1) Let $f_1, f_2 \in S_4$ be defined as:

$$f_1: \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 4 \\ 4 \mapsto 3 \end{array} \qquad\qquad f_2: \begin{array}{l} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \\ 4 \mapsto 4 \end{array}$$

(a) Find $f_2 \circ f_1$ and f_2^{-1}. [Your answer should be given in the same form as f_1 and f_2 are given above.]

Solution.

$$f_2 \circ f_1: \begin{array}{l} 1 \mapsto f_2(f_1(1)) = f_2(2) = 1 \\ 2 \mapsto f_2(f_1(2)) = f_2(1) = 3 \\ 3 \mapsto f_2(f_1(3)) = f_2(4) = 4 \\ 4 \mapsto f_2(f_1(4)) = f_2(3) = 2 \end{array} \qquad\qquad f_2^{-1}: \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \\ 4 \mapsto 4 \end{array}$$

□

(b) Find the 4×4 matrix M_{f_2} associated to f_2. [You do not need to justify this one.]

Solution.

$$M_{f_2} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

□

(c) Find $\text{sign}(f_2)$.

Solution.

$$\text{sign}(f_2) = \det M_{f_2} = \begin{vmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} = -1 \cdot \begin{vmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{vmatrix} = -1 \cdot (-1) = 1.$$

□

2) Let G be a group and $a \in G$. Prove that the subset

$$C_a(G) \stackrel{\text{def}}{=} \{x \in G \;:\; ax = xa\}$$

is a *subgroup* of G.

[**Note:** $C_a(G)$ is *not* the center of G. The center has all elements of G that commute with *every* other element of G, while $C_a(G)$ has all elements of G that commute with a. But, the proof that $C_a(G)$ is a subgroup is *very* similar to the proof the the center is a subgroup, done in class.]

Solution. We should show that $C_a(G) \neq \varnothing$, since the empty set is *not* a subgroup of G. But once can easily see that 1_G and a are both in $C_a(G)$.

We will do it with the *two-step method*. [The one step is not as nice in this case.]

(1) *Closed under multiplication:* Let $x, y \in C_a(G)$. [We need to prove that $x \cdot y \in C_a(G)$.] We have:

$$\begin{aligned} (x \cdot y) \cdot a &= x \cdot y \cdot a = x \cdot a \cdot y && [y \in C_a(G)] \\ &= a \cdot x \cdot y = a \cdot (x \cdot y) && [x \in C_a(G)]. \end{aligned}$$

(2) *Inverses:* Let $x \in C_a(G)$. [We need to show that $x^{-1} \in C_a(G)$, i.e., $x^{-1} \cdot a = a \cdot x^{-1}$.] Then:

$$\begin{aligned} x \cdot a = a \cdot x \quad &\Rightarrow \quad a = x^{-1} \cdot a \cdot x && \text{[multiply by } x^{-1} \text{ on the left]} \\ &\Rightarrow \quad a \cdot x^{-1} = x^{-1} \cdot a && \text{[multiply by } x^{-1} \text{ on the right]} \end{aligned}$$

□

Note: The subgroup $C_a(G)$ is called the *centralizer of a in G*.

3) Let $\phi : G \to G'$ be an isomorphism and $H \lhd G$. Show that $\phi(H) \lhd G'$.

[**Note:** Remember that

$$\phi(H) \stackrel{\text{def}}{=} \{\phi(x) \ : \ x \in H\}.]$$

Solution. First we prove that $\phi(H) < G'$, using the *one-step method*: Let $a', b' \in \phi(H)$. [We need to show that $a' \cdot (b')^{-1} \in \phi(H)$]. Then, [by definition of $\phi(H)$], there are $a, b \in H$, such that $\phi(a) = a'$ and $\phi(b) = b'$. Then, $a' \cdot (b')^{-1} = \phi(a) \cdot (\phi(b))^{-1} = \phi(a) \cdot \phi(b^{-1}) = \phi(a \cdot b^{-1})$. Since $a \cdot b^{-1} \in H$ [since $H < G$], we have that $a' \cdot (b')^{-1} \in \phi(H)$.

We now show that H is *normal*. Let $g' \in G'$ and $h' \in \phi(H)$. [We need to show that $g' \cdot h' \cdot (g')^{-1} \in \phi(H)$, i.e., that there is some $x \in H$ such that $g' \cdot h' \cdot (g')^{-1} = \phi(x)$.] Since $h' \in \phi(H)$, by definition there is $h \in H$ such that $h' = \phi(h)$. Also, since ϕ is an isomorphism, it is *onto*, and then there is $g \in G$ such that $g' = \phi(g)$. Then:

$$g' \cdot h' \cdot (g')^{-1} = \phi(g) \cdot \phi(h) \cdot \phi(g)^{-1} = \phi(g) \cdot \phi(h) \cdot \phi(g^{-1}) = \phi(g \cdot h \cdot g^{-1}).$$

Since $H \lhd G$, and $h \in H$, we have that $g \cdot h \cdot g^{-1} \in H$. Since $g' \cdot h' \cdot (g')^{-1} = \phi(g \cdot h \cdot g^{-1})$, we have that $g' \cdot h' \cdot (g')^{-1} \in \phi(H)$.

□

Note: We never used the fact that ϕ is one-to-one. Thus, *the statement is true for homorphisms that are only onto.*

4) Let S be the set of all real numbers except -1, and define the operation "$*$" by:

$$a * b = a + b + ab.$$

Prove that $(S, *)$ is an *Abelian* group, in which the identity is 0 and the inverse of $a \in S$ is $\tilde{a} \stackrel{\text{def}}{=} -a/(1+a)$. [I am not using a^{-1} for the inverse a for you not to think that it is $1/a$. With the operation "$*$", the inverse of a is *not* a^{-1}, is the $\tilde{a}$ above.]

[**Note:** It might be helpful to prove it is commutative (i.e., Abelian) first. Then, start with the easy parts!]

Solution. (0) *Closed under "$*$":* Let $a, b \in S$. Then $a * b \in S$ if it is a real number different from -1. Since $a, b \in S \subseteq \mathbb{R}$, and sums and products of real numbers are also real numbers, we need to show only that $a * b \neq -1$. But [by contradiction]:

$$\begin{aligned} a * b = -1 \quad &\Rightarrow \quad a + b + a \cdot b = -1 \\ &\Rightarrow \quad a + b \cdot (1 + a) = -1 \\ &\Rightarrow \quad b(1+a) = -(1+a) \\ &\Rightarrow \quad b = -1 \qquad \text{[since } a \neq -1\text{, we can divide by } (1+a)\text{]} \end{aligned}$$

But, since $b \in S$, we have that $b \neq -1$. [Contradiction!] Thus, if a, b in S, then $a * b \in S$.

(1) *Commutative:* We have

$$a * b = a + b + a \cdot b = b + a + b \cdot a = b * a$$

[since the addition and multiplication of $\mathbb{R}$ are commutative]. So, if S is a group, it is an *Abelian* group.

(2) *Identity:* For all a in S,

$$a * 0 = a + 0 + a \cdot 0 = a.$$

Since it is commutative, we also have $0 * a = a$. Hence 0 is the identity of S.

(3) *Associative:* Let $a, b, c \in S$. Then

$$\begin{aligned} a * (b * c) &= a * (b + c + bc) \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= (a * b) + c + (a * b)c \\ &= (a * b) * c. \end{aligned}$$

(4) *Inverse:* Let $a \in S$. Then, $-a/(1+a)$ is well defined [since $a \neq -1$, the denominator is not zero] and in S [if $-a/(1+a) = -1$, then $a = (1+a)$, which can never happen since $0 \neq 1$]. Moreover,

$$a * \left(\frac{-a}{1+a}\right) = a + \left(\frac{-a}{1+a}\right) + \frac{-a^2}{1+a} = \frac{a + a^2 - a - a^2}{1+a} = 0.$$

[Note that 0 is the identity of S.] Since S is commutative, we also have $(-a/(1+a)) * a = 0$. Thus, $-a/(1+a)$ is the inverse of a in S.

Thus, S is a group.

□