Alexander Schmidt

Einführung in die algebraische Zahlentheorie

Springer-Lehrbuch

Springer
Berlin Heidelberg New York
ISBN 978-3-540-45973-6

Kapitel 7

Der Große Fermatsche Satz

Die folgende Behauptung wurde 1637 von Fermat aufgestellt, wird verwirrenderweise Großer Fermatscher Satz genannt und wurde erst im Jahr 1994 von A. Wiles [Wi, TW] bewiesen.

Großer Fermatscher Satz (Wiles). *Für jede natürliche Zahl $n \geq 3$ hat die Gleichung*

$$X^n + Y^n = Z^n$$

keine nichttrivialen (d.h. $xyz \neq 0$) Lösungen $(x, y, z) \in \mathbb{Z}^3$.

Um Wiles' Beweis wiederzugeben, der auf den Techniken der arithmetischen algebraischen Geometrie und auf der Theorie der Modulformen beruht, fehlen uns in diesem Buch die Voraussetzungen. Wir werden den Großen Fermatschen Satz nur für kleine Exponenten beweisen und einige Ergebnisse ohne Beweis vorstellen.

Zunächst kann man die in Frage kommenden Exponenten n einschränken. Jede natürliche Zahl $n \geq 3$ ist durch 4 oder durch eine ungerade Primzahl p teilbar. Durch Ausklammern gibt uns daher jede nichttriviale Lösung der Gleichung $X^n + Y^n = Z^n$ eine nichttriviale Lösung der Gleichung $X^4 + Y^4 = Z^4$ oder eine nichttriviale Lösung einer Gleichung $X^p + Y^p = Z^p$ mit einer ungeraden Primzahl p. Um den Großen Fermatschen Satz zu beweisen, genügt es daher, diese beiden Fälle zu betrachten.

7.1 Der Fall $n = 4$

Im Fall $n = 4$ ist der Beweis elementar. Man kann sogar etwas mehr zeigen.

Satz 7.1.1. *Die Gleichung*

$$X^4 + Y^4 = Z^2$$

hat keine nichttrivialen ganzzahligen Lösungen.

Der Beweis beruht auf der Technik des „unendlichen Abstiegs“, d.h., gäbe es eine nichttriviale Lösung, so gäbe es auch eine in geeignetem Sinne kleinere nichttriviale Lösung.

Beweis. Angenommen die Gleichung hätte nichttriviale ganzzahlige Lösungen. Unter diesen sei (x, y, z) eine Lösung mit kleinstmöglichem Wert $|z| \in \mathbb{N}$. Wir werden aus (x, y, z) eine weitere nichttriviale Lösung (x', y', z') mit $|z'| < |z|$ konstruieren. Dies widerspricht der Annahme über (x, y, z) und zeigt den Satz.

Wir können o.B.d.A. annehmen, dass $x, y, z > 0$ gilt. Wären x und y nicht teilerfremd und p eine Primzahl mit $p \mid x$, $p \mid y$, so folgte $p^4 | z^2$ und daher $p^2 | z$. Die Gleichung

$$\left(\frac{x}{p}\right)^4 + \left(\frac{y}{p}\right)^4 = \left(\frac{z}{p^2}\right)^2$$

liefert dann eine weitere Lösung der Gleichung $X^4 + Y^4 = Z^2$ mit betragsmäßig kleinerer dritter Komponente. Analog schließt man, wenn $(x, z) > 1$ oder $(y, z) > 1$ ist. Also können wir x, y und z als paarweise teilerfremd annehmen. Die Zahlen x und y können nicht beide ungerade sein, weil sonst $z^2 \equiv 2 \mod 4$ gelten würde, was nicht möglich ist. Sei o.B.d.A. x ungerade, y gerade, also z ungerade. Wir schreiben die Gleichung in der Form

$$y^4 = (z - x^2)(z + x^2)$$

und betrachten den größten gemeinsamen Teiler $d = (z - x^2, z + x^2)$. Zunächst gilt $2 | d$. Gäbe es eine ungerade Primzahl p mit $p \mid d$, so folgte $p \mid 2z$, $p \mid 2x^2$, im Widerspruch zu $(x, z) = 1$. Wegen $4 \nmid 2z$ gilt $d = 2$. Das Produkt von $z - x^2$ und $z + x^2$ ist eine vierte Potenz. Wäre $z - x^2$ genau einmal durch 2 teilbar, gäbe es ganze Zahlen a, b mit $(a, b) = 1$, $2 \nmid a$ und $z - x^2 = 2a^4$, $z + x^2 = 8b^4$. Dies ist nicht möglich, weil dann $x^2 = 4b^4 - a^4$ kongruent -1 modulo 4 wäre. Daher ist $z + x^2$ genau einmal durch 2 teilbar, und es existieren ganze Zahlen a, b, $(a, b) = 1$, $2 \nmid b$ mit

$$\begin{aligned} z - x^2 &= 8a^4 \\ z + x^2 &= 2b^4. \end{aligned}$$

Aus $a = 0$ würde $z^2 = x^4$, also $y = 0$ folgen. Daher können wir o.B.d.A. $a, b > 0$ annehmen. Wegen $(a, b) = 1$ und $x^2 = b^4 - 4a^4$ gilt $(b, x) = 1$. Für eine ungerade Primzahl p folgen aus $p \mid (b^2 - x)$ und $p \mid (b^2 + x)$ die Aussagen $p | b$ und $p | x$. Daher gilt $(b^2 - x, b^2 + x) = 2$. Aus der Gleichung

$$4a^4 = (b^2 - x)(b^2 + x)$$

schließen wir die Existenz von $c, d \in \mathbb{Z}$ mit

$$\begin{aligned} b^2 - x &= 2c^4 \\ b^2 + x &= 2d^4 \ . \end{aligned}$$

So erhalten wir die Gleichung

$$c^4 + d^4 = b^2.$$

Wegen $2b^4 = z + x^2 \leq z^2 + x^4 < 2z^2$ folgt $b < z$. Mit (c, d, b) haben wir eine neue nichttriviale Lösung der Gleichung $X^4 + Y^4 = Z^2$ mit betragsmäßig kleinerer dritter Komponente gefunden. Wie am Anfang erklärt, beendet dies den Beweis. □

7.2 Der Satz von Sophie Germain

Von jetzt an sei $n = p$ eine ungerade Primzahl. Bei der Untersuchung der Gleichung

$$X^p + Y^p = Z^p$$

hat man seit jeher die folgende Fallunterscheidung gemacht.

1. Die Suche nach (nichttrivialen) Lösungen (x, y, z) mit $p \nmid xyz$, der sogenannte „erste Fall".
2. Die Suche nach nichttrivialen Lösungen (x, y, z) mit $p \mid xyz$, der sogenannte „zweite Fall".

Diese Fallunterscheidung taucht implizit auch in Wiles' Beweis auf. Das nächste Theorem beschreibt eine interessante Methode, den ersten Fall zu behandeln. Sie stammt von Sophie Germain.

Theorem 7.2.1. *Sei p eine ungerade Primzahl, so dass $2p + 1$ wieder eine Primzahl ist. Dann hat die Gleichung*

$$X^p + Y^p + Z^p = 0$$

keine ganzzahlige Lösung (x, y, z) mit $p \nmid xyz$.

Beweis. Sei $q = 2p + 1$ und (x, y, z) eine nichttriviale Lösung mit paarweise teilerfremden $x, y, z \in \mathbb{Z}$. Wir formen die Ausgangsgleichung in

$$(-z)^p = x^p + y^p = (x + y)(y^{p-1} - xy^{p-2} + \cdots + x^{p-1})$$

um. Wegen $p \nmid z$ gilt $p \nmid (x + y)$. Sei r ein Primteiler des größten gemeinsamen Teilers von $x + y$ und $y^{p-1} - xy^{p-2} + \cdots + x^{p-1}$. Dann gilt $r \neq p$ und $x \equiv -y \bmod r$. Daher gilt

$$0 \equiv y^{p-1} - xy^{p-2} + \cdots + x^{p-1} \equiv py^{p-1} \mod r.$$

Wir erhalten $r|y$ und folglich auch $r|z$ im Widerspruch zur Teilerfremdheit von y und z. Also gilt

$$(x + y, y^{p-1} - xy^{p-2} + \cdots + x^{p-1}) = 1.$$

Wegen der Eindeutigkeit der Primfaktorzerlegung existieren $a, t \in \mathbb{Z}$ mit

$$\begin{aligned} x + y &= a^p \\ y^{p-1} - xy^{p-2} + \cdots + x^{p-1} &= t^p. \end{aligned}$$

Aus Symmetriegründen erhalten wir auch ganze Zahlen b, c, s, u mit

$$\begin{aligned} x+z &= b^p \\ y+z &= c^p \\ z^{p-1}-yz^{p-2}+\cdots+y^{p-1} &= s^p \\ x^{p-1}-zx^{p-2}+\cdots+z^{p-1} &= u^p. \end{aligned}$$

Wegen $2p+1=q$ ist eine p-te Potenz stets kongruent 0, 1 oder -1 modulo q. Aus $q>3$ und der Kongruenz

$$x^p+y^p+z^p=0\equiv 0 \mod q$$

folgt, dass eine der drei Zahlen x,y,z durch q teilbar ist. O.B.d.A. gelte $q\,|\,x$. Die Zahlen y und z sind dann nicht durch q teilbar. Wir erhalten

$$q\,|\,2x=a^p+b^p-c^p.$$

Wieder nehmen die Summanden nur die Werte $0,\pm 1$ modulo q an und wir erhalten, dass eine der Zahlen a, b, c durch q teilbar ist. Wegen der paarweisen Teilerfremdheit von x, y und z und da x durch q teilbar ist, kann dies nur c sein. Außerdem folgt $q\,|\,(a^p+b^p)=(2x+y+z)$. Also gilt $y\equiv -z \bmod q$, und wir erhalten

$$s^p=z^{p-1}-yz^{p-2}+\cdots+y^{p-1}\equiv py^{p-1} \mod q.$$

Da weder y noch p durch q teilbar sind, gilt $py^{p-1}\equiv\pm 1 \bmod q$.

Nun gilt $(-z)^p=x^p+y^p=(x+y)t^p$. Modulo q schließen wir die Kongruenz $y^p\equiv yt^p$ und unter erneuter Verwendung von $2p+1=q$ erhalten wir $y\equiv\pm 1 \bmod q$. Folglich gilt $y^{p-1}\equiv 1 \bmod q$ und wir erhalten

$$\pm 1\equiv py^{p-1}\equiv p \mod q.$$

Aber wegen $q=2p+1$ kann p nicht kongruent ± 1 modulo q sein. Der gefundene Widerspruch zeigt die Aussage des Theorems. □

Theorem 7.2.1 wendet sich z.B. auf $p=3,5,11,23$ an. Es ist nicht bekannt, ob es unendlich viele Primzahlen p gibt, so dass $2p+1$ auch eine Primzahl ist.

7.3 Kummers Theorem

In diesem Abschnitt stellen wir, ohne Beweise zu geben, E. KUMMERs Resultate zum Großen Fermatschen Satz vor.

Substituiert man $T=\frac{X}{-Y}$ in der Zerlegung $T^p-1=\prod_{i=0}^{p-1}(T-\zeta_p^i)$, erhält man die Identität

$$X^p+Y^p=\prod_{i=0}^{p-1}(X+\zeta_p^i Y).$$

Kummers Idee war es, diese Identität auszunutzen, um die Fermat-Gleichung zu behandeln. Sie liegt im Körper $K=\mathbb{Q}(\zeta_p)$, den man aus den rationalen Zahlen durch Adjunktion einer p-ten Einheitswurzel erhält. Für einen modernen Beweis des folgenden Theorems sei der Leser auf [Wa], Thm. 6.23 und Thm. 9.3 verwiesen.

Theorem 7.3.1 (Kummer). *Sei p eine ungerade Primzahl und $K = \mathbb{Q}(\zeta_p)$. Gilt $p \nmid h_K$, so hat die Gleichung*

$$X^p + Y^p = Z^p$$

keine nichttriviale ganzzahlige Lösung.

Die Voraussetzung $p \nmid h_K$ kann in dem Sinne abgeschwächt werden, dass h_K „nicht oft“ durch p teilbar ist. Es war lange Zeit die Hoffnung, dass man diese abgeschwächte Bedingung für alle p zeigen kann (getan hat man dies für alle $p < 4\,000\,000$). Die Frage, ob das für alle Primzahlen p richtig ist, ist bis heute offen. Eine positive Antwort würde einen wesentlich einfacheren Beweis des Großen Fermatschen Satzes liefern.

Sei $K = \mathbb{Q}(\zeta_p)$. Man kann zeigen (siehe [Wa], Thm. 11.1), dass $h_K = 1$ nur für die Primzahlen

$$p = 3, 5, 7, 11, 13, 17, 19$$

gilt. Man nennt p **reguläre** Primzahl, wenn die Klassenzahl h_K nicht durch p teilbar ist. Gilt $p \mid h_K$, so heißt die Primzahl p **irregulär**. Mit anderen Worten hat Kummer den Großen Fermatschen Satz für alle regulären Primzahlen gezeigt. Die kleinste irreguläre Primzahl ist $p = 37$. Die nächsten sind

$$59, 67, 101, 103, 131, 149, 157, \ \ldots \ .$$

Heuristische Überlegungen (siehe [Wa], §5.3) legen nahe, dass etwa $e^{-\frac{1}{2}} \simeq 61\%$ der Primzahlen regulär und $1 - e^{-\frac{1}{2}} \simeq 39\%$ der Primzahlen irregulär sind. Computerberechnungen stützen diese Heuristik. Bis heute weiß man aber noch nicht einmal, ob es unendlich viele reguläre Primzahlen gibt. Aber man weiß, dass es unendlich viele irreguläre gibt ([Wa], Thm. 5.17).

Wie erkennt man, ob eine Primzahl regulär ist? Zu diesem Zweck betrachtet man die **Bernoulli-Zahlen** B_n, die eindeutig durch die Potenzreihenentwicklung

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}$$

gegeben sind. Es gilt $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$ und allgemeiner $B_{2n+1} = 0$ für $n \geq 1$. Die nächsten geraden Werte sind $B_4 = -\frac{1}{30}$, $B_6 = \frac{1}{42}$, $B_8 = -\frac{1}{30}$, $B_{10} = \frac{5}{66}$, $B_{12} = -\frac{691}{2730}$. Für die Bernoulli-Zahlen gilt der

Satz 7.3.2 (von Staudt-Clausen). *Für gerades positives n gilt*

$$B_n + \sum_{p-1|n} \frac{1}{p} \in \mathbb{Z}.$$

Insbesondere ist der Nenner von B_n (in gekürzter Schreibweise) genau durch die Primzahlen p mit $(p-1)|n$ teilbar .

Wir sehen, dass 2 und 3 stets im Nenner aufgehen, und dass für gerades $n < p-1$ der Nenner von B_n prim zu p ist. Für einen Beweis des von Staudt-Clausenschen Satzes sei der Leser auf [Wa], Thm. 5.10 verwiesen. Für einen modernen Beweis des folgenden Theorems siehe [Wa], Thm. 5.34.

Theorem 7.3.3 (Kummer). *Eine Primzahl p ist genau dann irregulär, wenn der Zähler einer der Bernoulli-Zahlen*

$$B_2, B_4, \ldots, B_{p-3}$$

durch p teilbar ist.

Zum Beispiel ist der Zähler von B_{12} durch 691 teilbar, weshalb 691 irregulär ist. Theorem 7.3.3 eröffnet die Möglichkeit zu Berechnungen. Der tiefere Sinn der Bernoulli-Zahlen erhellt sich erst im Zusammenhang mit der Riemannschen Zetafunktion, siehe Abschnitt 8.4.

7.4 Der Fall $n = 3$

Da wir die Arithmetik von $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ gut kennen, können wir die Fermat-Gleichung für $n = 3$ behandeln. Wir sammeln zunächst unser Wissen über $K = \mathbb{Q}(\zeta_3)$. Wir setzen $\zeta = \zeta_3 = \frac{1}{2}(-1+\sqrt{-3})$, $\lambda = 1-\zeta = \frac{1}{2}(3-\sqrt{-3})$.

Lemma 7.4.1. (i) $h_K = 1$.
(ii) $(1, \zeta)$ *ist eine Ganzheitsbasis von* $\mathcal{O}_K$.
(iii) $(3) = \mathfrak{p}^2$ *mit* $\mathfrak{p} = (\lambda)$.
(iv) $\{0, \pm 1\}$ *ist ein vollständiges Vertretersystem für die Restklassen mod* $\mathfrak{p}$.
(v) $E_K = \{\pm 1, \pm\zeta, \pm\zeta^2\}$ *und diese Menge ist auch ein vollständiges Vertretersystem für die primen Restklassen modulo* $\mathfrak{p}^2$.
(vi) *Für* $\alpha, \beta \in \mathcal{O}_K$ *und* $k \geq 1$ *gilt:* $\alpha \equiv \beta \bmod \mathfrak{p}^k \implies \alpha^3 \equiv \beta^3 \bmod \mathfrak{p}^{k+2}$.

Beweis. Behauptung (i) kann man daraus schließen, dass $\mathcal{O}_K$ euklidisch ist (siehe Abschnitt 6.10). Alternativ kann man Theorem 6.6.11 benutzen, um zu sehen, dass jede Idealklasse ein ganzes Ideal der Norm < 2 enthält. Behauptung (ii) folgt aus Satz 6.1.10. Zu (iii) bemerkt man, dass wegen $N(\lambda) = 3$ das Ideal $\mathfrak{p} = (\lambda)$ prim ist und (3) teilt. Wegen $\Delta_K = -3$ und nach Satz 6.1.10 verzweigt die Primzahl 3 in K, also gilt $(3) = \mathfrak{p}^2$. Die Zahlen $0, \pm 1$ sind inkongruent modulo 3, also auch inkongruent modulo $\mathfrak{p}$. Wegen $\mathfrak{N}(\mathfrak{p}) = 3$ gibt es aber nur drei verschiedene Restklassen modulo $\mathfrak{p}$. Dies zeigt (iv).

Die Aussage $E_K = \{\pm 1, \pm\zeta, \pm\zeta^2\}$ folgt aus den Sätzen 6.7.2 und 6.7.3. Es gibt $\varphi(\mathfrak{p}^2) = 6$ prime Restklassen modulo $\mathfrak{p}^2 = (3)$ und die Restklassen der sechs Einheiten sind offenbar prim. Es bleibt zu zeigen, dass keine zwei Elemente aus E_K kongruent modulo $\mathfrak{p}^2$ sind. Wäre für $i, j \in \{0, 1, 2\}$, $i \neq j$,

$$\pm\zeta^i \equiv \pm\zeta^j \mod \mathfrak{p}^2,$$

so folgte $1 \equiv \pm\zeta^{j-i} \bmod \mathfrak{p}^2$, also $\mathfrak{p}^2 | (1 \pm \zeta^{j-i})$. Nun ist für $j \neq i$ das Element $1+\zeta^{j-i} = -\zeta^{2(j-i)}$ eine Einheit, weshalb dieser Fall ausscheidet. Andererseits gilt $(1-\zeta) = \mathfrak{p}$ und $(1-\zeta^2) = (-\zeta^2)(1-\zeta) = \mathfrak{p}$, weshalb für $j \neq i$ auch $1+\zeta^{j-i}$ nicht durch $\mathfrak{p}^2$ teilbar ist. Daher sind die Elemente in E_K paarweise inkongruent modulo $\mathfrak{p}^2$, was (v) zeigt. Es bleibt (vi) zu zeigen. Ist $\alpha - \beta \in \mathfrak{p}^k$, so gilt wegen $3 \in \mathfrak{p}^2$

$$\alpha^3 - \beta^3 = (\alpha-\beta)^3 + 3\alpha\beta(\alpha-\beta) \in \mathfrak{p}^{k+2}. \qquad \square$$

Satz 7.4.2. *Für $3 \mid n$ hat die Gleichung*

$$X^n + Y^n = Z^n$$

keine nichttrivialen Lösungen in $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[\zeta_3]$.

Beweis. Wir können $n = 3$ annehmen und setzen $K = \mathbb{Q}(\sqrt{-3})$. Die Gleichung ist äquivalent zu $x^3 + y^3 + (-z)^3 = 0$, d.h. $x, y, -z$ spielen symmetrische Rollen. Sei (x, y, z) eine nichttriviale Lösung. Angenommen, x, y und z wären nicht paarweise teilerfremd. Wegen $x^3 + y^3 = z^3$ gibt es dann ein Primideal $\mathfrak{q}$ mit $\mathfrak{q} | (x)$, $\mathfrak{q} | (y)$ und $\mathfrak{q} | (z)$. Wegen $h_K = 1$ gilt $\mathfrak{q} = (\alpha)$ für ein $\alpha \in \mathcal{O}_K$, und wir können x, y, z durch α teilen. Auf diese Art und Weise erhalten wir nach endlich vielen Schritten eine Lösung (x, y, z) mit paarweise teilerfremden Zahlen $x, y, z \in \mathcal{O}_K$.

Sind x, y, z alle nicht durch $\mathfrak{p} = (\lambda)$ teilbar, so gilt nach (7.4.1)(iv) und (vi)

$$\pm 1 \equiv z^3 = x^3 + y^3 \equiv (\pm 1) + (\pm 1) \equiv 0, \pm 2 \mod \mathfrak{p}^3.$$

Dies ist nicht möglich, also haben wir den „ersten Fall“ erledigt, d.h. eine der drei Zahlen x, y, z muss durch $\mathfrak{p}$ teilbar sein.

Da x, y und $-z$ symmetrische Rollen spielen, gelte o.B.d.A. $\mathfrak{p} \mid z$. Um ein Abstiegsargument zu bekommen, zeigen wir nun mehr, nämlich

> *Es gibt keine paarweise teilerfremden $\alpha, \beta, \gamma \in \mathcal{O}_K$, so dass*
>
> $$\alpha^3 + \beta^3 = \varepsilon\lambda^{3m}\gamma^3$$
>
> *mit $\varepsilon \in E_K$, $\mathfrak{p} \nmid \alpha\beta\gamma$ und $m \in \mathbb{N}$ gilt.*

Nehmen wir an, es gäbe solche Tripel. Sei (α, β, γ) unter diesen eines mit minimalem $m \in \mathbb{N}$.

Behauptung 1: Für $i, j \in \{0, 1, 2\}$, $i \neq j$, gilt $(\alpha + \zeta^i\beta, \alpha + \zeta^j\beta) = \mathfrak{p}$.

Beweis: Sei $\mathfrak{q}$ ein Primideal mit $\mathfrak{q} \mid (\alpha + \zeta^i\beta)$, $\mathfrak{q} \mid (\alpha + \zeta^j\beta)$. Dann gilt $\mathfrak{q} | (\zeta^i - \zeta^j)\beta = \zeta^i(1 - \zeta^{j-i})\beta$. Nun gilt $\zeta^{j-i} \in \{\zeta, \zeta^2\}$. Wegen $1 - \zeta^2 = (1-\zeta)(-\zeta^2)$ schließen wir in jedem Fall

$$\mathfrak{q} \mid (\text{Einheit})(1-\zeta)\beta.$$

Folglich gilt $\mathfrak{q} = \mathfrak{p} = (1-\zeta)$ oder $\mathfrak{q} | \beta$. Analog erhalten wir

$$\mathfrak{q} \mid \zeta^{-i}(\alpha + \zeta^i\beta) - \zeta^{-j}(\alpha + \zeta^j\beta) = (\zeta^{-i} - \zeta^{-j})\alpha = (\text{Einheit})(1-\zeta)\alpha.$$

Dies impliziert $\mathfrak{q} = \mathfrak{p}$ oder $\mathfrak{q} \mid \alpha$. Die Annahme $\mathfrak{q} \neq \mathfrak{p}$ führt daher zum Widerspruch gegen die Teilerfremdheit von α und β, weshalb $\mathfrak{q} = \mathfrak{p}$ gilt. Es bleibt zu zeigen, dass $\mathfrak{p}$ in der Tat $\alpha + \zeta^i\beta$ teilt. Wegen

$$\mathfrak{p} \mid (\alpha+\beta)(\alpha+\zeta\beta)(\alpha+\zeta^2\beta) = \varepsilon\lambda^{3m}\gamma$$

teilt $\mathfrak{p}$ mindestens eine der Zahlen $\alpha+\zeta^i\beta$. Aber die Differenzen der Zahlen sind durch $\mathfrak{p}$ teilbar, also sind sie sämtlich durch $\mathfrak{p}$ teilbar. Das zeigt Behauptung 1.

Unter Verwendung von Behauptung 1 können wir nun, nach eventueller Multiplikation von α und β mit einer Potenz von ζ, annehmen, dass $\alpha + \zeta\beta$ und $\alpha + \zeta^2\beta$ genau einmal durch $\mathfrak{p}$ teilbar sind. Es gilt dann

$$\begin{aligned}(\alpha+\beta) &= \mathfrak{p}^{3m-2}\mathfrak{c}_1^3\\ (\alpha+\zeta\beta) &= \mathfrak{p}\mathfrak{c}_2^3\\ (\alpha+\zeta^2\beta) &= \mathfrak{p}\mathfrak{c}_3^3\end{aligned}$$

mit ganzen, von $\mathfrak{p}$ verschiedenen und paarweise teilerfremden Idealen $\mathfrak{c}_1, \mathfrak{c}_2, \mathfrak{c}_3$. Da $\mathfrak{p}$ ein Hauptideal ist, ist $\mathfrak{c}_i^3$, $i = 1, 2, 3$, ein Hauptideal. Wegen $3 \nmid h_K$ sind die Ideale $\mathfrak{c}_i$ bereits selbst Hauptideale. Sei $\mathfrak{c}_i = (c_i)$, $i = 1, 2, 3$.

Behauptung 2: Es gilt $m \geq 2$.

Beweis: Die Elemente $\alpha, \beta \in \mathcal{O}_K$ sind nicht durch $\mathfrak{p}$ teilbar. Daher können wir ihre Restklasse modulo $\mathfrak{p}^2$ durch eine der in Lemma 7.4.1(v) angegebenen Zahlen repräsentieren. Nach Lemma 7.4.1(vi) gilt daher

$$\alpha^3 + \beta^3 \equiv (\pm 1) + (\pm 1) \mod \mathfrak{p}^4.$$

Wegen $\mathfrak{p} \mid (\alpha^3 + \beta^3)$ gilt daher $\lambda^{3m}\varepsilon\gamma^3 = \alpha^3 + \beta^3 \equiv 0 \bmod \mathfrak{p}^4$ und deshalb muss $m \geq 2$ sein. Dies zeigt Behauptung 2.

Wir schreiben jetzt

$$\begin{aligned}\alpha+\beta &= \lambda^{3m-2}\varepsilon_1 c_1^3\\ \alpha+\zeta\beta &= \lambda\varepsilon_2 c_2^3\\ \alpha+\zeta^2\beta &= \lambda\varepsilon_3 c_3^3\end{aligned}$$

mit Einheiten ε_i, $i = 1, 2, 3$. Multiplizieren wir die erste Gleichung mit ζ, die zweite mit ζ^2 und addieren auf, so erhalten wir wegen $1 + \zeta + \zeta^2 = 0$ die Gleichung

$$0 = \lambda^{3m-2}\varepsilon_1\zeta c_1^3 + \lambda\varepsilon_2\zeta^2 c_2^3 + \lambda\varepsilon_3 c_3^3.$$

Division durch $\varepsilon_3\lambda$ ergibt eine Gleichung

$$\varepsilon'\lambda^{3(m-1)}c_1^3 = \eta c_2^3 + c_3^3$$

mit Einheiten $\varepsilon', \eta \in \mathcal{O}_K$. Da die c_i prim zu $\mathfrak{p}$ sind, folgt aus Lemma 7.4.1(iv), dass $c_i \equiv \pm 1 \bmod \mathfrak{p}$ ist. Nach Lemma 7.4.1(vi) gilt $c_i^3 \equiv \pm 1 \bmod \mathfrak{p}^3$ für $i = 1, 2, 3$. Wegen $m \geq 2$ erhalten wir

$$\eta(\pm 1) + (\pm 1) \equiv 0 \mod \mathfrak{p}^3.$$

Insbesondere ist die Einheit $\eta \equiv \pm 1 \bmod \mathfrak{p}^2$, und aus (7.4.1)(v) folgt $\eta = \pm 1$. Wir erhalten

$$c_3^3 + (\pm c_2)^3 = \varepsilon'\lambda^{3(m-1)}c_1^3.$$

Dies ist wieder eine Lösung einer Gleichung vom angegebenen Typ, aber mit λ-Exponenten $m - 1 \geq 1$. Wir hatten aber m minimal gewählt. Dieser Widerspruch beendet den Beweis. □