Invent. math. 70, 71–98 (1982)

*Inventiones mathematicae*


# Die Struktur der absoluten Galoisgruppe p-adischer Zahlkörper

Uwe Jannsen und Kay Wingberg

Fakultät für Mathematik, Universität Regensburg, Universitätsstr. 31, 8400 Regensburg, Bundesrepublik Deutschland

Das Ziel dieser Arbeit ist die Beschreibung der absoluten Galoisgruppe $G_k$ eines p-adischen Zahlkörpers $k$ über $\mathbb{Q}_p$, $p \neq 2$, durch Erzeugende und Relationen.

Nach Hasse [4] und Iwasawa [5] besitzt die Galoisgruppe $\mathcal{G} = G(T/k)$ der maximalen zahm-verzweigten Erweiterung $T$ von $k$ Erzeugende $\sigma$ und $\tau$ mit der definierenden Relation $\sigma\tau\sigma^{-1} = \tau^q$, $q$ die Mächtigkeit des Restklassenkörpers von $k$. Die Gruppe $\mu_T$ der Einheitswurzeln von $p$-Potenz-Ordnung in $T$ hat eine endliche Ordnung $p^s$, $s \geqq 1$, und die Operation von $\sigma$ und $\tau$ auf $\mu_T$ wird durch zwei Zahlen $g, h \in \mathbb{Z}_p$ gegeben derart, daß

$$\zeta^\sigma = \zeta^g, \zeta^\tau = \zeta^h$$

für $\zeta \in \mu_T$. Bezeichnet schließlich $n$ den Grad von $k$ über $\mathbb{Q}_p$, so läßt sich unser Hauptergebnis wie folgt formulieren.

*Die Gruppe $G_k$ ist isomorph zu der pro-endlichen Gruppe mit $n+3$ Erzeugenden $\sigma, \tau, x_0, \ldots, x_n$ und den folgenden definierenden Bedingungen bzw. Relationen:*

A) *Der von $x_0, \ldots, x_n$ erzeugte Normalteiler ist eine pro-p-Gruppe.*

B) *Die Elemente $\sigma$ und $\tau$ erfüllen die „zahme" Relation*

$$\sigma\tau\sigma^{-1} = \tau^q.$$

C) *Darüber hinaus genügen die Erzeugenden nur noch einer weiteren Relation:*

i) *für gerades $n$*

$$x_0^\sigma = (x_0, \tau)^g x_1^{p^s} [x_1, x_2] [x_3, x_4] \ldots [x_{n-1}, x_n],$$

ii) *für ungerades $n$*

$$x_0^\sigma = (x_0, \tau)^g x_1^{p^s} [x_1, y_1] [x_2, x_3] [x_4, x_5] \ldots [x_{n-1}, x_n].$$

*Hierbei ist*

$$(x_0, \tau) = (x_0^{h^{p-1}} \tau x_0^{h^{p-2}} \tau \ldots x_0^h \tau)^{\frac{\pi}{p-1}}$$

0020-9910/82/0070/0071/$05.60

*gesetzt* ($\pi$ *das Element aus* $\hat{\mathbb{Z}}$ *mit* $\pi\hat{\mathbb{Z}}=\mathbb{Z}_p$), *und es ist* (*im Fall* ii)) $y_1$ *ein Element aus der von* $x_1$, $\sigma$ *und* $\tau$ *erzeugten Untergruppe, dessen explizite Gestalt weiter unten angegeben wird.*

Setzt man in den Relationen $\tau=1$, so erhält man die Galoisgruppe der maximalen Erweiterung ohne zahme Verzweigung von $k$, wie sie von Koch in [12] beschrieben wurde.

Erzeugende und Relationen für $G_k$ wurden auch von Jakovlev in [6] angegeben, wobei aber mehrere Fehler eine umfassende Korrektur nötig machten. Diese wurde nur für gerades $n$ in [7] skizziert und ergab eine sehr komplizierte Relation in Form eines rekursiv gebildeten Limes. Überdies geht Jakovlev von drei Relationen für $G_k$ aus, während in dieser Arbeit und in [11] gezeigt wird, daß *zwei* genügen.

Der Beweis des Satzes wird in der folgenden Weise geführt. Es gibt eine im wesentlichen auf der lokalen Klassenkörpertheorie beruhende, kohomologische Charakterisierung der absoluten Galoisgruppe p-adischer Zahlkörper, die auf Koch [14] zurückgeht. Die Gruppe $G_k$ wird als sogenannte Demuškin(gruppen)formation über $\mathcal{G}$ gekennzeichnet, wobei der in [14] formulierte und in [19] ausführlich bewiesene Eindeutigkeitssatz besagt, daß zwei Demuškinformationen isomorph sind, falls die ihnen zugeordneten numerischen Invarianten übereinstimmen. Wir zeigen nun, daß die durch die obigen Erzeugenden und Relationen abstrakt definierte Gruppe eine Demuškinformation ist und durch die Wahl von $n$, $s$, $g$ und $h$ die gleichen Invarianten wie $G_k$ besitzt.

Da es sich bei pro-endlichen Gruppen um topologische Gruppen handelt, sind im folgenden alle Begriffe wie Untergruppe, Homomorphismus, Erzeugung, definierende Relationen usw. stets im topologischen Sinne zu verstehen.

## § 1. Definition von Demuškinformationen und Hauptresultate

*1.1.* Bezeichne $q=p^{f_0}$ eine Potenz der ungeraden Primzahl $p$ und $\mathcal{G}$ die pro-endliche Gruppe mit Erzeugenden $\sigma$ und $\tau$ und der definierenden Relation

$$\sigma\tau\sigma^{-1}=\tau^q$$

oder eine Faktorgruppe davon, deren Ordnung von $p^\infty$ geteilt wird.

**Definition** (Koch [14]). Seien $n, s \geqq 1$ natürliche Zahlen und $\alpha\colon \mathcal{G}\to(\mathbb{Z}/p^s)^*$ ein Charakter von $\mathcal{G}$.

Eine pro-endliche Gruppe $X$ heißt Demuškinformation über $\mathcal{G}$ vom Grad $n$, mit Torsion $p^s$ und Charakter $\alpha$, wenn es eine Surjektion $\phi\colon X\twoheadrightarrow\mathcal{G}$ mit pro-$p$-Gruppe als Kern gibt derart, daß für jeden offenen Normalteiler $\mathcal{H}\subseteq\operatorname{Ker}\alpha$ von $\mathcal{G}$ das Urbild $X_{\mathcal{H}}=\phi^{-1}(\mathcal{H})$ unter $\phi$ die folgenden Bedingungen erfüllt:

I) Es gilt $\dim H^1(X_{\mathcal{H}},\mathbb{F}_p)<\infty$, $\dim H^2(X_{\mathcal{H}},\mathbb{F}_p)=1$, und das Cupprodukt

$$H^1(X_{\mathcal{H}},\mathbb{F}_p)\times H^1(X_{\mathcal{H}},\mathbb{F}_p)\to H^2(X_{\mathcal{H}},\mathbb{F}_p)$$

definiert eine nicht-ausgeartete (antisymmetrische) Bilinearform auf $H^1(X_{\mathcal{H}},\mathbb{F}_p)$; ferner ist der $p$-Torsionsanteil von $X_{\mathcal{H}}^{\mathrm{ab}}$ zyklisch von der Ordnung $p^s$.

II) Wird $H^1(\mathscr{H},\mathbb{F}_p)$ vermöge der Inflation als Unterraum von $H^1(X_{\mathscr{H}},\mathbb{F}_p)$ aufgefaßt und ist bezüglich der obigen Bilinearform $H^1(\mathscr{H},\mathbb{F}_p)^\perp$ der dazu senkrechte Unterraum, so gilt mit $G=\mathscr{G}/\mathscr{H}$ die $\mathbb{F}_p[G]$-Isomorphie

$$H^1(\mathscr{H},\mathbb{F}_p)^\perp/H^1(\mathscr{H},\mathbb{F}_p)\cong\mathbb{F}_p[G]^n.$$

Weiter ist dieser $G$-Modul bezüglich der induzierten (nichtausgearteten) Bilinearform hyperbolisch, d.h., die direkte Summe zweier total-isotroper $G$-Untermoduln.

III) $\mathscr{G}$ operiert mit dem Charakter $\alpha$ auf $H^2(X_{\mathscr{H}},\mathbb{Z}/p^s)$, d.h., es gilt

$$\rho x=\alpha(\rho)x \quad \text{für } \rho\in\mathscr{G} \text{ und } x\in H^2(X_{\mathscr{H}},\mathbb{Z}/p^s).$$

*Bemerkungen.* a) Statt die Bedingungen für alle offenen Normalteiler $\mathscr{H}\subseteq\operatorname{Ker}\alpha$ von $\mathscr{G}$ zu fordern, kann man sich auch auf eine Umgebungsbasis der Eins beschränken.

b) In den drei Bedingungen können die Gruppen $X_{\mathscr{H}}$ durch ihre maximalen pro-$p$-Faktorgruppen $\tilde{X}_{\mathscr{H}}$ ersetzt werden (die Aussage I) bedeutet dann, daß alle $\tilde{X}_{\mathscr{H}}$ Demuškingruppen mit der Invarianten $p^s$ sind): Da die Inflation eine Isomorphie $H^1(\tilde{X}_{\mathscr{H}},\mathbb{F}_p)\cong H^1(X_{\mathscr{H}},\mathbb{F}_p)$ und eine Inklusion $H^2(\tilde{X}_{\mathscr{H}},\mathbb{Z}/p^r)\subseteq H^2(X_{\mathscr{H}},\mathbb{Z}/p^r)$ für $r\in\mathbb{N}$ liefert, ist für den Übergang von $X_{\mathscr{H}}$ zu $\tilde{X}_{\mathscr{H}}$ nur $H^2(\tilde{X}_{\mathscr{H}},\mathbb{F}_p)\neq 0$ zu zeigen; dies gilt aber wegen $\operatorname{Tor}(\tilde{X}_{\mathscr{H}}^{\mathrm{ab}})=(\operatorname{Tor}(X_{\mathscr{H}}^{\mathrm{ab}}))(p)\neq 0$.

Sind umgekehrt die Aussagen I)–III) für $\tilde{X}_{\mathscr{H}}=:X_{\mathscr{H}}/I_{\mathscr{H}}$ erfüllt, so erhält man mit $\mathscr{H}'=\phi(I_{\mathscr{H}})$ und $\bar{V}=\operatorname{Ker}(X_{\mathscr{H}}/I_{\mathscr{H}}\twoheadrightarrow\mathscr{H}/\mathscr{H}')$ das kommutative Diagramm mit exakten Zeilen

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \bar{V} & \longrightarrow & X_{\mathscr{H}}/I_{\mathscr{H}} & \longrightarrow & \mathscr{H}/\mathscr{H}' & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \bar{V} & \longrightarrow & X/I_{\mathscr{H}} & \longrightarrow & \mathscr{G}/\mathscr{H}' & \longrightarrow & 1,
\end{array}$$

wobei $\mathscr{H}/\mathscr{H}'=\tilde{\mathscr{H}}\cong\mathbb{Z}_p$ die maximale pro-$p$-Faktorgruppe von $\mathscr{H}$ ist. Da die kohomologische $p$-Dimension der Demuškingruppe $\tilde{X}_{\mathscr{H}}$ gleich zwei ist, ergibt sich $cd_p(X/I_{\mathscr{H}})\leqq cd_p(\bar{V})+cd_p(\mathscr{G}/\mathscr{H}')\leqq cd_p(X_{\mathscr{H}}/I_{\mathscr{H}})+1<\infty$, insbesondere $scd_p(X/I_{\mathscr{H}})=scd_p(X_{\mathscr{H}}/I_{\mathscr{H}})=2$ (vgl. [18], I., Prop. 14 und Prop. 31). Die Gruppe $X$ ist nun der projektive Limes der $X/I_{\mathscr{H}}$, da $\operatorname{Ker}\phi$ eine pro-$p$-Gruppe ist; damit erhalten wir

$$scd_p(X)=2.$$

Daraus folgt $H^2(I_{\mathscr{H}},\mathbb{Q}_p/\mathbb{Z}_p)=0$, also auch $H^2(I_{\mathscr{H}},\mathbb{Z}/p^r)=0$, und aus der Spektralsequenz $H^i(\tilde{X}_{\mathscr{H}},H^j(I_{\mathscr{H}},\mathbb{Z}/p^r))\Rightarrow H^{i+j}(X_{\mathscr{H}},\mathbb{Z}/p^r)$ die Isomorphie

$$H^2(\tilde{X}_{\mathscr{H}},\mathbb{Z}/p^r)\xrightarrow{\sim}H^2(X_{\mathscr{H}},\mathbb{Z}/p^r),$$

woraus die Bedingungen I)–III) auch für $X_{\mathscr{H}}$ folgen.

*1.2.* Wir wollen nun für vorgegebenes $\mathscr{G}$, $n$, $s$ und $\alpha$ eine Demuškinformation $X$ über $\mathscr{G}$ mit diesen Invarianten konstruieren. Bezeichnet $F_{n+1}$ die freie pro-endliche Gruppe mit Basis $z_0,\ldots,z_n$, so ist der Kern der kanonischen Projek-

tion des freien pro-endlichen Produkts $F_{n+1} * \mathcal{G}$ auf $\mathcal{G}$ gerade der von $z_0, \ldots, z_n$ (topologisch) erzeugte Normalteiler $Z=(z_0, z_1, \ldots, z_n)$ (s. Neukirch [17], 1.2). Der Normalteiler $I$ von $Z$, für den $Z/I$ die maximale pro-$p$-Faktorgruppe ist, ist auch normal in $F_{n+1} * \mathcal{G}$, und wir setzen

$$F(n+1, \mathcal{G}) = (F_{n+1} * \mathcal{G})/I$$
$$P = Z/I.$$

Bezeichnen wir die Bilder der $z_i$ in $F(n+1, \mathcal{G})$ mit $x_i$, $i=0, \ldots, n$, so besitzt $F(n+1, \mathcal{G})$ also die Erzeugenden $\sigma, \tau, x_0, \ldots, x_n$ und ist dadurch definiert, daß $\sigma$ und $\tau$ die Relationen von $\mathcal{G}$ erfüllen und der von $x_0, \ldots, x_n$ erzeugte Normalteiler eine pro-$p$-Gruppe ist.

$F(n+1, \mathcal{G})$ ist ein freies Objekt in der Kategorie der semidirekten Produkte von $\mathcal{G}$ mit einer pro-$p$-Gruppe $H$, wobei die Morphismen die stetigen Homomorphismen $f: H \cdot \mathcal{G} \to H' \cdot \mathcal{G}$ sind mit $f(H) \subseteq H'$ und $f|_{\mathcal{G}} = \mathrm{id}$ ([11], Satz 3.4). Die Gruppe $P$ ist eine freie Operatoren-pro-$p$-Gruppe mit freiem Erzeugendensystem $\{x_0, \ldots, x_n\}$ und Operatorenbereich $\mathcal{G}$ in der Terminologie von Koch [12].

Die Gruppe $X$ soll nun aus $F(n+1, \mathcal{G})$ durch eine weitere Relation hervorgehen. Sei dazu $\beta: \mathcal{G} \to \mathbb{Z}_p^\times$ eine Liftung des Charakters $\alpha$ (nicht notwendig ein Homomorphismus) und für eine Primzahl $\ell$ jeweils $\pi_\ell$ das Element aus $\hat{\mathbb{Z}}$ mit $\pi_\ell \hat{\mathbb{Z}} = \mathbb{Z}_\ell$. Weiter sei für $x, y \in F(n+1, \mathcal{G})$ und $\rho \in \mathcal{G}$ $[x, y] = xyx^{-1}y^{-1} = y^x y^{-1}$ der Kommutator,

$$(x, \rho) = (x, \rho)_\beta = (x^{\beta(1)} \rho x^{\beta(\rho)} \rho \ldots x^{\beta(\rho^{p-2})} \rho)^{\frac{\pi_p}{p-1}}$$

und

$$\{x, \rho\} = \{x, \rho\}_\beta = (x^{\beta(1)} \rho^2 x^{\beta(\rho)} \rho^2 \ldots x^{\beta(\rho^{p-2})} \rho^2)^{\frac{\pi_p}{p-1}}$$

(dies ist wohldefiniert, da $p-1$ in $\mathbb{Z}_p$ invertierbar ist).

Die Invarianten mögen der folgenden Bedingung genügen:

(+) Für ungerades $n$ ist auch $f_0$ ungerade sowie

$$\alpha(\tau)^{\frac{p-1}{2}} \equiv -1 \bmod p.$$

(Für eine Demuškinformation ist (+) fast immer erfüllt; die Spezialfälle betrachten wir in 5.2.)

Dann definieren wir

$$X = X(\mathcal{G}, n, s, \beta) = F(n+1, \mathcal{G})/(r),$$

wobei $(r)$ der von dem folgenden Element $r$ erzeugte (abgeschlossene) Normalteiler ist:

$$r = x_0^{-\sigma}(x_0, \tau)^{\beta(\sigma)^{-1}} x_1^{p^s} [x_1, x_2][x_3, x_4] \ldots [x_{n-1}, x_n] \quad \text{für gerades } n,$$
$$r = x_0^{-\sigma}(x_0, \tau)^{\beta(\sigma)^{-1}} x_1^{p^s} [x_1, y_1][x_2, x_3] \ldots [x_{n-1}, x_n] \quad \text{für ungerades } n,$$

mit

$$y_1 = x_1^{\tau_2^{p+1}} \{x_1, \tau_2^{p+1}\}^{\sigma_2 \tau_2^a} \{\{x_1, \tau_2^{p+1}\}, \sigma_2 \tau_2^a\}^{\sigma_2 \tau_2^b + \tau_2^{\frac{p+1}{2}}}$$

wobei $a, b \in \mathbb{Z}$ so gewählt sind, daß gilt

$$-\alpha(\sigma\tau^a) \bmod p \in (\mathbb{F}_p^\times)^2 \quad \text{und} \quad -\alpha(\sigma\tau^b) \bmod p \notin (\mathbb{F}_p^\times)^2.$$

Hier ist zur Abkürzung $\tau_2 = \tau^{\pi_2}$ und $\sigma_2 = \sigma^{\pi_2}$ gesetzt, und $x^{\rho+\rho'}$ steht für $x^\rho x^{\rho'}$.

*Bemerkung.* Da wegen (+) $\alpha(\tau) \bmod p$ ein Nicht-Quadrat in $\mathbb{F}_p^\times$ ist, gibt es immer Zahlen $a, b$ mit den gewünschten Eigenschaften. Möglich ist z.B.

$$a=0, \quad b=1 \quad \text{für} \quad -\alpha(\sigma) \bmod p \in (\mathbb{F}_p^\times)^2,$$
$$a=1, \quad b=0 \quad \text{für} \quad -\alpha(\sigma) \bmod p \notin (\mathbb{F}_p^\times)^2$$

oder auch

$$a=\frac{p-1}{2}, \quad b=\frac{p+1}{2} \quad \text{für } \alpha(\sigma) \bmod p \in (\mathbb{F}_p^\times)^2,$$
$$a=\frac{p+1}{2}, \quad b=\frac{p-1}{2} \quad \text{für } \alpha(\sigma) \bmod p \notin (\mathbb{F}_p^\times)^2,$$

falls man für $\alpha(\sigma) \equiv 1(p)$ nicht die Fälle $p \equiv 1(4)$ und $p \not\equiv 1(4)$ unterscheiden möchte.

Wir werden in §2 und §4 beweisen:

**Theorem 1.** *$X = X(\mathcal{G}, n, s, \beta)$ ist eine Demuškinformation über $\mathcal{G}$ vom Grad $n$, mit Torsion $p^s$ und Charakter $\alpha$.*

*1.3.* Hieraus ergibt sich nun eine Beschreibung der absoluten Galoisgruppe eines p-adischen Zahlkörpers durch Erzeugende und Relationen; etwas allgemeiner betrachten wir die Galoisgruppe einer $p$-abgeschlossenen Erweiterung, d.i. eine Erweiterung, die keiner $p$-Erweiterung mehr fähig ist.

**Theorem 2.** *Es sei $k$ ein p-adischer Zahlkörper vom Grad $n$ über $\mathbb{Q}_p$, $p \neq 2$, $q = p^{f_0}$ die Mächtigkeit des Restklassenkörpers von $k$, $L$ eine $p$-abgeschlossene Erweiterung von $k$, $T$ die maximale zahm-verzweigte Erweiterung von $k$ in $L$, $\mu_T$ die Gruppe der Einheitswurzeln von $p$-Potenz-Ordnung in $T$, $p^s = (\mu_T : 1) > 1$ und $\alpha: \mathcal{G} = G_{T/k} \to (\mathbb{Z}/p^s)^\times$ der Charakter mit $\zeta^\rho = \zeta^{\alpha(\rho)}$ für alle $\rho \in \mathcal{G}$, $\beta: \mathcal{G} \to \mathbb{Z}_p^\times$ eine Liftung von $\alpha^{-1}$ (als Abbildung), $\sigma, \tau$ seien Erzeugende von $\mathcal{G}$ mit $\sigma\tau\sigma^{-1} = \tau^q$. Dann gibt es eine Isomorphie pro-endlicher Gruppen*

$$G_{L|k} \cong F(x_0, \ldots, x_n; \mathcal{G})/(r),$$

*wobei $r$ wie in 1.2 mit den obigen $\sigma, \tau$ und $\beta$ gebildet wird.*

*Beweis von Theorem 2.* Die Gruppe $G_{L|k}$ ist eine Demuškinformation über $\mathcal{G}$ vom Rang $n$, der Torsion $p^s$ und Charakter $\alpha^{-1}$, wobei die Bedingung (+) für $n, f_0$ und $\alpha^{-1}$ erfüllt ist (s. Koch [14]).

Nach Theorem 1 trifft dies auch auf die Gruppe $F(x_0, \ldots, x_n; \mathcal{G})/(r)$ zu. Zwei Demuškinformationen über $\mathcal{G}$ mit gleichen Invarianten sind aber isomorph (s. [14] oder [19] für einen vollständigen Beweis).

*1.4.* Beispiele und Anwendungen:

a) Ist $L=\bar{k}$ der algebraische Abschluß von $k$, so ist $\sigma\tau\sigma^{-1}=\tau^q$ die einzige Relation von $\mathcal{G}$, und man erhält die in der Einleitung angegebene Beschreibung der absoluten Galoisgruppe $G_k$ von $k$ mit in wesentlichen zwei Relationen, indem man $\beta(\sigma)=g^{-1}$ und $\beta(\tau^i)=h^{p-1-i}$ setzt.

Für den Körper $k=\mathbb{Q}_p$ kann man durch geeignete Wahl von $\sigma$ ohne Einschränkung $g=1$ annehmen und dann $a=\frac{p-1}{2}$ und $b=\frac{p+1}{2}$ setzen. Daher besitzt $G_{\mathbb{Q}_p}$ vier Erzeugende $\sigma$, $\tau$, $x_0$, $x_1$ mit den definierenden Relationen

$$\tau^\sigma=\tau^p,$$
$$x_0^\sigma=(x_0,\tau)x_1^p[x_1,x_1^{\tau_2^{p+1}}\{x_1,\tau_2^{p+1}\}^{\sigma_2\tau_2^{\frac{p+1}{2}}}\{\{x_1,\tau_2^{p+1}\},\sigma_2\tau_2^{\frac{p-1}{2}}\}^{\sigma_2\tau_2^{\frac{p-1}{2}}+\tau_2^{\frac{p+1}{2}}}].$$

Für den Körper $k=\mathbb{Q}_p(\zeta_p)$, $\zeta_p$ eine primitive $p$-te Einheitswurzel, kann $\beta(\rho)=1$ für alle $\rho\in\mathcal{G}$ und damit $(x_0,\tau)=(x_0\tau)^{\pi_p}$ gesetzt werden. Dann besitzt $G_k$ $p+2$ Erzeugende $\sigma,\tau,x_0,\ldots,x_{p-1}$ mit den definierenden Relationen

$$\tau^\sigma=\tau^p,$$
$$x_0^\sigma=(x_0\tau)^{\pi_p}x_1^p[x_1,x_2]\ldots[x_{p-2},x_{p-1}].$$

(Es kommt natürlich jeweils wieder als Bedingung hinzu, daß der von den $x_i$ erzeugte Normalteiler $V$ eine pro-$p$-Gruppe ist, d.h., daß $x^{\pi_p}=x$ für alle $x\in V$ gilt.)

b) Ist $L$ die maximale Erweiterung von $k$ ohne zahme Verzweigung, so ist $\mathcal{G}\cong\hat{\mathbb{Z}}$ mit erzeugendem Element $\sigma$, und man erhält $G_{L|k}$, indem man $G_k$ durch den von $\tau$ erzeugten Normalteiler dividiert. Enthält $L$ eine primitive $p$-te Einheitswurzel, so kann man $\beta(\tau^i)=1$ für alle $i$ setzen, wodurch sich $(x_0,\tau)\equiv x_0 \bmod(\tau)$ ergibt. Weiter ist $n$ notwendig gerade, da $p-1=e(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ den Verzweigungsindex $e(k/\mathbb{Q}_p)=e(k(\zeta_p)/\mathbb{Q}_p)$ teilt. Man erhält also mit $\beta(\sigma)=g^{-1}$ die Relation

$$x_0^\sigma=x_0^g x_1^{p^s}[x_1,x_2]\ldots[x_{n-1},x_n]$$

(vgl. Koch [12], Satz 2).

Im anderen Fall gilt nach [12], Satz 1 oder [11], Satz 3.6a)

$$G_{L|k}\cong F(x_1,\ldots,x_n;\hat{\mathbb{Z}}).$$

c) Ist $n$ ungerade und $L\supseteq k(\zeta_p)$ eine $p$-abgeschlossene Erweiterung von $k$ derart, daß der Verzweigungsindex von $T/k(\zeta_p)$ ungerade ist, so kann in der Relation $r$ der Ausdruck $y_1$ durch $x_1^\tau$ ersetzt werden, wie in 5.2 gezeigt werden wird. Ist speziell $\mathbb{Q}_p(\zeta_p)_u$ die maximale Erweiterung von $\mathbb{Q}_p(\zeta_p)$ mit ungeradem Verzweigungsindex, so erhält man für die Galoisgruppe $G_{\mathbb{Q}_p(\zeta_p)_u/\mathbb{Q}_p}$ Erzeugende $\sigma$, $\tau$, $x_0$,

$x_1$ mit den Relationen

$$\sigma\tau\sigma^{-1}=\tau^p, \qquad \tau^{\pi_2(p-1)}=1,$$

$$x_0^\sigma=(x_0^{h^{p-1}}\tau x_0^{h^{p-2}}\tau\ldots x_0^h\tau)^{\frac{\pi_p}{p-1}}x_1^p[x_1,x_1^\tau]$$

(man wähle ein $\sigma$ mit $\alpha(\sigma)=1$).

d) Ist $n$ gerade und $\alpha(\tau)=1$ (z.B. für $\zeta_p\in k$), so kann man $G_k$ durch $n+2$ Erzeugende $\sigma, z, x_1, \ldots, x_n$ und die folgenden Bedingungen beschreiben:

A′) Der von $z^{\pi_p}, x_1, \ldots, x_n$ erzeugte Normalteiler ist eine pro-$p$-Gruppe.

B′) Mit $w=z^{-\sigma}z^{\pi_p g}x_1^{p^s}[x_1,x_2]\ldots[x_{n-1},x_n]$ gilt $w^\sigma=w^q$.

*Beweis.* Für $h=1$ ergibt sich die Relation

(i) $x_0^\sigma=(x_0\tau)^{\pi_p g}x_1^{p^s}[x_1,x_2]\ldots[x_{n-1},x_n]$.

Setzt man $z=x_0\tau$, so folgt aus $\tau^{-\sigma}=\tau^{-q}$ die Beziehung $(z^{-1}x_0)^{\sigma^2}=(z^{-1}x_0)^{q\sigma}$ und mit (i) erhalten wir $w^\sigma=w^q$. Umgekehrt ergibt sich mit $\tau=w^{-\sigma^{-1}}$ und $x_0=z\tau^{-1}=zw^{\sigma^{-1}}$ sofort die Relation (i) und aus $w^\sigma=w^q$ die Relation $B$: $\tau^\sigma=w^{-1}=w^{-q\sigma^{-1}}=\tau^q$. Es ist klar, daß die Bedingungen $A$ und $A'$ sich entsprechen.

e) Die explizite Angabe der Relationen im Theorem 2 erlaubt es uns, die Frage von Jarden und Ritter (s. „Normal automorphisms of absolute galois groups of p-adic fields", Duke Math. J. 47, 47-56 (1980)) nach der Vollständigkeit der absoluten Galoisgruppe von $\mathbb{Q}_p$ für $p\neq 2$ negativ zu beantworten. Wie zu vermuten war, besitzt die Gruppe $G_{\mathbb{Q}_p}$ äußere Automorphismen. Den Existenznachweis stellen wir an das Ende dieser Arbeit, da wir dazu einzelne Tatsachen aus dem Beweis von Theorem 1 benutzen.

## § 2. Beweisanfang von Theorem 1 und Beweis für gerades $n$

*2.1.* Das Element $\pi_\ell\in\hat{\mathbb{Z}}$ kann folgendermaßen definiert werden. Ist $\{p_1,p_2,p_3,\ldots\}$ die Menge aller von $\ell$ verschiedenen Primzahlen aus $\mathbb{Z}$ und wählen wir für jedes $m\in\mathbb{N}$ zwei $a_m, b_m\in\mathbb{Z}$ mit

$$1=a_m\cdot\ell^m+b_m\cdot p_1^m p_2^m\ldots p_m^m,$$

so können wir setzen

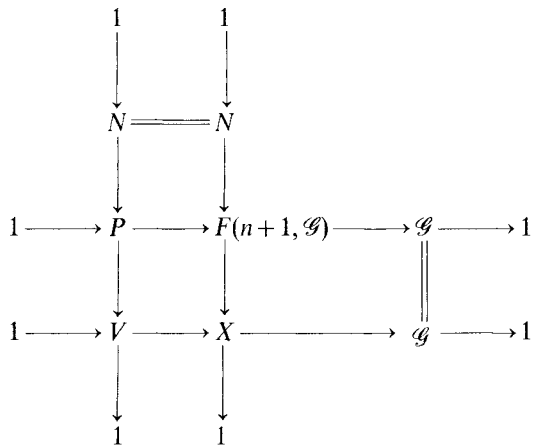
$$\Delta_\ell=\lim_{m\to\infty}a_m\ell^m\in\hat{\mathbb{Z}},$$

$$\pi_\ell=\lim_{m\to\infty}b_m p_1^m\ldots p_m^m\in\hat{\mathbb{Z}}.$$

Es gilt $\Delta_\ell+\pi_\ell=1$, $\Delta_\ell^2=\Delta_\ell$, $\pi_\ell^2=\pi_\ell$ und $\Delta_\ell\pi_\ell=0$; wir setzen im folgenden $\pi=\pi_p$. Die oben definierte Gruppe $P$ ist gerade der von $x_0,\ldots,x_n$ erzeugte Normalteiler; damit gilt

$$r\equiv(x_0,\tau)^{\beta(\sigma)^{-1}}\equiv(\tau^{p-1})^{\frac{\pi}{p-1}\cdot\beta(\sigma)^{-1}}\equiv\tau^{\pi\beta(\sigma)^{-1}}\equiv 1 \bmod P,$$

da die Ordnung von $\tau$ prim zu $p$ ist. Der von $r$ erzeugte Normalteiler $N=(r)$ liegt also in $P$, und wir erhalten mit $V=P/N$ das kommutative Diagramm



mit exakten Spalten und Zeilen.

Sei $\mathscr{H}$ ein offener Normalteiler von $\mathscr{G}$, der in $\operatorname{Ker}\alpha$ liegt, $U=U_{\mathscr{H}}$ das Urbild von $\mathscr{H}$ in $F(n+1,\mathscr{G})$, $X_{\mathscr{H}}$ das Urbild von $\mathscr{H}$ in $X$ und $G=\mathscr{G}/\mathscr{H}$.

*2.2.* Setzen wir $\bar{x}=x[P,U]$ für $x\in P$, so ist $P/[P,U]$ ein freier $\mathbb{Z}_p[G]$-Modul mit Basis $\bar{x}_0,\ldots,\bar{x}_n$. Dies wurde in [11] bewiesen und folgt aus dem Untergruppensatz für freie Produkte [2], der für das Urbild $U'$ von $\mathscr{H}$ in $F_{n+1}*\mathscr{G}$ die Isomorphie

$$U'\cong(\underset{\rho\in R}{*}F_{n+1}^{\rho})*\mathscr{H},\qquad R \text{ Restsystem für } \mathscr{G}/\mathscr{H},$$

liefert, woraus sich zusammen mit der exakten Sequenz

$$0\to H^1(\mathscr{H},\mathbb{Q}_p/\mathbb{Z}_p)\to H^1(U',\mathbb{Q}_p/\mathbb{Z}_p)\to H^1(Z,\mathbb{Q}_p/\mathbb{Z}_p)^{U'}\to 0$$

wegen $H^1(Z,\mathbb{Q}_p/\mathbb{Z}_p)^{U'}=H^1(P,\mathbb{Q}_p/\mathbb{Z}_p)^U=\operatorname{Hom}(P/[P,U],\mathbb{Q}_p/\mathbb{Z}_p)$ die Behauptung ergibt.

*2.3.* Sei $e$ die Ordnung von $\bar{\tau}=\tau\mathscr{H}\in G$, dann gilt

$$\begin{aligned}(x_0,\tau)&=(x_0^{\beta(1)}\tau x_0^{\beta(\tau)}\tau\ldots x_0^{\beta(\tau^{p-2})}\tau)^{\pi/p-1}\\&=(x_0^{\beta_0}x_0^{\beta_1\tau}x_0^{\beta_2\tau^2}\ldots x_0^{\beta_{e(p-1)-1}\tau^{e(p-1)-1}}\tau^{e(p-1)})^{\pi/e(p-1)}\end{aligned}$$

mit $\beta_j=\beta(\tau^{\langle j\rangle})$ für den Repräsentanten $\langle j\rangle$ zwischen 0 und $p-2$ von $j \bmod (p-1)$. Da $\tau^e\in U$ und $\tau^\pi=1$ ist, für $y\in P$ aber $y^\pi=y$, ergibt sich

$$(x_0,\tau)\equiv(x_0^{\lambda_{\mathscr{H}}})^\pi\tau^\pi\equiv x_0^{\lambda_{\mathscr{H}}} \bmod [P,U]$$

mit

$$\lambda_{\mathscr{H}}=\frac{1}{e}\sum_{i=0}^{e-1}\tau^i\beta_i',\qquad \beta_i'=\frac{1}{p-1}\sum_{\substack{j=0\\ j\equiv i \bmod e}}^{e(p-1)-1}\beta_j.$$

Wegen $\alpha(\tau^e)=1=\alpha(\tau^{p-1})$ ist dabei $\beta_i'$ eine Liftung von $\alpha(\tau^i)=\alpha(\tau)^i$. Weiter folgt

$$r\equiv x_0^{-\sigma}x_0^{\beta(\sigma)^{-1}\lambda_{\mathscr{H}}}x_1^{p^s} \bmod [P,U].$$

*2.4.* Aus der Spektralsequenz für $V=P/N$ erhalten wir durch Bildung der Fixmoduln unter $U$ die exakte Sequenz

$$0\to H^1(V,\mathbb{Q}_p/\mathbb{Z}_p)^U\to H^1(P,\mathbb{Q}_p/\mathbb{Z}_p)^U\to H^1(N,\mathbb{Q}_p/\mathbb{Z}_p)^U$$

und dual dazu die exakte Sequenz von $\mathbb{Z}_p[G]$-Moduln

$$N/[N,U]\xrightarrow{\psi}P/[P,U]\to V/[V,X_{\mathscr{H}}]\to 0.$$

Da $N$ als Normalteiler von $r$ erzeugt wird, wird $N/[N,U]$ als $\mathbb{Z}_p[G]$-Modul von $r[N,U]$ erzeugt. Wir erhalten daher mit 2.2 und 2.3 einen $\mathbb{Z}_p[G]$-Homomorphismus

$$\varphi\colon \mathbb{Z}_p[G]\xrightarrow{\varphi'}N/[N,U)\xrightarrow{\psi}P/[P,U]=\bigoplus_{i=0}^{n}\mathbb{Z}_p[G]\bar{x}_i$$

mit $\varphi'(1)=r[N,U]$ und daher $\varphi(1)=\bar{x}_0^{-\sigma+\beta(\sigma)^{-1}\cdot\lambda_{\mathscr{H}}}\cdot\bar{x}_1^{p^s}$. Die Ergebnisse aus [11], § 2 zeigen nun, daß $\varphi$ injektiv und damit $\varphi'$ ein Isomorphismus ist und daß $\operatorname{Coker}\varphi=\operatorname{Coker}\psi=V/[V,X_{\mathscr{H}}]$ ein kohomologisch trivialer $\mathbb{Z}_p[G]$-Modul ist, mit zyklischem Torsionsmodul der Ordnung $p^s$, auf dem $G$ mit dem Charakter $\alpha^{-1}$ operiert.

*2.5.* Die Injektivität von $\psi$ impliziert die Exaktheit der dualen Sequenz

$$0\to H^1(V,\mathbb{Q}_p/\mathbb{Z}_p)^{\mathscr{H}}\to H^1(P,\mathbb{Q}_p/\mathbb{Z}_p)^{\mathscr{H}}\xrightarrow{\psi^*}H^1(N,\mathbb{Q}_p/\mathbb{Z}_p)^U\to 0.$$

Nach Bildung des induktiven Limes über alle $\mathscr{H}$ erhalten wir die Surjektivität von $\tilde{\psi}$ in der Spektralsequenz

$$0\to H^1(V,\mathbb{Q}_p/\mathbb{Z}_p)\to H^1(P,\mathbb{Q}_p/\mathbb{Z}_p)\xrightarrow{\tilde{\psi}}H^1(N,\mathbb{Q}_p/\mathbb{Z}_p)^P$$

$$\to H^2(V,\mathbb{Q}_p/\mathbb{Z}_p)\to H^2(P,\mathbb{Q}_p/\mathbb{Z}_p).$$

Andererseits gilt $cd_p(P)=cd_p(Z)\leqq cd_p(F_{n+1}*\mathscr{G})=\max\{cd_p(F_{n+1}),\ cd_p(\mathscr{G})\}=1$, also $H^2(P,\mathbb{Q}_p/\mathbb{Z}_p)=0$. Es folgt

$$H^2(V,\mathbb{Q}_p/\mathbb{Z}_p)=0.$$

Dies eingesetzt in die Spektralsequenz

$$H^i(\mathscr{H},H^j(V,\mathbb{Q}_p/\mathbb{Z}_p))\Rightarrow H^{i+j}(X_{\mathscr{H}},\mathbb{Q}_p/\mathbb{Z}_p)$$

liefert wegen $cd_p(\mathscr{H})=1$

$$H^2(X_{\mathscr{H}},\mathbb{Q}_p/\mathbb{Z}_p)\cong H^1(\mathscr{H},H^1(V,\mathbb{Q}_p/\mathbb{Z}_p))=0,$$

da nach 2.4 für alle Normalteiler $\mathscr{H}' \subseteq \mathscr{H}$ von $\mathscr{G}$ die Gruppe $H^1(V, \mathbb{Q}_p/\mathbb{Z}_p)^{\mathscr{H}'}$ kohomologisch trivial unter $\mathscr{G}/\mathscr{H}'$ also auch unter $\mathscr{H}/\mathscr{H}'$ ist.

*2.6.* Wegen $cd_p(\mathscr{H}) = 1$ ist die Sequenz

$$0 \to H^1(\mathscr{H}, \mathbb{Q}_p/\mathbb{Z}_p) \to H^1(X_{\mathscr{H}}, \mathbb{Q}_p/\mathbb{Z}_p) \to H^1(V, \mathbb{Q}_p/\mathbb{Z}_p)^{X_{\mathscr{H}}} \to 0$$

exakt und dual dazu die Sequenz von $\mathbb{Z}_p[G]$-Moduln

$$0 \to V/[V, X_{\mathscr{H}}] \to \tilde{X}_{\mathscr{H}}^{\mathrm{ab}} \to \tilde{\mathscr{H}}^{\mathrm{ab}} \to 0,$$

wobei $\tilde{\mathscr{H}}^{\mathrm{ab}} = \tilde{\mathscr{H}}$ als abelsche Gruppe isomorph zu $\mathbb{Z}_p$ ist. Daraus folgt mit 2.4

$$\mathrm{Tor}\, \tilde{X}_{\mathscr{H}}^{\mathrm{ab}} \cong \mathrm{Tor}(V/[V, X_{\mathscr{H}}]) \cong \mathbb{Z}/p^s(\alpha^{-1}),$$

wobei $\mathbb{Z}/p^s(\alpha^{-1})$ den $\mathscr{G}$-Modul bezeichnet, auf dem $\mathscr{G}$ mit $\alpha^{-1}$ operiert und der als abelsche Gruppe isomorph zu $\mathbb{Z}/p^s$ ist. Weiter zerfällt die angegebene Sequenz wegen der kohomologischen Trivialität von $V/[V, X_{\mathscr{H}}]$, d.h. es gilt

$$\tilde{X}_{\mathscr{H}}^{\mathrm{ab}} \cong \tilde{\mathscr{H}}^{\mathrm{ab}} \oplus V/[V, X_{\mathscr{H}}]$$

*2.7.* Mit 2.5 erhalten wir für $i \in \mathbb{N}$ die exakte Sequenz

$$H^1(X_{\mathscr{H}}, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{p^i} H^1(X_{\mathscr{H}}, \mathbb{Q}_p/\mathbb{Z}_p) \to H^2(X_{\mathscr{H}}, \mathbb{Z}/p^i\mathbb{Z}) \to 0,$$

die die $\mathbb{Z}_p[G]$-Isomorphie

$$H^2(X_{\mathscr{H}}, \mathbb{Z}/p^i\mathbb{Z})^* \cong {}_{p^i}\mathrm{Tor}\, \tilde{X}_{\mathscr{H}}^{\mathrm{ab}}$$

liefert, wobei $*$ des Pontrjagindual bedeutet und ${}_{p^i}M = \{x \in M \mid p^i x = 0\}$ für einen $\mathbb{Z}_p[G]$-Modul $M$ gesetzt ist. Mit 2.6 ergibt sich insbesondere

$$\dim H^2(X_{\mathscr{H}}, \mathbb{F}_p) = 1,$$
$$H^2(X_{\mathscr{H}}, \mathbb{Z}/p^s) \cong \mathbb{Z}/p^s(\alpha).$$

*2.8.* Es bleiben die Aussagen über das Cupprodukt

$$H^1(\tilde{X}_{\mathscr{H}}, \mathbb{F}_p) \times H^1(\tilde{X}_{\mathscr{H}}, \mathbb{F}_p) \xrightarrow{\cup} H^2(\tilde{X}_{\mathscr{H}}, \mathbb{F}_p)$$

nachzuweisen. Dazu definieren wir die absteigende $p$-Zentralreihe einer pro-endlichen Gruppe $Y$ durch

$$Y^0 = Y,\ Y^i = (Y^{i-1})^p\, [Y^{i-1}, Y] \quad \text{für } i \geqq 1.$$

**Lemma 1.** *Sei $D$ eine pro-$p$-Gruppe mit $\dim H^1(D, \mathbb{F}_p) = m$, $\dim H^2(D, \mathbb{F}_p) = 1$ und $\{\rho_1, \ldots, \rho_m\}$ ein minimales Erzeugendensystem von $D$. Gilt in $D$ die Relation*

$$\prod_i \rho_i^{a_i p} \prod_{i<j} [\rho_i, \rho_j]^{a_{ij}} \equiv 1 \bmod D^2$$

*mit $a_i, a_{ij} \in \mathbb{Z}_p$, wobei mindestens ein $a_i$ oder $a_{ij}$ nicht durch $p$ teilbar ist, so gibt es ein Erzeugendes $\xi$ von $H^2(D, \mathbb{F}_p)$ derart, daß für die bezüglich $\{\rho_1, \ldots, \rho_m\}$*

*gebildete Dualbasis* $\{\chi_1, \ldots, \chi_m\}$ *von* $H^1(D, \mathbb{F}_p)$ *beim Cupprodukt* $H^1(D, \mathbb{F}_p) \times H^1(D, \mathbb{F}_p) \xrightarrow{\cup} H^2(D, \mathbb{F}_p)$ *gilt:*

$$\chi_i \cup \chi_j = -a_{ij}\xi \quad \text{für } i<j.$$

*Beweis.* Mit einer freien pro-$p$-Gruppe $F$ mit $m$ Erzeugenden $y_1, \ldots, y_m$ erhält man eine minimale Darstellung

$$1 \to R \to F \to D \to 1$$

$$y_i \mapsto \rho_i$$

von $D$. Für das Element

$$v = \prod_i y_i^{a_i p} \prod_{i<j} [y_i, y_j]^{a_{ij}} \in F^1$$

gilt nach Voraussetzung $v \in RF^2 \backslash F^2$, also $v = rf$ mit $f \in F^2$ und $r \in R \backslash R^p[R, F]$. Bezeichnet $\hat{r}$ das duale Basiselement von $\mathrm{Hom}(R/R^p[R, F], \mathbb{F}_p) = H^1(R, \mathbb{F}_p)^F$ und $\xi$ das Bild von $\hat{r}$ unter der Transgression

$$H^1(R, \mathbb{F}_p)^F \xrightarrow[\sim]{tg} H^2(D, \mathbb{F}_p),$$

die wegen der Minimalität der Darstellung ein Isomorphismus ist, so folgt die Behauptung mit einem Satz von Serre (s. [13], 7.23).

Bezeichnen wir mit $\tilde{z}$ das Bild von $z \in U$ unter der Projektion

$$U \twoheadrightarrow \tilde{X}_{\mathscr{H}},$$

so erhalten wir aus 2.3 wegen $[V, X_{\mathscr{H}}] \subset X^1_{\mathscr{H}}$ die Kongruenz

$$\tilde{x}_0^{\sigma} \equiv (\widetilde{x_0, \tau})^{\beta(\sigma)^{-1}} \equiv \tilde{x}_0^{\lambda_{\mathscr{H}} \beta(\sigma)^{-1}} \bmod \tilde{X}^1_{\mathscr{H}}. \tag{1}$$

Ist $I$ das von $p^s$ und $\tau^e - 1$ erzeugte abgeschlossene, zweiseitige Ideal von $\mathbb{Z}_p[\![\mathscr{G}]\!]$, so gilt aufgrund der Relation $\sigma\tau\sigma^{-1} = \tau^q$ und der Beziehung $\alpha(\tau^e) = 1 = \alpha(\tau^{p-1})$

$$\sigma\lambda_{\mathscr{H}} \equiv \lambda_{\mathscr{H}}\sigma \bmod I \quad \text{und} \quad \tau\lambda_{\mathscr{H}} \equiv \beta(\tau)^{-1}\lambda_{\mathscr{H}} \bmod I. \tag{2}$$

Aus (1) folgt damit

$$\tilde{x}_0^{\tau} \equiv \tilde{x}_0^{\beta(\tau)^{-1}} \bmod \tilde{X}^1_{\mathscr{H}}, \tag{3}$$

$$\tilde{x}_0^{\lambda_{\mathscr{H}}} \equiv \tilde{x}_0 \bmod \tilde{X}^1_{\mathscr{H}} \tag{4}$$

und hieraus wiederum

$$\tilde{x}_0^{\sigma} \equiv \tilde{x}_0^{\beta(\sigma)^{-1}} \bmod \tilde{X}^1_{\mathscr{H}}. \tag{5}$$

Daher ist für alle $a, b \in \mathbb{Z}_p$ und $\rho, \rho' \in \mathscr{G}$

$$[\tilde{x}_0^{a\rho}, \tilde{x}_0^{b\rho'}] \equiv 1 \bmod \tilde{X}^2_{\mathscr{H}}. \tag{6}$$

Als Konsequenz dieser Vertauschungsrelation und der Gleichheit $\tilde{\tau}^e = 1$ ergibt eine analoge Rechnung wie in 2.3

$$(\widetilde{x_0, \tau}) \equiv \tilde{x}_0^{\lambda_{\mathscr{H}}} \bmod \tilde{X}_{\mathscr{H}}^2, \tag{7}$$

insbesondere ist der rechte Ausdruck wohldefiniert.

Ist $f$ die Ordnung von $\sigma$ modulo dem von $\mathscr{H}$ und $\tau$ erzeugten Normalteiler, also $\sigma^f \equiv \tau^u \bmod \mathscr{H}$ für ein $u \geqq 0$, so ist $\alpha(\sigma^f \tau^{-u}) = 1$ und mit $\kappa_{\mathscr{H}} = \sum_{i=0}^{f-1} \sigma^i \beta(\sigma^i)$ gilt im Gruppenring $\mathbb{Z}_p[\![\mathscr{G}]\!]$

$$\begin{aligned}\kappa_{\mathscr{H}} \lambda_{\mathscr{H}} (\lambda_{\mathscr{H}} \beta(\sigma)^{-1} - \sigma) &\equiv \kappa_{\mathscr{H}} (\alpha(\sigma)^{-1} - \sigma) \lambda_{\mathscr{H}} \equiv (1 - \sigma^f \alpha(\sigma)^f) \lambda_{\mathscr{H}} \alpha(\sigma)^{-1} \\ &\equiv (1 - \sigma^f \tau^{-u} \alpha(\sigma^f \tau^{-u})) \lambda_{\mathscr{H}} \alpha(\sigma)^{-1} \equiv (1 - \sigma^f \tau^{-u}) \lambda_{\mathscr{H}} \alpha(\sigma)^{-1} \bmod I.\end{aligned}$$

Weiter ist für $v \in \mathbb{Z}_p[\![\mathscr{G}]\!]$ wegen (3) und (5)

$$\tilde{x}_0^{p^s v} \equiv \tilde{x}_0^{p^s a} \bmod \tilde{X}_{\mathscr{H}}^2$$

mit einem $a \in \mathbb{Z}_p$.

Aus dem oben Gezeigten erhalten wir wegen $\widetilde{\tau^e} = 1$ die Kongruenz

$$\begin{aligned}((\tilde{x}_0^{-\sigma} (\widetilde{x_0, \tau})^{\beta(\sigma)^{-1}})^{e \lambda_{\mathscr{H}}})^{\kappa_{\mathscr{H}}} &\equiv \tilde{x}_0^{\kappa_{\mathscr{H}} \lambda_{\mathscr{H}} (\lambda_{\mathscr{H}} \beta(\sigma)^{-1} - \sigma) e} \\ &\equiv (\tilde{x}_0^{\lambda_{\mathscr{H}}})^{(1 - \sigma^f \tau^{-u}) \alpha(\sigma)^{-1} e} \tilde{x}_0^{p^s a} \\ &\equiv [\tilde{x}_0^{\lambda_{\mathscr{H}}}, \widetilde{\sigma^f \tau^{-u}}]^{e \alpha(\sigma)^{-1}} \tilde{x}_0^{p^s a} \bmod \tilde{X}_{\mathscr{H}}^2\end{aligned}$$

mit $a \in \mathbb{Z}_p$, wobei nach (4) im Kommutator $\tilde{x}_0^{\lambda_{\mathscr{H}}}$ durch $\tilde{x}_0$ ersetzt werden kann. Durch Anwenden von $e \lambda_{\mathscr{H}} \kappa_{\mathscr{H}}$ auf die Relation $r$ folgt also für gerades $n$

$$\begin{aligned}1 \equiv \tilde{x}_0^{p^s a} \tilde{x}_1^{p^s \kappa_{\mathscr{H}} \lambda_{\mathscr{H}} e} [\tilde{x}_0, \widetilde{\sigma^f \tau^{-u}}]^{e \alpha(\sigma)^{-1}} \\ \cdot ([\tilde{x}_1, \tilde{x}_2] \dots [\tilde{x}_{n-1}, \tilde{x}_n])^{\kappa_{\mathscr{H}} \lambda_{\mathscr{H}} e} \bmod \tilde{X}_{\mathscr{H}}^2.\end{aligned} \tag{8}$$

Aus 2.4 und 2.6 ergibt sich mit (3) und (5) leicht, daß die Elemente $\widetilde{\sigma^f \tau^{-u}}, \tilde{x}_0, \tilde{x}_i^{\rho}$, $i = 1, \dots, n$, $\rho \in \mathscr{G}$ aus einem Restsystem für $\mathscr{G}/\mathscr{H}$, ein minimales Erzeugendensystem von $\tilde{X}_{\mathscr{H}}$ bilden; sei $\chi_\sigma, \chi_0, \rho\chi_i$, $i = 1, \dots, n$, $\rho \in G$, die entsprechende Dualbasis von $H^1(\tilde{X}_{\mathscr{H}}, \mathbb{F}_p)$. Da $\kappa_{\mathscr{H}} \lambda_{\mathscr{H}} e \equiv \sum_{\rho \in G} \alpha(\rho) \rho \bmod p\mathbb{Z}_p[G]$ ist, folgt aus (8) mit Lemma 1

$$\begin{aligned}\rho\chi_i \cup \rho\chi_{i+1} &= -\alpha(\rho)\xi, \quad i = 1, 3, \dots, n-1, \ \rho \in G \\ \chi_0 \cup \chi_\sigma &= -\alpha(\sigma)^{-1} e \xi,\end{aligned}$$

alle anderen Cupprodukte zwischen den Basiselementen sind Null, sofern sie nicht aus den obigen durch Vertauschung entstehen ($\xi$ ein erzeugendes Element von $H^2(\tilde{X}_{\mathscr{H}}, \mathbb{F}_p)$). Dies zeigt, daß das Cupprodukt für $\tilde{X}_{\mathscr{H}}$ eine nichtausgeartete Bilinearform darstellt, wobei der von $\chi_1, \dots, \chi_n$ aufgespannte freie $\mathbb{F}_p[G]$-Modul einerseits isomorph zu $H^1(\mathscr{H}, \mathbb{F}_p)^{\perp}/H^1(\mathscr{H}, \mathbb{F}_p)$ und andererseits die direkte Summe der beiden total isotropen $G$-Moduln

$$B_1 = \langle \chi_1, \chi_3, \dots, \chi_{n-1} \rangle_{\mathbb{F}_p[G]} \cong \mathbb{F}_p[G]^{\frac{n}{2}}$$

und

$$B_2 = \langle \chi_2, \chi_4, \ldots, \chi_n \quad \rangle_{\mathbb{F}_p[G]} \cong \mathbb{F}_p[G]^{\frac{n}{2}}$$

ist. Damit ist für gerades $n$ alles bewiesen.

*2.9.* Es ist $\tilde{y}_1 \equiv \tilde{x}_1^{\delta} \bmod \tilde{X}_{\mathscr{H}}^1$ für ein $\delta \in \mathbb{F}_p[G]$ (s. §4). Daher ergibt sich für ungerades $n$ die Kongruenz

$$1 \equiv \tilde{x}_0^{p^s a}\, \tilde{x}_1^{p^s \kappa_{\mathscr{H}} \lambda_{\mathscr{H}} e}\, [\tilde{x}_0, \widetilde{\sigma^f \tau^{-u}}]^{e\alpha(\sigma)^{-1}}\, [\tilde{x}_1, \tilde{x}_1^{\delta}]^{\kappa_{\mathscr{H}} \lambda_{\mathscr{H}} e} \cdot ([\tilde{x}_2, \tilde{x}_3] \ldots [\tilde{x}_{n-1}, \tilde{x}_n])^{\kappa_{\mathscr{H}} \lambda_{\mathscr{H}} e} \bmod \tilde{X}_{\mathscr{H}}^2. \tag{9}$$

Wiederum mit Lemma 1 erhalten wir die orthogonale Zerlegung

$$H^1(\tilde{X}_{\mathscr{H}}, \mathbb{F}_p) = \langle \chi_\sigma, \chi_0 \rangle \perp \langle \chi_1 \rangle_{\mathbb{F}_p[G]} \perp (C_1 \oplus C_2)$$

wobei

$$C_1 = \langle \chi_2, \chi_4, \ldots, \chi_{n-1} \rangle_{\mathbb{F}_p[G]} \cong \mathbb{F}_p[G]^{\frac{n-1}{2}}$$

und

$$C_2 = \langle \chi_3, \chi_4, \ldots, \chi_n \quad \rangle_{\mathbb{F}_p[G]} \cong \mathbb{F}_p[G]^{\frac{n-1}{2}}$$

total-isotrope Räume sind, während $C_1 \oplus C_2$ nicht-ausgeartet bezüglich der Bilinearform ist. Wir haben daher noch zu zeigen, daß die Form auf $C_0 = \langle \chi_1 \rangle_{\mathbb{F}_p[G]} \cong \mathbb{F}_p[G]$ ebenfalls nicht-ausgeartet und hyperbolisch ist. Dazu werden wir im folgenden symplektische Moduln über dem Gruppenring $\mathbb{F}_p[G]$ etwas eingehender untersuchen.

Die $G$-Invarianz

$$\rho\chi \cup \rho\chi' = \alpha(\rho)(\chi \cup \chi')$$

des Cupprodukts läßt sich auch noch so deuten, daß mit der durch

$$(\sum_{\rho \in G} c_\rho \rho)^* = \sum_{\rho \in G} c_\rho \alpha(\rho)\, \rho^{-1} \tag{10}$$

auf dem Gruppenring $\mathbb{F}_p[G]$ gegebenen Anti-Involution $*$

$$(a\chi) \cup \chi' = \chi \cup (a^* \chi'), \qquad a \in \mathbb{F}_p[G],$$

gilt. Diese Situation betrachten wir nun allgemeiner.

## § 3. Symplektische Formen auf Gruppenringen

Sei $R$ ein kommutativer Ring (mit Eins) und $A$ eine assoziative $R$-Algebra (mit Eins) mit einer Anti-Involution $*$, d.h., einem $R$-linearen Endomorphismus $*$ von $A$ mit $(a^*)^* = a$ und $(ab)^* = b^* a^*$ für $a, b \in A$.

Eine $R$-Bilinearform

$$\phi\colon M \times M \to R$$

auf einem $A$-(Links-)Modul $M$ heißt invariant (bzgl. *), wenn für alle $x, y \in M$, $a \in A$

$$\phi(ax, y) = \phi(x, a^* y)$$

gilt. Die invarianten $R$-Bilinearformen entsprechen umkehrbar eindeutig den $A$-Homomorphismen

$$\tilde{\phi}\colon M \to \mathrm{Hom}_R(M, R)$$

vermöge $\tilde{\phi}(x)(y) = \phi(x, y)$, wobei die $A$-Modul-Struktur auf $\mathrm{Hom}_R(M, R)$ durch $(af)(x) = f(a^* x)$ für $x \in M$, $a \in A$ gegeben ist, und $\phi$ heißt links nicht-ausgeartet, wenn $\tilde{\phi}$ ein Isomorphismus ist.

Eine symmetrische oder antisymmetrische invariante, nicht-ausgeartete $R$-Bilinearform nennen wir im folgenden kurz eine *Form*; eine antisymmetrische Form nennen wir auch symplektisch (und $M$ dann einen symplektischen $A$-Modul). Eine Form heißt hyperbolisch, wenn $M$ in die direkte Summe zweier total-isotroper Untermoduln zerfällt. Die Bedeutung dieses Begriffes liegt darin, daß alle hyperbolischen symplektischen Formen auf $M$ äquivalent sind (s. [6]), wobei wie üblich zwei Formen $\phi$ und $\phi'$ äquivalent heißen, wenn es einen $A$-Isomorphismus $f\colon M \xrightarrow{\sim} M$ gibt mit $\phi(x, y) = \phi'(f(x), f(y))$ für alle $x, y \in M$.

**Lemma 2.** *Ein $A$-Modul $M$ besitzt genau dann eine hyperbolische symplektische Form, wenn er $R$-reflexiv ist (d.h., die kanonische Abbildung $M \to \mathrm{Hom}(\mathrm{Hom}(M, R), R)$ ein Isomorphismus ist) und in die direkte Summe zweier $A$-Moduln $B$ und $C$ mit $C \cong \mathrm{Hom}(B, R)$ zerfällt.*

*Beweis.* Die $R$-Reflexivität eines symplektischen Moduls $(M, \phi)$ folgt aus der Bijektivität von $\tilde{\phi}$; ist $M$ darüber hinaus direkte Summe der total isotropen Moduln $B$ und $C$, so folgt leicht $\mathrm{Hom}(B, R) \cong C^{\perp} = C$. Umgekehrt wird auf $M \cong B \oplus \mathrm{Hom}(B, R)$ durch

$$\phi(b + f, b' + f') = f(b') - f'(b)$$

eine hyperbolische Form definiert, wobei die Nicht-Ausgeartetheit aus der $R$-Reflexivität des direkten Summanden $B$ folgt.

Ein unzerlegbarer $A$-Modul $M$ heiße vom Typ I, wenn auf ihm eine symplektische Form existiert, und sonst vom Typ II.

**Lemma 3.** *Sei $A$ eine artinsch-noethersche $R$-Algebra, $M$ ein endlich erzeugter, $R$-reflexiver $A$-Modul und*

$$M = \Big(\bigoplus_{D_i \text{ vom Typ I}} D_i^{m_i}\Big) \oplus \Big(\bigoplus_{\substack{E_j \text{ vom Typ II} \\ E_j \cong \mathrm{Hom}(E_j, R)}} E_j^{n_j}\Big) \oplus \Big(\bigoplus_{\substack{F_k \text{ vom Typ II} \\ F_k \ncong \mathrm{Hom}(F_k, R)}} F_k^{r_k}\Big)$$

*eine Zerlegung von $M$ in unzerlegbare, paarweise nicht-isomorphe $A$-Moduln.*

a) *$M$ besitzt eine hyperbolische symplektische Form genau dann, wenn alle $m_i$ und $n_j$ gerade sind und $M \cong \mathrm{Hom}(M, R)$ gilt (hier wie überall ist eine $A$-Isomorphie gemeint).*

b) *Sind alle $n_j$ gerade und gilt $M \cong \mathrm{Hom}(M, R)$, so besitzt $M$ eine symplektische Form.*

c) *Ist 2 eine Einheit in $A$, so gilt auch die Umkehrung von* b).

*Beweis.* Da die Bildung der $R$-Duale die Klassen der $D_i$ und der $E_j$ respektiert, folgt aus der Existenz einer hyperbolischen Form mit Lemma 2, daß die $m_i$ und $n_j$ gerade sein müssen (man zerlege das $B$ aus Lemma 2). Weil mit $M$ auch alle direkten Summanden $R$-reflexiv sind, respektiert die $R$-Dual-Bildung auch die Klasse der $F_k$; insbesondere kann man bei einer Isomorphie $M \cong \mathrm{Hom}(M, R)$ die $k$ in Paare $(k, k')$ mit $F_{k'} \cong \mathrm{Hom}(F_k, R)$ und $r_k = r_{k'}$ einteilen. Lemma 2 zeigt daher, daß für $M \cong \mathrm{Hom}(M, R)$ (bzw. gerade $n_j$, bzw. gerade $m_i$) eine hyperbolische symplektische Form auf $\bigoplus_k F_k^{r_k}$ (bzw. $\bigoplus_j E_j^{n_j}$, bzw. $\bigoplus_i D_i^{m_i}$) existiert. Hieraus folgen a) und b); c) folgt aus der Tatsache, daß bei Invertierbarkeit der 2 jeder symplektische Modul orthogonale Summe von unzerlegbaren symplektischen Moduln ist, die als $A$-Moduln entweder unzerlegbar (und also vom Typ I) oder direkte Summe zweier total-isotroper, unzerlegbarer $A$-Moduln (also insbesondere hyperbolisch) sind (vgl. [8]) (für halbeinfaches $A$ ist dieses offensichtlich; in Lemma 5 und allem folgenden wird c) nur für halbeinfaches $A$ benutzt).

**Corollar.** *Ist $n$ ungerade, so existiert auf $M$ genau dann eine hyperbolische symplektische Struktur, wenn auf $M^n$ eine solche existiert. Ist 2 eine Einheit in $A$, so gibt es auf $M$ auch genau dann eine symplektische Struktur, wenn es auf $M^n$ eine solche gibt.*

Der Fall, der uns interessiert, ist $A = R[G]$ für eine endliche Gruppe $G$, wobei $R$ ein kommutativer, artinsch-noetherischer Ring ist und die Anti-Involution * auf $A$ durch einen Charakter $\alpha\colon G \to R^\times$ gegeben wird, vermöge

$$(\sum_{\rho \in G} c_\rho \rho)^* = \sum_{\rho \in G} c_\rho \alpha(\rho) \rho^{-1}. \tag{11}$$

Weiter betrachten wir $M = A$ als Linksmodul. Dieser besitzt eine ausgezeichnete symmetrische Form $\phi$, definiert durch $\phi(x, y) = \ell(xy^*)$ mit $\ell\colon A \to R$, $\ell(\sum_{\rho \in G} c_\rho \rho) = c_1$.

Für ein Element $d \in A$ mit $d^* = -d$ (bzw. $d^* = d$) ist durch

$$\phi_d(x, y) = \ell(xdy^*) \tag{12}$$

eine antisymmetrische (bzw. symmetrische), invariante $R$-Bilinearform auf $M = A$ definiert. Andererseits ist leicht zu sehen, daß jede solche $R$-Bilinearform $\phi$ von der Gestalt $\phi_d$ ist für ein $d$ mit den obigen Eigenschaften. Dabei ist $\phi_d$ genau dann nicht-ausgeartet, wenn $d$ eine Einheit ist; ferner sind zwei Formen $\phi_d$ und $\phi_{d'}$ genau dann äquivalent, wenn $d' = udu^*$ mit einer Einheit $u \in A$ ist.

**Lemma 4.** *Die Form $\phi_d$ ist genau dann hyperbolisch, wenn es ein Idempotentes $e \in A$ gibt mit $ed + de^* = d$.*

*Beweis.* Der Modul $Ae$ ist genau dann total-isotrop, wenn

$$\phi_d(xe, ye) = \ell(xedey^*) = 0$$

für alle $x, y \in A$ ist, also wenn $ede^* = 0$ gilt. Eine Zerlegung $M = B \oplus C = Ae + A(1-e)$ mit einem Idempotenten $e$ ist also genau dann hyperbolisch, wenn $ede^* = 0 = (1-e)d(1-e^*)$ ist. Das ist aber äquivalent zur Gleichung $ed + de^* = d$.

Dies motiviert die folgende

**Definition.** *Sei $A$ eine $R$-Algebra mit Anti-Involution $*$. Ein Element $d \in A$ heißt symmetrisch (bzw. antisymmetrisch), wenn $d^* = d$ (bzw. $d^* = -d$) ist, und hyperbolisch, wenn $ed + de^* = d$ für ein Idempotentes $e$ gilt. Zwei Elemente $d, d' \in A$ heißen äquivalent, wenn $d' = udu^*$ für eine Einheit $u \in A$ ist.*

**Lemma 5.** *Sei $G_2$ eine 2-Sylowgruppe von $G$, dann besitzt $R[G]$ als $R[G]$-Modul genau dann eine hyperbolische symplektische Struktur, wenn $R[G_2]$ als $R[G_2]$-Modul eine solche besitzt. (Die Involution auf $R[G_2]$ sei durch die Einschränkung von $*$ bzw. $\alpha$ gewonnen.) Ist 2 eine Einheit in $R$, so gilt die entsprechende Aussage auch für symplektische Strukturen.*

*Beweis.* Existiert eine (hyperbolische) antisymmetrische Einheit in $R[G_2]$, so liefert diese auch eine (hyperbolische) symplektische Form auf $R[G]$. Die umgekehrte Richtung folgt aus dem Corollar zu Lemma 3, da $R[G] \cong R[G_2]^{(G:G_2)}$ als $R[G_2]$-Modul und $(G: G_2)$ ungerade ist.

**Lemma 6.** *Sei $G$ eine endliche Gruppe, $G_2$ eine 2-Sylowgruppe von $G$ und $R = F$ ein Körper der Charakteristik ungleich 2. Weiter sei $\alpha: G \to F^\times$ ein Charakter und $*$ die Anti-Involution gemäß* (11).

a) *Die folgenden Aussagen sind äquivalent:*

i) *Auf $F[G]$ existiert eine symplektische Form bezüglich $*$.*

ii) *Auf $F[G_2^{ab}]$ existiert eine symplektische Form bezüglich $*$.*

iii) *Es gibt ein Element $1 \neq \bar{\rho} \in G_2^{ab}$, das die gleiche Ordnung hat wie sein Bild $\alpha(\bar{\rho})$ unter $\alpha$.*

b) *Auf $F[G]$ gibt es genau dann eine hyperbolische symplektische Form bezüglich $*$, wenn es eine symplektische gibt und in der Zerlegung von $F[G_2]$ in einfache Algebren $A_i$ kein $A_i$ ein (nicht-kommutativer) Schiefkörper ist. (Dies ist insbesondere erfüllt, wenn $F$ endlich oder algebraisch abgeschlossen oder wenn $G_2$ abelsch ist.)*

*Beweis.* Wegen Lemma 5 ist ohne Einschränkung $G = G_2$, also $G$ eine 2-Gruppe.

a) Der Schluß von i) nach ii) ist dann einfach (das Bild einer antisymmetrischen Einheit ist wieder eine solche).

Gilt ii) für $G_2 = G$ und ist $\bar{F}$ ein algebraischer Abschluß von $F$, so existiert auch auf $\bar{F}[G^{ab}]$ eine symplektische Form (bzgl. der induzierten Anti-Involution $*$). Zerlegt man diesen Gruppenring mit Hilfe der Idempotenten $e_\chi = (G^{ab}: 1)^{-1} \sum_{\rho \in G^{ab}} \chi(\rho)^{-1} \rho$ zu den Charakteren $\chi: G^{ab} \to \bar{F}^\times$

$$\bar{F}[G^{ab}] = \bigoplus_\chi \bar{F} e_\chi,$$

so sieht man, daß es kein $\chi$ mit $\chi^2=\alpha$ geben kann, wobei $\alpha$ als Charakter in $\bar{F}^\times$ aufgefaßt ist. Denn für ein solches $\chi$ würde * trivial auf $\bar{F}e_\chi$ operieren, in welchem Falle keine Einheit $d\in\bar{F}[G^{ab}]$ mit $d^*=-d$ existieren könnte.

Hieraus folgt iii); stellt man nämlich $G^{ab}$ als Produkt von zyklischen Gruppen $\langle\rho_i\rangle$ dar und wäre für jedes $\rho_i$ die Ordnung von $\rho_i$ echt größer als die von $\alpha(\rho_i)$, so erhielte man, indem man für jedes $i$ ein $\beta_i\in F^\times$ mit $\beta_i^2=\alpha(\rho_i)$ auswählte, einen wohldefinierten Charakter $\chi\colon G^{ab}\to\bar{F}^\times$ mit $\chi(\rho_i)=\beta_i$, also mit $\chi^2=\alpha$.

Aus iii) folgt, daß $F[G^{ab}]$ eine hyperbolische symplektische Form besitzt. Ist nämlich $1+\bar{\rho}\in G^{ab}$ mit $m=\operatorname{Ord}\bar{\rho}=\operatorname{Ord}\alpha(\bar{\rho})$, so gilt $\alpha(\bar{\rho})^{\frac{m}{2}}=-1$ und daher für $d=\bar{\rho}^{\frac{m}{2}}$

$$d^2=1,\ d^*=-d;$$

$d$ ist also eine hyperbolische antisymmetrische Einheit aus $F[G^{ab}]$ (für $e=\frac{1}{2}(1+d)$ gilt $e^2=e$ und $ed+de^*=d$).

Zerlegt man nun den halbeinfachen Gruppenring $F[G]$ in isotypische Komponenten bzw. die dazugehörigen einfachen Algebren $A_i$, die Matrizenringe $M_{n_i}(F_i)$ der Ordnung $n_i$ über Schiefkörpern $F_i$ sind, so teilen die $n_i$ die Gruppenordnung von $G$, sind also 2-Potenzen. (Dies ist für Charakteristik Null wohlbekannt und folgt für $\operatorname{Char}F\neq 2$ allgemein daraus, daß sich jede irreduzible Darstellung zu einer in Charakteristik Null liften läßt.) Insbesondere treten die irreduziblen Moduln, die zu Algebren $A_i$ mit $n_i\neq 1$ gehören, mit gerader Vielfachheit in $F[G]$ auf. Auf $M_1=\bigoplus_{n_i\neq 1} A_i$ existiert daher nach Lemma 3 eine hyperbolische symplektische Form (die Isomorphie $M_1\cong\operatorname{Hom}(M_1,F)$ folgt sofort aus der Isomorphie $F[G]\cong\operatorname{Hom}(F[G],F)$, die man z.B. aus der Existenz der kanonischen symmetrischen Form $\phi$ erhält). Die direkte Summe $M_2$ der kommutativen $A_i$ ist isomorph zum $F[G]$-Modul $F[G^{ab}]$ (dies folgt z.B. leicht durch Tensorieren mit $\bar{F}$ aus der klassischen Darstellungstheorie). Die nicht-kommutativen $A_i$ mit $n_i=1$ sind schließlich irreduzible Moduln vom Typ I (s. [16], 2.5) und treten in $F[G]$ mit Vielfachheit 1 auf.

Gilt nun iii), so besitzt $M_2$ eine hyperbolische symplektische Form und daher $F[G]$ auf jeden Fall eine symplektische Form.

b) Gilt iii) und gibt es keine nicht-kommutativen $A_i$ mit $n_i=1$, so besitzt $F[G]=M_1\oplus M_2$ sogar eine hyperbolische symplektische Form. Umgekehrt folgt aus der Existenz einer hyperbolischen Form mit Lemma 3, daß keine solchen $A_i$ auftreten dürfen. q.e.d.

*Bemerkung.* Für $\operatorname{Char}F=2$ ist die kanonische symmetrische Form auch antisymmetrisch, es existiert aber keine hyperbolische Form auf $F[G]$, da $F[G_2]$ unzerlegbar ist.

Das folgende Lemma ist nützlich zur Konstruktion von hyperbolischen antisymmetrischen Einheiten auf halbeinfachen Gruppenringen. Um dem Beweis von Theorem 1 für ungerades $n$ zu folgen, benötigt man nur den ersten Teil von a).

**Lemma 7.** *Sei $A=M_n(F)$ der Ring der $(n\times n)$-Matrizen über einem endlichen Körper $F$ von ungerader Charakteristik $p$ und * eine $\mathbb{F}_p$-lineare Anti-Involution auf $A$.*

a) *Operiert * nicht-trivial auf dem Zentrum $Z(A)$ von $A$, so gilt:*

i) *Alle antisymmetrischen Einheiten von $A$ (bzw. Formen auf $A$) sind äquivalent. Dasselbe gilt für die symmetrischen Einheiten/Formen.*

ii) *Die Einheiten/Formen sind genau dann hyperbolisch, wenn $n$ gerade ist.*

b) *Operiert * trivial auf $Z(A)$, so gilt:*

i) *Zwei symmetrische oder zwei antisymmetrische Einheiten sind genau dann äquivalent, wenn sich ihre Determinanten nur um ein Quadrat aus $F^\times$ unterscheiden.*

*Ist $n$ ungerade, so gibt es zwei Äquivalenzklassen von symmetrischen Einheiten/Formen und keine antisymmetrische Einheit/Form.*

*Ist $n$ gerade, so gibt es entweder zwei Äquivalenzklassen von symmetrischen Einheiten/Formen, und alle antisymmetrischen sind äquivalent, oder es gibt zwei Äquivalenzklassen von antisymmetrischen Einheiten/Formen, und alle symmetrischen sind äquivalent.*

ii) *Für gerades $n$ ist im ersten Fall jede antisymmetrische Einheit/Form hyperbolisch; im zweiten Fall ist eine antisymmetrische Einheit $d$ genau dann hyperbolisch, wenn*

$$\det d \equiv (-1)^{\frac{n}{2}} \bmod (F^\times)^2$$

*ist.*

*Beweis.* Die eindeutige Beziehung zwischen symmetrischen (antisymmetrischen, hyperbolischen) Einheiten und ebensolchen Formen auf $A$ wird genau wie bei den Gruppenringen durch eine Zuordnung

$$d \mapsto \psi_d \quad \text{mit} \quad \psi_d(x,y) = \ell(xdy^*)$$

mittels einer Involutionsspur $\ell: A \to R$ (vgl. [3], 7) hergestellt; hier ist es

$$\ell: M_n(F) \to \mathbb{F}_p, \ell(x) = sp_{F/\mathbb{F}_p} sp(x)$$

($sp$ bezeichnet die Matrixspur und $sp_{F/\mathbb{F}_p}$ die Spur von $F/\mathbb{F}_p$).

Ist $J$ der Automorphismus von $F = Z(A)$, der durch * induziert wird, und $^+$ die Anti-Involution auf $A = M_n(F)$ mit $(a_{ij})^+ = (a^J_{ji})$, so gilt

$$a^* = b a^+ b^{-1}$$

mit einer festen Einheit $b \in A$, für die $b^+ = \pm b$ gilt (dies folgt aus dem Satz von Skolem-Noether). Die Gleichheit $d^* = d$ (bzw. $d^* = -d$, bzw. $d' = udu^*$) ist dann äquivalent mit $\pm(db)^+ = db$ (bzw. $\pm(db)^+ = -db$, bzw. $d'b = u(db)u^+$). Durch Multiplikation mit $b$ entsprechen sich also für $b^+ = b$ symmetrische und antisymmetrische Einheiten bezüglich * und $^+$, für $b^+ = -b$ entsprechen sie sich in umgekehrter Weise. Die (anti-)symmetrischen Einheiten bezüglich $^+$ entsprechen wiederum in klassischer Weise den bezüglich $J$ (anti)hermiteschen $F$-Bilinearformen auf dem Vektorraum $V = F^n$. Dabei bleibt jeweils der Begriff der Äquivalenz erhalten.

Die Behauptungen a) i) und b) i) ergeben sich daher aus den folgenden wohlbekannten Tatsachen (vgl. Bourbaki, Algèbre, Kap. IX, §6, Ex. 3.4): Für $J \neq 1$ sind alle (anti-)hermiteschen Formen auf $V$ äquivalent. Für $J = 1$ gibt es

zwei Äquivalenzklassen von hermiteschen (=quadratischen) Formen auf $V$, wobei zwei Formen äquivalent sind, wenn die Determinanten der zugehörigen Matrizen kongruent $\bmod(F^\times)^2$ sind. Weiter gibt es für $J=1$ und ungerades $n$ keine antihermitesche Form, während für gerades $n$ alle antihermiteschen Formen äquivalent sind; ihre Determinante ist ein Quadrat. Dabei ist für ungerades $n$ notwendig $b^+=b$; für gerades $n$ entspricht der erste Fall $b^+=b$ und der zweite $b^+=-b$.

Es bleiben noch die Aussagen ii) über hyperbolische Formen zu zeigen. Sind alle Formen äquivalent, so ist nur zu untersuchen, wann überhaupt hyperbolische Formen existieren. Ist $M$ ein irreduzibler $A$-Modul, so gilt aber die $A$-Modul-Isomorphie $A\cong M^n$, außerdem gilt $\mathrm{Hom}(M,\mathbb{F}_p)\cong M$ wegen der $A$-Isomorphie $\mathrm{Hom}(A,\mathbb{F}_p)\cong A$ (die z.B. aus der Existenz der kanonischen Form $\psi_1$ folgt). Aus Lemma 2 folgt daher, daß hyperbolische Formen genau dann existieren, wenn $n$ gerade ist. Dies zeigt a)ii) und den ersten Teil von b)ii).

Für gerades $n$, $J=1$ und $b^+=-b$ betrachte man

$$c_0=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\qquad e_0=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix},$$

bzw. die Block-Diagonalmatrizen $c$, $e\in M_n(F)$, die aus $\frac{n}{2}$ Blöcken der Gestalt $c_0$ bzw. $e_0$ bestehen. Für diese gilt $c^+=c$, $e^2=e$, $ec+ce^+=c$ und $\det c=(-1)^{\frac{n}{2}}$. Daher ist $d=cb^{-1}$ eine hyperbolische antisymmetrische Einheit bezüglich $^*$; weiter gilt

$$\det d\equiv(-1)^{\frac{n}{2}}\bmod(F^\times)^2,$$

da $\det b$ ein Quadrat in $F^\times$ ist. Weil alle antisymmetrischen hyperbolischen Einheiten bzw. Formen äquivalent sind, folgt hieraus die zweite Aussage unter b)ii). q.e.d.

*3.2.* Wir betrachten nun speziell die endlichen Faktorgruppen der Gruppe $\mathcal{G}$ aus 1.1. Für ein Element $x$ einer (pro-)endlichen Gruppe bezeichne $\mathrm{Ord}_2 x$ den 2-Anteil der (supernatürlichen) Ordnung $\mathrm{Ord}\,x$ von $x$.

**Lemma 8.** *Sei $G$ eine endliche Gruppe mit Erzeugenden $\sigma$ und $\tau$, die der Relation $\sigma\tau\sigma^{-1}=\tau^{p^{f_0}}$ für eine ungerade Primzahl $p$ und $f_0\in\mathbb{N}$ genügen. Weiter sei $\alpha$: $G\to\mathbb{F}_p^\times$ ein beliebiger Charakter und $^*$ die Anti-Involution auf $\mathbb{F}_p[G]$ gemäß* (11). *Dann existiert genau dann eine symplektische Form bezüglich $^*$ auf $\mathbb{F}_p[G]$ (insbesondere auch eine hyperbolische symplektische Form), wenn eine der folgenden drei Bedingungen erfüllt ist:*

i) *Es gibt ein Element $\rho_0\in G$ mit $\mathrm{Ord}_2\rho_0=\mathrm{Ord}_2\alpha(\rho_0)\neq 1$.*

ii) *Es ist $f_0$ ungerade, $p\not\equiv 1(4)$, und für $\tau_2=\tau^{\pi_2}$ und $\sigma_2=\sigma^{\pi_2}$ gilt $\alpha(\tau_2)=1$, $\alpha(\sigma_2)=-1$ und $\sigma_2^2=\tau_2^{2x}$ für ein $x\in\mathbb{Z}_2$.*

iii) *Es ist $f_0$ ungerade und $\alpha(\tau)^{\frac{p-1}{2}}=-1$.*

*Beweis.* Die Elemente $\sigma_2$ und $\tau_2$ erzeugen eine 2-Sylowgruppe $G_2$ von $G$ und es gilt $\sigma_2\tau_2\sigma_2^{-1}=\tau_2^{p^{f_0}}$ (vgl. die Def. von $\pi_2$ in 2.1); insbesondere wird $[G_2,G_2]$ von $\tau_2^{p^{f_0}-1}$ erzeugt. Nach Lemma 6 gibt es genau dann eine symplektische (und dann auch eine hyperbolische) Form, wenn es ein $\bar{\rho}\in G_2^{ab}$ gibt mit $\mathrm{Ord}\,\bar{\rho}=\mathrm{Ord}\,\alpha(\bar{\rho})\neq 1$.

Ist dies der Fall, so gilt ohne Einschränkung $\mathrm{Ord}\,\bar{\rho}=2$; es gibt also ein $\rho=\tau_2^a\sigma_2^b\in G_2$ mit $\alpha(\rho)=-1$ und

$$\rho^2=\tau_2^{a(p^{f_0b}+1)}\sigma_2^{2b}=\tau_2^{(p^{f_0}-1)c}$$

für ein $c\in\mathbb{Z}$. Ist $f_0$ oder $b$ gerade oder $p\equiv 1(4)$, so ist $p^{f_0b}+1=2u$ mit ungeradem $u\in\mathbb{N}$, und mit $y=\dfrac{p^{f_0}-1}{2}cu^{-1}\in\mathbb{Z}_2$ und $\rho_0=\tau_2^{-y}\rho$ gilt $\rho_0^2=1$. Ist $\alpha(\tau_2^y)=1$, so erfüllt $\rho_0$ die Bedingungen unter i), während für $\alpha(\tau_2^y)=-1$ notwendig $f_0$ ungerade und $\alpha(\tau)^{\frac{p-1}{2}}=-1$ ist. Für $p\not\equiv 1(4)$ und ungerades $f_0$ und $b$ gilt offenbar $\sigma_2^2=\tau_2^{2x}$ mit einem $x\in\mathbb{Z}$. Für $\alpha(\tau_2)=-1$ ist $\alpha(\tau)^{\frac{p-1}{2}}=-1$, während für $\alpha(\tau_2)=1$ notwendig $\alpha(\sigma_2)=\alpha(\rho)=-1$ ist.

Bezeichnet $\bar{\rho}$ die Restklasse eines Elementes $\rho\in G$ in $G^{ab}$, so folgt die Umkehrung aus den Ungleichungen $\mathrm{Ord}_2\alpha(\rho_0)\leqq\mathrm{Ord}_2\bar{\rho}_0\leqq\mathrm{Ord}_2\rho_0=\mathrm{Ord}_2\alpha(\rho_0)$ für i) und $2=\mathrm{Ord}\,\alpha(\tau)^{\frac{p-1}{2}}=\mathrm{Ord}\,\alpha(\tau_2)^{\frac{p^{f_0}-1}{2}}\leqq\mathrm{Ord}\,\bar{\tau}_2^{\frac{p^{f_0}-1}{2}}\leqq 2$ für iii). Im Falle ii) ist $[G_2,G_2]=\langle\tau_2^2\rangle$ und daher $\mathrm{Ord}\,\bar{\sigma}_2=2=\mathrm{Ord}\,\alpha(\sigma_2)$. q.e.d.

*Bemerkung.* Wenn $G$ zerfallend ist (d.h., die Gruppenerweiterung $1\to\langle\tau\rangle\to G\to G/\langle\tau\rangle\to 1$ zerfällt), ordnet sich ii) der Bedingung i) unter. Dies liefert eine wesentlich einfachere Version von Satz 8 in [15]. Da die Ordnungen der Bilder unter $\alpha$ immer $p-1$ teilen, bleibt nur die Bedingung iii), falls die 2-Anteile der Ordnungen von $\langle\tau\rangle$ und $G/\langle\tau\rangle$ größer sind als der 2-Anteil von $(p-1)$.

**Lemma 9.** *Mit den Voraussetzungen und Bezeichnungen aus Lemma 8 gilt: Setzt man für ein $\rho\in G$, dessen Ordnung prim zu p ist,*

$$E(\rho)=E_\alpha(\rho)=\frac{1}{\mathrm{Ord}\,\rho}\sum_{i=1}^{\mathrm{Ord}\,\rho}\rho^{2i}\alpha(\rho)^{-i},$$

*so sind für beliebige $c_1$, $c_2$, $c_3$, $c_4\in\mathbb{F}_p^\times$ die folgenden Elemente aus $\mathbb{F}_p[G]$ hyperbolische antisymmetrische Einheiten:*

*Im Fall* i):

$$d=c_1(\rho_0-\rho_0^*).$$

*Im Fall* ii):

$$d=c_1(\sigma_2-\sigma_2^*)+c_2(\tau_2^x-(\tau_2^x)^*)E(\sigma_2).$$

*Im Fall* iii):

$$d=c_1(\tau_2^{p+1}-(\tau_2^{p+1})^*)+c_2(\sigma_2\tau_2^a-(\sigma_2\tau_2^a)^*)E(\tau_2^{p+1})$$
$$+[c_3(\sigma_2\tau_2^b-(\sigma_2\tau_2^b)^*)+c_4(\tau_2^{\frac{p+1}{2}}-(\tau_2^{\frac{p+1}{2}})^*)]E(\sigma_2\tau_2^a)E(\tau_2^{p+1}),$$

*falls a, b Elemente aus* $\mathbb{Z}$ *sind mit*

$$-\alpha(\sigma_2\tau_2^a)\in(\mathbb{F}_p^\times)^2, \qquad -\alpha(\sigma_2\tau_2^b)\notin(\mathbb{F}_p^\times)^2.$$

*Beweis.* Wir beweisen nur i) und iii); der Fall ii) ist ähnlich wie iii).

i) $d$ ist bereits Einheit in $\mathbb{F}_p[\langle\rho_0\rangle]$, da es hierin kein Nullteiler ist. Denn für ein $a\in\mathbb{F}_p[\langle\rho_0\rangle]$ mit $da=0$ ist $\rho_0^2 a=\alpha(\rho_0)a$, also

$$a=\rho_0^{\mathrm{Ord}\,\rho_0}a=\alpha(\rho_0)^{\frac{\mathrm{Ord}\,\rho_0}{2}}a=-a$$

und damit $a=0$. Weiter ist $d$ hyperbolisch, denn für $e=\frac{1}{2}(1+\rho_0^{\frac{\mathrm{Ord}\,\rho_0}{2}})$ gilt $e^2=e$ und $ed+de^*=d(e+e^*)=d$.

iii) Da $\sigma_2\tau_2\sigma_2^{-1}=\tau_2^{p^{f_0}}$ ist und $d$ in der von $\sigma_2$ und $\tau_2$ erzeugten 2-Sylowgruppe $G_2$ liegt, ist ohne Einschränkung $G=G_2$, $\sigma=\sigma_2$ und $\tau=\tau_2$. Für $\rho\in G$ ist dann $E(\rho)=\dfrac{1}{(G:1)}\sum\limits_{i=1}^{(G:1)}\rho^{2i}\alpha(\rho)^{-i}$, und es gelten die folgenden Tatsachen:

(13) Es ist $\rho^2E(\rho)=\alpha(\rho)E(\rho)$ bzw. $(\rho-\rho^*)E(\rho)=0$, insbesondere sind die $E(\rho)$ Idempotente; außerdem gilt $E(\rho)^*=E(\rho)$.

(14) Ist für ein zentrales Idempotentes $E_0$ das Idempotente $(1-E(\rho))E_0$ zentral, so ist $(\rho-\rho^*)(1-E(\rho))E_0$ eine Einheit in $\mathbb{F}_p[G](1-E(\rho))E_0$; dies folgt aus der Beziehung

$$(\rho-\rho^*)\frac{-1}{\mathrm{Ord}\,\rho}\rho\,\alpha(\rho)^{-1}[1+(1+\rho^2\alpha(\rho)^{-1})+(1+\rho^2\alpha(\rho)^{-1}+\rho^4\alpha(\rho)^{-2})$$

$$+\ldots+(1+\rho^2\alpha(\rho)^{-1}+\ldots+\rho^{2\,\mathrm{Ord}\,\rho-2}\alpha(\rho)^{-(\mathrm{Ord}\,\rho-1)})]=1-E(\rho).$$

(15) Alle Idempotenten aus $\mathbb{F}_p[\langle\tau\rangle]$ sind zentral in $\mathbb{F}_p[G]$, denn für $x\in\mathbb{F}_p[\langle\tau\rangle]$ gilt $\sigma x\sigma^{-1}=x^q$.

(16) Es gilt $\tau^{p^2-1}E(\tau^{p+1})=E(\tau^{p+1})$ und daher $\sigma\tau\sigma^{-1}E(\tau^{p+1})=\tau^{p^{f_0}}E(\tau^{p+1})=\tau^pE(\tau^{p+1})$; denn $p^2-1$ teilt $p^{f_0-1}-1$, weil $f_0$ ungerade ist.

(17) $\sigma^2E(\tau^{p+1})$ und $\tau^{p+1}E(\tau^{p+1})$ sind zentral, denn es ist

$$\tau\sigma^2\tau^{-1}E(\tau^{p+1})=\tau\tau^{-p^2}\sigma^2E(\tau^{p+1})=\sigma^2E(\tau^{p+1})$$

und

$$\sigma\tau^{p+1}\sigma^{-1}E(\tau^{p+1})=\tau^{p^2+p}E(\tau^{p+1})=\tau^{p+1}E(\tau^{p+1}).$$

Insbesondere ist wegen $(\sigma\tau^a)^2=\tau^{(p^{f_0}+1)p^{f_0}a}\sigma^2$ das Element $E(\sigma\tau^a)E(\tau^{p+1})$ zentral.

(18) Setzt man $E(-\rho)=\dfrac{1}{(G:1)}\sum\limits_{i=1}^{(G:1)}\rho^{2i}\alpha(\rho)^{-i}(-1)^i$, so gilt $\rho^2E(-\rho)=-\alpha(\rho)E(-\rho)$, insbesondere ist $E(-\rho)$ ein Idempotentes mit $E(\rho)+E(-\rho)=E(\rho^2)$ und $E(\rho)E(-\rho)=0$.

Wir setzen zur Abkürzung $g=\alpha(\sigma)$, $h=\alpha(\tau)$, $A=\mathbb{F}_p[G]$, $E_1=E(\tau^{p+1})$ und $E_2=E(\sigma\tau^a)$ sowie

$$A_1=A(1-E_1), \qquad A_2=A(1-E_2)E_1, \qquad A_3=AE_2E_1.$$

Dann ist offenbar $d=d_1+d_2+d_3$ mit

$$d_1=c_1(\tau^{p+1}-(\tau^{p+1})^*)(1-E_1)\in A_1,$$

$$d_2=c_2(\sigma\tau^a-(\sigma\tau^a)^*)(1-E_2)E_1\in A_2$$

und

$$d_3=[c_3(\sigma\tau^b-(\sigma\tau^b)^*)+c_4(\tau^{\frac{p+1}{2}}-(\tau^{\frac{p+1}{2}})^*)]E_2E_1\in A_3.$$

Nach (13), (15) und (17) sind die Idempotenten zentral und symmetrisch bezüglich *, daher sind offenbar $d_1$, $d_2$ und $d_3$ antisymmetrisch. Weiter sind $d_1$ und $d_2$ wegen (14) Einheiten in $A_1$ bzw. $A_2$. Bilden wir die zentralen Idempotenten $E_1^{\pm}=E(\pm\tau^{\frac{p+1}{2}})$, so gilt $E_1=E_1^+ + E_1^-$ sowie

$$(19)\qquad (\tau^{\frac{p+1}{2}}-(\tau^{\frac{p+1}{2}})^*)E_1^+=0 \quad \text{bzw.} \quad \tau^{p+1}E_1^+=h^{\frac{p+1}{2}}E_1^+=-hE_1^+,$$

$$(\tau^{\frac{p+1}{2}}-(\tau^{\frac{p+1}{2}})^*)E_1^-=2\tau^{\frac{p+1}{2}}E_1^- \quad \text{bzw.} \quad \tau^{p+1}E_1^-=hE_1^-.$$

Da $a-b$ ungerade ist, gilt weiter mit (16)

$$(20)\quad (\sigma\tau^b-(\sigma\tau^b)^*)E_2E_1^+=\sigma\tau^b(1-\tau^{(p+1)(a-b)}\tau^{-(p+1)a}\sigma^{-2}gh^b)E_2E_1^+$$
$$=\sigma\tau^b(1+h^{(a-b)}h^{-a}g^{-1}gh^b)E_2E_1^+=2\sigma\tau^bE_2E_1^+$$
$$\text{sowie } (\sigma\tau^b-(\sigma\tau^b)^*)E_2E_1^-=0.$$

Hieraus folgt

$$(21)\qquad d_3=2c_3\sigma\tau^bE_2E_1^+ + 2c_4\tau^{\frac{p+1}{2}}E_2E_1^-,$$

woraus man sehen kann, daß auch $d_3$ eine Einheit in $A_3$ ist.

Es bleibt zu zeigen, daß die $d_i$ hyperbolisch sind; dabei wird sich ergeben, daß es nur auf vier verhältnismäßig kleine Teilalgebren $B_1,\ldots,B_4$ von $A$ ankommt.

Im folgenden schreiben wir oft die zentralen Idempotenten, die eine Teilalgebra definieren, nicht mit, sondern benutzen nur die definierenden Gleichungen. Dies ist im folgenden Sinne korrekt: Mit (18) erhält man die Zerlegung

$$1=E(\rho)+\sum_{i=0}^{k-1}E(-\rho^{2^i}),\qquad \operatorname{Ord}\rho=2^k,$$

der Eins in orthogonale Idempotente, Sind nun für ein zentrales Idempotentes $E_0$ alle $E(-\rho^{2^i})E_0$ zentral, so ist $AE(\rho)E_0$ genau die Teilalgebra von $AE_0$, in der $\rho^2=\alpha(\rho)$ gilt; in $AE(-\rho^{2^i})E_0$ gilt gerade $\rho^{2^{i+1}}=-\alpha(\rho^{2^i})$ (diese Eigenschaften schließen sich aus).

Die Anti-Involution * permutiert die unzerlegbaren, paarweise orthogonale Idempotenten $e_1,\ldots,e_r$ von $\mathbb{F}_p[\langle\tau\rangle]$. Jedes $F_i=\mathbb{F}_p[\langle\tau\rangle]e_i$ ist ein Körper; der Grad $[F_i:\mathbb{F}_p]$ teilt dabei $\varphi(2^t)=2^{t-1}$ für $\operatorname{Ord}\tau=2^t$, ist also insbesondere eine 2-Potenz. Gilt $e_i^*=e_i$, so operiert * als Automorphismus auf $F_i$; es ist daher * die

Identität oder die Potenzierung mit $p^{2^m}$ für ein $m \geqq 0$. Im zweiten Fall gilt in $F_i$

$$\tau^* = \tau^{p^{2^m}} \quad \text{bzw.} \quad \tau^{p^{2^m}+1} = h,$$

und damit $\tau^{(p^{2^m}+1)(p-1)} = 1$. Für $m > 0$ ist $p^{2^m}+1 = 2u$ mit ungeradem $u$ und daher $\tau^{p^2-1} = \tau^{(p+1)(p-1)} = 1$. Da $F_i$ durch $\tau$ erzeugt wird, ist dann notwendig $[F_i : \mathbb{F}_p] \leqq 2$. In jedem Fall ist also $*$ die Identität oder die Potenzierung mit $p$ und somit $\tau^2 = h$ oder $\tau^{p+1} = h$ in $F_i$.

Die Summe $e_+$ der Idempotenten $e_i$ mit $e_i^* = e_i$ liegt daher in $A(E(\tau) + E(-\tau^{\frac{p+1}{2}}))$ und insbesondere in $A_2 \oplus A_3 = AE(\tau^{p+1})$, definiert durch die Gleichung $\tau^{2(p+1)} = h^{p+1} = h^2$. Die Summe $e_-$ der $e_j$ mit $e_j^* \neq e_j$ läßt sich in eine Summe $e_- = f_1 + f_2$ von zentralen Idempotenten mit $f_1^* = f_2$ aufspalten; daher ist auf $Ae_-$ jede Einheit $d$ hyperbolisch: es gilt $f_1 d + d f_1^* = d(f_1 + f_2) = d$ ($Ae_-$ ist ein hyperbolischer Ring, vgl. [16]). Dasselbe gilt auch für $A(1 - E(\tau) - E(-\tau^{\frac{p+1}{2}}))$ und insbesondere für $A_1 = A(1 - E(\tau^{p+1}))$.

Zerlegt man $A(E(\tau) + E(-\tau^{\frac{p+1}{2}}))$ in einfache Algebren, die Matrizenringe über endlichen Körpern sind, so gibt es nach Lemma 7 höchstens dort eine nicht-hyperbolische Einheit, wo $*$ trivial auf dem Zentrum operiert. (Man beachte, daß es auf $\mathbb{F}_p[G]$ (also auch auf jeder $*$-invarianten Faktoralgebra) nach Lemma 8 auf jeden Fall eine hyperbolische antisymmetrische Einheit gibt.) Nach (17) liegt $\sigma^2$ im Zentrum von $A_2 \oplus A_3$, es muß also gelten

$$\sigma^2 = (\sigma^2)^* \quad \text{bzw.} \quad \sigma^4 = g^2.$$

Daher sind nur noch die folgenden Teil-Algebren zu betrachten:

$$B_1 = AE(\sigma)E(\tau): \qquad \tau^2 = h, \quad \sigma^2 = g,$$

$$B_2 = AE(-\sigma)E(\tau): \qquad \tau^2 = h, \quad \sigma^2 = -g,$$

$$B_3 = AE(\sigma)E(-\tau^{\frac{p+1}{2}}): \quad \tau^{p+1} = h, \quad \sigma^2 = g,$$

$$B_4 = AE(-\sigma)E(-\tau^{\frac{p+1}{2}}): \quad \tau^{p+1} = h, \quad \sigma^2 = -g.$$

$B_1$ und $B_2$ liegen in $AE_1^+$, $B_3$ und $B_4$ liegen in $AE_1^-$. Weiter gilt $B_3 = AE_2E_1^-$ und folglich $B_4 \subseteq A_2$. Für gerades $a$ folgt aus den Relationen von $B_1$

$$(\sigma\tau^a)^2 = \sigma^2 \tau^{(p+1)a} = g(-h)^a = g h^a,$$

es gilt also $B_1 \subseteq AE_2E_1^+$ und analog $B_2 \subseteq (1-E_2)E_1^+ \subseteq A_2$. Für ungerades $a$ ist entsprechend $B_1 \subseteq A_2$ und $B_2 \subseteq AE_2E_1^+$. Schließlich gilt noch für $c \in \mathbb{Z}$

$$\text{auf } B_1\text{: } \sigma\tau^c - (\sigma\tau^c)^* = \sigma(\tau^c - (-\tau)^c) = \begin{cases} 0 & c \text{ gerade,} \\ 2h^{\frac{c-1}{2}}\sigma\tau, & c \text{ ungerade,} \end{cases}$$

$$\text{auf } B_2\text{: } \sigma\tau^c - (\sigma\tau^c)^* = \sigma(\tau^c + (-\tau)^c) = \begin{cases} 2h^{\frac{c}{2}}\sigma, & c \text{ gerade,} \\ 0, & c \text{ ungerade,} \end{cases}$$

und auf $B_4$: $\sigma\tau^a - (\sigma\tau^a)^* = \sigma\tau^a(1 - \tau^{-a(p+1)}\sigma^{-2} g h^a) = 2\sigma\tau^a$.

Es ist nun leicht nachzurechnen, daß $d_2+d_3$ auf den Algebren $B_i$ die folgende Gestalt $\Delta_i$ hat, wobei für die Elemente $\varepsilon_i$ gilt:

$$\varepsilon_i^2=\varepsilon_i, \qquad \varepsilon_i\Delta_i+\Delta_i\varepsilon_i^*=\Delta_i.$$

| Algebra $B_i$ | Relationen | $\Delta_i$ | $\varepsilon_i$ |
|---|---|---|---|
| $B_1$ | $\tau^2=h$<br>$\sigma^2=g$ | $a_1\sigma\tau$ | $\frac{1}{2}(\mu_1\tau+\nu_1\sigma)$<br>mit $\mu_1^2h+\nu_1^2g=1$ |
| $B_2$ | $\tau^2=h$<br>$\sigma^2=-g$ | $a_2\sigma$ | $\frac{1}{2}(1+\mu_2\tau+\nu_2\sigma)$<br>mit $\mu_2^2h-\nu_2^2=1$ |
| $B_3$ | $\tau^{p+1}=h$<br>$\sigma^2=g$ | $a_3\tau^{\frac{p+1}{2}}$ | $\frac{1}{2}(1+\mu_3\tau^{\frac{p+1}{2}}+\nu_3\sigma)$<br>mit $\mu_3^2h+\nu_3h=1$ |
| $B_4$ | $\tau^{p+1}=h$<br>$\sigma^2=-g$ | $a_3\sigma\tau^a$ | $\frac{1}{2}(1+\mu_4\sigma\tau^a)$<br>mit $-\mu_4^2gh^a=1$ |

wobei $a_1, \ldots, a_4$ gewisse Elemente aus $\mathbb{F}_p^\times$ sind. Die Gleichungen für die $\mu_i$ und $\nu_i$ sind immer mit $\mu_i, \nu_i \in \mathbb{F}_p^\times$ lösbar - die für $\mu_4$ aufgrund der Voraussetzung an $a$. Die antisymmetrische Einheit $d$ ist also auch hyperbolisch auf $B_1 \oplus B_2 \oplus B_3 \oplus B_4$ und damit auf ganz $A$.

Ein konzeptionellerer Beweis der letzten Tatsache ohne die Benutzung der $\varepsilon_i$ ergibt sich folgendermaßen. Die Algebren $B_1$ bis $B_4$ lassen sich jeweils in die Teile $F_i \oplus F_i\sigma$ aufspalten, $F_i=\mathbb{F}_p[\langle\tau\rangle]e_i$, wobei nur die $F_i$ mit $[F_i:\mathbb{F}_p]=2$ auftreten. Setzt man $\rho_i=\sigma\beta_i$ für ein $\beta_i \in F_i$ mit $N(\beta_i)=N_{F_i/\mathbb{F}_p}(\beta_i)=\sigma^{-2}\in\mathbb{F}_p$, so gilt $\rho_i^2=\sigma^2\beta_i^{p+1}=\sigma^2N(\beta_i)=1$ und $\rho_i x\rho_i^{-1}=x^p$ für $x\in F_i$. Es ist also $F_i\oplus F_i\sigma$ isomorph zum getwisteten Gruppenring $F_i(\langle\rho_i\rangle)$. Für diesen gilt aber die Isomorphie

$$F_i(\langle\rho_i\rangle) \xrightarrow[\sim]{\varphi} \mathrm{End}_{\mathbb{F}_p}(F_i)=M_2(\mathbb{F}_p),$$

indem man $x\in F_i$ mit $\varphi$ auf die Homothetie mit $x$ abbildet und $\rho_i$ auf den Frobenius-Automorphismus (s. [1], Chap. 12, Ex. 16). Unter $\varphi$ gilt daher $\det\rho_i=-1$ (dies folgt aus der Existenz einer Normalbasis für $F_i/\mathbb{F}_p$) und $\det x=N(x)$ für $x\in F_i$. Insbesondere gilt

$$\begin{aligned}
&\det\tau=h^{\frac{p+1}{2}}=-h && \text{in } B_1 \text{ und } B_2,\\
&\det\tau=h && \text{in } B_3 \text{ und } B_4,\\
&\det\sigma=\det\rho_iN(\beta_i)^{-1}=-\sigma^2.
\end{aligned}$$

Mit Lemma 7b) folgt nun leicht, daß auf $B_1$, $B_2$ und $B_3$ auch noch alle antisymmetrischen Einheiten äquivalent und damit hyperbolisch sind (auf $B_1$ und $B_2$ sind 1 und $\tau$ zwei nichtäquivalente symmetrische Einheiten, auf $B_3$ gilt dies für $\sigma$ und $\sigma\tau$), während auf $B_4$ gerade $\det\sigma\tau^a=gh^a$ gilt; wegen Lemma 7b) ii) und der Voraussetzung an $a$ ist daher $\sigma\tau^a$ hyperbolisch. q.e.d.

*Bemerkungen.* a) Die am Schluß des Beweises verwendete Methode zeigt noch, daß es auf $\mathbb{F}_p[G_2]$ gerade so viele Äquivalenzklassen von symplektischen Formen gibt wie auf $B_4$; die Anzahl ist $2^{(\mathrm{Ord}\,\tau_2, p+1)/2}$.

b) In [6], Lemma 45 und [10], Theorem 1, wurden für die oben betrachteten Gruppenringe Elemente angegeben, die hyperbolische symplektische Formen definieren sollen. Dies ist aber nicht nur in der Herleitung falsch ([6], Proposition 2 und [10], Lemmata 2, 3) sondern auch im Ergebnis. Beide Male sind z.B. die Formen nicht hyperbolisch (auf dem dortigen $A_1$), und in [10] ist die Antisymmetrie (auf $A_2$) verletzt.

## § 4. Ende des Beweises von Theorem 1 für ungerades $n$

Es war nur noch zu zeigen, daß das Cupprodukt durch die Gestalt von $y_1$ auf dem Teil $C_0 = \langle \chi_1 \rangle_{\mathbb{F}_p[G]} \cong \mathbb{F}_p[G]$ eine hyperbolische symplektische Form definiert. Es ist wieder $\alpha$ der Charakter, den $\beta$ liftet, und * die Anti-Involution gemäß (10) auf $\mathbb{F}_p[G]$.

**Lemma 10.** *Gilt* $y_1 \equiv x_1^{\delta} \bmod P^p[P, U_{\mathscr{K}}]$ *für ein* $\delta \in \mathbb{F}_p[G]$, *so definiert das Cupprodukt auf* $C_0$ *die (gemäß (12) gebildete) Form* $\phi_d$ *mit* $d = (\delta^0)^* - \delta^0$, *wobei* $^0$ *die durch* $\rho^0 = \rho^{-1}$, $\rho \in G$, *definierte Anti-Involution auf* $\mathbb{F}_p[G]$ *ist.*

*Beweis.* Ist $\delta = \sum_{\rho \in G} c_\rho \rho$ und $\gamma \in G$, so gilt

$$\begin{aligned}
[\tilde{x}_1, \tilde{y}_1]^{\kappa_{\mathscr{K}} \lambda_{\mathscr{K}} e} &\equiv [\tilde{x}_1, \tilde{x}_1^{\delta}]^{\sum_{\rho \in G} \beta(\rho)\rho} \\
&\equiv [\tilde{x}_1, \tilde{x}_1^{c_\gamma \gamma}] [\tilde{x}_1^{\gamma}, \tilde{x}_1^{c_{\gamma^{-1}}}]^{\alpha(\gamma)} \prod_{(\rho,\rho') \neq (1,\gamma),(\gamma,1)} [\tilde{x}_1^{\rho}, \tilde{x}_1^{\rho'}]^{a_{\rho\rho'}} \\
&\equiv [\tilde{x}_1, \tilde{x}_1^{\gamma}]^{c_\gamma - c_{\gamma^{-1}} \alpha(\gamma)} \prod [\tilde{x}_1^{\rho}, \tilde{x}_1^{\rho'}]^{a_{\rho\rho'}} \bmod \tilde{X}_{\mathscr{K}}^2.
\end{aligned}$$

Mit Lemma 1 folgt daher, daß das Cupprodukt auf $C_0$ eine antisymmetrische, invariante $\mathbb{F}_p$-Bilinearform $\psi$ induziert mit

$$\psi(x_1, \gamma x_1) = c_\gamma - c_{\gamma^{-1}} \alpha(\gamma).$$

Andererseits ist für $d = \sum_{\rho \in G} d_\rho \rho$

$$\phi_d(x_1, \gamma x_1) = \ell(d\gamma^{-1} \alpha(\gamma)) = d_\gamma \alpha(\gamma).$$

Da beide Bilinearformen aufgrund der Invarianz durch diese Werte für $\gamma \in G$ bestimmt sind, folgt die Gleichheit für $d_\gamma = c_\gamma \alpha(\gamma)^{-1} - c_{\gamma^{-1}}$. q.e.d.

Ähnlich wie in 2.3 zeigt man nun, daß für $\rho \in \mathscr{G}$, $p \nmid \mathrm{Ord}\,\rho$, das Element $\{x_1, \rho\}$ aus $P$ ist und die Kongruenz

$$\{x_1, \rho\} = \{x_1, \rho\}_\beta \equiv x_1^{E_{\alpha^{-1}}(\rho)} \bmod P^p[P, U_{\mathscr{K}}]$$

erfüllt. Für

$$y^1 = x_1^{\tau_2^{p+1}} \{x_1, \tau_2^{p+1}\}^{\sigma_2 \tau_2^a} \{\{x_1, \tau_2^{p+1}\}, \sigma_2 \tau_2^a\}^{\sigma_2 \tau_2^b + \tau_2^{\frac{p+1}{2}}}$$

gilt insbesondere $y_1 \equiv x_1^\delta \bmod P^p[P, U_{\mathscr{H}}]$ mit

$$\delta = \tau_2^{p+1} + \sigma_2\tau_2^a E_{\alpha^{-1}}(\tau_2^{p+1}) + (\sigma_2\tau_2^b + \tau_2^{\frac{p+1}{2}}) E_{\alpha^{-1}}(\sigma_2\tau_2^a) E_{\alpha^{-1}}(\tau_2^{p+1}).$$

Weiter ist

$$\begin{aligned}(\delta^0)^* - \delta^0 &= \alpha(\tau_2^{p+1})^{-1}(\tau_2^{p+1} - (\tau_2^{p+1})^*) + \alpha(\sigma_2\tau_2^a)^{-1}(\sigma_2\tau_2^a - (\sigma_2\tau_2^a)^*) E_\alpha(\tau_2^{p+1}) \\ &\quad + [\alpha(\sigma_2\tau_2^b)^{-1}(\sigma_2\tau_2^b - (\sigma_2\tau_2^b)^*) + \alpha(\tau_2^{\frac{p+1}{2}})^{-1}(\tau_2^{\frac{p+1}{2}} - (\tau_2^{\frac{p+1}{2}})^*)] \\ &\quad \cdot E_\alpha(\sigma_2\tau_2^a) E_\alpha(\tau_2^{p+1}).\end{aligned}$$

Lemma 9 zeigt daher: Ist $f_0$ ungerade, $\alpha(\tau)^{\frac{p-1}{2}} \equiv -1(p)$, $-\alpha(\sigma\tau^a) \bmod p \in (\mathbb{F}_p^\times)^2$ und $-\alpha(\sigma\tau^b) \bmod p \notin (\mathbb{F}_p^\times)^2$, so ist $d = (\delta^0)^* - \delta^0$ eine antisymmetrische hyperbolische Einheit, bzw. $\phi_d$ eine hyperbolische symplektische Form auf $C_0 \cong \mathbb{F}_p[G]$. Damit ist Theorem 1 auch für ungerades $n$ bewiesen.

## § 5. Äußere Automorphismen von $G_k$ und Ergänzungen

*5.1.* Es soll zunächst ein äußerer Automorphismus von $G_{\mathbb{Q}_p}$ konstruiert werden. Nach dem Beispiel a) zu Theorem 2 ist $G_{\mathbb{Q}_p}$ isomorph zur pro-endlichen Gruppe $F(x_0, x_1; \mathscr{G})/(r)$ mit

$$r = x_0^{-\sigma}(x_0, \tau) x_1^p [x_1, y_1] \equiv x_0^{-\sigma}(x_0, \tau)[x_1, x_1^\delta] \bmod P^2$$

für ein $\delta \in \mathbb{F}_p[\![\mathscr{G}]\!] = \varprojlim_{\mathscr{H} \lhd \mathscr{G} \text{ offen}} \mathbb{F}_p[\mathscr{G}/\mathscr{H}]$. Für den Automorphismus $\psi$ von $F(x_0, x_1; \mathscr{G})$ mit

$$\psi(\sigma) = \sigma, \quad \psi(\tau) = \tau, \quad \psi(x_0) = x_0, \quad \psi(x_1) = x_1^{1+p}$$

gilt die Kongruenz $\psi(r) \equiv r \bmod P^2$. Daher induziert $\psi$ einen Automorphismus $\bar{\psi}$ von $G_{\mathbb{Q}_p}/V^2$ für $V = P/(r) = \operatorname{Ker}(G_{\mathbb{Q}_p} \twoheadrightarrow \mathscr{G})$, der $V/V^2$ in sich abbildet und somit mit der Projektion auf $\mathscr{G}$ verträglich ist. Nach Satz 2 aus [19] läßt sich $\bar{\psi}$ zu einem Automorphismus $\tilde{\psi}$ von $G_{\mathbb{Q}_p}$ liften. Bezeichnet $\bar{x}_1$ das Bild von $x_1$ in $V$, so gilt $\tilde{\psi}(\bar{x}_1) \equiv \bar{x}_1^{1+p} \bmod V^2$. Wäre nun $\tilde{\psi}$ ein innerer Automorphismus, so gäbe es ein $y \in G_{\mathbb{Q}_p}$ mit $\tilde{\psi}(\bar{x}_1) = \bar{x}_1^y$. Da $\bar{x}_1$ in $V/V^1$ einen freien $\mathbb{F}_p[\![\mathscr{G}]\!]$-Modul erzeugt, muß $y \in V$ sein und damit

$$\bar{x}_1^{1+p} \equiv \bar{x}_1 \bmod [V, V].$$

Dies stellt einen Widerspruch zur Torsionsfreiheit von $V^{\mathrm{ab}}$ dar.

Für p-adische Zahlkörper $k \neq \mathbb{Q}_p$ induziert der Automorphismus $\psi$ von $F(x_0, \ldots, x_n; \mathscr{G})$ mit $\psi(\sigma) = \sigma$, $\psi(\tau) = \tau$, $\psi(x_i) = x_i$ für $i \neq n$ und $\psi(x_n) = x_n x_{n-1}$ direkt einen äußeren Automorphismus von $G_k = F(x_0, \ldots, x_n; \mathscr{G})/(r)$, da $\psi(r) = r$ gilt.

5.2. Durch die Untersuchungen in §4 ist es möglich, notwendige und hinreichende Bedingungen für die Existenz einer Demuškinformation zu vorgegebenem $\mathcal{G}, n, s, \alpha$ anzugeben und sie in allen Fällen explizit zu beschreiben. Es zeigt sich, daß die Voraussetzung (+) keine große Einschränkung bedeutete.

**Theorem 3.** *Es gibt genau dann eine Demuškinformation über $\mathcal{G}$ vom Rang n mit Torsion $p^s$ und Charakter $\alpha$, wenn n gerade ist oder eine der Bedingungen* i)–iii) *aus Lemma* 8 *(entsprechend) für $\mathcal{G}$ und $\tilde{\alpha}: \mathcal{G} \to (\mathbb{Z}/p^s)^\times \twoheadrightarrow \mathbb{F}_p^\times$ erfüllt ist.*

*In den noch nicht behandelten Fällen* i) *und* ii) *für ungerades n, erhält man eine explizite Beschreibung wie folgt: Wird eine Relation r wie in* 1.2 *für ungerades n definiert mit*

$$y_1 = x_1^{\rho_0} \qquad \textit{im Fall i)},$$
$$y_1 = x_1^{q_2}\{x_1, \sigma_2\}^{\tau_2^x} \qquad \textit{im Fall ii)},$$

*so ist $F(x_0, \ldots, x_n; \mathcal{G})/(r)$ eine Demuškinformation über $\mathcal{G}$ mit Invarianten n, s und $\alpha$.*

*Beweis.* Aus der Bedingung II folgt mit dem Corollar zu Lemma 3, daß für jeden offenen Normalteiler $\mathcal{H} \subseteq \operatorname{Ker}\alpha$ von $\mathcal{G}$ eine hyperbolische symplektische Struktur auf dem Gruppenring $\mathbb{F}_p[G]$, $G = \mathcal{G}/\mathcal{H}$, existiert (bzgl. $*_\alpha$), daß also für $G$ und den induzierten Charakter $\tilde{\alpha}: G \to \mathbb{F}_p^\times$ eine der drei Bedingungen von Lemma 8 erfüllt ist. Es ist nun leicht zu sehen, daß dann auch $\mathcal{G}$ (mindestens) einer dieser Bedingungen genügt.

Umgekehrt gilt für das oben definierte $y_1$ die Kongruenz

$$y_1 \equiv x_1^\delta \bmod P^p[P, U_{\mathcal{H}}] \quad \text{mit} \quad \delta = \rho_0 \qquad \text{im Fall i)},$$
$$\text{bzw.} \quad \delta = \sigma_2 + \tau_2^x E_{\alpha^{-1}}(\sigma_2) \quad \text{im Fall ii)}.$$

Analog dem bereits behandelten Fall iii) folgt mit Lemma 9 und Lemma 10 die Behauptung.

*Bemerkung.* a) Im Beispiel c) von §1 liegt gerade der Fall i) mit $\rho_0 = \tau$ vor, denn es ist $(p-1)_2 = \operatorname{Ord}_2 \tilde{\alpha}(\tau) \leqq \operatorname{Ord}_2 \tau \leqq [k(\zeta_p): k]_2 \leqq (p-1)_2$, wobei für eine natürliche Zahl $m$ der 2-Anteil mit $m_2$ bezeichnet ist.

b) Wenn die 2-Sylowgruppen von $\mathcal{G}$ nicht „zu klein" sind, nämlich wenn die 2-Anteile der super-natürlichen Ordnungen von $\langle\tau\rangle$ und $\mathcal{G}/\langle\tau\rangle$ größer sind als $(p-1)_2$ (insbesondere also für $\mathcal{G} = \langle\sigma, \tau | \sigma\tau\sigma^{-1} = \tau^q\rangle$), so ist Bedingung (+) aus 1.2 also hinreichend und notwendig für die Existenz einer Demuškinformation über $\mathcal{G}$.

## Literatur


1. Auslander, M., Buchsbaum, D.: Groups, Rings, Modules. New York: Harper and Row 1974
2. Binz, E., Neukirch, J., Wenzel, G.H.: A subgroup theorem for free products of pro-finite groups. J. Algebra **19**, 104–109 (1971)
3. Fröhlich, A., McEvett, A.M.: Forms over rings with involution. J. Algebra **12**, 79–104 (1969)
4. Hasse, H.: Zahlentheorie. Akademie-Verlag. Berlin: 1963
5. Iwasawa, K.: On Galois groups of local fields. Trans. Am. Math. Soc. **80**, 448–469 (1955)

6. Jakovlev, A.V.: The galois group of the algebraic closure of a local field. Math. USSR-Izv. **2**, 1231–1269 (1968)
7. Jakovlev, A.V.: Remarks on my paper "The galois groups of the algebraic closure of a local field". Math. USSR-Izv. **12**, 205–206 (1978)
8. Jakovlev, A.V.: Symplectic spaces with operators over commutative rings. Vestnik Leningr. Univ. Math. **2**, 339–346 (1976)
9. Jakovlev, A.V.: Symplectic-space structures on a module. Vestnik Leningr. Univ. Math. **4**, 65–72 (1977)
10. Jakovlev, A.V.: Structure of the multiplicative group of a simply ramified extension of a local field of odd degree. Math. USSR Sbornik **35**, 581–591 (1979)
11. Jannsen, U.: Über Galoisgruppen lokaler Körper. Invent. math. **70**, 53–69 (1982)
12. Koch, H.: Über Galoissche Gruppen von p-adischen Zahlkörpern. Math. Nachr. **29**, 77–111 (1965)
13. Koch, H.: Galoissche Theorie der $p$-Erweiterungen. VEB Deutscher Verlag der Wissenschaften. Berlin: 1970
14. Koch, H.: The galois group of a $p$-closed extension of a local field. Soviet. Math. Dokl. **19**, 10–13 (1978)
15. Koch, H.: Über Darstellungsräume und die Struktur der multiplikativen Gruppe eines $p$-adischen Zahlkörpers. Math. Nachr. **26**, 67–100 (1963)
16. McEvett, A.M.: Forms over Semisimple Algebres with Involution. J. Algebra **12**, 105–113 (1969)
17. Neukirch, J.: Freie Produkte pro-endlicher Gruppen und ihre Kohomologie. Arch. d. Math. **12**, 337–357 (1971)
18. Serre, J-P.: Cohomologie galoisienne. Lect. Notes in Math., Vol. 5. Berlin-Heidelberg-New York: Springer 1973
19. Wingberg, K.: Der Eindeutigkeitssatz für Demuškinformationen. Invent. math. **70**, 99–113 (1982)

Oblatum V-1981 & 25-V-1982