

# 현대대수1및실습

## 임기정

임복희 교수님께서 담당하시는 2021년 1학기 현대대수1및실습 1 분반 안의, Noether 조에서 만든 노트입니다. 딱딱한 현대대수학을 최대한 쉽게 풀어 쓰고자 노력하였습니다.

### 1 1주차 노트 정리

현대대수1및실습을 수강하셨다면 마땅히 알아야 할 “군”이라는 낱말의 뜻에 대하여 논하기 위해서는, 이항 구조(binary structure)부터 알아야 합니다.

집합  $S$ 가 이항 구조가 되기 위해서는 이항 연산(binary operator)  $*$ 을 가져야 합니다. 이때  $*$ 이 이항 연산이라 함<sup>1</sup>은 그것이

(a)  $S \times S$ 를 정의역(domain)으로 가지면서

(b)  $S$ 를 공역(codomain)을 가져야 하며

(c) 잘 정의된(well defined)

함수이어야 함을 의미합니다. 각 조건에 대하여 설명하자면 다음과 같습니다:

1. 조건 (a)의 뜻은 아무  $a \in S$ 와 아무  $b \in S$ 에 대하여 순서쌍  $(a, b)$ 를  $*$ 에게 입력으로 줄 수 있어야 한다는 것이고;
2. 조건 (b)의 뜻은 입력  $(a, b)$ 에 대한  $*$ 의 출력  $a * b$ 이 항상  $S$ 의 원소이어야 한다는 것이며;
3. 조건 (c)의 뜻은 그 출력이 딱 하나로 결정되어야 한다는 것입니다.

이때  $*$ 이 조건 (a)를 어긴다면  $*$ 가  $S$  위의 모든 것들에서 정의되지 않는다(not everywhere defined)고 하고, 조건 (b)를 어긴다면  $S$ 는  $*$  아래에서 닫혀 있지 않다(not closed under  $*$ )고 하며, 조건 (c)를 어긴다면  $*$ 이 잘 정의되지 않았다(not well defined)고 합니다.

---

<sup>1</sup>참고 문헌 [1] 20쪽, 정의 2.1 인용

만약 \*이 이 모든 조건들을 지킨다면 이항 연산이 되는데, 이때 이항 연산이 된다는 사실을

$$\begin{aligned} S \times S &\xrightarrow{*} S \\ (a, b) &\mapsto a * b \end{aligned}$$

와 같이 적을 수 있습니다.

이때 공집합이 아닌 집합  $S$ 가 이항 연산  $* : S \times S \rightarrow S$ 을 가지면 순서쌍  $(S, *)$ 을 이항 구조라고 부릅니다. 참고로 “이항 구조”의 동의어에는 “아군”(groupoid)와 “마그마”(magma)가 있습니다.<sup>2</sup>

마그마  $(S, *)$ 가 군<sup>3</sup>(group)이 되기 위해서는 다음 세 조건을 만족시켜야 합니다:

1. 결합 법칙(associative law)<sup>4</sup>이 성립해야 함:

$$(\forall a \in S) (\forall b \in S) (\forall c \in S) [(a * b) * c = a * (b * c)] \quad (1)$$

이어야 합니다. 다시 말해, 모든  $a, b, c \in S$ 에 대하여  $(a * b) * c = a * (b * c)$ 이어야 합니다.

(1)이 성립할 때 그리고 그럴 때에만 “\*이  $S$  위에서 결합적이다”라고 말합니다.

2. 항등원(identity)<sup>5</sup>이 존재해야 함: 적당한  $e \in S$ 가 존재해서

$$(\forall a \in S) [e * a = a * e = a] \quad (2)$$

이어야 합니다. 이때  $e$ 를 \*에 대한 항등원(identity element for \*)이라고 합니다.

한 가지 주목할 만한 점은 항등원은 많아야 한 개 밖에 존재하지 않는다는 사실입니다.<sup>6</sup> 이 사실을 증명하기 위해서는  $e_1 \in S$ 가

$$(\forall a \in S) [e_1 * a = a * e_1 = a] \quad (2-1)$$

를 만족한다고 가정한 상태에서  $e = e_1$ 을 이끌어내면 충분합니다.

이렇게만 해도 충분한 이유를 생각해 봅시다.  $e_1 \in S$ 이  $e$ 와 다르다면 항등원이어서는 안 된다는 걸 보이면, 자동적으로 항등원은  $e$  밖에 없게 됩니다. 그런데 “ $e_1 \in S$ 이  $e$ 와 다르다면 항등원이어서는 안 된다”의 대우 명제가 바로 “ $e_1 \in S$ 가 (2-1)을 만족시킨다면  $e = e_1$ 이다”이기 때문입니다. 이제 본격적으로 증명을 해보도록 하겠습니다.

<sup>2</sup>참고 문헌 [1] 38쪽 인용

<sup>3</sup>참고 문헌 [1] 37쪽, 정의 4.1 인용

<sup>4</sup>참고 문헌 [1] 23쪽, 정의 2.12 인용

<sup>5</sup>참고 문헌 [1] 32쪽, 정의 3.12 인용

<sup>6</sup>참고 문헌 [1] 32쪽, 정리 3.13 인용

*Proof.* 먼저,  $e_1 \in S$ 를 하나 잡은 뒤 그  $e_1$ 이 (2-1)을 만족시킨다고 가정하겠습니다. 그러면 (2)의  $a$  자리에  $e_1$ 을 넣음으로써

$$e * e_1 = e_1 * e = e_1$$

을 얻을 수 있고, (2-1)의  $a$  자리에  $e$ 를 넣음으로써

$$e_1 * e = e * e_1 = e$$

을 얻을 수 있습니다. 따라서  $e_1 * e = e_1$ 이고  $e_1 * e = e$ 임을 알 수 있습니다. 이것들로부터

$$e = e_1 * e = e_1$$

를 얻게 되는데, 이로써 ( $e = e_1$ 을 보였기 때문에) 증명을 마칠 수 있습니다.  $\square$

3. 각 원소마다 역원(*inverse*)<sup>7</sup>을 가져야 함: 각각의  $a \in S$ 마다, 어떤  $b \in S$ 가 존재해서

$$a * b = b * a = e \tag{3}$$

이어야 합니다. 이 경우 각각의  $a \in S$ 에 대하여 (3)을 만족시키는  $b \in S$ 가 유일하게 존재합니다! 따라서 그  $b$ 를  $a^{-1}$ 과 같이 쓸 수 있고  $a$ 의 역원(*inverse of  $a$* )라고 부릅니다.

이를 증명하는 것은 꽤나 어려워 보이지만, 전과 비슷하게 임의의 역원 후보  $b_1$ 에 대하여  $b = b_1$ 일 수 밖에 없음을 보이면 됩니다.

*Proof.* 먼저,  $a \in S$ 를 하나 뽑겠습니다. 그러면 가정에 의하여 어떤  $b \in S$ 가 (3)을 만족시킵니다. 이때  $b_1 \in S$ 가

$$a * b_1 = b_1 * a = e \tag{3-1}$$

를 만족시킨다고 가정한다면,

$$b = b * e \tag{by (2)}$$

$$= b * (a * b_1) \tag{by (3-1)}$$

$$= (b * a) * b_1 \tag{by (1)}$$

$$= e * b_1 \tag{by (3)}$$

$$= b_1 \tag{by (2)}$$

---

<sup>7</sup>참고 문헌 [1] 37쪽, 정의 4.1 인용

를 얻게 되고, 증명을 마칠 수 있습니다.  $\square$

참고로 결합 법칙을 만족시키는 마그마를 반군(*semigroup*)이라고 하고, 항등원이 존재하는 반군을 모노이드(*monoid*)라고 합니다.<sup>8</sup> 즉, 군은 각 원소마다 역원을 가지는 모노이드입니다.

또한 “아벨 군”(abelian group)의 개념을 소개할까 합니다. 이항 구조  $(S, *)$ 가 주어졌을 때,  $*$ 이 가환(commutative)<sup>9</sup>하다고 함은

$$(\forall a \in S) (\forall b \in S) [a * b = b * a] \quad (4)$$

이어야 한다는 뜻인데,  $*$ 이 가환한 군을 아벨 군이라고 부릅니다.<sup>10</sup>

이제, 군의 예를 하나 공부해 봅시다.

그 예는 원군(circle group)입니다. 집합  $S^1$ 을

$$S^1 := \{z \in \mathbb{C} : |z| = 1\} \quad (5)$$

와 같이 두고, 복소수의 곱셈으로부터 이항 연산  $*$  :  $S^1 \times S^1 \rightarrow S^1$ 을 유도(induce)<sup>11</sup>하면,

$$(S^1, *)$$

는 군이 됩니다! 이것이 사실임을 증명할 것인데, 그 전에 다뤄야 할 개념이 있습니다.

“ $*$ 은  $S^1$  위에서 복소수 곱셈의 유도된 연산(induced operation)이다”라고 함은, 이항 연산  $*$ 을 복소수의 곱셈의 정의역을  $S^1 \times S^1$ 으로 줄여서 얻었다는 뜻입니다. 그런데 이때  $*$ 이 이항 연산이라는 보장이 있을까요? 만약 없다면, 우리는 무엇을 확인해 보아야 될까요?

이항 구조  $(S, *)$ 가 주어졌다고 합시다. 이제  $S$ 의 부분 집합  $S'$ 를 하나 잡고,  $*$ '을

$$\begin{aligned} S' \times S' &\xrightarrow{*'} S' \\ (a, b) &\mapsto a * b \end{aligned}$$

로 정의할게요. 그러면  $*$ '이 이항 연산이 되기 위한 조건들 중 (a)와 (c)는,  $*$ 이 이항 연산이라는 가정에 의하여, 이미 성립합니다.  $*$ '는 자신의 정의역에서  $(a, b) \mapsto a * b$ 으로 정의되었으니까요! 이제 남은 조건은 (b) 뿐인데, 안타깝게도, 이걸 성립하지 않을 수도 있습니다. 따라서  $(S', *)'$ 가 이항 구조임을 보이기 위해서는,  $S'$ 에서 (서로 같을 수도 있는) 두 원소  $a$ 와  $b$ 를 아무렇게나 뽑아서  $*$ 에 주더라도, 그 출력  $a * b$ 가  $S'$  밖으로 절대 못 나간다는 것을 보여야 합니다.

<sup>8</sup>참고 문헌 [1] 42쪽 인용

<sup>9</sup>참고 문헌 [1] 22쪽, 정의 2.11 인용

<sup>10</sup>참고 문헌 [1] 38쪽, 정의 4.3 인용

<sup>11</sup>참고 문헌 [1] 21쪽, 정의 2.4 인용

만약 그러하다면,  $S'$ 를  $*$ 에 대하여 닫혀 있다(*closed under  $*$* )고 합니다. 즉, 집합  $S' \subseteq S$ 가 연산  $*$  :  $S \times S \rightarrow S$ 에 대하여 닫혀 있을 필요충분조건은

$$(\forall a \in S') (\forall b \in S') [a * b \in S']$$

가 성립한다는 것입니다.

이상의 논의로부터  $(S^1, *)$ 가 마그마라는 걸 보이는 것부터 시작해야 되는 걸 알 수 있습니다. 그렇게 하기 위하여, 두 원소  $z_1 \in S^1$ 와  $z_2 \in S^1$ 를 아무렇게나 골라 봅시다. 그렇다면,  $z_1 z_2 \in \mathbb{C}$  이고  $|z_1| = |z_2| = 1$ 이어야 하기 때문에,

$$\begin{aligned} |z_1| |z_2| = 1 &\implies |z_1 z_2| = 1 \\ &\implies z_1 z_2 \in S^1 \end{aligned}$$

입니다. 따라서 다음 단계<sup>12</sup>로 넘어갈 수 있습니다.

이제  $(S^1, *)$ 이 반군임을 증명해 보겠습니다. 우리는 이미 복소수의 곱셈이 결합 법칙을 만족시키는 것을 알고 있습니다. 그런데  $S^1$ 은  $\mathbb{C}$ 의 부분 집합입니다. 그러니까 모든  $a, b, c \in S^1$ 에 대하여,

$$(a * b) * c = a * (b * c) \tag{6}$$

이 성립하겠죠? 왜냐하면, (6)을 만족시킨다는 것을 검증받아야 될 모든 삼중쌍

$$(a, b, c) \in S^1 \times S^1 \times S^1$$

들은 전부 집합  $\mathbb{C} \times \mathbb{C} \times \mathbb{C}$ 의 원소이므로, 복소수의 곱셈의 결합 법칙이 보증해 주기 때문이죠.  $*$ 가 복소수의 곱셈으로부터 유도되었다는 사실을 상기하신다면, 쉽게 이해가실 거예요.

이제  $(S^1, *)$ 이 모노이드임을 증명해 보겠습니다.  $S^1$ 의 원소들 중 항등원을 하나 찾아서, 그것이 (2)를 만족시킨다는 것을 보이면 충분합니다. 그런데, 복소수의 곱셈에 대한 항등원인 1이  $S^1$ 에 속해버린 이상, 1이  $S^1$ 의 항등원이 되지 않을까요? 아까와 같은 이유에 의하여, 더 큰 세상에서 보증 받았으므로, 답은 “예”입니다.

드디어  $(S^1, *)$ 이 군임을 증명해 보겠습니다. 그렇기 위해서는, 각 원소  $a \in S^1$ 마다 어떤  $b \in S^1$ 가 (3)을 만족시키는 것을 보이면 충분합니다. 이제  $a \in S^1$ 를 하나 잡겠습니다. 그러면

$$a * (1/a) = (1/a) * a = 1$$

---

<sup>12</sup> $(S^1, *)$ 이 반군임을 증명하기

이므로,  $(1/a$ 가 역원임을 보이기 위해서는)  $1/a \in S^1$ 임만 보이면 충분합니다. 그런데  $1/a \in \mathbb{C}$ 이고  $|a| = 1$ 이므로,

$$\begin{aligned} |1| = 1 &\implies |a(1/a)| = 1 \\ &\implies |a| |1/a| = 1 \\ &\implies 1 |1/a| = 1 \\ &\implies |1/a| = 1 \\ &\implies 1/a \in S^1 \end{aligned}$$

를 얻게 됩니다.

이상의 논의로부터  $(S^1, *)$ 를 군이라고 부를 수 있음을 알 수 있습니다. 추가적으로, 그것은 아벨 군이기도 합니다. 아까와 마찬가지로, 이 사실도  $*$ 가 복소수의 곱셈으로부터 유도된 연산임을 이용하면, 어렵지 않게 보일 수 있습니다.

노트를 쓰다 보니까 쓸데없는 호기심이 발동하네요. 모노이드  $(M, *)$ 이 주어졌다고 가정하고,  $M$ 의 항등원을  $e$ 라고 하겠습니다. 그렇다면  $e \notin M'$ 인 집합  $M' \subseteq M$ 을 어떻게 잡든지  $M'$  안에는  $M'$  위의  $*$ 의 유도된 연산에 대한 항등원이 존재하지 않아야 할까요? 이는 방금 전  $(S^1, *)$ 이 모노이드임을 보일 때와 반대인 상황인데, 답은 “아니오”입니다.

$*$	0	1
0	0	1
1	1	1

반례 중 하나는 다음과 같습니다:  $M := \{0, 1\}$ 로 두고,  $*$ 을 위의 표와 같이 정의하면,  $*$ 에 대한 항등원은 0입니다. 이때  $M' := \{1\}$ 로 두면,  $1 * 1 = 1$ 이므로 1은  $M'$  위의  $*$ 의 유도된 연산의 항등원입니다.

## 2 2주차 노트 정리

앞에서 군의 정의와 군의 예 중 하나인 원군을 배웠습니다. 이제 다른 예들도 알아보시다:

1. “정수 덧셈군”이라고 불리는 군  $(\mathbb{Z}, +)$ :

이 군은 0을 항등원으로 가지고, 각  $i \in \mathbb{Z}$ 마다  $i \in \mathbb{Z}$ 의 역원은  $-i$ 이에요. 더구나 이 군은 아벨 군입니다.

2. “복소수 곱셈군”이라고 불리는 군  $(\mathbb{C}^*, *)$ :

여기서,  $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ 입니다. 이 군은 1을 항등원으로 가지고, 각  $z \in \mathbb{C}^*$ 마다  $z^{-1}$ 을 역원으로 가집니다. 더구나 이 군은 아벨 군입니다. 여기서 모든 복소수들의 집합  $\mathbb{C}$ 에서 0을 제외하였는데, 그 이유는 복소수의 곱셈에 대한 0의 역원이라고 부를 수 있는 복소수가 존재하지 않기 때문입니다. 단,  $\mathbb{C}$ 에서 0을 빼냈기 때문에 닫혀 있는지 확인해 봐야 합니다. 이 군도 정수 덧셈군과 마찬가지로 아벨 군이죠.

3. 방금까지 원소의 개수가 무한한 군을 살펴 보았는데, 이제 원소의 개수가 유한한 군을 살펴 보겠습니다. 집합  $U_6$ 를

$$U_6 := \{z \in \mathbb{C} : z^6 = 1\}$$

로 두고,  $*$ 를 복소수의 곱셈으로부터  $U_6$  위로 유도된 연산으로 두면,  $(U_6, *)$ 는 군입니다.

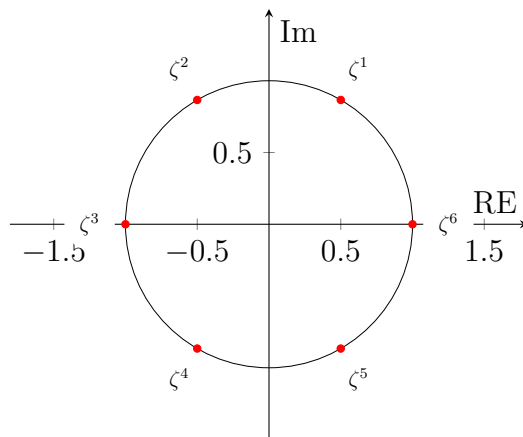


Fig. 1: 복소 평면 위의  $U_6$

보시다시피  $U_6 = \{\zeta^1, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6\}$ 인데, 여기서 복소수  $\zeta$ 는

$$\zeta := e^{i\pi/3} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$$

으로 정의되었습니다. 이때

- 항등원을  $\zeta^6 = 1$ 으로;
- 각  $n \in \{1, 2, \dots, 6\}$ 에 대하여  $\zeta^n$ 의 역원을  $\zeta^{6-n} = 1/\zeta^n$ 으로

두면,  $(U_6, *)$ 가 군의 정의를 만족시킴을 알 수 있습니다.

4. 그 외에도  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$ 은 모두 군이면서 아벨 군이고,
5.  $(\mathbb{R}^*, *)$  역시 군입니다. (아벨 군이기도 하죠.) 여기서,  $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ 입니다.

그런데  $(\mathbb{R}, +)$ 은 군으로서  $(\mathbb{C}, +)$  안에 들어갈 수 있네요? “군으로서 안에 들어갈 수 있다”라는 개념을 정의하려면, “부분군”과 “군 동형”의 개념이 필요합니다.

먼저 부분군(subgroup)<sup>13</sup>에 대하여 알아 보겠습니다. 만약 군  $G$ 의 부분 집합  $H$ 가  $G$ 의 이항 연산 아래에 닫혀 있고,  $G$ 로부터 유도된 연산을 가지는  $H$ 가 그 자신이 군이면  $H$ 는  $G$ 의 부분 군이라고 합니다.  $H$ 가  $G$ 의 부분군인 경우, 그 사실을 “ $H \leq G$ ” 또는 “ $G \geq H$ ”라고 적어서 나타냅니다.

군  $G$ 의 항등원  $e$ 이라면, 당연히 집합  $\{e\}$ 는  $G$ 의 부분군입니다. (심지어 아벨 군이기도 합니다.) 이를  $G$ 의 자명한(trivial) 부분군이라고 합니다.<sup>14</sup> 자명한 부분군이 아닌 부분군을 가르켜 비자명(nontrivial) 부분군이라고 부릅니다.<sup>15</sup>

$G$ 가 군이면  $G$  자신도  $G$ 의 부분군입니다.  $G$ 를  $G$ 의 비진부분군(improper subgroup)이라고 합니다.<sup>16</sup>  $G$ 가 아닌  $G$ 의 부분군을 가르켜 진부분군(proper subgroup)이라고 부릅니다.<sup>17</sup>

그런데 언제 부분 집합이 부분군이 되는지 생각해 봅시다. 그러면 어떠한 군  $(G, *)$ 가 주어 지더라도, 임의의 집합  $H \subseteq G$ 가  $G$ 의 부분군일 때 그리고 그럴 때에만 다음 조건들이 모두 성립함을 알 수 있습니다:<sup>18</sup>

1.  $H$ 가  $G$ 의 이항 연산 아래에 닫혀 있다. 다시 말해, 논리식

$$(\forall a \in H) (\forall b \in H) [a * b \in H] \quad (7)$$

가 성립한다는 뜻입니다.

2.  $G$ 의 항등원이  $H$ 에 속한다. 다시 말해, 논리식

$$e \in H \quad (8)$$

가 성립한다는 뜻입니다.

3. 각  $a \in H$ 에 대하여,  $a$ 의 역원이  $H$ 에 속한다. 다시 말해, 논리식

$$(\forall a \in H) (\exists b \in H) [a * b = b * a = e] \quad (9)$$

가 성립한다는 뜻입니다.

*Proof.* 먼저, 파트 (a)에서 필요한 보조 정리를 하나 증명하고; 그 다음, 파트 (b)에서  $H \leq G$ 이 성립한다고 가정한 뒤 조건 1, 2, 3이 성립함을 보이고; 마지막으로, 파트 (c)에서 조건 1, 2, 3이 성립한다고 가정한 뒤  $H \leq G$ 임을 보이겠습니다.

<sup>13</sup>참고 문헌 [1] 49쪽, 정의 5.4 인용

<sup>14</sup>참고 문헌 [1] 49쪽, 정의 5.5 인용

<sup>15</sup>참고 문헌 [1] 49쪽, 정의 5.5 인용

<sup>16</sup>참고 문헌 [1] 49쪽, 정의 5.5 인용

<sup>17</sup>참고 문헌 [1] 49쪽, 정의 5.5 인용

<sup>18</sup>참고 문헌 [1] 51쪽, 정의 5.14 인용



- (a) 군  $(G, *)$ 가 주어졌다고 하겠습니다. 그러면 임의의  $a \in G$ 와 임의의  $b \in G$ 에 대하여 (10)과 (11)이 성립합니다:<sup>19</sup>

$$(\exists x \in G) [a * x = b \wedge (\forall y \in G) [a * y = b \rightarrow x = y]] \quad (10)$$

$$(\exists x \in G) [x * a = b \wedge (\forall y \in G) [y * a = b \rightarrow x = y]] \quad (11)$$

다시 말해,  $x$ 에 대한 방정식  $a * x = b$ 은 유일한 해를 가지고, 또 다른  $x$ 에 대한 방정식  $x * a = b$ 도 유일한 해를 가진다는 뜻입니다.

*Proof of (a).* 먼저, (10)이 성립하는 것부터 보이겠습니다.  $x := a^{-1} * b$ 로 두면,

$$\begin{aligned} a * x &= a * (a^{-1} * b) \\ &= (a * a^{-1}) * b \\ &= e * b \\ &= b \end{aligned}$$

이고,  $a * y = b$ 인 임의의  $y \in G$ 에 대하여,

$$\begin{aligned} a * x = b &\implies a * x = a * y \\ &\implies a^{-1} * (a * x) = a^{-1} * (a * y) \\ &\implies (a^{-1} * a) * x = (a^{-1} * a) * y \\ &\implies e * x = e * y \\ &\implies x = y \end{aligned}$$

이므로, (10)이 성립함을 알 수 있습니다.

이제, (11)이 성립함을 보이겠습니다. 아까와 비슷하게  $x := b * a^{-1}$ 로 두면,

$$\begin{aligned} x * a &= (b * a^{-1}) * a \\ &= b * (a^{-1} * a) \\ &= b * e \\ &= b \end{aligned}$$

---

<sup>19</sup>참고 문헌 [1] 40쪽, 정의 4.15 인용

이고,  $y * a = b$ 인 임의의  $y \in G$ 에 대하여,

$$\begin{aligned}
 x * a = b &\implies x * a = y * a \\
 &\implies (x * a) * a^{-1} = (y * a) * a^{-1} \\
 &\implies x * (a * a^{-1}) = y * (a * a^{-1}) \\
 &\implies x * e = y * e \\
 &\implies x = y
 \end{aligned}$$

이므로, (11)이 성립함을 알 수 있습니다. □

- (b) 먼저  $H \leq G$ 라고 가정합니다. 그러면  $H$ 는  $G$ 의 부분군이므로, 부분군의 정의에 의하여,  $*$ 에 대하여 닫혀 있고;  $H$  위에서  $*$ 의 유도된 이항 연산  $*$ '에 대하여,  $(H, *)$ 는 그 자체로 군이어야 합니다.

여기서  $H$ 가  $*$ 에 대하여 닫혀 있으므로 조건 1이 성립함을 알 수 있습니다.

또한  $H$ 는 군이기 때문에, 공집합이 아니어야 하므로 어떤  $h_0 \in H$ 가 존재함을 알 수 있고; 보조 정리 (a)를 적용하여 어떤  $e' \in H$ 가 존재하여

$$h_0 *' e' = h_0 \wedge (\forall h \in H) [h_0 *' h = h_0 \rightarrow e' = h]$$

가 성립함을 알 수 있습니다. 이때 보조 정리 (a)를 군  $(G, *)$ 에 적용하면, 어떤  $x \in G$ 가

$$h_0 * x = h_0 \wedge (\forall y \in G) [h_0 * y = h_0 \rightarrow x = y]$$

를 만족시킴을 알 수 있는데,  $y$ 에  $G$ 의 항등원  $e$ 를 넣음으로써  $x = e$ 를 얻을 수 있습니다. 이제  $y$ 에  $e'$ 를 넣으면  $x = e'$ 가 도출되는데,  $e = e' \in H$ 를 얻게 됩니다. 따라서 조건 2가 성립함을 알 수 있습니다. 물론,  $e$ 가  $*$ '에 대한 항등원임도 쉽게 증명할 수 있습니다. 귀뜸만 하자면, 더 큰 군에서도 항등원으로서의 의무를 수행하며 살았는데 개가 부분군으로 이사 가더라도 여전히 (오히려 더 가벼운) 항등원으로서의 의무를 수행할 수 있다는 말을 증명으로 잘 바꾸면 된다고 말씀드리겠습니다.

조건 3이 성립함을 보이기에 앞서 주장 [1]을 증명하겠습니다.

주장 [1]:  $x * y = e$ 를 만족시키는 임의의  $x \in G$ 와  $y \in G$ 에 대하여  $y * x = e$ 이다.

*Proof of the claim.*  $x \in G$ 와  $y \in G$ 가  $x * y = e$ 를 만족시킨다고 가정하겠습니다. 이때  $z := y * x$ 로 두고,  $z * z = z$ 를 보이면 충분합니다. 그 까닭은 양변에  $z^{-1}$ 을 곱하여  $z = e$ 를

얻을 수 있기 때문입니다. 그런데

$$\begin{aligned}
 z * z &= (y * x) * (y * x) \\
 &= y * (x * (y * x)) \\
 &= y * ((x * y) * x) \\
 &= y * (e * x) \\
 &= y * x \\
 &= z
 \end{aligned}$$

가 도출되네요. 이로써 주장 [1]의 증명이 끝났습니다. □

이제  $H$ 에서 원소 하나를 뽑아  $a$ 라고 부르겠습니다. 그러면 보조 정리 (a)에 의하여 어떤  $b \in H$ 가 존재하여

$$a *' b = e \wedge (\forall h \in H) [a *' h = e \rightarrow b = h]$$

가 성립합니다. 이제 보조 정리 (a)를 군  $(G, *)$ 에 적용하면, 어떤  $x \in G$ 가

$$a * x = e \wedge (\forall y \in G) [a * y = e \rightarrow x = y]$$

를 만족시킴을 알 수 있는데,  $y$ 에  $b$ 를 넣음으로써  $x = b$ 를 얻습니다. 따라서  $a * b = e$ 를 얻게 되고, 주장 [1]에 의하여  $b * a = e$ 를 얻습니다. 이로써 조건 3의 증명이 끝났습니다.

(c) 이제  $G$ 의 부분 집합인  $H$ 가 조건 1, 2, 3을 모두 만족시킨다고 가정하겠습니다.

먼저,  $H$ 가  $*$  아래에 닫혀 있음을 보여야 하는데, 이는 조건 1이 보장합니다.

이제  $*'$ 을  $H$  위에서  $*$ 의 유도된 이항 연산이라고 하겠습니다. 그러면  $(H, *')$ 는 이항 구조가 되는데, 이것이 군임을 보이면 충분합니다. 그런데 이는  $S^1$ 이 군임을 보였던 과정을 반복하여 증명할 수 있습니다. □

여기서 흥미로운 점들 중 하나는 (거칠게 말하면) 보조 정리 (a)의 역이 성립한다는 사실입니다. 정확히 말씀드리자면, 조건 (10)과 (11)을 만족시키는 임의의 반군  $(G, *)$ 은 군입니다. 이를 증명하기 앞서 더 재밌는 정리를 증명해 보겠습니다!

## References

- [1] J.B. FRALEIGH. 현대대수학(제7판). Pearson, 2009.