* Galois Field

$A(x) = a_2 x^2 + a_1 x + a_0$

We will focus on $GF(2^3)$.

Element of $GF(2^3) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$

a_2	a_1	a_0	$A(x)$
0	0	0	$= 0$
0	0	1	$= 1$
0	1	0	$= x$
0	1	1	$= x+1$
1	0	0	$= x^2$
1	0	1	$= x^2+1$
1	1	0	$= x^2+x$
1	1	1	$= x^2+x+1$

Addition

Ex-1

$A(x) = x^7 + x^6 + x^4 + x$

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

$A(x) + B(x) = x^7 + x^6 + x^4(1+1) + x^2 + (1+1)$

$= \boxed{x^7 + x^6 + x^2}$

* We need to do $\boxed{\text{mod } 2}$ in every step. $(1+1) \bmod 2 = 0$

Ex-2

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

$B(x) = x^2 + 1$.

$A(x) + B(x) = x^2(1+1) + x + (1+1)$

$= \boxed{x}$

** The element/result should be in set.

Multiplication

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

$B(x) = x^2 + 1$.

$A(x) \cdot B(x) = (x^2+x+1) \cdot (x^2+1)$

$= x^4 + x^3 + \underline{x^2 + x^2} + x + 1$

$= \boxed{x^4 + x^3 + x + 1}$

But it is not in the Set.

we need to use another polynomial as modular variable. (irreduceable polynomial).

for. $\boxed{GF(2^3) = x^3 + x + 1} = P(x)$

$GF(2^8) = x^8 + x^4 + x^3 + x + 1$. (AES)

A.B	P(x)	
$(\cancel{x^4} + x^3 + \cancel{x} + 1)$	$(x^3 + x + 1)$	$= x + 1$

$$
\begin{array}{l}
\cancel{x^4} + \cancel{x^2} + x^2 + \cancel{x} \quad (\times x) \\
\hline
\cancel{x^3} + x^2 + \cancel{1} \\
\cancel{x^3} + x + \cancel{1} \quad (\times 1) \\
\hline
\boxed{x^2 + x}
\end{array}
$$

This is the answer of $A(x) \cdot B(x)$ as it is present in the Set.

* Inverse

Suppose, $c(x) = \boxed{x^5 + x^4 + x + 1}$

we need to find $c^{-1}(x)$.

To calculate the inverse, we need to find,

$$c(x) \cdot \underbrace{c^{-1}(x)}_{??} = 1 \bmod p(x).$$

But we can find the inverse from $\boxed{\text{table } 4{\cdot}2}$ (P-99).

$c(x) = x^5 + x^4 + x + 1 = 0011\ 0011 = 33)_8$.

from table 4·2,

$33 \rightarrow 6C$.

So, $c^{-1}(x) = 6C = 0110\ 1100$

$= \boxed{x^6 + x^5 + x^3 + x^2}$

Finally, Inverse of $(x^5 + x^4 + x + 1) = x^6 + x^5 + x^3 + x^2$