Homework 2

9.34.

σ가 홀수 길이$(= 2k+1)$의 순환치환

$$\sigma = (a_0, a_1, \cdots, a_{2k-1}, a_{2k})$$

라 하자. 그러면 σ^2는 다음과 같다.

$$\sigma^2(a_i) = a_{i+2} \qquad (\text{여기서, } + = +_{2k+1})$$

이를 이용하여 a_0를 포함하는 궤도를 찾으면,

$$a_0 \xrightarrow{\sigma^2} a_2 \xrightarrow{\sigma^2} a_4 \xrightarrow{\sigma^2} \cdots \xrightarrow{\sigma^2} a_{2k} \xrightarrow{\sigma^2} a_1 \xrightarrow{\sigma^2} a_3 \xrightarrow{\sigma^2} \cdots \xrightarrow{\sigma^2} a_{2k-1} \xrightarrow{\sigma^2} a_0$$

이므로,

$$\sigma^2 = (a_0, a_2, \cdots, a_{2k}, a_1, \cdots a_{2k})$$

이고, 이는 두 원소 이상을 포함하는 궤도가 많아야 하나 뿐이므로 순환치환이다.

10.40.

임의의 원소 $a \in G$에 대해서 G의 부분순환군 $\langle a \rangle$을 생각하자. $|\langle a \rangle| = k$라 하면, 순환군의 성질에 의해 $a^k = e$라는 것을 안다. 여기서 $|G| < \infty$이고, $\langle a \rangle \leq G$이므로 Lagrange 정리를 이용하면,

$$\begin{aligned} |\langle a \rangle| \,\Big|\, |G| &\iff k \mid n \\ &\iff \exists q \in \mathbb{Z} \mid (n = kq) \end{aligned}$$

인 것을 알 수 있다. 따라서,

$$a^n = a^{kq} = \left(a^k\right)^q = e^q = e$$

이다.

결론. 모든 $a \in G$에 대해서

$$a^n = e$$

임을 알 수 있다.

10.45.

먼저 위수가 n인 유한순환군을 G라고 하면, $\exists a \in G \mid \langle a \rangle = G$이다. G의 항등원은 e라고 하자. 그러면, $a^k = e$를 만족하는 가장 작은 양의 자연수 k는 n이다. 이를 이용하면

$$G = \left\{a^0 = e, a^1, \cdots, a^{n-1}\right\}$$

임을 알 수 있다.

이제 다음 두 명제를 증명하자.

1. n의 각 약수 d를 위수로 갖는 부분군이 존재한다.

$k = \frac{n}{d}$라 하면,

$$k = \frac{n}{d} \implies k \mid n$$

이다. 이를 이용하여 $\langle a^k \rangle$의 위수를 생각해보면,

$$\left|\langle a^k \rangle\right| = \frac{n}{\gcd(n,k)} = \frac{n}{k} = d$$

인 것을 확인 할 수 있다.

따라서, 모든 n의 약수 d에 대해, d를 위수로 갖는 부분군은

$$\langle a^{\frac{n}{d}} \rangle$$

로 존재한다. □

예시로 $d = n$인 경우에는 $\langle a^{\frac{n}{n}} \rangle = \langle a \rangle = G$를 생각할 수 있고, $d = 1$인 경우에는 $\langle a^{\frac{n}{1}} \rangle = \langle e \rangle = \{e\}$를 생각할 수 있다.

2. 위 부분군들이 모든 부분군이다.

G의 임의의 부분군 H이 모두 1.의 부분군꼴로 표현됨을 보이자.

먼저 H가 순환군임을 보이자.
H가 부분군이므로 $e \in H$이고, 이제 H의 위수에 따라서 Case를 나누어서 생각하겠다.

Case 1. $|H| = 1$

$$H = \{e\} = \langle e \rangle = \langle a^0 \rangle$$

이므로, H는 순환군이다.

Case 2. $|H| > 1$

$|H| > 1$이므로 $|H| \ \{e\} \geq 1$이다. 따라서,

$$\exists m \in \mathbb{N} \mid a^m \in H, m < n$$

이다. 따라서 $a^m \in H$를 만족하는 가장 작은 자연수 m을 p를 생각할 수 있다. 그러면 $a^1, a^2, \cdots, a^{p-1} \notin H$이고 $a^p \in H$이다. 먼저 $H \supset \langle a^p \rangle$이다.

이제 임의의 $k \in \mathbb{Z} \mid a^k \in H$를 생각하자. 나눗셈 알고리즘을 이용하여 k를 p로 나누면

$$k = pq + r \qquad (0 \leq r < p)$$

이다. 그러므로

$$a^r = a^{pq-k} = (a^p)^q (a^k)^{-1} \in H$$

이고, $a^r \in H, 0 \leq r < p$ 이고 p가 $a^m \in H$를 만족하는 가장 작은 자연수 m이므로 $r = 0$이다. 즉, 임의의 $k \in \mathbb{Z} \mid a^k \in H$를 만족하는 k에 대해

$$k = pq \iff p \mid k$$

이다. 그러므로, $H \supset \langle a^p \rangle$이다.

따라서, $H = \langle a^p \rangle$이므로, H은 순환군이다.

결론. Case 1, Case 2인 경우 모두에 대해 H는 순환군이므로, 순환군 G의 임의의 부분군 H는 순환군이다. □

G의 임의의 부분군 H는 순환군이므로

$$H = \langle a^s \rangle$$

꼴로 나타낼 수 있음을 안다. 이제 $d = |H|$라 하면,

$$d = |H| = |\langle a^s \rangle| = \frac{n}{\mathtt{gcd}(n, s)}$$

이다. 여기서 자연스럽게 $d \mid n$을 알 수 있고, $k = \frac{n}{d}$라 하면

$$\begin{aligned}\mathtt{gcd}(n, s) = \frac{n}{d} &\iff \mathtt{gcd}(n, s) = \mathtt{gcd}(n, k) \\ &\iff \langle a^s \rangle = \langle a^k \rangle\end{aligned}$$

이므로, 1.의 부분군 꼴로 나타낼 수 있다. 따라서 $|H|$가 d인 부분군을 유일하게 존재한다.

위에서 $d \mid n$인 d에 대해서 $|H| = d$를 만족하는 부분군 H가 유일하게 존재하는 것을 증명하였으며, $d \nmid n$인 경우에는 Lagrange 정리에 의해서 $|H| = d$를 만족하는 부분군 H가 존재하지 않음을 안다. 따라서, G가 갖는 부분군들은 n의 각 약수 d를 갖는 유일한 부분군들 뿐임을 알 수 있다.

10.46.

10.45.와 비슷하게 시작하겠다.
먼저 위수가 n인 유한순환군을 G라고 하면, $\exists a \in G \mid \langle a \rangle = G$이다. G의 항등원은 e라고 하자. 그러면, $a^k = e$를 만족하는 가장 작은 양의 자연수 k는 n이다. 이를 이용하면

$$\begin{aligned}G &= \{a^0 = e, a^1, \cdots, a^{n-1}\} \\ &= \{a^1, \cdots, a^{n-1}, a^n = e\}\end{aligned}$$

임을 알 수 있다.

이제 G의 각각의 원소 a^i $(1 \leq i \leq n)$가 생성하는 부분군을 생각해보자.

$$d = \mathtt{gcd}(n, i)$$

라고 하면,

$$\begin{aligned}\mathtt{gcd}(n, i) = d &\iff \mathtt{gcd}(n, \frac{n}{d}) \\ &\iff \langle a^i \rangle = \langle a^{\frac{n}{d}} \rangle\end{aligned}$$

이므로, a^i가 10.45.에서 보인 위수가 d인 유일하게 존재하는 부분군의 생성원임을 알 수 있다. 즉, a^i $(1 \leq i \leq n)$는 $\langle a^{\frac{n}{\mathtt{gcd}(n,i)}} \rangle$의 생성원이다.

이제 세는 입장을 바꾸자. G의 모든 부분군들의 생성원의 개수는 $n = |G|$일 것이다. 10.45.에서 보인 위수가 d인 유일하게 존재하는 부분군을$\langle a^{\frac{n}{d}} \rangle$라고 하였으므로,

$$n = \sum_{d \mid n} (\langle a^{\frac{n}{d}} \rangle \text{의 생성원의 개수})$$

이다. $\langle a^{\frac{n}{d}} \rangle \sim \mathbb{Z}_d$이고 $\mathbb{Z}_d$의 생성원의 개수는 $\phi(d)$로 알려져 있으므로,

$$\begin{aligned}(\langle a^{\frac{n}{d}} \rangle \text{의 생성원의 개수}) &= (\mathbb{Z}_d \text{의 생성원의 개수}) \\ &= \phi(d)\end{aligned}$$

이다. 이를 이용하면

$$\begin{aligned}n &= \sum_{d \mid n} (\langle a^{\frac{n}{d}} \rangle \text{의 생성원의 개수}) \\ &= \sum_{d \mid n} \phi(d)\end{aligned}$$

이다.

11.6.

$\mathbb{Z}_n$에서 m의 위수는 $\frac{n}{\mathtt{gcd}(n,m)}$이다. 그러므로, $\mathbb{Z}_4$에서 3의 위수는 4, $\mathbb{Z}_{12}$에서 10의 위수는 6, $\mathbb{Z}_{15}$에서 9의 위수는 5이다.

$(a_1, a_2, \cdots, a_n) \in \prod_{i=1} nG_i$이고, r_i가 G_i에서 a_i의 위수라고 하면, $\prod_{i=1} nG_i$에서 $(a_1, a_2, \cdots, a_n)$의 위수는 모든 r_i의 최소공배수이므로,

$$\mathbb{Z}_3 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15} \text{에서} (3, 10, 9) \text{의 위수} = \mathtt{lcm}(4, 6, 9) = 36$$

이다.

11.11.

$\mathbb{Z}_2 \times \mathbb{Z}_4$에서 위수가 4인 원소를 찾으면,

$$(0, 1), (0, 3), (1, 1), (1, 3)$$

이다. 이들로 생성된 부분군들이 위수가 4인 모든 부분군이므로,

$$\begin{aligned}\langle (0, 1) \rangle = \langle (0, 3) \rangle &= \{0\} \times \mathbb{Z}_4 \\ \langle (1, 1) \rangle = \langle (1, 3) \rangle &= \{(0, 0), (1, 1), (0, 2), (1, 3)\}\end{aligned}$$

이다.

11.50.

a.

G의 임의의 원소 $(a,b) \in G$를 생각해보자.

$$\begin{aligned} \exists (a,e_K) \in & H \times \{e\}, (e_H, b) \in e \times K, \\ (a,b) =& (he_H, e_K k) \\ =& (a,e_K) \times (e_H, b) \end{aligned}$$

이므로, 적당한 $h \in H, k \in K$에 대해 $(a,b) = hk$로 나타내진다.

b.

임의의 원소 $h = (a,e_K) \in H, k = (e_H, b) \in K$에 대해서

$$hk = (a,e_K)(e_H,b) = (e_H a, be_K) = (e_H,b)(a,e_K) = kh$$

가 성립함을 알 수 있다.

c.

$\alpha : G \to H, \alpha((a,b)) = a$라 하고, $\beta : G \to K, \beta((a,b)) = b$라 하자.

$$\begin{aligned} x \in H \cap K &\iff x \in H \text{ and } x \in K \\ &\iff \beta(x) = e_K \text{ and } \alpha(x) = e_H \\ &\iff x = (e_H, e_K) = e \end{aligned}$$

이므로 성립한다.

11.52.

먼저 유한가환군은 유한개의 원소를 가지므로, 유한 생성된다고 할 수 있다. 즉, 유한가환군 G에 대해서 유한생성가환군의 기본정리를 사용하면,

$$G \simeq \mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

의 형태로 순환군의 직접곱과 동형이다. 여기서 p_i는 소수이지만 서로 다를 필요는 없고, r_i들은 양의 정수이다. 그 직접곱은 인수들의 가능한 재배열을 제외하면 유일하다. 여기서 G는 유한군이므로, 인수 $\mathbb{Z}$의 개수는 0개일 것이다. 즉, 유한가환군은

$$G = \prod_{i=1}^{n} \mathbb{Z}_{(p_i)^{r_i}} \qquad (p_i\text{는 소수, } r_i\text{는 양의 정수})$$

의 형태로 나타낼 수 있다.

본 문제의 증명 G가 유한 가환군일 때,

$$G\text{가 순환군이 아니다.} \iff \exists p, \exists H \le G \mid H \simeq \mathbb{Z}_p \times \mathbb{Z}_p$$

를 보이는 것은

$$G\text{가 순환군이다.} \iff \forall p, \forall H \le G \mid H \nsim \mathbb{Z}_p \times \mathbb{Z}_p$$

($\nsim$은 "동형이 아니다"를 의미한다.)

이다. 따라서 이를 증명해보자.

($\Longrightarrow$) G가 유한 가환군이고 순환군이므로,

$$\forall H \le G \mid H\text{는 순환군}$$

이다. (10.45.에서 증명하였고, 책에서도 증명되어있다.)

그러나 $\mathbb{Z}_p \times \mathbb{Z}_p$은 순환군이 아니다.

pf. [귀류법] 만약 $\mathbb{Z}_p \times \mathbb{Z}_p$가 순환군이라고 가정하면,

$$\mathbb{Z}_p \times \mathbb{Z}_p = \langle (a,b) \rangle$$

이고, $|\mathbb{Z}_p \times \mathbb{Z}_p| = p^2$이므로,

$$k(a,b) = (0,0)$$

을 만족하는 최소의 양의 정수 k는 p^2이어야 한다. 그러나

$$p(a,b) = (pa,pb) = (0,0)$$

이므로 모순이다. 따라서, $\mathbb{Z}_p \times \mathbb{Z}_p$은 순환군이 아니다. □

따라서 G의 임의의 부분군 H는 순환적이므로 순환군이 아닌 $\mathbb{Z}_p \times \mathbb{Z}_p$와는 동형일 수 없다.

($\Longleftarrow$) G가 유한 가환군이므로,

$$G \simeq \prod_{i=1}^{n} \mathbb{Z}_{(p_i)^{r_i}} \qquad (p_i\text{는 소수, } r_i\text{는 양의 정수})$$

꼴로 나타낼 수 있다.

먼저 $i \neq j \implies p_i \neq p_j$임을 보이자.

pf. [귀류법] 만약 $i \neq j, p_i = p_j$인 i,j가 존재한다고 가정하자. 일반성을 잃지않고, $i = 1, j = 2$라고 생각하고, $p_1 = p_2 = p$라 하면,

$$G \simeq \mathbb{Z}_{(p)^{r_1}} \times \mathbb{Z}_{(p)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \tag{1}$$

이므로, $\mathbb{Z}_{(p)^{r_1}}$의 부분군 $\langle p^{r_1-1} \rangle \simeq \mathbb{Z}_p$와 $\mathbb{Z}_{(p)^{r_2}}$의 부분군 $\langle p^{r_2-1} \rangle \simeq \mathbb{Z}_p$ 다음 부분군 H을 생각하면,

$$H = \langle p^{r_1-1} \rangle \times \langle p^{r_2-1} \rangle \times \langle 0 \rangle \times \langle 0 \rangle \times \cdots \times \langle 0 \rangle$$

$H \simeq \mathbb{Z}_p \times \mathbb{Z}_p$임을 알 수 있다. 이를 만족하는 부분군 H가 존재하지 않는다는 것에 모순되므로, $i \neq j, p_i \neq p_j$이다. □

그러면 G는 서로 다른 소수 $p_1, p_2, \cdots, p_n$에 대해

$$G \simeq \prod_{i=1}^{n} \mathbb{Z}_{(p_i)^{r_i}} \qquad (r_i\text{는 양의 정수})$$

꼴로 나타낼 수 있고, $i \neq j \implies \texttt{gcd}((p_i)^{r_i}, (p_j)^{r_j}) = 1$이므로, 11.6. 따름정리에의해,

$$G \simeq \prod_{i=1}^{n} \mathbb{Z}_{(p_i)^{r_i}} = \mathbb{Z}_X \qquad (X = \textstyle\prod_{i=1}^{n} (p_i)^{r_i})$$

이다. 여기서 $G \simeq \mathbb{Z}_X$은 순환군이다.

13.44.

$|G| < \infty$일 때,

$$\phi[G] = \{\phi(g) \mid g \in G\}$$

라 하면, $\phi : G \to \phi[G]$는 onto 함수이므로, $|\phi[G]| \le |G| < \infty$ 이므로 $|\phi[G]|$는 유한이다.

$$H = \mathrm{Ker}(\phi)$$

라 하자. 일단 $|H| < \infty$이다.

$$\forall g \in G, gH = \{x \in G \mid \phi(x) = \phi(g)\}$$

이다.

$$\forall g \in G, |H| = |gH| \tag{1}$$

임을 보이겠다.

pf. 함수 $\mu : H \to gH$를 생각하면, 임의의 $gh_1, gh_2 \in gH$에 대해

$$gh_1 = gh_2 \iff h_1 = h_2$$

이므로 1-1함수 이고, 임의의 $z \in gH$에 대해

$$\mu(g^{-1}z) = z$$

이므로 onto이다. 즉, μ는 일대일 대응이다. 따라서, $|H| = |gH|$ 라 할 수 있다. □

$$S = \{aH \mid a \in G\}$$

를 생각하면, (1)을 이용하여

$$|G| = |S|\,|H|$$

이므로,

$$|S| \,\Big|\, |G| \tag{2}$$

이다. 이제 $\alpha : S \to \phi[G]$, $\alpha(gH) = \phi(g)$로 정의하고, α가 Well-Defined이고 일대일대응임을 보이자.

위에서 $gH = \{x \in G \mid \phi(g) = \phi(x)\}$이므로, 임의의 $a, b \in gH$에 대해 $\phi(a) = \phi(b) = \phi(x)$이므로 대표값으로 $\phi(g)$을 사용해도 문제가 없다. 즉, Well-Defined이다.

$\forall \phi(x), \phi(y) \in \phi[G]$에 대해

$$\begin{aligned}\phi(x) = \phi(y) &\iff \phi^{-1}[\{\phi(x)\}] = \phi^{-1}[\{\phi(y)\}] \\ &\iff xH = yH\end{aligned}$$

이므로 1-1이고, $\forall \phi(x) \in \phi[G]$에 대해

$$\alpha(xH) = \phi(x)$$

이므로 onto이다. 따라서 α는 일대일 대응이다.

따라서,

$$|S| = |\phi[G]| \tag{3}$$

이다.

(2), (3)에 의해서

$$|\phi[G]| \,\Big|\, |G|$$

이다.

13.45.

$\phi : G \to G'$이 군의 준동형사상이므로, G가 군일때 $\phi(G) \subset G'$도 군이다. 그러므로, $\phi(G) \le G'$이고, $|G'| < \infty$이므로 Lagrange 정리에 의해서

$$|\phi(G)| \,\Big|\, |G'|, |\phi(G)| < \infty$$

임을 알 수 있다.

13.47.

준동형사상 $\phi : G \to G'$에 대해

$$H = \mathtt{Ker}(\phi)$$

라 하면, $H \le G$이다. $|G| = p < \infty$이므로, Lagrange 정리에 의해서

$$|H| \,\Big|\, |G| = p \qquad (p\text{는 소수})$$

이므로, $|H| = 1$ or p이다. $p > 1$이므로 다음 두 Case 중 하나이다.

Case 1. $|H| = p$

$$|H| = |G| = p, H \le G \implies H = G$$

이다. 따라서 모든 $g \in G$에 대해,

$$\phi(g) = e'$$

이므로 ϕ는 자명 준동형사상이다. 이 때, $|G| > 1$이므로 서로 다른 임의의 원소 $a, b \in G$에 대해 $\phi(a) = \phi(b) = e$이므로 ϕ는 일대일함수가 아니다.

Case 2. $|H| = 1$

$e \in H$인 것을 상기하면, $H = \{e\}$이다. 이제 임의의 원소 $g \in G$에 대해 $\phi(g)$에 대응하는 원소는 오직 좌잉여류

$$a\{e\} = \{a\}$$

이다. 따라서, ϕ는 일대일 준동형사상이다. 이 때, $|G| > 1$이므로 e가 아닌 원소 $a \in G$가 존재하여 $\phi(a) \neq \phi(e) = e'$이므로 ϕ는 자명 준동형사상이 아니다.

따라서, $|G|$가 소수이면, 준동형사상 $\phi : G \to G'$은 자명 준동형사상이거나 일대일 사상 중의 하나이다.

14.8.

$|\langle(1,1)\rangle|$은 순환군이므로,

$$|\langle(1,1)\rangle| \text{은 } k(1,1) = (0,0)\text{을 만족하는 최소 자연수}$$

이다. $k(1,1) = (0,0)$일 k의 조건을 찾아보자. 첫 번째 원소가 0이 되기 위해서는 $1 \in \mathbb{Z}_{11}$을 11의 배수만큼 더해야한다. 즉, $11 \mid k$이다. 비슷하게 두 번째 원소가 0이 될 조건은 $1 \in \mathbb{Z}_{15}$을 15의 배수만큼 더해야한다. 따라서 $15 \mid k$이다. 따라서, $165 \mid k$이고 이 조건을 만족하는 최소 자연수 k은 165이다. 따라서,

$$|\langle(1,1)\rangle| = 165$$

이다.

그러면 $|\langle(1,1)\rangle| = |\mathbb{Z}_{11} \times \mathbb{Z}_{15}| = 165$이고,

$$\langle(1,1)\rangle \leq \mathbb{Z}_{11} \times \mathbb{Z}_{15}$$

이므로,

$$\langle(1,1)\rangle = \mathbb{Z}_{11} \times \mathbb{Z}_{15}$$

이다. 따라서, $\mathbb{Z}_{11} \times \mathbb{Z}_{15}/\langle(1,1)\rangle \simeq \{e\}$이고,

$$|\mathbb{Z}_{11} \times \mathbb{Z}_{15}/\langle(1,1)\rangle| = 1$$

이다.

14.34.

주어진 위수 n에 대해 유일한 부분군 H를 생각하자.

$\forall g \in G, gHg^{-1}$**는 군이며,** $\left|gHg^{-1}\right| = |H|$**이다.**

0. 닫힘 임의의 $gag^{-1}, gbg^{-1} \in gHg^{-1}$에 대해

$$\begin{aligned}(gag^{-1})(gbg^{-1}) &= gag^{-1}gbg^{-1} \\ &= gabg^{-1} \in gHg^{-1} \qquad (ab \in H)\end{aligned}$$

이므로 연산이 gHg^{-1}안에 닫혀있다.

1. 결합법칙 임의의 $gag^{-1}, gbg^{-1}, gcg^{-1} \in gHg^{-1}$에 대해

$$\begin{aligned}(gag^{-1}gbg^{-1})gcg^{-1} &= (gabg^{-1})gcg^{-1} \\ &= gabcg^{-1} \\ &= gag^{-1}(gbcg^{-1}) \\ &= gag^{-1}(gbg^{-1}gcg^{-1})\end{aligned}$$

이므로, 결합법칙이 성립한다.

2. 항등원 $e \in H$이므로, $e = geg^{-1} \in gHg^{-1}$이다. e는 G의 항등원이므로, gHg^{-1}에서도 항등원의 역할을 한다.

3. 역원 임의의 $gxg^{-1} \in gHg^{-1}$에 대해

$$gxg^{-1}g(x^-1)g^{-1} = e = g(x^{-1})g^{-1}gxg^{-1}$$

이므로, 역원인 $g(x^{-1})g^{-1} \in gHg^{-1}$가 존재한다. ($\because x^{-1} \in H$)

따라서, gHg^{-1}는 군이다.

$\phi : H \to gHg^{-1}$인 $\phi(x) = gxg^{-1}$를 생각하면,
임의의 $gag^{-1}, gbg^{-1} \in gHg^{-1}$에 대해

$$gag^{-1} = gbg^{-1} \iff ga = gb \iff a = b$$

이므로 1-1이고, 임의의 $a \in gHg^{-1}$에 대해

$$\exists b = g^{-1}ag \in H, \phi(b) = g(g^{-1}ag)g^{-1} = a$$

이므로 onto이다. 따라서 ϕ는 일대일대응 함수이고 이는

$$|H| = \left|gHg^{-1}\right|$$

를 의미한다.

$n = |H| = \left|gHg^{-1}\right|$이고 위수가 n인 부분군은 H로 유일하므로,

$$\forall g \in G \mid gHg^{-1} = H$$

이다. 따라서 H는 G의 정규부분군이다.

15.12.

$N = \langle(3,3,3)\rangle$라 하면, 임의의 $(x,y,z) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$에 대해

$$(0,a,b) + N \text{ or } (1,a,b) + N \text{ or } (2,a,b) + N \qquad (a, b \in \mathbb{Z})$$

중 하나로 표현 가능하다. 또한

$$(\{0\} \times \mathbb{Z} \times \mathbb{Z} + N)\dot{\bigcup}(\{1\} \times \mathbb{Z} \times \mathbb{Z} + N)\dot{\bigcup}(\{2\} \times \mathbb{Z} \times \mathbb{Z} + N) = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$$

이므로

$$\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}/\langle(3,3,3)\rangle \simeq \mathbb{Z}_3 \times \mathbb{Z} \times \mathbb{Z}$$

이다.

15.14.

중심

$\mathbb{Z}_3$은 가환군이므로, $\mathbb{Z}_3$의 중심은 $\mathbb{Z}_3$이다.

S_3의 원소는 다음 6개이다.

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \rho_1 = (1,2,3), \rho_2 = (1,3,2)$$
$$\mu_1 = (2,3), \mu_2 = (3,1), \mu_3 = (1,2)$$

S의 중심을 $Z(S)$라 하면, $\rho_0 \in Z(S)$이고, (항등원)

$$\begin{cases} \rho_1\mu_1 = \mu_3 \\ \mu_1\rho_1 = \mu_2 \end{cases} \begin{cases} \rho_2\mu_2 = \mu_3 \\ \mu_2\rho_2 = \mu_1 \end{cases} \begin{cases} \mu_2\mu_3 = \rho_1 \\ \mu_3\mu_2 = \rho_2 \end{cases}$$

이므로, $\rho_1, \rho_2, \mu_1, \mu_2, \mu_3 \notin Z(S)$이다. 따라서

$$Z(S) = \{\rho_0\}$$

이다.

직접곱의 연산은 각각의 군의 연산들로 이루어져 있으므로,
$\mathbb{Z}_3 \times S_3$의 중심은

$$\mathbb{Z}_3 \times \{\rho_0\}$$

이다.

교환자부분군
$\mathbb{Z}_3$은 가환군이므로, $\mathbb{Z}_3$의 교환자부분군은 $\{0\}$이다.

S_3의 교환자부분군을 $C(S_3)$라 하자, $\rho_2\mu_1\rho_2^{-1}\mu_1^{-1} = \phi_1$이므로
$C(S_3) \geq A_3$이다. 또한, S_3/A_3은 가환이므로 $C \leq A_3$이다.

따라서 $C(S_3) = A_3$이다.

직접곱의 연산은 각각의 군의 연산들로 이루어져 있으므로,
$\mathbb{Z}_3 \times S_3$의 교환자부분군은

$$\{0\} \times A_3$$

이다.