Please show your work and use words to explain your steps where appropriate.

Problem 1 (10pts) On the defintion of a group.

(a) Suppose that G is a non-empty set equipped an operation. What 4 things do I need to check to see if G is a group? Give details.

1: binary operation, or closure; $a*b \in G \quad \forall a,b \in G$.

2: associativity; $(a*b)*c = a*(b*c) \quad \forall a,b,c \in G$

3: identity; $\exists e \in G$ s.t. $a*e = e*a = a \quad \forall a \in G$

4: inverses; for each $g \in G$, $\exists h \in G$ s.t. $g*h = h*g = e$.

What additional property needs to hold for G to be an **Abelian** group?

5: $a*b = b*a \quad \forall a,b \in G$.

(b) Let $G = \mathbb{Z}_{\geq 0}$ be the set of non-negative integers. It can be shown that $x \star y = \max\{x,y\}$ (example: $3 \star 1 = \max\{3,1\} = 3$) is an associative, commutative (closed) binary operation on G with identity 0. However, G is not a group. Why? [Use a concrete counterexample.]

Consider $3*y = 0$ we find no inverse

Problem 2 (10pts) Let G is a group. Prove $Z(G)$ (the center of G) is a subgroup of G.

$Z(G) = \{x \in G \mid gx = xg \ \forall g \in G\}$. Observe $ge = g = eg$ thus $e \in Z(G) \neq \emptyset$. Let $a,b \in Z(G)$ thus $ag = ga$ and $bg = gb \ \forall g \in G$. Hence $g(ab) = agb = abg \Rightarrow ab \in Z(G)$. Also, $ag = ga \Rightarrow (ag)^{-1} = (ga)^{-1} \Rightarrow g^{-1}a^{-1} = a^{-1}g^{-1} \ \forall g \in G$ thus replacing g with g^{-1} we find $ga^{-1} = a^{-1}g \ \forall g \in G \therefore a^{-1} \in Z(G)$. Thus $Z(G) \leq G$ by two-step subgroup test.

Problem 3 (10pts) Let G be a group. **Prove:** for each $n \in \mathbb{N}$, if $a_1, \ldots, a_n \in G$ then $(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}$.

Consider $(ab)(b^{-1}a^{-1}) = aea^{-1} = aa^{-1} = e \therefore (ab)^{-1} = b^{-1}a^{-1}$ (*)

Suppose $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$ for some $n \in \mathbb{N}$. Consider,

$(\underbrace{a_1 \cdots a_n}_{a} \underbrace{a_{n+1}}_{b})^{-1} = a_{n+1}^{-1}(a_1 \cdots a_n)^{-1}$ by (*)

$= a_{n+1}^{-1} a_n^{-1} \cdots a_1^{-1}$ by induct. hypothesis.

Noting $n=1$ is just notation and $n=2$ is * we have shown $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1} \ \forall n \in \mathbb{N}$.

Problem 4 (10pts) Suppose $|g| = n$ where $n \in \mathbb{N}$. Prove $|g| = |xgx^{-1}|$ for each $x \in G$.

$(xgx^{-1})^n = (xgx^{-1})(xgx^{-1})\cdots(xgx^{-1})$ ← Lemma: $(xgx^{-1})^n = xg^nx^{-1}$ $\forall n \in \mathbb{N}$. Can prove carefully via induction

$= xg^nx^{-1}$

$= xex^{-1}$: $|g| = n \Rightarrow g^n = e$

$= e$

Thus, $|xgx^{-1}| \leq n$. Suppose $\exists j < n$, $j > 0$ for which $(xgx^{-1})^j = e$

then $xg^jx^{-1} = e \Rightarrow x^{-1}xg^jx^{-1}x = x^{-1}ex \Rightarrow g^j = e$ ↛ $|g| = n$

Hence $\underline{|xgx^{-1}| = n}$.

Problem 5 (10pts) Consider $\mathbb{Z}_{100}$. Find all the generators for $\langle 5 \rangle$. *I'll give you a hint:* 5 *is one of them.*

$|\langle 5 \rangle| = \frac{100}{5} = 20$

$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$

$\Rightarrow$ 5, 15, 35, 45, 55, 65, 85, 95 generators of $\langle 5 \rangle$.

Problem 6 (5pts) Suppose there exist $x, y \in G$ with $x \neq y^2$ and $x^2 = 1$ and $y^4 = 1$. Is G cyclic? Argue for or against.

Observe $y^4 = (y^2)^2 = 1$ hence $|\langle x \rangle| = |\langle y^2 \rangle| = 2$

and $\langle x \rangle \neq \langle y^2 \rangle$ ∴ we have <u>two</u> (at least) distinct subgroups of order two ∴ G not cyclic as the FT of C.G. says just one subgroup of each order that divides $|G|$.

Problem 7 (5pts) Draw a Cayley table for $U(8)$.

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$U(8) = \{1, 3, 5, 7\}$

$(xy)(xy) = 1$

$\Rightarrow yx = x^{-1}y.$

Problem 8 (10pts) Recall $D_n = \{1, x, \ldots, x^{n-1}, y, xy, \ldots, x^{n-1}y\} = \langle x, y \mid x^n = 1, y^2 = 1, (xy)^2 = 1\rangle$. Use the relations for D_{10} to simplify $x^{-3}y^2x^{15}yx^4y^{-22}$

$x^{-3}y^2x^{15}yx^4y^{-22} = x^{-3}x^5yx^4 = x^2yxxx$

$= x^2x^{-1}yxxx$

$= x^2x^{-1}x^{-1}yxx$

$= x^2x^{-1}x^{-1}x^{-1}yx$

$= x^2x^{-1}x^{-1}x^{-1}x^{-1}y$

$= x^{-2}y = \boxed{x^8y}$

$x^{10} = 1$

Lemma: $yx^n = x^{-n}y$

Problem 9 (15pts) Let $\alpha = (1234)$ and $\beta = (3476)$. Define $\tau = \alpha\beta$

(a.) Calculate the disjoint cycle decomposition of τ

$\tau = \alpha\beta = (1234)(3476) = \boxed{(123)(476)}$

(b.) Find the order of τ

$\text{lcm}(3,3) = \boxed{3}$

(c.) Write τ as a product of transpositions.

$\tau = \boxed{(13)(12)(46)(47)}$ or $(14)(13)(12)(36)(37)(34)$.

(d.) Find the inverse of $\tau(89)$.

$(\tau(89))^{-1} = (89)^{-1}\tau^{-1} = \boxed{(89)(321)(674)}$

(e.) Calculate τ^{100}

$\tau^{100} = \tau^{99}\tau = (\tau^3)^{33}\tau = \boxed{\tau} = (123)(476)$.

Problem 10 (12pts) List the orders of elements in $\mathbb{Z}_{50}$. Then determine the number of elements of each order.

Order =	1	2	5	10	25	50
Number of elements =	1	1	4	4	20	20

$\phi(5^2) = 5^2 - 5 = 25 - 5 = 20$

$\phi(50) = \phi(2)\phi(25) = 20$

Problem 11 (12pts) List the orders of elements in D_{50}. Then determine the number of elements of each order.

Order =	1	2	5	10	25	50
Number of elements =	1	51	4	4	20	20

Problem 12 (6pts) Prove that if $x \equiv y$ and $x' \equiv y'$ modulo n then $xy \equiv x'y'$ modulo n.

(I intended $x \equiv x'$ and $y \equiv y' \Rightarrow xy \equiv x'y'$.)

Suppose $x \equiv x'$ and $y \equiv y' \pmod{n}$ then $\exists j, k \in \mathbb{Z}$ for which $x' = x + jn$ and $y' = y + kn$ hence,

$$x'y' = (x + jn)(y + kn)$$
$$= xy + n(jy + xk + jkn)$$

Thus $(x'y' - xy)$ is divided by $n \Rightarrow x'y' \equiv xy \pmod{n}$.

Problem 13 (15pts) Find $\langle A \rangle = \left\langle \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \right\rangle$ in $\mathrm{GL}_2(\mathbb{Z}_6)$. What is the order of A? What is A^{-1}?

$$A^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}$$

$$A^3 = \underbrace{\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}}_{A}\underbrace{\begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}}_{A^2} = \begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \therefore \underline{|A| = 3}.$$

Moreover, $A^2 A = I$, $A^2 = \boxed{A^{-1} = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}}$

and $\underline{\langle A \rangle = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix} \right\}}$.

Remark: $A^{-1} = (1-0)^{-1}\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} = \underline{\begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}}$.

Problem 14 (5pts) Define the symmetry group of the circle $x^2 + y^2 = 1$ in $\mathbb{R}^2$ in terms of isometries (a sentence will do). Then geometrically explain why the symmetry group of the circle has elements of finite and infinite order.

- The isometries which map the circle to itself are the symmetries of the circle; S_1 circle then $\Omega(S_1) = \{ \phi \in \mathrm{Isom}(\mathbb{R}^2) \mid \phi(S_1) = S_1 \}$

- Isometries are composites of rotations, translations and reflections. Certainly rotations fix S_1. If we rotate by an irrational fraction of 2π then we can never return to exact start point. However, $R\left(\frac{2\pi}{n}\right)$ has order n.

Problem 15 choose your own adventure... of proof.

(a) Choose one of the following: (20pts)

I. Suppose that $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$. Prove that G is abelian.

II. Suppose that $(ab)^2 = a^2b^2$ for all $a, b \in G$. Prove that G is abelian.

(b) Choose one of the following: (15pts)

I. Prove any subgroup of a cyclic group is cyclic.

II. Prove that $U(n) = \{x \in \mathbb{Z}_n \mid \gcd(n, k) = 1\}$ forms a group with respect to multiplication modulo n.