

# Ukázka tělesa $GF(4) = GF(2^2)$

Pro čtyřprvkovou množinu  $T = \{0, 1, a, b\}$  definujeme operace sčítání a násobení takto:

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

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Pro takto definované operace  $+$  a  $\cdot$  platí všechny axiomy tělesa.

Jiný pohled na totéž těleso: vezmeme za prvky  $T$  polynomy maximálního stupně 1 s koeficienty v  $\mathbb{Z}_2$ , např.  $a = x$ ,  $b = x + 1$ . Násobení pak provádíme modulo polynom  $x^2 + x + 1$ .

+	0	1	x	x + 1
0	0	1	x	x + 1
1	1	0	x + 1	x
x	x	x + 1	0	1
x + 1	x + 1	x	1	0

·	0	1	x	x + 1
0	0	0	0	0
1	0	1	x	x + 1
x	0	x	x + 1	1
x + 1	0	x + 1	1	x