

# Eine kleine n-Ecks-Lehre

Autor(en): **Ruoff, Dieter**

Objektyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **43 (1988)**

Heft 5

PDF erstellt am: **23.09.2024**

Persistenter Link: <https://doi.org/10.5169/seals-40809>

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

# ELEMENTE DER MATHEMATIK

Revue de mathématiques élémentaires – Rivista di matematica elementare

*Zeitschrift zur Pflege der Mathematik  
und zur Förderung des mathematisch-physikalischen Unterrichts*

El. Math.

Vol. 43

Nr. 5

Seiten 129–160

Basel, September 1988

## Eine kleine $n$ -Ecks-Lehre

### Einleitung

In *El. Math.* 37 hat M. Jeger eine Reihe von Sätzen über Polygone zusammengestellt, von denen sich jeder im Rahmen der komplexen Zahlenebene elementar beweisen lässt. Die betreffenden Sätze können noch in einer anderen Hinsicht unter einem gemeinsamen Blickwinkel betrachtet werden; sie lassen sich nämlich ohne Ausnahme in der Sprache der von F. Bachmann begründeten  $n$ -Ecks-Theorie formulieren. Dies hat zur Folge, dass ihr Beweis nur die Faktorzerlegung von Polynomen und das Lösen linearer Gleichungssysteme erfordert.

In dem vorliegenden Artikel wird das Ziel verfolgt, den Kern der erwähnten  $n$ -Ecks-Theorie elementar, aber lückenlos zu entwickeln. Eine anspruchsvollere Darstellung der Theorie findet der Leser entweder in dem Originalwerk [1] oder, in ausgebauter Form, in [2].

Für die Anregung, eine zusammenfassende Arbeit über die  $n$ -Ecks-Theorie zu schreiben, möchte der Verfasser Herrn Professor M. Jeger seinen herzlichen Dank aussprechen. Dazu möchte er hervorheben, dass ihn lange Jahre der Zusammenarbeit an  $n$ -Ecks-Fragen erst mit J. Shilieto und später auch mit J. C. Fisher verbanden.

1. Wir denken uns im folgenden ein  $n$ -Eck als ein  $n$ -Tupel von Vektoren (*Ecken*) in einem Vektorraum  $V(K)$  [1\*]. Im Rahmen unserer Untersuchungen werden wir  $n$ -Ecke ausschliesslich mit anderen  $n$ -Ecken in Beziehung setzen,  $n$  also als eine jeweils feste Grösse betrachten. Unser Interesse wird sich dabei auf diejenigen Eigenschaften eines  $n$ -Ecks richten, welche aus den seine Ecken verbindenden zyklisch invarianten Linearbeziehungen hervorgehen. Diese grundlegend wichtigen, ein  $n$ -Eck  $A = (a_0, a_1, \dots, a_{n-1})$  beschreibenden Beziehungen werden am besten in rekursiver Form wiedergegeben:

$$a_{i+k} = c_0 a_i + c_1 a_{i+1} + \dots + c_{k-1} a_{i+k-1},$$
$$i = 0, 1, \dots, n-1; a_{i+v'} = a_{i+v} \quad \text{für } i+v' \equiv i+v \pmod{n}. \quad (1)$$

Eine rekursive Formel (1) mit  $k \leq n-1$  nennen wir *eigentlich*, die rekursive Formel  $a_{i+n} = 1 \cdot a_i + 0 \cdot a_{i+1} + \dots + 0 \cdot a_{i+n-1}$ , die von jedem beliebigen  $n$ -Eck  $A$  erfüllt wird, *trivial*. Unter der *Rekursionsformel* eines  $n$ -Ecks verstehen wir seine kürzeste rekursive



so können die in (1) bzw. (3) ausgedrückten Beziehungen indexfrei durch

$$(x^k - c_{k-1} x^{k-1} - \dots - c_1 x - c_0) A = \mathbf{0}, \quad \mathbf{0} = (\underline{0}, \underline{0}, \dots, \underline{0}), \tag{6}$$

wiedergegeben werden.

*Beispiele 4–6*

4. Die in den Beispielen 1–3 betrachteten Polygone entsprechen den nachstehend beschriebenen: Ein Parallelogramm ist ein Viereck  $A_4$ , das die Gleichung  $(x^3 - x^2 + x - 1) A_4 = \mathbf{0}$  erfüllt. Ein *Translations- $n$ -Eck*, d. h. ein  $n$ -Eck der Form  $A = (\underline{a}, \underline{a}, \dots, \underline{a})$ , genügt der Bedingung  $(x - 1) A = \mathbf{0}$ . Jedes beliebige  $n$ -Eck  $A$  befriedigt die Gleichung  $(x^n - 1) A = \mathbf{0}$ . – Es folgen einige weitere  $n$ -Ecke in indexfreier Beschreibung. 5. In einem  $n$ -Eck  $A$ , das  $(x^2 - 1) A = \mathbf{0}$  erfüllt, stimmt jede Ecke mit der zyklisch übernächsten überein. Falls  $n = 2m$  gilt, hat  $A$  die Form  $(\underline{a}, \underline{b}, \underline{a}, \underline{b}, \dots, \underline{a}, \underline{b})$  eines  $m$ -fach durchlaufenen Zweiecks. Ist  $n \neq 2m$ , so hat  $A$  die Form  $(\underline{a}, \underline{b}, \dots, \underline{a}, \underline{b}, \underline{a})$ , wobei zusätzlich gilt, dass die zweitletzte Ecke,  $\underline{b}$ , gleich der ersten Ecke,  $\underline{a}$ , ist. Damit wird  $A$  zum *Translations- $n$ -Eck*  $(\underline{a}, \underline{a}, \dots, \underline{a})$ . In ähnlicher Weise fällt in einem  $n$ -Eck, das der Gleichung  $(x^3 - 1) A = \mathbf{0}$  genügt, jede Ecke mit der zyklisch über-über-nächsten zusammen. Für  $n = 3m$  ist  $A$  ein  $m$ -fach durchlaufenes Dreieck  $(\underline{a}, \underline{b}, \underline{c}, \underline{a}, \underline{b}, \underline{c}, \dots, \underline{a}, \underline{b}, \underline{c})$ , für  $n \neq 3m$  ist  $A$  wiederum ein *Translations- $n$ -Eck*. 6. Erfüllt das  $n$ -Eck  $A$  die Beziehung  $(x + 1) A = \mathbf{0}$ , so hat  $A$  die Form  $(\underline{a}, -\underline{a}, \underline{a}, -\underline{a}, \dots)$ . Für  $n = 2m$  ist  $A$  ein  $m$ -fach durchlaufenes Zweieck mit Schwerpunkt  $\underline{0}$ , für  $n \neq 2m$  gilt  $A = \mathbf{0}$ .

Es erhebt sich die Frage, ob die in (5) definierte Verknüpfung von  $n$ -Ecken  $A, B, \dots$  aus  $V^n(K)$  mit Polynomen  $p(x), q(x), \dots$  aus dem Bereich  $K[x]$  bestimmten Gesetzen gehorcht. In der Tat vermögen wir leicht nachzuweisen, dass die erwähnten  $n$ -Ecke und Polynome die Beziehungen

$$(p(x) + q(x)) A = p(x) A + q(x) A, \tag{7a}$$

$$p(x)(A + B) = p(x) A + p(x) B, \tag{7b}$$

$$(p(x) q(x)) A = p(x)(q(x) A) \quad \text{und} \tag{7c}$$

$$1 \cdot A = A \tag{7d}$$

erfüllen, d. h. einen Modul mit Multiplikatorenbereich  $K[x]$  bilden. Aus (7c) und der Kommutativität unserer Polynome folgt zudem

$$p(x)(q(x) A) = q(x)(p(x) A). \tag{8}$$

Die Linksmultiplikation von  $n$ -Ecken mit  $x$  oder mit einem Polynom in  $x$  kommt einer Abbildung des Vektorraums der  $n$ -Ecke in sich gleich. Die Abbildung ist linear, wie aus (7b) und (7c) leicht folgt. Wir werden für sie den Bachmannschen Ausdruck einer *zyklischen Abbildung* brauchen.

3. Ein Polynom, welches, wie dasjenige in der obigen Formel (6), ein  $n$ -Eck  $A$  auf das Null- $n$ -Eck  $\mathbf{0} = (0, 0, \dots, 0)$  abbildet, wird ein *Annulator* von  $A$  genannt. Es zeigt sich, dass man die Eigenschaften eines Polygons am besten mit Hilfe seiner Annulatoren herleiten kann. Dabei liefern zwei Annulatoren, die sich lediglich um einen konstanten, nicht verschwindenden Faktor unterscheiden, dieselbe Information. Gewisse Polynome, wie das (gradlose) Körperelement  $0$  oder wie  $x^n - 1$ , annullieren sämtliche  $n$ -Ecke; besondere Aussagen über ein einzelnes  $n$ -Eck sind aus ihnen natürlich nicht herleitbar.

Es sei nun  $A$  ein  $n$ -Eck,  $p(x)$  ein Annulatorpolynom von  $A$  und  $m(x)$  ein Annulatorpolynom niedrigsten Grades von  $A$ . Dann ist  $p(x)$  durch  $m(x)$  ohne Rest teilbar. Wäre das Gegenteil der Fall, dann handelte es sich bei dem Restpolynom  $r(x) = p(x) - f(x)m(x)$  entgegen unseren Annahmen um einen Annulator von  $A$  mit einem niedrigeren Grad als dem von  $m(x)$ . Mit Hilfe des eben Bewiesenen folgt sofort, dass das  $n$ -Eck  $A$  von den und nur den Polynomen  $p(x)$  annulliert wird, welche  $m(x)$  als einen Faktor enthalten. Dividieren wir das Polynom  $m(x)$  durch seinen Anfangskoeffizienten  $c$ , so erhalten wir ein normiertes Polynom  $m_A(x)$ , das gleichermassen Teiler aller und nur der Annulatoren von  $A$  ist. Wir nennen  $m_A(x)$  *das zu A gehörige Polynom* oder den *minimalen Annulator* von  $A$  [2\*].

Soviel zur Menge der Annulatoren eines gegebenen  $n$ -Ecks  $A$ . Wir betrachten nun umgekehrt die Menge der von einem festen Polynom  $p(x)$  annullierten  $n$ -Ecke, seinen Kern. Diese letztere, bereits früher erwähnte Menge, die *zyklische Klasse* von  $p(x)$ , ist sowohl additiv als auch in bezug auf Multiplikation mit einem Skalar abgeschlossen und bildet daher einen Unterraum von  $V^n(K)$ . Aus der Kommutativität der zyklischen Abbildungen ergibt sich leicht, dass jede zyklische Abbildung  $t(x)$  die zyklische Klasse von  $p(x)$  in sich abbildet. Ist nämlich  $A$  ein beliebiges  $n$ -Eck der erwähnten Klasse, d. h. ein  $n$ -Eck, das der Gleichung  $p(x)A = \mathbf{0}$  genügt, dann erfüllt  $A$  auch  $t(x)p(x)A = \mathbf{0}$  und damit  $p(x)t(x)A = \mathbf{0}$ . Es folgt also, dass mit  $A$  auch  $t(x)A$  zur zyklischen Klasse von  $p(x)$  gehört.

Wir kommen nun zu zwei Sätzen aus der Modultheorie, welche für unsere Untersuchungen grundlegend sind. Ihr Beweis stützt sich auf den folgenden bekannten Satz: Sind  $p(x)$ ,  $q(x)$  zwei Polynome mit dem grössten gemeinsamen Teiler  $g(x)$ , so kann man stets Polynome  $p_1(x)$ ,  $q_1(x)$  finden, welche  $g(x) = p_1(x)p(x) + q_1(x)q(x)$  erfüllen [3\*]. In der Folge gilt mit  $p(x)A = q(x)A = \mathbf{0}$  stets auch  $GGT(p(x), q(x))A = \mathbf{0}$ .

*Zerlegungssatz.* Zu einem  $n$ -Eck, das durch das Produkt der teilerfremden Polynome  $p(x)$ ,  $q(x)$  annulliert wird, existieren eindeutig bestimmte  $n$ -Ecke  $B$ ,  $C$ , welche die Summe  $A$  haben und durch  $p(x)$  bzw.  $q(x)$  annulliert werden: Ist

$$p(x)q(x)A = \mathbf{0}, \quad GGT(p(x), q(x)) = 1, \quad (9)$$

so existiert genau ein Paar von  $n$ -Ecken  $B$ ,  $C$ , so dass

$$A = B + C, \quad p(x)B = q(x)C = \mathbf{0} \quad (10)$$

gilt.

*Beweis.* Erfüllen  $p_1(x)$ ,  $q_1(x)$  die Beziehung  $1 = p_1(x)p(x) + q_1(x)q(x)$ , dann genügen  $B = q_1(x)q(x)A$  und  $C = p_1(x)p(x)A$  den Gleichungen (10). Die Bedingung (10) be-

stimmt  $\mathbf{B}$ ,  $\mathbf{C}$  eindeutig. Genügen auch  $\mathbf{B}'$ ,  $\mathbf{C}'$  derselben, so können wir  $\mathbf{B}' = \mathbf{B}$ ,  $\mathbf{C}' = \mathbf{C}$  beweisen, indem wir aus  $\mathbf{B}' - \mathbf{B} = \mathbf{C} - \mathbf{C}'$  und  $p(x)(\mathbf{B}' - \mathbf{B}) = q(x)(\mathbf{C} - \mathbf{C}') = \mathbf{0}$  zunächst  $q(x)(\mathbf{B}' - \mathbf{B}) = p(x)(\mathbf{C} - \mathbf{C}') = \mathbf{0}$  und daraus  $GGT(p(x), q(x))(\mathbf{B}' - \mathbf{B}) = 1 \cdot (\mathbf{B}' - \mathbf{B}) = GGT(p(x), q(x))(\mathbf{C} - \mathbf{C}') = 1 \cdot (\mathbf{C} - \mathbf{C}') = \mathbf{0}$  herleiten.  $\square$

*Urbildsatz.* Wird das  $n$ -Eck  $\mathbf{B}$  durch das Polynom  $p(x)$  annulliert und ist  $q(x)$  zu  $p(x)$  teilerfremd, so existieren  $n$ -Ecke  $\mathbf{A}$ , die durch  $q(x)$  auf  $\mathbf{B}$  abgebildet werden: Ist

$$p(x)\mathbf{B} = \mathbf{0}, \quad GGT(p(x), q(x)) = 1, \tag{11}$$

so existieren  $n$ -Ecke  $\mathbf{A}$ , so dass

$$q(x)\mathbf{A} = \mathbf{B} \tag{12}$$

gilt.

*Beweis.* Erfüllen  $p_1(x), q_1(x)$  die Beziehung  $1 = p_1(x)p(x) + q_1(x)q(x)$ , dann gilt  $\mathbf{B} = p_1(x)p(x)\mathbf{B} + q_1(x)q(x)\mathbf{B} = \mathbf{0} + q_1(x)q(x)\mathbf{B} = q(x)q_1(x)\mathbf{B}$ . Das  $n$ -Eck  $\mathbf{A} = q_1(x)\mathbf{B}$  wird also durch  $q(x)$  auf  $\mathbf{B}$  abgebildet.  $\square$

Der Zerlegungssatz kann dahin ergänzt werden, dass mit  $p(x) \cdot \mathbf{B} = \mathbf{0}$  und  $q(x)\mathbf{C} = \mathbf{0}$  auch  $p(x)q(x) \cdot (\mathbf{B} + \mathbf{C}) = \mathbf{0}$  gilt. Zum Beweis des Urbildsatzes ist zu bemerken, dass das konstruierte Urbild  $\mathbf{A}$  von  $\mathbf{B}$  gleich  $\mathbf{B}$  durch  $p(x)$  annulliert wird. Mit dieser Sonder-eigenschaft steht  $\mathbf{A} = q_1(x)\mathbf{B}$  unter den Urbildern von  $\mathbf{B}$  allein da, weil sich aus  $q(x)\mathbf{A}' = q(x)\mathbf{A} = \mathbf{B}$  und  $p(x)\mathbf{A}' = p(x)\mathbf{A} = \mathbf{0}$  sofort  $GGT(p(x), q(x))(\mathbf{A}' - \mathbf{A}) = 1 \cdot (\mathbf{A}' - \mathbf{A}) = \mathbf{0}$  und damit  $\mathbf{A}' = \mathbf{A}$  ergibt.

Unsere beiden Sätze samt Ergänzungen können für zyklische Klassen formuliert werden. Sind  $p(x), q(x)$  teilerfremde Polynome, so ist die zyklische Klasse von  $p(x)q(x)$  die direkte Summe derjenigen von  $p(x)$  und derjenigen von  $q(x)$  (Zerlegungssatz); das Polynom  $q(x)$  bildet die zyklische Klasse von  $p(x)q(x)$  auf die (in ihr enthaltene) Klasse von  $p(x)$  ab und wirkt dabei als Permutation der letzteren Klasse (Urbildsatz).

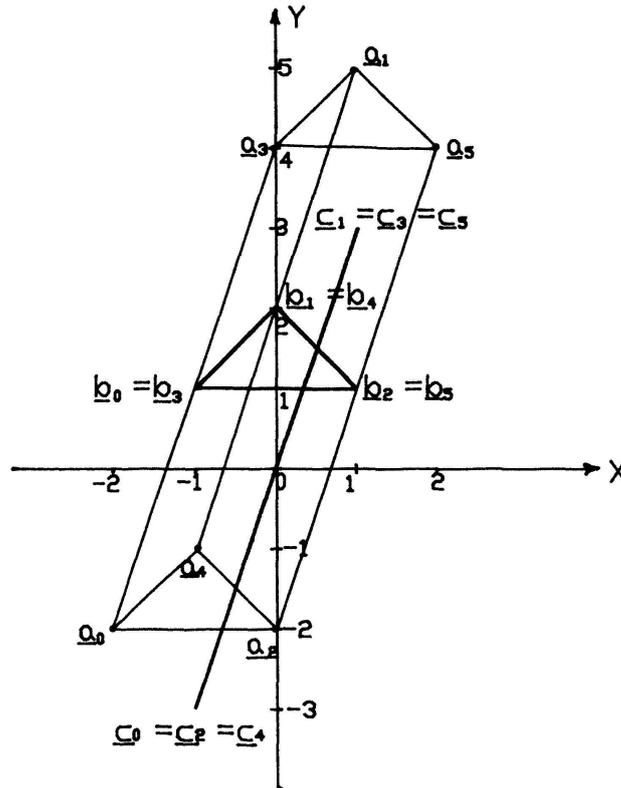
*Beispiel 7 (Zerlegungs- und Urbildsatz)*

Wir bezeichnen ein Sechseck  $\mathbf{A} = (\underline{a}_0, \underline{a}_1, \dots, \underline{a}_5)$  als *Prisma*, wenn seine grossen Diagonalen  $(\underline{a}_0 \underline{a}_3, \underline{a}_2 \underline{a}_5, \underline{a}_4 \underline{a}_1)$  parallelgleich sind, d. h. wenn sie die Seitenkanten eines dreiseitigen Prismas darstellen (Fig. 1). Die Ecken eines solchen Prismas bestimmen sich rekursiv aus der Formel  $\underline{a}_{i+4} - \underline{a}_{i+1} = -(\underline{a}_{i+3} - \underline{a}_i)$ ,  $i = 0, 1, \dots, 5$ , und genügen damit

$$(x^4 + x^3 - x - 1)\mathbf{A} = \mathbf{0}.$$

Aus der Faktorzerlegung

$$(x^4 + x^3 - x - 1) = (x^3 - 1)(x + 1), \quad GGT(x^3 - 1, x + 1) = 1,$$



Figur 1

ergibt sich mit Hilfe des Zerlegungssatzes die Existenz und Eindeutigkeit von Sechsecken  $B, C$ , die

$$A = B + C, \quad (x^3 - 1)B = (x + 1)C = 0$$

erfüllen. Unser Prisma ist also die Summe eines zweifach durchlaufenen Dreiecks und eines dreifach durchlaufenen Zweiecks mit Schwerpunkt  $\underline{0}$  (s. Beispiele 5, 6). Aus  $x^3 - 1 = (x^2 - x + 1)(x + 1) - 2$  (Eukl. Algorithmus) folgt

$$\left(-\frac{1}{2}\right)(x^3 - 1) + \left(\frac{1}{2}x^2 - \frac{1}{2}x + \frac{1}{2}\right)(x + 1) = 1$$

und daher nach dem Beweis des Zerlegungssatzes

$$B = \left(\frac{1}{2}x^2 - \frac{1}{2}x + \frac{1}{2}\right)(x + 1)A, \quad C = \left(-\frac{1}{2}\right)(x^3 - 1)A.$$

In unserer Figur ist das gegebene (zweidimensionale) Prisma  $A = ((-2, -2), (1, 5), (0, -2), (0, 4), (-1, -1), (2, 4))$  und damit  $B = ((-1, 1), (0, 2), (1, 1), (-1, 1), (0, 2), (1, 1))$ ,  $C = ((-1, -3), (1, 3), (-1, -3), (1, 3), (-1, -3), (1, 3))$ . Nach dem Beweis des Urbildsatzes hat  $B$  das Urbild  $A_u = \left(\frac{1}{2}x^2 - \frac{1}{2}x + \frac{1}{2}\right)B$  bezüglich  $x + 1$ , wobei  $A_u$  gleich  $B$  ein zweifach durchlaufenes Dreieck ist. Für  $B$  wie oben ist  $A_u = ((0, 0), (-1, 1), (1, 1), (0, 0), (-1, 1), (1, 1))$ .

4. Jedes  $n$ -Eck  $A$  genügt der Formel  $(x^n - 1)A = \mathbf{0}$ . Das bedeutet gemäss den Betrachtungen in Abschnitt 3, dass  $x^n - 1$  durch das zu  $A$  gehörige Annullatorpolynom ohne Rest teilbar ist. Ein Polynom  $m_A(x)$  besitzt also keineswegs eine beliebige Primteilerzerlegung, sondern vielmehr eine solche, deren Faktoren derjenigen von  $x^n - 1$ ,  $x^n - 1 = p_1(x)p_2(x)\dots p_k(x)$ , entnommen sind. Welche Polynome Primfaktoren  $p_i(x)$  von  $x^n - 1$  sind, hängt vom gegebenen Koeffizientenkörper  $K$  ab. Wir behaupten, dass wenn die Charakteristik von  $K$  kein Teiler von  $n$  ist,  $x^n - 1$  in paarweise verschiedene Primfaktoren zerfällt [4\*].

Zum Beweis gehen wir von einem Körper  $K$  aus, in dessen Polynombereich das Polynom  $x^n - 1$  den Faktor  $(p(x))^s$  besitzt, wo  $p(x)$  prim und  $s \geq 2$  ist. Die Ableitung  $nx^{n-1}$  von  $x^n - 1$  ist dann durch  $(p(x))^{s-1}$  teilbar und damit durch  $p(x)$ . Das Polynom  $p(x)$  ist dabei aber nicht gleich  $x$ , weil  $x$  kein Teiler von  $x^n - 1$  ist, was bedeutet, dass  $nx^{n-1}$ , um durch  $p(x)$  dividierbar zu sein, identisch verschwinden muss. Nun ist  $x^{n-1}$ ,  $n$ -mal zu sich selbst addiert, nur dann für alle  $x$  gleich 0, wenn der unseren Betrachtungen zugrunde liegende Körper  $K$  eine Charakteristik aufweist, die gleich  $n$  oder gleich einem echten Teiler von  $n$  ist. Unter den Bedingungen der Behauptung existiert der Teiler  $(p(x))^s$  von  $x^n - 1$  also nicht.  $\square$

Wir wollen im folgenden voraussetzen, dass das bezüglich unserer  $n$ -Ecke definierte Multiplikatorpolynom  $x^n - 1$  über dem gegebenen Koeffizientenkörper  $K$  in lauter verschiedene Primfaktoren zerfällt. Auf Grund des vorangegangenen entspricht diese Voraussetzung *der von nun an als erfüllt angesehenen Bedingung, dass der unserem Vektorraum  $V(K)$  zugrunde liegende Körper  $K$  eine Charakteristik besitzt, die kein Teiler von  $n$  ist* [5\*]. Wir beschließen diesen Abschnitt mit zwei unmittelbaren und wichtigen Konsequenzen des früheren Zerlegungssatzes, die nur unter den eben gemachten Bedingungen gültig sind.

*Zerlegungssatz (zweite Version) [6\*].* Ein  $n$ -Eck  $\neq \mathbf{0}$  kann in genau einer Weise als Summe von nichtverschwindenden  $n$ -Ecken dargestellt werden, welche Primfaktoren des Polynoms  $x^n - 1$  als Annullatoren haben. Die betreffenden Primfaktoren sind die minimalen Annullatoren der ihnen zugeordneten Summanden- $n$ -Ecke und ihr Produkt ist gleich dem minimalen Annullator  $m_A(x)$  von  $A$ .

*Bemerkung.* Wir betrachten hier nur solche Zerlegungen von  $A$ , in denen Glieder, die von denselben Polynomen annulliert werden, schon addiert sind.

*Beweis.* Es ist klar, dass das Null- $n$ -Eck  $\mathbf{0}$  die Konstante 1 als minimalen Annullator besitzt und jedes andere  $n$ -Eck ein nichtkonstantes Polynom. Wird das  $n$ -Eck  $A \neq \mathbf{0}$  von einem (normierten) Primpolynom annulliert, so handelt es sich bei diesem automatisch um den minimalen Annullator.

Gemäss dem früheren Zerlegungssatz gibt es genau eine Zerlegung von  $A$ ,  $A = B_1 + \dots + B_r$ , deren Glieder der Reihe nach von den Primfaktoren  $p_1(x), \dots, p_r(x)$  des zu  $A$  gehörigen Polynoms  $m_A(x)$  annulliert werden. Es kann dabei keines der  $n$ -Ecke  $B_i$  gleich  $\mathbf{0}$  sein, weil sonst  $A = B_1 + \dots + B_{i-1} + B_{i+1} + \dots + B_r$  und in der Folge  $(m_A(x)/p_i(x))A = \mathbf{0}$  wäre, entgegen der Definition von  $m_A(x)$ . Also ist für alle  $i$   $p_i(x)$  der minimale Annullator von  $B_i$  und die angegebene Zerlegung von  $A$  eine Summendarstellung im Sinne der Behauptung.

Liegt irgendeine andere Zerlegung von  $A$  vor, deren Glieder durch Primpolynome annulliert werden, so wird  $A$  wiederum vom Produkt derselben annulliert. Dieses Produkt ist damit durch  $m_A(x)$  teilbar und zählt in der Folge  $p_1(x), \dots, p_r(x)$  (nebst anderen Primpolynomen) unter seinen Faktoren. Wir behaupten, dass unsere neue Zerlegung von der Form  $A = B_1 + \dots + B_r + \mathbf{0} + \dots + \mathbf{0}$  ist. Zum Beweis stellen wir zuerst fest, dass wir die gegebenen Primfaktoren den angeführten Summanden in eineindeutiger Weise als Annullatoren zuordnen können. Nun bestimmen aber diese Faktoren (nach dem ersten Zerlegungssatz) die ihnen zugeordneten Summanden eindeutig. Das bedeutet, dass die vorliegende Zerlegung von  $A$  die angegebene Form hat. Weil in ihr aber  $\mathbf{0}$ -Terme auftreten, ist sie keine Zerlegung im Sinne der Behauptung. Die einzige solche ist also die im vorigen Abschnitt beschriebene.  $\square$

*Translationssatz.* Das  $n$ -Eck  $A$  hat genau dann den Schwerpunkt  $\underline{0}$ , wenn das zu ihm gehörige Annullatorpolynom  $m_A(x)$  nicht durch  $x - 1$  teilbar ist. Gilt  $m_A(x) = (x - 1)m_A^0(x)$ , so existieren eindeutig bestimmte Polygone  $T_A, A^0$ , welche

$$A = T_A + A^0, \quad (x - 1)T_A = m_A^0(x)A^0 = \mathbf{0},$$

erfüllen, wo  $T_A = (\underline{t}, \underline{t}, \dots, \underline{t})$  ein Translations- $n$ -Eck  $\neq \mathbf{0}$  und  $A^0$  ein  $n$ -Eck mit Schwerpunkt  $\underline{0}$  darstellt.

*Beweis.* Beachten wir den Zerlegungssatz, so müssen wir lediglich beweisen, dass wenn  $m_A(x)$  den Faktor  $x - 1$  nicht enthält,  $A$  den Schwerpunkt  $\underline{0}$  hat. Ist  $x - 1$  kein Faktor von  $m_A(x)$ , dann ist das Polynom  $x^{n-1} + x^{n-2} + \dots + 1$  wegen  $x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \dots + 1)$  durch  $m_A(x)$  teilbar. Es gilt dann also  $(x^{n-1} + x^{n-2} + \dots + 1)A = \mathbf{0}$ . Hat  $A$  den Schwerpunkt  $\underline{s}$ , dann hat das Polygon auf der linken Seite der letzten Gleichung den Schwerpunkt  $n\underline{s}$ . Das Polygon auf der rechten Seite hat den Schwerpunkt  $\underline{0}$ ; es gilt also  $n\underline{s} = \underline{0}$  und damit  $\underline{s} = \underline{0}$ .  $\square$

**5.** Wie wir im vorigen Abschnitt gesehen haben, baut sich jedes  $n$ -Eck aus einfachsten  $n$ -Ecken auf, welche schon von Primpolynomen annulliert werden. Dabei müssen diese primen Polynome Teiler von  $x^n - 1$  sein, was heisst, dass es gerade soviele Arten von Bausteinen gibt, wie Primfaktoren von  $x^n - 1$  [7\*]. Wir werden im folgenden, von der Primteilerzerlegung von  $x^n - 1$  im komplexen, reellen und rationalen Fall ausgehend die jeweils einfachsten  $n$ -Ecke charakterisieren.

Die Lösungen der Gleichung  $x^n = 1$ , die  $n$ ten Einheitswurzeln, sind im Rahmen des komplexen Zahlensystems mit  $w_0, w_1, \dots, w_{n-1}$  identisch, wo  $w_k = e^{\frac{k}{n}2\pi i} = \cos\left(\frac{k}{n}2\pi\right) + i \sin\left(\frac{k}{n}2\pi\right)$  ist für  $k = 0, 1, \dots, n - 1$ . Die Einheitswurzel  $w_k$  wird *primitiv* genannt, falls die minimale positive Grösse  $\nu$ , für die  $w_k = e^{\frac{\nu k}{n}2\pi i} = 1$  gilt, gleich  $n$  ist. Offensichtlich ist  $w_k$  genau dann primitiv, wenn  $k$  und  $n$  teilerfremd sind. Für alle  $n$  ist  $w_0 = 1$ .

Wir entnehmen dem vorangehenden Absatz, dass das Polynom  $x^n - 1$  die Primteilerzerlegung  $x^n - 1 = (x - w_0)(x - w_1)\dots(x - w_{n-1})$  aufweist. Ein  $n$ -Eck, das vom Faktor  $x - w_k$  dieser Zerlegung annulliert wird, ist augenscheinlich von der Form  $(\underline{a}, w_k \underline{a}, \dots, w_k^{n-1} \underline{a})$ , d. h. es liegt auf einer Geraden durch  $\underline{0}$  des Vektorraums  $V(\mathbb{C})$ .

Wir beschränken uns in den folgenden Untersuchungen auf den besonders interessanten Fall, dass der gegebene Vektorraum  $V(\mathbb{C})$  eindimensional und somit mit einer einzigen komplexen Geraden identisch ist. Seine Punkte können demgemäss als komplexe Skalare angesehen werden und damit als Elemente der *Gauss'schen Zahlenebene*. Ein betrachtetes  $n$ -Eck im besonderen wird zum  $n$ -Tupel komplexer Zahlen und so zu einer  $n$ -punktigen Figur in dieser Ebene [8\*].

Die für uns speziell wichtigen  $n$ -Ecke  $(a, w_k a, \dots, w_k^{n-1} a)$ ,  $a \neq 0$ , mit der  $(v + 1)$ ten Ecke  $w_k a = e^{\frac{vk}{n} 2\pi i} a$  gehen aus  $a$  durch hintereinander erfolgende Rotationen mit Zentrum 0 und Drehwinkel  $\frac{k}{n} 2\pi$  hervor.

Gilt  $GGT(k, n) = 1$ , d. h. ist  $w_k$  eine primitive  $n$ -te Einheitswurzel, so sind alle Ecken von  $A = (a, w_k a, \dots, w_k^{n-1} a)$  voneinander verschieden und  $A$  ist ein reguläres  $n$ -Eck mit Schwerpunkt 0. Für  $k \neq 1$  ist  $A$  ein konvexes, positiv umlaufenes Polygon; für  $k = n - 1$  können wir den Drehwinkel  $\frac{n-1}{n} 2\pi$  mit  $\frac{n-1}{n} 2\pi - 2\pi = -\frac{1}{n} 2\pi$  identifizieren, wodurch  $A$  als ein konvexes, negativ umlaufenes  $n$ -Eck erscheint; in allen anderen Fällen ist  $A$  ein Stern- $n$ -Eck.

Ist  $GGT(k, n) = u_k, u_k > 1$ , und setzen wir  $k = k' u_k, n = n_k u_k$ , so ist der  $w_k$  zugeordnete Rotationswinkel  $\frac{k}{n} 2\pi$  gleich  $\frac{k'}{n_k} 2\pi$ . Daraus und aus  $GGT(k', n_k) = 1$  folgt, dass es sich bei  $(a, w_k a, \dots, w_k^{n-1} a)$  um ein  $u_k$ -fach durchlaufenes reguläres  $n_k$ -Eck mit Zentrum 0 handelt. Ist  $k = 0, w_k = w_0 = 1$ , so stimmt  $A = (a, w_0 a, \dots, w_0^{n-1} a)$  mit dem Translations- $n$ -Eck  $(a, a, \dots, a)$  überein.

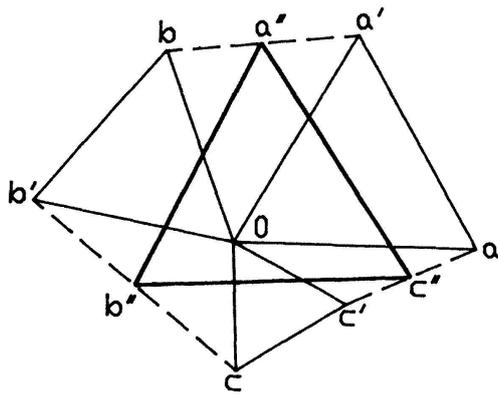
Die Bausteine aller komplexen  $n$ -Ecke sind also neben den Translations- $n$ -Ecken die regulären  $n$ -Ecke mit Zentrum 0 und die  $u_k$ -fach durchlaufenen regulären  $(n/u_k)$ -Ecke mit Zentrum 0. Ein  $n$ -Eck der Form  $(a, w_k a, \dots, w_k^{n-1} a)$ ,  $k \neq 0$ , wird im folgenden *k-regulär* genannt.

### Beispiele 8, 9

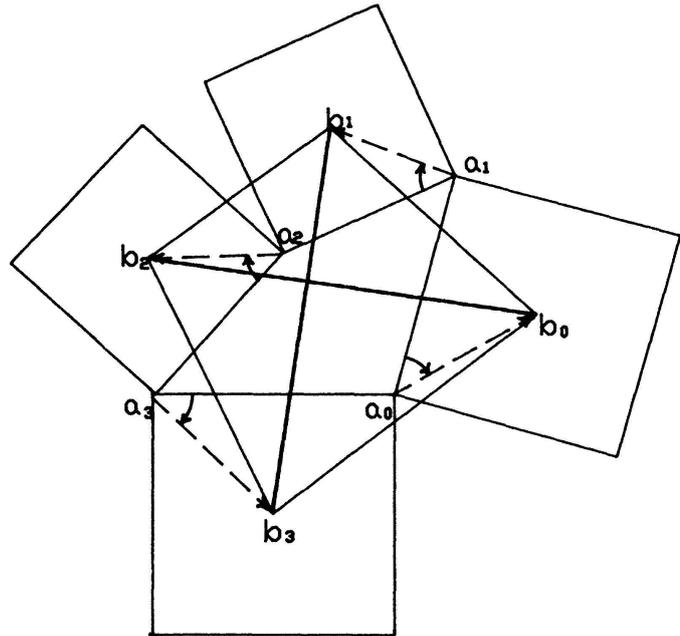
Es handelt sich bei ihnen um zwei Sätze aus der in der Einleitung zitierten Arbeit von M. Jeger (Primärquellen daselbst), für die wir einen Beweis im Sinne unserer Theorie geben.

8. (Propellersatz). Sind  $(0, a, a')$ ,  $(0, b, b')$  und  $(0, c, c')$  drei o.B.d.A. positiv umlaufene, gleichseitige Dreiecke, welche ihre erste Ecke im Ursprung haben, so ist das aus den Mittelpunkten der Strecken  $a' b, b' c$  und  $c' a$  gebildete Dreieck  $M = (a'', b'', c'')$  ebenfalls positiv umlaufen und gleichseitig (Fig. 2).

*Beweis.* Aus unseren Annahmen folgt, dass das Dreieck  $D = (a, b, c)$  durch eine  $60^\circ$ -Drehung um den Ursprung in  $D' = (a', b', c')$  übergeführt wird, d.h., dass  $D' = w_{6,1} D = e^{(1/6) 2\pi i} D$  gilt. Diese Gleichung können wir unseren Zwecken besser anpassen, wenn wir den zu regulären Sechsecken gehörigen Faktor  $w_{6,1} = \cos(\pi/3) + i \sin(\pi/3)$  durch  $-w_2 = -e^{2/3 2\pi i} = -\cos(4\pi/3) - i \sin(4\pi/3)$  ersetzen und so mit  $w_2$



Figur 2



Figur 3

eine regulären Dreiecken zugeordnete Zahl ins Spiel bringen. Beachten wir noch  $x\mathbf{D} = (b, c, a)$ , so haben wir

$$\mathbf{M} = \frac{1}{2}(x\mathbf{D} + \mathbf{D}') = \frac{1}{2}(x + w_{6,1})\mathbf{D} = \frac{1}{2}(x - w_2)\mathbf{D}$$

und in der Folge

$$(x - 1)(x - w_1)\mathbf{M} = \frac{1}{2}(x - 1)(x - w_1)(x - w_2)\mathbf{D} = \frac{1}{2}(x^3 - 1)\mathbf{D} = \mathbf{0}.$$

Aus der letzten Gleichung schliessen wir, dass  $\mathbf{M} = \mathbf{T}_M + \mathbf{M}^0$  ist, wo  $\mathbf{T}_M$  ein Translations- $n$ -Eck und  $\mathbf{M}^0$  ein positiv umlaufenes, reguläres (gleichseitiges) Dreieck mit Zentrum  $\mathbf{0}$  darstellt.  $\square$

9. Werden über den Seiten eines Vierecks Quadrate errichtet, und zwar entweder alle nach aussen oder alle nach innen, dann definieren die erhaltenen Quadratmittelpunkte ein Viereck, dessen Diagonalen gleichlang sind und aufeinander senkrecht stehen.

*Beweis.* Das gegebene Viereck sei als Quadrupel  $\mathbf{A} = (a_0, a_1, a_2, a_3)$  so durchlaufen, dass die konstruierten Quadrate in bezug auf es rechts liegen. Bilden die Mittelpunkte dieser Quadrate das Viereck  $\mathbf{B} = (b_0, b_1, b_2, b_3)$ , so werden die Verbindungsvektoren entsprechender Ecken von  $\mathbf{A}$  und  $\mathbf{B}$  durch eine Drehstreckung der Seitenvektoren von  $\mathbf{A}$  erhalten. Aus dem Seitenvektorenviereck  $(x - 1)\mathbf{A}$  erhalten wir das Viereck der Verbindungsvektoren  $\mathbf{B} - \mathbf{A}$ , indem wir jeden Vektor auf  $\sqrt{2}/2$  seiner Länge verkürzen und um  $-45^\circ$  drehen (s. Fig. 3). Es gilt also  $\mathbf{B} - \mathbf{A} = (\cos(-\pi/4) + i \sin(-\pi/4))(\sqrt{2}/2)(x - 1)\mathbf{A}$ , oder kürzer

$$\mathbf{B} = \frac{1}{2}[(1 - i)x + (1 + i)]\mathbf{A}.$$

Das Viereck der Diagonalvektoren von  $B$ ,  $D = (x^2 - 1)B$ , genügt in der Folge der Gleichung

$$D = \frac{1}{2}[(1-i)x^3 + (1+i)x^2 - (1-i)x - (1+i)]A.$$

Multiplizieren wir  $D$  mit  $x - w_1 = x - e^{(1/4)2\pi i} = x - i$ , so erhalten wir unter Beachtung von  $(x^4 - 1)A = 0$

$$(x - w_1)D = (x - i)D = \frac{1}{2}[(1-i)x^4 - (1-i)]A = 0.$$

Damit ist gezeigt, dass es sich bei  $D$  um ein positiv umlaufenes, konvexes, reguläres Viereck mit Schwerpunkt 0 handelt. Das Diagonalenviereck  $D$  von  $B$  ist also ein Quadrat mit Zentrum 0, was beweist, dass zwei benachbarte Diagonalenvektoren von  $B$  gleichlang sind und aufeinander senkrecht stehen.  $\square$

*Bemerkung.* Die Zerlegungstheorie komplexer  $n$ -Ecke kann auch von einem ganz anderen Ansatz her angegangen werden. Um diese zweite Interpretation zu erläutern, wählen wir ein beliebiges  $n$ -Eck  $A = (a_0, a_1, \dots, a_{n-1})$  und denken uns dasselbe vollständig in seine regulären und Translationskomponenten zerlegt:

$$A = (x_0, x_0, \dots, x_0) + (x_1, w_1 x_1, \dots, w_1^{n-1} x_1) + \dots + (x_{n-1}, w_{n-1} x_{n-1}, \dots, w_{n-1}^{n-1} x_{n-1}),$$

$$w_k = e^{\frac{k}{n}2\pi i} \quad \text{für } k = 0, 1, \dots, n-1. \quad (13)$$

Nicht auftretende Komponenten seien dabei als  $0$ - $n$ -Ecke eingefügt. Eine leichte Modifikation von (13) ergibt

$$A = x_0(1, 1, \dots, 1) + x_1(1, w_1, \dots, w_1^{n-1}) + \dots + x_{n-1}(1, w_{n-1}, \dots, w_{n-1}^{n-1}) \quad (14)$$

und wird bei Benutzung der Abkürzungen  $R_0 = (1, 1, \dots, 1)$ ,  $R_1 = (1, w_1, \dots, w_1^{n-1})$ ,  $\dots$ ,  $R_{n-1} = (1, w_{n-1}, \dots, w_{n-1}^{n-1})$  zu

$$A = x_0 R_0 + x_1 R_1 + \dots + x_{n-1} R_{n-1}. \quad (15)$$

Offensichtlich bilden die Polygone  $R_0, R_1, \dots, R_{n-1}$  eine Basis des Vektorraums aller komplexen  $n$ -Ecke. Aus den Gleichungen (13) berechnet sich die Koordinate  $x_k$  von  $A$  als

$$x_k = \frac{1}{n}(a_0 \bar{w}_k^0 + a_1 \bar{w}_k^1 + \dots + a_{n-1} \bar{w}_k^{n-1}), \quad k = 0, 1, \dots, n-1,$$

$$\bar{w}_k = e^{-\frac{k}{n}2\pi i}. \quad (16)$$

Sie ist der  $k$ te endliche Fourier-Koeffizient von  $A$  und die Gleichungen (14), (15) sind die endlichen Fourier-Reihen-Darstellungen von  $A$  (s. [5]).

Wir gehen nun zur Charakterisierung der einfachsten Polygone der reellen Ebene über und studieren zu diesem Zweck die Zerlegung von  $x^n - 1$  in Primfaktoren mit reellen Koeffizienten. Das reelle Zahlssystem ist im komplexen enthalten und so ist jedes reelle Polynom automatisch auch ein komplexes Polynom. Ein reelles Polynom braucht aber nicht unzerlegbar zu sein im komplexen Bereich.

Zunächst hat  $x^n - 1$  den reellen linearen Primteiler  $x - w_0 = x - 1$ , der zu den Translations- $n$ -Ecken  $(a, a, \dots, a)$ ,  $a \neq 0$ , gehört. Dazu kommt, falls  $n$  eine gerade Zahl ist, der Primteiler  $x - w_{n/2} = x + 1$ , welcher die  $n$ -Ecke der Form  $(a, -a, a, -a, \dots, a, -a)$  annulliert (s. das frühere Beispiel 6).

Alle anderen Primfaktoren haben, wie wir gleich zeigen werden, die Form

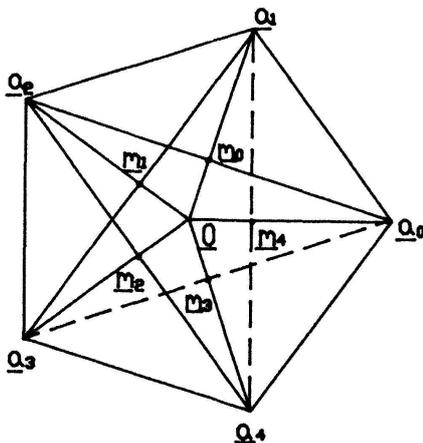
$$(x - w_k)(x - w_{n-k}) = x^2 - 2 \cos\left(\frac{k}{n} 2\pi\right)x + 1, \quad k \neq 0, \frac{n}{2}. \tag{17}_k$$

Aus der trigonometrischen Darstellung von  $w_k, w_{n-k}$  folgt, dass die Gleichung von (17) stimmt und dass  $w_k, w_{n-k}$  für  $k \neq 0, \frac{n}{2}$  nichtreelle Grössen sind. Auf der rechten Seite von (17) steht also ein reelles Primpolynom.

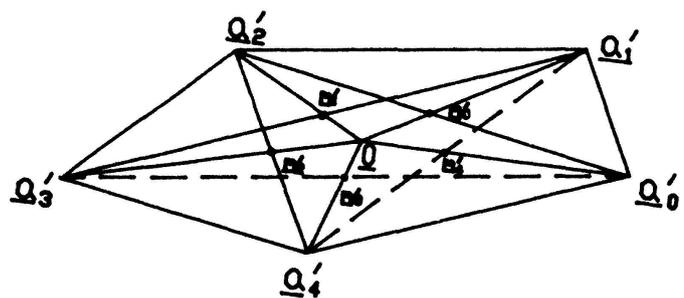
Zu den Polygonen, die vom Polynom in  $(17)_k$  annulliert werden, gehören zunächst einmal die euklidisch  $k$ -regulären  $n$ -Ecke [9\*]. Sind nämlich  $a_i, a_{i+1}, a_{i+2}$  drei zyklisch aufeinanderfolgende Ecken des  $k$ -regulären  $n$ -Ecks  $A = (a_0, a_1, \dots, a_{n-1})$  und ist  $m_i$  der Mittelpunkt von  $a_i, a_{i+2}$ , so gilt wegen  $|0, a_i| = |0, a_{i+1}|$  die Beziehung  $m_i = \frac{1}{2} \cdot (a_i + a_{i+2}) = \cos\left(\frac{k}{n} 2\pi\right) \cdot a_{i+1}$  (s. Fig. 4(a)). Und diese entspricht, für alle  $i$  beachtet, der Gleichung

$$\left(x^2 - 2 \cos\left(\frac{k}{n} 2\pi\right)x + 1\right) A = 0.$$

Wird eine lineare Transformation auf das  $n$ -Eck  $A$  angewandt, so entsteht aus demselben ein  $n$ -Eck  $A' = (a'_0, a'_1, \dots, a'_{n-1})$ , dessen Ecken durch die gleichen linearen Beziehungen verbunden sind. Es gilt also für alle  $i$   $\frac{1}{2}(a'_i + a'_{i+2}) = \cos\left(\frac{k}{n} 2\pi\right) a'_{i+1}$  und  $A'$  erfüllt  $\left(x^2 - 2 \cos\left(\frac{k}{n} 2\pi\right)x + 1\right) A' = 0$  (Fig. 4(b)).



Figur 4(a)



Figur 4(b)

Sind  $\underline{a}_0, \underline{a}_1$  zwei linear unabhängige Vektoren und  $\underline{a}'_0, \underline{a}'_1$  zwei beliebige weitere Vektoren, so gibt es genau eine lineare Transformation, die  $\underline{a}_0$  in  $\underline{a}'_0$  und  $\underline{a}_1$  in  $\underline{a}'_1$  überführt. (Sie bildet  $x = x_0 \underline{a}_0 + x_1 \underline{a}_1$  auf  $x' = x_0 \underline{a}'_0 + x_1 \underline{a}'_1$  ab.) Wir können also ein und nur ein  $n$ -Eck  $A'$  finden, dessen erste zwei Ecken  $\underline{a}'_0, \underline{a}'_1$  vorgegeben sind und das Glied um Glied aus  $A$  durch eine lineare Transformation hervorgeht. Nun ist  $A'$  aber überhaupt das einzige  $n$ -Eck, das die Anfangsecken  $\underline{a}'_0, \underline{a}'_1$  und den Annullator  $x^2 - 2 \cos \left( \frac{k}{n} 2 \pi \right) x + 1$  besitzt, da diese Vorgaben die späteren Ecken induktiv bestimmen. Die von  $x^2 - \cos \left( \frac{k}{n} 2 \pi \right) x + 1$  annullierten  $n$ -Ecke sind also entweder  $k$ -regulär oder sie gehen aus einem  $k$ -regulären  $n$ -Eck durch eine lineare Transformation hervor. Wir nennen die betreffenden  $n$ -Ecke, die wesentlichen Bausteine allgemeinerer  $n$ -Ecke, *k-affin-regulär* [10\*]. Der Begriff schliesst eindimensionale Polygone mit ein.

*Bemerkung.* Es gibt auch in der *Gauss*schen Zahlenebene  $k$ -affin-reguläre  $n$ -Ecke. Sie haben denselben Annullator und dieselbe Gestalt wie diejenigen in der reellen Ebene. Was sie aber von letzteren unterscheidet, ist, dass sie weiter zerlegt werden können, und zwar, wie aus (17) hervorgeht, in ein  $k$ -reguläres und ein  $(n - k)$ -reguläres  $n$ -Eck. Wir fügen hier noch an, dass der bekannte Satz von Napoleon-Barlotti (s. [2], [4]), der affin-reguläre und reguläre  $n$ -Ecke verbindet, in der *Gauss*schen Ebene bewiesen werden muss, weil die regulären  $n$ -Ecke in der reellen Ebene keine durch ein Polynom definierte zyklische Klasse darstellen.

*Beispiel 10*

Aus der Faktorzerlegung  $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$  folgt, dass jedes Viereck  $A$  die Darstellung  $A = (\underline{b}, \underline{b}, \underline{b}, \underline{b}) + (\underline{c}, -\underline{c}, \underline{c}, -\underline{c}) + (\underline{d}, \underline{e}, -\underline{d}, -\underline{e})$  besitzt. Wegen  $x^2 + 1 = (x - i)(x + i) = (x - w_1)(x - w_3) = x^2 - 2 \cos \left( \frac{1}{4} 2 \pi \right) x + 1$  gilt, dass der letzte Summand, ein Parallelogramm mit Schwerpunkt  $0$ , im Reellen unzerlegbar ist und durch eine lineare Transformation aus einem Quadrat  $(\underline{a}_i, \underline{a}_{i+1}) = \cos^{-1} \cos \left( \frac{1}{4} 2 \pi \right) = \frac{\pi}{2}$  hervorgeht.

Als letztes beschreiben wir die einfachsten Bausteine von  $n$ -Ecken in der rationalen Ebene. Für die dazu nötige Bestimmung der Primfaktoren von  $x^n - 1$  gehen wir wie im reellen Fall davon aus, dass die rationalen Primfaktoren gleich komplexen Primfaktoren oder gleich Produkten komplexer Primfaktoren sind.

Den diesbezüglichen Betrachtungen sei vorausgeschickt, dass wo wir von Teilern von  $x^n - 1$  sprechen, wir den komplexen Polynombereich anvisieren. Auch werden wir ohne besondere Erwähnung von der Äquivalenz der Aussagen « $k$  ist ein Teiler von  $l$ » und « $x^k - 1$  ist ein Teiler von  $x^l - 1$ » Gebrauch machen. Die Abkürzungen für «ist Teiler von» und «ist ein echter Teiler von» sind  $|, ||$ .

Wir beginnen mit zwei Definitionen. Die Menge  $C(t)$ , wo  $t|n$  gilt, umfasse diejenigen Primfaktoren von  $x^n - 1$ , die auch Teiler von  $x^t - 1$  sind, nicht aber Teiler von  $x^\tau - 1$  für  $\tau < t$ :

$$C(t) = \{x - w_k : x - w_k | x^t - 1, \not| x^\tau - 1, \text{ für } \tau < t, (t|n)\}. \tag{18}$$

Offenbar umfasst  $C(t)$  genau diejenigen linearen Polynome  $x - w_k$ , deren Konstante eine primitive  $t$ -te Einheitswurzel ist. Man beachte, dass das System der Mengen  $C(t)$  eine Klasseneinteilung der Menge aller Primteiler von  $x^n - 1$  darstellt. – Die Menge  $D(t)$ , wo  $t|n$  gilt, umfasse die sämtlichen Primfaktoren von  $x^t - 1$ :

$$D(t) = \{x - w_k : x - w_k | x^t - 1\}, \quad (t|n). \quad (19)$$

Zusammengenommen enthalten die Mengen  $D(t)$  alle Primteiler von  $x^n - 1$ , wobei sie sich aber gegenseitig überlappen. Für das folgende ist wichtig, dass  $D(t)$  die Vereinigungsmenge der Klassen  $C(\tau)$ , die  $\tau|t$  erfüllen, darstellt. Es gilt also

$$D(t) = \bigcup_{\tau|t} C(\tau) \quad (20)$$

und in der Folge

$$C(t) = D(t) \setminus \bigcup_{\tau||t} C(\tau). \quad (21)$$

Aus (20) folgt unschwer  $\bigcup_{\tau||t} C(\tau) = \bigcup_{\tau||t} D(\tau)$ , was mit (21) kombiniert

$$C(t) = D(t) \setminus \bigcup_{\tau||t} D(\tau) \quad (22)$$

ergibt. – Wir werden die Formeln (21), (22) im Zusammenhang mit gewissen Polynomen brauchen, die den Klassen  $C(t)$  zugeordnet sind. Unter dem *Kreisteilungspolynom*  $F_t(x)$  verstehen wir das Produkt der Polynome  $x - w_k$  aus  $C(t)$ .

Wir wollen im folgenden zeigen, dass die Kreisteilungspolynome  $F_t(x)$ ,  $t|n$ , rationale Koeffizienten haben. Dazu bemerken wir zuerst, dass das Produkt der komplexen Primpolynome aus  $\bigcup_{\tau||t} C(\tau)$  gleich  $\prod_{\tau||t} F_\tau(x)$  ist. Das mit ihm identische Produkt der

Primpolynome aus  $\bigcup_{\tau||t} D(\tau)$  (die Mengen  $D(\tau)$  überlappen) ist gleich dem

$KGV \{x^\tau - 1 : \tau || t\}$ . Daraus resultiert nach (21), (22)

$$F_t(x) = \frac{x^t - 1}{\prod_{\tau||t} F_\tau(x)} = \frac{x^t - 1}{KGV \{x^\tau - 1 : \tau || t\}} \quad (t|n). \quad (23)$$

Da Zähler und Nenner des zweiten Bruches rationale Koeffizienten haben, trifft das auch für den Quotienten  $F_t(x)$  zu. Man kann sogar zeigen, dass alle Kreisteilungspolynome ganzzahlige Koeffizienten haben und – für uns wichtiger – dass sie im rationalen Bereich prim sind [11\*].

**Beispiel 11.** (Bestimmung der in  $x^{20} - 1$  enthaltenen Kreisteilungspolynome)

Diese ergeben sich gemäss Formel (23) aus  $F_1(x)$ .

$$F_1(x) = x - w_0 = x - 1$$

$$F_2(x) = \frac{x^2 - 1}{F_1(x)} = \frac{x^2 - 1}{x - 1} = x + 1$$

$$F_4(x) = \frac{x^4 - 1}{F_1(x)F_2(x)} = \frac{x^4 - 1}{(x - 1)(x + 1)} = x^2 + 1$$

$$F_5(x) = \frac{x^5 - 1}{F_1(x)} = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1$$

$$F_{10}(x) = \frac{x^{10} - 1}{\text{KGV}\{x - 1, x^2 - 1, x^5 - 1\}} = \frac{x^{10} - 1}{(x + 1)(x^5 - 1)} = \frac{x^5 + 1}{x + 1}$$

$$= x^4 - x^3 + x^2 - x + 1$$

$$F_{20}(x) = \frac{x^{20} - 1}{\text{KGV}\{x - 1, x^2 - 1, x^4 - 1, x^5 - 1, x^{10} - 1\}} = \frac{x^{20} - 1}{(x^2 + 1)(x^{10} - 1)}$$

$$= \frac{x^{10} + 1}{x^2 + 1} = x^8 - x^6 + x^4 - x^2 + 1.$$

Wir nennen die von den Kreisteilungspolynomen  $F_t(x)$ ,  $t|n$ , annullierten Polygone, die Bausteine rationaler Polygone, *rational-regulär* (in [1]  $\mathcal{Q}$ -regulär). Ist  $F_t(x)$  der minimale Annullator des  $n$ -Ecks  $B = (b_0, b_1, \dots, b_{n-1})$ , so gilt wegen  $F_t(x)|x^t - 1$ , dass  $B$  ein  $(n/t)$ -fach durchlaufenes  $t$ -Eck darstellt. Ist  $t > 1$  und  $\tau$  irgendein echter Teiler von  $t$ , so sind nach (23)  $x^\tau - 1$  und  $F_t(x)$  teilerfremd. Nach dem Urbildsatz gibt es dann ein  $n$ -Eck  $A = (a_0, a_1, \dots, a_{n-1})$ , das  $(x^\tau - 1)A = B$  genügt. Die angegebene Beziehung zwischen  $A$  und  $B$  enthält insbesondere die Gleichungen  $a_{\tau+k} = a_k + b_k$ ,  $a_{2\tau+k} = a_{\tau+k} + b_{\tau+k} = a_k + b_k + b_{\tau+k}$ ,  $\dots$ ,  $a_{t+k} = a_k + b_k + b_{\tau+k} + \dots + b_{(t-\tau)+k}$  und, da sich die Ecken von  $B$  nach  $t$  Schritten wiederholen,  $a_{n+k} = a_k + (n/t)(b_k + b_{\tau+k} + \dots + b_{(t-\tau)+k})$ . Wegen  $a_{n+k} = a_k$  ist die Eckensumme des  $\tau$ -fach überspringenden  $(t/\tau)$ -Ecks  $(b_k, b_{\tau+k}, \dots, b_{(t-\tau)+k})$  gleich 0. (Diese Aussage gilt für jedes  $\tau$ ,  $\tau|t$ , und jedes (o.B.d.A.  $< \tau$  gehaltene)  $k$ .) Geometrisch gesprochen zeichnet sich ein rational-reguläres,  $(n/t)$ -fach durchlaufenes  $t$ -Eck also dadurch aus, dass seine zu jedem echten Teiler  $\tau$  von  $t$  existierenden  $\tau$ -fach überspringenden Teil- $(t/\tau)$ -Ecke denselben Schwerpunkt haben wie das  $t$ -Eck selbst [12\*].

**Schlussbemerkung**

Die  $n$ -Ecks-Theorie kann in mannigfacher Weise entwickelt und angewandt werden. Als  $n$ -Ecke können nicht nur  $n$ -Tupel von Vektoren angesehen werden, sondern auch unendliche Folgen von Vektoren, ja sogar die Punkte von Ovalen mit den Neigungswinkeln ihrer Tangentenvektoren als Indizes. Vor allem aber kann der Raum  $V^n(K)$ , in dem

ein  $n$ -Eck gesamthaft als ein Vektor auftritt, metrisiert werden. (Man beachte dazu den Titel «Perpendicular Polygons» von [2].) Es ist möglich, das innere Produkt zweier  $n$ -Ecke so zu definieren, dass das Normquadrat eines  $n$ -Ecks mit seiner Fläche oder mit der Summe seiner Seitenquadrate oder mit anderem mehr übereinstimmt. Als ein Anwendungsgebiet seien isoperimetrische Ungleichungen erwähnt.

Dieter Ruoff, University of Regina, Canada

#### LITERATURVERZEICHNIS [13\*]

- 1 F. Bachmann und E. Schmidt:  $n$ -Ecke. Bibliographisches Institut, Mannheim 1970.
- 2 J. C. Fisher, D. Ruoff und J. Shilleto: Perpendicular Polygons. Amer. Math. Monthly 92, 23–37 (1985).
- 3 M. Jeger: Komplexe Zahlen in der Elementargeometrie. El. Math. 37, 136–147 (1982).
- 4 D. Ruoff und J. Shilleto: Recursive Polygons. Boll. Mat. Un. Ital. (5) 15-B, 968–981 (1978).
- 5 I. J. Schoenberg: Mathematical Time Exposures. The Mathematical Association of America, Washington, D.C. 1982.

#### ANMERKUNGEN

- [1\*] Die Ausdrücke  $n$ -Eck und *Polygon* bedeuten im folgenden dasselbe. – Man beachte, dass unsere allgemeine Theorie keine Einschränkung der Dimension von  $V(K)$  verlangt. Hingegen muss von Abschnitt 4 an  $\text{Char } K \nmid n$  erfüllt sein.
- [2\*] Ist der minimale Annullator von  $A \neq 0$  in der früheren Formel (6) gleich  $m_A(x)$ , so stellt die entsprechende Linearbeziehung (1) die Rekursionsformel von  $A$  dar.
- [3\*] Mit  $g(x)$  ist auch  $h(x) = c \cdot g(x) (c \neq 0)$  grösster gemeinsamer Teiler von  $p(x)$  und  $q(x)$ , und es gilt  $h(x) = (c p_1(x)) p(x) + (c q_1(x)) q(x)$ . Um der Eindeutigkeit willen stipulieren wir, dass der GGT zweier Polynome den Anfangskoeffizienten 1 haben soll. In gleicher Weise wollen wir, wo von einem Primteiler eines Polynoms die Rede ist, einen solchen mit Anfangskoeffizient 1 verstehen.
- [4\*] Man beachte, dass wir von der Verschiedenheit von Polynomen mit Anfangskoeffizient 1 sprechen (s. Anmerkung 3).
- [5\*] Ist unsere Bedingung nicht erfüllt, dann auch nicht die zuerst genannte Voraussetzung: Für  $\text{Char}(K) = p \mid n$  gilt  $(x-1)^p = x^p - 1 \mid x^n - 1$ . Auch manche geometrischen Besonderheiten bestehen, falls  $\text{Char } K \mid n$  gilt, wie z. B., dass ein Vektor keinen  $n$ ten Teil und ein  $n$ -Eck darum keinen Schwerpunkt besitzt.
- [6\*] Dies ist im wesentlichen der *Hauptsatz* in [1].
- [7\*] In [1] wird dem verbandstheoretischen Aspekt dieses Aufbaus grosse Beachtung geschenkt. Die Menge der Teiler von  $x^n - 1$  mit den Operationen GGT, KGV bildet eine Boolesche Algebra, wobei die Primteiler die Rolle von Atomen haben. Die Menge der diesen Teilern zugeordneten Kerne (d. h. die Menge der zyklischen  $n$ -Ecks-Klassen) mit den Operationen Durchschnitt und Summe bildet eine isomorphe Boolesche Algebra. Wir verfolgen im vorliegenden Abschnitt das Ziel, die Atome dieser zweiten Booleschen Algebra geometrisch zu beschreiben.
- [8\*] In Anlehnung an den traditionellen Polygonbegriff behandeln wir in diesem Abschnitt  $n$ -Ecke *in der Ebene*. Die Zerlegungstheorie samt Begründung ist indessen dimensionsunabhängig und gewisse ihrer Konsequenzen sind am relevantesten für Polygone, die einen drei- oder höherdimensionalen Raum aufspannen (s. [4], pp. 7–10).
- [9\*] Wir denken uns die gegebene reelle Ebene im euklidischen Sinne metrisiert und die anvisierten  $n$ -Ecke wie im komplexen Fall durch Drehungen erzeugt.
- [10\*] Lineare Abbildungen erhalten die sog. affinen Eigenschaften eines regulären  $n$ -Ecks (Kollinearität, Parallelität, Teilverhältnis von Strecken).
- [11\*] Ein Beweis findet sich in den gängigen Algebrabüchern (z. B. von van der Waerden, Rédei, Birkhoff-MacLane).
- [12\*] Jedes  $p$ -Eck ( $p$  prim) mit Schwerpunkt  $Q$  ist trivialerweise ein rational-reguläres Polygon. In [1] wird der grosse Formenreichtum der regulären 8-, 10- und 12-Ecke figurlich demonstriert.
- [13\*] Ein wesentlich ausführlicheres Verzeichnis findet sich in [2].