Student Online Teaching Advice Notice

The materials and content presented within this session are intended solely for use in a context of teaching and learning at Trinity.

Any session recorded for subsequent review is made available solely for the purpose of enhancing student learning.

Students should not edit or modify the recording in any way, nor disseminate it for use outside of a context of teaching and learning at Trinity.

Please be mindful of your physical environment and conscious of what may be captured by the device camera and microphone during videoconferencing calls.

Recorded materials will be handled in compliance with Trinity's statutory duties under the Universities Act, 1997 and in accordance with the University's policies and procedures.

Further information on data protection and best practice when using videoconferencing software is available at https://www.tcd.ie/info_compliance/data-protection/.

7.2 Semigroups

Definition: A semigroup is a set endowed with an associative binary operation. We denote the semigroup $(A, *)$

Examples:

1. $(\mathbb{R}, +)$ and $(\mathbb{R}, \times)$ are semigroups.
2. Let A be a set and let $P(A)$ be its power set. $(P(A), \cap)$ and $(P(A), \cup)$ are both semigorups.
3. $(M_n, *)$, the set of $n \times n$ matrices with entries in $\mathbb{R}$ with the operation of matrix multiplication (which is associative $\rightarrow$ a bit gory to prove) forms a semigroup.

Since $*$ is associative on a semigroup, we can define a^n :
$a^1 = a$
$a^2 = a * a$
$a^3 = a * a * a$
$\vdots$
Recursively, $a^1 = a$ and $a^n = a * a^{n-1}, \forall n > 1$

NB: In $(\mathbb{R}, \times), \forall a \in \mathbb{R}, a^n = \underbrace{a \times a \times ... \times a}_{n\ times}$, whereas in $(\mathbb{R}, +), \forall a \in \mathbb{R}, a^n = \underbrace{a + a + ... + a}_{n\ times} = na$. Be careful what $*$ stands for!

Theorem: Let $(A, *)$ be a semigroup. $\forall a \in A, a^m * a^n = a^{m+n}, \forall m, n \in \mathbb{N}^*$.

Proof: By induction on m.

Base Case: $m = 1$ $\quad a^1 * a^n = a * a^n = a^{1+n}$

Inductive Step: Assume the result is true for $m = p$, **i.e.** $a^p * a^n = a^{p+n}$ and seek to prove that $a^{p+1} * a^n = a^{p+1+n}$

$a^{p+1} * a^n = (a * a^p) * a^n = a * (a^p * a^n) = a * a^{p+n} = a^{p+1+n}$

Theorem: Let$(A, *)$ be a semigroup. $\forall a \in A, (a^m)^n = a^{mn}, \forall m, n \in \mathbb{N}^*$

Proof: By induction on n.

Base Case: $n = 1$ $\quad (a^m)^1 = a^m = a^{m \times 1}$

Inductive Step: Assume the result if true for $n = p$, **i.e.** $(a^m)^p = a^{mp}$ and seek to prove that $(a^m)^{p+1} = a^{m(p+1)}$

$(a^m)^{p+1} = (a^m)^p * a^m = a^{mp} * a^m = a^{mp+m} = a^{m(p+1)}$ by the previous theorem.

7.2.1 General Associative Law

Let $(A, *)$ be a semigroup. $\forall a_1, ..., a_s \in A, a_1 * a_2 * ... * a_s$ has the same value regardless of how the product is bracketed.

Proof Use associativity of $*$.

qed

NB: Unless $(A, *)$ has a commutative binary operation, $a_1 * a_2 * ... * a_s$ does depend on the ORDER in which the $a_j's$ appear in $a_1 * a_2 * ... * a_s$

7.3 Identity Elements

Definition: Let $(A, *)$ be a semigroup. An element $e \in A$ is called an identity element for the binary operation $*$ if $e * x = x * e = x, \forall x \in A$.

Examples:

1. $(\mathbb{R}, +)$ has 0 as the identity element.
2. $(\mathbb{R}, \times)$ has 1 as the identity element.
3. Given a set A, $(P(A), \cup)$ has $\emptyset$ (the empty set) as its identity element, whereas $(P(A), \cap)$ has A as its identity element.
4. $(M_n, *)$ has I_n, the identity matrix, as its identity element.

Theorem A binary operation on a set cannot have more than one identity element, **i.e.** if an identity element exists, then it is unique.

Proof: Assume not (proof by contradiction). Let e and e' both be identity elements for a binary operation on a set A. $e = e * e' = e'$

qed

7.4 Monoids

Definition: A monoid is a set A endowed with an associative binary operation $*$ that has an identity element e. In other words, a monoid is a semigroup $(A, *)$, where $*$ has an identity element e.

Definition: A monoid $(A, *)$ is called commutative (or Abelian) if the binary operation $*$ is commutative.

Examples:

1. $(\mathbb{R}, +)$ is a commutative monoid with $e = 0$.
2. $(\mathbb{R}, \times)$ is a commutative monoid with $e = 1$.
3. Given a set A, $(P(A), \cup)$ is a commutative monoid with $e = \emptyset$.
4. $(M_n, *)$ is a monoid since $e = I_n$, but it is not commutative since matrix multiplication is not commutative.
5. $(\mathbb{N}, +)$ is a commutative monoid with $e = 0$, whereas $(\mathbb{N}^*, +)$ is merely a semigroup (recall $\mathbb{N}^* = \mathbb{N} \backslash \{0\}$)

Let $(A, *)$ be a monoid and let $a \in A$. We define $a^0 = e$, the identity element.

Theorem: Let $(A, *)$ be a monoid and let $a \in A$. Then $a^m * a^n = a^{m+n}, \forall m, n \in \mathbb{N}$.

Remark: Recall that we proved this theorem for semigroups if $m, n \in \mathbb{N}^*$. We now need to extend that result.

Proof: A monoid is a semigroup $\implies \forall a \in A, a^m * a^n = a^{m+n}$ whenever $m, n \in \mathbb{N}^*$, **i.e.** $m > 0$ and $n > 0$. Now let $m = 0$. $a^m * a^n = a^0 * a^n = e * a^n = a^n = a^{0+n}$
If $n = 0, a^m * a^n = a^m * a^0 = a^m * e = a^m = a^{m+0}$.

qed

Theorem: Let $(A, *)$ be a monoid, $\forall a \in A \ \forall m, n \in \mathbb{N}$, $(a^m)^n = a^{mn}$.

Remark: Once again, we had this result for semigroups when $m > 0$ and $n > 0$.

Proof: By the remark, we only need to prove the result when $m = 0$ or $n = 0$. If $m = 0, (a^0)^n = (e)^n = e = a^0 = a^{0 \times n}$. If $n = 0$, then $(a^m)^0 = e = a^0 = a^{0 \times m}$.

qed

7.5 Inverses

Task: Understand what an inverse is and what formal properties it satisfies.

Definition: Let $(A, *)$ be a monoid with identity element e and let $x \in A$. An element y of A is called the inverse of x if $x * y = y * x = e$. If an element $x \in A$ has an inverse, then x is called invertible.

Examples:

1. $(\mathbb{R}, +)$ has identity element 0. $\forall x \in \mathbb{R}, (-x)$ is the inverse of x since $x + (-x) = (-x) + x = 0$.
2. $(\mathbb{R}, \times)$ has identity element 1. $x \in \mathbb{R}$ is invertible only if $x \neq 0$. If $x \neq 0$, the inverse of x is $\frac{1}{x}$ since $x \times \frac{1}{x} = \frac{1}{x} \times x = 1$.
3. $(M_n, *)$ the identity element is I_n. $A \in M_n$ is invertible if $\det(A) \neq 0$. A^{-1} the inverse is exactly the one you computed in linear algebra. If $\det(A) = 0, A$ is NOT invertible.
4. Given a set $A, (P(A), \cup)$ has $\emptyset$ as its identity element. Of all the elements of $P(A)$, only $\emptyset$ is invertible and has itself as its inverse: $\emptyset \cup \emptyset = \emptyset \cup \emptyset = \emptyset$.