COLLOQUIUM MATHEMATICUM

VOL. XX 1969 FASC. 1

EIN EINFACHER BEWEIS DES DEDEKINDSCHEN DIFFERENTENSATZES

VON

W. NARKIEWICZ (WROCŁAW) UND A. SCHINZEL (WARSZAWA)

Der nachstehende wohlbekannte Dedekindsche Differentensatz wurde ursprünglich für den rationalen Zahlkörper als Grundkörper in [1] bewiesen. In Heckes Buch [3] (Satz 115) liegt ein Beweis für die relativ-Galoisschen Erweiterungen vor. In dieser Arbeit wird für den vollständigen Differentensatz ein Beweis erbracht, der nicht länger ist und nur solche Ergebnisse benötigt, welche dem eben erwähnten Satze in [3] vorangehen. Daß sie zu diesem Zweck schon ausreichen, hat uns selbst überrascht, insofern die uns bekannten bisherigen Beweise entweder sehr lang oder an lokale Betrachtungen gebunden sind. Unsere Bezeichnungen stimmen mit [3] überein.

Satz. *Es sei K eine endliche Erweiterung eines algebraischen Zahlkörpers k, und D ihre relative Differente. Wenn* $\mathfrak{p} = \mathfrak{P}^e \mathfrak{A}$ *mit* $\mathfrak{P} \nmid \mathfrak{A}$ *und* $e \not\equiv 0 \pmod{\mathfrak{P}}$ *gilt, dann ist die Differente D nicht durch $\mathfrak{P}^e$ teilbar.*

Beweis. Es sei R_k der Ring der ganzen Zahlen in k, und γ und δ Zahlen aus R_k, die folgende Bedingungen erfüllen:

$$(1)\qquad \gamma = \mathfrak{p}\mathfrak{a},\ \delta \equiv 0 \pmod{\mathfrak{a}},\ (\delta, \mathfrak{p}) = 1, \qquad \mathfrak{a} \text{ — Ideal in } k.$$

Wir bezeichnen mit A eine Primitivzahl $(\bmod\ \mathfrak{P})$, für welche

$$(2)\qquad A^{N(\mathfrak{P})} - A \not\equiv 0 \pmod{\mathfrak{P}^2}, \qquad A \equiv 0 \pmod{\mathfrak{A}}$$

(wo $N(\mathfrak{P})$ die absolute Norm des Ideals $\mathfrak{P}$ bezeichnet) gilt.

Jede ganze Zahl in K ist nach jeder Potenz von $\mathfrak{P}$ zu einer Zahl aus $R_k(A)$ kongruent. Außerdem ist die Zahl

$$\Delta = \frac{A^{N(\mathfrak{P})} - A}{\gamma}\,\delta$$

ganz in K. Aus der letzten Formel auf der Seite 145 in [3] folgt, daß die Zahl $\Delta \mu A^{hb}$ eine Darstellung in der Form $P(A)$ zuläßt, wo $P(t)$ ein Polynom mit Koeffizienten in R_k ist. Hier bedeutet hb eine geeignete positive, ganzrationale Zahl, und μ ist eine Zahl aus R_k, welche relativ prim zum Ideal $\mathfrak{p}$ ist. Es folgt

$$\delta\mu(A^{N(\mathfrak{P})}-A)^e A^{hb}-\gamma P(A) = 0$$

und, wenn $\varphi(t)$ das Minimalpolynom von A über k ist,

$$\delta\mu(x^{N(\mathfrak{P})}-x)^e x^{hb}-\gamma P(x) = \varphi(x)\psi(x)$$

mit einem Polynom $\psi(t)$ aus $R_k(t)$.

Durch Differenzierung und Substitution $x = A$ erhalten wir

$$\delta\mu e(A^{N(\mathfrak{P})}-A)^{e-1}(N(\mathfrak{P})A^{N(\mathfrak{P})}-1)A^{hb}+$$
$$+\delta\mu hb(A^{N(\mathfrak{P})}-A)^e A^{hb-1}-\gamma P'(A) = \varphi'(A)\psi(A).$$

Aber $\gamma \equiv 0 \pmod{\mathfrak{P}^e}$, und so ergibt sich

$$\delta\mu e(A^{N(\mathfrak{P})}-A)^{e-1}(N(\mathfrak{P})A^{N(\mathfrak{P})}-1) \equiv \varphi'(A)\psi(A) \pmod{\mathfrak{P}^e}.$$

Aus (1), (2) und $(\mu, \mathfrak{p}) = 1$ erhalten wir nun $\varphi'(a) \not\equiv 0 \pmod{\mathfrak{P}^e}$, und umsomehr $D \not\equiv 0 \pmod{\mathfrak{P}^e}$, w.z.b.w.

LITERATURNACHWEIS

[1] R. Dedekind, *Über die Diskriminanten endlicher Körper*, Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen 29 (1882), S. 1-56; *Werke*, Bd. I, S. 351-397, Braunschweig 1930.

[2] H. Hasse, *Zahlentheorie*, Berlin 1949.

[3] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig 1954.

[4] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker Vereinigung 4 (1894-95), S. 175-546.

MATHEMATISCHES INSTITUT DER UNIVERSITÄT, WROCŁAW
MATHEMATISCHES INSTITUT DER POLNISCHEN AKADEMIE DER WISSENSCHAFTEN

Reçu par la Rédaction le 11. 11. 1967