Die p-Vervollständigung der multiplikativen Gruppe einer p-Erweiterung eines irregulären $\mathfrak{p}$-adischen Zahlkörpers

Von *Uwe Jannsen* in Hamburg und *Kay Wingberg* in Berlin

Einleitung

Sei K/k eine endliche, galoissche p-Erweiterung $\mathfrak{p}$-adischer Zahlkörper über $\mathbb{Q}_p$ mit Galoisgruppe G. Die p-Vervollständigung

$$A(K) = \varprojlim K^* / K^{*p^n}$$

von K^* ist in natürlicher Weise ein $\mathbb{Z}_p[G]$-Modul. Im Fall eines regulären Grundkörpers k, d. h. k enthält keine p-ten Einheitswurzeln, wurde die Struktur von $A(K)$ in der Arbeit von Borevič [1] untersucht und für abelsche p-Erweiterungen in Erzeugenden und Relationen beschrieben. Für allgemeine p-Erweiterungen wurde dieser Fall in [8] gelöst. Ist der Grundkörper hingegen irregulär mit Irregularitätsexponenten $s \geqq 1$, d. h. k enthält genau die q-ten Einheitswurzeln, $q = p^s$, so wird die Beschreibung von $A(K)$ wesentlich komplizierter. Die $\mathbb{Z}_p[G]$-Modulstruktur wurde von Gerlovin in [4] vollständig mit Angabe der unzerlegbaren Bestandteile für zyklische p-Erweiterungen und $q \neq 2$ beschrieben. In der Arbeit von Borevič und El Musa [2] wird hinsichtlich der Beschreibung von $A(K)$ im allgemeinen Fall folgendes Resultat erzielt: Sei $q \neq 2$ und $1 \to R \to F \to G \to 1$ eine Darstellung von G durch eine freie pro-p-Gruppe F mit $n+2$ Erzeugenden, $n = [k : \mathbb{Q}_p]$, dann ist folgende Sequenz von $\mathbb{Z}_p[G]$-Moduln exakt:

$$0 \to R^{ab} \to A(K) \times \mathbb{Z}_p[G] \to C \to 0,$$

wobei C ein monogener, kohomologisch trivialer $\mathbb{Z}_p[G]$-Modul ist; weiter findet man ein $\xi \in \mathbb{Z}_p[G]$ und ein $w \in R^{ab}$, so daß unter Hinzufügen eines erzeugenden Elements e die $\mathbb{Z}_p[G]$-Isomorphie

$$A(K) \times Z_p[G] \cong (\mathbb{Z}_p[G]\, e \oplus R^{ab}) / \langle \xi e - w \rangle$$

gilt.

In der vorliegenden Arbeit wird nun $A(K)$ direkt untersucht und mit Hilfe kohomologischer Methoden die Zerlegung von $A(K)$ in unzerlegbare Bestandteile angegeben.

Sei $D = \mathrm{Gal}(k(p)/k)$ die Galoisgruppe des p-Abschlusses von k, dann induziert das Cupprodukt

$$\cup : H^1(D) \times H^1(D) \to H^2(D) \cong \mathbb{Z}/p\mathbb{Z}$$

0075-4102/79/0307-0025\$02.00

eine nicht-ausgeartete, antisymmetrische Bilinearform auf $H^1(D)$. Sei t die Dimension des Radikals des Teilraums $H^1(G)$ von $H^1(D)$ oder, äquivalent dazu, die Dimension des Radikals des Teilraums $K^{*p} \cap k^*/k^{*p}$ von k^*/k^{*p} bezüglich der nicht-ausgearteten, antisymmetrischen Bilinearform, die durch das Normrestsymbol

$$(\, , \,): k^*/k^{*p} \times k^*/k^{*p} \to \mathbb{Z}/p\mathbb{Z}$$

gegeben ist. Die Zahl t stellt eine Invariante der Körpererweiterung dar $(0 \leqq t \leqq d = \dim H^1(G))$. Es ist d die minimale Anzahl von Erzeugenden von G. Sei

$$1 \to R_d \to F_d \to G \to 1$$

eine minimale Darstellung von G durch eine freie pro-p-Gruppe F_d und $\tilde{K}$ der zyklotomische Zwischenkörper von K/k mit $p^\varkappa = [\tilde{K}:k]$, d. h. $\tilde{K} = k(\varrho')$, wobei ϱ' Einheitswurzel von maximaler p-Potenzordnung in K ist; dann gilt die $\mathbb{Z}_p[G]$-Modul-Isomorphie

$$A(K) \cong M \times \mathbb{Z}_p[G]^{n+2-(d+t)-\delta}, \quad \delta = \begin{cases} 0, & \varrho' \notin N_{K/k}(K^*)\, K^{*p} \\ 1, & \text{sonst} \end{cases},$$

wobei

$$M = (R_d^{ab} \times \mathbb{Z}_p[G]^{t+\delta})/\mathbb{Z}_p[G]$$

unzerlegbarer $\mathbb{Z}_p[G]$-Modul ist oder in die zwei unzerlegbaren Summanden

$$R_d^{ab} \quad \text{und} \quad M' \cong \mathbb{Z}_p[G]^{d+\delta}/\mathbb{Z}_p[G]$$

zerfällt. Im letzteren Fall ist notwendig $t = d$ und $\varrho' \in N_{K/\tilde{K}}(K^*)$. Für $d = 1$ ergeben sich wieder die entsprechenden Ergebnisse von Gerlovin für zyklische Erweiterungen.

I. Kohomologie von Gruppenerweiterungen

Sei D eine unendliche Gruppe mit der Eigenschaft

(E) $\quad \forall H \leqq D \; \forall R$ normal in H, $(H:R) < \infty$ gilt mit $g := H/R$

a) $H^1(g, R^{ab}) = 0$

b) $H^2(g, R^{ab}) \cong \mathbb{Z}/(g:1)\mathbb{Z}$

c) der 2-Kozykel χ, der der Gruppenerweiterung $1 \to R^{ab} \to H/[R, R] \to g \to 1$ zugeordnet ist, erzeugt $H^2(g, R^{ab})$.

Bekanntlich gilt der

Satz 1. 1. *Sei D eine Gruppe mit der Eigenschaft (E), so gilt mit den obigen Bezeichnungen*

$$H^3(g, R^{ab}) = 0.$$

Nach den Ergebnissen von J. Tate und Y. Kawada, [6], Th. 6, S. 103, und Th. B, S. 93, gelten die Sätze:

Satz 1. 2. *Sei D eine freie (pro-p-)Gruppe, dann hat D die Eigenschaft (E).*

Satz 1. 3. *Sei k ein $\mathfrak{p}$-adischer Zahlkörper und $D = \mathrm{Gal}(k(p)/k)$ die Galoisgruppe des p-Abschlusses, so hat D die Eigenschaft (E).*

Sei im folgenden G eine endliche Gruppe und K ein Integritätsbereich; mit $\mathfrak{A}_G$ bzw. $\mathfrak{A}_{K[G]}$ wollen wir die Menge aller endlich erzeugten G- bzw. $K[G]$-Moduln A bezeichnen, für die für alle Untergruppen g von G gilt:

a) $H^1(g, A) = 0$

b) $H^2(g, A) \cong \mathbb{Z}/(g:1)\mathbb{Z}$

c) $H^2(G, A) \xrightarrow{\mathrm{res}} H^2(g, A)$ ist surjektiv.

Mit (R, F) wollen wir eine Darstellung von G

$$1 \to R \to F \to G \to 1$$

durch eine freie Gruppe F und einen Normalteiler R bezeichnen.

Satz 1. 4. *Für alle $A \in \mathfrak{A}_G$ gibt es eine freie Darstellung (R, F) von G und eine exakte Sequenz*

$$0 \to X_R \to R^{ab} \to A \to 0$$

mit einem kohomologisch trivialen, torsionsfreien G-Modul X_R.

Beweis. Sei $\chi_E \in H^2(G, A)$ ein erzeugendes Element, dem die Gruppenerweiterung

$$1 \to A \to E \to G \to 1$$

zugeordnet ist; sei ferner (R, F) eine freie Darstellung von G, für die es eine Surjektion $\varphi: F \twoheadrightarrow E$ gibt. Dann ist

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] & E \arrow[r] & G \arrow[r] & 1 \\
1 \arrow[r] & R^{ab} \arrow[r] \arrow[u, two heads, "\bar{\varphi}"] & F/[R,R] \arrow[r] \arrow[u, two heads] & G \arrow[r] \arrow[u, equal] & 1
\end{tikzcd}$$

ein kommutatives Diagramm mit exakten Zeilen. Nach 1.2 gibt es ein erzeugendes Element χ_F von $H^2(G, R^{ab})$ und es gilt

$$H^2(\bar{\varphi})(\chi_F) = \chi_E;$$

also ist ebenfalls wegen 1.2 $\mathrm{res}\, H^2(\bar{\varphi})$ ein Isomorphismus von $H^2(g, R^{ab})$ auf $H^2(g, A)$. Sei $X_R = \mathrm{Ker}\,\bar{\varphi}$; aus der kurzen exakten Sequenz

$$0 \to X_R \to R^{ab} \to A \to 0$$

folgt wegen $H^1(g, A) = 0 = H^3(g, R^{ab})$ die exakte Kohomologiesequenz

$$0 \longrightarrow H^2(g, X_R) \longrightarrow H^2(g, R^{ab}) \xrightarrow{\sim} H^2(g, A) \longrightarrow H^3(g, X_R) \longrightarrow 0,$$

also $H^2(g, X_R) = H^3(g, X_R) = 0$ für alle $g \leqq G$. Das bedeutet aber, daß X_R kohomologisch trivial ist, und aus der Torsionsfreiheit von R^{ab} folgt die von X_R.

Bemerkung. Offenbar kann in Satz 1. 4 ein F mit endlich vielen Erzeugenden gewählt werden (wir schreiben F_n bei n freien Erzeugenden). Ist G eine p-Gruppe und $A=\mathfrak{A}_{\mathbb{Z}_p[G]}$, so gilt 1. 4 noch, wenn die freie Gruppe F durch eine freie pro-p-Gruppe ersetzt wird.

Lemma 1. 5. *Seien A und C endlich erzeugte $K[G]$-Moduln und A $K[G]$-projektiv, C K-projektiv, dann gilt*

$$\mathrm{Ext}(C, A)=0.$$

Beweis. K. Gruenberg, [5], Prop. 3, S. 224.

Lemma 1. 6. *Sei X ein kohomologisch trivialer, endlich erzeugter $\mathbb{Z}_p[G]$-Modul und $\mathbb{Z}_p$-frei, G eine p-Gruppe, dann ist X $\mathbb{Z}_p[G]$-frei.*

Beweis. Betrachte die exakte Sequenz

$$0 \longrightarrow X \xrightarrow{p} X \longrightarrow X/pX \longrightarrow 0,$$

dann ist $H^1(G, X/pX)=0$, also $X/pX \cong \mathbb{Z}/p\mathbb{Z}[G]^r$, $r\in\mathbb{N}$, und mit dem Lemma von Nakayama erhalten wir $X\cong\mathbb{Z}_p[G]^r$.

Korollar 1. 7. *Sei $A\in\mathfrak{A}_{\mathbb{Z}_p[G]}$ und torsionsfrei, G eine p-Gruppe, so gibt es eine Darstellung (R, F) von G durch eine freie pro-p-Gruppe F und ein $r\in\mathbb{N}$, so daß folgende $\mathbb{Z}_p[G]$-Isomorphie gilt:*

$$R^{ab}\cong A\times\mathbb{Z}_p[G]^r.$$

Beweis. Wegen 1. 4 gibt es einen kohomologisch trivialen, $\mathbb{Z}_p$-freien Modul X_R, der nach Lemma 1. 6 $\mathbb{Z}_p[G]$-frei ist, also $X_R=\mathbb{Z}_p[G]^r$, mit

$$0\to\mathbb{Z}_p[G]^r\to R^{ab}\to A\to 0.$$

Da A torsionsfrei, also $\mathbb{Z}_p$-frei ist, folgt nach Lemma 1. 5 die Behauptung.

Korollar 1. 8. *Seien die Voraussetzungen aus 1. 7 gegeben und (R_d, F_d) eine minimale Darstellung von G; dann gibt es ein $r\in\mathbb{N}_0$ mit*

$$A\cong R_d^{ab}\times\mathbb{Z}_p[G]^r.$$

Beweis. Sei (R_m, F_m) eine Darstellung nach Korollar 1. 7, $m\geqq d$, so daß

$$R_m^{ab}\cong A\times\mathbb{Z}_p[G]^{\bar{r}}$$

ist. Da andererseits

$$R_m^{ab}\cong R_d^{ab}\times\mathbb{Z}_p[G]^{m-d}$$

gilt und dies eine Zerlegung von R_m^{ab} in unzerlegbare Bestandteile darstellt (vgl. [8]), folgt aus der Gültigkeit des Krull-Schmidt-Theorems für $\mathbb{Z}_p[G]$-Moduln die Behauptung.

II. Eine exakte Sequenz für $A(K)$

Sei k ein irregulärer $\mathfrak{p}$-adischer Zahlkörper mit Irregularitätsexponenten s, $q=p^s$, und $n=[k:\mathbb{Q}_p]$. Mit $D_{n+2}=\mathrm{Gal}(k(p)/k)$ wollen wir die Galoisgruppe des p-Abschlusses von k bezeichnen. Bekanntlich gibt es eine Darstellung von D_{n+2} durch eine freie pro-p-Gruppe F_{n+2} mit $n+2$ freien Erzeugenden und einer definierenden Relation w_{n+2}:

$$1 \to r_{n+2} \to F_{n+2} \to D_{n+2} \to 1 \quad \text{mit } r_{n+2}=\langle w_{n+2}\rangle .$$

Sei K/k eine endliche, normale p-Erweiterung mit Irregularitätsexponenten $s+\varkappa$, $G=\mathrm{Gal}(K/k)$, $S_{n+2}=\mathrm{Gal}(k(p)/K)=\mathrm{Gal}(K(p)/K)$ und $d=\dim G/G^*$ die minimale Anzahl von Erzeugenden von G, $G^*=G^p[G,G]$; dann erhalten wir kanonisch folgende exakten Sequenzen:

$$1 \to S_{n+2} \to D_{n+2} \to G \to 1$$

$$1 \to R_{n+2} \to F_{n+2} \to G \to 1 .$$

Daraus folgt sofort

Satz 2. 1. *Für* $\bar{r}:=r_{n+2}\cdot[R_{n+2},R_{n+2}]/[R_{n+2},R_{n+2}]$ *ist folgende Sequenz exakt*

$$0 \to \bar{r} \to R^{ab}_{n+2} \to S^{ab}_{n+2} \to 0 .$$

Nach lokaler Klassenkörpertheorie gilt nun die $\mathbb{Z}_p[G]$-Isomorphie

$$A(K) \cong S^{ab}_{n+2} .$$

Ferner gilt

Satz 2. 2. $\bar{r} \cong \mathbb{Z}_p[G]$.

Beweis. Für den $\mathbb{Z}_p$-Rang von $\bar{r}$ ergibt sich nach 2. 1

$$\mathrm{rg}_{\mathbb{Z}_p}\bar{r}=\mathrm{rg}_{\mathbb{Z}_p}R^{ab}_{n+2}-\mathrm{rg}_{\mathbb{Z}_p}S^{ab}_{n+2}=(G:1)\cdot(n+1)+1-((G:1)\cdot n+1),$$

also gleich $(G:1)$. Da $\bar{r}$ aber durch ein Element erzeugt wird, ergibt sich die Behauptung.

Korollar 2. 3. *Folgende Sequenz von* $\mathbb{Z}_p[G]$*-Moduln ist exakt*

$$0 \to \mathbb{Z}_p[G] \to R^{ab}_{n+2} \to A(K) \to 0 .$$

2. 4. Sei $\xi_1,\dots,\xi_{n+2}$ eine Basis von F_{n+2}, dann ist folgende Sequenz exakt

$$0 \longrightarrow R^{ab}_{n+2} \xrightarrow[\varphi]{} \mathbb{Z}_p[G]^{n+2} \xrightarrow[\psi]{} I_G \longrightarrow 0$$

mit $\psi(d\xi_i)=\overline{\xi_i}-1$, wobei $\overline{}$ die Restklasse modulo R_{n+2} und $d\xi_i$ die kanonische Basis von $\mathbb{Z}_p[G]^{n+2}$ bezeichne, $\varphi(x\cdot[R_{n+2},R_{n+2}])=\sum_{i=1}^{n+2}\overline{\left(\frac{\partial x}{\partial\xi_i}\right)}\,d\xi_i$ mit den Partial-Derivationen $\frac{\partial x}{\partial\xi_i}$ von F_{n+2} in $\mathbb{Z}_p[F_{n+2}]$, siehe z. B. [8].

Sei $q \neq 2$, so gibt es eine Basis $x_1, \ldots, x_{n+2}$ von F_{n+2}, so daß die definierende Relation von D_{n+2} durch

$$w = x_1^q \cdot [x_1, x_2] \cdots [x_{n+1}, x_{n+2}]$$

gegeben ist; dann ist, wenn σ_i, $i = 1, \ldots, n+2$, die Bilder der Elemente x_i unter der Projektion von F_{n+2} auf G bezeichnen und $\varphi(w) := \varphi(w \cdot [R_{n+2}, R_{n+2}])$ gesetzt wird,

2. 5. $$\varphi(w) = \sum_{i=1}^{n+2} \overline{\left(\frac{\partial w}{\partial x_i}\right)} dx_i$$

mit
$$\overline{\frac{\partial w}{\partial x_1}} = \sum_{i=0}^{q-1} \sigma_1^i + \sigma_1^q \cdot (1 - \sigma_2)^{\sigma_1}$$

$$\overline{\frac{\partial w}{\partial x_i}} = \sigma_1^q \cdot [\sigma_1, \sigma_2] \cdots [\sigma_{i-1}, \sigma_i] \cdot (\sigma_{i-1} - 1)^{\sigma_i}, \ i \text{ gerade},$$

$$\overline{\frac{\partial w}{\partial x_{i+1}}} = \sigma_1^q \cdot [\sigma_1, \sigma_2] \cdots [\sigma_{i-1}, \sigma_i] \cdot (1 - \sigma_{i+2})^{\sigma_{i+1}}.$$

Sei $\tilde{K}$ der zyklotomische Zwischenkörper von K/k, dann gilt der

Satz 2. 6. *Sei* $q \neq 2$ *und* $\tilde{G} = \langle \sigma_1, \sigma_3, \sigma_4, \ldots, \sigma_{n+2} \rangle$ *Normalteiler in* G, *dann ist* $\tilde{K}$ *der Fixkörper von* $\tilde{G}$ *in* K.

Beweis. Aus 2. 3 folgt die exakte Sequenz

$$0 \to q \cdot \mathrm{Sp}_G \mathbb{Z}_p \cdot dx_1 \to \sum_{i=1}^{n+2} \mathrm{Sp}_G \mathbb{Z}_p \cdot dx_i \to A(K)^G \to 0,$$

da wegen 2. 4 $(R_{n+2}^{ab})^G = \sum_{i=1}^{n+2} \mathrm{Sp}_G \mathbb{Z}_p \cdot dx_i$ gilt. Also hat das Bild von $\varrho := \mathrm{Sp}_G \cdot dx_1 \in R_{n+2}^{ab}$ $(\psi(\mathrm{Sp}_G \cdot dx_1) = 0)$ in $A(K)$ die Ordnung q und stellt somit eine primitive q-te Einheitswurzel dar. Für das Element $\varrho' := \mathrm{Sp}_{\tilde{G}} \cdot dx_1 \in (R_{n+2}^{ab})^{\tilde{G}}$ gilt nun modulo $\mathbb{Z}_p[G]\ \varphi(w)$

$$0 \equiv \mathrm{Sp}_{\tilde{G}}\, \varphi(w) \equiv (q + 1 - \sigma_2)\, \mathrm{Sp}_{\tilde{G}} \cdot dx_1,$$

also

$$\sigma_2 \varrho' \equiv g \cdot \varrho' \quad \text{mit } g = 1 + q;$$

Sei $(G : \tilde{G}) = p^{\tilde{s}}$, so gilt

$$\varrho = \sum_{i=0}^{p^{\tilde{s}}-1} \sigma_2^i \varrho' \equiv \frac{g^{p^{\tilde{s}}} - 1}{g - 1} \cdot \varrho' = p^{\tilde{s}} \cdot u \cdot \varrho', \ u \text{ Einheit in } \mathbb{Z}_p;$$

also hat das Bild von ϱ' in $A(K)$ die Ordnung $p^{s+\tilde{s}}$ und $\tilde{K} = k(\overline{\varrho'})$ ist eine zyklotomische Erweiterung.

Angenommen ϱ' wäre modulo $\mathbb{Z}_p[G]\,\varphi(w)$ eine p-Potenz, dann gibt es α_i, $\alpha \in \mathbb{Z}_p[G]$, so daß

$$\mathrm{Sp}_{\tilde{G}} \cdot dx_1 = p \cdot \sum_{i=1}^{n+2} \alpha_i \cdot dx_i + \alpha \cdot \varphi(w),$$

also

$$\mathrm{Sp}_{\tilde{G}} = p \cdot \alpha_1 + \alpha \cdot \left(\sum_{i=0}^{q-1} \sigma_1^i + \sigma_1^q (1 - \sigma_2)^{\sigma_1} \right), \quad -p \cdot \alpha_i = \alpha \frac{\partial w}{\partial x_i}, \quad i \geqq 2,$$

und damit ist $\alpha \in \mathrm{Sp}_{\tilde{G}}\, \mathbb{Z}_p[G] + p \cdot \mathbb{Z}_p[G]$ und

$$\mathrm{Sp}_{\tilde{G}} = p \cdot \alpha_1 + (q+1-\sigma_2) \cdot \mathrm{Sp}_{\tilde{G}}\, \alpha',$$

also

$$\mathrm{Sp}_G \in p \cdot \mathbb{Z}_p[G],$$

was einen Widerspruch darstellt. Damit haben wir die Behauptung gezeigt.

III. Maximaler freier $\mathbb{Z}_p[G]$-Summand von $\mathcal{A}(\mathrm{K})$

Nach Korollar 2. 3 ist das Problem, die Relation $\bar{r}$ im $\mathbb{Z}_p[G]$-Modul R_{n+2}^{ab} „wiederzufinden". Als erste Aufgabe ist die Frage zu lösen, wie groß der Rang des maximalen freien $\mathbb{Z}_p[G]$-Summanden von $R_{n+2}^{ab}/\mathbb{Z}_p[G]$ ist. Wir betrachten dazu die nichtausgeartete, antisymmetrische Bilinearform, die durch das Normrestsymbol gegeben ist:

$$(\ ,\ ): k^*/k^{*p} \times k^*/k^{*p} \to \mathbb{Z}/p\mathbb{Z}.$$

Für den Teilraum $U := K^{*p} \cap k^*/k^{*p}$ gilt nun das

Lemma 3. 1. $U^\perp = N_{K/k}(K^*)\,k^{*p}/k^{*p}$, $\dim U^\perp = n+2-d$.

Beweis. Sei $K' := k(\sqrt[p]{\alpha_1}, \ldots, \sqrt[p]{\alpha_d}) = \mathrm{Fix}(G^*)$ mit $\alpha_1, \ldots, \alpha_d \in k^*$, dann ist nach lokaler Klassenkörpertheorie

$$N_{K/k}(K^*)\,k^{*p} = N_{K'/k}(K'^*) = \bigcap_{i=1}^{d} N_{k_i/k}(k_i^*) \quad \text{mit } k_i = k(\sqrt[p]{\alpha_i});$$

das heißt aber, wegen $U = \langle \alpha_1 k^{*p}, \ldots, \alpha_d k^{*p} \rangle$,

$$\alpha k^{*p} \in U^\perp \Leftrightarrow (\alpha, \alpha_i) = 1\ \forall i \Leftrightarrow \alpha \in N_{k_i/k}(k_i^*)\ \forall i \Leftrightarrow \alpha \in N_{K/k}(K^*)\,k^{*p}.$$

Die zweite Behauptung folgt aus $\dim U + \dim U^\perp = \dim k^*/k^{*p} = n+2$.

Lemma 3. 2. *Sei G eine endliche p-Gruppe und X ein $\mathbb{Z}/p\mathbb{Z}[G]$-Modul, dann gilt für $c_1, \ldots, c_n \in X$:*

$$\{\mathrm{Sp}_G c_1, \ldots, \mathrm{Sp}_G c_n\} \quad \mathbb{Z}/p\mathbb{Z}\text{-linear unabhängig in } X$$

$$\Leftrightarrow \{c_1, \ldots, c_n\} \quad \mathbb{Z}/p\mathbb{Z}[G]\text{-linear unabhängig in } X.$$

Beweis. Zum Beweis der nichttrivialen Richtung sei $M := \langle c_1, \ldots, c_n \rangle_{Z/pZ[G]}$ und

$$0 \longrightarrow \operatorname{Ker}\varphi \longrightarrow \mathbb{Z}/p\mathbb{Z}[G]^n \xrightarrow[\varphi]{} M \longrightarrow 0$$

die kanonische exakte Sequenz; dann ist auch

$$0 \to (\operatorname{Ker}\varphi)^G \to (\mathbb{Z}/p\mathbb{Z} \cdot \mathrm{Sp}_G)^n \to \mathrm{Sp}_G M \to 0$$

exakt. Da nach Voraussetzung $\dim_{Z/pZ} \mathrm{Sp}_G M = n$ ist, erhalten wir $\dim_{Z/pZ}(\operatorname{Ker}\varphi)^G = 0$, also $(\operatorname{Ker}\varphi)^G = 0$, und nach dem Lemma von Rim $\operatorname{Ker}\varphi = 0$.

Lemma 3. 3. *Sei G eine endliche p-Gruppe und X ein $\mathbb{Z}/p\mathbb{Z}[G]$-Modul, dann gilt*

$$\dim_{Z/pZ} \mathrm{Sp}_G X = \max\{j, \text{ es gibt } Y \subseteqq X \text{ mit } Y \cong \mathbb{Z}/p\mathbb{Z}[G]^j\}.$$

Beweis. Daß die linke Seite kleiner oder gleich der rechten ist, folgt aus 3. 2. Sei umgekehrt $\mathbb{Z}/p\mathbb{Z}[G]^j \cong Y \subseteqq X$, so ist Y auch direkter Summand, da jeder $\mathbb{Z}/p\mathbb{Z}[G]$-projektive Modul auch $\mathbb{Z}/p\mathbb{Z}[G]$-injektiv ist, [5], S. 226. Für $X \cong Y \times Z$ gilt dann aber

$$\mathrm{Sp}_G X \cong \mathbb{Z}/p\mathbb{Z}^j \times \mathrm{Sp}_G Z,$$

also $\dim_{Z/pZ} \mathrm{Sp}_G X \geqq j$.

Mit $h := \dim_{Z/pZ} N_{K/k}(K^*/K^{*p})$ gilt der

Satz 3. 4. *Sei $A(K) = B \times \mathbb{Z}_p[G]^j$, dann gilt $j \leqq h$.*

Beweis. Es ist unter der gemachten Voraussetzung

$$A(K)/A(K)^p \cong K^*/K^{*p} \cong \bar{B} \times \mathbb{Z}/p\mathbb{Z}[G]^j,$$

so daß aus Lemma 3. 3 die Behauptung folgt.

Damit haben wir die Aussage erhalten, daß $A(K)$ höchstens einen freien $\mathbb{Z}_p[G]$-Summanden vom Rang h enthalten kann. Im folgenden werden wir zeigen, daß $A(K)$ mindestens einen Summanden vom Rang $h-1$ enthält.

Lemma 3. 5. *Sei G eine endliche Gruppe und X ein torsionsfreier $\mathbb{Z}_p[G]$-Modul. Dann gilt:*

$\mathbb{Z}_p[G]^j$ ist direkter Summand von X genau dann, wenn $\mathbb{Z}/p\mathbb{Z}[G]^j$ direkter Summand von X/pX ist.

Beweis. Zum Beweis der nichttrivialen Richtung seien $\theta_1, \ldots, \theta_j \in X$, so daß $\bar{\theta}_1, \ldots, \bar{\theta}_j$ eine $\mathbb{Z}/p\mathbb{Z}[G]$-Basis des freien Summanden von X/pX bilden. Offenbar ist $M := \langle \theta_1, \ldots, \theta_j \rangle_{Z_p[G]}$ $\mathbb{Z}_p[G]$-frei und X/M torsionsfrei, denn es ist

$$\mathrm{rg}_{Z_p} M \leqq j \cdot (G:1) \quad \text{und} \quad \mathrm{rg}_{Z_p} X/M \leqq \dim_{Z/pZ} \bar{Y},$$

wenn $X/pX \cong \mathbb{Z}/p\mathbb{Z}[G]^j \times \bar{Y}$ ist, und andererseits

$$\mathrm{rg}_{Z_p} M + \mathrm{rg}_{Z_p} X/M = \mathrm{rg}_{Z_p} X = \dim_{Z/pZ} X/pX = j \cdot (G:1) + \dim_{Z/pZ} \bar{Y}$$

gilt, d. h. beide Moduln haben Maximalrang. Aus Lemma 1. 5 folgt die Behauptung.

Satz 3. 6. 1. *Es gibt einen $\mathbb{Z}_p[G]$-Modul Y, so daß $A(K) \cong Y \times \mathbb{Z}_p[G]^{h-1}$ gilt.*

2. *Es gibt genau dann einen $\mathbb{Z}_p[G]$-Modul Z mit $A(K) \cong Z \times \mathbb{Z}_p[G]^h$ wenn $\varrho' \notin N_{K/k}(K^*)K^{*p}$, wobei ϱ' eine primitive $p^{s+\varkappa}$-te Einheitswurzel aus K ist.*

Beweis. Sei $W := \langle \varrho' \rangle$ und $\tilde{A} := A(K)/W$, dann sind die Ränge der maximalen freien $\mathbb{Z}_p[G]$-Summanden von $A(K)$ und $\tilde{A}$ gleich; denn ist $A(K) = Y \times \mathbb{Z}_p[G]^j$, so folgt $W \subseteq Y$ und daher gilt $\tilde{A} = Y/W \times \mathbb{Z}_p[G]^j$. Andererseits existiert für eine Surjektion von $\tilde{A}$ auf $\mathbb{Z}_p[G]^j$ auch eine von $A(K)$ auf $\mathbb{Z}_p[G]^j$.

Nach Lemma 3. 5 und Lemma 3. 3 ist daher der Rang des maximalen freien $\mathbb{Z}_p[G]$-Summanden von $A(K)$ gleich

$$\begin{aligned}\dim_{Z/pZ} N_{K/k}(\tilde{A}/\tilde{A}^p) &= \dim_{Z/pZ} N_{K/k}(K^*)\, K^{*p} W / K^{*p} W \\ &= h - \dim_{Z/pZ}\big(K^{*p} W \cap N_{K/k}(K^*) K^{*p}\big)/K^{*p}.\end{aligned}$$

Es ist aber

$$\dim_{Z/pZ}\big(K^{*p} W \cap N_{K/k}(K^*) K^{*p}\big)/K^{*p} = \begin{cases} 0, & \text{falls } \varrho' \notin N_{K/k}(K^*)\, K^{*p} \\ 1, & \text{sonst} \end{cases}.$$

Sei $t := \dim_{Z/pZ} \operatorname{rad} U$ mit $\operatorname{rad} U = U \cap U^{\perp}$, dann gilt der

Satz 3. 7. *$n + 2 = d + t + h$.*

Beweis. Die Sequenz

$$\begin{array}{ccccccccc} 1 \longrightarrow & N_{K/k}(K^*)\, k^{*p} \cap K^{*p}/k^{*p} & \longrightarrow & N_{K/k}(K^*)\, k^{*p}/k^{*p} & \longrightarrow & N_{K/k}(K^*)\, K^{*p}/K^{*p} & \longrightarrow 1 \\ & \Vert & & \Vert & & \Vert & \\ & U \cap U^{\perp} & & U^{\perp} & & N_{K/k}(K^*/K^{*p}) & \end{array}$$

ist exakt.

Bemerkung 3. 8. Da wegen der exakten Sequenz

$$1 \to \mathbb{Z}/p\mathbb{Z} \to K^* \to K^{*p} \to 1$$

auch

$$k^* \longrightarrow K^{*p} \cap k^* \xrightarrow{\ \delta\ } H^1(G) \longrightarrow 1$$

exakt ist, erhalten wir

$$U = K^{*p} \cap k^*/k^{*p} \cong H^1(G).$$

Also läßt sich die Invariante t der Körpererweiterung auch durch

$$t = \dim_{Z/pZ} \operatorname{rad} H^1(G)$$

kennzeichnen, wobei zur Bildung des Radikals die nicht-ausgeartete, antisymmetrische Bilinearform zugrunde gelegt wird, die durch die Abbildung

$$\mathrm{tg}^{-1} \circ \cup(\ ,\ )(w_{n+2}^{-1}) : H^1(D_{n+2}) \times H^1(D_{n+2}) \to \mathbb{Z}/p\mathbb{Z}$$

gegeben ist (tg = Transgression, $\cup$ = Cupprodukt, siehe z. B. [7]).

IV. Unzerlegbare Bestandteile von $A(\mathrm{K})$

Auf Grund der kohomologischen Eigenschaften von $A(K)$ sind die unzerlegbaren Bestandteile dieses $\mathbb{Z}_p[G]$-Moduls für p-Gruppen von besonders einfacher Art, denn nach Satz 1. 3 ist $A(K) \cong S_{n+2}^{ab} \in \mathfrak{A}_{\mathbb{Z}_p[G]}$, und es gilt

Satz 4. 1. *Sei $A \in \mathfrak{A}_G$ oder $A \in \mathfrak{A}_{\mathbb{Z}_p[G]}$, G eine p-Gruppe, und $A = C_1 \times C_2$, so ist entweder C_1 oder C_2 kohomologisch trivial.*

Beweis. Da für alle Untergruppen g von G

$$H^1(g, C_1) = H^1(g, C_2) = 0, \quad \text{und} \quad H^2(g, C_1) \times H^2(g, C_2) = \mathbb{Z}/(g:1)\mathbb{Z}$$

gilt, ist entweder $H^2(g, C_1) = 0$ oder $H^2(g, C_2) = 0$.

Da $\mathrm{Tor}(A(K))$, die Torsionsgruppe von $A(K)$, eine zyklische p-Gruppe ist, erhalten wir

Satz 4. 2. *Sei $A(K) \cong M \times \mathbb{Z}_p[G]^{h-\delta}$ mit*

$$\delta = \begin{cases} 0, & \text{falls } \varrho' \notin N_{K/k}(K^*)K^{*p} \text{ ist} \\ 1, & \text{sonst} \end{cases},$$

dann gilt:

$$M \text{ ist unzerlegbar},$$

oder

$$M \cong R_d^{ab} \times \mathbb{Z}_p[G]^{t+\delta}/\mathbb{Z}_p[G],$$

wobei beide Summanden unzerlegbar sind.

Beweis. Sei $M = C_1 \times C_2$ und nach 4. 1 ohne Einschränkung C_1 kohomologisch trivial. Ist $\mathrm{Tor}(C_1) = 0$, so gilt nach 1. 6, daß $C_1 = \mathbb{Z}_p[G]^r$ ist, und nach 3. 6, daß $r = 0$ ist, also ist M unzerlegbar. Sei hingegen $\mathrm{Tor}(C_1) \neq 0$, so erhalten wir $\mathrm{Tor}(C_2) = 0$, da $\mathrm{Tor}\, M$ zyklisch ist. Also ist $C_2 \in \mathfrak{A}_{\mathbb{Z}_p[G]}$ und torsionsfrei, so daß nach 1. 8 und 3. 6

$$C_2 \cong R_d^{ab}$$

ist. Dann zeigt die exakte Sequenz

$$0 \to \mathbb{Z}_p[G] \to R_d^{ab} \times \mathbb{Z}_p[G]^{t+\delta} \to R_d^{ab} \times C_1 \to 0,$$

daß

$$C_1 \cong \mathbb{Z}_p[G]^{t+\delta}/\mathbb{Z}_p[G]$$

ist. Dieser Modul ist unzerlegbar, denn sei $C_1 = U_1 \times U_2$, so ist, da $\mathrm{Tor}(C_1)$ zyklisch ist und U_1 und U_2 kohomologisch trivial sind, entweder U_1 oder U_2 $\mathbb{Z}_p[G]$-frei, was aber wegen 3. 6 nicht sein kann.

Sei wie bisher $\tilde{K} = k(\varrho')$ der zyklotomische Zwischenkörper von K/k, dann gilt der

Satz 4. 3. *Sei $A(K) \cong R_d^{ab} \times C$, dann ist*

1) $\varrho' \in N_{K/\tilde{K}}(K^*)$,

2) $K^{*p} \cap k \subseteq N_{K/k}(K^*)k^{*p}$, *d.h.* $U \subseteq U^{\perp}$, *d.h.* $H^1(G)$ *ist isotroper Teilraum von* $H^1(D_{n+2})$, *also* $t = d$.

Beweis. Da C kohomologisch trivial ist und

$$\varrho' \in C^{\mathrm{Gal}(K/\tilde{K})} = \mathrm{Sp}_{\mathrm{Gal}(K/\tilde{K})}\, C$$

folgt die erste Aussage. Weiter ist $C^p \cap C^G \subseteqq \mathrm{Sp}_G\, C$ und

$$(R_d^{ab})^p \cap (R_d^{ab})^G = \big((R_d^{ab})^p\big)^G = \big((R_d^{ab})^G\big)^p,$$

da R_d^{ab} torsionsfrei ist. Es folgt

$$A(K)^p \cap A(K)^G \subseteqq N_{K/k}\big(A(K)\big) \cdot \big(A(K)^G\big)^p$$

und damit auch die Behauptung für K^*.

Wir erhalten also das Ergebnis

Satz 4. 4. *Es gilt die $\mathbb{Z}_p[G]$-Modul-Isomorphie*

$$A(K) \cong M \times \mathbb{Z}_p[G]^{n+2-(d+t)-\delta}, \quad \delta = \begin{cases} 0, & \varrho' \notin N_{K/k}(K^*)\,K^{*p} \\ 1, & sonst \end{cases},$$

wobei

$$M = (R_d^{ab} \times \mathbb{Z}_p[G]^{t+\delta}) / \mathbb{Z}_p[G]$$

unzerlegbarer $\mathbb{Z}_p[G]$-Modul ist oder es ist M direkte Summe zweier unzerlegbarer $\mathbb{Z}_p[G]$-Moduln

$$M = R_d^{ab} \times \mathbb{Z}_p[G]^{d+\delta} / \mathbb{Z}_p[G], \ (t = d).$$

Im zyklischen Fall erweisen sich die Bedingungen aus 4. 3 — die zweite ist dann trivial — auch als hinreichend dafür, daß R_d^{ab} direkter Summand von $A(K)$ ist [4]. Die Bedingung $\varrho' \notin N_{K/k}(K^*)K^{*p}$, d.h. $A(K)$ hat einen direkten freien $\mathbb{Z}_p[G]$-Summanden vom Rang h, ist für $q \neq 2$ im zyklischen Fall äquivalent mit der Aussage $\lambda = \varkappa$, mit

$$p^\lambda := \big(k^* : \langle N_{K/k}(K^*), \varrho\rangle\big), \qquad \varrho \ p^s\text{-te Einheitswurzel in } k.$$

Wir benötigen dafür das

Lemma 4. 5. *Sei G zyklische p-Gruppe, dann gilt für jede Untergruppe $H \neq \{1\}$ von G und $\bar{K} = K^H$ die $\mathbb{Z}_p[G]$-Isomorphie*

$$\Gamma := N_{K/\bar{K}}(K^*/K^{*p}) = \mathbb{Z}/p\mathbb{Z}[G/H]^n$$

Beweis. Nach 3. 7 ist

$$\dim_{Z/pZ} N_{G/H}(\Gamma) = \dim_{Z/pZ} N_{K/k}(K^*/K^{*p}) = n + 2 - d_G - t_G = n;$$

also enthält Γ wegen 3. 3 einen freien $\mathbb{Z}/p\mathbb{Z}[G/H]$-Modul vom Rang n. Ebenfalls mit 3. 7 erhalten wir

$$\dim_{Z/pZ} \Gamma = [\bar{K} : \mathbb{Q}_p] + 2 - d_H - t_H = n \cdot (G : H),$$

woraus die Behauptung folgt.

Speziell ist daher für eine zyklische p-Gruppe G und eine Untergruppe H von G

$$\big(N_{K/\bar{K}}(K^*/K^{*p})\big)^G = N_{G/H}(\Gamma) = N_{K/k}(K^*/K^{*p}).$$

Satz 4. 6. *Sei G zyklisch und $q \neq 2$, dann gilt*

$$\varrho' \notin N_{K/k}(K^*)\,K^{*p} \Leftrightarrow \lambda = \varkappa\,.$$

Beweis. Wegen $d = t = 1$ gilt

$$\tilde{K}^* \cap K^{*p} \subseteqq N_{K/\tilde{K}}(K^*)\,\tilde{K}^{*p}$$

und damit

$$N_{K/k}(K^*)\,K^{*p} \cap \tilde{K}^* \subseteqq N_{K/\tilde{K}}(K^*)\,K^{*p} \cap \tilde{K}^* \subseteqq N_{K/\tilde{K}}(K^*)\,\tilde{K}^{*p},$$

d. h. ist $\varrho' \in N_{K/k}(K^*)\,K^{*p}$, so ist es auch aus $N_{K/\tilde{K}}(K^*)\,\tilde{K}^{*p}$. Sei umgekehrt $\varrho' \in N_{K/\tilde{K}}(K^*)\,\tilde{K}^{*p}$; aus $(\varrho'^{\sigma-1})^{p^\varkappa} = 1$ für alle $\sigma \in G$ folgt $\varrho'^{\sigma-1} \in K^{*p^s}$ für alle $\sigma \in G$; insbesondere gilt mit der Folgerung aus 4. 4

$$\varrho' \cdot K^{*p} \in \big(N_{K/\tilde{K}}(K^*/K^{*p})\big)^G = N_{K/k}(K^*/K^{*p}),$$

also ϱ' Element von $N_{K/k}(K^*)K^{*p}$. Mit dem Reziprozitätshomomorphismus $(\ ,K/k)$ erhalten wir, da für $q \neq 2$ ohne Einschränkung $\varrho = N_{\tilde{K}/k}(\varrho')$ gilt,

$$\begin{aligned}\varrho' \in N_{K/k}(K^*)\,K^{*p} &\Leftrightarrow \varrho' \in N_{K/\tilde{K}}(K^*)\,\tilde{K}^{*p}\\ &\Leftrightarrow (\varrho, K/k) = \big(N_{\tilde{K}/k}(\varrho'), K/k\big) = (\varrho', K/\tilde{K}) \in \mathrm{Gal}(K/\tilde{K})^p = G^{p^{\varkappa+1}}\\ &\Leftrightarrow \lambda \geqq \varkappa + 1\,.\end{aligned}$$

Das ist aber die Behauptung, da immer $\lambda \geqq \varkappa$ gilt.

Literaturverzeichnis

[1] *Z. I. Borevič*, On the group of principal units of a normal p-extension of a regular local field, Proc. Math. Inst. Steklov **80** (1965), 31—47.

[2] *Z. I. Borevič, Ali Jusef El Musa*, Completion of the multiplicative group of p-extensions of an irregular local field, Zapiski naučn. Sem. Leningrad. Otd. mat. Inst. Steklov **31** (1973), 6—23.

[3] *R. H. Fox*, Free differential calculus. I, Derivation in the free group ring, Ann. Math. **57** (1953), 547—560.

[4] *E. L. Gerlovin*, Completion of the multiplicative group of a cyclic p-extension of a local field, Vestnik Leningrad Univ. **24** no. 7, (1969), 14—22.

[5] *K. Gruenberg*, Cohomological topics in group theory, Lecture notes in math. **143** (1970).

[6] *Y. Kawada*, On the structure of galois groups of some infinite extensions. II, Fac. Sci. Univ. Tokyo, Sec I. **7** (1954), 87—106.

[7] *J. P. Labute*, Classification of Demuškin groups, Canad. J. Math. **19** (1967), 106—132.

[8] *K. Wingberg*, Die Einseinheitengruppe von p-Erweiterungen regulärer $\mathfrak{p}$-adischer Zahlkörper als Galoismodul, J. reine angew. Math. **305** (1979), 206—214.

Alte Dorfstraße 36, D-2061 Meddewade
Straße des 17. Juni 135, D-1000 Berlin 12

Eingegangen 26. Juli 1978