- Polynomials
- Addition & Multiplication of Polynomials.

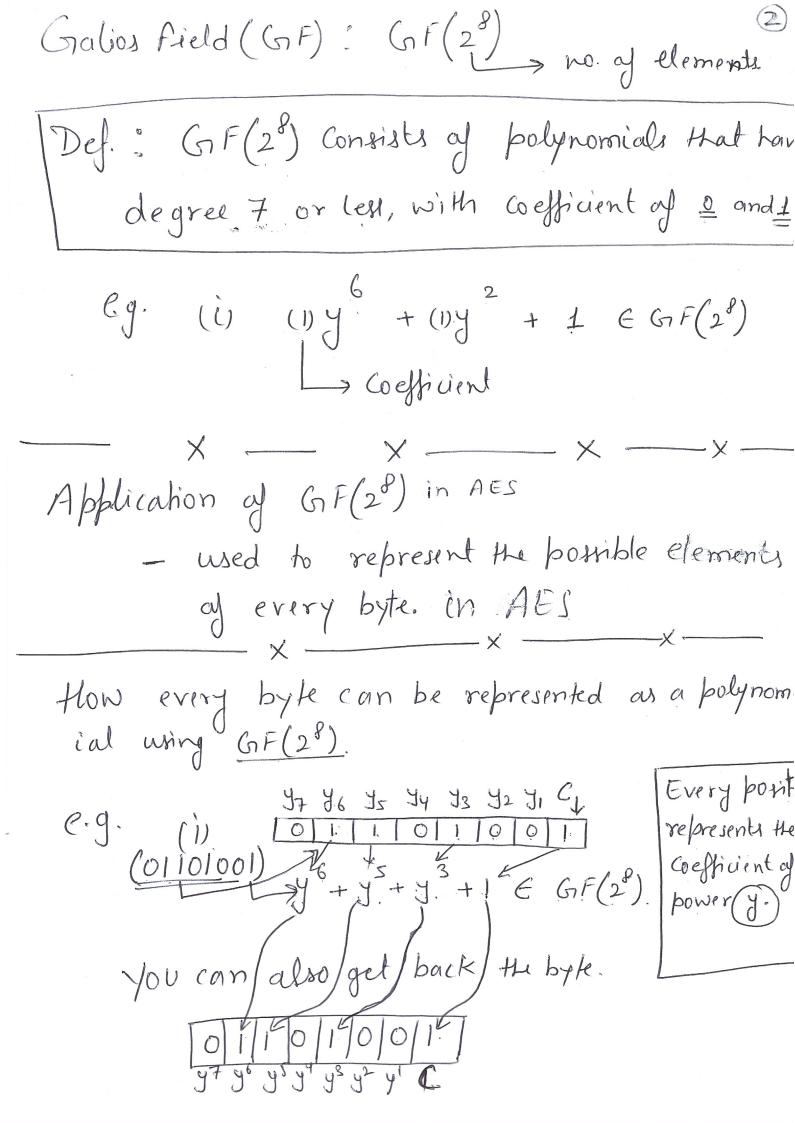
What are Polynomials! - An enpression that consisting of variables & Coefficients, involves only operations a) +1-, x and non-nægative intergor exponents of variables.

Ex. (i) 
$$3x^{2} + 4x + 7 \rightarrow Degree 2$$
  
(ii)  $4y^{3} + 2y^{2} + 1 \rightarrow Degree 3$   
(iii)  $3x^{2} - 4x + 1 \rightarrow not a polynomial$ 

Addition:

(i). 
$$(2y^2 + 5y^2 + 1) + (2y^2 + 5y + 3)$$
  
=>  $(4y^2 + 10y + 4)$ 

Multiplication: Ams: 
$$(i)$$
  $(3y+2) + (5y-2) = 15y+4y-4$ 

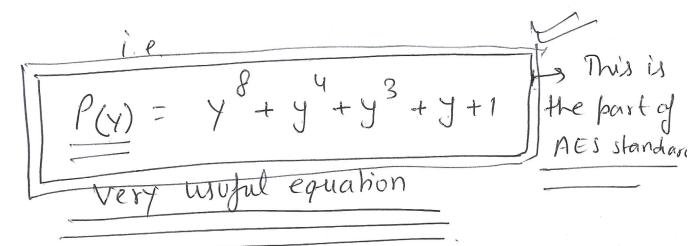


We can say that [GF(28) can Contain all possible bytes. Few operations in GF(28) Addition: GF makes use of (xOR) for the addition y + 4 + 1 - I + (do xor operation). 46+44+1 y7 + y9 + y - I + ( xor) + 1 + 1 - II y = + y,6 ~ Chf(2)  $y^5 + y^3 + 1 - T$ (11) y + y + y + 1 - II DIY7

## Multiplication in GF(28)

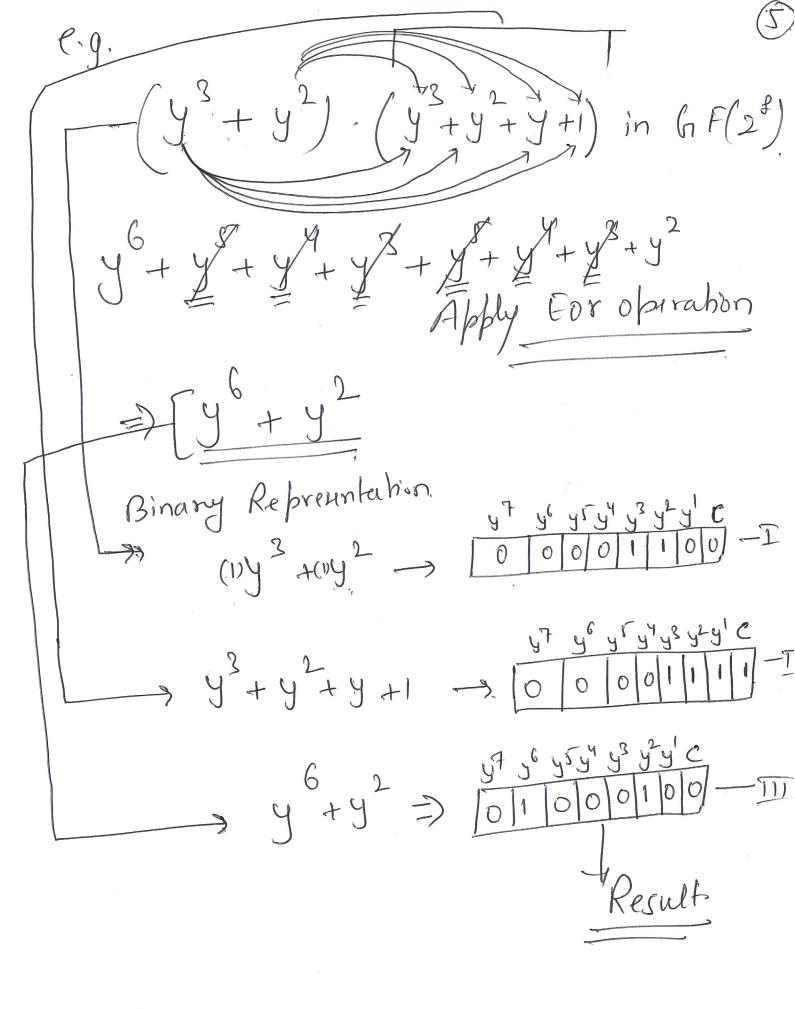
Note: This is again very usuful operation in AES

Another Note: - when you apply GF in poly nomial multiplication, then we need to do one extra step.



Ex. We have two polynomials  $A(Y) G B(Y) \text{ in } GF(2^{f})$   $A(Y) = A(Y) \cdot B(Y) \text{ mod } P(Y)$ 

-> Remainder of the divisi



Ex(ii). 
$$A(y) = (y^4 + y^2) - I$$
  
 $B(y) = (y^6 + y) - II$   
 $= (y^4 + y^2) * (y^6 + y)$   
 $= (y^4 + y^2) + y^3$   
 $= (y^4 + y^4) + y^4$   
 $= (y^4 + y^4) + y^4$