Über die Zerlegung strikte definiter Formen in Quadrate.

Über die Zerlegung strikte definiter Formen in Quadrate

Von W. Habicht, Schaffhausen

Als *Form* soll im folgenden eine ganze rationale homogene Funktion mit rationalen Koeffizienten bezeichnet werden. Eine Form $F(x_1, \ldots, x_n)$ in n Variablen heißt *definit,* wenn sie für kein reelles Wertsystem der Variablen negative Werte annimmt; sie heiße *strikte definit,* wenn sie für sämtliche reellen Wertsysteme der Variablen, mit Ausnahme des Wertsystems $(0, \ldots, 0)$, positive Werte annimmt.

Hilbert hat im Jahre 1900 die Frage aufgeworfen, ob sich jede definite Form als Quotient zweier Summen von Formenquadraten darstellen lasse[1]). Diese Frage wurde später von Artin in bejahendem Sinne beantwortet[2]). Jedoch liefert der *Artin*'sche Beweis keine explizite Vorschrift, die Zerfällung wirklich durchzuführen, sondern es ergibt sich dabei lediglich die Existenz einer Zerfällung im Rahmen eines allgemeinen Satzes der abstrakten Körpertheorie.

Das Ziel der vorliegenden Arbeit ist, den *Hilbert-Artin*'schen Satz für den Spezialfall strikte definiter Formen zu beweisen. Ich gebe also einen Beweis für den folgenden Satz:

Eine strikte definite Form läßt sich als Quotient zweier Summen von Formenquadraten darstellen.

Der Beweis unterscheidet sich wesentlich von dem *Artin*'schen, ist ganz elementar und darf als konstruktiv bezeichnet werden: er besteht nämlich in einer in endlich vielen Schritten durchführbaren Vorschrift, wie die Darstellung zu gewinnen sei. Den Ausgangspunkt des Beweises bildet ein Satz, der von *G. Pólya* aufgestellt und bewiesen worden ist[3]).

Der versprochene Beweis soll in vier Schritten geführt werden. Dabei enthält jeder einzelne Abschnitt ein an sich bemerkenswertes Resultat.

---

1) *D. Hilbert,* Mathematische Probleme. Göttinger Nachrichten 1900, S. 284, Nr. 17.

2) *E. Artin,* Über die Zerlegung definiter Funktionen in Quadrate. Abhandlungen Math. Seminar Hamburg, Bd. V, 1926, S. 100—115.

3) *G. Pólya,* Über positive Darstellung von Polynomen. Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich, LXXIII (1928). Vgl. auch *Hardy, Littlewood, Pólya,* Inequalities. Cambridge 1934, 2. 24, S. 57—60.

1. Der Satz von *Pólya* lautet:

Eine Form in n Variablen, die für alle nichtnegativen Wertsysteme der Variablen, mit Ausnahme des Wertsystems $(0, \ldots, 0)$, *positive Werte annimmt, läßt sich als Quotient zweier Formen mit lauter positiven Koeffizienten darstellen.*

Und zwar gibt *Pólya* eine Darstellung mit besonders einfachem Nenner; er beweist nämlich folgendes:

Es sei $G(x_1, \ldots, x_n)$ eine Form in n Variablen vom Grade r, und es sei

$$G(x_1, \ldots, x_n) > 0$$

für

$$x_1 \geqq 0, \ldots, x_n \geqq 0 \quad , \qquad x_1 + \cdots + x_n > 0 \; .$$

Dann geht aus $G(x_1, \ldots, x_n)$ bei wiederholter Multiplikation mit $x_1 + \cdots + x_n$ schließlich eine Form mit lauter positiven Gliedern hervor; das heißt für eine genügend große natürliche Zahl k ist

$$G(x_1, \ldots, x_n)\,(x_1 + \cdots + x_n)^k = \sum_{(\alpha)}^{r+k} p_{\alpha_1, \ldots, \alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n} \; , \qquad (1)$$

wo die $p_{\alpha_1, \ldots, \alpha_n}$ positive rationale Zahlen sind und die Summation sich über solche Wertsysteme $\alpha_1 \geqq 0, \ldots, \alpha_n \geqq 0$ der Indizes erstreckt, für die $\alpha_1 + \cdots + \alpha_n = r + k$ ist; es ergibt sich beim Beweis sogar, daß alle solchen Wertsysteme durchlaufen werden.

2. *Zu einer strikte definiten Form* $H(x_1, \ldots, x_n)$, *welche gerade ist in bezug auf jede ihrer n Variablen, gibt es eine andere Form* $S(x_1, \ldots, x_n)$, *so daß das Produkt* $H(x_1, \ldots, x_n)\, S(x_1, \ldots, x_n)$ *sich als Summe von Quadraten von Monomen darstellen läßt.*

Dabei ist als Monom eine Form in $x_1, \ldots, x_n$ bezeichnet, welche nur aus einem einzigen Glied besteht.

Es sei also $H(x_1, \ldots, x_n)$ eine Form vom Grade $s = 2r$, und es sei $H(x_1, \ldots, x_n) > 0$ für ein beliebiges nichtverschwindendes Wertsystem der Variablen. Außerdem sei $H(x_1, \ldots, x_n)$ gerade in bezug auf jede der Variablen; $H(x_1, \ldots, x_n)$ kann also als Form in $x_1^2, \ldots, x_n^2$ geschrieben werden:

$$H(x_1, \ldots, x_n) = G(x_1^2, \ldots, x_n^2) \; .$$

Setzen wir $x_1^2 = y_1, \ldots, x_n^2 = y_n$, so entspricht jedem Wertsystem der y_i, das den Bedingungen

$$y_1 \geqq 0, \ldots, y_n \geqq 0 \quad , \qquad y_1 + \cdots + y_n > 0$$

genügt, ein reelles nicht verschwindendes Wertsystem der x_i; für ein solches Wertsystem der y_i gilt also $G(y_1, \ldots, y_n) > 0$, d. h. die Form G erfüllt die Voraussetzungen des Satzes von *Pólya*. Demnach gibt es eine natürliche Zahl k, so daß in

$$G(y_1, \ldots, y_n)\,(y_1 + \cdots + y_n)^k = \sum_{(\alpha)}^{r+k} p_{\alpha_1, \ldots, \alpha_n}\, y_1^{\alpha_1} \cdots y_n^{\alpha_n}$$

sämtliche $p_{\alpha_1, \ldots, \alpha_n}$ positive rationale Zahlen sind. Führt man hierin wieder $x_1, \ldots, x_n$ als Variable ein und zerlegt jede der Zahlen $p_{\alpha_1, \ldots, \alpha_n}$ in eine Summe von Quadraten von rationalen Zahlen (was trivialerweise möglich ist), so folgt

$$H(x_1, \ldots, x_n)\,(x_1^2 + \cdots + x_n^2)^k = \sum_{(\alpha)}^{r+k} p_{\alpha_1, \ldots, \alpha_n}(x_1^{\alpha_1} \cdots x_n^{\alpha_n})^2 =$$

$$= \sum_{((\alpha))}^{r+k} (q_{\alpha_1, \ldots, \alpha_n}\, x_1^{\alpha_1} \cdots x_n^{\alpha_n})^2 \,. \qquad (2)$$

Die Summation in der letzten Summe erstreckt sich dabei wieder über sämtliche Wertsysteme der Indizes mit $\alpha_1 + \cdots + \alpha_n = r + k$; jedes Wertsystem kommt vor, es kann aber eventuell auch mehrere Male vorkommen.

Damit ist die Behauptung bewiesen; ja sogar noch mehr:

Eine strikte definite Form, welche gerade ist in bezug auf jede ihrer n Variablen, läßt sich als Quotient zweier Summen von Quadraten von Monomen darstellen[4].

3. Wir wollen uns jetzt freimachen von der Einschränkung, der die strikte definiten Formen in 2. unterworfen wurden, und beweisen:

Zu einer beliebigen strikte definiten Form $F(x_1, \ldots, x_n)$ gibt es eine andere Form $T(x_1, \ldots, x_n)$, so daß das Produkt $F(x_1, \ldots, x_n)\; T(x_1, \ldots, x_n)$ sich als Summe von Quadraten von Monomen darstellen läßt.

Es sei also $F(x_1, \ldots, x_n) > 0$ für ein beliebiges nichtverschwindendes Wertsystem der Variablen. Dann bilde man das Produkt

$$H(x_1, \ldots, x_n) = \prod_{\nu_1=0}^{1} \prod_{\nu_2=0}^{1} \cdots \prod_{\nu_n=0}^{1} F((-1)^{\nu_1} x_1, \ldots, (-1)^{\nu_n} x_n) \,. \qquad (3)$$

$H(x_1, \ldots, x_n)$ ist eine gerade Funktion in jeder einzelnen der Variablen $x_1, \ldots, x_n$; ferner ist $H(x_1, \ldots, x_n)$ strikte definit, da jeder der rechts stehenden Faktoren strikte definit ist. Die Form $H(x_1, \ldots, x_n)$ erfüllt also die in 2. gemachten Voraussetzungen; spaltet man von $H(x_1, \ldots, x_n)$

[4]) Dieser Satz findet sich schon bei *Pólya*; vgl. a. a. O. [3]), S. 144—145.

noch den Faktor $F(x_1, \ldots, x_n)$ ab, so folgt jetzt aus (2) in angemessener Bezeichnung die ausgesprochene Behauptung:

$$F(x_1, \ldots, x_n)\, T(x_1, \ldots, x_n) = \sum_{((\alpha))}^{h} (q_{\alpha_1, \ldots, \alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n})^2 \,. \tag{4}$$

4. Es sei $F(x_1, \ldots, x_n)$ wieder eine strikte definite Form vom (geraden) Grad $m = 2l$. Um nun zu einer *Darstellung von $F(x_1, \ldots, x_n)$ als Quotient zweier Summen von Formenquadraten* zu gelangen, geben wir der Überlegung eine neue Wendung.

Wir führen nämlich eine neue Unbestimmte u ein und betrachten an Stelle der Form $F(x_1, \ldots, x_n)$ von n Variablen die spezielle Form

$$F(x_1, \ldots, x_n) + u^m \tag{5}$$

von $n + 1$ Variablen. Da $u^m = u^{2l}$ für einen beliebigen nicht verschwindenden Wert von u positiv ausfällt, so ist die Form (5) wieder strikte definit.

Wir können also eine Form $T(x_1, \ldots, x_n, u)$ so konstruieren, daß

$$(F(x_1, \ldots, x_n) + u^m)\, T(x_1, \ldots, x_n, u) = \sum_{((\alpha))}^{h} (q_{\alpha_1, \ldots, \alpha_n, \alpha} x_1^{\alpha_1} \ldots x_n^{\alpha_n} u^{\alpha})^2 \tag{6}$$

ist. Die Summation erstreckt sich dabei über sämtliche nichtnegativen Wertsysteme der Indizes mit $\alpha_1 + \cdots + \alpha_n + \alpha = h$ (wobei, wie unter 2. bemerkt wurde, jedes Wertsystem eventuell mehrmals auftreten kann).

Nun fasse man in (6) die Form $F + u^m$ als Polynom in der Unbestimmten u und die Quadratbasen als Monome in u auf, und reduziere jede einzelne der Quadratbasen modulo $F + u^m$. Es sei $(q_{\alpha_1, \ldots, \alpha_n, \alpha} x_1^{\alpha_1} \ldots x_n^{\alpha_n})\, u^{\alpha}$ eine beliebige aus der Summe rechts in (6) herausgegriffene Quadratbasis. Die Division durch $F + u^m$ kann explizite durchgeführt werden. Es ist nämlich

$$u^{\alpha} = u^{m\beta+\gamma} = \left[(u^m)^{\beta} - (-F)^{\beta} \right] u^{\gamma} + (-F)^{\beta} u^{\gamma} \quad (\text{mit } 0 \leqq \gamma \leqq m - 1)\,.$$

Da der Ausdruck in der eckigen Klammer durch $F + u^m$ teilbar ist, folgt hieraus

$$(q_{\alpha_1, \ldots, \alpha_n, \alpha} x_1^{\alpha_1} \ldots x_n^{\alpha_n})\, u^{\alpha} = (F(x_1, \ldots, x_n) + u^m)\, Q + R \cdot u^{\gamma}\,; \tag{7}$$

dabei ist $Q = Q(x_1, \ldots, x_n, u)$ eine Form in $n + 1$ Variablen und $R = R(x_1, \ldots, x_n)$ eine (übrigens nicht identisch verschwindende) Form in n Variablen.

Der bei der Division durch $F + u^m$ verbleibende Rest ist also wieder ein Monom in der Unbestimmten u, und zwar vom Grade $\gamma \leqq m - 1$.

Nun bilde man die Ausdrücke (7) für sämtliche Quadratbasen rechts in (6). Quadriert man aus und nimmt die Vielfachen von $F + u^m$ auf die linke Seite, so erhält man aus (6)

$$(F(x_1, \ldots, x_n) + u^m)\, T^*(x_1, \ldots, x_n, u) = \sum_{\gamma=0}^{m-1} u^{2\gamma} \sum_{\delta} R^2_{\gamma\delta}(x_1, \ldots, x_n). \quad (8)$$

Dabei verschwindet insbesondere die Summe $\sum\limits_{\delta} R^2_{0\delta}$ nicht identisch: es gibt ja rechts in (6) mindestens ein nicht verschwindendes Glied mit $\alpha = 0$; dieses Glied bleibt beim Reduktionsprozeß unverändert bestehen, kommt also auch unter den Summengliedern rechts in (8) vor.

Aus (8) folgt zunächst, daß die Form $T^*(x_1, \ldots, x_n, u)$ als Polynom in u einen Grad $\leqq m - 2$ hat; (8) kann also geschrieben werden

$$(F(x_1, \ldots, x_n) + u^m) \cdot \sum_{\mu=0}^{m-2} C_\mu(x_1, \ldots, x_n)\, u^\mu = \sum_{\gamma=0}^{m-1} u^{2\gamma} \sum_{\delta} R^2_{\gamma\delta}\,. \quad (9)$$

Wir multiplizieren links aus und vergleichen links und rechts die Koeffizienten von u^0 und von u^m $(m = 2l)$:

$$F C_0 = \sum_{\delta} R^2_{0\delta}$$
$$C_0 = \sum_{\delta} R^2_{l\delta}\,.$$

Die rechte Seite der ersten Gleichung verschwindet nicht identisch, somit auch C_0 nicht. Also ist

$$F = \frac{\sum\limits_{\delta} R^2_{0\delta}}{\sum\limits_{\delta} R^2_{l\delta}}\,.$$

Damit ist eine Darstellung der strikte definiten Form $F(x_1, \ldots, x_n)$ als Quotient zweier Summen von Formenquadraten gewonnen, w.z.b.w.

Nebenbei gesagt, könnte man in (9) auch die Koeffizienten von u^2 und u^{m+2} oder von u^4 und u^{m+4} ... oder von u^{m-2} und u^{2m-2} vergleichen; (9) lieferte so nicht nur eine, sondern gleich l Darstellungen der gewünschten Art.

Es sei noch bemerkt, daß der Satz von *Pólya* auch dann noch gilt, wenn man als Koeffizientenkörper nicht den rationalen Zahlenkörper, sondern einen beliebigen archimedisch angeordneten Körper zugrunde legt. Überträgt man das oben angewandte Schlußverfahren auf diesen allgemeinern Fall, so folgt:

Eine strikte definite Form $F(x_1, \ldots, x_n)$ *in* n *Variablen mit Koeffizienten aus einem archimedisch angeordneten Körper* K *läßt sich in der Form*

$$F(x_1, \ldots, x_n) = \frac{\sum_\delta p_\delta R_\delta^2}{\sum_\delta p_\delta^* R_\delta^{*2}}$$

darstellen, wobei die R_δ, R_δ^* *gewisse Formen in* $x_1, \ldots, x_n$ *mit Koeffizienten aus* K, *die* p_δ, p_δ^* *positive Elemente aus* K *sind.*

(Eingegangen den 3. April 1940.)