Structural Properties

Definition

A *structural property* is a property that must be shared by any two isomorphic binary algebraic structures.

In fact, to show that two structures are not isomorphic, show that there is a property held by one but not the other.

Properties

1). Cardinality

2). Commutativity

3). Associativity

4). Identity Element

5). Inverse Elements

6). Equation Solutions

7). Idempotent Elements

Theorem

Let S, T be binary algebraic structures.

$$S \simeq T \implies |S| = |T|$$

Proof

Assume $S \simeq T$
There exists isomorphism $\phi : S \to T$
ϕ is a bijection
$\therefore |S| = |T|$

Theorem

Let S, T be binary algebraic structures.

$$\phi : S \to T \text{ is an isomorphism} \implies (\forall\, x, y \in S, xy = yx \implies \phi(x)\phi(y) = \phi(y)\phi(x))$$

Proof

Assume $\phi : S \to T$ is an isomorphism
Assume $x, y \in S$
Assume $xy = yx$
$\phi(xy) = \phi(x)\phi(y)$

$\phi(xy) = \phi(yx) = \phi(y)\phi(x)$
$\therefore \phi(x)\phi(y) = \phi(y)\phi(x)$

Example

$\langle \mathbb{R}, \cdot \rangle \not\simeq \langle M(\mathbb{R}), \cdot \rangle$ because $\langle \mathbb{R}, \cdot \rangle$ is commutative; however, $\langle M(\mathbb{R}), \cdot \rangle$ is not.

Theorem

Let S, T be binary algebraic structures.

$\phi : S \to T$ is an isomorphism $\implies$

$$(\forall\, x, y, z \in S, (xy)z = x(yz) \implies [\phi(x)\phi(y)]\phi(z) = \phi(x)[\phi(y)\phi(z)])$$

Proof

Assume $\phi : S \to T$ is an isomorphism
Assume $x, y, z \in S$
Assume $x(yz) = x(yz)$
$\phi((xy)z) = \phi(xy)\phi(z) = [\phi(x)\phi(y)]\phi(z)$
$\phi((xy)z) = \phi(x(yz))\phi(x)\phi(yz) = \phi(x)[\phi(y)\phi(z)]$
$\therefore [\phi(x)\phi(y)]p(z) = \phi(x)[\phi(y)\phi(z)]$

Definition

Let S be a binary algebraic structure. To say that $e \in S$ is an *identity* element for S means:

$$\forall\, a \in S, ea = ae = a$$

Theorem

A binary algebraic structure has at most one identity element.

Proof

Assume S is a binary algebraic structure
Assume $e_1, e_2 \in S$ are identity elements for S
$e_1 e_2 = e_1$
$e_1 e_2 = e_2$
$\therefore e_1 = e_2$

Theorem

Let S and T be binary algebraic structures

$\phi : S \to T$ is an isomorphism $\implies$

$$(e \text{ is an identity element for } S \implies \phi(e) \text{ is an identity element for } T)$$

Proof

Assume $\phi : S \to T$ is an isomorphism
Assume e is an identity element for S
$\forall\, s \in S, es = se = s$
ϕ is well-defined
$\exists\, \phi(e) \in T$
Assume $t \in T$
ϕ is onto
$\exists\, s \in S, \phi(s) = t$
ϕ is a homomorphism
$\phi(es) = \phi(e)\phi(s) = \phi(e)t$
$\phi(es) = \phi(se) = \phi(s)\phi(e) = t\phi(e)$
$\phi(es) = \phi(s) = t$
$\phi(e)t = t\phi(e) = t$
$\therefore\ \phi(e)$ is an identity for T

Example

$$S = a, b, c, d$$

$*$	a	b	c	d
a	a	c	b	d
b	c	d	a	c
c	b	a	c	a
d	d	c	a	b

$S \not\simeq \mathbb{Z}_4$ because Z_4 has an identity (0); however, S does not have an identity element.

Definition

Let S be a binary algebraic structure with identity e and let $a \in S$. To say that $b \in S$ is an inverse for a means:

$$ab = ba = e$$

Notation

Additive: $b = -a$

Multiplicative: $b = a^{-1}$

Theorem

Let S and T be binary algebraic structures such that e is an identity element for S.

$\phi : S \to T$ is an isomorphism $\implies$

$$(\forall\, a \in S, b \in S \text{ is an inverse for } a \implies \phi(b) \text{ is an inverse for } \phi(a))$$

Proof

Assume $\phi : S \to T$ is an isomorphism
Assume $a \in S$
Assume $b \in S$ is an inverse for a
$ab = ba = e$
ϕ is well-defined
$\exists\, \phi(a) \in T$ and $\exists\, \phi(b) \in T$
$\phi(e)$ is an identity for T
ϕ is a homomorphism
$\phi(ab) = \phi(a)\phi(b)$
$\phi(ab) = \phi(ba) = \phi(b)\phi(a)$
$\phi(ab) = \phi(e)$
$\phi(a)\phi(b) = \phi(b)\phi(a) = \phi(e)$
$\therefore \phi(b)$ is an inverse for $\phi(a)$

Theorem

Let S and T be binary algebraic structures.

$$\phi : S \to T \text{ is an isomorphism } \implies (\forall\, x, a \in S, xx = a \implies \phi(x)\phi(x) = \phi(a))$$

Proof

Assume $\phi : S \to T$ is an isomorphism
Assume $x, a \in S$
Assume $xx = a$
ϕ is well-defined
$\exists\, \phi(x), \phi(a) \in T$
ϕ is a homomorphism
$\phi(xx) = \phi(x)\phi(x)$
$\phi(xx) = \phi(a)$
$\therefore \phi(x)\phi(x) = \phi(a)$

Example

$\langle \mathbb{C}, \cdot \rangle \not\simeq \langle \mathbb{R}, \cdot \rangle$ because $\forall\, c \in \mathbb{C}$ the equation $zz = c$ has a solution in $\mathbb{C}$; however, $xx = -1$ has no solutions in $\mathbb{R}$.

ABC: $\exists\, \phi : \langle \mathbb{C}, \cdot \rangle \to \langle \mathbb{R}, \cdot \rangle$

$-1 \in \mathbb{R}$
ϕ is onto
$\exists\, c \in \mathbb{C}, \phi(c) = -1$
$zz = c$ has a solution in $\mathbb{C}$
ϕ is well-defined
$\exists\, x \in \mathbb{R}, \phi(z) = x$
ϕ is a homomorphism

$\phi(zz) = \phi(z)\phi(z) = xx = x^2$
$\phi(zz) = \phi(c) = -1$
$x^2 = -1$
Contradiction!
z has no image under ϕ
ϕ is not well-defined
no such ϕ exists
$\therefore \langle \mathbb{C}, \cdot \rangle \not\simeq \langle \mathbb{R}, \cdot \rangle$

Example

$\langle \mathbb{Z}, \cdot \rangle \not\simeq \langle \mathbb{Z}, + \rangle$ because $nn = n$ has two solutions in $\langle \mathbb{Z}, \cdot \rangle$; however, $m + m = m$ has only one solution in $\langle \mathbb{Z}, + \rangle$.

ABC: $\exists\, \phi : \langle \mathbb{Z}, \cdot \rangle \to \langle \mathbb{Z}, + \rangle$

Assume $n \in \langle \mathbb{Z}, \cdot \rangle$
Assume $nn = n$
$n^2 - n = 0$
$n(n-1) = 0$
$n = 0, 1$

ϕ is well-defined
$\exists\, m \in \langle \mathbb{Z}, + \rangle, \phi(n) = m$
ϕ is a homomorphism
$\phi(nn) = \phi(n) + \phi(n) = m + m$
$\phi(nn) = \phi(n) = m$
$m + m = m$
$2m = m$
$m = 0$

$\phi(0) = 0$ and $\phi(1) = 0$
ϕ is not one-to-one
Contradiction!
No such ϕ exists
$\therefore \langle \mathbb{Z}, \cdot \rangle \not\simeq \langle \mathbb{Z}, + \rangle$

Definition

Let S be a binary algebraic structure. To say that $a \in S$ is *idempotent* in S means $aa = a$.

Theorem

Let S and T be binary algebraic structures.

$\phi : S \to T$ is an isomorphism $\implies$

$$(\forall\, a \in S, a \text{ is idempotent in } S \implies \phi(a) \text{ is idempotent in } T)$$

Proof

Assume $\phi : S \rightarrow T$ is an isomorphism
Assume $a \in S$
Assume a is idempotent in S
$aa = a$
By previous theorem, $\phi(a)\phi(a) = \phi(a)$
$\therefore \phi(a)$ is idempotent in T