Instructions. Answer each of the questions on your own paper (except for problem 1, which should be answered on this paper), and be sure to show your work so that partial credit can be adequately assessed. Put your name on each page of your paper.

1. **[10 Points]** Fill in the blanks to complete the definition of group:

   A *group* is a set G together with a binary operation $*$ and a special element $e \in G$, called the $\boxed{\textbf{identity}}$,such that

   (a) for every x, y, $z \in G$,
   $$x * (y * z) = \boxed{(x * y) * z};$$

   (b) for all $x \in G$,
   $$x * e = \boxed{x} = e * x;$$

   (c) for every $x \in G$, there is $x' \in G$ with
   $$x * x' = \boxed{e} = x' * x.$$

   The element x' is called the $\boxed{\textbf{inverse}}$ of x.

2. **[20 Points]** Let G be a group and let $a \in G$.

   (a) Complete the definition of what it means for a to have finite order $o(a) = n$: *If n is a positive integer, then the element $a \in G$ has order n provided*

n is the smallest positive integer such that $a^n = e$.

   (b) Let $a \in G$ be an element of order $n = 3m$ and let $b = a^3$. What is the order of b? Prove that your answer is correct directly from the definition of order given in part (a).

   ▶ **Solution.** We claim that the order of b is m. To see this from the definition given above, note that $b^m = (a^3)^m = a^{3m} = a^n = e$. Moreover, if $0 < k < m$, then $0 < 3k < 3m = n$ and $b^k = (a^3)^k = a^{3k} \neq 3$ since $a^r \neq e$ for any positive integer $0 < r < n$, where $n = 3m$ is the order of a. Thus, we have shown that m is the smallest positive integer for which $b^m = e$, which means that $o(b) = m$. ◀

3. **[20 Points]** Let $G = \mathbb{Z}_{13}^*$.

   (a) What is the order of G?

   ▶ **Solution.** $|G| = |\mathbb{Z}_{13}^*| = \varphi(13) = 13 - 1 = 12$ (where $\varphi(n)$ denotes the Euler φ function). ◀

   (b) If $a \in G$, what are the possibilities for the order of a?

   ▶ **Solution.** Since $o(a)$ divides $|G| = 12$, it follows that $o(a)$ must be one of the divisors of 12, i.e., 1, 2, 3, 4, 6, or 12. ◀

(c) What is the order of the element $[2] \in G$?

▶ **Solution.** $[2]^4 = [3] \neq [1]$ so the order of $[2]$ is not 1, 2, or 4. Also, $[2]^6 = [-1] \neq [1]$ so the order of $[2]$ is not 3 or 6. Hence, from part (b), the only remaining possibility for the order of $[2]$ is 12. ◀

(d) Show that G is a cyclic group.

▶ **Solution.** Since $o([2]) = 12$ it follows that $|\langle [2] \rangle| = 12$ and since G also has order 12, it follows that the subgroup $\langle [2] \rangle$ is all of G. Hence, G is cyclic with generator $[2]$. ◀

4. **[16 Points]**

(a) State Lagrange's theorem.

▶ **Solution.** *If G is a finite group and H is a subgroup, then $|H|$ divides $|G|$.* ◀

(b) Suppose that H and K are subgroups of G and assume that the following data are given: $|H| = 9$, $|K| = 12$, $|G| < 100$. What are the possible values of $|G|$?

▶ **Solution.** From Lagrange's theorem $|G|$ must be a multiple of $|H| = 9$ and a multiple of $|K| = 12$. Hence $|G|$ must be a common multiple of 9 and 12, i.e., $|G|$ must be a multiple of $\text{lcm}[9, 12] = 36$. Since $|G|$ is assumed to be less than 100, this means that $|G|$ is 36 or 72. ◀

5. **[16 Points]**

(a) Give an example of two groups of order 6 which are not isomorphic. Explain why your examples are not isomorphic.

▶ **Solution.** $\mathbb{Z}_6$ and S_3 are both groups of order 6. However, $\mathbb{Z}_6$ is abelian and S_3 is not. Since abelian is a property of groups that is preserved by group isomorphism, it follows that $\mathbb{Z}_6$ and S_3 are not isomorphic. ◀

(b) Give an example of two groups of order 4 which are not isomorphic. Explain why your examples are not isomorphic.

▶ **Solution.** $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are both groups of order 4. Every element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2 or 1, while $\mathbb{Z}_4$ has two elements of order 4, namely $[1]_4$ and $[3]_4$. Thus, these two groups are not isomorphic since any group isomorphic to $\mathbb{Z}_4$ must have two elements of order 4. ◀

6. **[18 Points]** Let $H = \left\{ I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ A = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},\ B = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},\ C = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\}$.

   (a) The following table gives the multiplications between elements of H:

$\cdot$	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	A	I
C	C	B	I	A

   Explain why the above multiplication table shows that H is a subgroup of the group $\mathrm{GL}_2(\mathbb{R})$ of invertible 2×2 matrices with group operation matrix multiplication.

   ▶ **Solution.** H is a finite subset of the group $\mathrm{GL}_2(\mathbb{R})$, and from the table provided above, we see that whenever, x and y are in H, then so is the product xy (namely, every element of the multiplication table is an element of H). By the subgroup criterion for finite subsets of a group (Corollary 3.2.4, Page 105) it follows that H is a subgroup. ◀

   (b) Verify that $K = \{I,\ B\}$ is *not* a subgroup of H.

   ▶ **Solution.** Since $B^2 = A \notin K$, it follows that K is not closed under multiplication, and hence is not a subgroup of H. ◀

   (c) The set K is not a subgroup, but there is a subgroup of H consisting of 2 elements. Which two elements of H form a subgroup?

   ▶ **Solution.** $L = \{I,\ A\}$ is a subgroup, since all possible multiplications of elements of L, (given in the upper 2×2 left hand corner of the above multiplication table) are in L. ◀