Solutions

1. (3 points each) Give examples of the following, if they exist. Otherwise briefly explain why such examples do not exist.

   (a) Two nonisomorphic groups of order 20.

   Z_{20} and D_{10}. They are nonisomorphic because Z_{20} is abelian and D_{10} is not.

   (b) An infinite nonabelian group.
   $GL_2(\mathbb{R})$ or $SL_2(\mathbb{R})$ or similar with $\mathbb{R}$ replaced with $\mathbb{Q}$ or $\mathbb{C}$.

   (c) A group with two distinct subgroups of order 5.
   S_{10} with subgroups $H = \langle(1\,2\,3\,4\,5)\rangle$ and $K = \langle(6\,7\,8\,9\,10)\rangle$

   (d) A nonabelian group of order 11. not possible. We know all groups of prime order are cyclic and all cyclic groups are abelian.

   (e) An element of order 10 in S_7. $\alpha = (12)(34567)$, $|\alpha| = lcm(2, 5) = 10$.

   (f) An element of order 10 in A_7. not possible. We would need a 10-cycle, which isn't possible on 7 elements or we need a disjoint product of 2-cycles and 5-cycles. There is only room for ONE 2-cycle. Thus the permutation is odd.

2. (12 points) Consider the permutation group S_8, and let $\alpha = (1235)(24567)(1572)$.

   (a) Express α as a product of disjoint cycles.
   $(1674)(2)(35) = (1674)(35)$

   (b) What is the inverse of α?
   $(1476)(35)$

   (c) What is the order of α? 4, It's the least common multiple of 2 and 4.

   (d) Is α an even or odd permutation?
   even. $\alpha = (16)(17)(14)(35)$

3. (10 points)

   (a) State the definition of an automorphism of a group G.
   see text.

   (b) Find the group of automorphisms of the cyclic group Z_{18}.
   We know 1 generates Z_{18} and we know isomorphisms send generators to generators. Thus it is sufficient to find all generators of Z_{18}. Finally, we know that the generators of Z_{18} are those with exponents relatively prime to 18, namely: 1,5,7,11,13,17.
   Final answer:
   Let ϕ_i be defined as $\phi_i(a) = a^i$. Then $Aut(Z_{18}) = \{\phi_1, \phi_5, \phi_7, \phi_{11}, \phi_{13}, \phi_{17}\}$

   (c) List all subgroups of Z_{18}.
   We know subgroups correspond to divisors of 18, namely 1,2,3,6,8, and 18. Thus, Z_{18} has a unique subgroup of each of these orders.

Final answer:

order	subgroup
1	$\{1\}$
2	$\langle a^9\rangle = \{1, a^9\}$
3	$\langle a^6\rangle = \{1, a^6, a^{12}\}$
6	$\langle a^3\rangle = \{1, a^3, a^3, a^9, a^{12}\}$
9	$\langle a^2\rangle = \{1, a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}\}$
18	$\langle a\rangle = Z_{18}$

4. (10 points)

   (a) Show that $U(21)$ is not isomorphic to $\mathbb{Z}_{12}$.
   Recall that $U(21) = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$. Thus both $U(21)$ and $\mathbb{Z}12$ have 12 elements and both are abelian. Clearly we need to show that $U(21)$ isn't cyclic. Thus, we will look for distinct subgroups of the same order. An easy one is (using arithmetic mod 21) $20^2 = (-1)^2 = 1$ and a quick check (starting with 2,4,5) we find $8^2 = 64 = 1 \mod 21$. Since we have found two distinct subgroups of order 2: $\langle 20\rangle$ and $\langle 8\rangle$ we know $U(21)$ cannot be cyclic. Thus it cannot be isomorphic to $\mathbb{Z}_{12}$.

   (b) Show that D_6 is not isomorphic to A_4.

   Note that they are both nonabelian and both have 12 elements. I think the most obvious way to approach this is to consider orders of elements.

   We know D_6 contains a cyclic subgroup of order 6 – the subgroup of rotations. Thus, it has an element of order 6. On the other hand, we know A_4 only has elements of order 2 (like $(ab)(cd)$) or order 3 (like (abc)). You could also count the number of elements of order 2 in each group and show that those are not the same. Finally, we proved in class that A_4 cannot have a subgroup of order 6.

   Any one of those would suffice.

5. (20 points)

   (a) State the definition of a *group isomorphism*.
   see your text.

   (b) Define the following set of matrices:

$$G = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \,\middle|\, a \in \mathbb{Z} \right\}.$$

   The set G under matrix multiplication is a group. (You don't need to prove that G is a group.) Prove that G is isomorphic to $\mathbb{Z}$.

   Proof: Let $\phi : G \to \mathbb{Z}$ be defined as $\phi\left(\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}\right) = a$.
   ϕ is one-to-one: Assume there exist $M_1, M_2 \in G$ such that $\phi(M_1) = \phi(M_2) = a$. Then

by the definition of ϕ, $M_1 = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = M_2$. Thus, we have shown that ϕ is one-to-one.

<u>ϕ **is onto:**</u> Let $a \in \mathbb{Z}$. Then $M = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \in G$ and $\phi(M) = a$. Thus, we have shown that ϕ is onto.

<u>ϕ **is operation preserving:**</u> Now, for every $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \in G$,

$$\begin{aligned}
\phi\left(\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}\right) &= \phi\left(\begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}\right) && \text{(definition of matrix multiplication)} \\
&= a + b && \text{(definition of } \phi) \\
&= \phi\left(\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}\right) + \phi\left(\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}\right) && \text{(definition of } \phi)
\end{aligned}$$

6. (20 points)

   (a) State the definition of a *group*.
   see text.

   (b) Let $S = \{x \in \mathbb{R} \mid x \neq 0\}$ be the set of nonzero real numbers, and define a binary operation on S by the formula $a \star b = 2ab$. Is S with this binary operation a group? Prove or disprove.

   Yes. It is a group.
   <u>**Closure;**</u> For any two nonzero real numbers a and b, the number $2ab$ is a real number. So the set is closed under the operation.
   <u>**Associativity;**</u> Let $a, b, c \in S$. Now,

   $$a \star (b \star c) = a \star (2bc) = 2a2bc = 4abc,$$

   and

   $$(a \star b) \star c = (2ab) \star c = 2 \cdot 2abc = 4abc.$$

   Thus, associativity holds.
   <u>**Identity;**</u> Observe that $1/2 \in S$. For every $a \in S$, $(1/2) \star a = a = a \star (1/2)$. Thus, there exists an identity in S, namely $1/2$.
   <u>**Inverses;**</u> For every nonzero real number a, the number $1/(4a)$ is also a nonzero real number and $a \star \frac{1}{4a} = 2a/4a = 1/2 = \frac{1}{4a} \star a$. Thus, every element of S has an inverse in S.

7. (10 points) Prove that for any group G and any $a, b \in G$, $|ab| = |ba|$.
   Proof: We consider two cases: when $|ab|$ is infinite and when it is finite.
   <u>**Case 1:**</u> $|ab|$ is infinite.
   (by contradiction) Assume $|ba| = n > \infty$. Then $(ba)^n = e$. If we apply a on the left and b on the right of the previous equation we obtain $a(ba)^n b = ab$. But, using associativity, we see $a(ba)^n b = a(ba)(ba) \cdots (ba)b = (ab)^{n+1}$. Putting the previous two equations together we obtain $(ab)^{n+1} = ab$. Now we apply cancellation laws to obtain $(ab)^n = e$, a contradiction.

Thus, the order of ab is also infinite.

Case 2: $|ab|$ is finite.

Assume $|ab| = n$. Now using the same approach as above, we know $ba = bea = b(ab)^n a = (ba)^{n+1}$. Using the cancellation law, we conclude that $(ba)^n = e$. Thus $|ba| \mid n$. If we let $|ba| = m$ and apply the symmetric argument, we obtain $n \mid m$. Thus, $m = n$, which is what we wanted to prove.