ACTA ARITHMETICA
XXXI (1976)

Polynome mit nicht durch Restklassen beschreibbaren Primteilermengen

von

VOLKER SCHULZE (Clausthal-Zellerfeld)

Ist $f(x)$ ein irreduzibles Polynom aus dem Polynomring $\boldsymbol{Z}[x]$ der ganzen rationalen Zahlen in einer Unbestimmten x, so bezeichnen wir mit

$$P_f = \{p:\ p \text{ Primzahl, es gibt ein } a \in \boldsymbol{Z} \text{ mit } p \mid f(a)\}$$

die Primteilermenge von $f(x)$, mit K_f den Zerfällungskörper über dem Körper $\boldsymbol{Q}$ der rationalen Zahlen und mit G die zugehörige Galoisgruppe. Ist ξ eine Nullstelle von $f(x)$, so ist P_f bekanntlich bis auf endlich viele Ausnahmen gerade die Menge aller Primzahlen, die in $\boldsymbol{Q}(\xi)$ wenigstens einen Primidealfaktor ersten Grades besitzen. Eine einfache Charakterisierung von P_f ist nur in Spezialfällen bekannt, in denen P_f durch Restklassen beschrieben wird. Eine notwendige und hinreichende Aussage darüber, wann dies möglich ist, ergibt sich leicht aus den Zerlegungsgesetzen für Primideale in algebraischen Zahlkörpern. Nach [3] sind die beiden folgenden Eigenschaften gleichwertig:

E_1: *Es gibt einen Modul m derart, daß P_f bis auf endlich viele Ausnahmen aus allen Primzahlen besteht, die in gewissen Restklassen des Moduls m liegen.*

E_2: *Die Menge H aller Automorphismen aus G, die eine Nullstelle von $f(x)$ festlassen, ist Normalteiler in G mit abelscher Faktorgruppe.*

Ist G abelsch, so ist dies offenbar hinreichend, aber nicht notwendig dafür, daß $f(x)$ die Eigenschaft E_2 erfüllt. Die Eigenschaft E_2 erweist sich für den Fall, daß die Galoisgruppe nicht abelsch ist, als sehr einschneidend. Vereinzelte Beispiele von irreduziblen Polynomen mit nichtabelscher Galoisgruppe und der Eigenschaft E_2 werden in [1], [2] und [3] angegeben, umfangreichere Klassen solcher Polynome sind dagegen nicht bekannt. Umgekehrt lassen sich jedoch Klassen von irreduziblen Polynomen bestimmen, welche E_2 nicht erfüllen. Eine Aussage in diese Richtung macht der folgende Satz. Interessant an ihm ist, daß über die Struktur der Galoisgruppe G nur vorausgesetzt wird, daß G nicht abelsch ist.

Satz. *Ein irreduzibles Polynom von Primzahlpotenzgrad mit nichtabelscher Galoisgruppe erfüllt nicht* E_2.

Beweis. Wir führen die Annahme zum Widerspruch, daß das irreduzible Polynom $f(x)$ von Primzahlpotenzgrad p^a eine nichtabelsche Galoisgruppe G besitzt, und die Menge H aller Automorphismen aus G, die eine Nullstelle von $f(x)$ festlassen, ein Normalteiler mit abelscher Faktorgruppe ist. Dann ist der H zugeordnete Zwischenkörper K_H normal über $\boldsymbol{Q}$, und wegen der Irreduzibilität von $f(x)$ ist $H \neq G$. Das Polynom $f(x)$ zerfällt demnach in K_H in irreduzible Polynome gleichen Grades, also in Polynome von Primzahlpotenzgrad, d.h. für den Zerfällungskörper K_f von $f(x)$ über $\boldsymbol{Q}$ gilt

$$(1) \qquad p \mid [K_f : K_H].$$

Weiter gelte

$$[K_f : \boldsymbol{Q}] = m \cdot p^\beta, \qquad (p, m) = 1.$$

Dann besitzt G nach dem ersten Sylowschen Satz eine Untergruppe der Ordnung p^β, der ein Zwischenkörper K' mit

$$(2) \qquad [K' : \boldsymbol{Q}] = m, \qquad [K_f : K'] = p^\beta$$

zugeordnet ist. Wir betrachten K' als neuen Grundkörper. Wegen $([K' : \boldsymbol{Q}], p) = 1$ gilt für eine Nullstelle ξ von $f(x)$

$$p^a \mid [K'(\xi) : K'],$$

d.h. $f(x)$ ist irreduzibel über K'. Die K_f über K' zugeordnete Galoisgruppe G' ist p-Gruppe. Die Menge

$$H' = G' \cap H$$

aller Automorphismen aus G', die eine Nullstelle von $f(x)$ festlassen, ist offenbar Normalteiler in G'. Der H' zugeordnete Zwischenkörper $K_{H'}$ ist also normal über K'. Weiter gilt

$$|H'| = |G' \cap H| > 1,$$

also

$$(3) \qquad p \,\big|\, |H'|,$$

denn anderenfalls wäre $(K', K_H) = K_f$, und damit wegen (2)

$$p \nmid [K_f : K_H]$$

im Widerspruch zu (1).

Wir zeigen nun, daß es einen über K' normalen Körper K gibt mit $K_{H'} \subseteq K$ und $[K_f : K] = p$. Zunächst ist die Anzahl aller Körper R mit

$$(4) \qquad K_{H'} \subseteq R \subseteq K_f, \qquad [K_f : R] = p$$

gleich der Anzahl aller Untergruppen der Ordnung p von H'. Wegen (3) gibt es eine solche Untergruppe, und nach dem dritten Sylowschen Satz ist ihre Anzahl kongruent $1 \bmod p$. Da $K_{H'}$ normal über K' ist, besitzt mit R auch jeder zu R über K' konjugierte Körper die Eigenschaft (4). Weiter ist die Anzahl der zu R über K' konjugierten Körper wegen

$$[R : K'] = p^{\beta - 1}$$

Vielfaches von p, falls R nicht normal ist über K'. Insgesamt folgt die Existenz von K.

Hieraus ergibt sich nun ein Widerspruch. Einerseits muß nämlich jeder Automorphismus von $K_f | K$ als Automorphismus aus H' eine Nullstelle von $f(x)$ festlassen. Andererseits ist dies für einen von der Identität verschiedenen Automorphismus von $K_f | K$ nicht möglich, da K als von K_f verschiedene normale Erweiterung von K' keine Nullstelle des über K' irreduziblen Polynoms $f(x)$ enthalten kann, und außerdem für eine Nullstelle ξ von $f(x)$ gilt $K(\xi) = K_f$.

Literatur

[1] S. Nakatsuchi, *A Note on Certain Properties of Algebraic Number Fields*, Memoirs of Osaka Kyoiku University 17, Ser. III, No. 1 (1968), S. 1–10.

[2] A. Schinzel, *On a theorem of Bauer and some of its applications*, Acta Arith. 11 (1966), S. 333–344.

[3] V. Schulze, *Die Verteilung der Primteiler von Polynomen auf Restklassen*, J. Reine Angew. Math. 280 (1976), S. 122–133.

Eingegangen am 15. 4. 1975 (695)