1

Consider

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2), \tag{1}$$

a conterexample to commutivity is given by

$$\begin{aligned} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}. \end{aligned} \tag{2}$$

2

G consists of the invertible upper triangular real 2 by 2 matrices.

1. Show G is closed under multiplication.

Consider

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix} \in G. \tag{3}$$

2. Show G is closed under inverse.

Consider

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \frac{1}{ac}\begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} \in G. \tag{4}$$

3. Show that $G \leq \mathrm{GL}_2(\mathbb{F}_2)$.

Notice that G is non empty since $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$, and $G \subset \mathrm{GL}_2(\mathbb{F}_2)$ by definition, and G is closed under multiplication and inverse by (1) and (2). Thus $G \leq \mathrm{GL}_2(\mathbb{F}_2)$.

4. Show that $G$is not commutative, but its subset with $b = 0$ is a commutative subgroup.

Consider

$$\begin{aligned} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} &= \begin{pmatrix} 1 & 6 \\ 0 & 2 \end{pmatrix} \\ \neq \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 4 \\ 0 & 2 \end{pmatrix}. \end{aligned} \tag{5}$$

And so $G$is not commutative.

However, if $b = 0$, then

$$\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}\begin{pmatrix} d & 0 \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & 0 \\ 0 & cf \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & f \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}. \tag{6}$$

Also, the subset is non empty since $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is in the subset, and it is closed under multiplication and inverse by (1) and (2). Thus the subset with $b = 0$ is a commutative subgroup of G.

3

1. Order of each element in Q_8.

$$Q = \{\pm 1, \pm i, \pm j, \pm k\}. \tag{7}$$

We have $|1| = 1, |-1| = 2, |i| = 4, |-i| = 4, |j| = |-j| = |k| = |-k| = 4$.

2. Prove that D_8 and Q_8 are not isomorphic.

We consider the isomorphic property that if $\varphi : G \to H$ is an isomorphism, then for any $g \in G$, $|g| = |\varphi(g)|$. This implies that isomorphism preserves the order of elements, and so G and H must have the same number of elements of each order. We notice that in D_8,

$$|e| = 1, |r| = \left|r^3\right| = 4, \left|r^2\right| = 2, |s| = |sr| = \left|sr^2\right| = \left|sr^3\right| = 2. \tag{8}$$

Thus D_8 has 5 elemetns of order 2, while Q_8 has only one element of order 2. Thus D_8 and Q_8 are not isomorphic.

4.

1.

We verify each relations.

1.$M_{-1}^2 = M_1$

$$\mathbf{M}_{-1}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} (-1)(-1)+(0)(0) & (-1)(0)+(0)(-1) \\ (0)(-1)+(-1)(0) & (0)(0)+(-1)(-1) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{M}_1 \tag{9}$$

2. $M_i^2 = M_j^2 = M_k^2 = M_{-1}$.

$$\begin{aligned} \mathbf{M}_i^2 &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} i^2 & 0 \\ 0 & (-i)^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \mathbf{M}_{-1} \\ \mathbf{M}_j^2 &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \mathbf{M}_{-1} \\ \mathbf{M}_k^2 &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i^2 & 0 \\ 0 & i^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \mathbf{M}_{-1} \end{aligned} \tag{10}$$

All three relations hold.

3. $M_i M_j = M_k$.

$$\mathbf{M}_i\mathbf{M}_j = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} (i)(0)+(0)(-1) & (i)(1)+(0)(0) \\ (0)(0)+(-i)(-1) & (0)(1)+(-i)(0) \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \mathbf{M}_k \tag{11}$$

4. $M_j M_i = M_{-k}$:

$$\mathbf{M}_j\mathbf{M}_i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = \mathbf{M}_{-k} \tag{12}$$

2.Deduce that these eight matrices consitute a subgroup of $\mathrm{GL}_2(\mathbb{C})$ with the same multiplication table as Q_8, and thus Q_8 is a group.

Let H be the 8-matrix subgroup of $\mathrm{GL}_2(\mathbb{C})$ We verify the subgroup criteria for finite group H .

1. Closure: The relations we checked showed that any element in the set can be written as a product of generators, and any product of generators simplifies to an element in the set. Thus, H is **closed** under matrix multiplication.
2. Non empty: M_1 is the identity matrix, and is in H , and so H is non empty.

And so by the subgroup criterion, $H \leq \mathrm{GL}_2(\mathbb{C})$.

3. Show that the subgroup has the same multiplication table as Q_8.

The map $\varphi : Q_8 \mapsto \{M_x \mid x \in Q_8\}$ defined by $\varphi(x) = M_x$ (e.g., $\varphi(i) = M_i$, $\varphi(j) = M_j$, etc.) is a homomorphism because the generators i, j and M_i, M_j satisfy the same defining relations.

Since φ is a bijection between the two sets of 8 elements, it is an isomorphism. This means the matrix group and Q_8 have identical structures and multiplication tables.

4. Conclude that Q_8 is a group.

Let $\psi : Q_8 \to H$ be the bijection defined by $\psi(x) = \mathbf{M}_x$ for each $x \in Q_8$. By the verified relations, ψ respects the defining multiplication rules of Q_8, hence ψ is a homomorphism.

The associativity axiom for Q_8 now follows from the associativity of matrix multiplication in H. For any $x, y, z \in Q_8$:

$$\psi((xy)z) = \psi(xy)\psi(z) = (\psi(x)\psi(y))\psi(z) \tag{13}$$

Since matrix multiplication is associative in H:

$$(\psi(x)\psi(y))\psi(z) = \psi(x)(\psi(y)\psi(z)) \tag{14}$$

And since ψ is a homomorphism:

$$\psi(x)(\psi(y)\psi(z)) = \psi(x)\psi(yz) = \psi(x(yz)) \tag{15}$$

Thus, $\psi((xy)z) = \psi(x(yz))$. Since ψ is injective, it follows that $(xy)z = x(yz)$ in Q_8.

The existence of an identity element in Q_8 is confirmed by $\psi(1) = \mathbf{M}_1$, where $\mathbf{M}_1$ is the identity matrix in H. The existence of inverses for each element $x \in Q_8$ is confirmed by $\psi(x^{-1}) = \psi(x)^{-1}$, where $\psi(x)^{-1}$ is the matrix inverse in H. Finally, closure of Q_8 under its operation is inherent in its definition via the multiplication table.

Therefore, Q_8 satisfies all the group axioms (closure, associativity, identity, and inverses), and hence is a group._

5.

let $\varphi : G \to H$ be a homomorphism.

1. Prove that $\varphi(x^n) = \varphi(x)^n$ **for all** $n \in \mathbb{N}$.
We prove this by induction on n. Base case: $n = 1$. Trivially true since $\varphi(x^1) = \varphi(x) = \varphi(x)^1$.

Inductive step: Assume true for $n = k$, i.e., $\varphi(x^k) = \varphi(x)^k$. We want to show it is true for $n = k + 1$. Notice

$$\psi(x^{k+1}) = \psi(x^k x) \tag{16}$$

and homomorphism implies

$$\psi(x^k x) = \psi(x^k)\psi(x) = \psi(x)^{k+1}, \tag{17}$$

as wanted. Thus by induction, $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{N}$.

2. Do part 1 for $n = -1$ **and deduce that** $\varphi(x^n) = \varphi(x)^n$ **for all** $n \in \mathbb{Z}$.
Since homomorphisem preserves identity, we have

$$\varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x) = \varphi(e) = e. \tag{18}$$

Thus $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Let $m \in \mathbb{Z}, m < 0; n = -m, n \in \mathbb{N}$. Then consider

$$\varphi(x^m) = \varphi(x^{-n}) = \varphi\left((x^n)^{-1}\right) = \varphi(x^n)^{-1} = (\varphi(x)^n)^{-1} = \varphi(x)^{-n} = \varphi(x)^m. \tag{19}$$

Since we have proved part 1, we conclude that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

6.

Let $\theta : \Delta \to \Omega$ be a bijection. Define

$$\varphi : S_\Delta \to S_\Omega, \quad \text{by } \varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1}. \tag{20}$$

1. Prove that φ is well defined.
If $\sigma \in S_\Delta$, then $\sigma : \Delta \to \Delta$ is a bijection, and since θ, θ^{-1} are bijections, the composition

$$\phi(\sigma) = \theta \circ \sigma \circ \theta^{-1} : \Omega \to \Omega \tag{21}$$

is also a bijection. Hence $\phi(\sigma) \in S_\Omega$, so ϕ is well-defined.

2. Prove that φ is a bijection from S_Δ onto S_Ω.
Define

$$\psi : S_\Omega \to S_\Delta, \qquad \psi(\tau) = \theta^{-1} \circ \tau \circ \theta. \tag{22}$$

Then for any $\tau \in S_\Omega$,

$$(\phi \circ \psi)(\tau) = \phi(\theta^{-1} \circ \tau \circ \theta) = \theta \circ (\theta^{-1} \circ \tau \circ \theta) \circ \theta^{-1} = (\theta \circ \theta^{-1}) \circ \tau \circ (\theta \circ \theta^{-1}) = \tau, \tag{23}$$

so $\phi \circ \psi = \mathrm{id}_{S_\Omega}$. Similarly, for any $\sigma \in S_\Delta$,

$$(\psi \circ \phi)(\sigma) = \psi(\theta \circ \sigma \circ \theta^{-1}) = \theta^{-1} \circ (\theta \circ \sigma \circ \theta^{-1}) \circ \theta = (\theta^{-1} \circ \theta) \circ \sigma \circ (\theta^{-1} \circ \theta) = \sigma, \tag{24}$$

so $\psi \circ \phi = \mathrm{id}_{S_\Delta}$. Hence φ is bijective with inverse ψ.

3. Prove that φ is a homomorphism, i.e. $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$
For any $\sigma, \tau \in S_\Delta$,

$$\phi(\sigma \circ \tau) = \theta \circ (\sigma \circ \tau) \circ \theta^{-1} = (\theta \circ \sigma \circ \theta^{-1}) \circ (\theta \circ \tau \circ \theta^{-1}) = \phi(\sigma) \circ \phi(\tau). \tag{25}$$

Thus φ is a group homomorphism.

Therefore, ϕ is a bijective homomorphism, i.e., an isomorphism $S_\Delta \cong S_\Omega$.

7.

Let G, H be groups and let $\varphi : G \to H$ be a homomorphism. Prove that the image of $\varphi(G)$ is a subgroup of H, and that if φ is injective then G is isomorphic to $\varphi(G)$.

1.

Using the subgroup criterion, we see that $\varphi(G) \subset H$ by definition of the image, and $\varphi(G)$ is non empty since $e_H = \varphi(e_G) \in \varphi(G)$.

Also, let $x = \varphi(g_1), y = \varphi(g_2); g_1, g_2 \in G$. Notice that

$$xy^{-1} = \varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1 g_2^{-1}) \in \varphi(G), \tag{26}$$

and so $\varphi(G)$ is closed under inverse.Thus by the subgroup criterion, $\varphi(G) \leq H$. (Note that we used part 2 of problem 5 to show $\varphi(g_2)^{-1} = \varphi(g_2^{-1})$.)

2.

Define $\psi : G \to \varphi(G), \psi(g) := \varphi(g)$. Then ψ is a homomorphism since for any $g_1, g_2 \in G$,

$$\psi(g_1 g_2) = \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = \psi(g_1)\psi(g_2). \tag{27}$$

ψ is surjective by definition of $\varphi(G)$, and injective if φ is injective. Thus ψ is an isomorphism. ■

8.

Let G, H be groups and $\varphi : G \to H$ a homomorphism. Define

$$\ker(\varphi) := \{\, g \in G \mid \varphi(g) = e_H \,\}. \tag{28}$$

1. $\ker(\varphi)$ **is a subgroup of** G**.**
Use the subgroup test: a nonempty subset $K \subseteq G$ is a subgroup iff $\forall x, y \in K$, we have $xy^{-1} \in K$.

- Nonempty: $\varphi(e_G) = e_H$, so $e_G \in \ker(\varphi)$.
- Closure under xy^{-1}: If $x, y \in \ker(\varphi)$, then

$$\varphi(xy^{-1}) = \varphi(x)\,\varphi(y)^{-1} = e_H \cdot (e_H)^{-1} = e_H, \tag{29}$$

hence $xy^{-1} \in \ker(\varphi)$.

Therefore $\ker(\varphi) \leq G$.

2. φ **is injective** $\Longleftrightarrow$ $\ker(\varphi) = \{e_G\}$**.**
($\Rightarrow$) Suppose φ is injective. Let $g \in \ker(\varphi)$, so $\varphi(g) = e_H = \varphi(e_G)$. By injectivity, $g = e_G$. Hence $\ker(\varphi) = \{e_G\}$.

($\Leftarrow$) Suppose $\ker(\varphi) = \{e_G\}$. If $\varphi(g_1) = \varphi(g_2)$, then

$$\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e_H, \tag{30}$$

so $g_1 g_2^{-1} \in \ker(\varphi)$ and thus $g_1 g_2^{-1} = e_G$, i.e. $g_1 = g_2$. Hence φ is injective.