# Review of Algebra:-

- Polynomials
- Addition & Multiplication of Polynomials.

**What are Polynomials!** An expression that consisting of variables & coefficients, involves only operations of $+, -, \times$ and non-negative interger exponents of variables.

Ex. (i) $3x^2 + 4x + 7$ → Degree 2

(ii) $4y^3 + 2y^2 + 1$ → Degree 3

(iii) $3x^2 - 4x^{-1} + 1$ → not a polynomial

## Addition:

(i) $(2y^2 + 5y + 1) + (2y^2 + 5y + 3)$

$\Rightarrow \boxed{4y^2 + 10y + 4}$

## Multiplication:

(i) $(3y + 2) * (5y - 2) = 15y^2 + 4y - 4$ Ans:-

Galois field (GF) : $GF(2^8)$ → no. of elements

**Def.** : $GF(2^8)$ consists of polynomials that hav
degree 7 or less, with coefficient of 0 and 1

e.g. (i) $(1)y^6 + (1)y^2 + 1 \in GF(2^8)$

$(1)$ → coefficient

---

Application of $GF(2^8)$ in AES

- used to represent the possible elements of every byte. in AES

---

How every byte can be represented as a polynomial using $GF(2^8)$.

e.g. (i)

| $y_7$ | $y_6$ | $y_5$ | $y_4$ | $y_3$ | $y_2$ | $y_1$ | $C_0$ |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |

$(01101001)$

$y^6 + y^5 + y^3 + 1 \in GF(2^8)$

Every posit
represents the
coefficient of
power $y$.

You can also get back the byte.

| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
|---|---|---|---|---|---|---|---|
| $y^7$ | $y^6$ | $y^5$ | $y^4$ | $y^3$ | $y^2$ | $y^1$ | $C_0$ |

We can say that

**GF($2^8$) can contain all possible bytes.**

---

## Few operations in GF($2^8$)

**Addition:** GF makes use of (XOR) for the addition

ex (i) $y^6 + y^3 + y^1 + 1$ — I

$y^4 + y^3 + y^1$ — II

+ (do XOR operation)

$y^6 + y^4 + 1$

(ii) $y^7 + y^4 + y^2 + 1$ — I

$y^6 + y^4 + y^2 + 1$ — II

+ ( XOR)

$y^7 + y^6$ $\in$ GF($2^8$)

(iii) $y^5 + y^3 + 1$ — I

$y^5 + y^4 + y^2 + 1$ — II

[DIY]

# Multiplication in GF($2^8$)

Note: This is a very useful operation in AES

Another Note :- When you apply GF in polynomial multiplication, then we need to do one extra step.

i.e

$$P(Y) = Y^8 + Y^4 + Y^3 + Y + 1$$

→ This is the part of AES standard

Very useful equation

Ex. We have two polynomials $A(Y)$ & $B(Y)$ in GF($2^8$)

$$C(Y) = A(Y) \cdot B(Y) \bmod P(Y)$$

→ Remainder of the divisi

e.g.

$$(y^3 + y^2) \cdot (y^3 + y^2 + y + 1) \text{ in } GF(2^8)$$

$$y^6 + y^8 + y^4 + y^3 + y^8 + y^4 + y^3 + y^2$$

Apply Ex-or operation

$$\Rightarrow y^6 + y^2$$

Binary Representation

$(1)y^3 + (1)y^2 \rightarrow$

| $y^7$ | $y^6$ | $y^5$ | $y^4$ | $y^3$ | $y^2$ | $y^1$ | C |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |

— I

$y^3 + y^2 + y + 1 \rightarrow$

| $y^7$ | $y^6$ | $y^5$ | $y^4$ | $y^3$ | $y^2$ | $y^1$ | C |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |

— II

$y^6 + y^2 \Rightarrow$

| $y^7$ | $y^6$ | $y^5$ | $y^4$ | $y^3$ | $y^2$ | $y^1$ | C |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |

— III

Result

Ex (iii) $A(y) = (y^4 + y^2)$ — I

$B(y) = (y^6 + y)$ — II.

$= (y^4 + y^2) * (y^6 + y)$

$= y^{10} + y^5 + y^8 + y^3$

$\Rightarrow y^{10} + y^8 + y^5 + y^3 \in GF(2^8)$

not

Recall $P(y) = y^8 + y^4 + y^3 + y + 1$

$y^8 \leftrightarrow y^4 + y^3 + y + 1$

$= \underset{①}{y^{10}} + \underset{②}{y^8} + y^5 + y^3$

$y^{10} = y^2 \cdot y^8$

$\longrightarrow$ Replace $y^8$ with $y^4+y^3+y+1$

$\Rightarrow y^2 \cdot (y^4+y^3+y+1)$

$y^{10} \Rightarrow y^6+y^5+y^3+y^2 \in GF(2^8)$

$y^8$ = Replace with $y^4+y^3+y+1$

$= y^6 + y^5 + y^3 + y^2 + y^4 + y^3 + y + 1 + y^5 + y$

Recal EXOR

$$y^6+y^4+y^3+y^2+y+1$$

Byte Representation

| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|