Group Homomorphisms

When defining a homomorphism from a group in which there are several ways to represent the elements, caution must be exercised to ensure that the correspondence is a function.

Kernal of a Homomorphism

The kernel of a homomorphism ϕ from a group G to a group with identity e is the set
$x \in G \mid \phi(x) = e$. The kernel of ϕ is denoted by $\operatorname{Ker}\phi$ and clearly it forms a subgroup.

The kernel of an isomorphism is the trivial subgroup.

Relation with linear algebra: Every linear transformation is a group homomorphism and the null-space is the same as the kernel. An invertible linear transformation is a group isomorphism.

Properties of Homomorphisms

Theorem 10.1: Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let g be an element of G and let H be a subgroup of G. Then 1. ϕ carries the identity of G to the identity of $\overline{G}$. 2. $\phi(g^n) = (\phi(g))^n$ for all n in Z. 3. If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$. (easy) 4. $\phi(a) = \phi(b)$ if and only if $a \operatorname{Ker}\phi = b \operatorname{Ker}\phi$. (easy) 5. If $\phi(g) = g'$, then $\phi^{-1}(g') =$
$x \in G \mid \phi(x) = g' = g \operatorname{Ker}\phi$. (easy, $g \operatorname{Ker} \subseteq \phi^{-1}(g')$ is straight forward, for other dirn, we have, $\phi(x) = \phi(g') \rightarrow g'^{-1}x \in \operatorname{Ker}\phi$) 6. $\phi(H) =$
$\phi(h) \mid h \in H$ is a subgroup of $\overline{G}$. (easy) 7. If H is cyclic, then $\phi(H)$ is cyclic. (easy) 8. If H is Abelian, then $\phi(H)$ is Abelian. (easy) 9. If H is normal in G, then $\phi(H)$ is normal in $\phi(G)$. (easy) 10. If $|\operatorname{Ker}\phi| = n$, then ϕ is an n-to-1 mapping from G onto $\phi(G)$ (From 4 or 5 we see that $a \in b \operatorname{Ker}\phi$ Now $|b \operatorname{Ker}\phi| = n$) 11. If $|H| = n$, then $|\phi(H)|$ divides n. (let ϕ_H denote the restriction of ϕ to the elements of H. Then ϕ_H is a homomorphism from H onto $\phi(H)$. Suppose $|Ker\phi_H| = t$. Then, by property 5, ϕ_H is a t-to-1 mapping. So, $|\phi(H)|t = |H|$. 12. If $\overline{K}$ is a subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) =$
$k \in G \mid \phi(k) \in \overline{K}$ is a subgroup of G. (easy..) 13. If $\overline{K}$ is a normal subgroup of

$\overline{G}$, then $\phi^{-1}(\overline{K}) =$
$k \in G \mid \phi(k) \in \overline{K}$ is a normal subgroup of G. (easy..) (As a **Corollary**, $\operatorname{Ker}\phi$ is a normal subgroup of G. (take $\overline{K}$ as
e). *Note:* As we will soon see, converse is as well true) 14. If ϕ is onto and $\operatorname{Ker}\phi =$
e, then ϕ is an isomorphism from G to $\overline{G}$.

Examples:

- Consider the mapping ϕ from C to C given by $\phi(x) = x^4$. Since $(xy)^4 = x^4y^4$, ϕ is a homomorphism. Clearly, $\operatorname{Ker}\phi =$
  $x \mid x^4 = 1 =$
  $1, -1, i, -i$. So, we know that ϕ is a 4-to-1 mapping. Now let's find all elements that map to, say, 2. Certainly, $\phi(\sqrt[4]{2}) = 2$. Then, the set of all elements that map to 2 is
  $\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i$
- We determine all homomorphisms from Z_{12} to Z_{30}. By property 2 of Theorem 10.1, such a homomorphism is completely specified by the image of 1. That is, if 1 maps to a, then x maps to xa. Lagrange's Theorem and property 3 of Theorem 10.1 require that $|a|$ divide both 12 and 30. So, $|a| = 1$, 2, 3, or 6. Thus, $a = 0$, 15, 10, 20, 5, or 25. This gives us a list of candidates for the homomorphisms. That each of these six possibilities yields an operation-preserving, well- defined function can now be verified by direct calculations.

Theorem 10.2: (First Isomorphism Theorem) Let ϕ be a group homomorphism from G to $\overline{G}$. Then the mapping from $G/\operatorname{Ker}\phi$ to $\phi(G)$, given by $g\operatorname{Ker}\phi \to \phi(g)$, is an isomorphism. In symbols, $G/\operatorname{Ker}\phi \approx \phi(G)$. (function definition is valid, one-one follows from property 4 discussed above and onto is easy to see, operation preserving can be easily verified)

Corollary: If ϕ is a homomorphism from a finite group G to $\overline{G}$, then $|\phi(G)|$ divides $|G|$ and $|\overline{G}|$.

Examples:

- $Z/\langle n\rangle \approx Z_n$
- (N/C **Theorem**) Let H be a subgroup of a group G. Normalizer of H in G is $N(H) =$
  $x \in G \mid xHx^{-1} = H$ and the centralizer of H in G is $C(H) =$
  $x \in G \mid xhx^{-1} = h; \forall h \in H$. Consider the mapping from $N(H)$ to $Aut(H)$ given by $g \to \phi_g$, where ϕ_g is the inner automorphism of H induced by

g. This mapping is a homomorphism with kernel $C(H)$. So, by Theorem 10.3, $N(H)/C(H)$ is isomorphic to a subgroup of $Aut(H)$.

- Let G be a group of order 35. By Lagrange's Theorem, every nonidentity element of G has order 5, 7, or 35. If some element has order 35, G is cyclic. So we may assume that all nonidentity elements have order 5 or 7. However, not all such elements can have order 5, since elements of order 5 come 4 at a time (if $|x| = 5$, then $|x^2| = |x^3| = |x^4| = 5$) and 4 does not divide 34. Similarly, since 6 does not divide 34, not all nonidentity elements can have order 7. So, G has elements of order 7 and order 5. Since G has an element of order 7, it has a subgroup of order 7. Let us call it H. In fact, H is the only subgroup of G of order 7, for if K is another subgroup of G of order 7, we have by Theorem 7.2 that $|HK| = |H||K|/|H \cap K| = 7 \cdot 7/1 = 49$ (Intersection is
e because each element is a generator). But, of course, this is impossible in a group of order 35. Since for every a in G, aHa^{-1} is also a subgroup of G of order 7 (easy to prove), we must have $aHa^{-1} = H$. So, $N(H) = G$. Since H has prime order, it is cyclic and therefore Abelian. In particular, $C(H)$ contains H. So, 7 divides $|C(H)|$ and $|C(H)|$ divides 35. It follows, then, that $C(H) = G$ or $C(H) = H$. If $C(H) = G$, then we may obtain an element x of order 35 by letting $x = hk$ (since order of h, k is relatively prime and they commute, therefore order of $x = |h||k|$), where h is a nonidentity element of H and k has order 5. On the other hand, if $C(H) = H$, then $|C(H)| = 7$ and $|N(H)/C(H)| = 35/7 = 5$. However, 5 does not divide $|Aut(H)| = |Aut(Z_7)| = 6$. This contradiction shows that G is cyclic.

Theorem 10.3: Every normal subgroup of a group G is the kernel of a homomorphism of G. In particular, a normal subgroup N is the kernel of the mapping $g \to gN$ from G to G/N.

Proof: Define $\gamma : G \to G/N$ by $\gamma(g) = gN$. (This mapping is called the natural homomorphism from G to G/N.) Then, $\gamma(xy) = (xy)N = xNyN = \gamma(x)\gamma(y)$. Moreover, $g \in \operatorname{Ker}\gamma$ if and only if $gN = \gamma(e) = N$, which is true if and only if $g \in N$.

Examples:

- If G is a group of order 60 and G has a homomorphic image of order 12 that is cyclic (as it is cyclic, it is normal and thus its inverse will also be normal subgroup, also since it is cyclic, it has normal subgroups of order 1, 2, 3, 4, 6, 12), then G has normal subgroups of orders 5, 10, 15, 20, 30, and 60 (property 10).
- Suppose we are asked to find an infinite group that is the union of three proper subgroups. Instead of attempting to do this directly, we first make

the problem easier by finding a finite group that is the union of three proper subgroups. Observing that $Z_2 \oplus Z_2$ is the union of $H_1 = \langle 1, 0 \rangle$, $H_2 = \langle 0, 1 \rangle$, and $H_3 = \langle 1, 1 \rangle$, we have found our finite group. Now all we need do is think of an infinite group that has $Z_2 \oplus Z_2$ as a homomorphic image and pull back H_1, H_2, and H_3, and our original problem is solved. Clearly, the mapping from $Z_2 \oplus Z_2 \oplus Z$ onto $Z_2 \oplus Z_2$ given by $\phi(a, b, c) = (a, b)$ is such a mapping, and therefore $Z_2 \oplus Z_2 \oplus Z$ is the union of $\phi^{-1}(H_1) =$
$(a, 0, c,) \mid a \in Z_2, c \in Z, \phi^{-1}(H_2) =$
$(0, b, c) \mid b \in Z_2, c \in Z,$ and
$\phi^{-1}(H_3) =$
$(a, a, c) \mid a \in Z_2, c \in Z.$