Ueber den Algorithmus der Erhöhung.

B. Delaunay.

Im Iahre 1915 gelang es mir die unbestimmte Gleichung $X^3q+Y^3=1$ vollständig zu lösen *). Das war überhaupt das erste Beispiel einer Lösung einer (nicht trivialen) binären kubischen Gleichung. Der entscheidende Umstand lag damals in der Bemerkung dass aus $\varepsilon_0^m = P\cdot\sqrt[3]{q}+Q$ und den conjugierten Gleichungen man $\varepsilon_0^m+\theta\cdot\varepsilon_0'^m+\psi\cdot\varepsilon_0''^m=0$ bekommt, wo $\theta=e^{\frac{2\pi i}{3}}=\zeta$; $\psi=e^{\frac{4\pi i}{3}}=\zeta^2$ sind. Wenn man sich also den Beweis verschafft dass m sich nicht durch 3 u 2 teilen lässt, so kann man die Einheitswurzeln ζ und ζ^2 unter die Exponenten m hineinführen und denn Schluss ziehen dass $\zeta\cdot\varepsilon_0'+\zeta^2\cdot\varepsilon_0''$ (oder $\zeta^2\cdot\varepsilon_0'+\zeta\cdot\varepsilon_0''$), als Teiler von ε_0^m, eine Einheit ist, woraus man eine neue nicht triviale Bedingung erhält. [Das einzige wichtige Resultat über die unbestimmten Gleichungen 3-ten Grades, welches nicht meinen in Abhandlungen von 1915 und 1922 schon enthaltan war, erhielt T. Nagell (1925) **) indem er diese meine Methode auf die etwas allgemeinere Gleichung $AX^3+BY^3=1$ anwandt und mit ihrer Hilfe die Lösung dieser Gleichung auf diejenige meiner Gleichung $X^3q+Y^3=1$ zurückführte]. Man sieht aber nicht wie man diese Methode für die Gleichungen, welche nicht mit dem reinen, sondern mit dem allgemeinen kubischen Körper verknüpft sind, verwenden könnte, weil in diesem Falle θ und ψ keine Einheitswurzeln sind. Darum habe ich noch seit 1916 eine zweite Methode verwendet (den Algorithmus der Erhöhung) welche mich im Iahre 1919 zum vollständigen Beweise meines Hauptsatzes über die Anzahl der Darstellungen der Zahlen durch binäre kubische Formen von negativen Discriminante führte ***).

Ich will hier einige weitere Untersuchungen (welche in den C. R. 1921 und 1924 skiziert wurden) über diese meine zweite Methode mitteilen.

---

*) Journal der Math Ges. zu Charkow. 1915, so wie Mem. der S. Petersb. Akad. d. Wiss. 1922.

**) Journal de Math pures et appliquées, 1925.

***) Memoiren der S. Petersb. Akad. d Wiss. 1922.

1. Ueber eine notwendige Bedingung für die Lösbarkeit der unbestimmten Gleichung $\Phi(x, y) = 1$. Sei $Ax^3 + Bx^2y + Cxy^2 + Ey^3 = (A, B, C, E) = \Phi(x, y)$ eine gegebene binäre kubische Form, und seien ω_1 nnd ω_2 die Wurzeln der Gleichungen $\omega_1^3 - B\omega_1^2 + AC\omega_1 - A^2E = 0$ und $\omega_2^3 - C\omega_1^2 + BE\omega_2 - AE^2 = 0$, wobei $\omega_1\omega_2 = AE$. Man kann leicht beweisen (s. dieses Journal S. 40) dass der Modul $[\omega_1\ \omega_2\ 1]$ ein Ring ist. Wir werden diesen Ring $O(\Phi)$ oder $O[\omega_1\ \omega_2\ 1]$ bezeichnen. Seine Discriminante ist der Discriminante von Φ gleich. Aequivalenten Formen entspricht ein und derselbe Ring. Wie man es leicht aus der Theorie der Idealen sieht, kann nicht jede Form Φ als Norm (in $\Omega(\Phi) = \Omega\omega_2$) einer Zahl von der Form $\lambda \cdot X + \mu \cdot Y$, wo λ und μ ganze Zahlen aus $\Omega(\Phi)$ sind, dargestellt werden. Wenn aber Φ die Zahl 1 darzustellen fähig ist, so ist sie einer „ganzen" Form $f(x, y)$, d. h. einer solchen, bei welcher $E = 1$ ist, äquivalent, z. B. $(A, B, C, E) = (q, -p, n, 1)\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$, und wenn ρ die Wurzel von $\rho^3 = n\rho^2 + p\rho + q$ ist, so bekommen wir $(A, B, C, E) = N_\Omega(\lambda \cdot X + \mu \cdot Y)$, wo $\lambda = \alpha\rho + \gamma$; $\mu = \beta\rho + \delta$, d. h. hat dann Φ eine solche „ganze" Zerlegung in seinem eigenen Ringe, da $O(\Phi) = O[\rho^2, \rho, 1]$ ist. Wenn Φ primitif ist, was wir voraussetzen wollen, so sind die Zahlen λ, μ relatif prim. Wir haben aber $\frac{\lambda}{\mu} = \frac{\omega_2}{E}$ und also bekommen wir $E = \mu j$; $\omega_2 = \lambda \cdot j$, wo j eine ganze algebraische Zahl aus $\Omega(\Phi)$ ist. Die Zahl $\alpha E - \beta \cdot \omega_2$ des Ringes $O(\Phi)$ ist $= (\alpha \cdot \mu - \beta \cdot \lambda)\ j = j$, weil $\alpha \cdot \mu - \beta \cdot \lambda = 1$ ist. Das Ideal (ω_2, E) des Ringes $O(\Phi)$ muss also ein Hauptideal dieses Ringes sein. Wenn die Form Φ gegeben ist, kann man durch bekannte Methoden entscheiden ob das Ideal (ω_2, E) ein Hauptideal ist, und im Fall wo dies ist, die zugehöhrige gahze algebraische Zahl j berechnen. Dann können nur $\lambda = \frac{\omega_2}{j}$ und $\mu = \frac{E}{j}$ sein, oder von diesen Zahlen beide durch einen und denselben Einheitsfactor verschieden sein. „Für die Möglichkeit der Lösung der Gleichung $\Phi(x, y) = 1$ ist also das Vorhandensein einer solchen Zerlegung von Φ in seinem eigenen Ringe notwendig".

Beispiele zeigen aber dass diese Bedingung noch nicht hinreichend ist.

2. Ueber zwei Kongruenzen welchen alle Lösungen P, Q von $\Phi(x, y) = 1$ genügen müssen, wenn Φ eine binäre kubische Form von negativen Discriminante ist. Setzen wir voraus dass diese Bedingung erfüllt ist, und sei $\lambda = r\omega_1 + s\omega_2 + t$; $\mu = u\omega_1 + v\omega_2 + w$. Wenn wir $\Phi(P, Q) = 1$ haben, so ist $\lambda \cdot P + \mu \cdot Q$ eine positive Einheit des Ringes $O(\Phi)$. Wenn die Form Φ von negativen Discriminante ist, so hat der Ring $O(\Phi)$ nur eine einzige unabhängige Fundamentaleinheit. Sei $\varepsilon_0 = a\omega_1 + b\omega_2 + c$ die direckte positive Fundamentaleinheit d. h. diejenige für welche $0 < \varepsilon_0 < 1$ ist.

Man kann die 9 Zahlen a, b, c; r, s. t; u, v, w aus den Zahlen A, B, C, E durch bekannte Methoden berechnen. Man hat also $\lambda \cdot P + \mu \ Q = \varepsilon_0^m$. Man kann annehmen dass $m > 0$ ist, weil, wie man es leicht aus Zahlengeometrischen Gründen sieht, Lösungen (P, Q) mit $m < 0$ bei gegebenen λ, μ nur mit solchen m vorkommen können welche absolut genommen eine gewisse angebbare (nicht grosse) Grenze h nicht übersteigen. Man kann sie z. B. sogar auch alle finden. Oder kann man anstatt λ und μ, $\lambda \cdot \varepsilon_0^{-h}$, $\mu \cdot \varepsilon_0^{-h}$ nehmen, und dann werden gewiss schon keine Lösungen mit $m < 0$ vorhanden sein. Wir haben also $\lambda \cdot P + \mu \cdot Q = (rP + uQ)\ \omega_1 + (sP + vQ)\ \omega_2 + (tP + wQ) = F\omega_1 + G\omega_2 + H = \varepsilon = \varepsilon_0^m = (a\omega_1 + b\omega_2 + c)^m$. Wenn wir diese Gleichung für die konjugierten Ringe schreiben und substragieren, erhalten wir $F\ (\omega_1' - \omega_1'') + G\ (\omega_2' - \omega_2'') = \varepsilon_0'^m - \varepsilon_0''^m = (\varepsilon_0' - \varepsilon_0'') \cdot (U\omega_1 + V\omega + W) = [a\ (\omega_1' - \omega_1'') + b\ (\omega_2' - \omega_2'')] \cdot (U\omega_1 + V\omega_2 + W)$ wo U, V, W auch ganze rationale Zahlen sind. Wir haben

$$\omega_1' - \omega_1'' = \frac{AE(\omega_2'' - \omega_2')}{\omega_2' \ \omega_2''} = \frac{AE\,\omega_2(\omega_2'' - \omega_2')}{AE^2} = -\frac{\omega_2}{E}\ (\omega_2' - \omega_2'').$$

Also bekommen wir, nach geeigneter Kürzung, $-F\omega_2 + EG = (-a\omega_2 + Eb) \cdot (U\omega_1 + V\omega_2 + W)$. Die Vergleichung der Koefficienten gibt 3 Gleichungen durch deren Lösung wir $\Delta U = a\ (bF - aG)$; $\Delta \cdot V = b\ (bF - aG)$; $\Delta \cdot W = b\ (aC - bE)\ G + a\ (aA - bB)\ F$ bekommen, wo $\Delta = a^3A - a^2bB + ab^2C - b^3E$ ist. Sei $\delta = (a, b)$ und $a = a_1\delta$; $b = b_1\delta$ und bezeichnen wir $\frac{\Delta}{\delta^3}$ durch $\varkappa$, dann hahen wir $\varkappa \cdot \delta \cdot U = a_1\ (b_1F - a_1G)$; $\varkappa\delta V = b_1\ (b_1F - a_1G)$; $\varkappa \cdot \delta \cdot W = b_1\ (a_1C - b_1E)\ G + a_1\ (a_1A - b_1B)\ F$. Aus den beiden ersten Gleichungen, da $(a_1, b_1) = 1$ ist, bekommen wir $b_1F - a_1G \equiv 0 \pmod{\varkappa\delta}$ oder

$$P \cdot K + Q \cdot L \equiv 0 \pmod{\varkappa\delta} \quad \ldots\ldots\ldots\ldots\ldots (1)$$

wo $K = \begin{vmatrix} a_1 & b_1 \\ r & s \end{vmatrix}$; $L = \begin{vmatrix} a_1 & b_1 \\ u & v \end{vmatrix}$ ist, und aus der dritten

$$P\ \mathrm{K} + Q \cdot \mathrm{L} \equiv 0 \pmod{\varkappa\delta} \quad \ldots\ldots\ldots\ldots\ldots (2)$$

wo $\mathrm{K} = \begin{vmatrix} Ca_1\ b_1 - Eb_1^2, & Ba_1\ b_1 - Aa_1^2 \\ r & s \end{vmatrix}$;

$$\mathrm{L} = \begin{vmatrix} Ca_1\ b_1 - Eb_1^2, & Ba_1\ b_1 - Aa_1^2 \\ u, & v \end{vmatrix}.$$

Diesen Kongruenzen (1) und (2) müssen alle Lösungen P, Q der Gleichung $\Phi(x, y) = 1$ genügen.

3. Ueber den Fall, in welchem die Kongruenzen (1) und (2) identisch erfüllt, sind. Sei λ, μ eine Zerlegung von Φ

n $O(\Phi)$, dann ist $\lambda_\kappa = \lambda \cdot \varepsilon_0^\kappa$; $\mu_\kappa = \mu \cdot \varepsilon_0^\kappa$ auch eine solche Zerlegung. Wenn wir die Zahlen K, L, K, L für diese Zerlegung durch K_κ, L_κ K_κ, L_κ bezeichnen, so berechnet man leicht dass $K_1 = K \cdot c + \delta \cdot K$, $L_1 = Lc + \delta L$ und $K_1 \equiv Kc + \delta K\varphi$; $L_1 \equiv L \cdot c + \delta \cdot L \cdot \varphi$ (mod. $\varkappa\delta$) ist, wo $\varphi = -ACa_1^2 + (AE + BC)\, a_1 b_1 - BEb_1^2$ ist. Wenn die Kongruenzen (1) und (2) identisch erfüllt sind, d. h. $K \equiv L \equiv K \equiv L \equiv o$ (mod. $\varkappa\delta$) ist, so sind also die Kongruenzen (1_κ) und (2_κ) auch identisch erfüllt. — Sei σ ein gemeinsamer Teiler von K und L, dann ist σ auch Teiler von $\begin{vmatrix} r & s \\ u & v \end{vmatrix}$, da a_1 und b_1 relativ prim sind. $\begin{vmatrix} r & s \\ u & v \end{vmatrix}$ ist der Index des Moduls $[\lambda, \mu, 1]$ in Bezug auf den Modul $[\omega_1, \omega_2, 1]$. Setzen wir voraus, dass die Gleichung $\Phi(x, y) = 1$ eine Lösung hat, dann ist $\lambda = (\alpha\rho + \gamma) \cdot \varepsilon$; $\mu = (\beta\rho + \delta) \cdot \varepsilon$, wo ε eine Einheit ist, und eine Einheit des Ringes $[\omega_1, \omega_2, 1] = [\rho^2, \rho, 1]$, weil man $\alpha \cdot \mu - \beta \cdot \lambda = \varepsilon$ hat. Es sei $\varepsilon = A\rho^2 + B\rho + \Gamma$, wir haben dann

$$\begin{vmatrix} r & s \\ u & v \end{vmatrix} = \begin{vmatrix} A\alpha n + B\alpha + A\gamma, \\ A\beta n + B\beta + A\delta, \end{vmatrix}$$

$$\begin{vmatrix} A\alpha p + \Gamma\alpha + B\gamma \\ A\beta p + \Gamma\beta + B\delta \end{vmatrix} = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \cdot \begin{vmatrix} An + B, & A \\ Ap + \Gamma, & B \end{vmatrix} = ABn + B^2 - A^2p - A\Gamma = A',$$

wo A' der Koefficient von ρ_1^2 bei $\eta = \varepsilon^{-1}$ ist. Jeden g. g. Teiler von K und L ist also Teiler von diesem A'. Wenn $K \equiv L \equiv o$ (mod $\varkappa\delta$) und σ das Produkt aller verschiedenen Primzahlen ist, welche in $\varkappa$ aufgehen, dann muss A' durch $\sigma \cdot \delta$ teilbar sein. Die Zahl $N[A'(n - \rho) + B']$ ist der Index von η in Bezug auf $O(\rho)$ und, da η eine Potenz von ε_0^{-1} ist, muss sie sich durch den Index $\varkappa\delta^3$ von ε_0 in Bezug auf $O(\rho)$ teilen. Man sieht aber leicht, dass A' und B' δ als gemeinsamen Teiler haben müssen, d. h. $A' = A'_1 \cdot \delta$; $B' = B_1' \cdot \delta$, und also muss $N[A_1'(n - \rho) + B_1']$ sich durch $\varkappa$ teilen. Da aber $A_1' \equiv o$ (mod. $\varkappa$) ist, so muss $B_1'^3 \equiv o$ (mod. $\varkappa$) sein, d. h. $B_1' \equiv o$ (mod σ) sein. Wenn also die Kongruenz (1) identisch erfüllt ist, so ist σ Teiler von A_1' und B'_1. Wenn wir jetzt zu den Kongruenzen (1_1) (2_1) übergehen, so müssen sie sich nach der obengemachten Bemerkung, wenn (1) und (2) sich identisch erfüllen, auch identisch sein. Wenn wir also $\varepsilon \cdot \varepsilon_0 = A''\rho^2 + B''\rho + \Gamma''$ und $\varepsilon_0 = \bar{a}\rho^2 + \bar{b}\rho + \bar{c}$ setzen, so müssen auch A_1'' und B_1'' sich durch σ teilen. Wenn wir aber A_1'', B_1'' durch A', B', Γ' und $\bar{a}$, $\bar{b}$, $\bar{c}$ ausdrücken, so erhalten wir dass $\bar{a}\Gamma'$ und $\bar{b}\Gamma'$ sich durch σ teilen müssen, wenn man $\bar{a} = \bar{a_1}\ \delta$; $\bar{b} = \bar{b_1} \cdot \delta$ setzt, da aber $(\bar{a_1}\ \bar{b_1}) = 1$ ist (da, wie man es leicht sieht der g. g. Teiler von $\bar{a}$ und $\bar{b}$ ist derselbe wie derjenige von a und b, also δ) und Γ nicht durch σ teilbar sein kann, wenn $\sigma > 1$ ist, so muss $\sigma = 1$ sein. Daraus schliessen wir dass $\varkappa = \pm 1$ ist. Die Zahl $\bar{\rho} = a_1\omega_1 + b_1\omega_2$ in $O(\Phi)$ hat demnach in Bezug auf $O(\Phi)$ den Index ± 1, und also ist die Form $(\bar{q}, -\bar{p}, \bar{n}, 1)$, welche die Wurzel $\bar{\rho}$ hat, eine ganze der Form Φ äquivalente Form. Es ist so

eine Lösung der Gleichung $\Phi = 1$ gefunden. Wir werden aber gleich zeigen dass es deren ja auch zwei gefunden werden können.

In der Tat, aus $K \equiv L \equiv K \equiv L \equiv 0 \pmod{\varkappa\delta}$ bekommen wir leicht dass $r \equiv s \equiv u \equiv v \equiv 0 \pmod{\varkappa\delta}$ ist; z. B. $K \cdot (Ba_1b_1 - Aa_1^2) - Kb_1 = (-Aa_1^3 + Ba_1^2b_1 - Ca_1b_1^2 + Eb_1^3) \cdot s = -\varkappa \cdot s$. Es muss also $A' = \begin{vmatrix} r & s \\ u & v \end{vmatrix} \equiv 0 \pmod{\delta^2}$ sein. Die Einheit η und also auch ε liegt demnach im Ringe $O(\delta\rho)$. Es sei $\varepsilon = \varepsilon_0^{\tau}$, d. h. $(\overline{a} \cdot \delta\rho^2 + \overline{b_1}\delta\rho + \overline{c})^{\tau} = A_1\delta^2\rho^2 + B_1\delta\rho + \Gamma$. Durch die vergleichung der Koefficienten von ρ^2 bekommen wir daraus dass $\tau \cdot \overline{a_1}\ \delta\overline{c}^{\tau-1} \equiv 0 \pmod{\delta^2}$ ist. Da aber $(\overline{c}, \delta) = 1$ ist und $(\tau, \delta) = 1$ vorausgesetzt werden kann (da man anderfals von λ; μ zu $\lambda \cdot \varepsilon_0^{\kappa}$; $\mu \cdot \varepsilon_0^{\kappa}$ übergehen kann, so dass man anstatt τ, $\tau - k$ hat, und dabei k so wählt, dass $(\tau - k, \delta) = 1$ ist). So hat man $\overline{a_1} \equiv 0 \pmod{\delta}$. Die Einheit ε_0 selbst liegt also in dem Ringe $O(\delta\rho)$. Der Index von ε_0 in Bezug auf $O(\rho)$ ist gleich $\pm\delta^3$, da $\varkappa = \pm 1$ ist. Es ist also ε_0 eine Einheit im Ringe $O(\delta\rho)$ welche in Bezung auf diesen Ring den Index ± 1 hat. Die dem Ringe $O(\delta\rho)$ gehörige Form $(\delta^3 q, -\delta^2 p, \delta n, 1)$ ist also einer „reversiebelen" Form $(1, -p', n', 1)$ äquivalent. Die Gleichung $(\delta^3 q, -\delta^2 p, \delta n, 1) = 1$ hat also wenigstens 2 Lösungen $(0,1)$ und $(\delta X_1, Y_1)$ und folglich hat auch die Gleichung $(A, B, C, E) = 1$ 2 Lösungen, weil $(A, B, C, E) \sim (q, -\rho, n, 1)$ ist. Wir haben das Theorem: „Wenn die beiden Kongruenzen (1) und (2) identisch erfüllt sind und $\varkappa \neq \pm 1$ ist, hat die Gleichung $\Phi(x, y) = 1$ keine Lösungen, wenn aber $\varkappa = \pm 1$ ist, so hat sie zwei Lösungen, welche man auch berechnen kann".

4. Algorithmus der Erhöhung. Seien die Kongruenzen (1) und (2) nicht beide identisch erfüllt. Sei z. B. (1) nicht identisch. Wenn man dann durch d den g. g. Teiler von K, L und $\varkappa\delta$ bezeichnet und wenn $K = dK'$: $L = dL'$; $\varkappa\delta = d\varkappa'$ ist, so wird $PK' + QL' \equiv 0 \pmod{\varkappa'}$. Wenn jetzt weiter $(K', L') = d'$ und $K' = K'' \cdot d'$; $L = L''\ d'$ ist, so haben wir $(d', \varkappa') = 1$ und also $P \cdot K'' + Q \cdot L'' \equiv 0 \pmod{\varkappa'}$ wo schon $(K'', L'') = 1$ ist. Wenn wir von der Form (A, B, C, E) zu der Form (A', B', C', E') durch die Substitution $\begin{pmatrix} \alpha, & -L'' \\ \gamma, & K'' \end{pmatrix}$ übergehen, wo $\alpha \cdot K'' + \gamma \cdot L'' = 1$ ist, so bekommen wir $A'P'^3 + B'P'^2Q' + C'P'Q'^2 + E'Q'^3 = 1$, wo $P' \equiv 0 \pmod{\varkappa'}$ ist, weil $P' = P \cdot K'' + Q\ L''$ ist. Setzen wir $P' = \overline{P}\varkappa'$ und $\overline{A} = A'\varkappa'^3$; $B = B'\varkappa'^2$; $\overline{C} = C' \cdot \varkappa'$; $\overline{E} = E$, so bekommen wir die Gleichung $(\overline{A}, \overline{B}, \overline{C}, \overline{E}) = 1$ auf deren Lösung die Lösung der gegebehen Gleichung $(A, B, C, E) = 1$ reduciert ist. Die Form $(\overline{A}, \overline{B}, \overline{G}, \overline{E})$ hat aber eine $\varkappa'^6$ mal grössere Discriminante als die gegebene Form (A, B, C, E), und $\varkappa'$ ist $\neq \pm 1$ weil wir vorausgesetzt haben dass (1) nicht identisch ist. Von der Form $(\overline{A}, \overline{B}, \overline{C}, \overline{E})$ schreiten wir in derselben Weise zu einer Form $(\overline{\overline{A}}, \overline{\overline{B}}, \overline{\overline{C}}, \overline{\overline{E}})$ u. s. w. Dieses Verfahren kann nur dann abbrechen, wenn auf einem der Schritte entweder die zugehöhrige Form keine Zerlegung in

seinem eigenen Ringe hat, und dan hat die Gleichung $\Phi(x, y) = 1$, keine Lösungen, oder die Kongruenzen (1) und (2) identisch werden, und dann hat die Gleichung $\Phi(x, y) = 1$, wie wir gezeigt haben, entweder keine, oder 2 Lösungen, welche man dabei auf diesem Schritte auch finden kann.

5. Erster Fall, wenn die Gleichung $\Phi(x, y) = 1$ eine und nur eine Lösung hat. In deisem Falle, welcher sehr oft vorkommt, wird nach § 3 dieser Algorithmus gewiss *nicht endigen*. Die nähere Untersuchung dieses sehr merkwürdigen Umstandes behalten wir uns auf ein anderes Mal vor.

6. Zweiter Fall, wenn die Gleichung $\Phi(x, y) = 1$ wenigstens 2 Lösungen hat. In diesem Falle wird gewiss auf einem Schritte des Algorithmus der Erhöhung der Umstand auftreten das die Kongruenzen (1) und (2) identisch befriedigt werden. Das sieht man leicht aus Zahlengeometrischen Gründen welche wir im nähsten § auseinandersetzen wollen.

7. Das Annähern an die Lösungen mittels des Algorithmus der Erhöhung. Wenn man das quadratische Gitter (x, y), wo (x, y) alle Punkte der Ebene, welche in einem zu Grunde gelegtem rechtwinkeligen Koordinatensystem ganzzahlige Koordinaten x und y haben, betrachtet, so bilden alle Punkte (P, Q) deren ganzzahlige Koordinaten die Kongruenzen $K'' \cdot P + L'' \; Q \equiv 0 \pmod{\varkappa'}$ erfüllen, oder der unbestimmten Gleichung $K'' \cdot P + L'' \; Q = \varkappa' \cdot t$, wo t eine beliebige veränderliche ganze rationale Zahl ist, genügen, ein parallelogrammatisches Teilsystem in diesem Gitter. Iede weitere Erhöhung durch unseren Algorithmus führt immer zu einem neuen Teilsysteme welches wenigstens einen 2 Mal grösseren Inhalt seines Grundparallelogrammes hat und immer den Punkt (0,0) enthält. Wenn eine Lösung (P_1, Q_1) vorhanden ist, so reduciert sich die ganze Sache zur Wegschaffung von Punktreihen, welche der Punktreihe (0,0) (P_1, Q_1) parallel sind. Das kann ohne Ende gehen, wie es im Falle wo es nur eine Lösung gibt, ja auch, wie wir es gezeigt haben, tatsächlich auftritt. Wen es aber zwei Lösungen gibt, (P_1, Q_1) und (P_2, Q_2), so kann der Inhalt des Grundparallelogramms den Inhalt des Parallelogramms (0,0) (P_1, Q_1) (P_2, Q_2) nicht übersteigen, weil dieses Parallelogramm in allen Teilsystemen vorkommen muss, und also muss der Algorithmus endigen. Wenn vir in jedem Teilsystem das Minimum, d. h. den Punkt $(x_0\ y_0)$, welcher der nächste zum (0,0) ist, bestimmen, so wird gewiss die kleinste Lösung (P, Q) der Gleichung $\Phi(x, y) = 1$ sich in der Reihe dieser aufeinanderfolgenden Minima finden. So kann man die Lösung auch im Falle des § 5, wenn der Algorithmus unendlich ist, aufsuchen.

8. Die Berechnung der Zahlen λ, μ für die erhöhten Formen. Seien λ und μ für die gegebene Form $\Phi(x, y)$ schon berechnet, wie dies in dem § 1 angedeutet wurde, also wie die Zahl ϑ_0. Wenn wir nach § 4 von Φ zu der Form Φ' durch die Substitution $\begin{pmatrix} \alpha & -L'' \\ \gamma & K'' \end{pmatrix}$ übergehen, so sind $\lambda' = \alpha\lambda + \gamma\mu$; $\mu' = \mu K'' - \lambda L''$. Setzen wir voraus das dies schon geschehen ist, d. h. $\lambda' = \lambda$; $\mu' = \mu$. Dann ist

$(A, B, C, E) = N(\lambda, \mu)$; $(\overline{A}, \overline{B}, \overline{C}, \overline{E}) = N(\varkappa'\lambda, \mu) = (A\varkappa'^3, B\varkappa'^2, C\varkappa', E)$, die Basis dieser erhöhter Form ist $\omega_1 = \varkappa'^2\omega_1$; $\omega_2 = \varkappa'\omega_2 \cdot \varkappa' \cdot \lambda$ und μ ist eine Zerlegung von Φ in $O(\Phi)$, sie muss aber eine Zerlegung $\overline{\lambda}$, $\overline{\mu}$ in seinem eigenen Ringe $O(\Phi)$ haben, dann muss aber $\overline{\lambda} = \varkappa' \cdot \lambda\ \varepsilon_0^{\tau}$; $\overline{\mu} = \mu\ \varepsilon_0^{\tau}$ sein, wo τ ein ganzer positiver Exponent $< \nu$ ist, wenn ε_0^{ν} die erste Potenz ist welche in $O(\Phi)$ liegt.

9. Kriterium des Aufenthaltes. Es kann sein dass die Gleichung $\Phi(x, y) = 1$ gar keine Lösungen hat, man soll einen Umstand finden welcher auf einem oder anderen Schritte des Algorithmus der Erhöhung die Unnützlichkeit weiterer Rechnungen ins Licht setze. Wenn wir einen solches zuverlässiges Kriterium hätten, dessen Auftreten auf einem von Forn herein von oben begrenztem Schritte auftreten sollte, wäre das ganze Problem gelöst. Einen solches haben wir bis jetzt nicht gefunden. Wir können aber die folgenden zwei Kriterien anzeigen. Erstens kann es geschehen dass eine erhöhte Form keine Zerlegung in seinem eigenen Ringe hat, was man nach der Methode des § 8 immer beurteilen kann. Zweitens kann es geschehen dass die Kongruenzen (1) und (2) unvereinbar sind, was, wie man leicht sieht, dann und nur dann auftritt, wenn $\begin{vmatrix} r & s \\ u & v \end{vmatrix}$ nicht durch δ teilbar ist.

10. Zwei Beispiele. Sei die Form (2,0, 3,2), $D = -648$ gegeben; $\omega_1^3 + 6\omega_1 - 8 = 0$; $\omega_2^3 - 3\omega_2 - 8 = 0$, $\omega_1 - 1 = \varepsilon$ ist eine Einheit, die Zahlen λ und μ des Ringes O (2,0 3,2) müssen die Norm 2 haben; wenn man aber die bekannten Methoden benutzt, berechnet man leicht, dass im Ringe O (2,0, 3,2) es keine Zahlen mit der Norm 2 gibt. Die Form (2,0, 3,2) hat also keine Zerlegung in seinem eigenen Ringe. Hier tritt also der Fall des ersten Kriterium des Aufenthalts. Die Gleichung $(2,0\ 3,2) = 1$ hat also keine Lösungen. — Sei jetzt die Form (3,3, 4,2), $D = -516$ gegeben; $\omega_1^3 - 3\omega_1^2 + 12\omega_1 - 18 = 0$; $\omega_2^3 - 4\omega_2^2 + 6\omega_2 - 12 = 0$; wir berechnen die Zahlen λ und μ, sie sind $\lambda = -3 + \omega_2$; $\mu = 2 - \omega_1$; die Fundamentaleinheit des Ringes O (3,3, 4,2) ist $\varepsilon_0 = 23 - 7\omega_2$; $\delta = 7$; $\begin{vmatrix} r & s \\ u & v \end{vmatrix} = 1$ und ist durch 7 nicht teilbar, die Kongruenzen (1) und (2) sind also unvereinbar. Hier tritt also der Fall des zweiten Kriteriums des Aufenthaltes. Die Gleichung $(3,3\ 4,2) = 1$ hat also keine Lösungen. [Das ist u. a. die Form mit der kleinsten Discriminante welche die Zahl 1 aus nicht trivialen Gründen nicht darstellen kann].

11. Algorithmus der Erhöhung im Falle einer ganzen Form. Wenn die Form Φ „ganz" ist, z. B. $(q, -p, n, 1)$, so bekommen wir $K = a_1$; $L = 0$; $K = a_1b_1n - b_1^2$; $L = 0$ und also, da $(a_1, b_1) = 1$ ist, reducieren sich die beiden Kongruenzen (1) und (2) zu der einzigen $P \equiv 0 \pmod{\varkappa\delta}$, und wir bekommen so denjenigen Algorithmus der Erhöhung, welchen wir in unseren Abhandlung (1920 in C. R.) in den Memoiren der S.-Petersburger Akademie der Wissenschaften zum Beweise unseres Hauptsatzes, dass $(A, B, C, E) = 1$ nicht mehr als 5 Lösungen haben kann, benutzten.

12. Kriterium des Aufenthalts im Falle einer ganzen Form. In diesem Falle können niemals die Kriterien des § 9 auftreten, man kann aber ein anderes Kriterium angeben (sein analoges gibt es auch für allgemeine Formen). Wenn $\rho^3 = n\rho^2 + p\rho + q$ ist und $\varepsilon_0 = a\rho^2 + b\rho + c$, so kommt die Auflösung von $(q, -\rho, n, 1) = 1$ auf die Auffindung aller Potenzen $(a\rho^2 + b\rho + c)^m$ welche von der Form $P\rho + Q$, d. h. „binom" sind. Wenn a und b resp. durch k^2 und k teilbar sind, dann kann man anstatt ρ, $k\rho$ nehmen. Eine Einheit, bei welcher es keine solche Zahl $k > 1$ existiert, werden wir deshalb „reduciert" nennen. Keine Potenz von ε_0 kann binom sein, wenn ε_0 reduciert ist und wenn es eine ungerade Primzahl π existiert durch welche sich a und b teilen. In der Tat es se $a = a_1\pi$; $b = b_1\pi$, aber $a_1 \not\equiv 0 \pmod{\pi}$, dann ist der Koefficient von ρ^2 in ε_0^m gleich

$$m \cdot c^{m-1} \cdot \pi \cdot a_1 + \frac{m(m-1)}{1 \cdot 2} c^{m-2} \cdot \pi^2 \cdot A_2 +$$

$$+ \frac{m(m-1)(m-2)}{1 \cdot 2 \cdot 3} c^{m-3} \pi^3 A_3 + \ldots$$

wo A_2, A_3 ... ganze rationale Zahlen sind. Dieser Koefficient kann nicht gleich o sein weil $(a_1, \pi) = 1$ und $(c, \pi) = 1$ ist, und also, wenn m genau durch π^τ teilbar ist, so haben wir (wenn $\pi > 2$ ist) $\pi^2 > 3$, $\pi^3 > 4$ u. s. w.—Wir werden jeden gemeinsamen Teiler von a und b „Teiler" der Einheit ε_0 nennen.—Sei ε^μ die niedrigste Potenz der Fundamentaleinheit ε_0 welche den Teiler π besitzt. Es können dann zwei Fälle eintreten: entweder wird der Koefficient von ρ^2 in ε_0^μ nur durch π teilbar, oder wenigstens durch π^2. Im ersten Falle werden wir π von „erster" Art und im zweiten Falle von „zweiter" Art in bezug auf ε_0 nennen. Es ist anderseits leicht zu sehen dass, wenn ε_0^m den Teiler π hat, so ist, ε_0^m eine Potenz von ε_0^μ. Wenn wir also auf einem (nicht durchaus auf dem ersten) Schritte des Algorithmus der Erhöhung einen erhöhenden Multiplicator π begegnen, welcher eine Primzahl der Ersten Art in Bezug auf die anfängliche Fundamentaleinheit ist, so gibt es keine Lösungen und man kann die Rechnung aufheben. In allen Fällen wo wir diese Methode anwandten stiessen wir auf einen erthöhenden Multiplicator der ersten Art im allgemeinen auf dem ersten oder zweiten Schritte, und immer hat uns diese Methode die vollständige Lösung der Gleichung gegeben. Wir haben aber bis jetzt keinen Beweis gefunden dass es ind er Tat auf einem oder änderem Schritte des Algorithmus der Erhöhung, wenn es keine Lösungen sind, eine Primzahl der ersten Art begegnet wird.

Da es für ziemlich grosse π die Potenz ε_0^μ modulo π^2 zu berechnen sehr umständlich ist, so haben wir uns der folgenden zwei Determinanten, welche diese Rechnung erleichtern, bedient. Wir geben hier diese

Determinanten der Kürze wegen ohne Beweis. Wir werden varaussetzen dass π nicht ein Teiler der Discriminante von ρ ist. Dann kann die Primzahl π in $\Omega\rho$ nur entweder ein Produkt von 3 Primidealen $p_1p_2p_3$ des ersten Grades, oder eines Ideals des 2-ten q und eines des ersten Grades p sein, sie kann aber nich selbst Primideal sein da sie ein Teiler der Norm von $-a\rho+b+an$ ist.

Die notwendige und hinreichende Bedingung dass π von der zweiten. Art sei ist, im Falle $\pi=p_1p_2p_3$, $\triangle\equiv 0 \pmod{\pi}$ und im Falle $\pi=pq$ $\nabla\equiv 0 \pmod{\pi}$, wo

$$\triangle=\begin{vmatrix} \sigma_1+\dfrac{\psi(x_1)\ (2ax_1+b)}{\varepsilon_1\cdot f'(x_1)}, & x_1, & 1 \\ \sigma_2+\dfrac{\psi(x_2)\ (2ax_2+b)}{\varepsilon_2\cdot f'(x_2)}, & x_2, & 1 \\ \sigma_3+\dfrac{\psi(x_3)\ (2ax_3+b)}{\varepsilon_3\quad f'(x_3)}, & x_3, & 1 \end{vmatrix}.$$

hier ist $f(x)=x^3-nx^2-px-q=(x-x_1)\ (x-x_2)\ (x-x_3)+$ $+\pi\cdot\psi(x)$; $\sigma_i=\dfrac{\varepsilon_i^{\pi-1}-1}{\pi}$; $\varepsilon_i=ax_i^2+bx_i+c$ (wo $x_i=x_1, x_2, x_3$); $f'(x)=3\ x^2-2nx-p$

$$\nabla=\begin{vmatrix} \dfrac{\varepsilon_1^{\pi-1}-1}{\pi}+\dfrac{\psi(x_1)\ (2ax_1+b)}{\varepsilon_1\quad f'(x_1)}, & x_1, & 1 \\ \dfrac{(A-B\theta)^{\pi+1}-\nu}{\nu\pi}+\dfrac{\psi(\beta')\ (2a\beta'+b)}{(A+B\theta)\quad f'(\beta')}, & \beta', & 1 \\ \dfrac{(A+B\theta)^{\pi+1}-\nu}{\nu\pi}+\dfrac{\psi(\beta'')\ (2a\beta''+b)}{(A-B\theta)\quad f'(\beta'')}, & \beta'', & 1 \end{vmatrix}$$

wo $f(x)=(x-x_1)(x^2+hx+k)+\pi\quad\psi(x)$; wo $-\pi<h<\pi$; $h=2h_1$ ist; $\theta=\sqrt{h_1^2-k}$; $\beta'=-h_1+\theta$; $\beta''=-h_1-\theta$; $a\beta'^2+b\,\beta'+c=$ $=A+B\theta$; $\nu=A^2-B^2(h_1^2-k)$; $\varepsilon_1=ax_1^2+bx_1+c$; $f'(x)=3x^2-$ $-2nx-p$.

13. Beispiel. $(2, 6, 3, 1)=1$; $D=-216$ (Ueber diese specielle Gleichung, welche mit $U^3-V^2=-2$ verknüpft ist findet man eine ganze kleine Literatur, die erste Auflösung erfolgte 1926 durch A. Brauer, s. Math. Zeitschr. 25 B. 3H. S. 499, welcher zeigte dass im Falle wenn in der Gleichung $U^3-V^2=-k$, $k=2$ ist, kann man sie durch eine specielle Methode auflösen. Ich habe aber durch den Algorithmus der Erhöhung unter anderem alle Gleichungen $(A, B, C, E)=1$, deren Discriminanten absolut genommen kleiner als 301 sind, noch im Iahre 1920 vollständig gelöst; also auch diese Gleichung). Man hat $(2, 6, 3, 1)\sim(2, 3, 0, 1)$; $\rho^3=-3\rho+2$; $\varepsilon_0=-\rho^2-\rho+1$; $-a\rho+b+an=\rho-1$, d. h. $\varkappa=2$, $\delta=1$, also der erste Erhöherungs-

multiplicator ist $\pi = 2$. Man muss in den Ring $O(\rho)$ wo $\rho = 2\rho$ ist übergehen. Wir erhalten $\varepsilon_0^2 = -\rho^2 - 3\rho + 5$; $-a\rho + b + an = \rho - 3$, und also der zweite Multiplicator ist $\pi = 47$. Da 47 ziemlich gross ist werden wir uns der augeführten Detirminanten bedienen. $47 = pq$ in $\Omega\rho$, wir müssen alsso ∇ berechnen. $x^3 + 3x - 2 = (x - 25)(x^2 - 22x + 111) + 47(x^2 - 14x + 59)$, d. h. $x_1 = 25$; $\varepsilon_1 = 649$; $\sigma = \frac{649^{46} - 1}{47} \equiv 34 \pmod{47}$; $\beta' = 11 + \theta$, wo $\theta = \sqrt{10}$; $A + B\theta = -141 - 23\theta$, $\nu = 872 \pmod{47^2}$; die Zahl $872^{-1} \cdot 47^{-1} \cdot [(-141 + 23\theta)^{48} - 872] \equiv 10\theta - 2 \pmod{47}$. Wir bekommen also $\nabla \equiv 18\theta \pmod{47}$. Die Primzahl 47 ist also in Bezug auf $\varepsilon_0 = -\rho^2 - \rho + 1$ von der ersten Art, und also hat die Gleichung $(2, 6, 3, 1) = 1$ keine Lösungen. (Diese Gleichung bildet zufälligerweise das schwierigste Beispiel zwischen allen in denen $|D| \leqq 300$ ist. In fast allen anderen Fällen hat man keine Notvendigkeit sich der Δ oder ∇ zu bedienen.

Ich bin bis jetzt keiner einzigen Gleichung von der Form $AX^3 + BX^2Y + CXY^2 + EY^3 = 1$ (mit $D < 0$) begegnet welche durch die Methode der §§ 9 und 12 ich allgemein nicht Lösen konnte. Und dennoch habe ich keinen Beweis dessen dass diese Methode in allen Fällen hinreichend ist.

Tabelle aller Lösungen aller Gleichungen $(A, B, C, E) = 1$ mit $0 > -D \leqq 300$.

$D(A, B, C, E)$	(X, Y).				
23	(1,0,−1,1)	(0,1)(1,0)(1,1)(−1,1)(4,−3)	199	(1,4,1,1)	(0,1) (1,0)
31	(1,1,0,1)	(0,1) (1,0) (−1,1) (3,−2)	200	(4,3,2,1)	(0,1)
44	(1,1,−1,1)	(0,1)(1,0)(2,−1)(−103,56)	204	(3,1,1,1)	(0,1)
59	(1,2,0,1)	(0,1((1,0) (−2.1)	211	(1,10,6,1)	(0,1) (1,0)
76	(1,3,1,1)	(0,1) (1,0) (−36,13)	212	(2,4,1,1)	(0,1) (2,−1)
83	(1,2,−2,1)	(0,1) (1,0)	216	(2,3,0,1)	(0,1)
87	(1,2,−1,1)	(0,1) (1,0)	231	(1,5,−4,1)	(0,1) (1,0)
104	(2,−1,0,1,)	(0,1) (2,−3)	236	(1,−1,2,1)	(0,1)
107	(1,4,2,1)	(0,1) (1,0) (−7,2)	239	(3,−1,0,1)	(0,1) (3,−5)
108	(2,0,0,1)	(0,1) (1,−1)	243	(1,12,−1,1)	(0,1) (1,0)
116	(2,0,1,1)	(0,1)	244	(2,4,5,1)	(0,1)
135	(1,3,0,1)	(0,1) (1,0) (−3,1)	247	(1,4,−3,1)	(0,1) (1,0)
139	(1,6,4,1)	(0,1) (1,0)	255	(1,8,5,1)	(0,1) (1,0)
140	(1,5,3,1)	(0,1) (1,0)	268	(1,13,7,1)	(0,1) (1,0)
152	(2,−2,1,1)	(0,1)	279	(1,5,2,1)	(0,1) (1,0)
172	(2,0,2,1)	(0,1)	283	(1,4,0,1)	(0,1) (1,0) (−4,1)
175	(1,3,−2,1)	(0,1) (1,0)	300	(2,2,4,1)	(0,1)
176	(1,3,−1,1)	(0,1) (1,0)			

Об алгорифме повышения.

Б. Н. Делоне.

В настоящей статье автор излагает в весьма краткой форме свои дальнейшие исследования, относящиеся к выяснению того способа перехода от заданного неопределенного уравнения к другим со все большим и большим дискриминантом, который в мемуаре 1922 года, в Трудах Российской Академии Наук, дал автору возможность найти основную теорему о числе решений неопределенного уравнения $AX^3+BX^2Y+CXY+EY^3=1$, где (A, B, C, E) кубическая двойничная форма отрицательного определителя.
