제 7 장 해 설

§7.1 동치인 작용

군 G의 작용

$$G\times X \longrightarrow X, \quad (g, x) \longmapsto g\cdot x$$
$$G\times Y \longrightarrow Y, \quad (g, y) \longmapsto g\cdot y$$

에 대하여 적당한 일대일 대응 $\theta : X \longrightarrow Y$가 존재하여

(∗) $$\theta(g\cdot x) = g\cdot \theta(x) \qquad (g\in G,\ x\in X)$$

일 때, 이 두 작용은 서로 **동치**(同値, equivalent)인 작용이라고 한다.

위의 정의에서 작용 $G\times X \longrightarrow X$, $G\times Y \longrightarrow Y$에 의하여 정의되는 치환표현을 각각

$$\varphi : G \longrightarrow S(X), \qquad \psi : G \longrightarrow S(Y)$$

이라고 할 때, 조건 (∗) 는 모든 $g\in G$와 $x\in X$에 대하여 다음이 성립함을 뜻한다.

$$(\theta\circ\varphi(g))(x) = \theta(\varphi(g)(x))$$
$$= \psi(g)(\theta(x)) = (\psi(g)\circ\theta)(x)$$

즉, 조건 (∗) 는 모든 $g\in G$에 대하여

$$\theta\circ\varphi(g) = \psi(g)\circ\theta$$

임을 뜻한다.

$$\begin{tikzcd} X \arrow[r, "\varphi(g)"] \arrow[d, "\theta"'] & X \arrow[d, "\theta"] \\ Y \arrow[r, "\psi(g)"'] & Y \end{tikzcd}$$

정리 1 군 G가 작용 $G\times X \longrightarrow X$ 를 통하여 X에 추이적으로 작용할 때, 한 원소 $a\in X$에 대하여

$$H = G_a = \{ h\in G \mid h\cdot a = a\}$$

라 하고 또 $Y = \{xH \mid x\in G\}$ 이라고 하면 G의 작용

$$G\times Y \longrightarrow Y,\ (g,\ xH) \longmapsto gxH$$

는 추이적이고 또 작용 $G\times X \longrightarrow X$ 는 위의 작용과 동치이다.

증명 사상

$$G\times Y \longrightarrow Y,\ \ (g,\, xH) \longmapsto gxH$$

는 G의 작용이고 한 원소 $xH\in Y$에 대하여

$$\begin{aligned}\{g\cdot(xH) \mid g\in G\} &= \{gxH \mid g\in G\}\\ &= \{gH \mid g\in G\} = Y\end{aligned}$$

이므로, 이 작용은 추이적이다(정리 6.2.7 참조).

한편, 가정에 의하여 G는 X에 추이적으로 작용하므로 다음이 성립한다.

$$X = \{x\cdot a \mid x\in G\}$$

그런데, 임의의 $x,\, y\in G$에 대하여

$$\begin{aligned}x\cdot y = y\cdot a &\Longleftrightarrow (y^{-1}x)\cdot a = a\\ &\Longleftrightarrow y^{-1}x\in H\\ &\Longleftrightarrow xH = yH\end{aligned}$$

이므로

$$\theta\ :\ X\longrightarrow Y,\ \ \theta(x\cdot a) = xH$$

는 잘 정의된 사상이고 또 θ는 일대일 대응이다.

더우기, 임의의 $g\in G$와 $x\cdot a\in X$에 대하여 다음이 성립한다.

$$\begin{aligned}\theta(g\cdot(x\cdot a)) &= \theta((gx)\cdot a)\\ &= gxH = g\cdot(xH)\\ &= g\cdot(\theta(xa))\end{aligned}$$

$$\begin{tikzcd} X \arrow[r, "\varphi(g)"] \arrow[d, "\theta"'] & X \arrow[d, "\theta"] \\ Y \arrow[r, "\psi(g)"'] & Y \end{tikzcd}$$

따라서 작용 $G\times X\longrightarrow X$와 작용 $G\times Y\longrightarrow Y$는 서로 동치이다.

§7.2 위수 p^3 인 유한군

위수 2^3 인 유한군은 다음 유한군 중의 어느 한 군과 동형이다.

(1) Abel 군인 경우

$$C_8 \cong \mathbb{Z}_8 = \{0,1,3,4,5,6,7\},$$

$$C_2 \times C_4 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 = \{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2),(1,3)\},$$

$$C_2 \times C_2 \times C_2 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}$$

(2) Abel 군이 아닌 경우([31], [22] 참조)

$$D_4 = \langle \sigma, \tau \mid \sigma^4 = 1,\ \tau^2 = 1,\ \tau \circ \sigma \circ \tau^{-1} = \sigma^{-1} \rangle,$$

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

그 밖의 한 군

그리고, 홀수인 素數 p 에 대하여 위수 p^3 인 유한군은 다음 유한군 중의 어느 한 군과 동형이다

(1) Abel 군인 경우

$$C_{p^3} \cong \mathbb{Z}_{p^3},$$

$$C_p \times C_{p^2} \cong \mathbb{Z}_p \oplus \mathbb{Z}_{p^2},$$

$$C_p \times C_p \times C_p \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$$

(2) Abel 군이 아닌 경우([31] 참조).

$$M_3(p) = \langle x, y \mid x^{p^2} = y^p = 1,\ y^{-1}xy = x^{1+p} \rangle,$$

$$M(p) = \langle x, y, z \mid x^p = y^p = z^p = 1,\ [x,z] = [y,z] = 1, [x,y] = z \rangle$$

정리 1 군 G에서 두 원소 $x, y \in G$에 대하여 $z = [x, y]$가 x, y와 교환가능한 원소일 때, 모든 양의 정수 i, j에 대하여 다음이 성립한다.

(1) $[x^i, y^j] = z^{ij}$

(2) $[x^{-1}, y] = [x, y^{-1}] = [x, y]^{-1}$

(3) $(yx)^i = z^{\frac{i(i-1)}{2}} y^i x^i$

증명 (1) 먼저 $z = x^{-1}y^{-1}xy$이므로

$$y^{-1}xy = xz$$

이고, 가정에 의하여 $xz = zx$ 이므로 모든 양의 정수 i에 대하여 다음이 성립한다(문제 2.2.2).

$$y^{-1}x^i y = (y^{-1}xy)^i = (xz)^i = x^i z^i$$

따라서

$$y^{-2}x^i y^2 = y^{-1}(y^{-1}x^i y)y = y^{-1}x^i z^i y$$

이고 또 $z^i y = yz^i$이므로 위의 두 등식으로부터 다음 등식을 얻는다.

$$y^{-2}x^i y^2 = y^{-1}x^i yz^i = x^i z^i z^i = x^i z^{2i}$$

이와 같은 논법을 되풀이하면, 모든 양의 정수 i, j에 대하여 다음이 성립함을 알 수 있다.

$$y^{-j}x^i y^j = x^i z^{ij} \quad 즉 \quad [x^i, y^j] = z^{ij}$$

(2) 보충문제 2.15.3에 의하여 다음 등식이 성립한다.

$$e = [xx^{-1}, y] = [x, y][[x, y], x^{-1}][x^{-1}, y]$$

그런데, 가정에 의하여 $[x, y]$는 x와 교환가능한 원소이므로 $[x, y]$는 x^{-1}과도 교환가능한 원소이므로 $[[x, y], x^{-1}] = e$이고 따라서

$$e = [x, y]e[x^{-1}, y] = [x, y][x^{-1}, y]$$

이므로 $[x^{-1}, y] = [x, y]^{-1}$이다.

마찬가지로, $[x, y^{-1}] = [x, y]^{-1}$임을 증명할 수 있다.

(3) 먼저 $yx = z^0 yx$이므로, $i = 1$일 때 $(yx)^i = z^{\frac{i(i-1)}{2}} y^i x^i$이다.

이제 양의 정수 k에 대하여 $i = k$일 때 등식 (3)이 성립한다고 가정하면,

$$(yx)^{k+1} = (yx)^k (yx) = z^{\frac{k(k-1)}{2}} y^k x^k yx$$

이고 (1) 에 의하여

$$[x^k, y] = z^k \quad \text{즉} \quad x^k y = y x^k z^k = z^k y x^k$$

이므로

$$\begin{aligned}(yx)^{k+1} &= z^{\frac{k(k-1)}{2}} y^k x^k yx = z^{\frac{k(k-1)}{2}} y^k z^k y x^k x \\ &= z^{\frac{k(k-1)}{2}} z^k y^k y x^{k+1} = z^{\frac{k(k+1)}{2}} y^{k+1} x^{k+1}\end{aligned}$$

이고, 따라서 등식 (3) 은 $i = k+1$ 일 때에도 성립한다.

그러므로 등식 (3) 은 모든 양의 정수 i 에 대하여 성립한다.

정리 2 素數 p 에 대하여 위수 p^3 인 유한군 G 가 Abel 군이 아닐 때, 다음이 성립한다.

(1) $Z(G)$ 는 위수 p 인 순환군이고 $G/Z(G) \cong C_p \times C_p \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ 이다.

(2) $Z(G) = G'$

(3) 素數 p 가 홀수일 때, 모든 원소 $a, b \in G$ 에 대하여 $(ab)^p = a^p b^p$ 이다.

증명 (1) 정리 6.2.5 에 의하여 $|Z(G)| = p$ 이고 따라서 정리 2.7.7 에 의하여 $Z(G)$ 는 위수 p 인 순환군이다. 그러므로 잉여군 $G/Z(G)$ 의 위수는 p^2 이고, 따라서 다음이 성립한다(정리 2.10.15).

$$G/Z(G) \cong C_p \times C_p \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$$

$$\begin{tikzcd} G \arrow[d, dash, "p^2"'] \\ Z(G) = G' \arrow[d, dash, "p"'] \\ \{e\} \end{tikzcd}$$

(2) G 는 Abel 군이 아니므로 $G' \neq \{e\}$ 이고 잉여군 $G/Z(G)$ 는 Abel 군이므로 $G' \subseteq Z(G)$ 이다(정리 6.4.6).

그런데, $|Z(G)| = p$ 이고 $|G'| \,\big|\, |Z(G)|$ 이므로, $G' = Z(G)$ 이다.

(3) 素數 p 가 홀수일 때, G 의 임의의 원소 x, y 에 대하여 $z = [x, y]$ 이라고 하면, $z \in G' = Z(G)$ 이므로 $z^p = e$ 이고 z 는 x, y 와 교환가능한 원소이므로 양의 정수 i 에 대하여 다음이 성립한다(정리 2).

$$(yx)^i = z^{\frac{i(i-1)}{2}} y^i x^i$$

그런데, p는 홀수이고 $z^p = e$이므로

$$z^{\frac{p(p-1)}{2}} = (z^p)^{\frac{p-1}{2}} = e^{\frac{p-1}{2}} = e$$

이고 따라서 $(yx)^p = z^{\frac{p(p-1)}{2}} y^p x^p = y^p x^p$ 이다.

그러므로 임의의 $a, b \in G$에 대하여 $(ab)^p = a^p b^p$이다.

위의 정리와 관련된 사항에 대해서는 다음 문헌을 참고하기 바란다.

Gorenstein, D., Finite Groups, Harper & Row, New York, 1968,
Chelsea, New York, 1980, pp. 183, 191, 203

보기 1 군 $M_3(p)$ 의 임의의 원소 a, b에 대하여 $(ab)^p = a^p b^p$이지만 $M_3(p)$ 는 Abel 군이 아니다. 또, $M(p)$ 의 임의의 원소 a에 대하여 $a^p = 1$이고 따라서 임의의 a, b에 대하여 $(ab)^p = a^p b^p$이지만 $M(p)$ 는 Abel 군이 아니다.

보기 2 군 G의 두 원소 $a, b \in G$에 대하여

$$(ab)^2 = a^2 b^2$$

이면, $ab = ba$이다(문제 2.2.1).

위수 2^3인 정이면체군 D_4과 위수 2^3인 사원수군 Q_8에 대하여 다음이 성립한다.

(1) D_4에서 $\sigma \circ \tau \neq \tau \circ \sigma$이므로 $(\sigma \circ \tau)^2 \neq \sigma^2 \circ \tau^2$ 이다.

실제로, $(\sigma \circ \tau)^2 = 1$이지만 $\sigma^2 \circ \tau^2 = \sigma^2 \neq 1$이다.

(2) 사원수군 Q_8에서 $ij \neq ji$이므로 $(ij)^2 \neq i^2 j^2$이다.

실제로, $(ij)^2 = k^2 = -1, \quad i^2 j^2 = (-1)(-1) = 1$이다.

(3) 모든 원소 $a, b \in D_4$에 대하여 $a^4 = 1, \ (ab)^4 = a^4 b^4$이다.

(4) 모든 원소 $a, b \in Q_8$에 대하여 $a^4 = 1, \ (ab)^4 = a^4 b^4$이다.

§7.4.1 멱영군과 중심열

素數 p에 대하여 유한군 G 의 위수가 $|G| = p^n$ $(n \geq 0)$ 일 때, G를 유한 p-군이라고 한다.

유한 p-군에 대해서는 다음 정리가 성립한다.

정리 1 유한 p-군 G $(\neq \{e\})$ 에서 다음이 성립한다.

(1) $\{e\} \subsetneq N \lhd G$ 이면 $\{e\} \subsetneq N \cap Z(G)$ 이다.

(2) $\{e\} \subsetneq Z(G)$

정리 2 유한 p-군 G의 위수가 $|G| = p^n$ $(n \geq 1)$ 일 때, G에는 다음과 같은 정규부분군 N_n, N_{n-1}, $\cdots$, N_1, N_0 가 존재한다.

$$G = N_n \rhd N_{n-1} \rhd \cdots \rhd N_1 \rhd N_0 = \{e\},$$

$$G \rhd N_i, \quad |N_i| = p^i \qquad (0 \leq i \leq n)$$

특히, 유한 p-군은 가해군이다.

정리 3 유한 p-군 G $(\neq \{e\})$ 에서 G의 부분군 H에 대하여 다음이 성립한다.

(1) $H \subsetneq G$ 이면, $H \subsetneq N_G(H)$ 이다.

(2) $|G : H| = p$ 이면, $H \lhd G$ 이다.

정의 4 군 G $(\neq \{e\})$ 에서 다음 두 조건을 만족시키는 G의 부분군 H을 G의 **극대부분군**(極大部分群, maximal subgroup)이라고 한다.

(i) $H \subsetneq G$

(ii) K가 $H \subseteq K \subseteq G$ 인 G의 부분군이면, $K = H$ 또는 $K = G$ 이다.

정리 5 유한 p-군 G $(\neq \{e\})$ 에서 H가 G의 극대부분군이면, $H \lhd G$ 이고 또 잉여군 G/H는 위수 p인 순환군이고 $|G : H| = p$ 이다.

증명 이제 H가 G의 극대부분군이라고 하자.
이 때, 정리 3에 의하여 $H \subsetneq N_G(H) \subseteq G$이므로 $N_G(H) = G$이고 따라서 $H \lhd G$이다. 그러므로 잉여군 G/H가 정의되고, K/H가 G/H의 부분군이면 K는 $H \subseteq K \subseteq G$인 G의 부분군이므로 $K = H$ 또는 $K = G$이고 따라서 G/H 의 부분군은 $\{H\}$ 또는 G/H 뿐이므로 정리 2.5.7 에 의하여 잉여군 G/H는 위수 p인 순환군이고 $|G : H| = |G/H| = p$이다.

정의 6 군 G에서 각 정수 i (≥ 0)에 대하여 $Z_i(G)$를 다음과 같이 귀납적으로 정의한다.

(i) $Z_0(G) = \{e\}$, $Z_1(G) = Z(G)$

(ii) $i \geq 1$ 일 때, 표준준동형사상 $\pi_i : G \longrightarrow G/Z_i(G)$에 대하여 잉여군 $G/Z_i(G)$ 의 중심 $Z(G/Z_i(G))$ 에 대응하는 G의 정규부분군을 $Z_{i+1}(G)$로 정한다(따름정리 2.10.9). 즉,

$$
\begin{tikzcd}
G \arrow[r, "\pi_i"] \arrow[d, phantom, "\triangledown"] & G/Z_i(G) \arrow[d, phantom, "\triangledown"] \\
Z_{i+1}(G) \arrow[d, dash] & Z(G/Z_i(G)) \arrow[d, dash] \\
Z_i(G) & \{Z_i(G)\}
\end{tikzcd}
$$

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$$

또, $Z_i(G)$를 G의 **제 i 중심**(ith center)이라 하고

$$Z_0(G) = \{e\} \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \cdots$$

를 G의 **승중심열**(昇中心列 upper central series)이라고 한다.

분명히 $Z_i(G) \lhd G$이다. 또, 적당한 i에 대하여 $Z_i(G) = Z_{i+1}(G)$ 이면,

$$Z_i(G) = Z_{i+1}(G) = Z_{i+2}(G) = \cdots$$

이고 또 G의 승중심열은 G로 끝나지 않을 수도 있다.

정의 7 군 G에서 적당한 정수 m (≥ 0)에 대하여 $Z_m(G) = G$일 때, G를 **멱영군**(冪零群, nilpotent group) 이라고 한다.

그리고, G가 멱영군일 때, $G = Z_c(G)$ 인 가장 작은 정수 c를 멱영군 G의 **급수**(級數 class)이라고 한다.

보기 1 군 $\{e\}$ 는 급수 0 인 멱영군이다.

그리고, 군 $G \neq \{e\}$ 가 Abel 군이면, $Z_0 G) = \{e\} \neq G$, $Z_1(G) = G$ 이므로 G 는 급수 1 인 멱영군이다. 또, 군 G 에 대하여 다음이 성립한다.

G 는 급수 0 인 멱영군 $\Leftrightarrow$ $G = \{e\}$

G 는 급수 1 인 멱영군 $\Leftrightarrow$ $G \neq \{e\}$ 이고 G 는 Abel 군이다.

보기 2 정수 n (≥ 3) 에 대하여 대칭군 S_n 의 중심은 $Z(S_n) = \{1\}$ 이고 따라서 모든 정수 i (≥ 1) 에 대하여 $Z_i(S_n) = \{1\}$ 이다.

따라서 $n \geq 3$ 일 때, 대칭군 S_n 은 멱영군이 아니다.

보기 3 정수 n (≥ 3) 이 홀수일 때, 위수 $2n$ 인 정이면체군

$$D_n = \{1, \sigma, \cdots, \sigma^{n-1}, \tau, \sigma \circ \tau, \cdots, \sigma^{n-1} \circ \tau\}$$

의 중심은 $Z(D_n) = \{1\}$ 이다. 따라서 모든 정수 에 대하여

$$Z_0(D_n) = Z_1(D_n) = Z_2(D_n) = \cdots = \{1\}$$

이므로 D_n 은 멱영군이 아니다(문제 2.12.7).

보기 4 위수 8 인 사원수군 $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ 을 생각해 보자.

먼저 $Z(Q_8) = \{1, -1\}$ 이고 잉여군 $Q_8/Z(Q_8)$ 은 위수 4 인 Abel 군이므로 $Z(Q_8/Z(Q_8)) = Q_8/Z(Q_8)$ 이다(보기 2.9.6). 따라서

$$Z_0(Q_8) = \{1\}, \quad Z_1(Q_8) = \{1, -1\}, \quad Z_2(Q_8) = Q_8$$

이고, 따라서 Q_8 은 급수 2 인 멱영군이다.

그리고, 위수 8 인 정이면체군

$$D_4 = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma \circ \tau, \sigma^2 \circ \tau, \sigma^3 \circ \tau\}$$

에서 $Z(D_4) = \{1, \sigma^2\}$ 이고 또 잉여군 $D_4/Z(D_4)$ 는 위수 4 인 Abel 군이므로 $Z(D_4/Z(D_4)) = D_4/Z(D_4)$ 이다(보기 2.12.7). 따라서

$$Z_0(D_4) = \{1\}, \quad Z_1(D_4) = \{1, \sigma^2\}, \quad Z_2(D_4) = D_4$$

이고, 따라서 D_4 는 급수 2 인 멱영군이다.

정리 8 군 G가 유한 p-군이면, G는 멱영군이다.

증 명 이제 $|G| = p^n$ $(n \geq 0)$ 이라 하고, n에 관한 귀난법으로 정리를 증명한다.

먼저 $n = 0$ 인 경우에, $G = \{e\}$ 이고 또 $Z_0(G) = \{e\} = G$ 이므로 G는 멱영군이다.

이제 $n \geq 1$ 일 때, $0 \leq m \langle n$ 인 정수 m에 대하여 위수가 p^m 인 군이 모두 멱영군이라고 가정하고 $|G| = p^n$ 이라고 하자.

이 때, 정리 1에 의하여 $Z_1(G) = Z(G) \supsetneq \{e\}$ 이므로 다음이 성립한다.

$$|Z_1(G)| = p^k, \qquad k \geq 1$$

$$|G/Z_1(G)| = \frac{|G|}{|Z_1(G)|} = p^{n-k},$$

$$0 \leq n-k \langle n$$

$$\begin{tikzcd}[row sep=large]
G/Z_1(G) \arrow[d, dash, "p^{n-k}"] & G \arrow[d, dash, "p^{n-k}"'] \\
\{Z_1(G)\} & Z_1(G) \arrow[d, dash, "p^k"'] \\
 & \{e\}
\end{tikzcd}$$

그러므로 귀납법 가정에 의하여 적당한 정수 d (≥ 0) 에 대하여

$$G/Z_1(G) = Z_d(G/Z_1(G))$$

이고 따라서 $G = Z_{d+1}(G)$ 이므로 G는 멱영군이다.

정리 9 멱영군은 모두 가해군이다.

증 명 군 G가 멱영군이라 하고 적당한 정수 m (≥ 0) 에 대하여 $Z_m(G) = G$ 이라고 하자.

이 때, 각 정수 i $(0 \leq i \leq m-1)$ 에 대하여 $Z_i(G) \lhd G$ 이고

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$$

이므로 $Z_{i+1}(G)/Z_i(G)$ 는 Abel 군이다. 그러므로

$$G = Z_m(G) \rhd \cdots \rhd Z_1(G) \rhd Z_m(G) = \{e\}$$

는 G의 Abel 정규열이고, 따라서 G는 가해군이다(정의 5.11.2).

보기 1.5 대칭군 S_3는 가해군이지만 멱영군은 아니다(보기 6.10.1, 보기 2).

다음에는 멱영군의 특성에 대하여 논한다.

다음 정리는 정리 2.15.2를 다시 쓴 것이다.

정리 10 군 G에서 원소 $x, y, g \in G$에 대하여 다음이 성립한다.

(1) $[x, y] = e \Longleftrightarrow xy = yx$

(2) $[x, y]^{-1} = [y, x]$

(3) $f : G \longrightarrow \overline{G}$가 준동형사상이면, $f([x, y]) = [f(x), f(y)]$ 이다.

(4) ${}^g[x, y] = [{}^gx, {}^gy]$, $\quad [x, y]^g = [x^g, y^g]$

정의 11 군 G에서 H, K가 G의 부분군일 때,

$$[h, k] \qquad\qquad (h \in H,\ k \in K)$$

와 같은 꼴의 교환자 전체에 의하여 생성된 부분군을 H와 K의 **교환자 (부분)군**이라 하고 이것을 $[H, K]$로 나타낸다. 즉,

$$[H, K] = \langle [h, k] \mid h \in H,\ k \in K \rangle$$

정리 12 군 G의 부분군 H, K, H_1, K_1에 대하여 다음이 성립한다.

(1) $[H, K] = \{e\}$일 때 그리고 이때에만 모든 원소 $h \in H$와 모든 원소 $k \in K$에 대하여 $hk = kh$이다. 특히,

$$[H, G] = \{e\} \Leftrightarrow H \subseteq Z(G)$$

(2) $[H, K] = [K, H]$

(3) $f : G \longrightarrow \overline{G}$가 군 준동형사상이면, $f([H, K]) = [f(H), f(K)]$이다.

(4) 임의의 원소 $g \in G$에 대하여 다음 등식이 성립한다.

$${}^g[H, K] = [{}^gH, {}^gK], \quad [H, K]^g = [H^g, K^g]$$

(5) $H_1 \subseteq H,\ K_1 \subseteq K$이면, $[H_1, K_1] \subseteq [H, K]$ 이다.

증 명 (1) 정의와 정리 10에 의하여 (1) 이 성립한다.

(2) 임의의 $h \in H, k \in K$에 대하여 $[h, k]^{-1} = [k, h]$이고 또

$$\begin{aligned}[H, K] &= \langle [h, k] \mid h \in H, k \in K \rangle \\ &= \langle [h, k]^{-1} \mid h \in H, k \in K \rangle\end{aligned}$$

이므로 $[H, K] = [K, H]$ 이다.

(3) $f : G \longrightarrow \overline{G}$ 가 군 준동형사상일 때, 임의의 $h \in H, k \in K$ 에 대하여 $f([h, k]) = [f(h), f(k)]$ 이고 또

$$[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle,$$
$$f(H) = \{f(h) \mid h \in H\}, \quad f(K) = \{f(k) \mid k \in K\}$$

이므로 $f([H, K]) = [f(H), f(K)]$ 이다.

(4) 임의의 $h \in H, k \in K$ 와 $g \in G$ 에 대하여

$${}^{g}[h, k] = [{}^{g}h, {}^{g}k], \quad [h, k]^{g} = [h^{g}, k^{g}]$$

이므로 (3)에 의하여 ${}^{g}[H, K] = [{}^{g}H, {}^{g}K]$, $[H, K]^{g} = [H^{g}, K^{g}]$ 이다.

(5) 정의에 의하여 분명히 (5) 가 성립한다.

정리 13 군 G 의 두 부분군 H, K 에 대하여 다음이 성립한다.

(1) $[H, K] \subseteq H \Leftrightarrow K \subseteq N_G(H)$

(2) $[H, G] \subseteq H \Leftrightarrow H \lhd G$

(3) $H \lhd G$, $K \lhd G$ 이면, $[H, K] \lhd G$ 이고 또 $[H, K] \subseteq H \cap K$ 이다.

증 명 (1) 먼저 $[H, K] \subseteq H$ 이라고 하자.

이 때, 임의의 원소 $h \in H$ 와 임의의 원소 $k \in K$ 에 대하여

$$h^{-1}k^{-1}hk = [h, k] \in H$$

이므로 $k^{-1}hk \in H$ 이고 따라서 $k^{-1}Hk \subseteq H$ 이다. 여기서 k 대신에 k^{-1} 를 생각하면 $kHk^{-1} \subseteq H$ 즉 $H \subseteq k^{-1}Hk$ 를 얻으므로 $k^{-1}Hk = H$ 이다.

따라서 $K \subseteq N_G(H)$ 이다(정리 2.14.8).

역으로, $K \subseteq N_G(H)$ 이라고 하자. 이 때, 임의의 원소 $h \in H$ 와 임의의 원소 $k \in K$ 에 대하여 $k^{-1}hk \in H$ 이므로

$$[h, k] = h^{-1}(k^{-1}hk) \in H$$

이고 따라서 $[H, K] \subseteq H$ 이다.

(2) 앞의 (1) 에 의하여 다음이 성립한다.

$$[H, G] \subseteq H \Leftrightarrow G \subseteq N_G(H) \Leftrightarrow H \lhd G$$

(3) $H \lhd G$, $K \lhd G$ 이라고 하자. 이 때, 임의의 원소 $g \in G$ 에 대하여

$$[H, K]^g = [H^g, K^g] = [H, K]$$

이므로 $[H, K] \lhd G$ 이다(정리 12 참조).

그리고, $K \subseteq G = N_G(H)$, $H \subseteq G = N_G(K)$ 이고 따라서 (1) 에 의하여

$[H, K] \subseteq H$, $[H, K] = [K, H] \subseteq K$ 이므로 $[H, K] \subseteq H \cap K$ 이다.

정리 14 군 G 에서 원소 $x, y, z \in G$ 에 대하여 다음이 성립한다.

(1) $[xy, z] = [x, z]^y [y, z]$ (2) $[x, yz] = [x, z][x, y]^z$

증명 (1) $[xy, z] = (xy)^{-1} z^{-1} (xy) z = y^{-1} x^{-1} z^{-1} xyz$

$$= y^{-1} x^{-1} z^{-1} x (z y y^{-1} z^{-1}) yz$$
$$= y^{-1} (x^{-1} z^{-1} xz) y (y^{-1} z^{-1} yz)$$
$$= y^{-1} [x, z] y [y, z] = [x, z]^y [y, z]$$

(2) $[x, yz] = x^{-1} (yz)^{-1} x (yz) = x^{-1} z^{-1} y^{-1} xyz$

$$= x^{-1} z^{-1} (x z z^{-1} x^{-1}) y^{-1} xyz$$
$$= (x^{-1} z^{-1} xz) z^{-1} (x^{-1} y^{-1} xy) z$$
$$= [x, z] z^{-1} [x, y] z = [x, z][x, y]^z$$

정리 15 군 G 의 두 부분군 H, K 에 대하여 $\langle H, K \rangle = \langle H \cup K \rangle$ 이라고 할 때, $[H, K] \lhd \langle H, K \rangle$ 이다.

증 명 분명히 $[H, K] \subseteq \langle H, K \rangle$ 이므로 $[H, K]$ 는 $\langle H, K \rangle$ 의 부분군이다. 또, 임의의 $h \in H$, $k \in K$ 와 임의의 원소 $u \in H$, $v \in K$ 에 대하여

$$[hu, k] = [h, k]^u [u, k], \qquad [kv, h] = [k, h]^v [v, h]$$

이므로 다음이 성립한다(정리 12 참조).

$$[h, k]^u = [hu, k][u, k]^{-1} \in [H, K],$$
$$[k, h]^v = [kv, h][v, h]^{-1} \in [K, H] = [H, K]$$

그런데, $\langle H, K \rangle = \langle H \cup K \rangle$ 이므로 $[H, K] \lhd \langle H, K \rangle$ 이다.

정리 16 군 G에서 $N \lhd G$일 때, $\pi : G \longrightarrow G/N$를 준동형사상이라고 하면, G의 두 부분군 H, K에 대하여 다음이 성립한다.

$$[\pi(H), \pi(K)] = \pi([H, K])$$

즉 $[HN/N, KN/N] = [H, K]N/N$

$$\begin{tikzcd} & G \arrow[r, "\pi"] \arrow[d, dash] & G/N \arrow[d, dash] \\ & HN \arrow[dl, dash] \arrow[d, dash] & HN/N \arrow[d, dash] \\ H & N & \{N\} \end{tikzcd}$$

증 명 정리 12 에 의하여 $[\pi(H), \pi(K)] = \pi([H, K])$ 이다. 그런데,

$$\begin{aligned} \pi(H) &= \{hN \in G/N \mid h \in H\} \\ &= \{hnN \in G/N \mid h \in H, n \in N\} = HN/N \end{aligned}$$

이고, 마찬가지로 $\pi(K) = KN/N$, $\pi([H, K]) = [H, K]N/N$이다.

따라서 $[HN/N, KN/N] = [H, K]N/N$이다.

정리 17 군 G에서 $N \lhd G$일 때, G의 부분군 H에 대하여 다음 두 조건은 서로 동치이다.

(1) $[H, G] \subseteq N$ (2) $HN/N \subseteq Z(G/N)$

증 명 잉여군 G/N에서 두 원소 $h \in H, g \in G$에 대하여

$$(hN)^{-1}(gN)^{-1}(gN)(hN) = (h^{-1}g^{-1}gh)N = [h, g]N$$

이므로 다음이 성립한다.

$[H, G] \subseteq N$

$\Leftrightarrow$ 모든 원소 $h \in H$와 모든 원소 $g \in G$에 대하여 $[h, g] \in N$

$\Leftrightarrow$ 모든 원소 $h \in H$와 모든 원소 $g \in G$에 대하여

$(hN)^{-1}(gN)^{-1}(gN)(hN) = N$ 즉 $(hN)(gN) = g(N)h(N)$

$\Leftrightarrow$ 모든 원소 $h \in H$에 대하여 $hN \in Z(G/N)$

그런데, 잉여군 G/N에서

$$\{hN \in G/N \mid h \in H\} = \{hnN \in G/N \mid h \in H, n \in N\} = HN/N$$

이므로 위의 결과에 의하여 (1)과 (2) 는 서로 동치이다.

따름정리 18 군 G 에서 다음이 성립한다.

$$Z_i(G) \lhd G, \qquad [Z_{i+1}(G), G] \subseteq Z_i(G) \qquad (i \geq 0)$$

증 명 정의 6 에 의하여 $Z_i(G) \lhd G$ 이고 $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i)$ 이므로 정리 17 에 의하여 따름정리가 성립한다.

정의 19 군 G 에서 부분군들로 이루어진 열

$$(*) \qquad G = H_1 \supseteq H_2 \supseteq \cdots \supseteq H_n = \{e\}$$

에서 각 정수 i $(1 \leq i \leq n-1)$ 에 대하여 $[H_i, G] \subseteq H_{i+1}$ 일 때, (*) 를 G 의 **중심열**(中心列, central series)이라고 한다.

정의 20 군 G 에서 각 양의 정수 i (≥ 1) 에 대하여 부분군 $C_i(G)$ 를 다음과 같이 귀납적으로 정의한다.

(i) $C_1(G) = G$

(ii) $C_{i+1}(G) = [C_i(G), G] \quad (i \geq 1)$

그리고,

$$G = C_1(G) \supseteq C_2(G) \supseteq C_3(G) \supseteq \cdots$$

를 G 의 **강중심열**(降中心列, lower central series)이라고 한다.

위의 정의에서 각 양의 정수 i (≥ 1) 에 대하여 $C_i(G) \lhd G$ 이다.

실제로, $C_1(G) = G$ 이므로 $C_1(G) \lhd G$ 이고 또 $Ci(G) \lhd G$ 이라고 가정하면, $C_{i+1}(G) = [C_i(G), G]$ 이므로 정리 13 에 의하여 $C_{i+1}(G) \lhd G$ 이다. 그리고, 적당한 i 에 대하여 $C_i(G) = C_{i+1}(G)$ 이면

$$C_i(G) = C_{i+1}(G) = C_{i+2}(G) = \cdots$$

이고, 또 G 의 降중심열은 $\{e\}$ 로 끝나지 않을 수도 있다.

군 G 에서 $Z_i(G)$ 는 다음과 같이 정의된 G 의 정규부분군이다.

$Z_0(G) = \{e\}$, $Z_1(G) = Z(G)$,

$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$

정리 21 군 G가 아래와 같은 중심열을 가진 군이라고 하자.

(*) $$G = H_1 \supseteq H_2 \supseteq \cdots \supseteq H_n = \{e\}$$

이 때, 다음이 성립한다.

(1) 각 정수 i $(1 \le i \le n-1)$ 에 대하여

$$H_i \lhd G, \qquad H_i/H_{i+1} \subseteq Z(G/H_{i+1})$$

이고 H_i/H_{i+1} 은 Abel 군이다.

(2) 각 정수 i $(1 \le i \le n)$ 에 대하여 $C_i(G) \subseteq H_i$ 이다.

(3) 각 정수 j $(0 \le j \le n-1)$ 에 대하여 $H_{n-j} \subseteq Z_j(G)$ 이다.

증 명 (1) 정의 19 에 의하면, 각 정수 i $(0 \le i \le n-1)$ 에 대하여

$$[H_i, G] \subseteq H_{i+1} \subseteq H_i$$

이므로 정리 13 에 의하여 $H_i \lhd G$ 이고 또 정리 17 에 의하여

$$H_i/H_{i+1} \subseteq Z(G/H_{i+1})$$

이고 따라서 H_i/H_{i+1} 은 Abel 군이다.

(2) 먼저 $C_1(G) = G = H_1$ 이므로 $C_1(G) \subseteq H_1$ 이다.

그리고, 정수 i $(1 \le i \le n-1)$ 에 대하여 $C_i(G) \subseteq H_i$ 이라고 가정하면 다음이 성립한다(정리 2.3 (5)).

$$C_{i+1}(G) = [C_i(G), G] \subseteq [H_i, G] \subseteq H_{i+1}$$

그러므로 각 정수 i $(1 \le i \le n)$ 에 대하여 $C_i(G) \subseteq H_i$ 이다.

(3) 먼저 $H_n = \{e\} = Z_0(G)$ 이므로 $H_{n-0} \subseteq Z_0(G)$ 이다.

그리고, 정수 j $(0 \le j \le n-2)$ 에 대하여 $H_{n-j} \subseteq Z_j(G)$ 이라고 가정하면,

$$[H_{n-(j+1)}, G] \subseteq H_{n-j} \subseteq Z_j(G)$$

이므로 정리 17 에 의하여

$$H_{n-(j+1)}Z_j(G)/Z_j(G) \subseteq Z(G/Z_j(G)) = Z_{j+1}G)/Z_j(G)$$

이고 따라서 $H_{n-(j+1)} \subseteq Z_{j+1}(G)$ 이다.

그러므로 각 정수 j $(0 \le j \le n-1)$ 에 대하여 $H_{n-j} \subseteq Z_j(G)$ 이다.

$$\begin{array}{ccccccccccc}
Z_{n-1}(G) & \supseteq & Z_{n-2}(G) & \supseteq & \cdots & \supseteq & Z_1(G) & \supseteq & Z_0(G) = \{e\} & & \\
\cup & & \cup & & & & \cup & & \| & & \\
G = H_1 & \supseteq & H_2 & \supseteq & H_3 & \supseteq \cdots \supseteq & H_{n-1} & \supseteq & H_n = \{e\} & & \\
\| & & \cup & & \cup & & \cup & & \cup & & \\
G = C_1(G) & \supseteq & C_2(G) & \supseteq & C_3(G) & \supseteq \cdots \supseteq & C_{n-1}(G) & \supseteq & C_n(G) & &
\end{array}$$

정리 22 군 G에 대하여 다음 조건은 서로 동치이다.

(1) G는 멱영군이다.

(2) G는 적어도 한 개의 중심열을 가진다.

(3) 적당한 양의 정수 s $(s \geq 1)$에 대하여 $C_s(G) = \{e\}$이다.

증 명 (1) $\Longrightarrow$ (2) 군 G가 멱영군이라고 하자.

이 때, 적당한 정수 m에 대하여 $Z_m(G) = G$이고 또 가 정수 i (≥ 0)에 대하여 $[Z_{i+1}(G), G] \subseteq Z_i(G)$ 이므로(따름정리 18)

$$G = Z_m(G) \supseteq \cdots \supseteq Z_1(G) \supseteq Z_0(G) = \{e\}$$

는 G의 중심열이다.

(2) $\Longrightarrow$ (3) 군 G가 중심열

$$G = H_1 \supseteq H_2 \supseteq \cdots \supseteq H_n = \{e\}$$

을 가지면, 정리 21 에 의하여 $C_n(G) \subseteq H_n = \{e\}$이므로 $C_n(G) = \{e\}$이다.

(3) $\Longrightarrow$ (1) 적당한 양의 정수 s $(s \geq 1)$에 대하여 $C_s(G) = \{e\}$이라고 하자. 이 때, 각 정수 i $(1 \leq i \leq n-1)$에 대하여 $[C_i(G), G] = C_{i+1}(G)$이므로

$$G = C_1(G) \supseteq C_2(G) \supseteq \cdots \supseteq C_s(G) = \{e\}$$

는 G의 중심열이다. 따라서 정리 21 에 의하여

$$C_{s-j}(G) \subseteq Z_j(G) \qquad (0 \leq j \leq s-1)$$

이므로 $G = C_1(G) = C_{s-(s-1)}(G) \subseteq Z_{s-1}(G)$ 이다.

그러므로 $Z_{s-1}(G) = G$이므로 G는 멱영군이다.

앞의 정리의 증명에 의하여 G가 멱영군인 경우에 $Z_m(G) = G$이라고 하면 멱영군 G의 昇중심열

$$G = Z_m(G) \supseteq \cdots \supseteq Z_1(G) \supseteq Z_0(G) = \{e\}$$

는 중심열이고, 또 $C_s G) = \{e\}$이라고 하면 멱영군 G의 降중심열

$$G = C_1(G) \supseteq C_2(G) \supseteq \cdots \supseteq C_s(G) = \{e\}$$

는 중심열이다.

정리 23 군 G가 멱영군일 때, 급수가 $c\ (\geq 1)$이면 다음이 성립한다.

(1) $Z_c(G) = G, \quad Z_{c-1}(G) \neq G$

(2) G의 중심열은 적어도 $c+1$개의 항을 가지며, 꼭 $c+1$개의 항을 가진 중심열이 존재한다.

(3) $C_{c+1}(G) = \{e\}, \quad C_c(G) \neq \{e\}$

증 명 (1) 정의에 의하여 (1) 이 성립한다.

(2) 군 G를 멱영군이라 하고

$$G = H_1 \supseteq H_2 \supseteq \cdots \supseteq H_n = \{e\}$$

를 G의 중심열이라고 하자(정리 22). 이 때, 정리 21 에 의하여

$$G = H_1 = H_{n-(n-1)} \subseteq Z_{n-1}(G)$$

이므로 $Z_{n-1}(G) = G$이고 따라서 $c \leq n-1$ 즉 $c+1 \leq n$이다.

그리고, G의 昇중심열

$$G = Z_c(G) \supseteq \cdots \supseteq Z_1(G) \supseteq Z_0(G) = \{e\}$$

는 $c+1$개의 항를 가진 중심열이다.

(3) 정리 21 에 의하여

$$C_{c+1}(G) \subseteq Z_0(G) = \{e\}$$

이므로 $C_{c+1}(G) = \{e\}$이다. 그리고, 위의 (2)에 의하여 降중심열은 적어도 $c+1$개의 항을 가져야 하므로 $C_c(G) \neq \{e\}$이다.

앞의 정리로부터 다음 따름정리를 얻는다.

따름정리 24 군 G와 양의 정수 c에 대하여, G가 급수 c인 멱영군이기 위한 필요충분조건은 잉여군 $G/Z(G)$가 급수 $c-1$인 멱영군인 것이다.

정리 25 군 G에서 다음이 성립한다.

(1) H가 G의 부분군이면, 각 양의 정수 i에 대하여 $C_i(H) \subseteq C_i(G)$이다.

(2) 사상 $f : G \longrightarrow \overline{G}$가 군 준동형사상이면, 각 양의 정수 i에 대하여 $C_i(f(G)) \subseteq f(C_i(G))$ 이다.

증 명 (1) 먼저 $C_1(H) = H \subseteq G = C_1(G)$ 이다. 또, 양의 정수 i에 대하여 $C_i(H) \subseteq C_i(G)$ 이라고 가정하면, 정리 12에 의하여 다음이 성립한다.

$$C_{i+1}(H) = [C_i(H), H] \subseteq [C_i(G), G] = C_{i+1}(G)$$

따라서 각 양의 정수 i에 대하여 $C_i(H) \subseteq C_i(G)$ 이다.

(2) 먼저 $C_1(f(G)) = f(G) = f(C_1(G))$ 이다

그리고, 양의 정수 i에 대하여 $C_i(f(G)) \subseteq f(C_i(G))$ 이라고 가정하면, 정리 12에 의하여 다음이 성립한다.

$$\begin{aligned} C_{i+1}(f(G)) &= [C_i(f(G)), f(G)] \subseteq [f(C_i(G)), f(G)] \\ &\subseteq f([(C_i(G), G]]) = f(C_{i+1}(G)) \end{aligned}$$

따라서 각 양의 정수 i에 대하여 $C_i(f(G)) \subseteq f(C_i(G))$ 이다.

정리 26 군 G가 급수 c인 멱영군일 때, 다음이 성립한다.

(1) H가 G의 부분군이면, H는 멱영군이고 그 급수는 $\leq c$이다.

(2) 사상 $f : G \longrightarrow \overline{G}$가 군 준동형사상이면, $f(G)$는 멱영군이고 그 급수는 $\leq c$이다. 특히, $N \lhd G$일 때, 잉여군 G/N는 멱영군이고 그 급수는 $\leq c$이다.

증 명 (1) 정리 25 에 의하여

$$C_c(H) \subseteq C_c(G) = \{e\}$$

이므로 $C_c(H) = \{e\}$ 이고 따라서 H는 멱영군이고 그 급수는 $\leq c$이다.

(2) 정리 25 에 의하여

$$C_c(f(G)) \subseteq f(C_c(G)) = f(\{e\}) = \{\bar{e}\}$$

이고 따라서 $f(G)$ 는 멱영군이고 그 급수는 $\leq c$ 이다.

군 G 가 멱영군 [가해군] 이면, G 의 모든 부분군과 G 의 모든 준동형상은 멱영군 [가해군] 이다(정리 26, 정리 7.38 참조). 그리고, 군 G 의 한 정규부분군 N 에 대하여 N 과 잉여군 G/N 이 가해군이면, 군 G 는 가해군이다 (정리 7.3.9). 그러나, 다음 보기에서 알 수 있는 바와 같이 군 G 의 한 정규부분군 N 에 대하여 N 과 잉여군 G/N 이 멱영군이더라도 G 가 멱영군이 아닐 수 있다.

보기 5 대칭군 S_3 에서 $A_3 \lhd S_3$ 이고 A_3 와 잉여군 S_3/A_3 는 모두 멱영군이지만, S_3 는 멱영군이 아니다(보기 2).

정리 27 군 G_1, G_2 가 각각 급수 c_1, c_2 인 멱영군일 때, $c = \max\{c_1, c_2\}$ 이라고 하면 직적 $G = G_1 \times G_2$ 는 급수 c 인 멱영군이다.

증 명 계급수 c_1, c_2 에 관한 귀납법으로 정리를 증명한다.

먼저 $c_1 = 0$ 이면, $G_1 = \{e_1\}$ 이므로 $G_1 \times G_2 \cong G_2$ 이고 따라서 G 는 멱영군이고 그 급수는 $c_2 = c$ 이다. 마찬가지로, $c_2 = 0$ 이면 $G_1 \times G_2 \cong G_1$ 이고 G 는 멱영군이고 그 급수는 $c_1 = c$ 이다.

이제 $c_1 \geq 0$, $c_2 \geq 1$ 이라고 하자. 이 때, 보충문제 2.11.2 에 의하여

$$Z(G) = Z(G_1) \times Z(G_2),$$

$$G/Z(G) \cong G_1/Z(G_1) \times G_2/Z(G_2)$$

이고 또 $G_1/Z(G_1)$, $G_2/Z(G_2)$ 는 각각 급수가 $c_1 - 1$, $c_2 - 1$ 인 멱영군이다(따음정리 24). 따라서 귀납법 가정에 의하여 $G_1/Z(G_1) \times G_2/Z(G_2)$ 즉 $G/Z(G)$ 는 멱영군이고 그 급수는 $\max\{c_1 - 1, c_2 - 1\} = c - 1$ 이다.

그러므로 따름정리 24 에 의하여 G 는 멱영군이고 그 급수는 c 이다.

앞의 정리 27 로부터 다음 따름정리가 성립함을 알 수 있다.

따름정리 28 군 $G_1, \cdots, G_n$ $(n \geq 2)$ 가 각각 급수 $c_1, \cdots, c_n$ 인 멱영군일 때, $c = \max\{c_1, \cdots, c_n\}$ 이라고 하면 직적 $G = G_1 \times \cdots \times G_n$ 는 급수 c 인 멱영군이다.

다음 두 정리는 유한 p-군에 대해서도 성립한다(정리.1, 정리 3 참조).

정리 29 군 $G\ (\neq \{e\})$ 가 멱영군일 때, $\{e\} \subsetneq N \lhd G$ 이면 다음이 성립한다.

(1) $[N, G] \subsetneq N$

(2) $\{e\} \subsetneq N \cap Z(G)$, $\{e\} \subsetneq Z(G)$

증 명 양의 정수 i 에 대하여 N_i 를 다음과 같이 귀납적으로 정의하자.

(i) $N_1 = N$ (ii) $i \geq 1$ 일 때, $N_{i+1} = [N_i, G]$

이 때, $N \lhd G$ 이므로 모든 양의 정수 i 에 대하여 $N_i \lhd G$ 이다(정리 13).

그리고, $N_1 = N$, $N \subseteq G = C_1(G)$ 이다. 또, 양의 정수 i 에 대하여 $N_i \subseteq N$, $N_i \subseteq C_i(G)$ 이라고 가정하면 다음이 성립한다.

$$N_{i+1} = [N_i, G] \subseteq [N, G] \subseteq N,$$

$$N_{i+1} = [N_i, G] \subseteq [C_i(G), G] = C_{i+1}(G)$$

따라서 각 양의 정수 i 에 대하여 $N_i \subseteq N$, $N_i \subseteq C_i(G)$ 이다.

한편, 가정에 의하여 $G\ (\neq \{e\})$ 는 멱영군이므로 적당한 양의 정수 m 에 대하여 $C_m(G) = \{e\}$ 이다. 그런데, $N_m \subseteq C_m(G)$ 이므로 $N_m = \{e\}$ 이다.

(1) 이제 $N_2 = [N, G] = N = N_1$ 이라고 가정하면,

$$N = N_1 = N_2 = \cdots = N_m$$

으로 되어 $N_m = \{e\}$이라는 사실에 모순된다. 따라서 $N_2 = [N, G] \subsetneq N$ 이다.

(2) 정수 k 를 $N_k = \{e\} \subsetneq N_{k-1}$ 인 가장 작은 양의 정수라고 하자.

이 때, $[N_{k-1}, G] = N_k = \{e\}$ 이므로 정리 2.3 에 의하여

$$\{e\} \subsetneq N_{k-1} \subseteq N \cap Z(G)$$

이고 따라서 $\{e\} \subsetneq N \cap Z(G)$ 이다.

특히, $\{e\} \subsetneq G \cap Z(G) = Z(G)$ 이고 따라서 $\{e\} \subsetneq Z(G)$ 이다.

정리 30 군 $G\ (\neq \{e\})$ 가 멱영군일 때, $H \subsetneq G$ 인 G 의 모든 부분군 H 에 대하여 $H \subsetneq N_G(H)$ 이다.

증 명 군 G 를 멱영군이라 하고

$$(*) \qquad G = H_1 \supseteq H_2 \supseteq \cdots \supseteq H_n = \{e\}$$

를 G 의 중심열이라고 하자(정리 22). 또, H 를 $H \subsetneq G$ 인 G 의 부분군이라고 하자. 이 때, $H_n = \{e\} \subseteq H$, $H_1 = G \not\subseteq H$ 이므로 적당한 양의 k 에 대하여 $H_k \subseteq H$, $H_{k-1} \not\subseteq H$ 이다. 그런데, $(*)$ 는 G 의 중심열이므로 $[H_{k-1}, G] \subseteq H_k$ 이고 따라서 정리 23 에 의하여

$$[H_{k-1}, H] \subseteq [H_{k-1}, G] \subseteq H_k \subseteq H$$

이므로 정리 13 에 의하여 $H_{k-1} \subseteq N_G(H)$ 이고 따라서 $H \subsetneq N_G(H)$ 이다.

다음 정리는 유한군이 멱영군이기 위한 필요충분조건을 보여 주고 있다.

정리 31 군 $G\ (\neq \{e\})$ 가 유한군일 때, 다음 조건은 서로 동치이다.

(1) G 는 멱영군이다.

(2) $H \subsetneq G$ 인 G 의 모든 부분군 H 에 대하여 $H \subsetneq N_G(H)$ 이다.

(3) G 의 극대부분군은 모두 G 의 정규부분군이다.

(4) 임의의 素數 p 에 대하여 G 의 Sylow p-부분군은 G 의 정규부분군이다.

(5) G 는 적당한 素數 p 에 대하여 유한 p-군이거나 또는 G 의 Sylow 부분군들의 직적이다.

증 명 (1) $\Longrightarrow$ (2) 정리 30 에 의하여 (1) $\Longrightarrow$ (2) 이다.

(2) $\Longrightarrow$ (3) 조건 (2) 가 성립한다고 가정하고, M을 G의 극대부분군이라고 하자. 이 때, $M \subsetneq G$ 이므로 (2) 에 의하여

$$M \subsetneq N_G(M) \subseteq G$$

이고 M은 G의 극대부분군이므로 $N_G(M) = G$ 이고 따라서 $M \lhd G$ 이다.

(3) $\Longrightarrow$ (4) 조건 (3) 이 성립한다고 가정하고 임의의 素數 p에 대하여 P를 G의 Sylow p-부분군이라고 하자.

이 때, P가 G의 정규부분군이 아니라고 하면, $N_G(P) \subsetneq G$ 이므로 $N_G(P) \subseteq M \subsetneq G$ 인 G의 극대부분군 M이 존재하고 따름정리 6.4.9 에 의하여 $N_G(M) = M$ 이고, 또 조건 (3)에 의하여 $M \lhd G$ 즉 $N_G(M) = G$ 으로 되어 모순이 생긴다. 따라서 $P \lhd G$ 이다.

(4) $\Longrightarrow$ (5) 조건 (4) 가 성립한다고 가정하고, $|G| = p_1^{e_1} \cdots p_r^{e_r}$ 를 $|G|$의 표준분해라고 하자. 그리고, 각 정수 i $(1 \le i \le r)$ 에 대하여 P_i 를 G의 Sylow p_i- 부분군이라고 하자.

먼저 $r = 1$ 이면, $G = P_1$ 이고 G는 유한 p_1-군이다.

다음에 $r \ge 2$ 이라고 하자.

이 때, 각 i $(1 \le i \le r)$ 에 대하여 $P_i \lhd G$, $|P_i| = p_i^{e_i}$ 이다. 특히, $P_1 \lhd G$, $P_2 \lhd G$ 이므로 $P_1P_2 \lhd G$ 이고(정리 2.9.5), 또 $|P_1|$과 $|P_2|$가 서로 소이므로 $P_1 \cap P_2 = \{e\}$, $|P_1P_2| = p_1^{e_1} p_2^{e_2}$ 이다(보기 2.7.6).

이와 같은 논법을 되풀이하면 정수 i $(2 \le i \le r)$ 에 대하여 다음이 성립함을 알 수 있다.

$$P_i \cap P_1 \cdots P_{i-1} = \{e\},$$

$$|P_1 \cdots P_{i-1} P_i| = p_1^{e_1} \cdots p_i^{e_i}$$

따라서 $G = P_1 \dot{\times} \cdots \dot{\times} P_r$ 이다(정리 7.1.3).

(5) $\Longrightarrow$ (1) 유한 p-군은 멱영군이다(정리 8). 그리고, 유한 개의 멱영군의 직적은 멱영군이다(따름정리 28).

따라서 조건 (5) 가 성립하면, G는 멱영군이다.

§7.4.2 고차의 교환자부분군

여기서는 교환자부분군의 개념을 일반화 하기호 한다.

정의 1 군 G 의 원소 $x_1, x_2, \cdots, x_n$ 에 대하여 **高次의 교환자**(交換子, higher commutator) $[x_1, x_2, \cdots, x_n]$ 을 다음과 같이 귀납적으로 정의한다.

$$[x_1, x_2, x_3] = [[x_1, x_2], x_3],$$
$$[x_1, x_2, \cdots, x_n] = [[x_1, x_2, \cdots, x_{n-1}], x_n]$$

마찬가지로, 군 G 의 부분군 $H_1, H_2, \cdots, H_n$ 에 대하여 **고차의 교환자 부분군** $[H_1, H_2, \cdots, H_n]$ 을 다음과 같이 귀납적으로 정의한다.

$$[H_1, H_2, H_3] = [[H_1, H_2], H_3],$$
$$[H_1, H_2, \cdots, H_n] = [[H_1, H_2, \cdots, H_{n-1}], H_n]$$

앞의 정의에서 $[H_1, H_2, \cdots, H_n]$ 는 고차의 교환자

$$[h_1, h_2, \cdots, h_n] \qquad (h_i \in H_i)$$

를 모두 포함하지만, $n \geq 3$ 일 때 이와 같은 고차의 교환자 전체에 의하여 생성된 부분군은 $[H_1, H_2, \cdots, H_n]$ 과 일치하지 않을 수도 있다.

정리 2 군 G 에서 원소 $x, y, z \in G$ 에 대하여 다음이 성립한다.

(1) $[xy, z] = [x, z][x, z, y][y, z]$

(2) $[x, yz] = [x, z][x, y][x, y, z]$

(3) $[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = e$

증명 (1) $[xy, z] = (xy)^{-1}z^{-1}(xy)z = y^{-1}x^{-1}z^{-1}xyz$

$$= y^{-1}x^{-1}z^{-1}x(zyy^{-1}z^{-1})yz$$
$$= y^{-1}(x^{-1}z^{-1}xz)y(y^{-1}z^{-1}yz)$$
$$= y^{-1}[x, z]y[y, z] = [x, z]^y[y, z]$$

(2) $[x, yz] = x^{-1}(yz)^{-1}x(yz) = x^{-1}z^{-1}y^{-1}xyz$

$= x^{-1}z^{-1}(xzz^{-1}x^{-1})y^{-1}xyz$

$= (x^{-1}z^{-1}xz)z^{-1}(x^{-1}y^{-1}xy)z$

$= [x, z]z^{-1}[x, y]z = [x, z][x, y]^z$

(3) $[[x, y^{-1}], z]^y = y^{-1}[x^{-1}yxy^{-1}, z]y$

$= y^{-1}(yx^{-1}y^{-1}x)z^{-1}(x^{-1}yxy^{-1})zy$

$= (x^{-1}y^{-1}xz^{-1}x^{-1})(yxy^{-1}zy)$

$= (xzx^{-1}yx)^{-1}(yxy^{-1}zy)$

앞의 등식에서

$$a = xzx^{-1}yx, \quad b = yxy^{-1}zy, \quad c = zyz^{-1}xz$$

이라고 놓으면, 다음 등식을 얻는다.

$$[[x, y^{-1}], z]^y = a^{-1}b$$

여기서, b 는 a 의 x, y, z 를 순환적으로 y, z, x 로 바꾸어 놓은 식이고 c 는 b 의 x, y, z 를 순환적으로 y, z, x 로 바꾸어 놓은 식이다. 마찬가지로,

$$[[y, z^{-1}], x]^z = b^{-1}c, \quad [[z, x^{-1}], y]^x = c^{-1}a$$

이고, 따라서 다음 등식이 성립한다.

$$[[x, y^{-1}], z]^y[[y, z^{-1}], x]^z[[z, x^{-1}], y]^x$$
$$= a^{-1}bb^{-1}cc^{-1}a = e$$

정리 3 (세 부분군 보조정리) 군 G 의 세 부분군 H, K, L 에 대하여

$$[H, K, L] = \{e\}, \qquad [K, L, H] = \{e\}$$

이면, $[L, H, K] = \{e\}$ 이다.

증 명 이제 $[H, K, L] = \{e\}$, $[K, L, H] = \{e\}$ 이라 가정하고, 또 $x \in H$, $y \in K$, $z \in L$ 를 각각 H, K, L 의 임의의 원소라고 하자. 이때, 가정에 의하여

$$[x, y^{-1}, z] = [y, z^{-1}, x] = e$$

이므로 $[x, y^{-1}, z]^y = [y, z^{-1}, x]^z = e$ 이고 또 정리 2 (3) 에 의하여

$$[x, y^{-1}, z]^{y}[y, z^{-1}, x]^{z}[z, x^{-1}, y]^{x} = e$$

이므로 $[z, x^{-1}, y]^{x} = e$ 이고 따라서 다음이 성립한다.

$$[z, x^{-1}, y] = e$$

그런데, 정의에 의하여 부분군 $[L, H]$ 는

$$[z, x^{-1}] \qquad (z \in L,\ x \in H)$$

와 같은 꼴의 교환자 전체에 의하여 생성된 부분군이고 위의 결과에 의하여 이들 각 생성원은 원소 $z \in K$ 와 교환가능하다.

그러므로 $[L, H]$ 의 모든 원소와 K 의 모든 원소는 서로 교환가능하므로 $[L, H, K] = [[L, H], K] = \{e\}$ 이다.

따름정리 4 군 G 에서 $N \lhd G$ 일 때, G 의 세 부분군 H, K, L 에 대하여

$$[H, K, L] \subseteq N, \qquad [K, L, H] \subseteq N$$

이면, $[L, H, K] \subseteq N$ 이다.

증 명 사상 $\pi : G \longrightarrow G/N$ 를 준동형사상이라고 하자. 이 때,

$$[H, K, L] \subseteq N, \quad [K, L, H] \subseteq N$$

이면,

$$[\pi(H), \pi(K), \pi(L)] = \{\bar{e}\},$$
$$[\pi(K), \pi(L), \pi(H)] = \{\bar{e}\}$$

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[d, dash] & G/N \arrow[d, dash] \\ N & \{N\} \end{tikzcd}$$

이고 따라서 정리 3 에 의하여

$$[\pi(L), \pi(H), \pi(K)] = \{\bar{e}\}$$

이므로 $[L, H, K] \subseteq N$ 이다.

§7.4.3 Lie 다원환

환에서는 곱셈에 관한 결합법칙이 성립하지만, 다음에 정의하는 Lie 환과 Lie 다원환에서는 일반적으로 곱셈에 관한 결합법칙이 성립하지 않는다.

정의 1 덧셈군 L 위에 곱셈 $[\ ,\ ]$ 이 정의되어 있고, 이에 관하여 다음이 성립할 때, L 을 **Lie 환**(Lie ring)이라고 한다.

L.1 : $[x_1+x_2, y] = [x_1, y]+[x_2, y]$

L.2 : $[x, y_1+y_2] = [x, y_1]+[x, y_2]$

L.3 : $[x, x] = 0$

L.4 : $[[x, y], z]+[[y, z], x]+[[z, x], y] = 0$

정의 2 체 F 위의 벡터공간 L 위에 곱셈 $[\ ,\ ]$ 이 정의되어 있고, 이에 관하여 다음이 성립할 때, L 을 **Lie 다원환**(多元環, Lie algebra)이라고 한다.

L.1 : $[x_1+x_2, y] = [x_1, y]+[x_2, y]$,

$[x, y_1+y_2] = [x, y_1]+[x, y_2]$

L.2 : $[ax, y] = [x, ay] = a[x, y] \quad (a \in F,\ x, y \in L)$

L.3 : $[x, x] = 0$

L.4 : $[[x, y], z]+[[y, z], x]+[[z, x], y] = 0$

앞의 두 정의에서 $[x, y]$ 를 x, y 의 **Lie 곱**(Lie product)이라 하고 등식 L.4 를 **야코비 항등식**(Jacobi identity)이라고 한다.

Lie 환과 Lie 다원환에서 임의의 원소 x, y 에 대하여 다음이 성립한다.

$$[x, y] = -[y, x]$$

실제로, L.3 에 의하여

$$\begin{aligned} 0 &= [x+y, x+y] = [x, x]+[x, y]+[y, x]+[y, y] \\ &= [x, y]+[y, x] \end{aligned}$$

이므로 $[x, y] = -[y, x]$ 이다.

보기 1 환 R 에서 임의의 원소 $a, b \in R$ 에 대하여 Lie 곱 $[a, b]$ 를

$$[a, b] = ab - ba$$

로 정의하면, $(R, +, [\ ,\ ])$ 는 Lie 환이다. 실제로, 다음이 성립한다.

$$[a_1 + a_2, b] = (a_1 + a_2)b - b(a_1 + a_2) = a_1 b + a_2 b - ba_1 - ba_2$$
$$= a_1 b - ba_1 + a_2 b - ba_2 = [a_1, b] + [a_2, b]$$
$$[a, b_1 + b_2] = a(b_1 + b_2) - (b_1 + b_2)a = ab_1 + ab_2 - b_1 a - b_2 a$$
$$= ab_1 - b_1 a + ab_2 - b_2 a = [a, b_1] + [a, b_2]$$
$$[a, a] = aa - aa = 0$$
$$[[a, b], c] + [[b, c], a] + [[c, a], b]$$
$$= (ab - ba)c - c(ab - ba) + (bc - cb)a - a(bc - cb)$$
$$+ (ca - ac)b - b(ca - ac)$$
$$= abc - bac - cab - cba + bca - cba - abc - acb$$
$$+ cab - acb - bca - bac = 0$$

마찬가지로, 체 F 위의 다원환 A 에서 임의의 $a, b \in A$ 에 대하여

$$[a, b] = ab - ba$$

로 정의하면, A 는 체 F 위의 Lie 다원환을 이룬다.

보기 2 체 F 위의 n 차의 행렬 전체의 집합 $\mathrm{Mat}_n(F)$ 는 다음과 같이 정의된 연산에 관하여 체 F 위의 n^2 차원 다원환을 이룬다.

$$[a_{ij}]_{n\times n} + [b_{ij}]_{n\times n} = [a_{ij} + b_{ij}]_{n\times n},$$
$$a[a_{ij}]_{n\times n} = [a\,a_{ij}]_{n\times n}$$
$$[a_{ij}]_{n\times n}[b_{ij}]_{n\times n} = [c_{ij}]_{n\times n}, \quad c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \ \ (1 \le i, j \le n)$$

따라서 $\mathrm{Mat}_n(F)$ 에서 임의의 $A, B \in \mathrm{Mat}_n(F)$ 에 대하여 Lie 곱을

$$[A, B] = AB - BA$$

로 정의하면, $\mathrm{Mat}_n(F)$ 는 체 F 위의 Lie 다원환을 이룬다.

유한 단순군의 구조 연구와 분류 문제를 논할 때 단순 Lie 다원환에 관한 정리가 이용된다.