1. Let $R = \{(a, b) \mid a \equiv b \mod 5\}$ be a subset of $\mathbb{Z} \times \mathbb{Z}$. Prove or disprove that $aRb$ is an equivalence relation on $\mathbb{Z}$.

**Solution:** $R$ is reflexive: $a \equiv a \mod 5$ because $5|(a-a)$ . $R$ is symmetric: if $a \equiv b \mod 5$, i.e. $5|(a-b)$, then $5|(b-a)$, i.e. $b \equiv a \mod 5$. $R$ is transitive: if $a \equiv b \mod 5$ and $b \equiv c \mod 5$, i.e. $5$ divides $a-b$ and $b-c$, then $5|(a-c)$, i.e. $a \equiv c \mod 5$. Therefore, $R$ is an equivalence relation.

2. Let $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 2 & 7 & 3 & 1 & 5 \end{pmatrix}$ and $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 1 & 4 & 2 & 7 \end{pmatrix}$.

Compute $\pi^{-1}$, Determine orders and signs of $\pi$ and $\sigma$.

**Solution:** $\pi \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 2 & 7 & 3 & 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 4 & 7 & 6 & 5 \end{pmatrix}$.

$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 2 & 7 & 3 & 1 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 7 & 2 & 4 \end{pmatrix}$.

$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 2 & 7 & 3 & 1 & 5 \end{pmatrix} = (1475326)$, order=7.

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = (1354)(26)$, order=lcm(4,2) = 4.

Inversions in $\pi$: (4,1), (6,1), (2,1), (7,1), (3,1), (4,2), (6,2), (4,3), (6,3), (7,3), (6,5), (7,5). 12 inversions, thus sign($\pi$) = $(-1)^{12} = 1$.

Inversions in $\sigma$: (3,1), (6,1), (5,1), (3,2), (6,2), (5,2), (4,2), (6,4), (5,4), (6,5). 10 inversions, thus sign($\sigma$) = $(-1)^{10} = 1$.

3. Prove that for any permutation $\pi$, the permutation $\pi^{-1}(12)\pi$ is a transposition.

**Solution:** Let $k, l$ be such that $\pi(k) = 1, \pi(l) = 2$. Then $\pi^{-1}(1) = k, \pi^{-1}(2) = l$, so that $\pi^{-1}(12)\pi(k) = l$ and $\pi^{-1}(12)\pi(l) = k$, i.e. $\pi^{-1}(12)\pi$ permutes $k$ and $l$. Now let $m$ be any number distinct from $k$ and $l$. Since $m \neq k, l, \pi(m) \neq 1$ and the transposition $(12)$ leaves $\pi(m)$ in place. Therefore, $\pi^{-1}(12)\pi(m) = \pi^{-1}(\pi(m)) = m$. Hence, $\pi^{-1}(12)\pi$ leaves $m \neq k, l$ in place. We conclude that $\pi^{-1}(12)\pi = (kl)$, a transposition.

4. Let $a, b$ be elements of a group $G$. Solve equations $a^{-1}x = b$ and $xa^{-1}b = e$.

**Solution:** $a^{-1}x = b$: multiply by $a$ on the left: $aa^{-1}x = ab$. Thus $x = ab$.

$xa^{-1}b = e$: multiply by $b^{-1}$ on the right: $xa^{-1}bb^{-1}a = eb^{-1}a$. Thus $x = eb^{-1}a = b^{-1}a$.

5. Let $G$ be a group such that for any two elements $a, b$ in $G$, $(ab)^2 = a^2b^2$. Prove that $G$ is abelian.

**Solution:** $(ab)^2 = a^2b^2$ means $abab = aabb$. Multiply by $a^{-1}$ on the left and $b^{-1}$ on the right: $a^{-1}ababb^{-1} = a^{-1}aabb^{-1}$. Cancelling $a^{-1}a$ etc gives $ba = ab$ for all $a, b$. This means that $G$ is abelian.

6. Let $G$ be a group. Define the relation of *conjugacy* on $G$: $aRb$ if and only if there exists $g \in G$ such that $b = g^{-1}ag$. Prove that this is an equivalence relation.

**Solution:** $R$ is reflexive: $aRa$ because $e^{-1}ae = a$. $R$ is symmetric: if $aRb$, i.e. if $b = g^{-1}ag$ for some $g$, then $a = gb^{-1} = (g^{-1})^{-1}bg^{-1}$ and $bRa$. $R$ is transitive: if $aRb$, i.e. $b = g^{-1}ag$, and $bRc$, i.e. $c = h^{-1}bh$, then $c = h^{-1}g^{-1}agh = (gh)^{-1}a(gh)$.
and aRc. (Notice that the definition of relation requires that \( b = g^{-1}ag \) for some \( g \), i.e. for different pairs of \( a \) and \( b \), \( g \) may be different.)

7. Compute orders of the following elements of the group \((\mathbb{C}, \cdot)\): \(3i, \sqrt{2} + \sqrt{2}i\).

**Solution:** \((3i)^n = 3^n i^n\). Since \(|3^n i^n| = 3^n\) (or, equivalently, since \(3^n i^n\) equals either of \(3^n, -3^n, 3^n i, -3^n i\), \((3i)^n \neq 1\) for any \(n\). Hence \(3i\) has infinite order.

Taking subsequent powers of \(\sqrt{2} + \sqrt{2}i\) shows that \((\sqrt{2} + \sqrt{2}i)^8 = 1\). Alternatively, you can just compute \((\sqrt{2} + \sqrt{2}i)^8\) and take it from there.

8. For a matrix \(A\) denote its transpose by \(A^t\). \(A\) is orthogonal if \(A^{-1} = A^t\) (\(A^t\) means the transpose of \(A\)). Prove that the set of invertible orthogonal \(n \times n\) matrices is a subgroup of \(GL(n, \mathbb{R})\). (Hints: First recall – or deduce – that \((AB)^t = B^t A^t\) and \((A^{-1})^t = (A^t)^{-1}\).)

**Solution:** We have to prove that (1) if \(A\) and \(B\) are invertible orthogonal matrices, then so is \(AB\); (2) if \(A\) is an invertible orthogonal matrix, then so is \(A^{-1}\).

(1) \((AB)^t = B^t A^t = B^{-1} A^{-1} = (AB)^{-1}\).

(2) \((A^{-1})^t = (A^t)^{-1} = (A^{-1})^{-1}\).

9. Let \(R\) be a commutative ring such that \(1 + 1 = 0\). Prove that for any \(x, y \in R\), \((x + y)^2 = x^2 + y^2\).

**Solution:** \((x + y)^2 = (x + y)(x + y) = x^2 + xy + yx + y^2\) (distributive law). Since \(R\) is commutative, \(yx = xy\). Since \(1 + 1 = 0\), \(xy + xy = (1 + 1)xy = 0xy = 0\). Thus \((x + y)^2 = x^2 + 0 + y^2 = x^2 + y^2\).

10. Prove that the subset \(\{a + bj | a, b \in \mathbb{R}\}\) of \(H\) is a field.

**Solution:** Since \(\mathbb{H}\) is a unital ring, we only have to prove that every nonzero element of the form \(a + bj\) is invertible and that \((a + bj)(c + dj) = (c + dj)(a + bj)\) (commutativity of multiplication).

Invertibility of \(a + bj\): \((a + bj)(a - bj) = a^2 - b^2 j^2 = a^2 + b^2\). Therefore, \((a + bj)^{-1} = \frac{a - bj}{a^2 + b^2}\).

Commutativity of multiplication: \((a + bj)(c + dj) = ac + b c j + ad j + bd j^2 = ca + cj + b dj + db j^2 = (c + dj)(a + bj)\).