Körper

Eine Menge K, auf der eine Addition „$+$“ und eine Multiplikation „$\cdot$“ definiert sind, nennt man einen Körper, wenn folgendes gilt:

- Additive Gruppenstruktur: $(K, +)$ ist eine abelsche Gruppe mit neutralem Element 0 (Nullelement), d.h. für alle $a, b \in K$ gilt

$$\begin{aligned} a + b &= b + a \\ (a + b) + c &= a + (b + c) \\ a + 0 &= a \\ a + (-a) &= 0\,, \end{aligned}$$

  wobei $(-a)$ das inverse Element zu a bezeichnet.

- Multiplikative Gruppenstruktur: $(K\backslash\{0\},\cdot)$ ist eine abelsche Gruppe mit neutralem Element 1 (Einselement), d.h. für alle $a,b,c \in K\backslash\{0\}$ gilt

$$\begin{aligned} a \cdot b &= b \cdot a \\ (a \cdot b) \cdot c &= a \cdot (b \cdot c) \\ a \cdot 1 &= a \\ a \cdot a^{-1} &= 1\,, \end{aligned}$$

  wobei a^{-1} das inverse Element zu a bezeichnet.
- Distributivgesetz:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

  für alle $a,b,c \in K$.

Beispiel

Körper der rationalen, reellen und komplexen Zahlen

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Nullelement: 0, Einselement: 1

Inverses Element bezüglich der Multiplikation einer komplexen Zahl $z = x + \mathrm{i}y \neq 0$:

$$w = \frac{x}{x^2 + y^2} + \mathrm{i}\,\frac{-y}{x^2 + y^2}\;,$$

denn

$$\begin{aligned} z \cdot w &= (x + \mathrm{i}y)\left(\frac{x}{x^2 + y^2} + \mathrm{i}\,\frac{-y}{x^2 + y^2}\right) \\ &= \frac{x^2 - \mathrm{i}^2 y^2}{x^2 + y^2} + \mathrm{i}\,\frac{-xy + yx}{x^2 + y^2} = 1 + \mathrm{i}0 = 1 \end{aligned}$$

Beispiel

Gruppentafeln von Addition und Multiplikation für den Galois-Körper GF[2^2] mit 4 Elementen

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

z.B: $(a+1)\cdot b = b \cdot b = 1$, $-b = b$ ($\Longleftrightarrow b + b = 0$), $1/a = b$

Die Konstruktion von Körpern mit p^ℓ Elementen, $\ell \in \mathbb{N}$, ist für beliebige Primzahlen p durchführbar.

$\rightsquigarrow$ alle endlichen Körper