

Zur Vereinfachung von Wurzelausdrücken. Eine Anmerkung zur Aufgabe φ 28

Hans-Gert Gräbe, Leipzig

11. Januar 2015

In [1] stellt Friedhelm Götze aus Jena die Aufgabe, den Ausdruck

$$A = \frac{14}{\sqrt{78 + 52 \sqrt[4]{2} + 51 \sqrt[4]{4} + 34 \sqrt[4]{8}}}$$

zu vereinfachen und in eine nennerfreie Darstellung zu überführen. Reiner Möwald gibt in [2] durch geeignet „trickreiche“ Umformungen eine Lösung an, die allerdings die Schönheit der dahinter verborgenen Mathematik nicht erkennen lässt – dass sich nämlich *jeder* derartige Ausdruck als nennerfreie Linearkombination darstellen lässt und dafür auch ein einfaches algorithmisches Vorgehen bekannt ist. Diese beiden Aspekte möchte ich im folgenden kleinen Aufsatz darstellen. Eine ausführlicher Besprechung der Thematik ist in [4] zu finden.

1 Die Problemstellung

Rationale Ausdrücke wie

$$\frac{a^2}{(a-b)(a-c)} + \frac{b^2}{(b-a)(b-c)} + \frac{c^2}{(c-a)(c-b)} \quad (1)$$

lassen sich durch einfache Termumformungen oft substanziell vereinfachen. Ähnliches gilt für Wurzelausdrücke, wie zum Beispiel

$$\sqrt{2\sqrt{3} + 4} = 1 + \sqrt{3} \quad (2)$$

oder

$$\sqrt{11 + 6\sqrt{2}} + \sqrt{11 - 6\sqrt{2}} = 6. \quad (3)$$

Entsprechende Algorithmen sind auch in den meisten Computeralgebrasystemen (CAS) implementiert, allerdings aus hier nicht weiter zu besprechenden Gründen oft in Spezialpakete ausgelagert. Während MAPLE derartige Vereinfachungen automatisch vornimmt, sind andere CAS oft nur mit viel gutem Zureden bereit, diese Simplifikation vorzunehmen. Selbst

This material belongs to the Public Domain KoSemNet data base. It can be freely used, distributed and modified, if properly attributed. Details are regulated by the *Creative Commons Attribution License*, see <http://creativecommons.org/licenses/by/3.0>.

For the KoSemNet project see <http://www.lsgm.de/KoSemNet>.

das Normalformproblem, also jeweils die Vereinfachung der Differenz beider Seiten der Identitäten zu null, wird weder in MUPAD noch in MATHEMATICA oder MAXIMA allein durch den Aufruf von `simplify` gelöst. MUPAD (`radsimp`) und MATHEMATICA (`RootReduce`) stellen spezielle Simplifikationsroutinen für geschachtelte Wurzelausdrücke zur Verfügung, was bei MATHEMATICA im stärkeren `FullSimplify` integriert ist. MAXIMA [3] bietet eine solche Simplifikationsroutine `sqrtdenest` im Paket `sqdnst`.

Solche Wurzelausdrücke sind stets Nullstellen von Polynomen. Für $a = \sqrt{2\sqrt{3} + 4}$ etwa rechnet man $(a^2 - 4)^2 = 4 \cdot 3 = 12$ leicht nach, also ist a Nullstelle des Polynoms

$$P(x) = (x^2 - 4)^2 - 12 = x^4 - 8x^2 + 4,$$

welches sich in die algebraische Ersetzungsregel $a^4 \rightarrow 8a^2 - 4$ transformieren lässt. Wegen

$$P(x) = (x^2 - 2x - 2) \cdot (x^2 + 2x - 2) \tag{4}$$

ist a aber auch Nullstelle eines der beiden Faktorpolynome und damit existiert sogar eine algebraische Ersetzungsregel für a^2 .

Damit ist auch schon die Gültigkeit von (2) fast gezeigt, es bleibt allein zu begründen, welche der vier Nullstellen von (4) auf der rechten und welche auf der linken Seite steht. Dies kann man aber in diesem Fall durch eine einfache numerische Abschätzung entscheiden, da die vier Nullstellen genügend weit auseinander liegen.

Jede Zahl a , die Nullstelle eines Polynoms $P(x) \in \mathbb{Q}[x]$ ist, ist auch Nullstelle eines irreduziblen monischen Polynoms $Q(x) = x^d - r(x) \in \mathbb{Q}[x]$, also eines Polynoms, das sich (über \mathbb{Q}) nicht weiter in Faktoren zerlegen lässt und dessen Koeffizient vor der höchsten x -Potenz gleich eins ist. Hierbei ist $r(x) \in \mathbb{Q}[x]$ ein Polynom vom Grad kleiner als d .

Derartige Zahlen a bezeichnet man als *algebraische Zahlen*, das Polynom $Q(x)$ als *charakteristisches Polynom* der Zahl a und d als den *Grad* der algebraischen Zahl.

Ein erstes kleines Lemma beweist, dass dieses charakteristische Polynom und damit auch dessen Grad eindeutig bestimmt sind.

Lemma 1 *Unter allen Polynomen*

$$P := \{q(x) \in \mathbb{Q}[x] : q(a) = 0 \text{ und } lc(q) = 1\}$$

mit Leitkoeffizient 1 und Nullstelle a gibt es genau ein Polynom $p(x)$ kleinsten Grades. Dieses ist irreduzibel und jedes andere Polynom $q(x) \in P$ ist ein Vielfaches von $p(x)$.

Beweis: Division mit Rest in $\mathbb{Q}[x]$ ergibt

$$q(x) = s(x) \cdot p(x) + r(x)$$

mit $r = 0$ oder $\deg(r) < \deg(p)$. Wäre $r \neq 0$, so ergäbe sich wegen $q(a) = p(a) = 0$ auch $r(a) = 0$ und $\frac{1}{lc(r)}r(x) \in P$ im Gegensatz zur Annahme, dass $p(x) \in P$ minimalen Grad hat.

Wäre $p(x)$ reduzibel, so wäre a auch Nullstelle eines der Faktoren. Dieser würde also zu P gehören im Widerspruch zur Auswahl von $p(x)$. \square

2 Rechnen mit algebraischen Zahlen

Ist das Minimalpolynom $Q(x) = x^d - r(x)$ einer algebraischen Zahl a bekannt, so gilt $a^d = r(a)$ und es lassen sich alle arithmetischen Ausdrücke ohne Division, in denen (nur) a vorkommt, also $A(a) \in \mathbb{Q}[a]$, wie folgt vereinfachen: Multipliziere den Ausdruck vollständig aus, wende die algebraische Ersetzungsregel $a^d \rightarrow r(a)$ an, und fasse danach die Ausdrücke mit gleicher Potenz a^k zusammen.

Anwenden der algebraischen Ersetzungsregel bedeutet dabei, alle Potenzen a^k mit $k \geq d$ zu ersetzen, so dass im Ergebnis nur noch Potenzen a^k mit $0 \leq k \leq d-1$ vorkommen. Die Menge dieser Potenzen bezeichnen wir als *reduzierte Terme* T_{red} , die so berechnete Darstellung

$$A(a) = c_0 + c_1 a + c_2 a^2 + \cdots + c_{d-1} a^{d-1}$$

mit $c_i \in \mathbb{Q}$ als *reduzierte Darstellung* von $A(a)$.

Satz 1 Die reduzierte Darstellung von $A(a)$ ist eindeutig bestimmt.

Beweis: Sind

$$A(a) = c_0 + c_1 a + c_2 a^2 + \cdots + c_{d-1} a^{d-1} = c'_0 + c_1 a + c'_2 a^2 + \cdots + c'_{d-1} a^{d-1}$$

zwei Darstellungen des Ausdrucks $A(a)$, so gilt

$$(c_0 - c'_0) + (c_1 - c'_1) a + (c_2 - c'_2) a^2 + \cdots + (c_{d-1} - c'_{d-1}) a^{d-1} = 0.$$

und damit $c_0 = c'_0, \dots, c_{d-1} = c'_{d-1}$, denn sonst wäre a Nullstelle eines Polynoms vom einem Grad kleiner als d . \square

Dieses Vorgehen lässt sich unmittelbar auf das Rechnen mit mehreren algebraischen Zahlen verallgemeinern: Sind $\alpha_1, \dots, \alpha_s$ algebraische Zahlen vom Grad d_1, \dots, d_s , so ergeben sich aus den entsprechenden Minimalpolynomen

$$p_i(x) = x^{d_i} - q_i(x)$$

Ersetzungsformeln

$$\{\alpha_i^{d_i} \rightarrow q_i(\alpha_i), i = 1, \dots, s\},$$

die es erlauben, jeden polynomialen Ausdruck aus $R = \mathbb{Q}[\alpha_1, \dots, \alpha_s]$ in dessen *reduzierte Form* zu transformieren, d. h. ihn als Linearkombination der $D := d_1 \cdots d_s$ Produkte aus der Menge $T_{\text{red}} := \{\alpha_1^{j_1} \cdots \alpha_s^{j_s} : 0 \leq j_i < d_i\}$ zu schreiben.

Allerdings sind diese reduzierten Formen nur im Falle $s = 1$ eindeutig, da zwischen den verschiedenen algebraischen Zahlen $\alpha_1, \dots, \alpha_s$ algebraische Abhängigkeitsrelationen bestehen können, die lineare Abhängigkeitsrelationen in der Menge T_{red} nach sich ziehen.

Beispiel: $\alpha_1 = \sqrt{2} + \sqrt{3}$, $\alpha_2 = \sqrt{6}$. Es gilt $\alpha_1^2 - 2\alpha_2 - 5 = 0$.

3 Der Ring der algebraischen Zahlen

Satz 2 Jedes Element aus $R = \mathbb{Q}[\alpha_1, \dots, \alpha_s]$ ist wieder eine algebraische Zahl.

Statt eines Beweises demonstrieren wir das Vorgehen am Beispiel des Ausdrucks $c = a + b \in \mathbb{Q}[a, b]$ für die algebraischen Zahlen $a = \sqrt{2}$ und $b = \sqrt[3]{5}$. Der allgemeine Beweis lässt sich ähnlich führen.

Um zu zeigen, dass c eine algebraische Zahl ist, müssen wir ein Polynom $p(x) = \sum_{i=0}^n r_i x^i$ finden, für das $p(c) = \sum_{i=0}^n r_i c^i = 0$ gilt.

Wir setzen $p(x)$ mit unbestimmten Koeffizienten an und berechnen zunächst die Potenzen $c^i = (a + b)^i$ als Ausdrücke in a und b wie oben beschrieben. Dazu sind die binomischen Formeln sowie die algebraischen Ersetzungen $\{a^2 \rightarrow 2, b^3 \rightarrow 5\}$ anzuwenden, die sich aus den charakteristischen Polynomen von a bzw. b unmittelbar ergeben.

Diese Rechnungen lassen sich mit Bleistift und Papier ausführen, aber auch mit einem CAS, das algebraische Ersetzungen beherrscht. Für die folgenden Rechnungen habe ich das freie CAS MAXIMA [3] verwendet.

```
tellrat(a^2=2,b^3=5);
l:makelist(ratsimp((a+b)^n),n,0,10),algebraic;
```

$$\left[\begin{array}{l} 1, \\ b + a, \\ b^2 + 2ab + 2, \\ 3ab^2 + 6b + 2a + 5, \\ 12b^2 + (8a + 5)b + 20a + 4, \\ (20a + 5)b^2 + (25a + 20)b + 4a + 100, \\ (30a + 60)b^2 + (24a + 150)b + 200a + 33, \\ (84a + 210)b^2 + (350a + 81)b + 183a + 700, \\ (560a + 249)b^2 + (264a + 1400)b + 1120a + 1416, \\ (513a + 2520)b^2 + (2520a + 1944)b + 4216a + 3485, \\ (5040a + 2970)b^2 + (6160a + 8525)b + 6050a + 21032 \end{array} \right]$$

Wir sehen, dass sich alle Potenzen als Linearkombinationen von den sechs reduzierten Termen $1, a, b, b^2, ab, ab^2$ darstellen lassen. Mehr als sechs solcher Ausdrücke sind dann sicher linear abhängig. Wir bestimmen für unser Beispiel eine solche Abhängigkeitsrelation, indem wir eine Linearkombination von sieben verschiedenen Potenzen $(a+b)^i$ mit unbestimmten Koeffizienten r_i aufstellen und die r_i dann so bestimmen, dass die sechs Koeffizienten vor $1, a, b, b^2, ab, ab^2$ alle verschwinden.

```
p:sum(concat(r,i)*x^i,i,0,6);
p1:ratsimp(subst(x=a+b,f)),algebraic;
```

$$\begin{aligned} & ((30a + 60)b^2 + (24a + 150)b + 200a + 33) r_6 \\ & + ((20a + 5)b^2 + (25a + 20)b + 4a + 100) r_5 + (12b^2 + (8a + 5)b + 20a + 4) r_4 \\ & + (3ab^2 + 6b + 2a + 5) r_3 + (b^2 + 2ab + 2) r_2 + (b + a) r_1 + r_0 \end{aligned}$$

Dieses Polynom muss zunächst in die distributive Normalform gebracht werden, um es im zweiten Schritt rekursiv nach Potenzen von a und b zu sortieren und dann die Koeffizienten vor den reduzierten Termen zu extrahieren. Leider bietet MAXIMA keine bequeme Möglichkeit, die Koeffizienten eines Polynoms zu extrahieren, deshalb die umständliche Berechnung von `coeffs` und `sys`.

```
p2: expand(p1);
coeffs: map(lambda([u], makelist(coeff(u, b, j), j, 0, 2)),
            makelist(coeff(p2, a, i), i, 0, 1));
sys: flatten(coeffs);
```

$$\left[\begin{array}{l} r_0 + 2r_2 + 5r_3 + 4r_4 + 100r_5 + 33r_6, \quad r_1 + 6r_3 + 5r_4 + 20r_5 + 150r_6, \\ r_2 + 12r_4 + 5r_5 + 60r_6, \quad r_1 + 2r_3 + 20r_4 + 4r_5 + 200r_6, \\ 2r_2 + 8r_4 + 25r_5 + 24r_6, \quad 3r_3 + 20r_5 + 30r_6 \end{array} \right]$$

Das ist ein homogenes lineares Gleichungssystem, dessen Lösung von einem Parameter abhängt.

```
vars: makelist(concat(r, i), i, 0, 6);
sol: solve(sys, vars);
```

$$\left[[r_0 = 17\%r_4, r_1 = -60\%r_4, r_2 = 12\%r_4, r_3 = -10\%r_4, r_4 = -6\%r_4, r_5 = 0, r_6 = \%r_4] \right]$$

Ein Polynom mit der Nullstelle $c = a + b$ lautet also

```
p0: subst(%r4=1, subst(sol[1], p));
```

$$p_0 = x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17$$

Testen wir schließlich noch, ob dieses Polynom irreduzibel ist:

```
factor(p0);
```

Damit wissen wir, dass es sich bei diesem Polynom sogar um das Minimalpolynom von $c = a + b$ handelt.

4 Quotienten algebraischer Zahlen

Von einfachen algebraischen Zahlen wie etwa $1 + \sqrt{2}$ oder $\sqrt{2} + \sqrt{3}$ wissen wir, dass man die jeweilige Inverse dazu recht einfach darstellen kann, wenn man mit einer auf geeignete Weise definierten *konjugierten* Zahl erweitert. So gilt etwa

$$\frac{1}{1 + \sqrt{2}} = \frac{1 - \sqrt{2}}{1 - 2} = \sqrt{2} - 1 \quad \text{und} \quad \frac{1}{\sqrt{2} + \sqrt{3}} = \frac{\sqrt{3} - \sqrt{2}}{3 - 2} = \sqrt{3} - \sqrt{2}.$$

Damit kann man in diesen Fällen auch die Inverse einer algebraischen Zahl (und damit beliebige Quotienten) als lineare Kombination der reduzierten Terme darstellen. Es stellt sich die

Frage, ob dies auch für kompliziertere rationale Ausdrücke mit algebraischen Zahlen möglich ist. Wie sieht es z. B. mit

$$\frac{1}{\sqrt{2} + \sqrt{3} + \sqrt{5}}$$

aus?

AXIOM liefert als Ergebnis sofort

$$\frac{1}{6}\sqrt{3} + \frac{1}{4}\sqrt{2} - \frac{1}{12}\sqrt{30}$$

Für die anderen Systeme sind dazu spezielle Funktionen, Schalter und/oder Pakete notwendig, so in MAPLE die Funktion `rationalize` aus der gleichnamigen Bibliothek und in MUPAD die Funktion `radsimp`. In REDUCE muss der Schalter `rationalize` eingeschaltet sein. In MAXIMA ist dazu die rationale Normalform im Kontext `algebraic` zu berechnen:

```
a:sqrt(2)+sqrt(3)+sqrt(5);
ratsimp(1/a), algebraic;
```

$$-\frac{\sqrt{2}\sqrt{3}\sqrt{5} - 2\sqrt{3} - 3\sqrt{2}}{12}$$

Untersuchen wir, auf welchem Wege sich eine solche Darstellung finden ließe. Wie oben findet man heraus, dass $a = \sqrt{2} + \sqrt{3} + \sqrt{5}$ das charakteristische Polynom

$$p(x) = x^8 - 40x^6 + 352x^4 - 960x^2 + 576$$

hat, d. h. es gilt $a^8 - 40a^6 + 352a^4 - 960a^2 + 576 = 0$ oder

$$a^{-1} = \frac{-a^7 + 40a^5 - 352a^3 + 960a}{576}.$$

Ist das charakteristische Polynom bekannt, so ist es also nicht schwer, a^{-1} zu berechnen. Es werden einzig noch Ringoperationen benötigt, um den Ausdruck zu vereinfachen:

$$a^{-1} = \text{subst} \left(a = \sqrt{2} + \sqrt{3} + \sqrt{5}, \frac{-a^7 + 40a^5 - 352a^3 + 960a}{576} \right).$$

5 Die Aufgabe φ 28

Mit dem im letzten Abschnitt beschriebenen Verfahren kann man zwar nun auch Quotienten in Linearkombinationen reduzierter Terme überführen, allerdings muss für jeden Divisor erst umständlich das Minimalpolynom bestimmt werden. Wir zeigen am Beispiel der Aufgabe φ 28, dass ein Ansatz mit unbestimmten Koeffizienten, wie wir ihn schon oben bei der Bestimmung des Minimalpolynoms von $c = a + b$ erfolgreich angewendet haben, auch hier weiterhilft.

Gegeben sind in unserem Fall zwei algebraische Zahlen

$$a = \sqrt[4]{2} \text{ und } b = \sqrt{78 + 52a + 51a^2 + 34a^3}$$

und der zu vereinfachende Ausdruck $A = \frac{14}{b}$. Die Ersetzungsregeln der beiden algebraischen Zahlen lauten $a^4 \rightarrow 2$ und $b^2 \rightarrow 78 + 52a + 51a^2 + 34a^3$, als reduzierte Terme ergeben sich $T_{\text{red}} = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$. Wir suchen eine Linearkombination

$$p = r_0 + r_1 a + r_2 a^2 + r_3 a^3 + r_4 b + r_5 a b + r_6 a^2 b + r_7 a^3 b$$

mit $p \cdot b - 14 = 0$ und verfahren dazu wie oben (alle Rechnungen wiederum mit MAXIMA):

```
tellrat(b^2=78+52*a+51*a^2+34*a^3,a^4=2);
p:r0+r1*a+r2*a^2+r3*a^3+r4*b+r5*a*b+r6*a^2*b+r7*a^3*b;
u1:ratsimp(p*b-14),algebraic;
```

$$\begin{aligned} u_1 = & (78a^3 + 68a^2 + 102a + 104)r_7 + (52a^3 + 78a^2 + 68a + 102)r_6 \\ & + (51a^3 + 52a^2 + 78a + 68)r_5 + (34a^3 + 51a^2 + 52a + 78)r_4 \\ & + a^3 b r_3 + a^2 b r_2 + a b r_1 + b r_0 - 14. \end{aligned}$$

Dieser Ausdruck ist nach Termen aus T_{red} zu sortieren. Die Koeffizienten vor den reduzierten Termen ergeben ein lineares Gleichungssystem zur Bestimmung der r_i .

```
u2:expand(u1);
coeffs:map(lambda([u],makelist(coeff(u,a,j),j,0,3)),
  makelist(coeff(u2,b,i),i,0,1));
sys:flatten(coeffs);
```

$$\left[\begin{array}{l} 104r_7 + 102r_6 + 68r_5 + 78r_4 - 14, \quad 102r_7 + 68r_6 + 78r_5 + 52r_4, \\ 68r_7 + 78r_6 + 52r_5 + 51r_4, \quad 78r_7 + 52r_6 + 51r_5 + 34r_4, \quad r_0, \quad r_1, \quad r_2, \quad r_3 \end{array} \right]$$

Wir sehen bereits an dieser Stelle, dass $r_0 = r_1 = r_2 = r_3 = 0$ sein muss, der gesuchte Ausdruck also – anders als in Möwalds Lösung [2] – ein Vielfaches von b ist. Wir lösen dieses (inhomogene lineare) Gleichungssystem, setzen die in diesem Fall eindeutig bestimmte Lösung

```
vars:[r0,r1,r2,r3,r4,r5,r6,r7];
sol:solve(sys,vars);
```

$$\left[\left[r_0 = 0, \quad r_1 = 0, \quad r_2 = 0, \quad r_3 = 0, \quad r_4 = \frac{6}{7}, \quad r_5 = -\frac{4}{7}, \quad r_6 = -\frac{3}{7}, \quad r_7 = \frac{2}{7} \right] \right]$$

in p ein und erhalten

```
p0:subst(sol[1],p);
```

$$p_0 = \frac{2a^3 b - 3a^2 b - 4ab + 6b}{7} = \frac{b}{7} (2a^3 - 3a^2 - 4a + 6).$$

Die gestellte Aufgabe ist gelöst, allein die Differenz zu Möwalds Lösung $m = a^2 - 2a^2 + 2$ in [2] bleibt zu diskutieren. Möwalds größter Trick ist gleich in der ersten Umformung

$$78 + 52a + 51a^2 + 34a^3 = (3a^3 + a^2 + 5a + 4)^2$$

enthalten und zeigt, dass $b^2 - (78 + 52a + 51a^2 + 34a^3)$ über $\mathbb{Q}[a]$ nicht irreduzibel ist. Faktorisieren über algebraischen Erweiterungskörpern ist im Allgemeinen eine komplizierte Angelegenheit. In diesem speziellen Fall findet MAXIMA aber die Faktorisierung:

```
factor(b^2-(78+52*a+51*a^2+34*a^3),a^4-2);
```

$$(b - 3a^3 - a^2 - 5a - 4) (b + 3a^3 + a^2 + 5a + 4)$$

Nehmen wir dagegen Möwalds Lösung als Orakel („Da kam ein Wanderer des Wegs und sagte: m ist eine Lösung“), so liefert $p_0 = m$ eine algebraische Abhängigkeitsrelation zwischen den reduzierten Termen, aus der wir eine Darstellung für b extrahieren können:

```
m:a^3-2*a^2+2;  
solve(pp=m,b);
```

$$b = \frac{7a^3 - 14a^2 + 14}{2a^3 - 3a^2 - 4a + 6},$$

die wir wieder in eine Linearkombination der Terme a^0, a^1, a^2, a^3 umrechnen können

```
ratsimp(solve(pp=m,b)),algebraic;
```

$$b = 3a^3 + a^2 + 5a + 4$$

Wir haben damit also Möwalds Trick „reverse engineered“.

1. [1] Aufgabe φ 28 von Friedhelm Götze. Wurzel **48**, Heft 6 (2014), S. 143.
2. [2] Lösung der φ 28 von Reiner Möwald. Wurzel **49**, Heft 1
3. [3] Maxima 5.32.1, <http://maxima.sourceforge.net>
4. [4] Hans-Gert Gräbe: Skript zum Kurs „Einführung in das symbolische Rechnen“. Sommersemester 2012. <http://www.informatik.uni-leipzig.de/~graebe/skripte/esr12.pdf>

Attribution Section

graebe (2010-12-16)