풀이

STEP III 1995, 문제 7

순수수학 • 군과 동형사상

> **STEP III 1995, 7번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/95-s3-q7

핵심 아이디어

결합법칙(associativity)은 주어져 있으므로, 각 집합에 대해 확인할 것은 세 가지뿐이다. 닫혀 있음(closure), 항등원(identity)의 존재, 그리고 모든 원소의 역원(inverse)의 존재이다. 이 중 하나라도 깨지면 그 집합은 군(group)이 아니며, 구체적인 반례(counterexample) 하나면 충분하다. 동형사상(isomorphism)에 대해서는 모든 동형사상이 보존해야 하는 구조적 특징, 즉 원소의 개수와 원소들의 위수(order)를 살펴본다.

풀이

이 풀이 전체에서 "곱셈"은 상황에 따라 복소수의 보통 곱셈, 법 n에 대한 곱셈, 또는 행렬 곱셈을 뜻한다.

소문항 (i)

$S = \{z \in \mathbb{C} : |z| = 1\}$이라 하자.

- **닫혀 있음**: $|z| = |w| = 1$이면 $|zw| = |z||w| = 1$이다.
- **항등원**: $1 \in S$이고 $1z = z1 = z$이다.
- **역원**: $|z| = 1$이면 $z \neq 0$이고, ($z\bar{z} = |z|^2 = 1$이므로) $z^{-1} = \bar{z}$이며, 이것의 절댓값도 1이다.

따라서 S는 (무한) 군이다.

소문항 (ii)

법 4에 대한 곱셈에서 집합 $\{0,1,2,3\}$은 닫혀 있고 항등원 1을 가지지만, 모든 b에 대해 $0 \times b \equiv 0 \not\equiv 1$이므로 0은 역원을 갖지 않는다. 따라서 이 집합은 군이 **아니다**. (0을 빼도 소용이 없다. $2b$는 항상 짝수이므로 2는 여전히 역원을 갖지 않으며, 사실 $2 \times 2 \equiv 0$이므로 $\{1,2,3\}$은 닫혀 있지조차 않다.)

소문항 (iii)

덧셈정리(compound-angle formulae)를 이용하면

$$\mathrm{M}(\alpha)\mathrm{M}(\beta) = \begin{pmatrix} c_\alpha c_\beta - s_\alpha s_\beta & -(s_\alpha c_\beta + c_\alpha s_\beta) \\ s_\alpha c_\beta + c_\alpha s_\beta & c_\alpha c_\beta - s_\alpha s_\beta \end{pmatrix} = \mathrm{M}(\alpha+\beta),$$

이다. 여기서 $c_\alpha = \cos\alpha$, $s_\alpha = \sin\alpha$ 등으로 썼다. cos와 sin의 주기(period)는 2π이므로, γ를 $\alpha+\beta$를 $[0,2\pi)$ 안으로 줄인 값이라 하면 $\mathrm{M}(\alpha+\beta) = \mathrm{M}(\gamma)$이다. 따라서 다음이 성립한다.

- **닫혀 있음**: 집합에 속한 두 행렬의 곱은 다시 이 집합에 속한다.
- **항등원**: $\mathrm{M}(0) = I$이다.
- **역원**: $0 < \theta < 2\pi$에 대해 $\mathrm{M}(\theta)\mathrm{M}(2\pi-\theta) = \mathrm{M}(2\pi) = I$이고, $\mathrm{M}(0)$은 자기 자신이 역원이다.

따라서 이 집합은 군이다.

소문항 (iv)

법 8에 대하여

$$3^2 = 9 \equiv 1, \qquad 5^2 = 25 \equiv 1, \qquad 7^2 = 49 \equiv 1,$$
$$3 \times 5 = 15 \equiv 7, \qquad 3 \times 7 = 21 \equiv 5, \qquad 5 \times 7 = 35 \equiv 3.$$

이다. 1이 포함된 자명한 곱까지 더하면 곱셈표 전체가 얻어지고(곱셈은 가환(commutative)이다), 모든 곱이 $\{1,3,5,7\}$에 속하므로 이 집합은 닫혀 있다. 항등원은 1이고, 각 원소는 자기 자신이 역원이다. 따라서 이것은 위수가 4인 군이며, 1이 아닌 모든 원소의 위수는 2이다.

소문항 (v)

단위행렬 I는 정수 성분을 가지고, 이 집합은 닫혀 있지만(정수의 곱과 합은 정수이다) 역원 조건이 성립하지 않는다. 영행렬은 아예 역행렬을 갖지 않는다. 가역인 행렬이라도 문제가

될 수 있다. $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$는 실수 행렬에서 역행렬 $\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix}$를 가지며, 역행렬은 유일하므로 A는 정수 성분의 역행렬을 갖지 않는다. 따라서 이 집합은 군이 아니다.

> **생각해 보기** 영행렬을 지목하는 것만으로 정말 충분할까, 아니면 모든 행렬에 대해 무언가를 말해야 할까?

집합이 군이 아님을 보이려면 역원이 없는 원소 하나면 충분하다. 두 번째 예는 문제가 특이 행렬(singular matrix)보다 더 깊은 곳에 있음을 보여 준다. 정수 행렬이 정수 역행렬을 가질 필요충분조건은 행렬식(determinant)이 ± 1인 것이다. 두 행렬식이 모두 정수이면서 $\det A \det A^{-1} = 1$이기 때문이다. 이런 행렬들로 제한하면 실제로 군이 된다.

소문항 (vi)

법 5에 대하여 2의 거듭제곱은

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8 \equiv 3, \quad 2^4 = 16 \equiv 1.$$

이다. 따라서 $\{1,2,3,4\} = \{2^0, 2^1, 2^2, 2^3\}$이고, 지수를 법 4로 읽으면 $2^a 2^b = 2^{a+b}$이다. 그러므로 이 집합은 닫혀 있고, 1이 항등원이며, 2^a의 역원은 2^{4-a}이다. 이것은 군이며, 2(또는 3)로 생성되는 위수 4의 순환군(cyclic group)이다.

동형사상

군인 것은 (i), (iii), (iv), (vi)이므로 짝은 여섯 개이다.

(i)과 (iii)은 동형이다. 절댓값이 1인 모든 복소수는 $0 \le \theta < 2\pi$인 $e^{i\theta}$ 꼴로 유일하게 쓸 수 있다. $\phi(e^{i\theta}) = M(\theta)$로 정의하자. $[0, 2\pi)$ 안의 서로 다른 θ는 서로 다른 행렬을 주므로(첫째 열 $(\cos\theta, \sin\theta)$가 θ를 결정한다) 이것은 전단사(bijection)이다. 또한 곱셈을 보존한다. $e^{i\alpha}e^{i\beta} = e^{i(\alpha+\beta)}$이고 $M(\alpha)M(\beta) = M(\alpha+\beta)$이며, 두 군 모두에서 각은 법 2π로 줄인다. 기하학적으로 두 군은 모두 원점을 중심으로 한 평면의 회전들이다.

(i) 또는 (iii)과 (iv) 또는 (vi): 동형이 아니다. 동형사상은 전단사이므로 두 군의 원소 개수가 같아야 한다. 군 (i)과 (iii)은 무한군이고, (iv)와 (vi)는 각각 원소가 네 개이다. 이것으로 네 짝이 해결된다.

> **생각해 보기** (iv)와 (vi)는 둘 다 원소가 네 개이고 둘 다 가환이다. 무엇으로 이 둘을 구별할 수 있을까?

(iv)와 (vi): 동형이 아니다. 동형사상 ϕ는 모든 원소의 위수를 보존한다. $\phi(g)^n = \phi(g^n)$이고, ϕ는 단사(injective)이며 항등원을 항등원으로 보내므로, 이것이 항등원일 필요충분조건은 g^n이 항등원인 것이다. (vi)에서 원소 2의 위수는 4이다. (iv)에서는 모든 원소 g가 $g^2 = 1$을 만족하므로 위수가 4인 원소가 없다. 따라서 동형사상은 존재하지 않는다.

정리하면, 동형인 짝은 (i)과 (iii)뿐이다.

검산

컴퓨터로 곱셈표 전체를 직접 조사하여 (iv)와 (vi)의 닫혀 있음, 항등원, 역원 성질을 확인했다. 그 결과 법 4에서 0과 2는 역원을 갖지 않고, 원소들의 위수는 (iv)에서 $1,2,2,2$, (vi)에서 ($1,2,3,4$에 대해) $1,4,4,2$임을 확인했다. 또한 10^4개의 무작위 각에서 $\mathrm{M}(\alpha)\mathrm{M}(\beta) = \mathrm{M}(\alpha+\beta)$와 $\mathrm{e}^{\mathrm{i}\theta}$와의 대응을 확인했다. (iv)는 손으로도 빠르게 확인할 수 있다. $(2k+1)^2 = 4k(k+1)+1$이고 $k(k+1)$은 짝수이므로, 어떤 홀수를 제곱해도 법 8로 1이 된다.

흔한 실수

- (iv)와 (vi)가 "둘 다 원소가 네 개이므로" 동형이라고 말하는 것. 크기가 같은 것은 필요조건이지만 충분조건은 아니다.
- (v)에서 $\det A \neq 0$만 확인하는 것. 역행렬도 정수 성분을 가져야 한다.
- (ii)를 법 4에 대한 덧셈으로 읽는 것. 덧셈에 대해서라면 위수 4의 순환군이 되어 (vi)와 동형이지만, 문제는 곱셈을 명시하고 있다.

STEP 너머

동형을 무시하면 위수 4인 군은 정확히 두 개이다. (vi)와 같은 순환군 C_4와, (iv)와 같은 클라인 4원군(Klein four-group) $C_2 \times C_2$이다. 원소의 위수로 작은 군들을 분류하는 것은 대학 군론 강의에서 가장 먼저 하는 일 중 하나이다. (i)과 (iii)의 원군(circle group)은 리 군(Lie group), 즉 매끄러운 곡선이나 곡면이기도 한 군의 가장 간단한 예이다. (v)에서 나온 행렬식이 ± 1인 정수 행렬들은 군 $\mathrm{GL}_2(\mathbb{Z})$를 이루며, 이 군은 정수론에서 중요하다. 더 읽어 보려면 Allenby의 *Rings, Fields and Groups*(환, 체, 군)가 좋은 출발점이다.

Beyond STEP 풀이: https://beyondstep.keithmcnulty.org/ko/. 풀이 글은 CC0 1.0이다. 문제 자체의 저작권은 © Cambridge University Press & Assessment에 있으며 여기에 싣지 않는다. 영어 원문을 기계 번역하였으며 아직 검토되지 않았다.