Astérisque

HELMUT KOCH
B. B. VENKOV

Über den p-klassenkörperturm eines imaginär-quadratischen zahlkörpers

Astérisque, tome 24-25 (1975), p. 57-67
<http://www.numdam.org/item?id=AST_1975__24-25__57_0>

Société Mathématique de France
Astérisque 24-25 (1975)

ÜBER DEN p-KLASSENKÖRPERTURM EINES IMAGINÄR-QUADRATISCHEN ZAHLKÖRPERS

von

Helmut KOCH und B. B. VENKOV

-:-:-:-

Sei k ein imaginär-quadratischer Zahlkörper, p eine von 2 verschiedene Primzahl und K die maximale unverzweigte p-Erweiterung von k. Im folgenden interessieren wir uns für die Struktur der Galoisschen Gruppe G von K/k als Pro-p-Gruppe. Dabei gehen wir von bekannten arithmetischen Sätzen über die Struktur von G aus. Die hier durchgeführte Untersuchung ist rein gruppentheoretischer Natur.

Insbesondere interessieren wir uns für den Fall, daß G endlich ist, d. h. daß der Klassenkörperturm K/k nach endlich vielen Schritten abbricht.

Bezüglich der verwendeten gruppentheoretischen Bezeichnungen und Rechenregeln, insbesondere über höhere Kommutatoren, verweisen wir auf [1], Kapitel 10, und [3], § 7.

1. - Nach I. R. Schafarewitsch (siehe [3]) ist G eine Pro-p-Gruppe, deren Erzeugendenrang d gleich dem Relationenrang gleich dem Rang der p-Klassengruppe von k ist. Auf G operiert der Automorphismus σ, der jedes Element von k in

sein konjugiert-komplexes überführt. σ hat die Ordnung 2. Aus der Klassenkörpertheorie ist bekannt, daß σ auf $G/[G,G]$, d. h. auf der p-Klassengruppe, durch Übergang zum Reziproken operiert. Wir bezeichnen eine endlich erzeugte Pro-p-Gruppe G mit den folgenden drei Eigenschaften als Schursche σ-Gruppe:

1) Der Erzeugendenrang ist gleich dem Relationenrang

2) $G/[G,G]$ ist endlich

3) Auf G operiert ein Automorphismus σ der Ordnung 2, der auf $G/[G,G]$ den Übergang zum Reziproken erzeugt.

Wir interessieren uns im folgenden für die Struktur der Schurschen σ-Gruppen.

2. - Für eine beliebige Pro-p-Gruppe H bezeichnet $H^{(n)}$ das n-te Glied der absteigenden Zentralreihe.

Sei $1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$ eine Repräsentation von G durch die freie Pro-p-Gruppe F mit den Erzeugenden $s_1, \ldots, s_d$ und dem Relationenmodul R mit den Erzeugenden $r_1, \ldots, r_d$. Wir setzen σ zu einem Automorphismus von F fort, der ebenfalls mit σ bezeichnet wird.

Die in 1. aufgezählte Information über G läßt sich folgendermaßen ausdrücken:

Die Erzeugenden $s_1, \ldots, s_d$ können so gewählt werden, daß für $i = 1, \ldots, d$

$$r_i \equiv s_i^{q_i} \mod F^{(2)} \tag{1}$$

und

(2) $$s_i^{\sigma} \equiv s_i^{-1} \mod R\,F^{(2)}$$

(3) $$s_i^{\sigma^2} \equiv s_i \mod R$$

gilt, wobei q_i eine durch p teilbare p-Potenz ist.

(4) R ist invariant bei σ .

3. - LEMMA 1. - Bei passender Wahl der Erzeugenden $s_1, \ldots, s_d$ gilt

$$s_i^{\sigma} \equiv s_i^{-1} \mod R \quad \text{für} \quad i = 1, \ldots, d .$$

Beweis : $s'_i = s_i^{\frac{1}{2}} s_i^{-\frac{1}{2}\sigma}$ unterscheidet sich von s_i nur um ein Element aus $RF^{(2)}$, und es wird

$$s'^{\sigma}_i \equiv s_i^{\frac{1}{2}\sigma} s_i^{-\frac{1}{2}} \equiv (s_i^{\frac{1}{2}} s_i^{-\frac{1}{2}\sigma})^{-1} \equiv s'^{-1}_i \mod R .$$

Daher ist $\{s'_i \mid i = 1, \ldots, d\}$ ein Erzeugendensystem von F mit den gewünschten Eigenschaften.

LEMMA 2. - Bei passender Fortsetzung von σ auf F gilt $\sigma^2 = 1$ und $h^{\sigma} \equiv h^{(-1)^n} \mod F^{(n+1)}$ für $h \in F^{(n)}$.

Beweis : Die erste Behauptung ist klar wegen Lemma 1 : Bei passender Wahl der Erzeugenden können wir $s_i^{\sigma} = s_i^{-1}$ setzen. Zum Beweis der zweiten Behauptung bemerken wir, daß $F^{(n)} \mod F^{(n+1)}$ von den Elementen der Form $(s_{i_1}, \ldots, s_{i_n})$ erzeugt wird, wobei $1 \leq i_k \leq d$ für $k = 1, \ldots, n$ ist. Weiter ist

$$(s_{i_1}, \ldots, s_{i_n})^{\sigma} \equiv (s_{i_1}^{-1}, \ldots, s_{i_n}^{-1}) \equiv (s_{i_1}, \ldots, s_{i_n})^{(-1)^n} \mod F^{(n+1)} .$$

Im folgenden setzen wir immer $\sigma^2 = 1$ und $h^\sigma \equiv h^{-1} \bmod F^{(2)}$ für $h \in F$ voraus.

SATZ 1. - Die erzeugenden Relationen $r_1, \ldots, r_d$ einer Schurschen σ-Gruppe können stets so gewählt werden, daß

$$r_i = \rho_i \rho_i^{-\sigma} \quad , \quad i = 1, \ldots, d \ ,$$

gilt, wobei ρ_i ein Element von F mit

$$\rho_i \equiv s_i^{\frac{1}{2}q_i} \bmod F^{(2)} \tag{5}$$

ist.

Seien andererseits ρ_i, $i = 1, \ldots, d$ beliebige Elemente von F mit (5). Dann genügt der von $\{r_i = \rho_i \rho_i^{-\sigma} \mid i = 1, \ldots, d\}$ erzeugte Relationenmodul R den Bedingungen (1), (4) und F/R ist eine Schursche σ-Gruppe. Genauer gilt

$$r_i^\sigma = r_i^{-1} \ . \tag{6}$$

Beweis : Sei $\{r_1, \ldots, r_d\}$ ein erzeugendes Relationensystem, das den Bedingungen (1), (4) genügt. $r'_i = r_i^{\frac{1}{2}} r_i^{-\frac{1}{2}\sigma}$ unterscheidet sich von r_i nur um ein Element aus $F^{(2)} = [F, F]$.

$$\{ r'_i \ , \ r_i r'^{-1}_i \mid i = 1, \ldots, d \}$$

ist ein nichtminimales erzeugendes Relationensystem, aus dem gewisse d Relationen weggelassen werden dürfen. Eine Relation der Form r'_i, kann nicht weggelassen werden, da $G/[G,G]$ endlich ist. Daher ist $\{r'_i \mid i = 1, \ldots, d\}$ erzeugendes Relationensystem, das mit $\rho_i = r_i^{\frac{1}{2}}$ den Bedingungen des ersten Teils von Satz 1 genügt. Der zweite Teil ist offensichtlich.

Sei $\{F_i \mid i = 1, 2, \ldots\}$ die Zassenhaus-Filtrierung (siehe [3], § 7) von F

Das Relationensystem $\{r_i \mid i = 1, \ldots, d\}$ werde minimal bezüglich der Zassenhaus-Filtrierung folgendermaßen gewählt : Wir konstruieren induktiv

Teilrelationensysteme R_n, $n = 1, 2, \ldots$, und setzen dann

$$\{ r_i \mid i = 1, \ldots, d \} = \bigcup_{n=1}^{\infty} R_n .$$

Sei $R_1 = \emptyset$. Wenn R_{n-1} schon konstruiert ist, setzen wir

$$R_n = R_{n-1} \cup \{ r_1^{(n)}, \ldots, r_{a_n}^{(n)} \} ,$$

wobei die $r_1^{(n)}, \ldots, r_{a_n}^{(n)}$ zusammen mit den Elementen aus R_{n-1} mod F_{n+1} ein minimales Erzeugendensystem von RF_{n+1}/F_{n+1} als Normalteiler von F/F_{n+1} bilden. Die natürlichen Zahlen a_n sind dann Invarianten von G (siehe hierzu [2]). Offenbar gilt

$$\sum_{n=2}^{\infty} a_n = d .$$

SATZ 2. - Die Invarianten a_n einer Schurschen σ-Gruppe können nur für ungerades n von 0 verschieden sein.

Bemerkung : Wir erinnern daran, daß wir grundsätzlich $p \neq 2$ voraussetzen. Für $p < n$ besagt Satz 2, daß die Relationen $r_i \in F_n$, $r_i \notin F_{n+1}$ abgesehen von p-ten Potenzen mit Kommutatoren von ungeradem Gewicht n beginnen : $r_i \in F^{(n)} F^p$, $r_i \notin F^{(n+1)} F^p$.

Beweis von Satz 2. : Wie man leicht sieht, kann man ein Relationensystem gleichzeitig minimal bezüglich der Zassenhaus-Filtrierung und mit der Eigenschaft (6) wählehn.

F_n wird mod F_{n+1} von den Elementen der Form

$$(s_{i_1}, \ldots, s_{i_k})^{p^\lambda} \quad \text{mit} \quad k p^\lambda = n$$

erzeugt. Daher gilt bei $p \neq 2$

$$h^\sigma \equiv h^{(-1)^n} \mod F_{n+1} \text{ für } h \in F_n .$$

Für gerades n wird also

$$r_i^{\sigma} \equiv r_i \mod F_n$$

und wegen (6)

$$r_i \equiv 1 \mod F_{n+1} , \quad \text{q. e. d.}$$

COROLLAR. - Sei G endlich. Dann ist $d \leq 2$. Für $d = 2$ gibt es bezüglich der Invarianten a_n höchstens drei Typen : $a_3 = 2$, $a_3 = a_5 = 1$, $a_3 = a_7 = 1$.

Beweis : Nach [3], Satz 7.2. wäre für $d \geq 3$ und $R \subset F_3$

$$d > \frac{d^3}{3^3} \cdot 2^2 \geq \frac{d}{3} 2^2 .$$

Für $d = 2$, $R \subset F_5$ wäre

$$2 > \frac{2^5}{5^5} \cdot 4^4 = \frac{4^9}{10^5} = \left(\frac{1024}{1000}\right)^2 \cdot \frac{10}{4}$$

Nach [3], Satz 7.20, wäre im Falle $a_3 = a_9 = 1$.

$$\varphi(t) = 1 - 2t + t^3 + t^9 > 0 \quad \text{für} \quad 0 < t < 1 .$$

Jedoch wird $\varphi(0,7) < 0$.

Daraus folgt die Behauptung. (Tatsächlich sind schon die Pro-p-Gruppen mit zwei Erzeugenden und zwei Relationen vom Typ $a_3 = a_8 = 1$ unendlich).

4. - In Ergänzung zu Satz 1 beweisen wir den folgenden Fortsetzungssatz für Relationen.

SATZ 3. - Sei $r \in F$ mit

$$r^{\sigma} \equiv r^{-1} \mod F^{(n)} .$$

Für ungerade n gilt dann

$$(7) \qquad (rx)^{\sigma} \equiv (rx)^{-1} \mod F^{(n+1)} \text{ für alle } x \in F^{(n)} .$$

Für gerades n gibt es mod $F^{(n+1)}$ genau ein $x \in F^{(n)}$ mit

$$(8) \qquad (rx)^{\sigma} \equiv (rx)^{-1} \mod F^{(n+1)} .$$

Beweis : Sei $r^{\sigma} \equiv r^{-1}y \mod F^{(n+1)}$, $y \in F^{(n)}$. Für ungerades n wird

$$r = r^{\sigma^2} = (r^{-1}y)^{\sigma} \equiv (r^{-1}y)^{-1} y^{-1} = ry^{-2} \mod F^{(n+1)}$$

und daher $y \in F^{(n+1)}$.

Weiter gilt $(rx)^{\sigma} \equiv r^{-1}x^{-1} \equiv (rx)^{-1} \mod F^{(n+1)}$.

Für gerades n und $x \in F^{(n)}$ wird

$$(rx)^{\sigma} \equiv r^{-1}yx \equiv (rx)^{-1} yx^2 \mod F^{(n+1)}$$

(8) ist daher genau dann erfüllt, wenn $x \equiv y^{-\frac{1}{2}} \mod F^{(n+1)}$ gesetzt wird.

5. - In diesem Abschnitt geben wir zwei Beispiele, die das vorhergehende illustrieren.

Beispiel. - Sei $r_1 = s_1^{q_1} (s_1, s_2, s_1)^{\alpha_1} (s_1, s_2, s_2)^{\beta_1}$, $\alpha_1, \beta_1 \in \mathbb{Z}_p$

$r_2 = s_2^{q_2} (s_1, s_2, s_1)^{\alpha_2} (s_1, s_2, s_2)^{\beta_2}$, $\alpha_2, \beta_2 \in \mathbb{Z}_p$

$\alpha_1 q_2 q_1^{-1} + \beta_2 \not\equiv 0 \pmod p$, $\alpha_1\beta_2 - \alpha_2\beta_1 \not\equiv 0 \pmod p$.

Dann ist $G = F/(r_1, r_2)$ eine endliche Schursche σ-Gruppe vom Typ $a_3 = 2$ mit $G^{(4)} = \{1\}$.

Beweis : Offenbar ist

$$r_i^{\sigma} \equiv r_i^{-1} \mod F^{(4)}, \quad i = 1, 2 . \tag{9}$$

Wir setzen zur Abkürzung

$$(s_1, s_2, s_1, s_1) = h_1 , \ (s_1, s_2, s_1, s_2) = h_2 , \ (s_1, s_2, s_2, s_2) = h_3 .$$

Dann wird

$$(r_1, s_1) \equiv h_1^{\alpha_1} h_2^{\beta_1} \pmod{F^{(5)}}, \ (r_2, s_2) \equiv h_2^{\alpha_2} h_3^{\beta_2} \pmod{F^{(5)}}$$

$$(r_1, s_2)^{q_2 q_1^{-1}} (r_2, s_1) \equiv (s_1^{q_1}, s_2)^{q_2 q_1^{-1}} h_2^{\alpha_1 q_2 q_1^{-1}} h_3^{\beta_1 q_2 q_1^{-1}} (s_2^{q_2}, s_1) h_1^{\alpha_2} h_2^{\beta_2} \pmod{F^{(5)}}.$$

Wegen

$$(s_1^{q_1}, s_2)^{q_2 q_1^{-1}} (s_2^{q_2}, s_1) \equiv 1 \pmod{R F^{(5)}}$$

erhält man insgesamt

$$h_1^{\alpha_1} h_2^{\beta_1} \equiv 1 , \ h_2^{\alpha_2} h_3^{\beta_2} \equiv 1 , \ h_1^{\alpha_2} h_2^{\alpha_1 q_2 q_1^{-1} + \beta_2} h_3^{\beta_1 q_2 q_1^{-1}} \equiv 1 \pmod{R F^{(5)}} .$$

Die Determinante

$$\begin{vmatrix} \alpha_1 & \beta_1 & 0 \\ 0 & \alpha_2 & \beta_2 \\ \alpha_2 & \alpha_1 q_2 q_1^{-1} + \beta_2 & \beta_1 q_2 q_1^{-1} \end{vmatrix} = (\alpha_2 \beta_1 - \beta_2 \alpha_1)(\alpha_1 q_2 q_1^{-1} + \beta_2)$$

ist nach Voraussetzung $\not\equiv 0 \pmod p$. Daher folgt

$$h_1 \equiv h_2 \equiv h_3 \equiv 1 \pmod{R F^{(5)}} , \text{ d. h.}$$

$$F^{(4)} \subseteq R F^{(5)} . \tag{10}$$

Aus (10) folgt

$$F^{(n)} \subseteq R F^{(n+1)} \text{ für } n \geq 4$$

und daher

$$F^{(4)} \subseteq R \,. \tag{11}$$

(11) ist gleichbedeutend mit $G^{(4)} = \{1\}$. Da $G/G^{(4)}$ offenbar endlich ist, folgt, daß G endlich ist. G ist Schursche σ-Gruppe wegen (9) und (11).

Wir wollen jetzt zeigen, daß Schursche σ-Gruppen vom Typ $a_3 = 1$, $a_5 = 1$ und daher erst recht vom Typ $a_3 = 1$, $a_7 = 1$ unendlich sein können. Dazu bedienen wir uns der Methode von Golod-Schafarewitsch. Wir müssen von der Zassenhaus-Filtrierung zu allgemeineren Filtrierungen übergehen, die von Lazard [4] untersucht wurden und daher im folgenden als Lazard-Filtrierungen bezeichnet werden :

Der vervollständigte Gruppenring $F_p[[F]]$ der freien Pro-p-Gruppe F mit den Erzeugenden $s_1, \ldots, s_d$ über den Körper F_p mit p Elementen ist isomorph zum nichtkommutativen Potenzreihenring $F_p[[x_1, \ldots, x_d]]$ in den Unbestimmten $x_1, \ldots, x_d$. Der Isomorphismus ist gegeben durch die Zuordnung

$$s_i \longrightarrow 1 + x_i \quad \text{für} \quad i = 1, \ldots, d \,.$$

Im folgenden identifizieren wir $F_p[[F]]$ mit $F_p[[x_1, \ldots, x_d]]$. In $F_p[[x_1, \ldots, x_d]]$ führen wir ein Bewertung ν ein, indem wir für $\nu(x_i)$ beliebige positive ganze Zahlen τ_i nehmen. Für eine beliebige Potenzreihe

$P(x_1, \ldots, x_d) = \sum a_{i_1, \ldots, i_k} x_{i_1} \cdots x_{i_k}$ setzen wir

$$\nu(P(x_1, \ldots, x_d)) = \min \{ \sum_{\lambda=1}^{k} \nu(x_{i_\lambda}) \mid a_{i_1, \ldots, i_k} \neq 0 \} \,.$$

Als Lazard-Filtrierung von Typ $\tau_1, \ldots, \tau_d$ bezeichnen wir dann die Filtrierung $\{F^{(\lambda)} \mid \lambda \in N\}$ von F, die durch

$$F^{(\lambda)} = \{h \in F \mid \nu(h-1) \geq \lambda\}$$

gegeben ist

Sei G eine Pro-p-Gruppe, die durch die Repräsentationen

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

gegeben ist, wobei R von den Relationen $r_1, \ldots, r_b$ erzugt werde. Wir definieren d_k als Anzahl der Erzeugenden s_i mit $\nu(s_i - 1) = k$ und b_k als Anzahl der Relationen r_i mit $\nu(r_i - 1) = k$. Dann gilt

SATZ 4. - Sei G endlich. Dann ist

$$\varphi(t) = 1 + (b_1 - d_1)t + (b_2 - d_2)t^2 + \ldots > 0$$

für $0 < t < 1$.

Der Beweis von Satz 4 ist vollständing analog zum Beweis von Satz 7.20 in [3] (*).

Beispiel 2. - Sei $R = (r_1, r_2)$,

$$r_1 = s_1^p (s_1, s_2, s_2)\,(s_1^{-1}, s_2^{-1}, s_2^{-1})^{-1}\, s_1^p$$

$$r_2 = s_2^p (s_1, s_2, s_1, s_1, s_2)(s_1^{-1}, s_2^{-1}, s_1^{-1}, s_2^{-1}, s_2^{-1})^{-1}\, s_2^p \quad .$$

Dann ist $G = F/R$ eine Schursche σ-Gruppe vom Typ $a_3 = 1$, $a_5 = 1$, die für genügend großes p unendlich ist.

Beweis : Wegen Satz 1 ist G eine Schursche σ-Gruppe. Man rechnet leicht nach, daß $r_2 F_6$ nicht in $(r_1) F_6/F_6$ enthalten ist (hier bezeichnet (r_1) den von r_1 erzeugten Normalteiler von F). Daher ist G vom Typ $a_3 = 1$, $a_5 = 1$. Weiter wenden wir Satz 4 an und setzen dazu $\nu(s_1 - 1) = 1$, $\nu(s_2 - 1) = \tau$. Dann gehört

---

(*) Satz 4 wurde unabhängig und bereits früher von I. V. Andojskij bewiesen.

bei $p \geq 1+2\tau$ zu G das Polynom $\varphi(t) = 1 - t^{\tau} - t + t^{1+2\tau} + t^{3+2\tau}$. Wir wollen zeigen, daß dieses Polynom für genügend großes τ negativ wird. Dazu setzen wir

$$t = 1 - \frac{1}{\tau} .$$

Dann wird

$$\varphi(t) = \frac{1}{\tau} - (1 - \frac{1}{\tau})^{\tau} + (1 - \frac{1}{\tau})^{1+2\tau} + (1 - \frac{1}{\tau})^{3+2\tau} = \psi(\tau)$$

$$\lim_{\tau \to \infty} \psi(\tau) = -e^{-1} + 2e^{-2} < 0 , \qquad \text{q.e.d.}$$

-:-:-:-

LITERATUR

[1] M. HALL. - The theory of groups, New York, (1959).

[2] H. KOCH. - Zum Satz von Golod-Schafarewitsch, Math. Nachr. 42, (1969), 321-333.

[3] H. KOCH. - Galoissche Theorie der p-Erweiterungen, Berlin, (1970).

[4] M. LAZARD. - Groupes analytiques p-adiques. Publ. math. I. H. E. S. 26 (1965), 389-603.

-:-:-:-

Die vorliegende Arbeit gibt nur einen Teil meines Vortrags in Bordeaux wieder. Der andere Teil erscheint demnächst im Crelle-Journal.

-:-:-:-

Helmut KOCH
108 BERLIN-DDR,
Mohrenstr. 39, ZIMM
Akademie der Wissenschaften
der DDR