## I.2.3 **The group $S_3$**

a) Compile the group table for the symmetric group $S_3$. Is $S_3$ abelian?

b) Find all subgroups of $S_3$. Which of these are abelian?

(7 points)

**Solution**

a) The elements of $S_3$ are

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \; , \; P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \; , \; P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \; , \; P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \; , \; P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \; , \; P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

1pt

With this representation, the group table reads

| | $P_1$ | $P_2$ | $P_3$ | $P_4$ | $P_5$ | $P_6$ |
|---|---|---|---|---|---|---|
| $P_1$ | $P_1$ | $P_2$ | $P_3$ | $P_4$ | $P_5$ | $P_6$ |
| $P_2$ | $P_2$ | $P_1$ | $P_5$ | $P_6$ | $P_3$ | $P_4$ |
| $P_3$ | $P_3$ | $P_4$ | $P_1$ | $P_2$ | $P_6$ | $P_5$ |
| $P_4$ | $P_4$ | $P_3$ | $P_6$ | $P_5$ | $P_1$ | $P_2$ |
| $P_5$ | $P_5$ | $P_6$ | $P_2$ | $P_1$ | $P_4$ | $P_3$ |
| $P_6$ | $P_6$ | $P_5$ | $P_4$ | $P_3$ | $P_2$ | $P_1$ |

$S_3$ is not abelian: E.g., $P_2 \circ P_3 = P_5$, but $P_3 \circ P_2 = P_4$. 1pt

b) Consider the group table from part a), and consider subsets of $S_3$ that contain

- 5 elements: $\{P_2, P_3, P_4, P_5, P_6\}$ does not contain $E = P_1$.
  $\{P_1, P_3, P_4, P_5, P_6\}$ is not closed since $P_3 \circ P_4 = P_2$.
  The other 4 candidates are not closed either. 1pt
- 4 elements: The subset must contain $P_1 \Rightarrow$ We need to conider only
  $\{P_1, P_2, P_3, P_4\}$ is not closed since $P_2 \circ P_3 = P_5$.
  $\{P_1, P_2, P_3, P_5\}$ is not closed since $P_3 \circ P_2 = P_4$.
  $\{P_1, P_2, P_4, P_5\}$ is not closed since $P_4 \circ P_2 = P_3$.
  $\{P_1, P_3, P_4, P_5\}$ is not closed since $P_3 \circ P_4 = P_2$.
  The other 6 candidates are not closed either. 1pt
- 3 elements: Consider $\{P_1, P_4, P_5\}$, whose group table is

| | $P_1$ | $P_4$ | $P_5$ |
|---|---|---|---|
| $P_1$ | $P_1$ | $P_4$ | $P_5$ |
| $P_4$ | $P_4$ | $P_5$ | $P_1$ |
| $P_5$ | $P_5$ | $P_1$ | $P_4$ |

  This is an abelian subgroup!

  Whereas, $\{P_1, P_2, P_3\}$ is not closed since $P_2 \circ P_3 = P_5$,
  and the same for the other 8 candidates. 1pt
- 2 elements: $\{P_1, P_2\}$, $\{P_1, P_3\}$, and $\{P_1, P_6\}$ are abelian subgroups, whereas
  $\{P_1, P_4\}$ and $\{P_1, P_5\}$ are not closed. 1pt
- 1 element: $\{P_1\}$ trivially is an abelian subgroup, none of the other elements are. 1pt

**Summary:** The subgroups of $S_3$ are $\{P_1, P_4, P_5\}$, $\{P_1, P_2\}$, $\{P_1, P_3\}$, $\{P_1, P_6\}$, $\{P_1\}$.
They all are abelian.

I.2.4 **Subgroups**

Let $(G, \vee)$ be a group and let $H \subset G$ with $H \neq \emptyset$. Show that $H$ is a subgroup of $G$ if and only if $a, b \in H$ implies $a \vee b^{-1} \in H$.

(5 points)

**Solution**

We first show that the condition is sufficient, i.e., that $a, b \in H \;\Rightarrow a \vee b^{-1} \in H$ implies that H is a subgroup. 1pt

Suppose $a, b \in H$. Then $a \vee b^{-1} \in H$ since $H$ is a group.
In particular, $b = a \in H$ implies $a \vee a^{-1} = e \in H$
and if $a = e$, then $e \vee b^{-1} = b^{-1} \in H$ (*).
So the requirements **iii.** (existence of a neutral element) and **iv.** (existence of an inverse) from ch. I §2.1 Def. 1 are fulfilled. 1pt
Also, requirement **ii.** (associativity) is fulfilled since $G$ and $H$ share the associative operation $\vee$.

Now consider $a \vee b = a \vee (b^{-1})^{-1} \in H$, since from (*) we know that $b^{-1} \in H$ if $b \in H$.
So requirement **i.** (closure) is fulfilled.

Now we have shown that $H$ is a group, i.e., the condition is sufficient. 1pt

Next we show that the condition is necessary, i.e., that $a, b \in H \;\not\Rightarrow a \vee b^{-1} \in H$ implies that $H$ is not a subgroup. 1pt

Suppose $\exists a, b \in H$ such that $a \vee b^{-1} \notin H$.
In order for $H$ to be a group, $b \in H$ must imply $b^{-1} \in H$.
Now we have $a, b^{-1} \in H$, but $a \vee b^{-1} \notin H$.
Thus requirement i (closure) is violated, and hence $H$ is not a group. 1pt

Now we have shown that the condition is necessary, which completes the proof.

**I.3.1. Fields**

a) Show that the set of rational numbers $\mathbb{Q}$ forms a commutative field under the ordinary addition and multiplication of numbers.

b) Consider a set $F$ with two elements, $F = \{\theta, e\}$. On $F$, define an operation "plus" (+), about which we assume nothing but the defining properties

$$\theta + \theta = \theta \quad , \quad \theta + e = e + \theta = e \quad , \quad e + e = \theta$$

Further, define a second operation "times" ($\cdot$), about which we assume nothing but the defining properties

$$\theta \cdot \theta = e \cdot \theta = \theta \cdot e = \theta \quad , \quad e \cdot e = e$$

Show that with these definitions (and **no** additional assumptions), $F$ is a field.

(7 points)

**Solution**

a) $\mathbb{Q}$ is a group under addition with neutral element $0 \in \mathbb{Q}$:

(i) $q_1 + q_2 \in \mathbb{Q} \; \forall \; q_1, q_2 \in \mathbb{Q}$
(ii) Addition of rational numbers is associative and commutative
(iii) The number zero is an element of $\mathbb{Q}$, and $0 + q = q \; \forall \; q \in \mathbb{Q}$
(iv) Let $q \in \mathbb{Q}$. Then $\exists - q \; : \; q + (-q) = 0$. 1pt

Furthermore, $\mathbb{Q} \setminus \{0\}$ is a group under multiplication:

(i) $q_1 q_2 \in \mathbb{Q} \; \forall \; q_1, q_2 \in \mathbb{Q}$
(ii) Multiplication of rational numbers is associative and commutative
(iii) The number 1 is an element of $\mathbb{Q}$, and $1 \cdot q = q \; \forall \; q \in \mathbb{Q}$
(iv) Let $q \in \mathbb{Q} \setminus \{0\}$. Then $\exists q^{-1} \equiv 1/q \; : \; q \cdot q^{-1} = 1$

Finally, ordinary addition and multiplication on $\mathbb{Q}$ are distributive. $\Rightarrow \mathbb{Q}$ is a commutative field.

1pt

b) We need to show that $F$ is a group under addition.

(i) $a + b \in F \; \forall \; a, b \in F$ by definition $\Rightarrow$ Closure ✓
(ii) $(\theta + e) + \theta = e + \theta = e = \theta + (e + \theta)$
$(e + e) + \theta = \theta + \theta = \theta = e + (e + \theta)$
$\Rightarrow$ "+" is associative 1pt
(iii) $\theta$ is the neutral element by definition
(iv) $-\theta = \theta$ and $-e = e$ by definition $\Rightarrow$ existence of an inverse ✓
(v) "+" is commutative by definition

$\Rightarrow F$ is an abelian group under "+" 1pt

We also need to show that $F \setminus \{\theta\}$ is a group under the multiplication "$\cdot$". But $F \setminus \{\theta\} = \{e\}$, and hence the group axioms are all fulfilled by definition. 1pt

Finally, we need to check the distributive laws. Since the multiplication is abelian we only need to show that

$$(a+b)\cdot c = a\cdot c + b\cdot c \;\forall a,b,c \in F \qquad (*)$$

(i) $c = \theta \Rightarrow (a+b)\cdot c = (a+b)\cdot\theta = a\cdot c + a\cdot b \;\forall\; a,b \in F$ 1pt

(ii) $c = e$. If either $a = \theta$ or $b = \theta$, $(*)$ holds.
If $a = b = e$, then $(e+e)\cdot e = \theta\cdot e = \theta$
and $e\cdot e + e\cdot e = \theta + \theta = \theta$

$\Rightarrow$ The distributive laws hold

$\Rightarrow$ $F$ is a field. 1pt

### I.4.1 Function space

Consider the set $C$ of continuous functions $f : [0,1] \to \mathbb{R}$. Show that by suitably defining an addition on $C$, and a multiplication with real numbers, one can make $C$ an additive vector space over $\mathbb{R}$.

(2 points)

### Solution

On $C$, define

$$(f+g)(x) : -f(x) + g(x)$$

If $f$ and $g$ are continuous, then so is the such defined $f+g$. $\Rightarrow$ Closure ✓

Furthermore, since $f(x) \in \mathbb{R}$, $C$ inherits all other group properties of $(\mathbb{R}, +)$.

$\Rightarrow C$ is an additive group. 1pt

Now define multiplication with scalars $\lambda \in \mathbb{R}$ by

$$(\lambda f)(x) := \lambda\, f(x)$$

If $f$ is continuous, then so is the such defined $(\lambda f)$.

Furthermore, since $\lambda \in \mathbb{R}$ and $f(x) \in \mathbb{R}$, this multiplication with scalars is bilinear and associative, as it inherits these properties from $\mathbb{R}$ under ordinary addition and multiplication of numbers.

Finally,

$$(1\, f)(x) = 1\, f(x) = f(x) \qquad \forall\, x \in [0,1] \qquad \Rightarrow \qquad 1\, f = f$$

$\Rightarrow C$ is an $\mathbb{R}$-vector space. 1pt