Problem Set 2: Group Homomorphisms and Isomorphisms

Himmy

July 21, 2021

Problem 1. Let x and y be two elements of a group G. Assume that each of the elements x, y and xy has order 2. Prove that the set $H = \{1, x, y, xy\}$ is a subgroup of G, and it has order 4.

Solution. H must satisfy the following 3 conditions:

1. Identity: The identity 1 is contained in H.
2. Closed: Need to show that all permutations of products between elements of H is itself an element of H. Since all elements $x, y, xy \in H$ have order 2, then $x^2 = y^2 = (xy)^2 = 1 \in H$. xy is also clearly in H. For the less trivial permutations:
   - $yx = 1yx1 = (x^2)yx(y^2) = x(xy)(xy)y = x(xy)^2y = x1y = xy \in H$

     This is an important point since it shows that $yx = xy$ (is commutative).
   - $x(xy) = (xx)y = 1y = y \in H$
   - $(xy)x = (yx)x = y(xx) = y1 = y \in H$
   - $y(xy) = y(yx) = (yy)x = 1x = x \in H$
   - $(xy)y = x(yy) = x1 = x \in H$
3. Inverse: Since all elements of H are order two, they are all inverses of themselves, thus clearly the inverse of each element is an element of H.

□

Problem 2. Let G be a group and let $a \in G$ have order k. If p is a prime divisor of k, and if there is $x \in G$ with $x^p = a$, prove that x has order pk.

Solution. Assume that p is the smallest integer such that $x^p = a$. If a has order k, then $a^k = 1$. It follows that $(x^p)^k = a^k = 1$. To prove that x has order pk, we must prove that there is no other $n \in \mathrm{Z}^+$ such that $n < pk$ and $x^n = 1$.

- Case 1: Suppose $\exists n < p$ such that $x^n = 1$, then by Proposition 2.4.3 [Artin], $\exists r \leq n$ such that $x^r = a$, contradicting the assumption that p is the smallest integer satisfying $x^p = a$.
- Case 2: Suppose $\exists n = p$ such that $x^n = 1$, then $a = x^p = x^n = 1$, contradicting the assumption that k has a prime divisor p (if $a = 1$ then a has order 1 and thus the only divisor p is 1 which is not prime).
- Case 3: Suppose $\exists n$ such that $p < n < pk$ and $x^n = 1$, then by Proposition 2.4.3 [Artin] n must be a divisor of pk (since $x^{pk} = 1$ iff $r = 0$ for $pk = nq + r$ where q, r are integers). Since p is prime, n must be a divisor for k. But if pk is divisible by both p and n, then that implies that $a = x^p = x^{pk} = x^k = 1$ which is a contradiction for the same reason as in Case 2.

□

Problem 3. If G is a group in which $x^2 = 1$ for every $x \in G$, prove that G must be abelian.

Solution. Let $x, y \in G$, then

$$xy = 1xy1 = (y^2)xy(x^2) = y(yx)(yx)x = y(yx)^2x = y(1)x = yx$$

where the $(yx)^2 = 1$ is true because $yx \in G$ by definition of a group. Since we chose x, y arbitrarily, G satisfies the commutative law. □

Problem 4. If G is a group with an even number of elements, prove that the number of elements in G of order 2 is odd. In particular, G must contain an element of order 2.

Solution. If G is a group, for every element $g \in G$ there exists $g^{-1} \in G$. If g and g^{-1} are *not* distinct then $gg = 1$, so either g has order two or g is the identity. Thus the converse is that if g has order > 2 then g and g^{-1} are distinct elements. Additionally, if g has order n, then $g^n = 1 \Rightarrow 1 = (g^{-1})^n$ so the inverse of every element $g^{-1} \in G$ has the same order as $g \in G$.

If G starts with an even number of elements, one of those elements in the identity which is its own inverse. We "remove" the identity from our count so that the remaining number of elements is odd. For element that has order > 2, we can "remove" it and its inverse from our count, leaving us with a total count that is still odd. Furthermore, there will always remain at least one unpaired element which must have order 2 (be an inverse of itself). □

Problem 5. Let H be a subgroup of G and

$$C(H) = \{g \in G : gh = hg \ \forall h \in H\}$$

Prove that $C(H)$ is a subgroup of G. This is known as the *centralizer* of H in G.

Solution. A subgroup must satisfy the following 3 conditions:

1. Identity: Since G is a group, it has an identity $1 \in G$. It follows that $1h = h1$ for all $h \in H$ since every element is also an element $h \in G$. Thus $1 \in C(H)$.
2. Closed: Let $a, b \in C(H)$, then $a, b \in G$ and $ah = ha$ and $bh = hb$ for all $h \in H$. Then
$$(ab)h = a(bh) = a(hb) = (ah)b = (ha)b = h(ab)$$
so $ab \in C(H)$.
3. Inverse: Let $a \in C(H)$, then
$$ah = ha \Rightarrow a^{-1}ah = a^{-1}ha \Rightarrow h = a^{-1}ha \Rightarrow ha^{-1} = a^{-1}haa^{-1} \Rightarrow ha^{-1} = a^{-1}h.$$
In other words, if $a \in C(H)$, then $a^{-1} \in C(H)$.

□

Problem 6. Let G be a group, let X be a set, and let $f : G \to X$ be a bijection. Show that there is a unique operation on X so that X is a group and f is an isomorphism.

Solution. Let $\circ$ be the operation on G and let $\star$ be the operation on X such that $\star(x_1, x_2) := \{f(f^{-1}(x_1) \circ f^{-1}(x_2)) \mid f : G \to X,\ x_1, x_2 \in X\}$. To show that X is a group with this operation, it must satisfy the following 3 conditions:

1. Identity: Let $1_G \in G$ be the identity in G and let $1_X = f(1_G) \in X$. For any $x \in X$,
$$1_X \star x = f(f^{-1}(1_X) \circ f^{-1}(x)) = f(1_G \circ f^{-1}(x)) = f(f^{-1}(x)) = x.$$
A similar argument can be used to show that $x \star 1_X = x$.
2. Closure: For any $x_1, x_2 \in X$, $x_1 \star x_2 = f(f^{-1}(x_1) \circ f^{-1}(x_2))$. Since G is a group, $f^{-1}(x_1) \circ f^{-1}(x_2) \in G$, and therefore $f(f^{-1}(x_1) \circ f^{-1}(x_2)) \in X$.
3. Inverse: For any $x \in X$, there exists $y = f(f^{-1}(x)^{-1}) \in X$ (since G is a group, every element $f^{-1}(x) \in G$ has an inverse $f^{-1}(x)^{-1} \in G$). It follows that
$$x \star y = f(f^{-1}(x) \circ f^{-1}(f(f^{-1}(x)^{-1}))) = f(f^{-1}(x) \circ f^{-1}(x)^{-1}) = f(1_G) = 1_X$$
A similar argument can be used to show that $y \star x = 1_X$.

Lastly, to show that f is isomorphic it suffices to show that f is a homomorphism.

$$f(a) \star f(b) = f(f^{-1}(f(a)) \circ f^{-1}(f(b))) = f(a \circ b)$$

□

Problem 7. Determine the center of $GL_n(\mathbb{R})$.
Hint: You are asked to determine the invertible matrices A that commute with every invertible matrix B. Do not test with a general matrix B. Test with elementary matrices.

Solution. Note this question is similar to Exercise 3.D.16 from LADR [Axler]: "Suppose V is finite-dimensional and $T \in \mathcal{L}(V)$. Prove that T is a scalar multiple of the identity if and only if $ST = TS$ for every $S \in \mathcal{L}(V)$." The difference here is that we are dealing exclusively with invertible maps.

We prove the converse in one direction: If T is not a scalar multiple of the identity then $ST \neq TS$ for every invertible $S \in \mathcal{L}(V)$. Since T is not a scalar multiple of the identity, there exists some $v \in V$ for which v, Tv are linearly independent. By 2.33 in LADR we can extend to a basis of $V : v, Tv, v_3, \ldots, v_n$. Now let's choose an invertible S such that $Sv = v$, $S(Tv) = a_1v + a_2Tv$ where $a_1, a_2 \neq 0$, and $Sv_j = v_j$ for $j = 3, \ldots, n$. Then

$$Tv \neq a_1v + a_2Tv \Rightarrow T(Sv) \neq S(Tv) \Rightarrow (TS)v \neq (ST)v.$$

Given how we've selected S, it is an invertible map. Therefore we've proven that if $ST = TS$ for every invertible map $S \in \mathcal{L}(V)$, then T is a scalar multiple of the identity. □

Problem 8. Suppose given on E an (associative and commutative) addition under which all the elements of E are invertible and a multiplication which is *non-associative*, but commutative and doubly distributive with respect to addition. Suppose further that $n \in \mathbb{Z}, n \neq 0$ and $nx = 0$ imply $x = 0$ in E. Show that if, writing $[x, y, z] = (xy)z - x(yz)$, the identity

$$[xy, u, z] + [yz, u, z] + [zx, u, y] = 0$$

holds, then $x^{m+n} = x^m x^n$ for all x (show, by induction on p, that the identity $[x^q, y, x^{p-q}] = 0$ holds for $1 \leq q < p$).

Solution. TBD □