Ein Lemma von Euler zum Beweis der Fermatschen Vermutung im Fall $n = 3$

Lukas-Fabian Moser, SS 2013

Lemma (Euler 1760)**.** *Ist s eine ungerade Zahl und $s^3 = u^2 + 3v^2$ mit teilerfremden Zahlen $u, v \in \mathbb{Z}$, so ist $s = t^2 + 3w^2$ mit $t, w \in \mathbb{Z}$, und dabei gilt*

$$u = t(t^2 - 9w^2),$$
$$v = 3w(t^2 - w^2).$$

Skizze eines falschen Beweises. Rechne im Ring $\mathbb{Z}[\sqrt{-3}]$: Hier gilt $s^3 = (u + v\sqrt{-3}) \cdot (u - v\sqrt{-3})$. Die Teilerfremdheit von u und v impliziert die Teilerfremdheit der beiden Faktoren dieser Produktdarstellung; deswegen muß jeder einzelne von ihnen eine dritte Potenz sein, d.h. $u + v\sqrt{-3} = (t + w\sqrt{-3})^3$ und damit auch $u - v\sqrt{-3} = (t - w\sqrt{-3})^3$. Insgesamt ergibt sich $s^3 = (t^2 + 3w^2)^3$, also $s = t^2 + 3w^2$, und die angegebenen Beziehungen ergeben sich durch Ausmultiplizieren von $(u + v\sqrt{-3}) = (t + w\sqrt{-3})^3$. □

Dieser Beweis enthält mehrere Lücken, von denen eine wirklich gravierend ist: Zum einen fehlt der Nachweis der Teilerfremdheit (was auch immer das heißen soll, siehe unten) von $u + v\sqrt{-3}$ und $u - v\sqrt{-3}$, zum anderen folgt (wie man durch genaues Betrachten einer Primfaktorzerlegung bemerkt) aus der Voraussetzung, ein Produkt $a \cdot b$ sei eine n-te Potenz, *nicht*, daß a und b jeweils n-te Potenzen sein müssen, sondern nur, daß sie sich nur um eine Einheit von einer n-ten Potenz unterscheiden (beispielsweise ist $(-4) \cdot (-9) = 36 = 6^2$ ein Quadrat in $\mathbb{Z}$, aber weder -4 noch -9 sind Quadrate). Diese Lücke läßt sich aber ohne weiteres schließen, weil die einzigen Einheiten von $\mathbb{Z}[\sqrt{-3}]$ die Zahlen ± 1 sind, und diese sind jeweils drite Potenzen.

Wirklich schwerwiegend ist aber der folgende Fehler: Der Ring $\mathbb{Z}[\sqrt{-3}]$ ist nicht faktoriell (es ist etwa $2 \cdot 2 = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$, wobei 2 und $1 \pm \sqrt{-3}$ irreduzibel sind). Man kann also nicht sinnvoll von Primfaktorzerlegung sprechen, und insbesondere läßt sich aus der Tatsache, daß ein Produkt eine dritte Potenz ist, nichts über die Faktoren folgern. Genau dieser Fehler wurde von berühmten Mathematikern des 19. Jahrhunderts begangen, und er führte zur Entwicklung von Begriffen wie *Ideal*, *ganzer Abschluß*, *faktorieller Ring*, ...

Um einen (hoffentlich) korrekten Beweis des Lemmas zu geben, formulieren wir es um zur folgenden äquivalenten Version:

Lemma. *Ist s eine ungerade Zahl und $s^3 = u^2 + 3v^2$ mit teilerfremden Zahlen $u, v \in \mathbb{Z}$, so ist $u + v\sqrt{-3}$ eine dritte Potenz in $\mathbb{Z}[\sqrt{-3}]$.*

Beweis der Äquivalenz beider Lemmata. Die Voraussetzungen sind identisch, so daß wir nur die Äquivalenz der Schlußfolgerungen zeigen müssen.

Die Formel $u + v\sqrt{-3} = (t + w\sqrt{-3})^3$ mit $t, w \in \mathbb{Z}$ ist aber (durch direktes Ausmultiplizieren und Koeffizientenvergleich) äquivalent zu den angegebenen Ausdrücken für u und v. Sind beide erfüllt, so folgt außerdem durch komplexes Konjugieren $u - v\sqrt{-3} = (t - w\sqrt{-3})^3$ und damit

$$s^3 = (u + v\sqrt{-3})(u - v\sqrt{-3}) = (t + w\sqrt{-3})^3 \cdot (t - w\sqrt{-3})^3 = (t^2 + 3w^2)^3,$$

also $s = t^2 + 3w^2$. □

Der Beweis des Lemmas wird nun möglich, indem man in einem etwas größeren Ring rechnet, der tatsächlich faktoriell ist:

Es sei $\omega = \frac{1}{2}(-1 + \sqrt{-3})$ eine primitive dritte Einheitswurzel und $R := \mathbb{Z}[\omega]$ der Ring der *Eisensteinzahlen*. Dies ist ein euklidischer Ring mit der (multiplikativen) Höhenfunktion $N : a + b\omega \mapsto (a + b\omega)(a + b\overline{\omega}) = a^2 + b^2 - ab$. Ein Element $a + b\omega \in R$ liegt genau dann im Unterring $\mathbb{Z}[\sqrt{-3}] \subset R$, wenn b *gerade* ist.

Für spätere Rechnungen notieren wir noch, daß $\omega^2 = -\omega - 1$ ist (dies kann man direkt nachrechnen oder aus der Beziehung $\omega^3 = 1$ durch Anwendung der geometrischen Summenformel folgern – wer die Kreisteilungspolynome kennt, weiß es ohnehin).

Wir benötigen noch einige Hilfsaussagen über den Ring R:

Lemma.

i) Die invertierbaren Elemente von R sind genau ± 1, $\pm\omega$, $\pm\omega^2$.[1]

ii) Die Elemente $\sqrt{-3}$ und 2 sind Primelemente in R.

Beweis.

i) Ein Element $r \in R$ ist genau dann invertierbar, wenn $N(r) = 1$ ist: Denn aus $r \cdot r^{-1} = 1$ folgt $N(r) \cdot N(r^{-1}) = 1$, also $N(r) = 1$, da alle Normen natürliche Zahlen sind. Ist umgekehrt $N(r) = 1$, so bedeutet das $1 = r \cdot \overline{r}$, es ist also $\overline{r} \in R$ ein Inverses zu r.

   Für $r = a + b\omega$ ist $N(r) = 1$ aber äquivalent zu $1 = a^2 + b^2 - ab$, also $2 = 2a^2 + 2b^2 - 2ab = a^2 + b^2 + (a - b)^2$. Für ganzzahlige a, b muß dann eine der Zahlen a, b, $a - b$ verschwinden, und damit ergeben sich die Lösungen $(a, b) \in \{(\pm 1, 0), (0, \pm 1), (\pm 1, \pm 1)\}$, also die sechs angegebenen Einheiten.

[1] Dies sind zufälligerweise genau die sechsten Einheitswurzeln.

ii) Da R faktoriell ist, genügt es zu zeigen, daß die angegebenen Elemente irreduzibel sind. Ist aber $\sqrt{-3} = a \cdot b$, so folgt $N(\sqrt{-3}) = 3 = N(a) \cdot N(b)$. Dann ist aber $N(a) = 1$ oder $N(b) = 1$, d.h. einer der Faktoren ist invertierbar. (Eigentlich zeigt dieses Argument: Ist $N(r)$ eine Primzahl, so ist $r \in R$ ein Primelement.

Für die Zahl 2 muß man ein wenig genauer hinsehen: Aus $2 = a \cdot b$ folgt $N(2) = 4 = N(a) \cdot N(b)$. Sind weder a noch b Einheiten, so muß $N(a) = N(b) = 2$ sein. Aber die Norm 2 kommt niemals vor, Widerspruch. □

Beweis des Eulerschen Lemmas. Wir argumentieren in mehreren Schritten:

i) *Es gilt* $3 \nmid u$.

Andernfalls hätten wir mit $u = 3u'$ die Gleichung $s^3 = 9u'^2 + 3v^2$. Dann würde $3 \mid s^3$ folgen, daraus $3 \mid s$ und deswegen sogar $27 \mid s^3$. Das bedeutete aber wiederum $9 \mid 3v^2$, also $3 \mid v^2$ und deswegen $3 \mid v$ im Widerspruch zur Teilerfremdheit von u und v.

ii) *Die Zahlen* $u + v\sqrt{-3}$ *und* $u - v\sqrt{-3}$ *sind in* R *teilerfremd.*

Denn ist $r \in R$ ein gemeinsamer Teiler beider Zahlen, so teilt er auch ihre Summe $2u$ und ihre Differenz $2v\sqrt{-3}$. Aber u und v sind auch in R nicht beide durch 2 teilbar (denn Doppelte von Elementen von R haben die Form $x + y\sqrt{-3}$ mit *geraden* x, y), und da 2 in R ein Primelement ist, ist r damit ein gemeinsamer Teiler von u und $v\sqrt{-3}$. Aber u ist nicht durch das Primelement $\sqrt{-3}$ teilbar, denn sonst wäre $N(\sqrt{-3}) = 3 \mid N(u) = u^2$. Also ist r ein gemeinsamer Teiler von u und v, aber diese sind wegen ihrer Teilerfremdheit in $\mathbb{Z}$ auch in R teilerfremd: Denn es existieren $x, y \in \mathbb{Z}$ mit $xu + yv = 1$, und diese Gleichung, in R gelesen, zeigt die Teilerfremdheit von u und v. Also ist r eine Einheit.

iii) $u + v\sqrt{-3}$ *ist eine Kubikzahl in* R.

Da $(u + v\sqrt{-3})(u - v\sqrt{-3}) = u^2 + 3v^2 = s^3$ eine Kubikzahl ist und beide Faktoren teilerfremd sind, muß jeder Faktor bis auf eine Einheit eine Kubikzahl sein: Es gibt also $a, b \in \mathbb{Z}$ und eine Einheit $\lambda \in R$ mit $u + v\sqrt{-3} = \lambda(a + b\omega)^3$ oder, ausgeschrieben (und $\sqrt{-3} = 2\omega + 1$ eingesetzt)

$$(u + v) + 2v\omega = \lambda \cdot \left((a^3 + b^3 - 3ab^2) + (3a^2b - 3ab^2)\omega\right).$$

Nun ist $\pm\lambda \in \{1, \omega, \omega^2\}$. Da aber $\pm\omega$ und $\pm\omega^2$ keine Kubikzahlen in R sind, müssen die wir beiden letzten Fälle ausschließen.

a) Wäre $\lambda = \pm\omega$, so wäre

$$\begin{aligned}(u + v) + 2v\omega &= \pm\omega \cdot \left((a^3 + b^3 - 3ab^2) + (3a^2b - 3ab^2)\omega\right) \\ &= \pm\left((3ab^2 - 3a^2b) + (a^3 + b^3 - 3a^2b)\omega\right),\end{aligned}$$

aber das ist nicht möglich, weil $3ab^2 - 3a^2b = 3ab(b - a)$ stets gerade ist, $u + v$ jedoch ungerade.

b) Wäre $\lambda = \pm\omega^2$, so wäre

$$(u+v) + 2v\omega = \pm\left((a^3+b^3-3a^2b) + (a^3+b^3-3ab^2)\omega\right),$$

aber auch dies ist unmöglich: Denn beide Koeffizienten auf der rechten Seite sind modulo 2 identisch, aber $u+v$ ist ungerade und $2v$ gerade.

Also ist $\lambda = \pm 1$; insbesondere ist λ eine Kubikzahl, und das bedeutet, daß $u + v\sqrt{-3}$ eine Kubikzahl ist.

iv) *$u + v\sqrt{-3}$ ist eine Kubikzahl in $\mathbb{Z}[\sqrt{-3}]$.*

Wir haben $a, b \in \mathbb{Z}$ gefunden mit $(a+b\omega)^3 = u + v\sqrt{-3}$. Wir hätten gerne, daß b gerade ist (denn dann gilt $a + b\omega \in \mathbb{Z}[\sqrt{-3}]$. Der Trick ist, gegebenenfalls $a + b\omega$ zu ersetzen durch $\omega \cdot (a+b\omega)$ oder $\omega^2 \cdot (a+b\omega)$: Denn dies ändert nichts an der Ganzzahligkeit oder dem Wert der dritten Potenz, aber es ist

$$\begin{aligned} \omega \cdot (a+b\omega) &= -b + (a-b)\omega \\ \text{und } \omega^2 \cdot (a+b\omega) &= (b-a) - a\omega, \end{aligned}$$

und von den drei Zahlen $b, a-b, -a$ ist mindestens eine gerade. □