풀이

STEP III 1993, 문제 5

순수수학 • 군과 사원수

> **STEP III 1993, 5번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/93-s3-q5

이 문제는 *Beyond STEP*의 6.7 절 **사원수군**에서 단계별 안내와 함께 자세히 다룬다: https://beyondstep.keithmcnulty.org/ko/ch06/quaternions.html

핵심 아이디어

이 연산은 임의로 정한 것처럼 보이지만, 첫 번째 부분의 네 가지 곱을 보면 그 구조가 드러난다. $(z,0)$ 꼴의 쌍은 보통의 복소수처럼 곱해지고, 두 번째 자리는 $j^2=-1$을 만족하는 새로운 기호 j처럼 행동한다. 이 기호는 자신이 지나가는 모든 것을 켤레(conjugate)로 바꾼다. 이 네 가지 곱을 구하고 나면, S_1의 여덟 원소는 $u\in\{1,i,-1,-i\}$에 대하여 $(u,0)$과 $(0,u)$일 뿐이다. 따라서 닫힘, 역원, 위수는 몇 줄의 일반적인 계산으로 얻어지며, 64칸짜리 표를 만들 필요가 없다.

풀이

결합법칙과 교환법칙

$z=(z_1,z_2)$, $w=(w_1,w_2)$, $u=(u_1,u_2)$라 하자. 풀이 전체에서 $(ab)^*=a^*b^*$, $(a\pm b)^*=a^*\pm b^*$, $a^{**}=a$를 사용한다. 먼저

$$z\circ w=(z_1w_1-z_2w_2^*,\ z_1w_2+z_2w_1^*),$$

이므로 $(z\circ w)\circ u$의 두 성분은 다음과 같다.

$$(z_1w_1-z_2w_2^*)u_1-(z_1w_2+z_2w_1^*)u_2^*=z_1w_1u_1-z_1w_2u_2^*-z_2w_1^*u_2^*-z_2w_2^*u_1,$$
$$(z_1w_1-z_2w_2^*)u_2+(z_1w_2+z_2w_1^*)u_1^*=z_1w_1u_2+z_1w_2u_1^*+z_2w_1^*u_1^*-z_2w_2^*u_2.$$

한편 $w \circ u = (w_1u_1 - w_2u_2^*,\ w_1u_2 + w_2u_1^*)$이므로 $z \circ (w \circ u)$의 두 성분은 다음과 같다.

$$z_1(w_1u_1 - w_2u_2^*) - z_2(w_1u_2 + w_2u_1^*)^* = z_1w_1u_1 - z_1w_2u_2^* - z_2w_1^*u_2^* - z_2w_2^*u_1,$$
$$z_1(w_1u_2 + w_2u_1^*) + z_2(w_1u_1 - w_2u_2^*)^* = z_1w_1u_2 + z_1w_2u_1^* + z_2w_1^*u_1^* - z_2w_2^*u_2.$$

우변이 항별로 일치하므로 $\circ$는 결합법칙(associativity)을 만족한다.

교환법칙(commutativity)은 성립하지 않는다. 예를 들어

$$(0,1) \circ (i,0) = (0-0,\ 0+1\cdot i^*) = (0,-i), \qquad (i,0) \circ (0,1) = (0-0,\ i\cdot 1+0) = (0,i).$$

네 가지 곱

정의에 $\circ$을 대입하면

$$(z,0) \circ (w,0) = (zw,\ 0), \qquad (z,0) \circ (0,w) = (0,\ zw),$$
$$(0,z) \circ (w,0) = (0,\ zw^*), \qquad (0,z) \circ (0,w) = (-zw^*,\ 0).$$

집합 S_1

$U = \{1, i, -1, -i\}$라 하자. 그러면

$$S_1 = \{(u,0) : u \in U\} \cup \{(0,u) : u \in U\},$$

이고, A, C, E, G는 첫 번째 종류, B, D, F, H는 두 번째 종류이다.

닫힘. 집합 U는 곱셈, 켤레복소수 취하기($i^* = -i$), 부호 바꾸기에 대하여 닫혀 있다. 네 가지 곱에 의해 S_1의 두 원소의 곱은 $z, w \in U$에 대하여 $(zw,0)$, $(0,zw)$, $(0,zw^*)$, $(-zw^*,0)$ 중 하나이다. zw와 $\pm zw^*$는 모두 U에 속하므로, 모든 곱은 S_1에 속한다. 즉 S_1은 닫혀(closure) 있다.

항등원. 임의의 $(w_1,w_2) \in S$에 대하여

$$(1,0) \circ (w_1,w_2) = (w_1,\ w_2), \qquad (w_1,w_2) \circ (1,0) = (w_1,\ w_2\cdot 1^*) = (w_1,w_2),$$

이므로 $A = (1,0)$은 양쪽 항등원(identity)이며, S_1에 속한다.

역원과 위수. 첫 번째 종류의 원소에 대해서는 $(z,0) \circ (w,0) = (zw,0)$이므로, 이들은 U의 복소수와 똑같이 행동한다. 따라서 A는 위수(order) 1이고 자기 자신이 역원(inverse)이며, $E = (-1,0)$은 위수 2이고 자기 자신이 역원이다. 또 $C = (i,0)$과 $G = (-i,0)$은 각각 위수 4이고 서로의 역원이다.

> ? **생각해 보기** 두 번째 종류의 원소를 제곱하면 무엇이 되는가?

네 가지 곱 중 마지막 것에 의해, $u \in U$에 대하여

$$(0,u) \circ (0,u) = (-uu^*,\ 0) = (-|u|^2,\ 0) = (-1,0) = E.$$

따라서 B, D, F, H는 모두 제곱하면 E가 된다. E의 위수가 2이므로, 이들은 각각 위수 4이다. 역원을 구하자. $(0,u)\circ(0,w) = (-uw^*, 0)$이 $(1,0)$과 같을 필요충분조건은 ($uu^* = 1$을 이용하면) $w^* = -1/u = -u^*$, 즉 $w = -u$이다. 반대 순서로 확인해 보면 $(0,-u)\circ(0,u) = (uu^*, 0) = (1,0)$도 성립한다. 따라서 $(0,u)$의 역원은 $(0,-u)$이다.

정리하면 다음과 같다.

원소	A	B	C	D	E	F	G	H
역원	A	F	G	H	E	B	C	D
위수	1	4	4	4	2	4	4	4

군. 이제 네 공리를 모두 확인했다. S_1은 $\circ$에 대하여 닫혀 있다. 연산은 S 전체에서 결합법칙을 만족하므로, 특히 S_1에서도 만족한다. $A \in S_1$은 항등원이고, 모든 원소는 S_1 안에 역원을 가진다. 따라서 S_1은 $\circ$에 대하여 위수 8인 군(group)이다. 이 군은 비아벨군(non-abelian group)이다. $B\circ C = H$이지만 $C\circ B = D$이기 때문이다.

부분군과 행렬

위의 곱을 이용하면 $B = (0,1)$의 거듭제곱은

$$B^2 = E, \qquad B^3 = E\circ B = (-1,0)\circ(0,1) = (0,-1) = F, \qquad B^4 = E\circ E = A.$$

따라서 $\{A, B, E, F\} = \{B^0, B^1, B^2, B^3\}$은 B가 생성하는 순환 부분군(cyclic subgroup)이다. $B^m \circ B^n = B^{m+n}$이고 지수를 법 4에 대하여 줄일 수 있으므로 이 집합은 닫혀 있으며, A와 각 B^k의 역원 B^{4-k}를 포함한다. 따라서 이것은 위수 4인 부분군이다.

$M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$이라 하자. 그러면

$$M^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I, \qquad M^3 = -M, \qquad M^4 = I,$$

이므로 M이 생성하는 군은 $\{I, M, -I, -M\}$이며, 이 역시 위수 4인 순환군이다. 위수가 같은 두 순환군은 항상 동형(isomorphic)이다. 여기서 사상

$$A \mapsto I, \quad B \mapsto M, \quad E \mapsto -I, \quad F \mapsto -M,$$

즉 $B^k \mapsto M^k$는 전단사(bijection)이고 $B^m \circ B^n = B^{m+n} \mapsto M^{m+n} = M^m M^n$을 만족한다. 따라서 두 군은 **동형이다.**

검산

- 원소의 위수는 군의 위수를 나눈다. 위수 1, 2, 4는 모두 8을 나누고, 부분군에서는 2와 4가 4를 나눈다.

- 복소수 관점: $(z,0)\circ(w,0) = (zw,0)$이므로 $C\circ C = (i^2,0) = E$이며, 이는 정확히 $i^2 = -1$과 같다.
- 짧은 컴퓨터 검사로 복소수 쌍의 무작위 세 쌍 10 000개에 대하여 결합법칙을 확인했고, 8×8 곱셈표 전체를 만들어 닫힘, 항등원, 위의 역원과 위수, 그리고 $B\circ C = H \neq D = C\circ B$를 확인했으며, $B^k \mapsto M^k$가 곱셈을 보존함을 확인했다.

흔한 실수

- 켤레를 빠뜨리는 것: $(0,z)\circ(w,0)$은 $(0,zw)$가 아니라 $(0,zw^*)$이다. 교환법칙이 성립하지 않는 이유가 바로 여기에 있다.
- 수치 예 하나로 결합법칙을 보이는 것. 예는 법칙이 **성립하지 않음**을 보일 수는 있지만, 법칙을 증명하려면 일반적인 전개가 필요하다.
- 한 군은 복소수의 쌍으로, 다른 군은 행렬로 이루어져 있다는 이유로 "동형이 아니다"라고 결론 내리는 것. 동형은 곱셈의 구조에 관한 것이지, 원소가 무엇인지에 관한 것이 아니다.

STEP 너머

이 연산은 해밀턴(Hamilton)의 **사원수**(*quaternion*) 곱셈이다. 쌍 (z_1,z_2)는 $z_1 + z_2 j$를 나타내며, 여기서 $j^2 = -1$이고 $jz = z^* j$이다. 군 S_1은 **사원수군**(*quaternion group*) $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$이다. 이 군은 모든 부분군이 정규부분군(normal subgroup)인 가장 작은 비아벨군이며, 위수 8인 또 다른 비아벨군(정사각형의 대칭군)과는 위수 2인 원소가 단 하나뿐이라는 점에서 다르다. Allenby의 *Rings, Fields and Groups*(환, 체, 군)는 위수가 작은 군과 사원수를 다룬다.

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.