현대대수학 이론 목차

Chapter 1 군(Group)

1.1 군의 정의와 예

정의 1.1 집합 $G(\neq \varnothing)$ 위에 이항연산 $*$이 정의되어 있고 임의의 원소 $a, b, c \in G$에 대하여 다음이 성립하면 $(G, *)$을 **군(group)**이라고 한다.

(1) $a * b \in G$

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

(3) 특정한 원소 $e \in G$가 존재하여, 모든 원소 $a \in G$에 대하여 등식 $a * e = a = e * a$가 성립한다.

(4) 각 $a \in G$에 대하여 $a * d = e = d * a$인 원소 $d \in G$가 존재한다. ($d = a^{-1}$로 표기한다.)

특별히 $a * b = b * a$을 만족하는 군을 **가환군(abelian group)**이라 한다.

정의 1.2 군 $(G, *)$에서

(1) G가 무한집합일 때 이 군을 **무한군(infinite group)**이라 하고,

(2) G가 유한집합일 때 이 군을 **유한군(finite group)**이라고 하며 $|G| = n$인 경우 n을 이 군의 **위수(order)**라고 한다.

예제 1.1

(1) 집합 $G = \{\pm 1, \pm i\}$에 곱셈 연산이 주어지면 군이 된다.

(2) $\mathbb{Q}^*$, $\mathbb{Q}^{**}$, $\mathbb{R}^*$, $\mathbb{R}^{**}$를

$$\mathbb{Q}^* = \mathbb{Q} - \{0\},\ \mathbb{Q}^{**} = \{x \in \mathbb{Q} \mid x > 0\}$$
$$\mathbb{R}^* = \mathbb{R} - \{0\},\ \mathbb{R}^{**} = \{x \in \mathbb{R} \mid x > 0\}$$

라 정의하면

$$(\mathbb{Z}, +),\ (\mathbb{Q}, +),\ (\mathbb{R}, +),\ (\mathbb{Q}^*, \times),\ (\mathbb{R}^*, \times),\ (\mathbb{Q}^{**}, \times),\ (\mathbb{R}^{**}, \times)$$

은 모두 군이 된다.

(3) 양의 정수에 곱셈 연산이 주어지면 군이 되지 않는다.

『풀이』

예제 1.2

$M_n(\mathbb{R})$, $GL_n(\mathbb{R})$, $SL_n(\mathbb{R})$을

$M_n(\mathbb{R})$: 실계수 $n\times n$ 행렬을 모두 모아 놓은 집합

$GL_n(\mathbb{R})=\{A\in M_n(\mathbb{R})\mid \det(A)\neq 0\}$

$SL_n(\mathbb{R})=\{A\in M_n(\mathbb{R})\mid \det(A)=1\}$

으로 정의 할 때, $(M_n(\mathbb{R}),+)$, $(GL_n(\mathbb{R}),\bullet)$, $(SL_n(\mathbb{R}),\bullet)$는 각각 군이 됨을 증명하여라.

『풀이』

예제 1.3

$\mathbf{1}=\begin{bmatrix}1&0\\0&1\end{bmatrix}, \boldsymbol{i}=\begin{bmatrix}i&0\\0&-i\end{bmatrix}, \boldsymbol{j}=\begin{bmatrix}0&1\\-1&0\end{bmatrix}, \boldsymbol{k}=\begin{bmatrix}0&i\\i&0\end{bmatrix}$에 대하여 $Q=\{\pm\mathbf{1},\pm\boldsymbol{i},\pm\boldsymbol{j},\pm\boldsymbol{k}\}$에 행렬의 곱셈연산이 주어지면 군이 된다. 이 군을 사원수군(quaternion group)이라 한다.

『풀이』

$\bullet$	1	-1	i	$-i$	j	$-j$	k	$-k$
1								
-1								
i								
$-i$								
j								
$-j$								
k								
$-k$								

예제 1.4

$(\mathbb{Z}_n, +)$은 군이 됨을 보여라.

『풀이』

예제 1.5

$\mathbb{Z}_n^* = \{[a]_n \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$에 대하여 $(\mathbb{Z}_n^*, \times)$은 군이 됨을 보여라.

『풀이』

예제 1.6

S_3는 합성 연산에 대하여 군이 됨을 보여라.

『풀이』

예제 1.7

D_4는 합성 연산에 대하여 군이 됨을 보여라.

『풀이』

집합 $\{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$의 임의의 원소 A, B에 대하여 연산 $\triangle$를
$$A \triangle B = (A \cup B) - (A \cap B)$$
로 정의할 때, $\triangle$에 대한 $\{1\}$의 역원을 구하시오. [1993]

『풀이』

다음 명제의 진위를 판정하고 이유를 설명하시오. [1994]
"모든 군에서 교환법칙이 성립한다."

『풀이』

정리 1.1 $(G, *), (H, \circ)$을 군이라 하자. $G \times H$의 연산 $\bullet$을
$$(g, h) \bullet (g', h') = (g * g', h \circ h')$$
이라 정의하면 $G \times H$는 군이다. 또한, G와 H가 가환군이면 $G \times H$는 가환군이고, G와 H가 유한군이면 $G \times H$는 유한군이며 $|G \times H| = |G||H|$이다.

『증명』

예제 1.8

(1) $\mathbb{Z} \times \mathbb{Z}_6$에서 $(3, 5) \bullet (7, 4)$, 항등원, $(7, 4)$의 역원을 구하여라.

(2) $\mathbb{R}^* \times D_4$에서 $(2, \rho) \bullet (9, \tau)$, 항등원, $(8, \rho^3)$의 역원을 구하여라.
(단, $\mathbb{R}^* = \mathbb{R} - \{0\}$는 곱셈 연산에 관한 군이다.)

『풀이』

1.2 군의 기본 정리

정리 1.2 군 G에서 임의의 원소 $a, b, c \in G$에 대하여 다음이 성립한다.
(1) G는 유일한 항등원을 갖는다.
(2) $ab = ac$이면 $b = c$이고, $ba = ca$이면 $b = c$이다.
(3) G의 각 원소는 유일한 역원을 갖는다.

『증명』

따름정리 1.3 군 G에서 임의의 원소 $a, b, c \in G$에 대하여 다음이 성립한다.
(1) $(ab)^{-1} = b^{-1}a^{-1}$
(2) $(a^{-1})^{-1} = a$

『증명』

군 G의 임의의 원소 g에 대하여 $g^{-1} = g$이면, G는 가환군임을 보이시오. [1999]

『풀이』

정의 1.3 곱셈군 G에서 임의의 원소 $a \in G$와 정수 n에 대하여 a^n을 다음과 같이 정의한다.

$$a^n = \begin{cases} a \cdots a & , n > 0 \\ e & , n = 0 \\ a^{-1} \cdots a^{-1} & , n < 0 \end{cases}$$

덧셈군 G에서 임의의 원소 $a \in G$와 정수 n에 대하여 na을 다음과 같이 정의한다.

$$na = \begin{cases} a + \cdots + a & , n > 0 \\ 0 & , n = 0 \\ (-a) + \cdots + (-a) & , n < 0 \end{cases}$$

정리 1.4 군 G에서 임의의 원소 $a \in G$와 정수 m, n에 대하여 다음이 성립한다.

(1) $a^m a^n = a^{m+n}$

(2) $(a^m)^n = a^{mn}$

『증명』

정의 1.4 군 G에서 원소 $a \in G$에 대하여

(1) $a^k = e$인 양의 정수 k가 존재하는 경우에 a를 **유한 위수(finite order)**를 가진 원소라 하고, $a^n = e$인 가장 작은 양의 정수 n을 a의 **위수(order)**라고 하며 $|a| = n$으로 나타낸다.

(2) 모든 양의 정수 k에 대하여 $a^k \neq e$일 때, a는 **무한 위수(infinite order)**를 가진 원소라고 한다.

예제 1.9

(1) S_3, D_4, Q의 원소의 위수를 모두 구하여라.

(2) $\mathbb{R}^*$에서 $1/2$은 무한 위수를 갖는다.

(3) 군 G에 대하여 항등원을 제외한 모든 원소의 위수가 2이면 가환군이다.

(4) 유한군의 원소는 모두 유한 위수를 갖는다.

(5) 모든 원소의 위수가 유한인 무한군이 존재한다. **(예제 1.33)**

『풀이』

정리 1.5 군 G에서 임의의 원소 $a \in G$에 대하여 다음이 성립한다.

(1) a가 무한 위수를 가지면 각각의 $k \in \mathbb{Z}$에 따라 a^k는 모두 다르다.

(2) $i \neq j$일 때, $a^i = a^j$이면 a는 유한 위수를 갖는다.

(3) a의 위수가 n일 때, $a^k = e \Leftrightarrow n \mid k$이고, $a^i = a^j \Leftrightarrow i \equiv j \pmod{n}$이다.

(4) $|a| = n$이면 $|a^m| = \dfrac{n}{\gcd(n, m)}$이다.

『증명』

예제 1.10

(1) $\mathbb{Z}_{24}$에서 20의 위수를 구하여라.

(2) $\mathbb{Z}_{16}\times\mathbb{Z}_{18}$의 원소 $(12, 15)$의 위수를 구하여라.

『풀이』

다음 명제의 진위를 판정하고 이유를 설명하시오. [2011]

"$G=\mathbb{Z}_{12}\times\mathbb{Z}_{7}$의 원소 $(3, 1)$의 위수(order)는 28이다."

『풀이』

예제 1.11

군 G의 원소 a, b에 대하여 다음이 성립함을 증명하여라.

$$|a|=|a^{-1}|,\ |b|=|aba^{-1}|,\ |ab|=|ba|$$

『풀이』

예제 1.12

군 G의 원소 a, b에 대하여 다음 물음에 답하여라.

(1) $ab = ba$이고 $|a|$와 $|b|$가 서로소이면 $|ab| = |a||b|$임을 증명하여라.

(2) $ab \neq ba$ 이거나 $|a|$와 $|b|$가 서로소가 아닌 경우 $|ab| = |a||b|$이 성립하지 않는 예를 구하여라.

『풀이』

1.3 부분군

정의 1.5 군 G에서 G의 부분집합 $H(\neq \varnothing)$가 G의 연산에 관하여 군을 이룰 때, H를 군 G의 **부분군(subgroup)**이라 하고 $H \leq G$로 표기한다.

예제 1.13

(1) $\mathbb{R}^{**}$는 곱셈 군 $\mathbb{R}^{*}$의 부분군이다.
(2) $(\mathbb{Z}, +)$는 $(\mathbb{R}, +)$의 부분군이다.
(3) $GL_2(\mathbb{R})$은 $M_2(\mathbb{R})$의 부분군이 아니다.
(4) $\mathbb{Z}_n^*$는 $\mathbb{Z}_n$의 부분군이 아니다.

『풀이』

정의 1.6

(1) G와 $\{e\}$를 G의 **자명한 부분군(trivial subgroup)**이라 한다.
(2) G와 $\{e\}$가 아닌 G의 부분군을 **진부분군(proper subgroup)**이라 한다.

정리 1.6 군 G에서 G의 부분집합 $H(\neq \varnothing)$가 다음을 만족하면 H는 G의 부분군이다.

(1) $a, b \in H \Rightarrow ab \in H$
(2) $a \in H \Rightarrow a^{-1} \in H$

『증명』

정리 1.7 군 G에서 G의 부분집합 $H(\neq \varnothing)$가

$$a, b \in H \Rightarrow ab^{-1} \in H$$

다음을 만족하면 H는 G의 부분군이다.

『증명』

예제 1.14

$H=\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix} \mid b\in\mathbb{R}\right\}$는 $GL(2,\ \mathbb{R})$의 부분군이다.

『풀이』

군 G가 유한군(finite group)이고 H가 G의 부분군일 때, 다음 명제의 진위를 판정하고 이유를 설명하시오. [2010]

(1) G와 H의 부분군의 개수가 같으면 $G=H$이다.

(2) $H^{-1}=\{a^{-1}\mid a\in H\}$는 G의 부분군이다.

『풀이』

정리 1.8 군 G에서 유한 부분집합 $H(\neq\varnothing)$에 대하여 $a,b\in H \Rightarrow ab\in H$가 성립하면 H는 군 G의 부분군이다.

『증명』

예제 1.15

(1) $H=\{f\in S_5 \mid f(1)=1\}$은 S_5의 부분군이다.

(2) $H=\{e, \rho, \rho^2, \rho^3\}$은 D_4의 부분군이다.

(3) $H=\{(0, 0), (3, 0), (0, 2), (3, 2)\}$는 $\mathbb{Z}_6\times\mathbb{Z}_4$의 부분군이다.

『풀이』

정리 1.9 군 G의 부분군 H, K에 대하여 $HK=\{hk \mid h\in H, k\in K\}$라 정의한다. 그러면 HK가 G의 부분군이기 위한 필요충분조건은 $HK=KH$인 것이다.

『증명』

정의 1.7 군 G에서 $Z(G)=\{a\in G \mid \forall g\in G, ag=ga\}$를 G의 **중심(center)**이라 한다.

예제 1.16

S_3와 D_4의 중심을 찾아라.

『풀이』

정리 1.10 군 G의 중심 $Z(G)$는 G의 부분군이다.

『증명』

정리 1.11 군 G에서 $a \in G$에 대하여 $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$는 a를 포함하는 G의 최소의 부분군이다. 즉, H가 a를 포함하는 G의 부분군이면 $\langle a \rangle \subset H$가 성립한다.

『증명』

예제 1.17

$\mathbb{Z}_{15}^*$의 원소 7과 13에 대하여 $\langle 7 \rangle$, $\langle 13 \rangle$을 구하여라.

『풀이』

정의 1.8

(1) 군 G와 $a \in G$에 대하여 $\langle a \rangle$를 a에 의하여 생성되는 **순환 부분군(cyclic subgroup)**이라 한다.

(2) 군 G에 대하여 $G = \langle a \rangle$인 $a \in G$가 존재할 때, G는 **순환군(cyclic group)**이라 하고 a를 **생성원(generator)**이라 한다.

※ 순환군은 가환군이다. 또한 순환군의 생성원은 유일하지 않다.

정리 1.12 군 G에서 $a \in G$에 대하여 다음이 성립한다.

(1) a가 무한 위수를 가지면 $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$는 무한 부분군이며 각각의 $k \in \mathbb{Z}$에 따라 a^k는 모두 다르다.

(2) $|a| = n$이면 $\langle a \rangle$는 위수 n을 갖는 부분군이며 $\langle a \rangle = \{e = a^0, a^1, a^2, a^3, \cdots, a^{n-1}\}$이다.

『증명』

정리 1.13 순환군의 모든 부분군은 순환군이다.

『증명』

정리 1.14 위수 n인 순환군 $G=\langle a\rangle$에 대하여 다음이 성립한다.

(1) $d \mid n$인 d에 대하여 $\langle a^{n/d}\rangle$는 위수 d인 G의 부분군이고 $\langle a^{n/d}\rangle=\{x\in G \mid x^d=e\}$이 성립한다.

(2) $d \mid n$인 d에 대하여 d의 위수를 가지는 부분군이 유일하게 존재한다.

(3) $d \mid n$인 d에 대하여 d의 위수를 가지는 원소는 $\varphi(d)$개 이다.

(4) G는 $\varphi(n)$개의 생성원을 갖는다.

『증명』