한국수학사학회지 제19권 제1호(2006년 2월), 33-42

조합대상의 동형사상 문제의 특성화와 역사적 고찰

한양대학교 자연과학대학 수학과 **박홍구**
hpark@hanyang.ac.kr

본 논문은 조합론 분야에서 매우 중요하게 다루는 조합대상들의 동형문제에 관한 이론적 배경의 연구와 아울러 역사적 배경을 고찰해본다. 또한, 유한체에서 케일리대상들의 동형사상 문제에 대한 부분적인 결과를 소개한다.

주제어 : 조합대상, 케일리대상, 그래프, 디자인, 유한체, 치환다항식

0. 서론

본 장에서는 조합대상의 동형문제와 관련된 몇 가지 중요하고 기초적인 정의들을 소개하기로 한다.

임의의 한 첨수집합(index set) G에 대해 꼭지점(vertex)들의 집합 $V=\{v_a | a\in G\}$와 $V\cup 2^V\cup 2^{2^V}\cup\cdots$의 부분집합으로 이루어진 구조(structure) S를 갖는 대상(object)을 G의 조합대상(combinatorial object)이라 말하고, $C=[G, S]$로 표기한다. 조합대상의 구체적인 예로, 그래프(graph), 다이그래프(digraph), 순환그래프(circulant graph), 디자인(design)등이 있다. 만일, 주어진 두 조합대상 C와 D 사이에 전단사함수가 존재해서 이 함수가 두 조합대상의 구조를 보전할 경우, 이 함수를 두 조합대상 C와 D의 동형사상(isomorphism)이라 정의한다. 조합대상 $C=[G, S]$에서 자기 자신으로 가는 동형사상을 C의 자기동형사상(automorphism)이라 하고 이러한 자기동형사상들의 집합 $Aut(C)$는 함수결합의 연산에 관해 군을 형성하며, G에서의 대칭군(symmetric group) S_G의 부분군이 된다. G가 유한군일 때, G의 임의의 한 원소 a와 모든 $x\in G$에 대해 사상 $t_a : G\to G$를 $t_a(x)=x+a$로 정의할 경우, T를 모든 평행이동(translation) $t_a(x)$들의 집합이라 말한다. 만일 T가 $Aut(C)$의 부분집합이 될 경우 G의 조합대상 $C=[G, S]$를 G의 케일리대상(Cayley object)이라 정의한다(참조: [2]). 이와 같이 정의된 C의 꼭지점들의 집합은

$V=\{v_a | a\in G\}$가 된다. 집합족 $K=\{S\in V\cup 2^V\cup 2^{2^V}\cdots\}$의 한 부분집합족 Λ에 대해, V와 Λ의 모든 원소 S로 구성된 G의 케일리대상 $C=[G, S]$들의 집합을 Ω라 하자. 이때, Ω의 모든 대상들이 서로 동형이 되면 G는 Λ에 대해 CI-성질(CI-property)을 만족한다고 말하거나 혹은 G를 Λ-CI-군(Λ-CI-group)이라 부른다. 만일 G가 K에 대해 CI-성질을 만족하면 G를 간단히 CI-군이라 부른다. 여기서, CI는 케일리 동형사상(Cayley isomorphism)의 약자를 의미한다.

양정수 n에 대해 $N=\{0, 1, \cdots, n-1\}$의 부분집합 S가 $-S\equiv S \pmod n$을 만족할 때, 꼭지점들의 집합 $\{v_0, v_1, \cdots, v_{n-1}\}$과 모서리들의 집합 E로 구성된 그래프가 다음조건을 만족할 경우 이 그래프를 순환그래프(circulant graph)라 정의하고 $G(n, S)$로 표기 한다. 즉, $i, j\in N$에 대해, $v_iv_j\in E \Leftrightarrow j-i \pmod n\in S$.

1. 케일리 대상의 동형문제

1930년부터 오늘에 이르기까지 조합대상의 동형문제에 대한 연구 및 역사적 배경은 크게 두 가지로 분류해 생각해볼 수 있다. 즉, 아담의 추론(Adam's conjecture)([1])과 배이스(Bays)([5])와 램바씨(Lambossy)([11])에 의해 제기된 유한소수체(finite prime field)의 케일리대상들의 동형문제에 대한 일반화이다. 그간 연구의 주된 형태는 아담의 추론을 해결할 수 있는 이론의 정립과 이의 일반화이었다. 특히, 1970년대 그리고 1980년대에 걸쳐 수많은 수학자들에 의해 집중적으로 연구되어져 왔으며, 괄목할만한 많은 결과들이 발표되었다. 이에 비해 두 번째의 경우 일반적인 대상 즉 유한체(finite field)의 케일리대상에 대한 동형문제는 극히 소수에 의해서만 다루어져왔다.

다음 1.1절 그리고 1.2절을 통해 아담의 추론과 관련된 케일리대상의 동형사상 문제와 주요결과들을 중심으로 동형문제의 이론적 배경 및 역사적 배경을 분석해 본다. 또한, G가 일정한 조건을 갖는 유한체일 때 G의 케일리대상들의 동형사상에 관한 몇 가지 성질을 유도하며, 유한체에서 치환다항식의 기본성질들을 적용하여 이 두 조합대상 사이의 동형사상을 치환다항식으로 표현해 보도록 한다.

1.1. 아담의 추론

현재까지 케일리대상의 주된 동형문제는 1967년 아담이 논문[1]에서 제기한 10가지 문제들 중의 하나에서부터 시작되었다. 여기서 제시된 문제는 다음과 같으며 오늘날 아담의 추론으로 불리고 있다.

[아담의 추론, 1967] 임의의 두 순환그래프 $G(n, S)$와 $G(n, S')$이 동형이 되기 위한 필요충분조건은, $S = uS'$을 만족하는 단위원소(unit) u가 N내에 존재할 때이다.

위의 아담의 추론에서 주어진 순환그래프는 당연히 Z_n의 케일리대상이 되며, 만일 $\gcd(n, u) = 1$일 경우 아담의 추론이 성립함을 어렵지 않게 보일 수 있다(참조: [3, 5, 11]). 이 이외 일반적인 경우 이 추론이 성립하는지를 보이는 문제는 그렇게 간단하지가 않다. 더 나아가 위의 추론이 성립할 수 있는 케일리대상을 구체적으로 찾는 문제는 매우 어려운 문제임을 알 수 있다. 위수가 n인 유한군인 경우 위수의 형태에 따라 케일리대상의 구조를 정확히 파악한다는 것은 매우 어렵기 때문이다. 아담의 추론에 대한 반례는 1970년 엘스파스(Elspas)와 터너(Turner)에 의해 처음으로 제기되었으며, 이들은 논문 [9]를 통해 꼭지점들의 수가 8인 유향그래프(directed graph)와 꼭지점들의 수가 16인 비유향그래프(undirected graph)는 아담의 추론을 만족하지 못한다는 사실을 밝혔다. 이를 시점으로 1970년대에 걸쳐 수많은 반례들이 찾아졌다. 참고로 그래프의 형태에 따라 1970-1980년대에 찾아진 주요 반례들을 요약하면 다음 <표 1>과 같다.

<표 1> 아담의 추론에 대한 반례

조합대상		n(꼭지점의 수)	참고문헌
그래프	유향그래프	8	엘스파스, 터너([9])
	비유향그래프	16	
		25	윌슨([4])
		16, 24, 25, 27, 32, 36	메케이([4])[1]
		16과 27의 배수	알스패취, 파슨([2])
		소수 $p \geq 5$, $p^2 \mid n$	
		$n > 8, 8 \mid n$	헬, 커크패트릭([2])
		$8m$, $m > 1$; $9m$, $m > 2$	팰피([14])

1970년대 말에서 1990년대에 걸쳐 다음 '일반화된 아담의 추론'에 관한 동형문제가 많은 수학자들에 의해 본격적으로 연구되어졌다.

[일반화된 아담의 추론] 유한군 G가 K에 대해 CI-군일 경우, 임의의 두 G의 케일리대상 $[G, S], [G, S']$이 동형이 되기 위한 필요충분조건은, $S = uS'$을 만족하는 단위원소 u가 G에 존재할 때이다.

이시기에 매우 주목할 만한 결과가 1977년 바바이(Babai)([3])에 의해 발표되었으며, 이 결과는 이후 많은 수학자들에 영향을 주었을 뿐만 아니라 특히 임의의 두 Z_n의 케일리대상이 동형이 될 필요충분조건을 밝히는데 중요한 방법론을 제시해주었다.

1) 컴퓨터를 이용하여 $n \leq 37$일 때 아담의 추론이 만족되지 않는 비유향그래프를 모두 찾아냄.

정리 1.1.1. [L. Babai, 1977] G가 위수 n인 유한군일 때, G가 CI-군이 되기 위한 필요충분조건은, S_G의 임의의 두 n-순환(n-cycle) G_1, G_2가 $\langle G_1, G_2 \rangle$ 내에서 공액(conjugate)이 될 경우이다.

1979년 알스패취(Alspach)와 파슨(Parson)([2])은, 서로 다른 소수 p와 q에 대해 $G = Z_{pq}$인 그래프(graph)와 다이그래프(digraph)의 경우 아담의 추론이 성립됨을 밝혔다. 또한, 위수가 p^2일 경우 아담의 추론이 일반적으로 성립하지 않으며, 이 경우 아담의 추론이 성립할 수 있는 구체적인 조건을 찾았다. G의 위수가 일정한 조건을 갖는 비소수일 경우 역시 아담의 추론이 만족된다는 사실이 1970년대와 1980년에 걸쳐 엘스파스와 터너([9]) 이외 몇몇 수학자들에 의해 알려 졌다. 또한, 일정한 조건을 갖는 소수 p에 대해 특별한 경우의 조합대상인 경우에도 아담의 추론이 만족된다는 사실이 밝혀지기도 했다(참조: [4], [6], [9], [10], [14]).

이 시기에 가장 집중되었던 동형문제는 "양정수 n에 대해, 임의의 두 Z_n의 케일리대상이 동형이 되기 위한 필요충분조건은 과연 무엇인가? 즉, Z_n이 CI-군이 되기 위한 필요충분조건은 무엇인가?"이었다. 1987년 팔피(Palfy)([14])는 바바이에 의해 밝혀진 정리 1.1.1과 관련된 몇 가지 결과들을 이용하여 임의의 두 Z_n의 케일리대상이 동형이 되기 위한 필요충분조건을 다음과 같이 찾아냈다.

정리 1.1.2. [P. P. Palfy, 1987] G를 위수가 n인 유한군 그리고 ϕ를 오일러 파이-함수(Euler ϕ-function)라고 하자. G가 CI-군이기 위한 필요충분조건은, $n=4$ 혹은 G가 $\gcd(n, \phi(n)) = 1$을 만족하는 순환군(cyclic group)일 때이다.

팔피는 Z_n의 케일리대상에 대한 동형문제를 두 가지 흥미로운 방법을 통해 해결하였다. 첫째, 기본적인 접근방법으로 $\gcd(n, \phi(n)) = 1$일 경우 임의의 두 케일리대상 $[Z_n, S], [Z_n, S']$에 대한 동형을 증명하는 일이다. 정리 1.1.1을 적용할 경우, 만일 대칭군 S_G 즉 S_n의 임의의 두 n-순환 α, β가 순환군(cyclic group) $\langle \alpha, \beta \rangle$ 내에서 공액이 되면 주어진 두 케일리대상은 동형이 된다. 이를 보이기 위해 n을 나누는 소수들의 수에 대한 귀납법을 적용하여 증명을 유도해낸다. n이 소수인 경우는 당연히 결과를 만족하므로 합성수인 경우만을 고려하면 된다. 이때 $\langle \alpha, \beta \rangle$의 차수(degree)는 합성수이고 $\langle \alpha, \beta \rangle$는 n-순환을 포함한다. 따라서 번사이드(Burnside)와 쉬(Schur)의 정리[17, pp.65]에 의해 S_n내에서 $\langle \alpha, \beta \rangle$의 수학적 구조(군의 구조)에 관한 명확한 성질을 규명할 수 있다. 즉, $\langle \alpha, \beta \rangle$는 S_n내에서 비원시부분군(imprimitive subgroup)이거나 $\langle \alpha, \beta \rangle \neq A_n$을 만족하는 이중추이부분군(doubly transitive subgroup)이 된다. 여기서, A_n은 차수가 n인 교대군(alternating group)이

다. 마지막 경우는 n이 홀수이므로 $\langle \alpha, \beta \rangle \leq A_n$ 즉, $\langle \alpha, \beta \rangle = A_n$인 경우이다. 결국 임의의 두 케일리 대상 $[Z_n, S], [Z_n, S']$에 대한 동형을 증명하기 위해서는 귀납법을 적용하여 위의 3가지 각각의 경우 정리 1.1.1의 필요조건을 만족하는지를 보이면 된다.

둘째, 바바이는 논문 [3]에서 유한군 G가 $Z_p, Z_4, Z_2 \times Z_2$일 때 정리 1.1.1이 성립함을 보였으며, 특히 $|G| = 2p$일 때 G의 한 부분집합 H에 대해 $R \subseteq H^4$을 만족하는 자명하지 않은 사원관계(quaternary relation) R이 존재하면, 임의의 두 G의 케일리대상은 동형이 될 수 없음을 보였다. 여기서, 사원관계 R은 어떤 정수 a, b, c, d에 대해, $\{(w, x, y, z) \in H^4 \mid w^a x^b y^c z^d = 1\}$로 표현할 수 있는 집합을 의미한다. 팰피는 보다 일반적으로, 위의 조건을 만족하는 사원관계가 존재하지 않을 경우 G는 CI-군이 됨을 밝혔다. 이와 더불어, $n \neq 4$, $\gcd(n, \phi(n)) \neq 1$일 때, 임의의 Z_n의 케일리 대상에 대해 위의 조건을 만족하는 사원관계가 존재하지 않는다는 사실을 보일 수 있었다. 따라서 이상 두 가지 사실로 부터 정리 1.1.2의 결과를 유도해 낼 수 있었다.

이 결과는 동형을 이루는 Z_n의 케일리대상들의 구조적 특징을 보여주는 한 예로서, 이들을 구조적 측면에서 보면 각 대상의 구조 내에 이항관계(binary relation), 혹은 삼원관계(ternary relation)는 존재해도 그이상의 관계를 만족하는 부분구조 형태가 존재하지 않음을 알 수 있다. 이는 동형사상 문제의 해결에 한 가지 매우 유용한 방법을 제시해 주었다고 볼 수 있다.

이상 언급한 내용과 관련해 본 논문에서는 직접적으로 다루지는 않았지만 최근 케일리그래프(Cayley graph)에 대한 CI-군들의 특성화에 대한 부분적인 결과들이 콘더(Conder)와 리(Li)([8]), 리(Li)([12]), 그리고 리(Li)와 프래저(Praeger)([13])에 의해 발표되었다. 케일리 그래프의 CI-군에 대한 연구 역시 오랜 기간 연구되어져 왔으나 현재까지 구체적으로 밝혀진 CI-케일리그래프는 극히 소수에 불과하다(참조: [8]).

1.2. 유한체에서의 동형사상 문제

아담의 추론이 발표되기 훨씬 전인 1930년 그리고 1931년에 배이즈와 램바씨는 유한군 $G = Z_p$가 CI-군이 됨을 밝혔다. 그러나 동형문제와 관련된 많은 논문들에선 이러한 사실이 1970년 엘스파스와 터너에 의해 처음으로 밝혀졌다고 알려져 있으며, 배이즈는 1931년 소수를 위수로 갖는 순환 스타이너 삼중계(cyclic Steiner triple system)의 동형사상군을 특성화하였다고만 알려져 있다. 특히, 위에서 언급한 두 사람은 임의의 두 Z_p의 케일리대상이 동형일 경우, 이 두 대상은 Z_p의 치환다항식(permutation polynomial) $f(x) = ax$에 의해 동형이 된다는 사실도 알아냈다.

정리 1.2.1. [Bays and Lambossy, 1930-1931] p가 소수이고 a가 0이 아닌 유한소수체 Z_p의 원소일 때 동형인 유한소수체의 두 케일리대상은 $f(x)=ax$를 만족하는 함수 f에 의해 동형이 된다.

실제 80년대 초까지 발표된 논문들은 거의 케일리대상의 동형군을 특성화하는데 초점을 맞추어 왔다. 아담의 추론을 만족하는 동형군(isomorphic family)들은 실제 $f(x)=ax$에 의해 동형이 됨을 알 수 있으며, 이 이외의 경우, 즉 일정한 조건하에 동형을 이루는 두 케일리대상의 동형사상을 주어진 군에서 정확히 정의한다는 것이 매우 어렵다는 사실을 알 수 있다(참조:[2], [3], [10]). 위의 정리로부터 한 가지 흥미로운 문제를 발견할 수 있다. 즉, 만일 G가 일반적인 유한체일 때 임의의 두 케일리대상의 동형사상군은 무엇이며 이들 각 동형사상을 표현하는 치환다항식은 무엇인가? 현재까지 G가 유한체일 때 케일리 대상들의 동형문제에 대한 결과는 거의 미미한 상태이다. 앞으로 이에 대한 보다 심도 있는 연구가 요구되어진다.

이와 관련된 한 가지 흥미로운 연구는 1985년 브랜드(Brand)([6])에 의한 결과로 $f(x)=ax$가 아닌 다른 형태의 치환다항식에 의해 동형이 되는 케일리대상들을 찾아냈다. 즉, $n\geq 2$일 때 차분모임(difference family)과 위상개념을 적용한 1-회전구조(1-rotational structure)를 이용하여 1-회전 $2-(2\cdot 4^{n-1}+1, 3, 2)$ 디자인(design)들을 만든 후, $f(x)=ax$가 아닌 이차형식을 취하는 다항식에 의해 동형이 되는 두 쌍의 $2-(2\cdot 4^{n-1}+1, 3, 2)$ 디자인들을 처음으로 찾아냈다.

마지막으로, 유한체의 케일리대상에 관한 동형문제를 해결하기 위한 한 가지 연구방법 및 이를 통해 얻어진 부분적인 결과들을 간략히 소개하기로 한다. 소수 p와 양정수 n에 대해 $q=p^n$의 원소를 갖는 유한체를 $GF(q)$라 하고, A를 $GF(q)$의 가역아핀일차변환(invertible affine linear transformation)이라 하자. 여기서 $GF(q)$는 $GF(p)$에서 벡터공간으로 본다. 우선 $G=GF(q)$인 임의의 두 케일리대상이 동형일 경우 이러한 동형사상들을 포함하는 일정한 형태의 모임을 특성화한 후 유한체의 치환다항식 이론들을 적용하여 동형문제를 해결할 수 있는 방법을 유도할 예정이다. 이는 $Aut(C)$의 실로우 p-부분군의 특성화를 통해 구할 수 있다. 즉, P가 $T<P<A$를 만족하는 $Aut(C)$의 실로우 p-부분군(Sylow p-subgroup) 그리고 Q를 $Aut(C)$의 한 p-부분군이라 하자. 주어진 함수 f가 G의 케일리대상 C, D사이의 동형사상일 경우 $f^{-1}Pf$는 $Aut(D)$의 실로우 p-부분군이 된다. W가 $Q<W$를 만족하는 $Aut(D)$의 한 실로우 p-부분군이면 $\phi W\phi^{-1}=f^{-1}Pf$를 만족하는 함수 π를 $Aut(D)$에서 찾을 수 있다. 따라서, $\pi Q\pi^{-1}\subset fPf^{-1} \Leftrightarrow f^{-1}\pi Q\pi^{-1}f \subset P$. 이고 f가 동형사상이므로 C와 D는 $H_Q(P)$의 한 원소에 의해 동형이 됨을

알 수 있다. 따라서 $V=GF(q)$인 임의의 두 케일리대상들 사이에 동형사상이 필히 $H_T(P)$내에 존재함을 알 수 있다. 다음으로 유한체의 치환다항식의 성질을 $H_T(P)$에 적용하여 동형사상을 치환다항식으로 변환시킬 수 있는 적절한 P를 찾는다. 특히, $n=2$일 경우 위의 방법에 의해 동형이 되는 $GF(q)$의 두 케일리대상의 동형사상은 $a,\ b\in GF(q)$에 대해 $f(x)+a=f(x+b)$를 만족하는 $GF(q)$의 다항식 $f(x)$를 특성화함으로서 구할 수 있다(참조: [15], [16]). 이와 같이 얻은 결과를 요약하면 다음 정리 1.2.2와 같다.

정리 1.2.2. $GF(p^2)$의 케일리대상들은 $f(x)=a(\psi(bx))^2+w(x)$를 만족하는 함수 $f: GF(p^2)\to GF(p^2)$에 의해 동형이 된다. 여기서, $a,\ b\in GF(q)$, $\psi(x)=x^p-\cdots-x\in GF(q)[x]$, 그리고 w는 $GF(p)$에서 가역아핀일차변환이다.

다음으로 $G=GF(p)\oplus GF(p)$의 케일리대상들의 동형사상에 대한 함수형태를 분석해 보기로 한다. G가 유한군일 때 G에서 자기 자신으로 사상하는 평행이동이 G의 조합대상들의 자기동형사상이 될 경우, 이 대상을 G-대상이라 정의 하자. π가 S_G의 원소일 때 $GF(q)^n$-대상 C와 $\pi(C)$는 동형이 된다. $GF(q)^n$은 $GF(q)$상에서 표준 n-차원 벡터공간이 되며, 만일 $GF(q)^{n-1}$에서 $GF(q)$로 사상하는 임의의 함수 e에 대해

(1) $$f(x_1,\cdots,x_n)=(x_1,\cdots,x_{n-1},x_n-e(x_1,\cdots,x_{n-1}))$$

을 만족하는 함수 $f: GF(q)^n\to GF(q)^n$의 역함수는 다음과 같다.

(2) $$f^{-1}(x_1,\cdots,x_n)=(x_1,\cdots,x_{n-1},x_n+e(x_1,\cdots,x_{n-1}))$$

만일 e가 이차함수일 경우 f가 C와 $K=GL(GF(q)^n, GF(q))$의 자기동형사상이 아니고 $f(C)$가 $Aut(C)$의 부분군이면, $f(C)$는 $GF(q)^n$-대상이 됨을 어렵지 않게 보일 수 있다. T가 $Aut(C)$의 실로우 p-부분군이 아니라 가정하고 $H=\langle T, f^{-1}Tf\rangle$라 하자. H는 p-군 이므로 H의 중심(center)의 위수는 1보다 크다. T의 모든 원소와 가환인 치환의 집합은 오로지 T이고 $f^{-1}Tf$와 가환인 집합은 오로지 $f^{-1}Tf$임을 쉽게 알 수 있다. 따라서 $f^{-1}Tf$ 내에 0 아닌 평행이동이 존재함을 알 수 있다. 평행이동 $t_{(0,1)}$이 H의 중심에 속하도록 $GF(p)$에서 G의 기저를 적당히 바꿀 수 있다. 그러므로 $H=\langle t_{(0,1)}, t_{(1,0)}, L\rangle$을 만족하면서 $t_{(0,1)}$과 가환이 되는 일차변환 L을 구할 수 있다. 이러한 L의 성질과 군론의 기본개념을 적용하면 $GF(p)$의 어떤 원소 c에 대해 $L=\begin{pmatrix}1 & 0\\ c & 1\end{pmatrix}$이 된다. 이로 부터 $GF(p)$의 임의의 원소 $u,\ v$에 대해

$f^{-1}t_{(u,v)}f = t_{(r,s)}L^k$를 만족하는 정수 k와 $GF(p)$의 원소 r, s를 구할 수 있다. $f(0,0) = f(0,0)$이므로 (u,v)는 $f(r,s)$의 함수 값이 된다. f는 전단사함수이므로 $GF(p)$의 임의의 두 원소 r, s에 대해 $f^{-1}t_{f(r,s)}f = t_{(r,s)}L^k$를 만족하면서 r, s의 값에 의존하는 정수 k가 존재하게 된다. 이와 같이 $GF(p)$의 임의의 두 원소 x, y는 $f(r,s)+f(x,y) = f(x+r, y+t+ckx)$를 만족하게 된다. 또한 동일한 방법을 적용할 경우 $GF(p)$의 임의의 두 원소 x, y에 대해 $f^{-1}t_{f(x,y)}f = t_{(x,y)}L^d$이 성립하면서, $f(r,s)+f(x,y) = f(x+r, y+t+cdx)$를 만족하는 정수 d가 존재한다. f가 전단사함수이고 c가 0이 아니므로 $f(r,s)+f(x,y) = f(x+r, y+t+zdx)$을 만족하는 z를 어렵지 않게 구할 수 있다. 이 경우 x에 대해 귀납법을 적용하면 다음의 결과를 유도해 낼 수 있다. 즉, 함수 f가 전단사함수일 경우, $GF(p)$의 모든 원소 x, y, r, s에 대해 $f(x,y) = xf(1,0)+(y-(zx(x-1)/2))f(0,1)$. 따라서 $GF(p)$의 모든 원소 x, y에 대해 $f(x,y) = ix+j(y-(zx(x-1)/2))$를 만족하는 정수 i, j를 구할 수 있으며, 각 변수의 좌표사상(coordinate map)은 이차형식이 됨을 알 수 있다. 이상의 결과를 정리하면 다음과 같다.

정리 1.2.3. C, D를 동형인 $GF(p)\oplus GF(p)$-대상이라 하자. 만일 T를 포함하는 $Aut(C)$의 실로우 p-부분군 P가 존재하고, P가 A의 부분군이면, C, D 사이의 동형사상은 다항식 $f(x,y) = ix+j(y-(zx(x-1)/2))$에 의해 표현되어질 수 있다. 또한, 만일 T가 $Aut(C)$의 실로우 p-부분군이면 C, D는 Z_p에서의 선형사상에 의해 동형이 된다.

2. 결론

조합대상들의 동형사상문제는 지금도 조합론 분야에서 매우 중요하게 다루는 문제 중의 하나이다. 1930년 배이스와 램바씨 그리고 1967년 아담의 추론을 시초로 수많은 수학자들은 이 문제의 해결을 위해 여러 연구 방법을 시도하여 왔다. 일반적인 조합대상의 동형문제의 해결은 제 2장에서 언급한 바와 같이 팰피의 주목할 만한 연구결과에도 불구하고 그래프, 디자인 등 각 특정한 케일리대상군들의 수학적 구조의 복잡성을 통일할 수 있는 통합이론의 부족으로 일반적인 케일리대상의 동형문제는 아직도 난제로 남아 있으나 지속적인 연구가 진행 중에 있다. 그럼에도 불구하고 특정한 형태의 대상들 즉 그래프, 다이그래프, 혹은 디자인들 사이의 동형사상의 특성화에 대한 부분에서는 오늘날 까지 수많은 수학자들의 헌신과 노력으로 비교적 짧은 기간 동안에 매우 괄목할 만한 결과들이 많이 밝혀졌다.

베이스와 램바씨의 결과에서 나타났듯이 $GF(p)$-대상인 경우 동형사상은 $f(x)=ax$ 로 표현되는 다항식 즉 $GF(p)$의 치환다항식임을 알 수 있었다. 1.2절에서 보았듯이 $n=2$인 $GF(q)$-대상 혹은 $GF(p)\oplus GF(p)$-대상인 경우 일정한 형식을 지니는 치환다항식들에 의해 동형이 됨을 알 수 있었다. 이를 보다 일반적인 $GF(q)$-대상들에 대해 적용할 경우 위의 결과에서 보듯이 이들의 동형사상은 일정한 형식을 취하는 치환다항식으로 표현이 가능함을 엿볼 수 있다. 즉, 동형인 두 $GF(q)$-대상 $C=[GF(q), S]$와 $D=[GF(q), J]$ 사이의 동형사상은 라그랑주의 보간법공식(Lagrange interpolation formula)에 의해 x^n-x를 법으로 차수가 q보다 작은 $GF(q)$의 치환다항식으로 유일하게 표현할 수 있다. 이에 대한 보다 구체적인 다항식을 얻기 위한 한 가지 방법으로 (1)에서 주어진 $Aut(C)$의 부분군 $H_Q(P)$에 대한 보다 면밀한 이론적 고찰이 향후 요구되어진다.

감사의 글 : 본 논문이 완성되기 까지 두 번에 걸쳐 논문의 오류들을 면밀히 지적해주신 세 분의 심사위원들께 감사의 말씀드립니다.

참고 문헌

1. Adam, A., *Research Problem 2-10*, J. Combin., Theory 2(1967), 393.
2. Alspach, B., and Parson, T. D., *Isomorphism of Circulant Graphs and Designs*, Discrete Math. 25(1979), 97-108.
3. Babai, L., *Isomorphism Problem for a Class of Point-symmetric Structures*, Acta Math. Acad. Sci. Hungar. 29(1977), 329-336.
4. Babai, L., and Frankl, P., *Isomorphism of Cayley Graphs I,* Colloq. Math Soc. J. Bolyai, 18. Combinatorics Keszthely, (1976), North-Holland, Amsterdam, (1978), 35-52.
5. Bays, S., *Sur les systemes cycliques de triple de steiner differents pour N premier (ou Puissance de nombre Premier) de la forme 6n+1*, Comment. Math. Helv. 2(1930), 294-305: II-VI, Comment. Math. Helv. 3(1931), 22-41, 122-147, 307-325.
6. Brand, N., *Isomorphic Designs that are not multiplier equivalent*, Discrete Math. 57(1985), 159-163.
7. Brand, N., *Design Isomorphism and Group Isomorphism*, Geometricae Dedicae 27(1988), 282-294.

8. Conder, M. and Li, C. H., *On Isomorphisms of Finite Cayley Graphs*, Europ. J. Combinatorics, 19(1998), 911-919.
9. Elspas, B., and Turner, J., *Graphs with Circulant Adjacency Matrices*, J. Combin. Theory 9(1970), 297-307.
10. Godsil, C. D., *On Cayley Graph Isomorphism,* Ars Combin. 15(1983), 231-246.
11. Lambossy, P., *Sur une maniere de differencier les fonctions cycliques d'une forme donnee*, Comment. Math. Helv. 3(1931), 69-102.
12. Li, C. H., *On Finite groups with the Cayley Isomorphism Property, II*, J. Combin. Theory, Series A 88(1999), 19-35.
13. Li, C. H. and Praeger, C. E., *On the Isomorphism Problem for Finite Cayley Graphs of Bounded Valency*, Europ. J. Combinatorics, 20(1999), 279-292.
14. Palfy, P. P., *Isomorphism Problem for Relational Structures with a Cyclic Automorphism*, European J. Combin. 8(1987), 35-43.
15. Park, H. G., *Polynomials Satisfying $f(x+a)=f(x)+c$ over finite fields*, Bull. Kor. Math. Soc. 29(1992), No. 2, 277-283.
16. Park, H. G., *Polynomial Isomorphisms of Cayley Objects over the fields of order p^2*, J. Kor. Math. Soc. 30(1993), No. 1, 41-49.
17. Wielandt, H., *Finite Permutation Groups*, Academic Press, New York, (1964).

A Characterization of Isomorphism Problem of Combinatorial objects and the Historical Note

Department of Mathematics, Hanyang University **Hong Goo Park**

In this paper, we study the theoretical and historical backgrounds with respect to isomorphism problem of combinatorial objects which is one of major problems in the theory of Combinatorics. And also, we introduce a partial result for isomorphism problem of Cayley objects over a finite field.

Key words : combinatorial object, Cayley object, graph, design, finite fields, permutation polynomials

2000 mathematics Subject Classification : 12F10

ZDM Subject Classification : H20

논문 접수 : 2006년 1월 9일 심사완료 : 2006년 2월