Fünfter Artikel.

Über die durch Quadratwurzeln lösbaren algebraischen Gleichungen und über die Konstruierbarkeit der regulären Polygone

von Federigo Enriques in Bologna.

Die Entscheidung der Frage, ob eine geometrische Konstruktionsaufgabe elementar, d. h. dadurch, daß man mit den Daten Operationen mit dem Lineal und dem Zirkel vornimmt, lösbar ist, wird von der analytischen Geometrie auf eine algebraische Frage zurückgeführt.

Von der Art, wie diese Reduktion vor sich geht, und von den mit ihr verknüpften Untersuchungen handelt G. Castelnuovo im vierten Artikel. Uns genügt es hier, den fundamentalen Schluß (vgl. pg. 125) in Erinnerung zu bringen:

Es sei eine bestimmte geometrische Aufgabe vorgelegt und sie sei auf das Aufsuchen derjenigen Punkte der Ebene, die zu gewissen gegebenen Punkten derselben Ebene in vorgeschriebenen Beziehungen stehen, zurückgeführt; die notwendige und hinreichende Bedingung dafür, daß die Konstruktion der gesuchten Punkte durch Operationen mit den Instrumenten Lineal und Zirkel, die man mit den Daten (und, wenn man will, auch mit beliebigen Punkten, Geraden und Kreisen) vornimmt, ausgeführt werden kann, lautet dann: man muß die cartesischen Koordinaten der unbekannten Punkte dadurch erhalten können, daß man mit den Koordinaten der Daten rationale Operationen und aufeinanderfolgende Quadratwurzelausziehungen (in endlicher Zahl) vornimmt.

Wir wollen Ausdrücke, die aus gegebenen Größen durch Ausführung rationaler Operationen und das Ausziehen von Quadratwurzeln gebildet sind, kurz mit dem Namen „(irrationale) Quadratwurzel-

ausdrücke“ bezeichnen; daher werden wir die vorstehende Bedingung für die Lösbarkeit einer Aufgabe aussprechen können, indem wir sagen: die Koordinaten der unbekannten Punkte müssen aus den Koordinaten der Daten gebildete Quadratwurzelausdrücke sein.

Wir werden bald nachweisen, daß jeder Quadratwurzelausdruck einer algebraischen Gleichung genügt, deren Koeffizienten sich in den gegebenen Größen rational ausdrücken, d. h. in dem Rationalitätsbereiche der gegebenen Größen enthalten sind. Dadurch wird die Entscheidung der Frage, ob eine vorgelegte Aufgabe elementar lösbar ist, auf die Entscheidung der beiden folgenden Fragen zurückgeführt:

1. ob die Aufgabe selbst (nachdem sie zunächst in die weiter unten angedeutete Form gebracht worden ist) algebraisch ist, d. h. in der Lösung einer algebraischen Gleichung mit Koeffizienten, die in dem gegebenen Bereiche rational sind, besteht;

2. ob eine gegebene algebraische Gleichung in einem Rationalitätsbereiche, dem die Koeffizienten der Gleichung angehören, durch rationale Operationen und das Ausziehen von Quadratwurzeln gelöst werden kann.

Hinsichtlich der ersten Frage bemerken wir, daß die analytische Geometrie die Übersetzung geometrischer Beziehungen in analytische Beziehungen lehrt; wenn diese sich in algebraischer Form darstellen, so ist die erwähnte Frage sofort in bejahendem Sinne gelöst. Sie erscheint dagegen als viel schwieriger, wenn man zu analytischen Beziehungen gelangt, die sich nicht in algebraischer Form darstellen; denn es handelt sich dann darum, zu erkennen, ob diese analytischen Beziehungen (soweit die Bestimmung der Unbekannten in einem vorliegenden Falle in Frage kommt) durch algebraische Beziehungen ersetzt werden können; eine solche Untersuchung führt in der Tat zu den höchsten Aufgaben der Analysis (vgl. Art. VIII).

Wir wollen uns hier mit der zweiten Frage beschäftigen, indem wir einen allgemeinen Satz über den Grad derjenigen algebraischen Gleichungen aufstellen, welche durch Quadratwurzeln lösbar sind. Die Frage wird dadurch nicht erschöpft (und zu ihrer Erschöpfung sind umfangreichere Entwickelungen erforderlich); aber das so erhaltene Resultat genügt für die Anwendungen auf dem Gebiete der Elementargeometrie, die wir im Sinne haben.

Unter diesen Anwendungen treten vor allem diejenigen auf, welche sich auf die Konstruktionen der regulären Polygone und auf die Verdoppelung des Würfels und die Dreiteilung des Winkels beziehen; die erstgenannten werden in dem vorliegenden Artikel, die anderen im siebenten Artikel behandelt.

Von den Alten sind uns die elementaren Konstruktionen des regulären Polygons von 2^n Seiten, des gleichseitigen Dreiecks und des regulären Fünfecks überkommen, und dazu diejenigen der regulären Polygone von $2^n \cdot 3$, $2^n \cdot 5$, $3 \cdot 5$, $2^n \cdot 3 \cdot 5$ Seiten, die von den vorhergehenden abhängen.

Nun würde man z. B. die elementaren Konstruktionen des regulären Siebenecks und des regulären Neunecks suchen können und sich von den Schwierigkeiten, denen man dabei entgegenginge, keine Rechenschaft geben, wenn es nicht dazu gekommen wäre, daß man die Lösbarkeit dieser Aufgaben in Zweifel zog. Es würden also nutzlose Anstrengungen in immer größerer Zahl aufgewendet werden, und man würde dabei aus dem Mißerfolg nicht einmal irgend welche Belehrung über die Natur der vorgelegten Fragen davontragen.

Wenn aber jemand die Überzeugung gewonnen hätte, daß es sich in diesen Fällen um unlösbare Aufgaben handelt, wie würde der wohl den Mut haben, die Probe für die dann folgenden Fälle zu machen, bei denen die Schwierigkeiten offenbar beständig wachsen? Wenn festgestellt worden ist oder angenommen wird, daß die regulären Polygone von 7, 9, 11, 13, 14 Seiten nicht elementar konstruierbar sind, wie könnte es dann jemand in den Sinn kommen, die Konstruktion des Polygons von 17 Seiten zu suchen? Trotzdem liegt es tatsächlich so, daß die Konstruktion des Siebzehnecks möglich ist, während die Konstruktionen der regulären Polygone von 7, 9, 11, 13, 14 Seiten (mit dem Lineal und dem Zirkel) nicht möglich sind.

Darüber klärt die schöne Theorie der binomischen Gleichungen von Gauß auf.

Die Konstruktion des regulären Polygons von n Seiten hängt von der Auflösung der binomischen Gleichung

$$z^n = 1$$

ab, die, wenn man die Wurzel $z = 1$ wegläßt, sich auf die Gleichung

$$z^{n-1} + z^{n-2} + \cdots + 1 = 0$$

reduziert.

Damit das n-eck elementar konstruierbar ist, muß die vorstehende Gleichung (im absoluten Rationalitätsbereiche [1]) durch Quadratwurzeln lösbar sein. Nun hängt diese Lösbarkeit von der Form der Zahl n ab; und zwar ist, wie wir sehen werden, die Gleichung lösbar, wenn n, in Primfaktoren zerlegt, von der Form

$$n = 2^v (2^{2^{v_1}} + 1)\ (2^{2^{v_2}} + 1) \cdots (2^{2^{v_s}} + 1)$$

ist, wo die $v_1, v_2, \ldots v_s$ sämtlich voneinander verschieden sind.

In dieser Formel sind also alle regulären Polygone, die sich elementar konstruieren lassen, enthalten.[1])

Wir bringen im § 9 dieses Artikels einige eingehendere Bemerkungen über diese Polygone und schließen mit einem Hinweis auf das Problem des Siebenecks. Hinsichtlich der verschiedenen Konstruktionen des Siebzehnecks, deren theoretische Möglichkeit als Konsequenz des erwähnten allgemeinen Satzes wir hier nur hervorheben, verweisen wir auf den sechsten Artikel.

Wir zitieren schließlich die wichtigsten Arbeiten, in denen die Theorien, die den Gegenstand des gegenwärtigen Aufsatzes bilden, dargelegt sind und deren wir uns bei seiner Abfassung bedient haben:

1. Über die algebraischen Gleichungen, die durch Quadratwurzeln lösbar sind:

J. Petersen, *Theorie der algebraischen Gleichungen*, Kopenhagen 1878. — F. Klein, *Vorträge über ausgewählte Fragen der Elementargeometrie*, Leipzig 1895. — A. Capelli, *Lezioni di Algebra complementare*, Napoli 1895.

2. Über die Theorie der binomischen Gleichungen in Beziehung zu dem Problem der regulären Polygone:

Gauß, *Disquisitiones arithmeticae, sectio VII* (1801), Werke Bd. 1. — P. Bachmann, *Die Lehre von der Kreisteilung*, Leipzig 1872. — F. Klein, *Vorträge* usw., vgl. oben. — L. Bianchi, *Lezioni sulla teoria delle sostituzioni e delle equazioni algebriche secondo Galois*, Pisa 1896.

I.

§ 1. Reduktion der irrationalen Quadratwurzelausdrücke auf eine Normalform. Wir betrachten einen (Quadratwurzel-) Ausdruck x, der aus gewissen gegebenen Größen $1, \alpha, \beta, \ldots$, die unsern Rationalitätsbereich $[1, \alpha, \beta, \ldots]$ definieren, durch rationale Operationen und aufeinanderfolgende Quadratwurzelausziehungen gebildet ist. In dem angedeuteten Ausdrucke werden sich Glieder befinden, die übereinanderstehende Wurzelzeichen in verschiedener Anzahl enthalten; aus ihnen ist der Ausdruck selbst rational zusammengesetzt. Wir wollen sagen, ein Glied ist von der $m$ten Ordnung, wenn in ihm unter einem und demselben Wurzelzeichen noch $m-1$ andere Wurzelzeichen vorkommen. So sind z. B.

1) Hinsichtlich der Instrumente, die man zu den Konstruktionen benutzen kann, hat D. Hilbert bemerkt, daß hier der Zirkel durch den Streckenübertrager ersetzt werden kann (Vgl. Art. IV, § 11).

$$\sqrt{a+\sqrt{b}},\quad \sqrt{\sqrt{a}+\sqrt{b}},\quad \sqrt{\sqrt{\sqrt{a}+\sqrt{b}+\sqrt{c}},}$$

wo a, b, c rationale Ausdrücke darstellen, Glieder zweiter, dritter, vierter Ordnung.

Ein Glied $m$ter Ordnung kann durch $\sqrt{X}$ bezeichnet werden, worin X ein Quadratwurzelausdruck ist, der aus Gliedern $(m-1)$ter oder geringerer Ordnung gebildet ist.

In dem Ausdrucke x können sich Glieder $m$ter Ordnung befinden, die durch die übrigen Glieder $m$ter Ordnung und diejenigen geringerer Ordnung rational ausgedrückt werden können; wenn man diese Glieder dann durch die angedeuteten Ausdrücke ersetzt, kann man die Zahl der in x vorkommenden Glieder verringern.

Nehmen wir an, wir hätten wiederholt, solange es möglich ist, die Reduktionen, zu denen die in x enthaltenen Glieder $m$ter Ordnung Veranlassung geben, ausgeführt, dann die Reduktionen, zu denen die Glieder $(m-1)$ter Ordnung Veranlassung geben, und so fort; dann werden wir eine Darstellung von x haben, in der die Gliederzahl nicht weiter reduzierbar ist, insofern kein Glied mehr durch die übrigen Glieder derselben oder geringerer Ordnung rational ausgedrückt werden kann. Wir betrachten nun im besonderen jedes Glied $\sqrt{X}$ von x und führen in analoger Weise die Reduktion von X auf die kleinste Gliederzahl aus. Wir fahren in derselben Weise mit jedem Ausdrucke, der unter irgend einer Quadratwurzel in einem Gliede von X steht, fort, und so weiter. Wenn alle möglichen Reduktionen ausgeführt sind, dann haben wir endlich eine Darstellung von x, in der alle Wurzeln von einander unabhängig sind, so daß ihre Zahl in der angegebenen Weise nicht weiter reduziert werden kann.

Um die Sache deutlicher zu machen, nehmen wir z. B.

$$x=\sqrt{\sqrt{a}+\sqrt{b}+\sqrt{ab}}+\sqrt{c}+\sqrt{d}+\sqrt{\frac{c}{d}}.$$

Wir können unter dem ersten Wurzelzeichen

$$\sqrt{ab} \text{ durch } \sqrt{a}\cdot\sqrt{b}$$

ersetzen und das letzte Glied

$$\sqrt{\frac{c}{d}} \text{ durch } \frac{\sqrt{c}}{\sqrt{d}};$$

nach Ausführung dieser Reduktionen haben wir den Ausdruck

$$x=\sqrt{\sqrt{a}+\sqrt{b}+\sqrt{a}\cdot\sqrt{b}}+\sqrt{c}+\sqrt{d}+\frac{\sqrt{c}}{\sqrt{d}},$$

in dem alle Wurzeln von einander unabhängig sind.

Haben wir den Ausdruck x so weit reduziert, daß er nur unabhängige Wurzeln enthält, so betrachten wir in ihm ein Glied der höchsten Ordnung m, etwa $\sqrt{X}$; x kann dann als ein rationaler Ausdruck von $\sqrt{X}$ betrachtet werden, dessen Koeffizienten $a_1, a_2, \ldots, b_1, b_2, \ldots$ aus den anderen Gliedern rational gebildet sind, also:

$$x = \frac{a_1 + a_2\sqrt{X} + a_3(\sqrt{X})^2 + \cdots + a_{n+1}(\sqrt{X})^n}{b_1 + b_2\sqrt{X} + b_3(\sqrt{X})^2 + \cdots + b_{\nu+1}(\sqrt{X})^\nu}.$$

Aber da

$$(\sqrt{X})^2 = X,\ (\sqrt{X})^4 = X^2, \cdots,$$

so wird man

$$x = \frac{p + q\sqrt{X}}{r + s\sqrt{X}}$$

setzen können, wo p, q, r, s rational von den von $\sqrt{X}$ verschiedenen Gliedern $m$ter Ordnung und von Gliedern niedrigerer Ordnung abhängen. Nun ist

$$x = \frac{p + q\sqrt{X}}{r + s\sqrt{X}} = \frac{(p + q\sqrt{X})(r - s\sqrt{X})}{(r + s\sqrt{X})(r - s\sqrt{X})}$$
$$= \frac{pr - qsX}{r^2 - s^2X} + \frac{qr - ps}{r^2 - s^2X} \cdot \sqrt{X},$$

oder

$$x = A + B\sqrt{X},$$

wo A und B von den anderen Gliedern $m$ter Ordnung $\sqrt{Y}, \sqrt{Z}, \ldots$ und von Gliedern niedrigerer Ordnung abhängen.

Gehen wir nun daran, nacheinander die Ausdrücke A und B zu betrachten. Jeder von ihnen, z. B. A, kann in bezug auf $\sqrt{Y}$ in eine Form gebracht werden, die der für x erhaltenen analog ist:

$$A = A_1 + A_2\sqrt{Y},$$

wo A_1 und A_2 aus $\sqrt{Z}, \ldots$ und den Gliedern von niedrigerer Ordnung als m rational zusammengesetzt sind.

Verfahren wir in derselben Weise mit den neuen Ausdrücken A_1, A_2 usw., so kommen wir schließlich dazu, x durch einen ganzen Ausdruck in den Gliedern $m$ter Ordnung

$$\sqrt{X}, \sqrt{Y}, \sqrt{Z}, \ldots$$

darzustellen, in dem diese Glieder nur unter sich multipliziert sind, aber nicht in einer Potenz erscheinen; die Koeffizienten eines solchen Ausdrucks werden von Gliedern von niedrigerer Ordnung als m rational abhängen.

Es ist klar, daß die mit den Gliedern $m$ter Ordnung vorgenommene Reduktion sich auch hintereinander mit den Gliedern $(m-1)$ter Ordnung, die in x oder in den Ausdrücken $X, Y, Z, \ldots$ auftreten, vornehmen läßt, dann mit den Gliedern $(m-2)$ter Ordnung und so fort. Schließlich werden wir zu einer Darstellung von x gelangen, die wir Normalform nennen wollen; diese wird (wenn man von rationalen Größen in dem gegebenen Bereiche ausgeht) allein durch die Operationen der Addition, der Multiplikation und des Ausziehens von Quadratwurzeln gebildet sein, wobei jede Quadratwurzel nur in der ersten Potenz vorkommen wird.

Die nachfolgenden Erörterungen, die wir über Quadratwurzelausdrücke anstellen werden, gründen sich auf die Voraussetzung, daß diese zunächst auf unabhängige Quadratwurzeln reduziert und in der Normalform dargestellt sind die Zahl dieser Quadratwurzeln kann alsdann durch den Namen Grad des Quadratwurzelausdrucks bezeichnet werden.

§ 2. Herstellung einer algebraischen Gleichung, der ein Quadratwurzelausdruck genügt. Ein Quadratwurzelausdruck x vom Grade n genügt einer algebraischen Gleichung vom Grade 2^n mit (in dem gegebenen Rationalitätsbereiche) rationalen Koeffizienten.

Stellen wir uns vor, wir geben den n Wurzeln, die in dem Ausdrucke x enthalten sind, alle (positiven und negativen) Werte, die sie annehmen können, so werden wir 2^n Werte von x erhalten: $x_1, x_2, \ldots x_i, \ldots x_{2^n}$, und es werden einige von ihnen (wie wir bald zeigen werden) einander gleich sein können.

Wir bilden nun die Gleichung

$$f(x) = (x - x_1)(x - x_2)\cdots(x - x_{2^n}) = x^{2^n} + p_1 x^{2^n - 1} + \cdots + p_{2^n} = 0,$$

die die x_i zu Wurzeln hat.

Die Koeffizienten dieser Gleichung drücken sich durch die elementaren symmetrischen Funktionen der x_i mittels der Formeln

$$p_1 = -\Sigma x_i$$
$$p_2 = \Sigma x_i x_k$$
$$\cdots\cdots\cdots$$
$$p_{2^n} = x_1 x_2 \cdots x_{2^n}$$

aus. Es handelt sich darum zu beweisen, daß diese Koeffizienten rational sind.

Diese Eigenschaft geht aus der fundamentalen Tatsache hervor, daß die p_ν symmetrische Funktionen der x_i sind, d. h. daß sie un-

geändert bleiben, wenn man die Reihe der x_i in irgend einer Weise permutiert (z. B.

$$p_1 = -(x_1 + x_2 + \cdots + x_{2^n}) = -(x_2 + x_1 + x_3 + \cdots + x_{2^n}) = \cdots).$$

Vor allem werden die p_ν, da sie symmetrische Funktionen der x_i sind, sich nicht ändern dürfen, wenn man in irgend einer bestimmten Weise die Vorzeichen der Wurzeln, die in den x_i vorkommen, wechselt, da ein solcher Wechsel nur in der Ordnung der x_i selbst eine Permutation hervorbringt. Wenn z. B.

$$x = \sqrt{a + \sqrt{b}}$$

ist, so können wir die Werte des Ausdruckes x durch

$$x_1 = +\sqrt{a + \sqrt{b}}$$
$$x_2 = -\sqrt{a + \sqrt{b}}$$
$$x_3 = +\sqrt{a - \sqrt{b}}$$
$$x_4 = -\sqrt{a - \sqrt{b}}$$

bezeichnen, und dann sieht man, daß bei einem Wechsel des Vorzeichens von $\sqrt{b}$ sich x_1 mit x_3 und x_2 mit x_4 vertauscht: wechselt man dagegen das Vorzeichen bei beiden Wurzeln, so wird x_1 mit x_4 und x_2 mit x_3 vertauscht; wechselt man endlich das Vorzeichen der äußeren Wurzel $\sqrt{a + \sqrt{b}}$, so wird x_1 mit x_2 und x_3 mit x_4 vertauscht.

Nach dieser Vorbemerkung betrachten wir p_ν als einen Quadratwurzelausdruck, der aus den in x vorkommenden Wurzeln gebildet ist, und wir setzen voraus, daß dieser Ausdruck in die Normalform gebracht worden ist. Unter der Annahme, daß er Glieder $m$ter Ordnung, $\sqrt{X}, \sqrt{Y}, \sqrt{Z}, \ldots$, enthält, heben wir das Glied $\sqrt{X}$ hervor, indem wir schreiben

$$p_\nu = P + Q\sqrt{X}.$$

Da p_ν sich nicht ändert, wenn man das Vorzeichen von $\sqrt{X}$ wechselt, so erhalten wir

$$P + Q\sqrt{X} = P - Q\sqrt{X}$$

d. h.

$$Q\sqrt{X} = 0$$

und daher

$$Q = 0.$$

Also hängt p_ν von der Wurzel $\sqrt{X}$ nicht ab. In analoger Weise

hängt es auch nicht von $\sqrt{Y}, \sqrt{Z}, \ldots$ ab, und es kommen also in ihm höchstens Glieder vor, die Wurzeln $(m-1)$ter Ordnung enthalten.

Aber wenn man die vorstehende Überlegung in bezug auf die Glieder $(m-1)$ter Ordnung wiederholt, so sieht man, daß p_r auch nicht von diesen abhängen kann. Geht man nach und nach in derselben Weise weiter, so erkennt man, daß p_r von keiner Wurzel abhängt, d. h. daß p_r ein rationaler Ausdruck (in dem gegebenen Bereiche) ist. Also ist dargetan, daß $f(x)=0$ eine Gleichung mit rationalen Koeffizienten ist, w. z. b. w.

Wir haben bemerkt, daß unter den Werten $x_1, x_2, \ldots$ von x sich einige befinden können, die einander gleich sind; wenn z. B.

$$x = \sqrt{a} + \sqrt{b} + \sqrt{a} - \sqrt{b}$$

ist, so sind die Werte von x, die man durch den Wechsel des Vorzeichens von $\sqrt{b}$ erhält, einander gleich.

Nehmen wir an, man wählt unter den 2^n Werten von x alle voneinander verschiedenen Werte aus; es mögen z. B. die Werte $x_1, x_2, \ldots, x_r$ sein. Dann hat auch die Gleichung vom $r$ten Grade

$$\varphi(x) = (x-x_1)(x-x_2)\cdots(x-x_r) = 0$$

rationale Koeffizienten; das wird wie für $f(x)=0$ bewiesen.

Vergleicht man nun die beiden Gleichungen

$$f(x)=0 \quad \text{und} \quad \varphi(x)=0,$$

so sieht man, daß die erste alle Wurzeln der zweiten zu Wurzeln hat, und darum ist sie, wenn $r<2^n$ ist, „reduzibel", d. h. es ist

$$f(x) = \varphi(x)\cdot\psi(x),$$

wo $\psi(x)$ ein Polynom mit rationalen Koeffizienten ist.

§ 3. Über den Grad der irreduziblen Gleichungen, die durch Quadratwurzeln lösbar sind. Wir beweisen vor allem den Satz: Wenn eine algebraische Gleichung mit (in einem gegebenen Bereiche) rationalen Koeffizienten durch einen Wert eines Quadratwurzelausdrucks x erfüllt wird, so wird sie durch alle Werte von x erfüllt, die man erhält, wenn man die Wurzelvorzeichen vertauscht.

Es sei

$$F(x) = 0$$

die gegebene Gleichung.

Nehmen wir x als reduziert, d. h. mit nur unabhängigen Wurzeln und in der Normalform, an und betrachten wir ein Glied der höchsten Ordnung m, sagen wir $\sqrt{X}$, so ist

$$x = A + B\sqrt{X}.$$

Wir setzen diesen Ausdruck in F ein und reduzieren F auf die Normalform in bezug auf $\sqrt{X}$, so daß wir schreiben

$$F(x) = L + M\sqrt{X}.$$

L und M hängen von den andern in x vorkommenden Gliedern $m$ter Ordnung, $\sqrt{Y}$, $\sqrt{Z}$, ..., und von den Gliedern niedrigerer Ordnung ab.

Nun ist (nach Voraussetzung)

$$F(x) = L + M\sqrt{X} = 0;$$

daher ist entweder

$$L = M = 0$$

oder

$$\sqrt{X} = -\frac{L}{M};$$

aber die letzte Gleichung widerspricht der Annahme, daß alle in x enthaltenen Wurzeln voneinander unabhängig sind. Also ist bewiesen, daß

$$L = M = 0$$

und daher auch

$$L - M\sqrt{X} = 0$$

ist, so daß die Gleichung

$$F(x) = 0$$

nicht nur durch

$$x = A + B\sqrt{X},$$

sondern auch durch

$$x = A - B\sqrt{X}$$

erfüllt wird. In analoger Weise beweist man, daß $F(x) = 0$ durch die Werte erfüllt wird, die man erhält, wenn man irgendwie in dem Quadratwurzelausdrucke x das Vorzeichen der Glieder $m$ter Ordnung, $\sqrt{Y}$, $\sqrt{Z}$, ..., ändert.

Setzen wir der Einfachheit wegen voraus, daß in x nur zwei Glieder $m$ter Ordnung,

$$\sqrt{X} \text{ und } \sqrt{Y},$$

vorkommen, so werden wir haben

$$F(x) = L + M\sqrt{X},$$

wo

$$L = L_1 + L_2\sqrt{Y},$$
$$M = M_1 + M_2\sqrt{Y}$$

ist, und aus der Gleichung $F(x) = 0$ werden wir schließen

$$L_1 = L_2 = M_1 = M_2 = 0.$$

Nun sind L_1, L_2, M_1, M_2 Ausdrücke, die von Gliedern, in denen Quadratwurzeln vorkommen, nur solche von höchstens $(m-1)$ter Ordnung enthalten; in analoger Weise wie oben beweist man dann, daß diese Ausdrücke Null sind, wenn man die Wurzelvorzeichen der Glieder $(m-1)$ter Ordnung in x irgendwie vertauscht; daraus folgt, daß die Gleichung $F(x)=0$ erfüllt ist, wenn man in dem Quadratwurzelausdrucke x die Vorzeichen der Wurzeln, die die Glieder $(m-1)$ter Ordnung bilden, vertauscht.

Es ist klar, daß man diese Überlegung fortsetzen kann und dadurch zu dem Schlusse gelangt, daß, wenn die Gleichung

$$F(x)=0$$

durch einen Wert des Quadratwurzelausdrucks x erfüllt wird, sie auch durch alle diejenigen Werte erfüllt wird, welche man aus dem gegebenen erhält, wenn man das Vorzeichen der Wurzeln, die Glieder

$$m\text{ter},\ (m-1)\text{ter},\ (m-2)\text{ter}\ \ldots\ 1\text{ter Ordnung}$$

bilden, in beliebiger Weise wechselt.

Es bleibt noch zu zeigen übrig, daß die Gleichung $F(x)=0$ auch noch erfüllt wird, wenn man die Vorzeichen der Wurzeln, die unter einem andern Wurzelzeichen stehen, wechselt, z. B. die Vorzeichen der Wurzeln, die die Glieder des in $\sqrt{X}$ vorkommenden Ausdrucks X bilden. Aber das ist implizite schon bewiesen; denn, wenn

$$F(x)=L-M\sqrt{X}$$

ist, wo

$$L=M=0$$

ist, so wird immer

$$F(x)=0$$

sein, wie man auch immer das Vorzeichen der in X vorkommenden Wurzeln wechselt.

Also ist der Satz vollständig dargetan.

Er führt unmittelbar auf den Zusatz:

Wenn eine algebraische Gleichung

$$F(x)=0$$

mit rationalen Koeffizienten durch einen Wert eines Quadratwurzelausdrucks x erfüllt wird, und wenn man mit

$$\varphi(x)=0$$

diejenige Gleichung (mit rationalen Koeffizienten) bezeichnet, der alle verschiedenen Werte, die das x durch den

Wechsel der Vorzeichen der in ihm enthaltenen Wurzeln erhalten kann, genügen, so ist

$$F(x) = \varphi(x) \cdot \vartheta(x),$$

wo ϑ ein Polynom mit rationalen Koeffizienten ist.

Wenn $F(x) = 0$ eine irreduzible Gleichung ist, so muß sich also das Polynom ϑ auf einen konstanten Faktor reduzieren. —

Nehmen wir nun die oben betrachtete Gleichung $f(x) = 0$ wieder auf, d. h. die Gleichung vom Grade 2^n, die die 2^n Werte des Quadratwurzelausdrucks x zu Wurzeln hat, und r sei wieder die Zahl der voneinander verschiedenen Werte von x (vgl. pg. 145).

Wir haben bereits bemerkt, daß für den Fall $r < 2^n$

$$f(x) = \varphi(x) \cdot \psi(x)$$

ist, wo ψ ein Polynom mit rationalen Koeffizienten bedeutet. Nun hat die Gleichung $\psi(x) = 0$ einige Werte des Quadratwurzelausdrucks x zu Wurzeln und daher alle seine Werte; darum ist auch

$$\psi(x) = \varphi(x) \cdot \psi_1(x) \quad \text{und} \quad f(x) = \varphi^2(x) \cdot \psi_1(x),$$

wo ψ_1 ein neues Polynom mit rationalen Koeffizienten oder eine Konstante ist. Wenden wir auf ψ_1 (vorausgesetzt, daß es keine Konstante ist) die in bezug auf ψ dargelegte Schlußweise an und fahren wir so weiter fort, so müssen wir schließlich einen Quotienten finden, der sich auf eine Konstante c reduziert, so daß wir also erhalten:

$$f(x) = c\varphi^s(x);$$

in der Tat kann die Division nicht unbegrenzt fortgesetzt werden, da f einen endlichen Grad hat.

Da nun, wie gesagt, $f(x) = c\varphi^s(x)$ und r der Grad von φ und 2^n der Grad von f ist, so wird

$$rs = 2^n$$

sein, so daß weder r noch s einen von 2 verschiedenen Primfaktor enthalten kann; also wird der Grad der Gleichung

$$\varphi(x) = 0$$

$$r = 2^\nu$$

sein.

Daraus folgt, wenn man die vorstehenden Resultate zusammenfaßt, für eine irreduzible Gleichung der fundamentale Satz:

Wenn eine irreduzible algebraische Gleichung allein durch Quadratwurzeln (in einem gegebenen Rationalitätsbereiche, dem ihre Koeffizienten angehören) lösbar ist, so ist ihr Grad eine Potenz von 2.

Diese notwendige Bedingung ist jedoch nicht hinreichend; so ist z. B. eine allgemeine Gleichung achten Grades durch Quadratwurzeln nicht lösbar.

Die Bedingungen, denen eine Gleichung vom Grade 2^ν genügen muß, damit sie durch Quadratwurzeln lösbar ist, und die zu der wirklichen Lösung im allgemeinen anzuwendenden Prozesse sind von J. Petersen in verschiedenen Arbeiten eingehend studiert worden (vgl. z. B. die zitierte „*Theorie der algebraischen Gleichungen*").

II.

§ 4. Reduktion des Problems der regulären Polygone auf binomische Gleichungen. Wir wollen die im Vorstehenden gewonnenen Ergebnisse über die Lösbarkeit von Gleichungen durch Quadratwurzelausdrücke auf das Problem der Konstruktion der regulären Polygone anwenden.

Dazu müssen wir vor allen Dingen das Problem in eine analytische Form bringen. Und darum beginnen wir damit, ihm eine solche Form zu geben, daß Punkte gegeben sind und Punkte gesucht werden, die zu jenen in vorgeschriebenen Beziehungen stehen.

Hierzu bedarf es nur der folgenden sehr einfachen Bemerkungen:

a) Alle regulären n-ecke von derselben Seitenzahl sind einander ähnlich; also wird die Aufgabe, das reguläre n-eck zu konstruieren, das eine gegebene Seite hat, sofort auf die Aufgabe zurückgeführt, irgend ein reguläres n-eck zu konstruieren. Die Unbekannte ist der Winkel des Polygons oder, wenn man will, der zu einer Seite gehörige Zentriwinkel; die Seite erscheint bei der Untersuchung als ein willkürlicher Parameter.

b) Wenn man ein reguläres n-eck konstruieren kann, so kann man auch das reguläre n-eck konstruieren, das einem gegebenen Kreise einbeschrieben ist und eine gegebene Ecke hat, d. h. man kann den Kreis in n gleiche Bogen teilen, indem man von einem vorgeschriebenen Teilpunkte ausgeht, und umgekehrt.

Also ist das Problem der regulären Polygone vollkommen gleichwertig dem der Teilung des Kreises in n gleiche Teile, wofern man voraussetzen darf, daß der Mittelpunkt O des Kreises und ein Teilpunkt A gegeben sind. Es ist dabei gestattet, die Entfernung der beiden gegebenen Punkte, d. h. den Radius des Kreises, als Einheit anzunehmen.

In dieser Form besteht also die vorliegende Aufgabe, deren Daten Punkte sind, darin, $n-1$ (Teil-)Punkte zu suchen, die zusammen mit dem Punkte A die Ecken eines regulären n-ecks bilden.

Jeder dieser Punkte bestimmt mit A (in irgend einem der beiden Sinne) einen Bogen, der, mit n multipliziert, ein ganzes Vielfaches (ein m-faches) des ganzen Kreises ergibt, nämlich einen Bogen

$$\frac{2\pi m}{n}$$

(wo man $m < n$ nehmen kann).

Wir beziehen uns nun auf zwei rechtwinklige Koordinatenachsen, indem wir O zum Anfangspunkt und OA zur x-Achse nehmen. Der Punkt A wird dann die Koordinaten 1, 0 haben; die unbekannten Punkte werden gewisse Koordinaten

$$x_1, y_1;\ x_2, y_2;\ \cdots;\ x_{n-1}, y_{n-1}$$

haben, die der Gleichung des Kreises

$$x^2 + y^2 = 1$$

genügen, und es handelt sich gerade um die Bestimmung dieser Koordinaten, indem man von den allein gegebenen Größen 0, 1, die den absoluten Rationalitätsbereich [1] definieren, ausgeht.

Denken wir uns die Punkte der Ebene durch die Werte der komplexen Variablen

$$z = x + iy$$

dargestellt (nach Argand und Gauß). Jedem Werte z entsprechen bekanntlich ein Modul

$$\varrho = |\sqrt{x^2 + y^2}|$$

und ein Argument

$$\vartheta = \operatorname{arc\,tg} \frac{y}{x};$$

das sind die Polarkoordinaten des Punktes (x, y), der z darstellt, so daß

$$z = \varrho\,(\cos\vartheta + i \sin\vartheta).$$

Der Modul ist die absolute Entfernung des Punktes (x, y) vom Anfangspunkte (der Radius vector); das Argument ist der Winkel (die Anomalie), den die Gerade, die diesen Punkt mit dem Anfangspunkte verbindet, mit der x-Achse bildet.

Nun kann man die Multiplikation zweier komplexer Zahlen

$$z = x + iy, \quad z' = x' + iy'$$

ausführen: algebraisch nach den gewöhnlichen Rechnungsregeln, indem man

$$Z = zz' = (xx' - yy') + i(xy' + x'y)$$

setzt, oder geometrisch, indem man den Punkt bestimmt, der zu Polarkoordinaten

$$P = \varrho\varrho' = \left|\sqrt{x^2+y^2}\right| \cdot \left|\sqrt{x'^2+y'^2}\right|$$
$$\Theta = \vartheta + \vartheta' = \operatorname{arc\,tg}\frac{y}{x} + \operatorname{arc\,tg}\frac{y'}{x'},$$

d. h. das Produkt der Moduln und die Summe der Argumente hat.

Wir wenden diese geometrische Regel an und bilden die aufeinanderfolgenden Potenzen der komplexen Zahlen

$$z_s = x_s + iy_s,$$

die durch unsere unbekannten Punkte

$$(x_1, y_1); \ldots; (x_{n-1}, y_{n-1})$$

dargestellt werden.

Es ist der Modul

$$\left|\sqrt{x_s^2+y_s^2}\right| = 1$$

und das Argument

$$\frac{2\pi m}{n}$$

$$\left(\text{also } z_s = \cos\frac{2\pi m}{n} + i\,\sin\frac{2\pi m}{n}\right),$$

daher wird der Modul von z_s^h für jedes h gleich 1 sein, während sein Argument

$$\frac{2\pi mh}{n}$$

betragen wird. Für $h = n$ im besonderen wird sich der Punkt z_s^n auf der positiven x-Achse befinden und daher mit

$$A = (1, 0)$$

zusammenfallen; infolgedessen ist

$$z_s^n = 1.$$

Umgekehrt sei ein von A verschiedener Punkt (x, y) von der Beschaffenheit, daß

$$z^n = (x+iy)^n = 1$$

ist. Dieser Punkt muß einen Modul ϱ haben von der Art, daß $\varrho^n = 1$ ist, und daher den Modul 1; außerdem muß er ein Argument ϑ haben, das, mit n multipliziert, sich von 0 um ganze Vielfache von 2π unterscheidet, also

$$\vartheta = \frac{2\pi m}{n};$$

also ist der genannte Punkt einer der Punkte

$$(x_1, y_1); \ldots; (x_{n-1}, y_{n-1}),$$

die unserer Aufgabe genügen.

Wir schließen:

Das Problem der Konstruktion eines regulären n-ecks hängt von der Auflösung der binomischen Gleichung

$$z^n = 1$$

ab, und zwar von der Ermittelung ihrer von $z = 1$ verschiedenen Wurzeln, d. h. von der Auflösung der Gleichung

$$\frac{z^n - 1}{z - 1} = z^{n-1} + z^{n-2} + \cdots + 1 = 0.$$

Diese Gleichung läßt sich in zwei andere Relationen für x und y zerlegen; aber dies ist weder nötig noch nützlich. Wenn die angegebene Gleichung in z durch Quadratwurzeln (in dem durch die Koeffizienten gegebenen Rationalitätsbereiche [1]) gelöst werden kann, dann werden auch die Koordinaten x, y der unbekannten Punkte durch Quadratwurzeln ausgedrückt werden, da bei positiv genommenen Wurzeln

$$\sqrt{a + ib} = \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} + i\sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}}$$

ist, und daher wird das n-eck mit dem Lineal und dem Zirkel konstruierbar sein. Umgekehrt sind die x, y, wenn das n-eck konstruierbar ist, Quadratwurzelausdrücke, und daher werden auch die Wurzeln

$$z = x + iy$$

der binomischen Gleichung durch Quadratwurzeln ausdrückbar sein.

Das Problem der elementaren Konstruktion der regulären Polygone ist also auf die Aufgabe zurückgeführt, die Gleichung

$$z^n = 1$$

(wenn es möglich ist) durch Quadratwurzeln zu lösen.

§ 5. Irreduzibilität der Gleichung $\frac{z^p - 1}{z - 1} = 0$, wenn p eine Primzahl ist. Wir betrachten die Gleichung

$$z^p - 1 = 0$$

unter der Voraussetzung, daß p eine Primzahl ist. Entfernt man den linearen Faktor $z - 1$, so wird sie auf die Form

$$F(z) \equiv \frac{z^p - 1}{z - 1} = z^{p-1} + z^{p-2} + \cdots + z + 1 = 0$$

zurückgeführt.

Wir wollen nachweisen, daß diese Gleichung im absoluten Rationalitätsbereiche [1] irreduzibel ist, d. h. daß $F(z)$ nicht in ein Produkt

zweier Polynome mit rationalen (numerischen) Koeffizienten zerlegt werden kann.

Zu diesem Ende müssen wir ein Lemma über die Zerlegbarkeit der Polynome, das man Gauß verdankt, vorausschicken.

Es sei ein Polynom

$$f(z)=a_0z^n+a_1z^{n-1}+\cdots+a_n,$$

dessen Koeffizienten ganze Zahlen sind, gegeben; wir sagen, daß dieses Polynom primitiv ist, wenn die Zahlen $a_0, a_1, \ldots, a_n$ keinen gemeinsamen Teiler außer der Einheit haben.

Nun seien

$$f(z)=a_0z^n+a_1z^{n-1}+\cdots+a_n$$

und

$$\varphi(z)=b_0z^m+b_1z^{m-1}+\cdots+b_m$$

zwei primitive Polynome mit ganzen Koeffizienten. Wir bilden das Produkt

$$F(z)=f(z)\cdot\varphi(z)=c_0z^{m+n}+c_1z^{m+n-1}+\cdots+c_{m+n},$$

wo

$$c_0=a_0b_0$$
$$c_1=a_0b_1+a_1b_0$$

und im allgemeinen

$$c_k=a_0b_k+a_1b_{k-1}+\cdots+a_kb_0$$

ist, mit der Anmerkung, daß

$$a_r=0 \quad \text{für} \quad r>n$$
$$b_s=0 \quad \text{für} \quad s>m.$$

Wir wollen nun zeigen, daß das Polynom $F(z)$ primitiv ist, d. h. daß keine Primzahl $p\,(>1)$ existiert, die in allen Zahlen $c_0, c_1, \ldots, c_{m+n}$ aufgeht.

Ist eine Primzahl $p\,(>1)$ gegeben, so kann diese nicht in allen Koeffizienten a von f und ebenso nicht in allen Koeffizienten b von φ enthalten sein; es wird also einen ersten Koeffizienten a_r

$$(\text{wobei } r\leqq n)$$

und einen ersten Koeffizienten b_s

$$(\text{wobei } s\leqq m)$$

geben, die nicht durch p teilbar sind. Dann betrachten wir den Koeffizienten

$$c_{r+s}=a_0b_{r+s}+\cdots+a_{r-1}b_{s+1}+a_rb_s+a_{r+1}b_{s-1}+\cdots+a_{r+s}b_0.$$

Alle Glieder dieser Summe sind durch p teilbar bis auf a_rb_s; also ist c_{r+s} nicht durch p teilbar.

Die vorstehende Betrachtung führt uns auf den Beweis des

Lemma von Gauß: Wenn ein Polynom $F(z)$ mit ganzen Koeffizienten reduzibel ist, so kann es in ein Produkt zweier Polynome mit ganzen Koeffizienten zerlegt werden.

Wir können ohne eine Einschränkung annehmen, daß F ein primitives Polynom ist, denn sonst könnte man es in die Form μF_1 bringen, wo F_1 primitiv und μ (der größte gemeinsame Teiler der Koeffizienten von F) eine ganze Zahl ist, so daß es offenbar ausreichen würde, den Satz für F_1 zu beweisen.

Wir setzen also voraus, daß $F(z)$ sich in das Produkt zweier Polynome $f(z)$ und $\varphi(z)$ mit rationalen Koeffizienten zerlegen läßt, und wollen zeigen, daß es sich dann auch in ein Produkt zweier Polynome mit ganzen Koeffizienten zerlegen läßt.

Wir bringen alle Koeffizienten von f auf den kleinsten gemeinsamen Nenner a; die Zähler werden dann einen größten gemeinschaftlichen Teiler α haben, der zu a prim ist. In derselben Weise operieren wir mit den Koeffizienten von φ, indem wir sie auf den kleinsten gemeinsamen Nenner b bringen; der größte gemeinsame Teiler der Zähler der so umgewandelten Koeffizienten sei β. Dann werden die Polynome $\frac{af}{\alpha}$ und $\frac{b\varphi}{\beta}$ ganze Koeffizienten haben und primitiv sein; ihr Produkt

$$\frac{ab}{\alpha\beta} f\varphi = \frac{ab}{\alpha\beta} F$$

wird also ein Polynom mit ganzen Koeffizienten und primitiv sein.

Infolge der ersten Bedingung wird, da die Koeffizienten von F keinen gemeinsamen Teiler haben, jeder in $\alpha\beta$ enthaltene Primfaktor in ab aufgehen müssen, und darum wird $\alpha\beta$ in ab aufgehen; infolge der zweiten Bedingung wird der Quotient $\frac{ab}{\alpha\beta} = c$ (der, wie gesagt, eine ganze Zahl ist) gleich 1 sein müssen, sonst würden die Koeffizienten von cF sämtlich durch $c > 1$ teilbar sein.

Also ist $F(z)$ das Produkt zweier Polynome, die ganze Koeffizienten haben und primitiv sind: $\frac{a}{\alpha} f$ und $\frac{b}{\beta}\varphi$, w. z. b. w.

Auf Grund des Gaußschen Lemmas kann man nun, indem man das Eisensteinsche Verfahren[1]) anwendet, leicht den am Anfang dieses Paragraphen erwähnten Satz beweisen:

---

1) Journ. f. Math., Bd. 39, pg. 167. Zwei andere Beweise desselben Satzes sind von Kronecker gegeben worden, vgl. Journ. f. Math., Bd. 29 und Journal de math. 12, vol. 1. Vgl. Bachmann, l. c.

Die Gleichung $\frac{z^p-1}{z-1}=0$, wo p eine Primzahl darstellt, ist irreduzibel.

Setzt man

$$z=x+1,$$

so wird die vorstehende Gleichung zu dieser:

$$F(x)\equiv x^{p-1}+px^{p-2}+\frac{p(p-1)}{1\cdot 2}x^{p-3}+\cdots+\binom{p}{r}x^{p-r-1}+\cdots+p=0.$$

Offenbar genügt es, die Irreduzibilität von $F(x)=0$ zu beweisen, da aus

$$\frac{z^p-1}{z-1}=\varphi_1(z)f_1(z),$$

wo φ_1 und f_1 zwei Polynome sind, folgt

$$F(x)=\varphi_1(x+1)f_1(x+1)=\varphi(x)f(x),$$

wo φ und f zwei neue Polynome sind.

Nehmen wir an, daß $F(x)=0$ reduzibel ist, daß wir also haben

$$F(x)=f(x)\cdot\varphi(x),$$

wo f und φ zwei Polynome mit ganzen Koeffizienten in x sind:

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n,$$
$$\varphi(x)=b_0x^m+b_1x^{m-1}+\cdots+b_m.$$

Führt man dann die Multiplikation $f\varphi$ aus, so wird man ein Polynom erhalten, das F identisch gleich ist:

$$c_0x^{n+m}+c_1x^{n+m-1}+\cdots+c_{n+m};$$

und es wird sein Grad $n+m=p-1$ sein.

Also werden wir folgende Formeln haben:

$$\begin{aligned}
c_0&=a_0b_0=1\\
c_1&=a_0b_1+a_1b_0=p\\
c_2&=a_0b_2+a_1b_1+a_2b_0=\frac{p(p-1)}{2}\\
&\cdots\cdots\cdots\cdots\\
c_{n+m-1}&=a_{n-1}b_m+a_nb_{m-1}=\frac{p(p-1)}{2}\\
c_{n+m}&=a_nb_m=p,
\end{aligned}$$

und darum werden alle Koeffizienten c_i mit Ausnahme von c_0, durch die Primzahl p teilbar sein.

Nun lehrt die letzte dieser Gleichungen, eben weil p eine Primzahl ist, daß eine der beiden Zahlen a_n, b_m gleich ± 1 ist und die andere $\pm p$; es sei z. B.

$$a_n=1,\ b_m=p.$$

Setzt man diese Werte in die vorletzte Gleichung ein, so findet man

$$c_{n+m-1} = a_{n-1}p + b_{m-1},$$

und da p in c_{n+m-1} aufgeht, so ist b_{m-1} durch p teilbar, d. h.

$$b_{m-1} = pb'_{m-1}.$$

Betrachtet man in analoger Weise den Koeffizienten c_{n+m-2}, so findet man

$$c_{n+m-2} = a_{n-2}p + a_{n-1}b'_{m-1}p + b_{m-2},$$

und darum ist b_{m-2} durch p teilbar, d. h.

$$b_{m-2} = pb'_{m-2}.$$

So ergibt sich nacheinander aus den Ausdrücken $c_{n+m-3}, \ldots, c_0$, daß alle Koeffizienten $b_{m-3}, \ldots, b_0$ durch p teilbar sind; aber in bezug auf b_0 zeigt sich der Schluß sofort als irrig, da die Gleichung

$$c_0 = a_0 b_0 = 1$$

ergibt:

$$a_0 = \pm 1,\ b_0 = \pm 1.$$

Der Widerspruch, auf den man durch die Annahme, daß F zerlegbar sei, geführt worden ist, zeigt, daß die Gleichung $F = 0$ und daher die Gleichung

$$\frac{z^p - 1}{z - 1} = 0$$

irreduzibel ist, w. z. b. w.

§ 6. Unmöglichkeit, die regulären Polygone, deren Seitenzahl eine Primzahl p ist, zu konstruieren, wenn nicht p von der Form $2^n + 1$ ist. Erinnern wir uns nun des fundamentalen Resultats des § 3, so schließen wir:

Wenn die Gleichung $\frac{z^p - 1}{z - 1} = 0$, wo p eine Primzahl ist, durch Quadratwurzelausdrücke lösbar ist, so muß $p - 1$ eine Potenz von 2 sein:

$$p = 2^n + 1.$$

Und infolgedessen:

Es ist nicht möglich, ein reguläres Polygon, das eine Primzahl p zur Seitenzahl hat, mit dem Lineal und dem Zirkel zu konstruieren, wenn nicht p von der Form $2^n + 1$ ist.

So sind z. B. die regulären Polygone von 7, 11, 13, 19, ... Seiten mit den genannten Instrumenten nicht konstruierbar.

§ 7. Konstruierbarkeit der regulären Polygone, deren Seitenzahl eine Primzahl p ist, wenn p die Form $2^n + 1$

hat. Dem negativen Resultate des vorigen Paragraphen steht das folgende positive Resultat gegenüber:

Ein reguläres Polygon von p Seiten, wo p eine Primzahl von der Form $2^n + 1$ ist, ist mit dem Lineal und dem Zirkel konstruierbar.

Zum Beweise dieses Satzes muß man zeigen, daß die (irreduzible) Gleichung

$$\frac{z^p - 1}{z - 1} = z^{p-1} + z^{p-2} + \cdots + z + 1 = 0$$

durch aufeinander folgende Quadratwurzelausziehungen lösbar ist, wenn p eine Primzahl von der Form $2^n + 1$ ist.

Die Wurzeln unserer Gleichung, d. h. die von 1 verschiedenen $p$ten Einheitswurzeln, sind

$$\begin{aligned}
\varepsilon_1 &= \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}\\
&\cdots\cdots\cdots\cdots\\
\varepsilon_r &= \cos\frac{2\pi r}{p} + i\sin\frac{2\pi r}{p}\\
&\cdots\cdots\cdots\cdots\\
\varepsilon_{p-1} &= \cos\frac{2\pi(p-1)}{p} + i\sin\frac{2\pi(p-1)}{p}.
\end{aligned}$$

Man kann sie alle erhalten, wenn man die aufeinander folgenden Potenzen irgend einer Wurzel ε bildet. Geht man z. B. von $\varepsilon = \varepsilon_1$ aus, so hat man in der Tat $\varepsilon_r = \varepsilon^r$.

Geht man von der Wurzel $\varepsilon = \varepsilon_2$ aus, so erhält man:

$$\varepsilon_2 = \varepsilon,\ \varepsilon_4 = \varepsilon^2,\ \varepsilon_6 = \varepsilon^3, \cdots \varepsilon_{p-1} = \varepsilon^{\frac{p-1}{2}},$$

$$\varepsilon_1 = \varepsilon^{\frac{p-1}{2}+1},\ \varepsilon_3 = \varepsilon^{\frac{p-1}{2}+2},\ \varepsilon_5 = \varepsilon^{\frac{p-1}{2}+3}, \cdots \varepsilon_{p-2} = \varepsilon^{p-1}.$$

In analoger Weise sind die aufeinander folgenden Potenzen irgend einer Wurzel $\varepsilon = \varepsilon_r$ mit den Exponenten $1, 2, \ldots, p-1$ alle voneinander verschieden und sie stellen daher (in anderer Reihenfolge) die Wurzeln $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{p-1}$ dar. In der Tat kann für $h < p$, $k < p$ nicht

$$\varepsilon_r^{\,h} = \varepsilon_r^{\,k}$$

sein, ohne daß

$$\varepsilon_r^{\,h-k} = 1,$$

d. h.

$$\cos\frac{2\pi r(h-k)}{p} + i\sin\frac{2\pi r(h-k)}{p} = 1$$

wäre, woraus folgte

$$2\pi\frac{r(h-k)}{p} = 2\pi s,$$

wobei s eine ganze Zahl ist; und diese Gleichung ist unmöglich, weil p eine Primzahl ist und also weder in $r < p$ noch in $(h - k) < p$ aufgehen kann.

Man bemerke auch, daß immer die Gleichung

$$\varepsilon^{l+mp} = \varepsilon^l$$

besteht, da

$$\varepsilon^{mp} = 1$$

ist.

Wollen wir nun in dem Studium der Wurzeln unserer Gleichung tiefer gehen, so müssen wir der Zahlentheorie folgenden Satz entnehmen:[1])

Ist eine Primzahl p gegeben, so existieren unter den Zahlen $1, 2, \ldots, p-1$ immer Zahlen g von der Beschaffenheit, daß die Potenzen

$$g, g^2, \ldots, g^{p-1},$$

durch p dividiert, als Reste die Zahlen

$$1, 2, \ldots, p-1,$$

in anderer Reihenfolge genommen, ergeben.

Eine solche Zahl g heißt eine Primitivwurzel des Moduls p.

Wenn z. B. $p = 5$ ist und man beginnt damit, die Zahl 2 zu betrachten, so erhält man

$$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16,$$

und diese Zahlen geben, durch 5 dividiert, die Reste

$$2,\ 4,\ 3,\ 1;$$

also ist 2 eine Primitivwurzel des Moduls 5.

Wenn man in dem Fall, daß $p = 7$ ist, die aufeinander folgenden Potenzen von 2 bildet, so erhält man die Zahlen

$$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16,\ 2^5 = 32,\ 2^6 = 64,$$

die, durch 7 dividiert, die Reste

$$2,\ 4,\ 1,\ 2,\ 4,\ 1$$

ergeben, und daher ist 2 keine Primitivwurzel des Moduls 7. Dagegen geben die aufeinander folgenden Potenzen von 3

$$3^1 = 3,\ 3^2 = 9,\ 3^3 = 27,\ 3^4 = 81,\ 3^5 = 243,\ 3^6 = 729,$$

durch 7 dividiert, die Reste

$$3,\ 2,\ 6,\ 4,\ 5,\ 1;$$

daher ist die Zahl 3 eine Primitivwurzel des Moduls 7.

1) Vgl. z. B. Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet, hrsgeg. von R. Dedekind. Vierte Aufl., Braunschweig 1894, pg. 67.

Indem wir den allgemeinen Fall irgend einer Primzahl p ins Auge fassen, setzen wir voraus, wir hätten eine Primitivwurzel g des Moduls p bestimmt, und nun betrachten wir aufs neue eine Wurzel ε der Gleichung

$$\frac{z^p - 1}{z - 1} = 0.$$

Wenn wir die aufeinander folgenden Potenzen

$$\varepsilon^g, \varepsilon^{g^2}, \varepsilon^{g^3}, \ldots, \varepsilon^{g^{p-1}}$$

bilden, so erkennen wir, daß diese in anderer Reihenfolge die Wurzeln

$$\varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}$$

ergeben. In der Tat, bezeichnet man mit s_r den Rest der Division von g^r durch p (so daß also $g^r = ph + s_r$), so erhalten wir, da $\varepsilon^{ph} = 1$ ist,

$$\varepsilon^{g^r} = \varepsilon^{s_r}$$

wo s_r alle Werte $1, 2, \ldots, p-1$ (in andrer Reihenfolge) annimmt, wenn r nacheinander die Werte $1, 2, \ldots, p-1$ erhält.

Nun teilen wir die Wurzeln

$$\varepsilon^g, \varepsilon^{g^2}, \ldots, \varepsilon^{g^{p-1}}$$

in zwei Gruppen:

$$\varepsilon^g, \varepsilon^{g^3}, \ldots, \varepsilon^{g^{p-2}}$$
$$\varepsilon^{g^2}, \varepsilon^{g^4}, \ldots, \varepsilon^{g^{p-1}}$$

und setzen:

$$\eta_1 = \varepsilon^g + \varepsilon^{g^3} + \cdots + \varepsilon^{g^{p-2}}$$
$$\eta_2 = \varepsilon^{g^2} + \varepsilon^{g^4} + \cdots + \varepsilon^{g^{p-1}}.$$

Hierauf teilen wir jede der oben gebildeten Gruppen in zwei andere, indem wir setzen:

$$\left.\begin{aligned} \eta_{11} &= \varepsilon^g + \varepsilon^{g^5} + \cdots + \varepsilon^{g^{p-4}} \\ \eta_{12} &= \varepsilon^{g^3} + \varepsilon^{g^7} + \cdots + \varepsilon^{g^{p-2}} \end{aligned}\right\} \quad \eta_{11} + \eta_{12} = \eta_1$$

$$\left.\begin{aligned} \eta_{21} &= \varepsilon^{g^2} + \varepsilon^{g^6} + \cdots + \varepsilon^{g^{p-3}} \\ \eta_{22} &= \varepsilon^{g^4} + \varepsilon^{g^8} + \cdots + \varepsilon^{g^{p-1}} \end{aligned}\right\} \quad \eta_{21} + \eta_{22} = \eta_2.$$

In dieser Weise kann man fortfahren, indem man nacheinander Summen von

$$\frac{p-1}{4}, \frac{p-1}{8}, \ldots$$

Gliedern bildet, so daß man schließlich (da $p-1$ eine Potenz von 2 ist) zu Summen von nur einem Gliede gelangt, d. h. zu den Wurzeln unserer Gleichung. Die so angegebenen Summen führen

den Namen „Gaußsche Perioden“. Wir wollen zeigen, wie diese Perioden sich durch aufeinander folgende Quadratwurzelausziehungen berechnen lassen.

Bemerken wir vor allem, daß die Summe

$$\eta_1 + \eta_2 = \eta = \varepsilon^g + \varepsilon^{g^2} + \cdots + \varepsilon^{g^{p-1}} = -1$$

ist, da η, abgesehen vom Zeichen, durch den Koeffizienten von z^{p-2} in der Gleichung

$$z^{p-1} + z^{p-2} + \cdots + 1 = 0,$$

deren Wurzeln die ε oder die ε^{g^r} sind, dargestellt wird.

Betrachten wir ferner das Produkt $\eta_1 \eta_2$.

Führt man die Multiplikation der beiden Summen, die η_1 und η_2 bilden, aus, so erhält man eine Summe von Gliedern von der Form

$$\varepsilon^{g^r} \varepsilon^{g^s} = \varepsilon^{g^r + g^s} = \varepsilon^h = \varepsilon^{g^t},$$

d. h. eine Summe von Gliedern, von denen jedes sich in einer der beiden Gruppen, die η_1 und η_2 bilden, findet.

Nun ändert sich der Ausdruck

$$\eta_1 \eta_2 = \Sigma \varepsilon^{g^t}$$

nicht, wenn man in ihm ε durch ε^g ersetzt, weil durch eine solche Substitution (wie leicht zu erkennen ist, da nach dem *Fermat*schen Satz $g^p \equiv g \pmod{p}$ und also $\varepsilon^{g^p} = \varepsilon^g$ ist) nur

$$\eta_1 \text{ in } \eta_2 \text{ und } \eta_2 \text{ in } \eta_1$$

verwandelt wird. Diese fundamentale Tatsache hat die Konsequenz, daß die Summe $\Sigma \varepsilon^{g^t}$ jede Wurzel der Gleichung

$$\frac{z^p - 1}{z - 1} = 0$$

genau gleich oft, sagen wir ϱ-mal, als Summanden enthält, und daher ist

$$\eta_1 \eta_2 = \Sigma \varepsilon^{g^t} = \varrho \eta = -\varrho.$$

Um klar zu sehen, wie man zu dieser Konsequenz gelangt, fassen wir zunächst in der Summe $\Sigma \varepsilon^{g^t}$ die Summanden von gleichem Werte zusammen, indem wir schreiben

$$\eta_1 \eta_2 = \varkappa \varepsilon^{g^r} + \lambda \varepsilon^{g^s} + \cdots,$$

und nun zeigen wir, daß die ganzen Koeffizienten $\varkappa, \lambda, \ldots$ sämtlich einander gleich sind, wozu nur zu zeigen ist, daß keiner von ihnen kleiner als ein beliebig gewählter anderer sein kann.

Wenn z. B. in der genannten Summe das Glied $\varrho \varepsilon^g$ enthalten ist und man ε durch ε^g ersetzt, so wird sich in ihr das Glied $\varrho \varepsilon^{g^2}$ be-

finden, und aus diesem wird man der Reihe nach die Glieder $\varrho\varepsilon^{g^3}$, $\varrho\varepsilon^{g^4}$, ... ableiten, die sämtlich in der Summe selbst auftreten müssen. Wenn in der Summe das Glied $\varrho\varepsilon^{g^2}$ enthalten ist und man ersetzt in ihm ε durch ε^g und nimmt der Reihe nach dieselbe Substitution in den nach und nach erhaltenen Gliedern vor, so wird man die Glieder

$$\varrho\varepsilon^{g^3},\ \varrho\varepsilon^{g^4},\cdots,\varrho\varepsilon^{g^{p-1}},\ (\varrho\varepsilon^{g^p}=\varrho\varepsilon^g)$$

erhalten, die ebenso sämtlich in der Summe auftreten müssen.

Und so folgt im allgemeinen aus der Existenz des Gliedes $\varrho\varepsilon^{g^t}$, daß die Summe alle Glieder

$$\varrho\varepsilon^{g^{t+1}},\ \varrho\varepsilon^{g^{t+2}},\cdots,\varrho\varepsilon^{g^{t+p-1}}$$

enthalten muß, die in anderer Reihenfolge die Glieder

$$\varrho\varepsilon^g,\ \varrho\varepsilon^{g^2},\cdots,\varrho\varepsilon^{g^{p-1}}$$

darstellen.

Also sehen wir, daß $\eta_1+\eta_2$ und $\eta_1\eta_2$ ganze Zahlen sind, und daher genügen η_1 und η_2 der Gleichung zweiten Grades

$$x^2+x-\varrho=0$$

mit ganzen Koeffizienten.

Zur Lösung dieser Gleichung ist nur die Quadratwurzel $\sqrt{1+4\varrho}$ zu ziehen, da η_1 und η_2 sich durch diese Wurzel ausdrücken.

Wir gehen nun an die Berechnung der Gaußschen Perioden von $\frac{p-1}{4}$ Gliedern

$$\eta_{11},\ \eta_{12},\ \eta_{21},\ \eta_{22}.$$

Vor allem ist

$$\eta_{11}+\eta_{12}=\eta_1,\ \eta_{21}+\eta_{22}=\eta_2.$$

Nun bilden wir die Produkte

$$\eta_{11}\eta_{12},\ \eta_{21}\eta_{22}.$$

Betrachten wir z. B. das erste dieser Produkte, so sehen wir, daß es auf eine Summe von Gliedern von der Form ε^{g^t} gebracht werden kann, und zwar auf eine Summe, die sich nicht ändert, wenn man in jedem Gliede ε durch ε^{g^2} ersetzt; in der Tat werden durch diese Substitution nur die Perioden η_{11} und η_{12} mit einander vertauscht. Daraus schließt man (wie oben), daß, wenn der Ausdruck von $\eta_{11}\eta_{12}$ ein Glied von η_1 in bestimmter Anzahl, etwa ϱ_1-mal, enthält, er ebenso oft die anderen Glieder derselben Summe enthält (wenn z. B. $\eta_{11}\eta_{12}$ das Glied $\varrho_1\varepsilon^g$ enthält, dann enthält es auch $\varrho_1\varepsilon^{g^3}$, $\varrho_1\varepsilon^{g^5}$, ...); und in analoger Weise enthält der genannte Ausdruck, wenn er

ein Glied von η_2 ϱ_2-mal enthält, alle anderen Glieder ϱ_2-mal, so daß also

$$\eta_{11}\eta_{12} = \varrho_1\eta_1 + \varrho_2\eta_2$$

ist, wo ϱ_1 und ϱ_2 ganze Zahlen sind.

Also sind η_{11} und η_{12} Wurzeln der Gleichung zweiten Grades

$$x^2 - \eta_1 x + (\varrho_1\eta_1 + \varrho_2\eta_2) = 0.$$

Daher kann man η_{11} und η_{12}, wenn man von η_1 und η_2 ausgeht, durch das Ausziehen einer Quadratwurzel berechnen. Analog erhält man η_{21} und η_{22}.

Es ist nunmehr klar, wie man hierauf zur Berechnung der Perioden von $\frac{p-1}{8}$ Gliedern gelangen kann.

Betrachten wir z. B. η_{111} und η_{112}, so ist ihre Summe

$$\eta_{111} + \eta_{112} = \eta_{11},$$

und ihr Produkt drückt sich durch eine lineare Kombination mit ganzen Koeffizienten von η_{11}, η_{12}, η_{21}, η_{22} aus; also erhält man η_{111} und η_{112} durch das Ausziehen einer neuen Quadratwurzel, die sich über die bereits erhaltenen Perioden erstreckt.

Geht man in derselben Weise weiter vor, so kann man die Perioden von

$$\frac{p-1}{16}, \frac{p-1}{32}, \ldots$$

Gliedern konstruieren und schließlich die Perioden eines Gliedes

$$\left(\frac{p-1}{2^n} = 1\right),$$

d. h. die Wurzeln ε der vorgelegten Gleichung.

Wir können also schließen: Wenn p eine Primzahl von der Form $2^n + 1$ ist, so kann die Gleichung

$$\frac{z^p - 1}{z - 1} = 0$$

durch aufeinander folgende Quadratwurzelausziehungen gelöst werden, und daher ist das reguläre Polygon von p Seiten mit dem Lineal und dem Zirkel konstruierbar.

Anmerkung. In der vorstehenden Erörterung haben wir nicht der Ungewißheit Rechnung getragen, die bei der Wahl der Vorzeichen, die den nacheinander eingeführten Quadratwurzeln zu erteilen sind, sich darbietet. Und in der Tat braucht man mit dieser Ungewißheit sich nicht zu beschäftigen, wenn es sich nur um den Beweis handelt, daß die Perioden η sich durch Quadratwurzeln ausdrücken lassen und

daher die gegebene Gleichung $\frac{z^p - 1}{z - 1} = 0$ selbst durch die genannten Wurzeln lösbar ist. Geht man zur wirklichen Auflösung über, so wird man, wenn man die Unbestimmtheit der Vorzeichen der genannten Wurzeln bestehen läßt, alle Wurzeln ε der vorgelegten Gleichung erhalten. Aber wenn von vornherein eine besondere Wurzel ε für die Konstruktion der Perioden η vorgeschrieben sein sollte, so würde man, um zu ihrer Berechnung zu gelangen, die genannten Vorzeichen nach und nach in geeigneter Weise bestimmen müssen. Die hier auftretenden besonderen Regeln für die Bestimmung der Vorzeichen werden für den Fall $p = 17$ im sechsten Artikel erläutert werden, wo sie für die wirkliche Konstruktion des Siebzehnecks von Interesse sind.

§ 8. Über die Primzahlen von der Form $2^n + 1$. Die erhaltenen Resultate gewinnen durch folgende Bemerkung an Bedeutung.

Jede Primzahl von der Form $2^n + 1$ ist auch von der Form $2^{2^\nu} + 1$, das will sagen, wenn $2^n + 1$ eine Primzahl ist, so muß n seinerseits eine Potenz von 2 sein.

Um diesen Satz zu beweisen, hat man nur zu zeigen, daß, wenn n einen ungeraden Teiler $2k + 1$ hat:

$$n = h(2k + 1),$$

die Zahl

$$2^n + 1 = 2^{h(2k+1)} + 1$$

keine Primzahl sein kann.

Nun erkennt man sofort, daß die Zahl $2^{h(2k+1)} + 1$ keine Primzahl sein kann, da sie durch $2^h + 1$ teilbar ist. In der Tat wird das Binom

$$x^{2k+1} + 1$$

für $x = -1$ Null, und es ist also durch $x + 1$ teilbar. Man hat

$$x^{2k+1} + 1 = (x + 1)\,[x^{2k} - x^{2k-1} + \cdots + (-1)^\nu x^{2k-\nu} + \cdots + 1].$$

Setzt man hierin

$$x = 2^h,$$

so ergibt sich gerade, daß $2^{h(2k+1)} + 1$ durch $2^h + 1$ teilbar ist.

Nun können wir die Resultate der vorstehenden Nummern in folgender Weise aussprechen:

Die mit dem Lineal und dem Zirkel konstruierbaren regulären Polygone, deren Seitenzahl eine Primzahl p ist, sind diejenigen, für welche p von der Form

$$p = 2^{2^\nu} + 1.$$

ist.

Um die Tragweite dieser Aussage zu erkennen, wollen wir ν die Werte

$$\nu = 0, 1, 2, 3, 4$$

beilegen; dadurch erhalten wir die Primzahlen

$$p = 2^{2^\nu} + 1 = 3, 5, 17, 257, 65537.$$

Die Werte $p = 3, p = 5$ entsprechen den sehr bekannten Fällen des gleichseitigen Dreiecks und des regulären Fünfecks, während die folgenden Werte auf drei neue konstruierbare reguläre Polygone führen, unter denen besonders der Fall $p = 17$ bemerkenswert ist. Die Lösung der binomischen Gleichung $z^{17} = 1$ wurde von Gauß angegeben, und den geometrischen Konstruktionen des Siebzehnecks wandten sich spätere Arbeiten (von Legendre, Grunert, v. Staudt, Serret, Schröter, Gérard) zu, über die im sechsten Artikel berichtet wird.

Der Fall $p = 257$ wurde von Richelot[1]) studiert, dessen Resultate von Affolter und Pascal[2]) geometrisch interpretiert wurden.

Der Fall $p = 65537$ ist der Gegenstand einer sehr sorgfältigen Arbeit von Hermes[3]) gewesen.

Was passiert nun für $\nu > 4$? Erhält man noch Primzahlen

$$p = 2^{2^\nu} + 1$$

und daher neue konstruierbare reguläre Polygone?

Die bisher untersuchten Fälle beziehen sich auf die Zahlen, die den Werten

$$\nu = 5, 6, 7$$

entsprechen, d. h. auf die Zahlen

$$2^{2^5} + 1,\ 2^{2^6} + 1,\ 2^{2^7} + 1,$$

und dies sind, wie man gefunden hat, keine Primzahlen.

Daher ist es noch zweifelhaft, ob die Reihe der Zahlen

$$2^{2^\nu} + 1$$

andere Primzahlen enthält als die, welche den Werten

$$\nu = 0, 1, 2, 3, 4$$

entsprechen.

1) Journ. f. Math. Bd. 9 (1832).
2) Rendic. della R. Accademia di Napoli 1887.
3) Göttinger Nachrichten 1894.

§ 9. Anwendung der Gaußschen Methode auf den Fall des regulären Fünfecks. Wir wollen schließlich als Beispiel zeigen, wie die dargelegte Methode zur Lösung der Gleichung

$$z^5 = 1,$$

von der die Konstruktion des regulären Fünfecks abhängt, Anwendung findet.

Die Wurzeln der genannten Gleichung sind

$$1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4,$$

wo

$$\varepsilon = \cos\frac{2\pi}{5} + i \sin\frac{2\pi}{5}$$

ist.

Wir wählen eine Primitivwurzel des Moduls 5 aus; es sei $g = 2$. Dann werden die ε in folgender Weise geordnet:

$$\varepsilon^2, \varepsilon^4, \varepsilon^8 = \varepsilon^3, \varepsilon^{16} = \varepsilon.$$

Die zweigliedrigen Perioden sind dann gegeben durch

$$\eta_1 = \varepsilon^2 + \varepsilon^3, \quad \eta_2 = \varepsilon^4 + \varepsilon,$$

und es ist

$$\eta_1 + \eta_2 = \eta = -1,$$

$$\eta_1 \eta_2 = (\varepsilon^2 + \varepsilon^3)(\varepsilon^4 + \varepsilon) = \varepsilon^6 + \varepsilon^3 + \varepsilon^7 + \varepsilon^4 = \varepsilon + \varepsilon^3 + \varepsilon^2 + \varepsilon^4 = \eta = -1;$$

daher sind η_1 und η_2 die Wurzeln der Gleichung

$$x^2 + x - 1 = 0,$$

d. h.

$$\eta_1 = -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{5}$$
$$\eta_2 = -\tfrac{1}{2} \mp \tfrac{1}{2}\sqrt{5}.$$

Wir betrachten nun die eingliedrigen Perioden

$$\eta_{21} = \varepsilon^4, \quad \eta_{22} = \varepsilon,$$

wo

$$\eta_{21} + \eta_{22} = \eta_2$$
$$\eta_{21}\eta_{22} = \varepsilon^5 = 1$$

ist. Wir bilden also die Gleichung zweiten Grades

$$x^2 - \eta_2 x + 1 = 0$$

und erhalten, indem wir sie auflösen,

$$\varepsilon = \tfrac{1}{4}\left\{-1 \mp \sqrt{5} \pm \sqrt{-10 \pm 2\sqrt{5}}\right\}$$

oder

$$\varepsilon = \tfrac{1}{4}\left\{-1 \mp \sqrt{5} \pm i\sqrt{10 \mp 2\sqrt{5}}\right\}.$$

Die vier Wurzeln ε der binomischen Gleichung $z^5 = 1$ werden durch

diese Formel gegeben, wenn man den Wurzeln die Vorzeichen + und − erteilt. Man kann (auf sehr leichte Weise) geometrisch erkennen, daß die Wurzel

$$\varepsilon = \cos\frac{2\pi}{5} + i\,\sin\frac{2\pi}{5}$$

dadurch gegeben wird, daß man alle Wurzeln positiv nimmt, also

$$\varepsilon = \tfrac{1}{4}\left\{-1 + \sqrt{5} + i\sqrt{10 + 2\sqrt{5}}\right\}$$

setzt.

Die Formel

$$\eta_2 = 2\cos\frac{2\pi}{5} = \tfrac{1}{2}\left(-1 + \sqrt{5}\right)$$

gibt übrigens eine sehr einfache Konstruktion des regulären Fünfecks.

§ 10. Reguläre Polygone mit zusammengesetzter Seitenzahl. Wir wollen nun etwas über die Konstruierbarkeit der regulären Polygone von n Seiten, wo n eine zusammengesetzte Zahl ist, sagen. Vor allem bemerken wir, daß, wenn n sich in das Produkt zweier ganzer Zahlen p und q:

$$n = pq$$

zerlegen läßt und das reguläre n-eck gegeben ist, dann sofort das p-eck und das q-eck sich konstruieren lassen. In der Tat, ist der Kreisbogen $\frac{2\pi}{n}$ (dessen Sehne die Seite des n-ecks ist) oder, wenn man will, der zugehörige Zentriwinkel gegeben, so hat man ihn nur mit q zu multiplizieren, um den Bogen oder Winkel

$$\frac{2\pi q}{n} = \frac{2\pi}{p}$$

zu erhalten, von dem die Konstruktion des p-ecks abhängt.

Nehmen wir nun an, es sei n in seine Primfaktoren $p_1, p_2, \ldots, p_\nu$ zerlegt:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\nu^{\alpha_\nu}.$$

Damit die Konstruktion des n-ecks möglich ist, wird die Konstruktion der regulären Polygone von $p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_\nu^{\alpha_\nu}$ Seiten möglich sein müssen.

Die Konstruktion des regulären Polygons von p^α Seiten ($\alpha > 1$) hängt von der Lösung der binomischen Gleichung

$$z^{p^\alpha} = 1$$

ab, die (wie auch geometrisch klar ist) alle Wurzeln der Gleichung

$$z^{p^{\alpha-1}} = 1$$

enthält. Also ist nur die Gleichung

$$\frac{z^{p^\alpha}-1}{z^{p^{\alpha-1}}-1}=0$$

zu untersuchen. Diese Gleichung ist irreduzibel.

Dieser Satz wird nach demselben Eisensteinschen Verfahren bewiesen, das für den Fall $\alpha = 1$ zur Anwendung kam (§ 5).

Aus diesem Satze folgt, daß die genannte Gleichung nur dann durch Quadratwurzeln lösbar ist, wenn ihr Grad $p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$ eine Potenz von 2 ist. Aber die Zahl $p^{\alpha-1}$, wo $\alpha > 1$, kann nicht eine Potenz von 2 sein, wenn nicht $p = 2$ ist.

Daraus schließt man, daß es kein konstruierbares reguläres Polygon von p^α Seiten gibt, wenn

$$\alpha > 1,\ p > 2.$$

Wenn also das reguläre n-eck konstruierbar ist, so muß die Zahl

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

außer einer gewissen Potenz von 2 lauter verschiedene Primfaktoren (in der ersten Potenz) enthalten, und diese Faktoren p müssen sämtlich von der Form $2^{2^\nu}+1$ sein, da das reguläre Polygon von p Seiten konstruierbar sein soll (§ 8); also muß die Zahl n die Form

$$n = 2^\nu (2^{2^{\nu_1}}+1)(2^{2^{\nu_2}}+1)\cdots(2^{2^{\nu_s}}+1)$$

haben, wo die $\nu_1, \nu_2, \ldots, \nu_s$ sämtlich voneinander verschieden und

$$p_1 = 2^{2^{\nu_1}}+1,\ p_2 = 2^{2^{\nu_2}}+1, \cdots$$

Primzahlen sind.

Wir wollen nun noch nachweisen, daß, wenn n eine Zahl von der angegebenen Form ist, die Konstruktion des regulären n-ecks wirklich ausführbar ist.

Zu diesem Ende ist nur zu zeigen, wie man, „wenn die regulären Polygone von r und s Seiten gegeben sind, wo r und s zueinander prim sind, das reguläre Polygon von $n = rs$ Seiten konstruieren kann".

Setzt man die regulären Polygone von r und s Seiten als gegeben voraus, so sind auch die entsprechenden Zentriwinkel

$$a = \frac{2\pi}{r},\ b = \frac{2\pi}{s}$$

gegeben. Wenn nun r und s prim zueinander sind, dann kann man die unbestimmte Gleichung

$$sx - ry = 1$$

lösen, indem man zwei ganze Zahlen x und y, die ihr genügen, bestimmt. Dann wird

$$ax - by = 2\pi\left(\frac{x}{r} - \frac{y}{s}\right) = \frac{2\pi}{rs} = \frac{2\pi}{n}$$

sein, und man wird also die Konstruktion des Zentriwinkels des n-ecks (und darum die Konstruktion des n-ecks selbst) erhalten, indem man die Differenz zwischen den Winkeln ax und by bildet.

Als Beispiel betrachten wir den Fall des regulären Fünfzehnecks ($n = 15$), dessen Konstruktion sich aus der des gleichseitigen Dreiecks und der des regulären Fünfecks ableiten läßt. Wir lösen die unbestimmte Gleichung

$$3x - 5y = 1$$

auf, indem wir

$$x = 2,\ y = 1$$

setzen.

Der Zentriwinkel des Fünfzehnecks wird also konstruiert, indem man die Differenz zwischen dem doppelten Zentriwinkel des Fünfecks und dem Zentriwinkel des gleichseitigen Dreiecks bildet:

$$\frac{2\pi}{15} = 2 \cdot \frac{2\pi}{5} - \frac{2\pi}{3}.$$

Diese Konstruktion ist von der des Euklid, wo der Winkel

$$\frac{2\pi}{3} - \frac{2\pi}{5} = \frac{4\pi}{15}$$

halbiert wird, nicht wesentlich verschieden.

Fassen wir schließlich die erhaltenen Resultate zusammen, so können wir den Satz aussprechen:

Die mit dem Lineal und dem Zirkel konstruierbaren regulären n-ecke sind alle diejenigen und nur diejenigen, für welche die Zahl n, in Primfaktoren zerlegt, von der Form

$$n = 2^{\nu}(2^{2^{\nu_1}} + 1)(2^{2^{\nu_2}} + 1) \cdots (2^{2^{\nu_s}} + 1)$$

ist, wo die $\nu_1, \nu_2, \ldots, \nu_s$ voneinander verschieden sind.

§ 11. Bemerkung über die Bestimmung derjenigen regulären Polygone, welche nicht elementar konstruierbar sind. Wir wollen diesen Artikel mit einigen Andeutungen über die Bestimmung derjenigen regulären Polygone schließen, welche nicht mit dem Lineal und dem Zirkel konstruierbar sind. Und indem wir den einfachsten Fall eines regulären Polygons von p Seiten ins Auge fassen, wo p eine Primzahl ist, wollen wir an einem Beispiel dartun,

was uns in dieser Hinsicht die Gaußsche Methode für die Auflösung der binomischen Gleichung

$$z^p = 1$$

lehrt.

Nehmen wir also $p = 7$ und betrachten wir die Wurzeln der Gleichung $z^7 = 1$ (ohne $z = 1$):

$$\varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5, \varepsilon^6,$$

wo

$$\varepsilon = \cos\frac{2\pi\nu}{7} + i\sin\frac{2\pi\nu}{7} \quad (\nu = 1, \cdots, 6).$$

Wir wählen eine Primitivwurzel des Moduls 7 aus; es sei $g = 3$. Sie läßt uns die ε in folgender Weise ordnen:

$$\varepsilon^3, \varepsilon^{3^2} = \varepsilon^2, \ \varepsilon^{3^3} = \varepsilon^6, \ \varepsilon^{3^4} = \varepsilon^4, \ \varepsilon^{3^5} = \varepsilon^5, \ \varepsilon^{3^6} = \varepsilon.$$

Wir bilden die Perioden von drei Gliedern:

$$\eta_1 = \varepsilon^3 + \varepsilon^{3^3} + \varepsilon^{3^5} = \varepsilon^3 + \varepsilon^6 + \varepsilon^5$$
$$\eta_2 = \varepsilon^{3^2} + \varepsilon^{3^4} + \varepsilon^{3^6} = \varepsilon^2 + \varepsilon^4 + \varepsilon,$$

und erhalten

$$\eta_1 + \eta_2 = \eta = -1,$$
$$\eta_1\eta_2 = (\varepsilon^3 + \varepsilon^6 + \varepsilon^5)(\varepsilon^2 + \varepsilon^4 + \varepsilon) = \varepsilon^5 + \varepsilon^7 + \varepsilon^4 + \varepsilon^8 + \varepsilon^{10} + \varepsilon^7 + \varepsilon^7 + \varepsilon^9 + \varepsilon^6 = \eta + 3 = 2,$$

und daher genügen η_1 und η_2 der quadratischen Gleichung

$$x^2 + x + 2 = 0.$$

Sind dann η_1 und η_2 einmal berechnet, dann hängt die Bestimmung der Wurzeln ε von einer kubischen Gleichung ab. In der Tat erhält man z. B.

$$\varepsilon^2 + \varepsilon^4 + \varepsilon = \eta_2$$
$$\varepsilon^2 \cdot \varepsilon^4 + \varepsilon^2 \cdot \varepsilon + \varepsilon^4 \cdot \varepsilon = \eta_1$$
$$\varepsilon^2 \cdot \varepsilon^4 \cdot \varepsilon = 1,$$

und daher sind $\varepsilon^2, \varepsilon^4, \varepsilon$ die Wurzeln der Gleichung

$$x^3 - \eta_2 x^2 + \eta_1 x - 1 = 0.$$

Davon, daß man diese Reduktion wirklich ausführt, hängt die Möglichkeit ab, die Konstruktion des regulären Siebenecks auf die Dreiteilung eines Winkels zurückzuführen (vgl. Art. VII).

Das allgemeine Problem der binomischen Gleichung $z^p = 1$, wo p irgend eine Primzahl ist, gestattet immer (wie für $p = 7$) eine Reduktion, indem es sich auf die Lösung einer Reihe von Gleichungen niederen Grades zurückführen läßt. Wenn $p - 1$, in Primfaktoren zerlegt, von der Form

$$p - 1 = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3} \cdots$$

ist, so werden nach einander genau

α_1 Gleichungen zweiten Grades,
α_2 Gleichungen dritten Grades,
α_3 Gleichungen fünften Grades usw.

aufzulösen sein.

Eine solche Reduktion wird durch die Gaußsche Methode hervorgebracht, die dazu führt, nacheinander Perioden von

$$\frac{p-1}{2}, \frac{p-1}{4}, \cdots, \frac{p-1}{2^{\alpha_1}}$$

Gliedern, dann Perioden von

$$\frac{p-1}{2^{\alpha_1} \cdot 3}, \cdots, \frac{p-1}{2^{\alpha_1} 3^{\alpha_2}}$$

Gliedern, Perioden von

$$\frac{p-1}{2^{\alpha_1} 3^{\alpha_2} \cdot 5}, \cdots, \frac{p-1}{2^{\alpha_1} 3^{\alpha_2} 5^{\alpha_3}}$$

Gliedern usw. zu bilden.[1])

Vom geometrischen Standpunkte aus interessieren uns die ersten Fälle, in denen $p - 1$ nur die Zahlen 2 und 3 zu Primfaktoren hat, da man dann einfache Konstruktionen des p-ecks angeben kann, indem man einen Winkeldreiteiler oder eine feste Parabel anwendet, Hilfsmittel, mit denen man, wenn man außerdem das Lineal und den Zirkel benutzt, alle Aufgaben dritten Grades lösen kann (vgl. Art. VII).

Wir beschränken uns hier darauf, die folgenden Arbeiten anzuführen, die die einfachsten Fälle behandeln. Für $p = 7, 13, 97$ kann man nachsehen: E. Pascal, Giornale di Matematiche di Battaglini, vol. 25; für $p = 19, 37$: U. Amaldi, ebenda, vol. 30.

1) Vgl. Bachmann l. c., Bianchi l. c., wo auch die Formeln für die wirkliche Auflösung angegeben sind.

bis zu ihnen zurückgelegt hat, und es bleibt ihnen ihre innigere Berührung mit der Form, in der die praktischen Aufgaben gewöhnlich auftreten. Daher wollen wir von dem, was die alten Geometer uns gelehrt haben, nichts beiseite legen und wenden uns an eine breitere und höhere wissenschaftliche Ausbildung nur, um uns die Verhältnisse jener elementaren Geometrie klar zu machen, deren bewundernswerte Einzelheiten sehr wohl dem Glanze der modernen allgemeinen Begriffe entsprechen.

Berichtigungen.

S. 42, Z. 21 v. o. statt anM lies Man
S. 98, Z. 16 v. u. statt ; lies :
S. 112, Z. 3 v. u. und S. 113, Z. 3 v. o. statt $\frac{O}{O}\frac{M}{E}$ lies $\frac{OM}{OE}$
S. 113, Z. 11 v. o. statt $\frac{X'}{O'}\frac{E'}{E'}$ lies $\frac{X'E'}{O'E'}$
S. 117, Z. 15 v. o. statt $\frac{O'}{O'}\frac{M_x}{E_x}$ lies $\frac{OM_x}{OE_x}$
S. 120, Z. 1 v. u. statt Beziehnng lies Beziehung
S. 140, Z. 3 v. o. statt im § 9 lies in den §§ 8—10
S. 181, Z. 5 v. u. statt mit der Abszisse lies von der Abszisse
S. 270, Z. 8 v. u. statt arithmetich lies arithmetisch
S. 308, Z. 14 v. o. statt algebraischen lies algebraischer
S. 319, Z. 11 v. u. statt $\gamma_{n-1}{}^{(n-1)!}+\cdots+\gamma_1{}^{1!}$ lies $\gamma_{n-1}(n-1)!+\cdots+\gamma_1 1!$
