§ 10: KÖRPER

10.1. Def.: Ein Körper $(K,+,\cdot)$ besteht aus einer Menge K und zwei Verknüpfungen $+$ und $\cdot$ auf K, für die gilt:

a) $(K,+,\cdot)$ ist ein kommutativer Ring mit 1.

b) Inverse Elemente:
Zu jedem $a \in K$ mit $a \neq 0$ ex. ein a^{-1} mit $a^{-1} \cdot a = 1$.

10.2. Bemerkungen

a) $(K,+,\cdot)$ besteht somit aus den kommutativen Gruppen $(K,+)$ und $(K-\{0\},\cdot)$, zwischen denen ein Distributivgesetz gilt.

b) Statt $K-\{0\}$ schreibt man oft auch K^*.

c) Falls $(K^*,\cdot)$ nur eine nicht kommutative Gruppe ist, bezeichnet man $(K,+,\cdot)$ als Schiefkörper.

d) Im Englischen heißen Körper fields.

10.3. Beispiele

a) $(\mathbb{Z},+,\cdot)$ ist kein Körper, da zu $a \in \mathbb{Z}^*$ i.A. kein a^{-1} existiert.

b) $(\mathbb{Q},+,\cdot)$ und $(\mathbb{R},+,\cdot)$ sind Körper.

Weitere Beispiele folgen später.

Welche Eigenschaften gelten in Körpern?

10.4. Satz (Eigenschaften von Körpern)

In einem Körper $(K, +, \cdot)$ gilt:

a) $a \cdot 0 = 0 \quad \forall a \in K$

b) Nullteilerfreiheit:

Sind $a, b \in K$ mit $a \neq 0$ und $b \neq 0$, so ist auch $a \cdot b \neq 0$.

(d.h. aus $a \cdot b = 0$ folgt $a = 0$ oder $b = 0$.)

Beweis:

a) Da 0 neutrales Element bzgl. + ist, gilt:

$$\begin{aligned} a \cdot 0 + 0 &= a \cdot 0 \\ &= a \cdot (0 + 0) \\ &= a \cdot 0 + a \cdot 0 \\ &\quad \uparrow \text{Distr.} \end{aligned}$$

Addition von $-a \cdot 0$ auf beiden Seiten ergibt die Beh.

$$0 = a \cdot 0$$

b) Seien $a \neq 0$, $b \neq 0$.

Ann.: $a \cdot b = 0$

$$\Rightarrow \quad b = (a^{-1}a)\,b = a^{-1}\underbrace{(a \cdot b)}_{0} = a^{-1} \cdot 0 \overset{(a)}{=} 0$$

$\lightning$ zu $b \neq 0$. $\square$

Bem.: 10.4. a impliziert, dass man in Körpern nicht durch 0 dividieren darf: $q := \frac{a}{b}$ bedeutet $a = q \cdot b$.

Ist $b = 0$, folgt $a = 0$. Für $a = 0$ ist jedoch $a = q \cdot b$ für jedes $q \in K$ erfüllt. Somit macht auch $\frac{0}{0}$ keinen Sinn.

10.5. Endliche Körper

Wir betrachten den Restklassenring $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ mit der modularen Addition und Multiplikation. In 8.3 (g) haben wir gesehen (vgl. auch 7.12 und 7.13):

$(\mathbb{Z}_m^*, \cdot)$ ist eine kommutative Gruppe, falls m eine Primzahl ist.

Man kann sogar zeigen:

$(\mathbb{Z}_m, +, \cdot)$ ist genau dann ein Körper, wenn m eine Primzahl ist.

Beispiel 7.11 illustriert, dass $(\mathbb{Z}_6, +, \cdot)$ kein Körper sein kann, da es beispielsweise nicht nullteilerfrei ist. (und z.B. in $[2]$ kein multiplikatives Inverses existiert)

Allgemein bezeichnet man einen endl. Körper mit q Elementen als Galoisfeld $GF(q)$ (Evariste Galois, 1811–1832).

Galoisfelder ex. nur für Primzahlpotenzen $q = p^m$ und sind für ein festes q eindeutig (bis auf Isomorphie).

Für eine Primzahl p gilt also:

$$GF(p) = \mathbb{Z}_p$$

10.6. Der Körper der komplexen Zahlen

Problem:
- Manche Polynome haben in $\mathbb{R}$ keine Nullstellen
- Bsp.: $p(x) = x^2 + 1$
- Kann man $\sqrt{-1}$ sinnvoll definieren?

Ablilfe:

- Wir betten $\mathbb{R}$ in $\mathbb{C} := \mathbb{R}^2 = \{(a,b) \mid a,b \in \mathbb{R}\}$ ein, indem wir $\mathbb{R}$ als die x-Achse $\{(a,0) \mid a \in \mathbb{R}\}$ interpretieren.

  Dort muss gelten:
  - Addition: $(a,0) + (c,0) = (a+c, 0)$
  - Multiplikation: $(a,0) \cdot (c,0) = (a \cdot c, 0)$

- Suchen Erweiterung von Addition und Multiplikation auf $\mathbb{C}$, so dass
  - $(\mathbb{C}, +, \cdot)$ ein Körper ist
  - eine Zahl $(a,b) \in \mathbb{C}$ ex. mit $(a,b) \cdot (a,b) = (-1,0)$.

10.7. Def.: Auf $\mathbb{C} := \mathbb{R}^2 = \{(a,b) \mid a,b \in \mathbb{R}\}$ sind folgende Verknüpfungen definiert:

a) Addition:

$$(a,b) + (c,d) = (a+c,\ b+d) \qquad \forall a,b,c,d \in \mathbb{R}$$

b) Multiplikation

$$(a,b) \cdot (c,d) := (ac - bd,\ ad + bc)$$

$\forall a,b,c,d \in \mathbb{R}$.

10.8. Konsequenten

Mit Def. 10.7 gilt:

- Einschränkung auf x-Achse liefert Addition / Multiplikation der reellen Zahlen:

$$(a,0) + (c,0) = (a+c,0)$$
$$(a,0) \cdot (c,0) = (a \cdot c, 0) \qquad \forall\, a,c \in \mathbb{R}$$

- Das neutrale Element der Mult. auf $\mathbb{C}$ ist $(1,0)$:

$$(1,0) \cdot (c,d) = (c,d)$$

- In $\mathbb{C}$ ex. $\sqrt{-1}$, denn:

$$(0,1) \cdot (0,1) = (-1,0)$$

Für $(0,1)$ schreiben wir i (imaginäre Einheit).

10.9. Satz (Körper der komplexen Zahlen)

$(\mathbb{C}, +, \cdot)$ bildet einen Körper, den Körper der komplexen Zahlen.

Beweis: Elementar, abgesehen von der Existenz des inversen Elements der Multiplikation:

Für $(a,b) \neq (0,0)$ gilt: $(a,b)^{-1} := \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right)$.

Denn:

$$(a,b)\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right) = \left(\frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}, \frac{ab}{a^2+b^2} - \frac{ab}{a^2+b^2} \right)$$
$$= (1,0) \cdot$$

□

10.10 Praktisches Rechnen mit komplexen Zahlen

Statt (a,b) schreibt man $a+ib$, verwendet $i^2=-1$, und rechnet ansonsten wie mit reellen Zahlen.

Damit erhält man direkt Def. 10.7 für Addition / Multiplikation:

Addition: $(a+ib)+(c+id) = (a+b)+i(b+d)$

Multiplikation: $(a+ib)\cdot(c+id) = ac + aid + ibc + \underbrace{i^2}_{=-1} bd$

$= (ac-bd) + i(ad+bc)$

10.11. Def.: Zu einer komplexen Zahl $z = a+ib$ definiert man $\bar{z} := a-ib$ als das konjugierte Element zu z.

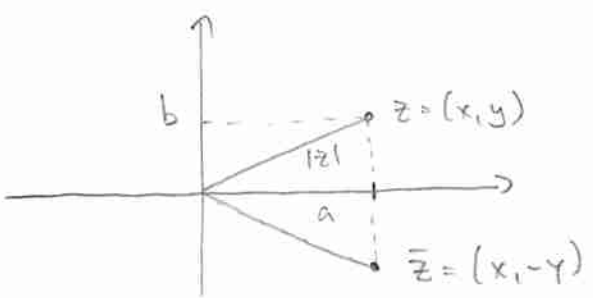
Ferner nennt man $|z| := \sqrt{z\bar{z}} = \sqrt{(a+ib)(a-ib)}$

$= \sqrt{a^2 - i^2 b^2} = \sqrt{a^2+b^2}$

den Betrag von z. Man nennt a den Realteil und b den Imaginärteil von z.

10.12. Geometrische Interpretation

Betrachtet man z als Vektor $(a,b) \in \mathbb{R}^2$, so ist $\bar{z}$ der an der x-Achse gespiegelte Vektor, und $|z| = \sqrt{a^2+b^2}$ ist die Länge des Vektors:



10.13. Wozu ist das konjugiert komplexe Element noch nützlich?

z.B. um bei komplexen Brüchen $\frac{a+ib}{c+id}$ den Nenner reell zu machen. Man erweitert mit $c-id$:

$$\frac{a+ib}{c+id}\cdot\frac{c-id}{c-id} = \frac{ac-aid+ibc-i^2bd}{c^2-cid+idc-i^2d^2}$$

$$= \frac{ac+bd+i(bc-ad)}{c^2+d^2}$$

$$= \frac{ac+bd}{c^2+d^2} + i\,\frac{bc-ad}{c^2+d^2}.$$

Welche Bedeutung hat $\mathbb{C}$ für die Nullstellen von Polynomen? Man kann zeigen:

10.14 Satz (Fundamentalsatz der Algebra)

Jedes komplexwertige Polynom $p \in \mathbb{C}[x]$ mit Grad > 0 hat eine Nullstelle in $\mathbb{C}$. („$\mathbb{C}$ ist algebraisch abgeschlossen")

Konsequenz: $p \in \mathbb{C}[x]$ mit $\deg(p)=n>1$ zerfällt in n Linearfaktoren:
$p(x) = \sum_{i=0}^{n} a_i x^i \Rightarrow \exists\, x_1,\dots,x_n \in \mathbb{C}: \; p(x) = a_n(x-x_1)\cdot\ldots\cdot(x-x_n)$.

10.15. Beispiel

$p(x) = 2x^2-3x+5$ hat die Nullstellen (a,b,c-Formel)

$$x_{1/2} = \frac{3 \pm \sqrt{3^2-4\cdot 2\cdot 5}}{2\cdot 2} = \frac{3\pm\sqrt{-31}}{4}$$

$$= \frac{3\pm\sqrt{31}\sqrt{-1}}{4} = \frac{3}{4} \pm \frac{\sqrt{31}}{4}\,i;$$

$$\Rightarrow p(x) = 2\left(x-\frac{3}{4}-\frac{\sqrt{31}}{4}i\right)\left(x-\frac{3}{4}+\frac{\sqrt{31}}{4}i\right).$$

10.16. Wozu sind komplexe Zahlen noch nützlich?

- Manche mathematischen Resultate lassen sich in $\mathbb{C}$ einfacher beschreiben und besser verstehen als in $\mathbb{R}$ (z.B. das Konvergenzverhalten von Potenzreihen (später)).
- Schwingungsvorgänge in elektrischen Schaltkreisen sind in $\mathbb{C}$ wesentlich kompakter darstellbar als in $\mathbb{R}$. Es gibt also sehr konkrete Anwendungen in der Elektrotechnik und der Technischen Informatik.