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*

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

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

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

gilt.

Aus Satz 1 gewinnen wir folgenden:

Satz 3. *Für ein System*

$$l_i(x) \qquad \left(i = 0, \pm 1, \ldots, \pm \frac{p-1}{2}\right) \tag{5}$$

von p linearen P-Polynomen bezeichne N die Anzahl der $x(\in P)$, für die (5) in alle verschiedenen Elemente von P übergeht. Dann und nur dann ist

$$N \geqq \frac{p-1}{2}, \tag{6}$$

wenn mit passender Reihenfolge

$$\left.\begin{aligned} l_i(x) &= l_0(x) + i^2(\alpha x + \beta) \\ l_{-i}(x) &= l_0(x) + i^2(\gamma x + \delta) \end{aligned}\right\} \qquad \left(i = 1, \ldots, \frac{p-1}{2}\right) \tag{7}$$

ist und einer der folgenden drei Fälle zutrifft:

$$\begin{aligned} &1)\ \ \alpha\delta - \beta\gamma \neq 0, \quad \chi(\alpha\gamma) \geqq 0, \\ &2)\ \ \alpha\delta - \beta\gamma = 0, \quad \chi(\alpha\gamma) = -1, \\ &3)\ \ \alpha = \gamma = 0, \quad \chi(\beta\delta) = -1, \end{aligned}$$

wobei χ den quadratischen Charakter für P bezeichnet (mit $\chi(0) = 0$). Entsprechend ist

$$N = \frac{p-1}{2}, \quad p-1, \quad \textit{bzw. } p. \tag{8}$$

Merkwürdig ist in diesem Satz, dass es sich um ein »lineares» Problem handelt und die Lösung »quadratisch» ist.

Diese an sich interessanten Sätze lassen Anwendungen zu auf ziemlich abseitsliegenden Gebieten, das sind die Gruppentheorie und die Theorie der Kreiskörper.

Für eine Gruppe $\mathfrak{G}$ mit dem Einselement E betrachten wir Produktzerlegungen

$$\mathfrak{G} = \mathfrak{H}_1 \ldots \mathfrak{H}_r, \tag{9}$$

wobei wir (ohne Einschränkung der Allgemeinheit) ein für allemal annehmen, dass

$$r \geqq 2; \ E \in \mathfrak{H}_i; \ \mathfrak{H}_i \neq E \qquad (i = 1, \ldots, r) \tag{10}$$

ist. Für gewöhnlich beschäftigt man sich nur mit den »klassischen» Fällen, wobei entweder alle $\mathfrak{H}_i$ Gruppen (Untergruppen von $\mathfrak{G}$) sind oder $r = 2$ und das eine von $\mathfrak{H}_1$, $\mathfrak{H}_2$ eine Gruppe, das andere ein Komplex ist (in diesem zweiten Fall handelt es sich nämlich um die Zerlegung von $\mathfrak{G}$ in rechts- oder linksseitigen

Nebengruppen). Wir lassen jetzt für die $\mathfrak{H}_1$ beliebige Komplexe zu, selbstverständlich so, dass die ausmultiplizierte rechte Seite von (9) jedes Element von $\mathfrak{G}$ einmal darstellt. Über solche »nichtklassischen» Zerlegungen kenne ich nur den schönen und wichtigen Satz von HAJÓS[1] (s. unten).

Von nun an sei $\mathfrak{G}$ endlich. Bezeichne dann n_i die Elementenzahl von $\mathfrak{H}_i$. Offenbar ist $n_1 \dots n_r$ die Ordnung von $\mathfrak{G}$. Ein besonders einfacher Fall liegt vor, wenn jedes $\mathfrak{H}_i$ von der Form

$$\mathfrak{H}_i = E, A_i, A_i^2, \dots, A_i^{n_i-1} \tag{11}$$

ist. (Da $\mathfrak{H}_i$ aus verschiedenen Elementen bestehen soll, muss die Ordnung von $A_i \geqq n_i$ sein, und »=» gilt hier dann und nur dann, wenn $\mathfrak{H}_i$ eine Gruppe ist.) Nun lautet der Satz von Hajós so. Wird in einer Zerlegung (9) einer endlichen Abelschen Gruppe $\mathfrak{G}$ (11) angenommen, so muss wenigstens ein $\mathfrak{H}_i$ eine Gruppe sein.[2] Der Satz liegt sehr tief und der Beweis ist mit unerwarteten Schwierigkeiten verbunden.

Ein noch ganz bedeutend schwierigerer Fall liegt vor, wenn man auch die einschränkende Annahme (11) von Hajós fallen lässt. Dann sind die Zerlegungen (9) sogar schon im verhältnismässig einfachen Fall einer endlichen zyklischen Gruppe $\mathfrak{G}$ nicht leicht zu beherrschen. Auf diesen, auch für die elementare Zahlentheorie interessanten Fall möchte ich ein andermal zurückkommen. Lässt man die zyklischen Gruppen ausser Acht, so steht vor uns als einfachster Fall eine Abelsche Gruppe von der Ordnung p^2 (dann kommt in (9) nur $r = 2$ in Betracht). Es ist nun merkwürdig, dass dieses »winzig kleine» Problem gar nicht so leicht ist, vielmehr bedürfen wir zur Beantwortung nicht nur Satz 1, sondern auch den auf diesem beruhenden Satz 3 (letzteren allerdings nicht in vollem Masse). So werden wir beweisen den:

Satz 4. *Ist die nichtzyklische Abelsche Gruppe $\mathfrak{G}$ von der Ordnung p^2 in das Produkt*

$$\mathfrak{G} = \mathfrak{H}\mathfrak{K} \tag{12}$$

von zwei Komplexen $\mathfrak{H}$, $\mathfrak{K}$ mit p Elementen zerlegt ($E \in \mathfrak{H}, \mathfrak{K}$), so ist $\mathfrak{H}$ oder $\mathfrak{K}$ eine Gruppe.

---

[1] G. HAJÓS, Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter, Math. Ztschr. 47 (1941), 427—467.

[2] Mit wiederholter Anwendung folgt, dass bei passender Reihenfolge der $\mathfrak{H}_i$ alle Produkte $\mathfrak{H}_1 \dots \mathfrak{H}_i$ $(i = 1, \dots, r)$ Gruppen sind, und so sind wir im wesentlichen wieder auf eine »klassische» Zerlegung gestossen. Mit obigem Satz bewies Hajós die berühmte Minkowskische Vermutung über lineare Ungleichungssysteme.

Es steht aus, ob auch für jede endliche Abelsche Gruppe $\mathfrak{G}$ eine der Faktoren in (9) eine Gruppe sein muss, wenn alle n_i Primzahlen sind. Ohne diese Einschränkung gilt das nicht nach folgenden zwei (brieflich mitgeteilten) Beispielen von Hajós.

Die durch die Basiselemente A, B, C von der Ordnung bzw. 4, 4, 2 erzeugte Abelsche Gruppe ist gleich dem Produkt

$$(E, A)(E, B)(E, A^2, A\,B^2, A^3\,B^2, C, A^2\,B\,C, A^2\,B^3\,C, B^2\,C).$$

Ist auch C von der Ordnung 4, so gilt die Zerlegung

$$(E, A)(E, B)(E, C)(E, A^2B, B^2\,C, C^2\,A, A^2\,B^3, B^2\,C^3, C^2\,A^3, A^2\,B^2\,C^2).$$

Die zweite Anwendung beruht teils wieder auf Satz 1 (ohne Satz 3), teils auf Satz 2. Bezeichne ϱ eine primitive p-te (komplexe) Einheitswurzel und K den durch ϱ erzeugten Kreisteilungskörper. Es wird bequem die Potenzen ϱ^x von ϱ auf zwei Arten zu bezeichnen, so dass wir für x nicht nur ganze rationale Zahlen, sondern auch die Elemente von P zulassen, indem wir P als den Restklassenkörper mod p [1] auffassen und die Restklasse x durch einen (beliebigen) Repräsentanten ersetzt denken. Wir bezeichnen mit P_n die Untergruppe vom Index n in der (multiplikativen) Gruppe der von 0 verschiedenen Elemente von P (nur $n = 1$, 2, 4 werden in Betracht kommen). Selbst diese Gruppe ist dann P_1. Da sie zyklisch von der Ordnung $p-1$ ist, existiert P_n nur im Falle $n \mid p-1$, und ist dann eindeutig bestimmt. Wir wählen ein erzeugendes Element ξ von P_1. Dann besteht die Faktorgruppe P_1/P_n aus den Elementen (Nebengruppen)

$$\xi^i P_n \qquad (i = 0, \ldots, n-1). \tag{13}$$

Summieren wir ϱ^x für alle Elemente x der Nebengruppe (13) und bezeichnen mit Γ_n^i die so erhaltene Summe. Offenbar sind diese die sogenannten $\frac{p-1}{n}$-gliedrigen Gaussischen Perioden in der Kreisteilungstheorie.[2]

Bezeichne $\mathfrak{p}$ das Primideal

$$\mathfrak{p} = \varrho - 1 \tag{14}$$

in K. Es ist wohlbekannt, dass für die Gaussische Summe

$$\Gamma = 1 + 2\,\Gamma_2^0 = \sum_{i=1}^{p} \varrho^{i^2} \tag{15}$$

[1] Die Restklassen sind dabei im Ring der ganzen rationalen Zahlen zu bilden.

[2] Insbesondere ist Γ_n^0 die Summe der ϱ^k, wobei k die n-ten Potenzreste mod p mit $0 < k < p$ durchläuft, und ähnlich hängen die übrigen Γ_n^i mit den Nebenklassen der Potenzreste zusammen.

oder anders

$$\Gamma = \Gamma_2^0 - \Gamma_2^1 = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \varrho^i \tag{16}$$

die Teilbarkeitseigenschaft

$$\mathfrak{p}^{\frac{p-1}{2}} \| \Gamma^1 \tag{17}$$

gilt. Die angekündigte (zweite) Anwendung wird zeigen, dass es sich in (17) um eine bisher unbekannte Maximaleigenschaft von Γ handelt.

Wir sehen aus (16), dass Γ so entsteht, dass man die Einheitswurzeln $\varrho^i (i = 1, \ldots, p-1)$ je mit dem Faktor $\left(\frac{i}{p}\right) (= \pm 1)$ versehen addiert. Man könnte erwarten, dass es unter allen Summen

$$B = \varrho \pm \varrho^2 \pm \cdots \pm \varrho^{p-1} \tag{18}$$

(deren Zahl 2^{p-2} ist) auch solche gibt, die durch eine höhere Potenz von $\mathfrak{p}$ als Γ teilbar sind. Noch allgemeiner betrachten wir Summen von der Form

$$B_r = \varrho^{x_1} \pm \varrho^{x_2} \pm \cdots \pm \varrho^{x_r} \quad (x_1 = 1;\ p \nmid x_2, \ldots, x_r;\ r \leqq p-1) \tag{19}$$

mit mod p verschiedenen $x_1, \ldots, x_r$, und dann sind wieder allgemeiner die Summen von der Form

$$A = \varrho^{x_1} + \varrho^{x_2} + \cdots + \varrho^{x_p} \qquad (x_1 = 0) \tag{20}$$

mit beliebigen $x_2, \ldots, x_p$.[2] Überraschenderweise nimmt Γ unter allen diesen Summen eine extreme Stellung ein nach dem folgenden:

Satz 5. *Es gilt* $\mathfrak{p}^{\frac{p-1}{2}} \| A$ *nur für*

$$A = 1 + 2\Gamma_2^0 (= \Gamma), \qquad A = 1 + 2\Gamma_2^1 (= -\Gamma), \tag{21}$$

$$A = \frac{p+1}{2} + \Gamma_2^0 \left(= \tfrac{1}{2}(p + \Gamma)\right), \quad A = \frac{p+1}{2} + \Gamma_2^1 \left(= \tfrac{1}{2}(p - \Gamma)\right) \tag{22}$$

und sonst ist $\mathfrak{p}^{\frac{p-1}{2}} \nmid A$, *wenn man von den trivialen Fällen* $A = 0$, p *absieht.*[3]

Insbesondere für die B_r gilt sogar der:

Satz 6. B_r $(r \leqq p-1)$ *ist höchstens durch* $\mathfrak{p}^{\frac{r}{2}}$ *teilbar.*[4]

Noch spezieller ist B unter den B_r stark ausgezeichnet durch den folgenden:

---

[1] »$a^x \| b$» bezeichnet »$a^x \mid b$, $a^{x+1} \nmid b$».

[2] Addiert man nämlich $1 + \varrho + \cdots + \varrho^{p-1} = 0$ zu B_r, so erscheint letzteres in der Tat in der Form (20).

[3] In diesen zwei Fällen sind die x_i paarweise inkongruent, bzw. alle kongruent 0 mod p.

[4] Hierzu ist zu bemerken, dass trivialerweise $\mathfrak{p} \nmid B_r$ ist, wenn die Anzahl der »+» und »−» Zeichen in (19) verschieden, insbesondere also wenn $2 \nmid r$ ist. Ähnliches bezieht sich auch auf die B_r.

Satz 7. *Abgesehen vom Fall* $B = \Gamma_2^0 - \Gamma_2^1 (= \Gamma)$ *mit* $\mathfrak{p}^{\frac{p-1}{2}} \| B$ *ist* B *höchstens durch* $\mathfrak{p}^{\frac{p-1}{4}}$ *teilbar. Dann und nur dann ist* $\mathfrak{p}^{\frac{p-1}{4}} \| B$, *wenn* $4 | p-1$ *und*

$$B = (\Gamma_4^0 - \Gamma_4^2) \pm (\Gamma_4^1 - \Gamma_4^3) \tag{23}$$

[1] *ist.*

Endlich geben wir Satz 1 auch folgende äquivalente Formulierung: [2]

Satz 8. *Das System der* $\frac{p-3}{2}$ *Gleichungen*

$$x_1^i + \cdots + x_{p-1}^i = 0 \qquad \left(i = 1, \ldots, \frac{p-3}{2}\right) \tag{24}$$

in den $p-1$ *Unbekannten* $x_1, \ldots, x_{p-1}$ *hat im Körper* P *(abgesehen von der Reihenfolge der* x_i*) nur sechs Lösungen, das sind die (mit Multiplizität gerechneten) Nullstellen der sechs Polynome* (2).

Die Sätze 1, 2, 3, 8 und auch Satz 4 lassen sich leicht durch Kongruenzen für den Modul p ausdrücken.

Alle unseren Sätze gestatten wahrscheinlich verschiedene Verallgemeinerungen.

§ 2. Beweis der Sätze 1, 2.

Für ein P-Polynom

$$f(x) = \alpha x^n + \beta x^m + \cdots \qquad (\alpha, \beta \neq 0;\ n > m \geqq 0)$$

nennen wir $n-m$ die *Senkung* von $f(x)$. Offenbar ist die Potenz $f^i(x)$ (für $p \nmid i$) und die Ableitung $f'(x)$ (für $p \nmid n, m$; $m > 0$) von derselben Senkung wie $f(x)$.

Wir beweisen Satz 1. Es ist klar, dass die Polynome (2) in lauter lineare Faktoren zerfallen (in P) und von der Form (1) sind. Nehmen wir umgekehrt an, dass (1) gilt, und dabei $f(x)$ in lauter lineare Faktoren (in P) zerfällt. Wir haben zu beweisen, dass $f(x)$ eins der Polynome (2) ist.

Neben $f(x)$ führen wir das Polynom

$$\bar{f}(x) = x f(x) = x^p + \gamma x^{\frac{p+1}{2}} + \cdots \tag{25}$$

ein und setzen

$$\bar{f}(x) = x^p - x + \varphi(x). \tag{26}$$

Bezeichne n den Grad von $\varphi(x)$. Dann ist nach (25)

$$n \leqq \frac{p+1}{2}. \tag{27}$$

---

[1] Schreiben wir kurz i für Γ_4^i und setzen $\mathfrak{p}^n \| B$, so sehen wir, dass das Maximum $n = \frac{p-1}{2}$ für $B = 0+2-1-3$ und das »zweite» Maximum $n = \frac{p-1}{4}$ für $B = 0+1-2-3$, $0+3-1-2$ eintritt.

[2] Vgl. Fussnote S. 282.

Da in den Fällen $\varphi(x) = 0$, x nach (25) $f(x) = x^p - x$, bzw. x^p ist und diese Polynome unter (2) gehören, so dürfen wir nachher

$$\varphi(x) \neq 0, x \tag{28}$$

annehmen.

Nach der Voraussetzung gilt eine Zerlegung

$$\bar{f}(x) = (x - x_1)^{e_1} \dots (x - x_k)^{e_k}, \tag{29}$$

wobei $x_1, \dots, x_k$ alle verschiedenen Nullstellen von $\bar{f}(x)$ (in P) bezeichnen. Da nach (26) $\bar{f}'(x) = -1 + \varphi'(x)$ ist, so folgt

$$\left| \frac{\bar{f}(x)}{(x - x_1) \dots (x - x_k)} \right| - 1 + \varphi'(x). \tag{30}$$

Die rechte Seite ist nach (28) (wegen $\varphi(0) = 0$) $\neq 0$, und so ergibt (30)

$$p - k \leqq n - 1. \tag{31}$$

Andererseits ist jedes x_i nach (26) eine Nullstelle auch von $\varphi(x)$, woraus

$$(x - x_1) \dots (x - x_k) \mid \varphi(x) \tag{32}$$

folgt. Dies ergibt weiter (wegen (28))

$$k \leqq n. \tag{33}$$

Die drei Ungleichungen (27), (31), (33) haben zur Folgerung

$$n = k = \frac{p+1}{2}, \tag{34}$$

auch muss in ihnen überall »=» gelten. Dann stehen in (30) und (32) beiderseits Polynome von gleichem Grade, und so entsteht nach Multiplizieren

$$a\bar{f}(x) = \varphi(x)(-1 + \varphi'(x))$$

mit irgendeinem Element $a (\neq 0)$ von P. Hieraus erhalten wir nach (26)

$$2ax^p - 2ax + (2a + 2)\varphi(x) = (\varphi^2(x))'. \tag{35}$$

Da $\varphi(x)$ nach (32) und (34) wenigstens zwei verschiedene Nullstellen hat, so enthält es wenigstens zwei nichtverschwindende Glieder. Für solche Polynome haben wir oben die Senkung definiert. Da $\varphi(x)$, $\varphi^2(x)$, $(\varphi^2(x))'$ von gleicher Senkung sind und die linke Seite von (35) nach (34) eine Senkung $\geqq \frac{p-1}{2}$ hat, so gilt das gleiche auch über $\varphi(x)$. Das ergibt nach (25), (26)

$$\varphi(x) = \gamma x^{\frac{p+1}{2}} + \beta x \tag{36}$$

mit einem Element $\beta(\neq 0)$ von P. Setzen wir dies in (35) ein:

$$2\alpha x^p - 2\alpha x + (2\alpha + 2)(\gamma x^{\frac{p+1}{2}} + \beta x) = (\gamma^2 x^{p+1} + 2\beta\gamma x^{\frac{p+3}{2}} + \beta^2 x^2)'.$$

Nach Ausführung der Differenziation ergibt sich durch Koeffizientenvergleichung (wegen $\gamma \neq 0$):

$$2\alpha = \gamma^2, \quad 2\alpha + 2 = 3\beta, \quad -\alpha + \alpha\beta + \beta = \beta^2.$$

Aus der letzten Gleichung folgt $\beta = 1$ oder $\beta = \alpha$. Im ersten Fall ist $(2\alpha = 1)\ \gamma^2 = 1$, im zweiten Fall $(\alpha = 2)\ \gamma^2 = 4$. Immer ist also $\pm\gamma = \beta = 1, 2$, und so haben wir nach (36)

$$\varphi(x) = \pm x^{\frac{p+1}{2}} + x \quad \text{oder} \quad \pm 2x^{\frac{p+1}{2}} + 2x.$$

Dies ergibt nach (25) und (26)

$$f(x) = x^{p-1} \pm x^{\frac{p-1}{2}} \quad \text{oder} \quad x^{p-1} \pm 2x^{\frac{p-1}{2}} + 1.$$

Diese Polynome gehören unter (2), womit wir Satz 1 bewiesen haben.

Für Satz 2 ist zunächst klar, dass die Polynome (4) von der Form (3) sind und in lauter verschiedene lineare Faktoren (in P) zerfallen. Nehmen wir umgekehrt an, dass ein Polynom $g(x)$ von der Form (3) in lauter verschiedene lineare Faktoren (in P) zerfällt. Offenbar sind alle Nullstellen von $g(x)$ $\left(\text{deren Zahl } \frac{p-1}{2} \text{ ist}\right)$ ebenfalls Nullstellen von

$$(g(x) - (x^{\frac{p-1}{2}} - 1))\,(g(x) - (x^{\frac{p-1}{2}} + 1)). \tag{37}$$

Der Grad dieses Produkts ist nach (3) gleich $2n\left(\leqq \frac{p-1}{2}\right)$, und so muss

$$n = \frac{p-1}{4} \qquad (4 \mid p-1) \tag{38}$$

sein, auch kann (37) nur in einem konstanten Faktor von $g(x)$ unterscheiden. Setzen wir zugleich

$$g(x) = x^{\frac{p-1}{2}} + \bar{g}(x) \qquad (g(x) = \gamma x^{\frac{p-1}{4}} + \cdots), \tag{39}$$

so folgt

$$\bar{g}^2(x) - 1 = \gamma^2(x^{\frac{p-1}{2}} + \bar{g}(x)). \tag{40}$$

Die Senkung der rechten Seite ist $\frac{p-1}{4}$, und dann gilt dasselbe über $\bar{g}(x)$. Hieraus folgt nach (39)

$$\bar{g}(x) = \gamma x^{\frac{p-1}{4}} + \alpha \tag{41}$$

mit $\alpha \neq 0$. Setzen wir dies in (40) ein, so bekommen wir durch Koeffizientenvergleichung

$$2\alpha = \gamma^2, \qquad \alpha^2 - 1 = \alpha\gamma^2.$$

Dies ergibt $\alpha^2 + 1 = 0$, $\gamma^2 = (\alpha + 1)^2$, $\gamma = \pm(\alpha + 1)$. Nach (39), (41) ist dann

$$g(x) = (x^{\frac{p-1}{4}} \pm 1)(x^{\frac{p-1}{4}} \pm \alpha).$$

Da $\alpha = \pm\sigma$ (mit $\sigma^2 = -1$) ist, so ist $g(x)$ von der Form (4), womit wir Satz 2 bewiesen haben.

§ 3. Beweis des Satzes 3.

Dem Beweis von Satz 3 schicken wir folgende Bemerkung voran. Addieren wir zu den Gliedern des Systems (5) ein (von i unabhängiges) lineares Polynom $l(x)$, so behält die Anzahl N auch für dieses neue System

$$l_i(x) + l(x) \qquad \left(i = 0, \pm 1, \ldots, \pm\frac{p-1}{2}\right)$$

ihren Wert. Nehmen wir insbesondere $l(x) = -l_0(x)$, so sehen wir, dass man sich im Satz 3 auf den Fall

$$l_0(x) = 0 \tag{42}$$

beschränken darf.

Vorläufig wollen wir nur beweisen, dass die Annahme (6) die Gleichungen (7) zur Folgerung hat. Die übrigen Behauptungen des Satzes werden sich dann leicht beweisen lassen. Setzen wir für die von $l_0(x)$ $(= 0)$ verschiedenen Glieder von (5):

$$l_i(x) = \alpha_i x + \beta_i \qquad \left(i = \pm 1, \ldots, \pm\frac{p-1}{2}\right). \tag{43}$$

Aus der Annahme folgt, dass dieses System an wenigstens $\frac{p-1}{2}$ Stellen x in alle Elemente $(\neq 0)$ von P übergeht.

Wir werden wiederholt den Kunstgriff anwenden, dass wir x durch $x + y$ ersetzen, wobei y ein beliebiges Element von P ist, und dann gilt das eben gesagte auch für

$$l_i(x+y) = \alpha_i x + (\alpha_i y + \beta_i) \qquad \left(i = \pm 1, \ldots, \pm \frac{p-1}{2}\right) \tag{44}$$

statt (43). Hieraus schliessen wir zunächst so, dass wir ein geeignetes $y = y_0$ wählen, wofür

$$\beta_i' = \alpha_i y_0 + \beta_i \qquad \left(i = \pm 1, \ldots, \pm \frac{p-1}{2}\right) \tag{45}$$

alle verschiedenen Elemente $(\neq 0)$ von P sind — ein solches y_0 gibt es nach dem über (43) gesagten — wir setzen (45) in (44) ein, dann geht

$$\alpha_i x + \beta_i' \qquad \left(i = \pm 1, \ldots, \pm \frac{p-1}{2}\right) \tag{46}$$

an wenigstens $\frac{p-3}{2}$ Stellen $x(\neq 0)$ in alle Elemente $(\neq 0)$ von P über. Dasselbe gilt auch für

$$\beta_i' x + \alpha_i \qquad \left(i = \pm 1, \ldots, \pm \frac{p-1}{2}\right) \tag{47}$$

statt (46). (Das sieht man so ein, dass man (46) durch x dividiert, was offenbar gestattet ist, und nachher $\frac{1}{x}$ durch x ersetzt.) Nach dem obigen Kunstgriff (mit $\frac{p-3}{2}$ statt $\frac{p-1}{2}$) nimmt das System

$$\beta_i' x + (\beta_i' y + \alpha_i) \qquad \left(i = \pm 1, \ldots, \pm \frac{p-1}{2}\right)$$

für jedes y in P an wenigstens $\frac{p-3}{2}$ Stellen x alle verschiedenen Elemente $(\neq 0)$ von P an. Das ist äquivalent damit, dass das Gleichungssystem

$$\sum_i (\beta_i' x + (\beta_i' y + \alpha_i))^k = \begin{cases} 0 & (k = 1, \ldots, p-2), \\ -1 & (k = p-1) \end{cases} \tag{48}$$

für jedes y in P wenigstens $\frac{p-3}{2}$ Lösungen x in P hat.[1] Für $k \leqq \frac{p-3}{2}$ ist aber der Grad von (48) (für x) kleiner als $\frac{p-3}{2}$, insbesondere für $k = \frac{p-3}{2}$ deshalb, da wegen (45)

$$\sum_i \beta_i^{\frac{p-3}{2}} = 0$$

[1] $\sum_i$ (später $\prod_i$) bezeichnet die Summe (das Produkt) über $i = \pm 1, \ldots, \pm \frac{p-1}{2}$. — Zu (48) ist zu bemerken, dass sich nach den Newtonschen Formeln die elementarsymmetrischen Funktionen von den Elementen $x_1, \ldots, x_n$ $(n < p)$ in P und die Potenzsummen $x_1^k + \cdots + x_n^k$ $(k = 1, \ldots, n)$ einander gegenseitig bestimmen. (Hiervon ist eine Folgerung die Äquivalenz der Sätze 1, 8). Sind weiter die $x_1, \ldots, x_n$ $(n = p-1)$ alle verschiedenen Elemente $(\neq 0)$ von P, so ist diese Potenzsumme $0 (k < p-1)$, bzw. $-1 (k = p-1)$.

gilt. Also verschwindet die linke Seite von (48) für $k \leqq \frac{p-3}{2}$ bei jedem y in P (und unbestimmtem x) identisch. Insbesondere folgt für das konstante Glied

$$\sum_i (\beta_i' y + \alpha_i)^k = 0 \qquad \left(k = 1, \ldots, \frac{p-3}{2}\right)$$

mit jedem y in P. Dies ist äquivalent mit dem Verschwinden der ersten $\frac{p-3}{2}$ elementarsymmetrischen Funktionen der $\beta_i' y + \alpha_i$, d. h. der Koeffizienten von $x^{p-1}, \ldots, x^{\frac{p+1}{2}}$ im Polynom

$$\prod_i (x - (\beta_i' y + \alpha_i)) = x^{p-1} + \cdots.$$

Da dies in lauter lineare Faktoren in P zerfällt, so folgt aus Satz 1 das Bestehen einer Gleichung

$$\prod_i (x - (\beta_i' y + \alpha_i)) = x^{\frac{p-1}{2} t} (x^{\frac{p-1}{2}} - 1)^u (x^{\frac{p-1}{2}} + 1)^v \quad (t + u + v = 2) \tag{49}$$

für jedes y in P. Wir unterscheiden folgende zwei Fälle:

1) Zuerst betrachten wir den Fall, in dem alle $\frac{\alpha_i}{\beta_i'}$ gleich sind (wegen (45) sind die β_i' von 0 verschieden). Dann gibt es ein y_1 in P mit

$$\alpha_i = \beta_i' y_1 \qquad \left(i = \pm 1, \ldots, \pm \frac{p-1}{2}\right). \tag{50}$$

Andererseits können wir nach (45) den $l_i(x)$ eine solche Reihenfolge geben, dass

$$\beta_i' = i^2 \alpha, \qquad \beta_{-i}' = i^2 \beta \qquad \left(i = 1, \ldots, \frac{p-1}{2}\right) \tag{51}$$

gilt (hierzu sind irgendzwei Elemente α, β in P mit $\chi(\alpha) = -\chi(\beta)$ geeignet). Aus (50) und (51) folgt noch

$$\alpha_i = i^2 \alpha y_1, \qquad \alpha_{-i} = i^2 \beta y_1 \qquad \left(i = 1, \ldots, \frac{p-1}{2}\right). \tag{52}$$

2) Im anderen Fall kommen unter den $\frac{\alpha_i}{\beta_i'}$ wenigstens zwei verschiedene Werte vor, die wir in der Form $-y_2$, $-y_3$ annehmen. Das hat zur Folgerung, dass in beiden Systemen

$$\left.\begin{aligned} &\beta_i' y_2 + \alpha_i \\ &\beta_i' y_3 + \alpha_i \end{aligned}\right\} \qquad \left(i = \pm 1, \ldots, \frac{p-1}{2}\right) \tag{53, 54}$$

die 0 vorkommt, und beide haben auch ein von 0 verschiedenes Element. Aus (49) folgt, dass es in beiden Systemen (53), (54) genau $\frac{p-1}{2}$ von 0 verschiedene Elemente gibt, und diese eben die Nullstellen von dem einen der Polynome $x^{\frac{p-1}{2}} \pm 1$ sind, wobei für beide Systeme jedes Vorzeichen möglich ist. Dabei lassen sich die Nullstellen von jedem dieser Polynome durch $i^2\alpha \left(i = 1, \ldots, \frac{p-1}{2}\right)$ angeben mit einem $\alpha (\neq 0)$ in P. Zunächst für (53) gilt dann bei passender Reihenfolge der $l_i(x)$:

$$\left.\begin{aligned} \beta'_i y_2 + \alpha_i &= i^2\alpha \quad (55)\\ \beta'_{-i} y_2 + \alpha_{-i} &= 0 \quad (56)\end{aligned}\right\} \qquad \left(i = 1, \ldots, \frac{p-1}{2}\right).$$

(Mit der Reihenfolge der $l_{-i}(x)\left(i = 1, \ldots, \frac{p-1}{2}\right)$ werden wir noch frei verfügen können.) Nach (55), (56) geht (54) in

$$\left.\begin{aligned} \beta'_i (y_3 - y_2) + i^2\alpha \quad (57)\\ \beta'_{-i}(y_3 - y_2) \quad (58)\end{aligned}\right\} \qquad \left(i = 1, \ldots, \frac{p-1}{2}\right)$$

über. Da (58) aus lauter von 0 verschiedenen Elementen besteht, muss nach obiger Bemerkung bei passender Reihenfolge der $l_{-i}(x)$ $\left(i = 1, \ldots, \frac{p-1}{2}\right)$

$$\left.\begin{aligned} \beta'_i (y_3 - y_2) + i^2\alpha &= 0 \quad (59)\\ \beta'_{-i}(y_3 - y_2) &= i^2\beta \quad (60)\end{aligned}\right\} \qquad \left(i = 1, \ldots, \frac{p-1}{2}\right)$$

gelten, wobei $\beta (\neq 0)$ ein Element in P ist. Aus (53), (54), (59), (60) folgt mit der Bezeichnung $y_4 = \frac{1}{y_3 - y_2}$

$$\beta'_i = -i^2\alpha y_4, \quad \alpha'_i = i^2\alpha y_2 y_4; \quad \beta'_{-i} = i^2\beta y_4, \quad \alpha'_{-i} = -i^2\alpha y_3 y_4 \quad \left(i = 1, \ldots, \frac{p-1}{2}\right).$$

Nach diesen Gleichungen und nach (51), (52) haben wir in beiden Fällen 1), 2) Zusammenhänge von der Form

$$\alpha_i = i^2\bar{\alpha}, \quad \beta'_i = i^2\bar{\beta}; \quad \alpha_{-i} = i^2\bar{\gamma}, \quad \beta'_{-i} = i^2\bar{\delta} \qquad \left(i = 1, \ldots, \frac{p-1}{2}\right) \tag{61}$$

mit festen Elementen $\bar{\alpha}, \bar{\beta}, \bar{\gamma}, \bar{\delta}$ in P. Da endlich nach (45) $\beta_i = \beta'_i - \alpha_i y_0$ ist, woraus nach (43) $l_i(x) = \alpha_i x + (\beta'_i - \alpha_i y_0)$ folgt, so gelten nach (61) in der Tat Gleichungen von der Form (7), womit wir den ersten Teil des Beweises beendet haben.

Den noch übriggebliebenen Teil des Satzes erledigen wir so, dass wir die $\alpha, \beta, \gamma, \delta$ bestimmen, für die (6) gilt, und zugleich berechnen wir auch den genauen Wert von N. Offenbar ist nach (7) $N=0$, wenn $\alpha=\beta=0$ oder $\gamma=\delta=0$ ist, und so schliessen wir diese Fälle gleich aus.

Das System (7) geht für ein x in P dann und nur dann in alle verschiedenen Elemente von P über, wenn $\chi(\alpha x+\beta)\chi(\gamma x+\delta)=-1$ ist. Hieraus folgt

$$N=\frac{1}{2}\sum_x{}'\left(1-\chi((\alpha x+\beta)(\gamma x+\delta))\right), \tag{62}$$

wobei man über die x in P mit Ausnahme von

$$(\alpha x+\beta)(\gamma x+\delta)=0 \tag{63}$$

zu summieren hat. Bezeichnet N_0 die Anzahl der Lösungen von (63), so folgt aus (62)

$$N=\frac{1}{2}\left(p-N_0-\sum_x\chi((\alpha x+\beta)(\gamma x+\delta))\right). \tag{64}$$

Sind λ, μ, ν beliebige Elemente in P mit $\Delta=\mu^2-4\lambda\nu$, so gilt nach Jacobsthal[1]

$$\sum_x\chi(\lambda x^2+\mu x+\nu)=\begin{cases}-\chi(\lambda) & (\lambda, \Delta\neq 0),\\ (p-1)\chi(\lambda) & (\lambda\neq 0;\ \Delta=0),\\ 0 & (\lambda=0;\ \mu\neq 0),\\ p\chi(\nu) & (\lambda=\mu=0).\end{cases}$$

Setzen wir hier $\lambda=\alpha\gamma$, $\mu=\alpha\delta+\beta\gamma$, $\nu=\beta\delta$ $(\Delta=(\alpha\delta-\beta\gamma)^2)$ ein, so bekommen wir

$$\sum_x\chi((\alpha x+\beta)(\gamma x+\delta))=\begin{cases}-\chi(\alpha\gamma) & (\alpha\gamma\neq 0;\ \alpha\delta-\beta\gamma\neq 0),\\ (p-1)\chi(\alpha\gamma) & (\alpha\gamma\neq 0;\ \alpha\delta-\beta\gamma=0),\\ 0 & (\alpha\gamma=0;\ \alpha\delta+\beta\gamma\neq 0),\\ p\chi(\beta\delta) & (\alpha\gamma=0;\ \alpha\delta+\beta\gamma=0).\end{cases}$$

Entsprechend ist $N_0=2, 1, 1, 0$, also nach (64) bzw.

$$N=\frac{1}{2}(p-2+\chi(\alpha\gamma)),\quad \frac{p-1}{2}(1-\chi(\alpha\gamma)),\quad \frac{p-1}{2},\quad \frac{p}{2}(1-\chi(\beta\delta)).$$

---

[1] E. JACOBSTHAL, Anwendungen einer Formel aus der Theorie der Quadratischen Reste, Dissertation Berlin 1906, S. 290. Im Grunde handelt es sich um die Formel

$$S_c=\sum_{x=0}^{p-1}\left(\frac{x^2+c}{p}\right)=\begin{cases}-1 & (p\nmid c),\\ p-1 & (p\mid c).\end{cases}$$

Ein einfacher Beweis entsteht so. Wegen $\left(\frac{x^2+c}{p}\right)\equiv(x^2+c)^{\frac{p-1}{2}} \pmod p$ bekommt man leicht $S_c\equiv -1 \pmod p$. Andererseits ist $|S_c|\leqq p$, und $2\nmid S_c (p\nmid c)$, bzw. $2\mid S_c (p\mid c)$.

Im ersten, zweiten und vierten Fall findet (6) bzw. für und nur für $\chi(\alpha\gamma)=1$, $\chi(\alpha\gamma)=-1$, $\chi(\beta\delta)=-1$ statt, und so sind alle Fälle mit erfülltem (6):

$$N=\begin{cases}\frac{1}{2}(p-1) & (\chi(\alpha\gamma)=1;\ \alpha\delta-\beta\gamma\neq 0),\\ p-1 & (\chi(\alpha\gamma)=-1;\ \alpha\delta-\beta\gamma=0),\\ \frac{1}{2}(p-1) & (\alpha\gamma=0;\ \alpha\delta+\beta\gamma\neq 0),\\ p & (\alpha\gamma=0;\ \chi(\beta\delta)=-1;\ \alpha\delta+\beta\gamma=0).\end{cases}$$

Der erste und dritte Fall ergeben zusammen eben Fall 1) im Satz 3, der zweite und vierte geht bzw. in Fall 2) und 3) über, und so haben wir Satz 3 bewiesen.

§ 4. Beweis des Satzes 4.

Im Fall $p=2$ ist Satz 4 trivial, deshalb nehmen wir $p\geqq 3$ an. Wählen wir zwei Basiselemente A, B von $\mathfrak{G}$. Dann lässt sich

$$\mathfrak{H}=\sum_{i=0}^{p-1}A^{\alpha_i}B^{\beta_i} \tag{65}$$

$$\mathfrak{K}=\sum_{i=0}^{p-1}A^{\gamma_i}B^{\delta_i} \tag{66}$$

annehmen (hier bezeichnet Σ nicht die Summe sondern die Vereinigungsmenge), wobei wir für die Exponenten wieder Elemente des Restklassenkörpers P genommen haben. Die Gleichung (12) dürfen wir in der Form

$$(E+A+\cdots+A^{p-1})(E+B+\cdots+B^{p-1})=\sum_{i=0}^{p-1}A^{\alpha_i}B^{\beta_i}\sum_{i=0}^{p-1}A^{\gamma_i}B^{\delta_i}$$

schreiben. Ersetzen wir A, B bzw. durch ϱ^x, ϱ, wobei x ein beliebiges Element von P ist. Dann entsteht eine richtige Gleichung (wobei Σ wieder das gewöhnliche Summenzeichen ist). Da der zweite Faktor links verschwindet (für $x=0$ verschwindet nur der zweite Faktor), so folgt

$$\sum_{i=0}^{p-1}\varrho^{\alpha_i x+\beta_i}\cdot\sum_{i=0}^{p-1}\varrho^{\gamma_i x+\delta_i}=0.$$

Da x insgesamt p Werte fähig ist, so gibt es $\frac{p+1}{2}$ Werte von x, für die z. B. der erste Faktor verschwindet, d. h.

$$\alpha_i x+\beta_i \qquad (i=0,\ldots,p-1) \tag{67}$$

in alle verschiedenen Elemente von P übergeht. Mit Anwendung von Satz 3 auf dieses System (67) folgt, da jetzt $N \geqq \frac{p+1}{2}$ ist, dass es (abgesehen von der Reihenfolge) einem System

$$l_0(x),\ l_0(x) + i^2(\alpha x + \beta),\ l_0(x) + i^2(\gamma x + \delta) \quad \left(i = 1, \ldots, \frac{p-1}{2}\right) \tag{68}$$

gleich ist mit $l_0(x) = \alpha_0 x + \beta_0$, und für die $\alpha, \beta, \gamma, \delta$ muss dabei Fall 2) oder 3) von Satz 3 vorliegen. Hier sind die Koeffizienten von x und die konstanten Glieder die Exponenten von A bzw. B in (65), und so besteht $\mathfrak{H}$ aus den Elementen

$$A^{\alpha_0} B^{\beta_0},\quad A^{\alpha_0 + i^2\alpha} B^{\beta_0 + i^2\beta},\quad A^{\alpha_0 + i^2\gamma} B^{\beta_0 + i^2\delta} \quad \left(i = 1, \ldots, \frac{p-1}{2}\right),$$

d. h. $A^{-\alpha_0} B^{-\beta_0} \mathfrak{H}$ besteht aus den Elementen

$$E, (A^{\alpha} B^{\beta})^{i^2},\qquad (A^{\gamma} B^{\delta})^{i^2} \qquad \left(i = 1, \ldots, \frac{p-1}{2}\right). \tag{69}$$

Im Fall 2) gilt $\beta = \alpha\varkappa$, $\delta = \alpha\gamma$ mit einem $\varkappa$ in P, und dabei ist $\chi(\alpha\gamma) = -1$. Dann schreibt sich (69) so

$$E, (A B^{\varkappa})^{i^2\alpha},\quad (A B^{\varkappa})^{i^2\gamma} \qquad \left(i = 1, \ldots, \frac{p-1}{2}\right).$$

Die $i^2\alpha$, $i^2\gamma$ durchlaufen alle Elemente ($\neq 0$) von P, und so ist dieser Komplex nichts anderes als die durch $A B^{\varkappa}$ erzeugte Gruppe.

Im Fall 3) ist $\alpha = \gamma = 0$, $\chi(\beta\delta) = -1$, und dann ist (69) die durch B erzeugte Gruppe.

In beiden Fällen ist $\mathfrak{H}$ eine Nebengruppe einer Untergruppe von $\mathfrak{G}$. Da aber $E \in \mathfrak{H}$ ist, muss $\mathfrak{H}$ eine Untergruppe von $\mathfrak{G}$ sein, Satz 4 ist richtig.

§ 5. Beweis der Sätze 5, 6, 7.

Wir schicken voran den:

Hilfssatz. *Es sei $p \geqq 3$ und*

$$\mathrm{P} = \sum_{i=1}^{r} \varrho^{x_i} \qquad (r > 0) \tag{70}$$

eine beliebige ganze Zahl des Kreiskörpers K,[1] *wobei wir die Exponenten x_i als Elemente des Restklassenkörpers P annehmen. Dann und nur dann gilt*

$$(\varrho - 1)^n \mid \mathrm{P} \qquad (0 < n < p), \tag{71}$$

[1] Ist nämlich $\mathrm{P} = a_0 + a_1\varrho + \cdots + a_{p-2}\varrho^{p-2}$ mit ganzen rationalen a_i, so addiere man $1 + \varrho + \cdots + \varrho^{p-1}$ so oft, bis nur nichtnegative Koeffizienten auftreten. Dann gilt (70).

wenn

$$p \mid r \tag{72}$$

und

$$f(x) = (x - x_1) \dots (x - x_r) = x^r + \gamma x^{r-n} + \cdots \tag{73}$$

ist, welches letztere bedeutet, dass $f(x)$ eine Senkung $\geqq r$ hat (oder $f(x) = x^r$ ist). Offenbar sind die zwei Bedingungen (72), (73) äquivalent jedem der folgenden Gleichungssysteme

$$\sum_{i=1}^{r} x_i^k = 0 \qquad (k = 0, \dots, n-1), \tag{74}$$

$$\sum_{i=1}^{r} \binom{x_i}{k} = 0 \qquad (k = 0, \dots, n-1). \tag{75}$$

Den Beweis dieses Hilfssatzes führen wir in seiner dritten (mit (75) ausgedrückten) Form aus, weiter nehmen wir hierzu die Exponenten x_i als positive ganze Zahlen an, was offenbar gestattet ist, aber dann tritt für (75) die Kongruenz

$$\sum_{i=1}^{r} \binom{x_i}{k} \equiv 0 \pmod{p} \qquad (k = 0, \dots, n-1) \tag{76}$$

ein. Im Fall $n = 1$ ist der Hilfssatz richtig, da dann sowohl (71) als auch (76) dasselbe ist wie $p \mid r$. Im übrigen Fall $n \geqq 2$ nehmen wir die Richtigkeit des Hilfssatzes für $n - 1$ (statt n) an. Dann und nur dann gilt (71), wenn $\varrho - 1 \mid \mathrm{P}$ und $(\varrho - 1)^{n-1} \left| \frac{1}{\varrho - 1} \mathrm{P} \right.$ ist. Von diesen Bedingungen ist die erste — wie wir schon bemerkt haben — nichts anderes als $p \mid r$, und deshalb lässt sich die zweite wegen $n < p$ durch $(\varrho - 1)^{n-1} \left| \frac{1}{\varrho - 1} (\mathrm{P} - r) \right.$ ersetzen. Die rechte Seite ist wegen (70)

$$\sum_{i=1}^{r} \sum_{j=0}^{x_i - 1} \varrho^j.$$

Nach der Induktionsannahme ist also die notwendige und hinreichende Bedingung von (71):

$$p \mid r, \ \sum_{i=1}^{r} \sum_{j=0}^{x_i - 1} \binom{j}{k} \equiv 0 \pmod{p} \qquad (k = 0, \dots, n-2).$$

Die innere Summe ist $\binom{x_i}{k+1}$, womit wir den Hilfssatz bewiesen haben.

Zum Beweis von Satz 5 nehmen wir an, dass für (20) $\mathfrak{p}^{\frac{p-1}{2}} \mid A$ gilt. Hieraus folgt nach dem Hilfssatz für die Exponenten x_i in (20):

$$(x - x_1) \cdots (x - x_p) = x^p + \gamma x^{\frac{p+1}{2}} + \cdots$$

mit einem γ in P. Wegen $x_1 = 0$ lässt sich hierfür

$$(x - x_2) \cdots (x - x_p) = x^{p-1} + \gamma x^{\frac{p-1}{2}} + \cdots$$

schreiben. Hieraus folgt nach Satz 1, dass die linke Seite eins der Polynome (2) sein muss. Entsprechend entstehen eben die im Satz 5 genannten sechs Fälle für A, und so ist die Richtigkeit dieses Satzes klar.

Satz 6 brauchen wir nur für den Fall zu beweisen, wo $2 \mid r$ und es in (19) gleichviel »+» und »—» Zeichen gibt.[1] Addieren wir dann $1 + \varrho + \cdots + \varrho^{p-1}\ (= 0)$ zu B_r, so geht B_r, wie schon bemerkt wurde,[2] in ein A über, das wir wieder in der Form (20) annehmen. Dabei gibt es jetzt unter den Exponenten x_i genau $p - \frac{r}{2}$ verschiedene. Diese sind Nullstellen von

$$f(x) = (x - x_1) \cdots (x - x_p) = x^p + \cdots \tag{77}$$

also auch von

$$f(x) - x^p + x.$$

Folglich ist dieses Polynom mindestens vom Grade $p - \frac{r}{2}$, und so hat $f(x)$ eine Senkung $\leqq \frac{r}{2}$. Hieraus folgt nach dem Hilfssatz die Richtigkeit des Satzes 6.

Zum Beweis von Satz 7 nehmen wir $\mathfrak{p}^{\frac{p-1}{4}} \mid B$ an, woraus folgt,[1] dass es in (18) gleichviel »+» und »—» Zeichen gibt. Wieder addieren wir $1 + \varrho + \cdots + \varrho^{p-1}$ zu B, dann erscheint es als ein A in (20). Wir gebrauchen auch jetzt die Bezeichnung (77). Offenbar hat dann $f(x)$ ausser $x_1 = 0$ lauter zweifache Nullstellen, und so gilt eine Gleichung

$$f(x) = x g^2(x), \tag{78}$$

wobei $g(x)$ in lauter verschiedene lineare Faktoren (in P) zerfällt. Wegen (18) ist $g(0) \neq 0$, $g(1) = 0$. Aus letzterem folgt $g(x) \neq x^{\frac{p-1}{2}} + 1$, da weiter im Satz 7 der Fall $B = \Gamma$ ausgeschlossen wurde, so folgt auch $g(x) \neq x^{\frac{p-1}{2}} - 1$. Wegen der Annahme folgt aus dem Hilfssatz, dass $f(x)$ eine Senkung $\geqq \frac{p-1}{4}$ hat. Dasselbe

[1] Siehe Fussnote 4, S. 277.

[2] Siehe Fussnote 2, S. 277.

gilt nach (77) über $g(x)$, und so folgt aus Satz 2, dass $4 \mid p-1$ und $g(x)$ eins der Polynome (4) ist. Wegen $g(1) = 0$ kommt dabei nur $t = 1\,(u = 0)$ in Betracht, also ist

$$g(x) = (x^{\frac{p-1}{4}} - 1)(x^{\frac{p-1}{4}} \pm \sigma).$$

Hieraus folgt, dass B in (23) gehört. Für diese B gilt bekanntlich $\mathfrak{p}^{\frac{p-1}{4}} \| B$, womit wir Satz 7 bewiesen haben.