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/.

7.6 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 implicit in the definition **i.e.** $\forall a, b \in A, a * b \in A$

Definition: A group $(A, *, e)$ is called commutative or Abelian 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 NOT Abelian.

5. Set $A = \mathbb{Z}$ and recall the equivalence relation $x \equiv y \bmod 3$ **i.e.** x and y have the same remainder under the division by 3. Recall that $\mathbb{Z}/\sim = \{0, 1, 2\}$, **i.e.** the set of equivalence classes under the partition determined by this equivalence relation. We denote $\mathbb{Z}/\sim = \{0, 1, 2\} = \mathbb{Z}_3$

   Consider $(\mathbb{Z}_3, \oplus_3, 0)$ where $\oplus_3$ is the operation of addition modulo 3, **i.e.** $1 + 0 = 1, 1 + 1 = 2, 1 + 2 = 3 \equiv 0 \bmod 3$.

Claim: $(\mathbb{Z}_3, \oplus_3, 0)$ is an Abelian group.

Proof of Claim: Associativity of $\oplus_3$ follows from the associativity of $+$, addition on $\mathbb{Z}$. Clearly, 0 is the identity (don't forget 0 stands for all elements with remainder 0 under division by 3, **i.e.** $\{0, 3, -3, 6, -6, ...\}$). To compute inverses recall that $a \oplus_3 a^{-1} = 0$, 0 is the inverse of 0 because $0 + 0 = 0$. 2 is the inverse of 1 because $1 + 2 = 3 \equiv 0 \bmod 3$, and 1 is the inverse of 2 because $2 + 1 = 3 \equiv 0 \bmod 3$.
More generally, consider the equivalence relation on $\mathbb{Z}$ given by $x \equiv y \bmod n$ for $n \geq 1$. $\mathbb{Z}/\sim = \{0, 1, ..., n-1\} = \mathbb{Z}_n$. All possible remainders under division by n are the equivalence classes. Let $\oplus_n$ be addition mod n. By the same argument as above, $(\mathbb{Z}_n, \oplus_n, 0)$ is an Abelian group.

Q: What if we consider multiplication mod n, **i.e.** $\otimes_n$. Is $(\mathbb{Z}_n, \otimes_n, 1)$ a group?

A: No! $(\mathbb{Z}_n, \otimes_n, 1)$ is not a group because 0 is not invertible: for any $a \in \mathbb{Z}_n$, $0 \otimes_n a = a \otimes_n 0 = 0 \neq 1$.

Q: Can this be fixed?

A: Troubleshoot how to get rid of 0.
Consider $\mathbb{Z}_n^* = \mathbb{Z}_n \backslash \{0\} = \{1, 2, ..., n-1\}$ all non-zero elements in $\mathbb{Z}_n^*$. This eliminates 0 as an element, but can 0 arise any other way from the binary operation? It turns out the answer depends on n. If n is not prime, say $n = 6$, we get **zero divisors**, i.e. elements that yield 0 when multiplied. These are <u>precisely</u> the factors of n. For $n = 6$, $\mathbb{Z}_6^* = \{1, 2, 3, 4, 5\}$ <u>but</u> $2 \otimes_6 3 = 6 \equiv 0 \mod 6$, so 2 and 3 are zero divisors.

Claim: If n is prime, then $(\mathbb{Z}_n^*, \otimes_n, 1)$ is an Abelian group.
Used in cryptography $\rightarrow$ n is taken to be a very large prime number.
As an example, let us look at the multiplication table for $\mathbb{Z}_5^*$ to see the inverse of various elements: $\mathbb{Z}_5^* = \mathbb{Z}_5 \backslash \{0\} = \{0, 1, 2, 3, 4\} \backslash \{0\} = \{1, 2, 3, 4\}$

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$1^{-1} = 1 \quad 1 \otimes_5 1 = 1$
$2^{-1} = 3 \quad 2 \otimes_5 3 = 6 \equiv 1 \mod 5$
$3^{-1} = 2 \quad 3 \otimes_5 2 = 6 \equiv 1 \mod 5$
$4^{-1} = 4 \quad 4 \otimes_5 4 = 16 \equiv 1 \mod 5$

The fact that $(\mathbb{Z}_n^*, \otimes_n, 1)$ is Abelian follows from the commutativity of multiplication on $\mathbb{Z}$.

6. Let $(A, *, e)$ be any group, and let $a \in A$.
Consider $A' = \{a^m \mid m \in \mathbb{Z}\}$ all powers of a. It turns out $(A', *, e)$ is a group called the <u>cyclic group</u> determined by a. $(A', *, e)$ is Abelian <u>regardless</u> of whether the original group was Abelian or not because of the theorem we proved on powers of a: $\forall m, n \in \mathbb{Z}$ $a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m$.
Cyclic groups come in two flavours: finite (A' is a finite set) and infinite (A' is an infinite set).
For example, let $(A, *, e) = (\mathbb{Q}^*, \times, 1)$
If $a = -1$ $\quad A' = \{(-1)^m \mid m \in \mathbb{Z}\} = \{-1, 1\}$ is finite.
If $a = 2$ $\quad A' = \{2^m \mid m \in \mathbb{Z}\} = \{1, 2, \frac{1}{2}, 4, \frac{1}{4}, ...\}$ is infinite.