# Zur arithmetischen Untersuchung der Polynome.

Von

Georg Pólya in Zürich.

## § 1.

Es sei $f(x)$ eine ganze rationale Funktion mit ganzen rationalen Koeffizienten, $n$ eine Zahl der Folge 0, 1, 2, 3, ... und $P_n$ der größte Primfaktor der Zahl $f(n)$. Ein längst bekannter, elementarer Satz[1]) der Zahlentheorie läßt sich auf folgende Form bringen: für jede nichtkonstante ganze rationale Funktion $f(x)$ ist

$$\lim_{n=\infty} P_n = \infty. \tag{1}$$

Herr Störmer[2]) hat (1) für drei spezielle Funktionen $f(x)$, nämlich für

$$x(x+1), \qquad x(x+2), \qquad x^3+1 \tag{2}$$

bedeutend verschärft, indem er es durch

$$\lim_{n=\infty} P_n = \infty \tag{3}$$

ersetzen konnte.

Herr Thue[3]) hat mit Hilfe seines bekannten, wichtigen Satzes über Diophantische Gleichungen das Resultat von Herrn Störmer, in-

[1]) Dies kommt bei dem bekannten elementaren Beweis für die Existenz unendlich vieler Primzahlen in arithmetischen Progressionen mit dem Anfangsgliede $+1$ vor. Vgl. etwa J. Schur, Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen. Sitzungsberichte der Berliner Math. Gesellschaft, 11. Jahrg. (1912), S. 40 bis 50.

[2]) Carl Störmer, Sur une équation indéterminée, C. R. 127 (1898), S. 752 bis 754.

[3]) Axel Thue, I. Bemerkungen über gewisse Näherungsbrüche algebraischer Zahlen. Skrifter af Videnskabs-Selskabet i Christiania 1908, Nr. 3. — II. Om en generel i store hele tal ulösbar ligning, ebendaselbst, Nr. 7. — III. Über Annäherungswerte algebraischer Zahlen. Journ. für Mathematik 135 (1909), S. 284 bis 305.

soweit es die beiden ersten Polynome (2) betrifft, weitgehend verallgemeinert. Sein Resultat läßt sich so aussprechen:

Satz I. *Ist $f(x)$ das Produkt zweier wesentlich verschiedenen, d. h. nicht nur um eine multiplikative Konstante verschiedenen rationalen Linearfaktoren, so gilt* (3).

Ist $f(x)$ das Produkt zweier nur unwesentlich verschiedenen Linearfaktoren, oder hat es allgemeiner die Form

$$c(ax+b)^m, \tag{4}$$

so ist (3) offenbar ungültig. [Den Fall $b=0$ beiseite gelassen, kann

$$(a,b)=1, \qquad a \geqq 1, \qquad b > a$$

vorausgesetzt werden. Setzt man

$$n = \frac{b}{a}(b^{\varphi(a)\nu} - 1),$$

wo $\nu = 1, 2, 3, \ldots$, so wird $P_n$ die größte in $bc$ aufgehende Primzahl sein, also für unendlich viele $n$ denselben Wert behalten.]

Welche Polynome sind es, für die (3), und welche sind es, für die nur (1) gültig ist? Ich will nicht auf naheliegende Vermutungen eingehen, ich begnüge mich heute damit, zu der aufgeworfenen Frage mit dem Beweise folgenden Satzes beizutragen:

Satz II. *Ist $f(x)$ ein irreduzibles Polynom vom zweiten Grade, so gilt* (3).

Satz II enthält das Resultat von Herrn Störmer über das letzte der Polynome (2).

## § 2.

Man verdankt Herrn Thue[4]) den folgenden wichtigen Satz:

„Es sei $F(x,y)$ eine irreduzible homogene binäre Form vom dritten oder höheren Grade mit ganzen rationalen Koeffizienten. Dann hat die Diophantische Gleichung

$$F(x,y) = c \tag{5}$$

nur endlich viele verschiedene ganzzahlige Lösungen."

Demselben Satze hat Herr Thue[5]) noch die folgende Fassung gegeben:

„Ist $c \gtrless 0$ und hat die Diophantische Gleichung (5) unendlich viele ganzzahlige Lösungen, so muß die binäre Form $F(x,y)$ Potenz einer

[4]) Vgl. loc. cit. [3]) III, Theorem IV, S. 303.
[5]) Vgl. loc. cit. [3]) II, S. 3.

Linearform oder einer indefiniten quadratischen Form sein, oder sie unterscheidet sich nur um eine multiplikative Konstante von einer solchen Potenz."

Diese zweite Fassung ist leicht aus der ersten herzuleiten. —

Der Beweis des Satzes I erfolgt nun so [6]): die beiden linearen Funktionen $ax + b$ und $cx + d$ seien wesentlich verschieden, d. h. es sei

$$\frac{b}{a} \gtrless \frac{d}{c}. \tag{6}$$

Man bezeichne mit $P_n$ den größten Primfaktor der beiden Zahlen $an + b$ und $cn + d$. Wäre (3) falsch, so könnte man gewisse endlich viele Primzahlen

$$p_1, p_2, \ldots p_l \tag{7}$$

und unendlich viele Werte $n$ finden, für welche $(an + b)(cn + d)$ durch keine von den Primzahlen (7) verschiedene Primzahl teilbar wäre. Für diese $n$ wäre

$$an + b = p_1^{a_1} p_2^{a_2} \ldots p_l^{a_l}, \qquad cn + d = p_1^{c_1} p_2^{c_2} \ldots p_l^{c_l}. \tag{8}$$

Man reduziere $a_1, \ldots a_l$, $c_1, \ldots c_l$ mod. 3. Aus (8) folgt dann

$$an + b = p_1^{r_1} p_2^{r_2} \ldots p_l^{r_l} x^3, \qquad cn + d = p_1^{s_1} p_2^{s_2} \ldots p_l^{s_l} y^3$$

$$(r_1, \ldots r_l,\ s_1, \ldots s_l = 0, 1 \text{ oder } 2),$$

wo für das Zahlensystem $r_1, \ldots r_l$, $s_1, \ldots s_l$ nur endlich viele [nämlich $3^{2l}$] Möglichkeiten bestehen.

Jedes $n$ der fraglichen Art liefert uns eine Lösung $x, y$ einer Diophantischen Gleichung von der Form

$$a\, p_1^{s_1} p_2^{s_2} \ldots p_l^{s_l} y^3 - c\, p_1^{r_1} p_2^{r_2} \ldots p_l^{r_l} x^3 = ad - bc.$$

Die rechte Seite ist nach (6) von 0 verschieden. Die linke Seite ist nicht die dritte Potenz einer Linearform von $x, y$. Die Annahme, daß unendlich viele $n$ der fraglichen Art existieren, führt also auf einen Widerspruch mit der zweiten Fassung des Thueschen Satzes, und somit ist Satz I bewiesen.

Dieses Beweisverfahren von Herrn Thue bedarf nur einiger Modifikation, um auch den Satz II mit seiner Hilfe zu erhalten.

## § 3.

Wäre der Satz II für das Polynom

$$f(x) = ax^2 + bx + c$$

[6]) Vg. loc. cit. [3]) I, Satz 12, S. 30.

falsch, so wäre er auch für das Polynom

$$f^*(x) = x^2 + bx + ac$$

falsch, wegen der Identität

$$af(x) = f^*(ax).$$

Ich kann also von vornherein den höchsten Koeffizienten von $f(x)$ als 1 annehmen, d. h.

$$f(x) = (x - \alpha)(x - \alpha')$$

setzen, wo $\alpha$ und $\alpha'$ konjugierte *ganze* algebraische Zahlen zweiten Grades bedeuten. Ich will ferner beim Beweise den Fall vor Augen behalten, wo $\alpha$ und $\alpha'$ reell sind. [Dieser Fall ist etwas verwickelter, wegen der unendlich vielen Einheiten im reellen quadratischen Körper.]

Ich habe einen Widerspruch aus der Annahme abzuleiten daß es unendlich viele rationale ganze $n$ gibt, für welche $f(n) = (n - \alpha)(n - \alpha')$ außer den Primzahlen

$$p_1, p_2, \dots p_r \tag{9}$$

keine andere Primfaktoren hat.

Die Wurzeln $\alpha$ und $\alpha'$ von $f(x)$ sollen im Körper liegen, der durch $\sqrt{D}$ erzeugt ist. Es seien in diesem Körper:

$1, \omega$ eine Basis der ganzen Zahlen,
$h$ die Klassenanzahl,
$\varepsilon$ die Grundeinheit,
$\mathfrak{p}_1, \mathfrak{p}_2, \dots \mathfrak{p}_l$ sämtliche Primidealteiler der Primzahlen (9).

Konjugierte Größen werden durch Akzent unterschieden: $\alpha$ und $\alpha'$, $\beta$ und $\beta'$, $\mathfrak{p}$ und $\mathfrak{p}'$ usw.

Ich habe einen Widerspruch aus der Annahme zu folgern, daß für unendlich viele rationale ganze $n$ das Ideal $(n - \alpha)$ eine Zerlegung der Art

$$(n - \alpha) = \mathfrak{p}_1^{a_1} \mathfrak{p}_2^{a_2} \dots \mathfrak{p}_l^{a_l}$$

zuläßt. Ich setze

$$(n - \alpha) = \mathfrak{p}_1^{r_1} \mathfrak{p}_2^{r_2} \dots \mathfrak{p}_l^{r_l} \mathfrak{r}^{3h},$$

wo

$$0 \leqq r_1 < 3h, \quad 0 \leqq r_2 < 3h, \quad \dots, \quad 0 \leqq r_l < 3h.$$

$\mathfrak{r}^{3h}$ ist die dritte Potenz eines gewissen Hauptideals $(x + \omega y)$. Daher ist

$$n - \alpha = \beta (x + \omega y)^3, \tag{10}$$

wo $\beta$ eine gewisse ganze Zahl des Körpers ist. Für das Ideal $(\beta)$ bestehen höchstens $3^l h^l$ verschiedene Möglichkeiten, denn dies ist die Anzahl der möglichen Zahlsysteme $r_1, r_2, \dots r_l$. Ein bestimmtes Ideal $(\beta)$

muß in (10) nur durch 6 verschiedene Zahlen vertreten werden, nämlich durch die Zahlen

$$\beta,\ \varepsilon\beta,\ \varepsilon^2\beta,\ -\beta,\ -\varepsilon\beta,\ -\varepsilon^2\beta.$$

Kurzum, es genügt zu beweisen, daß für gegebenes $\beta$ die Gleichung (10) nicht unendlich viele verschiedene Auflösungen in rationalen ganzen Zahlen $n$, $x$, $y$ haben kann. Aus

$$n-\alpha=\beta(x+\omega y)^3$$
$$n-\alpha'=\beta'(x+\omega' y)^3$$

folgt aber

$$\frac{\alpha'-\alpha}{\omega'-\omega}=\frac{\beta(x+\omega y)^3-\beta'(x+\omega' y)^3}{\omega'-\omega}=F(x,y), \tag{11}$$

wo $F(x, y)$ eine homogene binäre Form dritten Grades mit ganzen rationalen Koeffizienten bedeutet. $F(x, y)$ ist nicht die dritte Potenz einer Linearform, denn die drei Wurzeln der Gleichung

$$F(z,1)=0,$$

d. h. der Gleichung

$$\left(\frac{z+\omega}{z+\omega'}\right)^3=\frac{\beta'}{\beta}$$

sind alle verschieden. So folgt aus dem Thueschen Satze, daß die Diophantische Gleichung (11) nicht unendlich viele Auflösungen haben kann, und damit die Richtigkeit unseres Satzes II.

Aus den Thueschen Resultaten über Diophantische Gleichungen ergibt sich noch, daß (3) auch für das Polynom $x^n-1$ Gültigkeit behält, oder allgemeiner für solche Polynome, bei welchen eine gewisse Anzahl Koeffizienten, die dem höchsten Gliede folgen, $=0$ sind[7]). Die volle Entscheidung der im § 1 aufgeworfenen allgemeineren Frage ist aber wohl aus einer anderen Quelle zu schöpfen.

## § 4.

Ich will noch den Satz I in einer anderen Fassung aussprechen und daran einige Bemerkungen knüpfen.

Es seien

$$p_1,\ p_2,\ \dots\ p_r \tag{12}$$

$r$ gegebene Primzahlen, $r \geqq 2$. Man erteile in dem Ausdruck

$$p_1^{x_1}p_2^{x_2}\dots p_r^{x_r}$$

$x_1, x_2, \dots x_r$ alle mögliche nichtnegative ganzzahlige Wertsysteme. Die

[7]) Vgl. loc. cit. [3]) III, S. 304.

so erhaltenen ganzen Zahlen, nach aufsteigender Größe geordnet, bezeichne man mit

$$a_0, a_1, a_2, \ldots a_n, \ldots \tag{13}$$

Satz I′ ist dann äquivalent mit der Tatsache

$$\lim_{n=\infty} (a_{n+1} - a_n) = \infty. \tag{14}$$

Denn wäre $\lim_{n=\infty}$. inf. $(a_{n+1} - a_n) = k$, so wäre (3) für das Polynom $x(x+k)$ ungültig. Umgekehrt ist leicht einzusehen, daß Satz I nur für die Polynome $x(x+k)$ bewiesen zu werden braucht.

Nun lassen sich (14) noch folgende Eigenschaften der Zahlen $a_0, a_1, a_2, \ldots$ zur Seite stellen:

$$\lim_{n=\infty} \frac{a_{n+1}}{a_n} = 1, \tag{15}$$

$$\lim_{n=\infty} \frac{(\log a_n)^r}{n} = 1 \cdot 2 \ldots r \log p_1 \log p_2 \ldots \log p_r. \tag{16}$$

Diese Eigenschaften tragen zur besseren Auffassung von (14) bei, liegen aber viel weniger tief. Die Gleichung (15) beruht darauf, daß die Linearform

$$x_1 \log p_1 + x_2 \log p_2 + \ldots + x_r \log p_r$$

der ganzzahligen Variabeln $x_1, x_2, \ldots x_r$ nie verschwinden kann (abgesehen von $x_1 = x_2 = \ldots = x_r = 0$) und folglich beliebig kleine Werte annimmt. Die Formel (16) folgt aus der Abzählung der Gitterpunkte in dem durch die $r+1$ Ungleichungen

$$x_1 \geqq 0,\ x_2 \geqq 0, \ldots x_r \geqq 0,\ x_1 \log p_1 + x_2 \log p_2 + \ldots + x_r \log p_r \leqq \log a_n$$

abgegrenzten, abgeschlossenen, ebenwändigen, $r$-dimensionalen Bereich.

(Eingegangen am 4. August 1917.)