대수학(Algebra) 기초

발표자: 양유진

링크: https://youtu.be/Rqh00OrgeJs

HSU 한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

1. 대수학

대수학(Algebra)

: 일련의 공리들을 만족하는 수학 구조들의 일반적인 성질을 연구하는 수학 분야

- 숫자를 대신해 문자를 사용하는 방법
- 방정식 푸는 방법을 연구하는 학문으로부터 시작되었음
- 해석학, 기하학, 위상수학 발전에 지대한 영향을 미쳤음

2. 군 이항연산 정의

이항연산(Binary operation)

: 두 개의 항 간에 이루어지는 연산 ex) 사칙연산

항1 ● **항2** **=** **결과**

$$*: S \times S \to S$$

집합 S 위에서 이항연산 $*$ 은 $S \times S \to S$ 인 함수

$$(a, b) \mapsto a * b$$

$a * b$ 는 $(a, b) \in S \times S$에 대응되는 S의 원소 $*\big((a, b)\big)$를 나타냄.

2. 군 군 정의

군(Group)

3가지 조건을 만족한 $< G,\ * >$

이항연산 $*$가 적용되는 집합 G

결합법칙 성립

- 세 원소 $a, b, c \in G$ 에 대해 $(a * b) * c = a * (b * c)$

항등원 존재

- 항등원: 처음수가 되도록 만들어주는 수. ex) 1+0=1, 0은 덧셈의 항등원 | 2*1=2, 1은 곱셈의 항등원
- G 의 임의의 원소 a 에 대해 $a * e = a = e * a$ 가 되는 $e \in G$가 존재함.

역원 존재

- 역원: 연산 결과 항등원이 나오게 하는 원소. ex) 10의 덧셈 역원은 -10, 곱셈 역원은 1/10
- G 의 임의의 원소 a 에 대해 $a * x = e = x * a$ 가 되는 $x \in G$가 존재함.

3. 환 환 정의

환(Rings)

3가지 조건을 만족한 $< \boldsymbol{R}, +, \ \cdot >$

2개의 이항연산 $+, \cdot$ 를 가지는 집합 R

집합 R에는 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 가 들어갈 수 있음.

$\cdot$ (곱셈)은 결합법칙 성립

- 세 원소 $a, b, c \in R$ 에 대해 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

분배법칙 성립

- 세 원소 $a, b, c \in R$ 에 대해 $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + \mathrm{b} \cdot c$

$< \boldsymbol{R}, + >$ 는 가환군(아벨군)

- 가환군: 임의의 원소 a, b에 대해 항상 $a * b = b * a$ (**교환법칙**)이 성립하는 군 $< G, \ * >$
- R은 연산 +에 대해 닫혀 있고, 결합법칙을 만족하며 연산에 대해 항등원과 역원이 존재(군의 조건)

※ 집합 H의 임의의 원소 a, b에 대하여 $\mathrm{a} * b \in H \Rightarrow$ "H 는 $*$ 에 대하여 닫혀 있다."

부분환(Subring)

환 R의 두 연산에 관하여 환을 이루는 부분집합 $S(\neq \emptyset)$

S는 덧셈군 $< R,+>$ 의 부분군

- $\forall a, b \in S \rightarrow a - b \in S$
- 부분환 S는 뺄셈에 대해 닫혀 있음.

S는 곱셈군 $< R,\cdot>$ 의 부분군

- $\forall a, b \in S \rightarrow ab \in S$
- 부분환 S는 곱셈에 대해 닫혀 있음.

3. 환 아이디얼 정의

아이디얼, 이데알(Ideal)

환 R의 특수한 부분집합(부분환) I $(I \subseteq R)$

왼쪽 아이디얼(left ideal)

- $\forall r \in R,\ \forall i \in I$ 에 대해 $ri \in I$ 성립하는 경우, I는 R의 왼쪽 아이디얼

오른쪽 아이디얼(right ideal)

- $\forall r \in R,\ \forall i \in I$ 에 대해 $ir \in I$ 성립하는 경우, I는 R의 오른쪽 아이디얼

양쪽 아이디얼(two-sided ideal)

- $\forall r \in R,\ \forall i \in I$ 에 대해 $ri, ir \in I$ 성립하는 경우, I는 R의 양쪽 아이디얼

3. 환 몫환 정의

몫환(quotient ring)

환 R을 양쪽 아이디얼인 집합 I로 나눈 환 (R/I)

몫환은 두 연산에 대해 환을 이룸

1) $(a+I)+(b+I) \coloneqq (a+b)+I$
2) $(a+I)\cdot(b+I) \coloneqq (ab)+I$

아이디얼에 속한 원소를 모두 0으로 간주하여 얻을 수 있음.

- 몫환의 영원(Zero)은 원소 $0+I$ (아이디얼 I 그 자체)

4. 체 체 정의

체(Field)

모든 원소들이 곱셈에 대한 역원을 가지는 단위원이 존재하는 가환환 $< \boldsymbol{F}, +, \cdot >$

- 가환환: 곱셈에 대해서 교환 법칙을 만족하는 환
- 코드(부호)를 기술하는 데 사용될 수 있음.

$< F, + >$

- 항등원 존재
- 모든 성분에 대해 덧셈 역원 존재
- 결합법칙, 교환법칙 성립

$< F, \cdot >$

- 모든 성분에 대해 분배법칙 성립

4. 체 유한체 정의

유한체, 갈루아체(Finite Field)

유한개(q개)의 원소만을 갖는 체 $\boldsymbol{GF(q)}$ 혹은 $\boldsymbol{F_q}$

덧셈 연산 (+)

+	0	1
0	0	1
1	1	0

XOR 연산과 같음

곱셈 연산 (x)

x	0	1
0	0	0
1	0	1

AND 연산과 같음

- q 개의 유한개 원소를 갖는 유한체
- F_2 : 2개의 유한개 원소 {0, 1}을 갖는 2진 유한체

- 부호화 이론, 암호학에 많이 응용됨

감사합니다