Eine Algebra $A = \langle S, \oplus, \odot \rangle$ mit zwei zweistelligen Operatoren $\oplus$ und $\odot$ heisst *Körper* (engl. *field*), falls

K1. $\langle S, \oplus \rangle$ eine abelsche Gruppe mit neutralem Element $0 \in S$ ist,

K2. $\langle S \setminus \{0\}, \odot \rangle$ eine abelsche Gruppe mit neutralem Element $1 \in S$ ist und

K3. $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ für alle $a, b, c \in S$.

Eine Algebra $A = \langle S, \circ \rangle$ mit einem 2-stelligen Operator $\circ$ heisst **Gruppe**, falls

G1. $\circ$ assoziativ ist,

G2. $\cdot$ ein neutrales Element $e \in S$ besitzt und

G3. es zu jedem Element $a \in S$ ein Inverses gibt.

Lemma: In jedem Körper K gilt:

$$a \cdot 0 = 0 \cdot a = 0 \qquad \text{für alle } a \in K.$$

Beweis: Es sei a ein beliebiges Element aus K. Dann folgt aus den Axiomen in der Definition eines Körpers:

$$\begin{aligned} a \cdot 0 \quad &\overset{\mathbf{K1/G2}}{=} \quad a \cdot 0 + 0 \overset{\mathbf{K1/G3}}{=} a \cdot 0 + (a + (-a)) \overset{\mathbf{K1/G1}}{=} ((a \cdot 0) + a) + (-a) \\ &\overset{\mathbf{K2/G2}}{=} \quad ((a \cdot 0) + (a \cdot 1)) + (-a) \overset{\mathbf{K3}}{=} (a \cdot (0 + 1)) + (-a) \overset{\mathbf{K1/G2}}{=} (a \cdot 1) + (-a) \\ &\overset{\mathbf{K2/G2}}{=} \quad a + (-a) \overset{\mathbf{K1/G3}}{=} 0. \end{aligned}$$

Beispiel: Sei $K = \{0, 1, a, b\}$ und Addition und Multiplikation definiert durch

$\oplus$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\odot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Dann bildet $\langle K, \oplus, \odot \rangle$ einen Körper (Nachrechnen!).

Sei $K = \mathbb{Z}_5$, $f(x) = 2x^4 + x^3 + 3x + 1$ und $g(x) = 3x + 2$. Dann gilt:

$$
\begin{array}{l}
2x^4 + x^3 + x + 3 \;\div\; 3x + 2 \;=\; 4x^3 + x^2 + x + 3 \\
\underline{-\,(2x^4 + 3x^3)} \\
\qquad 3x^3 + x + 3 \\
\qquad \underline{-\,(3x^3 + 2x^2)} \\
\qquad\qquad 3x^2 + x + 3 \\
\qquad\qquad \underline{-\,(3x^2 + 2x)} \\
\qquad\qquad\qquad 4x + 3 \\
\qquad\qquad\qquad \underline{-\,(4x + 1)} \\
\qquad\qquad\qquad\qquad 2
\end{array}
$$

Hier ergibt sich also $t(x) = 4x^3 + x^2 + x + 3$ und $r(x) = 2$.

Beachte: $4x^3 \cdot (3x + 2) = 2x^4 + 3x^3$, da alle arithmetischen Operationen für die Koeffizienten modulo 5 ausgeführt werden müssen, denn wir betrachten hier ja nur Polynome in $Z_5[x]$!

Beispiel: $K = \mathbb{Z}_3, \pi(x) = x^2 + 1$

$\oplus$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[0]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[1]$	$[1]$	$[2]$	$[0]$	$[x+1]$	$[x+2]$	$[x]$	$[2x+1]$	$[2x+2]$	$[2x]$
$[2]$	$[2]$	$[0]$	$[1]$	$[x+2]$	$[x]$	$[x+1]$	$[2x+2]$	$[2x]$	$[2x+2]$
$[x]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$	$[0]$	$[1]$	$[2]$
$[x+1]$	$[x+1]$	$[x+2]$	$[x]$	$[2x+1]$	$[2x+2]$	$[2x]$	$[1]$	$[2]$	$[0]$
$[x+2]$	$[x+2]$	$[x]$	$[x+1]$	$[2x+2]$	$[2x]$	$[2x+1]$	$[2]$	$[0]$	$[1]$
$[2x]$	$[2x]$	$[2x+1]$	$[2x+2]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$
$[2x+1]$	$[2x+1]$	$[2x+2]$	$[2x]$	$[1]$	$[2]$	$[0]$	$[x+1]$	$[x+2]$	$[x]$
$[2x+2]$	$[2x+2]$	$[2x]$	$[2x+1]$	$[2]$	$[0]$	$[1]$	$[x+2]$	$[x]$	$[x+1]$

$\odot$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[2]$	$[0]$	$[2]$	$[1]$	$[2x]$	$[2x+2]$	$[2x+1]$	$[x]$	$[x+2]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[2x]$	$[2]$	$[x+2]$	$[2x+2]$	$[1]$	$[x+1]$	$[2x+1]$
$[x+1]$	$[0]$	$[x+1]$	$[2x+2]$	$[x+2]$	$[2x]$	$[1]$	$[2x+1]$	$[2]$	$[x]$
$[x+2]$	$[0]$	$[x+2]$	$[2x+1]$	$[2x+2]$	$[1]$	$[x]$	$[x+1]$	$[2x]$	$[2]$
$[2x]$	$[0]$	$[2x]$	$[x]$	$[1]$	$[2x+1]$	$[x+1]$	$[2]$	$[2x+2]$	$[x+2]$
$[2x+1]$	$[0]$	$[2x+1]$	$[x+2]$	$[x+1]$	$[2]$	$[2x]$	$[2x+2]$	$[x]$	$[1]$
$[2x+2]$	$[0]$	$[2x+2]$	$[x+1]$	$[2x+1]$	$[x]$	$[2]$	$[x+2]$	$[1]$	$[2x]$

BEISPIEL: $\mathbb{Z}_3[x] \,/\, x^2+1$

$\cdot$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[2]$	$[0]$	$[2]$	$[1]$	$[2x]$	$[2x+2]$	$[2x+1]$	$[x]$	$[x+2]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[2x]$	$[2]$	$[x+2]$	$[2x+2]$	$[1]$	$[x+1]$	$[2x+1]$
$[x+1]$	$[0]$	$[x+1]$	$[2x+2]$	$[x+2]$	$[2x]$	$[1]$	$[2x+1]$	$[2]$	$[x]$
$[x+2]$	$[0]$	$[x+2]$	$[2x+1]$	$[2x+2]$	$[1]$	$[x]$	$[x+1]$	$[2x]$	$[2]$
$[2x]$	$[0]$	$[2x]$	$[x]$	$[1]$	$[2x+1]$	$[x+1]$	$[2]$	$[2x+2]$	$[x+2]$
$[2x+1]$	$[0]$	$[2x+1]$	$[x+2]$	$[x+1]$	$[2]$	$[2x]$	$[2x+2]$	$[x]$	$[1]$
$[2x+2]$	$[0]$	$[2x+2]$	$[x+1]$	$[2x+1]$	$[x]$	$[2]$	$[x+2]$	$[1]$	$[2x]$

Primitives Element ist $[x+1]$:

$$[x+1]^2 = [x+1]\cdot[x+1] = [2x]$$
$$[x+1]^3 = [2x]\cdot[x+1] = [2x+1]$$
$$[x+1]^4 = [2x+1]\cdot[x+1] = [2]$$
$$[x+1]^5 = [2]\cdot[x+1] = [2x+2]$$
$$[x+1]^6 = [2x+2]\cdot[x+1] = [x]$$
$$[x+1]^7 = [x]\cdot[x+1] = [x+2]$$
$$[x+1]^8 = [x+2]\cdot[x+1] = [1]$$