Internat. Math. Nachrichten
Nr. 236 (2017), 39–51

Summen und Differenzen von Wurzeln

Hans Humenberger
Univ. Wien

Dieser Artikel ist die ausgearbeitete Fassung des Vortrags mit dem Titel „Summen und Differenzen von (Quadrat-)Wurzeln. An der Grenze zwischen elementarer und höherer Mathematik" bei der ÖMG-DMV-Tagung in Salzburg (11.–15.9.2017).

Einleitende Vorbemerkungen

In praktisch allen universitären Lehrveranstaltungen über Zahlentheorie bzw. Algebra (im weitesten Sinne) im Rahmen der Ausbildung von Lehramtsstudierenden kommt das Thema Wurzeln in Zusammenhang mit Irrationalität vor. Es gibt zahlreiche Beweise für $\sqrt{2} \notin \mathbb{Q}$. Der klassische Widerspruchsbeweis nach Euklid birgt (schon oft erprobt) die Gefahr, dass sein Prinzip auch auf andere Fälle gedankenlos übertragen wird. Bei diesem Beweis von $\sqrt{2} \notin \mathbb{Q}$ wird argumentiert $2 \mid p^2 \implies 2 \mid p$. Das Pendant, wenn man mit dieser Methode z.B. $\sqrt{8} \notin \mathbb{Q}$ beweisen möchte, wäre $8 \mid p^2 \implies 8 \mid p$, was ja nicht stimmt (das sieht man schon an $p = 4$). Wenn man also den klassischen Euklidischen Beweis für $\sqrt{2} \notin \mathbb{Q}$ favorisiert, dann sollte man auch unbedingt dazuüberlegen, wie dieser Beweis für z.B. $\sqrt{8} \notin \mathbb{Q}$ korrekt aussehen würde, und wo genau das Beweisprinzip bei $\sqrt{4}$ versagt. Man kann als Fazit jedenfalls festhalten, dass der Euklidische Beweis seine Tücken hat bei der Verallgemeinerung, dass nämlich Wurzeln aus natürlichen Zahlen entweder ganzzahlig oder irrational sind. (Es gibt keine Brüche, die Wurzeln aus natürlichen Zahlen sind.) Dies gilt nicht nur für Quadratwurzeln, sondern auch allgemein für k-te Wurzeln.

Mit einer anderen, aber immer noch elementaren Brille sind die zugehörigen Begründungen aber auch nicht komplizierter als jene für die Irrationalität von $\sqrt{2}$. Eine mögliche Grundlage ist das

Lemma. *(Lemma von Euklid, angewandt auf Primzahlen). Wenn eine Primzahl*

ISSN 0020-7926

ein Produkt von Zahlen teilt, so muss diese Primzahl mindestens einen Faktor teilen:

$$p \mid a \cdot b \implies p \mid a \text{ oder } p \mid b.$$

Analoges gilt für beliebig viele Faktoren:

$$p \mid a_1 \cdot \ldots \cdot a_n \implies \exists i : p \mid a_i.$$

Bei der Behandlung bzw. Verwendung dieses Lemmas in einem möglichen Schulunterricht wird man es nicht formal beweisen, denn aus Schülersicht ist dies kaum beweisbedürftig („Das ist ja eh klar, denn die unteilbare Primzahl kann ja nicht teilweise in einem und teilweise im anderen Faktor stecken!"). Jedenfalls lässt sich damit leicht allgemein zeigen[1]:

$$\sqrt[k]{a} \in \mathbb{Q} \implies \sqrt[k]{a} \in \mathbb{N} \quad (a \in \mathbb{N}, k \in \mathbb{N}_{\geq 2}). \tag{1}$$

Beweis. $\sqrt[k]{a} = \frac{p}{q}$ $(p \in \mathbb{N}, q \in \mathbb{N}^*$ mit $\mathrm{ggT}(p,q) = 1) \implies a \cdot q^k = p^k$. Jeder Primteiler von q müsste daher auch Primteiler von p^k und damit (Lemma von Euklid) von p sein. Wegen der Voraussetzung $\mathrm{ggT}(p,q) = 1$ kann q also gar keine Primteiler haben, d.h. $q = 1$, und das bedeutet schließlich $\sqrt[k]{a} = p \in \mathbb{N}$. □

Wie sieht die weit verbreitete Begründung des Lemmas von Euklid in Zahlentheoriebüchern und -lehrveranstaltungen aus? Meist wird kursorisch so vorgegangen: Zuerst kommt die Division mit Rest, dann der Euklidische Algorithmus und die sogenannte Darstellbarkeit des größten gemeinsamen Teilers (gemeint: $\mathrm{ggT}(a,b)$ als Linearkombination von a und b). Daraus kann dann das Lemma von Euklid gewonnen werden. Dies ist strukturell also ziemlich aufwendig. In meiner Zeit in Dortmund (2000 bis 2005) ist mir erstmals bewusst geworden, dass das Lemma von Euklid auch anders (einfacher?) zu erhalten ist. Damit kann dann auch auf eine intuitive, sehr nahe liegende Art und Weise die Eindeutigkeit der Primfaktorzerlegung begründet werden. Der sonst oft übliche Induktionsbeweis klärt ja nur, *dass* es so ist, er verschweigt aber in gewisser Weise das *warum* ("I believe it would be useful to introduce to the discussion an explicit distinction between proofs that prove and proofs that explain.", [3, S. 9]). Auch der bekannte Beweis mittels des Wohlordnungsprinzips (jede nichtleere Menge natürlicher Zahlen besitzt ein kleinstes Element) für die Eindeutigkeit der Primfaktorzerlegung ist nicht genetisch, auch er klärt nur das *dass*:

Beweis. (Indirekt) Angenommen, es gibt natürliche Zahlen > 1 mit zumindest zwei verschiedenen Primfaktorzerlegungen. Dann hat die Menge dieser Zahlen ein kleinstes Element a:

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s.$$

[1] Hier wollen wir $\mathbb{N} := \{0, 1, 2, \ldots\}$ und $\mathbb{N}^* := \{1, 2, \ldots\}$ setzen

Keine der Primzahlen p_i kann mit einer der Primzahlen q_j übereinstimmen, denn sonst könnte man durch diese Primzahl dividieren und man hätte zwei verschiedene Primfaktorzerlegungen einer noch kleineren Zahl.

O.B.d.A. ist $p_1 < q_1$. Wir bilden eine Zahl $n < a$:

$$n = (q_1 - p_1) \cdot q_2 \cdot \ldots \cdot q_s = \underbrace{q_1 \cdot q_2 \cdot \ldots \cdot q_s}_{=a=p_1\cdot\ldots\cdot p_r} - p_1 \cdot q_2 \cdot \ldots \cdot q_s$$

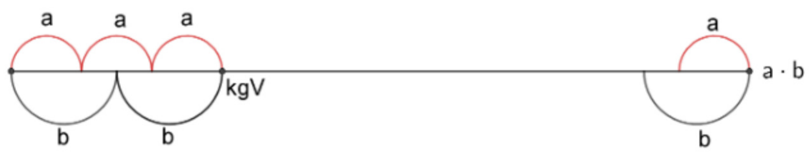
$$= p_1 \cdot (p_2 \cdot \ldots \cdot p_r - q_2 \cdot \ldots \cdot q_s).$$

p_1 tritt zwar als Faktor in der letzten Produktdarstellung auf, aber sicher nicht in der ersten: $p_1 \neq q_j$ und p_1 teilt nicht $q_1 - p_1$ (denn sonst müsste $p_1 \mid q_1$ gelten). Damit haben wir mit n eine kleinere Zahl als a gefunden mit zwei verschiedenen Primfaktorzerlegungen. Das ist ein Widerspruch. □

Wie könnte ein genetischerer Zugang zum Lemma von Euklid aussehen? Man braucht zwei Voraussetzungen: den *Satz vom kgV* und den *Satz vom kgV und ggT*, zwei strukturell sehr einfache Zusammenhänge.

Satz vom kleinsten gemeinsamen Vielfachen. *Jedes gemeinsame Vielfache von a und b ist ein Vielfaches des kleinsten gemeinsamen Vielfachen,* $\mathrm{kgV}(a,b)$.

Beweis. Das kgV kann auf der Zahlengeraden folgendermaßen bestimmt werden: Man trägt Vielfachenbogen der Länge a und Vielfachenbogen der Länge b ab. (Im Produkt $a \cdot b$ treffen diese Bogengirlanden einander ganz sicher, denn $b \cdot a = a \cdot b$.) Die Zahl, bei der die Girlanden einander erstmals treffen, ist definitionsgemäß das $\mathrm{kgV}(a,b)$.



Von dieser Zahl an beginnt das Muster der beiden Bogengirlanden von Neuem. Ein zweites Mal treffen sie also bei $2 \cdot \mathrm{kgV}(a,b)$, ein drittes Mal bei $3 \cdot \mathrm{kgV}(a,b)$ zusammen, usw. Die Bogengirlanden treffen einander also genau bei den Vielfachen von $\mathrm{kgV}(a,b)$. Das Produkt $a \cdot b$, bei dem die Girlanden einander ja auch treffen, muss also auch ein Vielfaches des $\mathrm{kgV}(a,b)$ sein. □

Satz. *(Satz vom kleinsten gemeinsamen Vielfachen und vom größten gemeinsamen Teiler).* $\mathrm{kgV}(a,b) \cdot \mathrm{ggT}(a,b) = a \cdot b$.

Wenn man die Eindeutigkeit der Primfaktorzerlegung voraussetzt, ist dieser Satz unmittelbar klar. Aber das wollen wir hier nicht tun, da wir umgekehrt das Lemma von Euklid dazu benutzen wollen, diese Eindeutigkeit zu zeigen.

Beweis. (a) Wir schreiben $\mathrm{kgV}(a,b) \cdot t = a \cdot b$ für eine Zahl t. Dies ist sicher möglich, da $a \cdot b$ ein gemeinsames Vielfaches von a und b und somit ein Vielfaches von $\mathrm{kgV}(a,b)$ ist. Wir behaupten, t ist ein gemeinsamer Teiler von a und b. Dies ist unmittelbar klar durch Umformung:

$$\frac{\mathrm{kgV}(a,b)}{a} \cdot t = b \quad \text{und} \quad \frac{\mathrm{kgV}(a,b)}{b} \cdot t = a\ .$$

Weil also t ein gemeinsamer Teiler von a und b ist, folgt: $\mathrm{ggT}(a,b) \geq t$ und somit

$$\mathrm{kgV}(a,b) \cdot \mathrm{ggT}(a,b) \geq a \cdot b. \tag{2}$$

(b) Wir schreiben $s \cdot \mathrm{ggT}(a,b) = a \cdot b$ für eine Zahl s. Dies ist sicher möglich, da schon a (auch b) ein Vielfaches von $\mathrm{ggT}(a,b)$ ist. Wir behaupten, dass s ein gemeinsames Vielfaches von a, b ist. Dies ist wieder klar durch Umformung:

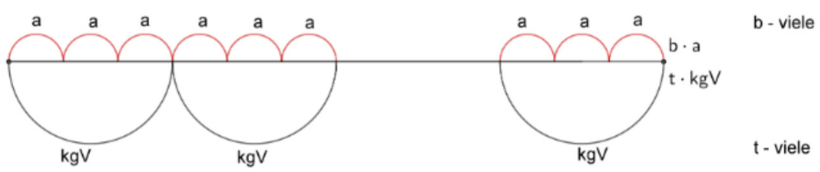
$$s = \frac{a}{\mathrm{ggT}(a,b)} \cdot b \quad \text{und} \quad s = a \cdot \frac{b}{\mathrm{ggT}(a,b)}.$$

Weil also s ein gemeinsames Vielfaches von a und b ist, folgt $\mathrm{kgV}(a,b) \leq s$ und somit

$$\mathrm{kgV}(a,b) \cdot \mathrm{ggT}(a,b) \leq a \cdot b. \tag{3}$$

Aus (2) und (3) folgt nun die Behauptung. □

Die zugehörigen algebraischen Umformungen könnten auch unterstützt oder gar ersetzt werden durch Veranschaulichungen mittels Bogengirlanden. (Das ist eventuell didaktisch von Belang; analog mit b-Bögen und entsprechend auch für die Umformung im 2. Absatz des Beweises.)



Hier ist t ein gemeinsamer Teiler von a und b. Die Anzahl der a-Bögen ist gleich b, die Anzahl der kgV-Bögen ist gleich t. Nun folgt daraus in wirklich sehr einfacher Weise das

Lemma. *(Lemma von Euklid, angewandt auf Primzahlen): Wenn $p \mid a \cdot b$, dann muss $p \mid a$ oder $p \mid b$ gelten.*

Beweis. Für $p \mid a$ ist die Behauptung erfüllt. Wenn a nicht durch p teilbar ist, dann ist $\operatorname{ggT}(p,a) = 1$, und wegen des Satzes vom kgV und ggT gilt: $\operatorname{kgV}(p,a) = p \cdot a$. $a \cdot b$ ist laut Voraussetzung ein gemeinsames Vielfaches von p und a und nach dem Satz vom kgV ein Vielfaches von $\operatorname{kgV}(p,a) = p \cdot a$, d.h. $a \cdot b = t \cdot (p \cdot a)$. Daraus folgt unmittelbar $b = t \cdot p$. □

Wendet man nun das Lemma von Euklid auf ein Produkt mehrerer Zahlen an, so ergibt sich sofort die Eindeutigkeit der Primfaktorzerlegung durch „schrittweises Durchkürzen“: Man zeigt, dass aus der Gleichheit zweier Primzahlprodukte die Gleichheit der Primzahlen selbst folgt:

$$p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s.$$

Aus $p_1 \mid q_1 \cdot q_2 \cdot \ldots \cdot q_s$ folgt, dass p_1 einen Faktor q_j teilt (Lemma von Euklid).

Da es sich um Primzahlen handelt, besteht Gleichheit: $p_1 = q_j$. Durch Umnummerierung kann man $p_1 = q_1$ erreichen. Beide Seiten der Gleichung (1) werden dann durch $p_1 = q_1$ dividiert. Man erhält die neue Gleichung $p_2 \cdot p_3 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s$, mit der man analog verfahren kann. Es folgt $p_2 = q_2$. In dieser Weise fährt man fort, bis die Gleichheit aller Faktoren und damit auch $r = s$ gezeigt ist.

Dies ist ein besonders elementarer, leicht nachvollziehbarer und gut erklärender Zugang zum Lemma von Euklid und zur Eindeutigkeit der Primfaktorzerlegung. Nun zum eigentlichen Thema dieses Aufsatzes: *Summen und Differenzen von Quadratwurzeln*.

Summen und Differenzen von Quadratwurzeln

Im Gegensatz zur Irrationalität von $\sqrt{2}$, sind Wurzel-Summen ein nicht besonders häufig diskutiertes Thema: Kann es z.B. sein, dass die Summe der Wurzeln natürlicher Zahlen wieder eine natürliche Zahl ist (außer im trivialen Fall, dass schon jede einzelne Wurzel eine natürliche Zahl ist)? Kann es sein, dass die Summe der Wurzeln rationaler Zahlen wieder eine rationale Zahl ist (außer im trivialen Fall, dass schon jede einzelne Wurzel eine rationale Zahl ist)? Intuitiv wird man diese Fragen wohl verneinen, aber wie kann man das begründen?

Ein Grund für das seltene Aufgreifen dieses Themas in Lehrveranstaltungen ist vielleicht, dass hier eine leichte Verallgemeinerbarkeit auf elementarem Niveau nicht mehr möglich zu sein scheint.

Wir werden sehen, dass die Begründung von

$$a,b \in \mathbb{Q},\ \sqrt{a} + \sqrt{b} \in \mathbb{Q} \implies \sqrt{a} \in \mathbb{Q}, \sqrt{b} \in \mathbb{Q}$$

und analog für $\mathbb{N}$ statt $\mathbb{Q}$ algebraisch noch einfach zu bewerkstelligen ist, das Pendant für m-te Wurzeln allerdings nicht mehr, erst recht nicht mehr im „gemischten“ Fall einer m-ten und einer n-ten Wurzel. Auch wenn man bei Quadratwurzeln bleibt, aber die Anzahl der Summanden erhöht, steht man ab vier Summanden vor großen Problemen, wenn man nicht Methoden der algebraischen Zahlentheorie verwendet. Wir werden im Folgenden bei Quadratwurzeln mögliche elementare Begründungen für den Fall bis zu drei Summanden angeben.

Dieser Problemkreis ist also gewissermaßen an der Grenze zwischen Elementarmathematik und Höherer Mathematik anzusiedeln, was man ihm a priori nicht unbedingt ansieht. Durch die Erfolge für den Fall mit wenigen Summanden könnte man durchaus vermuten, dass dies strukturell so weitergeht auch bei vielen Summanden, dass man also mit elementarer Algebra auskommt, nur der Aufwand sich ein wenig erhöhen wird. Das wird sich jedoch als falsch herausstellen – es gibt hier eine eindeutige strukturelle Grenze.

Zunächst widmen wir uns der Summe der Quadratwurzeln zweier rationaler Zahlen. Diese Summe ist nur dann rational, wenn schon jede einzelne Quadratwurzel rational ist. Dies wird man auch intuitiv wohl vermuten, es lässt sich auch leicht algebraisch nachvollziehen bzw. bestätigen:

Satz 1a. *Für rationale Zahlen a, b, c gilt*

$$\sqrt{a} + \sqrt{b} = c \implies \sqrt{a} \in \mathbb{Q},\ \sqrt{b} \in \mathbb{Q}. \tag{4}$$

Beweis 1. Klarerweise müssen $a, b, c \geq 0$ und $\sqrt{a}, \sqrt{b} \geq 0$ gelten. Für $c = 0$ muss auch $\sqrt{a} = 0 = \sqrt{b}$ sein, und die Behauptung ist damit erfüllt.

Für $c > 0$ folgt aus $\sqrt{a} + \sqrt{b} \in \mathbb{Q}$ und $(\sqrt{a} + \sqrt{b}) \cdot (\sqrt{a} - \sqrt{b}) = a - b \in \mathbb{Q}$ unmittelbar

$$\sqrt{a} - \sqrt{b} = \frac{a-b}{\sqrt{a} + \sqrt{b}} \in \mathbb{Q}.$$

Damit ist aber

$$(\sqrt{a} + \sqrt{b}) + (\sqrt{a} - \sqrt{b}) = 2\sqrt{a}$$

eine Summe von zwei rationalen Zahlen und damit rational. Es folgt, dass auch $\sqrt{a}$ rational ist.

Analog erhält man als Differenz von zwei rationalen Zahlen $(\sqrt{a} + \sqrt{b}) - (\sqrt{a} - \sqrt{b}) = 2\sqrt{b}$, d.h. $\sqrt{b} \in \mathbb{Q}$. □

Der Nachteil dieses Beweises ist, dass er nicht verallgemeinerbar ist auf mehr als zwei Wurzeln. Die Methode von Beweis 2 ist vielleicht weniger elegant, funktioniert aber dafür auch bei einigen weiteren Fällen (siehe unten) und ist vielleicht auch einfacher zu finden („durch Quadrieren versuchen, die Wurzeln wegzubringen“).

Beweis 2. Der Fall $c = 0$ bleibt gleich. Im Fall $c > 0$ erhält man aus $\sqrt{a} = c - \sqrt{b}$ durch Quadrieren zunächst $a = c^2 + b - 2c\sqrt{b}$ und daraus $\sqrt{b} = \frac{c^2+b-a}{2c} \in \mathbb{Q}$. Mit der Voraussetzung von (4) ist dann auch $\sqrt{a} \in \mathbb{Q}$. □

In welchen Fällen ist die Differenz der Quadratwurzeln zweier rationaler Zahlen selbst rational? Man wird wieder nur die trivialen Lösungen erwarten, aber diese spalten sich hier prinzipiell in zwei Möglichkeiten auf: Die Wurzeln stimmen überein (Differenz = 0), oder jede einzelne Wurzel ist rational. Auch das lässt sich algebraisch wieder ganz elementar nachvollziehen:

Satz 1b. *Für rationale Zahlen a,b,c gilt*

$$\sqrt{a}-\sqrt{b}=c \implies \sqrt{a}=\sqrt{b} \text{ oder } \sqrt{a}\in\mathbb{Q}, \sqrt{b}\in\mathbb{Q}. \tag{5}$$

Der Beweis ist im Fall $c \neq 0$ analog zu Satz 1a. Im Fall $c=0$ haben wir $\sqrt{a}=\sqrt{b}$. Die entsprechenden Sätze für natürliche statt rationale Zahlen folgen hieraus mit (1) unmittelbar.

Beim Thema dieses Abschnittes kann man in relativ nahe liegender Weise auch danach fragen, wann eine Summe bzw. Differenz zweier Quadratwurzeln rationaler Zahlen selbst eine Quadratwurzel einer rationalen Zahl ist: Was kann man aus $\sqrt{a}\pm\sqrt{b}=\sqrt{c}$ $(a,b,c\in\mathbb{Q})$ folgern? Anders gefragt: Unter welchen genauen Bedingungen an a,b,c ist diese Beziehung erfüllt?
Wir beginnen mit der Summe: Wann gilt $\sqrt{a}+\sqrt{b}=\sqrt{c}$ für rationale Zahlen a,b,c?
Klarerweise haben wir wieder $a,b,c\geq 0$ und $\sqrt{a},\sqrt{b},\sqrt{c}\geq 0$. Für $c=0$ muss auch $a=0=b$ sein. Im Fall $c>0$ muss mindestens einer der beiden Summanden auf der linken Seite positiv sein (o.B.d.A. $\sqrt{a}>0$). Dann erhalten wir durch Quadrieren zunächst

$$\sqrt{ab}=\frac{c-a-b}{2}\in\mathbb{Q}_0^+$$

und damit wegen $\sqrt{a}>0$,

$$\sqrt{b}=\frac{c-a-b}{2\sqrt{a}}=\frac{c-a-b}{2a}\cdot\sqrt{a}.$$

Der Bruch wird mit A bezeichnet. D.h. entweder gilt $b=0$ und $a=c$ oder $\sqrt{b}$ muss ein rationales Vielfaches von $\sqrt{a}$ sein (und umgekehrt): $\sqrt{b}=A\cdot\sqrt{a}$ bzw. $b=A^2\cdot a$. Insgesamt erhalten wir also:

Hilfssatz. *Gilt für rationale Zahlen $a,b,c\geq 0$, dass*

$$\sqrt{a}+\sqrt{b}=\sqrt{c},$$

dann tritt einer der beiden Fälle auf:

1. *$a = 0$ und $b = c$ (rational, nichtnegativ) oder $b = 0$ und $a = c$ (rational, nichtnegativ).*
2. *$\sqrt{b} = A \cdot \sqrt{a}$, $\sqrt{c} = (1+A) \cdot \sqrt{a}$ mit $a, A \in \mathbb{Q}^+$ beliebig.*

Bemerkung: Es ist auch jede in 1. bzw. 2. angegebene Möglichkeit auch wirklich eine Lösung, so dass man in der obigen Aussage die Implikation durch eine Äquivalen ersetzen könnte.

Die entsprechende Aussage für natürliche Zahlen lautet:

$$\begin{aligned} & \sqrt{a} + \sqrt{b} = \sqrt{c} \quad (a,b,c \in \mathbb{N}) \\ \Longrightarrow\; & a = 0, b = c \text{ oder } b = 0, a = c, \text{ oder} \\ & \sqrt{a} = q \cdot \sqrt{n}, \sqrt{b} = p \cdot \sqrt{n}, \sqrt{c} = (q+p) \cdot \sqrt{n} \text{ mit } n,p,q \in \mathbb{N}^*. \end{aligned} \tag{6}$$

Die Begründung der letzten Aussage ergibt sich dabei durch: $\sqrt{b}$ muss laut obigem Hilfssatz ein positives rationales Vielfaches von $\sqrt{a}$ sein: $\sqrt{b} = (p/q) \cdot \sqrt{a}$ ($p, q \in \mathbb{N}^*$, $\operatorname{ggT}(p,q) = 1$), d.h. $\sqrt{b} = \sqrt{(p^2/q^2) \cdot a}$; wegen $\operatorname{ggT}(p,q) = 1$ muss $q^2 \mid a$ gelten.

Nun betrachten wir dasselbe Problem für eine Differenz: Wann gilt $\sqrt{a} - \sqrt{b} = \sqrt{c}$ für rationale Zahlen a, b, c? Zur Bedingung $a, b, c \geq 0$ kommt hier a priori $a \geq b$ dazu. Wenn $c = 0$ ist, muss $a = b$ sein. Für $c > 0$ muss auch $a > 0$ sein. Wieder ergibt sich, dass entweder $b = 0 \wedge a = c$ oder $\sqrt{b}$ ein positiv rationales Vielfaches von $\sqrt{a}$ sein muss ($\sqrt{b} = A \cdot \sqrt{a}$), diesmal aber mit der Einschränkung $0 < A \leq 1$ (wegen $b \leq a$). Insgesamt erhalten wir hier:

$$\begin{aligned} & \sqrt{a} - \sqrt{b} = \sqrt{c} \quad (a,b,c \in \mathbb{Q}) \\ \Longrightarrow\; & c = 0, a = b \in \mathbb{Q}_0^+ \text{ oder } b = 0, a = c \in \mathbb{Q}_0^+, \text{ oder} \\ & b = A^2 \cdot a,\ c = (1-A)^2 \cdot a \text{ mit } a \in \mathbb{Q}^+,\ 1 \geq A \in \mathbb{Q}^+. \end{aligned}$$

Die entsprechende Aussage für natürliche Zahlen:

$$\begin{aligned} & \sqrt{a} - \sqrt{b} = \sqrt{c} \quad (a,b,c \in \mathbb{N}) \implies \\ & c = 0, a = b \in \mathbb{N} \text{ oder } b = 0, a = c \in \mathbb{N} \text{ oder} \\ & \sqrt{a} = q \cdot \sqrt{n} \text{ mit } n \in \mathbb{N}^*, \sqrt{b} = p \cdot \sqrt{n}, \sqrt{c} = (q-p) \cdot \sqrt{n} \text{ mit } p,q \in \mathbb{N}^*, p < q. \end{aligned}$$

Summen und Differenzen dreier Quadratwurzeln

Wir wollen in diesem Abschnitt Gleichungen der Art $\pm\sqrt{a} \pm \sqrt{b} \pm \sqrt{c} = d$ ($a, b, c, d \in \mathbb{Q}$) untersuchen. Dabei sind natürlich die beiden Fälle $(+,+,+)$ und $(-,-,-)$ als gleich zu betrachten, ebenso alle weiteren Fälle untereinander (ein Vorzeichen einfach, das andere doppelt). Man kann sich also beschränken auf $\sqrt{a} + \sqrt{b} + \sqrt{c} = d$ ($a, b, c, d \in \mathbb{Q}$) und $\sqrt{a} + \sqrt{b} - \sqrt{c} = d$ ($a, b, c, d \in \mathbb{Q}$). Die oben verwendete Methode wird auch hier zum Ziel führen.

Satz 2a.

$$\sqrt{a}+\sqrt{b}+\sqrt{c}=d\ (a,b,c,d\in\mathbb{Q}) \implies \sqrt{a},\sqrt{b},\sqrt{c}\in\mathbb{Q}$$

Beweis. Klarerweise muss $a,b,c,d\geq 0$ gelten. Wir können sogar $a,b,c>0$ annehmen, denn sonst wären wir bei Satz 1a. Für $d=0$ muss auch $\sqrt{a}=\sqrt{b}=\sqrt{c}=0$ sein, und die Behauptung ist damit erfüllt.
Im Fall $d>0$ erhält man aus $\sqrt{a}+\sqrt{b}=d-\sqrt{c}$ durch Quadrieren

$$\underbrace{\sqrt{a\cdot b}}_{>0}=\underbrace{\frac{d^2+c-a-b}{2}}_{=:A\in\mathbb{Q}^+}-d\cdot\sqrt{c}.$$

Diese Gleichung wird wieder quadriert, und man erhält $a\cdot b=A^2+d^2\cdot c-2A\cdot d\cdot\sqrt{c}$, woraus schließlich $\sqrt{c}=\frac{A^2+d^2\cdot c-a\cdot b}{2A\cdot d}\in\mathbb{Q}$ folgt. Wegen Satz 1a müssen dann auch $\sqrt{a},\sqrt{b}\in\mathbb{Q}$ sein. □

Satz 2b. *Falls für rationale Zahlen a,b,c,d die Beziehung*

$$\sqrt{a}+\sqrt{b}-\sqrt{c}=d$$

gilt, tritt einer der folgenden vier Fälle auf:

1. $a=d=0, b=c\in\mathbb{Q}_0^+$ *oder* $b=d=0, a=c\in\mathbb{Q}_0^+$;
2. $d=0$, $\sqrt{b}=A\cdot\sqrt{a}$, $\sqrt{c}=(1+A)\cdot\sqrt{a}$ *mit* $a,A\in\mathbb{Q}^+$ *beliebig;*
3. $\sqrt{a},\sqrt{b},\sqrt{c}\in\mathbb{Q}$;
4. $a=c, b=d^2$ *oder* $b=c, a=d^2$.

Beweis. Es gilt hier $a,b,c\geq 0$, das Vorzeichen von d ist unbestimmt. Für $d=0$ ergeben sich die beiden Fälle 1. und 2. direkt aus dem Hilfssatz. Im Fall $d>0$ erhält man aus $\sqrt{a}+\sqrt{b}=d+\sqrt{c}$ durch Quadrieren

$$\sqrt{a\cdot b}=\underbrace{\frac{d^2+c-a-b}{2}}_{=:A\in\mathbb{Q}}+d\cdot\sqrt{c}.$$

(Das Vorzeichen von $A\in\mathbb{Q}$ ist hier leider nicht klar.) Diese Gleichung wird wieder quadriert, und man erhält

$$a\cdot b=A^2+d^2\cdot c+2A\cdot d\cdot\sqrt{c},$$

woraus schließlich für $A\neq 0$ die Beziehung $\sqrt{c}=\frac{a\cdot b-A^2-d^2\cdot c}{2A\cdot d}\in\mathbb{Q}$ folgt. Wegen Satz 1a müssen dann auch $\sqrt{a},\sqrt{b}\in\mathbb{Q}$ sein (Fall 3.). Im Fall $A=0$ gilt $(a\cdot b=d^2\cdot c)\wedge(a+b=d^2+c)$ mit den „Lösungen" (a priori klar oder durch Lösen einer zugehörigen quadratischen Gleichung): $a=c, b=d^2$ bzw. $b=c, a=d^2$ (Fall 4.). □

Bemerkung: Die entsprechenden Sätze für natürliche statt rationale Zahlen folgen hieraus mit (1) und (6) unmittelbar.

Auch hier kann man in relativ nahe liegender Weise wieder danach fragen, wann eine Summe bzw. Differenz dreier Quadratwurzeln rationaler Zahlen selbst eine Quadratwurzel einer rationalen Zahl ist: Was kann man aus $\sqrt{a} \pm \sqrt{b} \pm \sqrt{c} = \sqrt{d}$ $(a,b,c,d \in \mathbb{Q})$ folgern?
Anders gefragt: Unter welcher Bedingung gilt $\sqrt{a} \pm \sqrt{b} \pm \sqrt{c} = \sqrt{d}$ $(a,b,c,d \in \mathbb{Q})$? Wir beschränken uns auf die Summe: $\sqrt{a} + \sqrt{b} + \sqrt{c} = \sqrt{d}$. (Die anderen Fälle $\sqrt{a} + \sqrt{b} - \sqrt{c} = \sqrt{d}$ bzw. $\sqrt{a} - \sqrt{b} - \sqrt{c} = \sqrt{d}$ gingen analog.)

Satz 3. *Gilt für rationale Zahlen a,b,c,d die Beziehung*

$$\sqrt{a} + \sqrt{b} + \sqrt{c} = \sqrt{d},$$

so tritt einer der drei folgenden Fälle ein:

1. Mindestens zwei der Zahlen a,b,c sind null, die dritte ist gleich d;
2. Genau eine der Zahlen $\sqrt{a}, \sqrt{b}, \sqrt{c}$ ist null, die anderen beiden sind positiv rationale Vielfache voneinander, $\sqrt{d}$ ist die Summe dieser beiden Wurzeln (also auch ein positives rationales Vielfaches jeder der beiden positiven Wurzeln);
3. Alle Wurzeln sind positiv und rationale Vielfache voneinander.

Beweis. Klarerweise haben wir $a,b,c,d \geq 0$ und $\sqrt{a}$, $\sqrt{b}$, $\sqrt{c}$, $\sqrt{d} \geq 0$ und $d \geq a,b,c$. Für $d = 0$ muss auch $a = b = c = 0$ sein (Fall 1.). Im Fall $d > 0$ muss mindestens einer der drei Summanden auf der linken Seite positiv sein (o.B.d.A. $\sqrt{c} > 0$). Dann erhalten wir durch Subtrahieren von $\sqrt{c}$ auf beiden Seiten und anschließendes Quadrieren zunächst $\sqrt{ab} + \sqrt{cd} = \frac{d+c-a-b}{2} \in \mathbb{Q}^+$. Mit Satz 1a muss dann $\sqrt{cd} = B \in \mathbb{Q}^+$ sein, und wegen $\sqrt{d} = B/\sqrt{c} = \frac{B}{c} \cdot \sqrt{c}$ ist klar, dass $\sqrt{d}$ ein positiv rationales Vielfaches von $\sqrt{c}$ sein muss: $\sqrt{d} = C \cdot \sqrt{c}$ mit $1 \leq C \in \mathbb{Q}^+$. Des Weiteren ist (wegen Satz 1a) $\sqrt{ab} = D \in \mathbb{Q}_0^+$. Für $a = 0$ oder $b = 0$ kann man den Hilfssatz benutzen (Fall 1. und 2.). Für $a,b > 0$ (insgesamt also $a,b,c,d > 0$) ist $d > c$ (d.h. $C > 1$) und analog $\sqrt{b}$ ein positiv rationales Vielfaches von $\sqrt{a}$, d.h. $\sqrt{b} = E \cdot \sqrt{a}$ mit $E \in \mathbb{Q}_0^+$. Damit haben wir

$$\sqrt{a} + \underbrace{E \cdot \sqrt{a}}_{\sqrt{b}} = \underbrace{C \cdot \sqrt{c}}_{\sqrt{d}} - \sqrt{c} \quad \text{bzw.} \quad \sqrt{c} = \underbrace{\frac{1+E}{C-1}}_{=:F \in \mathbb{Q}^+} \cdot \sqrt{a},$$

d.h. auch $\sqrt{c}$ und damit $\sqrt{d}$ sind positiv rationale Vielfache von $\sqrt{a}$ (Fall 3.). $\square$

Bemerkung zum Schulunterricht: Die bis hierher gegebenen Beweise sind von ihrem Niveau her so, dass sie sogar in der Schule in einem Wahlpflichtfach (das sich z.B. schwerpunktmäßig Fragen der Irrationalität widmet) möglich wären. Man kann dabei einerseits viel algebraisches Rüstzeug („das Rechnen mit Buchstaben") üben, man hat viele Möglichkeiten, Lernende nicht nur vorgegebene Beweise nachvollziehen zu lassen, sondern sie auch selbstständig arbeiten zu lassen (z.B. Satz 1a und 2a durch die Lehrkraft, andere Sätze durch Schülergruppen). Andererseits ist das mathematische Prinzip der Fallunterscheidung hier zentral verankert und tritt in elementarer Form auf. Man erhält des Weiteren ein vertieftes Verständnis von Rationalität-Irrationalität (vgl. auch [4]: $\log_{10} 2$ ist irrational; was ist die genaue Bedingung an die natürlichen Zahlen $a, b \geq 2$, sodass $\log_b a$ rational ist?, etc.), sieht selber am Horizont weiterführende Fragen (Wie ist das mit mehr als drei Quadratwurzeln? Wie ist das mit anderen Wurzeln?, etc.), bei denen aber das vorhandene Rüstzeug nicht ausreicht. Dies ist nicht selbstverständlich, denn bei vielen Fragen der Mathematik, bei denen das schulische Rüstzeug nicht ausreicht, kann man als Schüler/in die zugehörige Fragestellung bzw. die Problemlage gar nicht verstehen. Im Bereich der Zahlentheorie (z.B. Goldbachvermutung, etc.) ist ein Verstehen des geschilderten Problems aber oft relativ leicht möglich. Unter Umständen haben solche „Grenzerlebnisse" sogar etwas Faszinierendes, so dass dadurch die Motivation steigt, in diesem Bereich mehr wissen zu wollen, und die Mathematik als Wissenschaft hat da auch mehr zu bieten (Universität). Insgesamt ist dies sicher ein „skalierbares Thema" [5], das einen möglichen Einsatz auf verschiedenen Niveaustufen (Schule, Universität) hat.

Summen und Differenzen von Wurzeln – allgemeiner

Man könnte nun vermuten, dass zwar der algebraische Aufwand immer ein wenig größer wird, dass es aber prinzipiell möglich ist, mit der geschilderten Methode die Anzahl der Quadratwurzeln zu steigern, z.B. bei $\sqrt{a} + \sqrt{b} + \sqrt{c} + \sqrt{d} = e$ ($a, b, c, d, e \in \mathbb{Q}$) oder $\sqrt{a} + \sqrt{b} + \sqrt{c} + \sqrt{d} = \sqrt{e}$ mit $a, b, c, d, e \in \mathbb{Q}$. Aber das funktioniert nicht mehr, da dann durch Quadrieren die Anzahl der auftretenden Quadratwurzeln nicht mehr gesenkt werden kann.

Schon im Fall zweier (beliebiger) Wurzeln kommt man mit Elementarmathematik nicht mehr aus, da braucht man u.a. den Begriff des Minimalpolynoms, speziell dessen Eigenschaft: Wenn α Nullstelle eines beliebigen Polynoms f ist, dann muss das zugehörige Minimalpolynom p das Polynom f teilen (vgl. [1], dort aber sehr kurz und eigentlich etwas unsauber).

Satz 4a. *Wenn a, b, m, n positive ganze Zahlen mit $\sqrt[m]{a}, \sqrt[n]{b} \notin \mathbb{Q}$ sind, dann ist auch $\sqrt[m]{a} + \sqrt[n]{b} \notin \mathbb{Q}$.*

Beweis. Wir nehmen an, dass a, b, m, n minimal in folgendem Sinn sind: Es gibt keine kleineren positiven ganzen Zahlen a', b', c', d' mit $\sqrt[m']{a'} = \sqrt[m]{a}$ bzw. $\sqrt[n']{b'} = \sqrt[n]{b}$ (also so etwas wie z.B. $\sqrt[9]{8}$ sei verboten, dafür würden wir $\sqrt[3]{2}$ schreiben). Dann ist das sogenannte Minimalpolynom von $\sqrt[m]{a}$ über $\mathbb{Q}$ gegeben durch $f_a(X) = X^m - a$, analog jenes von $\sqrt[n]{b}$ durch $f_b(X) = X^n - b$. Annahme: $\sqrt[m]{a} + \sqrt[n]{b} = q \in \mathbb{Q} \implies \sqrt[n]{b} = q - \sqrt[m]{a}$; dann wäre $\sqrt[m]{a}$ Nullstelle von $f_b(q-X)$ und somit müsste (Minimalpolynom!) $f_a(X) \mid f_b(q-X)$; analog wäre $f_b(X) \mid f_a(q-X)$ und mit der Substitution $X \to q-X$ daher $f_b(q-X) \mid f_a(X)$. Also können sich $f_b(q-X)$ und $f_a(X)$ nur durch einen rationalen Faktor unterscheiden („assoziierte Polynome"), d.h. $f_b(q-X) = c \cdot f_a(X)$ mit $c \in \mathbb{Q}$: $(q-X)^n - b = c \cdot (X^m - a)$. Dies ist nur für $q = 0$ möglich (denn sonst hätte man ja wegen des Binomischen Lehrsatzes auch viele weitere Potenzen von X auf der linken Seite): $(-X)^n - b = c \cdot (X^m - a)$. Für gerades n ergibt sich daraus $n = m, c = 1$ und $a = b$, und damit $= 2\sqrt[m]{a}$ also $\sqrt[m]{a} \in \mathbb{Q}$, Widerspruch. Für ungerades n ergibt sich $c = -1, n = m$ und $a = -b$, Widerspruch. $\square$

Solche Beweise wären in der Schule nicht möglich, auch in der Ausbildung für Lehramtskandidaten an Universitäten ist das nicht überall möglich, weil die Algebra oft nicht in einem hinreichend tiefen Ausmaß vorkommt (und daher z.B. die Begriffe des Minimalpolynoms oder der Körpererweiterung gar nicht thematisiert werden).

Noch ein Stück abstrakter (tiefer in der algebraischen Zahlentheorie) ist der Beweis der entsprechenden allgemeinen Aussage:

Satz 4b: Aus $r_1, \ldots, r_n \in \mathbb{Q}^+$, $s_1, \ldots, s_n \in \mathbb{N}_{\geq 2}$ mit $\sqrt[s_1]{r_1}, \ldots, \sqrt[s_n]{r_n} \notin \mathbb{Q}$ folgt $\sum_{i=1}^n \sqrt[s_i]{r_i} \notin \mathbb{Q}$.

Beweis. (von G. Kuba). Wir betrachten den Körper $K = \mathbb{Q}[\sqrt[s_1]{r_1}, \ldots, \sqrt[s_n]{r_n}]$, dessen Grad d über $\mathbb{Q}$ jedenfalls mindestens 2 beträgt. Sei $T(\alpha)$ die Spur von $\alpha \in K$ bezogen auf K (es ist also $T(\alpha) = \sigma_1(\alpha) + \ldots + \sigma_d(\alpha)$, wobei $\sigma_1, \ldots, \sigma_d$ die Monomorphismen von K nach $\mathbb{C}$ sind). Da für $m, a \in \mathbb{N}$ im Fall $\sqrt[m]{a} \notin \mathbb{Z}$ das Minimalpolynom von $\sqrt[m]{a}$ von der Form $X^k - b$ mit $2 \leq k \leq m$ und $b \in \mathbb{N}$ ist, muss $T(\sqrt[s_i]{r_i}) = 0$ für alle $i \in \{1, \ldots, n\}$ und somit auch $T(\sum_{i=1}^n \sqrt[s_i]{r_i}) = 0$ gelten. Dagegen gilt $T(r) = d \cdot r$ für alle $r \in \mathbb{Q}$. Da die Zahl $\sum_{i=1}^n \sqrt[s_i]{r_i}$ trivialerweise positiv ist, kann dieselbe somit nicht rational sein. $\square$

Andere Beweise dafür finden sich in [2, 6].

Literatur

[1] Diskussionforum *stackexchange.com*, URL *http://math.stackexchange.com/questions/479092/sum-of-two-irrational-radicals-is-irrational*

[2] A.S. Besicovitch. On the Linear Independence of Fractional Powers of Integers. *Proc. Lond. Math. Soc.* 15 (1940), 3–6.

[3] G. Hanna. Some Pedagogical Aspects of Proof. *Interchange* 21/1 (1990), 6–13.

[4] H. Humenberger und B. Schuppar: Irrationale Dezimalbrüche – nicht nur Wurzeln! In: Realitätsnaher Mathematikunterricht – vom Fach aus und für die Praxis. Festschrift zum 60. Geburtstag für H.-W. Henn (A. Büchter et al., eds), Franzbecker, Hildesheim 2006, pp. 232–245.

[5] N. Hungerbühler. Skalierbare Themen im Mathematikunterricht. In: *Beiträge zum Mathematikunterricht 2015*, WTM-Verlag, Münster, pp. 26–33.

[6] P. Mihailescu. Aufgabe 835. *Elemente der Mathematik* 36 (1981), 19–20.

Anschrift des Verfassers:
Hans Humenberger
Universität Wien, Fakultät für Mathematik
Oskar-Morgenstern-Platz 1, 1090 Wien.
email hans.humenberger@univie.ac.at