Zur Approximation algebraischer Zahlen. I.

(Über den größten Primteiler binärer Formen.)

Von

Kurt Mahler in Göttingen.

Im Jahre 1908 zeigte Thue (1, 2) folgenden Satz: „*Ist ζ eine reelle algebraische Zahl n-ten Grades, Θ eine positive Zahl, so gibt es nur endlichviele verschiedene gekürzte rationale Zahlen p/q, die der Ungleichung*

$$\frac{p}{q} - \zeta \leqq q^{-\left(\frac{n}{2}+1+\Theta\right)}$$

genügen.“

Dieser Satz wurde 1920 von Siegel (3, 4, 5) verschärft; *er zeigte, daß man den Exponenten $n/2 + 1 + \Theta$ ersetzen darf durch*

$$\beta = \min_{s=1,2,\ldots,n-1} \left(\frac{n}{s+1} + s + \Theta\right);$$

ferner stellte er einen allgemeineren Satz auf über die Annäherung einer festen algebraischen Zahl durch algebraische Zahlen niedrigeren Grades.

In der vorliegenden Arbeit untersuche ich nur die Annäherung durch rationale Zahlen; jedoch wird die gleichzeitige Approximation reeller und P-adischer Wurzeln derselben algebraischen Gleichung untersucht. Das Hauptergebnis lautet folgendermaßen:

„*Bedeute $f(x)$ ein irreduzibles Polynom mit ganzen rationalen Koeffizienten vom Grad $n \geqq 3$, $P_1, P_2, \ldots, P_t$ endlichviele verschiedene Primzahlen, $\zeta, \zeta_1, \zeta_2, \ldots, \zeta_t$ je eine reelle, eine P_1-adische, eine P_2-adische, usw., eine P_t-adische Nullstelle von $f(x)$. Der gewöhnliche Absolutbetrag werde durch zwei senkrechte Striche, der P_τ-adische Wert durch zwei solche Striche mit dem Index P_τ bezeichnet. Es sei β der Siegelsche Exponent und $k \geqq 1$ eine feste Zahl. Dann besitzt die Ungleichung*

$$\min\left(1, \left|\frac{p}{q} - \zeta\right|\right) \prod_{\tau=1}^{t} \min\left(1, |p - q\zeta_\tau|_{P_\tau}\right) \leqq k \max\left(|p|, |q|\right)^{-\beta}$$

höchstens endlichviele Lösungen in gekürzten rationalen Zahlen p/q.“

Mit diesem Satz ist der folgende fast gleichwertig:

„*Bedeute $F(x, y)$ eine irreduzible Binärform mit ganzen rationalen Koeffizienten vom Grad $n \geqq 3$, p und q zwei teilerfremde ganze rationale Zahlen,*

$P_1, P_2, \ldots, P_t$ endlichviele verschiedene Primzahlen, $Q(p, q)$ das größte Potenzprodukt derselben, das in $F(p, q)$ aufgeht. Die Ungleichung

$$\frac{|F(p, q)|}{Q(p, q)} \leqq k \max(|p|, |q|)^{n-\beta}$$

besitzt dann höchstens endlichviele Lösungspaare p, q.“

Dieser verallgemeinerte Thuesche Satz wird benutzt, um zu zeigen, *daß der größte Primteiler binärer Formen von mindestens drittem Grad mit ganzen rationalen Koeffizienten, die im Körper der komplexen Zahlen mindestens drei verschiedene Linearformen als Teiler haben*[1]*, über alle Grenzen wächst, wenn für die Argumente zwei teilerfremde*[1] *ganze rationale Zahlen p, q mit* $\max(|p|, |q|) \to \infty$ *eingesetzt werden.*

Der Beweis dieser Sätze besteht in einer Übertragung des Siegelschen Beweises in der Arbeit (5) auf P-adische Körper. Man kann fast alle Überlegungen auch hier durchführen, da diese Körper bewertet sind. In der vorliegenden Arbeit gelingt es, durch einen einfachen Kunstgriff die Beweisführung möglichst lange im Bereiche der rationalen Zahlen zu belassen. Ermöglicht wird der Beweis durch die Ungleichung

$$|a| \prod_{\tau=1}^{t} |a|_{P_\tau} \geqq 1,$$

die für ganze rationale Zahlen ungleich Null gilt.

Eine weitere Arbeit wird Abschätzungen für die Lösungsanzahlen der hier betrachteten Ungleichungen gewidmet sein. Offenbar kann man alle Schlüsse und Sätze auch auf die Approximation algebraischer Zahlen durch algebraische Zahlen niederen Grades übertragen, indem man sich an die Arbeit (3) von Siegel hält.

Herrn Prof. Siegel möchte ich an dieser Stelle für eine Reihe von Verbesserungsvorschlägen danken. Mein Dank gilt ferner der Notgemeinschaft der Deutschen Wissenschaft für ihre Unterstützung.

Literaturverzeichnis.

A. Thue: (1) Om en general i store hele tal uløsbar ligning, Skrifter udgivne af Videnskabs-Selskabet i Cristiania (1908).

(2) Über Annäherungswerte algebraischer Zahlen, Journal für die reine und angewandte Mathematik **135** (1909), S. 284–305.

C. Siegel: (3) Approximation algebraischer Zahlen, Math. Zeitschr. **10** (1921), S. 173–213.

(4) Über Näherungswerte algebraischer Zahlen, Math. Annalen **84** (1921), S. 80–99.

(5) Über den Thueschen Satz, Videnskapsselskapets-Skrifter (1921), Mat. Naturv. Klasse Nr. 16.

K. Hensel: (6) Theorie der algebraischen Zahlen (1908), Leipzig, B. G. Teubner.

G. Pólya: (7) Zur arithmetischen Untersuchung der Polynome, Math. Zeitschr. **1** (1918), S. 143.

[1]) Ohne diese Einschränkung ist der Satz falsch.

Bezeichnungen:

$\overline{|F(x, y, \ldots)|}$ bedeutet das Maximum der Absolutbeträge der Koeffizienten des Polynoms $F(x, y, \ldots)$.

$|\alpha|$ bedeutet den gewöhnlichen Absolutbetrag.

$|\alpha|_P$ bedeutet den P-adischen Wert einer P-adischen Zahl.

$f(x)$ ist gewöhnlich ein irreduzibles Polynom mit ganzen rationalen Koeffizienten vom Grad $n \geqq 3$ und mit $\overline{|f(x)|} = a$. Eine reelle Nullstelle hiervon wird mit ζ, eine P_τ-adische Nullstelle mit ζ_τ bezeichnet; verschiedene gleichartige Nullstellen werden durch obere Indizes unterschieden.

$P_1, P_2, \ldots, P_t$ sind gewöhnlich endlichviele verschiedene Primzahlen.

p, q sind gewöhnlich zwei ganze rationale teilerfremde Zahlen; es wird zur Abkürzung $|p, q| = \max(|p|, |q|)$ geschrieben.

I.

1. Hilfssatz 1. *Zu zwei Polynomen mit ganzen rationalen Koeffizienten vom Grad n bzw. N:*

$$f(x) = \sum_{h=0}^{n} a_h x^{n-h}, \quad F(x) = \sum_{h=0}^{N} A_h x^{N-h}$$

gibt es zwei Polynome $F_0(x)$ und $F^*(x)$ mit ganzen rationalen Koeffizienten höchstens vom Grad $N-n$ bzw. $n-1$, so daß

$$a_0^d F(x) = f(x) F_0(x) + F^*(x) \quad (d = \max(0, N-n+1))$$

ist und folgende Ungleichungen bestehen:

$$\overline{|F_0(x)|} \leqq \overline{|F(x)|}\,(2\,\overline{|f(x)|})^d \quad \text{und} \quad \overline{|F^*(x)|} \leqq \overline{|F(x)|}\,(2\,\overline{|f(x)|})^d.$$

Beweis. Die Identität

$$1 \cdot F(x) = f(x) \cdot 0 + F(x)$$

zeigt, daß die Behauptung für $N \leqq n-1$ stimmt. Sie sei bereits für alle Polynome $F(x)$ vom Grad $N \leqq n+k-1$ nachgewiesen, wobei k eine nichtnegative ganze rationale Zahl bedeutet. Hat dann $F(x)$ den Grad $N = n+k$, so genügt offenbar das Polynom

$$\overline{F}(x) = a_0 F(x) - A_0 x^{N-n} f(x)$$

der Ungleichung

$$\overline{|\overline{F}(x)|} \leqq \overline{|F(x)|} \cdot (2\,\overline{|f(x)|})$$

und ist höchstens vom Grad $N-1 = n+k-1$. Also gibt es nach Annahme zwei Polynome $\overline{F}_0(x)$ und $\overline{F}^*(x)$ mit ganzen rationalen Koeffizienten höchstens vom Grad $N-n-1$ bzw. $n-1$, so daß

$$a_0^{\bar{d}}\,\overline{F}(x) = f(x)\,\overline{F}_0(x) + \overline{F}^*(x) \qquad (\bar{d} = \max(0, N-n) = d-1)$$

und

$$\overline{|\overline{F}_0(x)|} \leqq \overline{|\overline{F}(x)|}\,(2\,\overline{|f(x)|})^{\bar{d}}, \quad \overline{|\overline{F}^*(x)|} \leqq \overline{|\overline{F}(x)|}\,(2\,\overline{|f(x)|})^{\bar{d}}$$

ist. Setzt man

$$F_0(x) = a_0^{d-1} A_0 x^{N-n} + \overline{F}_0(x), \quad F^*(x) = \overline{F}^*(x),$$

so wird jetzt in der Tat

$$a_0^d F(x) = f(x) F_0(x) + F^*(x)$$

und die zu beweisenden Ungleichungen

$$\overline{|F_0(x)|} \leqq \overline{|F(x)|}\ (2\overline{|f(x)|})^d, \qquad \overline{|F^*(x)|} \leqq \overline{|F(x)|}\ (2\overline{|f(x)|})^d$$

sind erfüllt[2]).

2. Von jetzt ab bedeutet

$$f(x) = \sum_{h=0}^{n} a_h x^{n-h} \qquad (a = \overline{|f(x)|} \geqq 1)$$

eine Polynom mit ganzen rationalen Koeffizienten mindestens vom dritten Grad, das im Körper der rationalen Zahlen irreduzibel ist.

Seien r und s zwei natürliche Zahlen, von denen die erste groß, die zweite aber kleiner als n ist; ϑ bedeute eine feste positive Zahl, m diejenige natürliche Zahl, die der Ungleichung

$$m \leqq \left(\frac{n+\vartheta}{s+1} - 1\right) r < m+1$$

genügt. Zu jeder natürlichen Zahl A gibt es genau

$$N = (2A+1)^{(m+r+1)(s+1)}$$

Polynome

$$P(x, y) = \sum_{h=0}^{m+r} \sum_{k=0}^{s} A_{hk} x^h y^k$$

vom Grad $m+r$ in x, s in y mit ganzen rationalen Koeffizienten, die nur der Ungleichung

$$\overline{|P(x, y)|} \leqq A$$

genügen. Wird gesetzt

$$P_l(x, y) = \frac{1}{l!} \frac{\partial^l P(x, y)}{\partial x^l} \qquad (l = 0, 1, \ldots, m+r),$$

so besitzen auch diese Polynome ganze rationale Koeffizienten; speziell ist

$$P_l(x, x) = \sum_{h=0}^{m+r} \sum_{k=0}^{s} \binom{h}{l} A_{hk} x^{h+k-l} \quad (l = 0, 1, \ldots, m+r)$$

in x höchstens vom Grad $m+r+s-l$ und genügt der Ungleichung

$$\overline{|P_l(x, x)|} \leqq A \sum_{h=0}^{m+r} \binom{h}{l} = A \binom{m+r+1}{l+1}$$

$$\leqq A \sum_{k=0}^{m+r+1} \binom{m+r+1}{k} = 2^{m+r+1} A.$$

[2]) Der Hilfssatz bleibt offenbar richtig, wenn d durch eine größere Zahl ersetzt wird.

Nach 1. können zu $P_l(x, x)$ zwei Polynome $P_{l0}(x)$ und $P_l^*(x)$ mit ganzen rationalen Koeffizienten bestimmt werden, so daß

$$a_0^{m+r+1} P_l(x, x) = f(x) P_{l0}(x) + P_l^*(x) \quad (l = 0, 1, \ldots, m+r),$$

$$\max\left(\overline{|P_{l0}(x)|}, \overline{|P_l^*(x)|}\right) \leqq \overline{|P_l(x, x)|}\,(2a)^{m+r+1} \leqq 2^{m+r+1} A\,(2a)^{m+r+1} = (4a)^{m+r+1} A$$

ist, denn es besteht die Ungleichung

$$\max(0, m+r+s-l-n+1) \leqq m+r+1.$$

Also gibt es für das System der nr Koeffizienten der r Polynome

$$P_l^*(x) \qquad (l = 0, 1, \ldots, r-1)$$

höchstens

$$(2(4a)^{m+r+1} A + 1)^{nr} < ((2A+1)(4a)^{m+r+1})^{nr} = M$$

verschiedene Möglichkeiten. Bestimmt man die natürliche Zahl A durch

$$2A + 1 > (4a)^{(m+r+1)\frac{n}{\vartheta}} \geqq 2A - 1,$$

so ist aber

$$M < N$$

wegen

$$(m+r+1)(s+1) - nr \geqq \vartheta r.$$

Folglich gibt es dann in der Menge der N Polynome $P(x, y)$ mindestens zwei verschiedene Polynome $P'(x, y)$ und $P''(x, y)$, für die die zugeordneten Polynome

$$P_l'^*(x) \quad \text{und} \quad P_l''^*(x) \qquad (l = 0, 1, \ldots, r-1)$$

gliedweise der Reihe nach übereinstimmen. Die Differenz

$$R(x, y) = P'(x, y) - P''(x, y)$$

verschwindet nicht identisch; ferner ist

$$\overline{|R(x, y)|} \leqq 2A \leqq (4a)^{(m+r+1)\frac{n}{\vartheta}} + 1 \leqq 2(4a)^{(m+r+1)\frac{n}{\vartheta}},$$

und wenn

$$R_{hk}(x, y) = \frac{\partial^{h+k} R(x, y)}{h!\,k!\,\partial x^h\,\partial y^k}$$

gesetzt wird, so sind alle Polynome

$$R_{h0}(x, x) \qquad (h = 0, 1, \ldots, r-1)$$

ohne Rest durch $f(x)$ teilbar, also von der Form

$$R_{h0}(x, x) = f(x) H_h(x) \qquad (h = 0, 1, \ldots, r-1).$$

Offenbar bestehen folgende Taylorentwicklungen:

$$R_{i0}(x, y) = \sum_{h=0}^{m+r} \sum_{k=0}^{s} R_{h,k}(z, z) \binom{h}{i} (x-z)^{h-i} (y-z)^k \qquad (i = 0, 1, \ldots. m+r)$$

oder

$$R_{i0}(x, y) = (x-z)^{r-i} F_i(x, y, z) + (y-z) G_i(x, y, z) + f(z) H_i(x, z),$$

mit den Abkürzungen

$$F_i(x, y, z) = \sum_{h=r}^{m+r} \sum_{k=0}^{s} R_{hk}(z, z) \binom{h}{i} (x-z)^{h-r}(y-z)^k,$$

$$G_i(x, y, z) = \sum_{h=0}^{r-1} \sum_{k=1}^{s} R_{hk}(z, z) \binom{h}{i} (x-z)^{h-i}(y-z)^{k-1}, \quad (i = 0, 1, \ldots, m+r)$$

$$H_i(x, z) = \sum_{h=0}^{r-1} \frac{R_{h0}(z, z)}{f(z)} \binom{h}{i} (x-z)^{h-i}.$$

Diese neuen Funktionen sind sämtlich Polynome, und zwar haben $F_i(x, y, z)$ und $G_i(x, y, z)$ ganze rationale Koeffizienten. Für $i \geqq r$ verschwinden $G_i(x, y, z)$ und $H_i(x, z)$ identisch.

3. Da das Polynom $R(x, y)$ nicht identisch verschwindet, so sind in der Entwicklung nach Potenzen von y

$$R(x, y) = \sum_{k=0}^{s} u_k(x)\, y^k$$

nicht alle Polynome

$$u_0(x),\ u_1(x),\ \ldots,\ u_s(x)$$

identisch gleich Null. Seien etwa genau $s' + 1$ $(s' \geqq 0)$ von ihnen:

$$u_{k_0}(x),\ u_{k_1}(x),\ \ldots,\ u_{k_{s'}}(x)$$

linear unabhängig in bezug auf den Körper der rationalen Zahlen; da ihre Koeffizienten in diesem Körper liegen, so sind sie auch linear unabhängig in bezug auf den Körper der komplexen Zahlen.

Ihre Wronski-Determinante

$$\Delta(x) = \left| \frac{\partial^i u_{k_j}(x)}{\partial x^i} \right| \qquad (i, j = 0, 1, \ldots, s')$$

verschwindet also nicht identisch. Diese Determinante ist aber höchstens $(s+1)$-reihig und ihre Elemente sind Polynome mit ganzen rationalen Koeffizienten höchstens vom Grad $m + r$. Folglich ist $\Delta(x)$ ein Polynom mit ganzen rationalen Koeffizienten höchstens vom Grad $(s+1)(m+r)$.

Sei von jetzt ab $r \geqq s$, also erst recht $r \geqq s'$. Nach Annahme lassen sich die Polynome $u_k(x)$ linear mit offenbar rationalen Koeffizienten durch die Polynome $u_{k_j}(x)$ ausdrücken. Dadurch geht $R(x, y)$ über in eine Summe

$$R(x, y) = \sum_{j=0}^{s'} u_{k_j}(u)\, U_j(y)$$

mit gewissen $s' + 1$ Polynomen

$$U_0(y),\ U_1(y),\ \ldots,\ U_{s'}(y),$$

die rationale Koeffizienten haben, von niederem als n-tem Grade sind und von denen kein einziges identisch verschwindet. Differenziert man die Darstellung von $R(x, y)$ wiederholt nach x, so kommt man zu folgenden linearen Gleichungen für die Polynome $U_j(y)$:

$$R_{i0}(x, y) = \frac{1}{i!} \sum_{j=0}^{s'} u_{kj}^{(i)}(x)\, U_j(y) = (x-y)^{r-i} F_i(x, y, y) + f(y)\, H_i(x, y).$$

Sei $\Delta_j(x)$ die Unterdeterminante des Elementes $u_{k_0}^{(i)}(x)$ in der Determinante $\Delta(x)$; die vorige Gleichung werde mit $i!\,\Delta_i(x)$ multipliziert und über $i = 0, 1, \ldots, s'$ summiert; dann folgt

$$\Delta(x)\, U_0(y) = (x-y)^{r-s'} \sum_{i=0}^{s'} i!\,(x-y)^{s'-i}\, \Delta_i(x) F_i(x, y, y) + f(x) \sum_{i=0}^{s'} i!\, \Delta_i(x)\, H_i(x, y).$$

Dieser Gleichung entnimmt man aber, daß die sämtlichen Polynome

$$\Delta^{(h)}(x)\, U_0(x) \qquad (h = 0, 1, \ldots, r-s'-1)$$

und also auch die sämtlichen Polynome

$$\Delta^{(h)}(x) \qquad (h = 0, 1, \ldots, r-s'-1)$$

durch $f(x)$ teilbar sind, weil $U_0(x)$ von niederem Grad als das irreduzible Polynom $f(x)$ und daher hierzu teilerfremd ist.

Wegen der Irreduzibilität von $f(x)$ ist somit das Polynom $\Delta(x)$ durch $f(x)^{r-s'}$, also erst recht durch $f(x)^{r-s}$ teilbar; wird

$$\Delta(x) = f(x)^{r-s} D(x)$$

gesetzt, so ist auch $D(x)$ ein Polynom mit rationalen Koeffizienten und sein Grad übersteigt nicht den Wert

$$(s+1)(m+r) - (r-s)n = (s+1)\frac{n+\vartheta}{s+1} r - (r-s)n \leqq \vartheta r + (n-1)n = d^{3}).$$

4. Seien $\frac{p_1}{q_1}$ und $\frac{p_2}{q_2}$ zwei gekürzte rationale Zahlen und

$$\max(|p_2|, |q_2|) > 2(4a)^{(m+r+1)\frac{n}{\vartheta}},$$

also erst recht

$$\max(|p_2|, |q_2|) > |R(x, y)|.$$

---

[3]) Es gilt sogar $(s'+1)(m+r) - (r-s')n \geqq$ Grad von $D(x)$, woraus $s' = s$ für $\vartheta \leqq 1$ und großes r folgt, und damit werden die $U_j(y)$ wieder überflüssig. Bis 10. brauchte dann für $\frac{p_2}{q_2}$ nur die triviale Einschränkung $q_2 \neq 0$ gemacht zu werden. (Anmerkung von C. Siegel.)

In der Entwicklung nach Potenzen von x

$$R(x,y) = \sum_{h=0}^{m+r} x^h V_h(y)$$

ist mindestens eins der Polynome $V_h(y)$ nicht identisch Null. Seine Koeffizienten sind ganz rational und nach der vorigen Annahme kleiner als eine der Zahlen $|p_2|$ und $|q_2|$; das Polynom ist also nicht durch $q_2 y - p_2$ teilbar, folglich an der Stelle $y = \frac{p_2}{q_2}$ von Null verschieden. Als Funktion von x ist daher

$$R\left(x, \frac{p_2}{q_2}\right) = \sum_{j=0}^{s'} u_{k_j}(x)\, U_j\left(\frac{p_2}{q_2}\right)$$

nicht identisch gleich Null, so daß auch nicht alle Zahlen

$$U_j\left(\frac{p_2}{q_2}\right) \qquad (j = 0, 1, \ldots, s')$$

zugleich verschwinden. Ohne Einschränkung ist etwa $U_0\left(\frac{p_2}{q_2}\right) \neq 0$.

Wegen

$$\Delta(x)\, U_0(y) = \sum_{i=0}^{s'} i!\, \Delta_i(x)\, R_{i0}(x,y)$$

besteht aber die Identität

$$\Delta(x)\, U_0\left(\frac{p_2}{q_2}\right) = \sum_{i=0}^{s'} i!\, \Delta_i(x)\, R_{i0}\left(x, \frac{p_2}{q_2}\right).$$

Die linke Seite verschwindet nicht identisch in x und nimmt den Wert Null außer bei den Nullstellen von $f(x)$ nur noch bei den Nullstellen von $D(x)$ an. Das Polynom $f(x)$ kann wegen seiner Irreduzibilität die Zahl $\frac{p_1}{q_1}$ nicht zur Nullstelle haben. Dagegen könnte das Polynom $D(x)$ bei $x = \frac{p_1}{q_1}$ verschwinden, aber höchstens zur Ordnung d, da sein Grad nicht größer ist.

Mindestens eine der $d+1$ Zahlen

$$\Delta\left(\frac{p_1}{q_1}\right),\ \Delta'\left(\frac{p_1}{q_1}\right),\ \ldots,\ \Delta^{(d)}\left(\frac{p_1}{q_1}\right)$$

muß demnach von Null verschieden sein, etwa

$$\Delta^{(\delta)}\left(\frac{p_1}{q_1}\right) \neq 0.$$

Durch wiederholtes Differenzieren der Identität

$$\Delta(x)\, U_0\left(\frac{p_2}{q_2}\right) = \sum_{i=0}^{s'} i!\, \Delta_i(x)\, R_{i0}\left(x, \frac{p_2}{q_2}\right)$$

kommt man zu der Gleichung

$$\Delta^{(j)}\left(\frac{p_1}{q_1}\right) U_0\left(\frac{p_2}{q_2}\right) = \sum_{i=0}^{s'} \sum_{h=0}^{j} (i+h)! \binom{j}{h} \Delta_i^{(j-h)}\left(\frac{p_1}{q_1}\right) R_{i+h,0}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right),$$

deren linke Seite nach der vorigen Bemerkung nicht verschwindet, deren rechte Seite aber eine Linearform mit endlichen Koeffizienten in den Zahlen

$$R_{h,0}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) \qquad (h = 0, 1, \ldots, d + s')$$

ist. Folglich muß mindestens eine dieser Zahlen von Null verschieden sein, etwa die Zahl $R_{i,0}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right)$. Der Index i ist höchstens gleich

$$d + s \leqq \vartheta r + (n-1)\, n + s \leqq \vartheta r + n^2 - 1.$$

Von jetzt ab setzen wir voraus, daß

$$\vartheta \leqq \tfrac{1}{2},\ r \geqq 2n^2,$$

also erst recht

$$i \leqq r - 1$$

ist. In der Identität

$$R_{i0}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) = \left(\frac{p_1}{q_1} - z\right)^{r-i} F_i\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, z\right) + \left(\frac{p_2}{q_2} - z\right) G_i\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, z\right) + f(z)\, H_i\left(\frac{p_1}{q_1}, z\right)$$

ist dann die linke Seite von Null verschieden, während rechts der Faktor

$$\frac{p_1}{q_1} - z$$

zu einer positiven Potenz vorkommt.

5. Die bisherigen Entwicklungen haben zu folgendem Ergebnis geführt:

Hilfssatz 2. *Bedeute*:

$f(x)$ *ein irreduzibles Polynom mit ganzen rationalen Koeffizienten vom Grade* $n \geqq 3$,

a *die natürliche Zahl* $\overline{|f(x)|}$,

s *eine natürliche Zahl kleiner als* n,

r *eine natürliche Zahl größer oder gleich* $2n^2$,

$\vartheta \leqq \frac{1}{2}$ *eine positive Zahl*,

m *die natürliche Zahl* $m = \left[\left(\frac{n+\vartheta}{s+1} - 1\right) r\right]$.

Dann gibt es ein Polynom $R(x, y)$ *mit ganzen rationalen Koeffizienten, das in* x *höchstens vom Grad* $m + r$, *in* y *höchstens vom Grad* s *ist, der Ungleichung*

$$\overline{|R(x, y)|} \leqq 2(4a)^{(m+r+1)\frac{n}{\vartheta}}$$

genügt und folgende beiden Eigenschaften besitzt:

a) *Setzt man zur Abkürzung*

$$F_i(x, y, z) = \sum_{h=r}^{m+r} \sum_{k=0}^{s} R_{hk}(z, z)\binom{h}{i}(x-z)^{h-r}(y-z)^k,$$

$$G_i(x, y, z) = \sum_{h=0}^{r-1} \sum_{k=1}^{s} R_{hk}(z, z)\binom{h}{i}(x-z)^{h-i}(y-z)^{k-1}, \qquad \left(R_{hk}(x, y) = \frac{\partial^{h+k} R(x, y)}{h!\, k!\, \partial x^h\, \partial y^k}\right)$$

$$H_i(x, z) = \sum_{h=0}^{r-1} \frac{R_{h0}(z, z)}{f(z)}\binom{h}{i}(x-z)^{h-i},$$

so sind diese drei Funktionen Polynome in x, y, z, die ersten beiden sogar mit ganzen rationalen Koeffizienten, und genügen der Identität

$$R_{i0}(x, y) = (x-z)^{r-i} F_i(x, y, z) + (y-z) G_i(x, y, z) + f(z) H_i(x, z).$$

b) *Sind* $\frac{p_1}{q_1}$ *und* $\frac{p_2}{q_2}$ *zwei gekürzte rationale Zahlen mit*

$$\max(|p_2|, |q_2|) > 2(4a)^{(m+r+1)\frac{n}{\vartheta}},$$

so gibt es eine natürliche Zahl

$$i \leqq \vartheta r + n^2 - 1 \leqq r - 1,$$

so daß die Ableitung

$$R_{i0}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right)$$

nicht verschwindet.

II.

6. Die Gleichung

$$f(x) \equiv a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

ist nach Voraussetzung im Körper der rationalen Zahlen irreduzibel. Wir nehmen an, daß sie im Körper R der reellen Zahlen eine Wurzel ζ, im Körper R_1 der P_1-adischen Zahlen eine Wurzel ζ_1, im Körper R_2 der P_2-adischen Zahlen eine Wurzel ζ_2 usw., schließlich im Körper R_t der P_t-adischen Zahlen eine Wurzel ζ_t besitzt; dabei sind $P_1, P_2, \ldots, P_t$ endlichviele verschiedene Primzahlen. Die Körper $R, R_1, R_2, \ldots, R_t$ sind bewertete Körper; einer Zahl $\alpha \neq 0$ aus R wird als Wert $|\alpha|$ ihr absoluter Betrag, einer Zahl $\alpha_\tau \neq 0$ aus R_τ wird für $\tau = 1, 2, \ldots, t$ als Wert $|\alpha_\tau|_{P_\tau}$ diejenige Potenz $P_\tau^{e_\tau}$ zugeordnet, für die die Zahl $P_\tau^{e_\tau}\alpha_\tau$ eine P_τ-adische Einheit ist; die Zahl Null dagegen hat in allen Körpern den Wert Null. Da der Körper der rationalen Zahlen in allen Körpern $R, R_1, R_2, \ldots, R_t$ als Unterkörper enthalten ist, so sind

für seine Elemente sämtliche Bewertungen gleichzeitig definiert. Für ganze rationale Zahlen $\alpha \neq 0$ genügen diese Bewertungen speziell der Ungleichung

$$|\alpha| \prod_{\tau=1}^{t} |\alpha|_{P_\tau} \geqq 1.$$

Weiter gelten für Zahlen aus den Körpern $R, R_1, R_2, \ldots, R_t$ die Rechenregeln

$$|\alpha\beta| = |\alpha|\,|\beta|, \qquad |\alpha+\beta| \leqq |\alpha| + |\beta|,$$

$$\alpha_\tau \beta_\tau|_{P_\tau} = |\alpha_\tau|_{P_\tau}\,|\beta_\tau|_{P_\tau}, \quad |\alpha_\tau + \beta_\tau|_{P_\tau} \leqq \max\left(|\alpha_\tau|_{P_\tau}, |\beta_\tau|_{P_\tau}\right) \quad (\tau = 1, 2, \ldots, t).$$

Als Anwendung hiervon beweist man leicht die Ungleichungen

$$|\zeta| \leqq a+1; \quad |\zeta_\tau|_{P_\tau} \leqq a, \ (\tau = 1, 2, \ldots, t); \quad \prod_{\tau=1}^{t} \max\left(1, |\zeta_\tau|_{P_\tau}\right) \leqq a.$$

7. Nach Satz 2 und seinen Voraussetzungen ist offenbar die Zahl

$$\mathfrak{R}_i = q_1^{m+r-i} q_2^{s} R_{i0}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right)$$

ganz rational und von Null verschieden, ferner

$$R(x, y) \ll 2\,(4a)^{(m+r+1)\frac{n}{\vartheta}} \sum_{h=0}^{m+r} \sum_{k=0}^{s} x^h y^k,$$

also

$$R_{i0}(x, y) \ll 2\,(4a)^{(m+r+1)\frac{n}{\vartheta}} \sum_{h=0}^{m+r} \sum_{k=0}^{s} \binom{h}{i} x^{h-i} y^k.$$

Wegen

$$\binom{h}{i} \leqq \sum_{\iota=0}^{h} \binom{h}{\iota} = 2^h \leqq 2^{m+r}$$

und

$$\sum_{h=0}^{m+r} \binom{h}{i} x^{h-i} \ll 2^{m+r} \sum_{h=0}^{m+r-i} x^h \ll 2^{m+r} \sum_{h=0}^{m+r-i} \binom{m+r-i}{h} x^h = 2^{m+r}(1+x)^{m+r-i};$$

$$\sum_{k=0}^{s} y^k \ll \sum_{k=0}^{s} \binom{s}{k} y^k = (1+y)^k$$

folgt demnach

$$R_{i0}(x, y) \ll 2^{m+r+1}(4a)^{(m+r+1)\frac{n}{\vartheta}} (1+x)^{m+r-i}(1+y)^s$$

und hieraus

$$|\mathfrak{R}_i| \leqq 2^{m+r+1}(4a)^{(m+r+1)\frac{n}{\vartheta}} (|p_1| + |q_1|)^{m+r-i} (|p_2| + |q_2|)^s.$$

Für beliebige ganze rationale Zahlen p und q werde die Abkürzung

$$|p, q| = \max\left(|p|, |q|\right)$$

eingeführt; wegen

$$|p_1| + |q_1| \leqq 2|p_1, q_1|, \quad |p_2| + |q_2| \leqq 2|p_2, q_2|, \quad (m+r-i)+s \leqq m+r+n-1$$

ergibt sich dann

$$|\mathfrak{R}_i| \leqq 2^{2(m+r)+n}(4a)^{(m+r+1)\frac{n}{\vartheta}} |p_1, q_1|^{m+r-i} |p_2, q_2|^s.$$

Weil $\mathfrak{R}_i$ ganz rational ungleich Null ist und dieser Ungleichung genügt, so ergeben sich für die Bewertungen dieser Zahl nach 6. nun leicht die unteren Schranken

$$|\mathfrak{R}_i| \geqq 1,$$

$$|\mathfrak{R}_i|_{P_\tau} \geqq \{2^{2(m+r)+n}(4a)^{(m+r+1)\frac{n}{\vartheta}} |p_1, q_1|^{m+r-i} |p_2, q_2|^s\}^{-1}, \quad (\tau = 1, 2, \ldots, t),$$

$$\prod_{\tau=1}^{t} |\mathfrak{R}_i|_{P_\tau} \geqq \{2^{2(m+r)+n}(4a)^{(m+r+1)\frac{n}{\vartheta}} |p_1, q_1|^{m+r-i} |p_2, q_2|^s\}^{-1},$$

$$|\mathfrak{R}_i| \prod_{\tau=1}^{t} |\mathfrak{R}_i|_{P_\tau} \geqq 1.$$

8. Sei ferner

$$\mathfrak{F}_i = q_1^{m+r-i} q_2^s F_i\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \zeta\right), \quad \mathfrak{G}_i = q_1^{m+r-i} q_2^s G_i\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \zeta\right)$$

und

$$\left.\begin{aligned} \mathfrak{F}_{i\tau} &= q_1^m q_2^s F_i\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \zeta_\tau\right), \\ \mathfrak{G}_{i\tau} &= q_1^{m+r-i} q_2^{s-1} G_i\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \zeta_\tau\right). \end{aligned}\right\} \quad (\tau = 1, 2, \ldots, t)$$

Um für die Bewertungen dieser reellen bzw. P_τ-adischen Zahlen obere Schranken zu gewinnen, muß in beiden Fällen verschieden vorgegangen werden.

Für die beiden Zahlen $\mathfrak{F}_i$ und $\mathfrak{G}_i$ kommt man so zum Ziel: Ähnlich wie in 7. erhält man aus

$$R(x, y) \leqq 2(4a)^{(m+r+1)\frac{n}{\vartheta}} \sum_{\alpha=0}^{m+r} \sum_{\beta=0}^{s} x^\alpha y^\beta$$

die Majorante

$$R_{hk}(x, y) \leqq 2(4a)^{(m+r+1)\frac{n}{\vartheta}} \sum_{\alpha=0}^{m+r} \sum_{\beta=0}^{s} \binom{\alpha}{h}\binom{\beta}{k} x^{\alpha-h} y^{\beta-k},$$

wegen

$$|\zeta| \leqq a + 1$$

somit die Ungleichung

$$|R_{hk}(\zeta, \zeta)| \leqq 2(4a)^{(m+r+1)\frac{n}{\vartheta}} \sum_{\alpha=0}^{m+r} \sum_{\beta=0}^{s} \binom{\alpha}{h}\binom{\beta}{k} (a+1)^{\alpha+\beta-h-k}.$$

Von jetzt ab nehmen wir

$$\left|\frac{p_1}{q_1} - \zeta\right| \leqq 1, \quad \left|\frac{p_2}{q_2} - \zeta\right| \leqq 1$$

an, soweit diese Absolutbeträge vorkommen. Dann ist offenbar

$$\max\left(\left|F_i\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \zeta\right)\right|, \left|G_i\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \zeta\right)\right|\right) \leqq \sum_{h=0}^{m+r} \sum_{k=0}^{s} \binom{h}{i} |R_{hk}(\zeta, \zeta)| = S$$

und wenn man die letzte Schranke einsetzt und die Summationen über h und k ausführt:

$$S \leqq 2\,(4\,a)^{(m+r+1)\frac{n}{\vartheta}} \sum_{\alpha=0}^{m+r} \sum_{\beta=0}^{s} \binom{\alpha}{i} (a+1)^i (a+2)^{\alpha-i+\beta}.$$

Es ist aber wegen $a \geqq 1$

$$\binom{\alpha}{i} \leqq \sum_{i=0}^{\alpha} \binom{\alpha}{i} = 2^\alpha \leqq 2^{m+r},$$

$$\sum_{\alpha=0}^{m+r} \binom{\alpha}{i} (a+1)^i (a+2)^{\alpha-i} \leqq 2^{m+r} \sum_{\alpha=0}^{m+r} (a+2)^\alpha$$

$$\leqq 2^{m+r} \sum_{\alpha=0}^{m+r} \binom{m+r}{\alpha} (a+2)^\alpha = 2^{m+r}(a+3)^{m+r} \leqq (2 \cdot 4\,a)^{m+r},$$

$$\sum_{\beta=0}^{s} (a+2)^\beta \leqq \sum_{\beta=0}^{s} \binom{s}{\beta} (a+2)^\beta = (a+3)^s \leqq (4a)^s \leqq (4\,a)^{n-1} \leqq \tfrac{1}{4}(8\,a)^n,$$

also erhält man

$$S \leqq \tfrac{1}{2}(4\,a)^{(m+r+1)\frac{n}{\vartheta}} (8\,a)^{m+r+n},$$

und schließlich

$$\max(|\mathfrak{F}_i|, |\mathfrak{G}_i|) \leqq \tfrac{1}{2}(4\,a)^{(m+r+1)\frac{n}{\vartheta}} (8\,a)^{m+r+n} |q_1|^{m+r-i} |q_2|^s.$$

Noch einfacher kommt man zu Schranken für $\mathfrak{F}_{i\tau}$ und $\mathfrak{G}_{i\tau}$. Diese Ausdrücke sind Polynome in ζ_τ mit ganzen rationalen Koeffizienten höchstens vom Grad $m + r + s$; also ist

$$\max(|\mathfrak{F}_{i\tau}|_{P_\tau}, |\mathfrak{G}_{i\tau}|_{P_\tau}) \leqq \max(1, |\zeta_\tau|_{P_\tau})^{m+r+s}$$

$$\leqq \max(1, |\zeta_\tau|_{P_\tau})^{m+r+n-1} \qquad (\tau = 1, 2, \ldots, t).$$

Wegen

$$|\zeta_\tau|_{P_\tau} \leqq a \quad \text{und} \quad \prod_{\tau=1}^{t} \max(1, |\zeta_\tau|_{P_\tau}) \leqq a$$

folgt hieraus

$$\max(|\mathfrak{F}_{i\tau}|_{P_\tau}, |\mathfrak{G}_{i\tau}|_{P_\tau}) \leqq a^{m+r+n-1} \qquad (\tau = 1, 2, \ldots, t),$$

$$\prod_{\tau=1}^{t} \max(|\mathfrak{F}_{i\tau}|_{P_\tau}, |\mathfrak{G}_{i\tau}|_{P_\tau}) \leqq a^{m+r+n-1}.$$

9. Die Abschätzungen in 7. und 8. wenden wir auf die Gleichung

$$R_{i0}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) = \left(\frac{p_1}{q_1} - z\right)^{r-i} F_i\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, z\right) + \left(\frac{p_2}{q_2} - z\right) G_i\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, z\right)$$

$$+ f(z)\, H_i\left(\frac{p_1}{q_1}, z\right)$$

an, indem wir für z der Reihe nach $\zeta, \zeta_1, \zeta_2, \ldots, \zeta_t$ einsetzen; dann fällt jedesmal rechts das letzte Glied fort und man kommt zu folgenden Formeln:

$$\mathfrak{R}_i = \left(\frac{p_1}{q_1} - \zeta\right)^{r-i} \mathfrak{F}_i + \left(\frac{p_2}{q_2} - \zeta\right) \mathfrak{G}_i,$$
$$\mathfrak{R}_i = (p_1 - q_1\zeta_\tau)^{r-i} \mathfrak{F}_{i\tau} + (p_2 - q_2\zeta_\tau)\, \mathfrak{G}_{i\tau} \quad (\tau = 1, 2, \ldots, t),$$

aus welchen durch Übergang zu den Bewertungen

$$|\mathfrak{R}_i| \leqq 2 \max(|\mathfrak{F}_i|, |\mathfrak{G}_i|) \max\left(\left|\frac{p_1}{q_1} - \zeta\right|^{r-i}, \left|\frac{p_2}{q_2} - \zeta\right|\right),$$
$$|\mathfrak{R}_i|_{P_\tau} \leqq \max(|\mathfrak{F}_{i\tau}|_{P_\tau}, |\mathfrak{G}_{i\tau}|_{P_\tau}) \max(|p_1 - q_1\zeta_\tau|_{P_\tau}^{r-i}, |p_2 - q_2\zeta_\tau|_{P_\tau}) \quad (\tau = 1, 2, \ldots, t)$$

folgt. Jetzt werde für

$$|\mathfrak{R}_i|, |\mathfrak{R}_i|_{P_\tau}, |\mathfrak{F}_i|, |\mathfrak{F}_{i\tau}|_{P_\tau}, |\mathfrak{G}_i|, |\mathfrak{G}_{i\tau}|_{P_\tau}$$

ihre untere bzw. ihre obere Schranke eingesetzt; alsdann kommt man zu den Ungleichungen:

$$\max\left(\left|\frac{p_1}{q_1} - \zeta\right|^{r-i}, \left|\frac{p_2}{q_2} - \zeta\right|\right) \geqq \{(8a)^{m+r+n} (4a)^{(m+r+1)\frac{n}{\vartheta}} |q_1|^{m+r-i} |q_2|^s\}^{-1},$$
$$\max(|p_1 - q_1\zeta_\tau|_{P_\tau}^{r-i}, |p_2 - q_2\zeta_\tau|_{P_\tau}) \geqq \{2^{2(m+r)+n} a^{m+r+n-1} (4a)^{(m+r+1)\frac{n}{\vartheta}} |p_1, q_1|^{m+r-i} |p_2, q_2|^s\}^{-1},$$
$$\prod_{\tau=1} \max(|p_1 - q_1\zeta_\tau|_{P_\tau}^{r-i}, |p_2 - q_2\zeta_\tau|_{P_\tau}) \geqq \{2^{2(m+r)+n} a^{m+r+n-1} (4a)^{(m+r+1)\frac{n}{\vartheta}} |p_1, q_1|^{m+r-i} |p_2, q_2|^s\}^{-1},$$
$$\max\left(\left|\frac{p_1}{q_1} - \zeta\right|^{r-i}, \left|\frac{p_2}{q_2} - \zeta\right|\right) \prod_{\tau=1}^{t} \max(|p_1 - q_1\zeta_\tau|_{P_\tau}^{r-i}, |p_2 - q_2\zeta_\tau|_{P_\tau}) \geqq \{a^{m+r+n-1} (8a)^{m+r+n} (4a)^{(m+r+1)\frac{n}{\vartheta}} |q_1|^{m+r-i} |q_2|^s\}^{-1}.$$

Die Ausdrücke auf der rechten Seite kann man noch etwas vereinfachen. Nach Voraussetzung ist

$$n \geqq 3, \quad r \geqq 2n^2 \geqq 2 \cdot 3 \cdot n = 6n,$$

demnach

$$m + r + n \leqq m + r + \frac{r}{6} \leqq \left(1 + \frac{1}{6}\right)(m + r + 1);$$

somit hat man

$$(8a)^{m+r+n} \leqq (4a)^{3(m+r+1)},$$
$$2^{2(m+r)+n} a^{m+r+n-1} \leqq (4a)^{3(m+r+1)},$$
$$a^{m+r+n-1} (8a)^{m+r+n} \leqq (4a)^{3(m+r+1)},$$

und die obigen Ungleichungen gehen über in

$$\max\left(\left|\frac{p_1}{q_1}-\zeta\right|^{r-i}, \left|\frac{p_2}{q_2}-\zeta\right|\right) \geqq \left\{(4a)^{(m+r+1)\left(3+\frac{n}{\vartheta}\right)}|q_1|^{m+r-i}|q_2|^{s}\right\}^{-1},$$

$$\max\left(|p_1-q_1\zeta_\tau|_{P_\tau}^{r-i}, |p_2-q_2\zeta_\tau|_{P_\tau}\right) \geqq \left\{(4a)^{(m+r+1)\left(3+\frac{n}{\vartheta}\right)}|p_1,q_1|^{m+r-i}|p_2,q_2|^{s}\right\}^{-1},$$

$$\prod_{\tau=1}^{t}\max\left(|p_1-q_1\zeta_\tau|_{P_\tau}^{r-i}, |p_2-q_2\zeta_\tau|_{P_\tau}\right) \geqq \left\{(4a)^{(m+r+1)\left(3+\frac{n}{\vartheta}\right)}|p_1,q_1|^{m+r-i}|p_2,q_2|^{s}\right\}^{-1},$$

$$\max\left(\left|\frac{p_1}{q_1}-\zeta\right|^{r-i}, \left|\frac{p_2}{q_2}-\zeta\right|\right)\prod_{\tau=1}^{t}\max\left(|p_1-q_1\zeta_\tau|_{P_\tau}^{r-i}, |p_2-q_2\zeta_\tau|_{P_\tau}\right) \geqq \left\{(4a)^{(m+r+1)\left(3+\frac{n}{\vartheta}\right)}|q_1|^{m+r-i}|q_2|^{s}\right\}^{-1}.$$

Man beachte, daß bei der ersten und letzten von diesen Ungleichungen

$$\left|\frac{p_1}{q_1}-\zeta\right| \leqq 1, \quad \left|\frac{p_2}{q_2}-\zeta\right| \leqq 1$$

vorausgesetzt wird. Um in allen vier Fällen möglichst gleiche Formeln zu erhalten, ersetzen wir auf der rechten Seite dieser beiden Ungleichungen die Ausdrücke $|q_1|$ und $|q_2|$ durch $|p_1, q_1|$ und $|p_2, q_2|$, was offenbar erlaubt ist. Dann kommen wir schließlich zu dem Ergebnis, daß keine der vier Zahlen

$$E_{(1,0)} = (4a)^{(m+r+1)\left(3+\frac{n}{\vartheta}\right)}|p_1,q_1|^{m+r-i}|p_2,q_2|^{s}\max\left(\left|\frac{p_1}{q_1}-\zeta\right|^{r-i}, \left|\frac{p_2}{q_2}-\zeta\right|\right),$$

$$E_{(0,1)} = (4a)^{(m+r+1)\left(3+\frac{n}{\vartheta}\right)}|p_1,q_1|^{m+r-i}|p_2,q_2|^{s} \times \max\left(|p_1-q_1\zeta_\tau|_{P_\tau}^{r-i}, |p_2-q_2\zeta_\tau|_{P_\tau}\right),$$

$$E_{(0,t)} = (4a)^{(m+r+1)\left(3+\frac{n}{\vartheta}\right)}|p_1,q_1|^{m+r-i}|p_2,q_2|^{s} \times \prod_{\tau=1}^{t}\max\left(|p_1-q_1\zeta_\tau|_{P_\tau}^{r-i}, |p_2-q_2\zeta_\tau|_{P_\tau}\right),$$

$$E_{(1,t)} = (4a)^{(m+r+1)\left(3+\frac{n}{\vartheta}\right)}|p_1,q_1|^{m+r-i}|p_2,q_2|^{s}\max\left(\left|\frac{p_1}{q_1}-\zeta\right|^{r-i}, \left|\frac{p_2}{q_2}-\zeta\right|\right) \times \prod_{\tau=1}^{t}\max\left(|p_1-q_1\zeta_\tau|_{P_\tau}^{r-i}, |p_2-q_2\zeta_\tau|_{P_\tau}\right)$$

kleiner als Eins sein kann.

10. Von jetzt ab werden folgende vier Fälle unterschieden:
(1, 0): Untersuchung der Annäherung der einzelnen Zahl ζ.
(0, 1): Untersuchung der Annäherung der einzelnen Zahl ζ_τ.

$(0, t)$: Untersuchung der gleichzeitigen Annäherung von $\zeta_1, \zeta_2, \ldots, \zeta_t$.
$(1, t)$: Untersuchung der gleichzeitigen Annäherung von $\zeta, \zeta_1, \zeta_2, \ldots, \zeta_t$.

Bedeute k und Θ zwei positive Zahlen mit

$$k \geqq 1, \quad \beta = \frac{n}{s+1} + s + \Theta \leqq n,$$

ferner im Fall $(0, t)$ $\Gamma_1, \Gamma_2, \ldots, \Gamma_t$ t positive Zahlen mit

$$\sum_{\tau=1}^{t} \Gamma_\tau = 1,$$

und im Fall $(1, t)$ $\Gamma_0, \Gamma_1, \Gamma_2, \ldots, \Gamma_t$ $t+1$ positive Zahlen mit

$$\Gamma_0 + \sum_{\tau=1}^{t} \Gamma_\tau = 1.$$

An die früher eingeführten Größen sollen folgende Forderungen gestellt werden:

1. $$\vartheta \leqq \frac{1}{2}, \quad \vartheta < \frac{\Theta}{\beta},$$

2. $$r \geqq \frac{2n^3}{\vartheta} \geqq \frac{s+1}{s} \frac{n^3}{\vartheta},$$

3. $$|p_1, q_1| > (4a)^{\frac{\left(\frac{n}{s+1} + \vartheta\right)\left(3 + \frac{n}{\vartheta}\right)}{\min(1, \Theta - \beta\vartheta)}} k^{\frac{1 - \frac{s}{\beta} + \vartheta}{\Theta - \beta\vartheta}} = K,$$

4. $$(k^{-\frac{1}{\beta}} |p_1, q_1|)^r \leqq |p_2, q_2| < (k^{-\frac{1}{\beta}} |p_1, q_1|)^{r+1},$$

ferner im Fall $(1, 0)$:

5. $$\left|\frac{p_1}{q_1} - \zeta\right| \leqq k |p_1, q_1|^{-\beta},$$

6. $$\left|\frac{p_2}{q_2} - \zeta\right| \leqq k |p_2, q_2|^{-\beta};$$

im Fall $(0, 1)$:

5. $$|p_1 - q_1\zeta_\tau|_{P_\tau} \leqq k |p_1, q_1|^{-\beta},$$

6. $$|p_2 - q_2\zeta_\tau|_{P_\tau} \leqq k |p_2, q_2|^{-\beta};$$

im Fall $(0, t)$:

5. $$|p_1 - q_1\zeta_\tau|_{P_\tau} \leqq (k |p_1, q_1|^{-\beta})^{\Gamma_\tau} \quad \text{für } \tau = 1, 2, \ldots t,$$

6. $$|p_2 - q_2\zeta_\tau|_{P_\tau} \leqq (k |p_2, q_2|^{-\beta})^{\Gamma_\tau} \quad \text{für } \tau = 1, 2, \ldots t,$$

und im Fall $(1, t)$:

5. $$\left|\frac{p_1}{q_1} - \zeta\right| \leqq (k |p_1, q_1|^{-\beta})^{\Gamma_0};$$
$$|p_1 - q_1\zeta_\tau|_{P_\tau} \leqq (k |p_1, q_1|^{-\beta})^{\Gamma_\tau} \quad \text{für } \tau = 1, 2, \ldots t,$$

6. $$\left|\frac{p_2}{q_2} - \zeta\right| \leqq (k |p_2, q_2|^{-\beta})^{\Gamma_0};$$
$$|p_2 - q_2\zeta_\tau|_{P_\tau} \leqq (k |p_2, q_2|^{-\beta})^{\Gamma_\tau} \quad \text{für } \tau = 1, 2, \ldots t.$$

Zu diesen sechs Forderungen kommen die folgenden Bedingungen hinzu, die bereits früher gestellt wurden:

A: In allen vier Fällen:

$$r \geqq 2n^2,$$

B: In den Fällen $(1, 0)$ und $(1, t)$:

$$\left|\frac{p_1}{q_1} - \zeta\right| \leqq 1,$$

C: In den Fällen $(1, 0)$ und $(1, t)$:

$$\left|\frac{p_2}{q_2} - \zeta\right| \leqq 1,$$

D: In allen vier Fällen:

$$|p_2, q_2| > 2(4a)^{(m+r+1)\frac{n}{\vartheta}}.$$

Diese vier Ungleichungen sind jedoch Folgerungen aus 1 bis 6. In der Tat folgt A trivialerweise aus 1 und 2. Weiter ist

$$\frac{1 - \frac{s}{\beta} + \vartheta}{\Theta - \beta\vartheta} > \frac{1 - \frac{s}{\beta}}{\Theta} = \frac{1}{\beta} + \frac{n}{(s+1)\Theta\beta},$$

also

$$K > (4a)^{\left(\frac{n}{s+1} + \vartheta\right)\left(s + \frac{n}{\vartheta}\right)} k^{\frac{1}{\beta} + \frac{n}{(s+1)\Theta\beta}},$$

wegen 3 daher erst recht

$$|p_1, q_1| > k^{1/\beta},$$

so daß wegen 5 auch die Ungleichung B in beiden Fällen $(1, 0)$ und $(1, t)$ erfüllt ist. Weiter besteht wegen 2, 3 und 4 die Ungleichung

$$|p_2, q_2| > (4a)^{\left(\frac{n}{s+1} + \vartheta\right) r \left(s + \frac{n}{\vartheta}\right)} k^{\frac{n}{(s+1)\Theta\beta} \frac{2n^3}{\vartheta}}.$$

Hierin ist jedoch

$$\left(\frac{n}{s+1} + \vartheta\right) r = \frac{n + \vartheta}{s+1} r + \frac{s\vartheta r}{s+1} \geqq m + r + 1;$$

$$\frac{n}{(s+1)\Theta\beta} \frac{2n^3}{\vartheta} = \frac{1}{\beta} \frac{2n^4}{(s+1)\vartheta\Theta} \geqq \frac{1}{\beta};$$

daher gilt sowohl

$$|p_2, q_2| > k^{1/\beta},$$

als auch

$$|p_2, q_2| > (4a)^{(m+r+1)\left(s + \frac{n}{\vartheta}\right)} > 2(4a)^{(m+r+1)\frac{n}{\vartheta}}.$$

Aus 6 und der ersten dieser beiden Ungleichungen folgt in beiden Fällen $(1, 0)$ und $(1, t)$ die Bedingung C; die zweite Ungleichung ist mit D identisch.

Unter den Annahmen 1 bis 6 bleiben demnach alle bisherigen Schlüsse erhalten; speziell kann demnach keine der Zahlen $E_{(1,0)}$, $E_{(0,1)}$, $E_{(0,t)}$, $E_{(1,t)}$ kleiner als Eins sein.

11. Um diese Aussage zu prüfen, werde in der Definitionsgleichung dieser Zahlen für

$$\left|\frac{p_1}{q_1}-\zeta\right|,\quad \left|\frac{p_2}{q_2}-\zeta\right|,\quad |p_1-q_1\zeta_\tau|_{P_\tau},\quad |p_2-q_2\zeta_\tau|_{P_\tau}$$

ihr Wert nach den Forderungen 5 und 6 eingesetzt. Wegen

$$\max\left((k\,|\,p_1,q_1|^{-\beta})^{\Gamma_\tau(r-i)},\ (k\,|\,p_2,q_2|^{-\beta})^{\Gamma_\tau}\right)$$
$$=\max\left((k\,|\,p_1,q_1|^{-\beta})^{r-i},\ (k\,|\,p_2,q_2|^{-\beta})\right)^{\Gamma_\tau}\qquad\text{für } \tau=0,1,\ldots,t$$

gelangt man dann in allen vier Fällen zu derselben Abschätzung

$$E_{(1,0)}\leqq\max(E_1,E_2),\ E_{(0,1)}\leqq\max(E_1,E_2),$$
$$E_{(0,t)}\leqq\max(E_1,E_2),\ E_{(1,t)}\leqq\max(E_1,E_2),$$

wobei zur Abkürzung

$$E_1=(4a)^{(m+r+1)\left(3+\frac{n}{\vartheta}\right)}|p_1,q_1|^{m+r-i-\beta(r-i)}|p_2,q_2|^{s}k^{r-i},$$
$$E_2=(4a)^{(m+r+1)\left(3+\frac{n}{\vartheta}\right)}|p_1,q_1|^{m+r-i}|p_2,q_2|^{s-\beta}k$$

gesetzt wurde. Diese Ausdrücke gehen wegen 4 über in

$$E_1\leqq(4a)^{(m+r+1)\left(3+\frac{n}{\vartheta}\right)}|p_1,q_1|^{e_1}k^{f_1},\ E_2\leqq(4a)^{(m+r+1)\left(3+\frac{n}{\vartheta}\right)}|p_1,q_1|^{e_2}k^{f_2}$$

mit den Exponenten

$$e_1=m+r-i-\beta(r-i)+s(r+1)=(m+r-(\beta-s)r)+i(\beta-1)+s,$$
$$e_2=m+r-i+(s-\beta)r=(m+r-(\beta-s)r)-i\leqq e_1,$$
$$f_1=r-i-\frac{s}{\beta}(r+1)\leqq\left(1-\frac{s}{\beta}\right)r+1,\quad f_2=1-\frac{s-\beta}{\beta}r=\left(1-\frac{s}{\beta}\right)r+1.$$

Aus den Ungleichungen in Hilfssatz 2

$$m\leqq\left(\frac{n+\vartheta}{s+1}-1\right)r,\quad i\leqq\vartheta r+n^2-1$$

folgt aber

$$e_1\leqq-\left(\Theta-\frac{\vartheta}{s+1}\right)r+(\beta-1)(\vartheta r+n^2-1)+s$$
$$=-\left(\Theta-\left(\beta-\frac{s}{s+1}\right)\vartheta\right)r+(\beta-1)(n^2-1)+s;$$

aus

$$\beta\leqq n,\quad s\leqq n-1$$

folgt ferner

$$(\beta-1)(n^2-1)+s\leqq n^3.$$

Die Forderung 2 liefert demnach die Abschätzungen

$$\max(e_1,e_2)\leqq-(\Theta-\beta\vartheta)r,\qquad\max(f_1,f_2)\leqq\left(1-\frac{s}{\beta}+\vartheta\right)r,$$

so daß

$$\max(E_1,E_2)\leqq(4a)^{(m+r+1)\left(3+\frac{n}{\vartheta}\right)}|p_1,q_1|^{-(\Theta-\beta\vartheta)r}k^{\left(1-\frac{s}{\beta}+\vartheta\right)r},$$

wegen

$$m + r + 1 \leqq \left(\frac{n}{s+1} + \vartheta\right) r$$

demnach

$$\max(E_1, E_2) \leqq \left\{ |p_1, q_1|^{-(\Theta - \beta\vartheta)} (4a)^{\left(\frac{n}{s+1} + \vartheta\right)\left(3 + \frac{n}{\vartheta}\right)} k^{1 - \frac{s}{\beta} + \vartheta} \right\}^r$$

wird. Auf der rechten Seite dieser Ungleichung ist der Exponent

$$\Theta - \beta\vartheta$$

nach Forderung 1 positiv; Forderung 3 ergibt folglich

$$E_1 < 1, \quad E_2 < 1$$

und damit einen Widerspruch. Also sind in keinem der vier Fälle $(1, 0)$, $(0, 1)$, $(0, t)$, $(1, t)$ die Forderungen 1 bis 6 miteinander verträglich.

Damit ist gezeigt, daß zu den Wurzeln $\zeta, \zeta_1, \zeta_2, \ldots, \zeta_t$ und zu gegebenen positiven Zahlen ϑ, Θ, k, sowie $\Gamma_1, \Gamma_2, \ldots, \Gamma_t$ im Fall $(0, t)$ bzw. $\Gamma_0, \Gamma_1, \Gamma_2, \ldots, \Gamma_t$ im Fall $(1, t)$ unter den Voraussetzungen

$$k \geqq 1, \quad \beta = \frac{n}{s+1} + s + \Theta \leqq n, \quad \vartheta \leqq \frac{1}{2}, \quad \Theta - \beta\vartheta > 0,$$

$$\Gamma_1 + \Gamma_2 + \ldots + \Gamma_t = 1 \quad \text{bzw.} \quad \Gamma_0 + \Gamma_1 + \Gamma_2 + \ldots + \Gamma_t = 1$$

keine zwei gekürzten rationalen Zahlen $\frac{p_1}{q_1}$, $\frac{p_2}{q_2}$ mit

$$|p_1, q_1| > K, \quad |p_2, q_2| > \left(k^{-\frac{1}{\beta}} |p_1, q_1|\right)^{\frac{2n^3}{\vartheta}}$$

existieren, die in einem der vier Fälle $(1, 0)$, $(0, 1)$, $(0, t)$, $(1, t)$ den Ungleichungen (5) und (6) genügen. Also ist der folgende Hilfssatz bewiesen:

Hilfssatz 3. *Bedeute*:

$f(x)$ *ein irreduzibles Polynom mit ganzen rationalen Koeffizienten vom Grad* $n \geqq 3$,

a *die Zahl* $\overline{|f(x)|}$,

ζ *eine reelle Nullstelle von* $f(x)$,

$P_1, P_2, \ldots, P_t$ t *verschiedene Primzahlen*,

ζ_τ *für* $\tau = 1, 2, \ldots, t$ *eine* P_τ*-adische Nullstelle von* $f(x)$,

s *eine natürliche Zahl kleiner als* n,

ϑ, Θ, k *drei positive Zahlen mit*

$$\beta = \frac{n}{s+1} + s + \Theta \leqq n; \quad \vartheta \leqq \frac{1}{2}, \quad \vartheta < \frac{\Theta}{\beta}; \quad k \geqq 1,$$

K *die aus ihnen gebildete positive Zahl*

$$K = (4a)^{\frac{\left(\frac{n}{s+1} + \vartheta\right)\left(3 + \frac{n}{\vartheta}\right)}{\min(1, \Theta - \beta\vartheta)}} k^{\frac{1 - \frac{s}{\beta} + \vartheta}{\Theta - \beta\vartheta}},$$

$\Gamma_1, \Gamma_2, \ldots, \Gamma_t$ *im Fall* $(0, t)$ t *positive Zahlen der Summe* 1,

$\Gamma_0, \Gamma_1, \Gamma_2, \ldots, \Gamma_t$ *im Fall* $(1, t)$ $t + 1$ *positive Zahlen der Summe* 1.

Die Paare p, q teilerfremder ganzer rationaler Zahlen, die der Ungleichung

$$(1,0) \qquad \left|\frac{p}{q} - \zeta\right| \leqq k\,|p, q|^{-\beta},$$

bzw. der Ungleichung

$$(0,1) \qquad |p - q\zeta_\tau|_{P_\tau} \leqq k\,|p, q|^{-\beta},$$

bzw. den t Ungleichungen

$$(0,t) \qquad |p - q\zeta_\tau|_{P_\tau} \leqq (k\,|p, q|^{-\beta})^{\Gamma_\tau} \qquad (\tau = 1, 2, \ldots, t),$$

bzw. den $t+1$ Ungleichungen

$$(1,t) \qquad \left|\frac{p}{q} - \zeta\right| \leqq (k\,|p, q|^{-\beta})^{\Gamma_0},$$

$$|p - q\zeta_\tau|_{P_\tau} \leqq (k\,|p, q|^{-\beta})^{\Gamma_\tau} \qquad (\tau = 1, 2, \ldots, t)$$

genügen, befriedigen entweder alle die Ungleichung $|p, q| \leqq K$, oder es gibt auch solche Lösungen mit $|p, q| > K$, und wenn p_1, q_1 eine von ihnen mit möglichst kleinem $|p_1, q_1| > K$ ist, so befriedigen alle anderen hiervon die Ungleichung

$$|p_1, q_1| \leqq |p, q| < \left(k^{-\frac{1}{\beta}}\,|p_1 q_1|\right)^{\frac{2n^3}{9}}.$$

In diesem Satz ist speziell enthalten, daß die beiden Ungleichungen

$$\left|\frac{p}{q} - \zeta\right| \leqq k\,|p, q|^{-\beta}$$

und

$$|p - q\zeta_\tau|_{P_\tau} \leqq k\,|p, q|^{-\beta}$$

nur endlichviele Lösungen in Paaren p, q teilerfremder ganzer rationaler Zahlen besitzen (Satz von Thue-Siegel).

12. Es gelingt jetzt, den folgenden Satz zu beweisen:

Satz 1. *Bedeute $\zeta, \zeta_1, \zeta_2, \ldots, \zeta_t$ je eine reelle, eine P_1-adische, eine P_2-adische, ..., eine P_t-adische Nullstelle desselben irreduziblen Polynoms $f(x)$ mit ganzen rationalen Koeffizienten vom Grad $n \geqq 3$; sei ferner $k \geqq 1$ und β^* eine Zahl, die der Ungleichung*

$$\alpha < \beta^* \leqq n \quad \left(\alpha = \min_{s=1,2,\ldots,n-1}\left(\frac{n}{s+1} + s\right)\right)$$

genügt. Dann besitzt die Ungleichung

$$\min\left(1, \left|\frac{p}{q} - \zeta\right|\right) \prod_{\tau=1}^{t} \min\left(1, |p - q\zeta_\tau|_{P_\tau}\right) \leqq k\,|p, q|^{-\beta^*}$$

höchstens endlichviele Lösungen in Paaren p, q teilerfremder ganzer rationaler Zahlen.

Beweis. Da $\beta^* > \alpha$ ist, so gibt es eine natürliche Zahl $s < n$ und eine positive Zahl Θ, so daß

$$\beta = \frac{n}{s+1} + s + \Theta < \beta^*$$

ist, also

$$\beta^* = \beta\,(1 + \lambda)$$

mit einer positiven Zahl λ. Man hat wegen $k \geqq 1$

$$k\,|\,p, q\,|^{-\beta^*} = k^{-\frac{\beta^*-\beta}{\beta}}\,(k\,|\,p, q\,|^{-\beta})^{\frac{\beta^*}{\beta}} \leqq (k\,|\,p, q\,|^{-\beta})^{1+\lambda}.$$

Sei nun p, q irgendeine Lösung der Ungleichung

$$\min\left(1, \left|\frac{p}{q} - \zeta\right|\right) \prod_{\tau=1}^{t} \min\,(1, |\,p - q\,\zeta_\tau\,|_{P_\tau}) \leqq k\,|\,p, q\,|^{-\beta^*}$$

in teilerfremden ganzen rationalen Zahlen, und zwar möge

$$|\,p, q\,| > k^{1/\beta} > k^{1/\beta^*}, \quad \text{d. h.} \quad k\,|p, q\,|^{-\beta^*} < 1$$

sein. Dann gibt es $t+1$ nichtnegative Zahlen $\gamma_0, \gamma_1, \gamma_2, \ldots, \gamma_t$, die noch von p und q abhängen und deren Summe nicht kleiner als Eins ist, so daß die Gleichungen

$$\begin{aligned} \min\left(1, \left|\frac{p}{q} - \zeta\right|\right) &= (k\,|\,p, q\,|^{-\beta^*})^{\gamma_0}, \\ \min\,(1, |\,p - q\,\zeta_\tau\,|_{P_\tau}) &= (k\,|\,p, q\,|^{-\beta^*})^{\gamma_\tau} \qquad (\tau = 1, 2, \ldots, t) \end{aligned}$$

bestehen. Nach vorhin hat man

$$k\,|\,p, q\,|^{-\beta^*} \leqq (k\,|\,p, q\,|^{-\beta})^{1+\lambda};$$

also bestehen die Ungleichungen

$$\begin{aligned} \min\left(1, \left|\frac{p}{q} - \zeta\right|\right) &\leqq (k\,|\,p, q\,|^{-\beta})^{(1+\lambda)\gamma_0}, \\ \min\,(1, |\,p - q\,\zeta_\tau\,|_{P_\tau}) &\leqq (k\,|\,p, q\,|^{-\beta})^{(1+\lambda)\gamma_\tau} \qquad (\tau = 1, 2, \ldots, t). \end{aligned}$$

Jetzt werde eine natürliche Zahl v genommen, so daß

$$\lambda v \geqq t + 1$$

ist; es ist alsdann

$$(1 + \lambda)\,\gamma_\tau = \frac{g_\tau}{v} + \varrho_\tau \qquad (\tau = 0, 1, 2, \ldots, t),$$

wobei

$$g_\tau = [v\,(1 + \lambda)\,\gamma_\tau] \qquad (\tau = 0, 1, 2, \ldots, t)$$

nichtnegative ganze rationale Zahlen sind und die Reste

$$\varrho_\tau = (1 + \lambda)\,\gamma_\tau - \frac{g_\tau}{v} \qquad (\tau = 0, 1, 2, \ldots, t)$$

den Ungleichungen

$$0 \leqq \varrho_\tau < \frac{1}{v} \qquad (\tau = 0, 1, 2, \ldots, t)$$

genügen, folglich auch der Ungleichung

$$\sum_{\tau=0}^{t} \varrho_\tau \leqq \frac{t+1}{v} \leqq \lambda.$$

Wegen

$$\sum_{\tau=0}^{t} \gamma_\tau \geqq 1$$

folgt hieraus

$$\sum_{\tau=0}^{t} \frac{g_\tau}{v} = (1+\lambda) \sum_{\tau=0}^{t} \gamma_\tau - \sum_{\tau=0}^{t} \varrho_\tau \geqq (1+\lambda) - \lambda = 1,$$

also

$$g_0 + g_1 + \ldots + g_t \geqq v.$$

Es bestehen die Ungleichungen

$$\min\left(1, \left|\frac{p}{q} - \zeta\right|\right) \leqq (k\,|p, q|^{-\beta})^{(1+\lambda)\gamma_0} \leqq (k\,|p, q|^{-\beta})^{g_0/v},$$

$$\min(1, |p - q\zeta_\tau|_{P_\tau}) \leqq (k\,|p, q|^{-\beta})^{(1+\lambda)\gamma_\tau} \leqq (k\,|p, q|^{-\beta})^{g_\tau/v} \quad (\tau = 1, 2, \ldots, t).$$

Wenn nun die Summe der Zahlen

$$g_0, g_1, \ldots, g_t$$

den Wert v überschreitet, so bleiben die vorigen Ungleichungen richtig, wenn diese Zahlen ersetzt werden durch $t+1$ nichtnegative ganze rationale Zahlen

$$f_0, f_1, \ldots, f_t$$

mit

$$f_0 \leqq g_0,\ f_1 \leqq g_1,\ \ldots,\ f_t \leqq g_t;\ \sum_{\tau=0}^{t} f_\tau = v.$$

Damit ist jeder Lösung p, q von

$$\min\left(1, \left|\frac{p}{q} - \zeta\right|\right) \prod_{\tau=1}^{t} \min(1, |p - q\zeta_\tau|_{P_\tau}) \leqq k\,|p, q|^{-\beta^*}$$

mit $|p, q| \geqq k^{1/\beta}$ ein System von nichtnegativen ganzen rationalen Zahlen

$$f_0, f_1, \ldots, f_t$$

der Summe v zugeordnet worden, so daß die Ungleichungen

$$\min\left(1, \left|\frac{p}{q} - \zeta\right|\right) \leqq (k\,|p, q|^{-\beta})^{f_0/v},$$

$$\min(1, |p - q\zeta_\tau|_{P_\tau}) \leqq (k\,|p, q|^{-\beta})^{f_\tau/v} \qquad (\tau = 1, 2, \ldots, t)$$

bestehen; diese Zuordnung wird eindeutig, wenn z. B. verlangt wird, daß der Reihe nach $f_0, f_1, \ldots, f_t$ möglichst klein sind.

Unter ϑ und K verstehe man jetzt wieder zwei positive Zahlen, die zu β und k in der Beziehung wie in Hilfssatz 3 stehen; d. h. es sei

$$\vartheta \leqq \frac{1}{2}, \quad \vartheta < \frac{\Theta}{\beta}$$

und alsdann

$$K = (4a)^{\frac{\left(\frac{n}{s+1} + \vartheta\right)\left(3 + \frac{n}{\vartheta}\right)}{\min(1,\ \Theta - \beta\vartheta)}} k^{\frac{1 - \frac{s}{\beta} + \vartheta}{\Theta - \beta\vartheta}}.$$

Von nun ab betrachten wir nur noch solche Lösungen p, q von

$$\min\left(1, \left|\frac{p}{q}-\zeta\right|\right) \prod_{\tau=1}^{t} \min\left(1, |p-q\zeta_\tau|_{P_\tau}\right) \leqq k\,|p,q|^{-\beta^*},$$

für die $|p,q| > K$ ist; dann ist nach 10. erst recht $|p,q| > k^{1/\beta}$; um Satz 1 zu beweisen, genügt es, zu zeigen, daß die Anzahl dieser Lösungen endlich ist.

Alle diejenigen von diesen Lösungen, denen dieselben Zahlen

$$f_0, f_1, \ldots, f_t$$

zugeordnet sind, werden in der gleichen Klasse $C_{f_0 f_1 \ldots f_t}$ zusammengefaßt; es gibt

$$\binom{v+t}{t}$$

solche Klassen, nämlich so viel, wie die Anzahl der Lösungen der Gleichung

$$f_0 + f_1 + \ldots + f_t = v$$

in nichtnegativen ganzen rationalen Zahlen beträgt. Unter den Elementen p, q von $C_{f_0 f_1 \ldots f_t}$ werde dasjenige Element p_1, q_1 mit möglichst kleinem $|p_1, q_1| > K$ herausgegriffen. Hierfür und für die sämtlichen anderen Elemente der Menge bestehen die Ungleichungen

$$\min\left(1, \left|\frac{p}{q}-\zeta\right|\right) \leqq (k\,|p,q|^{-\beta})^{f_0/v},$$

$$\min\left(1, |p-q\zeta_\tau|_{P_\tau}\right) \leqq (k\,|p,q|^{-\beta})^{f_\tau/v} \qquad (\tau = 1, 2, \ldots, t).$$

Die Zahlen f_τ sind nicht alle Null und die Summe der nichtverschwindenden ist gleich v. Wenn etwa $f_\tau \neq 0$ ist, so hat man

$$(k\,|p,q|^{-\beta})^{f_\tau/v} < 1;$$

also muß die τ-te Ungleichung

$$\left|\frac{p}{q}-\zeta\right| \leqq (k\,|p,q|^{-\beta})^{f_0/v} \quad \text{bzw.} \quad |p-q\zeta_\tau|_{P_\tau} \leqq (k\,|p,q|^{-\beta})^{f_\tau/v}$$

lauten, je nachdem $\tau = 0$ oder $\tau \neq 0$ war.

Lassen wir von den Ungleichungen

$$\min\left(1, \left|\frac{p}{q}-\zeta\right|\right) \leqq (k\,|p,q|^{-\beta})^{f_0/v},$$

$$\min\left(1, |p-q\zeta_\tau|_{P_\tau}\right) \leqq (k\,|p,q|^{-\beta})^{f_\tau/v} \qquad (\tau = 1, 2, \ldots, t)$$

demnach alle mit verschwindendem f_τ fort, so besitzt das System der übrigen gerade die Form, wie sie im Hilfssatz 3 verlangt wurde, wenn man die nichtverschwindenden Zahlen $\frac{f_\tau}{v}$ mit den Zahlen Γ gleichsetzt. Aus diesem Hilfssatz folgt aber, daß alle Elemente von $C_{f_0 f_1 \ldots f_t}$ der Bedingung

$$|p_1, q_1| \leqq |p,q| < (k^{-\frac{1}{\beta}}\,|p_1, q_1|)^{\frac{2n^3}{\vartheta}}$$

genügen müssen, so daß es nur endlichviele gibt. Die Anzahl aller Klassen $C_{f_0 f_1 \dots f_t}$ ist endlich; ihre Vereinigungsmenge enthält folglich auch nur endlichviele Elemente; das war aber gerade zu zeigen.

III.

13. Bedeute

$$F(x,y) = a_0 x^n + a_1 x^{n-1} y + \dots + a_n y^n$$

eine irreduzible Binärform mit ganzen rationalen Koeffizienten vom Grad $n \geqq 3$. Wird zu den früher eingeführten Körpern $R, R_1, R_2, \dots, R_t$ der reellen bzw. der P_τ-adischen Zahlen ($\tau = 1, 2, \dots, t$) übergegangen, so zerfällt diese Form unter Umständen. Das Polynom

$$f(x) = F(x, 1)$$

möge im Körper R der reellen Zahlen die Nullstellen

$$\zeta, \zeta', \dots, \zeta^{(\nu-1)}$$

und für $\tau = 1, 2, \dots, t$ im Körper R_τ der P_τ-adischen Zahlen die Nullstellen

$$\zeta_\tau, \zeta'_\tau, \dots, \zeta_\tau^{(\nu_\tau - 1)}$$

haben; die Anzahlen ν und ν_τ können dabei irgendwelche der Werte

$$0, 1, 2, \dots, n$$

annehmen. Dann ist

$$F(x,y) = (x - \zeta y)(x - \zeta' y) \dots (x - \zeta^{(\nu-1)} y)\, G(x,y),$$
$$F(x,y) = (x - \zeta_\tau y)(x - \zeta'_\tau y) \dots (x - \zeta_\tau^{(\nu_\tau - 1)} y)\, G_\tau(x,y),$$

und zwar besitzen die Formen $G(x,y)$ bzw. $G_\tau(x,y)$ Koeffizienten aus R bzw. R_τ und lassen sich nur in nichtlineare Faktoren zerlegen, wenn sie reduzibel sind[4]).

14. Aus der Zerlegung von $F(x,y)$ in R folgt durch Differenzieren nach x:

$$\frac{F'(x,y)}{F(x,y)} = \frac{1}{x - \zeta y} + \frac{1}{x - \zeta' y} + \dots + \frac{1}{x - \zeta^{(\nu-1)} y} + \frac{G'(x,y)}{G(x,y)}.$$

(Der Index bedeute die partielle Ableitung nach x.) Da in dieser Identität rechts höchstens $n+1$ Summanden auftreten, so folgt aus ihr die Ungleichung

$$|F(x,y)| \geqq \frac{|F'(x,y)|}{n+1} \min\left(|x - \zeta y|, |x - \zeta' y|, \dots, |x - \zeta^{(\nu-1)} y|, \left|\frac{G(x,y)}{G'(x,y)}\right|\right).$$

Nach Annahme hat das Polynom $G(x,1)$ keine reelle Nullstelle und ist auch $G(1,0) \neq 0$; also ist die untere Schranke

$$\min_{\max(|x|,|y|)=1} (|G(x,y)|) = c^{\mathrm{I}}$$

positiv und demnach wegen der Homogenität

$$|G(x,y)| \geqq c^{\mathrm{I}} \max(|x|, |y|)^{n-\nu}.$$

---

[4]) Offenbar ist die Diskriminante von $F(x,y)$ nicht Null; da die Diskriminanten von $G(x,y)$ bzw. $G_\tau(x,y)$ hierin aufgehen, so können auch sie nicht verschwinden.

Weil $G'(x, y)$ ferner homogen von der Dimension $n - \nu - 1$ ist, so gibt es eine positive Zahl c^{II}, so daß für alle x und y

$$|G'(x,y)| \leqq c^{II} \max(|x|, |y|)^{n-\nu-1}$$

ist. Also ist stets

$$\left|\frac{G(x,y)}{G'(x,y)}\right| \geqq \frac{c^I}{c^{II}} \max(|x|, |y|).$$

Nach Voraussetzung ist $F(x, y)$ irreduzibel; somit ist seine Diskriminante von Null verschieden und es gibt je zwei Binärformen

$$H(x,y), \quad K(x,y)$$

der Dimension $n-2$ und

$$H_1(x,y), \quad K_1(x,y)$$

der Dimensionen $n-1$ mit rationalen Koeffizienten, so daß identisch

$$F(x,y)\,H(x,y) + F'(x,y)\,H_1(x,y) = x^{2n-2},$$
$$F(x,y)\,K(x,y) + F'(x,y)\,K_1(x,y) = y^{2n-2}$$

gilt. Da es sich um Formen handelt, so gibt es zwei positive Zahlen c^{III}, c^{IV}, so daß für alle x und y die Ungleichungen

$$|H(x,y)| \leqq c^{III} \max(|x|, |y|)^{n-2}, \quad |K(x,y)| \leqq c^{III} \max(|x|, |y|)^{n-2},$$
$$|H_1(x,y)| \leqq c^{IV} \max(|x|, |y|)^{n-1}, \quad |K_1(x,y)| \leqq c^{IV} \max(|x|, |y|)^{n-1}$$

bestehen. Seien jetzt x und y nicht beide gleich Null; wenn dann von den beiden letzten Identitäten diejenige mit absolut möglichst großer rechter Seite berücksichtigt wird, so ergibt sich, daß entweder

$$|F(x,y)| \geqq \frac{1}{2\,c^{III}} \max(|x|, |y|)^n$$

oder

$$|F'(x,y)| \geqq \frac{1}{2\,c^{IV}} \max(|x|, |y|)^{n-1}$$

sein muß.

Im letzteren Fall besteht wegen

$$|F(x,y)| \geqq \frac{|F'(x,y)|}{n+1} \min\left(|x-\zeta y|, |x-\zeta' y|, \ldots, |x-\zeta^{(\nu-1)} y|, \left|\frac{G(x,y)}{G'(x,y)}\right|\right)$$

und

$$\left|\frac{G(x,y)}{G'(x,y)}\right| \geqq \frac{c^I}{c^{II}} \max(|x|, |y|)$$

demnach die Ungleichung

$$|F(x,y)|$$
$$\geqq \frac{\max(|x|, |y|)^{n-1}}{2(n+1)\,c^{IV}} \min\left(|x-\zeta y|, |x-\zeta' y|, \ldots, |x-\zeta^{(\nu-1)} y|, \frac{c^I}{c^{II}} \max(|x|, |y|)\right).$$

Sei zur Abkürzung

$$c^\nu = \max(|\zeta|, |\zeta'|, \ldots, |\zeta^{(\nu-1)}|)$$

gesetzt. Für $|x| \geqq (c^\nu + 1)|y|$ ist dann offenbar

$$|x - \zeta^{(\lambda)} y| \geqq \max\left(\frac{|x|}{c^\nu + 1}, |y|\right) \geqq \frac{1}{c^\nu + 1} \max(|x|, |y|) \qquad (\lambda = 0, 1, \ldots, \nu - 1),$$

für $|x| < (c^\nu + 1)|y|$

$$|x - \zeta^{(\lambda)} y| = \left|\frac{x}{y} - \zeta^{(\lambda)}\right| |y| \geqq \frac{1}{c^\nu + 1} \max(|x|, |y|) \left|\frac{x}{y} - \zeta^{(\lambda)}\right| \quad (\lambda = 0, 1, \ldots, \nu - 1).$$

Faßt man alle diese Abschätzungen zusammen, so ergibt sich demnach die Existenz einer positiven Konstanten c, so daß für alle Werte von x und y

$$|F(x, y)| \geqq c \max(|x|, |y|)^n \min\left(\left|\frac{x}{y} - \zeta\right|, \left|\frac{x}{y} - \zeta'\right|, \ldots, \left|\frac{x}{y} - \zeta^{(\nu-1)}\right|, 1\right)$$

ist. Hieraus folgt insbesondere für teilerfremde ganze rationale Zahlen p und q die Abschätzung

$$|F(p, q)| \geqq c\,|p, q|^n \min\left(\left|\frac{p}{q} - \zeta\right|, \left|\frac{p}{q} - \zeta'\right|, \ldots, \left|\frac{p}{q} - \zeta^{(\nu-1)}\right|, 1\right).$$

15. Die Entwicklungen in 13. lassen sich auf die Zerlegung von $F(x, y)$ in den Körpern R_τ übertragen. Zuvor werde ein einfacher Stetigkeitssatz bewiesen[5]):

Hilfssatz 4. *Ein Polynom $g(x)$ mit P_τ-adischen Koeffizienten, nichtverschwindender Diskriminante und ohne Nullstellen im Körper der P_τ-adischen Zahlen besitzt eine positive untere Schranke*

$$\min(|g(x)|_{P_\tau}) = \gamma,$$

wenn für x alle P_τ-adischen Zahlen eingesetzt werden. Sind speziell alle Koeffizienten von $g(x)$ ganz P_τ-adisch, der höchste Koeffizient gleich Eins und die Diskriminante eine P_τ-adische Einheit, so ist für alle P_τ-adischen Zahlen

$$|g(x)|_{P_\tau} \geqq 1.$$

Beweis. Ohne Einschränkung darf angenommen werden, daß der höchste Koeffizient von $g(x)$ gleich Eins ist; das Polynom laute ausgeschrieben

$$g(x) = x^m + b_1 x^{m-1} + b_2 x^{m-2} + \ldots + b_m$$

und es werde zur Abkürzung

$$b = \max(1, |b_1|_{P_\tau}, |b_2|_{P_\tau}, \ldots, |b_m|_{P_\tau})$$

gesetzt. Für $|x|_{P_\tau} > b$ ist offenbar

$$|g(x)|_{P_\tau} = |x^m|_{P_\tau} > b^m \geqq 1;$$

wir beschränken uns daher von jetzt ab auf x-Werte mit

$$|x|_{P_\tau} \leqq b.$$

---

[5]) Dieser Satz und sein Beweis stammt von Hensel; in etwas anderer Bezeichnung steht er in dem Buch (6), S. 66—76.

Da die P_τ-adischen Werte der Koeffizienten der Polynome

$$\frac{g^{(l)}(x)}{l!} \qquad (l = 2, 3, \ldots, m)$$

alle höchstens gleich b sind, so wird folglich

$$\left|\frac{g^{(l)}(x)}{l!}\right|_{P_\tau} \leqq b \cdot b^{m-l} \leqq b^{m-1} \qquad (l = 2, 3, \ldots, m).$$

Die Diskriminante von $g(x)$

$$D = \begin{vmatrix} 1, & b_1, & b_2, & \ldots, & b_m & & & \\ & \ddots & & & & \ddots & & \\ & & \ddots & & & & \ddots & \\ & & & 1, & b_1, & b_2, & \ldots, & b_m \\ m, & (m-1)b_1, & (m-2)b_2, & \ldots, & 1 \cdot b_{m-1} & & & \\ & \ddots & & & & \ddots & & \\ & & \ddots & & & & \ddots & \\ & & & m, & (m-1)b_1, & (m-2)b_2, & \ldots, & 1 \cdot b_{m-1} \end{vmatrix}$$

ist nach Voraussetzung ungleich Null. Setzt man

$$h(x) = \begin{vmatrix} x^{m-2}, & b_1, & b_2, & \ldots, & b_m & & & \\ x^{m-3}, & \ddots & & & & \ddots & & \\ & \ddots & & & & & \ddots & \\ & & \ddots & & & & & \ddots \\ 1, & \ldots, & 1, & b_1, & b_2, & \ldots, & b_m & \\ 0, & (m-1)b_1, & (m-2)b_2, & \ldots, & 1 \cdot b_{m-1} & & & \\ 0 & \ddots & & & & \ddots & & \\ \vdots & & \ddots & & & & \ddots & \\ 0, & \ldots, & & m, & (m-1)b_1, & (m-2)b_2, & \ldots, & 1 \cdot b_{m-1} \end{vmatrix},$$

$$k(x) = \begin{vmatrix} 0, & b_1, & b_2, & \ldots, & b_m & & & \\ 0 & \ddots & & & & \ddots & & \\ & \ddots & & & & & \ddots & \\ & & \ddots & & & & & \ddots \\ 0, & \ldots, & 1, & b_1, & b_2, & \ldots, & b_m & \\ x^{m-1}, & (m-1)b_1, & (m-2)b_2, & \ldots, & 1 \cdot b_{m-1} & & & \\ x^{m-2} & \ddots & & & & \ddots & & \\ \vdots & & \ddots & & & & \ddots & \\ 1, & \ldots, & & m, & (m-1)b_1, & (m-2)b_2, & \ldots, & 1 \cdot b_{m-1} \end{vmatrix},$$

so besteht die Identität

$$g(x)\,h(x) + g'(x)\,k(x) = D.$$

$h(x)$ ist ein Polynom vom Grad $m-2$ und der P_τ-adische Wert seiner Koeffizienten ist höchstens gleich b^{2m-2}, demnach

$$|h(x)|_{P_\tau} \leqq b^{2m-2} \cdot b^{m-2} \leqq b^{3(m-1)}.$$

$k(x)$ ist ein Polynom vom Grad $m-1$ und der P_τ-adische Wert seiner Koeffizienten höchstens gleich b^{2m-2}, demnach

$$|k(x)|_{P_\tau} \leqq b^{2m-2} \cdot b^{m-1} = b^{3(m-1)}.$$

Aus

$$g'(x) = \frac{D - g(x)\,h(x)}{k(x)}$$

folgt also, daß entweder

$$|g(x)|_{P_\tau} \geqq d\,b^{-3(m-1)}$$

oder

$$|g(x)|_{P_\tau} < d\,b^{-3(m-1)}, \qquad |g'(x)|_{P_\tau} \geqq d\,b^{-3(m-1)}$$

sein muß; dabei ist

$$d = |D|_{P_\tau}$$

gesetzt.

Jetzt kann gezeigt werden, daß $|g(x)|_{P_\tau}$ nur dann in P_τ-adischen Punkten x beliebig klein sein kann, wenn das Polynom $g(x)$ eine P_τ-adische Nullstelle besitzt. Sei in der Tat ξ eine spezielle P_τ-adische Zahl mit

$$|\xi|_{P_\tau} \leqq b, \qquad |g(\xi)|_{P_\tau} < \min\left(\frac{d^2}{b^{7(m-1)}},\ \frac{d}{b^{3(m-1)}}\right)$$

und δ die P_τ-adische Zahl

$$\delta = -\frac{g(\xi)}{g'(\xi)};$$

es ist alsdann

$$|\delta|_{P_\tau} \leqq |g(\xi)|_{P_\tau} \cdot \frac{b^{3(m-1)}}{d} < 1,$$

ferner

$$\left|\sum_{l=2}^{m} \frac{g^{(l)}(\xi)}{l!}\,\delta^l\right|_{P_\tau} \leqq \left|\frac{g''(\xi)}{2}\,\delta^2\right|_{P_\tau}$$

$$\leqq \left|\frac{g''(\xi)}{2}\,\frac{g(\xi)}{g'(\xi)^2}\right|_{P_\tau} |g(\xi)|_{P_\tau} < b^{m-1}\,\frac{\frac{d^2}{b^{7(m-1)}}}{\frac{d^2}{b^{6(m-1)}}}\,|g(\xi)|_{P_\tau} = |g(\xi)|_{P_\tau}.$$

Folglich wird

$$|g(\xi+\delta)|_{P_\tau} < |g(\xi)|_{P_\tau},$$

denn es ist

$$g(\xi+\delta) = g(\xi) + g'(\xi)\,\delta + \sum_{l=2}^{m} \frac{g^{(l)}(\xi)}{l!}\,\delta^l = \sum_{l=2}^{m} \frac{g^{(l)}(\xi)}{l!}\,\delta^l.$$

Es werde jetzt der Reihe nach gesetzt:

$$\xi_1 = \xi + \delta, \qquad \delta_1 = -\frac{g(\xi_1)}{g'(\xi_1)}, \qquad \xi_2 = \xi_1 + \delta_1,$$
$$\delta_2 = -\frac{g(\xi_2)}{g'(\xi_2)}, \qquad \xi_3 = \xi_2 + \delta_2,$$
$$\delta_3 = -\frac{g(\xi_3)}{g'(\xi_3)}, \qquad \xi_4 = \xi_3 + \delta_3$$

usw. Indem man die letzten Abschätzungen fortwährend wiederholt, folgt hintereinander:

$$|\xi_1|_{P_\tau} \leqq b, \quad |g(\xi_1)|_{P_\tau} < |g(\xi)|_{P_\tau} < \min\left(\frac{d^2}{b^{7(m-1)}}, \frac{d}{b^{3(m-1)}}\right),$$
$$|\delta_1|_{P_\tau} \leqq \frac{b^{3(m-1)}}{d}\,|g(\xi_1)|_{P_\tau},$$
$$|\xi_2|_{P_\tau} \leqq b, \quad |g(\xi_2)|_{P_\tau} < |g(\xi_1)|_{P_\tau} < \min\left(\frac{d^2}{b^{7(m-1)}}, \frac{d}{b^{3(m-1)}}\right),$$
$$|\delta_2|_{P_\tau} \leqq \frac{b^{3(m-1)}}{d}\,|g(\xi_2)|_{P_\tau},$$
$$|\xi_3|_{P_\tau} \leqq b, \quad |g(\xi_3)|_{P_\tau} < |g(\xi_2)|_{P_\tau} < \min\left(\frac{d^2}{b^{7(m-1)}}, \frac{d}{b^{3(m-1)}}\right),$$
$$|\delta_3|_{P_\tau} \leqq \frac{b^{3(m-1)}}{d}\,|g(\xi_3)|_{P_\tau}$$

usw., also nach den Stetigkeitsgesetzen des P_τ-adischen Körpers:

$$\lim_{h\to\infty} |g(\xi_h)|_{P_\tau} = 0, \quad \lim_{h\to\infty} |\xi_{h+1} - \xi_h|_{P_\tau} = \lim_{h\to\infty} |\delta_h|_{P_\tau} = 0.$$

Die zweite Gleichung zeigt, daß die Zahlen ξ_h gegen einen Grenzwert ξ^* konvergieren; dieser Grenzwert ist nach der ersten Gleichung eine Nullstelle des Polynoms $g(x)$.

Wenn $g(x)$ keine Nullstelle besitzen soll, so muß demnach für jede P_τ-adische Zahl x

$$|g(x)|_{P_\tau} \geqq \min\left(b^m, \frac{d^2}{b^{7(m-1)}}, \frac{d}{b^{3(m-1)}}\right)$$

sein; der erste Teil von Hilfssatz 4 ist damit bewiesen. Die Voraussetzungen des zweiten Teiles verlangen offenbar

$$b = 1, \quad d = 1,$$

und dann folgt

$$|g(x)|_{P_\tau} \geqq 1,$$

so daß auch der zweite Teil bewiesen ist.

16. Aus der Zerlegung von $F(x, y)$ in R_τ ergibt sich durch Differenzieren nach x

$$\frac{F'(x,y)}{F(x,y)} = \frac{1}{x - y\zeta_\tau} + \frac{1}{x - y\zeta_\tau'} + \cdots + \frac{1}{x - y\zeta_\tau^{(\nu_\tau - 1)}} + \frac{G_\tau'(x,y)}{G_\tau(x,y)}$$
$$(\tau = 1, 2, \ldots, t)$$

und durch Übergang zu den P_τ-adischen Werten

$$|F(x,y)|_{P_\tau} \geqq |F'(x,y)|_{P_\tau}$$
$$\times \min\left(|x-\zeta_\tau y|_{P_\tau},\ |x-\zeta_\tau' y|_{P_\tau},\ \ldots,\ |x-\zeta_\tau^{(\nu_\tau-1)} y|_{P_\tau},\ \left|\frac{G_\tau(x,y)}{G_\tau'(x,y)}\right|_{P_\tau}\right)$$
$$(\tau = 1, 2, \ldots, t).$$

Jetzt werde für x und y zwei teilerfremde ganze rationale Zahlen p und q eingesetzt. Ist das Maximum der P_τ-adischen Werte der Koeffizienten von $G_\tau(x,y)$ gleich b, so gilt offenbar

$$|G_\tau'(p,q)|_{P_\tau} \leqq b.$$

Ferner hat keines der beiden Polynome

$$G_\tau(x,1) \quad \text{und} \quad G_\tau(1,x)$$

eine P_τ-adische Nullstelle; also gibt es nach dem vorigen Hilfssatz eine positive Zahl b', so daß für jede P_τ-adische Zahl x

$$|G_\tau(x,1)|_{P_\tau} \geqq b', \qquad |G_\tau(1,x)|_{P_\tau} \geqq b'$$

ist. Wegen der Homogenität von $G(x,y)$ folgt hieraus

$$|G_\tau(p,q)|_{P_\tau} = \left|G_\tau\left(\frac{p}{q},1\right) q^{n-\nu_\tau}\right|_{P_\tau} \geqq b' \, |q^{n-\nu_\tau}|_{P_\tau},$$
$$|G_\tau(p,q)|_{P_\tau} = \left|G_\tau\left(1,\frac{q}{p}\right) p^{n-\nu_\tau}\right|_{P_\tau} \geqq b' \, |p^{n-\nu_\tau}|_{P_\tau},$$

und da mindestens eine der beiden Zahlen p und q zu P_τ teilerfremd ist:

$$|G_\tau(p,q)| \geqq b', \qquad \left|\frac{G_\tau(p,q)}{G_\tau'(p,q)}\right|_{P_\tau} \geqq \frac{b'}{b}.$$

Da die Form $F(x,y)$ irreduzibel ist, so ist ihre Diskriminante Δ eine ganze rationale und von Null verschiedene Zahl. Ähnlich wie in 14. lassen sich zwei Binärformen mit ganzen rationalen Koeffizienten

$$H_1(x,y) \text{ vom Grad } n-2,$$
$$K_1(x,y) \text{ vom Grad } n-1$$

und zwei Binärformen mit ganzen rationalen Koeffizienten

$$H_2(x,y) \text{ vom Grad } n-2,$$
$$K_2(x,y) \text{ vom Grad } n-1$$

bestimmen, so daß identisch

$$F(x,y)\,H_1(x,y) + F'(x,y)\,K_1(x,y) = \Delta\, x^{2n-2},$$
$$F(x,y)\,H_2(x,y) + F'(x,y)\,K_2(x,y) = \Delta\, y^{2n-2}$$

ist; setzt man hierin p, q für x, y ein und beachtet wieder, daß mindestens eine dieser beiden Zahlen zu P_τ teilerfremd ist, so folgt durch Übergang zu den P_τ-adischen Werten

$$\max\left(|F(p,q)|_{P_\tau},\ |F'(p,q)|_{P_\tau}\right) \geqq |\Delta|_{P_\tau}.$$

Für

$$|F(p,q)|_{P_\tau} < |\Delta|_{P_\tau}$$

folgt daraus

$$|F'(p, q)|_{P_\tau} \geqq |\Delta|_{P_\tau},$$

so daß man zu der Ungleichung

$$|F(p, q)|_{P_\tau} \geqq |\Delta|_{P_\tau} \min\left(|p - q\zeta_\tau|_{P_\tau}, |p - q\zeta'_\tau|_{P_\tau}, \ldots, |p - q\zeta_\tau^{(\nu_\tau - 1)}|_{P_\tau}, \frac{b'}{b}\right)$$

gelangt. Setzt man

$$c_\tau = |\Delta|_{P_\tau} \min\left(1, \frac{b'}{b}\right),$$

so gilt die Ungleichung

$$|F(p, q)|_{P_\tau} \geqq c_\tau \min\left(|p - q\zeta_\tau|_{P_\tau}, |p - q\zeta'_\tau|_{P_\tau}, \ldots, |p - q\zeta_\tau^{(\nu_\tau - 1)}|_{P_\tau}, 1\right) \quad (\tau = 1, 2, \ldots, t)$$

auch noch für

$$|F(p, q)|_{P_\tau} \geqq |\Delta|_{P_\tau}$$

und also für alle Paare p, q. Diese Ungleichung für $|F(p, q)|_{P_\tau}$ ist fast genau von derselben Gestalt wie die Ungleichung für $|F(p, q)|$ in 13.

Wenn speziell die Primzahl P_τ genügend groß ist, so daß sie weder in der Diskriminante Δ von $F(x, y)$, noch in dem höchsten Koeffizienten $F(1, 0)$ dieser Form aufgeht, so ist

$$c_\tau = 1.$$

Denn man hat erstens $|\Delta|_{P_\tau} = 1$. Zweitens sind die P_τ-adischen Zahlen

$$\zeta_\tau, \zeta'_\tau, \ldots, \zeta_\tau^{(\nu_\tau - 1)}$$

alle ganz, denn die Koeffizienten ihrer Gleichung

$$\frac{1}{a_0} F(x, 1) \equiv x^n + \frac{a_1}{a_0} x^{n-1} + \ldots + \frac{a_n}{a_0} = 0$$

sind ganz P_τ-adisch. Also hat auch die Form

$$\frac{1}{a_0} G(x, y) = \frac{\frac{1}{a_0} F(x, y)}{(x - \zeta_\tau y)(x - \zeta'_\tau y) \ldots (x - \zeta_\tau^{(\nu_\tau - 1)} y)}$$

ganze P_τ-adische Koeffizienten und den höchsten Koeffizienten gleich Eins, so daß die Zahl $b = 1$ ist. Drittens ist die Diskriminante dieser Form eine ganze P_τ-adische Zahl und geht in Δ auf: also muß sie eine P_τ-adische Einheit sein. Es kann also die zweite Hälfte von Hilfssatz 4 herangezogen werden, so daß $b' = 1$ folgt. Das ergibt aber gerade

$$c_\tau = |\Delta|_{P_\tau} \min\left(1, \frac{b'}{b}\right) = 1.$$

17. Nach den Ergebnissen von 13. und 16. gilt für teilerfremde ganze rationale Zahlen p und q:

$$|F(p, q)| \geqq c\,|p, q|^n \min\left(\left|\frac{p}{q} - \zeta\right|, \left|\frac{p}{q} - \zeta'\right|, \ldots, \left|\frac{p}{q} - \zeta^{(\nu-1)}\right|, 1\right),$$

$$|F(p, q)|_{P_\tau} \geqq c_\tau \min\left(|p - q\zeta_\tau|_{P_\tau} |p - q\zeta'_\tau|_{P_\tau}, \ldots, |p - q\zeta_\tau^{(\nu_\tau - 1)}|_{P_\tau}, 1\right) \quad (\tau = 1, 2, \ldots, t).$$

Dabei sind $c, c_1, c_2, \ldots, c_t$ positive Konstante, die außer von der Form $F(x, y)$ nur von der Körpern $R, R_1, R_2, \ldots, R_t$ abhängen; es ist ferner $c_\tau = 1$, sobald die Grundzahl P_τ des Körpers R_τ eine gewisse Größe überschreitet. Also bleibt das Produkt

$$c\, c_1\, c_2 \ldots c_t$$

oberhalb einer positiven Schranke C, die allein von der Form $F(x, y)$, nicht aber von den Körpern $R, R_1, R_2, \ldots, R_t$, d. h. von den Primzahlen $P_1, P_2, \ldots, P_t$ abhängt. Multipliziert man die obigen Ungleichungen, so ist offenbar

$$Q(p, q) = \Big(\prod_{\tau=1}^{t} |F(p, q)|_{P_\tau} \Big)^{-1}$$

gerade gleich dem größten Potenzprodukt der Primzahlen P_τ, das in $F(p, q)$ aufgeht; also kommt man zu folgendem Hilfssatz:

Hilfssatz 5. *Bedeute*[6]):

$F(x, y)$ *eine irreduzible Binärform mit ganzen rationalen Koeffizienten vom Grad* $n \geqq 3$,

$P_1, P_2, \ldots, P_t$ *endlichviele verschiedene Primzahlen,*

$\zeta, \zeta', \ldots, \zeta^{(\nu-1)}$ *die sämtlichen reellen Nullstellen von* $F(x, 1)$,

$\zeta_\tau, \zeta'_\tau, \ldots, \zeta_\tau^{(\nu_\tau - 1)}$ *für* $\tau = 1, 2, \ldots, t$ *die sämtlichen* P_τ*-adischen Nullstellen von* $F(x, 1)$,

p *und* q *zwei beliebige teilerfremde ganze rationale Zahlen* $(q \neq 0)$,

$Q(p, q)$ *das größte Potenzprodukt der Primzahlen* $P_1, P_2, \ldots, P_t$, *das in* $F(p, q)$ *aufgeht.*

Dann gibt es eine positive Konstante C, *die allein von* $F(x, y)$, *nicht aber von den Primzahlen* P_τ *abhängt, so daß*

$$\frac{|F(p, q|}{Q(p, q)} \geqq C\, |p, q|^n \min\left(\left| \frac{p}{q} - \zeta \right|, \left| \frac{p}{q} - \zeta' \right|, \ldots, \left| \frac{p}{q} - \zeta^{(\nu-1)} \right|, 1 \right)$$

$$\times \prod_{\tau=1}^{t} \min\left(|p - q\zeta_\tau|_{P_\tau}, |p - q\zeta'_\tau|_{P_\tau}, \ldots, |p - q\zeta_\tau^{(\nu_\tau - 1)}|_{P_\tau}, 1 \right)$$

ist.

18. Der letzte Hilfssatz führt zusammen mit Satz 1 zu folgendem Ergebnis:

Satz 2. *Bedeute* $F(x, y)$ *eine irreduzible Binärform mit ganzen rationalen Koeffizienten vom Grad* $n \geqq 3$, p *und* q *zwei teilerfremde ganze rationale Zahlen,* $P_1, P_2, \ldots, P_t$ *endlichviele verschiedene Primzahlen und* $Q(p, q)$ *das größte Potenzprodukt der Primzahlen* P_τ, *das in* $F(p, q)$ *aufgeht.*

[6]) Im folgenden wird dieser Satz nur für $n \geqq 3$ gebraucht, jedoch bleibt er und sein Beweis offenbar auch für $n < 3$ richtig.

Genügt dann die Konstante β der Ungleichung

$$\beta > \min_{s=1,2,\ldots,n-1} \left(\frac{n}{s+1} + s\right),$$

so besitzt die Ungleichung

$$\frac{|F(p,q)|}{Q(p,q)} \leqq |p, q|^{n-\beta}$$

höchstens endlichviele Lösungspaare p, q.

Beweis. Nach dem letzten Hilfssatz ist

$$\frac{|F(p,q)|}{Q(p,q)} \geqq C\,|p, q|^n Z_0 \prod_{\tau=1}^{t} Z_\tau,$$

wenn

$$Z_0 = \min\left(\left|\frac{p}{q} - \zeta\right|, \left|\frac{p}{q} - \zeta'\right|, \ldots, \left|\frac{p}{q} - \zeta^{(\nu-1)}\right|, 1\right),$$

$$Z_\tau = \min\left(|p - q\zeta_\tau|_{P_\tau}, |p - q\zeta_\tau'|_{P_\tau}, \ldots, |p - q\zeta_\tau^{(\nu_\tau - 1)}|_{P_\tau}, 1\right) \quad (\tau = 1, 2, \ldots, t)$$

gesetzt wird. Seien jetzt von den Zahlen

$$\nu_0 = \nu,\ \nu_1,\ \nu_2, \ldots,\ \nu_t$$

etwa

$$\nu_{\mu_1},\ \nu_{\mu_2},\ \ldots,\ \nu_{\mu_u}$$

von Null verschieden, alle anderen aber gleich Null; dann ist

$$\frac{|F(p,q)|}{Q(p,q)} \geqq C\,|p,q|^n Z_{\mu_1} Z_{\mu_2} \ldots Z_{\mu_u}.$$

Es werde

$$k = \max\left(1, \frac{1}{C}\right)$$

gesetzt und für den Augenblick unter

$$|p - q\zeta_0^{(\lambda)}|_{P_0}$$

die Zahl

$$\left|\frac{p}{q} - \zeta^{(\lambda)}\right|$$

verstanden, wenn unter den Indizes $\mu_1, \mu_2, \ldots, \mu_u$ auch die Null zufälligerweise vorkommt.

Sind jetzt $\lambda_1, \lambda_2, \ldots, \lambda_u$ irgend u ganze rationale Zahlen mit

$$0 \leqq \lambda_1 \leqq \nu_{\mu_1} - 1; \quad 0 \leqq \lambda_2 \leqq \nu_{\mu_2} - 1; \quad \ldots; \quad 0 \leqq \lambda_u \leqq \nu_{\mu_u} - 1,$$

so besitzt nach Satz 1 die Ungleichung

$$\prod_{x=1}^{u} \min\left(|p - q\zeta_{\mu_x}^{(\lambda_x)}|_{P_{\mu_x}}, 1\right) \leq k\,|p,q|^{-\beta}$$

höchstens endlichviele Lösungen. Offenbar treten höchstens

$$n^{t+1}$$

verschiedene solche Ungleichungen auf, wenn für $\lambda_1, \lambda_2, \ldots, \lambda_u$ alle zulässigen Zahlen eingesetzt werden. Andererseits muß jede Lösung von

$$\frac{|F(p,q)|}{Q(p,q)} \leqq |p,q|^{n-\beta}$$

einer dieser Ungleichungen genügen; daraus folgt die Behauptung.

19. Einige Folgerungen, die sich aus dem letzten Satz ziehen lassen, seien hier aufgeführt:

Folgerung 1. *Bedeutet $F(x,y)$ eine irreduzible Binärform mit ganzen rationalen Koeffizienten vom Grad $n \geqq 3$, p und q zwei teilerfremde Zahlen und $P(p,q)$ die größte Primzahl, die in $F(p,q)$ aufgeht, so strebt gleichzeitig mit $|p,q|$ auch $P(p,q)$ über alle Grenzen.*

Denn wäre diese Behauptung falsch, so gäbe es endlichviele Primzahlen $P_1, P_2, \ldots, P_t$ und eine unendliche Folge von Paaren teilerfremder ganzer rationaler Zahlen p, q, für die $F(p,q)$ nur aus diesen Primzahlen zusammengesetzt wäre. Man hätte also in der bisherigen Bezeichnung

$$|F(p,q)| = Q(p,q)$$

und das widerspricht der Ungleichung

$$\frac{|F(p,q)|}{Q(p,q)} > |p,q|^{n-\beta},$$

die nach Satz 1 von einer Stelle an gilt und in der $\beta < n$ angenommen werden kann.

20. Folgerung 2. *Seien M_1, M_2, M_3 drei endliche Mengen von Primzahlen, deren Vereinigungsmenge aus lauter verschiedenen Primzahlen besteht. Wenn dann die natürliche Zahl Z_1 nur Primteiler aus M_1, die natürliche Zahl Z_2 nur Primteiler aus M_2 und die natürliche Zahl Z_3 nur Primteiler aus M_3 enthält, so besitzt die Gleichung*

$$Z_1 + Z_2 = Z_3$$

höchstens endlichviele Lösungen[7]).

Denn bestehe etwa die Menge M_1 aus den Primzahlen $P_1, P_2, \ldots, P_t$, die Menge M_2 aus den Primzahlen $Q_1, Q_2, \ldots, Q_u$ und die Menge M_3 aus den Primzahlen $R_1, R_2, \ldots, R_v$. Jeder Lösung der Gleichung

$$P_1^{p_1} P_2^{p_2} \ldots P_t^{p_t} + Q_1^{q_1} Q_2^{q_2} \ldots Q_u^{q_u} = R_1^{r_1} R_2^{r_2} \ldots R_v^{r_v}$$

in nichtnegativen ganzen rationalen Zahlen

$$p_1, p_2, \ldots, p_t; \quad q_1, q_2, \ldots, q_u; \quad r_1, r_2, \ldots, r_v$$

ordne man die vier natürlichen Zahlen

$$p = P_1^{[p_1/5]} P_2^{[p_2/5]} \ldots P_t^{[p_t/5]}, \quad q = Q_1^{[q_1/5]} Q_2^{[q_2/5]} \ldots Q_u^{[q_u/5]},$$

$$a = P_1^{p_1 - 5[p_1/5]} P_2^{p_2 - 5[p_2/5]} \ldots P_t^{p_t - 5[p_t/5]},$$

$$b = Q_1^{q_1 - 5[q_1/5]} Q_2^{q_2 - 5[q_2/5]} \ldots Q_u^{q_u - 5[q_u/5]}$$

[7]) Die Einschränkung, daß Z_1, Z_2, Z_3 *positive* ganze rationale Zahlen sind, ist offenbar überflüssig.

zu, so daß

$$a p^5 + b q^5 = R_1^{r_1} R_2^{r_2} \dots R_v^{r_v}$$

ist. Offenbar sind p und q teilerfremd. Dasselbe gilt für a und b; diese beiden Zahlen sind ferner höchstens endlichvieler verschiedener Wertepaare fähig. Die zugeordnete Binärform fünften Grades

$$F_{a,b}(x, y) = a x^5 + b y^5$$

ist im Körper der rationalen Zahlen irreduzibel, außer im Falle

$$a = b = 1,$$

wo die Zerlegung

$$F_{1,1}(x, y) = x^5 + y^5 = (x + y) G(x, y),$$
$$G(x, y) = x^4 - x^3 y + x^2 y^2 - x y^3 + y^4$$

besteht; der Faktor $G(x, y)$ ist aber wieder irreduzibel. Sind jetzt p und q irgendwelche teilerfremde Zahlen und wächst $|p, q|$ über alle Grenzen, so konvergiert nach Folgerung 1 auch der größte Primteiler von $F_{a,b}(p, q)$ bzw. von $G(p, q)$ gegen Unendlich. Die Gleichung

$$a p^5 + b q^5 = R_1^{r_1} R_2^{r_2} \dots R_v^{r_v}$$

läßt sich daher nur auf endlichviele Arten durch beliebige teilerfremde ganze rationale Zahlen befriedigen, erst recht daher nur endlichoft durch Zahlen der Mengen M_1 und M_2. Jede Lösung von

$$Z_1 + Z_2 = Z_3$$

gibt aber Anlaß zu der Lösung einer von endlichvielen Gleichungen dieser Gestalt; also hat diese Gleichung auch nur endlichviele Lösungen.

21. Folgerung 3. *Seien* $a_1, b_1, a_2, b_2, a_3, b_3$ *ganze rationale Zahlen mit*

$$(a_1, b_1) = 1, \quad (a_2, b_2) = 1, \quad (a_3, b_3) = 1,$$
$$\Delta_1 = a_2 b_3 - a_3 b_2 \neq 0, \quad \Delta_2 = a_3 b_1 - a_1 b_3 \neq 0, \quad \Delta_3 = a_1 b_2 - a_2 b_1 \neq 0.$$

Durchlaufen dann p *und* q *eine Folge teilerfremder ganzer rationaler Zahlen mit* $|p, q| \to \infty$, *so wächst der größte Primteiler von*

$$(a_1 p + b_1 q)(a_2 p + b_2 q)(a_3 p + b_3 q)$$

über alle Grenzen.

Beweis. Setzt man zur Abkürzung

$$L_1 = a_1 p + b_1 q, \quad L_2 = a_2 p + b_2 q, \quad L_3 = a_3 p + b_3 q,$$

so ist offenbar

$$\Delta_1 L_1 + \Delta_2 L_2 + \Delta_3 L_3 = 0,$$

also

$$\Delta_1 \Delta_2 \Delta_3 L_1 L_2 L_3 = - \Delta_1 L_1 \cdot \Delta_2 L_2 \cdot (\Delta_1 L_1 + \Delta_2 L_2).$$

Es werde

$$\Delta = (\Delta_1 L_1, \Delta_2 L_2)$$

gesetzt, so daß

$$\Delta \mid \Delta_1 \Delta_2 (L_1, L_2)$$

ist. Offenbar gilt aber

$$\Delta_3 p = -a_2 L_1 + a_1 L_2, \quad \Delta_3 q = b_2 L_1 - b_1 L_2,$$

wegen $(p, q) = 1$ also

$$(-a_2 L_1 + a_1 L_2,\ b_2 L_1 - b_1 L_2) = \Delta_3$$

und daher

$$(L_1, L_2) \mid \Delta_3, \quad \Delta \mid \Delta_1 \Delta_2 \Delta_3.$$

Die Zahl Δ ist demnach nur endlichvieler Werte fähig; zu gegebenen Werten der teilerfremden Zahlen

$$Z_1 = \frac{\Delta_1 L_1}{\Delta}, \quad Z_2 = \frac{\Delta_2 L_2}{\Delta}$$

können also nur endlichviele Wertepaare L_1, L_2 und folglich auch nur endlichviele Paare p, q mit $(p, q) = 1$ gehören, denn die letzteren sind durch Angabe von L_1, L_2 eindeutig bestimmt. Es werde jetzt angenommen, daß die Folgerung falsch sei, daß es also eine unendliche Folge von Paaren p, q mit $(p, q) = 1$ und $|p, q| \to \infty$ gibt, so daß der größte Primteiler von $L_1 L_2 L_3$ beschränkt bleibt. Dann zeigt die vorige Konstruktion, daß es auch eine unendliche Folge von Paaren ganzer rationaler teilerfremder Zahlen Z_1, Z_2 mit $\max(|Z_1|, |Z_2|) \to \infty$ gibt, für die der größte Primteiler von

$$Z_1 Z_2 (Z_1 + Z_2)$$

beschränkt ist. Offenbar ist nicht nur $(Z_1, Z_2) = 1$, sondern auch

$$(Z_1, Z_1 + Z_2) = 1, \quad (Z_2, Z_1 + Z_2) = 1.$$

Setzt man noch

$$Z_1 + Z_2 = Z_3,$$

so ist es also möglich, diese Gleichung unendlichoft zu befriedigen, indem man für Z_1 nur Primteiler einer endlichen Menge M_1, für Z_2 nur Primteiler einer endlichen Menge M_2, für Z_3 nur Primteiler einer endlichen Menge M_3 von Primzahlen zuläßt, wobei diese drei Mengen zu je zweien elementenfremd sind. Das ist aber nach Folgerung 2 unmöglich.

22. Folgerung 4. *Sei*

$$Q(x, y) = a_0 x^2 + a_1 x y + a_2 y^2$$

eine irreduzible quadratische Form,

$$L(x, y) = b_0 x + b_1 y$$

eine Linearform mit ganzen rationalen Koeffizienten. Durchläuft p, q eine unendliche Folge teilerfremder ganzer rationaler Zahlpaare mit $|p, q| \to \infty$, so wächst der größte Primteiler von

$$Q(p, q)\, L(p, q)$$

über alle Grenzen.

Folgerung 5. *Seien*

$$Q(x, y) = a_0 x^2 + a_1 x y + a_2 y^2, \quad Q^*(x, y) = b_0 x^2 + b_1 x y + b_2 y^2$$

zwei verschiedene irreduzible und zueinander teilerfremde quadratische Formen mit ganzen rationale Koeffizienten. Durchläuft p, q eine unendliche Folge teilerfremder ganzer rationaler Zahlpaare mit $|p, q| \to \infty$, so wächst der größte Primteiler von

$$Q(p, q)\, Q^*(p, q)$$

über alle Grenzen.

Beweis. In beiden Fällen kann man in gleicher Weise vorgehen. Wird

$$p' = \frac{a_0 b_0 p}{\Delta}, \quad q' = \frac{q}{\Delta}, \qquad \Delta = (a_0 b_0, q)$$

gesetzt, so ist offenbar

$$a_0^2 b_0^2 (a_0 p^2 + a_1 p q + a_2 q^2)(b_0 p + b_1 q) = \Delta^3 (p'^2 + a_1 b_0 p' q' + a_0 a_2 b_0^2 q'^2)(p' + a_0 b_1 q'),$$

$$a_0^3 b_0^3 (a_0 p^2 + a_1 p q + a_2 q^2)(b_0 p^2 + b_1 p q + b_2 q^2) = \Delta^4 (p'^2 + a_1 b_0 p' q' + a_0 a_2 b_0^2 q'^2)(p'^2 + a_0 b_1 p' q' + a_0^2 b_0 b_2 q'^2),$$

ferner Δ beschränkt, p' und q' teilerfremd und mit $|p, q|$ strebt auch $|p', q'|$ gegen Unendlich. Man kann sich also im ersten Fall auf die Untersuchung einer irreduziblen quadratischen Form und einer Linearform

$$Q(x, y) = x^2 + A_1 x y + A_2 y^2, \quad L(x, y) = x + B_1 y,$$

im zweiten Fall auf die zweier irreduzibler quadratischer Formen ohne gemeinsamen Faktor

$$Q(x, y) = x^2 + A_1 x y + A_2 y^2, \quad Q^*(x, y) = x^2 + B_1 x y + B_2 y^2$$

beschränken, die ganze rationale Koeffizienten und den höchsten Koeffizienten gleich Eins haben.

Sei jetzt $P_1, P_2, \ldots, P_t$ irgendeine endliche Menge von verschiedenen Primzahlen; p, q durchlaufe eine solche unendliche Folge von teilerfremden Zahlpaaren mit $|p, q| \to \infty$, so daß fortwährend

$$Q(p, q) = \mp P_1^{p_1} P_2^{p_2} \ldots P_t^{p_t}$$

ist, mit von p, q abhängigen nichtnegativen ganzen rationalen Zahlen $p_1, p_2, \ldots, p_t$.

Die Gleichung

$$Q(x, 1) \equiv x^2 + A_1 x + A_2 = 0$$

ist nach Voraussetzung irreduzibel; ihre beiden Wurzeln ζ, ζ' sind also konjugierte ganze algebraische Zahlen zweiten Grades und definieren einen quadratischen Zahlkörper K, dessen Basis etwa

$$1, \omega$$

ist, wobei ω eine ganze Zahl aus K bedeutet. Wir wollen konjugierte Ideale und Zahlen aus K durch einen Akzent unterscheiden.

Seien $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s$ die sämtlichen verschiedenen Primideale, die in $P_1, P_2, \ldots, P_t$ aufgehen; da in der Zerlegung

$$Q(p, q) = (p - q\zeta)(p - q\zeta')$$

die beiden Faktoren $p - q\zeta$ und $p - q\zeta'$ ganz algebraisch sind, so gestatten die zugehörigen Hauptideale eine Darstellung

$$(p - q\zeta) = \mathfrak{p}_1^{\pi_1}\mathfrak{p}_2^{\pi_2}\dots\mathfrak{p}_s^{\pi_s}, \quad (p - q\zeta') = \mathfrak{p}_1'^{\pi_1}\mathfrak{p}_2'^{\pi_2}\dots\mathfrak{p}_s'^{\pi_s}$$

mit nichtnegativen ganzen rationalen Exponenten $\pi_1, \pi_2, \dots, \pi_s$. Unter h die Klassenzahl von K verstanden, werde π_k zerlegt in der Form

$$\pi_k = 7h\lambda_k + \mu_k \qquad (k = 1, 2, \dots, s),$$

wobei die λ_k nichtnegative ganze rationale Zahlen, die μ_k aber Zahlen der Folge $0, 1, 2, \dots, 7h - 1$, also nur endlichvieler Werte fähig sind. Setzt man

$$\mathfrak{a} = \mathfrak{p}_1^{\mu_1}\mathfrak{p}_2^{\mu_2}\dots\mathfrak{p}_s^{\mu_s}, \qquad \mathfrak{a}' = \mathfrak{p}_1'^{\mu_1}\mathfrak{p}_2'^{\mu_2}\dots\mathfrak{p}_s'^{\mu_s},$$

$$\mathfrak{x} = \mathfrak{p}_1^{\lambda_1 h}\mathfrak{p}_2^{\lambda_2 h}\dots\mathfrak{p}_s^{\lambda_s h}, \qquad \mathfrak{x}' = \mathfrak{p}_1'^{\lambda_1 h}\mathfrak{p}_2'^{\lambda_2 h}\dots\mathfrak{p}_s'^{\lambda_s h},$$

so bestehen die Gleichungen

$$(p - q\zeta) = \mathfrak{a}\mathfrak{x}^7, \qquad (p - q\zeta') = \mathfrak{a}'\mathfrak{x}'^7.$$

Offenbar ist $\mathfrak{x} = (\xi)$ ein Hauptideal, also auch $\mathfrak{a} = (\alpha)$. Das Ideal (α) kann höchstens $(7h)^s$ verschiedene Werte annehmen. Geht man zu den Zahlen über, so ist

$$p - q\zeta = \varrho\alpha\xi^7, \qquad p - q\zeta' = \varrho'\alpha'\xi'^7,$$

wobei ϱ eine gewisse Einheit aus K bedeutet. Ist K nicht reell, so gibt es in diesem Körper als Einheiten höchstens sechs Einheitswurzeln; wir setzen

$$\varrho\alpha = \beta, \qquad \xi = \bar{p} + \bar{q}\omega$$

und dann kann β nur einen von höchstens $6(7h)^s$ verschiedenen ganzen Werten aus K annehmen, während $\bar{p}$ und $\bar{q}$ gewisse ganze rationale Zahlen sind.

Ist dagegen K ein reeller Körper, so muß ϱ von der Form

$$\varrho = \varepsilon\eta^g$$

sein, wo $\varepsilon = \mp 1$, η eine erzeugende Einheit aus K und g eine ganze rationale Zahl ist. Sei

$$g = 7e + f,$$

mit einer ganzen rationalen Zahl e und einer Zahl f, die einen der Werte 0, 1, 2, 3, 4, 5, 6 hat. Wir setzen

$$\varepsilon\eta^f\alpha = \beta, \qquad \eta^e\xi = \bar{p} + \bar{q}\omega,$$

und dann kann β nur einen von höchstens $14(7h)^s$ verschiedenen ganzen Werten aus K annehmen und sind $\bar{p}$ und $\bar{q}$ gewisse ganze rationale Zahlen.

Damit ist man in beiden Fällen zu der Darstellung

$$p - q\zeta = \beta(\bar{p} + \bar{q}\omega)^7, \qquad p - q\zeta' = \beta'(\bar{p} + \bar{q}'\omega')^7$$

gekommen. Sei

$$(\bar{p}, \bar{q}) = \Delta.$$

Wegen $(p, q) = 1$ und

$$\Delta^7 \mid (p - q\zeta,\ p - q\zeta')$$

ist offenbar

$$\Delta^7 | \zeta - \zeta',$$

so daß Δ nur endlichviele Werte annehmen kann. Es werde jetzt schließlich

$$\frac{\bar{p}}{\Delta} = p^*, \qquad \frac{\bar{q}}{\Delta} = q^*, \qquad \Delta^7 \beta = \gamma$$

gesetzt; damit ist man zu einer Darstellung

$$p - q\zeta = \gamma (p^* + q^* \omega)^7, \quad p - q\zeta' = \gamma' (p^* + q^* \omega')^7$$

gekommen, in der γ eine von endlichvielen ganzen Zahlen aus K, p^* und q^* aber ganze rationale teilerfremde Zahlen sind. Offenbar gilt

$$p = \frac{\zeta' \gamma (p^* + q^* \omega)^7 - \zeta \gamma' (p^* + q^* \omega')^7}{\zeta' - \zeta}, \qquad q = \frac{\gamma (p^* + q^* \omega)^7 - \gamma' (p^* + q^* \omega')^7}{\zeta' - \zeta};$$

diesen Gleichungen entnimmt man, daß mit $|p, q|$ auch $|p^*, q^*|$ über alle Grenzen wächst.

Die betrachtete p, q-Folge werde jetzt in die endlichvielen Teilfolgen T_γ zerlegt, zu denen die vorige Konstruktion dasselbe γ lieferte. Es genügt, diejenigen T_γ zu betrachten, in denen unendlichviele Paare vorkommen und für die Paare in jedem einzelnen solchen T_γ zu zeigen, daß der größte Primteiler von $L(p, q)$ bzw. $Q^*(p, q)$ über alle Grenzen wächst.

Es ist

$$L(p, q) = p + B_1 q, \quad Q^*(p, q) = (p - Z_1 q)(p - Z_2 q),$$

wobei Z_1 und Z_2 die Nullstellen von $Q^*(x, 1)$ sind. Hieraus ergibt sich

$$L(p, q) = F(p^*, q^*), \quad Q^*(p, q) = G(p^*, q^*),$$

wobei $F(x, y)$ und $G(x, y)$ die Formen siebten und vierzehnten Grades

$$F(x, y) = \frac{\gamma (\zeta' + B_1)(x + y\omega)^7 - \gamma' (\zeta + B_1)(x + y\omega')^7}{\zeta' - \zeta},$$

$$G(x, y) = \frac{\gamma (\zeta' - Z_1)(x + y\omega)^7 - \gamma' (\zeta - Z_1)(x + y\omega')^7}{\zeta' - \zeta} \times \frac{\gamma (\zeta' - Z_2)(x + y\omega)^7 - \gamma' (\zeta - Z_2)(x + y\omega')^7}{\zeta' - \zeta}$$

mit rationalen Koeffizienten sind. Die Nullstellen von $F(x, 1)$ bestimmen sich aus

$$\frac{x + \omega}{x + \omega'} = e^{2\pi i j/7} \left(\frac{\gamma' (\zeta + B_1)}{\gamma (\zeta' + B_1)}\right)^{1/7} \quad (j = 0, 1, 2, 3, 4, 5, 6),$$

die Nullstellen von $G(x, 1)$ aus

$$\frac{x + \omega}{x + \omega'} = e^{2\pi i j/7} \left(\frac{\gamma' (\zeta - Z_1)}{\gamma (\zeta' - Z_1)}\right)^{1/7} \quad (j = 0, 1, 2, 3, 4, 5, 6)$$

bzw.

$$\frac{x + \omega}{x + \omega'} = e^{2\pi i j/7} \left(\frac{\gamma' (\zeta - Z_2)}{\gamma (\zeta' - Z_2)}\right)^{1/7} \quad (j = 0, 1, 2, 3, 4, 5, 6).$$

Die drei Zahlen unter den Wurzelzeichen sind endlich und von Null verschieden, denn γ und γ' sind gemäß ihrer Konstruktion nicht Null und ζ

oder ζ' können weder gleich der ganzen rationalen Zahl $-B_1$, noch gleich einer der beiden Wurzeln Z_1, Z_2 des zu $Q(x, 1)$ teilerfremden Polynoms $Q^*(x, 1)$ sein.

Hieraus folgt, daß höchstens eine einzige Nullstelle von $F(x, 1)$ bzw. höchstens zwei von $G(x, 1)$ algebraisch von erstem oder zweitem Grade sind; denn sonst wäre eine primitive siebte Einheitswurzel rational durch endlichviele algebraischen Zahlen ersten oder zweiten Grades darstellbar, was bekanntlich nicht geht.

Also geht in $F(x, y)$ und $G(x, y)$ eine irreduzible Form mit ganzen rationalen Koeffizienten von mindestens drittem Grade auf; daraus und aus der Folgerung 1 ergibt sich, daß der größte Primteiler von

$$F(p^*, q^*) \quad \text{bzw.} \quad G(p^*, q^*)$$

über alle Grenzen wächst, wenn p^* und q^* alle unendlichvielen Paare teilerfremder ganzer rationaler Zahlen aus T_γ durchlaufen; also strebt gleichzeitig der größte Primteiler von $L(p, q)$ und $Q^*(p, q)$ über alle Grenzen und es ist gezeigt, daß der größte Primteiler der Formen

$$Q(p, q)\, L(p, q) \quad \text{und} \quad Q(p, q)\, Q^*(p, q)$$

nicht beschränkt ist, wenn p, q irgendeine unendliche Folge teilerfremder ganzer rationaler Zahlen mit $|p, q| \to \infty$ durchlaufen[8]).

Offenbar kann man die Folgerungen 1 bis 5 zusammenfassen in den Satz: *„Hat die Binärform $F(x, y)$ ganze rationale Koeffizienten und das Polynom $F(x, 1)$ mindestens drei verschiedene Nullstellen, wobei eine etwaige Nullstelle $x = \infty$ mitzuzählen ist, so wächst der größte Primteiler von $F(p, q)$ über alle Grenzen, wenn p, q eine Folge teilerfremder ganzer rationaler Zahlen mit $|p, q| \to \infty$ durchlaufen."*

Göttingen, im Januar 1932.

[8]) Wegen dieses Beweises vergleiche Pólya (7), S. 145 und Siegel (3), S. 204.

(Eingegangen am 6. 2. 1932.)