

기초 대수론

2003. 03. 25

목 차

- 군(Group)의 정의
- 환(Ring)의 정의
- 체(Field)의 정의

군(Group)의 정의

- $(G, *)$: 군

1) 결합 법칙 성립

$$a*(b*c) = (a*b)*c$$

2) 항등원 1의 존재

$$a*1 = 1*a = a$$

3) 역원 a^{-1} 의 존재

$$a*a^{-1} = a^{-1}*a = 1$$

- $(G, *)$: 군

$$G: \text{abelian} \Leftrightarrow a*b = b*a$$

군(Group)의 정의

- $(\mathbb{Z}_n, +)$
 - 1) 결합 법칙?
 - 2) 항등원은?
 - 3) a 의 역원은?
 - 4) abelian인가?
- $(\mathbb{Z}_n^*, \cdot)$
 - 1) 항등원은?
 - 2) a 의 역원은?
- $(\mathbb{Z}_n, \cdot)$ 는 군인가?

군(Group)의 정의

- 부분 군(Subgroup):

$(G, *)$: 군, H : G 의 부분 집합

$(H, *)$ 가 자체로 군이 되면

H 를 G 의 부분 군이라 부름.

- $(\mathbb{Z}_{16}, +)$ 에서

1) $\{ 0, 2, 4, 6, 8, 10, 12, 14 \}$

2) $\{ 0, 1, 3, 5, 7, 9, 11, 13, 15 \}$

군(Group)의 정의

- 군의 Order:

$|G|$: 군 G 의 원소의 개수

- Lagrange 정리:

G : 군, H : G 의 부분 군

$$\Rightarrow |H| \mid |G|$$

- $a \in G$,

$$\langle a \rangle = \{ a^i \mid 0 \leq i \leq |G| \}$$

군(Group)의 정의

- $|Z_{19}^*| = 18$

$$\langle 1 \rangle = \{ 1 \}$$

$$\langle 2 \rangle = \{ 1, 2, 4, 8, 16, 13, 5, 10, 9, 7, 3, 6 \}$$

$$\langle 4 \rangle = \{ 1, 4, 16, 13 \}$$

$$\langle 7 \rangle = \{ 1, 7, 18, 12, 15, 11 \}$$

$$\langle 18 \rangle = \{ 1, 18 \}$$

환(Ring)의 정의

- $(R, +, \cdot)$: 환

- 1) $(R, +)$: 항등원이 0인 abelian 군

- 2) 곱셈에 대한 결합 법칙

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

- 3) 곱셈에 대한 항등원 존재

$$1 \cdot a = a \cdot 1 = a$$

- 4) 배분 법칙

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

- $(R, +, \cdot)$: commutative ring $\Leftrightarrow a \cdot b = b \cdot a$

환(Ring)의 정의

• $(\mathbb{Z}, +, \cdot)$

1) $(\mathbb{Z}, +)$: abelian 군?

2) $+$ 에 대한 항등원은?

3) $\cdot$ 에 대한 결합 법칙 성립?

4) 곱셈에 대한 항등원은?

5) 배분 법칙 성립?

환(Ring)의 정의

• $(\mathbb{Z}_n, +, \cdot)$

1) $(\mathbb{Z}_n, +)$: abelian 군?

2) $+$ 에 대한 항등원은?

3) $\cdot$ 에 대한 결합 법칙 성립?

4) 곱셈에 대한 항등원은?

5) 배분 법칙 성립?

체(Field)의 정의

- $(F, +, \cdot)$: 체
 - 1) $(F, +, \cdot)$: commutative ring
 - 2) $a \in F, a \neq 0$ 에 대해서
$$a^{-1} \text{이 존재}$$
- $(\mathbb{Z}_p, +, \cdot)$
 - 1) $(\mathbb{Z}_p, +, \cdot)$: commutative ring
 - 2) 0 아닌 모든 원소는 역원이 있는가?
- $(\mathbb{R}, +, \cdot)$

체(Field)의 정의

- $\mathbb{Z}_p$ 에서

$$1 + 1 + \dots + 1 \stackrel{?}{=} 0$$

- $\mathbb{R}$ 에서

$$1 + 1 + \dots + 1 \stackrel{?}{=} 0$$

- Characteristic:

- 1을 더해서 0이 될 때 최소 반복 값을
체의 characteristic이라 함.
- 1을 계속 더해서 0이 되지 않을 때
체의 characteristic을 0이라 함.