ZWEI LÜCKENSÄTZE ÜBER POLYNOME IN ENDLICHEN PRIMKÖRPERN MIT ANWENDUNG AUF DIE ENDLICHEN ABELSCHEN GRUPPEN UND DIE GAUSSISCHEN SUMMEN.

Von

L. RÉDEI

in Szeged (Ungarn).

§ 1. Die zu beweisenden Sätze.

Bezeichne p eine positive Primzahl, P den endlichen Primkörper von der Charakteristik $p\,(\neq 2)$ mit dem Einselement 1. Polynome $f(x)$ (mit Koeffizienten) in P nennen wir kurz auch P-Polynome. Wir werden folgende zwei Sätze über P-Polynome von der Form $x^n + \gamma x^m + \cdots$ $(n > m)$ beweisen, die also hinter dem Anfangsglied im allgemeinen eine »Lücke» haben.

Satz 1. *Ein P-Polynom von der Form*

$$f(x) = x^{p-1} + \gamma x^{\frac{p-1}{2}} + \cdots \tag{1}$$

zerfällt in lauter lineare Faktoren (in P) dann und nur dann, wenn

$$f(x) = x^{\frac{p-1}{2}t}(x^{\frac{p-1}{2}} - 1)^u (x^{\frac{p-1}{2}} + 1)^v \qquad (t + u + v = 2) \tag{2}$$

gilt.

Satz 2. *Ein P-Polynom von der Form*

$$g(x) = x^{\frac{p-1}{2}} + \gamma x^n + \cdots \neq x^{\frac{p-1}{2}} \pm 1 \qquad \left(n \leqq \frac{p-1}{4};\ \gamma \neq 0;\ g(0) \neq 0\right) \tag{3}$$

zerfällt in lauter verschiedene lineare Faktoren (in P) dann und nur dann, wenn $4 \mid p - 1$ *und*

$$g(x) = (x^{\frac{p-1}{4}} - 1)^t (x^{\frac{p-1}{4}} + 1)^u (x^{\frac{p-1}{4}} - \sigma)^v (x^{\frac{p-1}{4}} + \sigma)^w \qquad (\sigma^2 = -1;\ t + u = v + w = 1) \tag{4}$$

gilt.