# „Wurzel aus $2$“ und „Wurzel aus $-1$“ Was ist das und wie rechnet man damit?

Franz Pauer
Institut für Mathematik, Universität Innsbruck,
Technikerstr. 13, A-6020 Innsbruck, Österreich.
Franz.Pauer@uibk.ac.at

## 1 Einleitung

Im Mathematikunterricht der vierten bzw. siebten Klasse der Sekundarstufe treten Probleme auf, die man in dem bis dahin bekannten Zahlbereich (dem Körper der rationalen Zahlen $\mathbb{Q}$ bzw. dem Körper der reellen Zahlen $\mathbb{R}$) nicht lösen kann. In der vierten Klasse möchte man zum Beispiel die Länge der Diagonale eines Quadrates mit Seitenlänge $1$ berechnen. Das müsste eine Zahl sein, deren Quadrat zwei ist. In $\mathbb{Q}$ gibt es aber keine solche Zahl. In der siebten Klasse sucht man nach einer Nullstelle des Polynoms $x^2 + 1$, also nach einer Zahl, deren Quadrat $-1$ ist. In $\mathbb{R}$, dem zu diesem Zeitpunkt bekannten Zahlbereich, existiert sie aber nicht. Also muss der Zahlbegriff erweitert und der Zahlbereich vergrößert werden.

Was sind aber diese neuen Zahlen wie zum Beispiel „Wurzel aus 2“ bzw. „Wurzel aus $-1$“? Man kann sie leicht definieren: Eine Wurzel aus $2$ ist eine Zahl, deren Quadrat $2$ ist. Eine Wurzel aus $-1$ ist eine Zahl, deren Quadrat $-1$ ist. Anders formuliert: Eine Wurzel aus $2$ ist eine Nullstelle des Polynoms $x^2 - 2$. Eine Wurzel aus $-1$ ist eine Nullstelle des Polynoms $x^2 + 1$.
Aber: Gibt es diese Zahlen? In $\mathbb{Q}$ jedenfalls nicht. Wenn es eine Wurzel aus $2$ bzw. $-1$ gibt, dann ist sie nicht eindeutig bestimmt: Wenn $a^2 = 2$ bzw. $-1$ ist, dann ist auch $(-a)^2 = 2$ bzw. $-1$.
Wenn es diese Wurzeln gibt: Wie stellt man sie (durch endlich viele Daten) dar, wie rechnet man damit am Computer?

Viele Nutzer des Computeralgebrasystems Maple sind überrascht, wenn dieses auf die Frage nach den Nullstellen des Polynoms $x^4 + x^3 - 1$ im Wesentlichen nichts anderes antwortet als „die erste Nullstelle, die zweite Nullstelle, die dritte

[1] Dieser Beitrag ist die schriftliche Ausarbeitung meines Vortrages beim Lehrerfortbildungstag am 28. März 2008 in Wien.

Nullstelle, die vierte Nullstelle“. Noch mehr überrascht dann, dass man mit diesen vier Nullstellen in Maple gut rechnen kann, zum Beispiel ist ihre Summe die Zahl $1$ und ihr Produkt die Zahl $-1$.

In diesem Beitrag wird ein einfaches Verfahren, Zahlbereichserweiterungen zu konstruieren, in denen gegebene Polynome Nullstellen haben, vorgestellt. Damit soll verständlich gemacht werden, wie ein Computeralgebrasystem mit Wurzeln rechnet. Insbesondere wird die Analogie der Konstruktion der Wurzeln aus $2$ und aus $-1$ verdeutlicht. Weiters soll angeregt werden, manche Aufgaben zum Rechnen mit Wurzeln im Schulunterricht präziser (und zugleich einfacher) zu formulieren.

In [TK] zum Beispiel findet man die Aufgaben
Aufgabe 2.13 d): Berechne und vereinfache: $(3 \cdot \sqrt{2} - 2) \cdot (\sqrt{2} + 2)$.
Aufgabe 2.26 j): Der Nenner ist wurzelfrei zu machen: $\frac{1}{1+\sqrt{3}}$.

Wird bei der ersten Aufgabe die Antwort $7.656854245\ldots$ akzeptiert und bei der zweiten die Antwort

$$\frac{1}{1+\sqrt{3}} = \frac{\frac{1}{1+\sqrt{3}}}{1} \; ?$$

Wenn nein, warum nicht?

In den Abschnitten 4 und 6 erläutern wir das oben genannte Verfahren am Beispiel der Konstruktion von Zahlbereichen, die eine Wurzel aus $2$ bzw. aus $-1$ enthalten. Die algebraischen Hilfsmittel dazu, die Division mit Rest von Polynomen, der Euklidische Algorithmus und der erweiterte Euklidische Algorithmus, werden in den Abschnitten 3 und 5 in Erinnerung gerufen (siehe dazu [GG], [L], [P1], [P2]). Im Abschnitt 7 wird das Verfahren für beliebige irreduzible Polynome vorgestellt. Die Beispiele wurden mit Maple 11 gerechnet.

# 2 Zahlbereichserweiterungen

Im Laufe der Schulzeit verändert sich mehrfach das, was wir mit dem Wort „Zahl“ bezeichnen. Unser Zahlbereich wird schrittweise erweitert. Der Anlass für die Erweiterung eines Zahlbereichs ist immer eine Aufgabe, die „eigentlich eine Lösung haben sollte“, aber im bekannten Zahlbereich nicht lösbar ist. In der folgenden Tabelle sind einige Aufgaben, die Zahlbereichserweiterungen motivieren, zusammengestellt.
Dabei bezeichnen $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ wie üblich die Mengen der natürlichen, ganzen, rationalen, reellen und komplexen Zahlen. Die Bedeutung von $\mathbb{Q}[\sqrt[n]{t}]$ wird in den Abschnitten 4, 6 und 7 erläutert.

| **Zahlbereichserweiterung** | **Motivation dafür z.B. durch die Aufgabe:** Finde eine Zahl $z$ so, dass |
|---|---|
| $\mathbb{N} \subseteq \mathbb{Z}$ | $3 + z = 2$ |
| $\mathbb{Z} \subseteq \mathbb{Q}$ | $3 \cdot z = 2$ |
| $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[n]{t}]$<br>$(n \in \mathbb{N}_{\geq 2},\, t \in \mathbb{Q})$ | $z^n = t$ |
| $\mathbb{Q} \subseteq \mathbb{R}$ | $z = \lim_{n\to\infty} t_n$<br>(für gewisse Folgen $(t_n)_{n\in\mathbb{N}}$ in $\mathbb{Q}$) |
| $\mathbb{R} \subseteq \mathbb{C}$ | $z^2 = -1$ |

„Erweitere den Zahlbereich $K$ (mit $+$ und $\cdot$) zum Zahlbereich $L$ (mit $+$ und $\cdot$)“ (um eine gegebene Aufgabe zu lösen) heißt

- $L$ als Menge, die $K$ enthält, angeben,
- die Rechenoperationen $+$ und $\cdot$ auf $K$ zu Rechenoperationen auf $L$ erweitern,

und zwar so, dass

- der „Rechenkomfort“ erhalten bleibt, das heißt alle Rechenregeln für $+$ und $\cdot$ in $K$ sollen auch in $L$ gelten (insbesondere: wenn $K$ ein Körper ist, dann soll $L$ auch ein Körper sein),
- die gegebene Aufgabe eine Lösung in $L$ hat

  und

- $L$ „möglichst klein“ ist.

# 3 Erinnerung: Division mit Rest von Polynomen

Ist $f$ ein Polynom, dann schreiben wir $grad(f)$ für den Grad von $f$ und $lk(f)$ für den Leitkoeffizienten von $f$.

**Satz** (*Division mit Rest von Polynomen*):
Zu je zwei Polynomen $f$ und $g$ mit $g \neq 0$ gibt es eindeutig bestimmte Polynome $m$ und $r$ mit den Eigenschaften

$$f = m \cdot g + r \quad \text{und} \quad [r = 0 \text{ oder } grad(r) < grad(g)] \,.$$

Dabei heißt $m$ der *polynomiale Quotient von $f$ und $g$* und $r$ der *Rest von $f$ nach Division durch $g$*.
**Divisionsalgorithmus:** Diese Polynome $m$ und $r$ können wie folgt berechnet werden:

- Setze $m := 0$ und $r := f$.
- Solange $r \neq 0$ und $grad(r) \geq grad(g)$ ist, ersetze $r$ durch $r - t \cdot g$ und $m$ durch $m + t$, wobei

  $$t := lk(r) \cdot lk(g)^{-1} \cdot x^{grad(r)-grad(g)}$$

  ist.

**Beispiel:** Seien

$$f := x^4 + 2x^3 - 2x^2 + x - 1 \qquad \text{und} \qquad g := x^2 - 2 \,.$$

Wir berechnen mit dem oben angegebenen Verfahren Polynome $m$ und $r$ mit $f = m \cdot g + r$ und ($r = 0$ oder $grad(r) < grad(g) = 2$). Dabei beginnen wir mit $r := f$ und schreiben die Zwischenrechnungen platzsparend untereinander.

$$\begin{array}{llllll} \mathbf{x^4} & +2x^3 & -2x^2 & +x & -1 & = (x^2+2x)g + (5x-1) \\ -x^4 & & +2x^2 & & & \\ & & & & & \\ & \mathbf{+2x^3} & & +x & -1 & \\ & -2x^3 & & +4x & & \\ & & & & & \\ & & & \mathbf{+5x} & -1 & \end{array}$$

Also ist $m = x^2 + 2x$ und $r = 5x - 1$.

Eine ausführlichere Darstellung der Division mit Rest und ihrer grundlegenden Bedeutung in der Algebra findet man zum Beispiel in [P1].

# 4 Konstruktion von Zahlbereichen, die $\mathbb{Q}$ und $\sqrt{2}$ bzw. $\sqrt{-1}$ enthalten

Es sei

$$\mathbb{Q}[x] := \{ \sum_{i=0}^{n} c_i x^i \,|\, n \in \mathbb{N},\, c_0, \ldots, c_n \in \mathbb{Q} \}$$

die Menge aller Polynome (in $x$) mit Koeffizienten in $\mathbb{Q}$. Mit den Rechenoperationen

$$\sum_{i=0}^{n} c_i x^i + \sum_{i=0}^{n} d_i x^i := \sum_{i=0}^{n} (c_i + d_i) x^i$$

und

$$\left( \sum_{i=0}^{n} c_i x^i \right) \cdot \left( \sum_{j=0}^{n} d_j x^j \right) := \sum_{k=0}^{2n} \Big( \sum_{\substack{i,\, j \\ i+j=k}} c_i d_j \Big) x^k$$

ist $\mathbb{Q}[x]$ ein kommutativer Ring (das heißt: es gelten dieselben Rechenregeln wie für die Addition und Multiplikation von ganzen Zahlen), aber kein Körper (das heißt: die Division ist nicht durch jedes Polynom $\neq 0$ möglich).

Wir betrachten nun die Menge $L := \{a + bx \,|\, a, b \in \mathbb{Q}\} \subseteq \mathbb{Q}[x]$ mit der Addition

$$(a + bx) + (c + dx) := (a + c) + (c + d)x$$

und der (neuen) Multiplikation

$$(a + bx) * (c + dx) :=$$

$$= \text{ Rest von } (a + bx) \cdot (c + dx) \text{ nach Division durch } x^2 - 2 \text{ bzw. } x^2 + 1\,.$$

Das Produkt $(a+bx)\cdot(c+dx)$ der Polynome $a+bx$ und $c+dx$ liegt nicht in $L$, wohl aber sein Rest nach Division durch $x^2-2$ bzw. $x^2+1$. Daher ist $(a+bx)*(c+dx)$ ein Element von $L$. Wir werden im Abschnitt 6 zeigen, dass alle Elemente $\neq 0$ in $L$ ein bezüglich $*$ inverses Element haben. Dann kann leicht nachgeprüft werden, dass in $L$ mit $+$ und $*$ alle Rechenregeln eines Körpers erfüllt sind.

Wir berechnen nun $x * x$, das Quadrat von $x$ in $L$. Nach Definition ist $x * x$ der Rest von $x \cdot x = x^2$ nach Division durch $x^2 - 2$ bzw. $x^2 + 1$, also $2$ bzw. $-1$.

Das heißt: $x \in L$ ist eine Wurzel aus $2$ bzw. $-1$! Es gibt also sowohl die Wurzel aus $2$ als auch die aus $-1$, wir haben sie soeben konstruiert. Wir schreiben daher

$$\sqrt{2} \text{ bzw. } \sqrt{-1} \text{ (oder } i) \text{ anstatt } x$$

und

$$\mathbb{Q}[\sqrt{2}] \text{ bzw. } \mathbb{Q}[\sqrt{-1}\,] \text{ (oder } \mathbb{Q}[i]) \text{ anstatt } L\,.$$

Alle Elemente von $L$ können eindeutig in der Form $a + bx$ mit $a, b \in \mathbb{Q}$ angeschrieben werden, in der neu eingeführten Schreibweise somit in der Form $a + b\sqrt{2}$ bzw. $a + bi$. Damit kann präzisiert werden, was mit Aufgaben wie zum Beispiel

Berechne und vereinfache $(3 \cdot \sqrt{2} - 2) \cdot (\sqrt{2} + 2)$!

gemeint ist, nämlich:
Berechne rationale Zahlen $a$ und $b$ so, dass

$$(3 \cdot \sqrt{2} - 2) \cdot (\sqrt{2} + 2) = a + b\sqrt{2}$$

ist!

In einer Programmiersprache wird man die Elemente von $L$ durch Paare von rationalen Zahlen darstellen, also $(a, b)$ anstatt $a + bx$ oder $a + b\sqrt{2}$ bzw. $a + bi$ schreiben. Die Summe und das Produkt zweier solcher Zahlenpaare ist dann

$$(a, b) + (c, d) = (a + c, b + d)\,,$$

$$(a, b) * (c, d) = (ac + 2bd, ad + bc) \text{ bzw. } (ac - bd, ad + bc)\,.$$

Die Zahlen $1$ $(= 1 + 0x)$ und $\sqrt{2}$ bzw. $i$ $(= 0 + 1x)$ werden dann durch die Zahlenpaare $(1, 0)$ und $(0, 1)$ dargestellt. Insbesondere ist

$$(0, 1)^2 = (2, 0) \text{ bzw. } (-1, 0)\,.$$

# 5 Erinnerung: Der erweiterte Euklidische Algorithmus

Ein Polynom $h$ *teilt* ein Polynom $f$ in $\mathbb{Q}[x]$, wenn es in $\mathbb{Q}[x]$ ein Polynom $g$ gibt so, dass $f = g \cdot h$ ist. In diesem Fall ist $f$ ein *Vielfaches* von $h$. Ein Polynom ist *normiert*, wenn sein Leitkoeffizient $1$ ist. Der *größte gemeinsame Teiler zweier Polynome* in $\mathbb{Q}[x]$ ist das normierte Polynom größten Grades, das beide teilt. Der größte gemeinsame Teiler zweier Polynome $f$ und $g$ (kurz: $ggT(f, g)$) kann mit dem Euklidischen Algorithmus (mehrfaches Anwenden der Division mit Rest) berechnet werden. Mit dem erweiterten Euklidischen Algorithmus wird darüber hinaus eine Darstellung des $ggT(f, g)$ als Summe von Vielfachen von $f$ und $g$ ermittelt:
**Satz:** Es seien $f, g$ Polynome, beide $\neq 0$. Es gibt Polynome $u, v$ so, dass

$$u \cdot f + v \cdot g = ggT(f, g)$$

ist. Diese können mit dem folgenden Verfahren (erweiterter Euklidischer Algorithmus) berechnet werden:

- Setze $A := (A_1, A_2, A_3) := (f, 1, 0)$ und
  $B := (B_1, B_2, B_3) := (g, 0, 1)$ .
- Solange $B_1$ das Polynom $A_1$ nicht teilt, berechne den polynomialen Quotienten $m$ von $A_1$ und $B_1$ und setze
  $C := B$,
  $B := A - m \cdot C := (A_1 - m \cdot C_1, A_2 - m \cdot C_2, A_3 - m \cdot C_3)$ und
  $A := C$.
- Wenn $B_1$ das Polynom $A_1$ teilt, setzt man
  $u := lk(B_1)^{-1} \cdot B_2$ und $v := lk(B_1)^{-1} \cdot B_3$ .

Denn: Wenn zwei Tripel von Polynomen $S$ und $T$ die Eigenschaft

$$S_1 = f \cdot S_2 + g \cdot S_3 \quad \text{bzw.} \quad T_1 = f \cdot T_2 + g \cdot T_3$$

haben, dann auch alle Tripel $S - mT$, wobei $m$ ein Polynom und $mT$ das Tripel $(mT_1, mT_2, mT_3)$ ist. Die ersten zwei Tripel im Algorithmus haben diese Eigenschaft, daher auch alle anderen auftretenden Tripel. Für die ersten Komponenten der Tripel wird der euklidische Algorithmus durchgeführt, für das letzte Tripel $B$ gilt daher $lk(B_1) \cdot ggT(f, g) = f \cdot B_2 + g \cdot B_3$.

In allen Computeralgebrasystemen ist der erweiterte Euklidische Algorithmus implementiert. In Maple wird er nach Eingabe des Befehls gcdex ausgeführt. Gibt man Polynome $f$, $g$ ein, die mit dem Symbol $x$ dargestellt werden, dann berechnet gcdex$(f, g, x, u, v)$ Polynome $u$ und $v$ so, dass $ggT(f, g) = u \cdot f + v \cdot g$ ist.

**Beispiel** (Maple 11):

```
> f:=x^4+2*x^3-2*x^2+x-1;
```

$$f := x^4 + 2\,x^3 - 2\,x^2 + x - 1$$

```
> g:=x^2-2;
```

$$g := x^2 - 2$$

```
> gcdex(f,g,x,u,v);
```

$$1$$

```
> u; v;
```

$$\frac{1}{49} + \frac{5\,x}{49}$$

$$-\frac{25}{49} - \frac{5}{49}\,x^3 - \frac{11}{49}\,x^2 - \frac{2}{49}\,x$$

```
> 1=u*f+v*g;
```

$$1 = (\frac{1}{49} + \frac{5\,x}{49}) \cdot f + (-\frac{25}{49} - \frac{5}{49}\,x^3 - \frac{11}{49}\,x^2 - \frac{2}{49}\,x) \cdot g$$

# 6 Division in $\mathbb{Q}[\sqrt{2}]$ bzw. $\mathbb{Q}[i]$

Wir schreiben in diesem Abschnitt $y$ für 2 bzw. $-1$ und $L$ für $\mathbb{Q}[\sqrt{2}]$ bzw. $\mathbb{Q}[i]$.

Das Polynom $x^2 - y$ ist in $\mathbb{Q}[x]$ irreduzibel, das heißt, es kann nicht als Produkt von zwei Polynomen in $\mathbb{Q}[x]$ kleineren Grades geschrieben werden. Daher ist $ggT(x^2 - y, a + bx) = 1$ , für alle $a, b \in \mathbb{Q}$ (mit $a \neq 0$ oder $b \neq 0$).

Kann in $L$ dividiert werden? Anders formuliert: Gibt es zu allen Polynomen $0 \neq f := a + bx \in L$ ein Polynom $g \in L$ mit $g * f = 1$?

Weil $x^2 - y$ irreduzibel ist und $f \neq 0$ den Grad 1 hat, muss $ggT(x^2 - y, f) = 1$ sein. Wir können daher mit dem erweiterten Euklidischen Algorithmus Polynome $u, v \in \mathbb{Q}[x]$ berechnen mit

$$u \cdot (x^2 - y) + v \cdot f = 1\ .$$

Der Rest von $u \cdot (x^2 - y) + v \cdot f$ nach Division durch $x^2 - y$ ist daher 1, andererseits (weil $u \cdot (x^2 - y) + v \cdot f$ die Summe eines Vielfachen von $x^2 - y$ und von $v \cdot f$ ist) ist er auch gleich dem Rest von $v \cdot f$ nach Division durch $x^2 - y$, also gleich $v * f$. Daher ist $v * f = 1$. Sei $r \in L$ der Rest von $v$ nach Division durch $x^2 - y$, dann ist $v = m \cdot (x^2 - y) + r$ und ($r = 0$ oder $grad(r) < 2$). Somit folgt

$$1 = v * f = ((x^2 - y) + r) * f = r * f$$

und $r = f^{-1} \in L$. Daher ist $L$ ein Körper.

Seien $f$ und $g$ Elemente von $L$ und $f \neq 0$. Den *Nenner von $\frac{g}{f}$ wurzelfrei machen* bedeutet also, die eindeutig bestimmten rationalen Zahlen $a$ und $b$ mit $g * f^{-1} = a + bx \in L$ zu berechnen. Die Überlegungen oben zeigen, dass das immer möglich ist. Aufgaben wie

„Mache den Nenner von $\frac{1}{c\sqrt{2}+d}$ wurzelfrei!“

(wobei $c$ und $d$ rationale Zahlen sind, von denen mindestens eine nicht 0 ist) sollten daher (ebenso einfach, aber genauer) in der Form

„Berechne rationale Zahlen $a$ und $b$ so, dass $\frac{1}{c\sqrt{2}+d} = a + b\sqrt{2}$ ist!“

gestellt werden.

**Beispiel: Rechnen mit „Wurzel aus 2 “ in Maple**

Zunächst wird mit dem Befehl *irreduc* überprüft, ob das Polynom $x^2 - 2$ in $\mathbb{Q}[x]$ irreduzibel ist.

```
> irreduc(x^2-2);
```

$$true$$

Dann wählen wir für RootOf($Z^2 - 2$), das dem Element $\sqrt{2}$ in $\mathbb{Q}[\sqrt{2}]$ entspricht, die Abkürzung $\alpha$.

```
> alias(alpha=RootOf(Z^2-2));
```

$$\alpha$$

```
> alpha^2;
```

$$\alpha^2$$

Mit *evala(*$alpha^2$*)* werden die eindeutig bestimmten rationalen Zahlen $a, b$ mit $\alpha^2 = a + b\alpha$ berechnet.

```
> evala(alpha^2);
```

$$2$$

Mit *evala(*$(1-2*alpha+3*alpha^2)*(2+alpha^3)-9*alpha-3$*)* werden die eindeutig bestimmten rationalen Zahlen $a, b$ mit $(1-2\alpha+3\alpha^2)\cdot(2+\alpha^3)-9\alpha-3 = a + b\alpha$ berechnet.

```
> evala((1-2*alpha+3*alpha^2)*(2+alpha^3)-9*alpha-3);
```

$$3 + \alpha$$

Nun werden die eindeutig bestimmten rationalen Zahlen $a, b$ mit $\frac{1}{3\alpha+4} = a+b\alpha$ berechnet:

```
> evala(1/(3*alpha+4));
```

$$-2 + \frac{3\,\alpha}{2}$$

Dazu wurde der erweiterte Euklidische Algorithmus verwendet:

```
> gcdex(x^2-2,3*x+4,x,u,v);
```

$$1$$

```
> v;
```

$$-2 + \frac{3\,x}{2}$$

```
> subs(x=alpha,v);
```

$$-2 + \frac{3\,\alpha}{2}$$

Abschließend „machen wir den Nenner von $\frac{1}{(5\sqrt{2}+1)^3}$ wurzelfrei“, das heißt, wir lassen uns von Maple die eindeutig bestimmten rationalen Zahlen $a, b$ mit $\frac{1}{(5\sqrt{2}+1)^3} = a + b\sqrt{2}$ berechnen:

```
> evala((5*alpha+1)^(-3));
```

$$-\frac{151}{117649} + \frac{265\,\alpha}{117649}$$

**Beispiel: Rechnen mit „Wurzel aus $-1$“ in Maple**

Ersetzen wir das Polynom $x^2 - 2$ durch das Polynom $x^2 + 1$, rechnet Maple in $\mathbb{Q}[i]$ (statt wie oben in $\mathbb{Q}[\sqrt{2}]$).

```
> irreduc(x^2+1);
```

$$true$$

```
> alias(i=RootOf(Z^2+1));
```

$$i$$

```
> 1/(4-3*i);
```

$$\frac{1}{4-3\,i}$$

```
> evala(1/(4-3*i));
```

$$\frac{4}{25} + \frac{3\,i}{25}$$

# 7 Konstruktion von Nullstellen irreduzibler Polynome

Sei $K$ ein Körper (zum Beispiel $\mathbb{Q}$ oder $\mathbb{R}$), $h$ ein normiertes irreduzibles Polynom in $K[x]$ und sei

$$L := \{ \sum_{i=0}^{n} c_i x^i \mid n < grad(h),\ c_0, \ldots, c_n \in K \} \subseteq K[x] .$$

Mit der Addition von Polynomen und der (neuen) Multiplikation

$$f * g := \text{ Rest von } f \cdot g \text{ nach Division durch } h$$

($f, g \in L$) ist $L$ ist ein Körper. Es genügt zu zeigen, dass es zu jedem von $0$ verschiedenen Element $f \in L$ ein Polynom $g \in L$ mit $g * f = 1$ gibt. Die anderen Rechenregeln eines Körpers sind leicht nachzuprüfen.
Sei $0 \neq f \in L$, dann ist $ggT(f, h) = 1$, weil $h$ irreduzibel ist und $grad(f)$ kleiner als $grad(h)$ ist. Wir können daher mit dem erweiterten Euklidischen Algorithmus Polynome $u, v \in \mathbb{Q}[x]$ berechnen mit

$$u \cdot h + v \cdot f = 1 .$$

Der Rest von $u \cdot h + v \cdot f$ nach Division durch $h$ ist daher $1$, andererseits (weil $u \cdot h + v \cdot f$ die Summe eines Vielfachen von $h$ und von $v \cdot f$ ist) ist er auch gleich dem Rest von $v \cdot f$ nach Division durch $h$, also gleich $v * f$. Daher ist $v * f = 1$.
Sei $r \in L$ der Rest von $v$ nach Division durch $h$, dann ist $v = m \cdot h + r$ und ($r = 0$ oder $grad(r) < grad(h)$). Somit folgt

$$1 = v * f = (h + r) * f = h * f + r * f = r * f$$

und $r = f^{-1} \in L$.

Weil $h$ normiert ist, ist der Grad von $p := h - x^{grad(h)}$ kleiner als der Grad von $h$. Somit ist $-p$ der Rest von $x^{grad(h)}$ nach Division von $p$ durch $h$. Multipliziert man in $L$ das Element $x$ $grad(h)$-mal mit sich selbst, erhält man also $-p$. Setzt man $x \in L$ in das Polynom $h$ ein, erhält man daher $-p+p$, also $0$. Somit ist $x \in L$ eine Nullstelle von $h \in K[x]$.

Alle Elemente von $L$ können in eindeutiger Weise als rationale Linearkombinationen von

$$1, x, \ldots, x^{grad(f)-1}$$

geschrieben werden.

**Beispiel:**

Sei $h := x^3 - 2 \in \mathbb{Q}[x]$ und $f := x^2 + x + 2$. Wir schreiben $\sqrt[3]{2}$ für die Nullstelle $x$ von $h$ in $L =: \mathbb{Q}[\sqrt[3]{2}]$. Dann ist

$$f * (-\frac{1}{2}x^2 + 1) = 1 \in L\,,$$

also

$$\frac{1}{\sqrt[3]{4} + \sqrt[3]{2} + 2} = -\frac{1}{2}\sqrt[3]{4} + 1\,.$$

**Beispiel: Rechnen mit einer „5-ten Wurzel aus 2“ (einer Nullstelle von $x^5 - 2$) in Maple**

```
> g:=x^5-2;
```

$$g := x^5 - 2$$

```
> irreduc(g);
```

$$true$$

Das Polynom $g \in \mathbb{Q}[x]$ ist irreduzibel. Wir wählen für RootOf($Z\hat{}5 - 2$), eine seiner Nullstellen, die Abkürzung $\beta$.

```
> alias(beta=RootOf(Z^5-2));
```

$$\beta$$

```
> u:=(2*beta^4-3*beta^3 -2*beta^2+beta-8)^(-1);
```

$$u := \frac{1}{2\,\beta^4 - 3\,\beta^3 - 2\,\beta^2 + \beta - 8}$$

Mit *evala(u)* werden die eindeutig bestimmten rationalen Zahlen $a, b, c, d, e$ mit $u = a + b\beta + c\beta^2 + d\beta^3 + e\beta^4$ berechnet.

```
> evala(u);
```

$$-\frac{416}{1923} + \frac{317}{1923}\,\beta + \frac{364}{1923}\,\beta^2 - \frac{37}{1923}\,\beta^3 - \frac{637}{3846}\,\beta^4$$

**Beispiel: Rechnen in Maple mit einer Nullstelle von**

$$x^8 + 3x^7 - 2x^5 - 10x^4 + x^3 - x^2 + 1$$

```
> k:=x^8+3*x^7-2*x^5-10*x^4+x^3-x^2+1;
```

$$k := x^8 + 3\,x^7 - 2\,x^5 - 10\,x^4 + x^3 - x^2 + 1$$

```
> irreduc(k);
```

$$true$$

Das Polynom $k$ ist irreduzibel. Mit *solve(*$k, x$*)* werden alle Nullstellen von $k$ bestimmt.

```
> solve(k,x);
```

$$\begin{aligned}&\mathrm{RootOf}(\%1,\ index = 1),\\ &\mathrm{RootOf}(\%1,\ index = 2),\\ &\mathrm{RootOf}(\%1,\ index = 3),\\ &\mathrm{RootOf}(\%1,\ index = 4),\\ &\mathrm{RootOf}(\%1,\ index = 5),\\ &\mathrm{RootOf}(\%1,\ index = 6),\\ &\mathrm{RootOf}(\%1,\ index = 7),\\ &\mathrm{RootOf}(\%1,\ index = 8)\end{aligned}$$

$$\%1 := \_Z^8 + 3\,\_Z^7 - 2\,\_Z^5 - 10\,\_Z^4 + \_Z^3 - \\ -\_Z^2 + 1$$

Wir wählen für eine der Nullstellen von $k$ die Abkürzung $\gamma$.

```
> alias(gamma=RootOf(k));
```

$$\gamma$$

```
> v:=(gamma^5+6*gamma^4-7*gamma^3+5)^(-1);
```

$$v := \frac{1}{\gamma^5 + 6\,\gamma^4 - 7\,\gamma^3 + 5}$$

Mit *evala(v)* werden die eindeutig bestimmten rationalen Zahlen $c_0, c_1, \ldots, c_7$ mit $v = c_0 + c_1\gamma + c_2\gamma^2 + \ldots + c_7\gamma^7$ berechnet.

```
> evala(v);
```

$$\frac{2996222909}{17089149995} + \frac{221692583}{17089149995}\,\gamma +$$
$$+\frac{793007037}{17089149995}\,\gamma^2 + \frac{3091950683}{17089149995}\,\gamma^3 +$$
$$+\frac{708890931}{17089149995}\,\gamma^4 - \frac{297915816}{17089149995}\,\gamma^5 -$$
$$-\frac{1211687627}{17089149995}\,\gamma^6 - \frac{361873652}{17089149995}\,\gamma^7$$

## Literatur


[GG] von zur Gathen, J., Gerhard, J.: Modern Computer Algebra.
Cambridge University Press, Cambridge, 1999

[L] Lüneburg, H.: Kleine Fibel der Arithmetik.
Bibliographisches Institut, Mannheim, 1988

[P1] Pauer, F.: Division mit Rest - der heimliche Hauptsatz der Algebra.
Didaktikhefte 37, 100-111, Österr. Math. Ges., Wien, 2005

[P2] Pauer, F.: Algebra. Skriptum.
Universität Innsbruck. 3. Auflage, 91 + 3 Seiten, Innsbruck, 2007

[TK] Timischl, W., Kaiser, W.: Ingenieur-Mathematik 2.
E. Dorner Verlag, Wien, 6. Auflage, 2007