2021년 2월
교육학석사(수학교육)학위논문

# 위수 60인 비아벨 단순군의 유일성

조선대학교 교육대학원

수학교육전공

신 주 한

# 위수 60인 비아벨 단순군의 유일성

The Uniqueness of The Non-Abelian
Simple Group of Order 60

2021년 2월

조선대학교 교육대학원

수학교육전공

신 주 한

# 위수 60인 비아벨 단순군의 유일성

지도교수 김 광 섭

이 논문을 교육학석사(수학교육)학위 청구논문으로 제출함.

2020년 10월

조선대학교 교육대학원

수학교육전공

신 주 한

신주한의 교육학 석사학위 논문을 인준함.

심사위원장 조선대학교 교수 이 관 규 인

심사위원 조선대학교 교수 오 동 렬 인

심사위원 조선대학교 교수 김 광 섭 인

2020년 12월

조선대학교 교육대학원

CONTENTS

# ABSTRACT

## The Uniqueness of Non-Abelian Simple Group of Order 60

Shin Ju Han
Advisor : Prof. Kwang-Seob Kim, Ph.D.
Major in Mathematics Education
Graduate School of Education, Chosun University

In mathematics, the classification of the finite simple groups is a theorem stating that every finite simple group is either cyclic, or alternating, or it belongs to a broad infinite class called the groups of Lie type, or else it is one of twenty-six or twenty-seven exceptions, called sporadic. Group theory is central to many areas of pure and applied mathematics and the classification theorem has been called one of the great intellectual achievements of humanity. The proof consists of tens of thousands of pages in several hundred journal articles written by about 100 authors, published mostly between 1955 and 2004. Simple groups can be seen as the basic building blocks of all finite groups, reminiscent of the way the prime numbers are the basic building blocks of the natural numbers. In this article, we see the case of order 60.

# 제 1 장

# 기초 군론

## 1.1 군의 기본 정의

**정의 1.1.** 군 $\langle G, * \rangle$는 이항연산 $*$ 이 집합 $G$위에 정의되어 있고, 다음 $g_1, g_2, g_3$를 만족하는 집합 $G$이다.

$g_1$ : 집합 $G$의 임의의 원소 $a$, $b$, $c$에 대하여

$$(a * b) * c = a * (b * c)$$

를 만족하는 결합법칙 $*$ 을 가진다.

$g_2$ : 집합 $G$의 임의의 원소 $x$에 대해서

$$e * x = x * e = x$$

가 되는 $G$의 원소 $e$가 존재한다. $e$는 $*$에 대한 항등원(identity element)이다.

$g_3$ : 각각의 원소 $a \in G$에 대응하는

$$a' * a = a * a' = e$$

인 $G$ 내의 원소 $a'$가 존재한다. 여기서 $a'$는 $a$의 역원(inverse)이다.

**예제 1.1.** 양의 유리수 $\mathbb{Q}^+$위에서 $*$를 $a*b=ab/2$로 정의하자. 그러면

$$(a*b)*c=\frac{ab}{2}*c=\frac{abc}{4}$$

이며 마찬가지로

$$a*(b*c)=a*\frac{bc}{2}=\frac{abc}{4}$$

이다. 그래서 $*$는 결합법칙을 만족한다. 모든 $a\in\mathbb{Q}^+$에 대하여

$$2*a=a*2=a$$

이므로 $*$에 대한 항등원은 2 임을 알 수 있다. 마지막으로

$$a*\frac{4}{a}=\frac{4}{a}*a=2$$

이므로 $a'=4/a$는 $a$에 대한 역원이고, 연산 $*$를 가지는 $\mathbb{Q}^+$는 군이다.

**정의 1.2.** 이항연산 $*$가 군 $G$ 위에서 가환이면 군 $G$는 아벨군(가환군)이라 한다.

**정의 1.3.** 만약 $G$가 군이면 $G$에 속하는 원소의 개수를 $G$의 위수(order) $|G|$ 라고 한다.

**정의 1.4.** 만약 $G$의 이항연산이 잘 정의되어 있고 그 연산을 가지는 $H\subset G$가 군이라면 $H$를 $G$의 부분군(subgroup)이라 부른다. $H\leq G$ 혹은 $G\geq H$는 $H$가 $G$의 부분군임을 나타내고, $H<G$ 혹은 $G>H$는 $H\leq G$이지만 $H\neq G$를 의미한다.

**정의 1.5.** 만약 $G$가 군이면 $G$ 자신을 제외한 다른 모든 부분군은 진부분군(proper subgroup)이라 하고, $G$ 자신은 비진부분군(improper subgroup)이라 한다. $G$의 자명(trivial) 부분군은 부분군 $\{e\}$이고, 비자명(nontrivial) 부분군은 $\{e\}$를 제외한 다른 모든 부분군이다.

**정의 1.6.** $G$가 군이라 하고 $a \in G$이라 하자. 그러면 $G$의 부분군 $H = \{a^n | n \in \mathbb{Z}\}$는 $a$에 의하여 생성된 순환 부분군(cyclic subgroup)이라고 부른다. 그리고 $\langle a \rangle$로 적는다.

**정의 1.7.** 만약 $\langle a \rangle = G$이면 $a \in G$가 $G$를 생성한다 하고 $a$를 $G$의 생성원이라 한다. 만약 $G$를 생성하는 $a \in G$가 존재하면 $G$를 순환군(cyclic group)이라고 한다.

**정의 1.8.** 집합 $A$의 치환(permutation)은 일대일이며 위로인 함수 $\phi : A \to A$이다. 그리고 만약 $A$를 유한군 $\{1, 2, \cdots, n\}$이라 하자. $A$의 모든 치환들의 군은 $n$문자에 대한 대칭군 (symmetric group on $n$ letters)이라 하고 $S_n$으로 나타낸다.

**정의 1.9.** 치환 $\sigma$를 집합 $A$의 치환이라 하자. 치환 $\sigma$의 궤도(orbits)란 동치관계에 의해서 결정된 동치류(equivalence classes)를 말한다.

**정의 1.10.** 치환 $\sigma \in S_n$의 두개 이상의 원소를 포함하는 궤도가 단 하나만 존재할 때, $\sigma$를 순환치환(cycle)이라 한다.

**정의 1.11.** 가장 큰 궤도에 있는 원소의 개수를 순환치환의 길이라 한다. 길이가 2인 순환치환을 호환(transposition)이라 한다. 유한집합에서의 치환은 호환의 짝수 개의 곱으로 표현되는가, 홀수 개의 곱으로 표현되는가에 따라서 각각 우치환(even) 또는 기치환(odd)이라 한다.

**정의 1.12.** 집합 $X(\neq \varnothing)$위의 대칭군 $S(X)$의 부분군을 집합 $X$위의 치환군(permutation)이라고 한다.

**정의 1.13.** 자연수 $n$개의 문자에 대한 우치환으로 구성된 $S_n$의 부분군을 $n$문자에 대한 교대군 $A_n$(alternating group $A_n$ on letters)이라 한다.

**정의 1.14.** 군 $H \leq G$라 하자. $aH \subset G$이고 $aH = \{ah \mid h \in H\}$는 $a \in H$인 $H$의 좌잉여류(left coset)라 하고 $Ha = \{ha \mid h \in H\}$를 $a \in H$인 우잉여류(right coset)라 한다.

군 $H$를 $G$의 부분군이라 하자. $G$에서의 $H$의 좌잉여류의 개수를 $G$에서의 $H$의 지수(index) $(G : H)$라고 한다.

**정의 1.15.** 군 $G$에서 군 $G'$으로 가는 사상 $\phi$가 만약 모든 $a, b \in G$에 대하여 준동형 성질

$$\phi(ab) = \phi(a)\phi(b)$$

를 만족하면 $\phi$를 준동형사상이라 한다.

**정의 1.16.** 사상 $\phi$는 집합 $X$에서 집합 $Y$로의 사상이고 $A \subseteq X$와 $B \subseteq Y$라고 하자. $\phi$ 아래 $Y$에서 $A$의 상(image of $A$ in $Y$ under $\phi$) $\phi[A]$는 $\{\phi(a) \mid a \in A\}$이다. 집합 $\phi[X]$는 $\phi$의 치역(range of $\phi$)이다. $X$에서의 $B$의 역상 $\phi^{-1}[B]$(inverse image $\phi^{-1}[B]$ of $B$ in $X$)는 $\{x \in X \mid \phi(x) \in B\}$이다.

**정의 1.17.** $\phi : G \to G'$를 군 준동형사상이라고 하자. 부분군 $\phi^{-1}[\{e'\}] = \{x \in G \mid \phi(x) = e'\}$은 $\phi$의 핵(kernel of $\phi$)이라 하고 Ker($\phi$)로 나타낸다.

**정의 1.18.** 군 $G$의 부분군 $H$의 좌와 우잉여류가 일치하면, 즉 모든 $g \in G$에 대하여 $gH = Hg$이면 $H$를 정규적(normal)이라 한다. $H$는 군 $G$의 정규부분군이라고

하자. 그러면 $H$의 잉여류들은 이항연산 $(aH)(bH) = (ab)H$ 아래서 군 $G/H$를 이룬다. 군 $G/H$는 $H$에 의한 $G$의 잉여군(factor group) 또는 상군(quotient group)이라고 한다.

**정의 1.19.** 군 $G \neq \{e\}$의 정규부분군이 $G$와 $\{e\}$만 존재한다고 하면 그 군을 단순군(simple group)이라고 한다.

**정의 1.20.** 군 $G$의 극대정규부분군(maximal mormal subgroup of group) $M$은 $M \neq G$이고 $M \subsetneq N$인 $N \lhd G$이 존재하지 않는 정규부분군이다.

## 1.2 군의 작용

**정의 1.21.** 집합 $X$와 군 $G$라 하자. $X$ 위 $G$의 작용(action of $G$ on $X$)은 다음의 성실을 만족하는 사상 $* : G \times X \to X$이다.

1. 모든 $x \in X$에 대하여 $ex = x$이다.
2. 모든 $x \in X$와 모든 $g_1, g_2 \in G$에 대하여 $(g_1 g_2)(x) = g_1(g_2 x)$이다.

이런 조건 아래서 $X$는 $G$-집합($G$-Set)이라 한다.

**정의 1.22.** (번사이드 형식) 유한군 $G$를 $X$를 유한 $G$-집합이라 하자. $G$ 아래 $X$속 궤도들의 개수를 $r$이라 하면

$$r \cdot |G| = \sum_{g \in G} |X_g|$$

가 된다.

## 1.3 동형사상

여기 1.3 동형사상에서 나오는 정리들은 [1] [1, §34]를 참고하였고 증명은 생략하도록 한다.

**정리 1.1.** (제1동형사상 정리) 사상 $\phi : G \to G'$를 핵 $K$를 갖는 준동형사상이라 하고 $\gamma_K : G \to G/K$를 표준 준동형사상이라 하자. 각 $x \in G$에 대하여 $\phi(x) = \mu(\gamma_K(x))$를 만족하는 동형사상 $\mu : G/K \to \phi(G)$가 유일하게 존재한다.

만약 $H$와 $N$이 군 $G$의 부분군이면,

$$HN = \{hn | h \in H, n \in N\}$$

이라 하자. $H$와 $N$의 이음(join) $H \vee N$은 $HN$을 포함하는 $G$의 모든 부분군들의 공통집합으로 정의된다. 그래서 $HN$을 포함하는 $H \vee N$은 $G$의 가장 작은 부분군이다. 물론 $H \vee N$은 $H$와 $N$을 모두 포함하는 $G$의 가장 작은 부분군이다. 왜냐하면 $H$와 $N$을 포함하는 어떤 부분군이라도 $HN$을 포함하기 때문이다. 일반적으로 $HN$은 $G$의 부분군일 필요는 없다.

**정리 1.2.** 군 $N$이 $G$의 정규부분군이고 군 $H$가 $G$의 임의의 부분군이면 $H \vee N = HN = NH$이다. 더욱이 $H$가 또한 $G$의 정규부분군이면 $HN$은 $G$의 정규부분군이다.

**정리 1.3.** (제2동형사상 정리) 군 $H$를 $G$의 부분군이라 하고 $N$을 $G$의 정규부분군이라 하면, $(HN)/N \simeq H/(H \cap N)$이다.

**정리 1.4.** (제3동형사상 정리) $K \leq H$인 $H$와 $K$가 $G$의 정규부분군이라 하자. 그러면 $G/H \simeq (G/K)/(H/K)$이다.

# 제 2 장

# 치환군과 교대군

## 2.1 치환의 기본개념과 몇가지 정리

**정리 2.1.** 집합 A를 공집합이 아닌 집합이라 하고 $S_A$를 $A$의 모든 치환의 모임이라 하자. 그러면 $S_A$는 치환의 곱셈 아래서 군을 이룬다.

증명 . 집합 $A$의 두 치환들의 합성이 $A$의 치환임을 이미 보였으므로 $S_A$는 치환의 곱셈 아래서 닫혀있다. 함수의 합성으로 정의되어 있는 치환의 곱셈은 결합적임을 알 수 있다. 그래서 결합법칙 만족한다. 또한 모든 $a \in A$에 대해서 $\iota(a) = a$인 치환 $\iota$가 당연히 항등원 역할을 한다. 그러므로 항등원 만족한다. 마지막으로 치환 $\sigma$에 대하여 역함수 $\sigma^{-1}$는 함수 $\sigma$의 방향을 반대로 하는 치환이다. 즉 $\sigma^{-1}(a)$는 $a = \sigma(a')$인 $A$의 원소 $a'$가 된다. 그런 원소 $a'$의 단 하나 존재는 함수로서 $\sigma$가 일대일이고 동시에 위로인 사실의 결과이다. 각 $a \in A$에 대하여

$$\iota(a) = a = \sigma(a') = \sigma(\sigma^{-1}(a)) = (\sigma\sigma^{-1})(a)$$

이고 또한

$$\iota(a') = a' = \sigma^{-1}(a) = \sigma^{-1}(\sigma(a')) = (\sigma^{-1}\sigma)(a')$$

이므로 $\sigma^{-1}\sigma$와 $\sigma\sigma^{-1}$이 둘 다 치환 $\iota$가 된다. 그러므로 역원이 만족한다. □

**정리 2.2.** (Cayley 정리) 모든군은 치환군에 동형이다.

증명 . $G$를 군이라 하자. $G$가 $S_G$의 부분군에 동형임을 보이자. 모든 $x, y \in G$에 대하여 $\phi(xy) = \phi(x)\phi(y)$인 일대일 함수 $\phi : G \to S_G$를 정의만 하면 된다. 모든 $x \in G$에 대하여 $\lambda_x : G \to G$를 모든 $g \in G$에 대하여 $\lambda_x(g) = xg$로 정의하기로 하자.($\lambda_x$를 $x$를 왼쪽에서 곱하는 것으로 생각하자). 모든 $c \in G$에 대하여 등식 $\lambda_x(x^{-1}c) = x(x^{-1}c)$ =는 $\lambda_x$가 $G$에서 $G$ 위로 사상함을 보인다. 만약 $\lambda_x(a) = \lambda(b)$이면 $xa = xb$이고 소거법에 의하여 $a = b$이다. 그리고 $\lambda_x$ 또한 일대일이므로 $G$의 치환이다. 지금 모든 $x \in G$에 대하여 $\phi : G \to S_G$를 $\phi(x) = \lambda_x$로 정의하자.

$\phi$가 일대일임을 보이기 위하여 $\phi(x) = \phi(y)$라고 가정하자. 그러면 $G$에서 $G$로 사상하는 함수로서 $\lambda_x = \lambda_y$이다. 특히 $\lambda_x(e) = \lambda_y(e)$이고 그래서 $xe = ye$이고 $x = y$이다. 그래서 $\phi$는 일대일이다. $\phi(xy) = \phi(x)\phi(y)$, 즉 $\lambda_{xy}(g) = \lambda_x\lambda_y$임을 보이는 것만 남았다. 지금 모든 $g \in G$에 대하여 $\lambda_{xy}(g) = (xy)g$을 얻는다. 치환 곱셈은 함수의 합성이고 그래서 $\lambda_x\lambda_y(g) = \lambda_x(\lambda_y(g)) = \lambda_x(yg) = x(yg)$이다. 그래서 결합법칙에 의하여 $\lambda_{xy} = \lambda_x\lambda_y$이다. □

**정리 2.3.** 유한집합의 모든 치환 $\sigma$는 서로 소인 순환치환들의 곱으로 나타난다.

증명 . $B_1, B_2, \cdots, B_r$를 $\sigma$의 궤도라 하고 $\mu_i$를

$$\mu_i(x) = \begin{cases} \sigma(x) & x \in B_i\text{인 경우} \\ x & x \notin B_i\text{인 경우} \end{cases}$$

로 정의된 순환치환이라 하자. 분명히 $\sigma = \mu_1\mu_2\cdots\mu_r$이다. 서로 다른 동치류들인 동치류 궤도 $B_1, B_2, \cdots, B_r$는 서로 소 이므로 순환치환 $\mu_1\mu_2\cdots\mu_r$도 또한 서로 소이다. □

**정리 2.4.** 만약 $n \geq 2$이면 $\{1, 2, 3, \cdots, n\}$의 모든 우치환의 모임은 대칭군 $S_n$의 위수 $n!/2$인 부분군을 이룬다.

증명 . $n \geq 2$일 때 $S_n$내의 우치환의 개수는 기치환의 개수와 같음을 보이자. 즉 $S_n$은 똑같이 나누어지고 양쪽의 원소 수는 $(n!)/2$이다. 이것을 보이기 위해 $n \geq 2$일 때 $A_n$을 $S_n$ 내의 우치환의 집합이라 하고 $B_n$을 기치환의 집합이라 하자. $A_n$에서 $B_n$ 위로의 일대일 함수를 정의할 것이다. 이것이 바로 $A_n$과 $B_n$이 같은 수의 원소를 가짐을 보이는 데 필요한 것이다.

$\tau$를 $S_n$속에 고정된 호환이라 하자. $n \geq 2$이므로 그것이 존재한다. $\tau = (1, 2)$라고 가정해도 좋다. 함수

$$\lambda_\tau : A_n \to B_n$$

을 $\lambda_\tau(\sigma) = \tau\sigma$로 정의한다. 즉 $\sigma \in A_n$은 $\lambda_\tau$에 의해서 $(1, 2)\sigma$는 (1+짝수)개 또는 홀수 개의 호환들의 곱으로 나타낼 수 가 있으므로 $(1, 2)\sigma$는 실제로 $B_n$에 속한다. 만약 $A_n$의 $\sigma$와 $\mu$에 대해서 $\lambda_\tau(\sigma) = \lambda_\tau(\mu)$이 사실이면

$$(1, 2)\sigma = (1, 2)\mu$$

이고, $S_n$이 군이므로 $\sigma = \mu$를 얻는다. 그래서 $\lambda_\tau$은 일대일 함수이다. 끝으로,

$$\tau = (1, 2) = \tau^{-1}$$

이고 그래서 만약 $\rho \in B_n$이면

$$\tau^{-1}\rho \in A_n$$

이고

$$\lambda_\tau(\tau^{-1}\rho) = \tau(\tau^{-1}\rho) = \rho$$

이므로 $\lambda_\tau$는 $B_n$ 위로이다. 집합의 원소 사이에 일대일 대응관계가 존재하므로 $A_n$의 원소의 수는 $B_n$의 원소의 수와 같다. □

## 2.2 치환군과 교대군의 성질

**정리 2.5.** 교대군 $A_n$은 $S_n$의 정규부분군이다.

증명 . 교대군 $A_n$이 항등치환이라면 우치환이므로 $A_n \neq \phi$이고, $A_n$이 $S_n$의 부분집합임에는 자명하다. 그리고 임의의 $\sigma, \tau \in A_n$에 대하여 $\sigma\tau^{-1}$ =(우치환)(우치환)$^{-1}$ =(우치환)$\in A_n$이 성립한다. 따라서 $A_n$은 $S_n$의 부분군이다. 임의의 $\delta \in S_n$와 임의의 $\rho \in A_n$에 대하여

$$\delta\rho\delta^{-1} = \begin{cases} (\text{우치환})((\text{우치환})(\text{우치환})^{-1} = (\text{우치환}) \in A_n, & \delta : (\text{우치환}) \\ (\text{기치환})((\text{우치환})(\text{기치환})^{-1} = (\text{우치환}) \in A_n, & \delta : (\text{기치환}) \end{cases}$$

이 성립힌다. 따라서 $A_n$은 $S_n$의 정규부분군이다.

□

**정리 2.6.** 교대군 $A_n$은 $n \geq 5$에 대하여 단순군이다.

증명 . (a) $n \geq 3$이면 $A_n$은 모든 3-순환치환을 포함한다.

3-순환치환중 임의의 원소 $(a, b, c) = (a, c)(a, b)$로 쓸 수 있으므로 모든 3-순환치환이 짝수 호환을 가지며 따라서 $A_n$에 포함된다.

(b) $n \geq 3$에 대하여 $A_n$은 3-순환치환에 의하여 생성됨을 보여라.

집합$A_n$의 원소 $\sigma$를 호환들의 곱으로 쓴다. 곱해진 호환들의 수는 $A_n$의 정의로부터 짝수이다. 처음 두 호환의 곱은 $(a, b)(c, d)$ 형식 또는 $(a, b)(a, c)$ 형식 또는 $(a, b)(a, b)$ 형식 중 하나이다. 만약 형태가 $(a, b)(a, b)$인 경우에는 곱을 합쳐서 삭제시킬수 있다. 그리고 $(a, b)(c, d)$=$(a, c, b)(a, c, d)$이고 앞에서 보인 $(a, c)(a, b)$=$(a, b, c)$이다. 다음 두 호환에서도 진행하여 3-순환치환의 곱으로 표현할 때까지 계속한다. 따라서 3-순환치환은 $A_n$을 생성한다.

(c) $n \geq 3$일 때 $r$과 $s$를 $\{1, 2, \cdots, n\}$의 고정된 원소라 하자. $1 \leq i \leq n$에 대하

여 $A_n$은 $n$개의 "특별한" 3-순환치환 $(r,s,i)$의 꼴에 의해 생성되는 것을 보이자.

고정된 원소 $r$과 $s$를 포함한 형태인

$$(r,s,i)^2 = (r,i,s)$$

$$(r,s,j)(r,s,i)^2 = (r,s,j)(r,i,s) = (r,i,j)$$

$$(r,s,j)^2(r,s,i) = (r,j,s)(r,s,i) = (s,i,j)$$

$$(r,s,i)^2(r,s,k)(r,s,j)^2(r,s,i) = (r,i,s)(r,s,k)(s,i,j) = (i,j,k)$$

이제 모든 3-순환치환은 $r$과 $s$를 포함하지 않고 $(i,j,k)$ 형태이거나 $r$이나 $s$중 하나만 포함한 $(r,i,j)$ 또는 $(s,i,j)$ 형태이거나 또는 $r$과 $s$가 모두 포함된 $(r,s,i)$ 혹은 $(r,i,s) = (s,r,i)$ 형태이다. 이 모든 형태는 특별한 3-순환치환에서 얻을수 있으며 특별한 3-순환치환이 $A_n$을 생성한다는 것을 알 수 있다.

(d) $n \geq 3$에 대하여 $N$을 $A_n$의 정규부분군이라 하자. $N$이 하나의 3-순환치환을 포함한다면 $N = A_n$이다.

원소 $(r,s,i) \in N$는 $j = 1,2,\cdot,n$에 대하여

$$((r,s)(i,j))(r,s,i)^2((r,s)(i,j))^{-1}$$

을 계산하여 $(r,s,j) \in N$을 얻게 함을 보이자. 먼저 $((r,s)(i,j))(r,s,i)^2((r,s)(i,j))^{-1}$를 정리하여 $(r,s)(i,j)(r,i,s)(i,j)(r,s)$=$(r,s,j)$를 얻는다. 따라서 $N$이 $A_n$의 정규부분군이고 3-순환치환을 포함하는 경우와 $r$과 $s$는 1에서 $n$까지의 두 숫자가 될 수 있으므로 $(r,s,i)$로 간주 할 수 있다. $N$은 모든 특별한 3-순환치환을 포함해야하므로 모두 $A_n$이 된다.

(e) $n \geq 5$에 대하여 $N$을 $A_n$의 비자명 정규부분군이라 하자. 다음 중 한가지가 성립해야 되며 각각의 경우에 $N = A_n$임을 보여라.

1) $N$은 3-순환치환을 포함한다.

앞에 $(d)$에 의해 $N$에 3-순환치환이 포함되어 있으면 $N = A_n$이 성립한다.

2) $N$은 3보다 큰 길이를 가진 서로소인 순환치환의 곱이 적어도 하나는 존재한다.

$a_1, a_2, \cdots, a_r$은 곱에 분리된 순환치환이 포함되어 있기때문에 $\mu$로 표시되지 않는다. 우리는

$$\begin{aligned}&\sigma^{-1}[(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}]\\&= (a_r, \cdots, a_2, a_1)\mu^{-1}(a_1, a_2, a_3)\mu(a_1, a_2, \cdots, a_r)(a_1, a_3, a_2)\\&= (a_1, a_3, a_r)\end{aligned}$$

를 가지고 있으며 이 원소는 $\sigma^{-1}$의 곱이고 $A_n$의 원소에 의한 $\sigma$의 켤레이기 때문에 $N$에 있다. 따라서 이 경우 $N$은 3-순환치환을 포함하고 (d)에 의해 $A_n$과 같다.

3) $N$은 $\sigma = \mu(a_4, a_5, a_6)(a_1, a_2, a_3)$꼴의 서로소인 곱을 포함한다.

$a_1, a_2, \cdots, a_6$은 $\mu$로 표시되지 않는다. 2)에서와 같이

$$\begin{aligned}&\sigma^{-1}[(a_1, a_2, a_4)\sigma(a_1, a_2, a_4)^{-1}]\\&= (a_1, a_3, a_2)(a_4, a_6, a_5)\mu^{-1}(a_1, a_2, a_4)\mu(a_4, a_5, a_6)(a_1, a_2, a_3)(a_1, a_4, a_2)\\&= (a_1, a_4, a_2, a_6, a_3)\end{aligned}$$

는 $N$에 있다. 따라서 $N$은 3보다 큰 길이의 순환치환을 포함하고 2)에 의해 $N = A_n$이다.

4) $N$은 $\sigma = \mu(a_1, a_2, a_3)$의 꼴의 서로소인 곱을 포함한다. 단, $\mu$는 서로소인 호환의 곱이다.

$a_1, a_2, a_3$은 $\mu$로 표시되지 않는다. 물론 $\sigma^2 \in N$이다. $\sigma \in N$이므로 $\sigma^2 = \mu(a_1, a_2, a_3)\mu(a_1, a_2, a_3) = (a_1, a_3, a_2) \in N$이다. 그래서 $N$은 3-순환치환을 포함하므로 (d)에 의해서 $N = A_n$이다

5) $N$은 $\sigma = \mu(a_3, a_4)(a_1, a_2)$꼴의 서로소인 곱을 포함한다. 단, $\mu$는 짝수개의

서로소인 호환의 곱이다.

$a_1, a_2, a_3, a_4$는 $\mu$로 표시되지 않는다. 2)에서와 같이

$$\begin{aligned}&\sigma^{-1}[(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}]\\&= (a_1, a_2)(a_3, a_4)\mu^{-1}(a_1, a_2, a_3)\mu(a_3, a_4)(a_1, a_2)(a_1, a_3, a_2)\\&= (a_1, a_3)(a_2, a_4)\end{aligned}$$

는 $N$에 있다. 그리고 $\alpha = (a_1, a_3)(a_2, a_4)$ $\beta = (a_1, a_3, i)$라 하자. 여기서 $i$는 $a_1, a_2, a_3, a_4$와 다르다. 그 다음 $\beta \in A_n$ 과 $\alpha \in N$ 과 $N$의 정규부분군은 $(\beta^{-1}\alpha\beta)\alpha \in N$을 의미한다. 계산하면

$$(\beta^{-1}\alpha\beta)\alpha = (a_1, i, a_3)(a_1, a_3)(a_2, a_4)(a_1, a_3, i)(a_1, a_3)(a_2, a_4) = (a_1, a_3, i)$$

따라서 이 경우에도 (d)에 의해 $N = A_n$이다. □

위와 같이 1장에서 군에 대한 기본적인 정의 및 정리, 2장에서 치환군과 교대군에 대한 정의 및 정리 그리고 교대군 $A_n$에 대한 $n \geq 5$일 때 단순군임을 보였다.

이제 우리가 보이고자 하는 위수 60에 대한 비아벨 단순군의 유일성을 실로우 정리를 기초로 하여 보일것이다. 3장에서는 증명에 필요한 실로우 정리와 정의를 간단하게 다룰것이고 4장에서 구체적으로 실로우정리를 이용하여 위수 60인 비아벨 단순군의 유일성을 보일것이다.

먼저 위수가 60인 비아벨 단순군 $G$의 실로우 5 부분군의 개수가 6개임을 실로우정리를 통해 보이고 군의 작용을 이용해서 $G$에서 치환군 $S_6$으로 가는 준동형 사상을 생각하여 $G$가 $S_6$로 포함됨을 보인다. 그리고 $S_6$에 포함될 때 $A_6$에도 포함되고 마지막으로 $G$와 $A_5$와 동형이 됨을 보이고 증명을 마무리 짓는다.

# 제 3 장

# Sylow 정리

## 3.1 Sylow 정리 소개

**정리 3.1.** 집합 $X$를 $G$-집합이라 하고 $x \in X$하자. 그러면 $|Gx| = (G : G_x)$이다. 만약 $|G|$가 유한이면 $|Gx|$는 $|G|$의 약수이다.

증명 . $Gx$부터 $G$에서 $G_x$의 좌잉여류들의 모임 위로 대응하는 일대일 사상 $\psi$를 정의하자. $x_1 \in Gx$라 하자. 그러면 $g_1 x = x_1$을 만족하는 $g_1 \in G$가 존재한다. $\psi(x_1)$을 $G_x$의 좌잉여류 $g_1 G_x$로 정의한다. $\psi$가 $g_1 x = x_1$을 만족하는 $g_1 \in G$의 선택과 관계없이 잘 정의됨을 보여야 한다. 또한 $g_1' x = x_1$이라 가정하자. 그러면 $g_1 x = g_1' x$이며 그래서 $g_1^{-1}(g_1 x) = g_1^{-1}(g_1' x)$이고 이로부터 $x = (g_1^{-1} g_1')x$를 얻는다. 그러므로 $g_1^{-1} g_1' \in G_x$이다. 그래서 $g_1' \in g_1 G_x$이며 $g_1 G_x = g_1' G_x$가 된다. 그러므로 사상 $\psi$는 잘 정의되었다.

사상 $\psi$가 일대일임을 보이기 위하여 $x_1, x_2 \in G_x$이고 $\psi(x_1) = \psi(x_2)$라 가정하자. 그러면 $x_1 = g_1 x, x_2 = g_2 x$이며 $g_2 \in g_1 G_x$를 만족하는 $g_1, g_2 \in G$가 존재한다. 그러면 적당한 $g \in G_x$에 대하여 $g_2 = g_1 g$이므로 $x_2 = g_2 x = g_1(gx) = g_1 x = x_1$이

다. 그러므로 $\psi$는 일대일이다.

마지막으로 $G$에서 $G_x$의 각 좌잉여류는 적당한 $x_1 \in Gx$에 대하여 $\psi(x_1)$의 꼴임을 보이면 된다. $g_1G_x$를 좌잉여류라 하자. 그러면 만약 $g_1x = x_1$이면 $g_1G_x = \psi(x_1)$이다. 그래서 $\psi$는 위로이다. 그러므로 $\psi$는 $Gx$에서 좌잉여류들의 모임 위로 일대일 대응한다. 그래서 $|Gx| = (G : G_x)$이다.

만약 $|G|$가 유한이면 등식 $|G| = |G_x|(G : G_x)$는 $|Gx| = (G : G_x)$가 $|G|$의 약수임을 보인다. □

**정리 3.2.** $G$를 위수가 $p^n$인 군이고 $X$를 유한 $G$-집합이라 할 때, $|X| \equiv |X_G| \pmod{p}$ 이다.

증명 . 식$|X| = |X_G| + \sum_{i=s+1}^{r} |Gx_i|$의 기호로 정리 3.1에 의하여 $|Gx_i|$ 는 $|G|$를 나눔을 안다. 결과적으로는 $p$는 $s+1 \le i \le r$에 대하여 $|Gx_i|$를 나눈다. 그러면 위에 식은 $|X| - |X_G|$가 $p$로 나누어 짐을 보인다. 그래서 $|X| \equiv |X_G| \pmod{p}$이다. □

**정의 3.1.** $p$를 소수라 하자. $G$의 모든 원소가 $p$의 멱을 위수로 가지면 $G$를 $p$군($p$-group)이라 한다. 군 $G$의 부분군은 그 자신이 $p$군이면 $G$의 $p$부분군($p$-subgroup)이라 한다.

**정리 3.3.** (Cauchy 정리) $G$가 유한군이고 $p$를 소수라 하자. $p$가 $|G|$를 나누면 $G$는 위수 $p$인 원소를 가진다. 즉, 위수 $p$인 부분군을 가진다.

증명 . $X$를 $G$에서 좌표들의 곱이 $e$가 되는 $G$의 모든 $p$-순서쌍 $(g_1,g_2,\cdots,g_p)$들의 집합이라 하자. 즉

$$X = \{(g_1, g_2, \cdots, g_p) \mid g_i \in G \text{ 그리고 } g_1g_2\cdots g_p = e\}$$

이다. $p$가 $|X|$을 나눈다는 것을 증명하자. $X$에 속하는 $p$-순서쌍을 구성하는 데 있어서 $g_1, g_2, \cdots, g_{p-1}$은 $G$의 임의의 원소들이며 $g_p$는 $(g_1 g_2 \cdots g_{p-1})^{-1}$로서 유일하게 결정된다고 할 수 있다. 그래서 $|X| = |G|^{p-1}$이며 $p$가 $|G|$를 나누므로 $p$는 $|X|$를 나눈다.

$\sigma$를 $S_p$에 속하는 순환치환 $(1, 2, 3, \cdots, p)$라 하자. $\sigma$를 $X$위에서

$$\sigma(g_1, g_2, \cdots, g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, \cdots, g_{\sigma(p)}) = (g_2, g_3, \cdots, g_p, g_1)$$

으로 작용한다고 하자. $g_1(g_2 g_3 \cdots g_p) = e$에서 $g_1 = (g_2, g_3, \cdots, g_p, g_1)^{-1}$이고 $(g_2 g_3 \cdots g_p) g_1 = e$이기 때문에 $(g_2, g_3, \cdots, g_p, g_1) \in X$이다. 그래서 $\sigma$는 $X$ 위에 작용하고 자연스럽게 $S_p$의 부분군 $\langle\sigma\rangle$가 반복에 의하여 $X$위에 작용한다고 간주할 수 있다.

이제 $|\langle\sigma\rangle| = p$이므로 정리 3.2를 적용하여 $|X| \equiv |X_{\langle\sigma\rangle}| \pmod{p}$가 된다. $p$가 $|X|$를 나누므로 $p$는 또한 $|X_{\langle\sigma\rangle}|$를 나누어야 한다. 이제 $X_{\langle\sigma\rangle}$를 조사해 보자. $(g_1, g_2, \cdots, g_p)$는 $g_1 = g_2 = \cdots = g_p$인 경우에 $\sigma$에 의해서 고정되므로 $\langle\sigma\rangle$에 의해 고정될 필요충분조건은 $g_1 = g_2 = \cdots = g_p$이다. $X_{\langle\sigma\rangle}$속에 적어도 한 원소, 즉 $(e, e, \cdots, e)$는 속함을 안다. $p$가 $|X_{\langle\sigma\rangle}|$를 나누므로 $X_{\langle\sigma\rangle}$속에는 적어도 $p$개는 존재해야 한다. 그러므로 $(a, a, \cdots, a) \in X_{\langle\sigma\rangle}$인 $a \in G, a \neq e$가 원소이므로 $a$는 위수 $p$를 갖는다. 물론 $\langle a\rangle$는 위수 $p$인 $G$의 부분군이다. □

**정의 3.2.** 부분군 $G_H$는 $G$에서 $H$의 정규화군(normalizer)이라 하고 지금부터 $N[H]$로 표현할 것이다.

**정리 3.4.** (제1 Sylow 정리) $G$가 유한군이고 $|G| = p^n m$이라 하자. 여기서 $n \geq 1$이며 $p$는 $m$을 나누지 않는다. 그러면

1. $G$는 $1 \leq i \leq n$에 대하여 위수 $p^i$인 부분군을 포함한다.
2. 위수 $p^i$인 $G$의 모든 부분군 $H$는 $1 \leq i < n$에 대하여 위수 $p^{i+1}$인 부분군의 정규부분군이다.

증명 . 1. Cauchy 정리 3.3에 의하여 $G$가 위수 $p$인 부분군을 포함함을 알고 있다. 귀납법을 이용하여 $i < n$에 대하여 위수 $p^i$인 부분군의 존재는 위수 $p^{i+1}$인 부분군의 존재를 유도함을 보인다. $H$를 위수 $p^i$인 부분군이라 하자. $i < n$이므로 $p$는 $(G : H)$를 나눈다. H를 유한군 $G$의 $p$부분군이라 하면 $(N[H] : H) \equiv (G : H) \pmod{p}$에 의하여 $p$는 $(N[H] : H)$를 나눈다. $H$가 $N[H]$의 정규부분군이므로 $N[H]/H$를 만들 수 있고, $p$가 $|N[H]/H|$를 나눔을 알 수 있다. Cauchy 정리에 의하여 잉여군 $N[H]/H$는 위수 $p$인 부분군 $K$를 갖는다. 만약 $\gamma : N[H] \to N[H]/H$가 표준 준동형사상이면 $\gamma^{-1}(K) = \{x \in N[H] \mid \gamma(x) \in K\}$는 $N[H]$의 부분군이고, 그러므로 $G$의 부분군이다. 이 부분군은 $H$를 포함하며 위수가 $p^{i+1}$이다.

2. 위의 1에서 구성을 반복하고 $|\gamma^{-1}(K)| = p^{i+1}$인 $H < \gamma^{-1}(K) \leq N[H]$임을 주목하라. $H$는 $N[H]$의 정규부분군이므로 $H$는 $N[H]$보다 물론 더 작은 군 $\gamma^{-1}(K)$의 정규부분군일 것이다. □

**정의 3.3.** 군 $G$의 Sylow $p$부분군($p$-subgroup) $P$는 $G$의 극대$p$부분군, 즉 더 큰 $p$부분군에 포함되지 않는 $p$부분군이다.

**정리 3.5.** (제2 Sylow 정리) $P_1, P_2$를 유한군 $G$의 Slyow $p$부분군이라 하자. 그러면 $P_1$과 $P_2$는 $G$의 공액 부분군이다.

증명 . 여기서 부분군 중 하나를 다른 것의 좌잉여류 위에 작용하게 하고 정리 3.2을 이용할 것이다. $\mathcal{L}$을 $P_1$의 좌잉여류의 집합이라 하고 $P_2$를 $y \in P_2$에 대하여 $y(xP_1) = (yx)P_1$에 의해 $\mathcal{L}$ 위에 작용시키자. 그러면 $\mathcal{L}$은 $P_2$-집합이다. 정리 3.2에 의하여 $|\mathcal{L}_{P_2}| \equiv |\mathcal{L}| \pmod{p}$이며 $|\mathcal{L}| = (G : P_1)$은 $p$로 나누어 지지 않으므로 $|\mathcal{L}_{P_2}| \neq 0$이다. $xP_1 \in \mathcal{L}_{P_2}$라 하자. 그러면 모든 $y \in P_2$에 대하여 $yxP_1 = xP_1$이므로 모든 $y \in P_2$에 대하여 $x^{-1}yxP_1 = P_1$이 된다. 그래서 모든 $y \in P_2$에 대해

$x^{-1}yx \in P_1$이며 $x^{-1}P_2x \leq P_1$이 된다. $|P_1| = |P_2|$이므로 $P_1 = x^{-1}P_2x$이어야만 하므로 $P_1$과 $P_2$는 실제로 공액 부분군이다. □

**정리 3.6.** (제3 Sylow 정리) $G$가 유한군이고 $p$가 $|G|$를 나눈다면 Sylow $p$부분군의 개수는 $p$를 법으로 1과 합동이며 $|G|$를 나눈다.

증명 . $P$를 $G$의 하나의 Sylow $p$부분군이라 하자. $\mathcal{J}$를 모든 Sylow $p$부분군의 모임이라 하고 $P$를 공액에 의해 $\mathcal{J}$ 위에 작용시키면 $x \in P$는 $T \in \mathcal{J}$를 $xTx^{-1}$로 대응시킨다. 정리 3.2에 의해 $|\mathcal{J}| \equiv |\mathcal{J}_P| \pmod{p}$이다. 이제 $\mathcal{J}_P$을 구해보자. 만약 $T \in \mathcal{J}_P$이면 모든 $x \in P$에 대하여 $xTx^{-1} = T$이다. 그래서 $P \leq N[T]$이다. 물론 $T \leq N[T]$이다. $P$와 $T$는 둘 다 $G$의 Sylow $p$부분군이므로 이들은 또한 $N[T]$의 Sylow $p$부분군이다. 그러면 정리 3.5에 의해 이들은 $N[T]$에서 공액이다. $T$가 $N[T]$의 정규부분군이므로, $T$는 $N[T]$에 속하는 유일한 공액이다. 그래서 $T$는 $P$이다. 그러면 $\mathcal{J}_P = \{P\}$가 된다. $|\mathcal{J}| \equiv |\mathcal{J}_P| = 1 \pmod{p}$이므로, Sylow $p$부분군의 개수는 $p$를 법으로 1과 항등이다.

이제 $G$를 공액에 의해 $\mathcal{J}$ 속에 단 하나의 궤도가 있다. 만약 $P \in \mathcal{J}$이면 정리 3.1에 의하여 $|\mathcal{J}| = |P$의 궤도$| = (G : G_P)$를 얻는다(사실 $G_P$는 $P$의 정규화이다). 그러나 $(G : G_P)$는 $|G|$의 약수이므로 Sylow $p$부분군의 개수는 $|G|$를 나눈다. □

**예제 3.1.** 위수가 15인 단순군이 존재하지 않음을 Sylow 정리를 이용하여 증명해 보자. $G$가 위수 15를 갖는다고 하자. $G$는 위수가 5인 정규부분군을 가짐을 주장한다. 정리 3.4에 의하여 $G$는 위수가 5인 부분군을 적어도 하나 가지며 정리 3.6에 의하여 이런 부분군의 개수는 5를 법으로 1과 합동이며 15의 약수가 된다. 1, 6, 11이 5를 법으로 1과 합동인 15보다 작은 모든 양 정수이고 이들 중에서 1만이 15를 나눌 수 있기 때문에 $G$는 위수가 5인 단 하나의 부분군 $P$를 갖는다. 그러나 각 $g \in G$에 대하여 $i_g(x) = gxg^{-1}$일 때 $G$의 내부자기동형사상 $i_g$는

$P$를 다시 위수가 5인 부분군 $gPg^{-1}$로 대응시킨다. 그러므로 모든 $g \in G$에 대하여 $gPg^{-1} = P$이므로 $P$는 $G$의 정규부분군이다. 그러므로 $G$는 단순군이 아니다.

## 3.2 실로우정리 응용

**정의 3.4.** 만약 군 $G$가 모든 잉여군 $H_{i+1}/H_i$가 가환이 되는 조성열 $\{H_i\}$를 갖는다면 $G$는 가해(solvable)하다라고 한다. 즉, 가해군에서는 모든 조성열 $\{H_i\}$가 가환인 잉여군 $H_{i+1}/H_i$를 가짐을 알 수 있다.

**정리 3.7.** 소수의 멱을 위수로 갖는 모든 군(즉 모든 유한$p$군)은 가해군이다.

증명 . 군 $G$가 위수 $p^r$을 갖는다면 정리 3.4로부터 $G$는 $1 \leq i < r$에 대하여 위수 $p^{i+1}$인 부분군 $H_{i+1}$속에 위수가 $p^i$인 정규부분군 $H_i$를 가짐을 즉시 알 수 있다. 그러면

$$\{e\} = H_0 < H_1 < H_2 < \cdots < H_r = G$$

는 조성열이다. 여기서 각 잉여군은 위수 $p$를 가지며 그러므로 가환이고 실제로 순환적이다. 그래서 $G$는 가해군이다. □

$X$를 $G$는 유한군인 유한 $G-$집합이라 하자. 그러면 식$|X| = |X_G| + \sum_{i=s+1}^{r} |Gx_i|$는 $x_i$가 $X$ 속의 $i$번째 궤도에 속하는 원소이면

$$|X| = |X_G| + \sum_{i=s+1}^{r} |Gx_i|$$

임을 보여준다. 이제 식 $|X| = |X_G| + \sum_{i=s+1}^{r} |Gx_i|$의 $X = G$이고 $G$ 위에서의 $G$의 작용이 공액인 특별한 경우를 생각해 보자. 그래서 $g \in G$는 $x \in X = G$를 $gxg^{-1}$에 대응시킨다. 그러면

$$X_G = \{x \in G \mid \text{모든 } g \in G\text{에 대하여 } gxg^{-1} = x\}$$

$$= \{x \in G \mid \text{모든 } g \in G\text{에 대하여 } gx = xg\} = Z(G)$$

는 $G$의 중심이 된다. 만약 식 $|X| = |X_G| + \sum_{i=s+1}^{r} |Gx_i|$에서 $c = |Z(G)|$이고 $n_i = |G_{x_i}|$라 하면

$$|G| = c + n_{c+1} + \cdots + n_r$$

을 얻는다. 여기서 $n_i$는 자기 자신에 의한 공액 아래서 $G$의 $i$번째 궤도에 속하는 원소의 개수이다. 식 $|X| = |X_G| + \sum_{i=s+1}^{r} |Gx_i|$에서 $|Gx_i|$는 $|G|$의 약수인 $|Gx_i| = (G : G_{x_i})$이므로 $c+1 \le i \le r$에 대하여 $n_i$는 $|G|$를 나눈다.

**정의 3.5.** 식 $|G| = c + n_{c+1} + \cdots + n_r$를 $G$의 류등식(class equation)이라 하고 $G$에 의한 공액 아래서 $G$ 속의 각 궤도를 $G$ 속의 공액류(conjugate class)라고 한다.

**정리 3.8.** 유한 비자명 $p$군 $G$의 중심은 비자명이다.

증명 . 군 $G$에 대한 식 $|G| = c+n_{c+1}+\cdots+n_r$에서 $c+1 \le i \le r$에 대하여 각 $n_i$는 $|G|$를 나눈다. 그래서 $p$는 각 $n_i$를 나누고 $p$는 $|G|$를 나눈다. 그러므로 $p$는 $c$를 나눈다. 이제 $e \in Z(G)$이므로 $c \ge 1$이다. 그러므로 $c \ge p$이며 $a \ne e$인 $a \in Z(G)$가 존재한다. □

**정리 3.9.** $G$가 $H \cap K = \{e\}$이고 $H \vee K = G$를 만족하는 정규부분군 $H$와 $K$를 포함하는 군이라하자. 그러면 $G$는 $H \times K$와 동형이다.

증명 . $k \in K$와 $h \in H$에 대하여 $hk = kh$임을 보이면서 증명을 시작한다. 교환자 $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$를 생각하라. $H$와 $K$가 $G$의 정규부분군이므로 괄호 안의 두 묶음은 각각 $K$와 $H$에 속하므로 $hkh^{-1}k^{-1}$은 $K$와 $H$ 둘 모두에 속한다. $K \cap H = \{e\}$이므로 $hkh^{-1}k^{-1} = e$, 즉 $hk = kh$이다.

$\phi : H \times K \to G$를 $\phi(h,k) = hk$로 정의하자. 그러면

$$\phi((h,k)(h',k')) = \phi((hh', kk') = hh'kk'$$
$$= hkh'k' = \phi(h,k)\phi(h',k')$$

이다. 그래서 $\phi$는 준동형사상이다. 만약 $\phi(h,k) = e$이다. 그리고 $h = k^{-1}$이므로 $h$와 $k$가 둘 다 $H \cap K$에 속한다. 그래서 $h = k = e$이다. 그러므로 $\mathrm{Ker}(\phi) = \{(e,e)\}$이고, $\phi$는 일대일이다. 정리 1.2에 의하여 $HK = H \vee K$이고 가정에 의하여 $H \vee K = G$이다. 그래서 $\phi$는 $G$ 위로이다. 그러므로 $H \times K \simeq G$가 된다. □

**정리 3.10.** 소수 $p$에 대하여 위수가 $p^2$인 모든 군 $G$는 가환이다.

증명 . 군 $G$가 순환군이 아니면 $e$를 제외한 모든 원소는 위수 $p$를 가져야만 한다. $a$를 그런 원소라 하자. 그러면 위수 $p$인 순환 부분군 $\langle a\rangle$는 $G$의 전체는 아니다. 또한 $b \notin \langle a\rangle$인 $b \in G$라 하자. 만약 $c \neq e$인 $\langle a\rangle \cap \langle b\rangle$에 속하는 원소 $c$가 $\langle a\rangle$와 $\langle b\rangle$를 생성하게 되므로 $\langle a\rangle = \langle b\rangle$이므로 $b \notin \langle a\rangle$에 모순이 된다. 그러므로 $\langle a\rangle \cap \langle b\rangle = \{e\}$이다. 정리 3.4에 의하여 $\langle a\rangle$는 위수 $p^2$인 $G$의 어떤 부분군 속에서 정규부분군이다. 즉 $G$에서 정규부분군이다. 마찬가지로 $\langle b\rangle$도 $G$에서 정규적이다. 이제 $\langle a\rangle \vee \langle b\rangle$는 $\langle a\rangle$를 진부분집합으로 포함하며 $p^2$을 나누는 위수를 가진 $G$의 부분군이다. 그러므로 $\langle a\rangle \vee \langle b\rangle$는 $G$ 전체이어야 한다. 그래서 정리 3.9에 의해 가정이 만족되므로 $G$는 $\langle a\rangle \times \langle b\rangle$와 동형이다. 그러므로 가환군이다. □

**정리 3.11.** $p$와 $q$가 $p < q$인 서로 다른 소수이면 위수 $pq$인 모든 군 $G$는 위수 $q$인 부분군을 단 하나 가지고 이 부분군은 $G$에서 정규부분군이다 그러므로 $G$는 단순군이 아니다. 만약 $q$가 $p$를 법으로 1과 합동이 아니면 $G$는 가환이며 순환군이다.

증명 . 정리 3.4과 정리 3.6은 $G$는 Sylow $q$부분군을 가지며 이 부분군의 개수는 $q$를 법으로 1과 합동이며 $pq$의 약수임을 보여준다. 그러므로 부분군의 개수는 $p$를 나누어야 한다. $p < q$이므로 유일한 가능성은 1이다. 그래서 $G$에는 단 하나의

Sylow $q$부분군 $Q$가 존재한다. 내부자기동형사상 아래서 $Q$는 위수가 같은 군, 즉 자신으로 대응하기 때문에 $Q$는 $G$에서 정규적이다. 그래서 $G$는 단순군이 아니다. 마찬가지로 $G$의 Sylow $p$부분군 $P$가 존재하여 이들의 개수는 $pq$를 나누고 $p$를 법으로 1과 합동이다. 그레서 이 개수는 1 또는 $q$이어야 한다. 만약 $q$가 $p$를 법으로 1과 합동이 아니면 그 개수는 1이어야 하고 $P$가 $G$에서 정규적이다. $q \not\equiv 1 \pmod{p}$이라 가정하자. $e$이외의 $Q$의 모든 원소는 위수가 $q$이고 $e$이외의 $P$의 모든 원소는 위수가 $p$이므로, $Q \cap P = \{e\}$를 얻는다. 또한 $Q \vee P$는 $Q$을 완전허게 포함하는 $G$의 부분군이며 위수가 $pq$를 나눈다. 그러므로 $Q \vee P = G$이며 정리 3.9에 의하여 $Q \vee P$는 $Q \times P$와 동형이므로 $\mathbb{Z}_q \times \mathbb{Z}_p$와 동형이다. 그래서 $G$는 가환이며 순환적이다. □

**정리 3.12.** 군 $H$와$K$가 군 $G$의 유한부분군이면

$$|HK| = \frac{(|H|)(|K|)}{|H \cap K|}$$

이다.

증명 . $HK = \{hk \mid h \in H, k \in K\}$임을 상기하라. $|H| = r, |K| = s$ 그리고 $|H \cap K| = t$라 하자. 이제 $HK$는 많아야 $rk$개의 원소를 갖는다. 그러나 $h_1, h_2 \in H$와 $k_1, k_2 \in K$에 대하여 $h_1k_1$이 $h_2k_2$와 같아질 가능성이 있다. 즉 약간의 원소가 없어질 수도 있다. $h_1k_1 = h_2k_2$이면

$$x = (h_2)^{-1}h_1 = k_2(k_1)^{-1}$$

라 하자. $x = (h_2)^{-1}h_1$은 $x \in H$임을 보이고, $x = k_2(k_1)^{-1}$은 $x \in K$임을 보인다. 그러므로 $x \in (H \cap K)$이고

$$h_2 = h_1x^{-1} \qquad \text{이며} \qquad k_2 = xk_1$$

이 된다. 한편 $y \in (H \cap K)$에 대하여 $h_3 = h_1y^{-1}, k_3 = yk_1$이라 두면 분명히 $h_3 \in H$와 $k_3 \in K$이면서 $h_3k_3 = h_1k_1$이다. 그래서 각 원소 $hk \in HK$는 $h_i \in H$와

$k_i \in K$에 대하여 $H \cap K$에 원소의 개수만큼, 즉 $t$번만큼 $h_i k_i$의 형태로 나타낼 수 있다. 그러므로 $HK$의 원소의 개수는 $rs/t$이다. □

**예제 3.2.** 위수가 48인 군은 단순군이 아니다. 실제로 위수가 48인 군은 위수가 16이거나 8인 정규부분군을 갖는다는 것을 보일 것이다. 정리 3.6에 의하여 $G$는 위수가 16인 Sylow 2부분군을 1개 또는 3개 갖는다. 위수가 16인 부분군이 단 하나 존재한다면 이제 익숙하게 된 논의에 의하여 그것은 $G$에서 정규적이다. 위수가 16인 부분군이 3개가 존재한다고 가정하고, 이들 중 2개를 $H$와 $K$라 하자. 그러면 $H \cap K$의 위수는 8이어야 한다. 왜냐하면 $H \cap K$의 위수가 4보다 적거나 같으면 정리 3.12에 의하여 $HK$는 적어도 $16 \cdot 16/4 = 64$개의 원소들을 갖는다. 이것은 $G$가 단지 48개의 원소를 갖는다는 사실에 모순된다. 그러므로 $H \cap K$는 $H$와 $K$에서 정규적이다(지수가 2라는 사실, 또는 정리 3.4에 의하여). 그러므로 $H \cap K$의 정규화군은 $H$와 $K$ 둘 다 포함하며 위수는 1보다 큰 16의 배수이고 48의 약수이어야 하므로 48이다. 그래서 $H \cap K$는 $G$에서 정규적이다.

**예제 3.3.** 위수가 $255 = 3 \cdot 5 \cdot 17$인 모든 군은 가환이다(그래서 유한생성가환군 기본정리에서 순환군이며 255는 소수가 아니므로 단순군이 아니다). 정리 3.6에서 위수가 255인 군 $G$는 위수가 17인 부분군 $H$를 단 하나 갖는다. 그러면 $G/H$는 위수가 15이며 가환이다. 군 $G$의 교환자부분군 $C$는 $H$에 포함된다. 그래서 $C$는 $H$의 부분군으로서 위수가 1이거나 17이다. 정리 3.6은 또한 $G$는 위수가 3인 부분군을 1개 또는 85개 가지며 위수가 5인 부분군을 하나 또는 51개 가진다. 그러나 위수가 3인 부분군을 85개 가지면 $G$는 위수가 3인 원소들을 적어도 170개가 필요하고, 위수가 5인 부분군을 51개 가지면 위수가 5인 원소를 204개 필요로 한다. 그러면 둘 다 합치면 $G$에서 375개의 원소가 필요하다. 그것은 불가능하다. 그러므로 $G$에서 위수 3이거나 5인 정규부분군 $K$가 존재한다. 그리하여 $G/K$는 위수가 $5 \cdot 17$이거나 $3 \cdot 17$이고, 어느 경우에나 정리 37.7은 $G/K$는 가환임을 보인다.

그러므로 $C$는 $C \leq K$이고 위수3, 5 또는 1을 갖는다. $C \leq H$는 $C$가 위수 17 또는 1을 가짐을 보여주므로 결론적으로 $C$의 위수는 1이 된다. 그러므로 $C = \{e\}$이며 $G/C \simeq G$는 가환이다. 그러면 $G$가 순환군임을 보인다.

# 제 4 장

# 위수 60인 비아벨 단순군의 동형

**정리 4.1.** $G$가 위수 60인 비아벨 단순군이라 하자. 그러면 $G$는 $A_5$와 동형이다.

증명 . Step1. $G$의 실로우5 부분군의 개수는 6개이고 $G \subset S_6$를 보이자.
우선 $G$의 실로우5 부분군의 갯수를 생각해보자. 그 갯수를 $n$이라하면, 실로우 제3정리에 의해서 $n$은 60의 배수인 동시에, 법 5에 대해서 1과 합동이 된다. 그러면 법 5에 대해서 1과 합동인 수들을 생각해보자. $1, 6, 11, 16, \cdots$ 그러면 이중에서 60의 배수가 되는 수는 1과 6 뿐이다. 그러나 $G$가 비아벨 단순군이라는 가정에 의해서, 1은 될수가 없다. 왜냐하면 실로우 5 부분군의 갯수가 1이라면 그 부분군은 정규부분군이 되기 때문이다. $G$는 단순군이기 때문에, 정규부분군을 가질수 없다. 따라서 $G$의 실로우 5부분군의 갯수는 6이다. 그리고 $P_1, \cdots, P_6$까지를 실로우 5 부분군이라 하자.

$$S = \{P_1, P_2, P_3, P_4, P_5, P_6\}$$

$g$를 $G$의 임의의 원소라고 하자. 그리고 $\{gP_1g^{-1}, gP_2g^{-1}, gP_3g^{-1}, gP_4g^{-1}, gP_5g{-}1, gP_6g^{-1}\}$와 $\{P_1, P_2, P_3, P_4, P_5, P_6\}$를 비교해보자. 그러면 실로우 제 2정리에 의해

서 두 집합은 집합적으로 같은 집합이 된다. 즉

$$gP_1g^{-1} = P_a,\ gP_2g^{-1} = P_b,\ gP_3g^{-1} = P_c,$$
$$gP_4g^{-1} = P_d,\ gP_5g^{-1} = P_e,\ gP_6g^{-1} = P_f$$

그러므로 $G$에서 $S_6$으로 가는 준동형사상 $\phi$가 존재한다. 즉, $\phi : G \to S_6$이다. $ker\phi$는 정규적이며 $G/ker\phi \simeq \phi[G]$이다. 여기서 $ker\phi$는 $\{e\}$인데 왜냐하면 $G$는 단순군이기 때문에 정규부분군이 되는 원소가 자기자신이거나 항등원 $\{e\}$만 존재하기 때문이다. 그리고 $\phi[G]$는 $S_6$의 부분군이므로 $\therefore G \simeq \phi[G] \subset S_6$이다.

Step2. $G \subset S_6$라 할 때 $G \subset A_6$임을 보이자.
먼저 $A_6$는 $S_6$의 정규부분군이다. $G$가 $A_6$안에 속하지 않는다고 가정하자. 즉, $G \not\subset A_6$라 가정하자. 그러면 $GA_6 = S_6$가 되는데, 왜냐하면 $A_6 \subset GA_6 \subset S_6$일 때, $A_6$의 위수는 360이고 $S_6$의 위수는 720이다. 그러면 $A_6$와 $S_6$사이에는 부분군이 존재하지 않아서 $A_6 = GA_6$ 이거나 $GA_6 = S_6$이어야 한다. 그러나 $A_6 \neq GA_6$이므로 $GA_6 = S_6$가 된다. $S_6 = GA_6/A_6$는 제 2동형정리에 의해 $G/(G \cap A_6)$와 동형이 된다. $S_6 = GA_6/A_6 = \mathbb{Z}_2$이고, 그러므로 $G \cap A_6$는 $\{e\}$아니면 $\{G\}$가 된다. $G \cap A_6$가 $\{e\}$이면 $G/\{e\}$는 $G$이고 즉 $\mathbb{Z}_2$와 $G$가 동형이 되서 모순이다. $G \cap A_6$가 $\{G\}$이면 $G/\{G\}$는 $e$이고 즉 $\mathbb{Z}_2$와 $e$가 동형이 되서 모순이다. 따라서 $G \not\subset A_6$는 모순이고, 결론적으로 $G \subset A_6$이다.
Step3. $G \subset A_6$ 일 때, $G$와 $A_5$의 동형임을 보이자.
$G$의 좌잉여류를 생각하자.

$$S = \{G, a_1G, a_2G, a_3G, a_4G, a_5G\}$$

$g$는 $G$의 임의의 원소일때, 각 집합의 원소에 $g$를 곱하면$\{gG,\ ga_1G,\ ga_2G,\ ga_3G,\ ga_4G,\ ga_5G\}$이고 $gG = G$이므로 $S = \{G, a_1G, a_2G, a_3G, a_4G, a_5G\}$가 된다. 즉

$$ga_1G = a_iG,\ ga_2G = a_jG,\ ga_3G = a_kG,$$
$$ga_4G = a_lG,\ ga_5G = a_mG$$

$g$는 $S_5$의 원소로 생각할수 있고 $G \subset S_5$이다. 그리고 $G \subset A_5$임을 보이자. 위에서 보였던 방법과 동일하게 $A_5$는 $S_5$의 정규부분군이고 $G$가 $A_5$안에 속하지 않는다고 가정하자. 즉, $G \not\subset A_5$라 가정하자. 그러면 $GA_5 = S_5$가 되는데, 왜냐하면 $A_5 \subset GA_5 \subset S_5$일 때, $A_5$의 위수는 60이고 $S_5$의 위수는 120이다. 그러면 $A_5$와 $S_5$사이에는 부분군이 존재하지 않아서 $A_5 = GA_5$ 이거나 $GA_5 = S_5$이어야 한다. 그러나 $A_5 \neq GA_5$이므로 $GA_5 = S_5$가 된다. $S_5 = GA_5/A_5$는 제 2동형정리에 의해 $G/(G \cap A_5)$와 동형이 된다. $S_5 = GA_5/A_5 = \mathbb{Z}_2$이고, 그러므로 $G \cap A_5$는 $\{e\}$아니면 $\{G\}$가 된다. $G \cap A_5$가 $\{e\}$이면 $G/\{e\}$는 $G$이고 즉 $\mathbb{Z}_2$와 $G$가 동형이 되서 모순이다. $G \cap A_5$가 $\{G\}$이면 $G/\{G\}$는 $e$이고 즉 $\mathbb{Z}_2$와 $e$가 동형이 되서 모순이다. 따라서 $G \not\subset A_5$는 모순이고, 결론적으로 $G \subset A_5$이다.

$\therefore G \subset A_5$ 이며, 서로의 위수가 60으로 동일하기 때문에 $G \simeq A_5$이다. □

# 참고문헌

[1] J. Fraleigh: A First Course in Abstract Algebra, 7th Edition (2002).