Der Vier-Quadrate-Satz von Lagrange

DBW

Herbst 2017

1 Was bewies Lagrange eigentlich?

Joseph Louis Lagrange bewies im achtzehnten Jahrhundert den folgenden Satz: Jede natürliche Zahl ist als Summe vierer Quadratzahlen (Null inklusive) darstellbar. So haben wir zum Beispiel:

$$0 = 0^2 + 0^2 + 0^2 + 0^2\,, \qquad 1 = 1^2 + 0^2 + 0^2 + 0^2\,, \qquad 2 = 1^2 + 1^2 + 0^2 + 0^2\,,$$
$$3 = 1^2 + 1^2 + 1^2 + 0^2\,, \qquad 4 = 1^2 + 1^2 + 1^2 + 1^2\,, \qquad 5 = 2^2 + 1^2 + 0^2 + 0^2\,.$$

Da $4 = 2^2$ könnte man sich fragen, ob die Darstellung mit Quadratzahlen vielleicht auch mit weniger ginge. Aber bei der Zahl 7 sieht man schon, dass man mindestens 4 Quadratzahlen braucht: $7 = 4 + 1 + 1 + 1$. Die wirklich essentielle Aussage von Lagrange ist also, dass man niemals mehr als 4 Quadratzahlen; schlimmer als bei der 7 gibt es nicht.
Im folgenden Text werden wir einige Teile aus dem Beweis durchnehmen, welchen Lagrange für seinen Satz gegeben hat. So kann man sich den ganzen Beweis mit den angebotenen Zutaten zusammenstellen. Die Zutaten habe ich nicht selbst zusammen gefunden, auch habe ich nicht den Originaltext von Lagrange gelesen. Meine Quelle war die zu diesem Thema hervorragende (englische) Wikipedia-Seite. Meine Notation hat sich automatisch etwas an sie angelehnt.

2 Eine Identität von Euler

Betrachten wir folgende Identität

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2\,.$$

Was sagt uns diese Identität? Falls $X = a^2 + b^2$ und $Y = c^2 + d^2$ Summen zweier Quadratzahlen sind, so ist auch ihr Produkt XY eine Summe zweier Quadratzahlen. Obige Identität schaut zuerst etwas gekünstelt aus, und vielleicht scheint sie eine algebraische Zufälligkeit zu sein. Ist sie aber nicht!
Betrachten wir die komplexen Zahlen $Z_1 = a + bi$ und $Z_2 = c + di$. Ihre Normen sind dann gegeben durch $|Z_1|^2 = a^2 + b^2$ und $|Z_2|^2 = c^2 + d^2$. Die Norm des Produkts $Z_1 Z_2 = (ac - bd) + (ad + bc)i$ ist durch $|Z_1 Z_2|^2 = (ac - bd)^2 + (ad + bc)^2$ gegeben. Da aber auch gilt $|Z_1 Z_2| = |Z_1|\,|Z_2|$ sieht man, dass die obige Identität eben kein Zufallstreffer ist.
Für Summen von vier Quadraten gilt eine ähnliche Schlussfolgerung: Falls $X = x_1^2 + x_2^2 + x_3^2 + x_4^2$ und $Y = y_1^2 + y_2^2 + y_3^2 + y_4^2$ Summen vierer Quadratzahlen sind, so ist das Produkt XY auch eine Summe vierer Quadratzahlen. Auch hier ist eine Identität als Begründung anzuführen, und diese heißt auch wohl Identität von Euler:

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) =& (-x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &+ (x_1y_3 + x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)^2\end{aligned}$$

Auch diese Identität ist keine Zufälligkeit, nur muss man aber etwas mit den Quaternionen herumspielen. Dazu habe ich dann am Ende einen Abschnitt über Quaternionen zusammengestellt.

3 Reduktion auf Primzahlen

Mit der Identität von Euler sieht man folgendes: Falls jede Primzahl als Summe von vier Quadraten zu schreiben ist, so auch jede ganze Zahl. Denn falls n eine ganze Zahl ist, aber keine Primzahl, so ist n als Produkt von $p_1 \cdots p_k$ zu schreiben. Wie folgt konstruiert man dann eine Darstellung von n als Summe vierer Quadratzahlen. Erstens findet man für alle Primzahlen $p_1, \ldots, p_k$ eine Darstellung als Summe von vier Quadratzahlen. Mit der Formel von Euler findet man dann eine Darstellung von $p_1 p_2$ als Summe von Quadratzahlen. Danach, aber wieder mit der Formel von Euler, eine Darstellung als Summe von vier Quadratzahlen von $p_1 p_2 p_3$ und so weiter, bis man eine Darstellung als Summe von vier Quadratzahlen von n hat.
Falls man für die Reduktion auf Primzahlen ein Interesse an einem etwas formaleren Beweis hat: Es sei $\mathcal{N}$ die Menge aller natürlichen Zahlen, für welche es keine Darstellung als Summe vierer Quadratzahlen gibt. Wir wissen schon, dass $0 \notin \mathcal{N}$ und $1 \notin \mathcal{N}$. Falls $\mathcal{N} \neq \emptyset$, so gibt es ein kleinstes Element $n > 1$, welches nicht als Summe vierer Quadratzahlen darstellbar ist. Da per Annahme n keine Primzahl sein kann, muss n zusammengesetzt sein, und somit gibt es eine Primzahl $p > 1$, die n teilt. Daher $n = n'p$. Da $n' < n$, ist n' als Summe vierer Quadratzahlen darstellbar. Aber dann sind p und n' als Summe vierer Quadratzahlen darstellbar, und daher mit der Formel von Euler n auch! Dies ist ein Widerspruch und beweist, dass der Satz bewiesen ist, falls er für Primzahlen bewiesen werden kann.

4 Quadrate modulo p

Wir schreiben $\mathbb{Z}_p = \mathbb{Z}/p \cdot \mathbb{Z}$ für die Restklassen modulo p. Oft werden wir representanten zwischen 0 und p wählen.
Jetzt nehmen wir an, dass $p > 2$. Betrachten wir die Menge aller Quadrate modulo p. Es sei $0 \leq x \leq (p-1)/2$, dann $(p-x)^2 = p^2 - 2px + x^2 \equiv x^2$ modulo p. Somit gibt es höchstens $(p+1)/2$ Quadrate, nämlich, die Quadrate 0^2, 1^2, 2^2 bis $(\frac{p-1}{2})^2$. Wir werden jetzt zeigen, dass es genau diese $(p+1)/2$ sind. Nehmen wir dazu an, $a^2 \equiv b^2$ modulo p, dann also $(a-b)(a+b) \equiv 0$ modulo p. Also muss p entweder $a-b$ oder $a+b$ (oder beide) teilen. Im ersten Fall gilt $a \equiv b$ modulo p und im zweiten Fall $a \equiv -b$ modulo p, was realisiert werden kann, indem wir $a = p - b$ wählen, sodass $0 \leq a, b < p$. Man realisiert sich bald, dass Folgendes gilt: Falls in $\mathbb{Z}_p$ die Gleichung $x^2 = a$ lösbar ist, so ist entweder $a = 0$ und es gibt eine Wurzel, oder $a \neq 0$ und es gibt zwei unterschiedliche Wurzeln.
Diejenigen, die nur am Beweise des Satzes von Lagrange interessiert sind, können gleich zum weiteren Abschnitt fortfahren. Falls man die obige Schlussfolgerung anders beweisen möchte, so lese man auch den nächsten Absatz und seine Schlussfolgerung:
Falls p eine Primzahl ist, bilden die Restklassen modulo p einen Körper. Tatsächlich ist jedes Element $x \in \mathbb{Z}_p$, das nicht Null ist, invertierbar. Das kann man wie folgt leicht einsehen: Es seien $0, 1, \ldots, p-1$ alle Restklassen modulo p und x sei nicht ein Vielfaches von p. Wir multiplizieren jedes Element in $\mathbb{Z}_p$ mit x. Wir bekommen dann wieder Restklassen modulo p. Nehmen wir an, es gibt zwei Elemente y_1 und y_2 in $\mathbb{Z}_p$ die dann auf dasselbe Element abgebildt werden, also $xy_1 \equiv xy_2$ modulo p. Dann also $x(y_1 - y_2) \equiv 0$ modulo p. Das bedeutet also, dass $x(y_1 - y_2)$ ein Vielfaches von p ist. Die Primfaktorzerlegung von $x(y_1 - y_2)$ muss also einen Faktor p enthalten. In der Primfaktorzerlegung von x kann dieser aber nicht sein, denn x ist nicht Null modulo p. Somit muss $y_1 - y_2$ durch p teilbar sein, was aber bedeutet $y_1 \equiv y_2$ modulo p. Somit wird die Menge der Restklassen $\mathbb{Z}_p$ durch die Multiplikation eins zu eins auf $\mathbb{Z}_p$ selbst abgebildet. Somit gibt es auch einen $y \in \mathbb{Z}_p$ mit $xy \equiv 1$ modulo p. Also ist x invertierbar.
Sei a ein Element von $\mathbb{Z}_p$, und betrachte das Polynom $X^2 - a$. Falls a eine Quadratzahl ist, so gilt $X^2 - a = X^2 - b^2 = (X-b)(X+b)$ für irgendein $b \in \mathbb{Z}_p$. Ein Polynom von Grad zwei kann aber höchstens zwei Nullstellen haben, somit hat jede Zahl höchstens zwei Wurzeln in $\mathbb{Z}_p$.

5 Das Schubfachprinzip

Es sei p eine Primzahl. Betrachten wir zwei Teilmengen von $\mathbb{Z}_p$: Q_1 enthält alle Quadratzahlen in $\mathbb{Z}_p$, und Q_2 enthält alle $-x^2-1$, wobei x alle Elemente von $\mathbb{Z}_p$ durchläuft:

$$Q_1 = \{0^2 = 0, 1^2 = 1, 2^2, \dots p^2 \equiv 0\}\,, \quad Q_2 = \{-0^2 - 1 \equiv p-1, -1^2 - 1 \equiv -2\,, \dots - p^2 - 1 \equiv p-1\}\,.$$

Wir wissen schon, dass Q_1 genau $(p+1)/2$ Elemente enthält, und daher enthält auch Q_2 genau $(p+1)/2$ Elemente. Beide zusammen haben also $p+1$ Elemente, genau 1 mehr, als es Restklassen modulo p gibt. Somit können sie nicht ganz unterschiedlich sein und es muss ein gemeinsames Element geben – dies ist das Schubfachprinzip: wenn man mehr Objekte als Schubfächer hat, dann wird beim Belegen der Schubfächer mit den Objekten ein Schubfach von mindestens zwei Objekten belegt werden. Somit gibt es a und b, sodass

$$a^2 + b^2 + 1 \equiv 0 \text{ (modulo } p)$$

m.a.W. es gibt eine ganze Zahl m, sodass

$$a^2 + b^2 + 1^2 + 0^2 = mp\,.$$

Für jede Primzahl gibt es also ein Vielfaches dieser Primzahl, welche sich also Summe von 4 Quadraten (sogar von drei) schreiben lässt. Um diese Tatsache gut ausnutzen zu können, definieren wir die Menge $\mathcal{M}$ als die Menge aller positiven ganzen Zahlen m, sodass mp sich als Summe von vier Quadratzahlen schreiben lassen. Dann wissen wir also, dass $\mathcal{M} \neq \emptyset$. Aber dann hat $\mathcal{M}$ ein minimales Element. Unsere Aufgbae ist es jetzt, zu zeigen, dass dieses minimale Element 1 ist.

6 Unendlcher Abstieg nach Fermat

Die Methode von Fermat ist eine, die oft angewand wird, um zu beweisen, dass $\sqrt{n}$ eine irrationale Zahl ist, falls n eben keine Quadratzahl ist. Sie benutzt die Tatsache, dass jede Untermenge der Menge der natürlichen Zahlen größer als Null ein kleinstes Element hat. Somit kann es keine unendliche strikt fallende Abfolge von Zahlen aus einer Teilmenge von $\mathbb{N}$ geben. Wir werden jetzt beweisen, dass die Menge $\mathcal{M}$ ein minimales element $m = 1$ hat.
Nehmen wir an, dass das minimale Element von $\mathcal{M}$ eine Zahl $m \neq 1$ ist. Somit gibt es also x_1, x_2, x_3 und x_4 sodass

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp > p\,.$$

Zu jedem x_i können wir ein eindeutiges y_i finden, sodass (1) $x_i \equiv y_i$ modulo m und (2) $-(m-1)/2 \leq y_i \leq m/2$. Man beachte also, dass man auf Restklassen modulo m übergeht! Das für y_i angegebene Intervall hat Länge $m - \frac{1}{2}$ und enthält also auf jeden Fall einen Endpunkt und daher genau m ganze Zahlen, somit kann man immer y_i genau in dem Intervall finden. In dieser Phase des Beweises ist es sinnvoll, anzumerken, dass die Annahme $m > 1$ hier essentiel ist, denn modulo 1 rechnen reduziert alle Zahlen auf 0.
Wir schreiben $x_i = l_i m + y_i$, wobei die l_i ganze Zahlen sind, sodass $x_i^2 \equiv y_i^2$ modulo m. Die Summe der Quadrate der y_i ergibt also Null modulo m. Daher gibt es eine ganze Zahl r, sodass

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = mr\,.$$

Welche Eigenschaften hat nun diese Zahl r? Erstens ist mal klar, dass sie nicht negativ ist, aber kann sie Null sein?
Damit sie Null ist, müssen also y_i Null sein. Somit sind alle x_i ein Vielfaches von m: $x_i = l_i m$ und daher ist $x_1^2 + x_2^2 + x_3^2 + x_4^2$ durch m^2 teilbar. Aber die Summe der Quadrate ist gleich mp und p ist

eine Primzahl, somit ist mp nicht durch m^2 teilbar. Wir erreichen also einen Widerspruch, wenn alle y_i Null sind. Somit kann r nicht Null sein.
Die höchstmögliche Zahl, die r sein könnte, finden wir, falls wir y_i so wählen, dass $|y_i|$ ihre größtmöglichen Werte haben, also wenn $y_i = m/2$. In diesem Fall haben wir $x_i = l_i m + m/2$, sodass $x_i^2 = l_i^2 m^2 + l_i m^2 + m^2/4$. In diesem Fall ist die Summe der Quadrate der x_i wieder durch m^2 teilbar, was nicht sein kann. Somit finden wir eine strikte Ungleichung:

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 < \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4} = m^2 \,.$$

Somit gilt $r < m$. Alles in allem finden wir also, dass $0 < r < m$.
Nun kommt ein gewalt guter Schritt: Betrachte das Produkt

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2) = mpmr = m^2 pr \,.$$

Wir wissen schon, dass wir die linke Seite als Summe vierer Quadrate schreiben können, und zwar also die Summe der Quadrate von

$$\begin{aligned} z_1 &= x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4 \\ z_2 &= x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3 \\ z_3 &= x_1 y_3 - x_3 y_1 + x_4 y_2 - x_2 y_4 \\ z_4 &= x_1 y_4 - x_4 y_1 + x_2 y_3 - x_3 y_2 \end{aligned}$$

und man beobachte, dass alle z_i durch m teilbar sind. Tatsächlich finden wir

$$z_1 = x_1(x_1 - l_1 m) + x_2(x_2 - l_2 m) + x_3(x_3 - l_3 m) + x_4(x_4 - l_4 m) = mp - (l_1 + l_2 + l_3 + l_4)m$$

aber auch

$$z_2 = x_1(x_2 - l_3 m) - x_2(x_1 - l_1 m) + x_3(x_4 - l_4) - x_4(x_3 - l_3 m) = m(l_1 - l_2 + l_3 - l_4) \,.$$

Ganz ähnliche Berechnungen zeigen, dass alle z_i durch m teilbar sind. (Man beobachte, dass die Struktur der z_1, z_2 und z_3 so ist, dass jeweils ein Term vorkommt, und dazu der Term mit den Indizes ausgetauscht und dem Vorzeichen umgedreht.)
Die Zahlen $w_i = z_i/m$ sind also ganze Zahlen, und wir haben

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = \frac{m^2 pr}{m^2} = rp \,.$$

Somit ist auch $r \in \mathcal{M}$ und m ist kein kleinstes Element mehr, da $m > r > 0$. Dies ist ein Widerspruch zur Annahme eines kleinsten Elementes $m > 1$. Darum ist das kleinste Element 1, und p ist als Summe vierer Quadratzahlen darstellbar.
Somit ist jede Primzahl als Summe vierer Quadratzahlen darstellbar, und daher jede natürliche Zahl.

7 Appendix: Quaternionen

In diesem Abschnitt erwähnen wir einiges über die Quaternionen, damit man den Hintergrund zur Identität von Euler etwas mehr versteht, oder sich besser an sie erinnern kann.
Die Menge der Quaternionen kann man als vierdimensionalen Vektorraum über die reellen Zahlen betrachten. Oder einfach als Erweiterung der Menge der komplexen Zahlen. Es gibt vier Basiseinheiten: 1, i, j und k, welche folgende Gleichugen erfüllen:

$$1^2 = 1 \,, \quad i^2 = j^2 = k^2 = -1 \,.$$

Bei der Multiplikation zwischen den i, j und k wird es aber recht interessant: die Multiplikation ist nicht kommutativ und durch folgende Regeln gegeben:

$$ij = k\,, \quad jk = i\,, \quad ki = j\,,$$

$$ji = -k\,, \quad kj = -i\,, \quad ik = -j\,.$$

Ein Quaternion ist dann ein Objekt von der Form $q = a \cdot 1 + b \cdot i + c \cdot j + d \cdot k$ wobei a, b, c, d reelle Zahlen sind.
Wie kann man sich die Quaternionen vorstellen? Im Prinzip genau so wie die komplexen Zahlen, nur halt etwas vierdimensional ... Eine Realisierungen anhand komplexer zwei-mal-zwei Matrizen ist möglich. Betrachte dazu die Pauli-Matrizen:

$$\sigma_1 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\,, \quad \sigma_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\,, \quad \sigma_3 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\,.$$

Man rechnet leicht nach, dass die Identifikation $i \leftrightarrow \sigma_1$, $j \leftrightarrow \sigma_2$ und $k \leftrightarrow \sigma_3$ eine Realisierung der Quaternionen als Matrizen ermöglicht, denn die Pauli-Matrizen erfüllen dieselben Bedingungen wie die Quaternionen.
Es gibt auch eine Darstellung ohne komplexe Zahlen, welche aber dann vierdimensionale Matrizen braucht:

$$i \leftrightarrow \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}\,, \quad j \leftrightarrow \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}\,, \quad k \leftrightarrow \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}\,.$$

Man kann also die i, j und k als Abkürzungen für Matrizen sehen, wenn man will. Dies erleichtert vielleicht die Vorstellung nicht so gigantisch viel, aber man eine mathematische Existenz der Quaternionen, falls diese etwas bedeutet, leichter begründen. Übrigens spielen die oben genannten Pauli-Matrizen bei der Darstellung der Rotationsgruppe eine wesentliche Rolle und an vielen Stellen in der Quantenmechanik tauchen sie auf. Die 4×4-Matrizen sind eine Abwandlung einiger sogenannten Dirac-Matrizen, welche bei den Darstellungen von Fermionen eine wichtige Rolle spielen.
Die Darstellung als 2×2-Matrizen ist besonders bequem und sie respektiert (genau so wie die vierdimensionale) eine wichtige Regel: die Darstellung des Produkts ist das (Matrix-)Produkt der Darstellungen. Seien dazu $q_1 = a + bi + cj + dk$ und $q_2 = w + xi + yj + zk$, dann

$$q_1 q_2 = (aw - bx - cy - dz) + (ax + bw + cz - dy)i + (ay + wc + dx - bz)j + (az + dw + by - cx)k$$

und das Ausmultiplizieren von

$$\begin{pmatrix} a + di & -c + bi \\ c + bi & a - di \end{pmatrix} \begin{pmatrix} w + zi & -y + xi \\ y + xi & w - zi \end{pmatrix}$$

ergibt

$$\begin{pmatrix} aw - zd - yc - xb + i(az + dw + by - cx) & -ay - xd - wc + bz + i(ax - dy + cz - bw) \\ wc - bz + ay + dx + i(wb + zc + xa - dy) & -yc - bx + aw - dz + i(-yb + xc - az - wd) \end{pmatrix}$$

was genau die Matrixdarstellung des Produkts darstellt.
Die konjugierte eines Quaternions $q = a + bi + cj + dk$ ist durch $\overline{q} = a - bi - cj - dk$ definiert. Man verifiziert leicht, dass

$$q\overline{q} = \overline{q}q = a^2 + b^2 + c^2 + d^2$$

was eine nicht negative reelle Zahl ist.
Die Norm eines Quaternions $q = a + bi + cj + dk$ ist durch $N(q) = \sqrt{a^2 + b^2 + c^2 + d^2}$ definiert. Stellen wir uns q als 2×2-Matrix vor, so ist

$$q = \begin{pmatrix} a + di & -c + bi \\ c + bi & a - di \end{pmatrix}.$$

Die Determinante dieser Matrix ist durch $(a + bi)(a - bi) - (-c + di)(c - di) = a^2 + b^2 + c^2 + d^2$, also durch das Quadrat der Norm.
Die Invertierbarkeit eines Quaternions hängt stark von der Norm ab: Ein Quaternion ist invertierbar genau dann, wenn die Norm nicht Null ist. Um dies einzusehen, kann man wie folgt vorgehen. Die Inverse Matrix von

$$\begin{pmatrix} a + di & -c + bi \\ c + bi & a - di \end{pmatrix}$$

existiert nur, wenn die Determinante nicht Null ist, und ist dann gegeben durch

$$\frac{1}{a^2 + b^2 + c^2 + d^2} \begin{pmatrix} a - di & c - bi \\ -c - bi & a + di \end{pmatrix}$$

wie man leicht nachrechnet. Aber dann ist die Inversen von $q = a + bi + cj + dk$ durch $q^{-1} = \frac{1}{N(q)^2}(a - bi - cj - dk)$ gegeben, also duch

$$q^{-1} = \frac{1}{N(q)^2}\overline{q}.$$

Seien q_1 und q_2. Dann gilt $N(q_1q_2) = N(q_1)N(q_2)$. Eine Begründung für diese Gleichheit kommt von der Darstellung der Quaternionen als komplexe 2×2-Matrizen, denn für Matrizen A und B gilt $\det(AB) = \det(A)\det(B)$, und das Matrixprodukt entspricht das Quaternionprodukt. Natürlich kann man auch einfach ausmultiplizieren.
Die Identität von Euler ist dann nichts anderes als $N(q_1)^2N(q_2)^2 = N(q_1q_2)^2$. Also

$$(a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2) = (aw-bx-cy-dz)^2+(ax+bw+cz-dy)^2+(ay+wc+dx-bz)^2+(az+dw+by-cx)^2$$

oder durch einere ästhetischer Wahl der Variablen und das Umdrehen einiger Vorzeichen in einem Quadrat:

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) =& (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2\end{aligned}$$

Die Wahl der Variablen ist hierbei: $x_1 = a$, $x_2 = b$, $x_3 = c$, $x_4 = d$, $y_1 = -w$, $y_2 = x$, $y_3 = y$, $y_4 = z$; also, fast wie man es erwarten würde, außer $y_1 = -w$, wo man ein Vorzeichen ändert.