Homework 1

3.26.

함수 $\phi : S \to S'$은 1-1, onto 이므로, 역함수 $\phi^{-1} : S' \to S'$(1-1, onto)가 존재한다. 그러므로, 임의의 $x', y' \in S'$에 대하여

$$\exists x, y \in S | x = \phi^{-1}(x'), y = \phi^{-1}(y')$$

이를 이용하면,

$$\begin{aligned}\phi^{-1}(x') * \phi^{-1}(y') =& x * y \\ =& \phi^{-1}(\phi(x * y)) \\ =& \phi^{-1}(\phi(x) *' \phi(y)) \quad (\phi\text{는 동형사상}) \\ =& \phi^{-1}(x' *' y')\end{aligned}$$

따라서, ϕ^{-1}은 $< S', *' >$에서 $< S, * >$위로의 동형사상이다.

3.27.

$\psi \circ \phi$은 전단사함수의 합성함수이므로 전단사함수이다. 모든 $x, y \in S$에 대해서,

$$\begin{aligned}\psi \circ \phi(x * y) =& \psi(\phi(x) *' \phi(y)) \qquad (\phi\text{가 동형사상}) \\ =& \psi \circ \phi(x) *'' \psi \circ \phi(y) \qquad (\psi\text{가 동형사상})\end{aligned}$$

따라서, $\psi \circ \phi$은 $< S, * >$에서 $< S'', *'' >$ 위로의 동형사상이다.

3.33.

a.

$$\phi(a + bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

ϕ는 전단사함수이다. 임의의 $x = a + bi, y = c + di \in \mathbb{C}$에 대해

$$\begin{aligned}\phi(x + y) =& \phi((a + c) + (b + d)i) \\ =& \begin{bmatrix} a + c & -b - d \\ b + d & a + c \end{bmatrix} \\ =& \begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \\ =& \phi(x) + \phi(y)\end{aligned}$$

따라서, $< \mathbb{C}, + >$와 $< \mathbb{H}, + >$는 동형이다.

b.

$$\phi(a + bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

ϕ는 전단사함수이다. 임의의 $x = a + bi, y = c + di \in \mathbb{C}$에 대해

$$\begin{aligned}\phi(x \cdot y) =& \phi((ac - bd) \cdot (bc + ad)i) \\ =& \begin{bmatrix} (ac - bd) & -(bc + ad) \\ (bc + ad) & (ac - bd) \end{bmatrix} \\ =& \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \\ =& \phi(x) \cdot \phi(y)\end{aligned}$$

따라서, $< \mathbb{C}, \cdot >$와 $< \mathbb{H}, \cdot >$는 동형이다.

4.29.

$\forall a \in G, a * a \neq e$라면, $\exists b \in G, a * b = b * a = e$이다.

또한, $b \neq c$인 $b, c \in G$에 대해 $a * b = a * c = e$일 수 없다.

짝수개의 원소를 갖는 군 G에 대해서, 만일 $a * a = e$를 만족하는 G의 원소 $a \neq e$가 존재하지 않는다면, 위 두 성질에 의해서 e를 제외한 홀수개의 원수가 짝을 이뤄야한다. 이는 불가능하므로 $a * a = e$를 만족하는 G의 원소 a가 존재한다.

4.30.

a.

$a, b, c \in R^*$에 대해 $(a * b) * c = a * (b * c)$임을 보이자.

$$\begin{aligned}(a * b) * c =& (|a|b) * c \\ =& ||a|b|\, c \\ =& |a||b|c \\ =& |a|(b * c) \\ =& a * (b * c)\end{aligned}$$

b.

$e = 1$ or -1이면 $e * a = a$이다.

$a > 0$이면 $a * 1 = a$이고, $a < 0$라면 $a * -1 = a$이다.

c.

결합법칙은 성립하지만, 모든 원소에 대한 공통된 항등원 e가 존재하지 않는다.

따라서 R^*는 이 이항연산을 갖는 군이 될 수 없다.

d.

각 원소에 대한 항등원이 존재하더라도, 모든 원소의 공통된 항등원이 아니라면 군이 될 가능성은 없다.

4.31.

$$\begin{aligned} x * x =& x \\ x^{-1} * x * x =& x^{-1} * x \\ e * x =& e \\ x =& e \end{aligned}$$

따라서, $x = e$이고 군에서 항등원은 유일하다.

4.32.

$$\begin{aligned} (a * b) * (a * b) =& e \\ a * (b * a) * b =& e \\ b * a =& a^{-1} * b^{-1} \\ b * a =& a * b \end{aligned}$$

따라서, $\forall x \in G | x * x = e$인 군 G은 가환이다.

4.37.

$$\begin{aligned} (b * c * a) * (b * c * a) =& b * c * (a * b * c) * a \\ =& b * c * a \end{aligned}$$

이다. 따라서, 4.31.에 의해

$$b * c * a = e$$

이다.

4.39.

1. *은 결합법칙이 성립한다.

2. $\forall x \in G | \exists e \in G, e * x = x$

pf. 어떤 $a \in G$에 대해, $\exists e \in G, e * a = a$이다.

$\forall x \in G, \exists y \in G | a * y = x$이므로
$e * a * y = a * y$
$\forall x \in G, e * x = x$

3. $\forall a \in G | \exists a^{-1} \in G, a^{-1} * a = e$

좌공리 1, 2, 3이 성립하면 군이다.

pf.

$$\begin{aligned} (a * a^{-1}) * (a * a^{-1}) &= a * (a^{-1} * a) * a^{-1} \\ &= (a * a^{-1}) \end{aligned}$$

이므로, 4.31.에 의해 $a * a^{-1} = e$이다.

또,

$$\begin{aligned} a * e =& a * (a^{-1} * a) \\ =& (a * a^{-1}) * a \\ =& e * a \\ =& a \end{aligned}$$

이므로, 좌공리 1, 2, 3이 성립하면 군이다. □

따라서, 집합 G은 군이다.

5.34.

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$A^2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$A^3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

$$A^4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I$$

위수는 4이다.

5.42.

동형사상이므로, ϕ는 전단사함수이다.

성질 1. $e_{G'} = \phi(e_G)$

$$\begin{aligned} \phi(x) =& \phi(e_G * x) \\ =& \phi(e_G) * \phi(x) \end{aligned}$$

$\therefore e_{G'} = \phi(e_G)$

성질 2. $\phi(a^{-1}) = \phi(a)^{-1}$

$$\begin{aligned} e_{G'} =& \phi(a * a^{-1}) \\ =& \phi(a) * \phi(a^{-1}) \end{aligned}$$

$\therefore \phi(a^{-1}) = \phi(a)^{-1}$

성질 3. $\forall n \in \mathbb{Z} | \phi(a^n) = \phi(a)^n$

1. $n = 0$인 경우

$\phi(a^0) = \phi(e_G) = e_{G'} = \phi(a)^0$ 이므로 성립한다.

2. $n = k$가 성립한다고 가정하고 $n = k+1$인 경우에 성립하는지 보자.

$$\begin{aligned} \phi(a^{k+1}) =& \phi(a * a^k) \\ =& \phi(a) *' \phi(a^k) \\ =& \phi(a) *' \phi(a)^k \\ =& \phi(a)^{k+1} \end{aligned}$$

이므로, 성립한다.

3. $n = k$가 성립한다고 가정하고 $n = k-1$인 경우에 성립하는지 보자.

$$\begin{aligned} \phi(a^{k-1}) =& \phi(a^{-1} * a^k) \\ =& \phi(a^{-1}) *' \phi(a^k) \\ =& \phi(a)^{-1} *' \phi(a)^k \\ =& \phi(a)^{k-1} \end{aligned}$$

이므로, 성립한다.

$\therefore \forall n \in \mathbb{Z} | \phi(a^n) = \phi(a)^n$이다.

결론 동형사상 ϕ가 존재하면, $G = \{a^n | n \in \mathbb{Z}\}$일 때, $G' = \{\phi(a)^n | n \in \mathbb{Z}\}$이다.

따라서, G가 순환적이면 G'도 순환적이다.

5.49.

귀류법 만약, $a^n = e$가 되는 $n \in \mathbb{Z}^+$가 존재하지 않는다고 가정하자. 그러면 $x, y \in \mathbb{Z}, x > y$인 x, y에 대해 $a^x \neq a^y$이다. 왜냐하면 $a^{x-y} \neq e$이기 때문이다.

$\therefore |\langle a \rangle| = \infty$

하지만, $\langle a \rangle \leq G$이고, $|G| < \infty$이므로 모순이다.

따라서, $\forall a \in G, \exists n \in \mathbb{Z}^+ | a^n = e$

5.57.

대우명제 순환군이 아닌 군은 비자명 진부분군을 갖는다.

순환군이 아닌 군을 G라고 하자. G는 항등원 e를 제외한 다른 원소를 적어도 하나 가진다. 없다면 $G = \{e\} = \langle e \rangle$이기 때문이다.

$a \in G, a \neq e$인 a에 대해 $\langle a \rangle \neq G$이다.

그리고 G는 a를 포함하는 군이므로, $\langle a \rangle \leq G$이다.

$\langle a \rangle < G$이므로, $\langle a \rangle$은 G의 비자명 진부분군이다. □

따라서, 비자명 진부부군을 갖지 않는 군은 순환군이다.

6.48.

전체 군을 G라고 하자. 유한개의 부분군 중 순환부분군들에 대해 생각하자. 순환부분군의 개수는 유한개(=k개)이고, 각각을

$$\langle a_1 \rangle, \langle a_2 \rangle, ..., \langle a_k \rangle$$

라 하자.

$$\bigcup_{i=1}^{k} \langle a_i \rangle = G\text{임을 보이자.}$$

pf. $\langle a_i \rangle$은 각각 G의 순환부분군이므로,

$$\bigcup_{i=1}^{k} \langle a_i \rangle \subset G \qquad (1)$$

임의의 $x \in G$에 대해 $\langle x \rangle$도 G의 순환부분군이므로, 어떤 $1 \leq y \leq k, y \in \mathbb{N}$가 존재하여

$$\langle x \rangle = \langle a_y \rangle$$

이다. 따라서, $\forall x \in G, \langle x \rangle \subset \bigcup_{i=1}^{k} \langle a_i \rangle$이므로

$$\bigcup_{i=1}^{k} \langle a_i \rangle \supset G \qquad (2)$$

(1), (2)에 의해 $\bigcup_{i=1}^{k} \langle a_i \rangle = G$이다. □

$\forall i \in \{1, 2, ..., k\}, \langle a_i \rangle$가 무한군이 아님을 보이자.

pf. 귀류법 어떤 $y \in \{1, 2, ..., k\}$가 존재하여 $\langle a_y \rangle$가 무한군인 순환부분군이라고 가정하자. $\langle a_y \rangle$의 위수는 무한인 순환군이므로 $\langle \mathbb{Z}, + \rangle$와 동형이고, 이는 무한히 많은 부분수환군을 갖는다. 따라서 $\langle a_y \rangle$은 무한히 많은 부분순환군을 가지며, 이들은 또한 G의 부분순환군이다.

하지만, G의 부분순환군은 k개로 유한하므로 불가능하다. 따라서, $\forall i \in \{1, 2, ..., k\}, \langle a_i \rangle$은 무한군이 아니다. □

결론 따라서, G은 k개의 위수가 유한한 부분순환군의 합집합이므로 유한군이다.

6.52.

$\mathbb{Z}_n$의 생성원의 개수는 n과 서로소인 $1 \le i \le n, i \in \mathbb{N}$의 개수와 같다. 즉, $\phi(n)$이다.

$\phi(p^r) = (p-1)p^{r-1}$이므로, $\mathbb{Z}_{p^r}$의 생성원의 개수는 $(p-1)p^{r-1}$이다.

6.55.

$\forall i \in \mathbb{N}, 1 \le i < p$에 대해 $\gcd(i,p) = 1$이므로,

$$\langle i \rangle = \langle 1 \rangle = \mathbb{Z}_p$$

이다. 따라서, $0 \in \mathbb{Z}_p$을 제외한 원소를 포함하는 군은 $\mathbb{Z}_p$가 될 수 밖에 없다. 그러므로, p가 소수이면 $\mathbb{Z}_p$는 비자명 진부분군을 갖지 않는다.

8.12.

$\{1, 2, 4, 3\}$

8.44.

$|D_n| = 2n$이다.

회전이동들로만 이루어진 치환(ρ_i)들은 군이며, 위수가 n이다.

8.45.

양 면의 중심을 연결하는 직선 기준으로 회전하는 부분군은 위수가 4이며, 직선은 총 3개 존재한다. 따라서, 적어도 위수가 4인 3개의 부분군을 갖는다.

대각선을 기준으로 회전하는 부분군은 위수가 3이며, 대각선은 총 4개 존재한다. 따라서, 적어도 위수가 3인 4개의 부분군을 갖는다.

또한 맞은편 선분의 두 중심을 연결하는 직선 기준으로 회전하는 부분군은 위수가 2이며, 직선은 총 6개 존재한다. 따라서, 적어도 위수가 2인 6개의 부분군을 갖는다.

이 군의 위수는 $(4-1) \times 3 + (3-1) \times 4 + (2-1) \times 6 + 1 = 24$이다.

(1)

$\phi : \mathbb{Z} \to n\mathbb{Z}$를 $\phi(i) = ni$로 정의하자.

1. ϕ는 전단사함수이다. 왜냐하면

$$\begin{aligned} \phi(i) &= \phi(j) \\ \Rightarrow ni &= nj \\ \Rightarrow i &= j \end{aligned}$$

이므로 단사함수이고,

$$\forall x \in n\mathbb{Z}, \exists k = \frac{x}{n} \in \mathbb{Z} \mid \phi(k) = x$$

이므로 전사함수이기 때문이다.

2. $\forall x, y \in \mathbb{Z} \mid \phi(x+y) = \phi(x) + \phi(y)$이다.

$\forall x, y \in \mathbb{Z}$에 대하여

$$\begin{aligned} \phi(x+y) =& n(x+y) \\ =& nx + ny \\ =& \phi(x) + \phi(y) \end{aligned}$$

따라서, $\langle \mathbb{Z}, + \rangle \simeq \langle n\mathbb{Z}, + \rangle$이다.

(2)

$x, y \in V$에 대해 binary operation $*$을

$$*(x,y) = \frac{x \cdot y}{2}$$

로 정의하자.

이제 $\langle V, * \rangle$이 Group인지 확인하자.

0. 닫혀있다. $\forall x, y \in V$에 대해, $x * y \in \mathbb{C}^*$이고

$$\begin{aligned} |x * y| =& \left| \frac{x \cdot y}{2} \right| \\ =& \frac{|x|\,|y|}{|2|} \\ =& 2 \end{aligned}$$

이므로 V는 $*$에 의해 닫혀있다.

1. 결합법칙 성립

$\forall a, b, c \in V$에 대하여

$$\begin{aligned} (a * b) * c =& \frac{a \cdot b}{2} * c \\ =& \frac{\frac{a \cdot b}{2} \cdot c}{2} \\ =& \frac{a \cdot \frac{b \cdot c}{2}}{2} \\ =& a * \frac{b \cdot c}{2} \\ =& a * (b * c) \end{aligned}$$

가 성립한다.

2. 항등원 존재 $\exists e = 2$에 대해 $\forall x \in Z \mid x * e = e * x = x$이다.

3. 역원 존재 $\forall x \in Z, \exists x^{-1} = \frac{4}{x} \mid x * x^{-1} = x^{-1} * x = e$이다.

따라서, $\langle V, * \rangle$은 Group이다. □

$\langle U, \cdot \rangle$와 $\langle V, * \rangle$가 동형임을 보이자.

$\phi : U \to V$를 $x \in U \mid \phi(x) = 2x$로 정의하자.

1. ϕ는 전단사함수이다. 왜냐하면

$$\begin{aligned} &\phi(i) = \phi(j) \\ \Rightarrow &2i = 2j \\ \Rightarrow &i = j \end{aligned}$$

이므로 단사함수이고,

$$\forall x \in V, \exists k = \frac{x}{2} \in U \mid \phi(k) = x$$

이므로 전사함수이기 때문이다.

2. $\forall x, y \in U \mid \phi(x \cdot y) = \phi(x) * \phi(y)$이다.

$\forall x, y \in U$에 대하여

$$\begin{aligned} \phi(x \cdot y) =& 2(x \cdot y) \\ =& \frac{2x \cdot 2y}{2} \\ =& (2x * 2y) \\ =& \phi(x) * \phi(y) \end{aligned}$$

이다.

따라서, $\langle U, \cdot \rangle$와 $\langle V, * \rangle$는 동형이다. □

(3)

$\forall \sigma \in \mathrm{Aut}(G), \sigma$는 전단사함수이며, $\forall x, y \in G, \phi(x \cdot y) = \phi(x) \cdot \phi(y)$가 성립한다.

(a) $\langle \mathbf{Aut}(G), \circ \rangle$이 Group인지 확인하자.

0. 닫혀있다. $\forall x, y \in \mathrm{Aut}(G)$에 대해 $x \circ y$은 두 전단사함수의 합성이므로 전단사함수이다.

또한, $\forall a, b \in G$에 대하여

$$\begin{aligned} (x \circ y)(a \cdot b) =& x(y(a \cdot b)) \\ =& x(y(a) \cdot y(b)) \\ =& x(y(a)) \cdot x(y(b)) \\ =& (x \circ y)(a) \cdot (x \circ y)(b) \end{aligned}$$

이다. 그러므로, $(x \circ y) \in \mathrm{Aut}(G)$이다.

따라서, $\mathrm{Aut}(G)$은 연산 $\circ$에 의해 닫혀있다.

1. 결합법칙 성립 함수의 합성연산은 결합법칙이 성립하므로, $\mathrm{Aut}(G)$에서 연산 $\circ$의 결합법칙은 성립힌다.

2. 항등원 존재 $e : G \to G \mid x \in G, e(x) = x$로 생각하면, $\forall \sigma \in \mathrm{Aut}(G)$에 대하여

$$e \circ \sigma = \sigma \circ e = \sigma$$

이다.

3. 역원 존재 $\forall \sigma \in G$에 대해 σ는 전단사함수이므로 역함수 σ^{-1}가 존재한다.

$$\sigma^{-1} \circ \sigma = \sigma \circ \sigma^{-1} = e$$

이다.

따라서, $\langle \mathrm{Aut}(G), \circ \rangle$은 Group이다.

(b) Find Aut($\mathbb{Z}_{12}$)

아래 풀이에서 곱셈은 mod12로의 곱셈을 의미한다.

$\forall \sigma \in \mathrm{Aut}(\mathbb{Z}_{12})$

$\mathbb{Z}_{12} = \langle 1 \rangle = \{n1 \mid n \in \mathbb{Z}\}$

By σ, $\mathbb{Z}_{12} = \langle \sigma(1) \rangle = \{n\sigma(1) \mid n \in \mathbb{Z}\}$

$\sigma(n1) = n\sigma(1)$이므로,

$$\sigma(x) = ax \qquad\qquad (a = \sigma(1))$$

꼴의 함수임을 알 수 있다.

$\gcd(a, 12) \neq 1$인 경우에는 σ가 전사함수가 아니게 되므로, $\gcd(a, 12) = 1$이다. 가능한 $\sigma(1) = a$는 $1, 5, 7, 11$이 있다. 이 a들에 대해서는 σ는 전단사함수이고,

$$\begin{aligned} \sigma(x +_{12} y) =& a(x +_{12} y) \\ =& ax +_{12} ay \\ =& \sigma(x) +_{12} \sigma(y) \end{aligned}$$

이므로 가능한 동형사상이다.

따라서,

$$\begin{aligned} \mathrm{Aut}(\mathbb{Z}_{12}) = \{&\sigma_1 : \mathbb{Z}_{12} \to \mathbb{Z}_{12} \mid \sigma_1(x) = x, \\ &\sigma_2 : \mathbb{Z}_{12} \to \mathbb{Z}_{12} \mid \sigma_2(x) = 5x, \\ &\sigma_3 : \mathbb{Z}_{12} \to \mathbb{Z}_{12} \mid \sigma_3(x) = 7x, \\ &\sigma_4 : \mathbb{Z}_{12} \to \mathbb{Z}_{12} \mid \sigma_4(x) = 11x\} \end{aligned}$$