Groups, Fields, and Vector Spaces

Homework #2 (2024-2025), Answers

Q1: Homomorphisms, kernels, normal subgroups

We showed that for any homomorphism $\varphi : G \to H$, the kernel of φ, i.e., the elements $g \in G$ for which $\varphi(g) = e_H$, is a subgroup of G. Show that it is a normal subgroup.

We need to show that if g is in the kernel and $b \in G$, then bgb^{-1} is also in the kernel. That is, if $\varphi(g) = e_H$, then $\varphi(bgb^{-1}) = e_H$.
Since φ is a homomorphism, $\varphi(bgb^{-1}) = \varphi(b)\varphi(g)\varphi(b^{-1}) = \varphi(b)\varphi(g)\left(\varphi(b)\right)^{-1}$.
Since g is in the kernel, $\varphi(b)\varphi(g)\left(\varphi(b)\right)^{-1} = \varphi(b)e_H\left(\varphi(b)\right)^{-1} = \varphi(b)\left(\varphi(b)\right)^{-1} = e_H$, as needed.
Q2: Inner and outer automorphisms

A. For $G = \mathbb{Z}_n$ (the cyclic group of order n), determine all of the automorphisms.

Since G consists of a generator x and its powers ($\{e, x, x^2, ..., x^{n-1}\}$), an automorphism is specified by its action on x. That is, if $\varphi(x) = x^k$, then, for any element x^a of the group, $\varphi(x^a) = \left(\varphi(x)\right)^a = \left(x^k\right)^a = x^{ka}$ by the homomorphism property, then the definition of φ, then the associative rule. (Note also that φ is guaranteed to be a homomorphism, since $\varphi(x^a)\varphi(x^b) = x^{ka}x^{kb} = x^{ka+kb} = x^{k(a+b)} = \varphi(x^{a+b}) = \varphi(x^a)\varphi(x^b)$.) Here, exponents are interpreted $\bmod\ n$, since $x^n = x^0 = e$.

So we only need to check that φ is 1-1, i.e., that there is an element x^m for which $\varphi(x^m) = x$. That is, can we find an m such that $\left(x^m\right)^k = x^{km} = x$? Since exponents are interpreted $\bmod\ n$, we need $km \equiv 1 \pmod{n}$, i.e., $km - nb = 1$ for some integer b. If k and n have a common factor, this is impossible, since the common factor divides the right side, and hence would have to divide 1. Conversely, if k and n are relatively prime, this is always possible (Euclid's Algorithm).

All of these automorphisms are outer automorphisms, since G is commutative.

B. Recall: For any group G, the automorphism group $A(G)$ is the group of isomorphisms of G, i.e, one-to-one mappings φ from G to G which preserve the group operation in G. The group operation in $A(G)$ is composition: $\varphi_1 \circ \varphi_2$ is the automorphism of G defined by $\varphi_1 \circ \varphi_2(g) = \varphi_1\left(\varphi_2(g)\right)$. We also said that there is a special set of automorphisms, the "inner" automorphisms. For any element α in G, the inner automorphism φ_α is defined by $\varphi_\alpha(g) = \alpha g \alpha^{-1}$. We called the mapping from G to $A(G)$ the "adjoint" map, and noted that it is a homomorphism from G to a subgroup of (and possibly all of) $A(G)$. We also noted that $Adj : G \to A(G)$ is, itself, a homomorphism: For any $g \in G$, $\left(\varphi_\alpha \circ \varphi_\beta\right)(g) = \varphi_\alpha\left(\varphi_\beta(g)\right) = \varphi_\alpha\left(\beta g \beta^{-1}\right) = \alpha\left(\beta g \beta^{-1}\right)\alpha^{-1} = \alpha\beta g \beta^{-1}\alpha^{-1} = (\alpha\beta) g (\alpha\beta)^{-1} = \varphi_{\alpha\beta}(g)$, so $Adj(\alpha) \circ Adj(\beta) = Adj(\alpha\beta)$.

Show that the inner automorphisms $I(G)$ are a normal subgroup of $A(G)$.

We need to show that, for any $\varphi_\alpha \in I(G)$ and any $\psi \in A(G)$, that $\psi^{-1} \circ \varphi_\alpha \circ \psi \in I(G)$. So we calculate the action of $\psi^{-1} \circ \varphi_\alpha \circ \psi$ on an arbitrary $g \in G$, recalling that the group operation in $A(G)$ is composition:

$\left(\psi^{-1} \circ \varphi_\alpha \circ \psi\right)(g) = \psi^{-1}\left(\varphi_\alpha\left(\psi(g)\right)\right) = \psi^{-1}\left(\alpha\psi(g)\alpha^{-1}\right)$, where the second step uses the definition of φ_α. Since ψ^{-1} is an automorphism of G, this is

$\psi^{-1}\left(\alpha\psi(g)\alpha^{-1}\right) = \psi^{-1}(\alpha)\psi^{-1}\left(\psi(g)\right)\psi^{-1}(\alpha^{-1}) = \psi^{-1}(\alpha)\psi^{-1}\left(\psi(g)\right)\left(\psi^{-1}(\alpha)\right)^{-1}$.

Using the composition rule in $A(G)$, this is

$\psi^{-1}(\alpha)\psi^{-1}\left(\psi(g)\right)\left(\psi^{-1}(\alpha)\right)^{-1} = \psi^{-1}(\alpha)\left((\psi^{-1} \circ \psi)(g)\right)\left(\psi^{-1}(\alpha)\right)^{-1} = \psi^{-1}(\alpha)(g)\left(\psi^{-1}(\alpha)\right)^{-1}$.

Using the definition of Adj applied to $\psi^{-1}(\alpha)$, we have $\left(\psi^{-1} \circ \varphi_\alpha \circ \psi\right)(g) = \varphi_{\psi^{-1}(a)}(g)$. Since this hold for any $g \in G$, we have $\psi^{-1} \circ \varphi_\alpha \circ \psi = \varphi_{\psi^{-1}(a)}$, and hence, that $\psi^{-1} \circ \varphi_\alpha \circ \psi \in I(G)$.

Q3: Direct sums of groups

Given two groups G and H with group operations $\circ_G$ and $\circ_H$, the direct sum $G \oplus H$ is a group consisting of ordered pairs of elements (g,h), with the group operation defined by

$(g_1,h_1) \circ (g_2,h_2) = (g_1 \circ_G g_2, h_1 \circ_H h_2)$.

A. Convince yourself that $G \oplus H$ is a group.

Associativity is inherited from G and H. The identity is (e_G, e_H). Inverses: $(g,h)^{-1} = (g^{-1}, h^{-1})$.

B. If G and H are finite, with sizes $|G|$ and $|H|$, what is the size of $G \oplus H$?

This is the number of possible ordered pairs (g,h), so $|G \oplus H| = |G||H|$.

C. Consider $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. What is its automorphism group?

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$ has four elements. Other than the identity, they are $a = (u,0)$, $b = (0,u)$ and $c = (u,u)$. Note that (writing the group operation as multiplication) $a^2 = b^2 = c^2 = 1$, and that the product of any two of $\{a,b,c\}$ is the third. So $\{a,b,c\}$ play identical roles, and any permutation of them is an automorphism of the group – i.e., the automorphism group of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is the six-element group of permutations on three objects (S_3).

Q4: A challenge

$G \oplus H \oplus K$ is defined analogously as a group of ordered triplets. What is the size of $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, and what is the size of its automorphism group?

$|G \oplus H \oplus K| = |G||H||K|$, so the size of $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ is 8. Sketch of automorphism group: $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has seven elements that are not the identity, and all are of order 2. We can think of these elements as 3-vectors with entries of 0 and 1, with the group operation being addition $\bmod 2$, i.e., a 3-dimensional vector space over the finite field $\mathbb{Z}_2$. Automorphisms of the group correspond to isomorphisms of the vector space. Working now in the vector space: consider how the isomorphism acts on a basis, which determines its action. It can take the first basis element v_1 to any of the seven nonzero elements, say $\varphi(v_1)$ (including v_1 itself). It can take the second basis element v_2 to any of the elements that are not linearly dependent on $\varphi(v_1)$, i.e., not the identity and not $\varphi(v_1)$; there are 6 such elements. Call this $\varphi(v_2)$. The third basis element must be taken to an element that is linearly independent of $\varphi(v_1)$ and $\varphi(v_2)$, i.e., not 0, $\varphi(v_1)$, $\varphi(v_2)$, or $\varphi(v_1) + \varphi(v_2)$, so, 4 possibilities. So the automorphism group is of size $168 = 7 \bullet 6 \bullet 4$, which is the same as the group of invertible 3×3 matrices with entries $\{0,1\}$, interpreted $\bmod 2$. (The standard notation for this is $GL(3,2)$.)