# 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/.**

## 7.5 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: $\emptyset \cup \emptyset = \emptyset \cup \emptyset = \emptyset$.

**Theorem:** Let $(A, *)$ be a monoid. If $a \in A$ has an inverse, then that inverse is unique.

**Proof:** By contradiction: Assume not, then $\exists a \in A$ s.t. both $b$ and $c$ in $A$ are its inverses, **i.e.** $a * b = b * a = e$, the identity element of $(A, *)$, and $a * c = c * a = e$, where $b \neq c$. Then $b = b * e = b * (a * c) = (b * a) * c = e * c = c$. $\Rightarrow\Leftarrow$

**qed**

Since every invertible element $a$ of a monoid $(A, *)$ has a unique inverse, we can denote the inverse by the more standard notation $a^{-1}$.

Next, we need to understand inverses of elements obtained via the binary operation:

**Theorem:** Let $(A, *)$ be a monoid, and let $a, b$ be invertible elements of $A$. Then $a * b$ is also invertible, and $(a * b)^{-1} = b^{-1} * a^{-1}$.

**Remark:** You might remember this formula from linear algebra when you looked at the inverse of a product of matrices $AB$.

**Proof:** Let $e$ be the identity element of $(A, *)$. $a * a^{-1} = a^{-1} * a = e$, and $b * b^{-1} = b^{-1} * b = e$. We would like to show $b^{-1} * a^{-1}$ is the inverse of $a * b$ by computing $(a * b) * (b^{-1} * a^{-1})$ and $(b^{-1} * a^{-1}) * (a * b)$ and showing both are $e$.

$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$

$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = (b^{-1} * e) * b = b^{-1} * b = e$

Thus $b^{-1} * a^{-1}$ satisfies the conditions needed for it to be the inverse of $a * b$. Since an inverse is unique, $a * b$ is invertible and $b^{-1} * a^{-1}$ is its inverse.

**qed**

**Theorem:** Let $(A, *)$ be a monoid, and let $a, b \in A$. Let $x \in A$ be invertible. $a = b * x \Leftrightarrow b = a * x^{-1}$. Similarly, $a = x * b \Leftrightarrow b = x^{-1} * a$

**Proof:** Let $e$ be the identity element of $(A, *)$.

First $a = b * x \Leftrightarrow b = a * x^{-1}$:

"$\Rightarrow$" Assume $a = b * x$. Then $a * x^{-1} = (b * x) * x^{-1} = b * x * x^{-1} = b * e = b$ as needed.

"$\Leftarrow$" Assume $b = a * x^{-1}$. Then $b * x = (a * x^{-1}) * x = a * (x^{-1} * x) = a * e = a$ as needed.

Apply the same type of argument to show $a = x * b \Leftrightarrow b = x^{-1} * a$.

**qed**

Let $(A, *)$ be a monoid. We can now make sense of $a^n$ for $n \in \mathbb{Z}, n < 0$ for every $a \in A$ invertible. Since $n$ is a negative integer, $\exists p \in \mathbb{N}$ s.t. $n = -p$. Set $a^n = a^{-p} = (a^p)^{-1}$.

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

**Proof:** When $m \geq 0$ and $n \geq 0$, we have already proven this result. The rest of the proof splits into cases.

**Case 1:** $m = 0$ or $n = 0$

If $m = 0$, $n \in \mathbb{Z}$, $a^m * a^n = a^0 * a^n = e * a^n = a^n = a^{0+n}$ as needed.

If $m \in \mathbb{Z}$, $n = 0$, $a^m * a^n = a^m * a^0 = a^m * e = a^m = a^{m+0}$ as needed.

**Case 2:** $m < 0$ and $n < 0$

$m < 0 \Rightarrow \exists p \in \mathbb{N}\, s.t.\, p = -m$. $n < 0 \Rightarrow \exists q \in \mathbb{N}\, s.t.\, q = -n$.

$a^m = a^{-p} = (a^p)^{-1}$ and $a^n = a^{-q} = (a^q)^{-1}$

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

**Case 3:** $m$ and $n$ have opposite signs.

Without loss of generality, assume $m < 0$ and $n > 0$ (the case $m > 0$ and $n < 0$ is handled by the same argument). Since $m < 0, \exists p \in \mathbb{N}\, s.t.\, p = -m$. This case splits into two subcases:

**Case 3.1:** $m + n \geq 0$

Set $q = m + n$. Then $a^{m+n} = a^q = e * a^q = (a^p)^{-1} * a^p * a^q = (a^p)^{-1} * a^{p+q} = a^{-p} * a^{p+q} = a^m * a^{-m+m+n} = a^m * a^n$

**Case 3.2:** $m + n < 0$

Set $q = -(m+n) = -m-n \in \mathbb{N}^*$. Then $a^{m+n} = a^{-q} = (a^q)^{-1} * e = (a^q)^{-1} * (a^{-n} * a^n) = (a^q)^{-1} * (a^n)^{-1} * a^n = (a^n * a^q)^{-1} * a^n = (a^{n+q})^{-1} * a^n = (a^{n-m-n})^{-1} * a^n = (a^{-m})^{-1} * a^n = (a^p)^{-1} * a^n = a^m * a^n$

**Theorem:** Let $(A, *)$ be a monoid, and let $a$ be an invertible element of $A$. $\forall m, n \in \mathbb{Z}, (a^m)^n = a^{mn}$.

**Proof:** We consider 3 cases:

**Case 1:** $n > 0$, **i.e.** $n \in \mathbb{N}^*$. $m \in \mathbb{Z}$ with no additional restrictions. We proceed by induction on $n$.

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

**Inductive Step:** We assume $(a^m)^n = a^{mn}$ and seek to prove $(a^m)^{n+1} = a^{m(n+1)}$. Start with $(a^m)^{n+1} = (a^m)^n * (a^m)^1 = a^{mn} * a^m = a^{mn+m} = a^{m(n+1)}$

**Case 2:** $n = 0$; no restriction on $m \in \mathbb{Z}$

$(a^m)^n = (a^m)^0 = e = a^0 = a^{m\times 0} = a^{mn}$

**Case 3:** $n < 0$; no restriction on $m \in \mathbb{Z}$.

Since $n < 0, \exists p \in \mathbb{N}\, s.t.\, p = -n$. By case 1, $(a^m)^p = a^{mp}$

$(a^m)^n = (a^m)^{-p} = ((a^m)^p)^{-1} = (a^{mp})^{-1} = a^{-mp} = a^{m(-p)} = a^{mn}$

## 7.6 Groups

A notion formally defined in the 1870's even though theorems about groups were proven as early as a century before that.

**Definition:** A group is a monoid in which every element is invertible. In other words, a group is a set $A$ endowed with a binary operation $*$ satisfying the following properties:

1. $*$ is associative, **i.e.** $\forall x, y, z \in A, (x * y) * z = x * (y * z)$
2. There exists an identity element $e \in A$, **i.e.** $\exists e \in A\, s.t. \forall a \in A, a * e = e * a = a$
3. Every element of $A$ is invertible, **i.e.** $\forall a \in A\ \exists a^{-1} \in A\, s.t.\, a * a^{-1} = a^{-1} * a = e$

**Notation for Groups:** $(A, *)$ or $(\underbrace{A}_{set}, \underbrace{*}_{operation}, \underbrace{e}_{identity})$

**Remark:** Closure under the operation $*$ is <u>implicit</u> in the definition **i.e.** $\forall a, b \in A, a * b \in A$

**Definition:** A group $(A, *, e)$ is called <u>commutative</u> or <u>Abelian</u> if its operation $*$ is commutative.

**Examples:**

1. $(\mathbb{R}, +, 0)$ is an Abelian group.

   $-x$ is the inverse of $x, \forall x \in \mathbb{R}$

2. $(\mathbb{Q}^*, \times, 1)$ $\quad$ $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ $\quad$ $(\mathbb{Q}^*, \times, 1)$ is Abelian

   $\forall q \in \mathbb{Q}^*, q^{-1} = \frac{1}{q}$ is the inverse.

3. $(\mathbb{R}^3, +, 0)$ vectors in $\mathbb{R}^3$ with vector addition forms an Abelian group.

   $(x, y, z) + (x', y', z') = (x + x', y + y', z + z')$ vector addition.

   $0 = (0, 0, 0)$ is the identity. $(-x, -y, -z) = -(x, y, z)$ is the inverse of $(x, y, z)$.

4. $(\widetilde{M_n}, *, I_n)$ $n \times n$ invertible matrices with real coefficients under matrix multiplication with $I_n$ as the identity element forms a group, which is <u>NOT</u> Abelian.