrow (H^y)^x = H^y \quad (4)$

(6) $x \in {_G H} \Rightarrow x \in H$ Bew: $x \in H^x \qquad x = x^{-1} h x \qquad x = h$

(7)
$$\bigcap_{H^x \neq H^y} H^x H^y = \bigcap_{x \in G} H^x \qquad (6)$$

Idee zu Grad p:

(a) Die Fktion zu KT aufstellen, Involutionen suchen, die sie fest lassen.

(b) Invarianten $\mathcal{F}(x_1x_2x_3)$ suchen. z.B. $\sum\limits_t f(x_1-t)f(x_2-t)f(x_3-t)$

(c) Für nicht 3-tra Gruppen: Ist $f(xy)$ inv bei $\mathfrak{G}_0$ irgendeinem $\mathfrak{H} \underset{p}{<} \mathfrak{G}$, so ist zu $F(xy) := \sum f(x-t; y-t) \cdot \varphi(x)$ stets Grad $f(x^g, y^g) \leq$ Grad $f(xy)$ Wenn $\exists f$ mit Gesamtgrad $< p-2$, so $\mathfrak{G}$ linear (das muß Bew für den Fall $|\mathcal{N}\mathfrak{P} : \mathfrak{P}| = p-1$ geben.)

(d) $x \to \varphi(x)$ beschreibt eine Permutation von F_p genau wenn

$$\sum_{t=0}^{p-1} \varphi(t)^{\nu} = 0$$

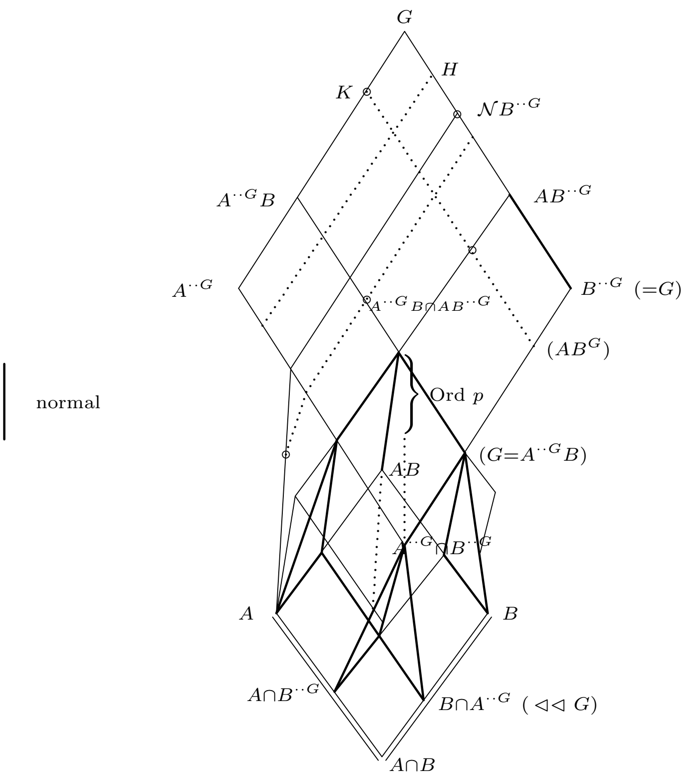
für $\nu = 0, 1, \cdots, p-2$ und $\varphi(x) \neq$ const.
Bew: sonst Vielfachheit x_λ von χ im Wertevorrat von φ:
$\varphi \neq 0$ gibt $\sum \lambda^\nu x_\nu = 0$ für r verschiedene $\lambda's$, $r < p-1$ $v_\nu \equiv 0$ Wid.

248/249

ω-Untergruppen

Aufgabe: Untersuche die ω-Kerne von G, das sind die Untergruppen von G, die zu jeder ω-Untergruppe von G eine konjugierte enthalten.

[Eingelegtes Skizzenblatt:]
XIII zu S. 250
Beh: A v B^x f alle $B^x \leq B^{\cdot\cdot G} \Rightarrow A^{\cdot\cdot G} \cap B^{\cdot\cdot G} \leq AB$
falls A, B Gegenbeisp mit maximalem $|A| + |B|$; $(AB)_G = 1$



[rote Beschriftungen sind eingeklammert.]

$(B \lhd A^G B)$
$A^G B \le H < G \Rightarrow B \lhd\lhd H \& B \lhd A^{\cdot\cdot G}B \cap B^{\cdot\cdot G}$
$A^{\cdot\cdot G}B \le H < G \Rightarrow B \lhd\lhd H$
$AB \le H < G \Rightarrow \underset{B}{\overset{A}{\text{oder}}} \lhd\lhd H \qquad N_{\min} \neq N' \Rightarrow N \le A^{\cdot\cdot G} \cap B^{\cdot\cdot G}$
$A, B \trianglelefteq A^{\cdot\cdot G}B \cap AB^{\cdot\cdot G}$
$A \trianglelefteq\trianglelefteq \mathcal{N}B^{\cdot\cdot G}$ wenn die $\neq G$, $B \lhd\lhd K$ wenn $\underset{B}{A}^G \le K < G$
[Nur schwach lesbare Textteile werden als ausradiert interpretiert.]

249/250

$\lhd\lhd$

Vermutung: G endl, (oder $\in \max sgp$); $A, B \le G$,

$$\forall x, y \in G(\text{ od } \left\{ \begin{array}{l} \forall y \in B^{\cdot\cdot G} \\ \forall x \in A^{\cdot\cdot G} \end{array} \right\} \quad A^x \text{ v } B^y) \Rightarrow A^{\cdot\cdot G} \cap B^{\cdot\cdot G} \le AB.$$

Das Gegenbeispiel mit kleinstem $|G : A| + |G : B|$ hat folgende Eigenschaften:

(1) $A, B \trianglelefteq AB$; $A^{\cdot\cdot G} \cdot B^{\cdot\cdot G} = G$, alle $A^{x \cdot\cdot G} \cdot B^{y \cdot\cdot G}$ konj in G

(2) $A \cap B^{\cdot\cdot G} \& A^{\cdot\cdot G} \cap B \lhd\lhd G$

(3) $A^{\cdot\cdot G} \cap B^{\cdot\cdot G} / A^{\cdot\cdot G} \cap B^{\cdot\cdot G} \cap AB = p$ Primzahl

(4) $M \cap B \lhd\lhd G$ wenn $A \leq M \lhd G$.

(5) $N_{\min} \lhd G \Rightarrow |N : N \cap AB| = p$, $|N| = p^\nu$.
Bew mit

(6) $d_G C = 2$, $C \leq D < G \Rightarrow D \cdot C^G < G$
insb. anwenden auf 1-köpf. perfektes C; $D = A$ od B.

(7) $AB \leq H < G \Rightarrow A \lhd\lhd H$ oder $B \lhd\lhd H$
Bew: sonst $A^{\cdot\cdot H} > A$ $B^{\cdot\cdot H} > B$.

$$\text{Ind: } \begin{cases} (A)^{\cdot\cdot G} \cap B^{\cdot\cdot G} \leq A^{\cdot\cdot H} B \\ A^{\cdot\cdot G} \cap (B)^{\cdot\cdot G} \leq AB^{\cdot\cdot H} \\ A^{\cdot\cdot H} \cap B^{\cdot\cdot H} \leq AB \Rightarrow A^{\cdot\cdot H} B \cap AB^{\cdot\cdot H} \leq AB \end{cases}$$

das gibt

$$A^{\cdot\cdot G} \cap B^{\cdot\cdot G} \leq AB$$

250/251

noch $\lhd\lhd$

8. $A^x \leq A^{\cdot\cdot G}$, $B^y \leq B^{\cdot\cdot G} \Rightarrow A^x \leq \mathcal{N} B^y$, $B^y \leq \mathcal{N} A^x$

Satz: 9 $AB \neq G$, A^x v B^y $\forall x, y \Rightarrow A^G B < G$ oder $AB^G < G$.

Folge: 10

$$A^x \text{ v } B^y \Rightarrow \begin{cases} A^{AB} \cap B^{AB} \trianglelefteq\trianglelefteq G & \text{da } \lhd\lhd A^G B \ \ \& \ \ \leq A^G \lhd G \\ A^{B^G} \cap B^{A^G} \trianglelefteq\trianglelefteq G & \text{da } B^{A^G} \leq \mathcal{N} A^{B^G} \end{cases}$$

trivial auch $A^{B^G} \cap B^G \lhd\lhd G$ [Zusatz: $A^{AB} = A^B$, $B^{AB} = B^A$]

Satz 11: $AB \neq G$,

genauer 12

$$A^x \text{ v } B^y \ \forall xy \Rightarrow \begin{cases} A \cdot B^{A^G} \neq G \ \ \& \\ BA^{B^G} \neq G \end{cases}$$

Note: $11 \Rightarrow 9$
Bew: Wähle $\overline{B}$ max.

$$\overline{B} = \langle B, B^{x_1}, \cdots \rangle \ , A\overline{B} \neq G.$$

Dann $A \leq \mathcal{N}\,\overline{B}$, aber auch $A \leq \mathcal{N}\,\overline{B}^t$, $\forall t \in G$: sonst

$$\exists a \in A : B^* := \langle \overline{B}^t, \overline{B}^{ta} \rangle > \overline{B}^t$$

$$AB^* = A\overline{B}^t \neq G$$

nun $A \cdot B^{*t^{-1}} \neq G$, $\overline{B} < B^{*t^{-1}}$.
Also $A^x \leq \mathcal{N}\,\overline{B}$ $\quad A^G \leq \mathcal{N}\,\overline{B}$

$$A \cdot B^{A^G} \leq A\overline{B}^{A^G} = A\overline{B} \neq G.$$

???, nochmals auf A angewandt (oder gleich $\overline{A}$, $\overline{B}$ maximal) bei festgehaltenem $\overline{B}$:

Satz 12.

$$\boxed{A^x \text{ v } B^y \ \ \forall x, y \in G, \quad AB \neq G \Rightarrow A^{B^G} \cdot B^{A^G} \neq G,\ A^{B^G} \cap B^{A^G} \trianglelefteq\trianglelefteq G} (\leftarrow 10)$$

Frage: $A^{\cdot\cdot G} \cap B^{\cdot\cdot G} \leq A^{B^G} \cap B^{A^G}$?
Vermutlich genügt $x \in A^{B^{\cdot\cdot G}}$, $y \in B^{A^{\cdot\cdot G}} \Rightarrow A^y$ v B^x

251/252

9′: A^x v B^y, $AB \neq G \Rightarrow$ entweder $A^G B^{A^G} \neq G$ oder $B^G A^{B^G} \neq G$

Satz 13: a) Ist $N' < N_{\min} \trianglelefteq G$, $A < G$, $A \cap N \neq 1$, so ist $AN < G$

allg: b) Ist $N_{\min} \trianglelefteq G$, $A < G$, $A \cap N \geq$ subnorm Ugr $\neq 1$ von N, so ist $AN < G$.

Frage 14: a) Was folgt aus $A^x \leq \mathcal{N}B \forall x \in G$?

b) Was folgt aus $A^x \leq \mathcal{N}B$ & $B \leq \mathcal{N}A^x$ $\ \forall x \in G$?

15. Def: für $A, B \leq G$ setze $A^{\cdot\cdot B} = A^{\cdot\cdot\langle A,B \rangle}$. Dann gilt $A^{\cdot\cdot B}$ ist monoton $\nearrow$ in A, B.

$$\langle A_1, A_2 \rangle^{\cdot\cdot B} \geqq \langle A_1^{\cdot\cdot B}, A_2^{\cdot\cdot B} \rangle$$

16. Frage: A^x v $B^y \Rightarrow A^{\cdot\cdot G} \cap B^{\cdot\cdot G} \cap AB \lhd\lhd G$?

16. Satz: (Enthält Kegel und meine) (wegen $A^{B^{A^{\cdot^{\cdot^{\cdot^{G}}}}}} \leq AB$)

$$A^x \text{ v } B^y \Rightarrow \begin{cases} A^{B^{A^{\cdot^{\cdot^{\cdot^{B^G}}}}}} = A^B \text{ wenn l.S. genügend lang} \\ A^B \cap B^A \lhd\lhd G \end{cases}$$

Bew: Wenn $AB = G$, so l.S. $\leqq A^{\langle AB \rangle} = A^B$, und $\geq A^{B^A}$
Wenn $AB < G$, so etwa $A^G B =: H < G$ $\quad$ (11)

$$(\text{l.S.})_H = A^{B \cdots B^H} \leq A^{B \cdots B^G}, \quad \geq A^{B \cdots B^{A^G}} = (\text{l.S.})_G$$

Ind: $(\text{l.S.})_H = A^B$
NB: Klar: $A^{B^{\cdot^{\cdot^{G}}}} \cap B^{A^{\cdot^{\cdot^{G}}}} \geq D^{A^{\cdot^{\cdot^{G}}}}$, $D = A \cap B$, also $D^{\cdot\cdot G} \leq A^D$, $D^{\cdot\cdot G} = D^{\cdot\cdot B}$
FRAGE: (ja) Ist für beliebige A, B in G stets $A^{B^{\cdot\cdot G}} \cap B^{A^{\cdot\cdot G}} \lhd\lhd G$?

252/253
29.11.65

Vertauschbarkeit & Subnormalität $\lhd\lhd$

(1)

$$(A,B,G) := \quad \left.\lim A^{B^{A^{\cdot^{\cdot^{\cdot^{B^G}}}}}}\right\} n \to \infty \quad = \cdots \ (n = N)$$

$\leftarrow$(e.g. oder A

Diese Folge fällt monoton

(G endlich; klappt auch in G mit Minbedgg)

(2) $(A,B,G) = (A^{\langle A,B\rangle}, B, G)$

3a,b p. 254 (3) $\overline{A} = (ABG)$, $\overline{B} = (BAG)$ sind die umfassenden Untergruppen von G mit $\overline{A} = A^{\overline{B}}$, $\overline{B} = B^{\overline{A}}$
Frage: auch für „$\leq$“?

Vor: Weiter sei nach (2) stets $A \leq \mathcal{N}B \& B \leq \mathcal{N}A$

(4) $(A,B,G) = (A,B,H)$ für

$$\begin{aligned} H_1 &= AB^G \\ H_2 &= BA^G \\ H_3 &= AB(A^G \cap B^G) \\ H_4 &= AB(A^{\cdot\cdot G} \cap B^{\cdot\cdot G}) \end{aligned}$$

(5) $(A,B,G) \cap (BAG) \trianglelefteq\trianglelefteq G$
Pf Indukt. (4) mit H_3, nebst

(6) Wenn $G = AB^G \cap BA^G$, so $(A,B,G) = A^G$
Bew: $A^{B^G} = A^{AB^G} = A^G$, $B^{A^G} = B^G$

Kegel:

(7) Wenn A^x v B^y und $AB < G$, so $G^* := AB(A^G \cap B^G) < G$

(8) $(A,B,G)^\varphi = (A^\varphi B^\varphi G^\varphi)$, wenn $\varphi \in \hom G$
obwohl Durchschnittsbildg „eingeht“; eliminiere dies. $(n = N)$

253/254

(3a) (A,B,G) ist isoton in allen Variablen

(3b) $(AAG) = A^{\cdot\cdot G}$

? 9 Wenn bei festem A, B ($\leq \mathcal{N}_A^B$, wohl entbehrlich) gesetzt wird $G^* := AB^G \cap BA^G$ und $H = G^{**\cdots\cdots *}$ das Endglied der absteigenden Kette, so ist mit $\overline{A} = (ABG)$ und $\overline{B} = (BAG)$

$$\begin{cases} \overline{A} = A^H, \quad \overline{B} = B^H \\ H = A\overline{B} = B\overline{A} \quad (AB = H = AB^H = BA^H) \end{cases}$$

Bew: $H = AB^H = BA^H$ als Endglied?

$$\overline{A} = A^{B^{A^{\cdot^{\cdot^{\cdot B^H}}}}} = A^{A\cdot B^{A\cdot B^{\cdot^{\cdot^{\cdot AB^H}}}}} = \cdots = A^H$$

ebenso $\overline{B} = B^H$
Also $\left.\begin{smallmatrix} A \\ B \end{smallmatrix}\right\} \leq H = AB^H = A\overline{B}$; ebenso $= B\overline{A}$ auch wenn $\begin{smallmatrix} A \\ B \end{smallmatrix} \not\leq \mathcal{N}_A^B$.

(9′)

$$\begin{cases} A \leq \mathcal{N}(BAG) \quad B \leq \mathcal{N}(ABG) \\ \quad A \cdot (BAG) \quad = \quad B \cdot (ABG) = G^{*\cdots *} \\ \qquad\qquad\qquad = \qquad (ABG)(BAG) \end{cases}$$

(10) $A^B = A \Rightarrow \underbrace{A \cap (BAG)}_{=D^{[G]}} \lhd\lhd G$

Bew: $D^{[G]} = D^{[AB^G \text{ oder } BA^G]} \lhd\lhd [\quad]$ (Indukt. anw.) und $\leq A^G \cap B^G \lhd G$.
Wenn $[\quad] = G_{1>0}$ $D^{[G]} = A \cap B^G$.
Es genügt $A \cap B^A \lhd\lhd B^A$ denn $AB = G \Rightarrow (BAG) = B^A$ Forts. XIV, 10

[Keine neue Seitennummer!] 254/254

$$|H| = \frac{|A|\,|\overline{B}|}{|A \cap \overline{B}|} = \frac{|\overline{A}|\,|\overline{B}|}{|\overline{A} \cap \overline{B}|}$$

Also

(11)

$$\begin{cases} |\overline{A} \cap \overline{B}| = |A \cap \overline{B}| \cdot |\overline{A} : A| = \frac{|\overline{A}|}{|A : A \cap \overline{B}|} \quad [\text{ auch ohne } \begin{smallmatrix} A \\ B \end{smallmatrix} \leq \mathcal{N}_A^B] \\ \overline{A} \cap \overline{B} \lhd\lhd G \end{cases}$$

(12) Wenn A^x v B^y, so $G^{*\cdots *} = AB$ (Kegel)

(13) Vermutung: Wenn $A, B \leq G$ sind und $A \trianglelefteq\trianglelefteq B^x$ gilt für mehr als $\frac{1}{2}|G|$ Elemente $x \in \mathfrak{G}$, so ist $A \lhd\lhd G$.
Ist richtig, wenn $A = A'$. Denn zu $A, A^x \exists$ mindestens 1 $y \in G \rightarrow A, A^x \trianglelefteq\trianglelefteq B^y$. also A v A^x, $A \lhd\lhd G$.
Stets ist wenigsten der perfekte Kern

$$A^* \lhd\lhd G.$$

[Keine Seitennummer eingetragen!] 254/[255]

Ist A nilpotent, $= P \times Q \times \cdots$, so ist $[P^x, Q^y] = 1$, also $(P^G, Q^G] = 1$, also P^G
Wenn $H < G$, so ist die Vor. für eine passende Konjugierte von $\overline{G}$ (statt G) erfüllt.
oBdA: Der "Subnormalisator" $\mathcal{S}A$ $(\subseteq G)$ enthält also zu jeder maximalen Untergr. M von G eine Konjugierte.

[255]/256

Unabhängige Untergruppen
besser: „$\{G : G_i\}$ unabh"

1 Def $\{G_i\}_{i=1\cdots n}$ unabh. in $G \iff \forall x_1, \cdots x_n \exists g \in \bigcap G_i x_i$.
Vielleicht bequemer: $\forall x_1 \cdots x_n \in G \exists g \in G$, $g_i \in G_i \rightarrow g g_i = x_i$
Achtung: Baer Nor Sol gps **???** nennt $\{G_\lambda\}$ indep $\iff \langle G_\lambda \rangle = \prod_{\otimes} G_\lambda$

2 eq: ... $\bigcap x_i G_i \neq \emptyset$ siehe schärfer: 10

$2\frac{1}{2}$ $\{G_i\}_{i \in I}$ un G, $A \subseteq I \Rightarrow \{G_i\}_{i \in A}$ un G.

3 $\{G_i\}$ un G, $G_i \leq H_i \leq G \Rightarrow \{H_i\}$ un G.

$3\frac{1}{2}$ G_1, G_2 un $G \iff G_1 G_2 = G$ Bew: $\bigcap H_i x_i \supseteq \bigcap G_i x_i \neq \emptyset$

Satz 4 Sei $\{G_i\}$ un G und $H \leq G$. Dann

$$\{G_i \cap H\} \text{ un } H \iff H \cap G_i = \bigcap H G_i$$

hatte Breuninger 16.10.65 für $n = 2$, $H \lhd G$, $\bigcap G_i \leq H$.
Bew: $\Rightarrow$ „$g \in \bigcap H G_i \Rightarrow g \in H \cap G_i$"
Bew: $g \in H g_i$ $\exists g_i \in G_i$ $y_i := g g_i^{-1} \in H$
$\exists h = h_i y_i = g g_i^{-1} y_i$; $h_i \in H \cap G_i \subseteq G_i$
$g = h y_i^{-1} g_i = hd$, $\quad d = y_i^{-1} g_i \in G_i$, $\quad d \in \bigcap G_i$, $\quad g \in H \cap G_i$

$\Leftarrow$ Sei $y_i \in H$ $\exists g = g_i y_i$, $g_i \in G$.
$g^{-1} = y_i^{-1} g_i^{-1} \in H G_i$, $\quad \forall i$
$= h^{-1} d$, $\quad d \in \bigcap G_i$, $h \in H$
$H \ni h = dg = d g_i y_i = h_i y_i$, $h_i \in H \cap G_i$

5 (Breuninger) $\{G_i\}$ un G, $N_i := \mathcal{N}G_i$, $K := \bigcap G_i$ $N := \bigcap N_i$, $\Rightarrow$
$N/K = \prod\limits_{\text{dir}} S_i/K$; $S_i = N \cap \bigcap\limits_{j \neq i} G_i = N/N \cap G_i$
$\approx \prod NG_i/G_i$
Bew: 4: $\{G_i \cap N\} \underset{\lhd}{\text{un}}\ N$

256/257

6 Ist G kompakt, so ist $\{G_i\}_{i \in I}$ un $G \iff$ jedes endl Teilsystem ist un G. (Alles obige gilt für beliebige Indexmengen!)

7 Für $A, B \subseteq I$ (= Indexmenge) definiere $G_A := \bigcap\limits_{i \in A} G_i$ usw.

Dann

$$\begin{aligned} G_{A \cup B} &= G_A \cap G_B \\ G_{A \cap B} &= G_A \cdot G_B \end{aligned}$$

auch für unendliche Überdeckungen von I usw aufschreiben!

Lemma (8) Zum Beweis der zweiten Formel:
Lemma:
(A fest) Das System $\{G_i \cap G_A\}_{i \in I}$ un G_A denn

$$x_i \in G_A \Rightarrow \exists g = g_i x_i;\ g_i \in G_i$$

für $i \in A$ ist $g = g_i x_i \in G_i \quad g \in G_A$
Bew 7_2: Nach 4 ist

$$\begin{aligned} G_A G_B &= \bigcap_{b \in B} G_A G_b \\ &= \bigcap_{b \in B} \bigcap_{a \in A} G_a G_b \overset{3\frac{1}{2}}{=} \bigcap_{a=b}\!\bigcap = \bigcap_{c \in A \cap B} G_c \end{aligned}$$

9 $\{G_i\}$ un $G \Rightarrow G$ wirkt simultan-transitiv auf

a) alle $G/G_i : \exists g \in G \to G_i g = G_i x_i$ für gegebene x_i
b) G wirkt simultan-transitiv auf den Klassen zu G_i konjugierter Gruppen
Bew: geg $x_i \in G_i \exists g \in G_i x_i; G_i^g = G_i^{x_i}$

257/258

unabhängige Untergruppen

10. $\{G_i\}$ un G; $x_i, y_i \in G \Rightarrow \bigcap x_i G_i y_i \neq \emptyset$
Bew: $\exists t \in G$, $t \in \bigcap x_i G$, $x_i G = tG$, $\bigcap x_i G_i y_i = \bigcap t G_i y_i = t \bigcap G_i y_i \neq \emptyset$

$\lhd\lhd$ 12.12.65

Lemma (1) $N \lhd G$, G/N perfekt: $A, B \leq G$,
$G = AN = BN \Rightarrow G = \underbrace{[A, B]}_{\substack{\text{Kommu-}\\ \text{tator}}} N$

(2) $N \lhd G$, G/N perfekt, $A, B \leq G$, $A, B \trianglelefteq \langle A, B\rangle$, $G = AN = BN$
$\Rightarrow G = (A \cap B)N$

(3) $N \lhd G$, $A \lhd\lhd G$, A minimal mit $AN = G$, G/N perfekt $\Rightarrow A \trianglelefteq G$

Satz (4) $A, B \trianglelefteq\trianglelefteq G$, G/B^G perfekt (Äq: $G = \langle A', B^G\rangle$ od wenn $|G| < \infty$ $G = \langle A', B\rangle$), $d_G A \leq 2$, $G = \langle A, B\rangle \Rightarrow G = AB = BA$
Frage: auch für $d_G A > 2$?
Beweis: Sei $A \ntrianglelefteq G$. Ind $d_G B = d$. $d \leq 1$ trivial.
$d \geq 2$

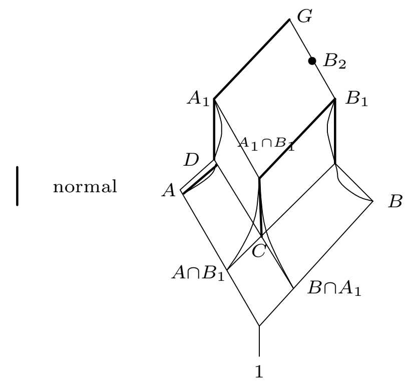


Bild 1

Nach Ind ist $(B \to B_1)$ $\underline{G = AB_1}$. Ferner $\underline{G = A_1 B}$, da $G = (A_1 B)^G$ und $A, B \lhd\lhd G$.
Das gibt Bild 1.
Fall I: aus $N \lhd G$, $N \subseteq AB$ folgt $N = 1$
$C \leq D$, $\forall b_1 \in B_1$ ist $C = C^{b_1} \leq D^{b_1}$ $\forall g \in G \exists b_1 \in B \cdot\ni\cdot D^g = D^{b_1}$
$C = D^g$ $\forall g \in G$
$C^g \leq D$, $C^G \leq D \leq AB$, $C^G = 1$, $C = 1$

Daher $A \cap B_1 = 1$, $G = AB_1$
Da $A \ntrianglelefteq G$ angenommen (sonst Beh trivial), $\exists$ $A^g \cdot\ni\cdot$ $A \cap A^g < A$.
Da $A, A^g \trianglelefteq A_1$, ist nach 2 auch

$$(A \cap A^g)B^G = G$$

Daher nach Ind: $G = (A \cap A^g) \cdot B_1$. Also

$$\begin{aligned} A &\le (A \cap A^g) \cdot B_1 \\ A &= (A \cap A^g) \cdot (A \cap B_1) \\ &= A \cap A^g \text{ wegen } A \cap B_1 = 1 \end{aligned}$$

Wid.
Fall II: $\exists N \lhd G$, $N \le AB$. Benutze

(5) Lemma: $A_1 B \le G$; $N_\lambda \trianglelefteq G$, $N_\lambda \subseteq AB$
$(\forall \lambda \in \Lambda) \Rightarrow$

$$\left[\prod_{\lambda \in \Lambda} N_\lambda\right] \subseteq AB = AB \cdot \prod N_\lambda$$

Bew: $|\Lambda| = 2$: $n_\lambda \in N_\lambda$

$$\begin{aligned} n_1 &= a_1 b_1 \\ n_1 n_2 &= a_1 b_1 n_2 \\ &= a_1 n_2' b_1 \\ &= a_1 (a_2' b_2') b_1 \in AB \end{aligned}$$

$|\Lambda| < \infty$ Indukt
$|\Lambda| = \infty$: $x \in \prod N_\lambda \Rightarrow x \in \overset{\text{fin}}{\prod}{}' N_\lambda$.

Damit Bew Fall II:
Wähle $N := \prod N_\lambda$, $N_\lambda \trianglelefteq G$, $N_\lambda \subseteq AB$

260/261

Dann gilt für $(x \to \overline{x})$ = nat hom $G \to \overline{G} = G/N$:
$\overline{G} = \langle \overline{A}, \overline{B} \rangle$; $\overline{M} \le \overline{A}\,\overline{B}$, $\overline{M} \trianglelefteq \overline{G} \Rightarrow \overline{M} = 1$; $\overline{G}/\overline{B}^{\overline{G}}$ perfekt. $d_{\overline{G}}(\overline{A}) \le 2$, $d_{\overline{G}}\overline{B} \le d$.
Also nach Teil I: $\overline{G} = \overline{A}\,\overline{B}$.
Das heißt $G = ANB = AB$

Satz (6): $A \lhd\lhd G$, $B \lhd\lhd G$, $G = \langle A, B \rangle$, $A \subseteq A'B \Rightarrow G = AB$
Äq: $A/(A \cap B)^A$ perfekt
Bew: Indukt $d = d_G A$, bei festem d nach $d_G B$.
$d = 1$ triv $\quad d_G B \le 1$ trivial
Fall $d = 2$ folgt aus (4): Für $N := B^G$ ist

$$G'N \ge A'N = \langle A, B \rangle = \langle A, B \rangle = G$$

also G/N perfekt.

Fr.: reicht $A/A'(A \cap B) \perp B/B'(A \cap B)$?

Fall $d > 2$: nach Induktion ist $G = AB_1 = A_1B$ ferner für $G^* := \langle A, H\rangle$:
$\underline{G^* = AH} = AKH = DH$ denn

$$\begin{aligned} A &= A'(A \cap B) \\ &= A'(A \cap H) \subseteq A'M \end{aligned}$$

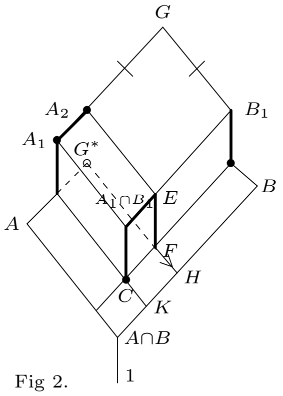


Fig 2.

$\mathcal{N}G^* \geq A_1 \cap B_1\ D, A_1; A_1 \cap B_1, F, E; A_1, E, A_2.$
Also $G^* \trianglelefteq A_2$, $d_G G^* \leq d_G A = 1$
Indukt: $G = G^*B = AH'B = AB$ denn $G^{*'}B \supseteq A'B \geq A$,
also $G^{*'}B \geq AB \supseteq AH = G^*$.

261/262

$\lhd\lhd$

(7) Vermutung (7):

$$A, B \lhd\lhd G, \qquad A/(A \cap B)A' \otimes B/(A \cap B)B' = 0$$
$$\Rightarrow AB = BA$$

NB Kriterien für $A \otimes B = 0$ siehe Fuchs, Buch Chap XI

(8) Frage: Gibt es Vertauschungssätze der Art:
Ist $A, B \lhd\lhd G$, so ist $[A, \cdots, A]_k$ v B wenn $k \geq f(d_G A)$?

262/263

Perm Gr mit regulärer Untergruppe

Satz: Sei $\mathfrak{G}$ tra $\mathfrak{H}$, $\mathfrak{H} \leq \mathfrak{G}$, $\mathfrak{H}$ additiv geschrieben, Sei $\mathfrak{U} \leq \mathfrak{G}$
Sei f_0 eine bei $\mathfrak{G}_0$ invariante Fktion

$$f_0 : \mathfrak{H} \to R (= \text{ Ring})$$

Sei $\mathfrak{F}$ eine bei $\mathfrak{U}$ inv. Menge von Fkt $f : \mathfrak{H} \to R$. Dann ist $f_0 \wedge \mathfrak{F}$ $(:= \{f_0 \wedge f | f \in \mathfrak{F}\})$ inv bei $\mathfrak{U}$.
Bew: Sei $\varphi \in f_0 \wedge \mathfrak{F}$, $u \in U$

$$\begin{aligned}
\varphi(x) &= \sum_\xi f_0(x-\xi) f(\xi) \\
\varphi(u(x)) &= \sum_\xi f_0(u(x)-\xi) f(\xi) \\
&= \sum_\xi f_0(u(x)-u(\xi)) f(u(\xi)) \\
&= \sum_\xi f_0((t_{\mathfrak{U}(\xi)} u)(x)) f(u(\xi))
\end{aligned}$$

$t_\rho(x) := x - \rho, \quad t_\rho \in \mathfrak{G}$
Nun ist aber

$$(t_{\mathfrak{U}(\xi)} u)(x) = (h_\xi t_\xi) x \text{ mit } h_\xi \in \mathfrak{G}_0$$

denn

$$0 = (t_{\mathfrak{U}(\xi)} u)(\xi) = (h_\xi t_\xi)(\xi) = h_\xi(t_\xi(\xi)) = h_\xi(0)$$

Also

$$\begin{aligned}
\varphi(u(x)) &= \sum f_0(h_\xi(x-\xi)) f(u(\xi)) \\
&= \sum f_0(x-\xi) f(u(\xi)) \\
&= \sum f_0(x-\xi) \overline{f}(\xi), \quad \overline{f} \in \mathfrak{F} \\
&\in f_0 \wedge \mathfrak{F}
\end{aligned}$$

Kürzerer Beweis: 199 (1)

263/264

3.1.66

Perm Gr von Grad p

(1) Ist m der kleinste unter den Graden der bei G invarianten Funktionenmoduln (Gr $\mathfrak{m} = \max$ Gr f, $f \in \mathfrak{m}$),
so sind alle Grade $0, m, 2m, \cdots, p-2, p-1$
es ist $m \big| p-2$
Bew: Grad $\mathfrak{m}^\perp = p - 2$- Grad $\mathfrak{m}$, wenn $\mathfrak{m} \neq 0$

(2) Ist i der kleinste unter den Graden der Invarianten von G_0, so sind

$$0, i, 2i, \cdots, p-1$$

alle Grade von Invarianten
Bew: Faltung

(3) Die aus einer Invariante Grad i hervorgehende Modul **???** hat Grad i.

(4) Ist G nicht 2-tra, so ist $i < p-1$, also $m|i|p-1$, $m|p-1$ aber auch $m|p-1$ also $m=1$; dh g linear, $\forall g \in G$

Variante:

(3′) Grad $f = i$, f inv $G_0 \Rightarrow$ deg $f \wedge \overset{\substack{\text{alle}\\ \text{fkt}}}{\mathfrak{M}} = i$
deg $f \wedge \mathfrak{M}_0 = i-1$

(4′) $\exists\ f$ mit $1 \leq i \leq p-2$, so existieren G-Moduln mit Grad $i, i-1$, also nach 2 ist $m\big|i-(i-1)$, $m=1$
Besser bei dieser Variante die Dimensionen der G-Moduln anschn.

(5) Faltung mit Invar. von G_0 ist G_1 Modul-Endomorphismus und umgekehrt. (centralizer ring)

264/265

6. Die Anzahl der Bahnen von G_0 ist die Anzahl der einköpf $\times$ 1-köpf G-Moduln.
Bew. Ordne Invar lexikographisch

7. Sind $\mathfrak{a}, \mathfrak{b}$ P-moduln (d.h. Faltideale in $\mathfrak{M}$) mit $\mathfrak{a} \wedge \mathfrak{b} \neq 0$, so ist jedes $x_i \in \mathfrak{a} + \mathfrak{b}$.
Bew. $\exists\ a \wedge \mathfrak{b} \neq 0$; also $\exists\ a \wedge b = 1$.

$$x_i = x_i(a \wedge b) = (x_i a) \wedge b + a \wedge (x_i b) \leq \mathfrak{a} + \mathfrak{b}$$

8. Ist G primitiv, so gibt es keine unter G invarianten Funktionenring außer $\mathfrak{c}$ und $\mathfrak{M}$.
Bew. Weierstraß-Stone
NB: Es gibt keine gemeinsame Nullstelle von $\mathfrak{m}$ (= G-Modul$\neq 0$)

9. Ist G pri, und sind $\mathfrak{a}, \mathfrak{b}$ P-moduln mit $\mathfrak{b} = \mathfrak{a}^{\perp}$, so ist $\mathfrak{a}\mathfrak{b} = \mathfrak{M}_0$.
Bew: sonst $\exists\, \mathfrak{m} \neq \mathfrak{c}$ mit $\mathfrak{m} \perp \mathfrak{a}\mathfrak{b}$, d.h. $\mathfrak{m}\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{M}_0$. Dann $\mathfrak{m}\mathfrak{b} \subseteq \mathfrak{a}^{\perp} = \mathfrak{b}$, der von $\mathfrak{m}$ erzeugte Ring $\hat{\mathfrak{m}}$ $\quad \hat{\mathfrak{m}}\mathfrak{b} \subseteq \mathfrak{b}$ also $\hat{m} = \mathfrak{M}$ nach 8: also $\mathfrak{M}\mathfrak{b} \subseteq \mathfrak{b}$; da $\mathfrak{b}$ keine feste Nullstelle hat, gibts zu $\xi \in \Omega\ b$, $b(\xi) \neq 0$ und $\mathfrak{b} \ni \delta_{\xi x} b$, also $\mathfrak{b} = \mathfrak{M}$.

[Zusatz zu (5) auf Seite 264:]
$\leftarrow$ insbesondere mit rank $G = 3$ = Anzahl der 1. Moduln in einer Komp[ositions]reihe von $\mathfrak{M}$.

265/266

1. Taam C.T.:	Compact linear transformations PAMS 11, 39-42 (mögliche andere Def von vollstetig)
2. Menon P.K.:	Difference sets in abelian groups PAMS 11, 368-376
3. Ostrowski, A.M.:	On some Conditions for non-vanishing of determinants. PAMS 12, 268-273
4. L. Solomon:	On the sum of the elements in the character table of a finite group. PAMS 12, 962-3
5. Le Varasseur, R:	Les groupes d'ordre fini ... Ann Univ Lyon (I) 15 1904 Paris, Ganthier-Villars

gibt Tabellen von Gruppen der Ordnung p^5.

266/Einband

Frame-Verallgemeinerung 131-143
(Rinderspacher gezeigt 3-75)
Verallgem. von D.G. Higman Tagungsbericht OW 22/1977
Dazu B. Weisfeiler, ebenda
ein Satz von Frame und Verschärfung:

$$\sum_{x \in H \leq G} \chi(x) \leq \sum_{y \in Hg} \chi(y)$$

Siehe Sonderdruck FRAME: Double ...
BAMS 49,81-92