Multiplikation von Polynomen mit Koeffizienten über GF(2^3)
- wird benötigt zur Konstruktion von Reed-Solomon-Codes -

Regeln:

- Alle Variablen x und alle Koeffizienten sind Elemente des zugrundeliegenden Galoisfeldes, hier GF(2^3), siehe Tabelle zu VL 5
- Jedem Galoisfeld-Element kann seine **binäre Kurzform-Darstellung** zugeordnet werden, z.B. $\alpha^6 = \alpha^2 + 1 \rightarrow 101$
- Jedes Element hat daher die **binäre Blockbreite** $b=m^*$ mit m^* als Grad des definierenden irreduziblen Polynoms des GF(2^{m^*}).
- Die Addition der Galoisfeld-Elemente wird am einfachsten durch **MOD 2 – Addition der Kurzformen** durchgeführt,
  z. B. $\alpha^3 + \alpha^4 \rightarrow 011 + 110 = 101 \rightarrow \alpha^6$
- Die Multiplikation und die Division wird am einfachsten über die **Addition bzw. Subtraktion der Exponenten** durchgeführt,
  z. B. $\alpha^3 \cdot \alpha^2 = \alpha^5$ oder $\alpha^6 / \alpha^2 = \alpha^4$, dabei **beachten**, dass sich die Galoisfeld-Elemente wiederholen, im GF(2^m) mit MOD (2^m-1), im GF(2^3) zum Beispiel mit MOD 7, also $\alpha^3 \cdot \alpha^6 = \alpha^9 = \alpha^2$ oder $\alpha^2 / \alpha^5 = \alpha^{-3} = \alpha^4$

Beispiel: Generatorpolynom zur Korrektur von t_{korr} = 1 Fehlerbündel der Breite b = m = 3 Bits

$g(x) = (x-\alpha^1)\cdot(x-\alpha^2)$
$= x^2 - \alpha^1 \cdot x - \alpha^2 \cdot x + \alpha^1 \cdot \alpha^2$
$= x^2 - (\alpha^1 + \alpha^2) \cdot x + \alpha^3$
$= x^2 - \alpha^4 \cdot x + \alpha^3$, da $\alpha^1 + \alpha^2 \rightarrow 010 + 100 = 110 \rightarrow \alpha^4$

$=$ **001 110 011** , in **binärer Kurzform**, da der Koeffizient 1 bei x^2 in Kurzform **001** ist

Beispiel: Generatorpolynom zur Korrektur von t_{korr} = 2 Fehlerbündeln der Breite b = m = 3 Bits

$g(x) = (x-\alpha^1)\cdot(x-\alpha^2)\cdot(x-\alpha^3)\cdot(x-\alpha^4)$
$= (x^2 - \alpha^4 \cdot x + \alpha^3) \cdot (x-\alpha^3) \cdot (x-\alpha^4)$
$= (x^2 - \alpha^4 \cdot x + \alpha^3) \cdot (x^2 - (\alpha^3 + \alpha^4) \cdot x + \alpha^7)$
$= (x^2 - \alpha^4 \cdot x + \alpha^3) \cdot (x^2 - \alpha^6 \cdot x + \alpha^7)$, da $\alpha^3 + \alpha^4 \rightarrow 011 + 110 = 101 \rightarrow \alpha^6$
$= (x^2 + \alpha^4 \cdot x + \alpha^3) \cdot (x^2 + \alpha^6 \cdot x + \alpha^7)$, da „-“ = „+“ im Z_2
$= (x^2 + \alpha^4 \cdot x + \alpha^3) \cdot (x^2 + \alpha^6 \cdot x + 1)$, da $\alpha^7 = \alpha^0 = 1$
$= x^4 + (\alpha^4 + \alpha^6) x^3 + (\alpha^3 + \alpha^{10} + 1) x^2 + (\alpha^9 + \alpha^4) x + \alpha^3 = x^4 + \alpha^3 x^3 + x^2 + \alpha^1 x + \alpha^3$ → **warum?**

= 001 011 001 010 011 , in binärer Kurzform