풀이

STEP III 1988, 문제 9

순수수학 • 군 원소의 위수

> **STEP III 1988, 9번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/88-s3-q9

핵심 아이디어

소문항 (i)은 나눗셈 정리(division algorithm)를 모양만 바꾼 것이다. N을 n의 배수와 나머지의 합으로 쓰면, n의 최소성 때문에 나머지가 0이 될 수밖에 없다. 소문항 (ii)가 성립하는 까닭은 g에 의한 켤레(conjugation)가 곱을 보존하기 때문이다. 그래서 켤레들의 곱에서는 안쪽의 $g^{-1}g$ 쌍이 모두 소거된다. 소문항 (iii)에서는 g에 의한 켤레를 거듭 적용한다. $g^5 = e$이므로 다섯 번 적용하면 h가 자기 자신으로 돌아오고, 이로부터 h의 위수(order)가 결정된다.

풀이

소문항 (i)

나눗셈 정리에 의해 q를 정수, $0 \le r < n$으로 하여 $N = qn + r$로 쓸 수 있다. (이는 0이나 음의 정수를 포함하여 모든 정수 N에 대해 성립한다.) 그러면 $g^n = e$이므로

$$e = g^N = (g^n)^q \, g^r = e^q g^r = g^r.$$

만약 r이 양수라면, r은 $g^r = e$를 만족하는 n보다 작은 양의 정수가 되는데, 이는 $n = o(g)$를 그러한 정수 중 **가장 작은** 것으로 정의한 데에 모순이다. 따라서 $r = 0$이므로 $N = qn$이고, n은 N을 나눈다.

소문항 (ii)

$m = 0$인 경우: 양변이 모두 e이다.

$m \ge 1$인 경우: m에 대한 수학적 귀납법(induction)을 쓴다. $m = 1$인 경우는 자명하다.

$gh^m g^{-1} = (ghg^{-1})^m$이라 하면

$$(ghg^{-1})^{m+1} = (ghg^{-1})^m (ghg^{-1}) = (gh^m g^{-1})(ghg^{-1})$$
$$= gh^m (g^{-1}g)hg^{-1} = gh^{m+1}g^{-1},$$

이므로 귀납법이 완성된다. (풀어 쓰면 $(ghg^{-1})(ghg^{-1})\cdots(ghg^{-1})$은 연쇄적으로 소거(telescoping)된다. 즉 가운데에 있는 모든 $g^{-1}g$가 소거된다.)

$m \leq -1$인 경우: 먼저 ghg^{-1}의 역원(inverse)은 $gh^{-1}g^{-1}$이다. 왜냐하면

$$(ghg^{-1})(gh^{-1}g^{-1}) = gh(g^{-1}g)h^{-1}g^{-1} = ghh^{-1}g^{-1} = e.$$

이제 $k \geq 1$로 하여 $m = -k$로 쓰자. h 대신 원소 h^{-1}에 양수인 경우의 결과를 적용하면

$$gh^m g^{-1} = g(h^{-1})^k g^{-1} = (gh^{-1}g^{-1})^k = ((ghg^{-1})^{-1})^k = (ghg^{-1})^{-k} = (ghg^{-1})^m.$$

따라서 이 항등식은 모든 정수 m에 대해 성립한다.

소문항 (iii)

$ghg^{-1} = h^2$를 쓰고, 이어서 $m = 2$일 때의 소문항 (ii)를 쓰면

$$g^2hg^{-2} = g\,(ghg^{-1})\,g^{-1} = gh^2g^{-1} = (ghg^{-1})^2 = (h^2)^2 = h^4,$$

이므로 원하는 결과를 얻는다.

같은 단계를 매번 똑같이 적용할 수 있다. 모든 $k \geq 0$에 대해 $g^k hg^{-k} = h^{2^k}$임을 보이자. $k = 0$일 때 이는 참이고, k일 때 성립한다면 $m = 2^k$일 때의 소문항 (ii)에 의해

$$g^{k+1}hg^{-(k+1)} = g\,(g^k hg^{-k})\,g^{-1} = gh^{2^k}g^{-1} = (ghg^{-1})^{2^k} = (h^2)^{2^k} = h^{2^{k+1}}.$$

$k = 5$로 두고 $g^5 = e$(따라서 $g^{-5} = e$이기도 하다)를 이용한 뒤 h^{-1}을 곱하면 다음을 얻는다.

$$h = g^5 hg^{-5} = h^{32}, \qquad \text{따라서} \qquad h^{31} = e$$

생각해 보기 우리는 $h^{31} = e$임을 안다. 왜 이로부터 $o(h)$가 단지 31 이하인 것이 아니라 정확히 31이 되는가?

소문항 (i)에 의해 $o(h)$는 31을 나눈다. 31은 소수(prime)이므로 $o(h)$는 1 또는 31이다. 그런데 $o(h) = 1$이면 $h = e$인데, 문제에서 그렇지 않다고 했다. 그러므로

$$o(h) = 31.$$

이러한 군은 실제로 존재하므로 주어진 조건들은 모순이 없다. 31을 법으로 하여 $h(x) = x + 1$, $g(x) = 2x$로 주어지는 $\{0, 1, \ldots, 30\}$의 치환(permutation)을 생각하자. 그러면 $g^5(x) = 32x = x$이고 $ghg^{-1}(x) = 2(\frac{x}{2} + 1) = x + 2 = h^2(x)$이며, h의 위수는 실제로 31이다.

검산

- 소수 31이 나오는 것은 자연스럽다. g에 의한 켤레는 h의 거듭제곱에 "지수에 2를 곱한다"로 작용하고, 다섯 번 두 배를 하면 처음으로 돌아와야 하므로 $o(h)$를 법으로 $2^5 \equiv 1$이다. 다시 말해 $o(h)$는 $2^5 - 1 = 31$을 나눈다.
- 31을 법으로 한 치환 $g(x) = 2x$와 $h(x) = x + 1$로 컴퓨터 검산을 하여 $g^5 = e$, $ghg^{-1} = h^2$, $k = 0, \ldots, 5$에 대해 $g^k h g^{-k} = h^{2^k}$, 그리고 $o(h) = 31$임을 확인하였다. 또한 수백 개의 무작위 치환에 대해 $-12 \leq m \leq 12$의 범위에서 (i)과 (ii)를 시험하였다.

흔한 실수

- (ii)에서 $m \geq 1$인 경우만 증명하는 것. 문제에서는 **임의의 정수**라고 했으므로 $m = 0$과 음수 m에 대해서도 각각 (짧은) 논증이 필요하다.
- $h^{31} = e$로부터 곧바로 $o(h) = 31$이라고 결론짓는 것. 이것으로는 $o(h) \mid 31$만 알 수 있다. 31이 소수라는 사실과 $h \neq e$라는 조건도 함께 필요하다.

STEP 너머

사상 $x \mapsto gxg^{-1}$은 G의 **자기동형사상**(automorphism), 즉 구조를 보존하는 전단사(bijection)이며, 소문항 (ii)는 그 결과 중 하나이다. 소문항 (iii)은 **반직접곱**(semidirect product)의 작은 예이다. g와 h로 생성되는 군의 위수는 $5 \times 31 = 155$이고, 이 군이 존재하는 것은 31을 법으로 2의 위수가 5이기 때문이다. 이러한 구성은 위수가 작은 군을 분류하는 데 핵심적인 역할을 한다. 위수, 켤레, 라그랑주 정리(Lagrange's theorem)에 대해서는 Allenby의 *Rings, Fields and Groups*(환, 체, 군)를 읽어 보기를 권한다.

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.