1. (a). What is the inverse of 7 in $U(11)$?
Solution: $7^{-1} = 8$

(b). Is $U(8)$ cyclic? Justify your answer.
Solution: No. For each $x$ in $U(8)$, $x^2 = 1$.

(c). Is $U(9)$ cyclic? Justify your answer.
Solution: Yes, it is generated by 2 (and also by 5).

(d). Is the symmetric group $S_3$ cyclic?
Solution: No, $S_3$ is not Abelian and every cyclic group is Abelian.

2. (a). List all the left cosets of $H = \{-1, 1\}$ in $Q_8$.
Solution: $\{-1, 1\}$, $\{-i, i\}$, $\{-j, j\}$, $\{-k, k\}$.

(b). List all of the subgroups of $(Z_{12}, +)$.
Solution: $\{0\}$, $\{0, 2, 4, 6, 8, 10\}$, $\{0, 3, 6, 9\}$, $\{0, 4, 8\}$, $\{0, 6\}$, $\{0\}$.

3. (a). The number of generators of $(Z_{99}, +)$ is __________
Solution: $\phi(99) = \phi(9)\phi(11) = 6 \times 10 = 60$.

(b). Suppose that $\sigma = (1, 2, 3, 4, 5)$. Then $\sigma^{102} = $ ________________
Solution: $\sigma^{102} = \sigma^{100} \cdot \sigma^2 = \sigma^2 = (1, 3, 5, 2, 4)$.

(c). Let $\sigma = (1,3,4)(5,7, 2, 6)$. The index of $\langle \sigma \rangle$ in $S_7$ is __________
Solution: $\frac{7!}{12} = 420$.

4. The remainder when $2^{100}$ is divided by 35 is __________
Solution: By Euler’s Theorem,
$2^{\phi(35)} \equiv 1 \mod 35 \Rightarrow 2^{24} \equiv 1 \mod 35 \Rightarrow 2^{96} \equiv 1 \mod 35$.
Hence, $2^{100} = 2^{96} \cdot 2^4 \equiv 2^4 \mod 35 \Rightarrow 2^{100} \equiv 16 \mod 35$.
So, the remainder is 16.
5. Let \( \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 6 & 1 & 7 & 9 & 8 & 4 & 2 & 3 \end{pmatrix} \) and \( \gamma = (1, 5, 6, 2, 4)(3, 7, 8) \).

(i). Express \( \sigma \) as a product of disjoint cycles.

Solution: \( \sigma = (1, 5, 9, 3)(2, 6, 8)(4, 7) \)

(ii). The order of \( \sigma \) is ______ Solution: 12.

(iii). Express \( \sigma \) as a product of transpositions.

Solution: \( \sigma = (1, 3)(1, 9)(1, 5)(2, 8)(2, 8)(2, 6)(4, 7) \)

(iv). \( \sigma^{-2} = \) _________________

Solution: \( \sigma^{-2} = (3, 5)(1, 9)(8, 2, 6) \)

(v). Find a permutation \( \delta \) such that \( \sigma \delta = (1, 2, 3, 4) \).

Solution: \( \delta = (1, 8, 6, 2, 9, 5)(3, 7, 4) \)

(vi). What is \( \sigma \gamma = \) _________________

Solution: \( \sigma \gamma = (1, 9, 3, 4, 5, 8)(2, 7) \).

6. Suppose that \( G \) is an abelian group and that \( a \) and \( b \) are distinct elements of \( G \) having order 2. Show that \( |G| \) is a multiple of 4.

Hint: What are the values of \( a(ab), b(ab), (ab)(ab) \)?

Solution: The set \( H = \{e, a, b, ab\} \) is a subgroup (verify that) and hence by LaGrange’s Theorem the order of \( H \), which is 4, must divide the order of \( G \). Hence the order of \( G \) is a multiple of 4.

7. Let \( G \) be a group of order \( n \) and \( m \) an integer relatively prime to \( n \). Let \( f: G \to G \) be defined by \( f(x) = x^m \). Show that \( f \) is a bijection.

Solution:
We will show that \( f \) is onto. Then the fact that \( G \) is finite is enough to guarantee that \( f \) is also 1-1.
Since \( n \) and \( m \) are relatively prime, there exist integers \( a \) and \( b \) such that \( an + bm = 1 \).
Let \( y \) be any element of \( G \). Then \( y = y^1 = y^{an+bm} = y^ay^bm = (y^a)^m(y^b)^m = (y^b)^m \).
Thus \( y = f(y^b) \) and so \( f \) is onto. Note that we used the fact that \( y^n = e \) since \( n \) is the order of the group.
8. Let $H$ be a subgroup of the group $G$ and define $x \equiv y \mod H \Leftrightarrow x^{-1}y \in H$.
Complete the following argument that this relation is an equivalence relation.

In each part *explain clearly* how $H$ being a subgroup is being used.

(i). $x \equiv y \mod H$ is reflexive since if $x$ is any element of $G$, then

(ii). $x \equiv y \mod H$ is symmetric since

(iii). $x \equiv y \mod H$ is transitive since

[See Your Notes]

9. Show that every group of prime order is cyclic.

**Solution:** Let $G$ be a group of order $p$, where $p$ is a prime and let $a$ be any non-
identity element of the group $G$. Then $o(a) > 1$ and by LaGrange’s Theorem,
$o(a)$ must divide $p$ and hence $o(a) = p$ and thus $a$ must generate $G$. 