한국수학사학회지 제19권 제2호(2006년 5월), 125-140

Schur환론의 발생과 발전, 군론과 그래프론에서의 역할

한남대학교 수학과 최은미
emc@hannam.ac.kr

군환의 특별한 부분환으로 정의된 수어환(Schur ring)은 치환군의 구조 연구를 위해 1933년 I.Schur에 의해 소개되었다. 그 후 30여 년 동안 군론과 표현론에서 응용되던 수어환은 1970년대에 이르러 획기적인 분기점을 맞이하게 된다. 조합론, 특별히 대수적 그래프에 관한 많은 연구 속에서, 그래프를 분류하기위해 수어환을 이용하려는 새로운 시도가 Klin과 Poschel에 의해 제안되었다. 이것은 당시 대수학에서 이룩해낸 유한단순군의 분류에 큰 도움을 받은 것이다. 이 논문에서는 수어환의 발생에 대한 역사적 배경과, 수어환이 군이론에서 어떻게 이용되었는지를 살펴보고, 또한 그래프이론에서의 역할을 조사한다.

주제어 : 군환, 수어환, 그래프, 케일리그래프, 순환그래프, 그래프의 동형

0. 서론

수어환은 유한군의 분할과 깊은 관계를 갖는 환으로서, 정칙(regular)부분군을 포함하는 치환군의 구조를 연구하기위해 1933년 I.Schur(1875-1941)에 의해 처음 소개되었다. Schur의 제자인 H.Wielandt(1910-2001)에 의해 수어환이라는 이름으로 정착되었으며, 그 후 수 십 년 동안 군론과 군표현론의 한 부분으로 연구되어왔다. 1950년 이후, 조합론적 대상물인 association scheme, cellular algebra, coherent configuration등이 소개되면서, 수어환은 association scheme의 특별한 종류라는 것이 밝혀졌다. 이로서 수어환은 대수 조합론의 주요 대상물로 주목되었으며, 특히 케일리그래프(Cayley)나 순환그래프(cyclic, 또는 circulant)등과 밀접한 관계가 있음이 알려졌다.

이 논문에서는 수어환을 군론과 그래프론적 관점에서 살펴보며 그 상호 관계에 대해 소개한다. 제 1장에서는 1933년 이전까지의 군론에 의거하여 수어환이 소개되어지는 역사적 배경을 살펴보며, Schur자신과 Wielandt로 이어지는 순수 군론에 입각한 초기의 수어환을 소개한다. 제 2장에서는 다양한 군을 택함에 따라 결정되는 수어환의 구조를 알아본다. 이 부분이 대수적 그래프론으로 확장되는 교두보가 되는데, 순환

군에서 만들어지는 수어환은 케일리그래프와 순환그래프의 동형문제(제 3장), 그리고 개수세기 문제(제 4장)를 직접적으로 해결해 주는 가장 좋은 도구로 인정받고 있다. 실제로 케일리그래프 내에는 아주 강력한 조합론적 불변성이 있는데 그것이 바로 케일리그래프로부터 만들어지는 수어환이다. 따라서 여러 케일리그래프들의 상관관계를 알기위해 불변성질인 수어환의 관계를 살펴보게 되는데, 이는 수어환의 대수적 성질로 인해 그래프를 보는 것 보다 환을 연구하는 것이 훨씬 용이하기 때문이다.

1. 수어환의 발생과 대수적 기본성질

Schur는 동일한 차수의 정칙부분군을 포함하는 치환군을 연구하기위해 새로운 환을 고안하였다. 유한 정칙부분군 H를 포함하는 치환군에 군환(group ring) $\mathbf{Z}[H]$를 대응시켰는데, 이것이 오늘날 수어환이라 불리는 대상물의 시초가 되었다.

수어환은 W.Burnside(1852-1927)가 제기한 문제를 해결하는 과정에서 발생하였다. 군 H의 정칙표현을 추이(transitive)부분군으로 포함하는 모든 원시군이 2-추이적(doubly transitive)일 때 H를 Burnside군 (B-군)이라 부른다([22]). 이러한 성질을 갖는 군의 예제가 Burnside에 의해 처음 알려졌기 때문에 B-군이라는 이름을 갖게 되었다.

정리 1. 소수멱을 위수로 하는 모든 순환군은 B-군이다(Burnside 1911).

1921년 Burnside는 합성수 위수의 모든 아벨군은 B-군일 것이라는 추측을 하였으나 후에 반증되었다(1936). Burnside 이후 좋은 결과를 최초로 만든 사람이 Schur이다.

정리 2. 합성수 위수의 모든 순환군은 B-군이다(Schur 1933).

그 후 Wielandt는 보다 강력한 형태의 결과를 발표하였다.

정리 3. 적어도 하나의 순환 Sylow부분군을 갖는 합성수 위수의 아벨군은 B-군이다. 또한 모든 dihedral군은 B-군이다(Wielandt 1935, 1949).

Schur는 Burnside의 연구에 기초하여 다음을 질문하였다: 집합 X와 대칭군 $\Sigma(X)$의 부분군 H를 사용하여 치환군 $(H;X)$를 표시하자. 하나의 정칙치환군 $(H;X)$를 포함하며 원시이지만 2-추이적이 아닌 치환군 $(G;X)$가 존재할 수 있는 조건은 무엇인가? $(H;X)$가 정칙이라면, H와 X는 일치하므로, 치환군 $(G;X)$는 집합 H에서 작용(act)하게 된다. 항등원 $e\in H$와 안정화부분군(stabilizer) $K=\{g\in G|e^g=e\}$에 대해, H 작용에 의한 K-궤도(orbit)를 생각해보자. 각각의 K-궤도들을 기저로 하는 $\mathbf{Z}[H]$의 $\mathbf{Z}$-부분가군을 $M(G;H)$라 하면, $M(G;H)$는

합성곱(convolution)에 관해 닫혀있으며, $\mathbf{Z}[H]$의 부분환이 됨을 Schur가 확인했다. $M(G;H)$를 추이적 가군이라 부르는데, 그는 추이적 가군의 주요 성질들을 공리화하여, 지금 수어환 (S-환)이라고 불리는 새로운 대상물을 고안하여 치환군론 연구에 사용하였다([17]).

항등원 e를 갖는 유한군 H와 단위원 1을 갖는 가환환 R, 그리고 원소 $\alpha=\sum_{h\in H}a_h h$ ($a_h\in R$)들로 구성된 군환 $R[H]$를 생각하자. $D\subseteq H$와 $t\in\mathbf{Z}$에 대해 $\overline{D}=\sum_{h\in D}a_h h\in R[H]$, $D^{(t)}=\{g^t|g\in D\}$ 그리고 $\alpha^{(t)}=\sum a_h h^{(t)}$로 표시하자. 임의의 H-자기동형사상 σ는 $\hat{\sigma}:R[H]\to R[H]$, $\hat{\sigma}(\sum a_h h)=\sum a_h\sigma(h)$인 환 자기동형사상으로 항상 확장된다. H의 공집합이 아닌 부분집합들 $D_0=\{e\}$, D_1, …, D_d가 다음을 만족한다고 하자.

(i) $H=\bigcup_0^d D_i$, $D_i\cap D_j=\emptyset$ (ii) $D_i^{(-1)}=D_i$ (iii) $\overline{D_iD_j}=\sum_{h=0}^{d}p_{ij}^h\overline{D_h}$ ($p_{ij}^h\in R$)

이 때 $\overline{D_0}$, …, $\overline{D_d}$에 의해 생성되는 부분대수 $S\subseteq R[H]$를 H의 $d+1$차원 S-환이라 하며, 각 D_i는 H의 S-기저(basic)집합이라 부른다. $\mathcal{S}=\mathcal{S}(S)=\{D_0,\cdots,D_d\}$라 할 때, S-환 S를 $(H,\mathcal{S})=\langle\overline{D_0},\cdots,\overline{D_d}\rangle$로 표현하기도 한다.

특별히 $\mathcal{S}=\{\{g\}|g\in H\}$일 때 $(H,\mathcal{S})=R[H]$는 S-환이므로, S-환은 군환(또는 군 대수)의 일반화된 개념이다. H의 S-환 S의 몇 가지 용어를 소개한다.

(i) 모든 D_i에 의한 군 $\langle D_i\rangle$가 $\{e\}$ 또는 H일 때, 원시(primitive)S-환이라 한다.

(ii) 모든 $\sigma\in AutH$에 대해 $\hat{\sigma}(\overline{D_i})=\overline{D_i}$일 때, 유리(rational)S-환이라 한다.

(iii) 모든 $\alpha\in S$ 에 대해 $\alpha^{-1}=\alpha$일 때, 대칭(symmetric)S-환이라 한다.

(iv) $S=\langle\overline{\{e\}},\overline{H-\{e\}}\rangle$를 자명한 S-환이라 하며, 유일한 2차원 S-환이다.

(v) 또한, 부분군 $K\leq H$가 $\overline{K}\in S$을 만족할 때, K를 S-부분군이라 한다.

S-환 $S=(H,\mathcal{S})$에 관한 다음의 성질들은 쉽게 볼 수 있다.

(i) S가 S-환인 것은 S가 $R[H]$의 부분대수로서 모든 $\alpha\in S$에 대해 $\alpha^{-1}\in S$이며 Hadamard곱 $\circ$ $(\sum a_h h)\circ(\sum b_h h)=\sum(a_h b_h)h$에 관해 닫혀있는 것과 동치이다.

(ii) 자명한 S-환은 원시 S-환이 된다. 또한 임의의 $d+1$차원 $S=(H,\mathcal{S})$가 원시일 동치조건은 $\langle D_i\rangle=H$ ($1\leq i\leq d$)인 것이다.

(iii) 부분군 $K\leq H$와 부분집합 $\mathcal{S}'\subseteq\mathcal{S}$에 대해 $S'=(K,\mathcal{S}')$이 S-환이 될 때,

S'은 S의 S-부분환이라고 부른다. 즉, $\mathcal{D}'$의 모든 원소 D_i, D_j에 대해 $\overline{D_iD_j}$이 $\overline{D_k}\in\mathcal{D}'$들의 1차 결합으로 표시되며 또한 $D_i^{(-1)}\in\mathcal{D}'$이면, $\cup_{D\in\mathcal{D}'}D$ ($=K$)는 H의 부분군이 되고 $S'=(K,\mathcal{D}')$는 S-부분환이다. 특히 $K\lhd H$일 때, S'은 S의 정규(normal)라 한다.

(iv) 자신과 $S_0=(\{e\},D_0)$만을 정규부분환으로 갖는 S-환을 단순(simple)이라 한다.

2. 유한군 구조와 수어환 구조의 관계

유한군 H의 대수적 구조는 H에서의 S-환 구조에 결정적인 영향을 미친다. 순환군의 모든 유리S-환들과, 소수 위수인 순환군 H에서의 S-환의 구조는 완벽히 결정되었으며, 임의의 위수를 갖는 순환군의 S-환에 관하여도 부분적인 결과들이 발표되었다([17]). 순환군의 S-환은 케일리그래프와 순환그래프등과 밀접한 관계를 갖게 되어, S-환의 개수문제는 그래프의 동형문제 또한 개수문제에 관한 많은 정보를 제공한다([13]). 이번 장에서는 유한군의 구조가 S-환의 구조에 미치는 관계를 알아본다.

(1) 아벨군, 순환군 또는 dihedral군에서 S-환.

아벨군 H의 S-환 $S=(H,\mathcal{D})$를 생각해보자. $\exp(H)=n$이며 $\mathcal{D}=\{D_0,\cdots,D_d\}$이면, $\mathbf{Z}_n^*$는 H에서 $(t,h)=h^t$ ($t\in\mathbf{Z}_n^*$, $h\in H$)로 작용한다. 고정된 $t\in\mathbf{Z}_n^*$에 대해 $\sigma\in AutH$, $\sigma(h)=h^t$라 하면, $\hat{\sigma}(S)=S$가 되어, $\hat{\sigma}$은 $\overline{D_0}$, $\cdots$, $\overline{D_d}$를 치환하게 된다([20]). 여기서, 각 D_i에 작용하는 σ의 궤도를 O_i라하고, $E_i=\cup_{D\subseteq O_i}D$ ($i=0,\cdots,d$)라 하면, $\overline{E_0}$, $\cdots$, $\overline{E_d}$는 S의 S-부분환을 생성하며, 이것은 유리 S-환이 된다.

특별히 H가 순환군일 때는, 모든 $\sigma\in AutH$에 대해 $\hat{\sigma}(S)=S$가 되며, 또한 $\sigma(h)=h^t$ ($h\in H$)인 정수 t ($(t,|H|)=1$)가 항상 존재한다. 따라서 S가 유리 S-환일 동치조건은, $(t,|H|)=1$인 모든 정수 t에 대해 $D_i^{(t)}=D_i$가 되는 것이다. 이러한 상황은 조합론적인 여러 대상물들에서 많이 볼 수 있어서, partial difference sets과 triple-sum-sets 등에서 나타난다([2, 16]).

이와 같이 S-환 S는 항상 유리 S-부분환 S_0로 줄여질 수 있으며, 이 때 S_0-기저집합은 $AutH$에 의해 추이적으로 치환된 S-기저집합들의 합집합이다. 더욱이 S_0-기저집합은 S의 적당한 기저집합 D_i에 대해 $\cup_{(t,|H|)=1}D_i^{(t)}$로 표시된다. 그러므로 S-환

의 구조를 효과적으로 보기위해, S-환 대신 유리 S-환을 먼저 조사하게 된다([11]).

한편, dihedral군 $D_n=\langle x,y|x^n=y^2=e,\ yxy=x^{-1}\rangle$의 S-환 S를 생각해보자.

정리 4.[20] 만약 S가 비대칭 S-환이라면, $\langle x\rangle$의 부분군에서 정의되는 S-환 S'이 존재하여 $\dim S'>2$이며 S의 정규 부분환이 된다.

실제로, S의 기저집합 D_i는 $\langle x\rangle$의 부분집합들 A_i, B_i에 의해 $D_i=A_i\cup yB_i$인 형태로 유일하게 표시되므로, A_i ($0\le i\le d$)와 $\emptyset\neq B_i$ ($2\le r+1\le i\le d$)를 사용하여

$$D_i=A_i \text{ for } 0\le i\le r<d\ ;\quad D_i=A_i\cup yB_i \text{ for } r+1\le i\le d$$

로 나타낸다. 그러면 $H=\cup_{i=0}^{r}A_i$는 $\langle x\rangle$의 부분군이 되며, $S'=(H,\{A_0,\cdots,A_r\})$은 S의 정규 S-부분환이 되어, 정리 4를 얻게 된다. 그러므로 S는 비단순이다.

특별히 $n=p$ (홀소수)일 때, $D_p=\langle x,y\rangle$ ($o(x)=p,\ o(y)=2$)의 비단순 S-환 S는 진 정규 S-부분환 S'을 포함하며, 이것은 D_p의 정규부분군 $H\neq\{e\}$의 S-환이다. 따라서 S'은 $\langle x\rangle\cong Z_p$의 S-환이며, S의 각 기저집합 D_i는 A 또는 yB ($A,B\subseteq\langle x\rangle$)로 표현된다. 이로서 D_i로 생성되는 S의 구조를 알아낼 수 있다.

잘 알려진 대로, p개의 꼭지점을 갖는 순환그래프의 분류는 $2p$개의 꼭지점을 갖는 꼭지점 추이그래프인 경우로 자연스럽게 확장된다. 따라서 케일리그래프를 연구하기 위해, 순환군 Z_{2p}와 dihedral군 D_p에서의 S-환에 관한 선행 연구가 필수적이다.

(2) S-환의 quotient와 inflation, 그리고 곱셈.

$K\lhd H$일 때 $\pi: H\to H/K$를 전형적 전사함수라 하자. H의 S-환 S로부터 H/K의 S-환 S'을 만들 수 있으며, 그와 반대로 S'으로부터 S를 만들 수도 있다. 각각의 과정을 going-down 그리고 lifting이라고 부른다.

정리 5.[11] $S=(H,\mathcal{D})$를 H의 S-환이라 하자. H/K의 S-환 S'이 존재하여, 임의의 $C\subset H/K$에 대해 $\overline{C}\in S'$일 동치조건은 $\overline{\pi^{-1}C}\in S$이다. 또한 $D\subseteq H$가 S-기저집합이고 $\overline{D}\equiv 0\pmod{\overline{K}}$이면, πD는 S-기저집합이다. 특히 K가 S-부분군이라면, 임의의 $D_1, D_2\in\mathcal{D}$에 대해 $\pi D_1\cap\pi D_2=\emptyset$이거나 $\pi D_1=\pi D_2$가 되어, $\hat{\pi}(S):=\oplus_{D\in\mathcal{D}}R\overline{\pi D}$는 H/K에서의 S-환이다.

증명을 위해, $T=\{\alpha\in S|\alpha\equiv 0\pmod{\overline{K}}\}$라 하면 T는 +, · 그리고 Hadamard곱 ∘에 관해 닫혀있으며 S의 부분 S-환이 된다. 따라서 $S':=\hat{\pi}(T)$는 H/K의 S-환이 된다.

반대로 H/K의 S-환 $S_{H/K}$로부터 H의 lifted S-환을 만들 수 있다.

정리 6.[13] $S_{H/K}$의 $\wp(S_{H/K})=\{E_1=\{K\}, E_2, \cdots, E_t\}$일 때, $D_0=\{e\}$, $D_1=K-\{e\}$, $D_i=\pi^{-1}E_i$ ($2\le i\le t$)라 하면 $\hat{\pi}^{-1}(S_{H/K}):=\oplus_0^t R\overline{D_i}$은 H의 S-환이 된다.

위와 같은 일반적인 lifting보다, 특별한 성질-가령 $K\le M\le H$일 때, H/K의 S-환으로부터 lift된 S-환을 다시 M으로 줄인 것이 M에서의 S-환 S_M이 되는 성질을 갖도록 할 수 도 있다.

정리 7. M/K는 $S_{H/K}$-부분군이며, S_M은 M의 S-환으로 $\hat{\pi}(S_M)=R[M/K]\cap S_{H/K}$이며 $K\in S_M$라고 하자. 그러면 H의 S-환 S가 존재하여 기저집합 $\wp(S)=\wp(S_M)\cup\{\pi^{-1}E\mid E\in\wp(S_{H/K}), E\not\subset M/K\}$를 갖는다. 또한 $S\cap R[M]=S_M$이며 $\hat{\pi}(S)=S_{H/K}$이 된다. 이 때 S는 $S_M\wedge S_{H/K}$로 표시되며 wedge곱이라 불린다.

이러한 과정은 새로운 S-환과 그래프를 만드는데 유용한 정보를 제공한다.

3. 그래프론과 수어환 이론의 관계

1933년에 정의된 이후 치환군 연구에 제한적으로 사용되던 S-환은 1970년을 기하여 대수 조합 분야의 대상물로 인식되어, 조합론에서는 translation association scheme이라고 불리며 케일리그래프의 성질을 연구하는데 필수적임이 알려졌다. S-환과 그래프의 상관관계를 잘 설명하기위해서는 대수 조합론의 전반적인 개념들인 association scheme, cellular algebra, coherent configuration등과의 관계를 살펴보아야 하나, 이 논문에서는 특별히 대수적 그래프와 S-환의 관계를 알아보는데 집중할 것이다.

그래프의 일반적 정의는 생략하고, 필요한 기호만 소개한다. (유향)그래프 $\Gamma=(V,E)$에서 V는 꼭지점 집합이고 $E\subseteq V\times V$는 이항관계로서 선분 집합이다. $(i,j)\in E$는 선분임을 뜻한다. 모든 그래프는 인접행렬(adjacency) $\Gamma=(a_{ij})_{i,j\in V}$로 항상 표시되는데, 이 때 성분 a_{ij}는 $(i,j)\in E$일 때 1이며, 그렇지 않으면 0으로 정한다.

유한군 H와 부분집합 $X\subseteq H$에 대해, $V=H$이고 $E=\{(h,hx)|h\in H, x\in X\}$인 그래프 (V,E)를 X에 대한 H의 케일리그래프라 하며, $Cay(H,X)$로 표시한다. 이 때, (H,X)는 $Cay(H,X)$의 케일리표현(representation)이라 하며, X는 연결집합이라 부른다. 특히 H가 순환군 $\mathbb{Z}_n$과 동형일 때, $Cay(H,X)$를 순환그래프라 하고, $\Gamma(n,X)$로 표시하기도 한다. 즉, 케일리그래프 Γ가 순환이면 각 꼭지점들에 순서가

있어서 그에 대응하는 인접행렬이 순환이 된다. 한편 $Aut\Gamma$는 꼭지점 집합 V에서 작용하며, 이 작용이 추이적일 때 Γ는 꼭지점 추이그래프라고 부른다([19]).

(i) $e \in X$이면, $Cay(H, X)$의 모든 꼭지점에서 닫힌곡선(loop)이 생기므로, 일반적으로 $e \notin X$을 가정하게 된다.

(ii) $Cay(H, X)$가 연결(connected)일 필요충분조건은 $\langle X \rangle = H$이다.

(iii) 모든 $x \in X$에 대해 $x^{-1} \in X$이면 인접행렬은 대칭이며 $Cay(H, X)$는 무향이다.

케일리그래프란 명칭은 현재 우리가 케일리 color다이어그램이라 부르는 대상물로부터 출발하였다. 1878년 A.Cayley(1821-1895)는 추상군을 그래픽으로 표현하면서 color 다이어그램을 소개하였다. 그 후 H.S.M.Coxeter(1907-2003)와 W.O.J.Moser는 주어진 군에서 생성원들의 상관관계를 알고 있을 때, 군의 구조를 연구하기위해 케일리 color다이어그램을 사용하였다. 케일리 color다이어그램은 1927년 O.Schreier (1901-1929)에 의해 Schreier coset 다이어그램으로 확장되었고, 다시 1964년 G.O.Sabidussi에 의해 오늘날의 그래프로 발전되었다([10]).

케일리그래프와 그 일반화인 꼭지점 추이그래프는 오랜 기간 동안 대수적 그래프론에서 활발히 다루어져왔다. 실제로 케일리그래프는 Ramanujan그래프와 expander를 만드는데 사용될([14, 15])뿐 만 아니라, 다른 조합론적 구조물들, 가령 통신 네트워크나([4, 7]) 디자인이론에서 difference set([16])을 만드는데 이용되기도 한다. 또한 군의 알고리즘 계산을 분석하는데([1]) 이용된다. 그래프를 적절히 활용하기위해서는 특정 불변성을 가진 그래프를 잘 선택해야한다. 이 때 일반적으로 고려되는 성질이, 작은 지름, 고정된 차수, 균등성(uniformity), short wire 등 이다.

1970년대에 들어와서 M.Klin, R.Poschel 그리고 M.Muzychuk는 S-환의 성질을 그래프 이론에 적용하는 연구를 최초로 시작하였다. 유한 단순군 분류의 도움을 받아, S-환의 분류가 그래프를 분별하는데 가장 효과적인 도구가 됨을 알아냈다([18]). 케일리그래프 $Cay(H, X)$의 연결집합 X로 생성되는 S-환 $\ll \overline{X} \gg$은 그래프의 조합론적 불변성이다. 케일리그래프들의 성질을 조사하는 대신에 연결집합에 의한 S-환을 관찰하게 되는데, S-환이 가진 대수적 성질로 인해 그 연구가 보다 수월하기 때문이다.

특별히 순환그래프를 분류함에 있어서 S-환 이론이 큰 도움이 되었는데, 이는 $\mathbf{Z}_n$의 S-환 $\mathcal{S}$와 그것의 자기동형군을 완벽히 결정할 수 있기 때문이다. 실제로, $\mathcal{S}$의 기저집합이 $D_0 = \{e\}, \cdots, D_d$일 때, S의 자기동형군을 $Aut(S) := \bigcap_{i=1}^{d} Aut(\mathbf{Z}_n, D_i)$로 정의한다. 그러면, 임의의 부분집합 $X \subseteq \mathbf{Z}_n - \{0\}$에 대해 X로 생성되는 $\ll \overline{X} \gg$ 형태인 $\mathbf{Z}_n$의 S-환이 항상 존재하며, 이 때 $Aut(\ll \overline{X} \gg) = Aut(\mathbf{Z}_n, X)$가 된다.

케일리그래프 연구에 S-환이 사용되는 한 예제로 다음을 볼 수 있다.

정리 8.[9] $Cay(Z_n, X)$를 연결 arc-추이순환그래프라 할 때, 임의의 $\ll\overline{X}\gg$-부분군 $\{0\}<H<Z_n$는 $H\cap X=\varnothing$이 된다.

증명을 위해, $Cay(Z_n, X)$의 연결집합 X로 생성되는 S-환 $\ll\overline{X}\gg$를 S라 표시하자. 그러면 X는 S의 기저집합이 되어, S-부분군인 H와 사이에서 $H\cap X=\varnothing$이거나 $X\subset H$가 된다. 만약 $X\subset H$라면 $\langle X\rangle=H<Z_n$이 되어 $Cay(Z_n, X)$가 연결그래프라는 점에 모순이 된다.

위 결과로 인해, 위수 n인 연결 arc-추이순환그래프 Γ는 4형태로 분류된다.

$\Gamma=K_n$ (완전그래프) ; $\Gamma=$정규 순환그래프;

$\Gamma=\Lambda[\overline{K_d}]$ (Λ: 위수 m인 연결 arc-추이순환, $n=md$, $\overline{K}$:complement);

$\Gamma=\Lambda[\overline{K_d}]-d\Lambda$ (Λ: 위수 m인 연결 arc-추이순환, $n=md$, $\gcd(d,m)=1$, $d>3$).

여기서 lexicographic곱 $A[B]$는 그래프로서 $V(A)\times V(B)$를 꼭지점집합으로 하며, $((a,b),(c,d))\in E(A[B])$인 것은 $(a,c)\in E(A)$ 또는 $(a=c)\wedge(b,d)\in E(B)$인 것이다.

4. 케일리그래프의 동형과 수어환의 동형

일반적으로 말하는 그래프의 동형문제란, 여러 그래프들 사이에 동형 관계를 판정하기에 적합한 알고리즘을 발견하는 것을 의미한다. 그래프들 사이의 동형이란 꼭지점 집합에서 정의되는 전단사 함수가 꼭지점의 인접과 비인접을 그대로 보존하는 것이다. 즉, 두 그래프 $\Gamma_i=(V_i, E_i)$ ($i=1,2$)에 대해, 전단사 함수 $\sigma: V_1\to V_2$가 존재하여 $(u,v)\in E_1\Leftrightarrow(\sigma(u),\sigma(v))\in E_2$를 만족할 때, Γ_1과 Γ_2는 동형이라 부른다. 동일한 그래프 $\Gamma=(V,E)$의 자기동형사상은 $\Gamma\to\Gamma$인 동형사상이며, 자기 동형사상의 모임은 자기동형군 $Aut(\Gamma)<\Sigma(V)$을 만든다. 따라서 케일리그래프 $Cay(H, X_i)$ ($i=1,2$)가 동형이면 자기동형 $\sigma\in Aut(H)$가 존재하여 $\sigma(X_1)=X_2$가 된다.

그래프의 동형문제를 해결하는 효과적인 방법은 그래프에 있는 조합론적 불변성을 조사하여 그 불변성 사이의 동형관계를 판단하는 것인데, 그 중에서 주목되는 것이 S-환이다. 순환군 Z_n의 S-환들이 동형이 될 동치조건은 그 S-환들이 완전히 일치하는 것이다([18]). 이 사실은 순환군의 S-환의 기저집합들의 구조를 밝힘으로서 증명된다.

(1) S-환 동형과 그래프의 동형

두개의 S-환 S_1과 S_2사이에 선형 전단사함수 $\psi : S_1 \to S_2$가 존재하여

$$\psi(\alpha^{(-1)}) = (\psi(\alpha))^{(-1)} \; ; \; \psi(\alpha \cdot \beta) = \psi(\alpha) \cdot \psi(\beta) \; ; \quad \psi(\alpha \circ \beta) = \psi(\alpha) \circ \psi(\beta)$$

($\cdot$, $\circ$는 보통의 곱과 Hadamard곱이며 $\alpha, \beta \in S_1$이다)을 만족할 때, ψ는 S-환 동형사상이라 한다. S_1과 S_2를 $(H, \mathcal{S}(S_1)) = \langle \overline{D_0}, \cdots, \overline{D_d} \rangle$과 $(K, \mathcal{S}(S_2)) = \langle \overline{D_0'}, \cdots, \overline{D_t'} \rangle$라고 표시하면 적당한 치환함수 $f \in \Sigma_d$ (대칭군)에 대해 $\psi(\overline{D_i}) = \overline{D'_{f(i)}}$ 로 정의된다. S-환 동형사상은 대수적 동형, 조합적 동형, 케일리 동형 등으로 세분화한다. 만약 전단사함수 $\theta : \mathcal{S}(S_1) \to \mathcal{S}(S_2)$, $D_i \mapsto D_i^{\theta}$가 존재하며 동시에 $\overline{D_i} \mapsto \overline{D_i^{\theta}}$가 S_1와 S_2의 동형사상을 유도할 때, 대수적 동형 (기호: $\cong_{alg}$)이라 부른다. 한편, 전단사함수 $\sigma : H \to K$가 있어 $d = t$이며 $\{Cay(H, D_i)^{\sigma} | i = 0, \cdots, d\} = \{Cay(K, D_i') | i = 0, \cdots, t\}$일 때, 조합적 동형 (기호: $\cong_{com}$)이라 부르며, 이 때 σ를 조합적동형사상이라 한다. 또한 $\sigma : H \to K$가 조합적동형사상인 동시에 군 동형사상일 때, S_1와 S_2는 케일리 동형 (기호: $\cong_{cay}$)이라 부른다. 조합적 동형 $\sigma : H \to K$는 $Cay(H, D_i)^{\sigma} = Cay(K, D_i^{\sigma *})$를 만족하는 전단사함수 $\sigma^* : \mathcal{S}(S_1) \to \mathcal{S}(S_2)$를 만들므로, 다음이 성립한다.

정리 9. $\sigma : S_1 \cong_{com} S_2$이면 $\sigma^* : S_1 \cong_{alg} S_2$이다. $S_1 \cong_{cay} S_2 \Rightarrow S_1 \cong_{com} S_2 \Rightarrow S_1 \cong_{alg} S_2$이지만, 그 역은 성립하지 않는다.

동일한 군 H위에서 $Cay(H, X)$의 동형을 조사하기위해, 임의의 $\sigma \in Aut(H)$를 택하면 σ는 H에서 작용하므로, $T = X^{\sigma}$라 하면 σ는 $Cay(H, X)$와 $Cay(H, T)$사이의 동형을 유도한다. 이 때 $\sigma : X \to T$를 케일리 동형사상이라 하고, X와 T는 동등(equivalent)하다고 한다. 그러나 $Cay(H, X)$, $Cay(H, T)$는 케일리동형사상 $X \to T$이 존재하지 않을 때도 동형이 될 수 있다.

그래프 $Cay(H, X)$가, 자신과 동형인 모든 $Cay(H, T)$에 대해 적당한 $\sigma \in Aut(H)$가 존재하여 $T = X^{\sigma}$가 될 때, $Cay(H, X)$를 H의 CI-그래프(Cayley Isomorphism)라 부른다. 또한 H의 모든 케일리그래프가 CI-그래프일 때, H는 CI-군이라 부른다. H에서의 어떠한 케일리그래프가 CI-그래프인지를 판정하는 문제는 오래 동안 풀리지 않고 있었던 문제이며, 몇몇 특별한 경우에 단편적으로 연구되었다. 이 문제는 "모든 순환그래프는 동일한 순환군에서의 CI-그래프이다" 라는 A.Adam의 추측(1967)으로 부터 비롯되었다. Adam의 추측은 Elspas와 Turner에 의해 반증되었으나, 이것은 CI-그래프의 연구를 촉진시켰으며, 한편 성립하는 경우에 관한 많은 연구가 진행되었

다([18]). Adam의 추측을 순환군위에서 기술하면 다음과 같다.

정리 10. X와 T가 동등이면 $\Gamma_1 = Cay(\mathbf{Z}_n, X)$와 $\Gamma_2 = Cay(\mathbf{Z}_n, T)$는 동형이다.

A.Adam(1967) : 그 역으로서, Γ_1과 Γ_2가 동형이면 X와 T는 동등한가?

정리 10은 쉽게 볼 수 있어서, 동형사상 $\sigma : \mathbf{Z}_n \to \mathbf{Z}_n$, $\sigma(v) = mv$ ($\gcd(m, n) = 1$)를 생각하자. 만약 $(u, v) \in E(\Gamma_1)$이면 $v - u \in X$이다. 그런데 $mu - mv \in mX = T$이므로 $\sigma(u, v) = (mu, mv) \in E(\Gamma_2)$이고 $Cay(\mathbf{Z}_n, mX) \cong Cay(\mathbf{Z}_n, X)$ 이다.

그러나 Adam의 추측에 관하여는, 8개의 꼭지점을 갖는 순환그래프가 최소의 반례로 제시되었고, $\mathbf{Z}_{p^2}$ ($p \geq 5$)는 CI-군이 아님이 밝혀졌다([3]). 반면 Turner는 $\mathbf{Z}_p$가 CI임을 보였으며([21]), Babai(1977)과 Alspach와 Parson(1979)는 각각 $\mathbf{Z}_{2p}$와 $\mathbf{Z}_{pq}$가 CI임을 보였다. 그러나 M.Klin은 S-환 이론을 사용하여 Adam의 문제의 궁극적 해결 방안을 보임으로써(정리 12), 그래프의 개수세기에서 많은 성과를 만들었다.

$Cay(H, X)$들의 동형과 그에 대응하는 S-환들 $\ll \overline{X} \gg$의 동형을 알아보자.

정리 11.[18] $\sigma : H \to K$가 $Cay(H, X)$와 $Cay(K, T)$의 동형이면, $\ll \overline{X} \gg \cong_{com} \ll \overline{T} \gg$는 조합적 동형이며, $|\wp(\ll \overline{X} \gg)| = |\wp(\ll \overline{T} \gg)|$이다. 즉, $\ll \overline{X} \gg \cong_{alg} \ll \overline{T} \gg$이다.

$Cay(\mathbf{Z}_n, X)$와 $Cay(\mathbf{Z}_n, T)$가 동형이면, 정리 12에 의해 $Cay(\mathbf{Z}_n, X) \cong Cay(\mathbf{Z}_n, T)$인 $\sigma \in Aut(\mathbf{Z}_n)$가 존재하여 $\sigma : \ll \overline{X} \gg \cong_{com} \ll \overline{T} \gg$, $\sigma^* : \wp(\ll X \gg) \cong \wp(\ll T \gg)$이며, 또한 $T = \cup\{D^{\sigma^*} | D \in \wp(\ll \overline{X} \gg),\ D \subseteq X\}$이다. $(\mathbf{Z}_n)_k$는 $\mathbf{Z}_n$의 부분집합으로 위수 n/k인 원소로 구성되며 $(X)_k := X \cap (\mathbf{Z}_n)_k$라 하자. 그러면 $(T)_k$는

$\cup\{D^{\sigma^*} \cap (\mathbf{Z}_n)_k | D \in \wp(\ll \overline{X} \gg),\ D \subseteq X\}$로 표시되며, 이제 적당한 정수 m_k가 존재하여 $m_k(\cup\{D \cap (\mathbf{Z}_n)_k \neq \emptyset | D \in \wp(\ll \overline{X} \gg),\ D \subseteq X\}) = m_k(X)_k$와 일치한다. 이로서 그래프에 관한 다음의 결과를 볼 수 있다.

정리 12.[18] (Ziben의 추측) $Cay(\mathbf{Z}_n, X)$와 $Cay(\mathbf{Z}_n, T)$가 동형이면 $k | n$인 모든 k에 대해 $m_k(X)_k = (T)_k$인 $m_k \in \mathbf{Z}_n^*$가 존재한다. 따라서 모든 $X \subseteq \mathbf{Z}_n^*$는 $\mathbf{Z}_n$의 CI-부분집합이다.

이제 S-환을 사용하여 Adam의 추측을 해결할 수 있다.

정리 13.[8] $K \leq \mathbf{Z}_p^*$를 위수 k인 부분군이라 하자. $\mathbf{Z}_p$의 모든 S-환은 적당한 정수 $k | p-1$에 대해 $S_k = \left\langle \overline{0}, \overline{K}, \overline{y_2 K}, \cdots, \overline{y_{\frac{p-1}{k}} K} \right\rangle$와 동형이다 (여기서 $y_i K$는 $\mathbf{Z}_p^* = \cup y_i K$인 coset들이다). 만약 $k < p-1$이면 $Aut(S_k) = Z_p \rtimes K$이며 정규화부분군 $N(Aut(S_k)) = Z_p \rtimes Z_p$이다. 한편 $k = p-1$이면 $Aut(S_k) = \Sigma_p = N(Aut(S_d))$이다.

그러므로 $[N(Aut(S_k)):Aut(S_k)]=\frac{p-1}{k}$ 이다.

정리 14. 모든 소수 p에 대해 Adam의 추측은 사실이다.

증명 : $Cay(Z_n, X)\cong Cay(Z_n, T)$이므로, $\ll \overline{X}\gg_k=\ll \overline{T}\gg_k$ ($k|p-1$) (정리 13)이며, 어떤 $\sigma\in N(Aut(\ll X\gg_k)$가 존재하여 $T=X^\sigma$이다. 또한 정리 13에 의해 $X^\sigma=mX\ m\in Z_p^*$가 존재한다.

S-환의 분류를 통해 그래프의 분류를 하는 과정을 예제로 살펴보자.

예제 1. Z_8에서의 순환그래프를 찾기 위해, Z_8에서의 S-환을 분석하여 CI-환인지를 결정한 후, 순환그래프의 동형문제를 조사한다.

(i) Z_8의 S-환은 다음과 같이 10개의 형태로 분류된다.

$S_1=\langle\overline{0},\ \overline{1,2,3,4,5,6,7}\rangle$, $S_2=\langle\overline{0},\ \overline{1,2,3,5,6,7},\ \overline{4}\rangle$, $S_3=\langle\overline{0,\ 1,3,5,7},\ \overline{2,6,4}\rangle$

$S_4=\langle\overline{0},\ \overline{1,3,5,7},\ \overline{2,6},\ \overline{4}\rangle$, $S_5=\langle\overline{0},\ \overline{1,3,5,7},\ \overline{2},\ \overline{6},\ \overline{4}\rangle$, $S_6=\langle\overline{0,\ 1,5},\ \overline{3,7},\ \overline{2,6},\ \overline{4}\rangle$

$S_7=\langle\overline{0,\ 1,5},\ \overline{3,7},\ \overline{2},\ \overline{6},\ \overline{4}\rangle$, $S_8=\langle\overline{0,\ 1,3},\ \overline{5,7},\ \overline{2,6},\ \overline{4}\rangle$, $S_9=\langle\overline{0,\ 1,7},\ \overline{3,5},\ \overline{2,6},\ \overline{4}\rangle$

$S_{10}=\langle\overline{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7}\rangle$

(ii) S_i ($1\le i\le 10$)중에서 CI-환을 판정해보자.

자명한 S-환인 S_1과 S_{10}은 CI이다. 한편 순환군에서 대수적 동형인 S-환들은 일치하므로([18]), Z_8에서 서로 다른 S-환은 대수적 동형이 아니다. 따라서 S_i의 대수적 동형사상들은 자기동형사상이 된다. S는 S_i ($1\le i\le 10$)중 하나이며, $f\in Aut_{alg}(S)$라 하자. 그러면 $f(D_0)=f(\{0\})=\{0\}$이며 f는 기저집합의 원소 개수를 그대로 보존한다. 그러므로 S의 기저집합들이 서로 다른 개수의 원소를 가진다면 $Aut_{alg}(S)$는 자명한 군이 되어 S는 CI-환이다. 따라서 S_i ($1\le i\le 4$)는 CI이다.

한편, $i=6,8,9$일 때 S-환들 S_i는 원소 1개를 갖는 기저집합으로 $\{0\}$과 $\{4\}$ 단 두 개를 가지며, 모든 $f\in Aut_{alg}(S_i)$에 대해 $f(\{0\})=\{0\}$이고 $f(\{4\})=\{4\}$이다. 또한 $\{2,6\}$은 $\{2,6\}+\{2,6\}=\{4\}$가 되는 유일한 대칭 기저집합으로서 $f(\{2,6\})=\{2,6\}$이다. 모든 $f\in Aut_{alg}(S_6)$는 $\{1,5\}$와 $\{3,7\}$을 그대로 보존하거나 혹은 서로 맞바꾸게 되는데, 어떤 경우든지 Z_8의 군 동형사상을 만들게 되어, 결국 S_6는 CI이다. 이러한 형태가 S_8과 S_9에서도 성립하여 S_i ($i=6,8,9$)는 모두 CI이다.

이제 S_7을 알아보자. 기저집합을 $D_1=\{1,5\}, D_2=\{3,7\}, D_3=\{2\}, D_4=\{6\}, D_5=\{4\}$로 편의상 표시하고 임의의 $f\in Aut_{alg}(S_7)$를 생각하자. 그러면 $f(D_3)=D_3$, $f(D_4)=D_4$이거나 $f(D_3)=D_4$, $f(D_4)=D_3$이다. f는 기저집합 원소의 개수를 보존하므로 치환 $(3,4)$, $(1,2)$ 또는 $(3,4)(1,2)$를 생각할 수 있으며, 실제로 이들은 S_7의 자

기동형사상이 된다. 한편 $Aut(\mathbf{Z}_8)$은 $\{\sigma_1(x)=x,\ \sigma_2(x)=5x,\ \sigma_3(x)=3x,\ \sigma_4(x)=7x\}$의 4원소로 구성되어있는데, 모든 σ_i는 S_7의 각 집합을 치환하며, 따라서 σ_i는 S_7의 대수적 자기동형사상이다. σ_1과 σ_2는 S_7의 모든 기저집합 $D_0,\cdots,D_5$위에서 자명하게 작용한다. 한편 σ_3와 σ_4는 치환 (3,4)(1,2)가 된다. 즉 대수적 동형사상 (3,4)와 (1,2)는 자기동형사상으로부터 만들어지지 않는다. 만약 그것들이 조합적 동형사상에 의해 만들어지지 않는다면 S_7은 여전히 CI-환이다. 가령 (3,4)로 확인해 보기위해

$$Cay(\mathbf{Z}_8, D_i)^g = Cay(\mathbf{Z}_8, D_i) \quad i=1,2,5 \qquad (*)$$
$$Cay(\mathbf{Z}_8, D_3)^g = Cay(\mathbf{Z}_8, D_4),\ Cay(\mathbf{Z}_8, D_4)^g = Cay(\mathbf{Z}_8, D_3)$$

를 만족하는 $g\in\Sigma_8$를 찾아보자. 모든 $x\in\mathbf{Z}_8$가 $x=x_0+2x_1$ ($x_0\in\{0,1\}$, $x_1\in\{0,1,2,3\}$)으로 유일하게 표시되므로 g를 $g(x_0+2x_1)=x_0+6x_1$으로 정의하면 (*)을 만족하게 된다. 따라서 S_7은 CI-환이 아니다.

(iii) $\mathbf{Z}_8$의 모든 S-환을 분석함으로써 $\mathbf{Z}_8$의 순환그래프의 동형문제를 해결할 수 있다. 즉, 꼭지점 8개를 갖는 두개의 동형 순환그래프는 곱셈자(multiplier)에 의해 공액(conjugate)이거나 그 둘 사이의 동형사상이 $g\in\Sigma_8$와 곱셈자의 곱으로 표현된다.

(2) 개수세기 (enumeration)

1970년대 중반부터 M.Klin, Ja.Golfand 그리고 R.Poschel 등은 그래프 동형류의 개수세기를 시작하였다. 그들은 $\mathbf{Z}_n$의 S-환 분류를 먼저 연구하여, Adam의 추측을 해결하고 그 결과를 순환그래프로 확장시키는 방법으로 진행했다. 이 시기에 n이 홀소수 p의 멱 p^m, $n=2$, pq (두 소수의 곱), pqr (세 소수의 곱)일 때, 그리고 제곱인수가 없는 n일 때의 S-환의 개수를 세었다.

순환그래프의 개수세기는 구성적(constructive)방법과 해석적(analytic)방법으로 분류된다([6, 3장]). 구성적 방법은 조합적 대상물의 각 동치류로 부터 대표원을 취함으로써 개수세기를 하는 것이다. 관심 대상물을 모두 포함하는 조직적인 구조물을 만들면 완벽한 정보를 알 수 있지만, 어떤 경우는 대표원들만을 택할 때조차 그 개수가 너무 많아서 다루지 못하기도 한다. 따라서 동형류의 개수를 먼저 조사한 후, 그것을 바탕으로 구성적 개수세기가 유효한지를 판단하게 되는데, 이것을 해석적 방법이라 한다. 즉, 해석적 방법은 수학의 전통적인 형태로서 생성함수를 통해 개수세기를 한다.

비동형 순환그래프의 개수세는 해석적 방법으로 ([8, 3.2])에서 제시된 과정이다.

(i) S-환 S_i를 모두 나열한다.

(ii) 임의의 $0\neq x\in\mathbf{Z}_n$를 포함하는 S_i의 기저집합을 $D_{(x)}$라 할 때, 원소 r개를 포함하는 기저집합의 개수 $d_{ir}=|\{D_{(x)}\in S_i \mid |D_{(x)}|=r, D_{(x)}\neq D_0\}|$ 를 계산한다.

(iii) 생성함수 $f_i(t) := \sum_{r=0}^{n-1} f_{ir}t^r := \prod_{r=1}^{n-1}(1+t^r)^{d_{ir}}$를 사용하여 S_i에 포함되는 모든 순환그래프의 개수를 센다. 특별히 $f_i(1)$이 S_i의 모든 labelled 순환그래프의 개수가 된다.

(iv) $g_i(t) = \sum_{r=0}^{n-1} g_{ir}t^r$는 비동형 순환그래프의 개수를 계산하는 생성함수라 하고, $g(t) := g(n,t)$ 는 n개의 꼭지점을 갖는 비동형 순환그래프의 개수를 세는 생성함수라 하자. 그러면 $g(1)$이 바로 n개의 꼭지점을 갖는 비동형 순환그래프의 개수가 된다.

(v) [8, 정리 3.5], $G_i = Aut(S_i)$와 정규화부분군 $N(G_i) = N_{\Sigma_n}(G_i)$라 할 때,

$g_i(t) = \frac{|G_i|}{|N(G_i)|}\left(f_i(t) - \sum_{S_j \subsetneq S_i} \frac{|N(G_j)|}{|G_j|} g_j(t)\right)$ 이며, $g(t) = \sum g_i(t)$가 된다.

예제 2. 이러한 단계를 통해 $\mathbf{Z}_6$의 비동형 순환그래프의 개수를 셀 수 있다.

(1) 먼저 $\mathbf{Z}_6$에서의 S-환을 나열하면,

$S_1 = \langle \overline{0,\ 1,2,3,4,5} \rangle$, $S_2 = \langle \overline{0,\ 1,2,4,5},\ \overline{3} \rangle$, $S_3 = \langle \overline{0,\ 1,3,5},\ \overline{2,4} \rangle$

$S_4 = \langle \overline{0,\ 1,5},\ \overline{2,4},\ \overline{3} \rangle$, $S_5 = \langle \overline{0,\ 1,3,5},\ \overline{2},\ \overline{4} \rangle$, $S_6 = \langle \overline{0,1,2,3,4,5} \rangle$

(2) d_{ir}을 계산하면

i	1	2	3	4	5	6
d_{ir}	$d_{15}=1$	$d_{21}=1, d_{24}=1$	$d_{32}=1, d_{33}=1$	$d_{41}=1, d_{42}=2$	$d_{51}=2, d_{53}=1$	$d_{61}=5$

(3) 생성함수 $f_i(t)$를 계산하면,

$f_1(t) = 1+t^5$; $f_2(t) = (1+t)(1+t^4)$; $f_3(t) = (1+t^2)(1+t^3)$

$f_4(t) = (1+t)(1+t^2)^2$; $f_5(t) = (1+t)^2(1+t^3)$; $f_6(t) = (1+t)^5$

(4) 함수 $g_i(t)$를 얻기 위해, 군 $G_i = Aut(S_i)$와 $N(G_i)$를 계산하면,

$G_1 = \Sigma_6$, $N(G_1) = G_1$; $G_2 = \Sigma_3 \wr \Sigma_2$, $N(G_2) = G_2$; $G_3 = \Sigma_2 \wr \Sigma_3$, $N(G_3) = G_3$;

$G_4 = D_6$, $N(G_4) = G_4$; $G_5 = \Sigma_2 \wr \mathbf{Z}_3$, $[N(G_5) : G_5] = 2$; $G_6 = \mathbf{Z}_6$, $[N(G_6) : G_6] = 2$

(5) 이제 생성함수 $g_i(t)$를 계산하면,

$g_1(t) = f_1(t) = 1+t^5$; $g_2(t) = f_2(t) - g_1(t) = t+t^4$; $g_3(t) = f_3(t) - g_1(t) = t^2+t^3$

$g_4(t) = f_4(t) - f_1(t) - f_2(t) - f_3(t) = t^2+t^3$; $g_5(t) = \frac{1}{2}(f_5(t) - g_1(t) - g_3(t)) = 0$

$g_6(t) = \frac{1}{2}(f_6(t) - g_1(t) - g_2(t) - g_3(t) - g_4(t) - 2g_5(t)) = 0$

따라서 $g(t) = 1+t+2t^2+2t^3+t^4+t^5$ 가 된다.

예제 3. Z_8에서의 비동형 순환그래프의 개수를 생성함수를 사용하여 세어보자.

(1) 예제 1에서와 같이 S_1으로 부터 S_{10}까지 나열하고, d_{ir}을 계산하면

$d_{17}=1$; $d_{21}=1, d_{26}=1$; $d_{33}=1, d_{34}=1$; $d_{41}=1, d_{42}=1, d_{44}=1$; $d_{51}=3, d_{54}=1$;
$d_{61}=1, d_{62}=3$; $d_{71}=3, d_{72}=2$; $d_{81}=1, d_{82}=3$; $d_{91}=1, d_{92}=3$; $d_{101}=7$

(2) 생성함수 $f_i(t)$를 계산하면,

$f_1(t)=1+t^7$; $f_2(t)=(1+t)(1+t^6)$; $f_3(t)=(1+t^3)(1+t^4)$;
$f_4(t)=(1+t)(1+t^2)(1+t^4)$; $f_5(t)=(1+t)^3(1+t^4)$; $f_6(t)=(1+t)(1+t^2)^3$;
$f_7(t)=(1+t)^3(1+t^2)^2$; $f_8(t)=(1+t)(1+t^2)^3$; $f_9(t)=(1+t)(1+t^2)^3$;
$f_{10}(t)=(1+t)^7$.

특별히 이 S_i에서의 모든 순환그래프의 개수인 $f_i(1)$을 계산하면 다음과 같다.

i	1	2	3	4	5	6	7	8	9	10
$f_i(1)$	2	4	4	8	16	16	32	16	16	128

i	1	2	3	4	5	6	7	8	9	10
$\|G_i\|$	8!	$2^4(4!)$	$2(4!)^2$	$2(8^2)$	$2(4^2)$	$4(2^4)$	16	16	16	8
$[N(G_i):G_i]$	1	1	1	1	2	3	4	2	2	4

(3) 생성함수 $g_i(t)$를 얻기 위해, $|G_i|$와 $[N(G_i):G_i]$를 계산하면,

(4) 따라서 $g_1(t)=f_1(t)=1+t^7$; $g_2(t)=1\cdot(f_2(t)-1\cdot g_1(t))=t+t^6$; …;

$g_7(t)=\frac{1}{4}(f_7(t)-g_1(t)-g_2(t)-g_3(t)-g_4(t)-2g_5(t)-2g_6(t))=0$, …;

i	1	2	3	4	5	6	7	8	9	10
$g_i(1)$	2	2	2	2	4	4	2	4	4	21

$g(t)=\sum_{i=1}^{10} g_i(t)$이다. 특별히 $g_i(1)$들은 다음과 같아서, $g(1)=g(8,1)=47$이다.

그래프의 개수를 세기위해 다양한 방법들이 개발되어 왔는데, 꼭지점의 개수가 많아질수록 그래프의 개수는 놀라울 만큼 빠르게 증가되기 때문에, 특정한 성질을 갖는 그래프로 제한되어 연구되었다. 최근에는 GAP (Group, Algorithm, Programming), 또는 COCO ([4, 5])등의 컴퓨터 패키지를 사용하여 조합적 대상물의 동형 분류에서 많은 성과를 올리고 있다.

5. 결론

우리는 위의 내용을 통해 Burnside와 Schur에 의한 B-군과 S-환의 기원과 발전 과정을 살펴보았다. 이 두 개념은 군론과 환론에서, 그리고 표현론에서 주요 대상물로 연구되어 왔음을 알았다. 30여년이 지나, 조합론의 부상과 더불어 그래프의 분류를 위해 S-환이 재조명되었으며, 최근에는 더욱 활발히 연구되고 있다. 특별히 1990년 이후 K.H.Leung, S.L.Ma, S.H.Man. W.C.Shiu, M.Muzychuk등이 지속적으로 발표한 S-환 구조에 대한 순수 대수적 연구와 더불어, 2000년 대의 I.Kovacs, J.Morris, C.H.Li 등에 의한 그래프 동형에 관한 연구는 서로 보완작용을 통해 발전하고 있다. 전혀 다른 분야로부터 기원한 S-환과 그래프의 만남은 양 분야에 획기적인 발전을 이루었으며, 현재 S-환은 수학의 여러 분야 - 군론, 표현론, 대수 조합론, 특별히 그래프론 등에서 다양하게 응용되고 있다.

참고 문헌

1. L.Babai, *Automorphism groups*, isomorphism, reconstruction, in R.L. Graham et.al. Handbook of Combin, Elsevier Science, Amsterdam, (1995) 1449-1540.
2. B.Courteau, J.Wolfman, *On triple-sum-sets and two or three weight codes*, Discrete Math. 50, (1984) 179-191.
3. B.Elspas, J.Turner, *Graphs with circulant adjacency matrices*, J.Combin. Theory 9, (1970) 297-307.
4. I.Faradzev, A.Ivanov, M.Klin, *Galois correspondence between permutation groups and cellular rings*, Graphs and Combin. 6, (1990) 303-332.
5. I.Faradzev, M.Klin, *Computer package for computations with coherent configurations*, Proc. Intern. Symp. on Symb. and Algebr. Computa. ISSAC 91 Bonn, July ACM, (1991) 219-223.
6. F.Fiedler, *Enumeration of Cellular algebras applied to graphs with prescribed symmetry*, Technische Univ. Dresden Fachrichtung Mathematik, 1998.
7. R.Heydemann, B.Ducourthial, *Cayley graphs and interconnection networks*, Graph symmetry: Algebraic methods and applications, NATO series C, Kluwer, 497, (1997) 167-226.
8. M.Klin, V.Liskovets, R.Poschel, *Analytical enumeration of circulant graphs with prime-squared number of vertices*, Seminaire Lotharingien De combinatoire B36.
9. I.Kovacs, *Classifying arc-transitive circulants*, J. Alg. Combinatorics, 20, (2004) 353-358.
10. C.Li, *On isomorphisms of finite Cayley graphs- a survey*, Discrete Math 256, (2002) 301-334.
11. K.Leung, S.Ma, *The structure of Schur rings over cyclic groups*, J. Pure Appl.

Alg. 66, (1990) 287-302.
12. K.Leung, S.Man, *On Schur rings over cyclic groups* II, J. Alg. 183, (1996) 273-285.
13. K.Leung, S.Man, *On Schur ring over cyclic groups*, Israel J. Math 106, (1998) 251-267.
14. A.Lubotzky, R.Phillips, P.Sarnak, *Ramanujan graphs*, Combin. 8 (1988) 261-277.
15. A.Lubotzky, *in Discrete groups*, Expanding graphs and invariant measures, Progress in Math. 125, Birkhauser, 1994.
16. S.Ma, *Partial difference sets*, Discrete Math. 52, (1984) 75-89.
17. M.Muzychuk, *The structure of rational Schur rings over cyclic groups*, Europ. J. Combin. 14, (1993) 479-490.
18. M.Muzychuk, M.Klin, R.Poschel, *The isomorphism problem for circulant graphs via Schur ring theory*, DIMACS 56, (2001) 241-264.
19. P.Potocnik, *On 2-arc transitive Cayley graphs of abelian groups*, Discrete Math 244, (2002) 417-421.
20. WShiu, *Schur rings over dihedral groups*, Chinese J. Math 18, (1990) 209-223.
21. J.Turner, *Point-symmetric graphs of prime order*, J. Combin. Theory 3, (1967) 136-145.
22. H.Wielandt, *Finite permutation groups*, Academic press, New York, 1964.

Genesis and development of Schur rings, as a bridge of group and algebraic graph theory

Department of Mathematics, Hannam University **Eun Mi Choi**

In 1933, I. Schur introduced a Schur ring in connection with permutation group and regular subgroup. After then, it was studied mostly for purely group theoretical purposes. In 1970s, Klin and Poschel initiated its usage in the investigation of graphs, especially for Cayley and circulant graphs. Nowadays it is known that Schur ring is one of the best way to enumerate Cayley graphs. In this paper we study the origin of Schur ring back to 1933 and keep trace its evolution to graph theory and combinatorics.

Key words: group ring, Schur ring, graph, Cayley graph, circulant graph, isomorphism

2000 Mathematics Subject Classification: 01, 05C, 05C25

논문 접수: 2006년 4월 8일, 심사 완료: 2006년 5월