Aufgabe

Satz I kann vielleicht auf Hallgruppen $\mathfrak{G}$ mit regulärer elementar abelscher Untergruppe erweitert werden. Wesentlich ist $g(x) \in \mathfrak{g} \to -g(-x) \in \mathfrak{g}$.

Siehe auch Satz II, 232

Bemerkung: Die Funktionen $f(x) = \alpha x + \beta x^p$ sind die sämtlichen additiven (d.h. Endomorphismen von K^+): $f(x+y) = f(x) + f(y)$

Der Schiefgrad $\mathfrak{G}$ ist die kleinste Zahl k mit $\varphi(x) = \sum f_\nu f_\nu - f_\kappa \quad \kappa \leq k$, f_i additiv

---

Satz: Ist $\mathfrak{G}$ 2-elementar-abelsch mit einer regulären Untergruppe $\mathfrak{g}$, dargestellt auf $\mathfrak{g}$, so gilt:

$$g(x) \in \mathfrak{g} \to -g(-x) \in \mathfrak{g}$$

Bew: Ist $f(x)$ inv. bez. $\mathfrak{g}_0$, so auch $f(-x)$;

daher $f(-g(x)) = f(-x)$

$f(-g(-x)) = f(x)$, $\quad -g(-x) \in \mathfrak{g}$

Fortsetzung Beweis Satz I: Es enthält keine k_ν vom Schiefgrad > 2, sonst konstanten Schiefgrad 2 für ganzes K, wid. zu A.

$\subset$ Schiefgrad $g = 1$, $k_\nu \in \mathfrak{g}_0$ beliebig $m \in \mathfrak{M}$; $\subset m =$ $\alpha x + \beta x^p$.

$m(x) \in \mathfrak{M}$, also $m(y) = \gamma x + \delta x^{p^r}$

$m(g(x+y)) = m(g(x)) + m(g(y))$

$g(x+y) - g(x) - g(y) = 0$

215
22.9.64

Satz I: Ist G eine [illegible] zur einfach transitiven Gruppe der Grades p^ν mit reg. el. ab. Ugr H, die nicht in G normal ist, so hat G entweder eine Invariante $f(x^{p^{\nu-1}}) \neq \text{const}$ ($x^{p^{\nu-1}}$?)

oder die "homogenen" Invarianten f_i von p-Index liegen für $i \geq \frac{p^\nu}{2}$ oberhalb der Diagonalen haben die Faltungstafel auf p.109 mit $c_{ij\nu} = 0$, d.h. $f_i \cdot f_j = 0$ für $n < i+j < \frac{3p^\nu}{2}$

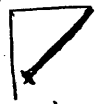
Beweis: Ord A sei G 2-abgeschl.

Wäre einer der $f_{\frac{p^\nu}{2}}, \dots, f_{p^\nu-1}$ ganz oberhalb der Diagonalen, so ganz im 1. Quadrant Q_1, also hätte $f_i(g)$ nur Exponenten oberhalb f_i, also in Q_1 [illegible] falls $x = f \cdot h$ Lösung h hat. [illegible] Nach Satz I, 210, [illegible] also das mehr als $x = f \cdot h$ unlösbar; [illegible] Nun

Hilfssatz: Ist f (homogen und) ≥ 1 und $f \cdot h = x$ unlösbar, dann ist $f = (\alpha x + x^p)^n$ mit passendem α und $\alpha^{p+1} = 1$

Beweis: Die zwei Faltungen $f \cdot h$, die homogen vom Grad 1 sind, sind also abhängig:

ehen = const $(\alpha x + \beta x^p)$. Nach Vorst.
$\beta \neq 0$, OBdA $\beta = 1$.

$f_0 = (\alpha x + x^p)^n$ ist eine Fktion dieser Eigenschaft.
gäbe es aber davon ein f " " ,
so könnte man c finden, so daß
$g = f - c f_0$ die Potenz x^{pn} nicht
enthält: $g =$  Dann $\exists h : g \wedge h = x$
im Widerspruch zu. $g \wedge h = \text{const}(\alpha x + x^p)$.

Schluß des Beweises $\overline{\text{II}}$:
Wäre ein f_i ganz oberhalb der Diag, $i \leq \frac{n-1}{2}$,
also f_i in Q_1, so wäre $f_i \wedge h$ invertierbar,
also $f_i = c \cdot (x^p + dx)^{ie}$.
Da $f_i = f_i^p = c^r(x + d^r x^p)^{ie}$,
wäre $+ c\, d = c^p$, $d = c^{p-1}$.
$f_i = c\, x^{ie} \cdot (x^{p-1} + c^{p-1})^{ie}$
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 $x \neq 0$. Widsp.

---

1 ~ p. 224
d.h. $i \leq \frac{3n}{2}$
3d
n
$x^{p+1} = 1$
mög
y

217 Noch Perugr mit reg Ngr. hy

Normierung von σ durch Änderung der Einheit von x

$\mathfrak{M}$ σ ein Automorphismus von $\mathfrak{g}$, $\mathfrak{w}$ ist

a) σ vertauschbar mit Faltung mod mit $g^\sigma = \sigma^{-1} g \sigma$:

b) $f \in \mathfrak{f}_0 \to f(x^\sigma) \in \mathfrak{f}_0^{(\sigma)}$

c) ferner $\mathfrak{M}$ (Einsform 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) in $x^p - x$ normieren durch Übergang von g zu g^σ.

Partielle Summation:

$$x \cdot [f \wedge g] = (xf) \wedge g + f \wedge xg$$

$$x^2 \cdot [f \wedge g] = (x^2 f) \wedge g + 2xf \wedge xg + f \wedge x^2 g$$

$$x^{p+1} [f \wedge g] = (x^{p+1} f) \wedge g + {}^{+}f_1 x^p g + x^p f \wedge xg$$

$$x^p [f \wedge g] = x^p f \wedge g + f \wedge x^p g \quad + {}^{*}f \wedge x^{p+1} g$$

Es gibt in K_p zwei Ableitungen:

$$f' = f(x+t)\big|_t \,, \quad f^{\chi} = f(x+t)_{t^p}$$

Rechenregeln aufstellen!

Hilbe 221(1)

Partielle Summation funktioniert auch

additiven Funktionen $l(x)$:

$$l(x+y) = l(x) + l(y)$$

also für $l(n) = \alpha x + \Lambda x^p$:

$$l[f \cdot g] = (lf)\cdot g + f \cdot lg$$

Bew:
$$= \sum l(x) f(x-t)\, g(t)$$
$$= \sum [l(x) - l(t)]\, f(x-t) g(t) + \sum l(t) f(x-t) g(t)$$

für g modulbeschränkt

Ist l additiv, so gilt

$$l^{\nu} \cdot l^{\kappa} = [x^{\nu} \cdot x^{\kappa}] \circ l \quad \text{wenn} \quad \begin{cases} n \in K, \\ l(n) \neq 0 \\ \Rightarrow n = 0 \end{cases}$$

und $f(l) \cdot \varphi(l) = 0 \quad \forall f, \varphi$ wenn

l ausgeartet: $\exists\, n_0 \neq 0$: $l(n_0) = 0$

dann dann tritt jeder Wert von l p-mal auf

219. $n=3$ Hier hat das f (vom Typ $2e$)
einen 1-Annullator, nämlich
auf der schrägsten Se oder Asymptote.
Denn auf der $(e-1)$ hat es $2e-1$
Nullstellen (alle diese Potenzen mit f
gefüllt, ergeben $e+2$ Linearverbindungen
von e Potenzen auf der Linie $e-1$).
Und wenn zwei Annullatoren
eine Abstands Defektsumme (Defekt =
Abst schrägste von $p^i \cdot 1$ aus gesehen
mit 0 beginnend) $< p-1$ haben,
wohl ihr ggT auch Annullator
(ggT der Formen $\sim x^{p^2}$, mit x^{p-p}).

WB
$k<p$, l additiv $\Rightarrow$ $l \wedge x^{p^{k-1}} = \alpha\, l^{k-1}$

$l^k \wedge x^{p^{k-1}\cdot p} = \beta\, l^{k-1}$

wenn $l = \alpha x + \beta x^p$.

$n=3$: Mit Hilfe
Linear[illegible]faktore
$f =$
Ansatz: Na[illegible] le
oder allg
dann M
dargestell
können
oberhalb
g vgl
dann L

*) an

Bem
Sind
Line
l
Sei u
α f.

Vielleicht
bekannt

Mit Hilfe des Annullators (Zerlegung von a^*) ≥ 2 Linearfaktoren) kann man zerlegen

$$f = \sum_{i=1}^{e} d_i l_i^{2e} \qquad a = \prod l_i$$

Ansatz: Man berechne dann z.B. für $x^{(p^2-1)-(2e-2)}$ oder allgemeiner für x^k als $\sum \beta_i l_i^k$ dann M dann auch jedes $g \in G$ als $\sum \cdot\, l_i^k$ darstellen. Hieraus sollte man sehen können, daß g und g^ν nur dann gerade oberhalb der Kante e liegen, wenn g ~~[illegible]~~ g nur oberhalb der Kante e liegt, d.h. in G_1. Dann Satz 5, S. 210 anwenden.

*) angestellt als Polynom in $x^{p^2-1}, \dots, x^{p^2-p}$

$= \frac{\partial}{\partial x}$ und $\frac{\partial}{\partial \bar{x}}$ $\quad (\bar{x} = x^p)$.

~~[illegible]~~

Sind $l_1, \dots, l_e$ verschiedene Linearformen, so sind für jedes $k \geq e$

$l_1^k, \dots, l_e^k$ linear (von derselben) unabhängig.

Sie müssen wir ebenso für Untersuchung der f_ν und dann der $g \in G$ –

Vielleicht empfiehlt es sich, für „symbolische Potenz" ein neues Wort zu finden!

22/1 **und Gruppen vom Grad p^2**

(1) Die Untersuchung des Rings der $f(z,\bar z)$ mit $z^p - \bar z = \bar z^p - z = 0$ ist wegen $z = x+iy$ gleichwertig mit $g(x,y)$ mit $x^p = x, y^p = y$ - denn

$$K[W]/_{u^p-u} \cong K[z,\bar z]/_{z^p-z,\ \bar z^p-\bar z} \cong K[x,y]/_{x^p-x,\ y^p-y}$$

↖ modulo u

Wenn form $q^2 = a(u^p-u) + b\cdot(\bar u^p - u)$; ohne a, b Komp.
$q^2 = a u^p + b\bar u^p$ wegen Homogenität; Grad $= 2q$

(wäre es wohl einfacher, erst zu

(2) Im Fall $n=3$ [illegible] (sagen: es gibt keine

als Leitform $b \neq g(x,y) \in K[x,y]$ vom Grad $k > \frac{p-1}{2}$)

eines Gruppenelements wobei linear

auftretende mit $q^2 = ax^p + by^p$ ⊕, wo a, b Formen

Siehe 223 des Grads $2k-p$

(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 $\partial b = 0$;

den gibts wegen Grad $b = 1$

dann $2g\cdot\delta g = \delta a \cdot x^p + (\delta b) y^p = \delta a \cdot x^p$

Wenn I. ($a \neq cb$, so) $g \mid x^p$ $g = x^k$

dann $g \cdot y^k$ wid!

Wenn II $a = cb$; so b [illegible] dann

$a \mid g^2$, $a \mid g^2$, $g^2 = ag_1$

I wenn also $a = c \cdot b$, so

$$g \cdot \frac{\partial g}{\partial x} = c_1 x^n + a y^n = (d_1 x + d_2 y)^n$$

$$g = (d_1 x + d_2 y)^k$$

$$g^2 = (d_1 x + d_2 y)^{2k} = (\alpha x^n + \beta y^n)$$

$\partial g \neq 0$ für jedes lineare g, dann

NB: für $f = l^k$, l linear polynom

mit g^2 entsprechend auf niedrige Potenzen:

$$f^\nu = \alpha^p \cdot e^{2\pi i p} = (\cdot x^n + \cdot y^n) e^{2\pi i p}$$

← ✱ in $K(z\bar{z})$ gilt die entsprechende Regel für

Grad niedrig: $f^\nu = \cdot z^n + \cdot \bar{z}^n$.

NB: Wenn $g = l^{\frac{p+1}{2}} \cdot g_1$, l linear,

dann $g^2 = l^p \cdot (l g_1^2)$

$$= \cdot x^n + \cdot y^n$$

Ja! Die Frage wäre ob nur dann. Sonst

223 invariant gegen $x \to \alpha x + \beta y$ mit $\begin{vmatrix} \alpha & \beta \\ c & d \end{vmatrix} \neq 0$

$y \to \gamma x + \delta y$

Daher kann $g^\nu = \cdot x^r + \cdot y^r$ nicht eintreten,

wenn $g = l_1^h + l_2^k$ $l_1 \neq \text{const} \cdot l_2$

NB: das sind nur $g = \sum^n l_1^k$, $n \leq e \cdot \nu$

denn oBdA $l_1 = x$, $l_2 = y$: $(x+y^h)^h = \cdot \to x^k \cdot y^k = \cdot \cdot$ ↓Grad x.

223 Noch p-Gruppen vom Grad p^2.

(1) Satz: Sei K ein Körper der Char p, $f \in K[x]$, $f \neq 0$,

25.9.64 $f^2 = r + s x^{p^\lambda}$, $\lambda \geq 0$, $r \neq 0$

Dann ist entweder

$\operatorname{Gr} f =: k \leq m+m'-\hat{q} \leq 2m-1$, $q^2 T(r,s)$, $\hat{q} = \operatorname{Grq}$

NB sogar $2k - p^\lambda < m+m'-\hat{q}$, wo $m = \max(\hat{r}, \hat{s})$, $m' = \max(\hat{r}', \hat{s}')$

$k = \#$ von 0 verschiedene Nullstellen von f $\prod (x-\alpha)^{p^\lambda} \mid f$ & $\alpha^{p^\lambda} \in K$

$r = a^{p^\lambda} s$ (also $a \in K$ wenn K vollkommen)

Bew. Man kann annehmen, daß r und s keinen $\neq 1$ gemeinsamen Faktor haben; dann ist $r'+ts' \neq 0$.

Bilde $R(t) := \operatorname{Dis}_x(r(x)+s(x)t) = h(t)$, $h' = \frac{dh}{dt}$

$= \operatorname{Res}_x(r+st, r'+s't) = \operatorname{Res}(h,h')$

Frage: Gibt es Relationen zwischen $f \cdot g$ "klein", f^2 klein? $\operatorname{Gr}_t R(t) \leq$ ... linear in $m+m'$, mit $m' = \max(\hat{r}', \hat{s}')$

Sei $(x-\xi)^n \mid f$, $n \geq 1$; $\Rightarrow h \equiv 0$

$(x-\xi)^{n+1} \mid f^2 = r + s x^{p^\lambda}$

$x \to x+\xi$: $x^{n+1} \mid r(x+\xi) + s(x+\xi) \cdot (x+\xi)^{p^\lambda}$ $(x^{p^\lambda} + \xi^{p^\lambda})$

$= r(x+\xi) + \xi^{p^\lambda} s(x+\xi) + x^{p^\lambda} s(x+\xi)$

wegen $n+1 < p^\lambda+1$: $x^{n+1} \mid$ (---) $= a_0 + a_1 x + \dots$, $a_0 = \dots = a_n = 0$

$R(t) = \operatorname{Res}(r(x+\xi) + s(x+\xi)\cdot\dots$

$= \pm$ Res. I. Wenn nun $\operatorname{Gr} h < n$,

so folgt $r(x+\xi) + \xi^{p^\lambda} s(x+\xi) \equiv 0$

$r(x) = -\xi^{p^\lambda} s(x)$ $\to \xi^{p^\lambda} \in K$

$f^2 = s(x) \cdot (-\xi^{p^\lambda} + x^{p^\lambda}) = s(x) \underbrace{(x-\xi)^{p^\lambda}}_{(x-\xi)^n}$ $\Rightarrow \beta(\alpha) \neq 0$

$\to$ fertig.

Sei nun r

$R(t) = \operatorname{Res}($

$= \operatorname{Res}($

$= \begin{vmatrix} a_0 + s & & \\ a_1 & s & \\ \vdots & & \\ a_{n-1} & & s \end{vmatrix}$

$a_0, \dots, a_{n-1}$ linear in t

$\operatorname{Gr} h \geq n$

also r

$(t$

Aus

linear in

läßt, folg

II: $k = \operatorname{Gr} f$

Lemma

$h := r$

einen quad

Nach Wegfall

von k, l und

$q = \dots$, und

$l_0 = \dots$

sei ξ weiter $\operatorname{gr} h \geq n = n_\xi$, für jede Wurzel ξ von f

$$R(t) = \operatorname{Res}_x\big(r(x+\xi) + s(x+\xi)\cdot t \;,\; \tfrac{d}{dx}\cdot\big)$$

$$= \operatorname{Res}_x\big(a_0 + a_1 x + a_2 x^2 + \dots + s(x+\xi)[t-\xi^p] \;,\; \tfrac{d}{dx}\cdot\big)$$

$$= \operatorname{Res}_x\big(a_0 + a_1 x + a_2 x^2 + \dots + s_0 + s_1 x + s_2 x^2 + \dots \;,\; \tfrac{d}{dx}\cdot\big)$$

$$= \begin{vmatrix} a_0 + s_0[t-\xi^p] & a_1 + s_1[\,] & \cdots \\ a_1 + s_1[\,] & 2a_2 + 2s_2[\,] & \cdots \\ \vdots & \vdots & \\ a_{n-1} + s_{n-1}[\,] & n a_n + n s_n[\,] & \cdots \end{vmatrix}$$

n Zeilen, weil $\operatorname{gr} h \geq n$

n Spalten

aber wegen $a_0 = \dots = a_{n-1} = 0$ haben wir

$$(t-\xi^p)^{n-1} \mid R(t),$$

Aus $\xi \neq \eta$ folgt $\xi^p \neq \eta^p$ wegen der p, die man ξ die Nullstellen von f durch laufen läßt, folgt, wenn $R(t) \not\equiv 0$,

$$\text{II:}\quad k = \operatorname{gr} f \leq \operatorname{gr} R(t) \leq n^2 - n$$

Setzen wir $R(t) \equiv 0$, d.h. $h := r(x) + s(x)\cdot t \in K(t)[x]$ hat

einen quadratischen Faktor $h = k^2 \cdot l$ $k, l \in K[t]$, $\operatorname{gr} k \geq 1$

Nach Wegschaffen des Nenners in t und Potenzen-Abziehen von k, l wird $k_0^{\nu} \cdot l_0 = h \cdot \varphi(t)$ - polynomiell, aber $\varphi = \text{const}$, und wegen t-Grad auch $k_0 \in K[x]$ unabhängig $l_0 = \dots + t \dots$, aber $k_0^2 \mid r$ und $k_0^{\nu} \mid s$ - Widl

Zusatz (1') Unter den Vor von (1)

$$f(x) = \sum_{\nu=1}^{k} c_\nu (x - \xi_\nu)^k \qquad n > \frac{n+1}{2} \text{ oder } n = 1$$

dann $(x-\alpha)^{\frac{n+1}{2}} \mid f$, o.B.d.A. $\alpha \geq 0$ durch Translation

also $x^{\frac{n+1}{2}} \mid f \qquad 0 = \sum_{\substack{\nu=1 \\ \xi_\nu \neq 0}}^{k} c_\nu \xi_\nu^{n\nu} \quad \nu = 0, \dots, \frac{n-1}{2}$

Sei $n > 1$, dann ist unter den $\xi_\nu \neq 0$, die Anzahl der von Null verschieden ist $> \frac{n+1}{2}$.

damit ist der Fall erledigt, dass die Aussage von p. 219 quadratfrei ist.

NB (2) Es könnte man (im zahmen Fall $p \geq 2$ mindestens für $n \geq 5$) versuch dürfen die Elemente $g \in G$ zu untersuchen, welche Fixpolynome, und $x^2 - x$ dann man durch einen Trans $x \to x + ax^p$ den Grad von g auf der betreffenden Bahnlänge was genauer bd.

NB (3) Man sollte die Untersuchung über die Einbettung regulärer Gruppen von diesem invariant führen (betrifft Automorphismen von G).

Exp g oberhalb Grenze könnte $\frac{5}{8}$ sein

Bew (2) Sei $g \in k[x]$ $\deg g < \frac{5}{8} p^2$ $g^2 = q(x) + s(x)(x^p - x)$

$= r(x) - x s(x) + s \cdot x^p$

n: $(x-\alpha)^{\frac{n+1}{2}} \mid g \quad x^{\frac{n+1}{2}} \mid g(x+\alpha) \to$

$k \geq 2n \to k < 2(n+1) = 2(2k-p^2)+1 \to$

Exp $g(x+\alpha)$

$g(x+\beta)$ durch

aber dieselben

(4) Sei $G_p f = \{ \hat{f} \leq \frac{2(p^\alpha - 1)}{3}, f = r + s \cdot (x^{p^\alpha} - x), p > 2 \}$

Dann enthält die Exponentenmenge $\mathrm{Exp} f$ einen Rest $e = \sum \mathrm{exp}^\nu$ mit $e_\nu > \frac{1}{2}$ $(\nu = 0, 1, \ldots, \alpha-1)$

Bew.: Nach S. 223 ist entweder $\mathrm{I}\ \hat{f} < 2(\hat{s}+1)$

oder $\mathrm{II}\ \exists\ (x+\xi)^{p^\alpha} \mid f^2$.

Im Fall I ist $\hat{f} < 2[2\hat{f} - p^\alpha] + 2 = 3\hat{f} - 2p^\alpha + 2$

$3\hat{f} > 2p^\alpha - 2$, was widerspricht.

Sei Fall II. Dann $(x+\xi)^{p^\alpha} \mid f^2$, $(x+\xi)^{\frac{p^\alpha+1}{2}} \mid f$

$(x+\xi)^{\frac{p^\alpha+1}{2}} \mid f(x+\xi)$ $\quad \varepsilon = \begin{cases} 0 & p = 2 \\ 1 & p > 2 \end{cases}$

↓

Der Exp liegt im "Quadrat" $e_\nu = \frac{p^\alpha+1}{2}$:

$$\frac{p^\alpha+1}{2} = \frac{p+1}{2}(1 - p + p^2 + \cdots + p^{2\alpha}) = \frac{p-1}{2} + p\cdot\frac{p-1}{2} + \cdots$$

$$\frac{p^\alpha+1}{2} = \frac{p+1}{2} + p\left(\frac{p-1}{2}\right) + p^\nu \frac{p-1}{2} + \cdots + p^{\alpha-1}\frac{p-1}{2}$$

$$\text{da } f(x+\xi) = \cdots p^{\frac{p^\alpha+1}{2}} \cdot g(x)$$

Siehe 247

$\mathrm{Exp}\, g(x+\alpha) \leq \frac{p^\alpha-1}{2}$ $\Rightarrow$ $\mathrm{Exp}\, g(x) \leq$ [redacted], da $g(x)$ aus $g(x+\beta)$ durch $x \to x^{p^\alpha}$ Substitution entsteht, $\bar{g} = g(x)^r$ offenbar aber dieselben Voraussetzungen, daher $\mathrm{Exp}\, \bar{g} \leq$ [redacted] $\Rightarrow \mathrm{Exp}\, g \leq$ [redacted] $\Rightarrow \hat{g} \leq \frac{p^\alpha-1}{2}$.

227 (1) Irreduzibler Fall $p \nmid n \geq 5$. Es x^2 aus $f_{n,i}$ darstellbar

Wurzel $g \in g \Rightarrow$ Schiefgrad $g =: \hat{g} \leq \frac{5(p-1)}{g}$

der homogene Teil höchsten Schiefgrads von g, $f_i^2 = a_i + S(x^{p^2} - x)$, so ist $\hat{a} < \frac{p-1}{4}$, also $\hat{g} \leq \frac{p^2-1}{4} \leq \frac{p^2-1}{4} < \frac{p-1}{4} p$

$\hat{a} < p\frac{p-1}{4}$. Nach 223 ist also $g_i \leq \ldots$

Fermat's

Darstellg der Funktionen $K_{p^a} \to K_{p^a}$:

(1) Der Ring der Funktionen $K_{p^a} \to K_{p^a}$ ist isomorph $K_{p^a}[x] \Big/ x^{p^a} - x = R_{K_{p^a}}$

(2) $R \cong K[u_1, \ldots, u_a] \Big/ (u_1^p - u_1, \ldots, u_a^p - u_a)$ wenn $K \supseteq K_{p^a}$

dabei $K = K[x] \Big/ x^{p^0} - x$

ohne 2-3 Bew.: Wähle $\alpha, \beta, \gamma \in K_{p^3}$ so daß mit $\alpha' = \alpha^p$, $\alpha'' = \alpha^{p^2}$ gilt, $\begin{vmatrix} \alpha & \alpha' & \alpha'' \\ \beta & \beta' & \beta'' \\ \gamma & \gamma' & \gamma'' \end{vmatrix} \neq 0$.

In R_K setze $u_1 := \alpha x + \alpha' x^p + \alpha'' x^{p^2}$

$u_2 := \beta x + \beta' x^p + \beta'' x^{p^2}$

$u_3 := \gamma x + \gamma' x^p + \gamma'' x^{p^2}$

dann

unge

Polyn

dann f

also

R_{K_p} ist

Unters

Fall d

wenn

Die

im $x^\tau =$ $x \neq$

Dann ist $u_i^p \equiv u_i \bmod x^{p^3} - x$.

Umgekehrt; definieren $K[u, u_1, u_2]$ drei Polynome x y z von u, u_1, u_2 durch

$$u_1 = \alpha x + \alpha' y + \alpha'' z$$
$$u_2 = \beta x + \beta' y + \beta'' z$$
$$u_3 = \gamma x + \gamma' y + \gamma'' z$$

dann folgt aus $u_i^p = u_i$:

$u_1 = \alpha x^{p^3} + \alpha' y^{p^3} + \alpha'' z^{p^3}$
$u_2 = \beta x^{p^3} + \beta' y^{p^3} + \beta'' z^{p^3}$
$u_3 = \gamma x^{p^3} + \gamma' y^{p^3} + \gamma'' z^{p^3}$

also

$$x = z^{p^3} \quad y = x^{p^3} \quad z = y^{p^3}$$

daher $x^{p^3} = x$.

Kapitel 6 ist geeignet schon zur Untersuchung der Abb von K_{p^α} in sich.

Alle der 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 Der Vorrat der Translationsgruppe (p, p, p) von K_{p^α}, die in $x \tau = x + \xi$, d.i. $u_1^\tau = u_1 + \alpha\xi + \alpha'\xi' + \alpha''\xi''$ usw., d.h.

Zzg die Translationen sind die p^d Transform

$T_\tau \quad x_i^\tau = x_i + \tau_i$ mit $\tau_i \in K_p$!

$(N\,T)_0$ ist $x_i' = \sum c_{ik} x_k$, $\det c_{ik} \neq 0$

$N\,T$ ist $x_i' = \sum c_{ik} x_k + d_i$.

Ist g auf K_p, 2-abgeschlossen und sind je zwei nichttriviale Nullen von g konjugiert (auch im trivialen Fall) so entsteht g mit $g(x)$ als auch $g(ax)$ $a \in K_p$, genau mit $f(x)$ (auch ohne 2-Abgeschlossenheit) $f(ax)$ eine Invariante von g, $\forall a \in K_p$.

$\xi \in K_{p^a} \Leftrightarrow (x_1, x_2, x_3) \in K$.

wo $x_i = \alpha \xi + \alpha' \xi^p + \alpha'' \xi^{p^2}$ usw.

---

(2) VB: Zur Behandlung der Pgr mit $\neq p$-Ind. K wird man den Körper K_{p^a} nur dann empfehlen, wenn g eine Nst der Ord p^a p/a ausgezeichnet ist, oder eine Kette von solchen; die wird man dann mit Teilkörpern von K_{p^a} identifizieren; oder wenn bestimmte Autom. von g interessieren, die man

besonders

In alle

Wenn es

ist der Körper a

Invarian

Abbildung

an Ampel:

$f \wedge g$

vorteilhaft

Veränder

wenn f.

insbesond

Mu

besteht,

dann

(

Wieder

Menge

bestimm

ist f

wenn für

besonders gut im K_p darstellen kann.

In allen anderen Fällen wird man besser als Koeffizienten den Vektorraum über K_p nehmen, etwa $v = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix}$ $x_i \in K_p$.

Invarianten sind Funktionen $f(\varphi)$, Abbildungen von Ω in sich sind Funktionen, z.B. $f(\varphi) = \begin{pmatrix} f_1(\varphi) \\ f_d(\varphi) \end{pmatrix}$, Faltung

$$f \wedge g = \sum_{A \in \mathfrak{D}} f(\varphi - A)\, g(A)$$

Vorteilhaft ist hier die Regel von der getrennten Veränderlichen: wenn $f(x_1 \dots x_d) = f'(x_1 \dots x_s) \cdot f''(x_{s+1} \dots x_d)$ und ähnlich $g, \dots$, dann $f \wedge g = (f' \wedge g') \cdot (f'' \wedge g'')$.

Insbesondere ist die Faltung von Monomen $x_1^{n_1} x_2^{n_2} \dots x_d^{n_d}$ leicht, nämlich variablenweise auszuführen. Dann benutzt man die Binomialformel mit $\binom{n_i + n_j + \dots}{n_i, n_j, \dots} = \prod \binom{n_i}{k_i}$ und p.

Wieder gilt, wenn $\operatorname{Exp} h(x_1 \dots x_d)$ die Menge der wirklich auftretenden Exponenten bezeichnet:

Ist f Invariante von $\mathfrak{g}_0$ und $x_1 = f \wedge \dots$, so ist für jedes $g \in \mathfrak{g}$ $\operatorname{Exp} g_1 \subseteq \operatorname{Exp} f$.

231

(a) Der Ring aller Funktionen auf endlichem Ω mit Werten aus einem Körper K mit $|K|>2$ ist ein Hauptidealring.

Beweis: T von f mit g, n die Funktion, die auf Träger f = Träger g $=1$ mit, sonst $=0$

Jedes Element von $K[x_1,\dots,x_n]/(x_i^{r_i}-x_i)_{i=1,\dots,n}$ ist Produkt von Faktoren $\sum c_\nu x_\nu + d$.

Beweis: $\cong K[x]/(x^p-x)$.

---

(2) Im Ring mit $\alpha=2$ ist $l_1 \wedge l_2 = \begin{cases} 1 \\ 0 \end{cases}$ wenn l_1, l_2 ein ab ; dabei $l_i = \varepsilon_{i1} x_1 + \varepsilon_{i2} x_2 + \varepsilon_{i3}$

Satz II Wenn G drei elementfremde rationale Komplexe $\neq \{1\}$ hat mit Längen $n_1 \le n_2 \le n_3$, so ist G regulär oder $G \triangleright \mathfrak{N} \neq \{1\}$ ... $G/\mathfrak{N}$ auflösbar.

Bew. G 2-reg. Bew.: Bestehe $\mathfrak{N}_1$ aus n_1 Vielfachen von p, $\mathfrak{N}$ die i-te von $\mathfrak{N}_1$ verschiedene Konjugierte, durch $l_\nu(x_1, x_2) = 0$ (l_ν linear), $\sum_{i=1}^{n_1} l_i^{p-1} =: f_1$ (wo bei $g_\alpha = \begin{cases} n_{\alpha-1} \text{ oft in } \mathfrak{N}_1 \\ n_\alpha \text{ oft } \notin \mathfrak{N}_1 \\ 0 \quad \alpha = 1 \end{cases}$)

ebenso $\sum_{j=1}^{n_2} m_j^{p-1} =: f_2$

Wegen $n_1 > 1$ stets $x_1, x_2 = f_1 \wedge \ldots$

aber für $\forall g \neq g_1$ $g_1, g_2 = f_1 \wedge \ldots$

daher, wenn h_1 Restglied $g_1 = l_1$; $g_1 h_1 = k$:

$$h_1 = \sum c_i l_i^k = \sum d_j m_j^k;$$

ebenso $\quad$ für $k \ge n_1 + n_2 - 1$ stets $l_1^k \cdots m_{n_2}^k$

also wenn stets $k \le n_1 + n_2 - 2 \le \frac{2(n+1)}{3} - 2 \le \frac{2}{3}(p-1)$

NB: Ebenso Restglied g_2; Das ganze gilt für $\frac{2}{3}$ Loch

Produkt von f mit $f = f_1 \wedge \ldots$ Ferner $\binom{n}{n_1}$ der $\binom{n}{n_2}$ l_1, l_2, l_3

$= f_2 \wedge \ldots$ jedes $\square$ ausgenommen stets also $g_1 g_1 g_1^2 g_2 = f_1 \wedge \ldots$

daher für $g_1^{\alpha_1} g_2^{\alpha_2} g_3^{\alpha_3} \le n - 2$ stets also usw.

233 Also ist Gesamtgrad $g_\nu < \frac{2(p-1)}{3}$; kurz: $\operatorname{Exp} g_\nu \subseteq \mathfrak{E}$.

[illegible]

Sonst ist x_1^ν und x^ν von der Form $f_1 \wedge \cdots$,

also ist nach VB 23.2 $\operatorname{Exp}\left\{\frac{g_1^\nu}{g^\nu}\right\} \subseteq \mathfrak{E}$.

Auf Leitgebiet h_1 wende (k) von S. 223 an:

$$h_1^\nu = r x_1^r s x_2^s \qquad \text{Gr } r,s = 2k \cdot p = m$$

$\Rightarrow$ entw. $h := g_r h_1 \leq 2m-1 = 4k - 2p - 1$ $\quad k \geq \frac{2p-1}{3}$ ↓ ↑

oder $\exists\ l^{\frac{p+1}{2}} \mid h_1 = \sum^{m} c_i l_i^k = \sum^{m_2} d_j m_j^k$

differenzierbar mit $m_1 - 1$ linear, die alle l_i außer einem l_0, zum Verschwinden bringen.

Wenn $m_1 - 1 \begin{cases} < \frac{p+1}{2} \\ < k \end{cases}$, so bleibt $l \mid l_0$, pos.

$l = l_0$

Wenn $m_2 - 1 < \begin{cases} \frac{p+1}{2} \\ k \end{cases}$, so kann $l = m_0$; ↓ ↑

(aber $l_i \neq m_j$.

Also ist

Der erste

also

Satz 11). f

Beweis: Vor

Lösu

von

Wenn

hat,

Hat

so gibt

$f_1(ax)$

dann $f_1 \wedge f$

Also ist $n_2 - 1 \geq \frac{p+1}{2}$ oder $\geq k$.

Im ersten Fall ist unmöglich wegen

$$\frac{p+1}{2} \leq n_2 \leq n_3 \Rightarrow n_1 + n_3 > p+1 ,$$

also [illegible] $k \leq n_2 - 1 < \frac{p+1}{2}$

$$k \leq \frac{p-1}{2}$$

Dann ist Satz 9 im 1. Quadrant.

I von 210 c: G einen ab $\geq n$ inhe
g/n anfl.

Satz 11. Sei G pri, Grad p^2, mit reg Ug.

G habe einen nichtidentischen rationalen Komplex; G habe einen irrationalen Komplex. Dann ist G elinear.

Bew: Nach 9 hat G nur einen mt rat Komplex, daher nur eine homogene Invariante f_0 vom Grad $p-1$.

Wenn G eine Kom Mo vom Grad $< \frac{2}{3}(p-1)$ hat, wie fertig wie früher (~225)

Hat G keine Kom Mo vom Grad, so gibts $f_1, f_2 \in f_0$ mit $f_1(gx) = a^{\alpha} f_1(x)$

$f_2(gx) = a^{\beta} f_2(x)$, $\alpha + \beta = p-1$, $\alpha \neq 0$, $\alpha \leq \beta$.

Dann $f_1 \wedge f_2 = c f_0 + d \Rightarrow f_0 \wedge f_1 \wedge f_2 = c f_0 \wedge f_0 = c \cdot e$

23.5 $e \not\equiv 0 \pmod p$, da $e = \sum f_0(-t) f_0(t)$

$= (p-1)\cdot\left[k(k-1)^\nu + (p+1-k)\,k^\nu\right]$

wenn der Rat Komplex aus k Ugr besteht.

Wegen g prim, $\nu \geq 1$, $k > 1$, daher $e \not\equiv 0 \pmod p$.

Also ist $f_0 - f_1 \not\equiv 0$, das ist aber

Nullstellen vom Grad $\alpha \leq \frac{p-1}{\nu}$.

HS: g 2-adv prim, reg (Ugr), Grad $p^\nu \Rightarrow$

entweder Rang $g \leq 3$, jeder Komplex rational.

oder $\exists D_2\ g^* = g_1 \otimes g_2$ Kronecker prod., $g_1 \cong g_2$ (vom Typ 2ν)

Ausnahmen bei Existenz eines Invariantenpolynoms vom Grad $\leq \frac{2}{3}(p-1)$ noch nachzuprüfen.

trifft Rg $g = 3$ auf ?

Dem I § 4 S. 234.

Kurt's g unimpri, Grad $g = p^2 \Rightarrow$ i.a. g einzeln: $f \triangleleft g$.

Unterlas

1) Def: $G \in \Sigma$

$\subset$ C

Nachkommen dies:

2) result:

problem:

---

3) Unte

Gres

---

4) Existen

Unterhaltung mit Mr. Cawlina, QMC, London 22.10.64

1) Def: $G \in Z :\Leftrightarrow$ If $G \rhd A \trianglerighteq B$ then $N_G A \trianglerighteq G$
(simple)

$G \in X :\Leftrightarrow A \trianglerighteq G \Rightarrow NA \trianglerighteq G$

[illegible] clear $X \subseteq Z$ .. Problem: $X = Z$?

$\in = \cap N_G A$, $A \trianglerighteq G$.

2) result: $G/W(G)$ nilp $\Rightarrow G \in X$
$\Leftarrow$?

problem:

---

3) Unterhaltung mit Barratt, Prof, Manchester:

Gpen $G_1 \times Z_\infty \cong G_2 \times Z_\infty \Rightarrow G_1 \cong G_2$?

---

4) At least D. Robinson erhalten Proc Camb Phil Soc 1964

23 ✝
31.1.65

Erweiterung der Theorie max. π-Gruppen.

nach Relativ-Fest sei $\mathfrak{G}$ die Menge der π-Gruppen (Ausschnitte) von G.

Sei J ein Ideal in $\mathfrak{G}$: $A \in \mathfrak{G}$, $B \in J$

$\Rightarrow A \to B \;\&\; B \to A \in J$ (gleichwertig: $\Rightarrow B \to A \in J$)

[Nb: $J\mathfrak{G} \subseteq J \Rightarrow \mathfrak{G} J \in J$]

Das Ideal habe die nachstehenden Eigenschaften:

I. $G_1 \trianglelefteq G_3$, $G_1 \in G_2 \trianglelefteq G_3$, $G_2/G_1 \in J$, $G_3/G_2 \in J$
$\Rightarrow G_3/G_1 \in J$ (in J integrabel / ad Abelsch)

II $G_0 \trianglerighteq G_1$, $G_0 \trianglerighteq G_2$, $G_1 \cap G_2 = G_3$,
$\exists\, I \in J$ mit $I \to G_0/G_i = G_0/G_i$ $(i = 1, 2)$
$\Rightarrow G_0/G_3 \in J$.

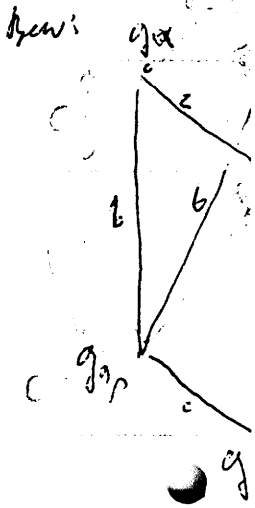
III $\forall$ $G_0 \trianglerighteq G_2$, $G_0 \trianglerighteq G_1 \trianglerighteq G_2$
und $G_0/G_1 \in J$, $J \to G_1/G_2 = \{G_2/G_2\}$,
es exist. $H/G_2 \leq J$, $HG_1 = G_0$, $H \cap G_1 = G_2$,
und je zwei solche H's sind konj. in G_0.

Dann sind vermutlich je zwei Maximalausschnitte in $\mathfrak{J}$, die dieselben Projektionen in eine K-Reihe von G ergeben, konjugiert in G.

Teilkonstit.p+

(1) $\mathfrak{G}$ tr
auf
$\mathfrak{G}$ ha
$\Rightarrow R :=$

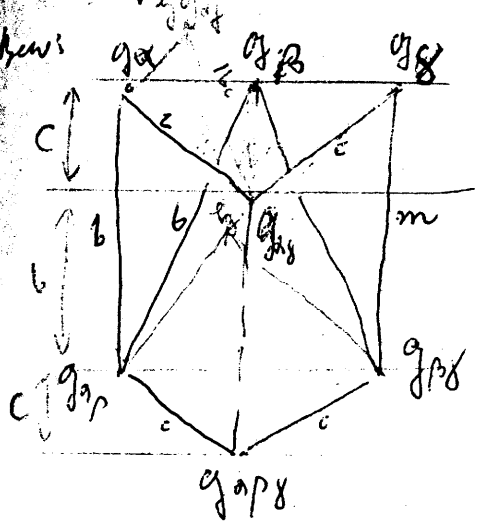
Bew:



$\mathfrak{G}_\alpha$, $\mathfrak{G}$
$\mathfrak{G}_{\alpha\beta} \leq [\mathfrak{G}_\alpha, \mathfrak{G}_\beta]$
Bew: $\mathfrak{G}_2 = \mathfrak{G}_3$
$|\mathfrak{G}_2| = 1$

(1) G tra Ω, G_α einfach für $|\Omega| = n$
auf β $G_\alpha \neq 1$ G_α mit Längen $b \geq c$
G habe keinen Teiler m mit $m \geq b$ und $m \mid bc$.
$\Rightarrow K := \langle G_\alpha, G_\gamma \rangle \leq G_{\alpha\gamma} G_\beta$; $c \leq |K : G_\alpha| \mid (b, n)$;

(1) Zerlegung Ω auf S. 235



Bew: wenn $c > 1$, so $G_{\alpha\beta} \cdot G_{\alpha\gamma} = G_\alpha$ einfach

$|G_{\alpha\gamma} : G_{\alpha\beta\gamma}| = b$

$|G_\alpha : G_{\alpha\beta\gamma}| = bc$

$bc = |G_\gamma : G_{\alpha\beta\gamma}| \leq |G_\gamma : G_\beta| |G_\gamma : G_{\beta\gamma}|$

$= cm$

$m \geq b$ $\quad m \mid bc$

$m = b$

dann stabilisiert

$G_{\alpha\gamma} G_{\beta\gamma} = G_\gamma$

$G_{\alpha\gamma}$ vtb mit $G_{\alpha\beta}$, $G_{\beta\gamma}$

$G_{\alpha\gamma}$ vtb $- \langle \downarrow \rangle =: L$

$G_\alpha, G_\gamma \leq G_{\alpha\gamma} L \leq G_{\alpha\gamma} G_\beta$

dann

$G_\alpha \leq \langle G_\alpha, G_\gamma \rangle : G_\alpha$ teilt b; wenn $c > 1$ so einfach.

Bew: $K = G_\alpha K \cap G_{\alpha\gamma} G_\beta$

$G_\gamma \leq K \leq G_\alpha G_\beta$ Wde!

239 Korollar 1": $g_\alpha g_\beta =: R \Rightarrow$

$g_\alpha, g_\beta \leq R \leq g_\alpha g_\beta$

$(g_\alpha : R) \mid n$

$(R : g_\alpha) \mid n$

Zusatz 1': Wenn $(R : g_\alpha) = b$, so ist

wegen $R \leq g_\alpha g_\beta$ aber sicher $R = g_\alpha g_\beta$

also g_α teilt g_β.

Frage: Gibt es einen für Normalteiler brauchbaren

2-Ne. Kern von g.

Frag

Gibt es ein

Element

(1) Zwei

gleiche

(2) g^3-

(3) $a^2 j$

Bew: $a^2 k$

$a i$

[1] Sa

[2]

[1] Frage:

[2] "

Frage von Dénes, J., Budapest 1965:

Gibt es eine Gruppe G, in der ein passendes Element $g \in G'$ nicht ein Kommutator ist?

Gruppen vom Grad p.

(1) Zwei Untergr. vom Index p, die keine Basen gleicher Länge besitzen, sind konjugiert.

denn von G_1 aus haben sie dieselbe Invariante.

(2) G 3-tra $\Rightarrow$ Kleinsche $q_p = 1$ $(\exists b)$

(3) $a^2 j_1 = b^2 j_2 \Rightarrow j_1 = j_2$ oder $a^2 = b^2$

Bew: $a^2 k(p-k) = b^2 l(p-l)$ o.B.d.A. $ak \geq bl$; $a,b > 0$

$ak = \delta bl + xp$ $\delta = \pm 1$ $\frac{p}{2} \geq x \geq 0$ $a^2, b^2 \leq \frac{p+1}{4}$

~~$a^2k^2 + b^2x^2p - 2abkx = k^2lp$~~

[1] $\delta a - b - 2\delta x = yp$

[2] $bly = x(a-x)$

[1] resp: $y = 0$

[2] " $x = 0 \to ak = bl$ $a(p-k) = b(p-l)$ $a = b$

oder $x = a \to ak = \delta bl + ap$ $a(p-k) = bl$ $ak = b(p-l)$ $a = b$

241 **Gruppen vom Grad p^2** Fortsetzung v. §3 25.9.65

Satz: Ist $j_1 j_2 = j_3 j_4$, so ist $j_1 = j_3$ oder $j_1 = j_4$.

Bew.: Sei $j_1 = \frac{k(p-k)}{p-1}$, $j_2 = \ell$, $j_3 = m$, $j_4 = n$

o.B.d.A. sei $k\ell \geq mn$. $k, \ell, m, n < \frac{p}{2}$

$$k(p-k)\ell(p-\ell) = m(p-m)n(p-n)$$

$$\text{(*)} \qquad k\ell = \delta mn + xp \qquad \delta = \pm 1$$

dabei $0 \leq k\ell - mn \leq xp \leq k\ell + mn < 2 \cdot \frac{p^2}{4}$ $\qquad 0 \leq x < \frac{p}{2}$

gibt eingesetzt $k\ell(p^2 - p(k+\ell) + k\ell) = \ldots$!

$$\begin{cases} m + n + \delta(2x - k - \ell) = py & \text{(I)} \quad \checkmark \\ mn(1-y) = (k-x)(\ell-x) & \text{(II)} \quad \checkmark \end{cases}$$

(I) liefert, da $x \geq 0$, wegen $k\ell \geq mn$: $-p < py < 2p$, $y = \begin{cases} 1 \\ 0 \end{cases}$ ✓

Fall $y = 1$: $(k-x)(\ell-x) = 0$ etwa $x = k$ (*) liefert $k(p-\ell) = -\delta mn$,

also $\delta = -1$. $\quad mn = k \cdot (p-\ell)$ & $m + n = k + (p-\ell)$ (aus I)

also $\{m, n\} = \{k, p-\ell\}$, etwa $m = p - \ell > \frac{p}{2}$ ↯

✓

Beweis

$y = 0$: I $\quad m + n = \delta(k + \ell - 2x)$

II $\quad mn = \delta(k-x) \cdot \delta(\ell - x)$ $\Big\}$ $\{m, n\} = \{\delta(k-x), \delta(\ell-x)\}$

etwa $m = \delta(k-x)$, $n = \delta(\ell - x)$; $x = k - \delta m = \ell - \delta n$

(*) $k\ell = \delta mn + kp - \delta mp$

$k(p-\ell) = \delta m(p-n)$ also $\delta > 0$, $\delta = +1$ ✓

(*) $k\ell = +(k-x)(\ell-x) + xp$ gibt $0 = x(p - k - \ell + x)$ ✓

Ist $x = 0$, so $m = k$, $j_1 = j_3$. Ist $x = 0$, so $m = k - x = p - \ell > \frac{p}{2}$, ↯

Gruppen vom Grad p.

Aus der Voraus. $k(p-k)\,\ell(p-\ell) = m(p-m)\,a^2(p-1)$, $a \neq 1$

Folgt:

(1) $k\ell = \delta m a + x p$

(2) $\delta(2x-k-\ell) + a(m+1) = y p$

(3) $(a-y)\,a\,m = (k-x)(\ell-x)$

(4) für $j = \frac{k(p-k)}{p-1}$, $j > 1$ $\quad \frac{k}{2} < j < k$; $\sqrt{p-1} < j \leq \frac{p+1}{4}$

Unter der Voraussetzung $k < m < \ell$, also $j_1 < j_3 < j_2$,

folgt:

(5) $\frac{k\ell}{4m} < a^2 < \frac{2k\ell}{m}$; (5') $j_1 < a^2 < j_2$

(6) $x < \ell$ (1)

(7) $y < a$ (2)

(8) $x < k$ (1) (5)

(9) $x > 0$ (1) (5)

(10) $(k-1)(\ell-1) + 2x + \delta a - 1 = p(x+\delta y)$

(11) $x + \delta y \geq 0$ (10)

(1') $a^2 m^2 < p j_1 j_2$

(1'') $am < \frac{1}{4} p^{3/2}$

(1''') $|x| < \frac{1}{4}(p+\sqrt{p})$

(3') $x\,m(p+x-k-\ell) = a\,m(a-y-\delta)$

2/43 (12) Zz. $j_1 j_2 = a^{\cdot} j_3$ wegen $\kappa\lambda = a\mu$, o.B.

26.9.65 i.A. $a \mid j_1$, $a \mid j_2$

Bew: Sei $q^{\alpha} \mid a$. Wähle $q \mid q$, $q \nmid \kappa$.

Dann $q^{\alpha} \mid \kappa\lambda$ $q^{\alpha} \mid \lambda\bar{\lambda} = j_2$

$q^{\alpha} \mid j_2$.

Andere, einfachere Bew. u. unsere auf dieser Seite

allg. Fahlenlehre

(13) Sind a, b, c, d paarweise teilerfremd, so

ist $n = a_1 bcd + ab_1 cd + abc_1 d + abcd_1$

mit $|a_1| < |a|$, $|b_1| < b$ usw.

Bew: $\frac{1}{abcd} < \frac{x_1}{a} + \frac{x_2}{b} + \frac{x_3}{c} + \frac{x_4}{d}$

wobei die x_i und a, sofern $\neq 0$, $< a$ sind

$n + \frac{1}{abcd} = \frac{y_1}{a} + \dots + \frac{y_n}{d}$ mit $0 \le y_i < a$

Andere wie oder es $= y_2 a b \cdot \dots \cdot y_n - 1$.

oder 3

Aus (12) folgt:

(14) genau in $j_1 j_2 \dots j_\nu$ $\kappa\lambda = p^{\alpha}\mu$ kommt nicht vor

$a = p^{\alpha} \Rightarrow$ [illegible]

* Andere Bew (12): $\kappa\lambda = a\mu \Rightarrow \lambda\bar{\mu} = \frac{a^2}{\alpha} \cdot \bar{\kappa}$

$\Rightarrow \bar{\kappa}\mu = \frac{\kappa\bar{\kappa}\lambda}{a} = \frac{j'}{a}\lambda$

* $\kappa\lambda = q\mu \Rightarrow \lambda\bar{\mu} = \frac{q\mu\bar{\mu}}{\kappa} = \frac{q\kappa\bar{\kappa}}{q\kappa} = \frac{\alpha^2}{a} \cdot \bar{\kappa}$

15. Soll $j_1, j_2 = a_3 j_3$ wegen Klasse sein

ist $j_1 j_2 j_3 = r^2$ mit $j_\alpha \mid r \mid j_\alpha j_\beta$.

$j_1 = a_2 a_3, \dots, \quad r = a_1 a_2 a_3$

16 Sei $K_1 K_2 = a_3 K_3^* + x_3 F$ und typisch.

dann ist $K_1 K_1^* = a_2 a_3 I + c_1 F$ "

$k_1^2 = a_2 a_3 + c_1 p$ "

$k_1 = a_2 a_3 + c_1$

$j_1 = a_2 a_3$

$k_1 (a_1 + x_1) = \text{typisch} = t = \text{const}$ Q

$a_1 c_1 + k_1 x_1 = \text{const}$

$k_1 k_2 = a_3 k_3 + x_3 p$

wenn $a_1 \le a_2 \le a_3$, so $a_2 a_3 < \frac{p}{4}$, daher $a_1, a_2 \sqrt{p}$

17 Jeder Teiler von $a_1 a_2 a_3$ ist 2^r-ter Restmod p

wenn $2^r \mid p-1$.

denn kein $q \mid a_1 a_2 a_3$ ist $= \bar{q}$ sonst jede Konjugierte q_i teilt,

$0 \le x_3 \le \begin{cases} k_1 \\ k_2 \end{cases}$ $\quad q_i \mid K \Leftrightarrow q_i \mid \bar{K}$

$k_1 (p - k_1) = a_2 a_3 (p-1)$ für $q \mid K$, $q \nmid \bar{K}$

Ersetzung von k durch $p-k$ oder

zyklische Vertauschung ergibt

entweder $\{a_1, a_2, a_3\} \to \{a_1, a_2, a_3\}$

oder $\to \{a_1, a_2, a_3'\}$

245

18. $kl - am = xp \Rightarrow |a| < \begin{cases} k^{2/3} \\ e^{1/3} \end{cases}$ oder $\Pi = 0$ (" $x(\ldots) = 0$ ")

$k(p-l) + am = (k-x)p$

$(p-k)l + am = (l-x)p$

$(p-k)(p-l) - am = (p-k-l+x)p$

oder $x \simeq \frac{kl}{p}$.

$x_3 \simeq \frac{k_1 k_2}{p}$

$x(k-x)(l-x)(p-k-l+x) \equiv 0 \mod a^3 m^2$

wenn $\Pi := kl \neq 0, \ldots$ $\quad |a^3 m^2| \leq k^2 l (p-l)$ wenn $k < l$

da $m \to p-m$ nichts an $|a|$ ändert, folgt

$|a^3| \left(\frac{p+1}{2}\right)^2 \leq k^2 l \frac{p-1}{2} \frac{p-1}{2}$

$|a^3| \leq k^2 \quad |a| \leq k^{2/3}$, ebenso

$|a| \leq l^{2/3}$

$|a_1| \leq |a_2| \leq |a_3| \Rightarrow |a_1| \geq p^{1/4}, \quad |a_2| \leq \frac{1}{2}\sqrt{p}, \quad |a_3| \leq \left(\frac{p}{12}\right)^{2/3}$

$|a_1 a_2 a_3|^2 = j_1 j_2 j_3 < \frac{p^3}{4^3}$

$|a_1 a_2 a_3| < \frac{p^{3/2}}{8}$

---

19. Der Automorphismus $g \to g^{KT}$ der Ordnung 2 von $\langle g, g^{KT} \rangle$ läßt ein Element eines 2-Sylow-Zentrums fest. Untersuchen?!

(11) Sei $l(\eta) = a_1 x_1 + a_2 x_2$, so ist für $0 \le i \le q = p-1$

$$l_{(\eta)}^{i} \wedge \left(x_1^{q} x_\nu^{q} \left(\frac{\partial'}{\partial x_1} + \frac{\partial^\nu}{\partial x_\nu} \right) \right) = -i\, l_{(\eta)}^{i-1} \cdot l(\eta', \eta_\nu)$$

(Verallgemeinerung der Differentiation)

(12) $f := \sum_\varrho{}' l_\varrho(\eta)^q$, $h := f \wedge \left(x_1^q x_\nu^q \left(\frac{\partial'}{\partial x_1} + \frac{\partial^\nu}{\partial x_\nu} \right) \right) \Rightarrow$

$$h^2 \Big|_{x_1^{q-2} x_2^{q-2}} = 2 \cdot \sum_{\varrho,\sigma} \frac{\beta_\varrho \beta_\sigma\, l_\varrho(\tau) \cdot l_\sigma(\tau)}{} \cdot \Delta_{\varrho\sigma}^{q-2}$$

$l_\varrho = a_\varrho x_1 + \beta_\varrho x_\nu$

$\tau := (\eta', \eta^\nu)$

$$\Delta_{\varrho\sigma} = \begin{vmatrix} \alpha_\varrho & \beta_\varrho \\ \alpha_\sigma & \beta_\sigma \end{vmatrix}$$

(13) Wenn $f(\eta) \in \mathfrak{i}\mathfrak{m}\, \mathfrak{G}_0$, dann $\sum f(\eta - t) f(\eta_1 - t) f(\eta_2 - t) =: {}^3f$ $\in \mathfrak{i}\mathfrak{m}\, \mathfrak{G}$.

Iterierte man auf $f = \sum' l_\varrho^q$ anwd. $\mathfrak{G}$ zweimal $\not\equiv 0$

(14) $$\sum_t t_1^\alpha t_2^\beta = \begin{cases} 1 & \alpha \text{ mal } \beta \text{ prv.-Vielfache von } q \\ 0 & \text{sonst} \end{cases}$$

(15) Von r^2 q-Produkten $l_\varrho^\alpha(\eta)\, l_\sigma^{q-\alpha}(\eta_\nu)$ $\quad \alpha = 0 \cdots q-1$

sind $\binom{r}{\alpha}$ ungleich, wenn $|\nu| \le q$.

Sei ϱ_0 max. α ($\ne 0$)

$$\sum c_{\varrho\sigma} l_\varrho^{\alpha} l_\sigma^{q-\alpha}(\eta_\nu) = 0 \overset{(11)}{\Rightarrow} \sum c_{\varrho\sigma} l_\varrho(\tau) \cdots$$

(17) $\mathfrak{A}$ sei $f = \sum_{\varrho=1}^{r} l_\varrho(\eta)^q$, $\mathfrak{A}$ ist $r(r-1) \ne p-2$ und Polynom invariant

$\mathfrak{A}$ linear

Bem: $\Sigma t g(t) = \sum_{g \in G} t_g g$ Polynom vom Grad p: Burnside-Lemma.

(1) $\exists$ invariante $f(x) = \sum_0^n a_\nu x^\nu$ $0 \le n < p$, wenn $G \neq E$ trans, $a_n \neq 0$

(2) $\Sigma t \mid f(x^g - t) \cdot f(x - t^g) = a_n(x-t^g)^n + a_{n-1}(x-t^g)^{n-1} \cdots$

$= a_n(-t) + \text{const}(t)$ $\quad c = \Sigma t f(x - g(t))$

Koeff von x^{n-1} in f^n $= \# x^n \cdot \cdots + x^{n-1}\left[a_n n \sum_t t - a_n \sum_t t\, g(t)\right]$

ist Konst $\neq 0$, also

$\text{Koeff}_{x^{n-1}} = \text{Koeff}_{t^n \text{ in } g(t)} \sum_t t g(t) = 0 \qquad x \perp g, \forall g$

A. Lemma: $\forall g \in G$, $\Sigma t g(t) \neq 0$ $\forall g \in G \Leftrightarrow G = C_p$.

Bew: (3) Aus $F(x) \perp g(x)$, $\forall g \in G$ folgt $F(h(x)) \perp g(x)$, $F'(x) \perp g(x)$, $\forall$ gr $h \le$ gr F

(3) $h(x) \perp g(x)$ $\forall g, h \in G$

(4) $m = \max \text{grad } g \Rightarrow 2m < p-1$

(5) $1, x, x^2, \ldots, x^{\frac{p-1}{2}} \perp g(x)$ $\forall g$

(6) $h^\kappa \perp g$ $\forall g, h$ $\quad \kappa = 0, 1, \ldots, \frac{p-1}{2}$

grad Gr $h^\kappa < p-1-m$ $\quad 0 \le \kappa \le \frac{p-1}{2}$

also $\kappa m < p-1-m$ wenn $\kappa m \le p-1$, $0 \le \kappa \le \frac{p-1}{2}$

(7) Wäre $m \ge 2$, so $\exists\, \kappa$: $0 \le \kappa \le \frac{p-1}{2}$ $\quad p-1 = \kappa m + r$ $\quad 0 \le r \le m$

$\kappa m \le p-1$ $\quad \kappa m < p-1$, $m = p-1-\kappa m \Rightarrow m$

Folge B

(1) Für f

(2) $(G^H)^g =$

(3) $G^H \le G$

(4) $x \in G^H \Rightarrow$

(5) $x \in G^H \Rightarrow$

(6) $x \in G^H =$

(7) $\bigcap H^x$

$H^x \neq H^y$

Folge

(a) die Relation

, wobei, d

(b) Invariant

(c) für nicht Σ

$F(x,y) := \Sigma f$

(d) wenn f ex

$x \to \varphi(x)$

Bew: zu

$= 0 \neq 1$ Σ

$\bigcap H^x H^y$

Für $H \leq G$ definiere ${}_G^{\bullet}H = \bigcap_{x,y \in G,\ H^x \neq H^y} H^x H^y$

(1) ${}_G^{\bullet}H$

(2) $({}_G^{\bullet}H)^g = {}_G^{\bullet}H$, $\forall g \in G$

(3) ${}_G^{\bullet}H \leq G$. $u, v \in {}_G^{\bullet}H$ $u = h_1^x h_2^y$, $v = h_3^y h_4^x$ $uv = h_1^x (h_2 h_3)^y h_4^x$

(4) $x \in {}_G^{\bullet}H \Rightarrow H^x = H$ denn $x \in HH^x$, Widerspruch

(5) $x \in {}_G^{\bullet}H \Rightarrow (H^y)^x = H^y$ (4)

(6) $x \in {}_G^{\bullet}H \Rightarrow x \in H$ denn $x \in H^x$ $x = x^{-1} h x$ $x = h$

(7) $\bigcap_{H^x \neq H^y} H^x H^y = \bigcap_{x \in G} H^x$ (6)

Ideen für Grad p's

(a) die Aktion von KT anschauen, Involutionen suchen, die nicht fest lassen.

(b) Invarianten $f(x_1, x_2, x_3)$ suchen.

$$\sum_t f_{\#}(x_1 - t) f_{\#}(x_2 - t) f(x_3 - t)$$

(c) für nicht 3-fache Gruppen: $\exists f(x,y)$ invariant unter C_p, aber für irgendeinen $g \in G$, $F(x,y) := \sum f(x - tg, y - t) \cdot \varphi(t)$ hat $\operatorname{grad} f(x^g, y^g) \leq \operatorname{grad} f(x,y)$ für φ vom Grad $\leq \frac{p-1}{2}$

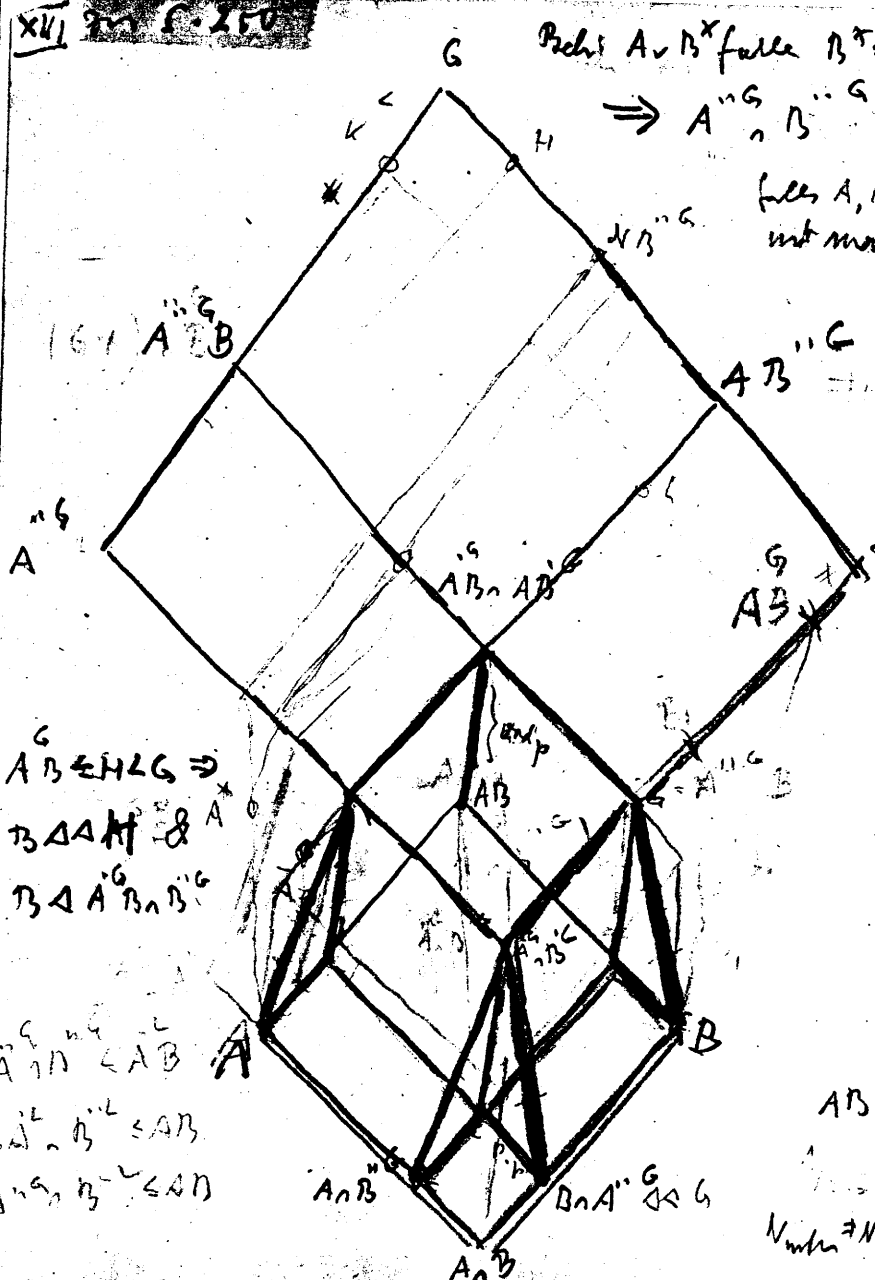
(d) wenn f nicht gesamtgrad $< p-1$, so ist $x \to \varphi(x)$ linear, aber für fast alle p keine Permutation von F_p genau wenn $\sum_{t=0}^{p-1} \varphi(t)^{\nu} = 0$ für $\nu = 0, 1, \ldots, p-2$ und $\varphi(t) \neq \text{const}$.

Bew: wenn vielfach mit x_α von x im Werte vorkommt, φ $\sum x^\nu x_\nu = 0$ für γ verschiedene x's, $r < p-1$ $x_\nu \equiv 0$

ω-Untergruppen.

Aufgabe: Untersuche die ω-Verwandten von G, das sind die Untergruppen von G, die zu jeder ω-Untergruppe von G eine konjugierte enthalten.

XVII Zu S. 250



Recht: $A \vee B^x$ falls $B^x \leq B^{\cdot G}$

$\Rightarrow A^{\cdot G} \cap B^{\cdot G} \leq AB$

falls A, B gegenseitig mit maximalem $|A|+|B|$

$(AB)_G = 1$

$A^{\cdot G} B^{\cdot G} = G$

$B \trianglelefteq A^{\cdot G} B$

$A^{\cdot G} B \leq H < G \Rightarrow B \trianglelefteq H$

$A^{\cdot G} \leq H < G \Rightarrow A \trianglelefteq H$

$A^{\cdot G} \cap B^{\cdot G} \leq AB$

$A^* \cap B^{\cdot G} \leq AB$

$A^{\cdot G} \cap B^{\cdot G} \leq A^* B$

$A^* B \cap B^* A \trianglelefteq A, B$

$A^* \cap B^{\cdot G} \leq AB$

$A^* B \cap B^* \in AB$

$A^{\cdot G} \cap B^{\cdot G} \leq A^* B \cap B^* \leq AB$

$= |A \cap B^{\cdot G}| \leq AB$

$A \trianglelefteq N B$ wenn $N \neq G$, $N \trianglelefteq B$ wenn $B \trianglelefteq K$ wenn $A^{\cdot G} \leq K < G$

normal

$AB \leq H < G \Rightarrow A \trianglelefteq H$ oder $B \trianglelefteq H$

$N_{\min} \neq N' \Rightarrow N \leq A \cap B^{\cdot G}$

Wenn $AB^{\cdot G} \cap K \leq AB$, $A^{\cdot G} \cap B \trianglelefteq A$, $A \cap B \trianglelefteq A$, $B^{\cdot G} \cap A \trianglelefteq A$, $A^{\cdot G} \leq A$, AB wenn $B \supset B$

Vereinbarung: G endl; (oder σmax sgp), $A, B \leq G$,

$(\forall x,y \in G \ (\text{oder } \forall x \in A^{\cdot\cdot G}, y \in B^{\cdot\cdot G}) \ A^x \vee B^y) \Rightarrow A^{\cdot\cdot G} \wedge B^{\cdot\cdot G} \leq AB$.

das Segenbeispiel 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 $A^{\cdot\cdot G} \cdot B^{\cdot\cdot G}$ konj in G

(2) $A \wedge B^{\cdot\cdot G} \trianglelefteq A^{\cdot\cdot G} \wedge B \trianglelefteq G$

(3) $A^{\cdot\cdot G} \wedge B^{\cdot\cdot G} \mid A^{\cdot\cdot G} \wedge B^{\cdot\cdot G} \wedge AB = p$ Primpotenz

(4) $M \wedge B \trianglelefteq G$ wenn $A \leq M \trianglelefteq G$.

(5) N min $\trianglelefteq G \Rightarrow |N : N \wedge AB| = p$, $|M = p^{\nu}$.

Beweis mit

(6) $d_G C = 2$, $C \leq D < G \Rightarrow D \cdot C^G < G$

Induktion anwenden auf 1 Kompl. perfekte C; $D \trianglelefteq A$ oder B

(7) $AB \leq H < G \Rightarrow A \trianglelefteq H$ oder $B \trianglelefteq H$

Beweis: $A^{\cdot\cdot H} > A$ $B^{\cdot\cdot H} > B$

Mod $\begin{cases} (A^{\cdot\cdot H})^{\cdot\cdot G} \wedge B^{\cdot\cdot G} \leq A^{\cdot\cdot H} B \\ A^{\cdot\cdot G} \wedge (B^{\cdot\cdot H})^{\cdot\cdot G} \leq A B^{\cdot\cdot H} \\ A^{\cdot\cdot H} \wedge B^{\cdot\cdot H} \leq AB \Rightarrow A^{\cdot\cdot H} \trianglelefteq AB \leq AB \end{cases}$

dann $A^{\cdot\cdot G} \wedge B^{\cdot\cdot G} \leq (A^{\cdot\cdot H} \wedge B)(A \wedge B^{\cdot\cdot H}) = (A^{\cdot\cdot H} \wedge B^{\cdot\cdot G})(A^{\cdot\cdot G} \wedge B^{\cdot\cdot H})$

$\leq AB$

und $\triangleleft\triangleleft$

8. $A^x \leq A^{\sim G}$, $B^y \leq B^{\sim G} \Rightarrow A^x \leq \mathcal{N}B^y$, $B^y \leq \mathcal{N}A^x$

Satz 9: $AB \neq G$, $A^x \vee B^y$ $\forall x,y \Rightarrow A^G \cap B^A < G$ oder $AB^G < G$.

Folge: 10 $A^x \vee B^y \Rightarrow \begin{cases} A^{AB} \cap B^{AB} \trianglelefteq G & \text{da } \triangleleft\triangleleft\ A^{C} B^{C} = \\ A^{B^G} \cap B^{A^G} \trianglelefteq G & \text{da } B^{AG} \leq \mathcal{N}AB^G \end{cases}$

und damit auch $AB^G \cap B^{AG} \trianglelefteq G$

Satz 11: $AB \neq G$, $A^x \vee B^y \Rightarrow \begin{cases} A \cdot B^A \neq G \ \& \\ B A^{B^G} \neq G \end{cases}$ $\forall x,y$

Note: $11 \neq 9$

Bew.: Wähle $\bar{B}$ maximal

$\bar{B} = \langle B, B^{x_1}, \ldots \rangle$, $A\bar{B} \neq G$.

Dann $A \leq \mathcal{N}\bar{B}$, aber

auch $A \leq \mathcal{N}\bar{B}^b$, $\forall b \in G$: denn

sonst $B^{x_i} \langle \bar{B}^a, \bar{B}^{ta} \rangle > \bar{B}^t$

$A B^{x_i} = A \bar{B}^b \neq G$

nun $A \cdot B^{x_i t^{-1}} \neq G$, $\bar{B} < B^{x_i t^{-1}}$.

Also $A^x \leq \mathcal{N}\bar{B}$ $A^G \leq \mathcal{N}\bar{B}$

$A \cdot B^{AG} \leq A\,\bar{B}^{AG} = A\bar{B} \neq G$.

(* oder Verk. d. Transversalen)

Klarer und schneller Aufgewandt bis Satz 12 einschließlich:

Satz 12. $A^x \vee B^y$ $\forall x,y \in G$, $AB \neq G \Rightarrow$

$A^{B^G} \cdot B^{AG} \neq G$, $A^{B^G} \cap B^{A^G} \trianglelefteq G$. $(\neq 10)$

Frage: $A^{\sim G} \cap B^{\sim G} \leq$?

Vermutung: Genügt $x \in A^{\sim G}$, $y \in B^{\sim G} \Rightarrow A^y \vee B^x$

$9'$: $A^x \vee B^y$,

Satz 13: $a_1 \ldots N' < N$

Beh.: b) $\ldots N_n$

Frage 14: a) W_i

15. Def.: für

Dann gilt

16. Frage: A^x

SATZ: Entha

16. $A^x \vee$

Bew.:

NB: Klar: $A^B \cap B$

FRAGE: ja ?

G: $A^x \vee B^y$, $AB \neq G$ $\Rightarrow$ entweder $A^{\overline{G}} B^A \neq G$ oder $B^{\overline{G}} A^B \neq G$

Satz 13 a) Sei $N < N_{min} \trianglelefteq G$, $A < G$, $A \cap N \neq 1$, dann ist $AN < G$.

Vfg: b) Sei $N_{min} \trianglelefteq G$, $A < G$, $A \cap N \geq$ nichttrivialer Teil von N,

Dann ist $AN < G$.

Frage 14: a) Was folgt aus $A^x \leq N_B$ $\forall x \in G$?

b) " " " $B \leq N_{A^x}$ " ?

15. Def: Für $A, B \leq G$ setze $A^{\cdot\cdot B} = A^{\cdot\cdot \langle A, B \rangle}$.

Dann gelt: $A^{\cdot\cdot B}$ ist monoton $\nearrow$ in A, B.

$$\langle A_1, A_2 \rangle^{\cdot\cdot B} \geq \langle A_1^{\cdot\cdot B}, A_2^{\cdot\cdot B} \rangle$$

16. Frage: $A^x, B^y \Rightarrow A^{\cdot\cdot G}, B^{\cdot\cdot G}, AB \trianglelefteq G$?

SATZ: (Enthält Kegel und mehr) B^G (negativ: $A^{A^x} = \langle B$)

16. $A^x \vee B^y \Rightarrow \begin{cases} A^{B^A} = A^B \\ AB, B^A \trianglelefteq G \end{cases}$ wenn A, B genügend klein

Bew: wenn $AB = G$, ist $1.S. = A^{\langle AB \rangle} = A^B$, und $= A^{B^A}$

wenn $AB < G$, so ohne $A^G B =: H < G$ (11)

$$(1.S.)_H = A^{B \cdot\cdot B^H} \leq A^{B \cdot\cdot B^G}, \geq A^{B \cdot\cdot B^{A^G}} = (1.S.)_G$$

und: $(1.S.)_H = A^B$

NB: Klar: $A^{B^{A^{-G}}} \geq D^{D^{-G}, H}$, $D = A \cap B$, also $D^G \leq A^D$, $D^{-G} = D^{-B}$

FRAGE: Ja/Nein für beliebige A, B in G stets $A^{\cdot\cdot G}, B^{\cdot\cdot G} \trianglelefteq G$?

25 Vertauschbarkeit & Subdirektprodukte 29.11.65

(1) $(A,B,G) := \lim A^{B^n}$ (n→∞ naiv = ... (n=N)) für diese Folge fällt monoton

(G endlich; klappt auch in G mit Mühe) $\langle A,B\rangle$

(2) $(A,B,G) = (A^{\langle A,B\rangle},B,G)$

(3) $\bar{A} = (A\,B\,G)$, $\bar{B} = (B\,A\,G)$ sind die umfassenden Untergruppen von G mit $\bar{A} = A^{\bar{B}}$, $\bar{B} = B^{\bar{A}}$ s.o. 6 p 254

Frage: auch für "≤"?

Vor Weiter nämlich (3) ob $A \leq NB$ & $B \leq NA$

(4) $(A,B,G) = (A,B,H)$ für $H_1 = AB^G$
$H_2 = BA^G$
$H_3 = AB(A^G \cap B^G)$
$H_4 = AB(A^{\langle G}\cap B^{\langle G})$

(5) $(A,B,G) \cap (B\,A\,G) \trianglelefteq\trianglelefteq G$

Bf mindest. (4) mit H_3, nebst

(6) Wenn $G = AB^G \cap BA^G$, so $(A,B,G) = A^G$

Bew: $A^{\bar{B}^G} = A^{AB^G} = A^G$, $B^{A^G} = B^G$

(7) Kegel Wenn A^x, B^y, und $AB < G$, so $G^* = AB(A^{\langle G}, B^{\langle G}) < G$

(8) $(A,B,G)^\varphi = (A^\varphi B^\varphi G^\varphi)$ wenn $\varphi \in \hom G$

(schwach Sylowsätze: "existiert", eliminierend $(n=N)$

(9a) $(A\,B$

(9b) $(A\,A^c$

(9) Wenn

wird

Bew'

$\bar{A} =$,

denn

Aus $\{A, B\} \leq H$

(9') $\{A,$

(10) $A^B = A \Rightarrow A \cap ($

genügt: $A \cap B^A \trianglelefteq B^A$

denn $AB < G \Rightarrow (B\,A\,G)$

(9a) $(A\ B\ G)$ ist isotop in allen Variablen

(9b) $(A\ A\ G) = A^{\prime\prime G}$

---

(9) Wenn bei festem A, B ($\in N_A^B$ wohldefiniert) gesetzt wird $G^* := A^{BG} \circ B^{AG}$ und

$$H = G^{*\cdots *}$$ der Endglied der absteigenden Kette ist

so mit $\bar{A} = (A\ B\ G)$ und $\bar{B} = (B\ A\ G)$

$$\begin{cases} \bar{A} = A^H, \quad \bar{B} = B^H \\ H < A\bar{B} = B\bar{A}\ AB\,H = AB^H = BA^H \end{cases}$$

Denn: $H = AB^H = BA^H$ als Endglied v.

$$\bar{A} = A^{B^H} = A^{A\cdot B} = A^H$$

$$\text{dann } \bar{B} < B^H$$

Aus $\begin{matrix} A \\ B \end{matrix} \} \in H = AB^H = A\bar{B}$, dann $= B\bar{A}$ $\quad$ auch wenn $\begin{matrix} A \\ B \end{matrix} \notin N_B^A$

$A \in N(BAG)$, $B \in N(ABG)$ $\quad$ $* \cdots *$

(9') $\begin{cases} A \cdot (B\,A\,G) = B \cdot (A\,B\,G) = G \\ = (A\,B\,G)(B\,A\,G) \end{cases}$

(10) $A^B = A \Rightarrow A \cap (B\,A\,G) \trianglelefteq G$

$A \cap B^A \trianglelefteq B^A$

denn $AB = G \Rightarrow (B\,A\,G) = B^A$

$= D^{[G]}$ Bew.: $D^{[G]} = D^{[AB^G \cap BA^G]}$ wenn $[\ ] = G_{1,2}$ $\quad$ "poln" $\quad$ (Induktion) $\quad$ so $[\ ]$ auch

$D^{[G]} = A \cap B^G$ $\quad$ $\in A^G \cap B^G \trianglelefteq G$

Forts. XII, 10

$$|H| = \frac{|A|\,|\bar{B}|}{|A\cap\bar{B}|} = \frac{|\bar{A}|\,|\bar{B}|}{|\bar{A}\cap\bar{B}|}$$

Satz

(11) $\left\{\begin{array}{l} |\bar{A}\cap\bar{B}| = |A\cap\bar{B}|\cdot|\bar{A}:A| = \dfrac{|\bar{A}|}{|A:A\cap\bar{B}|} \left[\text{auch ohne } A \trianglelefteq N_{\bar{B}}^{\bar{B}}\right] \\ \bar{A}\cap\bar{B} \trianglelefteq G \end{array}\right.$

(12) Wenn $A^x \leq B^y$, so $G^{x\to x} = AB$ (Kegel)

(13) Vermutung: Wenn $A, B \leq G$ sind und $A \trianglelefteq B^x$ gilt für mehr als $\frac{1}{2}|G|$ Elemente $x \in G$, so ist $A \trianglelefteq G$.

Es reicht, wenn $A = A'$.

Denn $\vdash A, A^x \exists$ minimales $x \in G$

$\to$ $A, A^x \trianglelefteq B^y$.

also $A \vee A^x$, $A \trianglelefteq G$.

Satz Es gibt genau den größten Kern $A^* \trianglelefteq G$.

$\mathfrak{Z}(A)$ Anfangsteil, $= P \times Q \times \dots$

$\alpha \in \mathbb{N}$ $\left[P^\alpha, Q^\beta\right] = 1$, aber

$\left(P^\alpha, Q^\alpha\right] = 1$, aber P^G

Wenn $H < \overline{G} < G$, so hat

die Ver. für eine passende Konjugierte

von $\bar{G}$ (statt G) erfüllt.

Daß der "Subnormalteiler" $\mathfrak{F}A$ ($\subseteq G$)

enthält aber in jeder maximalen

echten Untergr. M von G eine Konjugierte.

Unabhängige Untergruppen

Lemma 1 $\{G_i\}_{i=1\dots n}$ unabh. $\Leftrightarrow \forall x_1,\dots,x_n \exists g \in \bigcap G_i : x_i$

Vielleicht bequemer: $\forall x_1 \dots x_n \in G \; \exists g \in G,\ g_i \in G_i \to g g_i = x_i$

Achtung: Aus Nur-Gleichungen mit neuem G_1 folgt nicht $\bigcap G_i$ ändert ⇒ aber Mehrfach: $1 \neq \langle G_1 \rangle \cdot \prod_{i>1} G_i$

2 eq: $x_i G_i \neq \bigcap G_i$

2½ ? $\{G_i\}_{i\in I}$ 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.

3½ G_1, G_2 un $G \Leftrightarrow G_1 G_2 = G$ Bew: $\bigcap H_i x_i \geq \bigcap G_i x_i \neq \emptyset$

Satz 4 Sei $\{G_i\}$ un G und $H \leq G$. Dann

$$\{G_i \cap H\} \text{ un } H \iff H \cap G_i = \bigcap H G_i$$

Falls Bezeichnung 16 IV (5) für $n=2$, $H \triangleleft G$, $\bigcap G_i \in H$.

Bew: $\Rightarrow$ $g \in \bigcap H G_i \to g \in H \cap G_i$

Bew: $g \in H g_i$ $\exists g_i \in G_i$

$y_i := g g_i^{-1} \in H$

$\exists\ h = h_i y_i \quad h_i \in H \cap G_i \leq G_i$

$= g g_i^{-1} y_i$

$g = h y_i^{-1} g_i = h d$ mit $d = y_i^{-1} g_i \in G_i$, $d \in \bigcap G_i$

$g \in H \cap G_i$

$\Leftarrow$ Sei $y_i \in H$ $\exists\ g = g_i y_i$, $g_i \in G_i$.

$g^{-1} = y_i^{-1} g_i^{-1} \in H G_i$, bis

$= h^{-1} d$, $d \in \bigcap G_i$, $h \in H$

$H \ni h = dg = d g_i y_i = h_i y_i$, $h_i \in H \cap G_i$

5 $\{G_i\}$ un G, $N_i := N G_i \Rightarrow N/K \cong \prod S_i/K$; $S_i = N \cap \bigcap_{j\neq i} G_j \cong N/N G_i$

Bemerkung: $K := \bigcap G_i$ $N := \bigcap N_i$ $\cong \prod N G_i / G_i$ für Bew: $4 : \{G_i \cap N\}$ un N

6 Ist G_i kompakt, [illegible] so ist $\bigcap_{i\in I} G_i$ und [illegible] alle G_i abgeschlossen, so gelten diese Sätze auch für unendliche Indexmengen $\{G_i\}_{i\in I}$ nur $G \Leftrightarrow$ jedes endl. Teilsystem ist nun G.

(Das obige gilt für beliebige Indexmengen!)

7 Für $A, B \subseteq I$ (= Indexmenge) definiere $G_A := \bigcap_{i\in A} G_i$ usw.

Dann $G_{A\cup B} = G_A \cap G_B$

$G_{A\cap B} = G_A \cdot G_B$

(endliche Vereinigung über beliebige von I muss man explizit reduzieren!)

Lemma (8) Zum Bew der zweiten Formel: Lemma: (Aufgabe) Das System $\{G_i \cap G_A\}_{i\in I}$ um G_A ist

um $x_i \in G_A \Rightarrow \exists\, g = g_i x_i$; $g_i \in G_i$ für $i \in A$ fest

$g = g_i \cdot x_i \in G_i$

$g \in G_A$.

Bew $\supseteq$: Nach 4 ist

$$G_A G_B = \bigcap_{b\in B} G_A G_b = \bigcap_{b\in B}\bigcap_{a\in A} G_a G_b = \bigcap_{a=b} = \bigcap_{c\in A\cap B} G_c$$

9 $\{G_i\}$ um $G \Rightarrow$ G wirkt simultan-transitiv auf

a) alle G/G_i; $\forall g \in G \to \cdot\, G_i g = G_i x_i$ · fixgegebene x_i

b) G wirkt simultan-transitiv auf den Klassen in G_i konjugierter Gruppen

Bew: $g_g x_i \in G \exists\, g \in G_i x_i$; $G_i \overset{g}{=} G_{x_i}$

10. unabhängige Untergruppen

$\{G_i\}$ in G ; $x_i, y_i \in G \Rightarrow \bigcap x_i G_i y_i \neq \emptyset$

Bew.: $H_i := x_i G_i x_i^{-1}$

$t \in \bigcap G_i x_i^{-1}$

$G_i t = G_i x_i^{-1} = H_i$

$\bigcap x_i G_i y_i = \bigcap H_i z_i \quad z_i = x_i^{-1} y_i$

$\exists t \in G \quad t \in \bigcap x_i G \quad x_i G = tG$

$\bigcap x_i G_i y_i = \bigcap t G_i y_i = t \bigcap G_i y_i \neq \emptyset$

Lemma (1) $N \triangleleft G$

G

(2) $N \triangleleft G,$

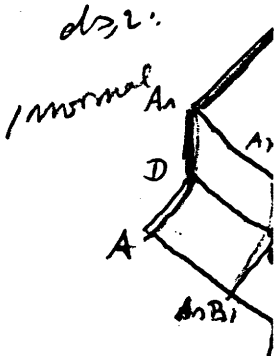
$A, B \triangleleft$

13) $N \triangleleft G,$

G/N

Satz (14) $A, B \triangleleft$

Beweis:



Bild

AA:

(1) $N \trianglelefteq G$, G/N perfekt, $A, B \leq G$,
$G = AN = BN \Rightarrow G = [A,B]N$
Kommutatoren

(2) $N \trianglelefteq G$, G/N perfekt, $A, B \leq G$,
$A, B \trianglelefteq \langle A, B\rangle$, $G = AN = BN \Rightarrow G = (A \cap B)N$

(3) $N \trianglelefteq G$, $A \trianglelefteq G$, A minimal mit $AN = G$,
G/N perfekt $\Rightarrow A \trianglelefteq G$

$A \trianglelefteq G = \langle A, B^G\rangle$ und $G = \langle A, B\rangle$

(Satz 4) $A, B \trianglelefteq G$ G/B^G perfekt, $d_G A \leq 2$, $G = \langle A, B\rangle$
$\Rightarrow G = AB = BA$
Frage: auch für $d_G A > 2$

Sei $A \not\trianglelefteq G$.
Beweis: Ind $d_G B = d$. $d \leq 1$ trivial.

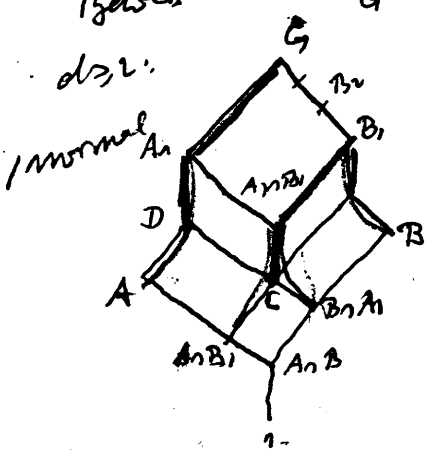


Bild 1

$d \geq 2$:
Nach Ind.-Vor. ($B \to B_1$)
$G = AB_1$
Ferner $G = A^1B$, da $G = \langle A, B\rangle^G$
mod $A, B \trianglelefteq G$.
Es gilt Bild 1.

Fall I: es $N \trianglelefteq G$, $N \subseteq AB$
$C \leq D$ folgt $N = 1$
$\forall b_1 \in B_1$ ist $C = C^{b_1} \leq D^{b_1}$
$\forall g \in G \; \exists b_1 \in B$ s.t. $D^g = D^{b_1}$
$C \leq D^g$ $\forall g \in G$
$C^g \leq D$ $C^G \leq D \leq AB$ $C = 1$ $C \trianglelefteq G$

260 Satz: $A \cap B_1 = 1 \quad G = AB_1$

Beh: $A \trianglelefteq G$ angenommen (nicht beh trivial),

$\exists\, A^g \Rightarrow \cdot \quad A \cap A^g < A$

Da $A, A^g \leq A_1$, folgt nach 2. Isom.

$$(A \cap A^g)\, B^G = G$$

Daher nach Ind: $G = (A \cap A^g) \cdot B_1$

Denn $A \leq (A \cap A^g) \cdot B_1$

$$A = (A \cap A^g) \cdot (A \cap B_1)$$
$$= A \cap A^g \quad \text{wegen } A \cap B_1 = 1$$

Widerspruch

Fall II: $\exists\, N \trianglelefteq G,\ N \leq AB$. Beweise

(5) Lemma: $A, B \leq G$; $N_\lambda \trianglelefteq G$, $N_\lambda \subseteq AB$

$(\lambda \in \Lambda)$ $\Rightarrow \left[\prod_{\lambda\in\Lambda} N_\lambda\right] \subseteq AB = AB \cdot \prod N_\lambda$

Bew: $|\Lambda| = 2$: $n_\lambda \in N_\lambda \quad n_1 = a_1 b_1$

$$n_1 n_2 = a_1 a_2 n_2$$
$$= a_1\, n_2' b_2 \in AB$$
$$= a_1 (a_2' b_2') b_2 \in AB$$

$|\Lambda| < \infty$ Induktion.

$|\Lambda| = \infty$: $x \in \prod N_\lambda \Rightarrow x \in \prod^{\text{fin}} N_\lambda$.

Damit Beweis Fall II:

Wähle $N := \prod N_\lambda$, $N_\lambda \trianglelefteq G$, $N \subseteq AB$

Dann gilt

$G = \langle$

Satz (6): A

Beweis Induktion

$d = 1$ trivial

Fall $d = 2$

G

Fall $d > 2$:

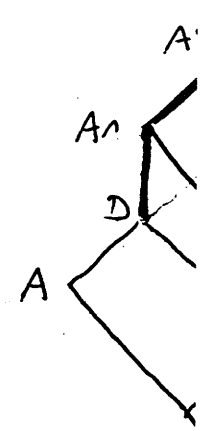


Fig 2.

Dann gilt für $\bar{G} = G/N$:

$\bar{G} = \langle \bar{A}, \bar{B} \rangle$; $\bar{N} \subseteq \bar{A}\,\bar{B}$, $N \trianglelefteq \bar{G} \Rightarrow \bar{N} = 1$;

$\bar{G}/\bar{B}^{\bar{G}}$ perfekt. $d_{\bar{G}}(\bar{A}) \leq 2$, $d_{\bar{G}}\bar{B} \leq d$.

Aus nach Teil I: $\bar{G} = \bar{A}\bar{B}$.

Das heißt $G = AN\,B = AB$

Satz (6): $A \trianglelefteq G$, $B \trianglelefteq G$, $G = \langle A, B \rangle$,

$A \subseteq A'B \Rightarrow G = AB$

Aq: $A/(A\cap B)$ perfekt

Bew Induktion $d = d_G A$, beispielsweise d nach $d_G B$.

$d_G B \leq 1$ trivial

$d = 1$ klar

Fall $d = 2$ folgt aus (4): für $N \trianglelefteq B^G$, N

$\therefore\ G'N \geq A'N = \langle A, B \rangle = \langle A, B \rangle = G$

also G/N perfekt.

$\Rightarrow$: Nebl $A/A'(A\cap B) \perp B/B'(A\cap B)$.

Fall $d > 2$: Nach Induktion ist $G = AB_1 = A_1 B$

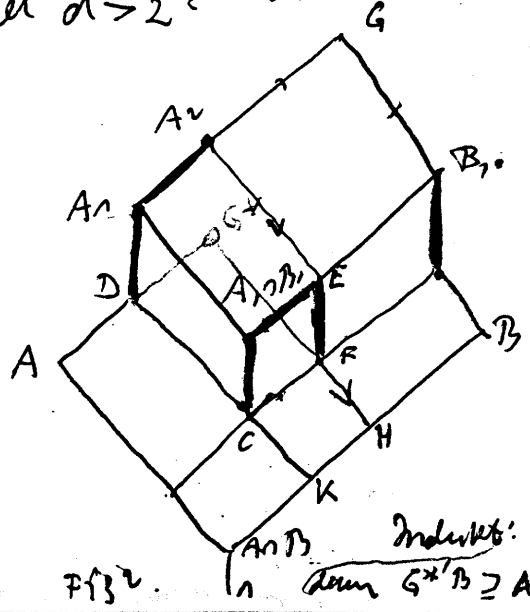


Fig 2.

ferner für $G^* := \langle A, H \rangle$:

$G^* = AH = AKH = DH$

denn

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

$= A'(A\cap H) \subseteq A'H$

$N G^* \geq A_1 \cap B_1$, [redacted]

D, A_1; $A_1\cap B_1$, F, E;

A_1, E, A_2 also

$G^* \trianglelefteq A_2$ $d_G G^* \leq d_G A - 1$

Induktion: $G = G^* B = AHB = {}^G AB$

denn $G^* B \supseteq A'B \supseteq A$, also $G^* 1 \supseteq AB \supseteq AH = G^*$.

262

(7) Vermutung (7):

$A, B \trianglelefteq G, \quad A/(A\cap B)A' \oplus B/(A\cap B)B' = 0$

$\Rightarrow AB = BA$

NB Kontrollen für $A \circ B = 0$ siehe Fuchs, Bush Chap. XI

(8) Frage: Gibt es Vertauschungssätze der Art:

wenn $A, B \trianglelefteq G$, wann $[A, \dots, A]_p \vee B$

wenn $R = f(d_G A)$?

Perm. Fortsetzung regulärer Untergruppe

Satz G top. Gr., $\mathfrak{g} \subset G$, $\mathfrak{g}$ additive Untergruppe. Sei $\mathfrak{R} \subseteq G$ Sei f_0 eine bei G_0 invariante Funktion

$$f_0 : \mathfrak{g} \to R \quad (= \text{Ring})$$

Sei $\mathfrak{F}$ eine bei $\mathfrak{R}$ inv. Menge von Fkt. $f : \mathfrak{g} \to R$.

Dann ist $f_0 \wedge \mathfrak{F}$ $(:= \{ f_0 \wedge f \mid f \in \mathfrak{F} \})$ invariant bei $\mathfrak{R}$.

Bew.: Sei $\varphi \in f_0 \wedge \mathfrak{F}$, $u \subset \mathfrak{R}$

$$\varphi(x) = \sum_\xi f_0(x-\xi) f(\xi)$$

$$\varphi|u(x) = \sum_\xi f_0(u(x)-\xi) f(\xi)$$

$$= \sum_\xi f_0(u(x)-u(\xi)) f(u(\xi))$$

$$= \sum_\xi f_0((t_{u(\xi)} u)(x)) f(u(\xi)) \qquad t(x) := x - \xi,\ b_\xi \in \mathfrak{g}$$

Nun ist aber

$$(t_{u(\xi)} u)(x) = (h_\xi t_\xi) x \quad \text{mit } h_\xi \in G_0$$

denn $0 = (t_{u(\xi)} u)(\xi) = (h_\xi t_\xi)(\xi) = h_\xi t_\xi(\xi) = h_\xi 0$

Also

$$\varphi|u(x) = \sum f_0(h_\xi(x-\xi)) f(u(\xi))$$

$$= \sum f_0(x-\xi) f(u(\xi))$$

$$= \sum f_0(x-\xi) \bar{f}(\xi), \quad \bar{f} \in \mathfrak{F}$$

$$\in f_0 \wedge \mathfrak{F}.$$

Körperer Beweis: 199 (1)

3.1.66
264

Perm Gr von Grad p

(1) Ist m der kleinste unter den Graden der bei G invarianten Funktionen modulo
$|G|_m = \max(|G|_f, f(x_m))$,
so sind alle Grade $0, m, 2m, \dots, p^{n-2}, p^{n-1}$
es ist $m \mid p^n - 1$

Bew.: Grad $x^t = p^{n-2}$ Grad x_m, wenn $m \nmid t$

(2) $2i$ sei der kleinste unter den Graden der Invarianten von G_0, so sind
$0, i, 2i, \dots, p^{n-1}$ alle Grade von Invarianten

(3) Es gibt keine invariante Form vom Grad i / bzw. Determinante
hat Grad i.

(4) ~~Satz~~ Ist G nicht 2-tra, so ist $2 \le p-1$

aber $m \mid i \mid p-1$, $m \mid p^n - 1$
aber auch $m \mid p^n - 1$

aber $\underline{m = 1}$; da χ linear, $\forall g \in G_0$

Variante:

(3') Grad $f = i$, f inv $G_0 \Rightarrow$ deg f_n alle $f_{nk} = i$
deg f_n alle $f_{nk} = i-1$

(4') $\exists f$ nicht $1 \le i \le p-2$, so existieren G-Moduln
nicht Grad $i, i-1$, aber nicht $2 \mid i$ $m \mid (i-(i-1))$
$m = 1$

Dann bei dieser Variante die Dimensionen der G-Moduln angeben.

(5) Allg.: Falls nicht Invar. von G_0 ist G-Modul-Homomorphismus
(entsteht durch χ) und umgekehrt
Endom