제 2 장　해　설

§ 2.1.1　공 리 계

§ 2.1.2　행렬식의 성질

§ 2.4.1　양의 정수의 분할

§ 2.4.2　우치환과 기치환

§ 2.7　유한 단순군

§ 2.10　반직적(半直積)

§ 2.11　대칭군과 교대군의 켤레류

§2.1.1 공 리 계

유클리드의 '기하학 원론'은 정의, 공준과 공리로부터 시작된다. 여기서 공리와 공준은 각각 '공통 개념'과 '요청'을 뜻한다. 유클리드의 첫째 공리

'동일한 것에 같은 것은 서로 같다.'

는 누구나 모두 공통적으로 알 수 있는 것이라고 생각하는 것인데 비하여 유클리드의 공준 (i) ~ (v) 는 기하학을 전개하는 데에는 적어도 이것만은 성립하는 것으로 인정하여야 한다는 요청을 의미한다.

유클리드의 '기하학 원론'에서 '요청'이란 '자명한 이치' 또는 '진리의 기초'라고 생각할 수 있다. 그러나, 非 유클리드 기하학의 탄생으로 이러한 생각은 바뀌게 되었고, 특히 Hilbert 이래 추상수학이 발전해감에 따라 공리의 의미는 달라지게 되었다.

한 학문을 전개해 나가기 위해서는 개념을 설명하는 용어가 필요하고 그 의미를 엄밀히 정의하여야 한다. 그런데, 한 용어를 정의하려면 여러 용어가 필요하고 이들 용어를 정의하려면 또 다른 용어들이 필요하게 되어, 이와 같은 과정을 되풀이면 결국 처음 용어를 정의할 수 없게 되거나 또는 처음 용어를 이용하여 다른 용어를 정의하게 되는 순환 논법에 빠지게 된다. 정리의 증명에 대해서도 마찬가지이다. 이러한 어려움을 피하기 위해서는 정의하지 않은 개념인 無定義 要素와 無定義 關係를 받아드리고 또 몇 개의 명제는 公理로 받아드려 이 공리를 증명 없이 이용할 필요가 있다. 이러한 관점에서 보면, 공리는 자명한 진리가 아니라 이론 전개를 위한 추론의 출발점으로서 가정한(즉, 요청된) 명제이다. 무정의 요소와 무정의 관계는 정의하지 않고 사용하지만, 그 내용은 공리에 의하여 규정된다. 예를 들어, 공리

'서로 다른 두 점을 지나는 직선은 단 하나 존재한다.'

는 무정의 요소인 '점'과 '직선'을 무정의 관계 ' … 를 지난다.' 로 결합시키는 방법을 설명해준다.

이와 같은 무정의 요소와 무정의 관계 그리고 이에 관한 공리들을 한 데 묶어 놓은 **공리계**(公理系 system of axioms) 로부터 출발하여 엄밀한 추론에 의하여 특정한 수학적 체계가 건설된다. 서로 다른 공리계는 전혀 다른

체계가 건설된다. 한 수학적 체계의 공리계를 만족시키는 구체적인 예를 이 체계의 **모형**(模型 model)이라고 한다. 일반적으로, 한 수학적 체계에 대한 모형은 여러 개가 있을 수 있다.

수학적 체계에 대한 공리계가 갖추어야 할 성질은 다음과 같다.

(1) 무모순성(consistency)

한 공리계에는 모순을 내포되어 있지 말아야 한다. 공리계가 모순을 내포하고 있다는 말은 이 공리계로부터 출발한 수학적 체계에서

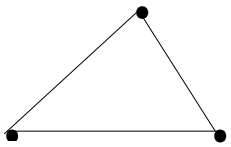
'한 명제 p와 그 부정 $\sim p$가 동시에 성립한다.'

는 것을 의미한다. 이러한 경우에 이로부터 모든 명제 q가 성립하게 된다. 실제로, 명제 p가 성립하므로 분명히 명제 'p 또는 q'가 성립하고, 한편 가정에 의하여 $\sim p$도 성립하므로 명제 q가 성립한다. 따라서 예를 들어 '$1 = 0$'과 같은 명제가 성립하게 되어 모순이 생긴다.

한 공리계를 만족시키는 모형이 적어도 하나 존재하는 경우에 이 공리계는 **무모순**(無矛盾 consistent)이라 한다. 유클리드 기하학과 非유클리드 기하학의 무모순성은 그 공리계에 대한 모형이 존재함을 보임으로써 밝힐 수 있다.

보기 1 다음과 같은 8개의 공리로 이루어진 공리계를 생각해 보자.

공리 1 : 한 직선이 한 점을 지나면, 이 점은 이 직선 위에 있다.
공리 2 : 한 점이 한 직선 위에 있으면, 이 점은 이 점을 지난다.
공리 3 : 임의의 서로 다른 두 점에 대하여, 이 두 점을 지나는 직선이 단 하나 존재한다.
공리 4 : 임의의 서로 다른 두 직선에 대하여, 이 두 직선은 꼭 한 개의 점을 공유한다.
공리 5 : 임의의 직선에 대하여, 이 직선 위에는 꼭 두 개의 점이 존재한다.
공리 6 : 임의의 점에 대하여, 이 점을 지나는 직선은 꼭 두 개 존재한다.
공리 7 : 점은 꼭 세 개 존재한다.
공리 8 : 직선은 꼭 세 개 존재한다.



이 공리계에 대한 모형이 존재하므로 이 공리계는 무모순이다. 실제로, 오른쪽 그림은 위의 공리계를 만족시키는 모형을 나타낸다.

이 공리계에서 '공리 1 ~ 공리 7'을 이용하여 '공리 8'을 증명할 수 있다. 실제로, '공리 7'에 의하여 서로 다른 세 점이 존재하고 또 '공리 3'에 의하여 세 직선이 존재한다. 한편, 이 세 직선 중에 어느 두 직선이 같다면 이 직선 위에 세 점이 존재하게 되어 '공리 5'에 모순되므로, 이들 세 직선은 모두 서로 다르다. 그리고, '공리 5'와 '공리 7'에 의하여 이들 세 직선 이외의 직선은 존재하지 않는다. 이 결과로부터,

공리 1 ~ 공리 7, 공리 9 : 직선은 꼭 두 개 존재한다.

로 이루어진 공리계는 모순을 내포하고 있음을 알 수 있다.

(2) 독립성

모순이 내포되지 않은 공리계에서 한 공리가 나머지 다른 공리로부터 유도될 때 이 공리는 나머지 다른 공리에 **종속적**(從屬的 dependent)이라고 한다. 이와는 반대로 한 공리가 나머지 다른 공리로부터 유도되지 않을 때 이 공리는 나머지 다른 공리와 **독립적**(獨立的 independent)이라 하고, 한 공리계에서 각 공리가 나머지 다른 공리와 독립일 때, 이 공리계는 **독립적**이라 한다.

한 공리계에서 다른 공리에 종속적인 공리는 공리계에서 제외시켜도 좋다. 예를 들어, 보기 1.3.1의 공리계에서 '공리 8'은 '공리 1 ~ 공리 7'에 종속적이므로 이 공리계에서 '공리 8'을 제외시켜도 좋다.

유클리드 기하학과 함께 두 종류의 非 유클리드 기하학이 성립한다는 사실은 제 5 공준이 다른 공리 및 공준과 독립적임을 말해 주고 있다.

(3) 완전성

한 공리계에 대한 두 모형에 대하여 각 무정의 요소 사이에 일대일 대응이 존재하고 또 이 일대일 대응에 의하여 공리계에서의 무정의 관계가 모두 보존될 때, 이 두 모형은 **동형**(同型 isomorphic)이라고 한다. 동형인 두 모형은 본질적으로 같다고 말할 수 있다.

보기 2 다음과 같은 공리계를 생각해 보자.

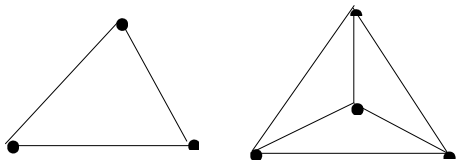
공리 1 : 한 직선이 한 점을 지나면, 이 점은 이 직선 위에 있다.

공리 2 : 한 점이 한 직선 위에 있으면, 이 점은 이 점을 지난다.

공리 3 : 임의의 서로 다른 두 점에 대하여 이 두 점을 지나는 직선이 단 하나 존재한다.

공리 4 : 임의의 서로 다른 두 직선에 대하여 이 두 직선은 꼭 한 개의 점을 공유한다.

오른쪽 두 그림은 위의 공리계에 대한 모형을 나타내며, 이 두 모형은 동형이 아니다.



한 공리계에 대한 임의의 모형이 모두 동형일 때, 이 공리계는 **범주적**(categorical)이라고 한다. 예를 들어, 힐버트가 설정한 유클리드 기하학의 공리계는 범주적이다(§1.2 참조). 한편, 힐버트 공리계에서 '평행선 공리'를 제외한 나머지 다른 공리를 택하여 새로운 공리계를 설정하면,

유클리드 기하학, 쌍곡적 非 유클리드 기하학,
타원적 非 유클리드 기하학

이 탄생하게 되는데, 이들 기하학에 대한 모형은 모두 서로 동형이 아니므로 이 새로운 공리계는 범주적이 아니다.

한 공리계로부터 출발한 수학적 체계에서 무정의 요소와 무정의 관계로 표현되는 모든 명제의 참과 거짓을 공리계를 이용하여 판정할 수 있을 때, 이 공리계는 **완전하다**(complete)고 한다. 예를 들어, Hilbert 가 설정한 유클리드 기하학의 공리계는 완전하다. 일반적으로, 범주적인 공리계는 완전하다.

한 집합 위에 이항연산(들)이 정의되어 있으면서 이 연산(들)에 관하여 어떤 공리계를 만족시킬 때, 이 집합과 연산(들)을 함께 묶어 이것을 **대수적 체계**(代數的 體系 algebraic system)라 하고 이 집합은 **대수적 구조**(代數的 構造 algebraic structure)를 가지고 있다고 한다. 앞으로, 논할 군, 덧셈군, 환, 가환환, 나눗셈환, 체, 와 같은 대수적 체계에 관한 공리계에 대해서는 동형이 아닌 모형이 많이 존재한다.

§2.1.2 행렬식의 성질

실수체 $\mathbb{R}$ 위의 n차의 행렬식에 대하여 다음 정리가 성립한다.

정리 1 실수체 $\mathbb{R}$ 위의 n차의 행렬 A에 대하여 $\det A^T = \det A$ 이다.

$$\begin{vmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

정리 2 실수체 $\mathbb{R}$ 위의 행렬 $A = [a_{ij}]_{n\times n}$에 대하여 서로 다른 두 행[열]을 서로 바꾸어 놓은 행렬을 B 이라고 하면, $\det B = -\det A$ 이다.

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = - \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

또, A의 서로 다른 두 행 [두 열]의 성분이 일치하면, $\det A = 0$ 이다.

정리 3 실수체 $\mathbb{R}$ 위의 행렬 $A = [a_{ij}]_{n\times n}$에 대하여 A의 한 행[열]을 k배 하여 얻은 행렬을 B이라고 하면 $\det B = k \det A$ 이다.

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ ka_{i1} & ka_{i2} & \cdots & ka_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = k \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

정리 4 실수체 $\mathbb{R}$ 위의 행렬 $A=[a_{ij}]_{n\times n}$에서 제 i 행]의 성분이 차례로 $b_1+c_1,\ b_2+c_2,\ \cdots,\ b_n+c_n$일 때 다음이 성립한다,

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \hline b_1+c_1 & b_2+c_2 & \cdots & b_n+c_n \\ \hline a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

$$= \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \hline b_1 & b_2 & \cdots & b_n \\ \hline a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \hline c_1 & c_2 & \cdots & c_n \\ \hline a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

정리 6 실수체 $\mathbb{R}$ 위의 행렬 $A=[a_{ij}]_{n\times n}$에 대하여 다음이 성립한다.

(1) A의 서로 다른 두 행 [두 열]의 대응하는 성분이 비례하거나 또는 일치하면, $\det A=0$ 이다.

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \hline a_{i1} & a_{i2} & \cdots & a_{in} \\ \hline ka_{i1} & ka_{i2} & \cdots & ka_{in} \\ \hline a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = k \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \hline a_{i1} & a_{i2} & \cdots & a_{in} \\ \hline a_{i1} & a_{i2} & \cdots & a_{in} \\ \hline a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = 0$$

특히, A의 한 행 [열]의 성분이 0 이면, $\det A=0$ 이다.

(2) A의 한 행에 다른 행의 k 배 [한 열에 다른 열의 k 배]를 더하여 얻은 행렬을 B 라고 하면, $\det B=\det A$ 이다.

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \hline a_{i1}+ka_{j1} & a_{i2}+ka_{j2} & \cdots & a_{in}+ka_{jn} \\ \hline a_{j1} & a_{j2} & \cdots & a_{jn} \\ \hline a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \hline a_{i1} & a_{i2} & \cdots & a_{in} \\ \hline a_{j1} & a_{j2} & \cdots & a_{jn} \\ \hline a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

정리 7 실수체 $\mathbb{R}$ 위의 행렬 $A=[a_{ij}]_{n\times n}$가 下 삼각행렬이거나 또는 上 삼각행렬이면, $\det A = a_{11}a_{22}\cdots a_{nn}$ 이다. 즉,

$$\begin{vmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{vmatrix} = a_{11}a_{22}\cdots a_{nn}$$

정리 8 실수체 $\mathbb{R}$ 위의 행렬 $A=[a_{ij}]_{n\times n}$ 에 대하여 다음이 성립한다.

(1) 제 i 행에 관한 전개 $(1\le i\le n)$

$$\det A = a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{ij}A_{ij} + \cdots + a_{in}A_{in}$$

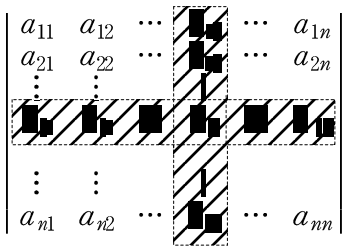
(2) 제 j 열에 관한 전개 $(1\le j\le n)$

$$\det A = a_{1j}A_{1j} + a_{2j}A_{2j} + \cdots + a_{ij}A_{ij} + \cdots + a_{nj}A_{nj}$$

정리 9 행렬 $A=[a_{ij}]_{n\times n}$ 에서 A 의 제 i 행과 제 j 열을 없애어 얻은 소행렬식(minor)을 M_{ij} 로 나타내면 다음이 성립한다

$$A_{ij} = (-1)^{i+j}M_{ij}$$

$M_{ij} =$



정리 10 (Vandermonde 의 행렬식) 실수체 $\mathbb{R}$ 위의 다음이 성립한다.

$$V = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^{\,2} & x_2^{\,2} & \cdots & x_n^{\,2} \\ \vdots & \vdots & \cdots & \vdots \\ x_1^{\,n-1} & x_2^{\,n-1} & \cdots & x_n^{\,n-1} \end{vmatrix} = (-1)^{\frac{(n-1)n}{2}} \prod_{i<j}(x_i - x_j)$$

$$= (-1)^{\frac{(n-1)n}{2}} (x_1-x_2)(x_1-x_3)\cdots(x_1-x_n)$$
$$(x_2-x_3)\cdots(x_2-x_n)$$
$$\cdots\cdots\cdots\cdots$$
$$(x_{n-1}-x_n)$$

§2.4.1 양의 정수의 분할

다음 사항은 [5] 의 §2.6 의 내용을 옮겨 쓴 것이다.
예를 들어, 5 는 다음과 같이 몇 개의 양의 정수의 합으로 나타낼 수 있다.

$$5 = 5,$$
$$5 = 1 + 4, \qquad 5 = 2 + 3,$$
$$5 = 1 + 1 + 3, \qquad 5 = 1 + 2 + 2,$$
$$5 = 1 + 1 + 1 + 2,$$
$$5 = 1 + 1 + 1 + 1 + 1$$

여기서 더하는 순서는 무시하고 예를 들어

$$5 = 1 + 4, \qquad 5 = 4 + 1$$

을 한 가지 표현 방법이라고 생각한다면, 5 를 양의 정수의 합으로 나타내는 방법은 모두 7 가지 있다. 그리고, 이러한 표현 중에서

$$5 = 1 + 1 + 3, \qquad 5 = 1 + 2 + 2$$

과 같이 5 를 세 항의 합으로 나타내는 방법은 2 가지 있다

정의 1 양의 정수 n 을 양의 정수의 합

$$n = a_1 + a_2 + \cdots + a_k \qquad (a_1 \le a_2 \le \cdots \le a_k)$$

으로 나타내는 것을 n 의 **분할**(分割 partition)이라고 한다. 또, 양의 정 n 을 양의 정수들의 합으로 나타내는 분할의 개수를 $p(n)$ 으로 나타낸다. 또, 양의 정수 n, k 에 대하여 위와 같이 n 을 꼭 k 개의 양의 정수의 합으로 나타내는 분할의 개수를 $p(n, k)$ 로 나타내고, $p(n, 0) = 0$ 으로 정한다.

보기 1 앞에서 본 바와 같이 $p(5) = 7$ 이고, 또 다음이 성립한다.

$$p(5,1) = 1, \quad p(5,2) = 2, \quad p(5,3) = 2,$$
$$p(5,4) = 1, \quad p(5,5) = 1$$

정리 2 양의 정수 n, k에 대하여 다음 등식이 성립한다.

(1) $p(n,0) = 0$, $p(n,1) = 1$, $p(n,n) = 1$

(2) $k > n$이면, $p(n,k) = 0$이다.

(3) $\sum_{k=1}^{n} p(n,k) = p(n,1) + p(n,2) + \cdots + p(n,n) = p(n)$

증 명 (1) 정의에 의하여 $p(n,0) = 0$이다.

그리고 n을 한 개의 양의 정수의 합으로 나타내는 방법은 $n = n$ 뿐이고 n을 n개의 양의 정수의 합으로 나타내는 방법은

$$n = 1 + 1 + \cdots + 1$$

뿐이므로 $p(n,1) = 1$, $p(n,n) = 1$이다.

(2) $k > n$일 때, k개의 양의 정수들의 합은 n보다 크므로 n을 k개의 양의 정수의 합으로 나타낼 수 없고 따라서 $p(n,k) = 0$이다.

(3) 정의 1 에 의하여 (3)이 성립한다.

보기 2 보기 1 과 다음 결과에 의하여 아래의 표를 얻는다.

$1 = 1,$

$2 = 2, \quad 2 = 1 + 1,$

$3 = 3, \quad 3 = 1 + 2, \quad 3 = 1 + 1 + 1$

$4 = 4, \quad 4 = 1 + 3, \quad 4 = 2 + 2,$

$4 = 1 + 1 + 2, \quad 4 = 1 + 1 + 1 + 1,$

$6 = 6, \quad 6 = 1 + 5,$

$6 = 2 + 4, \quad 6 = 3 + 3$

$6 = 1 + 1 + 4,$

$6 = 1 + 2 + 3, \quad 6 = 2 + 2 + 2,$

$6 = 1 + 1 + 1 + 3,$

$6 = 1 + 1 + 2 + 2,$

$6 = 1 + 1 + 1 + 1 + 2,$

$6 = 1 + 1 + 1 + 1 + 1 + 1$

$p(n,k)$ 와 $p(n)$

n	1	2	3	4	5	6	$p(n)$
1	1	0	0	0	0	0	1
2	1	1	0	0	0	0	2
3	1	1	1	0	0	0	3
4	1	2	1	1	0	0	5
5	1	2	2	1	1	0	7
6	1	3	3	2	1	1	11

정리 3 정수 $n\ (\geq 2)$과 $1 \leq k < n$인 양의 정수 k에 대하여 다음이 성립한다.

(1) $p(n, k) = p(n-1, k-1) + p(n-k, k)$

(2) $p(n, k) = p(n-k, 1) + p(n-k, 2) + \cdots + p(n-k, k)$

$$= \sum_{i=1}^{k} p(n-k, i)$$

증명 (1) 정수 n을 k개의 양의 정수들의 합으로 나타내는 분할 전체의 집합을 S라 하고, 이러한 분할 중에서 1을 포함하는 분할 전체의 집합을 A, 1을 포함하지 않는 분할 전체의 집합을 B라고 하자. 이 때,

$$|S| = p(n, k), \quad S = A \cup B,\ A \cap B = \emptyset$$

이므로 $p(n, k) = |A| + |B|$이다. 그런데, A에 속해 있는 n의 분할

$$n = 1 + a_2 + a_3 + \cdots + a_k \qquad (1 \leq a_2 \leq \cdots \leq a_k)$$

에 대하여 $n-1 = a_2 + a_3 + \cdots + a_k$는 $n-1$을 $k-1$개의 양의 정수들의 합으로 나타낸 분할이고, 역으로 $n-1$을 $k-1$개의 양의 정수들의 합으로 나타낸 등식

$$n-1 = a_2 + a_3 + \cdots + a_k \qquad (1 \leq a_2 \leq \cdots \leq a_k)$$

에 대하여 $n = 1 + a_2 + a_3 + \cdots + a_k$는 A에 속하는 n의 분할이다.

따라서 $|A| = p(n-1, k-1)$ 이다.

그리고, B에 속해 있는 n의 분할

$$n = a_1 + a_2 + \cdots + a_k \qquad (2 \leq a_1 \leq a_2 \leq \cdots \leq a_k)$$

에 대하여 $n-k = (a_1-1) + (a_2-1) + \cdots + (a_k-1)$은 $n-k$를 k개의 양의 정수의 합으로 나타낸 분할이고, 역으로

$$n-k = b_1 + b_2 + \cdots + b_k \qquad (1 \leq b_1 \leq b_2 \leq \cdots \leq b_k)$$

가 $n-k$을 k개의 양의 정수들의 합으로 나타낸 분할이면,

$$n = (b_1+1) + (b_2+1) + \cdots + (b_k+1)$$

은 n의 분할이고 또 $2 \leq b_1+1 \leq b_2+1 \leq \cdots \leq b_k+1$이므로 이 분할은 B에 속한다. 따라서 $|B| = p(n-k, k)$ 이다.

그러므로 $p(n,k) = |A| + |B| = p(n-1,k-1) + p(n-k,k)$ 이다.

(2) 위의 (1) 에 의하여 다음이 성립한다.

$$\begin{aligned}
p(n,k) &= p(n-1,k-1) + p(n-k,k)\\
p(n-1,k-1) &= p(n-2,k-2) + p(n-k,k-1)\\
p(n-2,k-2) &= p(n-3,k-3) + p(n-k,k-2)\\
&\vdots\\
p(n-(k-1),k-(k-1)) &= p(n-k,0) + p(n-k,1)\\
&= p(n-k,1)
\end{aligned}$$

이들 등식의 양변을 더하여 정리하면 다음 결과를 얻는다.

$$\begin{aligned}
p(n,k) &= p(n-k,k)+p(n-k,k-1)+\cdots+p(n-k,1)\\
&= p(n-k,1)+p(n-k,2)+\cdots+p(n-k,k)
\end{aligned}$$

보기 3 정리 3 (2) 에 의하여 다음 결과를 얻는다.

$$\begin{aligned}
&p(7,2) = p(5,1) + p(5,2) = 1+2 = 3,\\
&p(7,3) = p(4,1) + p(4,2) + p(4,3) = 1+2+1 = 4,\\
&p(7,4) = p(3,1) + p(3,2) + p(3,3) = 1+1+1 = 3,\\
&p(7,5) = p(2,1) + p(2,2) = 1+1 = 2,\\
&p(7,6) = p(1,1) = 1
\end{aligned}$$

이와 같은 방법으로, $p(8,k)$ 와 $p(8)$ 를 계산할 수 있다.

이제까지 얻은 결과를 종합하면 다음 표를 얻는다.

n	1	2	3	4	5	6	7	8	$p(n)$
1	1	0	0	0	0	0	0	0	1
2	1	1	0	0	0	0	0	0	2
3	1	1	1	0	0	0	0	0	3
4	1	2	1	1	0	0	0	0	5
5	1	2	2	1	1	0	0	0	7
6	1	3	3	2	1	1	0	0	11
7	1	3	4	3	2	1	1	0	15
8	1	4	5	5	3	2	1	1	22

보기 4 양의 정수 3 은

$$3 = 1+1+1, \quad 3 = 1+2, \quad 3 = 3$$

와 같이 분할되므로 다음이 성립한다.

$$p(3.3) = 1, \quad p(3,2) = 1, \quad p(3,1) = 1$$

$$p(3) = 1+1+1 = 3$$

따라서 대칭군 S_3 의 원소는 그 형에 따라 다음과 같이 분류된다.

형	원 소	개수	위수
{1, 1, 1}	1	1	1
{1, 2}	(1 2), (1 3), (2 3)	3	2
{3}	(1 2 3), (1 3 2)	2	3

보기 5 양의 정수 4 는

$$4 = 1+1+1+1, \quad 4 = 1+1+2,$$
$$4 = 1+3, \qquad 4 = 2+2, \qquad 4 = 4$$

와 같이 분할되므로 다음이 성립한다.

$$p(4.4) = 1, \quad p(4,3) = 1, \quad p(4,2) = 2, \quad p(4,1) = 1$$

$$p(4) = 1+1+2+1 = 5$$

따라서 대칭군 S_4 의 원소는 다음과 같이 5 개의 형으로 분류된다.

형	원 소	개수	위수
{1,1,1,1}	1	1	1
{1,1,2}	(1 2), (1 3), (1 4), (2 3), (2 4), (3 4)	6	2
{1,3}	(1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3)	8	3
{2,2}	(1 2)∘(3 4), (1 3)∘(2 4), (1 4)∘(2 3)	3	2
{4}	(1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2)	6	4

보기 6 양의 정수 5 는

$$5=1+1+1+1+1,\quad 5=1+1+1+2,$$
$$5=1+1+3,\qquad 5=1+2+2,$$
$$5=1+4,\qquad 5=2+3,\qquad 5=5$$

와 같이 분할되므로 다음이 성립한다.

$$p(5.5)=1,\ p(5,4)=1,\ p(5,3)=2,\ p(5,2)=2,\ p(5,1)=1$$
$$p(5)=1+1+2+2+1=7$$

따라서 대칭군 S_5 의 원소는 다음과 같이 7 개의 형으로 분류된다.

형	대표원	개 수	위수
{1, 1, 1, 1, 1}	1	1	1
{1, 1, 1, 2 }	(1 2)	10	2
{1, 1, 3}	(1 2 3)	20	3
{1, 2, 2}	(1 2)◦(3 4)	15	2
{1, 4}	(1 2 3 4)	30	4
{2, 3}	(1 2)◦(3 4 5)	20	6
{ 5 }	(1 2 3 4 5)	24	5

위의 표에서 예를 들어 {2,3} 형의 치환은 다음과 같이 20 개가 있다.

(1 2)◦(3 4 5), (1 3)◦(2 4 5), (1 4)◦(2 3 5), (1 5)◦(2 3 4),
(1 2)◦(3 5 4), (1 3)◦(2 5 4), (1 4)◦(2 5 3), (1 5)◦(2 4 3),
(2 3)◦(1 4 5), (2 4)◦(1 3 5), (2 5)◦(1 3 4),
(2 3)◦(1 5 4), (2 4)◦(1 5 3), (2 5)◦(1 4 3),
(3 4)◦(1 2 5), (3 5)◦(1 2 4),
(3 4)◦(1 5 2), (3 5)◦(1 4 5),
(4 5)◦(1 2 3),
(4 5)◦(1 3 2)

보기 7 보기 3 의 표에 의하여 $p(8)=22$ 이다.

따라서 대칭군 S_8 의 원소는 22 개의 형으로 분류된다.

§2.4.2 우치환과 기치환

치환 $\sigma \in S_n$ 의 표준분해가 다음과 같다고 하자.

$$(*) \qquad \sigma = (i_1\, i_2 \cdots i_r) \circ (j_1\, j_2 \cdots j_s) \circ \cdots \circ (l_1\, l_2 \cdots l_t)$$

$$r + s + \cdots + t = n, \qquad 1 \le r \le s \le \cdots \le t$$

이 때, $N(\sigma) = (r-1) + (s-1) + \cdots + (t-1)$ 이라 할 때, 치환 σ 가

$$\sigma = (a_1\, b_1) \circ (a_2\, b_2) \circ \cdots \circ (a_m\, b_m)$$

과 같이 m 개의 호환의 곱으로 분해되는 경우에 $N(\sigma)$ 가 짝수이면 m 도 짝수이고 $N(\sigma)$ 가 홀수이면 m 도 홀수임을 밝혀 m 이 짝수인지 홀수인지는 분해하는 방법에 관계없이 일정함을 증명한다.

먼저 (*) 에서 서로 다른 두 문자 a_i, b_i 가 한 순환치환에 들어 있으면 $N((a_i\, b_i) \circ \sigma) = N(\sigma) - 1$이지만 a_i, b_i 가 서로 다른 순환치환에 들어 있으면 $N((a_i\, b_i) \circ \sigma) = N(\sigma) + 1$ 이므로 $N((a_i\, b_i) \circ \sigma) = N(\sigma) \pm 1$ 이다. 실제로, 다음 등식이 성립한다.

$$(a_i\, b_i) \circ (a_i\, c_1 \cdots c_h\, b_i\, d_1 \cdots d_k) = (a_i\, c_1 \cdots c_h) \circ (b_i\, d_1 \cdots d_k),$$

$$(a_i\, b_i) \circ (a_i\, c_1 \cdots c_h) \circ (b_i\, d_1 \cdots d_k) = (a_i\, c_1 \cdots c_h\, b_i\, d_1 \cdots d_k)$$

한편, $\sigma = (a_1\, b_1) \circ (a_2\, b_2) \circ \cdots \circ (a_m\, b_m)$ 일 때,

$$(a_m\, b_m) \circ \cdots \circ (a_2\, b_2) \circ (a_1\, b_1) \circ \sigma = 1$$

이므로 앞의 결과에 의하여 다음이 성립한다.

$$N(\sigma) \pm 1 \pm 1 \cdots \pm 1 = N(1) = 0 \quad (\pm 1 \text{ 은 } m \text{ 개})$$

여기서 m 개의 ± 1 중에 $+1$ 과 -1 이 각각 m_1 개, m_2 개 있다고 하면,

$$N(\sigma) + m_1 - m_2 = 0, \qquad m = m_1 + m_2$$

이므로 $N(\sigma) = m - 2m_2$ 즉 $m = N(\sigma) + 2m_2$ 이다.

따라서 $N(\sigma)$ 가 짝수이면 m 도 짝수이고 $N(\sigma)$ 가 홀수이면 m 도 홀수이므로, m 이 짝수인지 홀수인지는 분해하는 방법에 관계없이 일정하다.

§2.7 유한 단순군

유한 단순군은 다음과 같은 네 가지 종류로 분류된다.

(1) 素數 위수의 순환군

(2) 교대군 A_n, $n \geq 5$

(3) Lie 형의 단순군

(4) 26 개의 散在 群(sporatic group)

유한 단순군의 분류에 관한 정리는 지난 50 여년간에 걸쳐 많은 군론학자의 노력에 의하여 1980 년대에 이르러 증명되었다. 유한 단순군의 분류에 관한 정리에 대한 증명은 대단히 길고 대단히 어려우며 이 정리를 이해하는 데에는 Lie 다원환(Lie algebra)에 관한 지식이 필요하다(해설 314 참조).

오늘날 유한군론의 중요 과제 중의 하나는 유한 단순군의 분류 정리에 대한 증명의 簡易化하는 문제와 이 정리를 이용하여 일반적인 유한군의 성질을 규명하는 일이며 이에 대해서는 다음 참고 문헌을 참조하기 바란다.

1. M. Aschbacher, The finite simple groups and their classification, Yale mathematical monographs **7**, , Yale University Pree, New Haven, 1980

2. Bourbaki, N., Groupes et algèbres de Lie , Chap. 4, 5 et 6, Hermann, Paris, 1968

3. R. Carter, Simple groups of Lie type, Wiley-Interscience, New York, 1972

4. R.L. Griess, the friendly giant, Invent. Math. **69** (1982), 1 − 101

5. R. Steinberg, Lectures on Chevalley groups, Lecture Notes, Yale University. 1968

6. Suzuki, M., Group theory, I, II, Springer-Verlag, New York, 1981, 1986

7. M. Suzuki(鈴木 通夫), 有限單純群, 紀伊國屋數學叢書 **28**, 일본, 紀伊國屋書店, 1987

대칭군 S_n에서 짝수개의 호환의 곱으로 나타내어지는 치환을 우치환이라 하고, S_n에 속하는 우치환 전체로 이루어지는 부분군 A_n을 n차의 교대군이라고 한다.

특히, $A_2 = \{1\}$이고, 교대군

$$A_3 = \{1, (1\ 2\ 3), (1\ 3\ 2)\} = \langle (1\ 2\ 3) \rangle$$

는 위수 3인 순환군이고 따라서 단순군이다(정리 2.9.10).

한편, 4차의 교대군 A_4에서

$$V_4 = \{1, (1\ 2)\circ(3\ 4), (1\ 3)\circ(2\ 4), (1\ 4)\circ(2\ 3)\}$$

는 A_4의 정규부분군이므로 A_4는 단순군이 아니다. 그리고, A_4의 정규부분군은 $\{1\}$, V_4, A_4 뿐이다.

정리 1 $n \geq 3$일 때, 대칭군 S_n에서 3항 순환치환 전체의 집합을 T_n이라고 하면 다음이 성립한다.

(1) 교대군 A_n은 T_n에 의하여 생성된다.

(2) $n \geq 5$이면, T_n은 교대군 A_n안에서 한 켤레류를 이룬다.

증 명 (1) 정리 2.4.15 에 의하여 (1) 이 성립한다.

(2) $n \geq 5$이라고 하자. 임의의 3항 치환 $(i\ j\ k) \in T_n$과 임의의 우치환 $\sigma \in A_n$에 대하여 다음이 성립한다.

$$\sigma\circ(i\ j\ k)\circ\sigma^{-1} = (\sigma(i)\ \ \sigma(j)\ \ \sigma(k)) \in T_n$$

그리고, 임의의 두 3항 순환치환 $(i\ j\ k), (a\ b\ c) \in T_n$에 대하여

$$\sigma(i) = a, \quad \sigma(j) = b, \quad \sigma(k) = c$$

인 치환 $\sigma \in S_n$를 생각하면 $\sigma\circ(i\ j\ k)\circ\sigma^{-1} = (a\ b\ c)$이다. 그런데 $\sigma \in A_n$이면, $(i\ j\ k), (a\ b\ c)$는 A_n안에서 켤레원소이다.

한편, $\sigma \notin A_n$인 경우에 σ는 기치환이다

그런데, $n \geq 5$이므로 $1, 2, \cdots, n$ 중에서 a, b, c가 아닌 서로 다른 두

문자 d, e를 택하여 $\tau = (d\ e)$ 이라고 하면 $\tau \circ \sigma \in A_n$이고

$$\tau \circ \sigma \circ (i\ j\ k) \circ \sigma^{-1} \circ \tau^{-1} = \tau \circ (a\ b\ c) \circ \tau^{-1} = (a\ b\ c)$$

이므로 이 경우에도 $(i\ j\ k), (a\ b\ c)$는 A_n 안에서 켤레원이다.

따라서 T_n은 교대군 A_n 안에서 한 켤레류를 이룬다.

정리 2 $n \geq 5$이면, 교대군 A_n은 단순군이다.

증 명 이제 $N\ (\neq \{1\})$을 교대군 A_n의 정유부분군이라 하고 N이 3항 순환치환을 하나도 포함하지 않는다고 가정하자.

이 때, $\tau \in N$, $\tau \neq 1$를 3항 순환치환이 아니라 가정하고 τ가 다음과 같은 꼴의 $\{r, s, \cdots, t\}$ 형의 치환이라고 하자(정리 2.6.5 참조).

$$\tau = (i_1\ i_2 \cdots i_r) \circ (j_1\ j_2 \cdots j_s) \circ \cdots \circ (l_1\ l_2 \cdots l_t)$$

$$n = r + s + \cdots + t, \qquad 1 \leq r \leq s \leq \cdots \leq t \leq n$$

그런데, $r \geq 4$인 경우에는

$$\tau = (a\ b \cdots c\ d) \circ \cdots$$

의 꼴이고, 한편 $1 \leq r \leq 3$인 경우에는 τ는 3항 순환치환이 아니고 길이가 2이상인 순환치환을 적어도 두 개 포함하므로 τ는

$$\tau = (a\ b \cdots) \circ (c\ d \cdots) \circ \cdots$$

와 같은 꼴로 나타내어진다(a, b, c, d는 서로 다른 네 문자).

여기서, 우치환 $\sigma = (a\ c\ d) \in A_n$를 택하여 $\rho = \tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1}$이라고 하면,

$\sigma \circ \tau^{-1} \circ \sigma^{-1} \in N$이므로 $\rho = \tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} \in N$이고 또 어느 경우에나

$$\rho = (\tau \circ \sigma \circ \tau^{-1}) \circ \sigma^{-1} = (b\ d\ *) \circ (a\ d\ c) \neq 1$$

이므로 ρ는 두 3항 순환치환의 곱이고 많아야 5개의 문자를 움직인다. 그리고, $\rho \in N$이고 N은 3항 순환치환을 포함하지 않으므로 ρ는 3항 순환치환이 아니고, 또 ρ는 우치환이므로 ρ는 5항 순환치환이거나 또는

서로 다른 두 호환의 곱이다. 그런데, ρ가

$$\rho = (i_1\ i_2\ i_3\ i_4\ i_5)$$

와 같은 꼴의 5항 순환치환인 경우에 $\gamma = (i_1\ i_2\ i_5)$ 이라고 하면,

$$(\rho \circ \gamma \circ \rho^{-1}) \circ \gamma^{-1} = \rho \circ (\gamma \circ \rho^{-1} \circ \gamma^{-1}) \in N$$

이고

$$(\rho \circ \gamma \circ \rho^{-1}) \circ \gamma^{-1} = (i_2\ i_3\ i_1) \circ (i_1\ i_5\ i_2) = (i_1\ i_5\ i_3)$$

이므로 N은 3항 순환치환을 포함하게 되어 모순이 생긴다. 그리고, ρ가

$$\rho = (i_1\ i_2) \circ (i_3\ i_4)$$

와 꼴의 서로 다른 두 호환의 곱인 경우에 $\gamma = (i_1\ i_2\ i_5)$ 이라고 하면

$$(\rho \circ \gamma \circ \rho^{-1}) \circ \gamma^{-1} = \rho \circ (\gamma \circ \rho^{-1} \circ \gamma^{-1}) \in N$$

이고

$$(\rho \circ \gamma \circ \rho^{-1}) \circ \gamma^{-1} = (i_2\ i_1\ i_5) \circ (i_1\ i_5\ i_2) = (i_1\ i_2\ i_5)$$

이므로 N은 3항 순환치환을 포함하게 되어 모순이 생긴다.

따라서 N은 적어도 한 개의 3항 순환치환을 포함한다. 한편, N이 3항 순환치환 τ를 포함하면, $N \lhd A_n$이므로 임의의 $\sigma \in A_n$에 대하여 $\sigma \circ \tau \circ \sigma^{-1} \in N$이고 따라서 정리 1 에 의하여 $N = A_n$이다.

그러므로 A_n은 단순군이다.

§2.10 반직적(半直積)

군 G 의 두 부분군 H, N에 대하여

$$G = HN, \quad N \lhd G, \quad H \cap N = \{e\}$$

일 때, G를 H, N의 **반직적**(半直積 semi-direct product)이라고 한다.

예를 들어, 군 G에서 $G = N_1 \dot{\times} N_2$ 일 때, G는 N_1, N_2 의 반직적이다.

반직적에 대하여 다음이 성립한다.

(1) 군 G가 H, N의 반직적일 때, 각 원소 $x \in G$는 단 한 가지 방법으로

$$x = hn \qquad (h \in H, \ n \in N)$$

과 같은 꼴로 나타내어진다.

실제로, $G = HN$이므로 각 $x \in G$는 위와 같은 꼴로 나타내어지고, 또

$$x = hn = h'n' \qquad (h, h' \in H, \ n, n' \in N)$$

이라고 가정하면 $h'^{-1}h = n'n^{-1} \in H \cap N = \{e\}$ 이므로 $h'^{-1}h = e$, $n'n^{-1} = e$이고 따라서 $h = h'$, $n = n'$ 이다.

(2) 다음과 같이 정의된 사상 동형사상이고 따라서 $H \cong G/N$이다.

$$\phi : H \longrightarrow G/N, \ \phi(h) = hN$$

실제로, 임의의 원소 $h_1, h_2 \in H$에 대하여

$$\phi(h_1 h_2) = h_1 h_2 N = (h_1 N)(h_2 N) = \phi(h_1)\phi(h_2)$$

이므로 ϕ는 준동형사상이다. 그리고

$$\begin{aligned} \operatorname{im}\phi &= \{\phi(h) \mid h \in H\} = \{hH \in G/N \mid h \in H\} \\ &= \{hnN \in G/N \mid h \in H, \ n \in N\} = G/N \end{aligned}$$

이므로 ϕ는 위로의 준동형사상이고, 또

$$\begin{aligned} h \in \ker\phi &\Rightarrow \phi(h) = eN \Rightarrow hN = eN \\ &\Rightarrow h \in N \cap H = \{e\} \Rightarrow h = e \end{aligned}$$

이므로 $\ker\phi = \{e\}$ 이고 따라서 ϕ는 일대일 준동형사상이다.

그러므로 ϕ는 동형사상이고, 따라서 $H \cong G/N$이다.

§2.11 대칭군과 교대군의 켤레류

치환 $\sigma = (1\ 2\ 3)$ 는 $\sigma = (1\ 2\ 3)$, $\sigma = (2\ 3\ 1)$, $\sigma = (3\ 1\ 2)$ 와 같이 3 가지 방법으로 순환치환으로 나타낼 수 있다. 그리고, 치환 σ 가 서로 소인 2 개의 3 항 치환 $\sigma_1 = (1\ 2\ 3)$, $\sigma_2 = (4\ 5\ 6)$ 의 곱

$$\sigma = \sigma_1 \circ \sigma_2 = (1\ 2\ 3) \circ (4\ 5\ 6)$$

일 때, σ_1 과 σ_2 는 각각 3 가지 방법으로 순환치환으로 나타낼 수 있고 또

$$\sigma = \sigma_1 \circ \sigma_2, \qquad \sigma = \sigma_2 \circ \sigma_1$$

이므로 σ 는 $2!\,3^2 = 18$ 가지 방법으로 순환치환의 곱으로 나타낼 수 있다.

일반적으로, σ 가 서로 소인 m 개의 k 항 순환치환의 곱

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_m$$

일 때, σ 는 $m!\,k^m$ 가지 방법으로 순환치환의 곱으로 나타낼 수 있다.

대칭군 S_n 에 속하는 치환 σ 의 표준분해가

$$(*) \qquad \sigma = (i_1\ i_2 \cdots i_r) \circ (j_1\ j_2 \cdots j_s) \circ \cdots \circ (l_1\ l_2 \cdots l_t)$$

$$n = r + s + \cdots + t, \qquad 1 \le r \le s \le \cdots \le t \le n$$

일 때, (*) 에서

1 항 순환치환의 개수가 $m_1\ (\ge 0)$ 개,

2 항 순환치환의 개수가 $m_2\ (\ge 0)$ 개,

$\vdots$

n 항 순환치환의 개수가 $m_n\ (\ge 0)$ 개

일 때, σ 를 $(m_1, m_2, \cdots, m_n)$ 형의 치환이라고 한다.

정리 1 대칭군 S_n 에 속하는 치환 σ 가 $(m_1, m_2, \cdots, m_n)$ 형의 치환일 때, σ 를 포함하는 켤레류에 속하는 치환의 개수는 다음과 같다.

$$\frac{n!}{m_1!\,1^{m_1}\,m_2!\,2^{m_2}\cdots m_n!\,n^{m_n}}$$

증명 먼저 n 개의 문자를 일렬로 늘어놓는 순열의 개수는 $n!$ 이고, 이러한 순열에 대하여 처음 m_1 개의 문자를 1 개씩 괄호로 묶고 다음에 $2m_2$ 의 문자를 2 개 씩 괄호로 묶는다. 이러한 과정을 계속하면, $n!$ 개의 순열을 $(m_1, m_2, \cdots, m_n)$ 형의 치환으로 나타낼 수 있다.

한편, 앞에서 본 바와 같이 $(m_1, m_2, \cdots, m_n)$ 형의 치환은

$$m = m_1!\,1^{m_1}\,m_2!\,2^{m_2}\cdots m_n!\;n^{m_n}$$

가지 방법으로 순환치환의 곱으로 나타낼 수 있다.

따라서 σ 를 포함하는 켤레류에 속하는 치환의 개수는 다음과 같다.

$$\frac{n!}{m_1!\,1^{m_1}\,m_2!\,2^{m_2}\cdots m_n!\;n^{m_n}}$$

보기 1 대칭군 S_5 의 켤레류는 다음과 같다(문제 6.2.3 참조).

켤레류	형	대표 원소	개 수
$\mathscr{C}_1$	{1, 1, 1, 1, 1}	1	1
$\mathscr{C}_2$	{1, 1, 1, 2}	(1 2)	10
$\mathscr{C}_3$	{1, 1, 3}	(1 2 3)	20
$\mathscr{C}_4$	{1, 2, 2}	(1 2)∘(3 4)	15
$\mathscr{C}_5$	{1, 4}	(1 2 3 4)	30
$\mathscr{C}_6$	{2, 3}	(1 2)∘(3 4 5)	20
$\mathscr{C}_7$	{ 5 }	(1 2 3 4 5)	24

(1) 대칭군 S_5 에서 치환 $\sigma = (1\ 2\ 3\ 4\ 5)$ 는 $(0, 0, 0, 0, 1)$ 형의 치환이므로 σ 를 포함하는 켤레류의 $\dfrac{5!}{1!\,5^1} = 24$ 이다.

(2) 대칭군 S_5 에서 $\sigma = (1\ 2)\circ(3\ 4\ 5)$ 는 $(0, 1, 1, 0, 0)$ 형의 치환이므로 σ 를 포함하는 켤레류의 크기는 $\dfrac{5!}{1!\,2^1\cdot 1!\,3^1} = 20$ 이다.

교대군 A_n, $n \geq 2$ 에서 두 우치환 σ, σ' 이 같은 형의 치환일지라도 σ, σ' 은 A_n 에서 한 켤레류에 속하지 않을 수도 있다.

정리 2 대칭군 S_n, $n \geq 2$에서 우치환 $\sigma \in A_n$에 대하여

$$\sigma' = (1\ 2) \circ \sigma \circ (1\ 2)^{-1}$$

이라 하고 $\mathscr{C}_\sigma$를 대칭군 S_n에서의 σ를 포함하는 켤레류라 하고 $\mathscr{D}_\sigma$, $\mathscr{D}_{\sigma'}$을 각각 A_n에서 σ와 σ'을 포함하는 켤레류라고 하면 다음이 성립한다.

(1) 두 우치환 σ, σ'이 A_n에서 켤레원소이면, $\mathscr{C}_\sigma = \mathscr{D}_\sigma = \mathscr{D}_{\sigma'}$이다.

(2) 두 우치환 σ, σ'이 A_n에서 켤레원소가 아니면, $\mathscr{C}_\sigma$는 $\mathscr{D}_\sigma$와 $\mathscr{D}_{\sigma'}$의 합집합으로 분할되고 이들 두 켤레류의 크기는 같다. 즉, 다음이 성립한다.

$$\mathscr{C}_\sigma = \mathscr{D}_\sigma \bigcup \mathscr{D}_{\sigma'}, \qquad |\mathscr{D}_\sigma| = |\mathscr{D}_{\sigma'}| = \frac{1}{2}|\mathscr{C}_\sigma|$$

증명 (1), (2) 대칭군 S_n에서

$$B_n = A_n \circ (1\ 2) = \{\tau \circ (1\ 2) \mid \tau \in A_n\}$$

이라고 하면, $S_n = A_n \bigcup B_n$, $A_n \cap B_n = \emptyset$이므로

$$\mathscr{C}_\sigma = \{\tau \circ \sigma \circ \tau^{-1} \mid \tau \in A_n\}$$
$$\bigcup \{(\tau \circ (1\ 2)) \circ \sigma' \circ (\tau \circ (1\ 2)^{-1} \mid \tau \in A_n\}$$

이고 또 우치환 $\tau \in A_n$에 대하여 다음이 성립한다.

$$\begin{aligned} \tau \circ (1\ 2) \circ \sigma \circ (\tau \circ (1\ 2))^{-1} &= \tau \circ ((1\ 2) \circ \sigma \circ (1\ 2)^{-1}) \circ \tau \\ &= \tau \circ \sigma' \circ \tau^{-1} \end{aligned}$$

그리고,

$$\mathscr{D}_\sigma = \{\tau \circ \sigma \circ \tau^{-1} \mid \tau \in A_n\}, \quad \mathscr{D}_{\sigma'} = \{\tau \circ \sigma' \circ \tau^{-1} \mid \tau \in A_n\}$$

이므로, σ와 σ'이 A_n에서 켤레원소이면, $\mathscr{C}_\sigma = \mathscr{D}_\sigma = \mathscr{D}_{\sigma'}$이다.

이제 σ와 σ'이 A_n에서 켤레원소가 아니라고 하자.

이 때, 위의 결과에 의하여 다음이 성립한다.

$$\mathscr{C}_\sigma = \mathscr{D}_\sigma \bigcup \mathscr{D}_{\sigma'}, \qquad \mathscr{D}_\sigma \cap \mathscr{D}_{\sigma'} = \emptyset$$

그리고,

$$B_n = A_n \circ (1\ 2) = (1\ 2) \circ A_n = \{(1\ 2) \circ \rho \mid \rho \in A_n\}$$

이므로 각 우치환 $\tau \in A_n$에 대하여 $\tau \circ (1\ 2) = (1\ 2) \circ \rho$인 우치환 $\rho \in A_n$가 존재하고 이때

$$\begin{aligned}\tau\circ\sigma'\circ\tau^{-1} &= \tau\circ(1\ 2)\circ\sigma\circ(1\ 2)^{-1}\circ\tau^{-1}\\ &= \tau\circ(1\ 2)\circ\sigma\circ(\tau\circ(1\ 2))^{-1}\\ &= (1\ 2)\circ\rho\circ\sigma\circ((1\ 2)\circ\rho)^{-1}\\ &= (1\ 2)\circ(\rho\circ\sigma\circ\rho^{-1})\circ(1\ 2)^{-1}\end{aligned}$$

이므로 $\mathscr{D}_{\sigma'}\subseteq(1\ 2)\circ\mathscr{D}_{\sigma}\circ(1\ 2)^{-1}$ 이므로 $|\mathscr{D}_{\sigma'}|\leq|\mathscr{D}_{\sigma}|$ 이고, 마찬가지로 $\sigma=(1\ 2)\circ\sigma'\circ(1\ 2)^{-1}$ 이므로

$$\tau\circ\sigma\circ\tau^{-1}=(1\ 2)\circ(\rho\circ\sigma'\circ\rho^{-1})\circ(1\ 2)^{-1}$$

이고 따라서 $\mathscr{D}_{\sigma}\subseteq(1\ 2)\circ\mathscr{D}_{\sigma'}\circ(1\ 2)^{-1}$ 이므로 $|\mathscr{D}_{\sigma}|\leq|\mathscr{D}_{\sigma'}|$ 이다.

위의 결과에 의하여 $|\mathscr{D}_{\sigma}|=|\mathscr{D}_{\sigma'}|$ 이고 또 $|\mathscr{C}_{\sigma}|=|\mathscr{D}_{\sigma}|+|\mathscr{D}_{\sigma'}|$ 이므로 $|\mathscr{D}_{\sigma}|=|\mathscr{D}_{\sigma'}|=\frac{1}{2}|\mathscr{C}_{\sigma}|$ 이다.

정리 3 대칭군 S_n, $n\geq 2$ 에서 우치환 $\sigma\in A_n$ 에 대하여

$$\sigma'=(1\ 2)\circ\sigma\circ(1\ 2)^{-1}$$

이라고 할 때, 다음이 성립한다.

(1) $C_{S_n}(\sigma)\not\subseteq A_n$ 일 때 즉 $C_{S_n}(\sigma)$ 가 기치환을 포함할 때 그리고 이때에만 $\sigma,\ \sigma'$ 은 A_n 에서 켤레원소이다.

(2) $C_{S_n}(\sigma)\subseteq A_n$ 일 때 즉 $C_{S_n}(\sigma)=A_n$ 일 때 그리고 이때에만 $\sigma,\ \sigma'$ 은 A_n 에서 켤레원소가 아니다.

증명 (1) 먼저 $C_{S_n}(\sigma)\not\subseteq A_n$ 일 때, ρ 를 $C_{S_n}(\sigma)$ 에 속하는 기치환이라고 하면 $\rho\circ\sigma\circ\rho^{-1}=\sigma$ 이므로

$$\begin{aligned}&((1\ 2)\circ\rho)\circ\sigma\circ((1\ 2)\circ\rho)^{-1}\\ &=(1\ 2)\circ(\rho\circ\sigma\circ\rho^{-1})\circ(1\ 2)\\ &=(1\ 2)\circ\sigma\circ(1\ 2)=\sigma'\end{aligned}$$

이고 또 $(1\ 2)\circ\rho\in A_n$ 이므로 A_n 에서 σ 와 σ' 는 켤레원소이다.

역으로, A_n 에서 σ 와 σ' 이 켤레원소라 하고 적당한 $\tau\in A_n$ 에 대하여

$$\tau\circ\sigma\circ\tau^{-1}=\sigma' \quad 즉 \quad \tau\circ\sigma\circ\tau^{-1}=(1\ 2)\circ\sigma\circ(1\ 2)^{-1}$$

이라고 하자. 이 때,

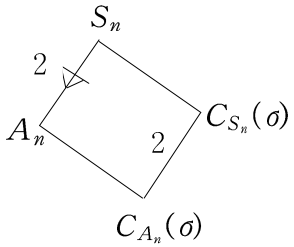
$$((1\ 2)\circ\tau)\circ\sigma=\sigma\circ((1\ 2)\circ\tau)$$

이므로 $\rho=(1\ 2)\circ\tau$ 이라고 하면, $\rho\in C_{S_n}(\sigma)$ 이고 또 ρ 는 기치환이고 따라서 $C_{S_n}(\sigma)\not\subseteq A_n$ 이다.

(2) 위의 (1) 에 의하여 $C_{S_n}(\sigma)\subseteq A_n$ 일 때 즉 $C_{S_n}(\sigma)=A_n$ 일 때 그리고 이때에만 $\sigma.\ \sigma'$ 은 A_n 에서 켤레원소가 아니다.

앞의 정리에서 $\mathscr{C}_\sigma$ 를 대칭군 S_n 에서의 σ 를 포함하는 켤레류라 하고 $\mathscr{D}_\sigma$ 를 A_n 에서 σ 를 포함하는 켤레류라고 하면,

$$A_n\lhd S_n,\quad |S_n:\ A_n|=2$$



이므로, $C_{S_n}(\sigma)\not\subseteq A_n$ 일 때

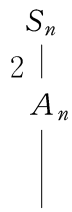
$$S_n=A_nC_{S_n}(\sigma),$$

$$C_{S_n}(\sigma)\cap A_n=C_{A_n}(\sigma)$$

이므로 다음이 성립한다.

$$|C_{S_n}(\sigma):\ C_{A_n}(\sigma)|=|S_n:\ A_n|=2,$$

$$|\mathscr{C}_\sigma|=|S_n:\ C_{S_n}(\sigma)|=|A_n:\ C_{A_n}(\sigma)|=|\mathscr{D}_\sigma|$$



$C_{A_n}(\sigma)=C_{S_n}(\sigma)$

한편, $C_{S_n}(\sigma)\subseteq A_n$ 일 때, $C_{A_n}(\sigma)=C_{S_n}(\sigma)$

이므로 다음이 성립한다.

$$|\mathscr{C}_\sigma|=|S_n:\ C_{S_n}(\sigma)|$$
$$=|S_n:\ A_n||A_n:\ C_{S_n}(\sigma)|$$
$$=2\,|A_n:\ C_{A_n}(\sigma)|=2\,|\mathscr{D}_\sigma|$$

그런데,

$$|S_n|=|\mathscr{C}_\sigma|\,|C_{S_n}(\sigma)|=|\mathscr{C}_\sigma|\,|C_{S_n}(\sigma):\ C_{A_n}(\sigma)|\,|C_{A_n}(\sigma)|,$$

$$|S_n|=2\,|A_n|=2\,|\mathscr{D}_\sigma|\,|C_{A_n}(\sigma)|$$

이므로 $|\mathscr{C}_\sigma|\,|C_{S_n}(\sigma):\ C_{A_n}(\sigma)|=2|\mathscr{D}_\sigma|$ 이다.

보기 2 대칭군 S_n, $n \geq 2$ 에서 우치환 σ가 $(m_1, m_2, \cdots, m_n)$ 형일 때,

$$m = m_1 ! 1^{m_1} m_2 ! 2^{m_2} \cdots m_n ! n^{m_n}$$

이라 하고 $\sigma' = (1\ 2) \circ \sigma \circ (1\ 2)^{-1}$ 이라고 하면 다음이 성립한다.

(1) m이 홀수일 때, 두 우치환 σ. σ' 은 A_n에서 켤레원소가 아니다.

실제로, 정리 1 에 의하여 $|\mathscr{C}_\sigma| = \frac{n!}{m}$ 이고 또

$$|S_n| = |\mathscr{C}_\sigma| \, |C_{S_n}(\sigma)|, \quad |S_n| = 2 |\mathscr{D}_\sigma| \, |C_{A_n}(\sigma)|$$

이므로 $2^a \mid n!$, $2^{a+1} \nmid n!$ 이라고 하면

$$2^a \nmid |\mathscr{C}_\sigma|, \quad 2^{a+1} \nmid |\mathscr{C}_\sigma|, \quad 2^a \nmid |\mathscr{D}_\sigma|$$

이고 따라서 $|C_{S_n}(\sigma) : C_{A_n}(\sigma)| = 1$ 즉 $C_{S_n}(\sigma) = C_{A_n}(\sigma)$ 이므로 두 우치환 σ. σ' 은 A_n에서 켤레원소가 아니다(정리 3).

여기서 m이 홀수이려면, $m_2 = m_4 = \cdots = 0$ 이어야 하고 또

$$m_1 = m_3 = \cdots = 0 \text{ 또는 } 1$$

이어야 한다.

(2) $m_2 \geq 1$ 일 때, σ. σ' 은 A_n에서 켤레원소이다.

예를 들어, $\sigma = (1\ 2) \circ \cdots \circ (l_1 \cdots l_t)$ 일 때,

$$\begin{aligned}(1\ 2) \circ \sigma \circ (1\ 2)^{-1} &= (2\ 1) \circ \cdots \circ (l_1 \cdots l_t) \\ &= (1\ 2) \circ \cdots \circ (l_1 \cdots l_t) = \sigma\end{aligned}$$

이므로 $(1\ 2) \circ \sigma = \sigma \circ (1\ 2)$ 이고 따라서 $(1\ 2) \in C_{S_n}(\sigma)$ 이고 또 $(1\ 2)$ 는 기치환이므로 σ. σ' 은 A_n에서 켤레원소이다(정리 3).

(3) $m_1, m_3, \cdots, m_{2k+1}, \cdots$ 중에서 적어도 하나가 2 이상이면, 두 우치환 σ. σ' 은 A_n에서 켤레원소이다.

예를 들어, $\sigma = (1) \circ (2) \circ \cdots \circ (l_1 \cdots l_t)$ 일 때,

$$(1\ 2) \circ \sigma \circ (1\ 2)^{-1} = \sigma \quad \text{즉} \quad (1\ 2) \circ \sigma = \sigma \circ (1\ 2)$$

이므로 $(1\ 2) \in C_{S_n}(\sigma)$ 이고 또 $(1\ 2)$ 는 기치환이므로 두 우치환 σ. σ' 은 A_n에서 켤레원소이다(정리 3). 그리고,

$$\sigma = (1\ 2\ 3) \circ (4\ 5\ 6) \circ \cdots \circ (l_1 \cdots l_t)$$

일 때, $\tau = (1\ 4) \circ (2\ 5) \circ (3\ 6)$ 이라고 하면

$$\tau \circ \sigma \circ \tau^{-1} = (4\ 5\ 6) \circ (1\ 2\ 3) \circ \cdots \circ (l_1 \cdots l_t)$$
$$= (1\ 2\ 3) \circ (4\ 5\ 6) \circ \cdots \circ (l_1 \cdots l_t) = \sigma$$

이므로 $\tau \circ \sigma = \sigma \circ \tau$ 이고 따라서 $\tau \in C_{S_n}(\sigma)$ 이고 τ 는 기치환이므로 두 우치환 σ, σ' 은 A_n 에서 켤레원소이다.

보기 3 대칭군 S_4 의 켤레류는 다음과 같다.

켤레류	형	대표 원소	개 수	위 수
$\mathscr{C}_1$	{1, 1, 1, 1}	1	1	1
$\mathscr{C}_2$	{1, 1, 2}	(1 2)	6	2
$\mathscr{C}_3$	{1, 3}	(1 2 3)	8	3
$\mathscr{C}_4$	{2, 2}	(1 2) ∘ (3 4)	3	2
$\mathscr{C}_5$	{ 4 }	(1 2 3 4)	6	4

이들 켤레류 중에서 우치환으로 이루어진 켤레류는 다음과 같다.

$\mathscr{C}_1 = \{1\}$,

$\mathscr{C}_3 = \{(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2),$
$(1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}$,

$\mathscr{C}_4 = \{(1\ 2) \circ (3\ 4), (1\ 3) \circ (2\ 4), (1\ 4) \circ (2\ 3)\}$,

(1) $\sigma = (1\ 2\ 3)$ 에 대하여 $\sigma' = (1\ 2) \circ \sigma \circ (1\ 2)^{-1}$ 이라고 하면,

$$\sigma' = (2\ 1\ 3) = (1\ 3\ 2)$$

이고 $C_{S_4}(\sigma) = \{1, \sigma, \sigma^2\} \subseteq A_4$ 이므로

$$|\mathscr{C}_\sigma| = |S_4 : C_{S_4}(\sigma)| = 8,$$
$$\mathscr{C}_\sigma = \{(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2),$$
$$(1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}$$

이고, σ 와 σ' 는 A_4 에서 켤레원소가 아니므로 $\mathscr{C}_\sigma$ 는 A_4 에서 다음 두 켤레류의 합집합으로 분할된다.

$$\mathscr{D}_\sigma = \{(1\ 2\ 3), (1\ 3\ 4), (1\ 4\ 2), (2\ 4\ 3)\},$$
$$\mathscr{D}_{\sigma'} = \{(1\ 3\ 2), (1\ 4\ 3), (1\ 2\ 4), (2\ 3\ 4)\}$$

실제로, $\sigma = (1\ 2\ 3) = (4) \circ (1\ 2\ 3)$ 는 $(1, 0, 1, 0)$ 형의 우치환이므로

$$m = m_1 ! 1^{m_1} m_3 ! 3^{m_3} = 1 ! 1^1 \cdot 1 ! 3^1 = 3$$

이고 따라서 σ와 σ' 는 A_4 에서 켤레원소가 아니고 다음이 성립한다.

$$|\mathscr{C}_\sigma| = \frac{4!}{3} = 8, \quad |\mathscr{D}_\sigma| = |\mathscr{D}_{\sigma'}| = \frac{8}{2} = 4$$

(2) $\sigma = (1\ 2) \circ (3\ 4)$ 에 대하여 $\sigma' = (1\ 2) \circ \sigma \circ (1\ 2)^{-1}$ 이라고 하면,

$$\sigma' = (2\ 1) \circ (3\ 4) = (1\ 2) \circ (3\ 4) = \sigma$$

이므로 σ, σ' 는 A_4 에서 켤레원소이다.

실제로,

$$C_{S_4}(\sigma) = \{1, (1\ 3\ 2\ 4), (1\ 2) \circ (3\ 4), (1\ 4\ 2\ 3),$$
$$(3\ 4), (1\ 3) \circ (2\ 4), (1\ 2), (1\ 4) \circ (2\ 3)\} \not\subseteq A_4$$

$$|\mathscr{C}_\sigma| = |S_4 : C_{S_4}(\sigma)| = \frac{24}{8} = 3$$

$$\mathscr{C}_\sigma = \{(1\ 2) \circ (3\ 4), (1\ 3) \circ (2\ 4), (1\ 4) \circ (2\ 3)\}$$

이고 A_4 에서 σ를 포함하는 켤레류를 $\mathscr{D}_\sigma$ 라고 하면 다음이 성립한다

$$\mathscr{D}_\sigma = \mathscr{C}_\sigma = \{(1\ 2) \circ (3\ 4), (1\ 3) \circ (2\ 4), (1\ 4) \circ (2\ 3)\}$$

여기서, $\sigma = (1\ 2) \circ (3\ 4)$ 는 $(0, 2, 0, 0)$ 형의 우치환이므로

$$m = m_2 ! 2^{m_2} = 2 ! 2^2 = 8$$

이고 따라서 $|\mathscr{C}_\sigma| = \frac{4!}{8} = 3$ 이다.

그러므로 교대군 A_4 의 켤레류는 다음과 같다.

켤레류	원 소	개 수
$\mathscr{D}_1$	1	1
$\mathscr{D}_2$	(1 2 3), (1 3 4), (1 4 2), (2 4 3)	4
$\mathscr{D}_3$	(1 3 2), (1 4 3), (1 2 4), (2 3 4)	4
$\mathscr{D}_4$	(1 2) ∘ (3 4), (1 3) ∘ (2 4), (1 4) ∘ (2 3)	3

보기 4 대칭군 S_5의 켤레류른 다음과 같다.

켤레류	형	대표 원소	개 수
$\mathscr{C}_1$	{1, 1, 1, 1, 1}	1	1
$\mathscr{C}_2$	{1, 1, 1, 2}	(1 2)	10
$\mathscr{C}_3$	{1, 1, 3}	(1 2 3)	20
$\mathscr{C}_4$	{1, 2, 2}	(1 2) ∘ (3 4)	15
$\mathscr{C}_5$	{1, 4}	(1 2 3 4)	30
$\mathscr{C}_6$	{2, 3}	(1 2) ∘ (3 4 5)	20
$\mathscr{C}_7$	{ 5 }	(1 2 3 4 5)	24

이들 켤레류 중에서 우치환으로 이루어진 켤레류는 다음과 같다.

$$\mathscr{C}_1 = \{1\},$$

$$\begin{aligned}\mathscr{C}_3 = \{&(1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,2\,5), (1\,5\,2),\\ &(1\,3\,4), (1\,4\,3), (1\,3\,5), (1\,5\,3), (1\,4\,5), (1\,5\,4),\\ &(2\,3\,4), (2\,4\,3), (2\,3\,5), (2\,5\,3), (2\,4\,5), (2\,5\,4),\\ &(3\,4\,5), (3\,5\,4)\},\end{aligned}$$

$$\begin{aligned}\mathscr{C}_4 = \{&(1\,2)\circ(3\,4), (1\,3)\circ(2\,4), (1\,4)\circ(2\,3)\},\\ &(1\,2)\circ(3\,5), (1\,3)\circ(2\,5), (1\,5)\circ(2\,3),\\ &(1\,2)\circ(4\,5), (1\,5)\circ(2\,4), (1\,4)\circ(2\,5),\\ &(1\,5)\circ(3\,4), (1\,3)\circ(4\,5), (1\,4)\circ(3\,5),\\ &(2\,5)\circ(3\,4), (3\,5)\circ(2\,4), (4\,5)\circ(2\,3)\},\end{aligned}$$

$$\mathscr{C}_7 = \{(1\,2\,3\,4\,5), \cdots, (5\,4\,3\,2\,1)\}$$

(1) $\sigma = (1\,2\,3)$ 에 대하여 $\sigma' = (1\,2)\circ\sigma\circ(1\,2)^{-1}$ 이라고 하면,

$$\sigma' = (2\,1\,3) = (1\,3\,2)$$

이고 $\sigma = (1\,2\,3) = (4)\circ(5)\circ(1\,2\,3)$ 는 $(2, 0, 1, 0, 0)$ 형의 우치환이므로

$$m = m_1!\,1^{m_1}\,m_3!\,3^{m_3} = 2!\,1^2\,1!\,3^1 = 6$$

이므로 $|\mathscr{C}_\sigma| = \dfrac{5!}{6} = 20$ 이다. 그리고,

$$(4\ 5)\circ\sigma\circ(4\ 5)^{-1}=(5)\circ(4)\circ(1\ 2\ 3)$$
$$=(4)\circ(5)\circ(1\ 2\ 3)=\sigma$$

이므로 $(4\ 5)\in C_{S_5}(\sigma)$ 이고 따라서 σ와 σ'는 A_4에서 켤레원소이고 A_4에서 σ를 포함하는 켤레류를 $\mathscr{D}_\sigma$라고 하면 다음이 성립한다.

$$\mathscr{D}_\sigma=\mathscr{C}_\sigma,\quad |\mathscr{D}_\sigma|=|\mathscr{C}_\sigma|=20$$

(2) $\sigma=(1\ 2)\circ(3\ 4)$에 대하여 $\sigma'=(1\ 2)\circ\sigma\circ(1\ 2)^{-1}$이라고 하면,

$$\sigma'=(2\ 1)\circ(3\ 4)=(1\ 2)\circ(3\ 4)=\sigma$$

이고 σ와 σ'는 A_5에서 켤레원소이므로 A_5에서 σ를 포함하는 켤레류를 $\mathscr{D}_\sigma$라고 하면 $\mathscr{D}_\sigma=\mathscr{C}_\sigma$이다.

(3) $\sigma=(1\ 2\ 3\ 4\ 5)$에 대하여 $\sigma'=(1\ 2)\circ\sigma\circ(1\ 2)^{-1}$이라고 하면,

$$\sigma'=(2\ 1\ 3\ 4\ 5)=(1\ 3\ 4\ 5\ 2)$$

이고 $\sigma=(1\ 2\ 3\ 4\ 5)$는 $(0,0,0,0,1)$형의 우치환이므로

$$m=m_5!\,5^{m_5}=1!\,5^1=5,\quad |\mathscr{C}_\sigma|=\frac{5!}{5}=24$$

이고 또 σ,σ'는 A_5에서 켤레원소가 아니다. 따라서 $\mathscr{C}_\sigma$는 A_5에서 두 켤레류 $\mathscr{D}_\sigma$, $\mathscr{D}_{\sigma'}$의 합집합으로 분할된다.

그러므로 A_5의 켤레류는 다음과 같다.

켤레류	대표 원소	개수
$\mathscr{D}_1$	1	1
$\mathscr{D}_2$	(1 2 3)	20
$\mathscr{D}_3$	(1 2)∘(3 4)	15
$\mathscr{D}_4$	(1 2 3 4 5)	12
$\mathscr{D}_5$	(1 3 4 5 2)	12