Časopis pro pěstování matematiky a fysiky

Štefan Schwarz

Über einen Satz von S. Lubelski

Časopis pro pěstování matematiky a fysiky, Vol. 69 (1940), No. 3-4, 146--147

Persistent URL: `http://dml.cz/dmlcz/123331`

Über einen Satz von S. Lubelski.

Štefan Schwarz, Bratislava.

(Eingegangen am 10. Januar 1940.)

Es handelt sich um einen äußerst kurzen und von den Hilfssätzen des Verfassers[1]) freien Beweis des folgenden interessanten Satzes:

Es sei $f(x)$ ein ganzes, ganzzahliges, nicht normales, irreduzibles Polynom. Es sei ferner $\varphi(x)$ eine Galoissche Resolvente von $f(x)$, D die Diskriminante von $\varphi(x)$ und p eine rationale Primzahl, für die $(D, p) = 1$. Dann ist $\varphi(x)$ mod p zerlegbar.

Beweis: Es sei K der Körper der rationalen Zahlen. Weiter $K' = K(\Theta)$, $K'' = K(\vartheta)$, wo Θ resp. ϑ den Gleichungen $f(\Theta) = 0$ resp. $\varphi(\vartheta) = 0$ genügen. Also

$$K \subset K' \subset K''.$$

Es sei weiter $\mathfrak{G}$ die Galoissche Gruppe von K'' bezüglich K, $\mathfrak{H}$ die zu K' gehörige Untergruppe von $\mathfrak{G}$, $\mathfrak{E}$ die Einheitsgruppe:

$$\mathfrak{G} \supset \mathfrak{H} \supset \mathfrak{E}.$$

Da K'' normal ist, ist sein Grad zugleich Ordnung von $\mathfrak{G}$. Er sei durch n bezeichnet.

Um die Behauptung zu beweisen, schließen wir folgendermassen. Ist $\varphi(x)$ mod p irreduzibel, so ist p in K'' unzerlegbar und der Grad des Primideals (p) ist n. Für jede ganze Zahl ω aus K'' gilt dann

$$\omega^{p^n} \equiv \omega \pmod{p}.$$

Die Substitution σ_p aus $\mathfrak{G}$, für die (unabhängig von ω) die Relation

$$\omega^p \equiv \sigma_p \omega \bmod p,$$

für jedes ganze ω aus K'' gilt, ist bekanntlich die Erzeugende der Zerlegungsgruppe $\mathfrak{G}_Z$ zu p.[2]) Die Zerlegungsgruppe ist offenbar

[1]) Vgl. S. Lubelski: Zur Reduzibilität von Polynomen in der Kongruenztheorie, Acta Aritmetica 1 (1936). S. 169—183; 2 (1937). S. 250—261.

[2]) Vgl. z. B. R. Fricke: Lehrbuch der Algebra III, S. 175.

zyklisch und ihre Ordnung ist gleich dem Grad von p, also n. Da aber auch die Ordnung von $\mathfrak{G}$ gleich n ist, gilt $\mathfrak{G}_Z = \mathfrak{G}$.

$\mathfrak{G}$ ist danach zyklisch. Da jede Untergruppe einer zyklischen Gruppe wieder zyklisch ist, ist auch $\mathfrak{H}$ zyklisch, also Normalteiler. Der zugehörige Körper K' ist also normal, entgegen der Voraussetzung. Die Annahme, daß $\varphi(x)$ mod p unzerlegbar ist, ist falsch; w. z. b. w.

Anmerkung: Es ist auch leicht einzusehen, daß dieser Satz und sein Beweis allgemeiner für Polynome $f(x)$ aus einem beliebigen Körper K und dessen Primideale $\mathfrak{p}$ gilt.

*

O jednej vete S. Lubelského.

(Obsah predošlého článku.)

V článku je podaný krátky dôkaz tejto vety.

Nech je $f(x)$ celočíselný, nie normálny, nerozložitelný mnohočlen. Nech je $\varphi(x)$ Galoisovou resolventou $f(x)$, ďalej D diskriminant mnohočlenu $\varphi(x)$ a p racionálne prvočíslo, pre ktoré platí $(D, p) = 1$. Potom je $\varphi(x)$ mod p rozložiteľné.