Chapter 6: Isomorphisms. *Notion first introduced by Galois about 175 years ago.*

Dr. Jehan Al-bar

December 5, 2010

Motivation

A Real life example demonstrating where this idea came from is counting in two different languages.
A formal method for determining whether two groups defined in different terms are really the same is given in this chapter.

Definition and Examples

Definition (Group Isomorphism)

An isomorphism ϕ from a group G to a group $\overline{G}$ is a one-to-one mapping from G onto $\overline{G}$ that preserves the group operation. That is

$$\phi(ab) = \phi(a)\phi(b) \quad \text{for all } a, b \in G.$$

If there is an isomorphism from G onto $\overline{G}$, we say that G and $\overline{G}$ are isomorphic and we write $G \approx \overline{G}$.

Note that in the definition of the isomorphism the operation on the left side of the equal sign is that of G. While the operation on the right side is that of $\overline{G}$. Also in that definition, indirectly it is suggested the isomorphic groups have the same order.

Steps to Show that a Group G is Isomorphic to the Group $\overline{G}$.

1. Define a function ϕ from G to $\overline{G}$.
2. Prove that ϕ is one-to-one; assume that $\phi(a) = \phi(b)$ and prove that $a = b$.
3. Prove that ϕ is onto; for any element $\overline{g} \in \overline{G}$, find an element $g \in G$ with $\phi(g) = \overline{g}$.
4. Prove that ϕ is operation preserving; that is to show $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

Steps to Show that a Group G is Isomorphic to the Group $\overline{G}$.

Step 4 says that the two processes, operating and mapping, can be done in either order without affecting the result. That is to be able to have the same result by combining two elements and then mapping, or by mapping two elements and then combining them.

Example

$\lim_{x\to a}(f(x)\cdot g(x)) = \lim_{x\to a} f(x) \lim_{x\to a} g(x)$
or
$\int_a^b (f+g)dx = \int_a^b fdx + \int_a^b gdx.$

Examples

1. Let G be the real numbers under addition and let $\overline{G}$ be the positive real numbers under multiplication. Then G and $\overline{G}$ are isomorphic under the mapping $\phi(x) = 2^x$.
2. Any infinite cyclic group is isomorphic to Z under the mapping $a^k = k$.
3. Any finite cyclic group $< a >$ of order n is isomorphic to Z_n under the mapping $a^k = k \ mod \ n$.
4. $U(10) \approx Z_4$ and $U(5) \approx Z_4$.

Non Examples

1. The mapping from $\mathcal{R}$ under addition to itself given by $\phi(x) = x^3$ is not an isomorphism.
2. $U(10) \not\approx U(12)$.

Cayley's Theorem

Theorem

Every group is isomorphic to a group of permutations.

Let G be any group. Consider the left regular representation of G denoted by $\overline{G} = \{T_g : g \in G\}$ where T_g is a function defined on G by $T_g(x) = gx$ for all $x \in G$. Then $G \approx \overline{G}$ under the isomorphism $\phi(g) = T_g$.

Example

Example

Consider the group $U(12) = \{1, 5, 7, 11\}$, Then the left regular representation $\overline{U(12)} = \{T_1, T_5, T_7, T_{11}\}$, where

$$T_1 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{bmatrix}, \ T_5 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{bmatrix},$$

$$T_7 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{bmatrix}, \ T_{11} = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{bmatrix}.$$ Cayley tables for $U(12)$ and $\overline{U(12)}$

Properties of Isomorphisms

Theorem (Properties of Isomorphisms Acting on Elements)

Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

- *ϕ carries the identity of G to the identity of $\overline{G}$.*
- *For every integer n and for every group element a in G, $\phi(a^n) = [\phi(a)]^n$.*
- *For any elements $a, b \in G$, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.*
- *$G =< a >$ if and only if $\overline{G} =< \phi(a) >$.*

Properties of Isomorphisms

Theorem (Properties of Isomorphisms Acting on Elements Continue)

- $|a| = |\phi(a)|$ *for all* $a \in G$ *(isomorphism preserve orders).*
- *For a fixed integer* k *and a fixed group element* $b \in G$ *, the equation* $x^k = b$ *has the same number of solutions in* G *as does the equation* $x^k = \phi(b)$ *in* $\overline{G}$*.*
- *If* G *is finite, then* G *and* $\overline{G}$ *have exactly the same number of elements of every order.*