풀이

STEP III 1989, 문제 3

순수수학 • 행렬군

STEP III 1989, 3번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

step.maths.org/questions/89-s3-q3

핵심 아이디어

$\mathbf{M}$은 $2\pi/m$만큼의 회전이므로 $\mathbf{M}^m = \mathbf{I}$이고, 그 거듭제곱의 합은 등비급수(geometric series)이다. 여기에 $\mathbf{I} - \mathbf{M}$을 곱하면 모든 항이 연쇄적으로 소거된다(telescope). 점화식(recurrence)은 $\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3$을 직접 써 보면 규칙이 분명히 보인다. 그다음 군(group)은 하나의 항등식에서 나온다. 이 식들 가운데 하나를 다른 하나에 대입하면 첨자가 더해질 뿐이므로, 원소들은 m을 법으로 하는 정수처럼 행동한다.

풀이

$\mathbf{M}$의 거듭제곱의 합

$\mathbf{M}$은 원점을 중심으로 $\theta = 2\pi/m$만큼 시계 반대 방향으로 회전하는 행렬이다. 이를 k번 적용하면 $k\theta$만큼 회전하므로

$$\mathbf{M}^k = \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix}, \qquad \text{특히} \qquad \mathbf{M}^m = \begin{pmatrix} \cos 2\pi & -\sin 2\pi \\ \sin 2\pi & \cos 2\pi \end{pmatrix} = \mathbf{I}.$$

($\mathbf{M}^{k+1} = \mathbf{M}\mathbf{M}^k$이므로 $\mathbf{M}^k$에 대한 공식은 덧셈정리(compound-angle formulae)로부터 귀납법(induction)으로 얻어진다.)

$\mathbf{S} = \mathbf{I} + \mathbf{M} + \cdots + \mathbf{M}^{m-1}$이라 하자. 이 행렬들은 모두 $\mathbf{M}$의 거듭제곱이므로 서로 교환 가능하고(commute), 곱은 연쇄적으로 소거된다.

$$(\mathbf{I} - \mathbf{M})\mathbf{S} = \mathbf{I} - \mathbf{M}^m = \mathbf{I} - \mathbf{I} = \mathbf{O}.$$

? **생각해 보기** 인수 $\mathbf{I} - \mathbf{M}$을 그냥 "약분"해도 될까?

$\mathbf{I}-\mathbf{M}$이 가역(invertible)일 때만 그렇다. 영행렬이 아닌 행렬들의 곱이 $\mathbf{O}$일 수도 있기 때문이다. 여기서

$$\det(\mathbf{I}-\mathbf{M}) = (1-\cos\theta)^2 + \sin^2\theta = 2-2\cos\theta,$$

이고, $m>1$이므로 $0<\theta\le\pi$이다. 따라서 $\cos\theta\neq 1$이고 행렬식(determinant)은 0이 아니다. $(\mathbf{I}-\mathbf{M})\mathbf{S}=\mathbf{O}$의 양변에 왼쪽에서 $(\mathbf{I}-\mathbf{M})^{-1}$을 곱하면 $\mathbf{S}=\mathbf{O}$를 얻으며, 이것이 증명하려던 결과이다.

$\mathbf{X}_k$에 대한 공식

처음 몇 항을 계산해 보면

$$\mathbf{X}_1 = \mathbf{P}\mathbf{X}_0+\mathbf{Q},\quad \mathbf{X}_2 = \mathbf{P}^2\mathbf{X}_0+\mathbf{P}\mathbf{Q}+\mathbf{Q},\quad \mathbf{X}_3 = \mathbf{P}^3\mathbf{X}_0+(\mathbf{P}^2+\mathbf{P}+\mathbf{I})\mathbf{Q},$$

이므로, $k\ge 0$에 대해 다음이 성립하리라고 추측할 수 있다.

$$\mathbf{X}_k = \mathbf{P}^k\mathbf{X}_0+\mathbf{S}_k\mathbf{Q},\qquad \text{여기서}\quad \mathbf{S}_k = \mathbf{I}+\mathbf{P}+\cdots+\mathbf{P}^{k-1}\quad(\mathbf{S}_0=\mathbf{O}).$$

$k=0$일 때 이 식은 $\mathbf{X}_0=\mathbf{X}_0$이 되므로 참이다. 어떤 $k\ge 0$에 대해 성립한다고 가정하자. 그러면

$$\begin{aligned}\mathbf{X}_{k+1} = \mathbf{P}\mathbf{X}_k+\mathbf{Q} &= \mathbf{P}^{k+1}\mathbf{X}_0+(\mathbf{P}+\mathbf{P}^2+\cdots+\mathbf{P}^k)\mathbf{Q}+\mathbf{Q}\\ &= \mathbf{P}^{k+1}\mathbf{X}_0+\mathbf{S}_{k+1}\mathbf{Q},\end{aligned}$$

이므로 $k+1$에 대해서도 성립하고, 귀납법에 의해 모든 $k\ge 0$에 대해 성립한다. 인수의 순서에 주의하라. $\mathbf{P}$는 처음부터 끝까지 왼쪽에서 곱해지며, $\mathbf{P}$와 $\mathbf{Q}$는 교환 가능하지 않을 수도 있다.

군

$\mathbf{X}_i$를 임의의 행렬 $\mathbf{X}_0$을 다른 행렬로 바꾸는 규칙, 즉 식 $\mathbf{P}^i\mathbf{X}_0+\mathbf{S}_i\mathbf{Q}$로 생각하자. $\mathbf{X}_0$ 자리에 $\mathbf{X}_j$를 대입하면

$$\begin{aligned}\mathbf{X}_i * \mathbf{X}_j &= \mathbf{P}^i(\mathbf{P}^j\mathbf{X}_0+\mathbf{S}_j\mathbf{Q})+\mathbf{S}_i\mathbf{Q}\\ &= \mathbf{P}^{i+j}\mathbf{X}_0+(\mathbf{P}^i\mathbf{S}_j+\mathbf{S}_i)\mathbf{Q}.\end{aligned}$$

이제 $\mathbf{P}^i\mathbf{S}_j = \mathbf{P}^i+\cdots+\mathbf{P}^{i+j-1}$이고, 여기에 $\mathbf{S}_i=\mathbf{I}+\cdots+\mathbf{P}^{i-1}$을 더하면 정확히 $\mathbf{S}_{i+j}$가 된다. 따라서 임의의 $\mathbf{P}$에 대해

$$\mathbf{X}_i * \mathbf{X}_j = \mathbf{X}_{i+j}.$$

(이는 놀라운 일이 아니다. 점화식을 j단계 진행한 뒤 i단계를 더 진행하는 것은 $i+j$단계를 진행하는 것과 같다.)

이제 $\mathbf{P} = \mathbf{M}$으로 두자. 첫 부분에 의해 $\mathbf{M}^m = \mathbf{I}$이고 $\mathbf{S}_m = \mathbf{O}$이므로

$$\mathbf{X}_m = \mathbf{X}_0,$$

즉 $\mathbf{X}_m$은 모든 행렬을 바꾸지 않고 그대로 두는 식이다. 그러면 임의의 k에 대해 $\mathbf{X}_{k+m} = \mathbf{X}_k * \mathbf{X}_m = \mathbf{X}_k$이므로, 식들의 수열은 주기 m으로 반복되고

$$G = \{\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \ldots\} = \{\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_m\}$$

는 유한집합이다. 군의 공리(group axioms)를 확인하자.

- **닫혀 있음**(*closure*). $\mathbf{X}_i * \mathbf{X}_j = \mathbf{X}_{i+j}$이고 $i + j \geq 1$이므로 이는 G에 속한다.
- **결합법칙**(*associativity*). $(\mathbf{X}_i * \mathbf{X}_j) * \mathbf{X}_k$와 $\mathbf{X}_i * (\mathbf{X}_j * \mathbf{X}_k)$는 모두 $\mathbf{X}_{i+j+k}$와 같다. (더 일반적으로, 대입은 함수의 합성이며 함수의 합성은 항상 결합법칙을 만족한다.)
- **항등원**(*identity*). $\mathbf{X}_m * \mathbf{X}_j = \mathbf{X}_{m+j} = \mathbf{X}_j$이고 $\mathbf{X}_j * \mathbf{X}_m = \mathbf{X}_j$이므로 $\mathbf{X}_m$이 항등원이다.
- **역원**(*inverses*). $1 \leq i < m$에 대해 $\mathbf{X}_i * \mathbf{X}_{m-i} = \mathbf{X}_{m-i} * \mathbf{X}_i = \mathbf{X}_m$이고, $\mathbf{X}_m$은 자기 자신의 역원이다. 각 역원은 G에 속한다.

따라서 G는 $*$에 대한 유한군이다.

실제로 이 군은 정확히 m개의 원소를 가진다. $\mathbf{X}_1, \ldots, \mathbf{X}_m$의 계수 $\mathbf{M}^1, \ldots, \mathbf{M}^m$은 $(0, 2\pi]$에 속하는 서로 다른 각만큼의 회전이므로, 이들은 서로 다른 식이기 때문이다. 모든 원소가 $\mathbf{X}_1$의 "거듭제곱"이므로 G는 위수(order)가 m인 순환군(cyclic group)이다.

검산

- $m = 2$이면 $\mathbf{M} = -\mathbf{I}$이고 합은 $\mathbf{I} + (-\mathbf{I}) = \mathbf{O}$이다. $m = 4$이면 $\mathbf{M}$은 4분의 1 회전이고 $\mathbf{I} + \mathbf{M} + \mathbf{M}^2 + \mathbf{M}^3 = \mathbf{I} + \mathbf{M} - \mathbf{I} - \mathbf{M} = \mathbf{O}$이다.
- 수치적으로 확인하면, 2부터 39까지의 모든 m에 대해 거듭제곱의 합은 (반올림 오차 범위에서) $\mathbf{O}$이다. 또한 임의로 고른 $\mathbf{P}$, $\mathbf{Q}$, $\mathbf{X}_0$에 대해 $\mathbf{X}_k$의 공식이 점화식과 일치하며, $\mathbf{P} = \mathbf{M}$이고 $\mathbf{Q}$와 $\mathbf{X}_0$을 임의로 고르면 점화식을 m단계 진행했을 때 정확히 $\mathbf{X}_0$으로 돌아온다.

흔한 실수

- $\mathbf{I} - \mathbf{M}$이 가역인지 확인하지 않고 약분하는 것.
- $\mathbf{Q}\mathbf{S}_k$나 $\mathbf{X}_0\mathbf{P}^k$로 쓰는 것. 행렬의 곱은 교환 가능하지 않으며, 점화식은 $\mathbf{P}$를 왼쪽에 둔다.
- $\mathbf{X}_0$을 항등원으로 보는 것. 위에 나열한 대로라면 $\mathbf{X}_0$은 G에 속하지 않는다. 항등원은 $\mathbf{X}_m$이며, 이것이 $\mathbf{X}_0$과 같은 것은 오직 $\mathbf{S}_m = \mathbf{O}$이기 때문이다.

STEP 너머

각 $\mathbf{X}_i$는 아핀 사상(affine map) $\mathbf{X} \mapsto \mathbf{AX} + \mathbf{B}$이고, $\mathbf{A}$가 가역인 아핀 사상들은 합성에 대해 군을 이룬다. 여기서 우리는 m제곱이 항등사상인 하나의 사상으로 생성되는, 위수 m의 순환 부분군을 찾은 것이다. $\mathbf{I} + \mathbf{M} + \cdots + \mathbf{M}^{m-1} = \mathbf{O}$라는 사실은 1의 m제곱근들의 합이 0이라는 사실의 행렬 버전이며, 그 일반적인 아이디어, 즉 군이 변환을 통해 집합에 작용한다는 생각은 군론(group theory) 첫 강의의 핵심이다. Allenby의 *Rings, Fields and Groups*(환, 체, 군)에서 이 내용을 발전시킨다.

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.