준수 : 03 사원수

July 11, 2015

Contents

1 군(群, Group)

정의 1) 군(群, Group)

다음 조건들을 만족시키면 집합 G는 연산 $\circ$에 대한 **군**이다.

1. $a \in G, b \in G$ 이면 $a \circ b \in G$ 이다.
2. $a \in G, b \in G, c \in G$ 이면 $(a \circ b) \circ c = a \circ (b \circ c)$ 이다.
3. 임의의 $a \in G$에 대해 $a \circ e = e \circ a = a$를 만족시키는 $e \in G$가 존재한다.
4. 임의의 $a \in G$에 대해 $a \circ x = x \circ a = e$를 만족시키는 $x \in G$가 존재한다.

정의 2) 가환군(可換群, Abelian Group)

군 G가 다음 추가조건을 만족시키면 **가환군**이라고 부른다.

5. $a \in G, b \in G$ 이면 $a \circ b = b \circ a$ 이다.

정의 3)

정의 1, 2에서 1번 조건은, 'G가 연산 $\circ$에 대해 닫혀있다.' 라고도 말할 수 있다. 2번 조건은 **결합법칙(associative law)**이라고 부른다. 3번 조건을 만족시키는 원소 e는 **항등원**이라고 부른다. 4번 조건을 만족시키는 원소 x는 a의 **역원**이라고 부르며, a^{-1} 이라고 쓴다. 5번 조건은 **교환법칙(commutative law)** 이라고 부른다.

예시 4)

(1) 자연수의 집합 $\mathbb{N}$은 덧셈에 대해 닫혀있다. 즉 $a \in \mathbb{N}$이고 $b \in \mathbb{N}$이면 $a + b \in \mathbb{N}$이다. 또 결합법칙이 성립한다. 즉 $a + (b + c) = (a + b) + c$이다. 하지만 항등원이 존재하지 않는다. 즉 임의의 $a \in \mathbb{N}$에 대해 $a + e = e + a = a$를 만족시키는 e의 값은 0인데 $0 \notin \mathbb{N}$이기 때문이다.

따라서 $\mathbb{N}$은 덧셈에 대한 군이 아니다.

(2) 정수의 집합 $\mathbb{Z}$는 덧셈에 대해 닫혀있고 결합법칙이 성립한다. 또 항등원이 존재한다. $0 \in \mathbb{Z}$이기 때문이다. 또한 임의의 정수 a에 대해서 $a + x = 0$을 만족시키는 x는 $-a$이며, $-a \in \mathbb{Z}$이다.

따라서 $\mathbb{Z}$는 덧셈에 대한 군이다. 또한 $\mathbb{Z}$는 덧셈에 대한 교환법칙을 만족시키므로 가환군이라고 볼 수 있다.

(3) 마찬가지로 유리수의 집합 $\mathbb{Q}$, 실수의 집합 $\mathbb{R}$, 복소수의 집합 $\mathbb{C}$도 덧셈에 대한 가환군이라는 것을 쉽게 보일 수 있다.

(4) 정수의 집합 $\mathbb{Z}$는 곱셈에 대해 닫혀있다. 즉 $ab \in \mathbb{Z}$이다. 또 결합법칙이 성립한다. 즉 $a(bc) = (ab)c$이다. 또한 항등원이 존재한다. 즉 임의의 $a \in \mathbb{Z}$에 대해, $ae = ea = a$를 만족하는 e의 값은 1인데 $1 \in \mathbb{Z}$이다. 하지만 모든 $\mathbb{Z}$의 원소에 대해 역원이 존재하지는 않는다. 예를 들어 $2 \in \mathbb{Z}$에 대한 역원 x는 $2x = 1$을 만족시키는 값으로서 $x = \frac{1}{2}$인데 $\frac{1}{2} \notin \mathbb{Z}$이기 때문이다. 또한 곱셈에 대한 0의 역원도 존재하지 않는다.

따라서 $\mathbb{Z}$는 곱셈에 대한 군이 아니다.

(5) 유리수의 집합에서 0을 뺀 집합인 $\mathbb{Q} - \{0\}$는 곱셈에 대해 닫혀있고, 결합법칙이 성립하며, 항등원이 존재한다. 이 때의 항등원은 1이다. 또 임의의 $a = \frac{p}{q} \in \mathbb{Q} - \{0\}$에 대해 $p \neq 0$이고 $q \neq 0$이므로 x를 $x = \frac{q}{p}$로 잡으면

$$ax = 1$$

이 성립하고 이때 $\frac{q}{p} \in \mathbb{Q} - \{0\}$이다.

따라서 $\mathbb{Q} - \{0\}$은 곱셈에 대한 군이며, 교환법칙도 만족하므로 가환군이다.

(6) 마찬가지로 $\mathbb{R} - \{0\}$, $\mathbb{C} - \{0\}$도 곱셈에 대한 가환군이라는 것을 쉽게 밝힐 수 있다.

예시 5)

집합 A를 정의역과 공역이 모두 $\{1, 2, 3\}$인 일대일 대응 함수들의 집합이라고 하자. 그러면 A는 '함수의 합성'이라는 연산에 대해 군을 이룬다. 즉

1. $f \in A$, $g \in A$이면 $f \circ g \in A$이다.
2. $f \in A$, $g \in A$, $h \in A$이면 $(f \circ g) \circ h = f \circ (g \circ h)$이다.
3. 임의의 $f \in A$에 대해 $f \circ I = I \circ f = I$이다.
4. 임의의 $f \in A$에 대해 $f \circ f^{-1} = f^{-1} \circ f = I$를 만족시키는 $f^{-1} \in A$가 존재한다.

하지만 일반적으로 $f \circ g \neq g \circ f$이므로 가환군은 아니다.

2 환(環, Ring)과 체(體, Field)

정의 6) 환(環, Ring)

다음 조건들을 만족시키면 집합 R은 두 연산 $+, \cdot$에 대해 **환**이다.

1. $a \in R$, $b \in R$이면 $a + b \in R$이다.
2. $a \in R$, $b \in R$, $c \in R$이면 $(a + b) + c = a + (b + c)$이다.
3. 임의의 $a \in R$에 대해 $a + 0 = 0 + a = 0$를 만족시키는 $0 \in R$가 존재한다.
4. 임의의 $a \in R$에 대해 $a + x = 0$를 만족시키는 $x \in R$가 존재한다.
5. $a \in R$, $b \in R$이면 $a + b = b + a$이다.
6. $a \in R$, $b \in R$이면 $a \cdot b \in R$이다.
7. $a \in R$, $b \in R$, $c \in R$이면 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$이다.
8. $a \in R$, $b \in R$, $c \in R$이면 $(a+b) \cdot c = a \cdot c + b \cdot c$이고 $a \cdot (b+c) = a \cdot b + a \cdot c$ 이다.

정의 6의 1–5번 조건에 의해 R은 첫 번째 연산인 '$+$에 대해 가환군이다. 이때의 항등원은 0이라고 쓴다. 4번 조건의 역원 x는 정의 1에서와는 달리 $-a$라고 표기한다. 8번 조건은 **분배법칙**이라고 부른다. 가끔 **좌분배법칙**과 **우분배법칙**으로 나누어서 부르기도 한다. $a \cdot b$는 간단히 ab라고 표기하기도 한다.

정의 7) 나눗셈환(Division Ring)

환 R이 다음 추가 조건을 만족시키면 **나눗셈환**이라고 부른다.

9. 임의의 $a \in R$에 대해 $a \cdot 1 = 1 \cdot a = 1$를 만족시키는 $1 \in R$가 존재한다.
10. 임의의 $a(\neq 0) \in R$에 대해 $ax = xa = 1$를 만족시키는 $x \in R$가 존재한다.

마지막 조건을 만족시키는 x, 즉 a의 두 번째 연산 $\cdot$에 대한 역원은 a^{-1}이라고 표기한다.

예시 8)

정수들의 집합 $\mathbb{Z}$는 환이지만, 나눗셈환은 아니다. 짝수인 정수들의 집합은 환이지만 나눗셈환이 아니며, 심지어 곱셈에 대한 항등원도 존재하지 않는다.

정의 9) 가환환(可換環, Commutative Ring)

환 R 이 다음 추가조건을 만족시키면 **가환환**이라고 부른다.

9*. $a \in R, b \in R$ 이면 $a \cdot b = b \cdot a$ 이다.

예시 10)

사원수의 집합 $\mathbb{H}$ 는 나눗셈환이지만 가환환은 아니다. 이차정사각행렬들의 집합 또한 가환환이 아니며 또한 나눗셈환도 아니다.

정의 11) 체(體, Field)

나눗셈환이면서 동시에 가환환인 것을 **체**라고 부른다.

예시 12)

유리수의 집합 $\mathbb{Q}$, 실수의 집합 $\mathbb{R}$, 복소수의 집합 $\mathbb{C}$ 등은 환이면서 곱셈의 교환법칙이 성립하고 곱셈의 항등원과 역원이 존재하므로 체이다.

3 $\mathbb{C}$ 는 체이다.

정리 13)

$\mathbb{C}$ 를 복소수의 집합이라고 하자. 즉 $\mathbb{C} = \{a + bi \mid a \in \mathbb{R}, b \in \mathbb{R}\}$ 이다. $\mathbb{C}$ 에 두 연산 $+$ 와 $\cdot$ 을

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \tag{1}$$

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \tag{2}$$

로 정의하자.

그러면 $\mathbb{C}$ 는 체이다. (실수의 집합인 $\mathbb{R}$ 이 체라는 것을 가정하자.)

증명). 체가 되기 위한 조건을 하나 하나 따져보면 된다.

1. $z_1 = a + bi \in \mathbb{C}$, $z_2 = c + di \in \mathbb{C}$ 라고 하면, (1) 에 의해 $(a + bi) + (c + di) = (a + c) + (b + d)i$ 이다. $\mathbb{R}$ 이 환이므로 $\mathbb{R}$ 은 덧셈에 대해 닫혀있다. 따라서 $a + c \in \mathbb{R}$, $b + d \in \mathbb{R}$ 이다. 그러므로 $z_1 + z_2 \in \mathbb{C}$ 이다.

3. $0 + 0i$ 를 간단히 0 이라고 쓰자. 그러면, 임의의 $z = a + bi \in \mathbb{C}$ 에 대해 $z + 0 = (a + bi) + (0 + 0i) = (a + 0) + (b + 0)i$ 이다. 0 이 실수의 덧셈에 대한 항등원이므로 $z + 0 = a + bi = z$ 이다. 마찬가지로 $0 + z = z$ 이다. 따라서 덧셈에 대한 항등원 0 이 존재한다.

4. 임의의 $z = a + bi \in \mathbb{C}$ 에 대해 $x = (-a) + (-b)i$ 라고 하면 $z + x = (a + bi) + [(-a) + (-b)i] = [a + (-a)] + [b + (-b)]i = 0 + 0i = 0$ 이다.

6. 1 번과 마찬가지로 하면 된다.

9. 임의의 $z = a+bi$ 에 대해 $z \cdot 1 = (a+bi)(1+0i) = (a \cdot 1 - b \cdot 0) + (a \cdot 0 + b \cdot 1)i = a + bi = z$ 이다. 마찬가지로 $1 \cdot z = z$ 이다. 따라서 곱셈에 대한 항등원 1 이 존재한다.

10. 임의의 $z = a + bi \neq 0$ 에 대해 $x = \frac{a-bi}{a^2+b^2}$ 라고 하면 $zx = (a+bi)\frac{a-bi}{a^2+b^2} = 1$ 이다.

나머지 것들은 다음과 같이 증명된다. (실수가 체라는 사실이 중요한 역할을 한다.)

$z_1 = a + bi$, $z_2 = c + di$, $z_3 = e + fi$, a, b, c, d, e, f 는 실수라고 가정하자.

2.

$$\begin{aligned}
(z_1 + z_2) + z_3 &= [(a + bi) + (c + di)] + (e + fi) \\
&= [(a + c) + (b + d)i] + (e + fi) \\
&= [(a + c) + e] + [(b + d) + f]i \\
&= [a + (c + e)] + [b + (d + f)]i \\
&= a + bi + [(c + e) + (d + f)i] \\
&= a + bi + [(c + di) + (e + fi)] \\
&= z_1 + (z_2 + z_3).
\end{aligned}$$

5.

$$\begin{aligned}
z_1 + z_2 &= (a + bi) + (c + di) \\
&= (a + c) + (b + d)i \\
&= (c + a) + (d + b)i \\
&= (c + di) + (a + bi) \\
&= z_2 + z_1.
\end{aligned}$$

7.

$$\begin{aligned}(z_1z_2)z_3 &= [(a+bi)(c+di)](e+fi)\\ &= [(ac-bd)+(ad+bc)i](e+fi)\\ &= [(ac-bd)e-(ad+bc)f]+[(ac-bd)f+(ad+bc)e]i\\ &= (ace-bde-adf-bcf)+(acf-bdf+ade+bce)i\end{aligned}$$

$$\begin{aligned}z_1(z_2z_3) &= (a+bi)[(c+di)(e+fi)]\\ &= (a+bi)[(ce-df)+(cf+de)i]\\ &= [a(ce-df)-b(cf+de)]+[a(cf+de)+b(ce-df)]i\\ &= (ace-adf-bcf-bde)+(acf+ade+bce-bdf)i\end{aligned}$$

따라서 좌변과 우변이 같다.

8.

$$\begin{aligned}z_1(z_2+z_3) &= (a+bi)[(c+di)+(e+fi)]\\ &= (a+bi)[(c+e)+(d+f)i]\\ &= [a(c+e)-b(d+f)]+[a(d+f)+b(c+e)]i\\ &= (ac+ae-bd-bf)+(ad+af+bc+be)i\\ &= [(ac-bd)+(ae-bf)]+[(ad+bc)+(af+be)]i\\ &= [(ac-bd)+(ad+bc)i]+[(ae-bf)+(af+be)i]\\ &= (a+bi)(c+di)+(a+bi)(e+fi)\\ &= z_1z_2+z_1z_3.\end{aligned}$$

(곱셈에 대한 교환법칙이 성립하므로 두 번째 등식은 증명할 필요가 없다.)

9*.

$$\begin{aligned}z_1z_2 &= (a+bi)(c+di)\\ &= (ac-bd)+(ad+bc)i\\ &= (ca-db)+(cb+da)i\\ &= (c+di)(a+bi)\\ &= z_2z_1.\end{aligned}$$

체가 되기 위한 조건들을 모두 만족시키므로 $\mathbb{C}$는 체이다.

□

4 $\mathbb{H}$는 나눗셈환이다.

정의 14) 사원수 (Quaternion)

실수 a, b, c, d에 대해

$$a + bi + cj + dk \tag{3}$$

처럼 표현되는 숫자를 **사원수 (Quaternion)**라고 부른다.

집합 $\mathbb{H}$를 사원수들의 집합이라고 하자. 즉

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

로 정의하자.

$\mathbb{H}$에 두 연산 $+$와 $\cdot$을

$$\begin{aligned}(a_1 + b_1 i + c_1 j + d_1 k) &+ (a_2 + b_2 i + c_2 j + d_2 k)\\ &= (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k\end{aligned} \tag{4}$$

$$\begin{aligned}(a_1 + b_1 i + c_1 j + d_1 k)&(a_2 + b_2 i + c_2 j + d_2 k)\\ &= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2)i\\ &\quad + (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2)j + (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2)k\end{aligned} \tag{5}$$

로 정의하자.

그러면 $\mathbb{H}$는 나눗셈환이다.

증명). 1번 조건과 6번 조건은 정의로부터 당연하다. 2번부터 5번까지의 조건도 거의 당연하다. $\mathbb{C}$가 체라는 사실을 증명할 때와 비슷하게 하면 될 것이다. 9번 조건은 (5) 번 식에 대입하면 쉽게 얻어진다.

마지막으로 $h_1, h_2, h_3 \in \mathbb{H}$일 때,

7. $(h_1 h_2)h_3 = h_1(h_2 h_3)$

8. $(h_1 + h_2)h_3 = h_1 h_3 + h_2 h_3$, $h_1(h_2 + h_3) = h_1 h_2 + h_1 h_3$

이고 임의의 $h \in \mathbb{H}$에 대해,

10. $hx = 1$을 만족시키는 $x \in H$가 존재한다

는 것을 증명해야 한다.

$\mathbb{C}$가 체라는 것을 증명했던 방법과 똑같이 직접적인 증명방법으로 접근하면, 가능은 하겠지만 굉장히 복잡하게 될 것이다. 가령 7번의 결합법칙을 증명하려면, 세 개의 사원수를 곱했을 때 나오는 64개의 항을 정리해야 할 것이다. 따라서 다른 방법으로 사원수를 표기하여 계산을 간단히 하자.

$$a + bi + cj + dk = (x, y) \quad (\text{단, } x = a + bi, y = c + di) \tag{6}$$

즉 복소수의 순서쌍으로 나타내자. 예를 들어

$$\begin{aligned}
1 + 2i + 3j + 4k &= (1 + 2i, 3 + 4i) \\
1 + 3j &= (1, 3) \\
-2 + 4k &= (-2, 4i) \\
k &= (0, i) \\
-2j &= (0, -2) \\
0 &= (0, 0)
\end{aligned}$$

등으로 나타내자.

그리고 두 복소수 순서쌍 사이의 덧셈을

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) \tag{7}$$

로 정의하면 ($x_1 = a_1 + b_1 i,\ y_1 = c_1 + d_1 i,\ x_2 = a_2 + b_2 i,\ y_2 = c_2 + d_2 i$) 원래 사원수의 덧셈인 (4) 번 식과 정확히 일치한다.

또한 두 복소수 순서쌍 사이의 곱셈을

$$(x_1, y_1)(x_2, y_2) = (x_1 x_2 - y_2 \overline{y_1}, \overline{x_1} y_2 + y_1 x_2) \tag{8}$$

로 정의하면,

$$\begin{aligned}
&(x_1x_2 - y_2\overline{y_1}, \overline{x_1}y_2 + y_1x_2)\\
=&\Big((a_1+b_1i)(a_2+b_2i) - (c_2+d_2i)(c_1-d_1i),\\
&\qquad\qquad (a_1-b_1i)(c_2+d_2i) + (c_1+d_1i)(a_2+b_2i)\Big)\\
=&\Big((a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i,\\
&\qquad\qquad (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2) + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)i\Big)\\
=&(a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i\\
+&(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)j + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)k
\end{aligned}$$

이 되어 원래 사원수의 곱셈인 (5) 번 식과 일치한다.

따라서 사원수를 (3) 번 식과 (4) 번 식, (5) 번식으로 덧셈과 곱셈을 생각하지 말고, 사원수를 (6) 번 식과 (7) 번 식, (8) 번 식을 통해 덧셈과 곱셈을 생각해도 아무 문제가 없다.

그러므로

$$\begin{aligned}
(h_1h_2)h_3 &= \Big((x_1,y_1)(x_2,y_2)\Big)(x_3,y_3)\\
&= \Big(x_1x_2 - y_2\overline{y_1}, \overline{x_1}y_2 + y_1x_2\Big)(x_3,y_3)\\
&= \Big((x_1x_2 - y_2\overline{y_1})x_3 - y_3\overline{(\overline{x_1}y_2 + y_1x_2)},\quad \overline{(x_1x_2 - y_2\overline{y_1})}y_3 + (\overline{x_1}y_2 + y_1x_2)x_3\Big)\\
&= \Big((x_1x_2 - y_2\overline{y_1})x_3 - y_3(x_1\overline{y_2} + \overline{y_1x_2}),\quad (\overline{x_1x_2} - \overline{y_2}y_1)y_3 + (\overline{x_1}y_2 + y_1x_2)x_3\Big)\\
&= \Big(x_1x_2x_3 - \overline{y_1}y_2x_3 - x_1\overline{y_2}y_3 - \overline{y_1x_2}y_3,\quad \overline{x_1x_2}y_3 - y_1\overline{y_2}y_3 + \overline{x_1}y_2x_3 + y_1x_2x_3\Big)\\
&= \Big(x_1x_2x_3 - x_1\overline{y_2}y_3 - \overline{y_1x_2}y_3 - \overline{y_1}y_2x_3,\quad \overline{x_1x_2}y_3 + \overline{x_1}y_2x_3 + y_1x_2x_3 - y_1\overline{y_2}y_3\Big)\\
&= \Big(x_1(x_2x_3 - \overline{y_2}y_3) - (\overline{x_2}y_3 - y_2x_3)\overline{y_1},\quad \overline{x_1}(\overline{x_2}y_3 + y_2x_3) + y_1(x_2x_3 - \overline{y_2}y_3)\Big)\\
&= (x_1,y_1)\Big(x_2x_3 - \overline{y_2}y_3, \overline{x_2}y_3 + y_2x_3\Big)\\
&= h_1(h_2h_3).
\end{aligned}$$

이기 때문에 7번 조건이 성립한다. 8번 조건도 마찬가지의 방법으로 증명할 수 있을 것이다.

10번 조건의 경우, 임의로 사원수 $(x_1, y_1) \neq (0,0)$ 가 주어졌을 때, $(x_1,y_1)(x_2,y_2) =$

1을 풀면

$$(x_1x_2 - y_2\overline{y_1}, \overline{x_1}y_2 + y_1x_2) = (1, 0)$$

$$\begin{cases} x_1x_2 - \overline{y_1}y_2 = 1 \\ y_1x_2 + \overline{x_1}y_2 = 0 \end{cases}$$

$$\begin{cases} x_1\overline{x_1}x_2 - \overline{x_1}\overline{y_1}y_2 = \overline{x_1} \\ y_1\overline{y_1}x_2 + \overline{x_1}\overline{y_1}y_2 = 0 \end{cases}, \qquad \begin{cases} x_1y_1x_2 - y_1\overline{y_1}y_2 = y_1 \\ x_1y_1x_2 + x_1\overline{x_1}y_2 = 0 \end{cases}$$

$$x_2 = \frac{\overline{x_1}}{x_1\overline{x_1} + y_1\overline{y_1}}, \qquad y_2 = -\frac{y_1}{x_1\overline{x_1} + y_1\overline{y_1}}$$

$$x_2 = \frac{\overline{x_1}}{{a_1}^2 + {b_1}^2 + {c_1}^2 + {d_1}^2}, \qquad y_2 = -\frac{y_1}{{a_1}^2 + {b_1}^2 + {c_1}^2 + {d_1}^2}$$

이므로 역원이 항상 존재한다.

$\mathbb{H}$가 나눗셈환이 되기 위한 모든 조건을 만족시키므로 $\mathbb{H}$는 나눗셈 환이다. $\square$