DET KGL. NORSKE VIDENSKABERS SELSKABS SKRIFTER. 1896. No. 7.

ÜBER DIE AUFLÖSBARKEIT EINIGER UNBESTIMMTEN GLEICHUNGEN

VON

AXEL THUE

AKTIETRYKKERIET I TRONDHJEM.
1897.

Über die Auflösbarkeit einiger unbestimmten Gleichungen

von

Axel Thue.

In der Gleichung:

$$F\,(x_1\ x_2 \cdots x_n) = o$$

bezeichne F eine ganze ganzzahlige homogene Function $(n-1)$ ten Grades der variablen Grössen $x_1 \cdots x_n$.

Ich behaupte, dass diese Gleichung sich immer in ganzen Zahlen $x_1 \cdots x_n$ *algemein auflösen lässt, wenn man die Function als eine Differenz zweier Produkten von $(n-1)$ linearen homogenen ganzzahligen Factoren der Grössen* $x_1 \cdots x_n$ *schreiben kann.*

Haben wir nämlich eine Gleichung von der Form:

$$P_1 \cdot P_2 \cdots P_{n-1} = Q_1 \cdot Q_2 \cdots Q_{n-1} \tag{I}$$

wo jedes P und jedes Q eine lineare homogene und ganzzahlige Function der Variablen $x_1 \cdots x_n$ ist, und diese Gleichung für ganzzahlige Werthe der Grössen $x_1 \cdots x_n$ besteht, dann bekommen wir statt der Gleichung ein System von Gleichungen:

$$\left.\begin{aligned} a_1 \cdot P_1 &= a_2 \cdot Q_1 \\ a_2 \cdot P_2 &= a_3 \cdot Q_2 \\ a_{n-1} \cdot P_{n-1} &= a_1 \cdot Q_{n-1} \end{aligned}\right\} \tag{II}$$

wo $a_1 \cdots a_{n-1}$ ganze Zahlen sind ohne irgend einen gemeinschaftlichen Divisor zu besitzen.

Gebe ich nemlich a_1 einen beliebigen rationalen Werth, so werden ja dadurch $a_2 \cdots a_{n-1}$ rational bestimmt, da $P_1 \cdots Q_{n-1}$ ganze Zahlen sind.

Die auf diese Weise gefundenen Grössen a können wir dann mit ihrem gemeinsamen Generalnenner multipliciren und endlich die erhaltenen Zahlen mit ihrem grössten gemeinschaftlichen Factor dividiren.

Unsere Zahlen a haben nun die oben erwünschten Eigenchaften.

Die Gleichungen in (II) können wir auch so schreiben:

$$\begin{aligned} A_1 \ x_1 + B_1 \ x_2 + \cdots + H_1 \ x_n &= o \\ A_2 \ x_1 + B_2 \ x_2 + \cdots + H_2 \ x_n &= o \\ &\qquad \qquad \text{(III)} \\ A_{n-1} x_2 + B_{n-1} x_2 + \cdots + H_{n-1} x_n &= o \end{aligned}$$

Also haben wir:

$$\frac{x_1}{x_n} = \frac{\triangle_1}{\triangle_n}$$

$$\frac{x_2}{x_n} = \frac{\triangle_2}{\triangle_n}$$

$$\cdots\cdots\cdots\cdots$$

$$\frac{x_{n-1}}{x_n} = \frac{\triangle_{n-1}}{\triangle_n}$$

oder

$$\begin{aligned} x_1 &= k \triangle_1 \\ x_2 &= k \triangle_2 \\ &\cdots\cdots\cdots \qquad \text{(IV)} \\ x_n &= k \triangle_n \end{aligned}$$

wo $\triangle_1 \cdots \triangle_n$ ganze, ganzzahlige und homogene Functionen $(n-1)$ ten Grades der Grössen $a_1 \cdots a_{n-1}$ sind.

k musz so beschaffen sein, dass $x_1 \cdots x_n$ ganze Zahlen werden.

Wir haben hier die Formen, der Zahlen x_1 x_n gefunden, wir sehen aber auch, dass diese Werthe der gegebenen Gleichung befriedigen.

Sind die Gleichungen (III) von einander abhängig, wird die obenstehende Entwickelung illusorisch. Von solchen Fällen aber wollen wir absehen.

Enthalten die Factoren in (I) mehrere Unbekannten als n *z.B.* $n+m$. so braucht man nur beide Seiten der Gleichung (I) mit einem Producte von m linearen homogenen und ganzzahligen Factoren zu multipliciren um die Gleichung durch unsere Methode auflösen zu können.

Sind dagegen die Anzahl der Unbekannten kleiner als n *z.B.* gleich $n-m$ und die Gleichung (I) doch in ganzen Zahlen möglich ist, dann erhalten wir des Systems (II) wegen statt dieser Gleichung in Allgemeinheit m homogene ganzzahlige Gleichungen $(n-m)$ ten Grades der ganzen Zahlen $a_1 \cdots a_{n-1}$.

Ist $F(x_1 \cdots x_n) = o$ nicht länger eine homogene Gleichung, können wir trotzdem, wie später gezeigt wird, in vielen Fällen unseres Verfahren benutzen um zu der ganzzahligen Auflösung der Gleichung zu erlangen.

Lässt sich die Gleichung: $F(x_1 \cdots x_n) = o$ auf die Form (I) bringen, so sicht man, dass jede gleichzeitige ganzzahlige Auflösung zweier Gleichungen

$$P_\alpha = o \qquad Q_\beta = o \qquad \alpha, \beta = 1, \cdots n-1$$

eine Lösung der Gleichung $F(x_1 \cdots x_n) = o$ giebt.

Umgekehrt können wir beweisen, dass wenn eine Gleichung:

$$F(x_1 \cdots x_n) = o$$

eine gewisse Anzahl solcher Lösungen

$$P_\alpha = o \qquad Q_\beta = o$$

besitzt, dann lässt sich die Gleichung auf die Form (I) bringen, wodurch wieder, wie gezeigt, die allgemeinste Lösung gefunden werden kann.

Man hat nämlich das folgende *Theorem:*

Verschwindet die ganze Function $F(x_1 \cdots x_n)$ *m ten Grades immer gleichzeitig mit den Producten*

$$U = P_1 \cdot P_2 \cdots P_p \qquad V = Q_1 \cdot Q_2 \cdots Q_q$$

wo die P und Q lineare Functionen der Grössen $x_1 \cdots x_n$ *sind, dann ist:*

$$F(x_1 \cdots x_n) = A \cdot U + B \cdot V$$

vorausgesetzt dass keine anderen der Factoren P und Q indentisch verschwinden, wenn zwei von ihnen gleich Null gesetzt werden.

A und B sind ganze Functionen vom Grade respective $m - p$ und $m - q$ in den Grössen $x_1 \cdots x_n$.

Infolge des Taylorschen Lehrsatzes bekommt mann:

$$F(x_1 x_2 x_3 \cdots x_n) \equiv F(a b x_3 \cdots x_n) + (x_1 - a) \cdot R + (x_2 - b) T$$

wo R und T ganze Functionen, der Grössen $a\ b\ x_3 \cdots x_n$ sind.

Ferner erhält man von den Gleichungen

$$P_h = (x_1 \cdots x_n) = o \qquad Q_k(x_1 \cdots x_n) = o$$

$$x_1 = \psi_1(x_3 \cdots x_n) \qquad x_2 = \psi_2(x_3 \cdots x_n)$$

wo ψ_1 und ψ_2 lineare Functionen der Grössen $x_3 \cdots x_n$ sind. Ist nun

$$F(\psi_1\ \psi_2\ x_3 \cdots x_n) \equiv o$$

dann erhalten wir also

$$F(x_1 \cdots x_n) \equiv (x_1 - \psi_1) R_0 + (x_2 - \psi_2) T_0$$

wo die ganzen Functionen R_0 und T_0 nur die Variablen $x \cdots x_n$ enthalten.

Nun hat man aber, wie leicht zu sehen ist,

$$x_1 - \psi_1 = \alpha P_h + \beta Q_k$$
$$x_2 - \psi_2 = \gamma P_h + \delta Q_k$$

wo $\alpha\ \beta\ \gamma\ \delta$ Konstanten sind. Also wird

$$F(x_2 \cdots x_n) = K P_h + H Q_k$$

wo K und H ganze Functionen der Grössen $x_1 \cdots x_n$ sind.

Mit Hülfe dieses Satzes haben wir *z.B.*

$$F(x_1 \cdots x_n) = K_1 P_1 + H_1 Q_1$$

Nun verschwindet F für $P_1 = o$ und $Q_2 = o$. Folglich hat man auch unter denselben Bedingungen $H_1 = o$ und also

$$H_1 = H_2 P_1 + H_3 Q_2 \text{ oder}$$

$$F = K_2 P_1 + H_4 Q_1 . Q_2$$

Geht man auf diese Weise fort, erhalten wir:

$$F = M P_1 + N . V$$

Diesen Satz können wir nun wieder benutzen. Wir haben nämlich dass F verschwindet wenn $P_2 = o$ und $V = o$ und folglich muss dann auch M verschwinden, oder infolge des erhaltenen Satzes

$$M = M_1 . P_2 + N_1 . V$$

d.h.

$$F = M_3 . P_1 P_2 + N_2 . V$$

Durch Wiederholung dieses Verfahrens wird somit unsere Behauptung bewiesen.

Von dem Satze, der auch auf die Geometrie anwendbar ist, kann man nun verschiedene Schlüsse ziehen.

Substituiren wir die in (IV) gefundene Werthe der Grössen $x_1 \cdots x_n$ in die Gleichungen (III) oder (II) so erhalten wir lauter Identitets gleichungen in den willkürlichen Variablen $a_1 \cdots a_{n-1}$. Die Determinanten $\triangle_1 \cdots \triangle_n$ müssen also so beschaffen sein, dass man immer die Gleichungen

$$(p_1 a_\alpha + q_1 a_\beta) \triangle_1 + \cdots + (p_n a_\alpha + q_n a_\beta) \triangle_n = o$$

$$\alpha < n - 1 \qquad \beta = \alpha + 1$$
$$\alpha = n - 1 \qquad \beta = 1$$

durch passende Wahl der Constanten p und q identisch befriedigen kann ohne dass alle p und q dadurch gleich Null zu setzen sind. In dieser Bemerkung die, wie man sieht, erweitert werden kann, besitzen wir eine Methode mit Hülfe deren die Eliminationsgleichung $F(x_1 \cdots x_n) = o$ der Gleichungen (IV) auf die Form (I) gebracht werden kann. Wir haben ferner auch hier ein Mittel zu beurtheilen ob gewisse unbestimmte Gleichungen algemein aufgelöst sind.

Wir wollen ein ganz einfaches Beispiel nehmen. Es sei

$$x = 2\,ab \qquad y = a^2 - b^2 \qquad z = a^2 + b^2$$

Werden a und b eliminiert bekommt mann:

$$z^2 = x^2 + y^2$$

Wir setzen:

$$(pa + qb)\,[2\,ab] + (p'a + q'\,b)\,[a^2 - b^2] + (p''a + q''b)\,[a^2 + b^2] = o$$

also: $q' = -p \qquad p' = q$

$q'' = -p \qquad p'' = -q$

oder $$a\,(p\,x + q\,y - q\,z) = b\,(-q\,x + p\,y + p\,z)$$
$$b\,(-q'\,x + p'\,y + p'\,z) = a\,(p'\,x + q'\,y - q'\,z)$$

Die Gleichung $z^2 = x^2 + y^2$ läszt sich also so schreiben

$$(px+qy-pz)\,(-q'x+p'y+p'z) = (-qx+py+pz)\,(p'x+q'y-q'z)$$

wo $p\ q\ p'\ q'$ ganz beliebige Grössen sind.

Wir gehen so zu einigen illustrirenden Beispielen unserer Methode über.

Auflösung der Gleichung

$$(a + b + c)\,(a + b - c)\,(a - b + c)\,(-a + b + c) = k^2$$

in ganzen Zahlen $a\,b\,c\,k$

$$p\,(a + b + c)\,(a + b - c) = qk$$
$$q\,(a - b + c)\,(-a + b + c) = pk$$

$$p^2\,(a + b + c)\,(a + b - c) = q^2\,(a - b + c)\,(-a + b + c)$$

Diese letzte Gleichung kann man ganz direct nach der Methode auflösen und also bekommt k auch einen ganzzahligen Werth.

Um unsere Gleichung gleich auf die Form (I) zu bringen braucht man nur $k = nm$ zu setzen. k ist das Doppelte des Areals eines Triangels, deren Seiten a, b und c sind. Mit Hülfe dieser Interpretation dei *unbestimmten* Gleichung können wir diese auf eine andere Weise lösen. Wegen der zwei Gleichungen

$$k = ab \sin C \qquad c^2 = a^2 + b^2 - 2\,ab \cos C$$

müssen nämlich die Sinus und die Cosinus der drei Winkel alle rational sein oder:

$$\sin C = \frac{2\,p\,q}{p^2 + q^2} \qquad \sin B = \frac{2\,x\,y}{x^2 + y^2} \quad .$$

$$c = p\,q\,(x^2 + y^2) \qquad b = x\,y\,(p^2 + q^2)$$

$$a = (qx + py)\,(xp - qy) \qquad k = 2^2 x\,y\,p\,q\,(xq + yp)\,(xp - yq)$$

Ein Beweis für die Unmöglichkeit der Fermat'schen Gleichung

$$A^6 + B^6 = C^6$$

Es wird gesucht die Formen der Zahlen a, b und c, die der Gleichung

$$a^3 + b^3 = c^2$$

Genüge leisten. a und b seien relative Primzalen und $b.a$ positiv oder negativ. Ist ferner vorausgesetzt, das c nicht durch 3 theilbar ist, bekommt man

$$a^2 - ab + b^2 > o$$
$$a + b > o$$

$$a + b = A^2$$
$$a^2 - ab + b^2 = B^2$$

Die letzte Gleichung giebt uns

$$ab = (B + a - b)\,(B - a + b)$$

$$pa = q\,(B + a - b)$$
$$qb = p\,(B - a + b)$$

$$\frac{a}{b} = \frac{q^2 - 2\,qp}{p^2 - 2\,qp}$$

Weil p und q relative Primzahlen sind, können $q^2 - 2\,qp$ und $p^2 - 2\,qp$ höchstens einen gemeinsamen Divisor 3 haben. In diesem Falle muss

$$p - 2\,q = 3r \qquad \text{und folglich}$$

$$\frac{q^2 - 2\,pq}{p^2 - 2\,qp} = \frac{-q\,(2\,r + q)}{r\,(3\,r + q)}$$

$$= \frac{(q + 2\,r)^2 - 2\,(q + 2\,r)\,r}{r^2 - 2\,(q + 2\,r)\,r} = \frac{q_1{}^2 - 2\,q_1\,p_1}{p_1{}^2 - 2\,q_1\,p_1}$$

Wir haben also:

$$a = \pm\,(q^2 - 2\,qp) \qquad b = \pm\,(p^2 - 2\,qp)$$

$$B = \mp\,(p^2 - pq + q^2)$$

Substituiren wir die Werthe von a und b in der Gleichung

$$a + b = A^2$$

so bekommt man $\quad p^2 + q^2 - 4\,pq = \pm\,A^2 \quad$ oder

$$(q - 2\,p)^2 - 3\,p^2 = \pm\,A^2$$

Hier kann man nicht das untere Zeichen benutzen. Sonst hätten wir nämlich:

$$3\,p^2 = A^2 + (q - 2\,p)^2$$

eine Gleichung die, wie man sofort sieht, unmöglich ist.

Wir haben also das obere Zeichen zu wählen und bekommen somit:

$$a = q^2 - 2\,qp \qquad b = p^2 - 2\,qp$$

$$(p - q)^2 - 2\,pq = A^2$$

$$2\,pq = (p - q + A)\,(p - q - A)$$

$$\alpha.\,2\,p = \beta\,(p - q + A)$$
$$\beta.\;\; q = \alpha\,(p - q - A)$$

$$\frac{p}{q} = \frac{\beta^2 + 2\alpha\beta}{2\alpha\beta - 2\alpha^2}$$

Da α und β relative Primzahlen sind, können $\beta^2 + 2\alpha\beta$ und $2\alpha\beta - 2\alpha^2$ keinen grösseren gemeinschaftlichen Divisor als 6 haben. Sind sie beide mit 3 theilbar, dann ist

$$\beta - \alpha = 3\gamma$$

und

$$\frac{\beta^2 + 2\alpha\beta}{2\alpha\beta - 2\alpha^2} = \frac{(\alpha+\gamma)(\alpha+3\gamma)}{2\alpha\gamma} = \frac{(\alpha+\gamma)^2 + 2\gamma(\alpha+\gamma)}{2\gamma(\alpha+\gamma) - 2\gamma^2} =$$

$$= \frac{\beta_1^2 + 2\alpha_1\beta_1}{2\alpha_1\beta_1 - 2\alpha_1^2}$$

Wir können folglich von diesem Falle absehen.

Sind $\beta^2 + 2\alpha\beta$ und $2\alpha\beta - 2\alpha^2$ beide mit 2 theilbar, so muss

$$\beta = -2\delta$$

und

$$\frac{\beta^2 + 2\alpha\beta}{2\alpha\beta - 2\alpha^2} = \frac{2\alpha\delta - 2\delta^2}{\alpha^2 + 2\alpha\delta} = \frac{2\alpha_1\beta_1 - 2\alpha_1^2}{\beta_1^2 + 2\alpha_1\beta_1}$$

Wir haben also entweder

$$p = \pm(\beta^2 + 2\alpha\beta) \qquad q = \pm(2\alpha\beta - 2\alpha^2)$$

wenn p und b nicht durch 2 theilbar sind, oder

$$p = \pm(2\alpha\beta - 2\alpha^2) \qquad q = \pm(\beta^2 + 2\alpha\beta)$$

wenn p und b durch 2 theilbar sind. Eine der Zahlen a und b muss folglich durch 2 theilbar sein.

Lasset uns der Einfachheit halber immer die gerade Zahl mit a bezeichnen, dann hat man, weil q mit 2 theilbar sein muss.

$$p = \pm(\beta^2 + 2\alpha\beta) \qquad q = \pm(2\alpha\beta - 2\alpha^2)$$

Ferner bekommt man durch Substitution der gefundenen Formen von q und p:

$$\begin{aligned} a &= 4\alpha(\alpha^3 - \beta^3) \\ b &= \beta(\beta^3 + [2\alpha]^3) \end{aligned} \qquad \text{(VI)}$$

wo also α und β positive oder negative relative Primzahlen sind

$$c = -(2\alpha^2 - \beta^2 + 2\alpha\beta)(4\alpha^4 - 4\alpha^3\beta + 6\alpha^2\beta^2 + 2\alpha\beta^3 + \beta^4)$$

Wir bemerken dass entweder

$$\alpha^3 - \beta^3 \quad \text{oder} \quad \beta^3 + (2\alpha)^3$$

mit 3 theilbar sein können.

Sonst wären namlich beide und also auch a und b mit 9 theilbar.

Durch die Gleichungen (VI) können wir nun beweisen, dass die unbestimmte Gleichung

$$P^6 + Q^3 = R^2$$

in ganzen Zahlen unmöglich ist, wenn R nicht durch 3 theilbar sein soll.

Wäre namlich diese Gleichung möglich, hatte man, weil P, Q und R als relative Primzahlen aufgefasst werden können,

$$n^2 = 4\alpha\,(\alpha^3 - \beta^3)$$

oder

$$m^2 = \beta\,(\beta^3 + (2\alpha)^3)$$

also

$$\alpha = k^2 \qquad \alpha^3 - \beta^3 = h^2$$

oder

$$\beta = k_1^2 \qquad \beta^3 + (2\alpha)^3 = h_1^2$$

In beiden Fällen bekam man folglich eine neue Gleichung

$$P_1^6 + Q_1^3 = R_1^2$$

mit denselben Eigenschaften wie die gegebene Gleichung aber mit kleineren Zahlen.

Durch Fortsetzung dieses Verfahrens würde man zuletzt eine Gleichung bekommen in welche eine der Zahlen gleich Null wäre. Aber dann müsste auch, wie man sofort sieht, eine der Zahlen P, Q, R gleich Null sein.

Aus diesem Satze leitet man die folgenden Corollare ab.

Die Gleichung

$$a^6 + b^6 = c^2$$

ist immer in ganzen Zahlen unauflösbar, gleichfalls die Gleichung

$$a^6 - b^6 = c^2$$

wenn c nicht durch 3 theilbar ist.

Setzen wir in den Gleichungen (VI)

$$\alpha = \mathrm{m}\sqrt[3]{\mathrm{A}} \qquad \beta = \mathrm{n}\sqrt[3]{\mathrm{B}}$$

$$a = \mathrm{x}\sqrt[3]{A} \qquad b = y\sqrt[3]{B}$$

so erhalten wir dadurch eine bekannte und sehr allgemeine Auflösung der Gleichung

$$A\,\mathrm{x}^3 + \mathrm{B}\,y^3 = z^2$$

in ganzen Zahlen x y z.

Es wird

$$\mathrm{x} = 4\,m\,(A\,\mathrm{m}^3 - B\,n^3)$$

$$y = n\,(B\,n^3 + A\,(2\,m)^3)$$

$$z = B^2\,n^6 - 20\,A\,B\,n^3\,m^3 - 8\,A^2\,m^6$$

Satz.

Ist $r - p$ nicht durch 3 theilbar und

$$B^2 = A\,C$$

dann lässt sich der Gleichung.

$$A\,p\,q^2 - 2\,B\,q\,r^2 + Crp^2 = 0$$

nicht in ganzen Zahlen befriedigen.

Man bekommt nämlich

$$r\,(B^2\,r^3 - A\,C\,p^3) = (A\,p\,q - B\,r^2)^2$$

$$r\,(r^3 - p^3) = U^2$$

oder wenn α der grösste gemeinschaftliche Divisor der Zahlen r und p ist

$$r = a r_1$$

$$p = a p_1$$

$$a r_1 \, (a^3 r_1{}^3 - a^3 p_1{}^3) = U^2$$

$$r_1 \, (r_1{}^3 - p_1{}^3) = U_1{}^2$$

$$r_1 = h^2 \qquad r_1{}^3 - p_1{}^3 = k^2$$

$$h^6 - p_1{}^3 = k^2$$