Über die Gleichung $x^3 + y^3 + z^3 = 0$

Von

Dr. F. Schmid

(Vorgelegt in der Sitzung am 17. Dezember 1942)

Wir nehmen an, die Gleichung

$$x^3 + y^3 \times z^3 = 0 \tag{1}$$

könne durch ganze rationale Zahlen befriedigt werden. Dabei dürfen wir voraussetzen, daß diese Zahlen zu je zweien teilerfremd seien. Da die Identität besteht:

$$(x + y + z)^3 \equiv x^3 + y^3 + z^3 + 3\ (y + z)\ (z + x)\ (x + y),$$

so folgt, daß in unserem Falle

$$(x + y + z)^3 = 3\ (y + z)\ (z + x)\ (x + y) \tag{2}$$

und diese Gleichung ist mit (1) gleichbedeutend.

Aus (1) folgt, daß $(y + z)$ in x^3, $(z + x)$ in y^3, $(x + y)$ in z^3 aufgeht, daher sind $(y + z)$, $(z + x)$ und $(x + y)$ zu je zweien teilerfremd. Ferner ist die rechte Seite der Gleichung (2) durch 3 teilbar, daher muß es auch die linke sein; da diese aber eine dritte Potenz ist, so muß sie auch durch 3^3 teilbar sein. Daher ist auch die rechte Seite von (2) durch 3^3 teilbar und daraus folgt, daß von den drei Faktoren rechts einer, aber auch nur einer, durch 3 teilbar ist. Nehmen wir ein für allemal an, daß $(x + y)$ und folglich z durch 3 teilbar sei, so müssen die 3 Faktoren $(y + z)$, $(z + x)$ und $3\ (x + y)$ zu je zweien relativ prim sein. Da aber ihr Produkt eine dritte Potenz ist, so können wir setzen:

$$\left.\begin{aligned} y + z &= p^3 \\ z + x &= q^3 \\ 3\,(x + y) &= r^3 \end{aligned}\right\}\ (3) \quad \text{oder} \quad \left.\begin{aligned} y + z &= p^3 \\ z + x &= q^3 \\ x + y &= \frac{r^3}{3} \end{aligned}\right\}\ (3\,\text{a})$$

Aus (2) und (3) folgt:

$$x + y + z = p\,q\,r.$$

Anderseits erhalten wir durch Addition der Gleichungen (3a)

$$2\,(x+y+z)=p^3+q^3+\frac{r^3}{3}.$$

Durch Kombination dieser beiden Gleichungen ergibt sich:

$$2\,p\,q\,r=p^3+q^3+\frac{r^3}{3}. \qquad (4)^{1}$$

In dieser Gleichung sind p, q, r zu je zweien teilerfremd, r ist durch 3 teilbar, p und q aber nicht.

Wir nehmen nun an, r sei genau durch 3^i teilbar ($i \geqq 1$). Weil aber $\frac{r^3}{3}$ genau durch 3^{3i-1} teilbar ist, und $3\,i-1>i$, so ist (p^3+q^3) genau durch 3^i teilbar, so wie die linke Seite von (4). Da ferner $p^3+q^3=(p+q)\;(p^2-pq+q^2)=(p+q)\;([p+q])^2-3pq)$, so folgt, daß beide Faktoren von (p^3+q^3) durch 3 teilbar sind, und zwar ist (p^2-pq+q^2) durch 3, aber nicht durch 3^2 teilbar, während $(p+q)$ durch 3^{i-1} teilbar ist; daher ist $i\geqq 2$. Setzen wir $r=3r'$, so ist r' genau durch 3^{i-1} teilbar und wir können die Gleichung (4) schreiben, wie folgt:

$$3pq\,.\,2r'=p^3+q^3+(2r')^3+(r')^3.$$

Addieren wir

$$3pq(p+q)=3p^2q+3pq^2,$$

so ergibt sich:

$$3pq[(p+q)+2r']=(p+q)^3+(2r')^3+(r')^3.$$

Wenn wir nun beiderseits durch $3[(p+q)+2r']$ dividieren, so erhalten wir:

$$pq=\frac{1}{3}\,(p+q)^2-\frac{1}{3}\,(p+q)\,2r'+\frac{1}{3}\,(2\,r')^2+\frac{r'^3}{3[(p+q)+2r']}. \qquad (5)$$

Da $(p+q)$ und r' durch 3 teilbar sind, so muß der Bruch auf der rechten Seite von (5) eine ganze Zahl darstellen, also $3[(p+q)+2r']$ in r'^3 aufgehen. Es läßt sich nun leicht zeigen, daß $3[(p+q)+2r']$

[1] Diese Gleichung hat Legendre in der ersten Auflage seiner „Theorie des Nombres“ auf ähnliche Art abgeleitet, er ist aber anscheinend über diesen Punkt nicht hinausgekommen und die Stelle ist in den späteren Auflagen weggeblieben.

und $\frac{r'^3}{3[(p+q)+2r']}$ teilerfremd sind. Da nämlich auf der rechten Seite von (5) das erste, zweite und dritte Glied durch 3 teilbar ist, die linke Seite von (5) aber nicht, so kann auch das letzte Glied rechts nicht durch 3 teilbar sein. Ist ferner δ eine Primzahl, welche von 3 verschieden ist und in $[(p+q)+2r']$ aufgeht, so muß sie auch in r'^3, also auch in r' und in $2r'$ und endlich auch in $[(p+q)+2r']-2r'=p+q$ aufgehen. Nehmen wir nun an, δ ginge auch in $\frac{r'^3}{3[(p+q)+2r']}$ auf, so müßte es in allen Gliedern auf der rechten Seite von (5) und also auch in $p\,q$ aufgehen. Dies ist aber unmöglich, da r' mit p und q keinen Faktor gemeinsam hat.

Wir können demnach setzen:

$$3[(p+q)+2r']=\rho^3, \quad \frac{r'^3}{3[(p+q)+2r']}=P^3, \quad r'=\rho\, P,$$

und hier sind ρ und P ganz, teilerfremd und es ist $\rho \equiv 0$ [mod 3].

Daraus folgt zunächst:

$$p+q=[(p+q)+2r']-2r'=\frac{1}{3}\rho^3-2\rho P;$$

weiter ergibt sich aus (5):

$$p\,q=\frac{1}{3}\left(\frac{1}{3}\rho^3-2\rho P\right)^2-\frac{2}{3}\left(\frac{1}{3}\rho^3-2\rho P\right)\rho P+\frac{4}{3}\rho^2P^2+P^3$$

oder:

$$p\,q=\frac{1}{27}\rho^6-\frac{2}{3}\rho^4 P+4\rho^2P^2+P^3.$$

Setzt man:

$$\left.\begin{aligned}(p+q)^2&=\left(\frac{1}{3}\rho^3-2\rho P\right)^2\\ 4pq&=\frac{4}{27}\rho^6-\frac{8}{3}\rho^4P+16\rho^2P^2+4P^3\end{aligned}\right\}$$

und subtrahiert die zweite Gleichung von der ersten, so folgt nach leichten Reduktionen:

$$(p-q)^2=-4P^3-27\left(\frac{1}{27}\rho^3-\frac{2}{3}\rho P\right)^2 \tag{6}$$

Bezeichnen wir nun mit t eine unbestimmte Größe und setzen wir die Gleichung an:

$$t^3 + P.t + \left(\frac{1}{27}\rho^3 - \frac{2}{3}\rho P\right) = 0, \tag{7}$$

so ist $(p-q)^2$ die Diskriminante von (7), (6) ist die zu (7) gehörige Diskriminantengleichung und es wird am Schluß gezeigt werden, daß (7) drei ganze, rationale Zahlen zu Wurzeln hat.

Nimmt man nun in (7) die Substitution vor

$$t = s - \frac{1}{3}\rho,$$

so erhält man die Gleichung:

$$s^3 - \rho s^2 + \left(\frac{1}{3}\rho^2 + P\right) s - \rho P = 0 \tag{8}$$

und da $\frac{1}{3}$ eine ganze Zahl ist, so sind auch die Wurzeln von (8) ganze rationale Zahlen. Bezeichnet man sie mit x_1, y_1 z_1, so ist

$$\rho = x_1 + y_1 + z_1, \quad \frac{1}{3}\rho^2 + P = x_1 y_1 + y_1 z_1 + z_1 x_1, \quad \rho P = x_1 y_1 z_1.$$

Mit Hilfe der Identität

$$\rho^3 \equiv 3\rho\left(\frac{1}{3}\rho^2 + P\right) - 3\rho P$$

erhalten wir jetzt

$$(x_1 + y_1 + z_1)^3 = 3(x_1 + y_1 + z_1)\ (x_1 y_1 + y_1 z_1 + z_1 x_1) - 3x, y_1 z_1$$

oder endlich:

$$(x_1 + y_1 + z_1)^3 = 3(x_1 + y_1)\ (y_1 + z_1)\ (z_1 + x_1). \tag{9}$$

Diese letzte Gleichung hat aber genau dieselbe Form wie die Gleichung (2) und daraus folgt, daß zwischen x_1, y_1 und z_1 wiederum die Beziehung

$$x_1^3 + y_1^3 + z_1^3 = 0 \tag{10}$$

besteht. Daraus kann man aber bekanntlich schließen, daß die Gleichung (1) in ganzen rationalen Zahlen unmöglich ist.

Es bleibt noch übrig zu zeigen, daß die Gleichung (7)

$$t^3+Pt+\left(\frac{1}{27}\rho^3-\frac{2}{3}\rho P\right)=0$$

drei ganze rationale Wurzeln besitzt. Man könnte dies mit Hilfe der Theorie des Körpers der dritten Einheitswurzeln beweisen, wir ziehen aber einen anderen Weg vor, der uns zu einem interessanten Resultat führen wird.

Aus (6) ersehen wir, daß die Diskriminante von (7) das Quadrat einer ganzen rationalen Zahl ist. Nun nehmen wir zunächst an, daß (7) irreduzibel und demnach die Wurzeln von (7), die wir mit τ_1, τ_2, τ_3 bezeichnen, kubische Irrationalzahlen seien. Dann läßt sich vor allem zeigen, daß ein durch eine solche Wurzel bestimmter Körper, etwa $k(\tau_1)$, auch die beiden anderen Wurzeln τ_2 und τ_3 enthalten müßte. Da nämlich

$$(\tau_1-\tau_2)\,(\tau_2-\tau_3)\,(\tau_3-\tau_1)=\pm\,(p-q)$$

eine ganze rationale Zahl ist, so ist es in $k(\tau_1)$ enthalten. Ferner ist $(\tau_1-\tau_2)\,(\tau_3-\tau_1)$, abgesehen vom Vorzeichen, gleich der Differente von τ_1 und daher auch in $k(\tau_1)$ enthalten. Also ist auch der Quotient

$$\frac{\pm\,(p-q)}{(\tau_1-\tau_2)\,(\tau_3-\tau_1)}=\tau_2-\tau_3$$

in $k(\tau_1)$ enthalten und da wegen (7) $\tau_2+\tau_3=-\tau_1$ ist, so sind τ_2 und τ_3 selbst in $k(\tau_1)$ enthalten.

Diese drei Wurzeln τ_1, τ_2, τ_3 sind zu je zweien teilerfremd, denn wenn wir sie in $k(\tau_1)$ in ihre idealen Primfaktoren zerlegen, so müßte ein solcher Primfaktor, der zweien von ihnen gemeinsam wäre, gemäß (7) auch in P und in $\left(\frac{1}{27}\rho^3-\frac{2}{3}\rho P\right)$ aufgehen, also auch in ρ und P, was nicht möglich ist.

Nun ist $(p-q)=\pm\,(\tau_1-\tau_2)\,(\tau_2-\tau_3)\,(\tau_3-\tau_1)$ nicht durch 3 teilbar, da $(p+q)$ durch 3 teilbar ist, p und q aber nicht. Nehmen wir also an, $\mathfrak{j}$ sei ein Primideal in $k(\tau_1)$, das in $(\tau_1-\tau_2)$ und $(\tau_2-\tau_3)$ gleichzeitig aufgeht, so müßte $\mathfrak{j}$ auch in

$$(\tau_1-\tau_2)-(\tau_2-\tau_3)=\tau_1+\tau_3-2\tau_2=-\,3\tau_2$$

aufgehen. Da $(p-q)$ nicht durch 3 teilbar ist, so kann $\mathfrak{j}$ nicht in 3, müßte also in τ_2 aufgehen; dann hätte aber τ_2 diesen Faktor $\mathfrak{j}$ mit τ_1 und τ_3 gemeinsam, was unmöglich ist. Daher können $(\tau_1-\tau_2)$

und $(\tau_2 - \tau_3)$ keinen idealen Primfaktor gemein haben und dasselbe gilt allgemein von je zweien dieser Wurzeldifferenzen.

Nun erhält aber die Diskriminante von $k(\tau_1)$ nach dem Satz von Minkowski mindestens eine Primzahl, eine sogenannte kritische Primzahl, als Faktor, und diese muß daher auch in $(p - q)$ aufgehen. Ist m diese Primzahl, so muß sie folglich mit irgendeiner der drei Wurzeldifferenzen, etwa mit $(\tau_1 - \tau_2)$, einen größten Teiler gemeinsam haben, der von 1 verschieden ist; wir setzen demnach:

$$\mathfrak{m}_1 = (m, [\tau_1 - \tau_2]).$$

$\mathfrak{m}_1$ kann aber nicht gleich m sein; denn die drei Wurzeldifferenzen sind konjugierte Größen und m müßte als rationale Primzahl in allen dreien zugleich aufgehen, was nach dem früher Bewiesenen nicht möglich ist. Daher ist $\mathfrak{m}_1$ verschieden von 1 und m und ein idealer Faktor von m. Dasselbe gilt von den beiden Idealen

$$\mathfrak{m}_2 = (m, [\tau_2 - \tau_3]) \text{ und } \mathfrak{m}_3 = (m, [\tau_3 - \tau_1]),$$

in welche $\mathfrak{m}_1$ durch die dem Körper $k(\tau_1)$ zugehörigen Substitutionen übergeht. Da das Produkt dieser drei konjugierten Ideale eine ganze rationale Zahl ist, so ist es durch m teilbar. Anderseits aber sind diese drei Ideale zu je zweien relativ prim, so wie die Wurzeldifferenzen, deren Faktoren sie sind, und daher muß ihr Produkt in m aufgehen, weil jeder einzelne Faktor desselben in m aufgeht. Also ist

$$m = \mathfrak{m}_1 \mathfrak{m}_2 \mathfrak{m}_3.$$

Es fragt sich nun, ob diese drei Ideale Primideale oder zusammengesetzt sind. Wäre $\mathfrak{m}_1$ ein zusammengesetztes Ideal, so wäre es das Produkt von zwei oder mehreren Primidealen und dasselbe würde von $\mathfrak{m}_2$ und $\mathfrak{m}_3$ gelten. Dann müßte aber die Primzahl m das Produkt von mehr als drei Primidealen sein, was nicht möglich ist, da eine rationale Primzahl nicht mehr (gleiche oder verschiedene) ideale Primfaktoren enthalten kann, als der Grad des Körpers angibt. (Ist allgemein der Grad des Körpers $= n$, ist die Zerlegung der Primzahl m dargestellt durch die Gleichung

$$m = \mathfrak{m}_1^{e_1} \mathfrak{m}_2^{e_2} \ldots \mathfrak{m}_r^{e_r}$$

und sind $f_1, f_2 \ldots f_r$ die Grade der einzelnen Pimideale, so folgt daraus

$$n = e_1 f_1 + e_2 f_2 + \ldots + e_r f_r.$$

Anderseits ist die Anzahl der gleichen oder verschiedenen Primideale, deren Produkt m ist,

$$= e_1 + e_2 + \quad + e_r,$$

kann also nie größer sein als n, da die Zahlen $f_1, f_2, \ldots f_r$ nicht kleiner sind als 1. Vergleiche hierzu etwa Bachmann: Zahlentheorie, 5. Teil, Allgem. Arithmetik der Zahlenkörper, c. 7, Nr. 6.)

Aus alledem würde sich also ergeben, daß $\mathfrak{m}_1$, $\mathfrak{m}_2$ und $\mathfrak{m}_3$ Primideale sein müßten, und daß demnach die Primzahl m das Produkt dieser drei voneinander verschiedenen Primideale wäre. Dies ist aber unmöglich, weil m nach unserer Voraussetzung in der Diskriminante des Körpers $k(\tau_1)$ aufgeht und eine solche Primzahl bekanntlich immer durch das Quadrat eines Primideals teilbar ist, also nicht das Produkt von lauter verschiedenen Primidealen sein kann. Unsere erste Annahme, daß (7) irreduzibel und alle Wurzeln von (7) irrational seien, ist also unzulässig.

Nehmen wir aber weiter an, (7) zerfiele in einen linearen und einen quadratischen Faktor, so daß also eine Wurzel rational, die beiden anderen aber quadratische Irrationalzahlen wären, so könnte die Diskriminante von (7) kein rationales Quadrat sein. Setzen wir nämlich für die zwei irrationalen Wurzeln

$$\frac{a+b\sqrt{d}}{c} \quad \text{und} \quad \frac{a-b\sqrt{d}}{c},$$

so ergäbe sich die dritte Wurzel aus (7) gleich

$-\frac{2a}{c}$ (a, b, c und d sind ganze rationale Zahlen, d ist durch kein Quadrat teilbar). Setzt man diese Werte für die Wurzeln in $(\tau_2-\tau_2)$ $(\tau_2-\tau_3)$ $(\tau_3-\tau_1)$ ein, so ergibt sich

$$p-q = \pm\frac{2b\sqrt{d}\,(9a^2-b^2d)}{c^3},$$

was unmöglich ist, da $(p-q)$ rational ist.

Es bleibt also nur die Annahme übrig, daß alle Wurzeln von (7) rational sind.

Der Beweis, den wir soeben beendet haben, bildet ein Gegenstück zu einer Untersuchung von Kronecker (Crelle, Bd. 56, oder Kroneckers Werke, Bd. I). Während nämlich Kronecker aus der anderweitig bewiesenen Unmöglichkeit der Gleichung (1) den Schluß zieht, daß die Diskriminante eines kubischen Körpers niemals ± 1 sein kann, also immer mindestens eine Primzahl enthalten muß, haben wir umgekehrt aus der anderweitig bewiesenen Existenz einer solchen Primzahl die Unmöglichkeit der Gleichung (1) abgeleitet.

Die Behauptung, „die Gleichung $x^3+y^3+z^3=0$ ist (in ganzen rationalen Zahlen) unmöglich“, ist also im Grunde gleichbedeutend mit der anderen Behauptung, „in jedem Körper dritten Grades gibt es mindestens eine kritische Primzahl“.