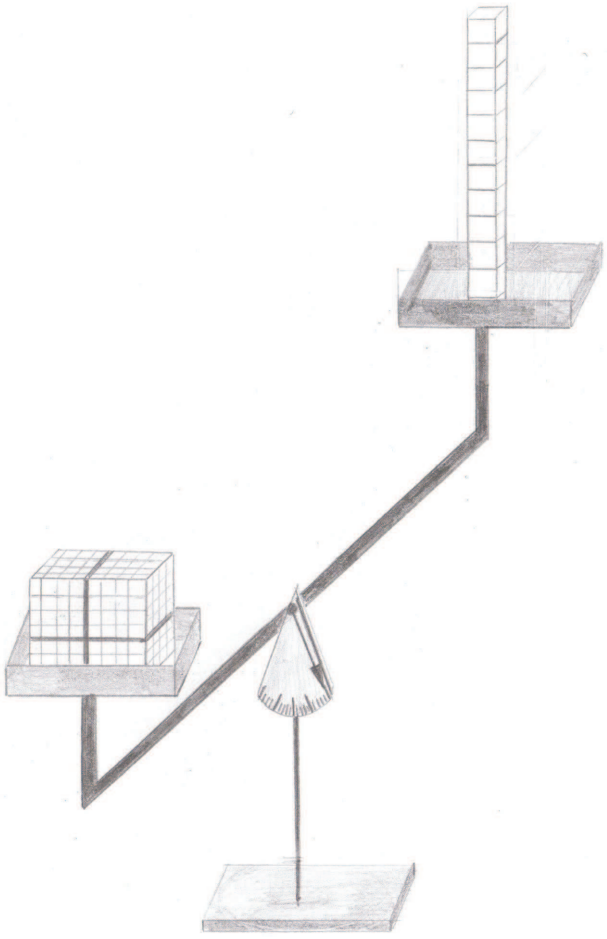
Ausarbeitung zum Vortrag im Seminar
der WE A$\ell$ZAGK zur

Catalanschen Vermutung

# Das Minus-Argument

von Hüseyin Özoguz

WS 08/09 in Bremen



# Einleitung

Diese Ausarbeitung stellt den Beweis von Theorem III aus Kapitel 11 von [1] dar.[1] Es konstatiert $p < 4q^2$ und $q < 4p^2$ für jede nichttriviale[2] Lösung $(x,y,p,q)$, mit $x,y \in \mathbb{Z}$ und $p,q$ prim, der Catalanschen Gleichung $x^p - y^q = 1$. In dem abschließenden Beweis der Catalanschen Vermutung folgt aus der Existenzannahme einer nichttrivialen Lösung mit $p,q \geq 3$ mit Theorem I und Theorem II schließlich $p = 1 + kq^2$ für ein $k \in \mathbb{N}$. Aus Theorem III folgt dann $k \in \{1,2,3\}$, und weil $p$ prim ist, bleibt nur $k = 2$. Nun ist 3 ein Teiler von $p = 1 + 2q^2 > 3$ für alle Primzahlen $q \neq 3$. Es bleibt $q = 3$ - im Widerspruch zu Theorem IV.

**Konventionen**
Das Quadrupel $(x,y,p,q) \in \mathbb{Z}^4$, mit $x,y \neq 0$ und $p,q$ prim,
sei eine Lösung der Catalanschen Gleichung.
$\zeta_p \in \mathbb{C}$ - primitive $p$-te Einheitswurzel
$G := Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$
$I := (1-\iota)S$ - wobei $S$ das Stickelberger Ideal ist
und $\iota \in G$ die komplexe Konjugation bezeichnet

**Beweisgang**
Das Ideal $I$ ist das Hauptobjekt des Beweises - daher die Kapitelüberschrift. Nach einer Betragsdefinition für Elemente aus $\theta \in \mathbb{Z}[G]$ zeigen kurze analytische und kombinatorische Argumente die Existenz von vielen $\theta$ aus $I$ mit kleinem Betrag - zu viele, um einem Widerspruch unter der Annahme $q > 4p^2$ zu entgehen.

Alle Verweise auf anderen Sätze/Lemmata beziehen sich auf [1]. Zwei Beweise wurden der Übersichtlichkeit wegen in den Anhang ausgelagert.

[1] bis auf einige unwesentliche Modifikationen
[2] d.h. $x,y \neq 0$

# Das Minus-Argument

**Lemma 11.1**
Die Abbildung $\varphi : \{\theta \in \mathbb{Z}[G] : (x-\zeta_p)^\theta \in \mathbb{Q}(\zeta_p)^{*q}\} \to \mathbb{Q}(\zeta_p)^*$ mit $\varphi(\theta) = \alpha$ für $\alpha^q = (x-\zeta_p)^\theta$ ist ein Monomorphismus.

*Beweis.* Für alle $\theta \in \text{domain}(\varphi)$ ist $\alpha \in \mathbb{Q}(\zeta_p)^*$ eindeutig bestimmt, denn sei $\beta \in \mathbb{Q}(\zeta_p)^*$ mit $\varphi(\theta) = \alpha^q = \beta^q$, also $(\frac{\alpha}{\beta})^q = 1$. Wegen $\mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$ und $q \geq 3$ gibt es in $\mathbb{Q}(\zeta_p)$ keine nichttrivialen $q$-ten Einheitswurzeln, also ist $\alpha = \beta$ und $\varphi$ wohldefiniert. Die Homomorphie von $\varphi$ ist trivial, bleibt die Injektivität zu zeigen:

Sei dafür $\theta = \sum_{\sigma \in G} n_\sigma \sigma \in \ker\varphi$, also $(x-\zeta_p)^\theta = \prod_{\sigma\in G}(x-\sigma(\zeta_p))^{n_\sigma} = 1$. Seien $\mu_1, \mu_2 \in G$ verschieden und $k_1, k_2 \in \{1, ..., p-1\}$ mit $\mu_1(\zeta_p) = {\zeta_p}^{k_1}$, $\mu_2(\zeta_p) = {\zeta_p}^{k_2}$. Sei oE $k_1 \geq k_2$, dann ist

$$(x-\mu_1(\zeta_p)) - (x-\mu_2(\zeta_p)) = {\zeta_p}^{k_2} - {\zeta_p}^{k_1} = (1-\zeta_p){\zeta_p}^{k_2} \sum_{i=0}^{k_1-k_2-1} {\zeta_p}^i.$$

Demnach haben die Ideale $(x-\sigma(\zeta_p))$ $(\sigma \in G)$ höchstens $(1-\zeta_p)$ als gemeinsamen Faktor. Nach Korollar 6.5 ist $x \equiv 1 \pmod p$, also haben die Ideale $(x-\sigma(\zeta_p))$ genau den Faktor $(1-\zeta_p)$ gemeinsam. Demnach sind die von $\frac{x-\sigma(\zeta_p)}{1-\zeta_p}$ erzeugten Ideale paarweise teilerfremd, wir betrachten deren Normen. Nach Korollar 6.5(iii) ist $|x| \geq q^{p-1}+q$, also $|x-\sigma(\zeta_p)| > q^{p-1}$ für alle $\sigma \in G$ und damit a fortiori
$N(x-\sigma(\zeta_p)) \geq q^{p-1} > p = N(1-\zeta_p)$, also $N\left(\frac{x-\sigma(\zeta_p)}{1-\zeta_p}\right)$>1. D.h. für jedes $\sigma \in G$ besitzt das Ideal $(x-\sigma(\zeta_p))$ einen von $(1-\zeta_p)$ verschiedenen Primfaktor, der keines der übrigen Ideale teilt. Also ist $\prod_{\sigma\in G}(x-\sigma(\zeta_p))^{n_\sigma} \neq 1$, falls ein $n_\sigma \neq 0$ ist, und der Kern von $\varphi$ ist trivial. □

**Definition**
Der Betrag von $\theta = \sum_{\sigma\in G} n_\sigma\sigma \in \mathbb{Z}[G]$ sei definiert durch $||\theta|| := \sum_{\sigma\in G} |n_\sigma|$.

**Satz 11.2**
Für alle $\theta \in (1-\iota) \subset \mathbb{Z}[G]$ und $\alpha \in \mathbb{Q}(\zeta_p)^*$ mit $(x-\zeta_p)^\theta = \alpha^q$ und jede Einbettung $\phi : \mathbb{Q}(\zeta_p) \to \mathbb{C}$ ist $|\phi(\alpha)| = 1$, und es gibt eine $q$-te Einheitswurzel $\xi \in \mathbb{C}$ mit $|\phi(\alpha) - \xi| \leq \frac{||\theta||}{q(|x|-1)}$.

*Beweis.* Die Betragsbildung ist unter jeder Einbettung und unter der komplexen Konjugation invariant. Wegen $\theta \in (1-\iota)$ ist $|(x-\zeta_p)^\theta| = 1$, also ist

$$1 = |\phi(\alpha^q)| = |\phi(\alpha)|^q = |\phi(\alpha)|.$$

Es folgt die Konstruktion von $\xi$:
Jedes $z \in \mathbb{C} \setminus \mathbb{R}_{\leq 0}$ lässt sich eindeutig darstellen als $z = re^{i\operatorname{Arg}(z)}$ mit $r \in \mathbb{R}_+$ und $\operatorname{Arg}(z) \in (-\pi, \pi)$, also ist $|\operatorname{Arg}(z)|$ die kürzeste Bogenlänge auf dem Einheitskreis zwischen 1 und $\frac{z}{|z|}$. Der Hauptwert des natürlichen Logarithmus ist dann gegeben durch $\ln(re^{i\operatorname{Arg}(z)}) = \ln(r) + i\operatorname{Arg}(z)$.

Es gilt $|\ln(z_1 z_2)| \leq |\ln(z_1)| + |\ln(z_2)|$ für alle $z_1, z_2, z_1 z_2 \in \mathbb{C} \setminus \mathbb{R}_{\leq 0}$:
Es ist $\operatorname{Re}(\ln(z_1 z_2)) = \operatorname{Re}(\ln(z_1) + \ln(z_2))$, es genügt also
$|\operatorname{Arg}(z_1 z_2)| \leq |\operatorname{Arg}(z_1) + \operatorname{Arg}(z_2)|$ zu zeigen. Es gibt genau
ein $k \in \{-1, 0, 1\}$, s.d. $(\operatorname{Arg}(z_1) + \operatorname{Arg}(z_2) + 2\pi k) \in (-\pi, \pi)$ ist, also ist

$$\operatorname{Arg}(z_1 z_2) = \operatorname{Arg}(z_1) + \operatorname{Arg}(z_2) + 2\pi k$$

und folglich $|\operatorname{Arg}(z_1 z_2) - 2\pi k| = |\operatorname{Arg}(z_1) + \operatorname{Arg}(z_2)|$. Also ist

$$|\operatorname{Arg}(z_1 z_2)| \leq |\operatorname{Arg}(z_1 z_2) - 2\pi k| = |\operatorname{Arg}(z_1) + \operatorname{Arg}(z_2)|.$$

Demnach ist $|\operatorname{Im}(\ln(z_1 z_2))| \leq |\operatorname{Im}(\ln(z_1) + \ln(z_2))|$, also ist

$$|\ln(z_1 z_2)| \leq |\ln(z_1) + \ln(z_2)| \leq |\ln(z_1)| + |\ln(z_2)|.$$

Wegen $x^\theta = 1$ ist $\alpha^q = (x - \zeta_p)^\theta = (1 - \frac{\zeta_p}{x})^\theta$, und wegen $|\frac{\zeta_p}{x}| < 1$ können wir die Taylorentwicklung des Logarithmus benutzen:

$$\begin{aligned}
|\operatorname{Arg}(\phi(\alpha)^q) = |\ln(\phi(\alpha)^q)| &= \left|\ln\left(\phi\left(\left(1 - \frac{\zeta_p}{x}\right)^\theta\right)\right)\right| = \left|\ln\left(\left(1 - \frac{\phi(\zeta_p)}{x}\right)^\theta\right)\right| \\
&\leq \sum_{\sigma \in G} |n_\sigma| \left|\ln\left(1 - \frac{\sigma(\phi(\zeta_p))}{x}\right)\right| = \sum_{\sigma \in G} |n_\sigma| \left|\sum_{m=1} -\frac{1}{m}\left(\frac{\sigma(\phi(\zeta_p))}{x}\right)^m\right| \\
&\leq \sum_{\sigma \in G} |n_\sigma| \sum_{m=1} \frac{1}{|x|^m} = \frac{||\theta||}{|x| - 1}
\end{aligned}$$

Es ist $\operatorname{Arg}(\phi(\alpha)^q)$ gerade gleich $q\operatorname{Arg}(\phi(\alpha))$ modulo $2\pi$. Demnach gibt es ein $k \in \mathbb{Z}$ mit $|\operatorname{Arg}(\phi(\alpha)^q)| = |q\operatorname{Arg}(\phi(\alpha)) - 2\pi k|$, also $|\operatorname{Arg}(\phi(\alpha)) - \frac{2\pi k}{q}| \leq \frac{||\theta||}{q(|x|-1)}$.
Setze $\xi := e^{\frac{2\pi i k}{q}}$, dann ist $|\phi(\alpha) - \xi| \leq |\operatorname{Arg}(\phi(\alpha)) - \frac{2\pi k}{q}| \leq \frac{||\theta||}{q(|x|-1)}$, weil der Bogen auf dem Einheitskreis zwischen $\phi(\alpha)$ und $\xi$ länger ist als die zugehörige Sehne. $\square$

**Aufgabe 11.3**
Es ist $\#\{(\lambda_1,...,\lambda_k) \in \mathbb{N}^k | \sum_{j=1}^k \lambda_j \leq s,\ s,k \in \mathbb{N},\ k>0\} = \binom{s+k}{s}$.
*Beweis.* Siehe Appendix. □

**Lemma 11.4**
Für alle $(k,s) \in \mathbb{N}^2 \setminus \{(2,6),(2,7),(2,8),(3,6)\}$ mit $k \geq 2,\ s \geq 6$ ist
$\binom{s+k}{s} > \frac{4}{3}(s+1)k^2+1$.
*Beweis.* Siehe Appendix. □

**Satz 11.3**
Es seien $p,q \geq 5$ Primzahlen mit $q > 4p^2$. Sei $M \subseteq I$ die Teilmenge aller Elemente, deren Betrag nicht größer als $\frac{3q}{2(p-1)}$ ist, dann ist $\#M \geq q+1$.

*Beweis.* Setze $s := \lfloor \frac{3q}{2(p-1)^2} \rfloor$. Nach Satz 9.3(ii) bilden die Elemente $e_i = (1-\iota)f_i \in I$ für $i = 1,...,\frac{p-1}{2}$ eine $\mathbb{Z}$-Basis von $I$ und nach Satz 9.4 ist die Hälfte der Koeffizienten dieser $e_i$ gleich 1, die andere Hälfte gleich $-1$. Also ist $||e_i|| = \sum_{\sigma \in G} |\pm 1| = p-1$.
Sei $U_1 := \{\theta \in I | \theta = \sum_{i=1}^{\frac{p-1}{2}} \lambda_i e_i,\ \sum_{i=1}^{\frac{p-1}{2}} \lambda_i \leq s,\ \lambda_i \in \mathbb{N}\}$. Für alle $\theta \in U_1$ ist
$||\theta|| \leq s(p-1) \leq \frac{3q}{2(p-1)}$. Nach Aufgabe 11.3 ist $\#U_1 = \binom{s+\frac{p-1}{2}}{s}$. Setze $U_2 := -U_1$, dann haben auch alle $\theta \in U_2$ die Eigenschaft $||\theta|| \leq \frac{3q}{2(p-1)}$ und es ist ebenso
$\#U_2 = \binom{s+\frac{p-1}{2}}{s}$. Es ist $U_1 \cap U_2 = \{0\}$. Also folgt mit Lemma 11.4 insgesamt
$\#M \geq \#(U_1 \cup U_2) = 2\binom{s+\frac{p-1}{2}}{s} - 1 \geq \frac{2}{3}(s+1)(p-1)^2+1 \geq q+1$.

Zu den Voraussetzungen von Lemma 11.4: Wegen $q > 4p^2$ ist $\lfloor \frac{3q}{2(p-1)^2} \rfloor \geq \frac{6p^2}{(p-1)^2} \geq 6$ und mit $p \geq 5$ ist auch $\frac{p-1}{2} \geq 2$.
Es bleibt zu zeigen, dass kein geordnetes Paar $\left(\frac{p-1}{2}, s\right)$ ein Element der Ausnahmemenge ist: Für $\frac{p-1}{2} = 2$ ist $p = 5$ und $s = \left\lfloor \frac{3q}{2(p-1)^2} \right\rfloor \geq \left\lfloor \frac{6p^2}{(p-1)^2} \right\rfloor = \lfloor \frac{150}{16} \rfloor = 9 > 8$.
Für $\frac{p-1}{2} = 3$ ist $p = 7$ und $s \geq \left\lfloor \frac{6p^2}{(p-1)^2} \right\rfloor = \lfloor \frac{294}{36} \rfloor = 8 > 6$. □

**Satz 11.5**
Es sei $q > 4p^2$. Zu jeder Einbettung $\phi : \mathbb{Q}(\zeta_p) \to \mathbb{C}$ gibt es ein $\theta \in I,\ \theta \neq 0$ mit $||\theta|| \leq \frac{3q}{p-1}$ und $(x-\zeta_p)^\theta = \alpha_\theta{}^q$ für ein $\alpha_\theta \in \mathbb{Q}(\zeta_p)^*$ und $|\phi(\alpha)-1| \leq \frac{2||\theta||}{q(|x|-1)}$.

*Beweis.* Nach Satz 7.2 ist $x-\zeta_p$ modulo $q$-ten Potenzen ein Element der Hindernisgruppe $H$. Nach Satz 10.1 annuliert $I$ die Hindernisgruppe, also ist auch $(x-\zeta_p)^\theta$ eine $q$-te Potenz für $\theta \in I$. Somit können wir Satz 11.2 anwenden, demnach gibt es für alle $\theta \in M \subset I$ eine $q$-te Einheitswurzel $\xi_\theta$ mit $|\phi(\alpha_\theta) - \xi_\theta| \leq \frac{||\theta||}{q(|x|-1)}$.

Wegen $\#M \geq q+1$ (Satz 11.3) gibt es nach dem Schubfachprinzip zwei verschiedene $\theta_1, \theta_2 \in M$ mit $\xi_{\theta_1} = \xi_{\theta_2} =: \xi$. Setze $\theta := \theta_1 - \theta_2$ und $\alpha_\theta := \frac{\alpha_{\theta_1}}{\alpha_{\theta_2}}$, dann ist $(x-\zeta_p)^\theta = {\alpha_\theta}^q$ und $\theta \neq 0$, sowie $||\theta|| = ||\theta_1 - \theta_2|| \leq ||\theta_1|| + ||\theta_2|| \leq \frac{3q}{p-1}$. Und außerdem ist

$$\begin{aligned} |\phi(\alpha_\theta) - 1| &= \left| \frac{\phi(\alpha_{\theta_1}) - \phi(\alpha_{\theta_2})}{\phi(\alpha_{\theta_2})} \right| = |\phi(\alpha_{\theta_1}) - \phi(\alpha_{\theta_2})| \\ &\leq |\phi(\alpha_{\theta_1}) - \xi| + |\phi(\alpha_{\theta_2}) - \xi| \leq \frac{2||\theta||}{q(|x|-1)} \end{aligned}$$ □

**Theorem III**
Seien $p, q \geq 3$ Primzahlen und $x, y \in \mathbb{Z}_{\neq 0}$ mit $x^p - y^q = 1$, dann ist $q < 4p^2$ und $p < 4q^2$.

*Beweis.* Nach Theorem IV können wir $p, q \geq 5$ annehmen. Wir nehmen $q > 4p^2$ oder $p > 4q^2$ an, o.E.[3] sei $q > 4p^2$. Sei $\phi : \mathbb{Q}(\zeta_p) \to \mathbb{C}$ eine Einbettung. Nach Satz 11.5 gibt es ein $\theta \in I$, $\theta \neq 0$ mit $||\theta|| \leq \frac{3q}{p-1}$, $(x-\zeta_p)^\theta = \alpha^q$ für ein $\alpha \in \mathbb{Q}(\zeta_p)^*$ und $|\phi(\alpha) - 1| \leq \frac{2||\theta||}{q(|x|-1)}$. Die Ungleichung stimmt auch für das komplex Konjugierte von $\phi(\alpha)$. Wegen $|\phi(\alpha)| = 1$ für jede Einbettung $\phi$ gilt für die übrigen $p-3$ Einbettungen $|\phi(\alpha) - 1| \leq 2$. Also gilt für die Norm des von $(\alpha - 1)$ erzeugten Ideals:

$$N(\alpha - 1) = \prod_{\sigma \in G} |\sigma(\alpha) - 1| \leq \left( \frac{2||\theta||}{q(|x|-1)} \right)^2 \cdot 2^{p-3} = \frac{2^{p-1}||\theta||^2}{q^2(|x|-1)^2}$$

Als nächstes schätzen wir $N(\alpha - 1)$ nach unten ab. Nach Satz 10.1 ist $I \subset \text{domain}(\varphi)$ für die Abbildung $\varphi$ aus Lemma 11.1 und wegen $\theta \neq 0$ ist auch $\alpha - 1 \neq 0$. Also gibt es eindeutig bestimmte teilerfremde ganze Ideale $\tilde{J}, J \subset \mathbb{Z}[\zeta_p]$ mit $(\alpha - 1) = \tilde{J}/J$. Weil $J(\alpha - 1)$ ein ganzes Ideal ist, ist auch $J(\alpha)$ ganz, d.h. es gibt ein ganzes Ideal $J'$, so dass $J'$, $J$ teilerfremd sind und $(\alpha) = J'/J$.
Dann ist $(\alpha)^q = (x-\zeta_p)^\theta = \prod_{\sigma \in G} (x - \sigma(\zeta_p))^{n_\sigma} = {J'}^q / J^q$.
Wegen $N((x-\zeta_p)^\theta) = 1$ ist $N(J') = N(J)$ und außerdem folgt durch Hochziehen der Nennerfaktoren $\prod_{\sigma \in G} (x - \sigma(\zeta_p))^{|n_\sigma|} = {J'}^q J^q$. Damit ist

$$\begin{aligned} N(J)^{2q} = N(J'J)^q &= N\left( \prod_{\sigma \in G} (x - \sigma(\zeta_p))^{|n_\sigma|} \right) \\ &\leq \prod_{\sigma \in G} \prod_{\sigma \in G} |x - \sigma(\zeta_p)|^{|n_\sigma|} \\ &\leq \prod_{\sigma \in G} (|x|+1)^{||\theta||} = (|x|+1)^{(p-1)||\theta||} \end{aligned}$$

[3] Für ungerade $p, q$ ist mit $(x, y, p, q)$ auch $(-y, -x, q, p)$ eine Catalansche Lösung. Falls es also eine Lösung mit $q > 4p^2$ gibt, so auch eine mit $p > 4q^2$ und umgekehrt.

wegen $|x|+1 \geq |x-c|$ für alle $c \in \mathbb{C}$ mit $|c| = 1$. Und folglich ist $N(J) \leq (|x|+1)^{\frac{(p-1)||\theta||}{2q}}$. Außerdem ist $J(\alpha-1)$ ein ganzes Ideal ungleich 0, also ist $N(J)^{-1} \leq N(\alpha-1)$. Durch Verbinden beider Abschätzungen für $N(\alpha-1)$ ergibt sich insgesamt

$$(|x|+1)^{-\frac{(p-1)||\theta||}{2q}} \leq N(J)^{-1} \leq N(\alpha-1) \leq \frac{2^{p-1}\,||\theta||^2}{q^2(|x|-1)^2}.$$

Wegen $|x| \overset{\geq}{} q^{p-1} \geq 7$ gilt $|x|+1 \leq \frac{4}{3}(|x|-1)$ und damit $(|x|+1)^{2-\frac{p-1}{2q}||\theta||} \leq \frac{16||\theta||^2}{9q^2}2^{p-1}$. Nun ist $||\theta|| \leq \frac{3q}{p-1}$ und es bleibt $(|x|+1)^{\frac{1}{2}} \leq \frac{16}{(p-1)^2}2^{p-1}$. Und schließlich folgt wegen $|x|+1 > q^{p-1}$ und $p \geq 5$ die Ungleichung $q^{\frac{p-1}{2}} \leq 2^{p-1}$ bzw. $\sqrt{q} \leq 2$, im Widerspruch zur Voraussetzung $q \geq 5$. Es ist demnach $q < 4p^2$. □

# Appendix

## Norm eines Ideals

Hier seien nur die notwendigsten Eigenschaften aufgezählt, eine Einführung findet sich z.B. in [3].
Sei $I \subseteq \mathbb{Z}[\zeta_p]$ ein Ideal. Die Norm von $I \neq 0$ sei definiert durch $N(I) := [\mathbb{Z}[\zeta_p] : I]$, das Nullideal habe die Norm 0. Diese Normsetzung ist mit der Norm von erzeugenden Elementen verträglich: Sei $I$ ein Hauptideal $I = (\alpha)$, dann ist $N(I) = |N(\alpha)|$.
Die Norm ist multiplikativ und für jedes ganze Ideal $I \neq 0$ ist $N(I) \geq 1$.

**Aufgabe 11.3**
Für $A := \{(\lambda_1, ..., \lambda_k) \in \mathbb{N}^k | \sum_{j=1}^k \lambda_j \leq s,\ s,k \geq 1\}$ ist $\#A = \binom{s+k}{s}$.

*Beweis.* Wir zeigen: Jede $k$-elementige Teilmenge $\{n_i\}_{i=1,...,k}$ der Menge $\{1, ..., s+k\}$ bestimmt eindeutig ein $k$-Tupel aus $A$ und umgekehrt, wobei $n_i < n_{i+1}$ für alle $i = 1, ..., k-1$ sei.

Sei $\{n_i\}_{i=1,...,k}$ eine $k$-elementige Teilmenge von $\{1, ..., s+k\}$. Wir setzen $n_0 := 0$ und definieren rekursiv $\lambda_i = n_i - n_{i-1} - 1$ für $i = 1, ..., k$. Dann ist $\lambda_i \geq 0$. Weiter ist $\sum_{i=1}^k \lambda_i = \sum_{i=1}^k (n_i - n_{i-1} - 1) = n_k - k$ und wegen $n_k \leq s + k$ ist $\sum_{i=1}^k \lambda_i \leq s$, also ist $(\lambda_1, ..., \lambda_k) \in A$. Zwei verschiedene $k$-elementige Teilmenge von $\{1, ..., s+k\}$ bestimmen nach dieser Vorschrift offensichtlich zwei verschiedene $k$-Tupel von $A$.
Es sei umgekehrt $(\lambda_1, ..., \lambda_k) \in A$. Wir setzen $n_i = \sum_{j=1}^i (\lambda_i + 1)$ für $i = 1, ..., k$. Dann ist $n_i < n_{i+1}$ für $i = 1, ..., k-1$. Wegen $\sum_{j=1}^k \lambda_i \leq s$ ist $n_k \leq s + k$ und damit ist $\{n_i\}_{i=1,...,k}$ eine $k$-elementige Teilmenge von $\{1, ..., s+k\}$. Verschiedene $k$-Tupel aus $A$ bestimmen offensichtlich verschiedene $k$-elementige Teilmengen von $\{1, ..., s+k\}$.

Es gibt $\binom{s+k}{k}$ $k$-elementige Teilmengen von $\{1, ..., s+k\}$, also ist $\#A = \binom{s+k}{k} = \binom{s+k}{s}$.□

**Lemma 11.4**
Für alle $(k,s) \in \mathbb{N}^2 \setminus \{(2,6), (2,7), (2,8), (3,6)\}$ mit $k \geq 2, s \geq 6$ ist $\binom{s+k}{s} > \frac{4}{3}(s+1)k^2 + 1$.

*Beweis.* (vgl. S.45 in [2]) Der Beweis ist eine doppelte Induktion $\langle k \mapsto k+1 \rangle$ und $\langle s \mapsto s+1 \rangle$. Um der Ausnahmemenge zu entgehen, setzen wir die Induktionsanker bei $(k,s) = (2,9), (4,6), (3,7)$ an. Für $(k,s) = (2,9)$ ist $\binom{9+2}{2} = 55 > \frac{163}{3} = \frac{4}{3}(9+1)2^2 + 1$, für $(k,s) = (4,6)$ ist $\binom{6+4}{4} = 210 > \frac{451}{3} = \frac{4}{3}(6+1)4^2 + 1$ und für $(k,s) = (3,7)$ ist

$\binom{7+3}{3} = 120 > 97 = \frac{4}{3}(7+1)3^2+1$.

Induktionsschritt $\langle k \mapsto k+1 \rangle$:

$$\binom{s+k+1}{k+1} = \frac{s+k+1}{k+1}\binom{s+k}{k} > \frac{4(s+k+1)(s+1)k^2}{3(k+1)} + 1$$

Für alle $k \geq 2$ gilt $(5+k)k^2 > (k+1)^3$: Dazu sei die Abbildung $f : \mathbb{R} \to \mathbb{R}$ durch $x \mapsto x^2 - \frac{3}{2}x - \frac{1}{2}$ definiert, sie besitzt genau die beiden Nullstellen $n_0 := \frac{3-\sqrt{17}}{4}$ und $n_1 := \frac{3+\sqrt{17}}{4}$, wobei $n_0 < n_1 < 2$ ist. Es ist $f(2) = \frac{1}{2} > 0$, also gilt $f(x) > 0$ für alle $x \in (n_1, \infty)$, insbesondere für alle $x \geq 2$. Weiterhin folgt

$$\begin{aligned} x^2 - \frac{3}{2}x - \frac{1}{2} > 0 &\Rightarrow 2x^2 - 3x - 1 > 0 \\ &\Rightarrow x^3 + 5x^2 = (5+x)x^2 > x^3 + 3x^2 + 3x + 1 = (x+1)^3. \end{aligned}$$

Wegen $s \geq 4$ und $k \geq 2$ ist $(s+k+1)k^2 \geq (5+k)k^2 > (k+1)^3$. Also ist $\frac{(s+k+1)k^2}{k+1} > (k+1)^2$ und somit $\frac{4(s+k+1)(s+1)k^2}{3(k+1)} + 1 > \frac{4}{3}(s+1)(k+1)^2 + 1$.

Induktionsschritt $\langle s \mapsto s+1 \rangle$:

$$\begin{aligned} \binom{s+1+k}{k} = \frac{s+1+k}{s+1}\binom{s+k}{k} &> \frac{4(s+k+1)(s+1)k^2}{3(s+1)} + 1 \\ &= \frac{4}{3}(s+k+1)k^2 + 1 > \frac{4}{3}(s+2)k^2 + 1 \end{aligned}$$

□

# Literatur


[1] René Schoof. *Catalan's Conjecture*, Springer, 2008.

[2] Jeanine Daems. *A Cyclomatic Proof of Catalan's Conjecture*, Masterarbeit, Universität Leiden, 2003.

[3] Jürgen Neukirch. *Algebraische Zahlentheorie*, Springer, 2007 (unv. Nachdruck des Erstdrucks von 1992).