A2)

Proof. Let $a, b \in G$. Since G is a group, we know that it contains the respective inverses a^{-1}, b^{-1}. Then, we have

$$\phi\left(ab \cdot a^{-1}b^{-1}\right) = \phi\left(ab\right) \circ \phi\left(a^{-1}b^{-1}\right)$$

$$\phi\left(ab \cdot a^{-1}b^{-1}\right) = \phi\left(a\right) \circ \phi\left(b\right) \circ \phi\left(a^{-1}\right) \circ \phi\left(b^{-1}\right)$$

$$\phi\left(ab \cdot a^{-1}b^{-1}\right) = \phi\left(a\right) \circ \phi\left(b\right) \circ \left[\phi\left(a^{-1}\right)\right]^{-1} \circ \left[\phi\left(b^{-1}\right)\right]^{-1}$$

$$\phi\left(ab \cdot a^{-1}b^{-1}\right) = \left[\phi\left(a^{-1}\right)\right]^{-1} \circ \left[\phi\left(b^{-1}\right)\right]^{-1} \circ \phi\left(a\right) \circ \phi\left(b\right)$$

$$\phi\left(ab \cdot a^{-1}b^{-1}\right) = a^{-1}b^{-1}ab$$

□

A3)
Non-empty:

$$(1)^2 + (1)^2 = c^2$$

$$1 + 1 = c^2$$

$$2 = c^2$$

$$c = \sqrt{2}$$

$$\text{and we can write } \sqrt{2} \text{ as } \frac{\sqrt{2}}{1} \in \mathbb{Q}^*$$

$ab^{-1} \in H$ part:

Let $(a + bi)$ and $(c + di)^{-1}$ be in H. Indeed, we have

$$(a + bi)(c + di)^{-1} = \left(\frac{(a + bi) \cdot (c - di)}{(c - di) \cdot (c - di)}\right) = \left(\frac{ac + bd}{c^2 + d^2}\right) + \left(\frac{bc - ad}{c^2 + d^2}\right) i \in H$$

A5)

Proof. Given elements a, b of G, and ab has finite order n. Hence, $|ab| = n \iff (ab)^n = e$. We need to show that n is the smallest integer such that $(ab)^n = e$.

$$(ab)^n = e \implies b(ab)\dots(ab)a = bea \implies (ba)^n = e \implies |ba| \leq n.$$

Now, show that there is no positive integer m such that $m < n$ and $(ba)^m = e$. But, if $|ba| < n$, then we could apply the same reasoning to find that $|ab| \leq |ba| < |ab|$, which is absurd. So, $|ba| = |ab| = n$.

□

B1)
Before we begin, we will prove some lemmas that will be useful later.

Lemma 1. *Let $(R, +, \cdot)$ be a ring whose zero is 0_R. Then, $\forall\, x \in R : 0_R \cdot x = 0_R = x \cdot 0_R$. In other words, the zero is a zero element for the ring product, thereby justifying its name.*

Proof. Because $(R, +, \cdot)$ is a ring, $(R, +)$ is a group. Since 0_R is the identity in $(R, +)$, we have $0_R + 0_R = 0_R$. From the cancellation laws, all group elements are cancelable, so every element of $(R, +)$ is cancelable for $+$. Hence,

$$\begin{aligned} x \cdot (0_R + 0_R) &= x \cdot 0_R \\ \implies (x \cdot 0_R) + (x \cdot 0_R) &= x \cdot 0_R \\ \implies (x \cdot 0_R) + (x \cdot 0_R) &= (x \cdot 0_R) + 0_R \\ \implies x \cdot 0_R &= 0_R \end{aligned}$$

Then,

$$\begin{aligned} (0_R + 0_R) \cdot x &= 0_R \cdot x \\ \implies (x \cdot 0_R) + (x \cdot 0_R) &= 0_R \cdot x \\ \implies (x \cdot 0_R) + (x \cdot 0_R) &= 0_R + (0_R \cdot x) \\ \implies 0_R \cdot x &= 0_R \end{aligned}$$

□

Lemma 2. *Let $(R, +, \cdot)$ be a ring. Suppose further that R is not the null ring. Let $f \in R$ such that $f^k = 0$ with $k \geq 1$ implies $f = 0$. Then, f is a zero divisor.*

Proof. Let 0_R be the zero fo R. By hypothesis, there exists $n \geq 1$ such that $x^n = 0_R$. If $n = 1$, then $x = 0_R$. By hypothesis, R is not the null ring, so we may choose $y \in R \setminus \{0\}$. Now, by our lemma 2, we have

$$y \cdot x = y \cdot 0_R = 0_R$$

Therefore, x is a zero divisor in R. If $n \geq 2$, define $y = x^{n-1}$. Then, we have

$$y \cdot x = x^{n-1} \cdot x = x^n = 0_R$$

So, x is the zero divisor in R.

$\square$

Now that we have finished with that, onto the main event!

Lemma 3. *Let* $(R, +, \cdot)$ *be an integral domain. Then,* R *is reduced.*

Proof. Let $x \in R$ such that $x^k = 0$ with $k \geq 1$ implies $x = 0$. Then, by our lemma 2, x is a zero divisor. So, by the definition of an integral domain, this means that $x = 0$. Therefore, the only element $x \in R$ such that $x^k = 0$ with $k \geq 1$ implies $x = 0$ of R is 0. Thus, R is reduced.

$\square$

Finally, an example of a reduced ring that is not an integral domain would be $\mathbb{Z}[x, y] \ \setminus (xy)$ or $\mathbb{Z} \times \mathbb{Z}$

B2) A complete characterization of the set of left ideals of the ring R of 2×2 matrices over $\mathbb{R}$ would be all of the matrices of the form

$$\begin{pmatrix} ar_1 & br_1 \\ ar_2 & br_2 \end{pmatrix}$$

where r_1 and r_2 run over all the real numbers, i.e. all of the matrices whose rows are scalar multiples of vector (a, b).

B3)

Proof. Associativity: Let $u_1, u_2, u_3 \in U(R)$. Then, in particular, u_1, u_2, u_3 are in R and since multiplication in R is associative, it is associative in $U(R)$

Invertibility: Let $u_1 \in R$. Then, there exists a $u_1^{-1} \in R$. Therefore, $u_1 u_1^{-1} = e = u_1^{-1} u_1$, where e is the identity element of R. Hence, $u_1 = \left(u_1^{-1}\right)^{-1}$. Thus, $u_1^{-1} \in U(R)$ whenever $u_1 \in R$

Identity: R has a unit identity. Let this unity be denoted by e (from above). Then, $e^{-1}e = e = ee^{-1}$ if e^{-1} exists. But, $ee = e$ and therefore, $e = e^{-1}$ and therefore $e \in U(R)$.

To show that it is closed under the binary operation:

If $a, b \in U(R)$, then a^{-1}, b^{-1} exist in R. Therefore, $(ab)\left(b^{-1}a^{-1}\right) = a\left(bb^{-1}\right)a^{-1} = aea^{-1} = aa^{-1} = e$ and R is commutative, so the same holds on the left. Therefore, $U(R)$ is closed $\left(a, b \in U(R) \textit{ implies that } ab \in U(R)\right)$. Thus, $U(R)$ is a group.

A necessary and sufficient condition for the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

to be a unit in the ring $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$ is that the determinant must be ± 1. In other words, the units of the ring $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$ is the set of 2×2 matrices with determinant equal to ± 1.

$\square$