MATH 402A - Solutions for Homework Assignment 3

Problem 7, page 55: We wish to find $C(a)$ for each $a \in S_3$. It is clear that $C(i) = S_3$. For any group $G$ and any $a \in G$, it is clear that every power of $a$ commutes with $a$ and therefore

$$(a) \subseteq C(a)$$

For $G = S_3$, there are six subgroups: $\{i\}$, one subgroup of order 3 generated by $f = (123)$, three subgroups of order 2, generated by $g = (13)$, $g' = (23)$, or $g'' = (13)$, and one subgroup of order 6, namely $S_3$ itself. Also note that every element $a \in S_3$ has order 2 or 3, except $a = i$.

Observe that if $H$ is a subgroup of $S_3$ of order 2 or order 3, then the only subgroups of $S_3$ containing $H$ are $H$ itself and $S_3$. (Such subgroups are called “maximal” subgroups.) This is clear from the above list of subgroups of $S_3$. (One could also see this by using Lagrange’s theorem concerning the orders of subgroups of a finite group.)

Suppose $a \in S_3$ has order 2 or 3. Let $H = (a)$, which has the same order as the element $a$. As pointed out above, we have $H \subseteq C(a)$. According to the observation in the previous paragraph, either $C(a) = H$ or $C(a) = S_3$. However, $C(a) = S_3$ implies that $a$ is in the center of $S_3$. This is not possible if $a$ has order 2 or 3 because $Z(S_3) = \{i\}$, as we pointed out one day in class. Therefore, $C(a) = (a)$ for every element $a \in S_3$ except $a = i$. That is, if $a = (123)$ or $a = (132)$, then $C(a) = (a) = \{i, (123), (132)\}$. If $a = (12), (13)$ or $(23)$, then $C(a) = \{i, a\}$ in each case.

Problem 10, page 55: We assume $G$ is an abelian group and $n$ is a positive integer. Let

$$A_n = \{a^n \mid a \in G\}$$

To see that $A_n$ is a subgroup of $G$, we verify the three requirements for a subgroup. First of all, let $e$ denote the identity element of $G$. Then $e = e^n$ and so $e \in A_n$. Now if $b \in A_n$, then $b = a^n$ for some $a \in G$. By the law of exponents, $b^{-1} = (a^{-1})^n$ and so $b^{-1} \in A_n$.

It remains to verify that $A_n$ is close under the group operation for $G$. Suppose that $c, d \in G$. We can write $c = a^n, d = b^n$, where $a, b \in G$. We have

$$(1) \quad a^n b^m = (ab)^n$$

for any positive integer $n$. This is because $G$ is assumed to be abelian. To prove (1), we use mathematical induction. For $n = 1$, (1) is obvious. Suppose (1) is true for some positive integer $n$. Then

$$(ab)^{n+1} = (ab)(ab)^n = (a^n b^n)(ab) = a^n(b^na)b = a^n(ab^n)b = (a^n a)(b^n b) = a^{n+1}b^{n+1}$$
which proves the identity for exponent \( n + 1 \). Hence, by the principle of mathematical induction, (1) holds for all \( n \geq 1 \).

Using (1), we obtain \( cd = a^n b^n = (ab)^n \). Since \( ab \in G \), it follows that \( cd \in A_n \). Hence \( A_n \) is closed under the group operation for \( G \).

**Problem 16, page 55:** Suppose that \( G \) is a group with no proper subgroups. Let \( e \) be the identity element of \( G \). One such group is \( G = \{ e \} \), which does not have prime order. Apart from this example, we will prove that \( G \) is finite and has prime order. Assume now that \( G \) has an element \( a \neq e \). We will fix such an element \( a \) in the rest of the argument.

First of all, \( G \) must be cyclic. To see this, consider \( H = (a) \), a subgroup of \( G \) containing \( a \). Hence \( H \neq \{ e \} \). Therefore, our assumption about \( G \) implies that \( H = G \). Thus, \( G = (a) \), the cyclic group generated by \( a \).

Now suppose that \( a \) has infinite order. This means that \( a^i \neq a^j \) for all pairs \( i, j \in \mathbb{Z} \) such that \( i \neq j \). Consider \( K = (a^2) \). This subgroup is \( \{a^{2j} \mid j \in \mathbb{Z} \} \). Since \( 2j \neq 1 \) for all \( j \in \mathbb{Z} \), we have \( a^{2j} \neq a^1 = a \). Thus, \( a \notin K \). Therefore, \( K \neq G \). Also, \( a^2 \neq e \) since \( a \) has infinite order. Thus, \( K \neq \{ e \} \). Therefore, \( K \) is a proper subgroup of \( G \). This contradicts our assumption about \( G \). Therefore, \( a \) must have finite order.

Suppose now that the order of \( a \) is \( m \). Then \( G = (a) \) has order \( m \). Since \( a \neq e \), we have \( m > 1 \). We will prove that \( m \) is a prime. Assume to the contrary that \( m = cd \), where \( c, d \in \mathbb{Z} \) with \( 1 < c, d < m \). Let \( b = a^d \). Let \( K = (b) \). Since \( 0 < d < m \), we have \( b = a^d \neq e \) and hence \( K \neq \{ e \} \). Therefore, by the assumption about \( G \), we have \( K = G \). Thus \( K \) has order \( m \). This means that \( b = a^d \) has order \( m \). However, \( b^c = a^{dc} = a^m = e \) and \( 0 < c < m \). Hence \( b \) cannot have order \( m \). This is a contradiction. Therefore, \( m \) is prime and hence, indeed, \( G \) has prime order.

**Problem 17, page 55:** Suppose \( G \) is a group and \( x, a \in G \). Let \( e \) be the identity element of \( G \). We want to prove that \( C(x^{-1}ax) = x^{-1}C(a)x \).

Two lemmas will be helpful.

**Lemma 1:** If \( u, v \in G \), then \( x^{-1}(uv)x = (x^{-1}ux)(x^{-1}vx) \).

The proof of this lemma is as follows:

\[
(x^{-1}ux)(x^{-1}vx) = (x^{-1}u)(xx^{-1})(vx) = (x^{-1}u)e(vx) = x^{-1}(uv)x
\]

**Lemma 2:** If \( u, v \in G \) and \( x^{-1}ux = x^{-1}vx \), then \( u = v \).
The proof of this lemma is as follows:

\[ x^{-1}ux = x^{-1}vx \quad \Rightarrow \quad x(x^{-1}ux)x^{-1} = x(x^{-1}vx)x^{-1} \quad \Rightarrow \quad eue = eve \quad \Rightarrow \quad u = v \]

1. We first prove the inclusion \( x^{-1}C(a)x \subseteq C(x^{-1}ax) \). Suppose that \( b \in x^{-1}C(a)x \). Then \( b = x^{-1}cx \) where \( c \in C(a) \). By definition, we have \( ca = ac \). Then, by lemma 1,

\[ b(x^{-1}ax) = (x^{-1}cx)(x^{-1}ax) = x^{-1}(ca)x = x^{-1}(ac)x = (x^{-1}ax)(x^{-1}cx) = (x^{-1}ax)b \]

and therefore \( b \in C(x^{-1}ax) \). Hence \( x^{-1}C(a)x \subseteq C(x^{-1}ax) \).

2. Now we prove the inclusion \( C(x^{-1}ax) \subseteq x^{-1}C(a)x \). Suppose that \( d \in C(x^{-1}ax) \). We can write \( d = x^{-1}cx \) for some \( c \in G \). To do this, simply take \( c = xd^{-1} \). Then

\[ x^{-1}cx = x^{-1}(xdx^{-1})x = (x^{-1}x)d(x^{-1}x) = ede = d \]

Now we use lemma 1 to obtain the following equations.

\[ d(x^{-1}ax) = (x^{-1}cx)(x^{-1}ax) = x^{-1}(ca)x, \quad (x^{-1}ax)d = (x^{-1}ax)(x^{-1}cx) = x^{-1}(ac)x. \]

Since \( d \in C(x^{-1}ax) \), we have \( d(x^{-1}ax) = (x^{-1}ax)d \). The above equations give

\[ x^{-1}(ca)x = x^{-1}(ac)x \]

Finally, by lemma 2, we have \( ca = ac \). Thus, \( c \in C(a) \). Therefore,

\[ d = x^{-1}cx \in x^{-1}C(a)x \]

proving the inclusion \( C(x^{-1}ax) \subseteq x^{-1}C(a)x \).

**Problem 19, page 55.** Suppose \( A \) and \( B \) are subgroups of an abelian group \( G \). Let \( H = AB = \{ab \mid a \in A, b \in B\} \). To see that \( H \) is a subgroup of \( G \), we verify the three requirements:

1. The identity element \( e \) of \( G \) is in \( A \) and \( B \). Since \( e = ee \), \( H \) contains \( e \) also.

2. \( H \) is closed under the group operation because if \( h_1 = ab \), \( h_2 = a_2b_2 \), where \( a_1, a_2 \in A \) and \( b_1, b_2 \in B \), then, using the assumption that \( G \) is abelian, we obtain

\[ h_1h_2 = (a_1b_1)(a_2b_2) = a_1(b_1a_2)b_2 = a_1(a_2b_1)b_2 = (a_1a_2)(b_1b_2). \]
Also, \( a_1a_2 \in A, \ b_1b_2 \in B \) since \( A \) and \( B \) are subgroups. Thus, \( h_1h_2 \in H \). This proves that \( H \) is closed under the group operation for \( G \).

3. Suppose \( h = ab \), where \( a \in A, \ b \in B \). Then

\[
h^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}
\]

and this is in \( H \) because \( a^{-1} \in A \) and \( b^{-1} \in B \).

We have proved that \( H \) is a subgroup of \( G \).

**Problem 20, page 55.** Let \( G = S_3 \). Let \( A = \{ i, (12) \} \) and \( B = \{ i, (23) \} \). Both \( A \) and \( B \) are subgroups of \( G \). Then

\[
AB = \{ i, (12), (23), (12)(23) \} = \{ i, (12), (23), (123) \}
\]

and this set is certainly not a subgroup of \( G \). The set contains (123), but not (123)

Thus, \( \sim \) is an equivalence relation on \( S \).

**Problem 1a, Page 63:** The set \( S \) is \( R \). For \( a, b \in R \), we write \( a \sim b \) if \( a - b \in Q \). Assume that \( a, b, c \in R \). We will verify (i) reflexivity, (ii) symmetry, and (iii) transitivity.

(i) \( a \sim a \) because \( a - a = 0 \in Q \), (ii) \( a \sim b \Rightarrow a - b \in Q \Rightarrow b - a \in Q \Rightarrow b \sim a \)

(iii) \( a \sim b, b \sim c \Rightarrow a - b, b - c \in Q \Rightarrow (a - b) + (b - c) \in Q \Rightarrow a - c \in Q \Rightarrow a \sim c \)

Thus, \( \sim \) is an equivalence relation on \( S \).

**Problem 1b, Page 63:** The set \( S \) is \( C \). For \( a, b \in C \), we write \( a \sim b \) if \( |a| = |b| \). Suppose that \( a, b, c \in C \).

(i) \( a \sim a \) because \( |a| = |a| \), (ii) \( a \sim b \Rightarrow |a| = |b| \Rightarrow |b| = |a| \Rightarrow b \sim a \),

(iii) \( a \sim b, b \sim c \Rightarrow |a| = |b|, |b| = |c| \Rightarrow |a| = |c| \Rightarrow a \sim c \)

Thus, \( \sim \) is an equivalence relation on \( S \).

**Problem 16, Page 64:** \( G = \{ a_1, ..., a_n \} \) is assumed to be an abelian group of order \( n \). Define \( f : G \to G \) by \( f(a) = a^{-1} \) for all \( a \in G \). Then \( f \) is a function that satisfies \( f \circ f = i \), the identity function from \( G \) to \( G \). This follows from the fact that \( (a^{-1})^{-1} = a \) for all \( a \in G \). Thus, \( f \) is an invertible function and must be a bijection from \( G \) to \( G \). Therefore,

\[
x = \prod_{i=1}^{n} a_i = \prod_{i=1}^{n} f(a_i) = \prod_{i=1}^{n} (a_i)^{-1} = (\prod_{i=1}^{n} a_i)^{-1} = (\prod_{i=1}^{n} a_i)^{-1} = x^{-1}
\]
We have repeatedly used the assumption that $G$ is abelian by rearranging the factors in some of the above products. In any case, we now have $x = x^{-1}$ and this implies that $x^2 = e$, the identity of $G$.

**Problem 17, Page 64:** We have $x^2 = e$. If $x \neq e$, then $x$ has order 2, by definition. We have proved that in any finite group $G$, the order of an element must divide the order of the group. Therefore, if $x \neq e$, then $|G|$ is divisible by 2. It follows that if $|G|$ is odd, then $x = e$.

**A:** Suppose $G$ is a group and $a \in G$ is an element of finite order. Let $m$ be the order of $a$. If $d$ is a positive divisor of $m$, determine the order of $a^d$. If $j \in \mathbb{Z}$, determine the order of $a^j$.

**Solution:** Suppose that $d$ is a positive divisor of $m$. Thus, $m = cd$, where $c$ is a positive integer. We will prove that $a^d$ has order equal to $c$. First of all, since $m$ is the order of $a$, we have $a^m = e$ and $a^t \neq e$ when $0 < t < m$. Here $e$ is the identity element of $G$. Now note that, by the law of exponents, we have $(a^d)^c = a^m = e$. Also, if $0 < i < c$, then $(a^d)^i = a^{di}$. But $0 < di < dc = m$ and hence $a^{di} \neq e$. Thus,

$$(a^d)^c = e, \quad (a^d)^i \neq e \quad \text{for } 0 < i < c$$

and therefore $a^d$ has order equal to $c = m/d$, as we stated.

Now consider $a^j$ where $j$ is any integer. Let $d = \gcd(j, m)$. We will prove that $a^j$ has the same order as $a^d$, namely $m/d$. The order of $a^j$ is equal to the order of the cyclic subgroup $H = (a^j)$ generated by $a^j$. The order of $a^d$ is equal to the order of the subgroup $K = (a^d)$ generated by $a^d$. Hence it suffices to prove that these subgroups are the same, which we will now prove. Since $H = (a^j)$, we have $a^j \in H$. Also, $a^m = e$. A basic theorem in elementary number theory implies that there exist $u, v \in \mathbb{Z}$ such that $uj + vm = d$. Therefore,

$$a^d = a^{uj + vm} = (a^j)^u(a^m)^v = (a^j)^u e^v = (a^j)^u \in H$$

It follows that every power of $a^d$ is in $H$ and so the subgroup $K = (a^d)$ must be contained in $H$. That is, $K \subseteq H$. However, since $d|j$, it is clear that $a^j$ is a power of $a^d$ and so $a^j \in K$. Hence $H \subseteq K$. Therefore, we have proved $H = K$. The stated result about the order of $a^j$ follows from this.

**B:** Let $G = A(T)$, where $T = \{1, 2, 3, 4\}$. Let $H = \{f \mid f \in G, f(4) = 4\}$.

First we show that $H$ is a subgroup of $G$. Clearly, $i \in H$ because $i(j) = j$ for all $j \in T$ and hence $i(4) = 4$. Also, if $f_1, f_2 \in H$, then $f_1(4) = 4, f_2(4) = 4$. Hence

$$f_1 \circ f_2(4) = f_1(f_2(4)) = f_1(4) = 4$$
This implies that \( f_1 f_2 = f_1 \circ f_2 \in H \). Thus, \( H \) is closed under the group operation for \( G \). Finally, suppose that \( f \in H \). Then \( f(4) = 4 \). Thus, the inverse function \( f^{-1} \) satisfies \( f^{-1}(4) = 4 \) and therefore \( f^{-1} \in H \). These remarks imply that \( H \) is a subgroup of \( G \).

Now suppose that \( g \in G \). We will consider the left coset \( gH \). Let \( j = g(4) \). Thus, \( j \in T \). Consider any element \( h \in H \). Then \( h(4) = 4 \) and

\[
g h(4) = g \circ h(4) = g(h(4)) = g(4) = j.
\]

Therefore, we have \( gH = \{gh \mid h \in H\} \subseteq \{f \mid f \in G, \ f(4) = j\} \).

To prove the reverse inclusion, suppose that \( f \in G \) satisfies \( f(4) = j \). Thus, \( f(4) = g(4) \). We can write \( f = gu \) by letting \( u = g^{-1}f \in G \). We want to prove that \( u \in H \). We have

\[
u(4) = g^{-1} f(4) = g^{-1} \circ f(4) = g^{-1}(f(4)) = g^{-1}(j) = 4,
\]

the final equality following from the fact that \( g(4) = j \) and \( g^{-1} \) is the inverse function for \( g \). Therefore, \( u(4) = 4 \), \( u \in H \), and \( f = gu \in gH \). This proves the inclusion

\[
\{f \mid f \in G, \ f(4) = j\} \subseteq gH.
\]

Combining the two inclusions, we see that \( \{f \mid f \in G, \ f(4) = j\} = gH \). Therefore, each left coset of \( H \) in \( G \) is indeed of the form stated in the problem.

The right cosets have the following description. If \( g \in G \) and \( g^{-1}(4) = j \), where \( j \in T \), then

\[
Hg = \{f \mid f \in G, \ f(j) = 4\}
\]

The proof is similar to the one for the left cosets. We have \( g(j) = 4 \). If \( h \in H \), then \( h(4) = 4 \) and so

\[
h g(j) = h(g(j)) = h(4) = 4
\]

and so \( h g \in \{f \mid f \in G, \ f(j) = 4\} \). Hence, \( Hg \subseteq \{f \mid f \in G, \ f(j) = 4\} \). Conversely, suppose \( f(j) = 4 \), then write \( f = u g \) where \( u \in G \). We have \( 4 = f(j) = u(g(j)) = u(4) \) and hence \( u \in H \). Thus, \( f \in Hg \). This proves the inclusion \( \{f \mid f \in G, \ f(j) = 4\} \subseteq Hg \). Therefore, the equality (2) is proved.