군, 환, 체, 유한체, 다항식

목차

도입: 한 개 연산(덧셈)이 가능한 집합

정수집합 $\mathbb{Z}$와 덧셈 연산 $+$

$\mathbb{Z}$의 임의의 두 원소 a, b에 대해 덧셈 연산을 수행한 결과 $a+b$는 $\mathbb{Z}$에 속함 (**덧셈에 대해 닫혀 있음**)

$3 + x = 5$
$(-3) + 3 + x = (-3) + 5$ **(덧셈의 역원)**
$0 + x = 2$ **(덧셈의 항등원 0)**
$x = 2$

$x + 2 + 1 = 5$
$(x + 2) + 1 = 5$
$x + (2 + 1) = 5$ **(덧셈 결합법칙)**
$x + 3 = 5$

$2 + x + 1 = 5$
$2 + 1 + x = 5$ **(덧셈 교환법칙)**
$(2 + 1) + x = 5$
$3 + x = 5$

군(group)
연산이 정의된 집합이 다음 성질들을 만족하면 군이라 함
① 닫혀 있음
② 항등원 존재
③ 집합 내 모든 원소에 대해 역원 존재
④ 결합법칙 성립

가환군(아벨군)
연산이 정의된 집합이 다음 성질들을 만족하면 가환군이라 함
① 닫혀 있음
② 항등원 존재
③ 집합 내 모든 원소에 대해 역원 존재
④ 결합법칙 성립
⑤ **교환법칙** 성립

도입: 두 개 연산(덧셈, 곱셈)이 가능한 집합

실수집합 R과 덧셈 연산 $+$, 곱셈 연산 $\times$

R의 임의의 두 원소 a, b에 대해 덧셈 연산을 수행한 결과 $a+b$는 R에 속함 (**덧셈에 대해 닫혀 있음**)
R의 임의의 두 원소 a, b에 대해 곱셈 연산을 수행한 결과 $a \times b$는 R에 속함 (**곱셈에 대해 닫혀 있음**)

$(5 \times (2 + x) + 1) \times 2 = 42$
$(\mathbf{5 \times 2} + \mathbf{5 \times x} + 1) \times 2 = 42$ (**분배법칙**)
$(10 + 5 \times x + 1) \times 2 = 42$
$(\mathbf{5 \times x} + \mathbf{10} + 1) \times 2 = 42$ (**덧셈 교환법칙**)
$(5 \times x + (\mathbf{10 + 1})) \times 2 = 42$ (**덧셈 결합법칙**)
$(5 \times x + 11) \times 2 = 42$
$\mathbf{5 \times x \times 2} + \mathbf{11 \times 2} = 42$ (**분배법칙**)
$5 \times (\mathbf{x \times 2}) + 11 \times 2 = 42$ (**곱셈 결합법칙**)
$5 \times (\mathbf{2 \times x}) + 11 \times 2 = 42$ (**곱셈 교환법칙**)
$10 \times x + 22 = 42$
$10 \times x + \mathbf{22} + (\mathbf{-22}) = 42 + (-22)$ (**덧셈 역원**)
$10 \times x + \mathbf{0} = 20$ (**덧셈 항등원 0**)
$10 \times x = 20$
$\frac{1}{\mathbf{10}} \times \mathbf{10} \times x = \frac{1}{10} \times 20$ (**곱셈 역원**)
$\mathbf{1} \times x = \frac{1}{10} \times 20$ (**곱셈 항등원 1**)
$x = 2$

체 (field)
2개 연산이 정의된 집합이 다음 성질들을 만족하면 체라 함

① 첫번째 연산에 대해 닫혀 있음
② 첫번째 연산에 대해 항등원 존재
③ 첫번째 연산에 대해 집합 내 모든 원소의 역원 존재
④ 첫번째 연산에 대해 결합법칙 성립
⑤ 첫번째 연산에 대해 교환법칙 성립

⑥ 두번째 연산에 대해 닫혀 있음
⑦ 두번째 연산에 대해 항등원 존재
⑧ 두번째 연산에 대해 첫번째 연산의 항등원을 제외한 집합 내 모든 원소의 역원 존재
⑨ 두번째 연산에 대해 결합법칙 성립
⑩ 두번째 연산에 대해 교환법칙 성립

⑪ 2개 연산에 대해 분배법칙 성립

대수적 구조

- 대수적 구조(algebraic structures)
  - 연산(operation)이 정의된 집합(set)
  - 군(group), 환(ring), 체(field)
- 군 (Group)
  - 다음 성질을 만족하는 하나의 연산(예: 덧셈)이 정의된 집합
    - 닫혀 있음, 결합법칙 성립, 항등원 존재, 모든 원소의 역원 존재
  - 아벨군
    - 교환법칙까지 성립하는 군
  - 예) $(Z, +)$, $(Z_n, +)$, $(Z_n^*, \times)$
- 환 (Ring)
  - 다음 성질을 만족하는 두 개 연산이 정의된 집합
    - 첫 번째 연산(예: 덧셈)에 대해 닫혀 있음, 결합법칙 성립, 항등원 존재, 모든 원소의 역원 존재, 교환법칙 성립
    - 두 번째 연산(예: 곱셈)에 대해 닫혀 있음, 결합법칙 성립
    - 두 연산에 대해 분배법칙 성립
  - 예) $(Z, +, \times)$, $(Z_n, +, \times)$
- 체 (Field)
  - 다음 성질을 만족하는 두 개 연산이 정의된 집합
    - 첫 번째 연산(예: 덧셈)에 대해 닫혀 있음, 결합법칙 성립, 항등원 존재, 모든 원소의 역원 존재 , 교환법칙 성립
    - 두 번째 연산(예: 곱셈)에 대해 닫혀 있음, 결합법칙 성립, 항등원 존재, 첫 번째 연산의 항등원을 제외한 모든 원소의 역원 존재 , 교환법칙 성립
    - 두 연산에 대해 분배법칙 성립
  - 예) $(Q,\ +,\ \times)$, $(R,\ +,\ \times)$, $(Z_p,\ +,\ \times)$

군 (Group)

군 (Group)
- 다음 4개 성질을 만족하는 이항연산 $\bullet$이 정의된 집합을 군(Group)이라고 함

① 닫혀 있음(Closure) → $\forall\, a, b \in G$ 에 대해 $a \bullet b \in G$
② 결합법칙(Associativity) 성립 → $\forall\, a, b, c \in G$ 에 대해 $(a \bullet b) \bullet c = a \bullet (b \bullet c)$
③ 항등원(Identity) 존재 → $\forall\, a \in G$ 에 대해 $a \bullet e = e \bullet a$인 $e \in G$가 존재
④ 모든 원소의 역원(Inverse) 존재 → $\forall\, a \in G$ 에 대해 $a \bullet x = x \bullet a = e$인 $x \in G$가 존재
→ 연산이 덧셈인 군의 경우 덧셈, 뺄셈이 가능 (뺄셈은 덧셈의 역원과의 덧셈으로 해석)
→ 연산이 곱셈인 군의 경우 뺄셈, 나눗셈이 가능 (나눗셈은 곱셈의 역원과의 곱셈으로 해석)

가환군 (Commutative group, abelian group)
- 위 4개 성질 뿐 아니라 아래 교환법칙까지 성립하는 군을 가환군 혹은 아벨군이라고 함

⑤ 교환법칙(Commutativity) 성립 → $\forall\, a, b \in G$ 에 대해 $a \bullet b = b \bullet a$

유한군 (finite group) vs. 무한군 (infinite group)
- 원소의 개수가 유한한 군을 유한군이라 하며, 무한한 경우 무한군이라 함

덧셈군 (additive group) vs. 곱셈군 (multiplicative group)
- 덧셈 연산이 정의된 군을 덧셈군이라 하며, 곱셈 연산이 정의된 군을 곱셈군이라 함

$(Z_4, +)$는 가환군이다
$Z_4 = \{0,1,2,3\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(Z_4, \times)$는 군이 아니다
$Z_4 = \{0,1,2,3\}$

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$(Z_4, +)$는 덧셈군이다. $Z_4 = \{0, 1, 2, 3\}$
- 항등원 0, 닫혀 있으며 결합법칙 성립
- 역원 존재: 0의 역원은 0, 1의 역원은 3, 2의 역원은 2, 3의 역원은 1

$(Z_4, \times)$는 군이 아니다. $Z_4 = \{0,1,2,3\}$
- 항등원 1
- 0과 2(4의 약수)의 역원 존재하지 않음

$(Z_4^*, \times)$는 곱셈군이다. $Z_4^* = \{1, 3\}$
- 항등원 1, 닫혀 있으며 결합법칙 성립
- 역원 존재: 1의 역원은 1, 3의 역원은 3

- 정수 집합 Z와, 유리수 집합 Q, 실수 집합 R은 모두 덧셈 연산 $+$에 대해 군이다
- Z, Q, R은 모두 곱셈 연산 $\times$에 대해 군이 아니다 → 0의 역원이 존재하지 않음
- $(Z_n, +)$는 가환군이다

환 (Ring)

환 (Ring)
- 다음 성질들을 만족하는 서로 다른 두 연산 $+$, $\times$ 이 정의된 집합을 환이라 함

① 첫번째 연산 $+$에 대해 가환군이다
② 두번째 연산 $\times$에 대해 닫혀 있으며, 결합법칙 성립
③ 두 연산에 대해 분배법칙 성립 → $\forall a, b, c \in G$ 에 대해 $a \times (b + c) = a \times b + a \times c$, $(a + b) \times c = a \times c + b \times c$
→ 첫번째, 두번째 연산이 각각 덧셈, 곱셈인 환의 경우 덧셈, 뺄셈, 곱셈은 가능하나 나눗셈은 불가

가환환 (Commutative group)
- 환의 두번째 연산에 대해 아래 교환법칙까지 성립하는 환을 가환환이라고 함
- 교환법칙(Commutativity) 성립 → $\forall a, b \in G$ 에 대해 $a \times b = b \times a$

- Z, Q, R은 모두 덧셈, 곱셈 연산에 대해 가환환이다
- $(Z_n, +, \times)$는 가환환이다

체 (Field)

체 (Field)
- 다음 성질들을 만족하는 서로 다른 두 연산이 정의된 집합을 체라 함

① 첫번째 연산에 대해 가환군이다(닫혀 있음, 결합법칙 성립, 항등원 존재, 모든 원소의 역원 존재, 교환법칙 성립)
② 두번째 연산에 대해 닫혀 있음, 결합법칙 성립, 항등원 존재, 첫번째 연산의 항등원을 제외한 모든 원소의 역원 존재, 교환법칙 성립
③ 두 연산에 대해 분배법칙 성립

→ 첫번째, 두번째 연산이 각각 덧셈, 곱셈인 체의 경우 덧셈, 뺄셈, 곱셈, 나눗셈(0으로 나누기는 제외) 가능

유한체 (Finite field)
- 원소의 개수가 유한한 체를 유한체라 함

갈루아체 (Galois field)
- 소수 p, 양의 정수 n에 대해 원소의 개수가 p^n인 체가 존재하며 이 유한체를 갈루아체(Galois field)라고 부르며 $GF(p^n)$으로 표기

- $(Q, +, \times)$는 체이다
- $(R, +, \times)$는 체이다
- 소수 p에 대해 $(Z_p, +, \times)$는 체이다

갈루아체 $GF(p), GF(p^n)$

$GF(p)$

- 소수 p에 대해 $GF(p)$는 덧셈과 곱셈의 두 연산이 정의된 집합 $Z_p = \{0, 1, \dots, p-1\}$일 수 있음
- 이 집합은 체이므로 덧셈의 역원이 존재하며, 0이 아닌 원소에 대해 곱셈의 역원이 존재함

$GF(2)$의 예 $(\{0,1\}, +, \times)$

- 집합은 0과 1의 두 개 원소만 가짐
- 덧셈, 뺄셈은 동일하며 0과 1에 대한 XOR 연산임
- 곱셈, 나눗셈은 동일하며 0과 1에 대한 AND 연산임

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

a	0	1
$-a$	0	1

a	0	1
a^{-1}		1

$GF(5)$의 예 $(\{0,1,2,3,4\}, +, \times)$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

a	0	1	2	3	4
$-a$	0	4	3	2	1

a	0	1	2	3	4
a^{-1}		1	3	2	4

암호학에서의 수의 집합과 연산

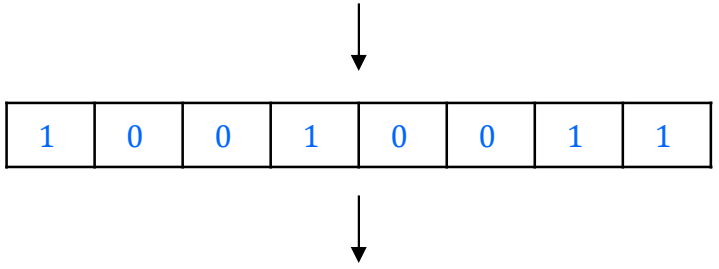
암호학에서의 수의 집합과 연산

- 암호학에서는 덧셈, 뺄셈, 곱셈, 나눗셈의 네 가지 연산 사용이 필요한 경우가 있음(즉 field 필요)
- 컴퓨터에서 양의 정수들은 n 비트 워드 단위로 처리됨(대부분의 경우 n의 값은 $8, 16, 32, 64$이며 정수 범위는 $0 \sim 2^n - 1$)
- 두 가지 가능한 field 사용법

① n 비트 워드의 경우, 2^n보다 작은 가장 큰 소수 p를 이용하여 Z_p에서 정의된 $GF(p)$를 사용 → $n = 8$인 경우 Z_{251}에서 정의된 $GF(251)$을 사용할 수 있으나 (251은 $256(= 2^8)$보다 적은 가장 큰 소수임), 251~255 범위 정수를 사용하지 못하는 단점 존재

② 원소의 개수가 2^n인 $GF(2^n)$를 사용 → $n = 8$인 경우, 모든 가능한 8 비트 비트열들의 집합 $\{00000000, 00000001, \dots, 11111111\}$을 사용할 수 있으나 이 집합의 원소를 정수로 생각하여 $Z_{256} = \{0, 1, \dots, 255\}$와 같은 집합으로 다룰 수는 없음. 즉 집합 $\{00000000, 00000001, \dots, 11111111\}$에 대해 체(field)의 성질을 만족하도록 두 개의 연산(덧셈, 곱셈)을 새롭게 정의해야 함 → 뒤에 설명되겠지만 $\{00000000, 00000001, \dots, 11111111\}$ 내 각 원소를 7차 다항식(표현)으로 해석하여 다항식들 간 덧셈, 곱셈을 정의함

$\{00000000, 00000001, \dots, 10010011, \dots, 11111111\}$

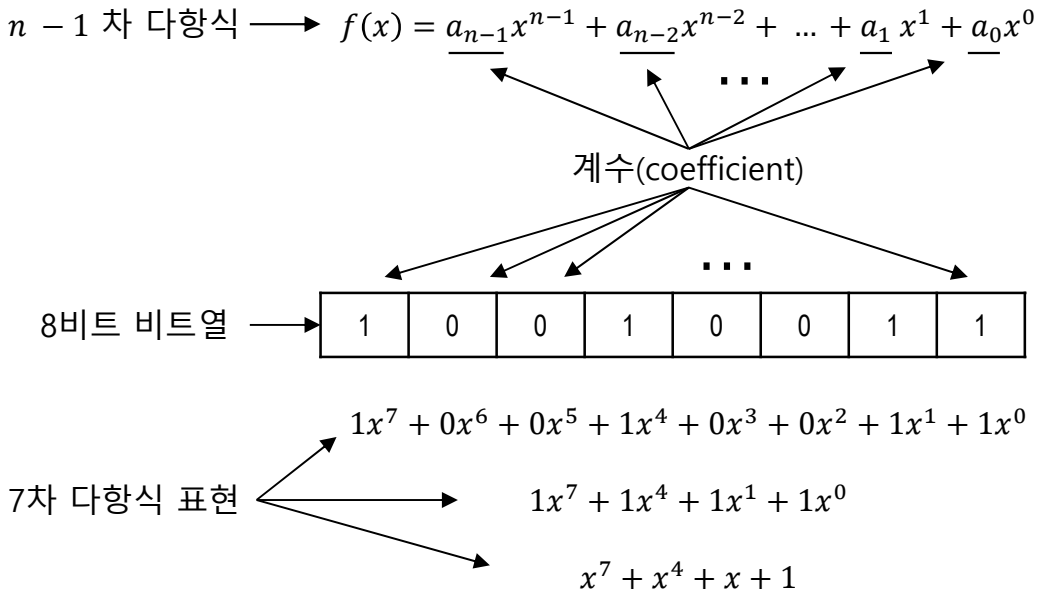


$1x^7 + 0x^6 + 0x^5 + 1x^4 + 0x^3 + 0x^2 + 1x^1 + 1x^0$

다항식

다항식 (polynomials)

- n 비트로 표현 가능한 모든 2^n 개 비트열들에 대해 덧셈, 뺄셈, 곱셈, 나눗셈을 자유롭게 수행하는 방법 필요
- n 비트 비트열에 대응하는 $n-1$ 차 다항식 표현을 정의하고 $n-1$ 차 다항식들 간 덧셈, 곱셈 방법을 새롭게 정의
- $n-1$ 차 다항식 $f(x)$ 에서 x^i은 n 비트 비트열 내 비트의 위치를 정의하며, x^i 항(term)의 계수(coefficient)는 비트의 값을 정의



다항식 연산

다항식 연산

- 다항식 연산 → 계수에 대한 연산과 다항식에 대한 연산으로 구분
- 다항식의 계수는 비트 값 0, 1을 가지므로 GF(2)를 사용하여 계수 연산 수행
- 두 다항식에 대한 연산을 위해 GF(2^n)을 사용. GF(2^n)의 원소는 n 비트 비트열에 대응하는 2^n 개 다항식들에 해당
- 두 다항식 덧셈은 동일 차수 항들의 계수 덧셈 수행. 덧셈 결과는 GF(2^n)에서 정의되는 집합의 범위를 벗어나지 않음
- 두 다항식 곱셈에서 n 차 이상 다항식이 생성되는 경우 소수다항식(prime polynomial)로 나눈 나머지를 그 결과로 취함
- n 차 prime polynomial은 n 보다 작은 차수의 다항식들로 나누어지지 않는 다항식으로 기약다항식(irreducible polynomial)이라고도 함
- n 차 prime polynomial은 하나 이상일 수 있으며 8차의 경우 prime polynomial의 한 예는 $x^8 + x^4 + x^3 + x + 1$
- 8비트 다항식 덧셈의 항등원 00000000, 8비트 다항식 곱셈의 항등원 00000001

다항식 덧셈 (동일 차수 항들의 계수 덧셈)

$$
\begin{array}{ll}
 & 0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0 \\
\oplus & 0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 \\
\hline
 & 0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0
\end{array}
$$

다항식 곱셈 (irreducible polynomial: $x^8 + x^4 + x^3 + x + 1$)

$$
\begin{aligned}
 & (x^5 + x^2 + x) \otimes (x^7 + x^4 + x^3 + x^2 + x) \\
= \; & x^5(x^7 + x^4 + x^3 + x^2 + x) + x^2(x^7 + x^4 + x^3 + x^2 + x) + x(x^7 + x^4 + x^3 + x^2 + x) \\
= \; & (x^{12} + x^9 + x^8 + x^7 + x^6) + (x^9 + x^6 + x^5 + x^4 + x^3) + (x^8 + x^5 + x^4 + x^3 + x^2) \\
= \; & x^{12} + x^7 + x^2
\end{aligned}
$$

$$
\left((x^5 + x^2 + x) \otimes (x^7 + x^4 + x^3 + x^2 + x)\right) mod\ (x^8 + x^4 + x^3 + x + 1) = x^5 + x^3 + x^2 + x + 1
$$

$$
\begin{array}{r|l}
 & x^4 + 1 \\
\hline
x^8 + x^4 + x^3 + x + 1 & x^{12} + x^7 + x^2 \\
 & x^{12} + x^8 + x^7 + x^5 + x^4 \\
\hline
 & x^8 + x^5 + x^4 + x^2 \\
 & x^8 + x^4 + x^3 + x + 1 \\
\hline
 & x^5 + x^3 + x^2 + x + 1
\end{array}
$$

계산결과가 7차를 초과하므로 prime polynomial로 모듈로 연산 수행

다항식 연산: 역원

다항식 연산: 역원

- 덧셈의 역원 → 한 다항식의 덧셈의 역원은 그 다항식 자신과 동일 (다항식 $f(x)$에 대해 $f(x) + f(x) = 0$)
- 곱셈의 역원 → Irreducible polynomial $P(x)$에 대해, 다항식 $f(x)$의 곱셈의 역원은 다음 식을 만족하는 $f(x)^{-1}$이며 확장 유클리드 알고리즘을 통해 곱셈의 역원 계산 가능

$$f(x)^{-1} \cdot f(x) \equiv 1 \left(mod\ P(x)\right)$$

GF(2^8)에서 irreducible polynomial $P(x) = x^8 + x^4 + x^3 + x + 1$에 대해,
x^5의 곱셈의 역원은 $x^5 + x^4 + x^3 + x$
즉 $(x^5) \otimes (x^5 + x^4 + x^3 + x)\ mod\ (x^8 + x^4 + x^3 + x + 1) = 1$

q	r1	r2	r	t1	t2	t
x^3	$x^8 + x^4 + x^3 + x + 1$	x^5	$x^4 + x^3 + x + 1$	0	1	x^3
$x + 1$	x^5	$x^4 + x^3 + x + 1$	$x^3 + x^2 + 1$	1	x^3	$x^4 + x^3 + 1$
x	$x^4 + x^3 + x + 1$	$x^3 + x^2 + 1$	1	x^3	$x^4 + x^3 + 1$	$x^5 + x^4 + x^3 + x$
$x^3 + x^2 + 1$	$x^3 + x^2 + 1$	1	0	$x^4 + x^3 + 1$	$x^5 + x^4 + x^3 + x$	0
	1	0		$x^5 + x^4 + x^3 + x$	0	

다항식 연산: 효율적 곱셈

다항식 곱셈 계산 $(x^5 + x^2 + x) \otimes (x^7 + x^4 + x^3 + x^2 + x)$

$x \otimes (x^7 + x^4 + x^3 + x^2 + x) = (x^8 + x^5 + x^4 + x^3 + x^2)$

$00000010 \otimes 10011110 = \mathbf{100111100}$

- 다항식 P에 다항식 x를 곱하는 것은 다항식 P의 비트열을 왼쪽으로 한 비트 쉬프트하는 것과 동일
- 다항식 P의 최상위 비트가 0인 경우 쉬프트만 수행
- 다항식 P의 최상위 비트가 1인 경우(즉 7차 다항식), 쉬프트 결과는 8차 다항식이 되므로 모듈러 연산 적용 필요

$$
\begin{array}{r|l}
 & 1 \\
\hline
x^8 + x^4 + x^3 + x + 1 & x^8 + x^5 + x^4 + x^3 + x^2 \\
 & x^8 + x^4 + x^3 + x + 1 \\
\hline
 & x^5 + x^2 + x + 1
\end{array}
$$

$$
\begin{array}{r|l}
 & 1 \\
\hline
100011011 & 100111100 \\
 & 100011011 \\
\hline
 & \mathbf{0}00100111
\end{array}
$$

			나눗셈
$x^0 \otimes (x^7 + x^4 + x^3 + x^2 + x)$		$x^7 + x^4 + x^3 + x^2 + x$	X
$x^1 \otimes (x^7 + x^4 + x^3 + x^2 + x)$	$x \otimes (x^7 + x^4 + x^3 + x^2 + x)$	$x^5 + x^2 + x + 1$	O
$x^2 \otimes (x^7 + x^4 + x^3 + x^2 + x)$	$x \otimes (x^5 + x^2 + x + 1)$	$x^6 + x^3 + x^2 + x$	X
$x^3 \otimes (x^7 + x^4 + x^3 + x^2 + x)$	$x \otimes (x^6 + x^3 + x^2 + x)$	$x^7 + x^4 + x^3 + x^2$	X
$x^4 \otimes (x^7 + x^4 + x^3 + x^2 + x)$	$x \otimes (x^7 + x^4 + x^3 + x^2)$	$x^5 + x + 1$	O
$x^5 \otimes (x^7 + x^4 + x^3 + x^2 + x)$	$x \otimes (x^5 + x + 1)$	$x^6 + x^2 + x$	X

- 8차 다항식 P를 8차 prime polynomial로 나눈 나머지은 8차 다항식 P와 prime polynomial 각각의 비트열을 XOR한 결과와 동일하며 XOR 결과 비트열에서 (8차 항의 계수에 해당하는)최상위 비트는 **0**임. 즉 8차 다항식 P와 8차 prime polynomial을 둘 다 7차까지만 표현하여 XOR 수행하면 됨

$$
\begin{array}{rl}
 & 00111100 \\
\oplus & 00011011 \\
\hline
 & 00100111
\end{array}
$$

$(x^5 + x^2 + x) \otimes (x^7 + x^4 + x^3 + x^2 + x)$
$= (x^6 + x^2 + x) \oplus (x^6 + x^3 + x^2 + x) \oplus (x^5 + x^2 + x + 1)$
$= x^5 + x^3 + x^2 + x + 1$

다항식 연산: 효율적 곱셈

			나눗셈
$x^0 \otimes (x^7+x^4+x^3+x^2+x)$		$x^7+x^4+x^3+x^2+x$	X
$\boldsymbol{x^1} \otimes (x^7+x^4+x^3+x^2+x)$	$x \otimes (x^7+x^4+x^3+x^2+x)$	$\boldsymbol{x^5+x^2+x+1}$	O
$\boldsymbol{x^2} \otimes (x^7+x^4+x^3+x^2+x)$	$x \otimes (x^5+x^2+x+1)$	$\boldsymbol{x^6+x^3+x^2+x}$	X
$x^3 \otimes (x^7+x^4+x^3+x^2+x)$	$x \otimes (x^6+x^3+x^2+x)$	$x^7+x^4+x^3+x^2$	X
$x^4 \otimes (x^7+x^4+x^3+x^2+x)$	$x \otimes (x^7+x^4+x^3+x^2)$	x^5+x+1	O
$\boldsymbol{x^5} \otimes (x^7+x^4+x^3+x^2+x)$	$x \otimes (x^5+x+1)$	$\boldsymbol{x^6+x^2+x}$	X

		계산결과		
$x^0 \otimes (x^7+x^4+x^3+x^2+x)$		10011110		
$\boldsymbol{x^1} \otimes (x^7+x^4+x^3+x^2+x)$	00111100	00100111	(00111100) ⊕ (00011011) (00100111)	직전 계산결과의 MSB=1 → Shift, XOR
$\boldsymbol{x^2} \otimes (x^7+x^4+x^3+x^2+x)$	01001110	01001110		직전 계산결과의 MSB=0 → Shift
$x^3 \otimes (x^7+x^4+x^3+x^2+x)$	10011100	10011100		직전 계산결과의 MSB=0 → Shift
$x^4 \otimes (x^7+x^4+x^3+x^2+x)$	00111000	00100011	(00111000) ⊕ (00011011) (00100011)	직전 계산결과의 MSB=1 → Shift, XOR
$\boldsymbol{x^5} \otimes (x^7+x^4+x^3+x^2+x)$	01000110	01000110		직전 계산결과의 MSB=0 → Shift

$(x^5+x^2+x) \otimes (x^7+x^4+x^3+x^2+x)$
$= (\boldsymbol{x^6+x^2+x}) \oplus (\boldsymbol{x^6+x^3+x^2+x}) \oplus (\boldsymbol{x^5+x^2+x+1})$
$= (00100111) \oplus (01001110) \oplus (01000110) = 00101111$
$= x^5+x^3+x^2+x+1$

효율적 다항식 곱셈 알고리즘

- 직전 계산결과의 최상위비트가 0인 경우 → 직전 계산결과를 1 비트 왼쪽 쉬프트하여 현재 계산결과를 생성
- 직전 계산결과의 최상위비트가 1인 경우 → 직전 계산결과를 1 비트 왼쪽 쉬프트한 후 prime polynomial과 XOR한 결과를 현재 계산결과로 생성 (XOR의 두 피연산자 모두 8차 항의 계수가 1이므로 8차 항 무시하고 0~7차까지의 항들(즉 8비트 비트열)에 대해 XOR 수행하면 됨)

References

- Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill, 2008
- William Stallings, Cryptography and Network Security: Principles and Practice, Sixth Edition, Prentice Hall, 2014
- Christof Paar, Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010
- 김명환, 수리암호학개론, 2019
- 정민석, 암호수학, 경문사, 2017
- 최은미, 정수와 암호론, 북스힐, 2019
- 이민섭, 정수론과 암호론, 교우사, 2008