풀이

# STEP III 1990, 문제 3

순수수학 • 군의 공리와 켤레

> **STEP III 1990, 3번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/90-s3-q3

## 핵심 아이디어

세 소문항 모두 군의 공리(group axioms)만으로 해결되며, 각 소문항에서 유용한 수는 한 원소를 다른 원소를 써서 다시 나타내는 것이다. 위수(order)가 2인 원소는 자기 자신이 역원이므로, (i)은 한 줄짜리 계산이 된다. (ii)와 (iii)에서 쓰는 도구는 **켤레**(*conjugation*)이다. $x \mapsto c^{-1}xc$는 곱을 보존하므로 거듭제곱을 거듭제곱으로 보낸다.

이 풀이 전체에서 $x * y$를 $xy$로, 항등원을 $e$로 쓴다.

## 풀이

### 소문항 (i)

원소 $x$의 위수가 2일 필요충분조건은 $x \neq e$이고 $x^2 = e$인 것이다. 두 번째 조건은 $x^{-1} = x$라는 뜻이다. 따라서

$$a^{-1} = a, \qquad b^{-1} = b, \qquad (ab)^{-1} = ab.$$

군의 임의의 원소에 대하여 $(ab)^{-1} = b^{-1}a^{-1}$이다. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = e$이기 때문이다. 그러므로

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba,$$

이고, $a$와 $b$는 교환한다.

### 소문항 (ii)

먼저 $dc$가 $cd$의 켤레임에 주목한다.

$$c^{-1}(cd)\,c = (c^{-1}c)\,dc = dc.$$

**?** **생각해 보기** $dc = c^{-1}(cd)c$로 쓰는 것이 위수를 다루는 데 왜 도움이 될까?

켤레가 거듭제곱을 그대로 통과하기 때문이다. 임의의 $x$와 임의의 양의 정수 $n$에 대하여

$$(c^{-1}xc)^n = (c^{-1}xc)(c^{-1}xc)\cdots(c^{-1}xc) = c^{-1}x^nc,$$

이다. 가운데에서 이웃한 $c\,c^{-1}$ 쌍이 모두 소거되기 때문이다. $x = cd$로 두면 $(dc)^n = c^{-1}(cd)^nc$를 얻는다. 이제

$$(dc)^n = e \iff c^{-1}(cd)^nc = e \iff (cd)^n = cec^{-1} = e,$$

이다. 여기서 두 번째 단계는 왼쪽에 $c$를, 오른쪽에 $c^{-1}$을 곱한 것이다(역방향은 $c^{-1}$과 $c$를 곱한다). 따라서 $(cd)^n = e$를 만족하는 양의 정수 $n$은 $(dc)^n = e$를 만족하는 양의 정수 $n$과 정확히 같다. 위수는 이러한 $n$ 중 가장 작은 것이므로, $cd$와 $dc$의 위수는 같다. 이러한 $n$이 없으면 둘 다 위수가 무한이므로, 이 경우에도 명제가 성립한다.

### 소문항 (iii)

$c^{-1}bc = b^r$이 주어져 있다. 양의 정수 $s$에 대하여, (ii)의 연쇄 소거(telescoping) 논법을 쓰면

$$c^{-1}b^sc = (c^{-1}bc)^s = (b^r)^s = b^{sr}.$$

$s = 0$일 때도 같은 식이 성립한다(양변이 모두 $e$이다). $s$가 음수이면 $t > 0$인 $t$로 $s = -t$라 쓰자. 그러면 $(c^{-1}b^tc)(c^{-1}b^{-t}c) = e$이므로 $c^{-1}b^sc = (c^{-1}b^tc)^{-1}$이다. 따라서

$$c^{-1}b^sc = (b^{tr})^{-1} = b^{-tr} = b^{sr}.$$

그러므로 모든 정수 $s$에 대하여 $c^{-1}b^sc = b^{sr}$이다.

두 번째 결과는 $n \geq 1$에 대한 수학적 귀납법(induction)으로 보이되, 모든 정수 $s$에 대하여 한꺼번에 보인다. $n = 1$인 경우는 방금 증명한 것이다. 모든 정수 $s$에 대하여 $c^{-n}b^sc^n = b^{sr^n}$이라고 가정하자. 그러면

$$\begin{aligned} c^{-(n+1)}\,b^s\,c^{n+1} &= c^{-1}(c^{-n}b^sc^n)c \\ &= c^{-1}\,b^{sr^n}\,c \\ &= b^{(sr^n)r} = b^{sr^{n+1}}, \end{aligned}$$

이다. 여기서 마지막 줄은 첫 번째 결과에서 $s$ 대신 정수 $sr^n$을 넣은 것이다. 이로써 귀납법이 완성되므로, 모든 양의 정수 $n$에 대하여 $c^{-n}b^sc^n = b^{sr^n}$이다.

**?** **생각해 보기** 첫 번째 결과를 굳이 음수 $s$에 대해서도 증명한 이유는 무엇일까?

$r$이 음수이면(예를 들어 정이면체군(dihedral group)에서 $c^{-1}bc = b^{-1}$인 경우), $s$가 양수일 때에도 $sr^n$은 음수가 될 수 있고, 귀납 단계에서는 $s$ 대신 $sr^n$을 넣어 첫 번째 결과를 적용한다. 첫 번째 결과를 모든 정수 $s$에 대하여 증명해 두면 $r$의 부호에 상관없이 귀납법이 작동한다.

## 검산

작은 군에서 확인해 보자. 정사각형의 대칭에서 두 대각선에 대한 반사와 그 곱(반 바퀴 회전)은 모두 위수가 2이고, (i)이 예측하는 대로 두 반사는 실제로 교환한다. $S_3$에서 $c = (12)$, $d = (13)$으로 잡으면 $cd$와 $dc$는 두 개의 3-순환이고, 둘 다 위수가 3이다. (iii)의 경우, 정이면체군에서 반사 $c$와 회전 $b$는 $c^{-1}bc = b^{-1}$을 만족하므로 $r = -1$이고, 공식은 $c^{-n}b^sc^n = b^{(-1)^n s}$를 예측한다. 이는 옳다. 반사로 두 번 켤레를 취하면 아무 변화도 없기 때문이다. 또한 세 명제를 모두 컴퓨터로 확인하였다. $S_4$의 조건에 맞는 모든 원소에 대하여((i)은 $S_5$에 대해서도) 빠짐없이 확인하였고, 13을 법으로 하는 사상 $x \mapsto ux + v$들의 군에서도 확인하였다.

## 흔한 실수

- $(ab)^{-1} = a^{-1}b^{-1}$로 쓰는 것. 순서가 뒤바뀌며, 바로 그 뒤바뀜 덕분에 (i)이 성립한다.
- (ii)에서 $(cd)^n = e \Rightarrow (dc)^n = e$만 증명하는 것. 양방향이 모두 필요하며(또는 대칭성을 써서 $c$와 $d$의 역할을 바꾼다), 위수가 무한인 경우도 언급해야 한다.
- (iii)의 두 번째 결과를 귀납법 대신 점 세 개를 찍어 "증명"하는 것.

## STEP 너머

사상 $x \mapsto c^{-1}xc$는 군의 **자기 동형 사상**(*automorphism*)이다. 즉 $G$에서 자기 자신으로 가는 전단사 함수(bijection)로서 연산을 보존하므로, 위수를 보존하고 거듭제곱을 거듭제곱으로 보낸다. 소문항 (iii)은 **반직접곱**(*semidirect product*)의 핵심 관계식이다. $b$와 $c$로 생성되고 $c^{-1}bc = b^r$을 만족하는 군에는 정이면체군($r = -1$)과, 소수를 법으로 하는 사상 $x \mapsto ux + v$들의 군이 포함된다. Allenby의 *Rings, Fields and Groups*(환, 체, 군)는 켤레와 이러한 예들을 꼼꼼하게 전개한다.

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.