# 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/.**

© Trinity College Dublin 2020

# 7 Abstract Algebra

**Task:** Understand binary operations, semigroups, monoids, and groups as well as their properties.

## 7.1 Binary Operations

**Definition:** Let $A$ be a set. A binary operation $*$ on $A$ is an operation applied to any two elements $x, y \in A$ that yields an element $x * y$ in $A$. In other words, $*$ is a binary operation on $A$ if $\forall x, y \in A, x * y \in A$.

**Examples:**

1. $\mathbb{R}, +$ addition on $\mathbb{R} : \forall x, y \in \mathbb{R}, x + y \in \mathbb{R}$
2. $\mathbb{R}, -$ subtraction on $\mathbb{R} : \forall x, y \in \mathbb{R}, x - y \in \mathbb{R}$
3. $\mathbb{R}, \times$ multiplication on $\mathbb{R} : \forall x, y \in \mathbb{R}, x \times y \in \mathbb{R}$
4. $\mathbb{R}, /$, division on $\mathbb{R}$ is NOT a binary operation because $\forall x \in \mathbb{R}\ \exists 0 \in \mathbb{R}$ s.t. $\frac{x}{0}$ is undefined (not an element of $\mathbb{R}$)
5. Let $A$ be the set of all lists or strings. Concatenation is a binary operation.

**Definition:** A binary operation $*$ on a set $A$ is called commutative if $\forall x, y \in A, x * y = y * x$

**Examples:**

1. $\mathbb{R}, +$ is commutative since $\forall x, y \in \mathbb{R}, x + y = y + x$
2. $\mathbb{R}, \times$ is commutative since $\forall x, y \in \mathbb{R}, x \times y = y \times x$
3. $\mathbb{R}, -$ is not commutative since $\forall x, y \in \mathbb{R}, x - y \neq y - x$ in general. $x - y = y - x$ only if $x = y$
4. Let $M_n$ be the set of $n$ by $n$ matrices with entries in $\mathbb{R}$, and let $*$ be matrix multiplication. $\forall A, B \in M_n, A * B \in M_n$, so $*$ is a binary operation, but $A * B \neq B * A$ in general. Therefore $*$ is not commutative.

**Definition:** A binary operation $*$ on a set $A$ is called associative if $\forall x, y, z \in A$ $(x * y) * z = x * (y * z)$

**Examples:**

1. $\mathbb{R}, +$ is associative since $\forall x, y, z \in \mathbb{R}, (x + y) + z = x + (y + z)$
2. $\mathbb{R}, \times$ is associative since $\forall x, y, z \in \mathbb{R}, (x \times y) \times z = x \times (y \times z)$
3. Intersection $\cap$ on sets is associative since $\forall A, B, C$ sets $(A \cap B) \cap C = A \cap (B \cap C)$.
4. Union $\cup$ on sets is associative since $\forall A, B, C$ sets $(A \cup B) \cup C = A \cup (B \cup C)$
5. $\mathbb{R}, -$ is not associative since $(1-3)-5 = -2-5 = -7$ but $1-(3-5) = 1-(-2) = 1+2 = 3$

**Remark:** When we are dealing with associative binary operations we can drop the parentheses, **i.e.** $(x * y) * z$ can be written $x * y * z$.

## 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 semigroups.
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 is 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 <u>ORDER</u> in which the $a_j's$ appear in $a_1 * a_2 * ... * a_s$