Galois-Feld GF(8)

Geben Sie die vollständigen Verknüpfungstabellen von GF(8) bezüglich ⊕ und ⊙ in 3-Bit-Dual-Darstellung an.

GF(8) - Polynomial

GF(8), ⊕ - Polynomial

⊕	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

GF(8), ⊗ - Polynomial auf x^3+x^2+1 reduziert

⊗	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	x^2+1	x^2+x+1	1	$x+1$
$x+1$	0	$x+1$	x^2+x	x^2+1	1	x	x^2+x+1	x^2+x
x^2	0	x^2	x^2+1	1	x^2+x+1	$x+1$	x	x^2+x
x^2+1	0	x^2+1	x^2+x+1	x	$x+1$	x^2+x	x^2	1
x^2+x	0	x^2+x	1	x^2+x+1	x	x^2	$\cancel{x}$	x
x^2+x+1	0	x^2+x+1	$x+1$	x^2+x	x^2+x	1	x^2	$x+1$

Galois-Feld GF(8)-2

GF(8)-Dual

GF(8), ⊕ -Dual

⊕	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

GF(8), ⊙ -Dual auf x^3+x^2+1 reduziert

⊙	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	100	110	101	111	001	100
011	000	011	110	101	001	011	111	110
100	000	100	101	001	111	100	010	110
101	000	101	111	010	100	110	100	001
110	000	110	001	111	010	100	010	010
111	000	111	101	011	011	001	100	100

Zwischenrechnungen

$(x+1)\cdot(x^2+1) = x^3+x^2+x+1$

$x^3+x^2+x+1 = 1\cdot(x^3+x^2+1) + x$

$\Rightarrow (x+1) \odot (x^2+1) = x$

$(x^2+x)\cdot(x+1) = x^3+x^2+x^2+x = x^3+2x^2+x$

$x^3+2x^2+x = 1\cdot(x^3+x^2+1) + x^2+x+1$

$\Rightarrow (x^2+x) \odot (x+1) = x^2+x+1$

$(x^2+x+1)\cdot(x+1) = x^3+x^2+x+x^2+x+1 = x^3+2x^2+2x+1$

$x^3+2x^2+2x+1 = 1\cdot(x^3+x^2+1)+x^2+x$

$\Rightarrow (x^2+x+1) \odot (x+1) = x^2+x$

$x^2\cdot x^2 = x^4$

$x^4 = \underbrace{x\cdot(x^3+x^2+1)}_{x^4+x^3+x} + x^3+x$ $\qquad x^3+x = 1\cdot(x^3+x^2+1)+x^2+x+1$

$\Rightarrow x^2 \odot x^2 = x^2+1$

$(x^2+1)\cdot x^2 = x^4+x^2$

$x^4+x^2 = \underbrace{x(x^3+x^2+1)}_{x^4+x^3+x} + x^3+x^2+x$

$x^3+x^2+x = 1\cdot(x^3+x^2+1)+x+1$

$\Rightarrow (x^2+1) \odot x^2 = x+1$

$(x^2+x)\cdot x^2 = x^4+x^2$

$x^4+x^2 = \underbrace{x(x^3+x^2+1)}_{x^4+x^3+x} + x^3+x^2+x+1$

$x^3+x^2+x+1 = 1\cdot(x^3+x^2+1)+x$

$\Rightarrow (x^2+x) \odot x^2 = x$

$(x^2+x+1)\cdot x^2 = x^4+x^3+x^2$

$x^4+x^3+x^2 = \underbrace{x(x^3+x^2+1)}_{x^4+x^3+x} + x^2+x$

$\Rightarrow (x^2+x+1) \odot x^2 = x^2+1$

$(x^2+1)\cdot(x^2+1) = x^4+2x^2+1$

$x^4+2x^2+1 = \underbrace{x(x^3+x^2+1)}_{x^4+x^3+x} + x^3+2x^2+x+1$

$x^3+2x^2+x+1 = 1\cdot(x^3+x^2+1)+x^2+x$

$\Rightarrow (x^2+1) \odot (x^2+1) = x^2+x$

Zwischenrechnungen 2

$(x^2+x)\cdot(x^2+1) = x^4+x^3+x^2+x$

$x^4+x^3+x^2+x = x(x^3+x^2+1) + x^2$

x^4+x^3+x

$\Rightarrow (x^2+x) \odot (x^2+1) = x^2$

$(x^2+x+1)\cdot(x^2+1) = (x^4+x^3+x^2+x^2+x+1)$

$= x^4+x^3+2x^2+x+1$

$x^4+x^3+2x^2+x+1 = x(x^3+x^2+1) + 2x^2+1$

x^4+x^3+x

$2x^2+1 = 1\cdot(x^3+x^2+1) + x^3+x^2$

$x^3+x^2 = 1(x^3+x^2+1)+1$

$\Rightarrow (x^2+x+1) \odot (x^2+1) = 1$

$(x^2+x)(x^2+x) = x^4+2x^3+x^2$

$x^4+2x^3+x^2 = x(x^3+x^2+1)+x^3+x^2+x+1$

x^4+x^3+x

$x^3+x^2+x+1 = 1\cdot(x^3+x^2+1)+x$

$\Rightarrow (x^2+x) \odot (x^2+x) = x$

$(x^2+x+1)\cdot(x^2+x) = x^4+x^3+x^2+x^3+x^2+x$

$= x^4+2x^3+2x^2+x$

$x^4+2x^3+2x^2+x = x\cdot(x^3+x^2+1)+x^3+2x^2+1$

x^4+x^3+x

$x^3+2x^2+1 = 1\cdot(x^3+x^2+1)+x^2$

$\Rightarrow (x^2+x+1) \odot (x^2+x) = x^2$

$(x^2+x+1)\cdot(x^2+x+1) = x^4+x^3+x^2+x^3+x^2+x+x^2+x+1$

$= x^4+2x^3+3x^2+2x+1$

$x^4+2x^3+3x^2+2x+1 = x\cdot(x^3+x^2+1)+x^3+3x^2+x$

x^4+x^3+x

$x^3+3x^2+x = 1\cdot(x^3+x^2+1)+2x^2+x+1$

$2x^2+x+1 = 1\cdot(x^3+x^2+1)+x^3+x^2+x$

$x^3+x^2+x = 1\cdot(x^3+x^2+1)+x+1$