Mathematische Mittheilungen

von

A. Meyer.

I. Ueber die Kriterien für die Auflösbarkeit der Gleichung $ax^2+by^2+cz^2+du^2=0$ *in ganzen Zahlen.*

1. Bekanntlich hat Legendre zuerst die Kriterien aufgestellt für die Auflösbarkeit der Gleichung

$$ax^2+by^2+cz^2=0$$

in ganzen oder, was auf dasselbe hinauskommt, rationalen Zahlen x, y, z, welche nicht sämmtlich Null sind. Für die Gleichung

$$ax^2+by^2+cz^2+du^2=0 \tag{1}$$

ist meines Wissens diese Frage noch nicht beantwortet. Die folgenden Bemerkungen sollen zur Lösung derselben beitragen.

Die Coefficienten a, b, c, d werden als ganz und von Null verschieden vorausgesetzt. Ferner darf man annehmen, dass sie keine quadratischen Factoren enthalten und dass je drei derselben keinen gemeinschaftlichen Theiler haben; denn in diese Form lässt sich die Gleichung (1) immer bringen. Ausserdem darf und soll vorausgesetzt werden, x, y, z, u seien ganze Zahlen ohne gemeinschaftlichen Theiler.

2. Ist nun p ein gemeinschaftlicher Primfactor von a und b, so sind c und d durch p nicht theilbar und aus (1) folgt die Congruenz

$$cz^2 + du^2 \equiv 0 \pmod{p},$$

so dass entweder $-cd\,R\,p$ sein muss (in der Bezeichnungsweise von Gauss, Disq. ar., Art. 131) oder, wenn $-cd\,N\,p$, z und u beide durch p theilbar. Im letztern Falle sei

$$a = a'p,\ b = b'p,\ z = z'p,\ u = u'p,$$

so dass (1) übergeht in

$$a'x^2 + b'y^2 + cpz'^2 + dpu'^2 = 0, \tag{2}$$

wo x, y durch p nicht theilbar sind, also $-a'b'\,R\,p$ sein muss. Je nachdem daher $-cd\,R\,p$ oder $N\,p$ ist, behalte man die Gleichung (1) bei oder ersetze sie durch (2). Ebenso verfahre man successive mit jeder Primzahl, welche in zweien der Coefficienten a, b, c, d aufgeht. Dabei ändert sich das Product von zwei Coefficienten entweder gar nicht oder doch nur um einen quadratischen Factor, so dass seine quadratischen Charaktere in Bezug auf die schon betrachteten Primfactoren unverändert bleiben (wäre ein bereits verschobener Primfactor nochmals zu verschieben, so wäre die Gleichung unauflösbar).

3. Ich nehme an, die Gleichung (1) sei bereits in der angegebenen Weise präparirt. Den grössten gemeinschaftlichen (positiven) Theiler zweier Zahlen a und b bezeichne ich im Folgenden mit (a, b) und setze

$$a = (a,b)\,(a,c)\,(a,d)\,\alpha,\quad b = (b,a)\,(b,c)\,(b,d)\,\beta,\quad c = (c,a)\,(c,b)\,(c,d)\,\gamma,$$
$$d = (d,a)\,(d,b)\,(d,c)\,\delta.$$

Dann sind die Zahlen

$$(a,b),\ (a,c),\ (a,d),\ (b,c),\ (b,d),\ (c,d),\ \alpha,\ \beta,\ \gamma,\ \delta$$

relativ prim und die vorgelegte Gleichung lautet

$$(3)\quad (a,b)\,(a,c)\,(a,d)\,\alpha\, x^2 + (b,a)\,(b,c)\,(b,d)\,\beta\, y^2 + (c,a)\,(c,b)\,(c,d)\,\gamma\, z^2 + (d,a)\,(d,b)\,(d,c)\,\delta\, u^2 = 0.$$

Aus den gemachten Voraussetzungen erkennt man sofort, dass für die Auflösbarkeit der Gleichung (3) folgende Bedingungen nothwendig sind:

I. a, b, c, d dürfen nicht sämmtlich gleiches Vorzeichen haben.

II. Es muss sein*)

$$-(a,c)\,(a,d)\,(b,c)\,(b,d)\,\gamma\,\delta\, R\,(a,b);\qquad -(b,a)\,(b,d)\,(c,a)\,(c,d)\,\alpha\,\delta\, R\,(b,c)$$
$$-(a,b)\,(a,d)\,(c,b)\,(c,d)\,\beta\,\delta\, R\,(a,c);\qquad -(b,a)\,(b,c)\,(d,a)\,(d,c)\,\alpha\,\gamma\, R\,(b,d)$$
$$-(a,b)\,(a,c)\,(d,b)\,(d,c)\,\beta\,\gamma\, R\,(a,d);\qquad -(c,a)\,(c,b)\,(d,a)\,(d,b)\,\alpha\,\beta\, R\,(c,d)$$

4. Es frägt sich nun, ob die Bedingungen I und II auch hinreichen. Wenn die Bedingung I erfüllt ist, können, ohne der Allgemeinheit zu schaden, a und b als positiv, c als negativ vorausgesetzt werden, während d positiv oder negativ sein kann. Dann lässt sich die Aufgabe dahin aussprechen:

Die Zahl

$$m = -\,d\,u^2 = -\,(d,a)\,(d,b)\,(d,c)\,\delta\, u^2$$

soll durch die indefinite ternäre quadratische Form

$$f = a\,x^2 + b\,y^2 + c\,z^2$$

dargestellt werden.

---

*) Ohne die Gleichung (1) auf die in Art. 2 angegebene Weise präparirt vorauszusetzen, kann man die Bedingungen II so formuliren:

Bezeichnet man zur Abkürzung das Product $(a,c)\,(a,d)\,(b,c)\,(b,d)$ mit $[ab,\, cd]$ und mit p_{ab} einen solchen gemeinschaftlichen ungeraden Primfactor von a und b, von welchem $\alpha\beta\gamma\delta$ quadratischer Rest ist, so muss sein:

$-[ab,\, cd]\ \alpha\beta$ quadr. Rest von jeder Primzahl p_{ab} und p_{cd}
$-[ac,\, bd]\ \alpha\gamma$ „ „ „ „ „ p_{ac} „ p_{bd}
$-[ad,\, bc]\ \alpha\delta$ „ „ „ „ „ p_{ad} „ p_{bc}

Die Invarianten*) von f

$$\Omega = (a,b)\,(b,c)\,(c,a), \qquad \Delta = -(d,a)\,(d,b)\,(d,c)\,\alpha\,\beta\,\gamma$$

sind relativ prim und enthalten keine quadratischen Factoren; die primitive Adjungirte von f ist

$$F = -(b,c)(c,d)(d,b)\beta\gamma X^2 - (c,d)(d,a)(a,c)\gamma\alpha Y^2 - (d,a)(a,b)(b,d)\alpha\beta Z^2.$$

Die Lösung unserer Aufgabe ist immer dann und nur dann möglich, wenn es eine binäre quadratische Form Φ der Determinante

$$\Delta m = (d,a)^2\,(d,b)^2\,(d,c)^2\,\alpha\,\beta\,\gamma\,\delta\,u^2$$

gibt, welche durch F dargestellt werden kann.**)

5. Von jetzt an beschränke ich mich auf den Fall, dass a, b, c, d ungerade sind. Dann lässt sich zeigen, dass die Bedingungen I und II, von einem Ausnahmefall abgesehen, auch hinreichen; es kann sogar und soll auch im Folgenden $u = 1$, Φ primitiv und die Darstellung von Φ durch F als eigentlich vorausgesetzt werden.

Unter den über die Vorzeichen von a, b, c, d gemachten Voraussetzungen ist die Determinante von F positiv, diejenige von Φ hat das Zeichen von $-\delta$. Ist δ positiv, so muss auch Φ eine positive Form sein, um durch F dargestellt werden zu können. Da nun die Determinante von Φ gleich Δm und $m = -(d,a)\,(d,b)\,(d,c)\,\delta$ zu Ω prim ist, so ist die nothwendige und hinreichende Bedingung dafür, dass Φ durch indefinite ternäre Formen der Invarianten Δ, Ω dargestellt werden könne: $\Omega\,\Phi$ muss quadratischer Rest von m sein***); also

$$\left(\frac{\Phi}{\mu}\right) = \left(\frac{\Omega}{\mu}\right)$$

in Bezug auf jeden Primfactor μ von m†).

*) Vergl. Smith, Phil. Trans., vol. 157, die Zeichen jedoch genommen wie bei Gauss, Disq. ar. Art. 267.

**) Gauss, Disq. ar. Art. 280.

***) Smith, l. c. Art. 10.

†) Gauss, Disq. ar. Art. 233.

Soll aber die ternäre Form, durch welche Φ dargestellt wird, mit F äquivalent sein, also Φ auch durch F dargestellt werden können, so ist, weil Ω prim zu $\varDelta$, nothwendig und hinreichend, dass sie mit F in dasselbe Geschlecht gehöre, d. h. dass

$$\left(\frac{\Phi}{\delta'}\right)=\left(\frac{F}{\delta'}\right)\,;\quad\left(\frac{m}{\omega}\right)=\left(\frac{f}{\omega}\right)$$

in Bezug auf jeden Primfactor δ' von $\varDelta$, ω von Ω*).

Also muss zunächst sein:

$$\left(\frac{\Omega\,F}{\mu}\right)=1\,,\quad\left(\frac{m\,f}{\omega}\right)=1$$

in Bezug auf jeden Primfactor μ von $(m,\varDelta)=(d,a)\,(d,b)\,(d,c)$ und jeden Primfactor ω von $\Omega=(a,b)\,(b,c)\,(c,a)$. Diese Bedingungen sind aber mit den Bedingungen II identisch.

Die noch übrig bleibenden Bedingungen sind:

$$(\alpha)\qquad\left(\frac{\Phi}{\delta'}\right)=\left(\frac{F}{\delta'}\right),\quad\left(\frac{\Phi}{\delta''}\right)=\left(\frac{\Omega}{\delta''}\right)$$

in Bezug auf jeden Primfactor δ' von $\varDelta$, δ'' von δ. Sie bestimmen das Geschlecht von Φ vollständig und sind immer erfüllbar, wenn $\varDelta m\equiv 3,5,7 \pmod 8$; denn ist $\varDelta m\equiv 3 \pmod 4$, so kommt zu den durch (α) vorgeschriebenen Charakteren in Bezug auf die Primfactoren von $\varDelta m$ noch einer (mod 4) hinzu, welcher der Existenzbedingung des Geschlechts gemäss gewählt werden kann, und ist $\varDelta m\equiv 5 \pmod 8$, so repräsentiren eigentlich und uneigentlich primitive Formen zusammen alle angebbaren Charaktere. Ist jedoch $\varDelta m\equiv 1 \pmod 8$, also $\alpha\,\beta\,\gamma\,\delta$

*) Vergl. meine Inauguraldissertation pag. 27 (der von Smith mit Ψ bezeichnete Supplementarcharakter ist durch die übrigen bestimmt).

$\equiv a\,b\,c\,d \equiv 1 \pmod 8$, so haben eigentlich und uneigentlich primitive Formen der Determinante $\varDelta m$ dieselben Charaktere, uud damit ein Geschlecht von Formen Φ existire, muss das Product aller seiner Charaktere in Bezug auf die Primfactoren von $\alpha\,\beta\,\gamma\,\delta$ gleich $+1$ sein, d. h. in verallgemeinertem Legendre'schen Zeichen

$$\left(\frac{\Phi}{\alpha\,\beta\,\gamma\,\delta}\right) = +1\,;$$

somit wegen (α)

$$\left(\frac{F}{\alpha\,\beta\,\gamma}\right)\left(\frac{\Omega}{\delta}\right) = +1$$

oder

$$\left(\frac{-(b,c)\,(c,d)\,(d,b)\,\beta\,\gamma}{\alpha}\right)\left(\frac{-(c,d)\,(d,a)\,(a,c)\,\gamma\,\alpha}{\beta}\right)\left(\frac{-(d,a)\,(a,b)\,(b,d)\,\alpha\,\beta}{\gamma}\right)$$
$$\left(\frac{(a,b)\,(b,c)\,(c,a)}{\delta}\right) = +1\,.$$

Setzt man, weil γ negativ ist, für einen Augenblick $\gamma = -\gamma'$, so wird

$$\left(\frac{-\beta\gamma}{\alpha}\right)\left(\frac{-\gamma\,\alpha}{\beta}\right)\left(\frac{-\alpha\,\beta}{\gamma}\right) = \left(\frac{\beta\,\gamma'}{\alpha}\right)\left(\frac{\gamma'\,\alpha}{\beta}\right)\left(\frac{\alpha\,\beta}{\gamma'}\right)\left(\frac{-1}{\gamma'}\right)$$

$$= (-1)^{\frac{\alpha-1}{2}\cdot\frac{\beta-1}{2}+\frac{\gamma'-1}{2}\cdot\frac{\alpha\beta+1}{2}} = (-1)^{\frac{-\alpha-\beta+\gamma'+\alpha\beta\gamma'}{4}} = (-1)^{\frac{\alpha+\beta+\gamma+\delta}{4}}\,.$$

Ist also $a\,b\,c\,d \equiv 1 \pmod 8$, so kommt zu den nothwendigen Bedingungen I und II noch hinzu die Bedingung

$$\left(\frac{(b,c)\,(c,d)\,(d,b)}{\alpha}\right)\left(\frac{(c,d)\,(d,a)\,(a,c)}{\beta}\right)\left(\frac{(d,a)\,(a,b)\,(b,d)}{\gamma}\right)\left(\frac{(a,b)\,(b,c)\,(c,a)}{\delta}\right)$$
$$= (-1)^{\frac{\alpha+\beta+\gamma+\delta}{4}}\,,$$

welche sofort noch vereinfacht werden soll.

6. Nach dem verallgemeinerten Reciprocitätssatze ist nämlich

$$\left(\frac{(b,c)\,(c,d)\,(d,b)}{\alpha}\right)=\left(\frac{\alpha}{(b,c)\,(c,d)\,(b,d)}\right)(-1)^{\frac{\alpha-1}{2}\cdot\frac{(b,c)\,(c,d)\,(d,b)-1}{2}}$$

u. s. w.; daher geht die letzte Gleichung des vorigen Artikels über in

$$(\beta)\qquad \left(\frac{\alpha\,\beta}{(c,d)}\right)\left(\frac{\alpha\,\gamma}{(b,d)}\right)\left(\frac{\alpha\,\delta}{(b,c)}\right)\left(\frac{\beta\,\gamma}{(a,d)}\right)\left(\frac{\beta\,\delta}{(a,c)}\right)\left(\frac{\gamma\,\delta}{(a,b)}\right)=(-1)^{\frac{\sigma}{4}},$$

wo

$$\begin{aligned}\sigma &= \alpha+\beta+\gamma+\delta\\ &+[(b,c)\,(c,d)\,(d,b)-1]\,(\alpha-1)+[(c,d)\,(d,a)\,(a,c)-1]\,(\beta-1)\\ &+[(d,a)\,(a,b)\,(b,d)-1]\,(\gamma-1)+[(a,b)\,(b,c)\,(c,a)-1]\,(\delta-1).\end{aligned}$$

Aus

$$\alpha\,\beta\,\gamma\,\delta\equiv 1 \pmod 8$$

und

$$\begin{aligned}\alpha\,\beta\,\gamma\,\delta &= [1+(\alpha-1)]\,[1+(\beta-1)]\,[1+(\gamma-1)]\,[1+(\delta-1]\\ &\equiv 1+\alpha+\beta+\gamma+\delta \pmod 4\end{aligned}$$

folgt aber

$$\alpha+\beta+\gamma+\delta\equiv 0 \pmod 4$$

und

$$\alpha-1\equiv\beta+\gamma+\delta-3 \pmod 4;$$

u. s. w. Daher ist

$$\begin{aligned}\sigma &\equiv \alpha+\beta+\gamma+\delta\\ &+[(b,c)(c,d)(d,b)-1]\,(\beta+\gamma+\delta-3)+[(c,d)(d,a)(a,c)-1]\,(\gamma+\delta+\alpha-3)\\ &+[(d,a)(a,b)(b,d)-1]\,(\delta+\alpha+\beta-3)+[(a,b)(b,c)(c,a)-1]\,(\alpha+\beta+\gamma-3)\\ &\equiv 4+\alpha\,[(c,d)\,(d,a)\,(a,c)+(d,a)\,(a,b)\,(b,d)+(a,b)\,(b,c)\,(c,a)]\\ &\quad+\beta\,[(d,a)\,(a,b)\,(b,d)+(a,b)\,(b,c)\,(c,a)+(b,c)\,(c,d)\,(d,b)]\\ &\quad+\gamma\,[(a,b)\,(b,c)\,(c,a)+(b,c)\,(c,d)\,(d,b)+(c,d)\,(d,a)\,(a,c)]\\ &\quad+\delta\,[(b,c)\,(c,d)\,(d,b)+(c,d)\,(d,a)\,(a,c)+(d,a)\,(a,b)\,(b,d)]\\ &-3\,[(b,c)\,(c,d)\,(d,b)+(c,d)\,(d,a)\,(a,c)+(d,a)\,(a,b)\,(b,d)+(a,b)\,(b,c)\,(c,a)]\\ &\hspace{20em}\pmod 8\end{aligned}$$

Da $(a, b)^2 \equiv 1 \pmod 8$ ist u. s. w., so lässt sich der zweite Summand der ersten Zeile dieser Congruenz in die Form bringen

$$\alpha\,[(a,b)^2 (c,d)(d,a)(a,c) + (a,c)^2 (d,a)(a,b)(b,d) + (a,d)^2 (a,b)(b,c)(c,a)]$$
$$= a\;[(a,b)(c,d) + (a,c)(b,d) + (a,d)(b,c)]\,,$$

analog die drei folgenden Summanden. Da ferner

$$[(a,b)-1]\;[(b,c)-1]\;[(c,a)-1] \equiv 0 \pmod 8\,,$$

so ist

$$(a,b)(b,c)(c,a) \equiv (a,b)(b,c) + (b,c)(c,a) + (c,a)(a,b) - (a,b) - (b,c) - (c,a) + 1 \pmod 8$$

und ebenso für die übrigen Glieder der letzten Zeile; daher wird

$$\sigma \equiv (a+b+c+d)\,[(a,b)(c,d) + (a,c)(b,d) + (a,d)(b,c)] - 3\,(\Sigma_2 - 2\,\Sigma_1) \pmod 8$$

wo Σ_1 die Summe der 6 Zahlen (a, b), (a, c), (a, d), (b, c), (b, d), (c, d) bedeutet, Σ_2 aber die Summe der Producte derselben zu je zwei, die drei Producte aus je zwei complementären wie $(a, b)\,(c, d)$ ausgeschlossen. Da nun

$$a+b+c+d \equiv o \pmod 4,\quad (a,b)(c,d)+(a,c)(b,d)+(a,d)(b,c) \equiv 1 \pmod 2,$$

so ist schliesslich

$$\sigma \equiv a+b+c+d - 3\,\Sigma_2 - 2\,\Sigma_1 \pmod 8\,.$$

Die linke Seite von (β) geht ferner mit Hülfe der Bedingungen II, nach welchen z. B. $\left(\frac{\alpha\,\beta}{(c,d)}\right) = \left(\frac{-(a,c)(a,d)(b,c)(b,d)}{(c,d)}\right)$ ist, und mit Hülfe des verallgemeinerten quadratischen Reciprocitätssatzes über in

$$(-1)^{\frac{\tau}{4}}\,,$$

wo

$$\tau \equiv \Sigma_2 - 2\,\Sigma_1 \pmod 8\,.$$

Daher geht endlich (β) über in

$$a+b+c+d \equiv 4\,\Sigma_2 \pmod 8$$

oder, weil Σ_2 als Summe von 12 ungeraden Zahlen gerade ist, in

III. $$a+b+c+d \equiv 0 \pmod 8.$$

Hieraus folgt:

Ist $abcd \equiv 3$, 5 oder 7 (mod 8), so sind die Bedingungen I und II für die Auflösbarkeit der Gleichung (1) hinreichend; ist aber $abcd \equiv 1$ (mod 8), so sind sie zusammen mit der Bedingung III hinreichend.

Man erkennt leicht, dass die Congruenzen $abcd \equiv 1$, $a+b+c+d \equiv 0$ (mod 8) von den in Art. 2 angegebenen Veränderungen der Gleichung (1) unabhängig sind.

7. Wegen der in Art. 5 getroffenen Beschränkung auf $u=1$, primitives Φ und eigentliche Darstellungen von Φ durch F bleibt es ungewiss, ob für $abcd \equiv 1$ (mod 8) die Bedingung III nothwendig ist. Dass dies wirklich der Fall ist, ergibt sich daraus, dass aus den Bedingungen

$$abcd \equiv 1 \pmod 8,\quad ax^2+by^2+cz^2+du^2=0$$

immer die Congruenz III folgt. Da nämlich die 4 Zahlen x, y, z, u keinen gemeinschaftlichen Theiler haben, so sind sie entweder alle ungerade oder zwei gerade, zwei ungerade. Im ersten Fall ergibt sich III sofort, im zweiten seien z. B. x, y ungerade, z, u gerade. Dann ist $a+b \equiv 0$ (mod 4). Je nachdem nun $a+b \equiv 0$ oder 4 (mod 8), ist $ab \equiv -1$ oder 3 (mod 8); daher auch $cd \equiv -1$ oder 3 (mod 8) und hinwieder $c+d \equiv 0$ oder 4 (mod 8); folglich

$$a+b+c+d \equiv 0 \pmod 8; \quad \text{w. z. b. w.}$$

8. Hebt man die Beschränkung auf ungerade Coefficienten auf, so erhält man in ähnlicher Weise den allgemeinern Satz:

Sind die Coefficienten der Gleichung

$$ax^2 + by^2 + cz^2 + du^2 = 0$$

ganze, von Null verschiedene Zahlen ohne quadratische Factoren und haben je drei derselben keinen gemeinschaftlichen Theiler, so ist die Gleichung in ganzen Zahlen (die nicht sämmtlich verschwinden) immer dann und nur dann lösbar, wenn die Bedingungen I und II (Art. 3, Anmerkung) erfüllt sind, und ausserdem

$a\,b\,c\,d \equiv 2, 3, 5, 6, 7 \pmod 8$

oder $a\,b\,c\,d \equiv 1 \pmod 8$ und zugleich $a+b+c+d \equiv 0 \pmod 8$

oder $a\,b\,c\,d \equiv 4 \pmod 8$ und (wenn a, b gerade, c, d ungerade)

entweder $\frac{1}{4}\,a\,b\,c\,d \equiv 3, 5, 7 \pmod 8$

oder $\frac{1}{4}\,a\,b\,c\,d \equiv 1 \pmod 8$ und zugleich $\frac{a}{2} + \frac{b}{2} + c + d$

$$\equiv \frac{(cd)^2 - 1}{2} \pmod 8.$$

9. Die vorige Gleichung ist nur ein Specialfall der folgenden

$$f_1 = \Sigma\, a_{ik}\, x_i\, x_k = 0 \qquad (a_{ik} = a_{ki}\,;\; i, k = 1, 2, 3, 4).$$

Setzt man die quaternäre Form f_1 primitiv und ihre Determinante $\Sigma \pm a_{11}\, a_{22}\, a_{33}\, a_{44} = \Delta_4$ von Null verschieden voraus, nimmt das Vorzeichen von f_1 so, dass der Trägheitsindex*) k von $f_1 \geqq 2$ wird, bezeichnet ferner den

*) D. h. die Anzahl der Quadrate, welche bei der Transformation der Form f_1 in eine Summe von 4 Quadraten durch reelle lineare Substitutionen mit positivem Vorzeichen erscheinen (vergl. Smith, Proc. R. Soc. vol. XIII u. XVI).

grössten gemeinschaftlichen Theiler aller Unterdeterminanten $m$ten Grades von $\varDelta_4$ mit $\varDelta_{\rm m}$, den Quotienten $\frac{\varDelta_{\rm m+1}}{\varDelta_{\rm m}} \frac{\varDelta_{\rm m-1}}{\varDelta_{\rm m}}$ mit $J_{\rm m}$ (hiebei ist $\varDelta_0 = \varDelta_1 = 1$, $J_{\rm k}$ negativ, die übrigen $J_{\rm m}$ positiv zu nehmen), den Quotienten aus $J_{\rm m}$ durch das grösste in $J_{\rm m}$ aufgehende Quadrat mit $i_{\rm m}$, die Zahl $i_{\rm m}$ oder $\frac{1}{2}\, i_{\rm m}$, je nachdem $i_{\rm m}$ ungerade oder gerade, mit $i'_{\rm m}$, die Quotienten aus $i_1\, i_2$ und $i_1\, i_3$ durch die grössten in ihnen aufgehenden Quadrate mit i_{12} und i_{13}, endlich die primitive zweite und dritte Concomitante von f_1 mit f_2 und f_3, so dass also

$$\varDelta_2 f_2 = (a_{11}a_{22} - a_{12}^2)\, x_{12}^2 + (a_{11}a_{33} - a_{13}^2)\, x_{13}^2 + \ldots + 2(a_{11}a_{23} - a_{12}a_{13}) x_{12} x_{13} + \ldots$$

$$\varDelta_3 f_3 = \begin{vmatrix} a_{22} & a_{23} & a_{24} \\ a_{32} & a_{33} & a_{34} \\ a_{42} & a_{43} & a_{44} \end{vmatrix} \xi_1^2 + \ldots\ldots \quad \text{(die adjungirte Form zu } f_1\text{);}$$

dann lassen sich die nothwendigen und hinreichenden Bedingungen für die Auflösbarkeit der Gleichung $f_1 = 0$ in ganzen Zahlen, die nicht sämmtlich verschwinden, folgendermassen ausdrücken:

Es muss sein

I. die Form f_1 indefinit;

II. $\left(\frac{f_1}{p}\right)\left(\frac{f_2}{p}\right)\left(\frac{f_3}{p}\right) = \left(\frac{-i_{12}}{p}\right)$, $\left(\frac{f_1}{p'}\right)\left(\frac{f_3}{p'}\right) = \left(\frac{-i_2}{p'}\right)$, $\left(\frac{f_2}{p''}\right) = \left(\frac{-i_3}{p''}\right)$

in Bezug auf alle ungeraden Primzahlen p, p', p'', von denen i_{13} quadratischer Rest ist und von welchen ausserdem

p zugleich in i_1, i_2, i_3,
p' zugleich in i_1 und i_3, aber nicht in i_2,
p'' in i_2, aber nicht in $i_1\, i_3$

aufgehen muss;

III. wenn die Formen f_1, f_2, f_3 eigentlich primitiv sind, $i_1 \equiv i_3 \pmod 2$, $i'_1\, i'_3 \equiv 1 \pmod 8$:

$$\psi\,(0,3) = (-1)^{\frac{i'_1+1}{2} \cdot \frac{i'_2+1}{2} + (i_2-1)\frac{i'^2_1-1}{8} + (i_1-1)\frac{i'^2_2-1}{8}},$$

wo ψ (0,3) den Simultancharakter*) von f_1, f_2, f_3 bedeutet; wenn f_1, f_3 eigentlich, f_2 uneigentlich primitiv sind, J_1 und J_3 gerade, $i_1\, i_3 \equiv 1 \pmod 8$:

$$(-1)^{\frac{f_1^2-1}{8} + \frac{f_3^2-1}{8}} = (-1)^{\frac{i_2^2-1}{8}};$$

wenn f_2 eigentlich primitiv ist, J_2 gerade, $i_1\, i_3 \equiv 1 \pmod 8$, $f_1\, f_3 \equiv 2\, i_2 \pmod 4$:

$$(-1)^{\frac{f_2^2-1}{8}} = (-1)^{\frac{i_1^2-1}{8}}.$$

Hiebei bedeutet f_m, wo es in einer Gleichung oder Congruenz vorkommt, eine durch die Form f_m darstellbare Zahl, welche ungerade oder das Doppelte einer ungeraden Zahl ist, je nachdem f_m eigentlich oder uneigentlich primitiv ist.

II. Ueber die Auflösung der Gleichung
$ax^2 + by^2 + cz^2 + du^2 + ev^2 = 0$
in ganzen Zahlen.

Man kann auch hier annehmen, dass die Coefficienten keine quadratischen Factoren enthalten und dass je drei keinen gemeinschaftlichen Theiler haben. Denn wäre z. B.

*) Smith, Proc. R. Soc. vol. XVI.

p ein gemeinschaftlicher Primfactor von a, b, c, so setze man (womit man allerdings die Lösung specialisirt)

$$a = a'p,\ b = b'p,\ c = c'p,\ u = u'p,\ v = v'p,$$

wodurch die Gleichung übergeht in

$$a'x^2 + b'y^2 + c'z^2 + dpu'^2 + epv'^2 = 0,$$

also das Product der Coefficienten durch p dividirt wird. Man wird das Verfahren so lange fortsetzen und die Gleichung vereinfachen können, als noch drei Coefficienten einen gemeinschaftlichen Theiler haben. Da nun nicht alle Coefficienten gleiches Vorzeichen haben dürfen, kann man a, b positiv, c negativ voraussetzen und die Aufgabe ist dann, u und v so zu wählen, dass die Zahl $-(du^2+ev^2)$ durch die indefinite Form $f=ax^2+by^2+cz^2$ dargestellt werden kann.

Setzt man wieder mit Beibehaltung der frühern Bezeichnung

$$a=(a,b)(a,c)\alpha,\ b=(b,a)(b,c)\beta,\ c=(c,a)(c,b)\gamma,\ d=(d,e)\delta,\ e=(d,e)\varepsilon,$$

so sind (a,b), (a,c), (b,c), α, β, γ relativ prim und prim zu (d,e), und man hat die Zahl

$$m = -(d,e)(\delta u^2 + \varepsilon v^2)$$

darzustellen durch die eigentlich primitive Form

$$f = (a,b)(a,c)\alpha x^2 + (b,a)(b,c)\beta y^2 + (c,a)(c,b)\gamma z^2$$

der Invarianten $\Omega = (a,b)(b,c)(c,a)$, $\Delta = \alpha\beta\gamma$. Da (d,e) prim ist zu $\Omega\Delta$ und die binäre Form $\delta u^2 + \varepsilon v^2$ eigentlich primitiv, kann man u und v so wählen, dass m prim wird zu $\Omega\Delta$. Beschränkt man sich auf ungerade Coefficienten a, b, c, d, e, so kann man ausserdem m ungerade und nicht congruent Δ (mod 8) voraussetzen. Die Lösung der Aufgabe ist dann immer möglich, wenn noch für jeden Primfactor ω von Ω

$$\left(\frac{m}{\omega}\right) = \left(\frac{f}{\omega}\right), \text{ d. h. } \left(\frac{\delta u^2 + \varepsilon v^2}{\omega}\right) = \left(\frac{-(d,e) f}{\omega}\right)$$

gemacht werden kann*). Da aber die Determinante $-\delta\varepsilon$ der Form $\delta u^2 + \varepsilon v^2$ prim ist zu Ω, so kann diesen Bedingungen immer Genüge geleistet werden. Hieraus folgt:

Die Gleichung

$$a x^2 + b y^2 + c z^2 + d u^2 + e v^2 = 0,$$

deren Coefficienten ungerade sind und nicht sämmtlich gleiches Vorzeichen haben, ist immer in ganzen Zahlen (die nicht alle Null sind) lösbar.

Unter denselben Voraussetzungen gilt dies offenbar auch von der allgemeinern Gleichung

$$a_1 x_1^2 + a_2 x_2^2 + \ldots\ldots + a_n x_n^2 = 0,$$

wenn $n > 4$ ist.

Dasselbe gilt auch, wenn die Coefficienten der Gleichung nicht sämmtlich ungerade sind, und hieraus folgt dann allgemein:

Die Gleichung

$$f(x_1, x_2, \ldots x_n) = \Sigma a_{ik} x_i x_k = 0, \; (a_{ik} = a_{ki};\; i,k = 1, 2, 3 \ldots n),$$

mit ganzzahligen Coefficienten a_{ik} ist in ganzen Zahlen, die nicht sämmtlich verschwinden, stets lösbar, wenn die Form $f(x_1, \ldots x_n)$ indefinit und die Anzahl n ihrer Variabeln grösser als vier ist.

*) Vergl. meine Inauguraldissertation, pag. 30.