갈루아 체

IT융합공학부 권혁동

HANSUNG UNIVERSITY 한성대학교

CryptoCraft LAB
https://crypto.modoo.at

Contents

1. 대수적 연산
2. 군(Group)
3. 환(Ring)
4. 체(Field)
5. 갈루아 체(Galois Field)

CryptoCraft LAB

1. 대수적 연산

연산에 대해 닫혀있다(Closure)

- 특정 집합의 원소가 **연산 결과 자신의 집합**으로 항상 돌아올 경우
  - 자연수: 덧셈과 곱셈에 닫혀있다
  - 정수: 덧셈과 뺄셈 및 곱셈에 닫혀있다
  - 유리수: 덧셈과 뺄셈, 곱셈 및 나눗셈에 닫혀있다
  - 무리수: 덧셈과 뺄셈, 곱셈 및 나눗셈에 닫혀있다

- 정의: $a, b \in A$, $a \circ b \in A$이면 A는 $\circ$에 닫혀있다

1. 대수적 연산

교환법칙(Commutative)

- 특정 집합의 원소가 **연산 순서를 바꿔도 결과가 동일**함
  - 복소수: 덧셈, 곱셈에 대해 교환법칙이 성립

- 정의: $a, b \in A$, $a \circ b = b \circ a$이면 A는 $\circ$에 대해 교환법칙이 성립

1. 대수적 연산

결합법칙(Associative)

- 특정 집합의 세개 이상의 원소가 **인접 동일 연산끼리 순서를 바꿔도 결과가 동일**함
  - 복소수: 덧셈, 곱셈에 대해 결합법칙이 성립

- 정의: <u>$a, b, c \in A$, $a \circ (b \circ c) = (a \circ b) \circ c$이면 A는 $\circ$에 대해 결합법칙이 성립</u>

1. 대수적 연산

분배법칙(Distributive)

- 특정 집합의 원소가 **연산자를 분배해도 그 결과가 동일**함
  - 복소수: 곱셈에 대해 분배법칙이 성립
- 정의: a, b, c $\in$ A

  $a \circ (b + c) = (a \circ b) + (a \circ c)$ 좌분배법칙

  $(b + c) \circ a = (b \circ a) + (c \circ a)$ 우분배법칙

  <u>좌, 우분배법칙 성립시 A는 $\circ$에 대해 분배법칙이 성립</u>

1. 대수적 연산

항등원(Identity)

- 특정 집합의 수에 대해서 **연산 결과 동일한 수가 나오게 하는 수**
  - 덧셈에 대한 항등원: 0
  - 곱셈에 대한 항등원: 1

- 정의: a, b $\in$ A

  $a \circ b = b$ 왼쪽 항등원, $b \circ a = b$ 오른쪽 항등원

  <u>왼쪽, 오른쪽 항등원 성립시 A의 항등원은 a</u>

1. 대수적 연산

역원(Inverse)

- **항등원이 존재**할 때 특정 집합의 수에 대해서 **연산 결과 항등원이 나오게 하는 수**이며 교환법칙이 성립
  - 덧셈에 대한 역원: -n
  - 곱셈에 대한 역원: 1/n

- 정의: $a, b \in A$, e(항등원)

  <u>$a \circ b = b \circ a = e$가 성립할 때, A의 역원은 a</u>

2. 군(Group)

- 어떤 집합에 이진연산이 가능한 집합
  - 정수, 유리수, 실수, 복소수 상에서의 덧셈, 곱셈
  - 행렬의 곱셈
- 특성
  1. 연산에 대해 닫혀있다
  2. 결합법칙, 교환법칙 성립
  3. 항등원, 역원 존재
  - 교환법칙이 성립할때는 아벨리안 군(Abelian Group)으로 칭함

3. 환(Ring)

- 결합법칙이 성립하는 ○, ■ 이진연산이 있는 집합이 있을 때
  1. ○는 군을 만족함
  2. ■는 닫혀있고 교환, 결합법칙이 성립함
  3. ■는 ○에 분배법칙이 적용됨

- 이때 두 연산자에 대해 교환법칙이 모두 성립한다면 가환환 (Commutative Ring)

4. 체(Field)

- ○, ■ 이진연산이 있는 집합이 있을 때
  1. ○, ■은 군을 만족하며 ■는 ○에 분배법칙이 적용됨
  2. 단, ○의 항등원은 ■에 대해 역원을 갖지 못한다

대수적 구조	연산자 예시	정수 집합 예시
군	(+ -) 또는 (× ÷)	Z_n 또는 $Z_n{}^*$
환	(+ -) 그리고 (×)	Z
체	(+ -) 그리고 (× ÷)	Z_p

5. 갈루아 체(Galois Field)

- 체에서 유한개의 원소를 가지는 체(Finite Field)
  - q개의 원소를 가지는 유한체의 표현: GF(q)

- 특성
  1. 원소의 수가 항상 소수(p)의 거듭제곱($p^n=q$)
  2. 전영(0) 원소를 제외한 나머지 원소는 순환군을 이룸

- 컴퓨터 상에서는 2^n으로 원소의 수가 유한하므로 갈루아 체가 적용