Q1. Let $(G, \cdot)$ be a group and let $H \leq G$. Define

$$X = \{aH \mid a \in G\}$$

I.e. X is the set of left cosets of H. Define $\star : X \times X \longrightarrow X$ by: for all $a, b \in G$,

$$(aH) \star (bH) = (a \cdot b)H.$$

(i) We say that H is *normal* if for all $h \in H$ and for all $g \in G$, $ghg^{-1} \in H$. Prove that if H is normal, then $(X, \star)$ is a group. Note that you need to check that $\star$ is a well-defined function.

(ii) Find an example of a group $(G, \cdot)$ and $H \leq G$ such that $(X, \star)$ is not a group.

(5 marks)

Q2. Let G be the set of 2×2 invertible real matrices and let $\cdot$ be matrix multiplication. Show that $(G, \cdot)$ is a group. Let

$$A = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Find the orders of A, B and $A \cdot B$.
(4 marks)

Q3. Let G be the set of 4×4 invertible real matrices and let $\cdot$ be matrix multiplication. Note that $(G, \cdot)$ is a group. Find $n \in \mathbb{N} \cup \{\infty\}$ such that

$$C_n = \left\langle \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\rangle$$

(2 marks)

Q4. Prove, without using the product formula for $\varphi(n)$, that if p is prime, then

$$\varphi(p^k) = p^k - p^{k-1}$$

(3 marks)

Q5 Prove that for all $n \in \mathbb{N}\backslash\{0\}$, $n^3 + 2n$ and $n^4 + 3n^2 + 1$ are relatively prime.
(2 marks)

Q6. Prove that every subgroup of a cyclic group is cyclic.
(2 marks)

Q7. Show that if $a, b, c \in \mathbb{N}$ with $a^2 + b^2 = c^2$, then $3 \mid ab$.
(3 marks)

Q8. Find a generator of the group $((\mathbb{Z}/11\mathbb{Z})^*, \otimes_{11})$.
(2 marks)

Q9. Find the inverse of $[12]_{89}$ in the group $((\mathbb{Z}/89\mathbb{Z})^*, \otimes_{89})$.
(2 marks)

Q10. What is the order of $[27]_{56}$ in the group $((\mathbb{Z}/56\mathbb{Z})^*, \otimes_{56})$?
(2 marks)

Q11. Draw a Cayley Table for the group $((\mathbb{Z}/9\mathbb{Z})^*, \otimes_9)$. Is $((\mathbb{Z}/9\mathbb{Z})^*, \otimes_9)$ cyclic?
(3 marks)

Q12. Let $(G, \cdot)$ be a group and let $a \in G$ be an element of order n. It follows that $\langle a \rangle_G = C_n \leq G$. Let $b \in \langle a \rangle_G$. Therefore $b = a^s$ for $0 \leq s < n$.

(i) Prove that $\langle b \rangle_G$ is C_m where

$$m = \frac{n}{\gcd(s, n)}$$

(ii) Prove that $\langle a^t \rangle_G = \langle b \rangle_G$ if and only if $\gcd(s, n) = \gcd(t, n)$

(4 marks)