

현대대수1및실습

임기정

임복희 교수님께서 담당하시는 2021년 1학기 현대대수1및실습 1 분반 안의, Noether 조의 이름으로 작성된 노트 정리입니다. 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 함¹은 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.

¹참고 문헌 [1] 20쪽, 정의 2.1 인용

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

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

와 같이 적을 수 있습니다.

이때 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.²

마그마 $(S, *)$ 가 군³(group)이 되기 위해서는 다음 세 조건을 만족시켜야 합니다:

1. 결합 법칙(associative law)⁴이 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)⁵이 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.⁶ 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.

²참고 문헌 [1] 38쪽 인용

³참고 문헌 [1] 37쪽, 정의 4.1 인용

⁴참고 문헌 [1] 23쪽, 정의 2.12 인용

⁵참고 문헌 [1] 32쪽, 정의 3.12 인용

⁶참고 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*)⁷을 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,

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

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

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

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

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

⁷참고 문헌 [1] 37쪽, 정의 4.1 인용

를 얻게 되고, 증명을 마칠 수 있습니다. □

참고로 결합 법칙을 만족시키는 마그마를 반군(*semigroup*)이라고 하고, 항등원이 존재하는 반군을 모노이드(*monoid*)라고 합니다.⁸ 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)⁹하다고 함은

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

이어야 한다는 뜻인데, $*$ 이 가환한 군을 아벨 군이라고 부릅니다.¹⁰

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)¹¹하면,

$$(S^1, *)$$

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.

⁸참고 문헌 [1] 42쪽 인용

⁹참고 문헌 [1] 22쪽, 정의 2.11 인용

¹⁰참고 문헌 [1] 38쪽, 정의 4.3 인용

¹¹참고 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 단계¹²로 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,

$$(a * b) * c = a * (b * c) \quad (6)$$

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 보증 서주기 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, 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

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

¹² $(S^1, *)$ 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, 아벨 군이기도 하는데, 이 사실 역시 $*$ 가 복소수의 곱셈으로부터 유도된 연산임을 이용하면 어렵지 않게 보일 수 있습니다.

증명을 하다 보니까 쓸데없는 호기심이 발동하네요. 모노이드 $(M, *)$ 이 주어졌다고 가정하고, M 의 항등원을 e 라고 하겠습니다. $e \notin M'$ 인 집합 $M' \subseteq M$ 을 무엇으로 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.

References

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