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

Franz Pauer
Institut für Mathematik, Universität Innsbruck,
Technikerstr. 13/7, A-6020 Innsbruck, Österreich.
Franz.Pauer@uibk.ac.at

Vortrag beim ÖMG-LehrerInnenfortbildungstag
2008 in Wien

28. März 2008

## Einleitung

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 $x^2 + 1$.

Fragen:

- Gibt es eine solche Zahl?

- Wenn ja, ist sie eindeutig bestimmt?

Zur 1. Frage: In $\mathbb{Q}$ gibt es beide nicht.
Zur 2. Frage:
Wenn $a^2 = 0$ ist, dann ist auch $(-a)^2 = 0$.

## Inhalt

# 1. Zahlenbereichserweiterungen

| **Erweiterung** | **motiviert 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>$(n \in \mathbb{N}_{\geq 2},\ t \in \mathbb{Q})$ | $z^n = t$ |
| $\mathbb{Q} \subseteq \mathbb{R}$ | $z = \lim_{n\to\infty} t_n, \quad t_n \in \mathbb{Q}$ |
| $\mathbb{R} \subseteq \mathbb{C}$ | $z^2 = -1$ |

„Erweitere den Zahlbereich $K$ (mit $+$ und $\cdot$) zum Zahlbereich $L$“ (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

- den „Rechenkomfort“ erhalten, d.h. 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 muss eine Lösung in $L$ haben

- $L$ soll „möglichst klein“ sein

## 2. Erinnerung: Division mit Rest von Polynomen

**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

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

$m$ ... polynomialer Quotient von $f$ und $g$
$r$ ... Rest von $f$ nach Division durch $g$

**Divisionsalgorithmus** (Berechnung von $m$ und $r$):

- 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

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

**Beispiel:**

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

Berechne $m$ und $r$ mit $f = m \cdot g + r$ und
($r = 0$ oder $grad(r) < grad(g)$)!

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

Also:

$$m = x^2 + 2x \qquad r = 5x - 1\,.$$

## 3. Konstruktion der Erweiterungen $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$ und $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{-1}]$

$\mathbb{Q}[x] := \{ \sum_{i=0}^{n} c_i x^i \mid n \in \mathbb{N},\ c_0, \ldots, c_n \in \mathbb{Q} \}$
Polynomring (in $x$) über $\mathbb{Q}$.

$\mathbb{Q} \subseteq L := \{a + bx \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{Q}[x]$ mit der Addition von Polynomen

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

und der (neuen) Multiplikation

$(a+bx) * (c+dx) :=$ Rest von $(a+bx) \cdot (c+dx)$

nach Division durch $x^2 - 2$ bzw. $x^2 + 1$

Das Produkt $(a + bx) \cdot (c + dx)$ liegt nicht in $L$, wohl aber sein Rest nach Division durch $x^2 - 2$ bzw. $x^2 + 1$ !

Noch zu zeigen: Alle Elemente $\neq 0$ in $L$ haben ein inverses Element.
Dann kann leicht nachgeprüft werden: Für $+$ und $*$ auf $L$ sind alle Rechenregeln eines Körpers erfüllt.

Was ist $x * x$?
$x * x$ ist der Rest von $x^2$ nach Division durch $x^2 - 2$ bzw. $x^2 + 1$, wegen $x^2 = 1.(x^2 - 2) + 2$ bzw. $x^2 = 1.(x^2 + 1) - 1$ also $2$ bzw. $-1$.

**Daher ist**

$$x \in L$$

**eine Wurzel aus $2$ bzw. $-1$, wir schreiben für $x$**

$$\sqrt{2} \textbf{ bzw. } i$$

**und für $L$**

$$\mathbb{Q}[\sqrt{2}] \textbf{ bzw. } \mathbb{Q}[i].$$

Alle Elemente von $L$ können eindeutig in der Form $a + b\sqrt{2}$ bzw. $a + bi$ mit $a, b \in \mathbb{Q}$ angeschrieben werden!

Aufgaben wie z.B.

Vereinfache $(2\sqrt{2} + 3)^2 \cdot \sqrt{2}$ !

können präziser formuliert werden, z.B.:
Berechne rationale Zahlen $a$ und $b$ so, dass

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

ist!

## 4. Erinnerung: Der erweiterte Euklidische Algorithmus

**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, dann ist $u := lk(B_1)^{-1} \cdot B_2$ und $v := lk(B_1)^{-1} \cdot B_3$ .

Beispiel:

```
>   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;
```

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

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

Sei $y := 2$ bzw. $-1$. Das Polynom $x^2 - y$ ist in $\mathbb{Q}[x]$ irreduzibel, dh. es kann nicht als Produkt von zwei Polynomen 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? Gibt es zu $f := a + bx = a + b\sqrt{y}$ ein Polynom $g \in \mathbb{Q}[x]$ mit $g * f = 1$?

Berechne mit dem erweiterten Euklidischen Algorithmus Polynome $u, v \in \mathbb{Q}[x]$ mit

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

Einsetzen von $\sqrt{y} \in L$ auf beiden Seiten ergibt

$$0 + v(\sqrt{y}) * f(\sqrt{y}) = 1 \ .$$

Daher ist $f = f(\sqrt{y})$ in $L$ invertierbar und

$$f^{-1} = v(\sqrt{y}) \, .$$

Ist $grad(v) > 1$, ersetzt man $v$ durch seinen Rest nach Division durch $x^2 - y$, aus $v = m \cdot (x^2 - y) + r$ und ($r = 0$ oder $grad(r) < 2$) folgt

$$v(\sqrt{y}) = 0 + r(\sqrt{y}) \, .$$

$L$ ist also ein Körper und hat auch alle anderen gewünschten Eigenschaften.
Ein Element $1/f$ von $L$ „wurzelfrei machen“ bedeutet: Rationale Zahlen $a, b$ mit der Eigenschaft

$$(f^{-1} =) 1/f = a + b\sqrt{y}$$

berechnen.

## 6. Rechnen mit „Wurzel aus 2“ in Maple

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

$$true$$

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

$$\alpha$$

```
> alpha^2;
```

$$\alpha^2$$

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

$$2$$

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

$$(1 - 2\,\alpha + 3\,\alpha^2)\,(2 + \alpha^3) - 10\,\alpha - 3$$

```
> evala(%);
```

$$3$$

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

$$\frac{1}{3\,\alpha+4}$$

```
> evala(%);
```

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

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

$$1$$

```
> v;
```

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

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

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

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

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

```
> factor(x^2-2,alpha);
```

$$(x+\alpha)\,(x-\alpha)$$

## Rechnen mit „Wurzel aus -1“ in Maple

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

$$true$$

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

$$i$$

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

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

```
>  evala(%);
```

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

```
>  factor(x^2+1,i);
```

$$(x+i)\,(x-i)$$

## 7. Algebraische Zahlen

Sei $h$ ein irreduzibles Polynom in $\mathbb{Q}[x]$ mit und sei $L := \{\sum_{i=0}^{n} c_i x^i \,|\, n < grad(h),\, c_0, \ldots, c_n \in \mathbb{Q}\}$ mit der Addition von Polynomen und der Multiplikation

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

$L$ ist ein Körper:
Sei $0 \neq f \in L$, dann ist $ggT(f, h) = 1$.
Berechne Polynome $u, v$ mit $u \cdot h + v \cdot f = 1$ (erw. Euklidischer Algorithmus).
Sei $g \in L$ der Rest von $v$ nach Division durch $h$.
Dann ist $g * f = 1$.

Das Polynom $h$ hat in diesem Körper eine Nullstelle, und zwar $x$.
Alle Elemente von $L$ können in eindeutiger Weise als rationale Linearkombinationen von

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

geschrieben werden.

Beispiel:

Sei $h := x^3 - 2$ 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

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

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

```
> restart;
```

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

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

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

$$true$$

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

$$\beta$$

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

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

```
> evala(%);
```

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

**Rechnen in Maple mit einer Nullstelle von $x^8 + 3\,x^7 - 2\,x^5 - 10\,x^4 + x^3 - x^2 + 1$**

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

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

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

$$true$$

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

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

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

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

$$\delta$$

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

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

```
>  evala(%);
```

$$\frac{2996222909}{17089149995}+\frac{221692583}{17089149995}\,\gamma+$$

$$+\frac{793007037}{17089149995}\,\gamma^2+\frac{3091950683}{17089149995}\,\gamma^3+$$

$$+\frac{708890931}{17089149995}\,\gamma^4-\frac{297915816}{17089149995}\,\gamma^5-$$

$$-\frac{1211687627}{17089149995}\,\gamma^6-\frac{361873652}{17089149995}\,\gamma^7$$