TH BINGEN
University of Applied Sciences

Brüche und rationale Funktionen

Euklidische Ringe, Quotientenkörper

Dieter Kilsch

eh. Technische Hochschule Bingen

24. November 2020

Bruchrechnung in $\mathbb{Q} = Q(\mathbb{Z})$

Operationen

Operationen in $\mathbb{Z}$ und $\mathbb{Q}$

In der Menge der ganzen Zahlen $\mathbb{Z}$ kann man

- addieren,
- subtrahieren,
- multiplizieren
- aber dividieren nur mit Rest: $19 : 7 = 2$ REST $5 = 3$ REST -2.

In der Menge der rationalen Zahlen $\mathbb{Q}$ kann man auch dividieren.

- Bei den Operationen ist Kürzen wichtig.
- Kürzen heißt: Zähler und Nenner durch den größten gemeinsamen Teiler dividieren.
- In der Regel: Nenner positiv.

Bruchrechnung in $\mathbb{Q} = Q(\mathbb{Z})$

Operationen

Operationen in $\mathbb{Z}$ und $\mathbb{Q}$

In der Menge der ganzen Zahlen $\mathbb{Z}$ kann man

- addieren,
- subtrahieren,
- multiplizieren
- aber dividieren nur mit Rest: $19 : 7 = 2$ REST $5 = 3$ REST -2.

In der Menge der rationalen Zahlen $\mathbb{Q}$ kann man auch dividieren.

- Bei den Operationen ist Kürzen wichtig.
- Kürzen heißt: Zähler und Nenner durch den größten gemeinsamen Teiler dividieren.
- In der Regel: Nenner positiv.

Bruchrechnung in $\mathbb{Q} = Q(\mathbb{Z})$

Operationen

Operationen in $\mathbb{Z}$ und $\mathbb{Q}$

In der Menge der ganzen Zahlen $\mathbb{Z}$ kann man

- addieren,
- subtrahieren,
- multiplizieren
- aber dividieren nur mit Rest: $19 : 7 = 2$ REST $5 = 3$ REST -2.

In der Menge der rationalen Zahlen $\mathbb{Q}$ kann man auch dividieren.

- Bei den Operationen ist Kürzen wichtig.
- Kürzen heißt: Zähler und Nenner durch den größten gemeinsamen Teiler dividieren.
- In der Regel: Nenner positiv.

Bruchrechnung in $\mathbb{Q} = Q(\mathbb{Z})$

Operationen

Operationen in $\mathbb{Z}$ und $\mathbb{Q}$

In der Menge der ganzen Zahlen $\mathbb{Z}$ kann man

- addieren,
- subtrahieren,
- multiplizieren
- aber dividieren nur mit Rest: $19 : 7 = 2$ REST $5 = 3$ REST -2.

In der Menge der rationalen Zahlen $\mathbb{Q}$ kann man auch dividieren.

- Bei den Operationen ist Kürzen wichtig.
- Kürzen heißt: Zähler und Nenner durch den größten gemeinsamen Teiler dividieren.
- In der Regel: Nenner positiv.

Bruchrechnung in $\mathbb{Q} = Q(\mathbb{Z})$

Operationen

Operationen in $\mathbb{Z}$ und $\mathbb{Q}$

In der Menge der ganzen Zahlen $\mathbb{Z}$ kann man

- addieren,
- subtrahieren,
- multiplizieren
- aber dividieren nur mit Rest: $19 : 7 = 2$ REST $5 = 3$ REST -2.

In der Menge der rationalen Zahlen $\mathbb{Q}$ kann man auch dividieren.

- Bei den Operationen ist Kürzen wichtig.
- Kürzen heißt: Zähler und Nenner durch den größten gemeinsamen Teiler dividieren.
- In der Regel: Nenner positiv.

Bruchrechnung in $\mathbb{Q} = Q(\mathbb{Z})$

Operationen

Operationen in $\mathbb{Z}$ und $\mathbb{Q}$

In der Menge der ganzen Zahlen $\mathbb{Z}$ kann man

- addieren,
- subtrahieren,
- multiplizieren
- aber dividieren nur mit Rest: $19 : 7 = 2$ REST $5 = 3$ REST -2.

In der Menge der rationalen Zahlen $\mathbb{Q}$ kann man auch dividieren.

- Bei den Operationen ist Kürzen wichtig.
- Kürzen heißt: Zähler und Nenner durch den größten gemeinsamen Teiler dividieren.
- In der Regel: Nenner positiv.

Bruchrechnung in $\mathbb{Q} = Q(\mathbb{Z})$

Operationen

Operationen in $\mathbb{Z}$ und $\mathbb{Q}$

In der Menge der ganzen Zahlen $\mathbb{Z}$ kann man

- addieren,
- subtrahieren,
- multiplizieren
- aber dividieren nur mit Rest: $19 : 7 = 2$ REST $5 = 3$ REST -2.

In der Menge der rationalen Zahlen $\mathbb{Q}$ kann man auch dividieren.

- Bei den Operationen ist Kürzen wichtig.
- Kürzen heißt: Zähler und Nenner durch den größten gemeinsamen Teiler dividieren.
- In der Regel: Nenner positiv.

Bruchrechnung in $\mathbb{Q} = Q(\mathbb{Z})$

Operationen

Operationen in $\mathbb{Z}$ und $\mathbb{Q}$

In der Menge der ganzen Zahlen $\mathbb{Z}$ kann man

- addieren,
- subtrahieren,
- multiplizieren
- aber dividieren nur mit Rest: $19 : 7 = 2$ REST $5 = 3$ REST -2.

In der Menge der rationalen Zahlen $\mathbb{Q}$ kann man auch dividieren.

- Bei den Operationen ist Kürzen wichtig.
- Kürzen heißt: Zähler und Nenner durch den größten gemeinsamen Teiler dividieren.
- In der Regel: Nenner positiv.

Bruchrechnung in $\mathbb{Q} = Q(\mathbb{Z})$

ggT(190,68)=2:

$$
\begin{aligned}
190 &= 2 \cdot 68 + 54 \\
68 &= 1 \cdot 54 + 14 \\
54 &= 3 \cdot 14 + 12 \\
14 &= 1 \cdot 12 + 2 \\
12 &= 6 \cdot 2 + 0
\end{aligned}
$$

Bruchrechnung in $\mathbb{Q} = Q(\mathbb{Z})$

ggT(190,68)=2:

$$\begin{aligned} 190 &= 2 \cdot 68 + 54 \\ 68 &= 1 \cdot 54 + 14 \\ 54 &= 3 \cdot 14 + 12 \\ 14 &= 1 \cdot 12 + 2 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

$$\begin{aligned} 190 &= 3 \cdot 68 + (-14) \\ 68 &= (-5) \cdot (-14) + 2 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

Bruchrechnung in $\mathbb{Q} = Q(\mathbb{Z})$

ggT(190,68)=2:

$$\begin{aligned} 190 &= 2 \cdot 68 + 54 \\ 68 &= 1 \cdot 54 + 14 \\ 54 &= 3 \cdot 14 + 12 \\ 14 &= 1 \cdot 12 + 2 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

$$\begin{aligned} 190 &= 3 \cdot 68 + (-14) \\ 68 &= (-5) \cdot (-14) + 2 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

Daraus folgt, dass der Rest betragsmäßig klein sein muss!

Bruchrechnung in $\mathbb{Q} = Q(\mathbb{Z})$

ggT(190,68)=2:

$$\begin{aligned} 190 &= 2 \cdot 68 + 54 \\ 68 &= 1 \cdot 54 + 14 \\ 54 &= 3 \cdot 14 + 12 \\ 14 &= 1 \cdot 12 + 2 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

$$\begin{aligned} 190 &= 3 \cdot 68 + (-14) \\ 68 &= (-5) \cdot (-14) + 2 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

Daraus folgt, dass der Rest betragsmäßig klein sein muss!

Euklidischer Algorithmus: $p = q \cdot s + r$

- Rest berechnen mit Residue, aber im Bereich $(-q/2,\ q/2)$.
- p/q zur nächsten ganzen Zahl runden und dann Rest berechnen.

Bruchrechnung in $\mathbb{Q} = Q(\mathbb{Z})$

ggT(190,68)=2:

$$\begin{aligned} 190 &= 2 \cdot 68 + 54 \\ 68 &= 1 \cdot 54 + 14 \\ 54 &= 3 \cdot 14 + 12 \\ 14 &= 1 \cdot 12 + 2 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

$$\begin{aligned} 190 &= 3 \cdot 68 + (-14) \\ 68 &= (-5) \cdot (-14) + 2 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

Daraus folgt, dass der Rest betragsmäßig klein sein muss!

Euklidischer Algorithmus: $p = q \cdot s + r$

- Rest berechnen mit Residue, aber im Bereich $(-q/2,\ q/2)$.
- p/q zur nächsten ganzen Zahl runden und dann Rest berechnen.

Bruchrechnung in $\mathbb{Q} = Q(\mathbb{Z})$

Division mit Rest: $p = q \cdot s + r$

```
      (p q)←(2/1 ¯1×44)(1⌽2 2/1 ¯1×6)
      r←(p-q×r),[1.5]r←⌈¯.5+p÷q
      p,'=',r[;1],'×',q,'+',r[;2],'|',':',[1.5]q|p
 44 =  2 ×  6 +  7 |:  2
 44 =  2 × ¯6 + ¯7 |: ¯4
¯44 = ¯2 × ¯6 +  7 |: ¯2
¯44 = ¯2 ×  6 + ¯7 |:  4

      (p q)←(2/1 ¯1×45)(1⌽2 2/1 ¯1×6)
      r←((p-r)÷q),[1.5]r←(-q×(2×|r)>|q)+r←q|p
      p,'=',r[;1],'×',q,'+',r[;2],'|',':',[1.5]q|p
 45 =  7 ×  6 +  3 |:  3
 45 = ¯8 × ¯6 + ¯3 |: ¯3
¯45 =  7 × ¯6 + ¯3 |: ¯3
¯45 = ¯8 ×  6 +  3 |:  3

      (p q)←(6E6⍴44)(6)
      t←⎕ts⋄r←(p-q×r),r←⌈¯.5+p÷q⋄1000⊥¯2↑⎕ts-t
187
      t←⎕ts⋄r←((p-r)÷q),r←(-q×(2×|r)>|q)+r←q|p⋄1000⊥¯2↑⎕ts
129
```

Euklidische Ringe

Verallgemeinerung

Definition (Euklidischer Ring)

Ein kommutativer Ring $(R, +, \cdot)$ mit Eins 1 ist ein Euklidischer Ring genau dann, wenn

1. *R hat keine Nullteiler:* $\forall r, s \in R \backslash \{0\} : \; r \cdot s \neq 0$.
2. *Es gibt eine Funktion $\varphi : R \backslash \{0\} \to \mathbb{N}_0$ mit folgenden Eigenschaften:*
   1. $\forall r, s \in R \backslash \{0\} : \; \varphi(rs) \geq \varphi(r)$ *Diese Funktion heißt Euklidische Funktion, Euklidische Norm oder Euklidischer Wert.*
   2. $\forall p, q \in R \backslash \{0\} \; \exists r, s \in R : \; p = qs + r \; \wedge \; (r = 0 \; \vee \; \varphi(r) < \varphi(q))$ *Dieser Algorithmus heißt Euklidischer Algorithmus.*

Euklidische Ringe

Verallgemeinerung

Definition (Euklidischer Ring)

Ein kommutativer Ring $(R, +, \cdot)$ mit Eins 1 ist ein Euklidischer Ring genau dann, wenn

1. *R hat keine Nullteiler:* $\forall r, s \in R \backslash \{0\} : \; r \cdot s \neq 0$.
2. *Es gibt eine Funktion* $\varphi : R \backslash \{0\} \to \mathbb{N}_0$ *mit folgenden Eigenschaften:*
   1. $\forall r, s \in R \backslash \{0\} : \; \varphi(rs) \geq \varphi(r)$ *Diese Funktion heißt Euklidische Funktion, Euklidische Norm oder Euklidischer Wert.*
   2. $\forall p, q \in R \backslash \{0\} \; \exists r, s \in R : \; p = qs + r \; \wedge \; (r = 0 \; \vee \; \varphi(r) < \varphi(q))$ *Dieser Algorithmus heißt Euklidischer Algorithmus.*

Euklidische Ringe

Verallgemeinerung

Definition (Euklidischer Ring)

Ein kommutativer Ring $(R, +, \cdot)$ mit Eins 1 ist ein Euklidischer Ring genau dann, wenn

1. *R hat keine Nullteiler:* $\forall r, s \in R \backslash \{0\} : \ r \cdot s \neq 0$.
2. *Es gibt eine Funktion* $\varphi : R \backslash \{0\} \to \mathbb{N}_0$ *mit folgenden Eigenschaften:*
   1. $\forall r, s \in R \backslash \{0\} : \ \varphi(rs) \geq \varphi(r)$ *Diese Funktion heißt Euklidische Funktion, Euklidische Norm oder Euklidischer Wert.*
   2. $\forall p, q \in R \backslash \{0\} \, \exists r, s \in R : \ p = qs + r \ \wedge \ (r = 0 \ \vee \ \varphi(r) < \varphi(q))$ *Dieser Algorithmus heißt Euklidischer Algorithmus.*

Euklidische Ringe

Verallgemeinerung

Definition (Euklidischer Ring)

Ein kommutativer Ring $(R, +, \cdot)$ mit Eins 1 ist ein Euklidischer Ring genau dann, wenn

1. *R hat keine Nullteiler:* $\forall r, s \in R \backslash \{0\} : \ r \cdot s \neq 0$.
2. *Es gibt eine Funktion* $\varphi : R \backslash \{0\} \to \mathbb{N}_0$ *mit folgenden Eigenschaften:*
   1. $\forall r, s \in R \backslash \{0\} : \ \varphi(rs) \geq \varphi(r)$ *Diese Funktion heißt Euklidische Funktion, Euklidische Norm oder Euklidischer Wert.*
   2. $\forall p, q \in R \backslash \{0\} \, \exists r, s \in R : \ p = qs + r \ \wedge \ (r = 0 \ \vee \ \varphi(r) < \varphi(q))$ *Dieser Algorithmus heißt Euklidischer Algorithmus.*

Euklidische Ringe

Bemerkung

a *Euklidische Ringe sind Hauptidealringe: Jedes Ideal ist von einem Element erzeugt.*

b *Jeder Hauptidealring hat eine fast-eindeutige Primfaktorzerlegung: Sie ist eindeutig bis auf eine Multiplikation mit einer Einheit.*

Euklidische Ringe

Bemerkung

a *Euklidische Ringe sind Hauptidealringe: Jedes Ideal ist von einem Element erzeugt.*

b *Jeder Hauptidealring hat eine fast-eindeutige Primfaktorzerlegung: Sie ist eindeutig bis auf eine Multiplikation mit einer Einheit.*

Euklidische Ringe

Beispiel

Euklidische Ringe sind:

a. $\mathbb{Z}$ *mit* $\varphi(z) = |z|$,

b. *der Polynomring*
$K[x] = \{a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \mid a_i \in K (i = 0, \ldots, n)\}$
über einem Körper K *mit* $\varphi(p(x)) = \operatorname{grad} p$,

c. *der Ring der Gaußschen ganzen Zahlen* $\mathbb{Z}[i]$ *mit*
$\varphi(a + \mathrm{i}\, b) = a^2 + b^2$, *s. [4].*

Euklidische Ringe

Beispiel

Euklidische Ringe sind:

a. $\mathbb{Z}$ *mit* $\varphi(z) = |z|$,

b. *der Polynomring*
$K[x] = \{a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \mid a_i \in K (i = 0, \ldots, n)\}$
über einem Körper K *mit* $\varphi(p(x)) = \operatorname{grad} p$,

c. *der Ring der Gaußschen ganzen Zahlen* $\mathbb{Z}[i]$ *mit*
$\varphi(a + \mathrm{i}\, b) = a^2 + b^2$, *s. [4].*

Euklidische Ringe

Beispiel

Euklidische Ringe sind:

a. $\mathbb{Z}$ *mit* $\varphi(z) = |z|$,

b. $K[x] = \{a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \mid a_i \in K (i = 0, \ldots, n)\}$ *über einem Körper* K *mit* $\varphi(p(x)) = \operatorname{grad} p$,

c. *der Ring der Gaußschen ganzen Zahlen* $\mathbb{Z}[i]$ *mit* $\varphi(a + \mathrm{i}\, b) = a^2 + b^2$, *s. [4].*

Euklidische Ringe

Beispiel

Euklidische Ringe sind:

a. $\mathbb{Z}$ *mit* $\varphi(z) = |z|$,

b. $K[x] = \{a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \mid a_i \in K (i = 0, \ldots, n)\}$ *über einem Körper* K *mit* $\varphi(p(x)) = \operatorname{grad} p$,

c. $\mathbb{Z}[i]$ *mit* $\varphi(a + \mathrm{i}\, b) = a^2 + b^2$, *s. [4].*

Beispiel

- *[5]: die Ringe der ganzen Zahlen in den Zahlkörpern* $\mathbb{Q}[\sqrt{-d}]$ *sind für* $d = 1, 2, 3, 7, 11$ *euklidisch. Sie enthalten* $\mathbb{Z}[\sqrt{-d}]$.
  Für $d = 19, 43, 67, 163$ *sind diese Ringe Hauptidealringe (und keine Euklidischen Ringe).*

Euklidische Ringe

Beispiel

Euklidische Ringe sind:

a. $\mathbb{Z}$ *mit* $\varphi(z) = |z|$,

b. $K[x] = \{a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \mid a_i \in K (i = 0, \ldots, n)\}$ *über einem Körper* K *mit* $\varphi(p(x)) = \operatorname{grad} p$,

c. $\mathbb{Z}[i]$ *mit* $\varphi(a + \mathrm{i}\, b) = a^2 + b^2$, *s. [4].*

Beispiel

- *[4]:* $\mathbb{Z}[x, y]$ *und* $\mathbb{R}[x, y]$ *sind Ringe mit eindeutiger Primfaktorzerlegung aber keine Hauptidealringe.*

Euklidische Ringe

Beispiel

- *[5]: die Ringe der ganzen Zahlen in den Zahlkörpern* $\mathbb{Q}[\sqrt{-d}]$ *sind für* $d = 1, 2, 3, 7, 11$ *euklidisch. Sie enthalten* $\mathbb{Z}[\sqrt{-d}]$.
  Für $d = 19, 43, 67, 163$ *sind diese Ringe Hauptidealringe (und keine Euklidischen Ringe).*
- *[4]:* $\mathbb{Z}[\sqrt{-3}]$ *ist kein Ring mit eindeutiger Primfaktorzerlegung:* $4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$.
  Er ist damit echt enthalten im Ring der ganzen Zahlen in $\mathbb{Q}[\sqrt{-d}]$.

Euklidische Ringe

Einheiten

Beispiel (Schöne Nenner)

a. $\mathbb{Z}$: *Der Nenner soll positiv sein: Ggf. muss durch -1 gekürzt werden.*

b. $\mathbb{K}[x]$: *Der Nenner soll Hauptkoeffizienten 1 haben: Ggf. muss durch den Hauptkoeffizienten gekürzt werden.*

c. $\mathbb{Z}[i]$: *Realteil und Imaginärteil sollen positiv sein: Ggf. muss durch* i, -1 *oder* $-\mathrm{i}$ *gekürzt werden.*

Euklidische Ringe

Einheiten

Beispiel (Schöne Nenner)

a. $\mathbb{Z}$: *Der Nenner soll positiv sein: Ggf. muss durch -1 gekürzt werden.*

b. $\mathbb{K}[x]$: *Der Nenner soll Hauptkoeffizienten 1 haben: Ggf. muss durch den Hauptkoeffizienten gekürzt werden.*

c. $\mathbb{Z}[i]$: *Realteil und Imaginärteil sollen positiv sein: Ggf. muss durch* $\mathrm{i}, -1$ *oder* $-\mathrm{i}$ *gekürzt werden.*

Euklidische Ringe

Einheiten

Beispiel (Schöne Nenner)

a. $\mathbb{Z}$: *Der Nenner soll positiv sein: Ggf. muss durch -1 gekürzt werden.*

b. $\mathbb{K}[x]$: *Der Nenner soll Hauptkoeffizienten 1 haben: Ggf. muss durch den Hauptkoeffizienten gekürzt werden.*

c. $\mathbb{Z}[i]$: *Realteil und Imaginärteil sollen positiv sein: Ggf. muss durch* i, -1 *oder* $-\mathrm{i}$ *gekürzt werden.*

Euklidische Ringe

Einheiten

Beispiel (Schöne Nenner)

a. $\mathbb{Z}$: *Der Nenner soll positiv sein: Ggf. muss durch -1 gekürzt werden.*

b. $\mathbb{K}[x]$: *Der Nenner soll Hauptkoeffizienten 1 haben: Ggf. muss durch den Hauptkoeffizienten gekürzt werden.*

c. $\mathbb{Z}[i]$: *Realteil und Imaginärteil sollen positiv sein: Ggf. muss durch* i, -1 *oder* $-\mathrm{i}$ *gekürzt werden.*

Definition (Einheiten eines Ringes)

Für einen Ring R *ist* $R^\times$ *die Menge aller Einheiten, d.h. dei Menge aller Zahlen durch die man alle Ringelemente dividieren kann.*

Euklidische Ringe

Einheiten

Definition (Einheiten eines Ringes)

Für einen Ring R ist $R^\times$ die Menge aller Einheiten, d.h. dei Menge aller Zahlen durch die man alle Ringelemente dividieren kann.

Beispiel

a. $\mathbb{Z}^\times : \{\pm 1\}$
b. $K[x]^\times : K \backslash \{0\}$
c. $\mathbb{Z}[i]^\times : \{\pm 1, \pm \mathrm{i}\}$

Euklidische Ringe

Einheiten

Definition (Einheiten eines Ringes)

Für einen Ring R ist $R^\times$ die Menge aller Einheiten, d.h. dei Menge aller Zahlen durch die man alle Ringelemente dividieren kann.

Beispiel

a. $\mathbb{Z}^\times : \{\pm 1\}$
b. $K[x]^\times : K \backslash \{0\}$
c. $\mathbb{Z}[i]^\times : \{\pm 1, \pm \mathrm{i}\}$

Euklidische Ringe

Einheiten

Definition (Einheiten eines Ringes)

Für einen Ring R ist $R^\times$ die Menge aller Einheiten, d.h. dei Menge aller Zahlen durch die man alle Ringelemente dividieren kann.

Beispiel

a. $\mathbb{Z}^\times : \{\pm 1\}$
b. $K[x]^\times : K \backslash \{0\}$
c. $\mathbb{Z}[i]^\times : \{\pm 1, \pm \mathrm{i}\}$

Euklidische Ringe

Charakter

Definition (Einheiten eines Ringes)

Für einen Ring R ist $R^\times$ die Menge aller Einheiten, d.h. dei Menge aller Zahlen durch die man alle Ringelemente dividieren kann.

Beispiel

a. $\mathbb{Z}^\times$: $\{\pm 1\}$
b. $K[x]^\times$: $K \backslash \{0\}$
c. $\mathbb{Z}[i]^\times$: $\{\pm 1, \pm \mathrm{i}\}$

Definition (Charakter)

Für einen Ring R heißt eine Funktion $\psi : R \mapsto R^\times$ ein Charakter, wenn er linear bez. der Einheiten ist: $\psi(e \cdot r) = e \cdot \psi(r)$.

Euklidische Ringe

ggT und kgV — gcd and lcm

Bemerkung (Kürzen)

Kürzen heißt, Zähler und Nenner durch den größten gemeinsamen Teiler dividieren.

Verfahren (Euklidischer Algorithmus: Division mit Rest)

R sei ein euklidischer Ring mit euklidischer Funktion φ, $a, b \in R$.
Berechnung von $\mathrm{ggT}(a,b)$ *mit* $\varphi(a) \geq \varphi(b)$*:*

$$\Rightarrow \quad \exists r, s \in R : \; a = bs + r \; \wedge \; (r = 0 \; \vee \; \varphi(r) < \varphi(b))$$

1. Fall $r = 0 \quad \Rightarrow \quad \mathrm{ggT}(a,b) = b$
2. Fall $\varphi(r) < \varphi(b) : \mathrm{ggT}(a,b) = \mathrm{ggT}(b,r)$, *rekursiv weiter rechnen.*

Euklidische Ringe

ggT und kgV — gcd and lcm

Bemerkung (Kürzen)

Kürzen heißt, Zähler und Nenner durch den größten gemeinsamen Teiler dividieren.

Verfahren (Euklidischer Algorithmus: Division mit Rest)

R sei ein euklidischer Ring mit euklidischer Funktion φ, $a, b \in R$.
Berechnung von $\mathrm{ggT}(a,b)$ *mit* $\varphi(a) \geq \varphi(b)$*:*

$$\Rightarrow \quad \exists r, s \in R : \; a = bs + r \; \wedge \; (r = 0 \; \vee \; \varphi(r) < \varphi(b))$$

1. Fall $r = 0 \quad \Rightarrow \quad \mathrm{ggT}(a,b) = b$
2. Fall $\varphi(r) < \varphi(b) : \mathrm{ggT}(a,b) = \mathrm{ggT}(b,r)$, *rekursiv weiter rechnen.*

Quotientenkörper

Definition

Der Quotientenkörper eines nullteilerfreien Rings ist die Menge aller Paare $\{a/b \mid a \in R \wedge b \in R \backslash \{0\}\}$.
Die arithmetischen Operationen sind die bekannten Regeln für Bruchrechnung.

Quotientenkörper

Definition

Der Quotientenkörper eines nullteilerfreien Rings ist die Menge aller Paare $\{a/b \mid a \in R \wedge b \in R \backslash \{0\}\}$.
Die arithmetischen Operationen sind die bekannten Regeln für Bruchrechnung.

Satz

Kürzen heißt, Zähler und Nenner eines Bruchs durch einen gemeinsamen Teiler dividieren.

Quotientenkörper

Satz

Kürzen heißt, Zähler und Nenner eines Bruchs durch einen gemeinsamen Teiler dividieren.
Kürzen eines Bruchs durch den Charakter des Nenners liefert einen Bruch, dessen Nenner den Charakter 1 hat, also „schön“ ist.

Mit $e = \psi(q)$ folgt

$$\frac{p}{q} = \frac{\frac{p}{e}}{\frac{q}{e}}$$

und $\psi\left(\frac{q}{e}\right) = \psi(q)\frac{1}{e} = 1.$ □

Ring - Euklidischer Ring - Quotientenkörper der Brüche

Das Ring-Modell

1. Initialisierung: Tiefe eines Elements, Eins, Null

```
r←RΔinit
⍝ V1.1  08.01.1993  D.Kilsch      KhAlZ
⍝ Initialisations for the ring of integers.
rΔt←0               ⍝ depth of a ring element
rΔnull←0            ⍝ zero in Z
rΔeins←1            ⍝ unity in Z
⍝⎕←'Ring initialisiert'
```

2. liefert Addition und Multiplikation `RΔa`, `RΔm`,
3. liefert euklidische Funktion, euklidischen Algorithmus und Charakter `RΔe`, `RΔef`, `RΔc`

Ring - Euklidischer Ring - Quotientenkörper der Brüche

Das Ring-Modell

1. Initialisierung: Tiefe eines Elements, Eins, Null

```
r←RΔinit
⍝ V1.1  08.01.1993  D.Kilsch      KhAlZ
⍝ Initialisations for the ring of integers.
rΔt←0               ⍝ depth of a ring element
rΔnull←0            ⍝ zero in Z
rΔeins←1            ⍝ unity in Z
⍝⎕←'Ring initialisiert'
```

2. liefert Addition und Multiplikation `RΔa`, `RΔm`,
3. liefert euklidische Funktion, euklidischen Algorithmus und Charakter `RΔe`, `RΔef`, `RΔc`

Ring - Euklidischer Ring - Quotientenkörper der Brüche

Das Ring-Modell

1. Initialisierung: Tiefe eines Elements, Eins, Null

```
r←RΔinit
⍝ V1.1  08.01.1993  D.Kilsch      KhAlZ
⍝ Initialisations for the ring of integers.
rΔt←0               ⍝ depth of a ring element
rΔnull←0            ⍝ zero in Z
rΔeins←1            ⍝ unity in Z
⍝═══════════════════════════════════════════════
```

2. liefert Addition und Multiplikation `RΔa`, `RΔm`,
3. liefert euklidische Funktion, euklidischen Algorithmus und Charakter `RΔe`, `RΔef`, `RΔc`

Ring - Euklidischer Ring - Quotientenkörper der Brüche

Die Routinen zum Euklidischen Ring:

1. Initialisierung:

```
r←Δinit
⍝ V1.1  08.01.1993  D.Kilsch     KhAlEukl
⍝ Initialisation of an Euclidean ring
⍝=
⍝ called routines:
RΔinit              ⍝ initialisation of the ring
⍝
⍝ global variables:
Δt←rΔt              ⍝ depth of an element
Δnull←rΔnull        ⍝ zero
Δeins←rΔeins        ⍝ unity
⍝═══════════════════════════════════════════════════════════
```

2. Addition und Multiplikation vom Ring RΔa, RΔm,
3. Subtraktion: Addition des negativen Elements RΔs,
4. ggT, kgV

Ring - Euklidischer Ring - Quotientenkörper der Brüche

Die Routinen zum Euklidischen Ring:

1. Initialisierung:

```
r←Δinit
⍝ V1.1  08.01.1993  D.Kilsch     KhAlEukl
⍝ Initialisation of an Euclidean ring
⍝=
⍝ called routines:
RΔinit              ⍝ initialisation of the ring
⍝
⍝ global variables:
Δt←rΔt              ⍝ depth of an element
Δnull←rΔnull        ⍝ zero
Δeins←rΔeins        ⍝ unity
⍝
```

2. Addition und Multiplikation vom Ring RΔa, RΔm,
3. Subtraktion: Addition des negativen Elements RΔs,
4. ggT, kgV

Ring - Euklidischer Ring - Quotientenkörper der Brüche

Die Routinen zum Euklidischen Ring:

1. Initialisierung:

```
r←∆init
⍝ V1.1  08.01.1993  D.Kilsch      KhAlEukl
⍝ Initialisation of an Euclidean ring
⍝=
⍝ called routines:
R∆init                ⍝ initialisation of the ring
⍝
⍝ global variables:
∆t←r∆t                ⍝ depth of an element
∆null←r∆null          ⍝ zero
∆eins←r∆eins          ⍝ unity
⍝───────────────────────────────────────────────────
```

2. Addition und Multiplikation vom Ring `R∆a`, `R∆m`,
3. Subtraktion: Addition des negativen Elements `R∆s`,
4. ggT, kgV

Ring - Euklidischer Ring - Quotientenkörper der Brüche

Die Routinen zum Euklidischen Ring:

1. Initialisierung:

```
r←Δinit
⍝ V1.1  08.01.1993  D.Kilsch     KhAlEukl
⍝ Initialisation of an Euclidean ring
⍝=
⍝ called routines:
RΔinit               ⍝ initialisation of the ring
⍝
⍝ global variables:
Δt←rΔt               ⍝ depth of an element
Δnull←rΔnull         ⍝ zero
Δeins←rΔeins         ⍝ unity
⍝━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
```

2. Addition und Multiplikation vom Ring `RΔa`, `RΔm`,
3. Subtraktion: Addition des negativen Elements `RΔs`,
4. ggT, kgV

Ring - Euklidischer Ring - Quotientenkörper der Brüche

Die Routinen zum Quotientenkörper:

1. Initialisierung:

```
r←Δinit
⍝ V1.1  08.01.1993  D.Kilsch     KhAlQuot
⍝ Initialisation of a quotient field
⍝=
⍝  called routins:
RΔinit
⍝=
⍝  global variables
Δt←rΔt+1                    ⍝ depth of a field element
Δnull←rΔnull rΔeins         ⍝ zero of the field
Δeins←rΔeins rΔeins         ⍝ unity of the field
⍝═══════════════════════════════════════════════════
```

2. Einbettung des Rings: `Δq`
3. Kürzen `Kurzen`,
4. Addition, Subtraktion, Multiplikation, Division: Nach Regeln der Bruchrechnung, am Ende Kürzen

Ring - Euklidischer Ring - Quotientenkörper der Brüche

Die Routinen zum Quotientenkörper:

1. Initialisierung:
2. Einbettung des Rings: `Δq`
3. Kürzen `Kurzen`,
4. Addition, Subtraktion, Multiplikation, Division:
   Nach Regeln der Bruchrechnung, am Ende Kürzen

Ring - Euklidischer Ring - Quotientenkörper der Brüche

Die Routinen zum Quotientenkörper:

1. Initialisierung:
2. Einbettung des Rings: `Δq`
3. Kürzen `Kurzen`,
4. Addition, Subtraktion, Multiplikation, Division:
   Nach Regeln der Bruchrechnung, am Ende Kürzen

Ring - Euklidischer Ring - Quotientenkörper der Brüche

Die Routinen zum Quotientenkörper:

1. Initialisierung:
2. Einbettung des Rings: `∆q`
3. Kürzen `Kurzen`,
4. Addition, Subtraktion, Multiplikation, Division:
   Nach Regeln der Bruchrechnung, am Ende Kürzen

```
r←a ∆a b
⍝ V1.1  08.01.1993  D.Kilsch     KhAlQuot
⍝ Addition of fractions
⍝ a,b  S,V  fractions
⍝─────────────────────────────────────────────────
→(∧/∆t=≡¨a b)/1+⎕LC⋄r←a ∆a¨b⋄→0
→((1≠(⍴⍴a),⍴⍴b)∨2≠(⍴a),⍴b)/F1
r←Kurzen(R∆a/a R∆m¨⌽b),⊂(2⊃a)R∆m 2⊃b
→0
⍝─────────────────────────────────────────────
F1:('∆a: Structure of left or right argument wrong:: '
```

Ganze Zahlen $\mathbb{Z}$ — Brüche $\mathbb{Q} = Q(\mathbb{Z})$ Euklidischer Ring

Definition

1. *Euklidische Funktion: Betrag*
2. *Euklidischer Algorithmus: Division mit Rest, Betrag kleiner als halber Devisorbetrag*

Ganze Zahlen $\mathbb{Z}$ — Brüche $\mathbb{Q} = Q(\mathbb{Z})$ Euklidischer Ring

Definition

1. *Euklidische Funktion: Betrag*
2. *Euklidischer Algorithmus: Division mit Rest, Betrag kleiner als halber Devisorbetrag*

Ganze Zahlen $\mathbb{Z}$ — Brüche $\mathbb{Q} = Q(\mathbb{Z})$

Beispiele

```
      Δinit      ⍝ KHAlZ -Eukl -Quot
      1 4 Δa 1 12
1 3
      Δdar 1 4 Δa 1 12
 1/3
      Δdar (1 2)(3 4)Δa.Δm(1 5)(2 7)
  11/35
```

Ganze Zahlen $\mathbb{Z}$ — Brüche $\mathbb{Q} = Q(\mathbb{Z})$

Beispiele

Hilbertmatrix

```
      ⎕init    ⍝ KHAlZ -Eukl -Quot Khmatrix
      11 ¯4↑mat←÷¯1+(⍳6)∘.+⍳6
 1.000E0    5.000E¯1   3.333E¯1   2.500E¯1   2.000E¯1   1.667E¯1
 5.000E¯1   3.333E¯1   2.500E¯1   2.000E¯1   1.667E¯1   1.429E¯1
 3.333E¯1   2.500E¯1   2.000E¯1   1.667E¯1   1.429E¯1   1.250E¯1
 2.500E¯1   2.000E¯1   1.667E¯1   1.429E¯1   1.250E¯1   1.111E¯1
 2.000E¯1   1.667E¯1   1.429E¯1   1.250E¯1   1.111E¯1   1.000E¯1
 1.667E¯1   1.429E¯1   1.250E¯1   1.111E¯1   1.000E¯1   9.091E¯2
      Det mat
5.367299886E¯18
      11 ¯4↑mat+.×⌹mat
 1.000E0    0.000E0    0.000E0    2.910E¯11  0.000E0    0.000E0
 1.137E¯13  1.000E0    0.000E0    1.455E¯10  5.821E¯11  0.000E0
¯5.684E¯14  0.000E0    1.000E0    8.731E¯11 ¯2.910E¯11  0.000E0
¯1.137E¯13 ¯1.819E¯12  7.276E¯12  1.000E0    2.910E¯11  1.455E¯11
 1.137E¯13 ¯1.819E¯12  2.910E¯11  0.000E0    1.000E0   ¯1.455E¯11
 0.000E0    0.000E0    7.276E¯12  2.910E¯11  0.000E0    1.000E0
```

Ganze Zahlen $\mathbb{Z}$ — Brüche $\mathbb{Q} = Q(\mathbb{Z})$

Beispiele

Hilbertmatrix

```
      ∆init    ⍝ KHAlZ -Eukl -Quot -Matr
      ∆dar mat←1,¨¯1+(⍳6)∘.+⍳6    ⍝ with fractions
    1  1/2  1/3  1/4   1/5   1/6
  1/2  1/3  1/4  1/5   1/6   1/7
  1/3  1/4  1/5  1/6   1/7   1/8
  1/4  1/5  1/6  1/7   1/8   1/9
  1/5  1/6  1/7  1/8   1/9  1/10
  1/6  1/7  1/8  1/9  1/10  1/11
      Aldet mat                  ⍝ determinant: Laplace
1 1.863134203E17
      ∆dar inv←0 6↓2⊃2 Algaut mat,∆q 6 6⍴7↑1   ⍝ Gauss
    36     ¯630     3360     ¯7560     7560     ¯2772
  ¯630    14700    ¯88200    211680  ¯220500     83160
  3360   ¯88200    564480  ¯1411200  1512000   ¯582120
 ¯7560   211680  ¯1411200   3628800 ¯3969000   1552320
  7560  ¯220500   1512000  ¯3969000  4410000  ¯1746360
 ¯2772    83160   ¯582120   1552320 ¯1746360    698544
      ∆dar mat ∆a.∆m inv         ⍝ product with inverse
  1  0  0  0  0  0
  0  1  0  0  0  0
  0  0  1  0  0  0
  0  0  0  1  0  0
  0  0  0  0  1  0
  0  0  0  0  0  1
```

Ganze Zahlen $\mathbb{Z}$ — Brüche $\mathbb{Q} = Q(\mathbb{Z})$

Beispiele

```
      mat←3 3⍴1 ¯2 5 ¯5 ¯8 9 9 3 16
      ⎕dar mat←(⎕q⍤2 mat)⎕d 3 3⍴⎕q⍤2⍳9
   1    ¯1   5/3
¯5/4   ¯8/5   3/2
 9/7    3/8  16/9
      ⎕dar ⎕ldet mat                    ⍝ Det. with Laplace
¯2357/480
      ⎕dar ⎕m/1 1⌽2⊃0 ⎕lgaut mat        ⍝ Det. with Gauss
¯2357/480
      ⎕dar ¯1 ¯1↑2⊃0 0 1 ⎕lgaut mat     ⍝ .. special
¯2357/480
      1 ⎕lzeim mat, ⎕q 1 2 3            ⍝ linear equations
┌     1   ¯1  5/3 │ 1 ┐
│ ¯5/4  ¯8/5  3/2 │ 2 │
└  9/7   3/8 16/9 │ 3 ┘
      1 ⎕lzeim 2⊃2 ⎕lgaut mat,⎕q 1 2 3   ⍝... solution
┌ 1 0 0 │  ¯7054/7071 ┐
│ 0 1 0 │ 73880/49497 │
└ 0 0 1 │ 34551/16499 ┘
```

$\mathbb{R}[x]$ und $\mathbb{R}(x) = Q(\mathbb{R}[x])$: Ringverknüpfungen

Datenmodell

a $p(x) = a_o + a_1 x \ldots a_n x^n$ wird als Vektor $(a_0, a_1, \ldots, a_n)$ dargestellt.

b Addition, Subtraktion komponentenweise

c Multiplikation: $\sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{m} b_j x^j = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i$

$\mathbb{R}[x]$ und $\mathbb{R}(x) = Q(\mathbb{R}[x])$: Ringverknüpfungen

Datenmodell

a $p(x) = a_o + a_1 x \ldots a_n x^n$ wird als Vektor $(a_0, a_1, \ldots, a_n)$ dargestellt.

b Addition, Subtraktion komponentenweise

c Multiplikation: $\sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{m} b_j x^j = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i$

$\mathbb{R}[x]$ und $\mathbb{R}(x) = Q(\mathbb{R}[x])$: Ringverknüpfungen

Datenmodell

a $p(x) = a_o + a_1 x \ldots a_n x^n$ wird als Vektor $(a_0, a_1, \ldots, a_n)$ dargestellt.

b Addition, Subtraktion komponentenweise

c Multiplikation: $\sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{m} b_j x^j = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i$

$\mathbb{R}[x]$ und $\mathbb{R}(x) = Q(\mathbb{R}[x])$: Ringverknüpfungen

Datenmodell

a $p(x) = a_o + a_1 x \ldots a_n x^n$ wird als Vektor $(a_0, a_1, \ldots, a_n)$ dargestellt.

b Addition, Subtraktion komponentenweise

c Multiplikation: $\sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{m} b_j x^j = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i$

$$\begin{pmatrix} a_0 & a_1 & \ldots & a_n & 0 & 0 & \ldots & 0 \\ 0 & a_0 & \ldots & a_{n-1} & a_n & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & \ldots & a_0 & a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

$$(b_0, b_1, \ldots, b_m) \quad (a_0 b_0, a_0 b_1 + a_1 b_0, \quad \ldots \quad \ldots, \quad a_n b_m)$$

$\mathbb{R}[x]$ und $\mathbb{R}(x) = Q(\mathbb{R}[x])$: Ringverknüpfungen

Datenmodell

a $p(x) = a_o + a_1 x \ldots a_n x^n$ wird als Vektor $(a_0,\ a_1,\ \ldots,\ a_n)$ dargestellt.

b Addition, Subtraktion komponentenweise

c Multiplikation: $\sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{m} b_j x^j = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i$

$$\begin{pmatrix} a_0 & a_1 & \ldots & a_n & 0 & 0 & \ldots & 0 \\ 0 & a_0 & \ldots & a_{n-1} & a_n & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & \ldots & a_0 & a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

$(b_0,\ b_1,\ \ldots,\ b_m)$ $\quad (a_0 b_0,\ a_0 b_1 + a_1 b_0,\quad \ldots \quad \ldots,\quad a_n b_m)$

```
r←b+.×((⍴,b),r-1)⍴(r←⍴a,b)↑a
```

$\mathbb{R}[x]$ und $\mathbb{R}(x) = Q(\mathbb{R}[x])$:

Initialisierung

```
r←RΔinit
⍝ V1.1  25.11.2020  D.Kilsch      KhAlPoly
⍝ Initialisation for the ring of polynomials.
⍝=
rΔt←1           ⍝ depth of a ring element
rΔnull←,0       ⍝ zeor of the ring
rΔeins←,1       ⍝ unity of the ring
Δvx←0 1         ⍝ variable
Δvar←'x'        ⍝ name of variable
⍝═══════════════════════════════════════════════════════════════════════
```

$\mathbb{R}[x]$ und $\mathbb{R}(x) = Q(\mathbb{R}[x])$: Polynome als Euklidischer Ring

Definition

1. *Euklidische Funktion:* $\varphi(p(x)) = \operatorname{grad} p(x)$ *für* $p \in \mathbb{R}[x]$.
2. *Euklidischer Algorithmus: Polynomdivision mit Rest. Der Rest hat kleineren Grad als der Divisor.*
3. *Charakter: Hauptkoeffizient*

$\mathbb{R}[x]$ und $\mathbb{R}(x) = Q(\mathbb{R}[x])$:

Beispiele

```
      ∆init   ⍝ KhAlPoly, -Eukl, -Quot
⍝     (x^2-2x+1)÷(2x-2):
      1 ∆dar (1 ¯2 1)1 ∆d (¯2 2)1
 -.5+.5x
⍝     (x^5-1)÷(x-1):
      ∆dar (¯1 0 0 0 1)1 ∆d (¯1 1)1
 1+x+x^2+x^3
⍝     (1+x+x^2+x^3+x^4+x^5)÷(1+x):
      ∆dar (∆q 1 1 1 1 1 1) ∆d (∆q 1 1)
 1+x^2+x^4
      1 ∆dar (1 ¯2 1)(1 1)∆d (¯2 2 5)1
 .2-.4x+.2x^2/-.4+.0x+1.4x^2+x^3
```

$\mathbb{R}[x]$ und $\mathbb{R}(x) = Q(\mathbb{R}[x])$:

Beispiele

```
      Δinit   ⍝ KhAlPoly, -Eukl, -Matr
      mat←4 4⍴1 ¯2 5 ¯5 ¯8 9 9 3 16,⍳11
      RΔdar Alchpo,⍤mat      ⍝ determinant in ring
-4604+1699x-5x^2-19x^3+x^4
      Δinit   ⍝ KhAlPoly, -Eukl, -Quot, -Matr
      (1 1⍉mat)←(1 1⍉mat),⍤¯1
      Δdar Δq ,⍤mat          ⍝ determinant quotient field
 1-x   ¯2    5   ¯5
  ¯8  9-x    9    3
  16    1  2-x    3
   4    5    6  7-x
      Δdar Aldet mat                ⍝ Laplace
-4604+1699x-5x^2-19x^3+x^4
      Δdar Δm/1 1⍉2⍥0 Algaut mat    ⍝ Gauss
-4604+1699x-5x^2-19x^3+x^4
      Δdar 2⍥0 0 1 Algaut mat       ⍝ Gauss special
 1  2/-1+x          ¯5/-1+x                              5/-1+x
 0       1  49-9x/-7-10x+x^2                 -37-3x/-7-10x+x^2
 0       0                1  -640+107x-3x^2/1071-76x-12x^2+x^3
 0       0                0          -4604+1699x-5x^2-19x^3+x^4
      Δdar ¯1 ¯1↑2⍥0 0 1 Algaut mat ⍝   = " =
-4604+1699x-5x^2-19x^3+x^4
```

$\mathbb{C}[x]$ und $\mathbb{C}(x) = Q(\mathbb{C}[x])$:

Beispiele

hinzugefügt/added 25.11.2020

```
      Δinit   ⍝ KhAlPoly, -Eukl, -Quot, -Matr
      Δvar←'z'
      mat←2 2⍴1 0J1 0J¯1
      (1 1⌷mat)←(1 1⌷mat),⍤¯1
      Δdar mat←Δq mat
 1-z  0J1
0J¯1  1-z
      Δdar Aldet mat                    ⍝ Laplace
-2z+z*2
      Δdar Δm/1 1⌷2⊃0 Algaut mat        ⍝ Gauss
-2z+z*2
      Δdar 2⊃0 0 1 Algaut mat           ⍝ special Gauss
 1   0J¯1/-1+z
 0     -2z+z*2
      Δdar ¯1 ¯1↑2⊃0 0 1 Algaut mat ⍝   = " =
-2z+z*2
```

$\mathbb{C}[x]$ und $\mathbb{C}(x) = Q(\mathbb{C}[x])$:

$\mathbb{Q}[x]$ und $\mathbb{Q}(x) = Q(\mathbb{Q}[x]) = Q(\mathbb{Z}[x])$: Gebrochen ration. Funkt.

1. Koeffizienten des Rests bei Division ganzer Polynome nicht ganz.
2. Datenmodell ?

$\mathbb{C}[x]$ und $\mathbb{C}(x) = Q(\mathbb{C}[x])$:

$\mathbb{Q}[x]$ und $\mathbb{Q}(x) = Q(\mathbb{Q}[x]) = Q(\mathbb{Z}[x])$: Gebrochen ration. Funkt.

1. Koeffizienten des Rests bei Division ganzer Polynome nicht ganz.
2. Datenmodell ?

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$: Ringverknüpfungen

Datenmodell für $\mathbb{Z}[i]$

a. Teilmenge der komplexen Zahlen

b. Addition, Multiplikation, Subtraktion von $\mathbb{C}$

c. Initialisierung (Tiefe, Eins, Null) wie für $\mathbb{Z}$

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$: Ringverknüpfungen

Datenmodell für $\mathbb{Z}[i]$

a. Teilmenge der komplexen Zahlen
b. Addition, Multiplikation, Subtraktion von $\mathbb{C}$
c. Initialisierung (Tiefe, Eins, Null) wie für $\mathbb{Z}$

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$: Ringverknüpfungen

Datenmodell für $\mathbb{Z}[i]$

a. Teilmenge der komplexen Zahlen
b. Addition, Multiplikation, Subtraktion von $\mathbb{C}$
c. Initialisierung (Tiefe, Eins, Null) wie für $\mathbb{Z}$

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$: Euklidischer Ring

Definition

a *Euklidische Funktion:* $\varphi(a + \mathrm{i}\, b) = a^2 + b^2$. *Diese ist das Quadrat des (euklidischen) Abstands in* $\mathbb{R}^2$.

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$: Euklidischer Ring

Definition

a *Euklidische Funktion:* $\varphi(a + \mathrm{i}\, b) = a^2 + b^2$. `r×+r`

```
      r←1000 1000 ⍴(4J17)*⍳9
      t←⍞⋄ts⋄s←10○r*2⋄1000⊥⍣¯2↑⍞⋄ts-t
265
      t←⍞⋄ts⋄s←(10○r)*2⋄1000⊥⍣¯2↑⍞⋄ts-t
94
      t←⍞⋄ts⋄s←(|r)*2⋄1000⊥⍣¯2↑⍞⋄ts-t
47
      t←⍞⋄ts⋄s←r×+r⋄1000⊥⍣¯2↑⍞⋄ts-t
15
```

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$: Euklidischer Ring

Definition

a *Euklidische Funktion:* $\varphi(a + \mathrm{i}\,b) = a^2 + b^2$. `r×+r`

b *Euklidischer Algorithmus mit*

1. `s←⌊p÷q` *und* `r←p−q×s` *und damit* $p = q \cdot s + r$.
   Berechnung mit Modulo-Funktion (Residue):
   LRM: `q|p is p−q×⌊p÷q+q=0`
2. `⌊` *macht die Zuordnungen gemäß der Zeichnung:*

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$: Euklidischer Ring

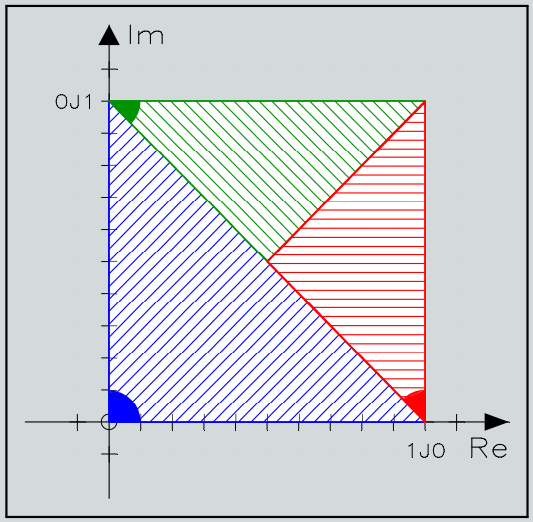
Definition

a *Euklidische Funktion:* $\varphi(a + \mathrm{i}\,b) = a^2 + b^2$. `r×+r`

b *Euklidischer Algorithmus mit* `⌊` *und* `|:` `r←q|p ⋄s←(p−r)÷q`

1. `s←⌊p÷q` *und* `r←p−q×s` *und damit* $p = q \cdot s + r$.
2. `⌊` *macht die Zuordnungen gemäß der Zeichnung:*

$$\begin{array}{rcl} \text{Aus } \left|\frac{p}{q} - \lfloor\frac{p}{q}\right| < 1 & & \text{folgt} \\ \varphi(r) & = & |p - q \cdot s|^2 \\ & = & |q|^2 \left|\frac{p}{q} - s\right|^2 \\ & < & |q|^2 = \varphi(q). \end{array}$$



Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$: Euklidischer Ring

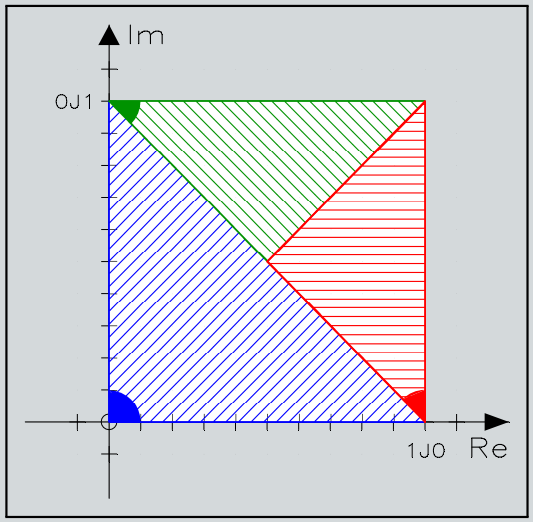
Definition

a *Euklidische Funktion:* $\varphi(a + \mathrm{i}\,b) = a^2 + b^2$. `r×+r`

b *Euklidischer Algorithmus mit* `⌊` *und* `|:` `r←q|p ⋄s←(p−r)÷q`

1. `s←⌊p÷q` *und* `r←p−q×s` *und damit* $p = q \cdot s + r$.
2. `⌊` *macht die Zuordnungen gemäß der Zeichnung:*

$$\begin{array}{rcl} \text{Aus } \left|\frac{p}{q} - \lfloor \frac{p}{q} \right| < 1 & & \text{folgt} \\ \varphi(r) & = & |p - q \cdot s|^2 \\ & = & |q|^2 \left|\frac{p}{q} - s\right|^2 \\ & < & |q|^2 = \varphi(q). \end{array}$$



Abstand zum Gitterpunkt zu groß für gute Iteration!

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$: Euklidischer Ring

Definition

a *Euklidische Funktion:* $\varphi(a + \mathrm{i}\,b) = a^2 + b^2$. `r×+r`

b *Euklidischer Algorithmus mit* `⌊` *und* `|:` `r←q|p ⋄s←(p−r)÷q`

1. `s←⌊p÷q` *und* `r←p−q×s` *und damit* $p = q \cdot s + r$.
2. `⌊` *macht die Zuordnungen gemäß der Zeichnung:*

```
      a b
68272J75646 16974J8402
      1|,9 11∘.Oa b
0 0 0 0
      1|,9 11∘.Or←((a−r)÷b),r←b|a
0 0.9999999991 0 0
      1|,9 11∘.OR←1 0J1+.×⌊.5+9 11∘.Or
0 0 0 0
```

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$: Euklidischer Ring

Definition

a *Euklidische Funktion:* $\varphi(a + \mathrm{i}\,b) = a^2 + b^2$. `r×+r`

b *Euklidischer Algorithmus mit* `⌊` *und* `|`: `r←q|p ⋄s←(p−r)÷q`

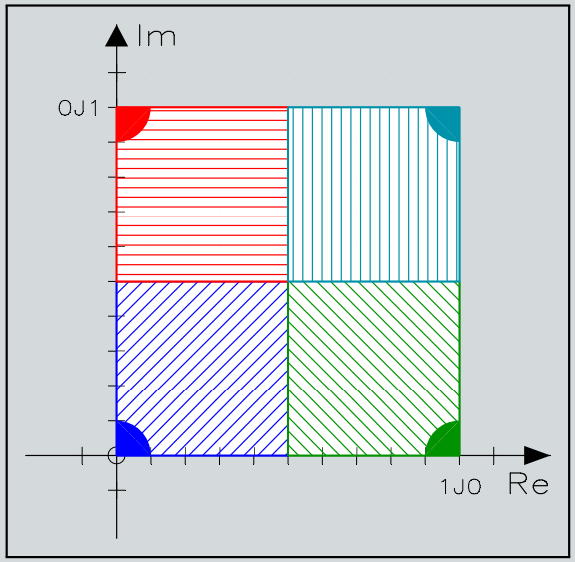
c *Euklidischer Algorithmus mit Runden zum nächsten Gitterpunkt*

$\frac{p}{q} = u + \mathrm{i}\,v \in \mathbb{Q}[i]$ *hat 4 benachbarte Gitterpunkte* $\lfloor u \rfloor + \mathrm{i}\lfloor v \rfloor$, $\lfloor u \rfloor + \mathrm{i}\lceil v \rceil$, $\lceil u \rceil + \mathrm{i}\lfloor v \rfloor$, $\lceil u \rceil + \mathrm{i}\lceil v \rceil$.

Der nächstgelegene Gitterpunkt:
$s = x + \mathrm{i}\,y$, $r := p - q \cdot s$.

$|x - u| \leq \frac{1}{2}$, $|y - v| \leq \frac{1}{2}$

$\Rightarrow \quad \varphi(r) < \varphi(q)$ *([4])*



Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$: Euklidischer Ring

Definition

a *Euklidische Funktion:* $\varphi(a + \mathrm{i}\,b) = a^2 + b^2$. `r×+r`

b *Euklidischer Algorithmus mit* `⌊` *und* `|`: `r←q|p ⋄s←(p−r)÷q`

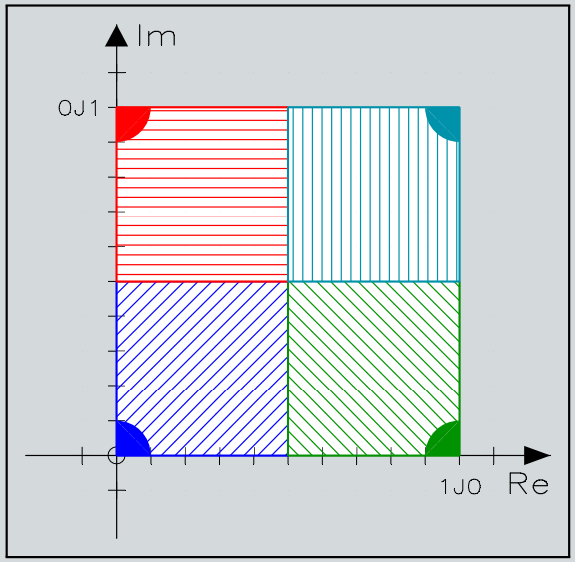
c *Euklidischer Algorithmus mit Runden zum nächsten Gitterpunkt*

$\frac{p}{q} = u + \mathrm{i}\,v \in \mathbb{Q}[i]$ *hat 4 benachbarte Gitterpunkte* $\lfloor u \rfloor + \mathrm{i}\lfloor v \rfloor$, $\lfloor u \rfloor + \mathrm{i}\lceil v \rceil$, $\lceil u \rceil + \mathrm{i}\lfloor v \rfloor$, $\lceil u \rceil + \mathrm{i}\lceil v \rceil$.

Der nächstgelegene Gitterpunkt:
$s = x + \mathrm{i}\,y$, $r := p - q \cdot s$.

$|x - u| \le \frac{1}{2}$, $|y - v| \le \frac{1}{2}$

$\Rightarrow \quad \varphi(r) < \varphi(q)$ *([4])*



`s←(1⌷r)+0J1×2⌷r←⌈¯0.5+9 11○p÷q⋄r←s,p−q×s`

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$: Euklidischer Ring

Definition

a *Euklidische Funktion:* $\varphi(a + \mathrm{i}\,b) = a^2 + b^2$. `r×+r`

b *Euklidischer Algorithmus mit* `⌊` *und* `|:` `r←q|p ⋄s←(p−r)÷q`

c *Euklidischer Algorithmus mit Runden zum nächsten Gitterpunkt*

```
s←(1⌷r)+0J1×2⌷r←⌈¯0.5+9 11○p÷q⋄r←s,p−q×s
```

d *Charakter:* $\psi(a + \mathrm{i}\,b) = \begin{cases} 1 & a > 0 \wedge b \geq 0 \\ \mathrm{i} & a \leq 0 \wedge b > 0 \\ -1 & a < 0 \wedge b \leq 0 \\ -\mathrm{i} & a \geq 0 \wedge b < 0 \end{cases}$

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$: Euklidischer Ring

Definition

a *Euklidische Funktion:* $\varphi(a + \mathrm{i}\,b) = a^2 + b^2$. `r×+r`

b *Euklidischer Algorithmus mit* `⌊` *und* `|:` `r←q|p ⋄s←(p−r)÷q`

c *Euklidischer Algorithmus mit Runden zum nächsten Gitterpunkt*
`s←(1⌷r)+0J1×2⌷r←⌈¯0.5+9 11○p÷q⋄r←s,p−q×s`

d *Charakter:* $\psi(a + \mathrm{i}\,b) = \left\{ \begin{array}{ll} 1 & a > 0 \wedge b \geq 0 \\ \mathrm{i} & a \leq 0 \wedge b > 0 \\ -1 & a < 0 \wedge b \leq 0 \\ -\mathrm{i} & a \geq 0 \wedge b < 0 \end{array} \right\}$

$\psi(e \cdot (a + \mathrm{i}\,b)) = e\psi(a + \mathrm{i}\,b)$

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$: Euklidischer Ring

Definition

a *Euklidische Funktion:* $\varphi(a + \mathrm{i}\,b) = a^2 + b^2$. `r×+r`

b *Euklidischer Algorithmus mit* `⌊` *und* `|:` `r←q|p ⋄s←(p−r)÷q`

c *Euklidischer Algorithmus mit Runden zum nächsten Gitterpunkt*

```
s←(1⌷r)+0J1×2⌷r←⌈¯0.5+9 11○p÷q⋄r←s,p−q×s
```

d *Charakter:* $\psi(a + \mathrm{i}\,b) = \left\{ \begin{array}{ll} 1 & a > 0 \wedge b \geq 0 \\ \mathrm{i} & a \leq 0 \wedge b > 0 \\ -1 & a < 0 \wedge b \leq 0 \\ -\mathrm{i} & a \geq 0 \wedge b < 0 \end{array} \right\}$

$\psi(e \cdot (a + \mathrm{i}\,b)) = e\psi(a + \mathrm{i}\,b)$

```
r←¯12○r−(○0.5)|r←12○r
```

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$:

Beispiele

```
      ]init          ⍝ KhAlZi, -Eukl, -Quot
      (a b)←(1J5 4J¯7)(¯1J12 7J17)
      ]dar c←a ]a b
 ¯16J25/31J27
      (÷/c)≡(÷/a)+(÷/b)
1
```

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$:

Beispiele

```
      ]init          ⍝ KhAlZi, -Eukl, -Quot, -Matr, KhMatrix
      n←4⋄mat←(¯4J¯7+(⍳n))∘.,(2J1×⍳n)
      (1 1⌷mat)←(1 1⌷mat)+n↑,(⍳3)∘.×2J¯5×⍳3
      ]dar mat
  ¯1J¯12/4J¯4   ¯3J¯7/4J2     ¯3J¯7/6J3    ¯3J¯7/8J4
   ¯2J¯7/2J1  2J¯17/8J¯8     ¯2J¯7/6J3    ¯2J¯7/8J4
   ¯1J¯7/2J1   ¯1J¯7/4J2  5J¯22/12J¯12    ¯1J¯7/8J4
    0J¯7/2J1    0J¯7/4J2      0J¯7/6J3  4J¯17/12J¯6
      Det ⌹⍤¨2 mat                    ⍝ real LU-decompos.
¯11.23053108J¯40.56266719
      ⌹/Aldet mat                     ⍝ Laplace
¯11.23053108J¯40.56266719
      ⌹/⊃]m/1 1⌷2⊃1 Algaut mat        ⍝ Gauss
¯11.23053108J¯40.56266719
      ⌹/⊃det←¯1 ¯1↑2⊃0 0 1 Algaut mat ⍝   = " =
¯11.23053108J¯40.56266719
      ]dar det
 4914541J¯4781776/78336J142848
```

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$:

Beispiele

```
      Δdar inv←0 n↓2⊃2 Algaut mat,Δq n nρ(n+1)↑1
  41516J9548/236276J9001   ¯3344J¯1712/14743J41358   ¯2928J¯1584/14743J41358
¯32128J21536/236276J9001   73832J10136/236276J9001  ¯25664J15328/236276J9001
¯45360J20880/236276J9001  ¯40080J17040/236276J9001   100452J6996/236276J9001
¯70056J¯3528/236276J9001  ¯60984J¯4872/236276J9001  ¯53928J¯5544/236276J9001
      □pp←6◇(÷/¨mat)+.×÷/¨inv
 1.00000E0                ¯5.55112E¯17J¯5.55112E¯17 8.32667E¯17               9
¯1.11022E¯16J1.11022E¯16   1.00000E0                 5.55112E¯17J¯4.16334E¯17 0
 5.55112E¯17               5.55112E¯17J 1.38778E¯17 1.00000E0                2
 0.00000E0J1.11022E¯16    ¯5.55112E¯17J 4.16334E¯17 0.00000E0                1
      Δdar mat Δa.Δm inv
  1   0   0   0
  0   1   0   0
  0   0   1   0
  0   0   0   1
```

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$:

Beispiele

```
      n←5◊mat←(¯4J¯7+(⍳n))∘.,(2J1×⍳n)
      (1 1⌹mat)←(1 1⌹mat)+n↑,(⍳3)∘.×2J¯5×⍳3
      Δdar mat
  ¯1J¯12/4J¯4   ¯3J¯7/4J2     ¯3J¯7/6J3    ¯3J¯7/8J4    ¯3J¯7/10J5
   ¯2J¯7/2J1  2J¯17/8J¯8     ¯2J¯7/6J3    ¯2J¯7/8J4    ¯2J¯7/10J5
   ¯1J¯7/2J1   ¯1J¯7/4J2  5J¯22/12J¯12    ¯1J¯7/8J4    ¯1J¯7/10J5
    0J¯7/2J1    0J¯7/4J2      0J¯7/6J3  4J¯17/12J¯6     0J¯7/10J5
    1J¯7/2J1    1J¯7/4J2      1J¯7/6J3    1J¯7/8J4  9J¯27/18J¯15

      Δdar inv←0 n↓2⊃2 Algaut mat,Δq n nρ(n+1)↑1
Kurzen: Cancellation fails
Δa[7]  r←Kurzen(RΔa/a RΔm¨⌽b),⊂(2⊃a)RΔm 2⊃b
                ^
Δs[6]  b[1]←-b[1]◊r←a Δa b
                  ^ ^
Δs[5]  →(∧/Δt=≡¨a b)/1+⎕LC◊r←a Δs¨b◊→0                    ⍝ Subtraction in each ce
       ^                      ^
Algaus[39]  mat[m;]←mat[m;]Δs(mat[m;j]Δd mat[j;j])∘.Δm mat[j;]
                  ^       ^
Algaut[35]  →(0≠(1⊃r)←1⊃mat←(j,3↑ip)Algaus mat)/FX◊mat←2⊃mat
                          ^       ^
      Δdar inv←0 n↓2⊃2 Algaut mat,Δq n nρ(n+1)↑1
                   ^ ^
      x←2*52 53 54◊x+1-x ◊(-x)+1+x
1 0 0
```

Gaußzahlen $\mathbb{Z}[i]$ und $\mathbb{Q}[i] = Q(\mathbb{Z}[i])$:

Beispiele

Die Fehler bei großen Zahlen können durch Verbessern der Addition und Multiplikation noch etwas in Richtung größerer Zahlen verschoben werden, aber irgendwann treten sie auf. Zum Vermeiden müssen größere Speicherbereiche für die Zahlen benutzt werden, die durch eine Accu-Technik implementiert werden können.

Accu-Technik

Accu-Darstellung großer Zahlen

1. Accu-Länge: n Bits mit erlaubtem Überlauf: $b = 2^{50}$ oder $b = 10^{15}$.
2. Darstellung als Vektor $a = \sum_{k=0}^{n} a_k b^k \leftrightsquigarrow (a_0, a_1, \ldots, a_n)$.
3. Addition: $a + b = \sum_{k=0}^{n} (a_i + b_i) \cdot b^k$.
4. Überlauf: $(\ldots, \tilde{a}_k + b, a_{k+1}, \ldots) \rightsquigarrow (\ldots, \tilde{a}_k, a_{k+1} + 1, \ldots)$, gegebenenfalls neue Accu-Zelle ergänzen.
5. Multiplikation: Anzahl der Ziffern kann sich verdoppelt, daher muss zunächst ein Accu mit halber Bitlänge $\tilde{b} \approx \sqrt{b}$ erzeugt werden. Die Multiplikation entspricht dann der Polynommultiplikation:
$\left(\sum_{k=0}^{r} a_k \tilde{b}^k\right) \cdot \left(\sum_{l=0}^{s} a_l \tilde{b}^l\right) = \sum_{k=0}^{r+s} \left(\sum_{l=0}^{k} a_l b_{k-l}\right) \tilde{b}^k$.

Accu-Technik

Accu-Darstellung großer Zahlen

1. Accu-Länge: n Bits mit erlaubtem Überlauf: $b = 2^{50}$ oder $b = 10^{15}$.
2. Darstellung als Vektor $a = \sum_{k=0}^{n} a_k b^k \leftrightsquigarrow (a_0, a_1, \ldots, a_n)$.
3. Addition: $a + b = \sum_{k=0}^{n} (a_i + b_i) \cdot b^k$.
4. Überlauf: $(\ldots, \tilde{a}_k + b, a_{k+1}, \ldots) \rightsquigarrow (\ldots, \tilde{a}_k, a_{k+1} + 1, \ldots)$, gegebenenfalls neue Accu-Zelle ergänzen.
5. Multiplikation: Anzahl der Ziffern kann sich verdoppelt, daher muss zunächst ein Accu mit halber Bitlänge $\tilde{b} \approx \sqrt{b}$ erzeugt werden. Die Multiplikation entspricht dann der Polynommultiplikation:
$\left(\sum_{k=0}^{r} a_k \tilde{b}^k\right) \cdot \left(\sum_{l=0}^{s} a_l \tilde{b}^l\right) = \sum_{k=0}^{r+s} \left(\sum_{l=0}^{k} a_l b_{k-l}\right) \tilde{b}^k$.

Accu-Technik

Accu-Darstellung großer Zahlen

1. Accu-Länge: n Bits mit erlaubtem Überlauf: $b = 2^{50}$ oder $b = 10^{15}$.
2. Darstellung als Vektor $a = \sum_{k=0}^{n} a_k b^k \leftrightsquigarrow (a_0, a_1, \ldots, a_n)$.
3. Addition: $a + b = \sum_{k=0}^{n} (a_i + b_i) \cdot b^k$.
4. Überlauf: $(\ldots, \tilde{a}_k + b, a_{k+1}, \ldots) \rightsquigarrow (\ldots, \tilde{a}_k, a_{k+1} + 1, \ldots)$, gegebenenfalls neue Accu-Zelle ergänzen.
5. Multiplikation: Anzahl der Ziffern kann sich verdoppelt, daher muss zunächst ein Accu mit halber Bitlänge $\tilde{b} \approx \sqrt{b}$ erzeugt werden. Die Multiplikation entspricht dann der Polynommultiplikation:
$\left(\sum_{k=0}^{r} a_k \tilde{b}^k\right) \cdot \left(\sum_{l=0}^{s} a_l \tilde{b}^l\right) = \sum_{k=0}^{r+s} \left(\sum_{l=0}^{k} a_l b_{k-l}\right) \tilde{b}^k$.

Accu-Technik

Accu-Darstellung großer Zahlen

1. Accu-Länge: n Bits mit erlaubtem Überlauf: $b = 2^{50}$ oder $b = 10^{15}$.
2. Darstellung als Vektor $a = \sum_{k=0}^{n} a_k b^k \leftrightsquigarrow (a_0, a_1, \ldots, a_n)$.
3. Addition: $a + b = \sum_{k=0}^{n} (a_i + b_i) \cdot b^k$.
4. Überlauf: $(\ldots, \tilde{a}_k + b, a_{k+1}, \ldots) \rightsquigarrow (\ldots, \tilde{a}_k, a_{k+1} + 1, \ldots)$, gegebenenfalls neue Accu-Zelle ergänzen.
5. Multiplikation: Anzahl der Ziffern kann sich verdoppelt, daher muss zunächst ein Accu mit halber Bitlänge $\tilde{b} \approx \sqrt{b}$ erzeugt werden. Die Multiplikation entspricht dann der Polynommultiplikation:
$$\left(\sum_{k=0}^{r} a_k \tilde{b}^k\right) \cdot \left(\sum_{l=0}^{s} a_l \tilde{b}^l\right) = \sum_{k=0}^{r+s} \left(\sum_{l=0}^{k} a_l b_{k-l}\right) \tilde{b}^k.$$

Accu-Technik

Accu-Darstellung großer Zahlen

1. Accu-Länge: n Bits mit erlaubtem Überlauf: $b = 2^{50}$ oder $b = 10^{15}$.
2. Darstellung als Vektor $a = \sum_{k=0}^{n} a_k b^k \leftrightsquigarrow (a_0, a_1, \ldots, a_n)$.
3. Addition: $a + b = \sum_{k=0}^{n} (a_i + b_i) \cdot b^k$.
4. Überlauf: $(\ldots, \tilde{a}_k + b, a_{k+1}, \ldots) \rightsquigarrow (\ldots, \tilde{a}_k, a_{k+1} + 1, \ldots)$, gegebenenfalls neue Accu-Zelle ergänzen.
5. Multiplikation: Anzahl der Ziffern kann sich verdoppelt, daher muss zunächst ein Accu mit halber Bitlänge $\tilde{b} \approx \sqrt{b}$ erzeugt werden. Die Multiplikation entspricht dann der Polynommultiplikation:
$\left(\sum_{k=0}^{r} a_k \tilde{b}^k\right) \cdot \left(\sum_{l=0}^{s} a_l \tilde{b}^l\right) = \sum_{k=0}^{r+s} \left(\sum_{l=0}^{k} a_l b_{k-l}\right) \tilde{b}^k$.

Zusammenfassung

1. Datenmodell für $\mathbb{Q}$, $\mathbb{R}[x]$, $\mathbb{Z}[i]$ gut.
2. Überlagerung der arithmetischen Funktionen funktioniert.
3. $\mathbb{Z}[i]$: Nächster Gitterpunkt statt $\lfloor \rfloor$ ist wichtig.

Zusammenfassung

1. Datenmodell für $\mathbb{Q}$, $\mathbb{R}[x]$, $\mathbb{Z}[i]$ gut.
2. Überlagerung der arithmetischen Funktionen funktioniert.
3. $\mathbb{Z}[i]$: Nächster Gitterpunkt statt $\lfloor \rceil$ ist wichtig.

Zusammenfassung

1. Datenmodell für $\mathbb{Q}$, $\mathbb{R}[x]$, $\mathbb{Z}[i]$ gut.
2. Überlagerung der arithmetischen Funktionen funktioniert.
3. $\mathbb{Z}[i]$: Nächster Gitterpunkt statt $\lfloor \rfloor$ ist wichtig.

Ausblick

1. Multiplikation für Quotientenkörper verbessern durch vorgezogenes Kürzen,
2. Tiefe für Quotientenkörper um zwei erhöhen,
3. $\mathbb{Z}[\sqrt{-d}]$ für $d = 2, 3, 7, 11$.
4. Datenmodell für $\mathbb{Q}[x]$,
5. $\mathbb{C}[x]$ testen (ist erledigt, 25.11.2020),
6. Accu-Technik benutzen.

Ausblick

1. Multiplikation für Quotientenkörper verbessern durch vorgezogenes Kürzen,
2. Tiefe für Quotientenkörper um zwei erhöhen,
3. $\mathbb{Z}[\sqrt{-d}]$ für $d = 2, 3, 7, 11$.
4. Datenmodell für $\mathbb{Q}[x]$,
5. $\mathbb{C}[x]$ testen (ist erledigt, 25.11.2020),
6. Accu-Technik benutzen.

Ausblick

1. Multiplikation für Quotientenkörper verbessern durch vorgezogenes Kürzen,
2. Tiefe für Quotientenkörper um zwei erhöhen,
3. $\mathbb{Z}[\sqrt{-d}]$ für $d = 2, 3, 7, 11$.
4. Datenmodell für $\mathbb{Q}[x]$,
5. $\mathbb{C}[x]$ testen (ist erledigt, 25.11.2020),
6. Accu-Technik benutzen.

Literatur I


Hahn, W. und K. Mohr: *APL/PCXA*.
Hanser, München, 1988.


Kaplansky, E.: *Fields and Rings*.
Chicaga Lecture Notes in Mathematics Series, 2. ed., 1972.


Lang, S.: *Algebra*.
Graduate Texts in Mathematikmatics. Springer, New York, 3. ed., 1971.


Robinson, D. J.: *Abstract Algebra: An Introduction with Applications*.
De Gruyter Textbook. Walter de Gruyter, Berlin, 2^{nd} ed., 2015.


Samuel, P.: *On euclidean rings*.
Journal Algebra, 19:282–301, 1971.
https://doi.org/10.1016/0021-8693(71)90110-4.

Literatur II

Sims, C. C.: *Abstract Algebra – A computational Approach*. Wiley, New York, 1984.