유한체

https://youtu.be/VB_cFPNabD4

유한체의 정의

유한체 연산 실습

유한체 파이썬 구현

유한체 정의

유한체의 성질

- **유한성 (finiteness)** : 원소의 개수가 유한
- **폐쇄성 (closure)** : 연소의 결과도 동일 집합의 원소
- **결합성 (associativity)** : a + (b + c) = (a + b) + c, a x (b x c) = (a x b) x c
- **교환성 (community)** : a + b = b + a , a x b = b x a
- **분산성 (distribution)** : a x (b + c) = a x b + a x c
- **항등원 존재 (identity)** : 각 요소 a 에 대해 덧셈 항등원과 곱셈 항등원 존재
- **역원 존재 (inverse)** : 각 요소 a 에 대해 덧셈과 곱셈 역원 존재, 단, 덧셈 항등원에 대한 곱셈 역원은 존재하지 않는다.

유한체 정의

- 수학에서의 유한체는 아래 성질을 만족하는 2개의 연산자 (+ , x)를 가진 집합이다.

체(Field) 란 원소들 간의 덧셈, 곱셈의 연산 결과가 다시 그 안에 있는 닫힘성을 갖는 대수적 구조를 말한다.

원소들이 집합을 이룰때, 덧셈과 곱셈 연산을 자유롭게 사용할 수 있다.(2개 연산자 사용)

집합의 각 원소가 0이 아닌 원소로 나눌 수 있는 대수적 구조이다. (곱셈 역원 존재)

즉, 0으로 나누는 것을 제외하고는, 사칙연산을 비교적 자유롭게 사용 가능한 대수적 구조이다.

유한체 정의

유한체의 특징

1. a와 b가 집합에 속해있으면, a + b와 a x b도 집합 안에 있다.(집합 위에 두 연산 +,x가 닫혀 있음.)
2. 집합에 0으로 표기하는 원소가 존재하고, 집합 내 다른 원소 a와 + 연산 결과는 a이다.(+ 연산에 대한 항등원 존재)
3. 집합에 1로 표기하는 원소가 존재하고 집합 내 다른 원소 a와 x 연산 결과는 a이다.(+ 연산에 대한 항등원 존재)
4. 집합의 원소 a와 + 연산 결과가 0이 되게 하는 원소 b가 역시 집합에 속해있고 이러한 b를 –a로 표기한다. (+ 연산에 대한 a의 역원 –a 존재)
5. 0이 아닌 집합의 원소 a에 대해 a x b = 1 이 되게 하는 원소 b가 역시 집합에 속해 있고 이러한 b를 a^{-1}로 표기한다 (x 연산에 대한 a의 역원 a^{-1} 존재)

유한체 정의

유한체의 성질

1번 성질

- 덧셈과 곱셈에 대하여 닫혀있다.

- 덧셈과 곱셈의 **연산 결과가 집합 안에 있도록 두 연산을 정의**해야한다.

- 원소가 { 0 , 1 , 2 } 인 집합이 있다고 가정 할 때, 덧셈에 대해 닫혀있지 않다.
- 1 + 2 = 3 이고, 3은 집합 안에 없기 때문
- 2 + 2 = 4 인 경우도 4가 집합 안에 없기 때문

- 반면 원소가 { 0 , 1, -1 }인 집합이 있다고 가정 할 때, 일반 곱셈에 대해 닫혀있다.
- 임의의 2개 원소의 곱셈 결과가 항상 집합 안에 존재하기 때문

- 수학에서 위 2개의 집합이 모두 **곱셈에 대하여 닫혀있도록 정의** 가능하다.

- 하지만 여기서 알아야할 중요한 개념은 **다른 방식으로 곱셈과 덧셈이 정의 가능**하다는 점이다.

유한체 정의

2번,3번 성질

- 덧셈과 곱셈에 대한 항등원이 **집합 내에 있다는 개념**이다.
- 이들은 각각 집합에서 0 과 1을 의미한다.

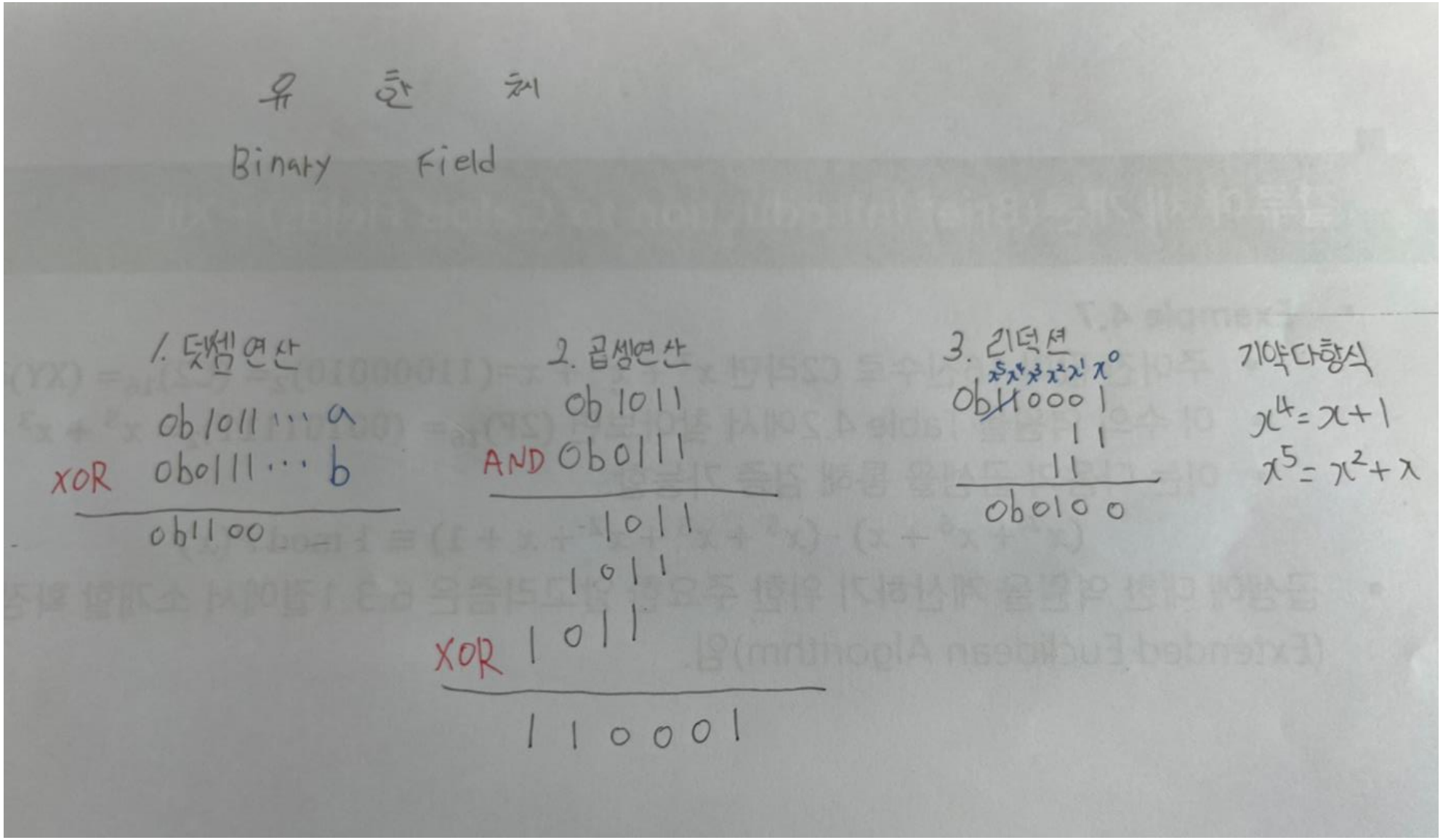
4번 성질

- 덧셈에 대한 역원이 **집합 내에 있다는 뜻**이다.
- 집합 내에 a가 존재 할 때 –a 또한 집합 내에 존재한다는 듯이다.
- 이는 **덧셈에 대한 역원을 사용하여 뺄셈 또한 정의가 가능하다는 것을 의미**한다.

5번 성질

- 곱셈에 대하여 4번과 똑같은 성질을 지닌다는 것을 의미한다.
- A가 집합 내에 존재할 때, a^{-1} 또한 집합 내에 존재할 수 있다는 것을 의미한다.
- 즉 a x a-1 = 1 이다.
- 이는 **곱셈에 대한 역원을 사용하여 나눗셈 또한 정의가 가능하다는 것을 의미**한다.

유한체 연산 실습


유 한 체
Binary Field
1. 덧셈연산
0b1011 ··· a
XOR 0b0111 ··· b
0b1100
2. 곱셈연산
0b1011
AND 0b0111
1011
1011
XOR 1011
110001
3. 리덕션
0b1000 1
11
11
0b0100
기약다항식
$x^4 = x + 1$
$x^5 = x^2 + x$

유한체 파이썬 구현

```python
def Add(a, b):
    d = a^b
    return d

def Mul(a,b,n):
    c = 0

    for i in range(n):
        if (b >> i & 1):
            c = c ^ (a << i)


    # if (b & 1):
    #     c = c ^ a
    #
    # if ((b >> 1) & 1):
    #     c = c ^ (a << 1)
    #
    # if ((b >> 2) & 1):
    #     c = c ^ (a << 2)
    #
    # if ((b >> 3) & 1):
    #     c = c ^ (a << 3)

    return c
```

```python
a = 0b1011
b = 0b0111
d = bin(Add(a,b))
c = bin(Mul(a,b,4))

print(d)
print(c)
```

```
C:\Users\82103\miniconda3\python.exe "C:\Users\82103\Desktop\새 폴더\rcr5 python\pyRC5-master\encrypt.py"
0b1100
0b110001

종료 코드 0(으)로 완료된 프로세스
```

Q & A