Solutions 02

1. Let X be any set. The identity map $\mathrm{id}_X : X \to X$ is defined, for all x in X, by $x \mapsto x$ and the projection $\pi_1 : X \times X \to X$ is defined, for all x and y in X, by $(x, y) \mapsto x$. For any two maps $\varphi : X \to X$ and $\psi : X \to X$, the map $\varphi \,||\, \psi : X \to X \times X$ is defined, for all x in X, by $x \mapsto \big(\varphi(x), \psi(x)\big)$ and the map $\varphi \times \psi : X \times X \to X \times X$ is defined, for all x and y in X, by $(x, y) \mapsto \big(\varphi(x), \psi(y)\big)$. For the one-element set $\{\varnothing\}$, there exists a unique map $\eta : X \to \{\varnothing\}$ defined, for all x in X, by $\eta(x) = \varnothing$.

Suppose that the set X is nonempty and consider three maps $\beta : X \times X \to X$, $\varepsilon : \{\varnothing\} \to X$, and $\iota : X \to X$ satisfying the following three conditions:

(associativity) $\quad \beta \circ (\beta \times \mathrm{id}_X) = \beta \circ (\mathrm{id}_X \times \beta)$
(right identity) $\quad \beta \circ (\mathrm{id}_X \times \varepsilon) = \mathrm{id}_X \circ \pi_1$
(right inverse) $\quad \beta \circ (\mathrm{id}_X \,||\, \iota) = \varepsilon \circ \eta$

Prove that the quadruple $(X, \beta, \varepsilon, \iota)$ defines a group.

Solution. The conditions assert that the diagrams

$$
\begin{array}{ccc}
X \times X \times X & \xrightarrow{\beta \times \mathrm{id}_X} & X \times X \\
{\scriptstyle \mathrm{id}_X \times \beta}\downarrow & & \downarrow{\scriptstyle \beta} \\
X \times X & \xrightarrow[\beta]{} & X
\end{array}
\qquad
\begin{array}{ccc}
X \times \{\varnothing\} & \xrightarrow{\mathrm{id}_X \times \varepsilon} & X \times X \\
{\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \beta} \\
X & \xrightarrow[\mathrm{id}_X]{} & X
\end{array}
\qquad
\begin{array}{ccc}
X & \xrightarrow{\mathrm{id}_X \,||\, \iota} & X \times X \\
{\scriptstyle \eta}\downarrow & & \downarrow{\scriptstyle \beta} \\
\{\varnothing\} & \xrightarrow[\varepsilon]{} & X
\end{array}
$$

commute. For any elements x and y in X, define the binary operator $\star : X \times X \to X$ by $x \star y := \beta(x, y)$. The first condition implies that, for any elements x, y, and z in X, we have

$$
\begin{aligned}
(x \star y) \star z = \beta(x \star y, z) &= \beta\big(\beta(x, y), z\big) \\
&= \big(\beta \circ (\beta \times \mathrm{id}_X)\big)(x, y, z) \\
&= \big(\beta \circ (\mathrm{id}_X \times \beta)\big)(x, y, z) \\
&= \beta\big(x, \beta(y, z)\big) = \beta(x, y \star z) = x \star (y \star z)\,,
\end{aligned}
$$

which gives the associativity of this binary operator. Set $e := \varepsilon(\varnothing)$. The second condition implies that, for any x in X, we have

$$x \star e = \beta\big(x, \varepsilon(\varnothing)\big) = \big(\beta \circ (\mathrm{id}_X \times \varepsilon)\big)(x, \varnothing) = \big(\mathrm{id}_X \circ \pi_1\big)(x, \varnothing) = \mathrm{id}_X\big(\pi_1(x, \varnothing)\big) = x\,,$$

which shows that the element e in X is a right identity for this associative binary operator. The third condition implies that, for any x in X, we have

$$x \star \iota(x) = \big(\beta \circ (\mathrm{id}_X \,||\, \iota)\big)(x) = (\varepsilon \circ \eta)(x) = \varepsilon\big(\eta(x)\big) = \varepsilon(\varnothing) = e\,,$$

which proves that the element $\iota(x)$ in X is a right inverse for the element x. Using the right inverse $\iota^2(x)$ in X of the element $\iota(x)$ in X, we obtain

$$x = x \star e = x \star \big(\iota(x) \star \iota^2(x)\big) = \big(x \star \iota(x)\big) \star \iota^2(x) = e \star \iota^2(x)\,.$$

For any x in X, it follows that $e \star x = e \star \big(e \star \iota^2(x)\big) = (e \star e) \star \iota^2(x) = e \star \iota^2(x) = x$, so the element e is a two-sided identity for this binary operator. Moreover, we see that $x = e \star \iota^2(x) = \iota^2(x)$, which demonstrates that $e = \iota(x) \star \iota^2(x) = \iota(x) \star x$.

Hence, the element $x^{-1} := \iota(x)$ is a two-sided inverse of the element x. Therefore, the quadruple $(X, \beta, \varepsilon, \iota)$ defines a group. $\square$

2. For any nonnegative integer n, the ***sign function*** $\operatorname{sgn} \colon \mathfrak{S}_n \to \mu_2 := \{\pm 1\}$ is defined by $\operatorname{sgn}(\sigma) := (-1)^{n-c}$ where the permutation σ is the product of c disjoint cycles.

i. For any permutation σ and any transposition ϖ, prove $\operatorname{sgn}(\varpi\,\sigma) = -\operatorname{sgn}(\sigma)$.

ii. For any permutations σ and τ, show that $\operatorname{sgn}(\sigma\,\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$.

iii. When the permutation σ is the product of m transpositions, demonstrate that $\operatorname{sgn}(\sigma) = (-1)^m$.

Solution.

i. Let $\varpi = (a\ b)$ and let $\sigma = \omega_1\,\omega_2\,\cdots\,\omega_c$ be the factorization of the permutation into disjoint cycles. When a and b both appear in one cycle ω_j where $1 \leqslant j \leqslant c$, we have

$$\varpi\,\omega_j = (a\ b)(a\ c_1\ c_2\ \cdots\ c_r\ b\ d_1\ d_2\ \cdots\ d_s) = (a\ c_1\ c_2\ \cdots\ c_r)(b\ d_1\ d_2\ \cdots\ d_s)$$

and $\varpi\,\sigma$ factors into $c+1$ disjoint cycles. We deduce that

$$\operatorname{sgn}(\varpi\,\sigma) = (-1)^{n-(c+1)} = (-1)(-1)^{n-c} = -\operatorname{sgn}(\sigma)\,.$$

On the other hand, when a and b appear in disjoint cycles of σ, there exists indices i and j such that $\omega_i = (a\ c_1\ c_2\ \cdots\ c_r)$ and $\omega_j = (b\ d_1\ d_2\ \cdots\ d_s)$. It follows that

$$\varpi\,\omega_i\,\omega_j = (a\ b)(a\ c_1\ c_2\ \cdots\ c_r)(b\ d_1\ d_2\ \cdots\ d_s) = (a\ c_1\ c_2\ \cdots\ c_r\ b\ d_1\ d_2\ \cdots\ d_s)$$

and $\varpi\,\sigma$ factors into $c-1$ disjoint cycles. We deduce that

$$\operatorname{sgn}(\varpi\,\sigma) = (-1)^{n-(c-1)} = (-1)(-1)^{n-c} = -\operatorname{sgn}(\sigma)\,.$$

ii. Let $\sigma = \varpi_1\,\varpi_2\,\cdots\,\varpi_m$ be a factorization of σ into transpositions. We proceed by induction on m. The base case $m = 0$ is vacuous. The case $m = 1$ is precisely part *i.* Using the part *i* twice and the induction hypothesis, we obtain

$$\begin{aligned}\operatorname{sgn}(\sigma\,\tau) &= \operatorname{sgn}(\varpi_1\,\varpi_2\,\varpi_3\,\cdots\,\varpi_m\,\tau)\\ &= -\operatorname{sgn}(\varpi_2\,\varpi_3\,\cdots\,\varpi_m\,\tau)\\ &= -\operatorname{sgn}(\varpi_2\,\varpi_3\,\cdots\,\varpi_m)\operatorname{sgn}(\tau)\\ &= \operatorname{sgn}(\varpi_1\,\varpi_2\,\varpi_3\,\cdots\,\varpi_m)\operatorname{sgn}(\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)\,.\end{aligned}$$

iii. The factorization of a transposition ϖ_i in $\mathfrak{S}_n$ into disjoint cycles consists of 1 cycle of length 2 and $n-2$ cycles of length 1, so $\operatorname{sgn}(\varpi_i) = (-1)^{n-(n-1)} = -1$. Part *ii* implies that

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\varpi_1\,\varpi_2\,\cdots\,\varpi_m) = \operatorname{sgn}(\varpi_1)\operatorname{sgn}(\varpi_2)\cdots\operatorname{sgn}(\varpi_m) = (-1)^m\,. \qquad \square$$

3. The ***quaternion group*** is the subgroup of $\mathrm{SL}(2,\mathbb{C})$ generated by the eight matrices:

$$\mathbf{I} := \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \quad \mathbf{A} := \begin{bmatrix}\mathrm{i} & 0\\ 0 & -\mathrm{i}\end{bmatrix}, \quad \mathbf{B} := \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}, \quad \mathbf{C} := \begin{bmatrix}0 & \mathrm{i}\\ \mathrm{i} & 0\end{bmatrix},$$

$$-\mathbf{I} := \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}, \quad -\mathbf{A} := \begin{bmatrix}-\mathrm{i} & 0\\ 0 & \mathrm{i}\end{bmatrix}, \quad -\mathbf{B} := \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}, \quad -\mathbf{C} := \begin{bmatrix}0 & -\mathrm{i}\\ -\mathrm{i} & 0\end{bmatrix}.$$

i. Determine the order of the quaternion group.

ii. Find a minimal set of generators for the quaternion group.
iii. Show that the quaternion group is not isomorphic to the dihedral group D_4.

Solution.

i. All products in the quaternion group appear in Figure 1. It follows that this group has order 8.

$\star$	$\mathbf{I}$	$-\mathbf{I}$	$\mathbf{A}$	$-\mathbf{A}$	$\mathbf{B}$	$-\mathbf{B}$	$\mathbf{C}$	$-\mathbf{C}$
$\mathbf{I}$	$\mathbf{I}$	$-\mathbf{I}$	$\mathbf{A}$	$-\mathbf{A}$	$\mathbf{B}$	$-\mathbf{B}$	$\mathbf{C}$	$-\mathbf{C}$
$-\mathbf{I}$	$-\mathbf{I}$	$\mathbf{I}$	$-\mathbf{A}$	$\mathbf{A}$	$-\mathbf{B}$	$\mathbf{B}$	$-\mathbf{C}$	$\mathbf{C}$
$\mathbf{A}$	$\mathbf{A}$	$-\mathbf{A}$	$-\mathbf{I}$	$\mathbf{I}$	$\mathbf{C}$	$-\mathbf{C}$	$\mathbf{B}$	$-\mathbf{B}$
$-\mathbf{A}$	$-\mathbf{A}$	$\mathbf{A}$	$\mathbf{I}$	$-\mathbf{I}$	$-\mathbf{C}$	$\mathbf{C}$	$-\mathbf{B}$	$\mathbf{B}$
$\mathbf{B}$	$\mathbf{B}$	$-\mathbf{B}$	$-\mathbf{C}$	$\mathbf{C}$	$-\mathbf{I}$	$\mathbf{I}$	$\mathbf{A}$	$-\mathbf{A}$
$-\mathbf{B}$	$-\mathbf{B}$	$\mathbf{B}$	$\mathbf{C}$	$-\mathbf{C}$	$\mathbf{I}$	$-\mathbf{I}$	$-\mathbf{A}$	$\mathbf{A}$
$\mathbf{C}$	$\mathbf{C}$	$-\mathbf{C}$	$\mathbf{B}$	$-\mathbf{B}$	$-\mathbf{A}$	$\mathbf{A}$	$-\mathbf{I}$	$\mathbf{I}$
$-\mathbf{C}$	$-\mathbf{C}$	$\mathbf{C}$	$-\mathbf{B}$	$\mathbf{B}$	$\mathbf{A}$	$-\mathbf{A}$	$\mathbf{I}$	$-\mathbf{I}$

Figure 1. Multiplication table for the quaternion group

ii. Since $\mathbf{A}^0 = \mathbf{I}$, $\mathbf{A}^1 = \mathbf{A}$, $\mathbf{A}^2 = -\mathbf{I}$, $\mathbf{A}^3 = -\mathbf{A}$, $\mathbf{B}^0 = \mathbf{I}$, $\mathbf{B}^1 = \mathbf{B}$, $\mathbf{B}^2 = -\mathbf{I}$, $\mathbf{B}^3 = -\mathbf{B}$, $\mathbf{A}\mathbf{B} = \mathbf{C}$, and $\mathbf{B}\mathbf{A} = -\mathbf{C}$, the two elements $\mathbf{A}$ and $\mathbf{B}$ generate the quaternion group. From Figure 1, we also see that the quaternion group is not cyclic.

iii. By definition, the dihedral group D_4 is the automorphism group of a square. It is isomorphic to the subgroup of $\mathrm{SL}(2, \mathbb{R})$ generated the matrices

$$\mathbf{T} := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad \text{and} \qquad \mathbf{R} := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The cyclic subgroups of the quaternion group are

$$\langle \mathbf{I} \rangle = \{\mathbf{I}\}, \quad \langle \mathbf{A} \rangle = \langle -\mathbf{A} \rangle = \{\mathbf{I}, \mathbf{A}, -\mathbf{I}, -\mathbf{A}\}, \quad \langle \mathbf{C} \rangle = \langle -\mathbf{C} \rangle = \{\mathbf{I}, \mathbf{C}, -\mathbf{I}, -\mathbf{C}\},$$
$$\langle -\mathbf{I} \rangle = \{\mathbf{I}, -\mathbf{I}\}, \quad \langle \mathbf{B} \rangle = \langle -\mathbf{B} \rangle = \{\mathbf{I}, \mathbf{B}, -\mathbf{I}, -\mathbf{B}\},$$

whereas the cyclic subgroups in D_4 are

$$\langle \mathbf{R}^2 \rangle = \{\mathbf{I}\}, \quad \langle \mathbf{T}^2 \rangle = \{\mathbf{I}, \mathbf{T}^2\}, \quad \langle \mathbf{T}^2\mathbf{R} \rangle = \{\mathbf{I}, \mathbf{T}^2\mathbf{R}\}, \quad \langle \mathbf{T} \rangle = \langle \mathbf{T}^3 \rangle = \{\mathbf{I}, \mathbf{T}, \mathbf{T}^2, \mathbf{T}^3\},$$
$$\langle \mathbf{R} \rangle = \{\mathbf{I}, \mathbf{R}\}, \quad \langle \mathbf{T}\mathbf{R} \rangle = \{\mathbf{I}, \mathbf{T}\mathbf{R}\}, \quad \langle \mathbf{T}^3\mathbf{R}^2 \rangle = \{\mathbf{I}, \mathbf{T}^3\mathbf{R}\}.$$

Since the quaternion group has 6 elements of order 4 and the dihedral group D_4 has 2 elements of order 4, they cannot be isomorphic. Alternatively, the quaternion group and the dihedral group D_4 have maximal cyclic subgroups of different orders, so they cannot be isomorphic. □