SOLUTIONS

Show all of your work for complete credit and do not be afraid to write too much. It is better to have some incorrect steps than it is to leave a problem blank.

| Problem 1 | ______ 32 points |
| Problem 2 | ______ 22 points |
| Problem 3 | ______ 24 points |
| Problem 4 | ______ 22 points |
| Bonus     | ______ 10 points |

| Total     | ______ 100 points |
1. For each of the following statements, circle either true or false. If false, explain why or give a counterexample. If true, provide a proof.

(a) The subset of nonzero rational numbers $Q = \{2^n 4^m | n, m \in \mathbb{Z}\}$ forms a group under the operation of multiplication. True / False

True, note that $Q \subset \mathbb{Q}$ and $2^0 4^0 = 1 \in Q \implies Q \neq \emptyset$. So we only need to check that $Q$ is closed and that every element of $Q$ has an inverse.

$$(2^n 4^m)(2^{n'} 4^{m'}) = 2^{n+n'} 4^{m+m'} \in Q \implies Q \text{ is closed.}$$

$$(2^n 4^m)(2^{-n} 4^{-m}) = 1 \implies \text{every element of } Q \text{ has an inverse in } Q.$$ Thus, $Q$ is a subgroup of $\mathbb{Q}$ under the operation of multiplication.

(b) For every element $a$ in a group $G$, $C(a) \leq Z(G)$. True / False

False, the correct statement would have been $Z(G) \leq C(a)$ since every element of $Z(G)$ commutes with $a$ and is therefore in $C(a)$. As a counterexample, consider

$$D_4 = \{e, r, r^2r^3, s, sr, sr^2, sr^3 | s^2 = r^4 = e, sr = r^3s\}.$$ In this example, we have that $C(r) = \langle r \rangle$ and $Z(G) = \langle e \rangle$. 

1
(c) For all $a, b \in D_4$, $ab \neq ba$. True / False

False, There are many counterexamples. Here are a few:

\begin{align*}
r^n r^m &= r^m r^n, \forall n, m \in \{0, 1, 2, 3\}, \\
ab_a &= a^{-1} a, \forall a \in D_4, \\
ab e &= e a, \forall a \in D_4, \\
s a^2 &= r^2 s.
\end{align*}

(d) The set $N = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}$ is a cyclic subgroup of $SL_2(\mathbb{R})$. True / False

True, first note that $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in N$ shows that $N$ is not the empty set. Also, $N \subseteq SL_2(\mathbb{R})$ since

$$\det \left( \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \right) = 1.$$ 

Thus, we only need to show that $N$ is closed and that every element of $N$ has an inverse inside $N$. This follows from:

\begin{align*}
\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & n + m \\ 0 & 1 \end{pmatrix} \in N, \\
\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\
\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
\end{align*}

The subgroup $N$ is cyclic since

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$
2. Find all of the cyclic subgroups of the group $U(14)$. Are there any subgroups of $U(14)$ that are not cyclic? Explain your answer.

$U(14) = \{1, 3, 5, 9, 11, 13\}$

$\langle 1 \rangle = \{1\}$

$\langle 3 \rangle = \{1, 3, 5, 9, 11, 13\} = U(14) = \langle 5 \rangle$

$\langle 9 \rangle = \{1, 9, 11\} = \langle 11 \rangle$

$\langle 13 \rangle = \{1, 13\}$

We proved in class that every subgroup of a cyclic group must be cyclic. Since $U(14) = \langle 3 \rangle$, there are no subgroups which are not cyclic.
3. Let \( p \) and \( q \) be two distinct primes of the additive group \( \mathbb{Z} \).

(a) Prove that the set \( \langle p \rangle \cap \langle q \rangle \) is a subgroup of \( \mathbb{Z} \).

\[
\langle p \rangle \text{ and } \langle q \rangle \text{ are both groups } \quad \implies 0 \in \langle p \rangle, \ 0 \in \langle q \rangle \\
\implies 0 \in \langle p \rangle \cap \langle q \rangle \\
\implies \langle p \rangle \cap \langle q \rangle \neq \emptyset
\]

Since \( \langle p \rangle \cap \langle q \rangle \subseteq \langle p \rangle \), we only need to check for closure and the existence of inverses. Let \( x, y \in \langle p \rangle \cap \langle q \rangle \). Both \( \langle p \rangle \) and \( \langle q \rangle \) are groups so that \( x + y \in \langle p \rangle \) and \( x + y \in \langle q \rangle \). Thus, \( x + y \in \langle p \rangle \cap \langle q \rangle \). Similarly, \( -x \in \langle p \rangle \) and \( -x \in \langle q \rangle \) giving \( -x \in \langle p \rangle \cap \langle q \rangle \).

(b) Prove that the subgroup \( \langle p \rangle \cap \langle q \rangle \) is cyclic by explicitly finding its generator.

Claim: \( \langle pq \rangle = \langle p \rangle \cap \langle q \rangle \).

If \( x \in \langle pq \rangle \), then \( x = pqk \) for some \( k \in \mathbb{Z} \). Hence, \( x \in \langle p \rangle \) and \( x \in \langle q \rangle \) \( \implies \) \( x \in \langle p \rangle \cap \langle q \rangle \) and we conclude that

\[
\langle pq \rangle \subseteq \langle p \rangle \cap \langle q \rangle . \tag{1}
\]

Now suppose that \( y \in \langle p \rangle \cap \langle q \rangle \). Since \( y \in \langle p \rangle \), we have that \( y = pa \) for some \( a \in \mathbb{Z} \). Also, \( y \in \langle q \rangle \) gives \( q | y \implies q | pa \). However, we are assuming that \( p \) and \( q \) are distinct primes. By Euclid’s Lemma, \( q | a \). Writing \( a = q\ell \) for some \( \ell \in \mathbb{Z} \), we have \( y = pa = pq\ell \in \langle pq \rangle \).

Thus

\[
\langle p \rangle \cap \langle q \rangle \subseteq \langle pq \rangle . \tag{2}
\]

Putting together (1) and (2), we complete the proof of the claim.
4. Let $a$ be an element of a group $G$. Prove that the set

$$H = \{aga^{-1} \mid g \in G\}.$$

is a subgroup of $G$.

The set $H$ is nonempty since $aea^{-1} = aa^{-1} = e \in H$. So, again we only need to check closure and the existence of inverses. Let $axa^{-1}, aya^{-1} \in H$. Then

$$(axa^{-1})(aya^{-1}) = ax(a^{-1}a)ya^{-1} = a(xy)a^{-1} \in H.$$ 

Also, if $axa^{-1} \in H$, then

$$(axa^{-1})(ax^{-1}a^{-1}) = ax(a^{-1}a)x^{-1}a^{-1} = a(x^{-1}a)^{-1} = aa^{-1} = e,$$

$$(ax^{-1}a^{-1})(axa^{-1}) = ax^{-1}(a^{-1}a)x(a^{-1}) = a(x^{-1}x)a^{-1} = aa^{-1} = e.$$ 

Thus, $H$ is closed and every element in $H$ has an inverse in $H$, proving that $H \leq G$. The group $H$ (which depends upon the fixed element $a \in G$) is called a conjugate of $G$. 

5
BONUS  Let $G$ and $G'$ be groups and assume that $f : G \rightarrow G'$ is a function that satisfies the property

$$f(g_1g_2) = f(g_1)f(g_2), \quad \text{for all } g_1, g_2 \in G. \quad (3)$$

Prove that the image of $G$ under $f$ (denoted $Im(f)$) is a subgroup of $G'$. In other words, prove that

$$Im(f) = \{f(g) \mid g \in G\} \leq G'.$$

Since we are considering two groups $G$ and $G'$ in this problem, the identities will be denoted by $e_G$ and $e_{G'}$, respectively. We first need to show that $Im(f)$ is a nonempty subset of $G'$. If $g \in G$, then by property (3), we have that

$$f(g) = f(ge_G) = f(g)f(e_G),$$

$$f(g) = f(e_Gg) = f(e_G)f(g),$$

which proves that $f(e_G) = e_{G'} \in Im(f)$. To see that $Im(f)$ is closed, let $f(g_1), f(g_2) \in Im(f)$. Then

$$f(g_1)f(g_2) = f(g_1g_2) \in Im(f).$$

Now suppose that $f(g) \in Im(f)$. Then

$$f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_{G'},$$

$$f(g^{-1})f(g) = f(g^{-1}g) = f(e_G) = e_{G'},$$

implying that $f(g^{-1}) = (f(g))^{-1} \in Im(f)$. Functions between groups that satisfy property (3) are called homomorphisms and will play an important role in the material that we will soon be covering. In particular, we just proved that a homomorphism preserves the group structure of $G$ in $G'$. 

6