1. Determine all homomorphisms from \( \mathbb{Z}_6 \) to \( \mathbb{Z}_2 \oplus \mathbb{Z}_8 \).

**Proof.** Let us denote a homomorphism by \( \phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \oplus \mathbb{Z}_8 \). Since \( \mathbb{Z}_6 \) is a cyclic group, the map is automatically determined by the image of a generator, namely 1.

Let \( \phi(1) = (x, y) \). Recall the fact that, for any homomorphism \( \psi : G \to H \), for any \( g \in G \), \( |\phi(g)| \mid |g| \); hence the order of \((x, y)\) must divide the order of 1 in \( \mathbb{Z}_6 \), i.e. 6. On the other hand, the order of \((x, y)\) must divide 16 too, as it is an element of a group of order 16. Thus, \(|(x, y)| = \gcd(6, 16) = 2\); hence, \((x, y)\) must have order either 1 or 2.

There exists only one element of order 1 in \( \mathbb{Z}_2 \oplus \mathbb{Z}_8 \): \((0, 0)\).

There exists three elements of order 2 in \( \mathbb{Z}_2 \oplus \mathbb{Z}_8 \): \((0, 4)\), \((1, 0)\), \((1, 4)\).

Therefore, there exists four homomorphisms, where 1 can be mapped to \((0, 0)\), \((0, 4)\), \((1, 0)\), or \((1, 4)\), respectively. \(\square\)

2. Can there be a homomorphism from \( \mathbb{Z}_{30} \) onto \( \mathbb{Z}_3 \oplus \mathbb{Z}_3 \)? Explain your answer.

**Proof.** If \( \phi : G \to H \), and if \( G \) is cyclic, then \( \phi(G) \) is also cyclic. Denote an arbitrary homomorphism from \( \mathbb{Z}_{30} \) to \( \mathbb{Z}_3 \oplus \mathbb{Z}_3 \) by \( \psi \). Then, \( \psi(\mathbb{Z}_{30}) \) is cyclic, while \( \mathbb{Z}_3 \oplus \mathbb{Z}_3 \) is not, since \( \gcd(3, 3) = 3 \neq 1 \). Thus, \( \psi(\mathbb{Z}_{30}) \neq \mathbb{Z}_3 \oplus \mathbb{Z}_3 \), and hence there cannot be a surjective homomorphism. \(\square\)

Another solution;

**Proof.** Suppose there exists an onto homomorphism \( \psi : \mathbb{Z}_{30} \to \mathbb{Z}_3 \oplus \mathbb{Z}_3 \). Then, \( \psi(\mathbb{Z}_{30}) = \mathbb{Z}_3 \oplus \mathbb{Z}_3 \). Applying the first isomorphism theorem, \( \mathbb{Z}_{30}/\ker \psi \cong \psi(\mathbb{Z}_{30}) = \mathbb{Z}_3 \oplus \mathbb{Z}_3 \). By using Lagrange’s theorem, this yields \(|\mathbb{Z}_{30}| / |\ker \psi| = 30 / 3 = 9 = |\mathbb{Z}_3 \oplus \mathbb{Z}_3|\); however there exists no integer \( x \) satisfying \( 30 \cdot x = 9 \). Thus, there exists no homomorphism from \( \mathbb{Z}_{30} \) onto \( \mathbb{Z}_3 \oplus \mathbb{Z}_3 \). \(\square\)

3. Suppose that \( \phi : \mathbb{Z}_{20} \to \mathbb{Z}_{20} \) is a homomorphism with \( \phi(7) = 3 \). Determine a formula for \( \phi(x) \). Is \( \phi \) an automorphism?

**Proof.** Note that \( \phi(7) + \phi(7) + \phi(7) = \phi(7 + 7 + 7) = \phi(1) \), as 21 is congruent to 1 modulo 20. Thus, \( \phi(1) = 3\phi(7) = 9 \), and hence for any \( x \in \mathbb{Z}_{20} \), we have \( \phi(x) = x\phi(1) = 9x \).

Observe that 9 is also a generator in \( \mathbb{Z}_{20} \), since \( \gcd(9, 20) = 1 \). Thus, \( \phi \) is sending a generator to a generator, and hence \( \phi \) must be surjective. Also, note that \( \ker \phi = \{ x \in \mathbb{Z}_{20} : 9x \equiv 0 \pmod{20} \} = \{0\} \).

As kernel is trivial, the map is injective as well. Therefore, this map is an automorphism. \(\square\)

4. What is the order of factor group \( \mathbb{Z}_{40}/\langle 28 \rangle \)?

**Proof.** Remark that the smallest non-zero positive integer \( m \) satisfying \( 40 \mid 28m \) is \( m = 10 \). Thus, \( \langle 28 \rangle \subset \mathbb{Z}_{40} \) has order 10. By Lagrange’s theorem, the order of factor group is \( |\mathbb{Z}_{40}| / |\langle 28 \rangle| = 40 / 10 = 4 \). \(\square\)
5. let $M_2(\mathbb{Z})$ be the ring of all $2 \times 2$ matrices over the integers and let

$$R = \left\{ \begin{pmatrix} a & a + 2b \\ a + b & b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}.$$

Prove or disprove that $R$ is a subring of $M_2(\mathbb{Z})$.

Proof. One can show that $R$ is not closed under multiplication. Observe the fact that every matrix $M = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ in $R$ satisfies that the trace, i.e. the sum of diagonal entries, is equal to the lower left entry, i.e. $a_{21}$. Consider two arbitrary matrices in $R$, namely $\begin{pmatrix} a & a + 2b \\ a + b & b \end{pmatrix}$ and $\begin{pmatrix} c & c + 2d \\ c + d & d \end{pmatrix}$.

Then, the product of these matrices is

$$\begin{pmatrix} a & a + 2b \\ a + b & b \end{pmatrix} \begin{pmatrix} c & c + 2d \\ c + d & d \end{pmatrix} = \begin{pmatrix} ac + (a + 2b)(c + d) & a(c + 2d) + (a + 2b)d \\ (a + b)c + b(c + d) & (a + b)(c + 2d) + bd \end{pmatrix}.$$

Note that the sum of diagonal entries is

$$ac + (a + 2b)(c + d) + (a + b)(c + 2d) + bd = 3ac + 3bc + 3ad + 5bd,$$

which is not always equal to the lower left entry of the product, $(a + b)c + b(c + d) = ac + 2bc + bd$. Thus, the product of two matrices in $R$ is not necessarily an element of $R$, and hence $R$ is not closed under matrix multiplication. Therefore, $R$ is not a subring of $M_2(\mathbb{Z})$. \qed