Abstract Algebra
Lecture 7
Wednesday, 9/22/2010

1 Isomorphism Theorems

Motivating Question: Let $\varphi : G \to G'$ be a homomorphism. How far is φ from being an isomorphism?
Answer 1: Perhaps there exist $x, y \in G$, $x \neq y$, such that $\varphi(x) = \varphi(y)$ i.e. φ is not injective. In other words, $\ker(\varphi)$ is non-trivial, or $\ker(\varphi) \neq \{1\}$. We know that the kernel is a normal subgroup: $\ker(\varphi) \trianglelefteq G$. It is possible that this is the trivial subgroup – just the identity. Or it could contain other elements: $\varphi(x) = \varphi(y) \Rightarrow \varphi(xy^{-1} = 1$, i.e. $xy^{-1} \in \ker(\varphi)$, in which case the kernel is nontrivial and φ is not injective.
Answer 2: Perhaps φ is not surjective.

1.1 The First Isomorphism Theorem, or The Homomorphism Theorem

Theorem: "If we get rid of these problems, then our problems are solved."
Let $\varphi : G \to G'$ be a homomorphism of groups. Then $\ker(\varphi) \trianglelefteq G$, and $\mathrm{Im}(\varphi) \leq G'$, and

$$\boxed{G/\ker(\varphi) \cong \mathrm{Im}(\varphi).}$$

Ex: Let $\varphi : \mathbb{Z} \to \mathbb{Z}_2$ (under addition and addition mod 2) defined by $\varphi(n) = n \mod 2$. Then $\ker(\varphi) = \{n \in \mathbb{Z} \mid \varphi(n) = 0\} = \{n \in \mathbb{Z} \mid n = 0 \mod 2\} = 2\mathbb{Z}$. Then the First Isomorphism Theorem says that $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$.

Proof: We have previously shown that $\ker(\varphi) \trianglelefteq G$, and $\mathrm{Im}(\varphi) \leq G'$. Let $K = \ker(\varphi)$ and $I = \mathrm{Im}(\varphi)$. Let $\psi : G/K \to I$ be given by $\psi(Kg) = \varphi(g)$.
Claim: ψ is well defined. Suppose $Kg = Kg'$. Then $g'g^{-1} \in K$. Then $\varphi(g'g^{-1}) = 1$, and therefore $\varphi(g') = \varphi(g)$.
Claim: ψ is a homomorphism. Inspect $\psi(KxKy) = \psi(Kxy) = \varphi(xy) = \varphi(x)\varphi(y) = \psi(Kx)\psi(Ky)$.
Claim: ψ is injective. Suppose $\psi(Kx) = \psi(Ky)$. Then $\varphi(x) = \varphi(y)$. So $\varphi(xy^{-1} = 1$. In other words, $xy^{-1} \in k$, which is true if and only if $Kx = Ky$. Thus ψ is surjective.
Claim: ψ is surjective. Let $a \in \mathrm{Im}(\varphi)$. So there exists $x \in G$ such that $a = \varphi(x)$. Consider $Kx \in G/K$. Then $\psi(Kx) = \varphi(x) = a$. Thus ψ is surjective.
Since ψ is a well-defined bijective homomorphism, it is an ismorphism, as desired. ■

1.2 Direct Products, Centers, and Inner Automorphisms

Defn: Let A, B be groups. The **direct product** of A and B is a group which, as a set, is

$$A \oplus B = \{(a,b) \mid a \in A, b \in B\}$$

under the operation

$$(a,b) \star (a',b') = (aa', bb').$$

Ex: $\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$. Consider $\varphi : \mathbb{Z}_2 \oplus \mathbb{Z}_2 \to \mathbb{Z}_2$, $(a,b) \mapsto a$. Then $\operatorname{Im}(\varphi) = \{0,1\} = \mathbb{Z}_2$, and $\ker(\varphi) = \{(0,0),(0,1)\}$. Since there is only one group with 2 elements, $\ker(\varphi) \cong \mathbb{Z}_2$. By the First Isomorphism Theorem, $(\mathbb{Z}_2 \oplus \mathbb{Z}_2)/\ker(\varphi) \cong \mathbb{Z}_2$.

Defn: The **center** $Z(G)$ of a group G is the set of all elements which commute with all elements of G, i.e.

$$Z(G) = \{x \in G \mid xg = gx \forall g \in G\}.$$

This is sometimes called the **centralizer** of G.

Theorem: The center of a group is a subgroup, i.e. $Z(G) \leq G$.

Defn: The relation $g \sim g' \iff g = xg'x^{-1}$ for some $x \in G$ is an equivalence relation called **conjugation**. We say $g, g' \in G$ are **conjugates**.

Defn: For an element $x \in G$, the **inner automorphism** of G induced by x is $T_x : G \to G$ defined by $T_x(g) = xgx^{-1}$.

Theorem: The set of all inner automorphisms of G form a group.

$$\operatorname{Inn}(G) = \{T_x \mid x \in G\}, \qquad T_x \star T_y = T_x \circ T_y.$$

Theorem:

$$G/Z(G) \cong \operatorname{Inn}(G).$$

Proof: Consider $\psi : G \to \operatorname{Inn}(G)$, $x \mapsto T_x$. (Left as an exercise for the reader – show that this is a homomorphism.) ψ is manifestly surjective, i.e. $\operatorname{Inn}(G) = \operatorname{Im}(G)$. Also, $\ker(\psi) = \{x \in G \mid \psi(x) = I_G\} = \{x \in G \mid T_x = I_G\} = \{x \in G \mid xgx^{-1} = g \forall g \in G\} = \{x \in G \mid xg = gx \forall g \in G\} = Z(G)$. Then this is of the form for the First Isomorphism Theorem, so $G/Z(G) \cong \operatorname{Inn}(G)$ as desired. ■