Potenzsummen von ganzen Zahlen und Polynomen

Teilnehmer:

André Stenzel	Heinrich-Hertz-Oberschule
Christian Rekittke	Andreas-Oberschule
Jana Schulz	Andreas-Oberschule
Jannis Hessel	Herder-Oberschule
Konrad Steiner	Heinrich-Hertz-Oberschule
Pascal Gussmann	Heinrich-Hertz-Oberschule
Robert Altmann	Heinrich-Hertz-Oberschule

Gruppenleiter:

Olaf Teschke	Humboldt-Universität zu Berlin

Die Gruppe beschäftigte sich mit klassischen zahlentheoretischen Problemen über den ganzen Zahlen und ihrer Variante über Polynomringen. Als Motivation wurde zunächst die scheinbar einfache Gleichung $a+b=c$ betrachtet. Es stellte sich heraus, dass sich im Falle von komplexen Polynomen eine starke Aussage über die Anzahl der verschiedenen vorhandenen Nullstellen machen lässt (Satz von Mason), die weitgehende Folgerungen impliziert. So kann zum Beispiel elementar und elegant der „Satz von Fermat für Polynome“ bewiesen werden.
Auf der Suche nach vergleichbaren Resultaten in $\mathbb{Z}$ stößt man auf die *abc* - Vermutung, aus der man ebenfalls die Unlösbarkeit einer Reihe von bekannten Gleichungen folgern könnte.
Danach wurde das Problem der Darstellbarkeit von Zahlen und Polynomen als Summen von Potenzen untersucht. Mit klassischen Methoden wurden der zwei-Quadrate-Satz und der vier-Quadrate-Satz von Lagrange bewiesen und das analoge Problem für höhere Potenzen (Waring-Problem) diskutiert. Für Polynome stellt sich heraus, dass dieses Problem eine anschauliche geometrische Interpretation besitzt und auf eine Frage über Sekantenvarietäten zurückgeführt werden kann. Eine Dimensionsbestimmung liefert dann ein umfassendes Resultat.

1 $a + b = c$

Im ersten Teil beschäftigen wir uns mit Gleichungen der Form $a+b=c$ und stellen fest, dass damit starke Einschränkungen für die Zahl der verschiedenen Primfaktoren von $a \cdot b \cdot c$ verbunden sind. Für Polynome werden wir eine erstaunliche Abschätzung überraschend elementar beweisen und daraus z.B. den Satz von Fermat für Polynome folgern.

1.1 Der Satz von Mason und Satz von Fermat für Polynome

1.1.1 Grundlegende Begriffe

Es sei $f \in \mathbb{C}[x]$, d.h. f ist ein Polynom mit komplexen Koeffizienten. Nach dem Fundamentalsatz der Algebra zerfällt es in ein Produkt von Linearfaktoren

$$f(x) = c \cdot \prod_{i=1}^{m} (x - \alpha_i).$$

Dies lässt sich auch schreiben als

$$f(x) = c \cdot \prod_{i=1}^{r} (x - \alpha_i)^{m_i},$$

dabei ist m_i die Vielfachheit der Nullstelle β_i. Der Grad des Polynoms $\deg(f)$ ergibt sich dann als

$$\deg(f) = \sum_{i=1}^{r} m_i.$$

Wir schreiben weiterhin $n_0(f)$ für die Anzahl der verschiedenen Nullstellen

$$n_0(f) := r.$$

Damit gilt natürlich $n_0(f) \leq \deg(f)$. Andererseits können beide Zahlen natürlich erheblich differieren, z.B. hat $(x-1)^{1001}$ einen hohen Grad, aber $n_0 = 1$. Ziel ist es, unter bestimmten Voraussetzungen auch eine Abschätzung in die andere Richtung zu erhalten.

1.1.2 Hilfsätze

Der ggt (größter gemeinsamer Teiler) von Polynomen ist das Produkt aller gemeinsamen Primfaktoren, in unserem Fall (da ja komplexe Polynome immer eine Nullstelle haben) der gemeinsamen Linearfaktoren.

Lemma 1.1. *Sei f aus $\mathbb{C}[x]$, dann gilt* $\deg[\mathrm{ggt}(f, f')] = \deg(f) - n_0(f)$.

Beweis: Sei α_i eine Nullstelle von f mit Vielfachheit m_i. Dann ist

$$f = (x - \alpha_i)^{m_i} \cdot g, \quad x - \alpha_i \nmid g$$

$$f' = m_i \cdot (x - \alpha_i)^{m_i - 1} \cdot g + (x - \alpha_i) \cdot g'$$

$$f' = (x - \alpha_i)^{m_i - 1} \cdot [m_i \cdot g + (x - \alpha_i) \cdot g']$$

Offensichtlich gilt also:

$$(x - \alpha_i)^{m_i - 1} \nmid m_i \cdot g + (x - \alpha_i) \cdot g'$$

Jeder Linearfaktor $(x - \alpha_i)$ kommt also in der Linearfaktorzerlegung von f' genau $m_i - 1$ mal vor.

$$\Rightarrow \deg[\mathrm{ggt}(f, f')] = (m_1 - 1) + (m_2 - 1) + ... + (m_r - 1)$$

$$\Rightarrow \deg[\mathrm{ggt}(f, f')] = \sum_{i=1}^{r} (m_i - 1) = -r + \sum_{i=1}^{r} m_i = \deg(f) - n_0(f)$$

Lemma 1.2. *Seien f, g aus $\mathbb{C}[x]$, dann gilt:*

$$n_0(f \cdot g) \leq n_0(f) + n_0(g)$$

Die Gleichheit gilt genau dann, wenn der ggt *von f und g gleich* 1 *ist.*

1.1.3 Satz von Mason - Beweis nach der Variante von Noah Snyder(2000)

Satz 1.3 (Mason 1983)**.**

$$\max\{\deg(f), \deg(g), \deg(h)\} \leq n_o(f \cdot g \cdot h) - 1$$

Beweis (nach der Variante von Noah Snyder, 2000): Wir benutzen die einfache Identität

$$\begin{aligned} f \cdot g' - f' \cdot g &= f \cdot g' + f \cdot f' - f \cdot f' - f' \cdot g \\ &= f(g' + f') - f'(f + g) = f \cdot h' - f' \cdot h. \end{aligned}$$

Es sind $f \cdot g' \neq 0$ und $f' \cdot g \neq 0$, da f und g nicht konstant sind. Außerdem gilt $f \cdot g' - f' \cdot g \neq 0$, da sonst f das Produkt $f' \cdot g$ teilen würde. Da f und g teilerfremd sind, müßte $f \mid f'$ gelten, was schon wegen des kleineren Grades unmöglich ist.

Nun gilt:

$$\begin{aligned} \operatorname{ggt}(f, f') &\mid f \cdot g' - f' \cdot g \\ \operatorname{ggt}(g, g') &\mid f \cdot g' - f' \cdot g \\ \operatorname{ggt}(h, h') &\mid f \cdot g' - f' \cdot g \end{aligned}$$

Da f, g, h paarweise teilerfremd sind, gilt:

$$\begin{aligned} &\operatorname{ggt}(f, f') \cdot \operatorname{ggt}(g, g') \cdot \operatorname{ggt}(h, h') \mid f \cdot g' - f' \cdot g \\ \Rightarrow\ &\deg[\operatorname{ggt}(f, f') \cdot \operatorname{ggt}(g, g') \cdot \operatorname{ggt}(h, h')] \leq \deg(f \cdot g' - f' \cdot g) \end{aligned}$$

Wir erhalten die Ungleichung

$$\begin{aligned} &\Rightarrow \deg[\operatorname{ggt}(f, f'] \cdot \operatorname{ggt}(g, g') \cdot \operatorname{ggt}(h, h')] \leq \deg(f \cdot g') = \deg(f) + \deg(g) - 1 \\ &\Rightarrow \deg[\operatorname{ggt}(f, f')] + \deg[\operatorname{ggt}(g, g')] + \deg[\operatorname{ggt}(h, h')] \leq \deg(f) + \deg(g) - 1 \\ &\overset{\text{Lemma 1.1}}{\Rightarrow} \deg(f) - n_0(f) + \deg(g) - n_0(g) + \deg(h) - n_0(h) \leq \deg(f) + \deg(g) - 1 \\ &\Rightarrow \deg(h) \leq n_0(f) + n_0(g) + n_0(h) - 1 \end{aligned}$$

Da f, g und h immer noch teilerfremd sind, gilt:

$$\overset{\text{Lemma 1.2}}{\Rightarrow} \deg(h) \leq n_0(f \cdot g \cdot h) - 1$$

Da nun gilt $f + g = h \Leftrightarrow f + (-h) = -g \Leftrightarrow g + (-h) = f$, lässt sich analog zeigen:

$$\begin{aligned} \deg(f) &\leq n_0(f \cdot g \cdot h) - 1 \\ \deg(g) &\leq n_0(f \cdot g \cdot h) - 1 \end{aligned}$$

Da die Ungleichungen für $\deg(f), \deg(g)$ und $\deg(h)$ gelten, gilt schließlich auch:

$$\max\{\deg(f), \deg(g), \deg(h)\} \leq n_0(f \cdot g \cdot h) - 1$$

1.1.4 Die FERMATsche Gleichung für Polynome

Es seien f, g, h paarweise teilerfremde, nicht konstante Polynome in $\mathbb{C}[x]$.

Auf die Gleichung

$$f^n + g^n = h^n$$

ist der Satz von Mason also anwendbar mit

$$\deg(f^n) \leq n_0(f \cdot g \cdot h) - 1$$

$$\deg(g^n) \leq n_0(f \cdot g \cdot h) - 1$$

$$\deg(h^n) \leq n_0(f \cdot g \cdot h) - 1$$

da, wenn die Ungleichung für den maximalen Grad gilt, sie natürlich auch für alle Grade einzeln gilt.
Desweiteren lassen sich auch die rechten Seiten mit Lemma 2 als $n_0(f) + n_0(g) + n_0(h) - 1$ darstellen. Durch Summation erhalten wir

$$\begin{aligned} \deg(f^n) + \deg(g^n) + \deg(h^n) &\leq 3(n_0(f) + n_0(g) + n_0(h) - 1) \\ \Rightarrow n \cdot (\deg(f) + \deg(g) + \deg(h)) &\leq 3(\deg(f) + \deg(g) + \deg(h) - 1) \end{aligned}$$

Somit kann die FERMATsche Gleichung für Polynome für $n \geq 3$ keine Lösungen besitzen.

Für $n = 2$ gibt es übrigens die klassische Lösung $(x^2-1)^2+(2x)^2 = (x^2+1)^2$. Man erhält sie zum Beispiel, indem man die rationalen Punkte auf dem Einheitskreis durch Geraden mit rationalem Anstieg durch $(0, 1)$ parametrisiert (dies liefert zudem auch alle Pythagoräischen Tripel, d.h. alle ganzen Zahlen a, b, c mit $a^2 + b^2 = c^2$).

1.2 Die *abc*-Vermutung

Wir versuchen, für ganze Zahlen mit $a + b = c$ eine Art „Mason"-Satz zu formulieren.
Es seien $a, b, c \in \mathbb{Z}$ paarweise teilerfremd.

Als „Grad" einer ganzen Zahl wird der Betrag der Zahl gewählt. Dies kann z.B. durch die Division mit Rest motiviert werden - bei Polynomen hat der Rest einen kleinerer Grad als der Divisor, bei ganze Zahlen einen kleineren

Betrag.

Wodurch könnte n_0 ersetzt werden? Bei Polynomen wird die Anzahl der verschiedenen Nullstellen, also der Primfaktoren gezählt. Wir sind dort in der einfachen Situation, dass alle Primfaktoren denselben Grad haben. Dagegen treten im allgemeinen in der Primzerlegung

$$a = \prod_{i=1}^{n} p_i^{m_i}$$

Faktoren mit unterschiedlichem Betrag auf. Wir definieren daher

$$N_0 := \prod_{i=1}^{n} p_i,$$

also das Produkt der verschiedenen Primfaktoren.

1. Versuch:
Gilt $\max\{|a|, |b|, |c|\} \leq N_0(a \cdot b \cdot c)$ für ganze Zahlen?
Gegenbeispiel:

$$2^{10} + 1 = 1025 = 5^2 \cdot 41$$

$$N_0(a \cdot b \cdot c) = 2 \cdot 1 \cdot 5 \cdot 41 = 410 < 2^{10} + 1$$

2.Versuch:
Ausgleich durch eine Konstante $K \in \mathbb{R}$

$$\max\{|a|, |b|, |c|\} \leq K \cdot N_0(a \cdot b \cdot c)$$

Gegenbeispiel:

$$a = 3^{2^n}, b = -1$$

Es gilt ferner für alle n, dass $2^n | (3^{2^n} - 1)$ (induktiv leicht zu zeigen).

$$\begin{aligned} \Rightarrow N_0(3^{2^n} - 1) = N_0(2^n \cdot \frac{3^{2^n} - 1}{2^n}) &\leq N_0(2^n) \cdot N_0(\frac{3^{1^n} - 1}{2^n}) \leq 2 \cdot \frac{3^{2^n} - 1}{2^n} \\ \Rightarrow N_0(a \cdot b \cdot c) &\leq 1 \cdot 3 \cdot 2 \cdot \frac{3^{2^n}}{2^n} \\ \Rightarrow \max\{|a|, |b|, |c|\} = 3^{1^n} &\leq k \cdot 3 \cdot 2 \cdot \frac{3^{2^n} - 1}{2^n} \end{aligned}$$

$\Rightarrow$ Es existiert kein $k \in \mathbb{R}$, sodass dies für alle n gilt!

Die Ungleichung würde aber stimmen, wenn die rechte Seite in eine minimal höhere Potenz als 1 erhoben würde. Dies führt zu folgender

Vermutung (*abc*-Vermutung). *Seien* $a, b, c \in \mathbb{Z}$, $a + b = c$.

$$\forall\ \epsilon > 0\ \exists\ K(\varepsilon): \quad \max\{|a|, |b|, |c|\} \leq K(\varepsilon) N_0(a \cdot b \cdot c)^{1+\epsilon}$$

Bisher sind keine Gegenbeispiele bekannt, und es gibt eine Reihe von Ergebnissen, die auf die Richtigkeit der Vermutung hindeuten.

1.3 Die Anwendungen der *abc*-Vermutung

1.3.1 Die FERMATsche Gleichung

Seien $x, y, z \in \mathbb{Z}$ mit $x^n + y^n = z^n, n \in \mathbb{N}$.

Aus der *abc*-Vermutung folgt:

$$\begin{array}{rrcl}
 & \max\{|x^n|, |y^n|, |z^n|\} & \leq & K(\varepsilon) \cdot N_0(x^n \cdot y^n \cdot z^n)^{1+\varepsilon} \\
\Rightarrow & |x^n| \cdot |y^n| \cdot |z^n| & \leq & (K(\varepsilon) \cdot N_0(x \cdot y \cdot z)^{1+\varepsilon})^3 \\
\Rightarrow & (|x \cdot y \cdot z|)^n & \leq & K(\varepsilon)^3 \cdot N_0(x \cdot y \cdot z)^{3+3\varepsilon} \\
\Rightarrow & (|x \cdot y \cdot z|)^n & \leq & K(\varepsilon)^3 \cdot (|x \cdot y \cdot z|)^{3+3\varepsilon} \\
\Rightarrow & (|x \cdot y \cdot z|)^{n-3\varepsilon-3} & \leq & K(\varepsilon)^3
\end{array}$$

(1) Wenn $x \cdot y \cdot z \geq 2$, so muss offensichtlich ein n_0 existieren, sodass gilt:

$$\forall n \geq n_0 : (|x \cdot y \cdot z|)^{n-3\varepsilon-3} > K(\varepsilon)^3.$$

Für genügend große n gibt es also nur die trivialen Lösungen mit $x \cdot y \cdot z = 0$.

(2) Fixiert man $n \geq 4$, kann die Gleichung nur endlich viele Lösungen haben, da ab einer gewissen Größe von $|x \cdot y \cdot z|$ die Ungleichung nicht mehr erfüllt wird.

1.3.2 Die CATALANsche Gleichung

$\forall x, y, n \in \mathbb{N}^* : x^n - y^m = 1$ hat für $m, n \geq 2$ und $y \neq 0$ keine Lösung außer $3^2 - 2^3 = 1$.

Annahme: Die CATALANsche Gleichung ist erfüllt.

(1) $m = n = 2$ ist nicht möglich, da die Differenz zweier Quadrate $\neq 0$ immer größer als 1 ist.

(2) Sei $m > 2 \vee n > 2$
Mit der *abc*-Vermutung folgt dann:

$$\max\{x^n, y^m\} \leq k(\epsilon) \cdot N_0(x^n \cdot y^m)^{1+\varepsilon}$$

$$\begin{aligned}
\Rightarrow m \cdot \ln(y) < n \cdot \ln(x) &\leq (1+\varepsilon) \cdot \ln(N_0(x^n \cdot y^m)) + \ln(K(\varepsilon)) \\
\Rightarrow \qquad n \cdot \ln(x) &\leq (1+\varepsilon) \cdot \ln(N_0(x \cdot y)) + \ln(K(\varepsilon)) \\
&\leq (1+\varepsilon) \cdot \ln(x \cdot y) + \ln(K(\varepsilon)) \\
m \cdot \ln(y) &\leq (1+\varepsilon) \cdot \ln(N_0(x \cdot y)) + \ln(K(\varepsilon)) \\
&\leq (1+\varepsilon) \cdot \ln(x \cdot y) + \ln(K(\varepsilon))
\end{aligned}$$

$\Rightarrow m \cdot n \cdot (\ln(x) + \ln(y)) \leq (1+\varepsilon) \cdot (m+n) \cdot (\ln(x) + \ln(y)) + (m+n) \cdot \ln(K(\varepsilon))$
$m \cdot n > m + n$ gilt nach Voraussetzung (da $m = n = 2$ nicht möglich ist). Demnach ist diese Ungleichung nur für endlich viele x, y erfüllt.
Also kann auch die CATALANsche Gleichung höchstens von endlich vielen x, y erfüllt werden.

1.3.3 Die Gleichung $x^l + y^m = z^n$

Seien $x, y, z \in \mathbb{Z}$ mit $x^l + y^m = z^n, l, m, n \in \mathbb{N} \setminus \{0, 1, 2, 3\}$.

Aus der *abc*-Vermutung folgt:

$$\begin{aligned}
\max\{|x^l|, |y^m|, |z^n|\} &\leq K(\varepsilon) \cdot N_0(x^l \cdot y^m \cdot z^n)^{1+\varepsilon} \\
|x^l| \cdot |y^m| \cdot |z^n| &\leq (K(\varepsilon) \cdot N_0(x \cdot y \cdot z)^{1+\varepsilon})^3 \\
|x|^l \cdot |y|^m \cdot |z|^n &\leq K(\varepsilon)^3 \cdot N_0(x \cdot y \cdot z)^{3+3\varepsilon}
\end{aligned}$$

Fixiert man $l, m, n \geq 4$, kann die Gleichung nur endlich viele Lösungen haben, da ab einer gewissen Größe von $|x \cdot y \cdot z|$ die Ungleichung sonst nicht mehr erfüllt wird. Ebenso sieht man, dass für hinreichend große l, m, n keine Lösung mehr existieren kann.

2 Das Waring-Problem für ganze Zahlen

In diesem Abschnitt beschäftigen wir uns mit der Frage, ob man eine ganze Zahl n als Summen von Potenzen

$$n = a_1^k + \ldots a_g^k$$

darstellen kann und wieviele Summanden man dazu benötigt. Wir beginnen mit dem Fall $k = 2$, also Summen von Quadraten.

2.1 Der Zwei-Quadrate-Satz

Welche Zahlen lassen sich als Summe zweier Quadrate schreiben? Wir probieren z.B.

$$2 = 1^2 + 1^2, \quad 20 = 4^2 + 2^2, \quad 65 = 7^2 + 4^2 = 8^2 + 1^2.$$

Es fällt auf, dass die Zahlen, die sich als Summe zweier Quadrate schreiben lassen, nur bestimmte Primfaktorzerlegungen haben. Der Grund dafür ist das folgende Lemma:

Lemma 2.1. $(A^2 + B^2) \cdot (U^2 + V^2) = (AU + BV)^2 + (AV - BU)^2$

Diese Identität kann leicht durch Ausmultiplizieren berechnet werden. Man kann sie aber auch interpretieren als die Betragsgleichung $|z_1||z_2| = |z_1 z_2|$ für komplexe Zahlen $z_1 = A + Bi$, $z_2 = V + Ui$.

Korollar 2.2. *Das Problem der Darstellung als zwei Quadrate kann auf das Problem für Primfaktoren reduziert werden.*

Welche Primzahlen sind als Summe zweier Quadrate darstellbar? Z.B. sind

$$2 = 1^2 + 1^2 \ ; \ 53 = 2^2 + 7^2 \ ; \quad \text{aber } 19 = 3^2 + 3^2 + 1^2$$

Wir beobachten, dass alle Rest 1 bei der Division durch 4 lassen. Tatsächlich gilt:

Satz 2.3. *Sei p eine ungerade Primzahl. p ist die Summe von zwei Quadraten genau dann, wenn gilt:*

$$p \equiv 1(\mod 4)$$

Beweis: Wir beweisen zunächst die einfache Richtung. Wenn p die Summe von 2 Quadraten ist, dann muss eines der beiden Quadrate gerade und eines ungerade sein. Selbiges gilt somit auch für die Zahlen selber. Da gilt:

$$a = 2n+1 \Leftrightarrow a \equiv 1(\mod 4) \vee a \equiv 3(\mod 4) \Leftrightarrow p^2 \equiv 1(\mod 4)$$

$$b = 2k \Leftrightarrow bp \equiv 0(\mod 4) \vee b \equiv 2(\mod 4) \Leftrightarrow p^2 \equiv 0(\mod 4)$$

Somit gilt:

$$p \equiv a^2 + b^2(\mod 4) \Leftrightarrow p \equiv 0 + 1(\mod 4) \Leftrightarrow p \equiv 1(\mod 4)$$

Wenn p die Summe zweier Quadrate ist, ist es auch kongruent zu $1 \mod 4$. Für den Beweis der Umkehrung benötigen wir folgendes Lemma:

Lemma 2.4. *(i) (Satz von Wilson) p ist eine Primzahl genau dann, wenn*

$$(p-1)! \equiv -1(\mod p)$$

(ii) Sei p eine Primzahl, dann ist $((\frac{p-1}{2})!)^2 \equiv (-1)^{\frac{p+1}{2}}(\mod p)$

Beweis: (i) Jede Restklasse $\neq 0$ ist modulo einer Primzahl p invertierbar. Im Produkt $(p-1)!$ erscheint damit also zu jeder Restklasse ihre Inverse. Diese kürzen sich zu 1 mit Ausnahme von ± 1, die ihre eigenen Inversen sind. Daher ist das Produkt für Primzahlen -1.
Umgekehrt ist der $\text{ggt}((p-1)!, p) \geq 2$, wenn p keine Primzahl ist.

$$(ii)\ (p-1)! \equiv (-1)\cdot 1\cdot \ldots \cdot(-\frac{p-1}{2})(\frac{p-1}{2}) \equiv ((\frac{p-1}{2})!)^2 \cdot (-1)^{\frac{p-1}{2}} \overset{(i)}{\equiv} -1 (\mathrm{mod}\, p).$$

Insbesondere gibt es für Primzahlen $p \equiv 1(\mod 4)$ eine Zahl x mit $x^2 + 1 = Mp$ (dabei ist offenbar $M \leq p-1$), also haben wir ein Vielfaches von p als Summe zweier Quadrate $A^2 + B^2$ dargestellt. Wir beginnen nun

ein Reduktionsverfahren, um M zu verkleinern. Dabei setzen wir $U \equiv A(\mod M)$ und $V \equiv B(\mod M)$. Es gilt dann $U^2+V^2 = Mr$ mit $r \leq M-1$. Wir verwenden nun erneut die Quadrateidentität 2.1 und erhalten

$$(A^2+B^2)\cdot(U^2+V^2) = (AU+BV)^2+(AV-BU)^2 = M^2rp.$$

Desweiteren ist offenbar $AU+BV \equiv A^2+B^2 \equiv 0(\mod M)$ und $AV-BU \equiv AB-BA \equiv 0(\mod M)$, daher teilt M die Zahlen $AU+BV$ und $AV-BU$, und es gilt

$(\frac{AU+BV}{M})^2+(\frac{AV-BU}{M})^2 = rp$, wir haben also ein kleineres Vielfaches

von p als Summe zweier Quadrate dargestellt. Der Schluß auf $M=1$ folgt durch Iteration.

Korollar 2.5. *Jede Primzahl $p \equiv 1(\mod 4)$ läßt sich eindeutig als Summe zweier Quadrate darstellen.*

Die Existenz einer Darstellung $p = A^2+B^2$ folgt aus dem eben bewiesenem Satz, die Eindeutigkeit aus der Zerlegung $A^2+B^2 = (A+Bi)(A-Bi)$ und der Tatsache, dass in $\mathbb{Z}+i\mathbb{Z}$ die Primzerlegung eindeutig ist (letzteres kann man z.B. aus der Existenz einer Division mit Rest bzgl. des Betrags folgern).

Als Folgerung aus der Quadratidentität erhalten wir den zwei-Quadrate-Satz für beliebige natürliche Zahlen:

Korollar 2.6. *$n \in \mathbb{N}$ mit der Primzerlegung $n = \prod_{i=1}^{r} p_i^{m_i}$ ist als Summe zweier Quadrate darstellbar genau dann, wenn jedes $P_i \equiv 3(\mod 4)$ nur mit gerader Vielfachheit vorkommt.*

2.2 Satz von Lagrange

Mit Hilfe der Ideen des vorigen Abschnitts beweisen wir nun analog den

Theorem 2.7 (Satz von Lagrange)**.** *Jede natürliche Zahl ist Summe von vier Quadraten.*

Beweis: Der Beweis verläuft analog zum zwei-Quadrate-Satz. Zunächst wird eine Identität benutzt, die das Problem auf Primfaktoren zurückführt. Dann finden wir durch Restklassenüberlegung eine Quadratzerlegung eines

Vielfachen. In einem Abstiegsverfahren, das wiederum die Identität benutzt, können wir dann dieses Vielfache auf eins reduzieren.
Es gilt

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

mit

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \\ z_3 &= x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 \\ z_4 &= x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2. \end{aligned}$$

Diese Identität kann man übrigens analog zur zwei-Quadrate-Identität als Betragsgleichung von Produkten auffinden, in disem Fall im Schiefkörper der Quaternionen.
Ferner ist $2 = 1^2 + 1^2 + 0^2 + 0^2$. Es genügt also zu zeigen, daß jede Primzahl Summe von 4 Quadraten ist.
Es sei also p eine ungerade Primzahl. Die $\frac{p+1}{2}$ Zahlen x^2 mit $0 \leq x \leq \frac{p-1}{2}$ sind paarweise inkongruent $\mod p$, ebenso die $\frac{p+1}{2}$ Zahlen $-1 - y^2$ mit $0 \leq y \leq \frac{p-1}{2}$. Da es genau p Restklassen $\mod p$ gibt, dies aber insgesamt $p + 1$ Zahlen sind, gibt es ein x, sodass $x^2 \equiv -1 - y^2 (\mod p)$ ist. Ein Vielfaches von p lässt sich also in der Form $1 + x^2 + y^2$ darstellen:

$$m \cdot p = 0^2 + 1^2 + x^2 + y^2$$

Darin ist $0 < m < p$ (wegen $1 + x^2 + y^2 < 1 + 2\left(\frac{p}{2}\right)^2 < p^2$). Es sei m_0p das kleinste Vielfache von p, welches sich in der Form

$$m_0p = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

mit $0 < m_0 < p$ darstellen lässt, worin x_1, x_2, x_3, x_4 nicht alle durch p und auch nicht durch m_0 teilbar sind. Angenommen, es sei $m_0 > 1$. Aus der Minimaleigenschaft von m_0 folgt, dass dann m_0 ungerade sein muss. Wäre m_0 gerade, so hätten wir

$$x_1 + x_2 + x_3 + x_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 (\mod 2)$$

d.h., die x_i sind zu je zweien kongruent $\mod 2$. Es sei o.B.d.A. $x_1 \equiv x_2 (\mod 2)$ und $x_3 \equiv x_4 (\mod 2)$. Dann haben wir die Darstellung

$$\frac{m_0}{2} \cdot p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

im Widerspruch zur Minimalität von m_0. Man kann also

$$x_i = b_i \cdot m_0 + y_i$$

mit $(i = 1, 2, 3, 4)$ setzen, wobei b_i so gewählt wurde, dass $|y_i| < \frac{1}{2}m_0$ ist. Da x_1, x_2, x_3, x_4 nicht alle durch m_0 teilbar sind, ist wenigstens ein $y_i > 0$. Somit ist

$$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4 \cdot \left(\frac{1}{2}m_0\right)^2 = m_0^2.$$

Aus $x_i = b_i m_0 + y_i$ folgt andererseits

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0(\mod m).$$

Daher ist

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_1 \cdot m_0$$

mit $0 < m_1 < m_2$. Es folgt demnach die Darstellung

$$m_0^2 m_1 p = z_1^2 + z_2^2 + z_3^2 + z_4^2.$$

Jedes der z_i ist darin aber wegen $x_i \equiv y_i(m_0)$ durch m_0 teilbar, also $z_i = m_0 t_i$. Es folgt

$$m_1 p = t_1^2 + t_2^2 + t_3^2 + t_4^2$$

mit $0 < m_1 < m_0 < p$, was ein Widerspruch zur Minimaleigenschaft von m_0 ist. Es muss somit $m_0 = 1$ sein, q.e.d.

2.3 Das Waring-Problem

In seinem Buch *Meditationes Algebraicae* schrieb Waring 1770: „Jede Zahl ist Summe von neun Kubikzahlen, neunzehn Biquadraten und so weiter... “ Zuvor hatte Lagrange bereits bewiesen, dass jede Zahl als Summe von vier Quadratzahlen darstellbar ist (siehe 2.7). Daher wurde nach Waring das folgende Problem benannt:

Problem 2.8 (Waring-Problem). *Gibt es zu jedem Exponenten k eine kleinste Zahl $g(k)$, so dass jede natürliche Zahl n als Summe*

$$n = a_1^k + \cdots + a_{g(k)}^k$$

von k-ten Potenzen darstellbar ist?

Hilbert bewies 1909, dass ein solches $g(k)$ für alle $k \in \mathbb{N}$ existiert. Die Bestimmung der Zahlen $g(k)$ erwies sich als deutlich schwieriger und wurde erst in den letzten Jahrzehnten abgeschlossen. Warings Vermutung, dass $g(3) = 9$ und $g(4) = 19$ ist, konnten gezeigt werden. Allgemein gibt es drei Fälle, wobei im Hauptfall das folgende Resultat gilt:

Theorem 2.9. *Sei $k > 4$ und $2^k \cdot \{(\frac{3}{2})^j\} + [(\frac{3}{2})^j] \leq 2^k$. Dann ist*

$$\Rightarrow g(k) = 2^k + [(\frac{3}{2})^k] - 2.$$

Der Beweis ist allerdings extrem schwierig.

Bei weiteren Untersuchungen stellt man fest, dass oft nur wenige Zahlen wirklich $g(k)$ Summanden benötigen. So sind im Fall $k = 3$ die Zahlen

$$23 = 2 \cdot 2^3 + 7 \cdot 1^3 \text{ und } 239 = 5^3 + 3 \cdot 3^3 + 4 \cdot 2^3 + 1^3$$

die einzigen Zahlen, die neun Kuben benötigen. Weitere fünfzehn Zahlen benötigen acht Kuben (die größte ist 8042), alle anderen höchstens sieben. Dies führt auf das bisher ungelöste

Problem 2.10 (Großes Waring-Problem). *Finde die Zahl $G(k)$, das ist die kleinste Anzahl, so dass sich fast alle natürlichen Zahlen (d.h. bis auf endlich viele) als Summe von $G(k)$ k-ten Potenzen schreiben lassen.*

Dieses Problem ist noch deutlich schwerer und weitgehend ungelöst. So ist z.B. unklar, ob $G(3) = 7$. Bisher weiß man nur, dass $G(2) = 4$ und $G(4) = 16$.

3 Das Waring-Problem für Polynome

In diesem Abschnitt betrachten wir das analoge Problem für Polynome aus $\mathbb{C}[x]$, d.h. die Frage, wann man ein Polynom als Summe von Potenzen anderer Polynome darstellen kann. Wir werden im ersten Teil schnell sehen, dass diese Frage relativ leicht beantwortbar, aber nicht besonders interessant ist. Deshalb werden wir uns auf das Problem der Darstellung als Potenzsummen von linearen Polynomen einschränken. Es erweist sich, dass dies eine schöne geometrische Interpretation und eine anschauliche Antwort besitzt.

3.1 Potenzsummen beliebiger Polynome

Wir beginnen wieder mit dem quadratischen Fall. Dieser ist besonders einfach wegen der Identität

$$P^2 = (\frac{P+1}{2})^2 + (i\frac{P-1}{2})^2,$$

d.h. jedes komplexe Polynom P (mit beliebig vielen Variablen!) ist Summe zweier Quadrate. Stimmt das auch für Kuben? Wir untersuchen dies im einfachen Fall des Polynoms x.

Satz 3.1. *x ist nicht Summe zweier Kuben.*

Beweis: Allgemein lässt sich jede Summe zweier Kuben darstellen als:

$$A^3 + B^3 = (A+B) \cdot (A+\xi B) \cdot (A+\xi^2 B),$$

wobei ξ eine dritte Einheitswurzel $\neq 1$ ist. Damit müsste x als Polynom 1. Grades darstellbar sein als Produkt dreier Faktoren. Von diesen Faktoren muss demnach einer ersten Grades und zwei konstant sein. Da dafür offensichtlich A und B konstant sein müssten (leicht nachzurechnen), führt dies automatisch zu einem Widerspruch, da dann $A^3 + B^3 \neq x$.
Übrigens könnten wir den Beweis auch mit dem Satz von Mason führen. Die Anwendung auf $x = A^3 + B^3$ liefert nämlich $n_0(A) + n_0(B) + 1 - 1 \geq \max\{\deg(A^3), \deg(B^3)\}$, also $\deg(A) + \deg(B) \geq 3\max\{\deg(A), \deg(B)\}$. Dies ist unmöglich für nichtkonstante A und B.

Damit kann nicht jedes Polynom als Summe zweier Kuben dargestellt werden. Wir können aber durch Untersuchung der Darstellung von x zeigen, dass jedes Polynom Summe dreier Kuben ist; es gilt nämlich

$$\left(\frac{x}{6}+1\right)^3 + \left(\frac{x}{6}-1\right)^3 + \left(\frac{-x}{\sqrt{108}}\right)^3 = x.$$

Durch Substitution erhält man also für jedes beliebige komplexe Polynom P (mit beliebig vielen Variablen!):

$$\left(\frac{P}{6}+1\right)^3 + \left(\frac{P}{6}-1\right)^3 + \left(\frac{-P}{\sqrt{108}}\right)^3.$$

Demnach ist jedes Polynom als Summe von drei Kuben darstellbar.

Analog kann man x auch als Summe von höheren Potenzen darstellen, man sieht allerdings bereits hier, dass diese nicht sehr ergiebig, sondern im Gegenteil sogar sehr kompliziert sind. Als abstraktes Resultat mag eine solche Darstellung befriedigen, aber das Resultat sieht sehr unschön und willkürlich aus. Eine solche Zerlegung sagt uns nicht über die Eigenschaften von P, zumal die einzelnen Summanden höheren Grad als P haben. Effizienter wäre eine Darstellung als Potenzsumme von Polynomen mit kleinerem Grad, am besten von linearen. Dies soll uns im folgenden beschäftigen. Dazu führen wir zunächst den Begriff eines homogenen Polynoms ein.

3.2 Homogenisierung

Definition 3.2. *Ein Polynom $P \in \mathbb{C}[x_0, \ldots, x_n]$ heisst homogen vom Grad d, wenn $P(\lambda x_0, \ldots, \lambda x_n) = \lambda^d P(x_0, \ldots, x_n)$ für beliebige $\lambda \in \mathbb{C}$ gilt.*

Bemerkung: Diese Eigenschaft ist äquivalent zu der Tatsache, dass in der Darstellung $P = \sum_{i_0,\ldots,i_n} x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_n^{i_n}$ für alle Monome gilt: $i_0 + \cdots + i_n = d$. Homogene Polynome haben den Vorteil, dass sich bei Summation der Grad nicht verändern kann (es sei denn, es ergibt sich das Nullpolynom). Wir können durch eine leichte Modifikation jedes Polynom aus $\mathbb{C}[x_1, \ldots, x_n]$ in eine homogene Form überführen, indem wir einfach in jedem Monom den Grad durch Multiplikation mit Potenzen einer zusätzlichen Variablen x_0 auffüllen. So wird zum Beispiel aus $3x_1^2 + 4x_1 + 1$ das Polynom $3x_1^2 + 4x_1x_0 + x_0^2$. Offenbar ist diese Zuordnung umkehrbar eindeutig.
Im Folgenden wollen wir daher die Darstellbarkeit von homogenen Polynomen (mit mehreren Variablen) in der Form $P = \sum_{j=1}^{k} L_j^d$, wobei L_j Linearformen sind, untersuchen.

3.3 Quadriken

Wie im Fall ganzer Zahlen betrachten wir zunächst den quadratischen Fall. Es sei also $P(x_0, \ldots, x_n) = \sum_{i,j=0}^{n} a_{ij} x_i x_j$. Man kann P auch als Produkt

$$P(x_0, \ldots, x_n) = (x_0, \ldots, x_n) \cdot A \cdot (x_0, \ldots, x_n)^T$$

darstellen, wobei $A = (a_{ij})_{i,j=1}^{n}$ die Koeffizientenmatrix ist. Der folgende Satz aus der linearen Algebra gibt uns dann die Lösung unseres Problems:

Satz 3.3. *Nach einer linearen Koordinatentransformation ist A eine Matrix, die auf der Haupdiagonalen nur Nullen und Einsen und ansonsten nur Nullen enthält. Mit anderen Worten, $P = L_1^2 + \cdots + L_{k+1}^2$ mit $k \leq n$.*

Beweis: Der symmetrische Gauß-Algorithmus (d.h. nach jeder Zeilenoperation wird dieselbe Operation in den Spalten ausgeführt) liefert in den komplexen Zahlen das gewünschte Ergebnis.
Beispiel: $P(x_0, x_1) = x_0^2 + 4x_0x_1 + 3x_1^2$ lässt sich darstellen als $(x_0 + 2x_1)^2 + (ix_1)^2$.

3.4 Der (projektive) Raum der Polynome vom Grad d

Nun betrachten wir homogene Polynome beliebigen Grades. Wir überlegen uns leicht mit kombinatorischen Argumenten:

Proposition 3.4. *Es gibt $\binom{n+d}{d}$ Monome in den Variablen $x_0, \ldots, x_n$ vom Grad d.*

Beweis: Wir wiederholen zunächst einige Basisresultate der Kombinatorik.

$$n! = 1 \cdot 2 \cdot \ldots \cdot n$$

wird benutzt, um die Anzahl aller möglichen Permutationen einer n-elementigen Menge zu berechnen. Mit dem Binomialkoeffizienten

$$\binom{n}{k} = \frac{n!}{d! \cdot (n-k)!}$$

kann man bestimmen, wie viele Möglichkeiten es gibt, aus einer n-elementigen Menge k verschiedene Elemente auszuwählen.
Die analoge Frage nach der Anzahl der Möglichkeiten, aus einer n-elementigen Menge k Elemente auszuwählen, wobei auch mehrfache Auswahl desselben Elements zugelassen ist, ergibt die Formel

$$\binom{n+k-1}{k} = \frac{(n+k-1)!}{(n-1)! \cdot k!}.$$

Das Bilden der von Monomen vom Grad d aus den $n+1$ Variablen $x_0, \ldots x_n$ entspricht einer Auswahl von d Elementen aus $(n+1)$, wobei ein Element öfters ausgewählt werden kann. Dies sind also nach den vorherigen Überlegungen genau $\binom{n+1+d-1}{d}$ Stück.

Zur Abkürzung setzen wir ab jetzt $\mathbf{N} := \binom{n+d}{d}$. Wir können nun ein Polynom $\sum_{i_0+\cdots+i_n=d} a_{i_0\ldots i_n} x^{i_0\ldots i_n}$ vom Grad d auch als Vektor mit N Koordinaten $(\ldots, a_{i_0\ldots i_n}, \ldots)$ auffassen und somit den Vektorraum $\mathbb{C}^{\mathbf{N}}$ als Raum der Polynome vom Grad d interpretieren. Da allerdings für die Darstellung als Potenzsumme $L_1^d + \cdots + L_k^d$ konstante Vielfache irrelevant sind, ist es natürlicher, die Polynome als Punkte im projektiven Raum $\mathbb{P}^{N-1}$ zu betrachten (also den Raum der Geraden in $\mathbb{C}^{\mathbf{N}}$ durch den Nullpunkt). Die Koeffizienten des Polynoms ergeben dann die homogenen Koordinaten $[\cdots : a_{i_0\ldots i_n} : \ldots]$, z.B. entspricht $x_0^2 + 4x_0x_1 + 3x_1^2$ dem Punkt $[1:4:3]$ im $\mathbb{P}^2$.

3.5 Die Veronese-Abbildung

Im Fall von Polynomen höheren Grades $d \geq 3$ können wir das Waring-Problem auf eine geometrische Fragestellung zurückführen. Dazu interpretieren wir die homogenen Polynome vom Grad d als Punkte im affinen Raum $\mathbb{C}^{\mathbf{N}}$ bzw. im projektiven Raum $\mathbb{P}^{N-1}$ ($N = \binom{n+d}{d}$). Eine natürliche Frage ist dann: Welche geometrische Form hat die Teilmenge der Potenzen von Linearformen L^d?

Man berechnet mit Hilfe der multinomischen Formel

$$(a_0x_0 + \cdots + a_nx_d)^d = \sum_{i_0+\ldots i_n=d} \frac{d!}{i_0! \ldots i_n!} \prod_{j=1}^{n} (a_jx_j)^{i_j},$$

dass solche Potenzen Koordinaten der Form $[\cdots : \frac{d!}{i_0!\ldots i_n!} \prod_{j=1^n} (a_j)^{i_j} : \cdots]$ im $\mathbb{P}^{N-1}$ haben. Nach einer koordinatenweisen Stauchung mit dem Faktor $\frac{d!}{i_0!\ldots i_n!}$ entspricht dies gerade dem Bild der sogenannten Veronese-Abbildung

$$\begin{array}{rcl} \nu_d : \mathbb{P}^n & \to & \mathbb{P}^{N-1} \\ [a_0 : \cdots : a_n] & \mapsto & [a_0^d : \cdots : a_n^d], \end{array}$$

wobei die Koordinaten im Bildraum gerade alle Monome vom Grad d durchlaufen.

Beispiel: Ein einfaches Beispiel hierfür ist die rationale Normkurve (auch „verdrehte Kubik“ genannt):

$$\begin{array}{rcl} \nu_3 : \mathbb{P}^1 & \to & \mathbb{P}^3 \\ [a_0 : a_1] & \mapsto & [a_0^3 : a_0^2a_1 : a_0a_1^2 : a_1^3]. \end{array}$$

Man sieht übrigens leicht, dass diese Kurve gerade durch die Gleichungen

$$xw = yz, \quad xz = y^2, \quad yw = z^2$$

gegeben ist (wenn $[x : y : z : w]$ die Koordinaten des $\mathbb{P}^3$ bezeichnen).
Für allgemeine n, d sind die Bilder von ν_d (dies sind die sogenannten „Veronese-Varietäten ") komplizierter, aber ebenfalls als Nullstellenmengen von Polynomen beschreibbar. Die Veronese-Abbildung erweist sich außerdem als eineindeutig. Insbesondere ist das Bild $\nu(\mathbb{P}^n)$ ebenfalls n-dimensional.

3.6 Sekantenvarietäten

Der nächste Schritt geht von der natürlichen Frage aus, welche Punkte im $\mathbb{P}^{N-1}$ Polynomen der Form $L_1^d + L_2^d$ entsprechen. Man rechnet direkt aus, dass dies gerade die Punkte sind, die auf der Geraden durch die Punkte L_1^d und L_2^d liegen. Dasselbe gilt für $k+1$ Summanden:

Satz 3.5. *Ein Polynom ist als Summe $L_1^d + \ldots L_{k+1}^d$ darstellbar, genau dann wenn der zugehörige Punkt im $\mathbb{P}^{N-1}$ in dem Raum liegt, der durch die Punkte $L_1^d, \ldots, L_{k+1}^d$ auf der Veronese-Varietät aufgespannt wird.*

Geraden durch zwei Punkte der Menge $\nu_d(\mathbb{P}^n)$ bezeichnet man als Sekanten. Dementsprechend liegt die folgende Definition nahe:

Definition 3.6. *Die Sekantenvarietät $Sec_k\nu_d(\mathbb{P}^n)$ ist die Menge der Punkte aller k-dimensionalen Räume, die durch $k+1$ Punkte auf $\nu_d(\mathbb{P}^n)$ gehen, zuzüglich der Grenzwerte dieser Punkte.*

Warum nehmen wir die Grenzwerte hinzu? Dies sind Punkte, die auf Tangenten der Veronese-Varietät liegen, und bilden in diesem Sinne eine Abschließung der Sekantenräume (wir „füllen die Lücken"). Man überlegt sich leicht, dass diese Menge relativ klein ist (es gibt viel mehr Sekanten als Tangenten). Der Vorteil dieser Abschliessung ist, dass dann $Sec_k\nu_d(\mathbb{P}^n)$ ebenfalls durch polynomiale Gleichungen im $\mathbb{P}^{N-1}$ beschrieben werden kann.
Durch diese Überlegungen haben wir folgende Modifikation des Waring-Problems erreicht:

Problem 3.7. *Für welche k ist $Sec_k\nu_d(\mathbb{P}^n) = \mathbb{P}^{N-1}$?*

Dabei ist zu bemerken, dass dies dem „großen “ Waring-Problem entspricht, nämlich der Frage, mit wieviel Summanden wir „fast alle“ Polynome darstellen können (mit Ausnahme der Punkte auf den Tangenten). Wir können die Frage sogar noch etwas weiter vereinfachen. Das Problem ist nämlich äquivalent zur Gleichheit der Dimension, d.h. wir prüfen

$$\dim Sec_k\nu_d(\mathbb{P}^n) = N-1?$$

Warum reicht dies aus? Der Grund ist, dass eine polynomiale Gleichung sofort die Dimension um 1 reduziert. Wenn also die Dimension der Sekantenvarietät $N-1$ ist, heisst das nichts anderes, als dass das zugehörige polynomiale Gleichungssystem leer ist, mit anderen Worten sie ist der ganze Raum $\mathbb{P}^{N-1}$.

3.7 Dimensionszählung und der Satz von Alexander und Hirschowitz

Wir überlegen uns nun, welche Dimension die Sekantenvarietät haben kann. Man überlegt sich schnell die folgende Abschätzung:

Lemma 3.8. $\dim Sec_k\nu_d(\mathbb{P}^n) \leq (k+1)n + k$

Beweis: Wenn wir $k+1$ Punkte auf einem n-dimensionalen Raum unabhängig voneinander auswählen, entspricht dies $(k+1)n$ Parametern. Hinzu kommt die Dimension k des k-ten Sekantenraumes.

Leider kann die Dimension echt kleiner als die rechte Seite werden, zum Beispiel wenn $\nu_d(\mathbb{P}^n)$ Geraden enthält (dann kommt durch die Sekante keine Dimension hinzu) oder wenn die Menge zu „flach “ ist (z.B. schon in einem m-dimensionalem ($m < N-1$) projektiven Unterraum des $\mathbb{P}^{N-1}$ enthalten wäre). Dies ist etwa für Quadriken der Fall (Satz 3.3). Dort hatten wir gesehen, dass wir $n+1$ Summanden benötigen. Würde hingegen im Lemma für $d = 2$ Gleichheit gelten, hätten wir $\dim Sec_k\nu_2(\mathbb{P}^n) = (k+1)n + k = \binom{n+2}{2} - 1$, also $k+1 = \frac{n+2}{2} < n+1$.
Dagegen gibt es für höhere Grade das schöne Resultat, dass in fast allen Fällen Gleichheit gilt.

Theorem 3.9 (Satz von Alexander-Hirschowitz). *Sei $d \geq 3$. Dann ist*

$$\dim Sec_k\nu_d(\mathbb{P}^n) = \min\{N-1, (k+1)n + k\}$$

für alle Tripel (n, d, k) mit Ausnahme der vier Fälle

$$(n, d, k) = (4, 3, 6), (2, 4, 4), (3, 4, 8), (4, 4, 13).$$

Durch Umstellen folgern wir:

Korollar 3.10. *Fast alle homogenen Polynome vom Grad $d \geq 3$ in $\mathbb{C}[x_0, \dots x_n]$ lassen sich als Summe $L_1^d + \cdots + L_{k+1}^d$ schreiben, wenn*

$$k + 1 \geq \frac{\binom{n+d}{d}}{(n+1)}$$

ist, mit Ausnahme der Fälle $(n, d) = (4, 3), (2, 4), (3, 4), (4, 4)$.

In den Ausnahmefällen stellt sich heraus, dass wir mit einem zusätzlichen Summanden auskommen (d.h. $8, 6, 10$ bzw. 15). Das $k + 1$ kommt in den Summationsindex, da ja einer k-Sekante $k + 1$ Summanden entsprechen (etwa im Geradenfall, also bei $k = 1$, zwei Summanden).

Beispiele:
1. Der einfachste Fall ist die verdrehte Kubik im $\mathbb{P}^3$, also $n = 1$, $d = 3$. Wir erhalten $k + 1 = 4/4 = 1$, also die Geradensekanten (und -tangenten) der Kurve füllen den Raum. Daher ist fast jedes homogene Polynom 3. Grades in zwei Unbekannten als Summe zweier Potenzen darstellbar. Äquivalent dazu ist die Aussage (wenn wir wieder von homogenen zu inhomogenen Polynomen übergehen, indem wir $x_0 = 1$ setzen), dass fast jedes Polynom in einer Variablen vom Grad ≤ 3 Summe zweier Kuben von Linearformen ist. Hier sehen wir auch, dass echte Ausnahmepunkte existieren, denn z.B. x ist nicht als Summe zweier Kuben darstellbar (siehe 3.1).
2. Im Fall von $n = d = 5$ und $n = 4$, $d = 6$ erhalten wir

$$k + 1 = \frac{\binom{5+5}{5}}{5+1} = \frac{252}{6} \text{ bzw. } k + 1 = \frac{\binom{4+6}{4}}{4+1} = \frac{210}{5},$$

also in beiden Fällen DIE ANTWORT:

42

The End