$x^2 = y^3 + 1$

Vortrag im Rahmen des Seminars der WE AℓZAGK im
Wintersemester 2008/2009 an der Universität Bremen

André Scholz

13. November 2008

Im Seminar zur Catalanschen Vermutung haben wir bisher die beiden Spezialfälle $x^p = y^2 + 1$ und $x^2 = y^q + 1$ mit $q \geq 5$ behandelt. In diesem Vortrag wird ein hübscher Beweis von W. McCallum für den Spezialfall $x^2 = y^3 + 1$ vorgestellt. Fasst man diese Gleichung als elliptische Kurve E über $\mathbb{Q}$ auf, kann man mit üblichen Methoden zeigen, dass die Gruppe $E(\mathbb{Q})$ der rationalen Punkte in E endlich ist und die Ordnung 6 hat. Damit wäre dieser Fall schnell erledigt.

W. McCallum ging allerdings, mit Hilfe der Körpernorm, einen anderen interessanten Weg.

1 Die Körpernorm

Der Begriff der Körpernorm wird für endliche Körpererweiterungen definiert und unterscheidet sich wesentlich von dem Begriff der Vektornorm.

Definition 1.1 (Körpernorm) *Sei L/K eine endliche Körpererweiterung. Für jedes $a \in L$ ist mit $f\colon L \to L$, $x \mapsto ax$ eine K-lineare Abbildung gegeben. Ihre Determinante* det f *wird* Norm $\mathcal{N}_{L/K}(a)$ von a *genannt.*

Die wichtigsten Eigenschaften der Körpernorm sind:

- Sie bildet L nach K ab.
- $\mathcal{N}_{L/K}(a \cdot b) = \mathcal{N}_{L/K}(a) \cdot \mathcal{N}_{L/K}(b)$
- $\mathcal{N}_{L/K}(a) = 0 \quad \Leftrightarrow \quad a = 0$
- Ist $a \in K$, so gilt $\mathcal{N}_{L/K}(a) = a^{[L:K]}$.
- $a \in \mathbb{Z}[\alpha]$ ist genau dann eine Einheit, wenn $\mathcal{N}_{\mathbb{Q}[\alpha]/\mathbb{Q}}(a) = \pm 1$.

Die Körpernorm kann auch mit Hilfe der K-Homomorphismen von L in einen algebraischen Abschluss $\bar{K}$ von K berechnet werden.

Satz 1.2 *Sei L/K eine endliche Körpererweiterung mit $[L:K] = qr$, wobei r die Anzahl der Elemente σ in $\mathrm{Hom}_K(L, \bar{K})$, der Menge aller K-Homomorphismen von L in einen algebraischen Abschluss von K, sei. Dann gilt für jedes Element $a \in L$*

$$\mathcal{N}_{L/K}(a) = \left(\prod_{i=1}^{r} \sigma_i(a) \right)^q$$

Ein Beweis findet sich bei Bosch [2006] S. 196ff.

Beispiel 1.3 Wir berechnen die Norm von $a = v + u\sqrt[3]{2} \in \mathbb{Q}[\sqrt[3]{2}]$. Die $\mathbb{Q}$-Homomorphismen in $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{2}], \bar{\mathbb{Q}})$ bilden $\sqrt[3]{2}$ jeweils auf $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$ bzw. $\rho^2\sqrt[3]{2}$, mit der primitiven dritten Einheitswurzel ρ, ab. Diese hat das Minimalpolynom $x^2 + x + 1$. Sei $\alpha := \sqrt[3]{2}$. Dann ist

$$\begin{aligned}
\mathcal{N}_{\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}}\left(v + u\sqrt[3]{2}\right) &= (v + u\alpha)\left(v + \rho u\alpha\right)\left(v + \rho^2 u\alpha\right) \\
&= (v + u\alpha)\left(v^2 + \underbrace{\left(\rho^2 + \rho\right)}_{=-1} vu\alpha + u^2\alpha^2\right) \\
&= v^3 + \underbrace{\left(\rho^2 + \rho + 1\right)}_{=0} v^2 u\alpha + \underbrace{\left(\rho^2 + \rho + 1\right)}_{=0} vu^2\alpha^2 + u^3\alpha^3 \\
&= v^3 + 2u^3
\end{aligned}$$

Aus $v^3 + 2u^3 = (v + u\sqrt[3]{2})(v^2 - vu\sqrt[3]{2} + u^2\sqrt[3]{4})$ erkennt man, dass jedes $a = v + u\sqrt[3]{2} \in \mathbb{Z}[\sqrt[3]{2}]$ mit Norm $\mathcal{N}_{\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}}(a) = \pm 1$ eine Einheit in $\mathbb{Z}[\sqrt[3]{2}]$ ist. Das Inverse ist direkt ablesbar. Das Inverse zu $\eta = -1 + \sqrt[3]{2}$ mit der Norm $\mathcal{N}_{\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}}(\eta) = (-1)^3 + 2 \cdot 1^3 = 1$ ist beispielsweise

$$\eta^{-1} = \underbrace{(-1)^2}_{v^2} - \underbrace{(-1)}_{v} \cdot \underbrace{1}_{u} \cdot \sqrt[3]{2} + \underbrace{1^2}_{u^2} \cdot \sqrt[3]{4} = 1 + \sqrt[3]{2} + \sqrt[3]{4}.$$

Ein weiteres Hilfsmittel, das uns gelegen kommen wird, ist der Begriff der p-Bewertung.

Definition 1.4 (p-Bewertung) *Für $n \in \mathbb{N}$ ist die p-*Bewertung $\nu_p(n)$ von n *der Exponent der Primzahl p in der Primfaktorzerlegung $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Beispielsweise ist $\nu_{p_1}(n) = \alpha_1$.*

Jedes Element x in $\mathbb{Q}[\sqrt[3]{2}]$ läßt sich eindeutig in der Form $x = a + b\sqrt[3]{2} + c\sqrt[3]{4}$, mit $a, b, c \in \mathbb{Q}$ schreiben. Im Weiteren betrachten wir den Ring $\mathbb{Z}[\sqrt[3]{2}]$, also die x aus $\mathbb{Q}[\sqrt[3]{2}]$ mit Koeffizienten $a, b, c \in \mathbb{Z}$. Der Koeffizient c sei im Weiteren der $\sqrt[3]{4}$-Koeffizient von x genannt.

2 McCallums Beweis des Spezialfalls

Zu McCallums Beweis benötigen wir noch zwei kurze Hilfssätze, von denen sich der zweite als der eigentlich interessante in diesem Vortrag herausstellt.

Lemma 2.1 *Die Einheitengruppe von $\mathbb{Z}[\sqrt[3]{2}]$ wird erzeugt von -1 und $\sqrt[3]{2}-1$.*

Eine Beweisskizze findet sich bei Schoof [2008] S. 20, als Übung 4.4.

Proposition 2.2 *Sei $n \in \mathbb{Z}$ und η die Einheit $\sqrt[3]{2}-1$. Der $\sqrt[3]{4}$-Koeffizient von η^n ist genau dann gleich Null, wenn $n \in \{0,1\}$.*

Beweis Das Inverse von η ist mit $\vartheta = 1+\sqrt[3]{2}+\sqrt[3]{4}$ gegeben. Die Zahlen 1, $\sqrt[3]{2}$ und $\sqrt[3]{4}$ sind linear unabhängig über $\mathbb{Q}$. Mit Induktionsanfang ϑ und Induktionsschritt

$$\begin{aligned}\vartheta^{m+1} &= \vartheta^m \cdot \vartheta = \left(a+b\sqrt[3]{2}+c\sqrt[3]{4}\right)\cdot\left(1+\sqrt[3]{2}+\sqrt[3]{4}\right)\\ &= \underbrace{(a+2b+2c)}_{>0} + \underbrace{(a+b+2c)}_{>0}\sqrt[3]{2} + \underbrace{(a+b+c)}_{>0}\sqrt[3]{4}\end{aligned}$$

sieht man, dass die Koeffizienten von ϑ^m bezüglich der Basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ für $m>0$ alle positiv sind. Damit wird der $\sqrt[3]{4}$-Koeffizient von η^n für negative n niemals Null.

Sei also jetzt $n \geq 0$. Wir betrachten $p = 1+\sqrt[3]{2}$. Wegen $p^3 = 3+3\sqrt[3]{2}+3\sqrt[3]{4} \in 3\mathbb{Z}[\sqrt[3]{2}]$ liegt für $k \geq 0$ die Potenz p^k und damit ihr $\sqrt[3]{4}$-Koeffizient in $3^{\lfloor \frac{k}{3} \rfloor}\mathbb{Z}[\sqrt[3]{2}]$. Dieser sei im Weiteren mit c_k, die beiden anderen in natürlicher Reihenfolge mit a_k bzw. b_k, bezeichnet.

Es ist hilfreich, dass der $\sqrt[3]{4}$-Koeffizient von $\eta^n = (\sqrt[3]{2}-1)^n = (-2+p)^n$ genau dann verschwindet, wenn der von $\left(-\frac{\eta}{2}\right)^n = \left(1-\frac{p}{2}\right)^n$ verschwindet. Für jedes $n \in \mathbb{N}$ haben wir die binomische Formel

$$\left(-\frac{\eta}{2}\right)^n = \left(1-\frac{p}{2}\right)^n = \sum_{k=0}^{n}\binom{n}{k}\left(-\frac{p}{2}\right)^k$$

Der $\sqrt[3]{4}$-Koeffizient von $\left(-\frac{\eta}{2}\right)^n$ hängt nur von den $\sqrt[3]{4}$-Koeffizienten der Summanden in der obigen Summe ab. Der $\sqrt[3]{4}$-Koeffizient von η^n verschwindet also genau dann, wenn

$$0 = \sum_{k=0}^{n}\binom{n}{k}\left(-\frac{1}{2}\right)^k c_k$$

ist. Wegen $c_0 = c_1 = 0$ verschwinden die ersten beiden Summanden. Sei also $n \geq 2$. Nach Division durch $n(n-1)$ erhalten wir mit $\frac{1}{n(n-1)}\binom{n}{k} = \frac{1}{k(k-1)}\binom{n-2}{k-2}$ die Gleichung

$$0 = \sum_{k=2}^{n}\frac{1}{k(k-1)}\binom{n-2}{k-2}\left(-\frac{1}{2}\right)^k c_k.$$

Es wurde schon gezeigt, dass c_k ein Vielfaches von $3^{\lfloor \frac{3}{k} \rfloor}$ ist. Wegen $\nu_3(3^l) = l < 3^{l-1}$ für $l > 1$ ist für $k \geq 5$ die 3-Bewertung von $k(k-1)$ streng kleiner als $\left\lfloor \frac{k}{3} \right\rfloor$. Damit sind alle Summanden mit $k \geq 5$ Vielfache von 3.

Mit den Koeffizienten

$$\begin{aligned} c_2 &= c_1 + b_1 = 1 \\ c_3 &= c_2 + b_2 = c_2 + b_1 + a_1 = 1 + 1 + 1 = 3 \\ c_4 &= c_3 + b_3 = c_3 + b_2 + a_2 = c_3 + b_1 + a_1 + a_1 + 2c_1 = 3 + 1 + 1 + 1 + 0 = 6 \end{aligned}$$

und $\frac{1}{2} \equiv 2 \pmod 3$ ergibt sich unter dem Moduloskop modulo 3

$$\begin{aligned} 0 &\equiv \frac{1}{2}\left(-\frac{1}{2}\right)^2 + \frac{1}{2 \cdot 3}(n-2)\left(-\frac{1}{2}\right)^3 3 + \frac{1}{3 \cdot 4}\frac{(n-2)(n-3)}{2}\left(-\frac{1}{2}\right)^4 6 \pmod 3 \\ &\equiv -1 - (n+1) + (n+1)n \pmod 3 \\ &\equiv n^2 + 1 \pmod 3. \end{aligned}$$

Dies ist aber für kein n erfüllt. So kann es also kein $n \geq 2$ geben, für das der $\sqrt[3]{4}$-Koeffizient von η^n gleich Null ist. □

Jetzt haben wir alle Mittel in der Hand, um McCallums Beweis nachzuvollziehen.

Satz 2.3 *In $\mathbb{Z}$ sind $(x, y) = (\pm 3, 2)$ die einzigen nichttrivialen Lösungen der Gleichung*

$$x^2 - y^3 = 1.$$

Beweis Sei $x, y \in \mathbb{Z} \setminus \{0\}$ eine Lösung der Gleichung $x^2 - y^3 = 1$. Dann haben wir

$$(x-1)(x+1) = y^3. \tag{1}$$

Angenommen x sei gerade. Dann sind die Faktoren auf der linken Seite teilerfremd, und es gibt $u, v \in \mathbb{Z}$ mit $x - 1 = u^3$ und $x + 1 = v^3$. Damit haben wir $v^3 - u^3 = 2$. Mit $v^3 - (v-1)^3 = 3 \cdot \left(v^2 - v + \frac{1}{3}\right) \geq 7$ für $v \leq -1$ und $v \geq 2$ erkennt man, dass u und v verschiedene Vorzeichen haben müssen und daher $v = 1$ und $u = -1$ sein muss. Das bedeutet aber, dass $x = 0$ ist.

Sei also x ungerade. Durch geeignete Wahl des Vorzeichens sichern wir uns $x \equiv 1 \pmod 4$. Teilen wir (1) durch 8, so erhalten wir

$$\frac{x-1}{4}\frac{x+1}{2} = \left(\frac{y}{2}\right)^3.$$

Wieder sind die Faktoren auf der linken Seite teilerfremd, und wir erhalten

$$\frac{x-1}{4} = u^3 \qquad \text{und} \qquad \frac{x+1}{2} = v^3,$$

für gewisse $u, v \in \mathbb{Z}$. Es ist

$$v^3 - 2u^3 = 1.$$

Die Zahl $\epsilon = v - u\sqrt[3]{2}$ hat also die Norm $\mathcal{N}_{\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}}(\epsilon) = 1$. Nach Lemma 2.1 wissen wir, dass $\epsilon = \pm\eta^n$, mit $\eta = \sqrt[3]{2} - 1$ ist. Da η ebenfalls die Norm 1 besitzt, muss wegen der Gleichheit $\mathcal{N}(a \cdot b) = \mathcal{N}(a) \cdot \mathcal{N}(b)$ sogar $\epsilon = +\eta^n$ sein. Da der $\sqrt[3]{4}$-Koeffizient von ϵ verschwindet, liefert die Proposition

$$v - u\sqrt[3]{2} = 1 \qquad \text{oder} \qquad v - u\sqrt[3]{2} = \sqrt[3]{2} - 1.$$

Im ersten Fall haben $u = 0$ und damit $y = 0$, also die triviale Lösung. Im zweiten Fall erhalten wir $u = v = -1$ und damit $x = -3$ und $y = 2$, so dass $x = \pm 3$, $y = 2$ die einzigen nichttrivialen Lösungen in $\mathbb{N}$ der Gleichung

$$x^2 - y^3 = 1$$

sind. □

Literatur

Siegfried Bosch. *Algebra.* Springer, Berlin, 6. Auflage, 2006. ISBN 978-3-540-29880-9.

René Schoof. *Catalan's Conjecture.* Springer, London, 1. Auflage, 2008. ISBN 978-1-84400-184-8.