MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

Tagungsbericht 2/1969

Heidelberger Seminar über Algebra und Zahlentheorie

8.2. bis 10.2.1969

Thema: Demuskingruppen

Das Ziel der Tagung, die unter der Leitung von P.Roquette (Heidelberg) stand, war ein Bericht über die Struktur der maximalen p-Faktorgruppe und der p-Sylowgruppen der Galoisgruppe des algebraischen Abschlusses eines p-adischen Körpers k über diesem Körper, welche wir im folgenden kurz als die Galoisgruppe des Körpers k bezeichnen werden. Das Interesse für diese Untersuchungen ergibt sich aus der folgenden Fragestellung: Wann kann eine endliche p-Gruppe über k oder über einer endlichen Körpererweiterung von k als Galoisgruppe realisiert werden ?

Teilnehmer

J.K.Arason, Göttingen
K.Doerk, Mainz
P.Draxl, Göttingen
G.Frey, Heidelberg
H.Göhner, Heidelberg
U.Göhner, Tübingen
P.Hahnel, Heidelberg
B.Hain, Clausthal
R.Jebens, Frankfurt a.M.
K.Keller, Heidelberg
B.Klaiber, Mainz
H.Lange, Göttingen
J.Leicht, Heidelberg
F.Lorenz, Heidelberg
G.Martens, Heidelberg
H.Pfeuffer, Göttingen
H.Popp, Heidelberg
K.Radbruch, Tübingen
J.Ritter, Heidelberg
P.Roquette, Heidelberg
G.Tamme, Göttingen

Gefördert durch DFG Deutsche Forschungsgemeinschaft

Vortragsauszüge:

RADBRUCH: Die maximale p-Faktorgruppe der Galoisgruppe eines p-adischen Körpers, falls dieser die p-ten Einheitswurzeln nicht enthält.

Mit Hilfe von Sätzen aus der lokalen Klassenkörpertheorie und der Theorie der freien Gruppen wurde der folgende Satz nach einem Beweis von Schafarewich gezeigt: Sei k eine endliche Erweiterung der rationalen p-adischen Zahlen vom Grade n, welche die p-ten Einheitswurzeln nicht enthält, G die Galoisgruppe der maximalen p-Erweiterung: dann ist G eine freie pro-p-Gruppe mit n+1 Erzeugenden.

LORENZ: Kohomologische Beschreibung der Erzeugenden und definierenden Relationen von pro-p-Gruppen. Anwendung dieser Ergebnisse auf die maximale p-Faktorgruppe der Galoisgruppe eines p-adischen Körpers.

Sei G eine pro-p-Gruppe und $H^i(G) = H^i(G,\mathbb{Z}/p)$. E heißt ein Erzeugendensystem von G, falls der von E bezüglich der Komplemente der endlichen Teilmengen erzeugte Filter gegen die Eins konvergiert und das algebraische Erzeugnis von E in G dicht ist. Die folgenden Aussagen sind dann gleichwertig:

(a) Es existiert ein Erzeugendensystem von G der Kardinalität r.
(b) Es existiert ein surjektiver Homomorphismus der von r erzeugten freien pro-p-Gruppe F(r) auf G.
(c) $r \geqslant \dim H^1(G)$.

$\dim H^1(G)$ heißt der Rang von G. Ist G eine pro-p-Gruppe, sodaß $H^2(G)$ endliche Dimension besitzt, r der Rang von G, R der Kern eines surjektiven Homomorphismus von F(r) auf G, dann gilt:

n Elemente von R erzeugen R als Normalteiler von F(r) ist gleichbedeutend damit, daß $n \geqslant \dim H^2(G)$ gilt.

Mit Hilfe der Euler-Poincare-Charakteristik wurde nun ein kohomologietheoretischer Beweis für den im vorangegangenen

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Vortrag bewiesenen Satz gegeben. Danach wurde gezeigt: Ist k ein p-adischer Körper vom Grade n über den rationalen p-adischen Zahlen, der die p-ten Einheitswurzeln enthält und G die maximale p-Faktorgruppe der Galoisgruppe von k, so hat G den Rang n+2 und $H^2(G)$ ist eine zyklische Gruppe der Ordnung p.

Eine pro-p-Gruppe endlichen oder abzählbaren Ranges heißt Demuskingruppe, wenn $H^2(G)$ eine zyklische Gruppe und das Cup-Produkt $H^1(G) \times H^1(G) \to H^2(G)$ eine nichtausgeartete Bilinearform ist. Wenn G eine Demuskingruppe endlichen Ranges mit unendlich vielen Elementen ist, dann hat G die kohomologische Dimension 2; falls G nur endlich viele Elemente besitzt, ist G die Gruppe der Ordnung 2.

ROQUETTE: <u>Die maximale p-Faktorgruppe der Galoisgruppe eines p-adischen Körpers, der die p-ten Einheitswurzeln enthält, ist eine Demuskingruppe.</u>

Nach den Ergebnissen des vorangegangenen Vortrags mußte nur noch gezeigt werden, daß das Cup-Produkt nichtausgeartet ist. Dies wurde unter Benutzung der Kummerschen Theorie und unter Hervorhebung des Zusammenhangs mit dem Normrestsymbol getan.

MARTENS: <u>Einführung der Invarianten, die zur Klassifikation der Demuskingruppen durch Relationen benötigt werden.</u>

Sei G eine Demuskingruppe, I die unterliegende abelsche Gruppe des dualisierenden Moduls von G. I ist dann ein zyklischer Modul der Ordnung p^e oder von der Form $\mathbb{Q}_p/\mathbb{Z}_p$. Im ersten Fall wird die Invariante $s(G) = p^e$ gesetzt, im zweiten Fall: $s(G) = 0$ (d.h. $e = \infty$). Die G-Modulstruktur des dualisierenden Moduls liefert einen stetigen Homomorphismus χ von G in $\mathrm{Aut}(I) = (\mathbb{Z}/_{p^e})^x$ bzw. $\mathbb{Z}_p^x$. Das Bild dieses Homomorphismus ist die Invariante $B = \mathrm{Im}\ \chi$.

Aus dem Vortrag von Lorenz folgt nun, daß die abelsche Gruppe $G/_{(G,G)} = G_a$ entweder torsionsfrei oder der Torsionsbestandteil zyklisch von p-Potenzordnung ist. Die Invariante q(G) ist die Ordnung des Torsionsbestandteils von G_a.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

Durch das in der Definition einer Demuskingruppe auftretende Cup-Produkt ist eine Linearform $b(v) = v \cup v$ für $v \in H^1(G)$ gegeben. Es sei A der von den isotropen Vektoren erzeugte Teilraum von $H^1(G)$. Man setzt die Invariante $t(G) = 1$, falls $A = V$ gilt, d.h. wenn das Cup-Produkt alternierend ist, was für $p \neq 2$ immer erfüllt ist. Sei nun $A \neq V$ und A' das orthogonale Komplement von A bezüglich der durch das Cup-Produkt gegebenen Bilinearform. Ist $A' \neq 0$ und $A' \subset A$, so setzt man $t(G) = 1$, ist $A' \neq 0$ und $A' \not\subset A$, so setzt man $t(G) = -1$ und $t(G) = 0$, falls $A' = 0$.

FREY: <u>Klassifikation der Demuskingruppen endlichen Ranges mit</u> $q(G) \neq 2$.

Eine solche Demuskingruppe G läßt sich als Quotient einer von $x_1,\ldots,x_n$ erzeugten freien pro-p-Gruppe F modulo dem von der Relation

$$x_1^q(x_1,x_2)(x_3,x_4)\ldots(x_{n-1},x_n)$$

erzeugten abgeschlossenen Normalteiler darstellen, d.h. sie ist durch die Invariante $q(G) = q$ eindeutig bestimmt. Der Beweis erfolgt mittels Approximation entlang der q-Filtrierung von F: $F_1 = F$, $F_{n+1} = F_n^q(F,F_n)$.

POPP: <u>Beschreibung der Demuskingruppen endlichen Ranges, falls</u> $q(G) = 2$.

Diese Demuskingruppen lassen sich wieder als Quotient einer von $x_1,\ldots,x_n$ erzeugten freien pro-p-Gruppe schreiben, wobei eine der folgenden Relationen herausgeschnitten werden muß:

(1) n gerade, $(B:B^2) = 2$: $x_1^{2+a}(x_1,x_2)(x_3,x_4)\ldots(x_{n-1},x_n)$ mit $a = 2^f$, f eine natürliche Zahl, $f \geqslant 2$.

(2) n gerade, $(B:B^2) = 4$: $x_1^2(x_1,x_2)x_3^a(x_3,x_4)\ldots(x_{n-1},x_n)$ mit $a = 2^f$, $f \in \bar{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$, $f \geqslant 2$.

(3) n ungerade: $x_1^2x_2^a(x_2,x_3)\ldots(x_{n-1},x_n)$ mit $a = 2^f$, $f \in \bar{\mathbb{N}}$, $f \geqslant 2$.

GÖHNER, H.: Allgemeine Sätze über Demuskingruppen.

In diesem Vortrag wurden die beiden folgenden Sätze bewiesen:

Sei G eine Demuskingruppe abzählbaren Ranges. Dann existiert eine absteigende Folge H_i ($i \in \mathbb{N}$) abgeschlossener Normalteiler von G mit $\bigcap H_i = 1$ und jeder Quotient G/H_i ist eine Demuskingruppe endlichen Ranges. Umgekehrt: ist G eine pro-p-Gruppe abzählbaren Ranges, die eine Folge abgeschlossener Normalteiler mit den obigen Eigenschaften besitzt, dann ist G entweder eine freie pro-p-Gruppe oder eine Demuskingruppe.

Mit Hilfe dieses Satzes erhält man das folgende Korollar:
Eine Demuskingruppe abzählbaren Ranges hat die kohomologische Dimension 2.

Ist G eine Demuskingruppe vom Rang > 1, dann ist jede offene Untergruppe Demuskingruppe und jede abgeschlossene Untergruppe mit unendlichem Index ist eine freie pro-p-Gruppe.

RITTER: Klassifikation der Demuskingruppen abzählbaren Ranges.

Sei G eine solche Demuskingruppe, F eine freie pro-p-Gruppe mit abzählbar vielen Erzeugenden x_i ($i \in \mathbb{N}$),

$$m(j,s) = \prod_{i \geqslant j} x_{2i-1}^{s}(x_{2i-1},x_{2i}),$$

dann läßt sich diese Demuskingruppe in der Form $G \cong F/(r)$ schreiben, wobei r die folgende Form hat:

(1) $q(G) = q = p^h \neq 2 : r = x_1^q(x_1,x_2)m(2,s)$ mit $s = s(G) = p^e$ ($e \in \bar{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$) und $e \geqslant h$

(2) $q(G) = 2,\ t(G) = 1 : r = x_1^{2+a}(x_1,x_2)(x_3,x_4)m(3,s)$ mit $s = s(G) = 2^e$, $a = 2^f$, $e,f \in \bar{\mathbb{N}}$, $e > f \geqslant 2$

oder $r = x_1^2(x_1,x_2)x_3^a(x_3,x_4)m(3,s)$ mit s und a wie vorher und der Beziehung $e \geqslant f \geqslant 2$

(3) $q(G) = 2$, $t(G) = -1$: $r = x_1^2 x_2^a (x_2,x_3) \prod_{i\geq 2} x_{2i}^s (x_{2i},x_{2i+1})$

mit s und a wie vorher und $e \geq f \geq 2$

(4) $q(G) = 2$, $t(G) = 0$: $r = m(1,2) \prod_{i<j} (x_i,x_j)^{b_{ij}}$ mit

$b_{ij} \in 2\mathbb{Z}_2$

HAHNEL: <u>Die p-Sylowgruppe der Galoisgruppe eines p-adischen Körpers ist eine Demuskingruppe abzählbaren Ranges.</u>

Zuerst wurde die Umkehrung des in dem vorangegangenen Vortrag bewiesenen Satzes gezeigt, d.h. ist F eine freie pro-p-Gruppe abzählbaren Ranges mit den Erzeugenden x_i, und r eine Relation der Form (1) bis (4), so ist $G = F/(r)$ eine Demuskingruppe mit den Invarianten $q(G)$, $s(G)$, $t(G)$ wie in dem vorangehenden Satz und für die Invariante $\mathrm{Im}\,\chi$ erhält man die folgenden Werte:

(1) $\chi(x_2) = (1-q)^{-1}$, $\chi(x_i) = 1$ für $i \neq 2$

(2) $\chi(x_2) = -(1+2^f)^{-1}$, $\chi(x_i) = 1$ für $i \neq 2$

bezw. $\chi(x_2) = -1$, $\chi(x_4) = (1-2^f)^{-1}$, $\chi(x_i) = 1$ für $i \neq 2,4$

(3) $\chi(x_1) = -1$, $\chi(x_3) = (1-2^f)^{-1}$, $\chi(x_i) = 1$ für $i \neq 1,3$.

Aus dem Beweis des Satzes erhielt man noch das folgende Korollar: Ist $q(G) \neq 2$, dann ist die Invariante $q(G)$ durch die Invarianten $s(G)$ und $\mathrm{Im}(\chi)$ bestimmt. Denn sei $s(G) = p^e$, I der dualisierende Modul von G als abelsche Gruppe, dann gilt: $\mathrm{Aut}(I) = (\mathbb{Z}_p/p^e\mathbb{Z}_p)^x \subseteq \mathrm{End}(I) = \mathbb{Z}_p/p^e\mathbb{Z}_p$ und $q(G) = \max\{q'$

$= p^h \mid \mathrm{Im}\,\chi \subseteq 1 + q'\,\mathrm{End}(I)\}$

Außerdem konnte mit Hilfe der im Beweis entwickelten Methoden noch der folgende Satz bewiesen werden: Sei k eine endliche Erweiterung der rationalen p-adischen Zahlen und G eine p-Sylowuntergruppe der Galoisgruppe von k, k' die Körpererweiterung von k, die man durch Adjunktion einer primitiven p-ten Einheitswurzel erhält, a der Grad von k' über den rationalen

Gefördert durch DFG Deutsche Forschungsgemeinschaft

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

p-adischen Zahlen, dann ist G eine Demuskingruppe abzählbaren Ranges, der dualisierende Modul von G ist der G-Modul der aus allen Einheitswurzeln mit p-Potenzordnung besteht und es gilt: $t(G) = (-1)^a$.

Dazu erhält man wieder ein Korollar: Ist $q(G) \neq 2$, dann ist $q(G) = p^h$ die höchste p-Potenz, sodaß k' eine primitive p^h-te Einheitswurzel enthält.

ROQUETTE: <u>Ergänzungen zu den vorangegangenen Vorträgen. Die Galoisgruppe der maximal unverzweigten p-Erweiterung eines Funktionenkörpers einer Variablen über einem algebraisch abgeschlossenen Grundkörper.</u>

Ist G die maximale p-Faktorgruppe der Galoisgruppe eines p-adischen Körpers k, der die p-ten Einheitswurzeln enthält, dann folgt aus den vorangehenden Vorträgen, daß G eine Demuskingruppe ist. Die Invariante $q(G) = p^h$ ist die maximale p-Potenz, sodaß k eine primitive p^h-te Einheitswurzel enthält, falls $p \neq 2$ ist.

Das Interesse für die maximale p-Faktorgruppe G der Galoisgruppe von k entspringt der folgenden Fragestellung: Wann kann eine endliche p-Gruppe H als Galoisgruppe über k realisiert werden? Dies ist genau dann der Fall, falls sich H als Quotient von G darstellen läßt. Aus dem Vorangehenden erhält man nun, falls k ein p-adischer Körper ist, die folgenden notwendigen Bedingungen:

Sei n der Grad von k über den rationalen p-adischen Zahlen, n(H) der Rang von H. Damit sich H als Galoisgruppe realisieren läßt, muß folgendes erfüllt sein:

(1) Falls k nicht p-ten Einheitswurzeln enthält:
   $n(H) \leq n+1$

(2) Falls k die p-ten Einheitswurzeln enthält:
   $n(H) \leq n+2$ und es gibt ein System von n+2 Erzeugenden von H, die einer Demuskinrelation genügen.

Entsprechend ergibt sich: H läßt sich dann und nur dann als Galoisgruppe über einer endlichen Erweiterung von k realisieren, wenn sich H als Quotient einer der untereinander konjugierten p-Sylowgruppen der Galoisgruppe von k darstellen läßt.

Sei nun k ein Funktionenkörper einer Variablen vom Geschlecht g über einem algebraisch abgeschlossenen Grundkörper. Ist $p = \mathrm{char}\ k > 0$ und G die Galoisgruppe der maximal unverzweigten p-Erweiterung von k, dann ist G eine freie pro-p-Gruppe vom Rang $\leq g$. Ist p eine Primzahl verschieden von der Charakteristik von k, dann ist G eine Demuskingruppe vom Rang 2g mit der Relation $(x_1,x_2)(x_3,x_4)\ldots(x_{2g-1},x_{2g}) = 1$. Ist $\mathrm{char}\ k = p > 0$ und G die maximale p-Erweiterung von k, d.h. man läßt an allen Stellen von k Verzweigungen zu, dann sieht man sofort, daß G eine freie pro-p-Gruppe ist.
Problem: Wie sieht die Galoisgruppe der maximalen nur an endlich vielen Stellen verzweigten p-Erweiterung von k aus?

P.Hahnel (Heidelberg)