## Werk

**Label:** Article

**PURL:** https://resolver.sub.uni-goettingen.de/purl?31311028X_0069|log46


## Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

# 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 $\Theta$ resp. $\vartheta$ 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 $\omega$ aus $K''$ gilt dann

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

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

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

für jedes ganze $\omega$ 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.