SOLUTIONS FOR PROBLEM SET 6

A. Suppose that $G$ is a group and that $H$ is a subgroup of $G$ such that $[G : H] = 2$. Suppose that $a, b \in G$, but $a \not\in H$ and $b \not\in H$. Prove that $ab \in H$.

SOLUTION: Since $[G : H] = 2$, it follows that $H$ is a normal subgroup of $G$. Consider the quotient group $G/H$. It is a group of order 2. The identity element in that group is $H$. The other element (the element which is not the identity) in that group is of order 2. If $a \in G$, but $a \not\in H$, then $aH$ is that other element in $G$. Thus, we have $(aH)^2 = H$. However, if $b \in G$, but $b \not\in H$, then $bH$ is also the other element. That is, we have $bH = aH$.

Therefore, we have $(aH)(bH) = (aH)(aH) = (aH)^2 = H$. Now, $(aH)(bH) = abH$. Thus, we have $abH = H$. This means that $ab \in H$, which is what we wanted to prove.

B: This problem concerns the group $G = \mathbb{Q}/\mathbb{Z}$. We will use the symbol $+$ for the group operation. The identity element in $G$ is $0 + \mathbb{Z} = \mathbb{Z}$ and will be denoted by $e$.

(a) We will prove that every element of $G$ has finite order. If $g \in G$, then $g = r + \mathbb{Z}$, where $r \in \mathbb{Q}$. There exists a positive integer $n$ such that $nr \in \mathbb{Z}$. (For example, one could write $r$ in reduced form and let $n$ be the denominator of $r$.) We then have

$$ng = n(r + \mathbb{Z}) = nr + \mathbb{Z} = \mathbb{Z},$$

the last equality following from the fact that $nr \in \mathbb{Z}$. The second equality is a consequence of the definition of addition in the quotient group $\mathbb{Q}/\mathbb{Z}$. We have proved that $ng$ is the identity element in $G$ and therefore $g$ has finite order. Thus, every element of $G$ indeed has finite order.

(b) We will prove that every finite subgroup of $G$ is a cyclic group. Suppose $H$ is a finite subgroup of $G$. Let $|H| = t$. Then $H = \{h_1, ..., h_t\}$, where $h_i = r_i + \mathbb{Z}$ and $r_i \in \mathbb{Q}$ for $1 \leq i \leq t$. We can write the rational numbers $r_1, ..., r_t$ in the following way

$$r_i = \frac{n_i}{m}$$

where $m$ is a positive integer and $n_i \in \mathbb{Z}$ for $1 \leq i \leq t$. To do this, we can take $m$ to be any positive integer which is a multiple of the denominators of all the rational numbers $r_1, ..., r_t$, i.e., a common denominator for those rational numbers. Let

$$a = \frac{1}{m} + \mathbb{Z} \in G$$

1
Then we have
\[ n_i a = n_i \left( \frac{1}{m} + \mathbb{Z} \right) = \frac{n_i}{m} + \mathbb{Z} = r_i + \mathbb{Z} = h_i \]
for \( 1 \leq i \leq t \). Therefore, \( H \subset \langle a \rangle \), the cyclic subgroup of \( G \) generated by \( a \). Since \( H \) is a subgroup of a cyclic group, we can conclude that \( H \) itself is a cyclic group. We are using one of the propositions we have proved about cyclic groups.

(c) An example of a proper subgroup of \( G \) which is infinite. Let

\[ H = \{ g \in G \mid |g| = 2^m, \text{ where } m \text{ is a nonnegative integer} \} \]

To verify that \( H \) is a subgroup of \( G \), note that the identity element has order 1 = \( 2^0 \) and so is in \( H \). Also, if \( h \in H \), then its inverse \(-h\) has the same order as \( h \) and so the inverse \(-h\) is in \( H \). Also, if \( h_1, h_2 \in H \), then let their orders be \( 2^{m_1}, 2^{m_2} \), respectively. Let \( m = \max\{m_1, m_2\} \). Then \( 2^m h_1 = e \) and \( 2^m h_2 = e \), where \( e \) is the identity element of \( G \). Since \( G \) is an abelian group, we have

\[ 2^m(h_1 + h_2) = 2^m h_1 + 2^m h_2 = e + e = e \]

and so the order of \( h_1 + h_2 \) must divide \( 2^m \). It follows (from number theory) that \( |h_1 + h_2| \) is a power of 2 and therefore \( h_1 + h_2 \in H \). Thus, \( H \) is closed under the group operation for \( G \). We have verified that \( H \) is a subgroup of \( G \).

Suppose \( m \) is any positive integer. Let \( h_m = \frac{1}{2^m} + \mathbb{Z} \). Then

\[ 2^m h_m = 2^m \left( \frac{1}{2^m} + \mathbb{Z} \right) = 1 + \mathbb{Z} = \mathbb{Z} = e, \quad 2^{m-1} h_m = 2^{m-1} \left( \frac{1}{2^m} + \mathbb{Z} \right) = \frac{1}{2} + \mathbb{Z} \neq e \]

and hence \( h_m \) has order equal to \( 2^m \). Thus, the cyclic subgroup \( \langle h_m \rangle \) has order \( 2^m \). Since \( m \) can be chosen as large as we wish, it is clear that \( H \) cannot be finite.

To show that \( H \neq G \), consider the element \( g = \frac{1}{3} + \mathbb{Z} \in G \). Clearly, \( g \neq e \) and \( 3g = e \). Thus, \( g \) has order 3 and so \( g \notin H \). Hence \( H \neq G \).

(d) We will prove that if \( H \) is a subgroup of \( G \) such that \( [G : H] \) is finite, then \( H = G \). 

**Proof.** Suppose that \( H \) is a subgroup of \( G \) of finite index. Since \( G \) is abelian, \( H \) will be a normal subgroup of \( G \). The quotient group \( G/H \) is finite, by assumption. Let \( n = |G/H| \). Then every element of \( G/H \) has order dividing \( n \). This means that, for every \( g \in G \), \( n(g + H) \) is the identity element of \( G/H \), which is the coset \( H \). Thus, \( n(g + H) = H \). But, \( n(g + H) = ng + H \). It follows that \( ng \in H \) for all \( g \in G \).
Let \( nG \) denote \( \{ng \mid g \in G \} \). We have proved that \( nG \subseteq H \subseteq G \). We will now prove that \( nG = G \). To see this, suppose that \( f \in G \). Write \( f = r + \mathbb{Z} \), where \( r \in \mathbb{Q} \). Let \( s = \frac{1}{n}r \). Then \( s \in \mathbb{Q} \). Let \( g = s + \mathbb{Z} \). Then

\[
ng = n(s + \mathbb{Z}) = ns + \mathbb{Z} = r + \mathbb{Z} = f.
\]

Since \( f \in G \) is arbitrary, we have proved that \( nG = G \). Since \( nG \subseteq H \subseteq G \), we can now conclude that \( H = G \).

**C:** Suppose that \( G \) is a group and that \( N \) and \( M \) are normal subgroups of \( G \). TRUE OR FALSE: If \( G/M \cong G/N \), then \( N \cong M \). If this statement is true, give a proof. If it is false, give a specific counterexample.

**SOLUTION:** The statement is false. Here is a counteexample. Let \( G = D_4 \), the group of symmetries of a square. We can regard \( D_4 \) as a subgroup of \( S_4 \). Suppose that \( N \) is the Klein 4-group. Then \( N \) is a subgroup of \( D_4 \) and \( [G : N] = |G|/|N| = 8/4 = 2 \). Since the index is 2, it follows that \( N \) is a normal subgroup of \( G \). Furthermore, \( G/N \) is a group of order 2. It must be a cyclic group of order 2. Note that every element of \( N \) has order 1 or 2. Thus, \( N \) has no element of order 4.

On the other hand, let \( M \) be the subgroup of \( D_4 \) consisting of the rotations. Then \( M \) is a cyclic group of order 4. It has two elements of order 4. Furthermore, we have \( [G : M] = |G|/|M| = 8/4 = 2 \). Thus \( M \) is a normal subgroup of \( G \) and \( G/M \) is a group of order 2. Thus, \( G/M \) is a cyclic group of order 2.

Thus, both \( G/N \) and \( G/M \) are cyclic groups of order 2 and are therefore isomorphic to each other. However, \( N \) and \( M \) are not isomorphic to each other. The group \( M \) has elements of order 4, but the group \( N \) has no such elements.

**D:** If \( G \) is an abelian group, then every subgroup of \( G \) is a normal subgroup. Is the converse of that fact true? If true, give a proof. If false, give a counterexample.

**SOLUTION:** The statement is false. The group \( G = Q_8 \) is a counterexample. This group is nonabelian. However, every subgroup of \( G \) is a normal subgroup of \( G \). This is obvious for \( G \) itself and for the trivial subgroup \( \{1\} \). It is also true for any subgroup \( H \) of \( G \) such that \( |H| = 4 \). This is so because if \( |H| = 4 \), then \( [G : H] = 2 \). Therefore, such a subgroup \( H \) will be a normal subgroup of \( G \).
It remains to consider subgroups $H$ of $G$ such that $|H| = 2$. However, there is only one such subgroup, namely $H = \{1, -1\}$. But this subgroup is actually the center of $G$, and is therefore a normal subgroup of $G$.

**E:** Suppose that $G$ is a group. Suppose that $a, b \in G$. We proved the following result in class one day: If $a$ is conjugate to $b$ in $G$, then $|a| = |b|$.

In general, the converse is not true. Consider the groups $G = S_n$ where $n \geq 1$. Show that the converse of the above result is true if $n \leq 3$, but that the converse is false if $n \geq 4$.

**SOLUTION:** The converse is the following statement: If $|a| = |b|$, then $a$ is conjugate to $b$ in $G$.

In any group, the identity element is the only element of order 1, and is certainly conjugate to itself. Thus, we need only consider elements which are not of order 1.

The group $S_3$ contains two elements of order 3, namely $(123)$ and $(132)$, both of which are 3-cycles and therefore conjugate to each other in $S_3$. Also, $S_3$ contains 3 elements of order 2, namely $(12), (13)$, and $(23)$. They are all 2-cycles and therefore conjugate to each other in $S_3$. This takes care of all the elements of $S_3$.

The converse is also true for $S_1$ and $S_2$ which have only one element of each possible order.

Now consider $S_n$ where $n \geq 4$. We know that two elements $a$ and $b$ in $S_n$ are conjugate in $S_n$ if and only if $a$ and $b$ have the same cycle decomposition type. Consider the following two elements:

$$a = (1 \ 2) \quad \text{and} \quad b = (1 \ 2)(3 \ 4) \ .$$

Since $n \geq 4$, we can consider $a$ and $b$ as elements in $S_n$. Both $a$ and $b$ have order 2. However, their cycle decomposition types are different. Therefore, $a$ and $b$ cannot be conjugate in $S_n$. This shows that the statement in this question is false when $G = S_n$ and $n \geq 4$.

**F:** Suppose that $G$ is a group of order 35. Suppose that $H$ is a subgroup of $G$ and that $H$ has order 7. Prove that $H$ is a normal subgroup of $G$. Furthermore, prove that if $g \in G$ has order 7, then $g \in H$.

**SOLUTION:** In general, suppose that $G$ is a group and that $H$ is a subgroup of finite index. Let $n = [G : H]$. We proved in class that there exists a homomorphism $\varphi : G \to S_n$ such
that $\text{Ker}(\varphi) \subseteq H$. This homomorphism is the so-called Generalized Cayley Homomorphism corresponding to the subgroup $H$ of $G$.

Suppose that $G$ is a group of order 35 and that $H$ is a subgroup of $G$ of order 7. Then we have $n = [G : H] = |G|/|H| = 35/7 = 5$. By the proposition just cited, there exists a homomorphism $\varphi : G \rightarrow S_5$ such that $\text{Ker}(\varphi) \subseteq H$. Let $K = \text{Ker}(\varphi)$. Thus, $K$ is a subgroup of $H$. By Lagrange’s theorem, $|K|$ divides $|H| = 7$. Hence $|K| = 1$ or 7.

If $|K| = 1$, then $\varphi$ would be injective and therefore $G$ would be isomorphic to $\varphi(G)$, a subgroup of $S_5$. Therefore, $S_5$ would then have a subgroup of order 35. By Lagrange’s theorem, it would then follow that 35 divides $|S_5|$. However, $|S_5| = 120$ which is not divisible by 35. It follows that $|K| \neq 1$.

We have therefore proved that $|K| = 7$. Since $K \subseteq H$ and $|H| = 7$, it follows that $H = K$. Since $K$ is the kernel of a homomorphism, $K$ must be a normal subgroup of $G$. Hence $H$ is a normal subgroup of $G$.

Finally, suppose that $g \in G$ and $|g| = 7$. Then $g^7 = e$, the identity element in $G$. Thus, $g^7 \in H$. Since $H$ is a normal subgroup of $G$, we can consider the quotient group $G/H$. The group $G/H$ has order equal to $\left[ G : H \right] = |G|/|H| = 35/7 = 5$. The identity element in $G/H$ is $H$. Consider the element $gH$ in $G/H$. Let $k$ denote the order of $gH$. Since $G/H$ is a group of order 5, we know that $k$ divides 5. Thus, $k = 1$ or $k = 5$. Furthermore, since $g^7 \in H$, we have

$$(gH)^7 = g^7H = H$$

and therefore $gH$ is an element of $G/H$ whose order must divide 7. Thus, $k$ divides 7. Since 5 does not divide 7, we have $k \neq 5$. Therefore, $k = 1$. It follows that $gH = H$. This implies that $g \in H$, as we wanted to prove.

**G:** Let $G = S_n$, where $n \geq 3$. Let $H = \{ \sigma \in G \mid \sigma(n) = n \}$. Then $H$ is a subgroup of $G$ and $[G : H] = n$. As explained in class, there is a homomorphism $\varphi : G \rightarrow S_n$ which we called the “Generalized Cayley Homomorphism corresponding to the subgroup $H$ of $G$”. Show that $\varphi$ is an isomorphism from $G$ to $S_n$.

**SOLUTION:** Notice that $\varphi$ is a homomorphism from $G$ to $S_n$, and both groups have order $n!$. To prove that $\varphi$ is bijective, it suffices to prove that $\varphi$ is injective. That is, it suffices to prove that $\text{Ker}(\varphi) = \{i\}$, where $i$ denotes the identity element in $G$. Let $X = \{1, 2, \ldots, n\}$. Then $i$ is just the identity map of $X$ to itself.

Let $N = \text{Ker}(\varphi)$. Then $N$ is a normal subgroup of $G = S_n$. We also know that $N \subseteq H$. We want to prove that $N = \{i\}$. Suppose to the contrary that $N \neq \{i\}$. We will obtain a contradiction, thereby proving that $N = \{i\}$. This will complete the proof.
Suppose that $\sigma \in N$, but $\sigma \neq i$. Now $\sigma$ is a bijection of the set $X = \{1, 2, \ldots, n\}$ to itself. Furthermore, since $\sigma \in H$, we know that $\sigma(n) = n$. Also, since $\sigma \neq i$, there exists at least one $x \in X$ such that $\sigma(x) \neq x$. Thus, we must have $x \neq n$. Let $y = \sigma(x)$. Thus, $y \neq x$. Since $x \neq n$ and $\sigma$ is a bijection, it follows that $\sigma(x) \neq \sigma(n)$. That is, $y \neq n$. Thus, we have $1 \leq y \leq n - 1$ and $y \neq x$.

Let $\tau$ be the 2-cycle $(x \ n)$, regarded as an element of $S_n$. Thus, we have $\tau(x) = n$. But $y \neq x$ and $y \neq n$, and so $\tau(y) = y$. Let $\sigma' = \tau \sigma \tau^{-1}$. By the Conjugacy Principle, and the fact that $\sigma(x) = y$, it follows that

$$\sigma'(\tau(x)) = \tau(y)$$

which means that $\sigma'(n) = y$. But $y \neq n$ and hence $\sigma'(n) \neq n$. Therefore, $\sigma' \notin H$. Since $N \subseteq H$, it follows that $\sigma' \notin N$.

Thus, we have $\sigma \in N$, but $\sigma' = \tau \sigma \tau^{-1} \notin N$. Therefore, $\tau N \tau^{-1} \neq N$. This contradicts the fact that $N$ is a normal subgroup of $G$. Therefore, we can now conclude that $N = \{i\}$. This suffices to conclude that $\varphi$ is a bijective map and therefore an isomorphism from $G$ to $S_n$. 
