Problem Set 2 : Group Homomorphisms and Isomorphisms

July 15, 2021

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 $H \coloneqq \{1, x, y, xy\}$ is a subgroup of G, and it has order 4.

Solution

Note that H contains the identity element. Also, since x, y, xy are of order 2 then they are their own inverse; it follows that H is closed under inverses. It remains to check that H is closed under multiplication.

For $h \in H$, clearly $h1, 1h \in H$, and also $h^2 = 1 \in H$. Trivially, the product of x and y (in that order) is in h. Now we need to tackle some non-obvious products. For instance, $(x)(xy) = x^2y = 1y = y \in H$. Similarly $(xy)(y) = x \in H$

If the order of xy is 2 then $(xy)^2 = xyxy = 1$. By multiplying by x^{-1} from the left and y^{-1} from the right to get $yx = x^{-1}y^{-1} = xy$ since x, y are of order two, hence their own inverses. So, $yx \in H$. Actually, from $xyxy = 1$ we can conclude that $(y)(xy) = x$ and $(xy)(x) = y$, by multiplying by x^{-1} on the left and y^{-1} respectively. All in all, we have the following Cayley table.

	1	x	y	xy
1	1	x	y	xy
x	x	1	xy	y
y	y	xy	1	x
xy	xy	y	x	1

We have yet to prove that all elements of H are distinct, so that H has an order of 4. Clearly $x, y, xy \neq 1$ since 1 has order 1, not order 2. If $x = y$ then $xy = x^2 = 1$, which contradicts our previous assertion; hence $x \neq y$. If $x = xy$ then by cancellation $1 = y$; again, a contradiction. Similarly, $y = xy$ is impossible. Thus, $|H| = 4$.

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

Note that the order of x^p is k. But we have the following result,

$$|x^p| = \frac{|x|}{\gcd(|x|, p)} = k. \tag{1}$$

As p is a prime, $\gcd(|x|, p)$ is either 1 or p. If we assume, for the sake of contradiction, that it is 1 then we get $|x| = k$ from equation (1). In the identity $x^p = a$ we can raise both sides of the equation by the integer k/p to get $x^k = a^{k/p}$. Since k is the order of a and $0 < k/p < k$ we have that $x^k = a^{k/p} \neq e$, contradicting $|x| = k$. So, $\gcd(|x|, p)$ must be p; and by equation (1) we get $|x| = pk$ as desired.

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 $xy \in G$ and so $(xy)^2 = xyxy = 1$. But then we multiply by x on the left and by y on the right to get $xxyxyy = xy$. This is $(x^2)yx(y^2) = yx = xy$.

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

In a group each element has a unique inverse, which is not shared by any other element ($y^{-1} = x^{-1}$ implies $x = y$). Think of the group as a bag of elements and consider the following algorithm. At each step, we find an element which is *not* its own inverse, and subsequently remove it from the bag, along with its inverse. The algorithm terminates when all the elements left in the bag are their own inverses.

By our previous remarks, we are always removing two elements at a time, so that the parity of the number of elements in the bag remains the same. If we start with a group of even order, the resulting bag has an even number of elements. Furthermore, in this resulting bag we can find the identity, which is its own inverse. Remove it from the bag and we are left with an odd number of elements in the bag; these are all the non-identity elements of G which are their own inverses. But if x is one such element then $x = x^{-1}$ and so $x^2 = e$; since $x \neq e$ it follows that $|x| = 2$. Conversely, all elements of order 2 are their own inverses (and are not the identity). We are done.

5. Let H be a subgroup of G and

$$C(H) = \{\, g \in G \colon gh = hg \text{ for all } h \in H \,\}.$$

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

Solution

Clearly $e \in C(H)$ since the identity commutes with all elements of G. Let $g, g' \in C(H)$. If $h \in H$ then

$$(gg')h = g(g'h) = g(hg') = (gh)g' = (hg)g' = h(gg'),$$

where we have used associativity and the fact that g and g' both commute with h. Hence $gg' \in C(H)$ and the centralizer is closed under composition. Similarly, we have

$$g^{-1}h = g^{-1}(h^{-1})^{-1} = (h^{-1}g)^{-1} = (gh^{-1})^{-1} = (h^{-1})^{-1}g^{-1} = hg^{-1},$$

where we have used the formula for the inverse of a product and the fact that $h^{-1} \in H$ and hence g commutes with h^{-1}. Hence $C(H)$ is closed under inverses. Thus it is a subgroup of G.

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

Solution

If f is a bijection then $f \times f\colon G \times G \to X \times X$ defined by $f \times f(a, b) = (f(a), f(b))$ is also a bijection. To see this, notice that it has a two-sided inverse $f^{-1} \times f^{-1}$ defined in the obvious way.

Let $m_G\colon G \times G \to G$ be the multiplication map of G. We require that there exists a unique $m_X\colon X \times X \to X$ such that the following diagram commutes.

$$\begin{array}{ccc} G \times G & \xrightarrow{f \times f} & X \times X \\ {\scriptstyle m_G}\downarrow & & \downarrow{\scriptstyle m_X} \\ G & \xrightarrow[f]{} & X \end{array}$$

Indeed, this requirement is just that $m_X \circ (f \times f) = f \circ m_G$. We can apply the inverse of $f \times f$ on the right to both sides of the equality to prove that m_X exists and is uniquely determined by f and the multiplication map of G. The commutativity of the diagram guarantees that f is a homomorphism, hence an isomorphism.

7. Determine the center of $GL_n(\mathbb{R})$.

Solution

First, I will talk about conjugation in $GL_n(\mathbb{R})$ and linear maps. One can significantly shorten this proof by avoiding any mention of linear maps and working solely with matrices. However, I have written the following thinking of someone who may need the additional intuition.

Linear automorphisms on $\mathbb{R}^n$ correspond to matrices in $GL_n(\mathbb{R})$. However, exactly how this isomorphism (between matrices and linear transformations) is defined depends on the basis of $\mathbb{R}^n$ that we choose.

For instance, consider the linear transformation in $\mathbb{R}^2$ of a 90° counter-clockwise rotation about the origin. If we are using the standard basis we may write this as the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, which roughly translates to "move $\hat{\mathbf{i}}$ to the column vector (0 1) and move $\hat{\mathbf{j}}$ to the column vector (-1 0)". If we wanted to emphasize the dependence of the matrix on the choice of basis we could further translate as "move $\hat{\mathbf{i}}$ to $\hat{\mathbf{j}}$ and move $\hat{\mathbf{j}}$ to the $-\hat{\mathbf{i}}$". Of course, changing $\hat{\mathbf{i}}, \hat{\mathbf{j}}$ for other basis vectors would, in general, make our matrix (thinking of it as just an array of numbers) to not represent the desired rotation any more.

Nevertheless, it is possible to translate between different choices of bases. Let L be a linear automorphism of $\mathbb{R}^n$. We say an $n \times n$ matrix M represents L on the basis B if, for all $v \in \mathbb{R}^n$ we have that $L(v) = Mv$, where v is written as a column vector in the basis B. It is a theorem of linear algebra that, if B, B' are bases of $\mathbb{R}^n$ and if M represents L, a linear automorphism of $\mathbb{R}^n$, in B then $X^{-1}MX$ represents L in B', where X is the matrix whose columns are the basis vectors of B' (written as column vectors in the basis B).

The center of $GL_n(\mathbb{R})$ is all matrices $Z \in GL_n(\mathbb{R})$ that satisfy $ZX = XZ$ for all $X \in GL_n(\mathbb{R})$. Experimentation suggests that the answer is all nonzero multiples of the identity. An equivalent condition to the one stated above is $Z = X^{-1}ZX$. What does this means in terms of linear mappings? I encourage you to think about this before reading on.

We are looking for linear automorphisms L of $\mathbb{R}^n$ such that if we choose a basis of $\mathbb{R}^n$, say the standard basis, and find the associated matrix representing L, call it Z, then this matrix in fact represents L in all possible bases! This will be made more explicit in the next paragraph.

Let $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ be arbitrary bases of $\mathbb{R}^n$. We want L to have the property that, for all $1 \leq i \leq n$, if $L(u_i) = c_{i,1}u_1 + \ldots c_{i,n}u_n$ where the c's are scalars then $L(v_i) = c_{i,1}v_1 + \ldots c_{i,n}v_n$. Some thought will reveal that this property guarantees that the matrices representing L are identical, independently of the basis we choose, and their entries are the c's

To finish this off, we can consider the two bases $\{u_1, \ldots, u_i, \ldots u_n\}$ and $\{-u_1, -u_2, \ldots, u_i, \ldots, -u_n\}$ for each i. Then the property of L says that

$$0 = L(u_i) - L(u_i) = 2c_{i,1}u_1 + \ldots 2c_{i,i-1}u_{i-1} + 2c_{i,i+1}u_{i+1} + \ldots 2c_{i,n}u_n.$$

As the u's are linearly independent, it follows that all the c's are zero except those of the form $c_{i,i}$ (i.e. our matrix is diagonal).

We can use the same trick. Consider the bases $\{u_1, \ldots, u_i, \ldots u_j, \ldots u_n\}$ and $\{u_1, \ldots, u_j, \ldots, u_i, \ldots u_n\}$ (swapping u_i and u_j) for all $i < j$. Then $L(u_i) = c_{i,i}u_i$ and $L(u_j) = c_{j,j}u_j$. The defining property of L will imply that $c_{i,i} = c_{j,j}$; i.e. all the entries of the diagonal are equal. This is enough to show the associated matrix is a multiple of the identity and the claim follows.

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 for all non-zero integers n, we have that $nx = 0$ implies $x = 0$ for all $x \in E$. 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 $x \in E$.

Solution