Week 2.

Defn. (Binary Operation)

A binary operation $*$ on a set S is a function mapping $S \times S$ into S, i.e., $* : S \times S \to S$. $\forall\ (a,b) \in S \times S,\ \ *((a,b)) =_{def} a * b$.

Defn. (q-ary Operation)

A q-ary operation is a function $* : \underbrace{S \times S \times \cdots \times S}_{q-tuple} \to S$.

Defn. (Closed)

Let $*$ be a binary operation on S and $H \subseteq S$. The subset H is closed under $*$ if $*|_{H\times H} : S\times S \to H$ or $*((a,b)) = a*b \in H,\ \forall\ (a,b) \in H\times H$. "$*|_{H\times H}$ is an induced operation of $*$ on H."

Defn. A binary operation $*$ on a set S is

(i) commutative iff $a * b = b * a,\ \forall\ a,b \in S$;

(ii) associative iff $(a * b) * c = a * (b * c),\ \forall\ a,b,c \in S$;

(iii) idempotent iff $a^2 = a * a = a,\ \forall\ a \in S$; and

(iv) nilpotent iff $a^2 = c$ where $a \in S$ and c is a constant. (fixed element)

e.g. Theorem (Associativity of Composition)

Let S be a set and let f, g and h be functions mapping S into S. Then $f \circ (g \circ h) = (f \circ g) \circ h$.

Defn. Let S be a set with a binary operation $*$ on S. Then $< S, * >$ is known as a binary algebraic structure or a **groupoid**.

Defn. A groupoid $< S, * >$ is a **semigroup** if $*$ is associative on S.

Defn. A groupoid $< S, * >$ is a **quasigroup** if $\forall\ a, b \in S,\ a * x = b$ and $y * a = b$ have unique solution in S. (Or $< S, * >$ has latin property.)

Defn. An element $e \in S$ in a groupoid $< S, * >$ is an identity element for $*$ if $\forall\ a \in S,\ e*a = a*e = a$. ($e$ is an identity element of $< S, * >$.)

Theorem If e is an identity element of $< S, * >$, then e is unique.

Proof. Let e' and e'' be two identity elements.
Then $e' * e'' = e'$ and also $e' * e'' = e''$. ■

Defn. A semigroup with identity element is called a **monoid**.

Defn. Let $< S, * >$ be a monoid. Then an element a' is an inverse element of $a \in S$ if $a' * a = a * a' = e$.

Defn. Let $< S, * >$ be a monoid and for each $a \in S$, a has an inverse element. Then $< S, * >$ is called a group.

Theorem A semigroup $< G, * >$ with latin property is a group.

Proof. It suffices to prove that $< G, * >$ has an identity element and $\forall\ a \in G$, a has a unique inverse element.

$a * x = a$ has a unique solution e_a, i.e., $a * e_a = a$.

$a * (e_a * a) = (a * e_a) * a = a * a$. (unique solution)

$\Rightarrow e_a * a = a$

$\forall\ b \in G,\ b * e_a = (y * a) * e_a = y * (a * e_a) = y * a = b.$

($\exists\ y$, s.t. $y * a = b$)

$\exists\ x$, s.t. $a * x = b$, $e_a * b = e_a * (a * x) = (e_a * a) * x = a * x = b.$

$\Rightarrow e_a$ is in fact an identity element of $< G, * >$, call it "e".

Now, $\forall\ a,\ \exists\ a'$, s.t. $a * a' = e$ and $\exists\ a''$, s.t. $a'' * a = e$.

$a'' = a'' * e = a'' * (a * a') = (a'' * a) * a' = e * a' = a'.$ ■

Defn. Let $< S, * >$ be a groupoid. An element e is a left iden-

tity (inverse) element if $e * a = a (a' * a = e)\ \forall\ a \in S$, and an element e is a right identity (inverse) element if $a * e = a (a * a' = e)\ \forall\ a \in S$.

Theorem (One-sided Conditions)

Let $< G, * >$ be a semigroup with a left identity element e and a left inverse element a' exists for each $a \in G$. Then $< G, * >$ is a group.

Proof. By assumption, $\forall\ a \in G,\ e * a = a$ and $a' * a = e$.

Claim: $\forall\ a \in G,\ a * e = a$.

Let a'' be the element such that $a'' * a' = e$.
(left inverse element of a'.)
Then $a'' * e = a'' * (a' * a) = (a'' * a') * a = e * a = a$.
Therefore $a * e = (a'' * e) * e = a'' * (e * e) = a'' * e = a$. (1)
Claim: $\forall\ a \in G$, if $a' * a = e$, then $a * a' = e$.
Since $a'' * e = a''$ and by (1) $a'' * e = a,\ a'' = a$.
By $a'' * a' = a * a'$, we have the claim. ■

Defn. (Abelian Group)

A group $< G, * >$ is called abelian if $*$ is commutative on G.

e.g. $< \mathbb{Z}, + >$ is an abelian group.

Fact All groups with at most five elements are abelian.

Proof. Do it yourself.

Defn. Let $< S, * >$ and $< S', *' >$ be two groupoid. An isomorphism of S with S' is a one-to-one function mapping S onto S' such that $\phi(x * y) = \phi(x) *' \phi(y)$ for all $x, y \in S$. (2)

Note. (2) is called a homomorphism property.

Defn.

$$(2) + \begin{cases} \phi \text{ is a function } \rightarrow \phi \text{ is a homomorphism.} \\ \phi \text{ is a one-to-one function } \rightarrow \phi \text{ is a monomorphism.} \\ \phi \text{ is an onto function } \rightarrow \phi \text{ is an epimorphism.} \\ \phi \text{ is a bijection } \rightarrow \phi \text{ is an isomorphism.} \end{cases}$$

Example $< \mathbb{R}, + >$ and $\mathbb{R}^+, \cdot$ are groups. Prove that this two groups are isomorphic.

Proof. Define $\phi : \mathbb{R} \rightarrow \mathbb{R}^+$ by $\phi(x) = e^x \ \forall \ x \in \mathbb{R}$.
Then ϕ is a bijection and $\phi(x + y) = e^{x+y} = e^x \cdot e^y = \phi(x) \cdot \phi(y)$.

(*) How to show that two structures are isomorphic?

Step 1. Define a mapping ϕ. (It is a function!)

Step 2. Show that ϕ is one-to-one.

Step 3. Show that ϕ is onto.

Step 4. Show that the homomorphism property of ϕ holds.

Note. If two structures are isomorphic, then they have the same structural properties.

Theorem If $< S, * >$ has an identity element e, then $< S', *' >$ has an identity element $e' = \phi(e)$ provided $< S, * >$ and $< S', *' >$ are isomorphic.

Proof. $\forall \ s' \in S', \ \exists!\ s$, such that $\phi(s) = s'$.
$s' * e' = \phi(s) *' \phi(e) = \phi(s * e) = \phi(s) = s'$.
Similarly, $e' *' s' = s'$. ■

Theorem Let $< S, * > \cong < S', \circ >$ and $x * x = c$ has a unique solution for all $c \in S$. Then, for all $c' \in s', \ y * y = c'$ has a unique solution in S'.

Proof. Let a_c be the unique solution of $x * x = c$ where $\phi(c) = c'$.

Then $\phi(a_c)$ is the unique solution of $y \circ y = c'$.
$(\phi(a_c) \circ \phi(a_c) = \phi(a_c * a_c) = \phi(c) = c'.)$ ■

Theorem If $< S, * > \cong < S', 0 >$, then $|S| = |S'|$.

Proof. Trivial.

Examples:

1. $< \mathbb{Q}, + >$ and $< \mathbb{Z}, + >$ are not isomorphic.
   $x + x = c$ has a unique solution for each $c \in \mathbb{Q}$, but not in $\mathbb{Z}$.
2. $< \mathbb{C}, \cdot >$ and $< \mathbb{R}, \cdot >$ are not isomorphic.
   $x \cdot x = c$ has a unique solution for each $c \in C$, but not in $\mathbb{R}$.
3. $< M_2(\mathbb{R}), \cdot >$ and $< \mathbb{R}, \cdot >$ are not isomorphic where $M_2(\mathbb{R})$ is the set of all real 2×2 matrices.
   The first one is not commutative but the second one is commutative.
4. $< \mathbb{Q}, + >$ and $< \mathbb{R}, + >$ are not isomorphic.
   There cardinalities are different.