x^2+x+1 irr. over $\mathbb{F}_2$

$\mathbb{F}_4 = \mathbb{F}_2[x]/\langle x^2+x+1\rangle \;\cdot\; \{a_0+a_1\alpha \mid a_0,a_1 \in \mathbb{F}_2\}$

$\alpha = [x]$ $\qquad \alpha^2+\alpha+1=0$

+	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	1	0	α

·	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

$\mathbb{F}_{16} = \mathbb{F}_4[x]/\langle x^2+x+\alpha\rangle$ $\qquad \beta = [x]$ $\qquad \beta^2+\beta+\alpha=0$

$\Leftrightarrow \beta^2+\beta=\alpha$

$\{a_0+a_1\beta \mid a_0,a_1 \in \mathbb{F}_4\}$

$= \{0, 1, \alpha, \alpha+1, \beta, \beta+1, \beta+\alpha, \beta+\alpha+1,$
$\alpha\beta, \alpha\beta+1, \alpha\beta+\beta, \alpha\beta+\alpha+1,$
$(\alpha+1)\beta, (\alpha+1)\beta+1, (\alpha+1)\beta+\alpha,$
$(\alpha+1)\beta+\alpha+1\}$

Rechenbeispiel:

$(\alpha\beta+\alpha)\cdot(\beta+\alpha+1)$

$= \alpha\beta^2+\alpha^2\beta+\alpha\beta+\alpha\beta+\alpha^2+\alpha$

$= \alpha(\beta+\alpha)+(\alpha+1)\beta+\alpha\beta+\alpha\beta+(\alpha+1)+\alpha$

$= \alpha\beta+\alpha^2+\alpha\beta+\beta+1 = \alpha+1+\beta+1$

$= \alpha+\beta$