Assignment 01

Due Time : 8:15, March 11, 2020 (Wednesday)

Name : 陈 稼 霖
Student ID : 45875852
Score : _____

Problem 1 Score: _____. Let E be the identity of a group G, a and b be any two elements in the group, a^{-1} and b^{-1} be respectively the inverse of a and b. Using the definition of a group, show that

(1) If $ca = a$, then $c = E$;

(2) If $ca = E$, then $c = a^{-1}$;

(3) The inverse of (ab) is $b^{-1}a^{-1}$.

Solution: (1) Post-multiplying both sides of the equation

$$ca = a \tag{1}$$

by a^{-1}, we get

$$c = cE = caa^{-1} = aa^{-1} = E. \tag{2}$$

(2) Post-multiplying both sides of the equation

$$ca = E \tag{3}$$

by a^{-1}, we get

$$c = cE = caa^{-1} = Ea^{-1} = a^{-1}. \tag{4}$$

(3) Using the associative law for group multiplication, we have

$$(ab)(a^{-1}b^{-1}) = a(bb^{-1})a^{-1} = aEa^{-1} = aa^{-1} = E, \tag{5}$$

and

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}Eb = b^{-1}b = E. \tag{6}$$

Therefore, the inverse of (ab) is $(b^{-1}a^{-1})$.

□

Problem 2 Score: _____. Show that the set of nonzero complex numbers is a group under the ordinary multiplication.

Solution: The set of nonzero complex numbers under the ordinary multiplication satisfies all the four group axioms:

1. **Closure:** The multiplication of two nonzero complex number is a nonzero complex number, $a \times b = c$.
2. **Associativity:** The ordinary multiplication associativity, $(a \times b) \times c = a \times (b \times c)$.
3. **Identity:** The number 1 is the identity element, since $a \times 1 = 1 \times a = a$ for any nonzero complex number a.
4. **Inverse:** The inverse of any nonzero complex number a is its reciprocal $\frac{1}{a}$, since $a \times \frac{1}{a} = \frac{1}{a} \times a = 1$.

Therefore, the set of nonzero complex numbers is a group under the ordinary multiplication. □

Problem 3 Score: _____. Show that there is only one group of order three. Using a step-by-step procedure, construct the multiplication table for the group.

Solution: Suppose $G = \{E, a, b\}$ is a group of order 3. We construct its multiplication table step by step. First, since the identity element E labels both the first row and first column, the first row and first column of the multiplication table is the same as the row indices and the column indices, respectively, as shown in table 1.

Table 1:

	E	a	b
E	E	a	b
a	a		
b	b		

Since each row has no repeated elements and the second row already has a, $a \times a$ can not be equal to a, but only e or b. If $a \times a = e$, then we must have $a \times b = b$. In this way, we will have two b in the third column, as shown in table 2, which is not allowed.

Table 2:

	E	a	b
E	E	a	b
a	a	e	b
b	b		

As a result, $a \times a = b$ is the only possible case and thus $a \times b = e$, as shown in table 3.

Table 3:

	E	a	b
E	E	a	b
a	a	b	e
b	b		

Using the similar method, because the second column already has a and b, we know that $b \times a = e$. And because the third column already has b and e, we know that $b \times b = a$. Finally, we have the multiplication table of order 3, as shown in table 4, which is the only possible 3×3 multiplication table. Therefore, there is only one group of order 3. □

Table 4:

	E	a	b
E	E	a	b
a	a	b	e
b	b	e	a

Problem 4 Score: _____. Show that a group must be an Abelian group if the order of any element except the identity in the group is 2.

Solution: Suppose in group $G = \{E, a, b, \cdots\}$, the order of any element a except the identity E is 2. This means that for any element a (including the identity) of G, $aa = E$. For every pair of elements a and b of G, ab is also an element of G, so $(ab)(ab) = E$. In this way,

$$ab = aEb = a(ab)(ab)b = (aa)(ba)(bb) = E(ba)E = ba, \tag{7}$$

so a and b commute. Therefore, group G is an Abelian group. □

Problem 5 Score: _____. Show that every subgroup of a cyclic group is also cyclic.

Solution: Suppose $C_n = \{E, a, a^2, \cdots, a^{n-1}\}$ is a cyclic group of order n, where a is its generator. $S = \{E, a^{n_1}, a^{n_2}, \cdots, a^{n_K}\}$ is an arbitrary subgroup of C_n, where $n_k \in \{1, 2, \cdots, n-1\}$ for $k \in \{1, 2, \cdots, K\}$ and $n_k < n_l$ for $k < l$.

For an arbitrary element $a^{n_k} \in S$, since a^{n_1} and a^{n_k} are both elements of the cyclic group C_n, we have $n_k = qn_1 + r$, where q is the integer quotient and $0 \leq r < n_1$ is the integer remainder of n_k/n_1. In this way, we can write

$$a^{n_k} = a^{qn_1 + r}. \tag{8}$$

Multiply both side of the above equation by a^{-qn_1}, we get

$$a^r = a^{-qn_1 + n_k}. \tag{9}$$

Since $a^{n_1} \in S$, $a^{2n_1} = a^{n_1}a^{n_1} \in S$.
Since $a^{n_1} \in S$ and $a^{2n} \in S$, $a^{3n_1} \in a^{n_1}a^{2n_1} \in S$.
$\cdots$
In this way, we know that $a^{qn_1} \in S$.
Since $a^{qn_1} \in S$, $a^{-qn_1} \in S$.
Since $a^{-qn_1} \in S$ and $a^{n_k} \in S$, $a^r = a^{-qn_1 + n_k} \in S$.
Since $0 \leq r < n_1$ and n_1 is the smallest in $\{n_1, n_2, \cdot, n_K\}$, $r = 0$ and thus $a^{n_k} = a^{qn_k}$, which means that any arbitrary element $a^{n_k} \in S$ is the power of a^{n_1}.
Therefore, any subgroup S of a cyclic group C_n is also cyclic. □