풀이

STEP II 1991, 문제 9

순수수학 • 행렬군

> **STEP II 1991, 9번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/91-s2-q9

핵심 아이디어

모든 것은 한 가지 사실에 기초한다. 5를 법으로 하는 정수는 체(field)를 이룬다. 즉 0이 아닌 모든 나머지(residue)는 곱셈에 대한 역원을 가지며, 0이 아닌 나머지들의 곱은 결코 0이 되지 않는다. 바로 이 성질 덕분에 대각 성분이 제대로 행동하므로, 닫힘성과 역원은 거의 공짜로 얻어진다. 마지막 부분에서는 $M^2 = I$를 풀어 위수(order)가 1 또는 2인 원소를 명시적으로 구한 다음, 그중 두 원소를 곱했을 때 여전히 그 집합 안에 머무르는지 확인한다.

풀이

이하 모든 계산은 5를 법으로 하며, 편의상 4를 -1로 쓰기도 한다. 일반적인 원소를 다음과 같이 쓴다.

$$M(a,b,c) = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \qquad a,c \in \{1,2,3,4\},\ b \in \{0,1,2,3,4\}.$$

G는 군이다

닫힘성(closure). 두 원소를 곱하면 다음을 얻는다.

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix}.$$

이것은 성분이 5를 법으로 하는 상삼각행렬(upper triangular matrix)이다. 대각 성분 ad와 cf는 0이 아니다. 5가 소수(prime)이므로 $5 \mid ad$이면 $5 \mid a$ 또는 $5 \mid d$인데, 어느 쪽도 성립하지 않기 때문이다. 따라서 곱은 G에 속한다.

결합법칙(associativity)은 행렬 곱셈이 결합적이므로 주어진 것이다.

항등원(identity). $I = M(1,0,1)$은 G에 속하고, 모든 M에 대하여 $IM = MI = M$이다.

역원(inverse). 5를 법으로 하는 0이 아닌 모든 나머지는 역원을 가진다($1^{-1} = 1, 2^{-1} = 3, 3^{-1} = 2, 4^{-1} = 4$). 따라서 $M(a,b,c) \in G$가 주어지면 다음 행렬을 만들 수 있다.

$$N = \begin{pmatrix} a^{-1} & -a^{-1}bc^{-1} \\ 0 & c^{-1} \end{pmatrix},$$

$a^{-1}, c^{-1} \neq 0$이므로 이 행렬은 G에 속한다. 곱셈 공식을 이용하면

$$MN = \begin{pmatrix} aa^{-1} & -aa^{-1}bc^{-1} + bc^{-1} \\ 0 & cc^{-1} \end{pmatrix} = I, \qquad NM = \begin{pmatrix} a^{-1}a & a^{-1}b - a^{-1}bc^{-1}c \\ 0 & c^{-1}c \end{pmatrix} = I.$$

따라서 모든 원소는 G 안에 역원을 가지며, G는 군(group)이다.

G의 위수

a를 고르는 방법은 4가지, b는 5가지, c는 4가지이고, 서로 다른 선택은 서로 다른 행렬을 준다. 따라서

$$|G| = 4 \times 5 \times 4 = 80.$$

G는 가환인가?

아니다. $A = M(1,1,1), B = M(2,0,1)$로 두면

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \qquad BA = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix},$$

이므로 $AB \neq BA$이고, G는 가환(commutative)이 아니다.

위수가 1 또는 2인 원소

원소 M의 위수가 1 또는 2일 필요충분조건은 $M^2 = I$이다. 곱셈 공식에 의해

$$M(a,b,c)^2 = \begin{pmatrix} a^2 & b(a+c) \\ 0 & c^2 \end{pmatrix},$$

이므로 $a^2 = 1, c^2 = 1, b(a+c) = 0$이어야 한다.

5를 법으로 $1, 2, 3, 4$의 제곱은 $1, 4, 4, 1$이므로, $a^2 = 1$이면 반드시 $a = \pm 1$이고, 마찬가지로 $c = \pm 1$이다.

- $a = c$이면 $a + c = \pm 2 \neq 0$이다. $\mathbb{Z}_5$에는 영인자(zero divisor)가 없으므로 $b(a+c) = 0$이면 $b = 0$이다. 이로부터 I와 $-I$를 얻는다.

- $c = -a$이면 $a + c = 0$이므로 b는 아무 값이어도 된다. 이로부터 $b = 0, 1, \ldots, 4$에 대한 10개의 행렬 $M(1, b, -1)$과 $M(-1, b, 1)$을 얻는다.

따라서 위수가 1 또는 2인 원소들의 집합 H는 정확히 12개의 원소를 가진다.

? 생각해 보기 자기 자신이 역원인 원소들의 집합은 자동으로 닫혀 있을까?

아니다. 이 집합은 I를 포함하고 각 원소가 자기 자신의 역원이므로, 항등원과 역원 공리는 자동으로 성립한다. 실패할 수 있는 것은 닫힘성뿐이며, 비가환군에서는 대개 실패한다. $X^2 = Y^2 = I$이면 $(XY)^2 = XYXY$인데, X와 Y가 교환되지 않는 한 이것이 I로 정리될 필요는 없다.

여기서도 닫힘성이 실패한다. H의 두 원소 $X = M(1, 1, -1)$과 $Y = M(1, 0, -1)$을 택하면

$$XY = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

이 행렬은 $a = c = 1$이지만 $b = -1 \neq 0$이므로, 앞의 분류에 의해 H에 속하지 않는다. (실제로 $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}$이므로 이 행렬의 위수는 5이다.) 따라서 H는 닫혀 있지 않으며, G의 부분군(subgroup)이 아니다.

라그랑주(Lagrange) 정리를 알고 있다면 더 빠른 논증이 있다. 부분군의 위수는 군의 위수를 나누어야 하는데, $12 \nmid 80$이다.

검산

80개의 행렬 전체를 컴퓨터로 간단히 나열해 보면 닫힘성, 역원 공식, 그리고 위의 쌍에 대해 $AB \neq BA$임이 확인된다. 모든 원소를 제곱해 보면 $M^2 = I$의 해는 예측한 대로 정확히 12개이고, $XY = M(1, 4, 1)$의 위수는 5이다. 손으로는 $M(-1, 3, 1)^2 = I$임을 확인해 보자. 비대각 성분은 $3(-1 + 1) = 0$이다.

흔한 실수

- 역원이 G에 속함을 보이는 것을 잊는 경우. 역원의 대각 성분 a^{-1}, c^{-1}이 0이 아니어야 한다.
- $M^2 = I$이면 M이 반드시 대각행렬이라고 가정하여, $b \neq 0$인 원소 $M(1, b, -1)$과 $M(-1, b, 1)$을 빠뜨리는 경우.
- H에 대해 항등원과 역원 공리만 확인하는 경우. 실패하는 공리는 닫힘성이다.

STEP 너머

G는 유한체(finite field) $\mathbb{F}_5$ 위의 가역 2×2 상삼각행렬들의 군으로, $\mathrm{GL}_2(\mathbb{F}_5)$의 **보렐 부분군**(*Borel subgroup*)이다. $a = c = 1$인 행렬들은 위수가 5인 정규부분군(normal subgroup)을 이루며, G는 이 부분군과 대각행렬들로부터 반직접곱(semidirect product)으로 만들어진다. 유한체 위의 행렬군은 군론 입문 강의에서 풍부한 예의 원천이 된다. 더 알고 싶다면 Allenby의 *Rings, Fields and Groups*(환, 체, 군)를 참고하라.

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.