Group Theory

Solutions to the Problems in Homework Assignment 01

Spring, 2020

1. 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 inverses of a and b. Using the definition of a group, show that

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

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

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

   (a) Making use of $c = cE$, $aa^{-1} = E$, and $ca = a$, we have

   $$c = cE = caa^{-1} = (ca)a^{-1} = aa^{-1} = E.$$

   (b) Making use of $c = cE$, $aa^{-1} = E$, and $ca = E$, we have

   $$c = cE = c(aa^{-1}) = (ca)a^{-1} = Ea^{-1} = a^{-1}.$$

   (c) We consider the product $(b^{-1}a^{-1})(ab)$. If the result of this product is equal to E, then $b^{-1}a^{-1}$ is the inverse of ab. Computing the product $(b^{-1}a^{-1})(ab)$ directly, we have

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

   Thus, $b^{-1}a^{-1}$ is indeed the inverse of ab.

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

   We examine whether the four group axioms are satisfied.

   (a) **Closure.**
   For two nonzero complex numbers $a = a_r + ia_i$ and $b = b_r + ib_i$, we have under the ordinary multiplication

   $$ab = (a_r + ia_i)(b_r + ib_i) = (a_r b_r - a_i b_i) + i(a_r b_i + a_i b_r).$$

   Obviously, the above result is a nonzero complex number. Thus, the product of any two elements is also in the group.

   (b) **Associativity.**
   Let $c = c_r + ic_i$. We have

   $$\begin{aligned}
   a(bc) &= (a_r + ia_i)[(b_r + ib_i)(c_r + ic_i)] = (a_r + ia_i)[(b_r c_r - b_i c_i) + i(b_r c_i + b_i c_r)] \\
   &= a_r b_r c_r - a_r b_i c_i - a_i b_r c_i - a_i b_i c_r + i(a_i b_r c_r - a_i b_i c_i + a_r b_r c_i + a_r b_i c_r) \\
   &= (a_r b_r - a_i b_i)c_r - (a_r b_i + a_i b_r)c_i + i[(a_i b_r + a_r b_i)c_r - (a_i b_i - a_r b_r)c_i] \\
   &= [(a_r b_r - a_i b_i) + i(a_i b_r + a_r b_i)]c_r + i[(a_r b_r - a_i b_i) + i(a_r b_i + a_i b_r)]c_i \\
   &= [(a_r b_r - a_i b_i) + i(a_i b_r + a_r b_i)](c_r + ic_i) = (ab)c.
   \end{aligned}$$

   Thus, the associative law is satisfied.

   (c) **Identity element.**
   The number 1 is the identity element.

   (d) **Inverse elements.**
   The inverse of an element is its reciprocal. For any arbitrary element $a = a_r + ia_i$, we have

   $$a^{-1} = \frac{1}{a} = \frac{1}{a_r + ia_i} = \frac{a_r - ia_i}{a_r^2 + a_i^2} = \frac{a_r}{a_r^2 + a_i^2} - i\frac{a_i}{a_r^2 + a_i^2}$$

   which is obviously in the group.

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

Let the group of order three be $G = \{E, a, b\}$. We first construct its multiplication table. The first row and column can be trivially filled. We then have the following uncompleted multiplication table.

$$\begin{array}{c|ccc} & E & a & b \\ \hline E & E & a & b \\ a & a & & \\ b & b & & \end{array}$$

In consideration that the product of two different elements of the group is also in the group, we have $ab = ba = E$. Then, the uncompleted multiplication table becomes

$$\begin{array}{c|ccc} & E & a & b \\ \hline E & E & a & b \\ a & a & & E \\ b & b & E & \end{array}$$

Because an element of the group appears only once in any row and column, we see from the above uncompleted multiplication table that $a^2 = b$ and $b^2 = a$. We then have the following completed multiplication table.

$$\begin{array}{c|ccc} & E & a & b \\ \hline E & E & a & b \\ a & a & b & E \\ b & b & E & a \end{array}$$

Because there is a unique way to construct the multiplication table of a group of order three, there is only one group of order three up to isomorphism.

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

Let a and b be any two arbitrary elements of the group. According to the statement of the problem, we have

$$a^2 = E, \; b^2 = E,$$

where E is the identity element. Making use of the fact that ab and ba are the elements of the group, we have

$$(ab)(ab) = E.$$

On the other hand, the product of ab and ba is given by

$$(ab)(ba) = a(bb)a = aEa = a^2 = E.$$

Because of the uniqueness of an element in each row and each column of the multiplication table, we have

$$ab = ba.$$

Because a and b are any two arbitrary elements of the group, the group is an Abelian group.

5. Show that every subgroup of a cyclic group is also cyclic.

Assume that the cyclic group G is of order n and is given by $G = \{E, a, a^2, \cdots, a^{n-1}\}$ with $a^n = E$. If $n = 1$, then $G = \{E\}$ and the conclusion is true. We now assume that $n > 1$. Obviously, the two trivial subgroups of G, $\{E\}$ and G, are cyclic. We now consider a subgroup $S = \{E, b_1, b_2, \cdots, b_{s-1}\}$ of G with the order s of S greater than 1. Since G is a cyclic group, all the elements of S are of the form a^p with $p \leq n$. Assume that the elements of S are arranged in the order of the increasing power of a except the identity E.

Assume that a^ℓ is the element of the lowest power in S with ℓ a positive integer. If an element of S is not of the form $(a^\ell)^k$ with k a positive integer and $k\ell \leq n$, then it can be written as $(a^\ell)^p a^r$ with p and r positive integers, $p\ell + r \leq n$, and $r < \ell$. Because of the closure property of S, $(a^\ell)^p a^r$ is the product of the element $(a^\ell)^p$ and the element a^r. This indicates that the element of the lowest power in S is a^r with $r < \ell$, which is in contradiction with the assumption that a^ℓ is the element of the lowest power in S. Thus, all the elements of S are of the form $(a^\ell)^k$ with k a positive integer, which implies that the element b_j of S with $j = 1, 2, \cdots, s-1$ can be expressed as $b_j = (a^\ell)^j$ with $(a^\ell)^s = a^{s\ell} = a^n = E$. Hence, a subgroup S of G is of the form

$$S = \{E, a^\ell, a^{2\ell}, \cdots, a^{(s-1)\ell}\} \text{ with } a^{s\ell} = a^n = E.$$

Therefore, every subgroup of a cyclic group is also cyclic.