Proofs involving Homomorphisms/Isomorphisms

December 12, 2009

Let G be an abelian group. Prove that the function $\varphi : G \to G$ defined by $\varphi(x) = x^{-1}$ is an isomorphism of G onto itself.

Proof Let $x, y \in G$. Then $\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1}$. Since G is abelian, then $y^{-1}x^{-1} = x^{-1}y^{-1} = \varphi(x)\varphi(y)$. Since $\varphi(xy) = \varphi(x)\varphi(y)$, then φ is a homomorphism. Now, suppose that $\varphi(x) = \varphi(y)$. By definition of φ, we have $x^{-1} = y^{-1}$, and it follows that $x = y$. Since $\varphi(x) = \varphi(y)$ implies that $x = y$, then φ is one-to-one. Now, $\varphi(x^{-1}) = (x^{-1})^{-1} = x$, so φ is onto. We have shown that φ is a homomorphism and is bijective. Therefore, φ is isomorphic. ■

Let G be an abelian group, and let $n \in \mathbb{Z}^+$. Prove that the function $\phi : G \to G$ defined by $\phi(x) = x^n$ is a homomorphism.

Proof Let $x, y \in G$. Then $\phi(xy) = (xy)^n$. Since G is abelian, then $(xy)^n = x^n y^n = \phi(x)\phi(y)$. Since $\phi(xy) = \phi(x)\phi(y)$, then we conclude that ϕ is a homomorphism. ■

Let $\alpha : G_1 \to G_2$ and $\beta : G_2 \to G_3$ be group homomorphisms. Prove that $\beta\alpha : G_1 \to G_3$ is a homomorphism and that $\ker(\alpha) \subseteq \ker(\beta\alpha)$.

Proof Let $x, y \in G_1$. Since α and β are homomorphisms, then $\beta\alpha(xy) = \beta(\alpha(xy)) = \beta(\alpha(x)\alpha(y)) = \beta\alpha(x)\beta\alpha(y)$. Hence, $\beta\alpha$ is a homomorphism. Now, let $k \in \ker(\alpha)$. By definition of kernel, $\alpha(k) = e_2$, where e_2 is the identity element of G_2. It follows that $\beta(\alpha(k)) = \beta(e_2) = e_3$, where e_3 is the identity element of G_3. So $k \in \ker(\beta\alpha)$, and by definition of subset, it follows that $\ker(\alpha) \subseteq \ker(\beta\alpha)$. ■

Let $f : G \to H$ be a homomorphism of G onto H. Prove that if G is abelian, then H is abelian.

Proof Let $x, y \in H$. Since f is onto, then there exist elements a, b in G such that $f(a) = x$ and $f(b) = y$. Now, since f is a homomorphism, then $xy = f(a)f(b) = f(ab)$. Since G is abelian, then $f(ab) = f(ba) = f(b)f(a) = yx$. Since $xy = yx$, then H is abelian as desired. ■

***Theorem 1*: Let $f : G_1 \to G_2$ be a homomorphism of G_1 onto G_2. If G_1 is cyclic, then G_2 is also cyclic.**

Proof Let $G_1 = \langle x \rangle$ be a group with a generator x. Let $b \in G_2$. Since f is onto, then there exists an element a in G_1 such that $f(a) = b$. Since G_1 is cyclic, then $a = x^k$ for some $k \in \mathbb{Z}$. It follows that $b = f(a) = f(x^k) = [f(x)]^k$, so $G_2 = \langle f(x) \rangle$. Hence, G_2 is cyclic. ■

***Theorem 2*: Let α be an arbitrary permutation in S_n. Then the function $f : S_n \to \mathbb{Z}_2$ defined as $f(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is an odd permutation} \\ 0 & \text{if } \alpha \text{ is an even permutation} \end{cases}$ is a homomorphism.**

Proof Let $\alpha, \beta \in S_n$. If α and β are both even, then $\alpha\beta$ is even and $f(\alpha\beta) = 0 = 0 + 0 = f(\alpha) + f(\beta)$. Likewise, if α and β are both odd, then $\alpha\beta$ is even and $f(\alpha\beta) = 0 = 1 + 1 = f(\alpha) + f(\beta)$. Now, if α is odd and β is even, then $\alpha\beta$ is odd and $f(\alpha\beta) = 1 = 1 + 0 = f(\alpha) + f(\beta)$. In all cases, $f(\alpha\beta) = f(\alpha) + f(\beta)$. Hence, f is a homomorphism. ■

***Theorem 3*: Let $f : G \to G'$ be a homomorphism. If H is a subgroup of G, then $f(H) = \{f(h) | h \in H\}$ is a subgroup of G'.**

Proof Since H is a subgroup, then $e \in H$. This implies that $f(e) \in f(H)$, so $f(H)$ is nonempty. Now, let $c, d \in f(H)$. Since f is onto, then $f(c) = a$ and $f(d) = b$ for some $a, b \in H$. Since f is a homomorphism, then $cd = f(a)f(b) = f(ab)$. Since $ab \in H$, then $f(ab) \in f(H)$ and $f(H)$ is closed under binary operations. Also, $c^{-1} = [f(a)]^{-1} = f(a^{-1})$. Since $a^{-1} \in H$, then $f(a^{-1}) \in f(H)$ and $f(H)$ has an identity element. Hence, $f(H)$ is a subgroup. ■

***Theorem 4*: Let $f : G \to G'$ be a homomorphism. If M is a subgroup of G', then $f^{-1}(M) = \{x \in G | f(x) \in H\}$ is a subgroup of G.**

Proof To start, $e \in f^{-1}(M)$ since $f(e) = e'$, and $e' \in M$. Now, let $a, b \in f^{-1}(M)$. Then $f(a)$ and $f(b)$ are in M. By definition of homomorphism, $f(ab) = f(a)f(b)$, and $f(a)f(b) \in M$ since M is a subgroup. So $ab \in f^{-1}(M)$ and $f^{-1}(M)$ is closed under binary operations. Finally, $f(a^{-1}) = [f(a)]^{-1}$ and $[f(a)]^{-1} \in M$, implying that $a^{-1} \in f^{-1}(M)$. Hence, $f^{-1}(M)$ is a subgroup. ■

***Theorem 5*: Let $\phi : G \to G'$ be a group homomorphism. The homomorphism ϕ is one-to-one if and only if $\ker(\phi) = \{e\}$.**

Proof:

$\Rightarrow$Suppose that ϕ is one-to-one. Trivially, $e \in \ker(\phi)$ so that $\phi(e) = e'$. Now, let $x \in \ker(\phi)$, so that $\phi(x) = e'$. Since ϕ is one-to-one, this implies that $x = e$. This shows that $\ker(\phi) = \{e\}$.
$\Leftarrow$Suppose that $\ker(\phi) = \{e\}$ and that $\phi(a) = \phi(b)$ for some $a, b \in G$. If we multiply both sides of the equation by $[\phi(b)]^{-1}$, we obtain $\phi(a)\,[\phi(b)]^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) = e'$, implying that $ab^{-1} \in \ker(\phi)$. It follows from our assumption that $ab^{-1} = e$, and thus $a = b$. This shows that ϕ is one-to-one.
This completes the proof. ■