QF Group Theory CC2022
By
Zaiku Group

Lecture 07

Delivered by Bambordé Baldé

Friday, 20/05/2022

Binary Operation on a Set

Definition 1.0

Let S be a nonempty set. Informally, a binary operation $*$ on S is a rule that takes any two elements $a, b \in S$ to generate another element $a * b \in S$.

- More formally, a binary operation $*$ on S is a map $* : S \times S \longrightarrow S$.
- Hence, given $(a, b) \in S \times S$, $a * b$ is just an abbreviation for $*((a, b))$ i.e. $a * b$ is an abuse of notation!
- It is possible to equip a set S with more than one binary operation! For example, the algebraic structures of rings and fields are obtained that way.

Definition 1.1

Let S be a nonempty set. A binary operation $*$ on S is said to be commutative (or abelian) if $a * b = b * a$ for any pairs $a, b \in S$. Otherwise, whenever we have $a * b \neq b * a$ for some $a, b \in S$, we say that $*$ is a noncommutative (or non-abelian) binary operation on S.

Binary Operation Examples (Part A)

Example 1

Let S be the set of natural numbers $\mathbb{N}$ and let the operation $*$ be the ordinary addition of natural numbers $+$.

- $+$ defines a binary operation on $\mathbb{N}$ right?

Example 2

Let us consider $S = \{a \in \mathbb{N} \mid a \text{ is odd } \}$ and $*$ be the ordinary multiplication of natural numbers $\times$.

- Does $\times$ define a binary operation on S?

Example 3

Let consider again $S = \{a \in \mathbb{N} \mid a \text{ is odd } \}$ and let now $*$ be the ordinary addition of natural numbers $+$.

- Does $+$ also define a binary operation on S?

Binary Operation Examples (Part B)

Example 1

Let A be a non-empty set and let $S = \{f : A \longrightarrow A \mid f \text{ is a bijection } \}$. Now suppose that $*$ is the composition $\circ$ of maps in S.

- Is $\circ$ a binary operation on S? If yes, is it abelian or non-abelian?

Example 2

Let S be the set $M_n(\mathbb{C})$ of $n \times n$ matrices with complex entries and let the operation $*$ be the ordinary matrix multiplication.

- Is $*$ also a binary operation on $M_n(\mathbb{C})$? Is it abelian or non-abelian?

Example 3

Let S be the set denote $GL(n, \mathbb{C})$ of invertible $n \times n$ matrices with complex entries and let the operation $*$ be still the ordinary matrix multiplication.

- Is $*$ also a binary operation on $GL(n, \mathbb{C})$? Is it abelian or non-abelian?
- What if $*$ is now the ordinary addition of matrices?

Semigroup Structure

Definition 1.2

A semigroup is a pair $(S, *)$ where S is a nonempty set and $*$ is a binary operation on S such that $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$.

- The condition $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$ is called the 'associativity law' and we say that the operation $*$ is associative.
- Whenever the operation $*$ is understood from the context and fixed, we just say S is a semigroup and we omit writing the pair $(S, *)$.
- A semigroup $(S, *)$ is said to be abelian or non-abelian if $*$ is a abelian or non-abelian binary operation respectively.

Definition 1.3

Let $(S, *)$ be a semigroup and $S' \subseteq S$. Then S' is said to be subsemigroup of $(S, *)$ if $(S', *)$ is also a semigroup.

- Obviously, $(S, *)$ is trivially a subsemigroup of itself!

Semigroup Examples

Example 1

Let A be a non-empty set and let $S = \{f : A \longrightarrow A \mid f \text{ is a bijection } \}$. Now suppose that $*$ is the composition $\circ$ of maps in S.

- Is S a semigroup under $\circ$? If yes, is it abelian or non-abelian?

Example 2

Let S be the set $M_n(\mathbb{C})$ of $n \times n$ matrices with complex entries and let the operation $*$ be the ordinary matrix multiplication.

- Is $M_n(\mathbb{C})$ a semigroup under matrix multiplication? Is it abelian or non-abelian? What about under matrix addition?

Example 3

Let S be the set denote $GL(n, \mathbb{C})$ of invertible $n \times n$ matrices with complex entries and let the operation $*$ be still the ordinary matrix multiplication.

- Is $GL(n, \mathbb{C})$ a semigroup under matrix multiplication?

Semigroups Structure Challenge

1. Let $(S, *)$ be a semigroup and let $S' = \{a \in S \mid a * x = x * a \text{ for all } x \in S\}$.Is it true that $(S', *)$ is a subsemigroup of $(S, *)$?
2. Let $(S_1, *_1)$ and $(S_2, *_2)$ be two semigroups. Construct a semigroup structure on the Cartesian product $S_1 \times S_2$ using the respective semigroup structure. Can you generalise your construction to $(S_1, *_1), (S_2, *_2), \ldots, (S_n, *_n)$?
3. Assuming that $(S_1, *_1)$ is abelian and $(S_2, *_2)$ is non-abelian, is your constructed semigroup structure on $S_1 \times S_2$ abelian or non-abelian?
4. Identify at least a nontrivial subsemigroup structure for the constructed semigroup structure on $S_1 \times S_2$ above.
5. Let $\mathbb{Z}_2 = \{0, 1\}$, $\mathbb{Z}_3 = \{0, 1, 2\}$ and $\mathbb{Z}_4 = \{0, 1, 3\}$. Identify at least a semigroup structure for $\mathbb{Z}_2$, $\mathbb{Z}_3$ and $\mathbb{Z}_4$.
6. Identify at least a subsemigroup structure (if any) from the identified semigroup structures on $\mathbb{Z}_2$, $\mathbb{Z}_3$ and $\mathbb{Z}_4$ above.

Lecture 01 Content Ends Here

Content for Lecture 02 Starts in the Next Slide!

Semigroup Recap

Semigroup definition recap

A semigroup is a pair $(S, *)$ where S is a nonempty set and $*$ is a binary operation on S such that $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$.

- Now that we have the basic algebraic structure of semigroup, our goal is to start exploring:

1. Interesting properties that the algebraic structure gives us e.g. identify some interesting behaviours that certain elements have.
2. Explore structure preserving maps between semigroups (homomorphisms).

Semigroup Idempotent Elements

Definition 1.0

Given a semigroup $(S, *)$ and $a \in S$, we define $a^2 = a * a$.

- Can you generalise the above to the power of an arbitrary $n \in \mathbb{N}$?

Definition 1.1

Let $(S, *)$ be a semigroup. An element $a \in S$ is idempotent if $a^2 = a$.

- We denote by $Idem(S)$ the set of all idempotent elements in S i.e $Idem(S) = \{a \in S \mid a^2 = a\}$. Obviously, we may have $Idem(S) = \emptyset$.
- Interestingly, we may also have $Idem(S) = S$ (aka a band).

Homework Challenge 1

Let $(S, *)$ be a semigroup. You're encouraged to try answer the following:

1. Is it true that $Idem(S)$ is a subsemigroup of $(S, *)$?
2. Is it true that if $a \in Idem(S)$ then $a^n = a$ for all $n \in \mathbb{N}$?

Idempotent Elements (Boring Examples)

- Let $(S, *) = (\mathbb{Z}, \times)$ where $\times$ is the ordinary multiplication in $\mathbb{Z}$. Then 1 and 0 are the only idempotent elements i.e. $Idem(\mathbb{Z}) = \{0, 1\}$?
- Now if $(S, *) = (\mathbb{Z}, +)$ where $+$ is the ordinary addition in $\mathbb{Z}$ then $Idem(\mathbb{Z}) = \{0\}$?
- Let now $(S, *) = (\mathbb{R}, \times)$ where $\times$ is the ordinary multiplication in $\mathbb{R}$. Then $Idem(\mathbb{R}) = \{0, 1\}$?
- If $(S, *) = (\mathbb{R}, +)$. Then again $Idem(\mathbb{R}) = \{0\}$?
- Similarly, if now $(S, *) = (\mathbb{C}, \times)$ where $\times$ is the ordinary multiplication in $\mathbb{C}$. Then $Idem(\mathbb{C}) = \{0, 1\}$. Obviously if $(S, *) = (\mathbb{C}, +)$, then $Idem(\mathbb{C}) = \{0\}$.

Question: Are there examples of semigroup structure where $Idem(S)$ is not trivial/boring like the examples above?

Idempotent Elements (Matrix Examples)

- Consider the set $M_2(\mathbb{R})$ of two by two matrices over the reals, then:
  1. Trivially,
  $$0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$
  and
  $$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
  are idempotent in respect to matrix multiplication!
  2. Nontrivial examples are
  $$0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$
  and
  $$0 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Side note: The eigenvalues of idempotent matrices are either 0 or 1.

Idempotent Elements (mod 3 Example)

- Consider $\mathbb{Z}_3 = \{0, 1, 2\}$ with the binary operation $+$ defined by the following table:
  Clearly $Idem(\mathbb{Z}_3) = \{0\}$ right?
- Let us now define the binary operation $\times$ on $\mathbb{Z}_3$ via the following table:
  Clearly $Idem(\mathbb{Z}_3) = \{0, 1\}$ right?

Idempotent Elements (mod 4 Example)

- Consider now $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with the binary operation $+$ defined by the following table:
  Clearly $Idem(\mathbb{Z}_4) = \{0\}$ right?
- Let us now define the binary operation $\times$ on $\mathbb{Z}_4$ via the following table:
  Clearly $Idem(\mathbb{Z}_4) = \{0, 1\}$ right?
- Unfortunately, $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ is boring too when it comes $Idem(\mathbb{Z}_5)$ because: $Idem(\mathbb{Z}_5) = \{0\}$ with the respect to $+$ and $Idem(\mathbb{Z}_5) = \{0, 1\}$ with the respect $\times$!

Idempotent Elements (mod 6 Example)

- Consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ in respect to mod 6 multiplication table defined below:
- Clearly we now have a non-boring example because $Idem(\mathbb{Z}_6) = \{0, 1, 3, 4\}$?!!
- Interestingly, $Idem(\mathbb{Z}_7)$, $Idem(\mathbb{Z}_8)$ and $Idem(\mathbb{Z}_9)$ are also trivial/boring!

Question: What makes mod 6 case above special? Are there other mod n examples for $n > 6$?

Hint: It has to do with prime numbers! Can you guess why prime numbers play a role in this?

Idempotent Elements (mod $n > 6$ Examples)

- For $\mathbb{Z}_{10} = \{0,1,2,3,4,5,6,7,8,9\}$ under mod 10 multiplication we have $Idem(\mathbb{Z}_{10}) = \{0,1,5,6\}$?
- For $\mathbb{Z}_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$ under mod 12 multiplication we have $Idem(\mathbb{Z}_{12}) = \{0,1,4,6,9\}$?
- For $\mathbb{Z}_{14} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13\}$ under mod 14 multiplication we have $Idem(\mathbb{Z}_{14}) = \{0,1,7,8\}$?
- For $\mathbb{Z}_{15} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14\}$ under mod 15 multiplication we have $Idem(\mathbb{Z}_{15}) = \{0,1,6,10\}$?

Question: What do the above examples and $\mathbb{Z}_6$ have in common regarding prime numbers?
Extra hint: They break an interesting property of prime numbers!!
By the way, $\mathbb{Z}_{18}$, $\mathbb{Z}_{20}$, $\mathbb{Z}_{21}$, $\mathbb{Z}_{22}$, $\mathbb{Z}_{24}$, $\mathbb{Z}_{26}$, and $\mathbb{Z}_{28}$ are also part of the gang!

-

Semigroup Homomorphisms

Definition 1.2

Let $(S_1, *_1)$ and $(S_2, *_2)$ be semigroups. A map $f : S_1 \longrightarrow S_2$ is a homomorphism if $f(a *_1 b) = f(a) *_2 f(b)$ for all $a, b \in S_1$.

- Let $(S_1, *_1) = (\mathbb{R}, +)$ and $(S_2, *_2) = (\mathbb{R}^+, \times)$. Now consider the map $f : \mathbb{R} \longrightarrow \mathbb{R}^+$ defined as $f(x) = e^x$ for all $x \in \mathbb{R}$. Is this map a homomorphism?
- Let $M_2(\mathbb{R})$ the semigroup of 2 by 2 real matrices under ordinary matrix multiplication. Recall that given any matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$\in M_2(\mathbb{R})$, the determinant $det(A) : M_2(\mathbb{R}) \longrightarrow \mathbb{R}$ is defined as $det(A) = ad - bc$. Is this a homomorphism to the semigroup $(\mathbb{R}, +)$ or the semigroup $(\mathbb{R}, \times)$?

FHE Side note

Side notes:

- Classical Homomorphic Encryption (HE), homomorphism is the underpinning mathematical notion of HE.
- The early HE schemes such as the ones proposed by Rivest and ElGammal were built on groups and so use group homomorphisms.
- Modern Fully Homomorphic Encryption (FHE) schemes are built on rings and fields.
- Can we run quantum computations homomorphically? This question naturally leads to Quantum Homomorphic Encryption (QHF)!

Homomorphism Challenge

Homework Challenge 2

Let $(S_1, *_1)$ and $(S_2, *_2)$ be semigroups. Now suppose that $f : S_1 \longrightarrow S_2$ is a semigroup homomorphism.

1. Is it true that if $a \in Idem(S_1)$ then $f(a) \in Idem(S_2)$?
2. Is it true that $Im(f) = \{f(a) \mid a \in S_1\}$ is a subsemigroup of $(S_2, *_2)$?

Homework Challenge 3

Let $(S_1, *_1)$, $(S_2, *_2)$ and $(S_3, *_3)$ be semigroups. Now suppose that the maps $f : S_1 \longrightarrow S_2$ and $g : S_2 \longrightarrow S_3$ are homomorphisms.

1. Is the composition map $g \circ f : S_1 \longrightarrow S_3$ a homomorphism?
2. Suppose that f is invertible. Is $f^{-1} : S_2 \longrightarrow S_1$ also a homomorphism?

Homomorphism Challenge Extra

Homework Challenge 4

Consider the sets $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_6$,$\mathbb{Z}_{10}$, $\mathbb{Z}_{11}$,$\mathbb{Z}_{12}$, $\mathbb{Z}_{14}$ and $\mathbb{Z}_{15}$. Try construct homomorphisms between these sets under both mod n addition and mod n multiplication.

Semigroup Isomorphisms

Definition 1.3

Let $(S_1, *_1)$ and $(S_2, *_2)$ be semigroups. A homomorphism $f : S_1 \longrightarrow S_2$ is called an isomorphisms if it's bijective.

- We write $S_1 \simeq S_2$ and say the two semigroups are isomorphic if there exists an isomorphism between the two.
- Isomorphisms are the structure preserving maps of semigroups i.e. two isomorphic semigroups are from an algebraic point of view indistinguishable.

Homework Challenge 5

Let $(S_1, *_1)$, $(S_2, *_2)$ and $(S_3, *_3)$ be semigroups. Now suppose that the maps $f : S_1 \longrightarrow S_2$ and $g : S_2 \longrightarrow S_3$ are isomorphisms.

- Is the composition map $g \circ f : S_1 \longrightarrow S_3$ an isomorphism i.e. does $S_1 \simeq S_2$ and $S_2 \simeq S_3$ imply $S_1 \simeq S_3$?

Semigroup Idempotent Challenges

Challenge 1

You're encouraged to take on the following challenges:

1. Let $(S, *)$ be a semigroup. Prove that if $E(S) \neq \emptyset$, then $E(S)$ is a subsemigroup of $(S, *)$.
2. Identify $E(S)$ (if any) for these cases: $(S, *) = (\mathbb{N}, \times)$, $(S, *) = (\mathbb{N}, +)$, $(S, *) = (\mathbb{Z}, \times)$, $(S, *) = (\mathbb{Z}, +)$, $(S, *) = (\mathbb{Q}, \times)$, $(S, *) = (\mathbb{Q}, +)$, $(S, *) = (\mathbb{R}, \times)$, $(S, *) = (\mathbb{R}, +)$, $(S, *) = (\mathbb{C}, \times)$.

Challenge 2

You're encouraged to take on the following challenges:

1. Identify $E(S)$ (if any) for the following cases using the identified or constructed semigroup structures from the previous section: $\mathbb{Z}_2 = \{0, 1\}$, $\mathbb{Z}_3 = \{0, 1, 2\}$ and $\mathbb{Z}_4 = \{0, 1, 3\}$, $P[3]_{\mathbb{Z}}$, $P[3]_{\mathbb{Z}_2}$, $P[3]_{\mathbb{Z}_3}$.

Lecture 03 Starts Here

The Zero Element

Definition 1.0

Let $(S, *)$ be a semigroup. An element $\boldsymbol{z} \in S$ is called a 'zero element' or 'absorbing element' if $\boldsymbol{z} * a = a * \boldsymbol{z} = \boldsymbol{z}$ for all $a \in S$.

- Obviously it follows that $\boldsymbol{z} * \boldsymbol{z} = \boldsymbol{z}$! Hence, $\boldsymbol{z}$ is idempotent right?!

Homework Challenge 1

Let $(S, *)$ be a semigroup with a zero element $\boldsymbol{z} \in S$.

- Is it true that $\boldsymbol{z}$ is unique i.e. if $\boldsymbol{z}_1$ and $\boldsymbol{z}_2$ are two zero elements then $\boldsymbol{z}_1 = \boldsymbol{z}_2$?

Homework Challenge 2

Let $(S_1, *_1)$ and $(S_2, *_2)$ be semigroups. Now suppose that a map $f : S_1 \longrightarrow S_2$ is a homomorphism and there is a zero element $\boldsymbol{z} \in S_1$.

- Is it true that $f(\boldsymbol{z})$ is a zero element in S_2?

The Zero Element (Examples)

1. If $(S, *) = (\mathbb{R}, \times)$, then the zero element $\boldsymbol{z}$ is the ordinary 0!
2. What if $(S, *) = (\mathbb{R}, +)$? Is the ordinary 0 still a zero element as per our definition?
3. If we now consider the semigroup $M_2(\mathbb{R})$ of 2 by 2 matrices over the reals under matrix multiplication. Then the zero element is of course the zero matrix i.e.
$$\boldsymbol{z} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$
.
4. Consider $M_2(\mathbb{R})$ under the matrix addition. Is the zero matrix
$$\boldsymbol{z} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$
still a zero element?
Obviously the above is true for $M_n(\mathbb{R})$ for any $n \geq 1$.

The Zero Element (mod 3 Example A)

- Clearly there is no zero element right?

The Zero Element (mod 3 Example B)

- There is now a zero element right?!

The Zero Element (Remarks)

1. Symbols only have a formal meaning based on the rules of the game that we are considering! For example, the behaviour of the symbol 0 depends on the binary operation $*$ under consideration. Hence, the interpretation/meaning that we give to 0 depends on the semigroup structure.
2.

Nilpotent Elements

Definition 1.1

Let $(S, *)$ be a semigroup with a zero element $\boldsymbol{z} \in S$. An element $a \in S$ is called nilpotent if there exists a natural number $n \in \mathbb{N}$ such that $a^n = \boldsymbol{z}$.

- Obviously the zero element $\boldsymbol{z}$ itself is nilpotent right?
- We'll denote by $Nilp(S)$ the set of all nilpotent elements in S i.e $Nilp(S) = \{a \in S$ such that there exists some $n \in \mathbb{N} \mid a^n = \boldsymbol{z}\}$.
- Obviously, we may have $Nilp(S) = \{\boldsymbol{z}\}$ or even $Nilp(S) = \emptyset$!
- Is it true that if $Nilp(S) \neq \emptyset$ then $Nilp(S)$ is a subsemigroup?

Homework Challenge 3

Let $(S_1, *_1)$ and $(S_2, *_2)$ be semigroups with zero elements. Now suppose that $f : S_1 \longrightarrow S_2$ is a homomorphism.

- Is it true that if $a \in S_1$ is nilpotent then $f(a)$ is nilpontent in S_2?

Nilpotent Elements (Boring Examples)

- Let $(S, *) = (\mathbb{Z}, \times)$ where $\times$ is the ordinary multiplication in $\mathbb{Z}$. Then 0 is the only nilpotent element i.e. $Nilp(\mathbb{Z}) = \{0\}$?
- Now if $(S, *) = (\mathbb{Z}, +)$ where $+$ is the ordinary addition in $\mathbb{Z}$ then $Nilp(\mathbb{Z}) = \emptyset$?
- Let now $(S, *) = (\mathbb{R}, \times)$ where $\times$ is the ordinary multiplication in $\mathbb{R}$. Then $Nilp(\mathbb{R}) = \{0\}$?
- If $(S, *) = (\mathbb{R}, +)$. Then again $Nilp(\mathbb{R}) = \emptyset$?
- Similarly, if now $(S, *) = (\mathbb{C}, \times)$ where $\times$ is the ordinary multiplication in $\mathbb{C}$. Then $Nilp(\mathbb{C}) = \{0\}$. Obviously if $(S, *) = (\mathbb{C}, +)$, then $Nilp(\mathbb{C}) = \emptyset$.
- Can you notice anything interesting when the binary operation $*$ is the notion of 'addition'?

Question: Are there examples of semigroup structure where $Nilp(S)$ is not trivial/boring like the examples above?

Nilpotent Elements (Matrix Examples)

- Consider the set $M_2(\mathbb{R})$ of two by two matrices over the reals, then:
  1. Trivially,
  $$0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$
  is nilpotent in respect to matrix multiplication!
  2. Nontrivial examples are
  $$0 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$
  ,
  $$0 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$
  ,
  $$0 = \begin{bmatrix} 0 & 0 \\ -3 & 0 \end{bmatrix}$$
  and
  $$0 = \begin{bmatrix} 0 & 7 \\ 0 & 0 \end{bmatrix}$$

Question: Do you notice anything about the trace and determinant?

Nipotent Elements (mod 3 Example A)

- Consider $\mathbb{Z}_3 = \{0, 1, 2\}$ with the binary operation $+$ defined by the following table:
  $Nilp(\mathbb{Z}_3) = \emptyset$ right?

Nilpotent Elements (mod 3 Example B)

- Consider $\mathbb{Z}_3 = \{0, 1, 2\}$ again but now with $\times$ defined by the following table:
  $Nilp(\mathbb{Z}_3) = \{0\}$ right?

Nilpotent Elements (mod 4 Example A)

- Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with the binary operation $+$ defined by the following table:
  $Nilp(\mathbb{Z}_4) = \emptyset$ right?

Nilpotent Elements (mod 4 Example B)

- Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ again but now with $\times$ defined by the following table:
- We finally have a nontrivial example because $Nilp(\mathbb{Z}_4) = \{0, 2\}$ right?!

Question 1: Are there more nontrivial examples for $n > 4$?
Spoiler alert: Unfortunately $\mathbb{Z}_5$ is boring too i.e. $Nilp(\mathbb{Z}_5) = \{0\}$!
Question 2: What about $\mathbb{Z}_6$? Is it boring too i.e. $Nilp(\mathbb{Z}_6) = \{0\}$?

Nilpotent Elements (mod 6 Example)

- Consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ with $\times$ defined by the following table:
- Unfortunately $Nilp(\mathbb{Z}_6) = \{0\}$ right?!

Spoiler alert: Unfortunately $\mathbb{Z}_7$ is boring too i.e. $Nilp(\mathbb{Z}_7) = \{0\}$!
Question: Are there really more nontrivial examples for $n > 4$?

Nilpotent Elements (mod 8 Example)

- Consider $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ with $\times$ defined by the following table:
- We have another nontrivial example because $Nilp(\mathbb{Z}_8) = \{0, 4\}$ right?!

Spoiler alert: $\mathbb{Z}_9$ is nontrivial too because $Nilp(\mathbb{Z}_9) = \{0, 3, 6\}$!
Question: Can you figure out why $\mathbb{Z}_4$, $\mathbb{Z}_8$ and $\mathbb{Z}_9$ are special?

Nilpotent Elements (mod $5, 7, 9$ Tables)

Nilpotent Elements (mod $n > 9$ Multiplication)

- For $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $Nilp(\mathbb{Z}_{10}) = \{0\}$.
- For $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $Nilp(\mathbb{Z}_{11}) = \{0\}$.
- For $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, $Nilp(\mathbb{Z}_{12}) = \{0, 6\}$.
- For $\mathbb{Z}_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, $Nilp(\mathbb{Z}_{13}) = \{0\}$.
- For $\mathbb{Z}_{14} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$, $Nilp(\mathbb{Z}_{14}) = \{0\}$.
- For $\mathbb{Z}_{15} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$, $Nilp(\mathbb{Z}_{15}) = \{0\}$.
- For $\mathbb{Z}_{16} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$, $Nilp(\mathbb{Z}_{16}) = \{0, 4, 8, 12\}$.
- For $\mathbb{Z}_{17} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$, $Nilp(\mathbb{Z}_{17}) = \{0\}$.
- For $\mathbb{Z}_{18} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17\}$, $Nilp(\mathbb{Z}_{18}) = \{0, 6\}$.

Question: Can you now figure out what's going on?

By the way, $\mathbb{Z}_{20}$, $\mathbb{Z}_{24}$, $\mathbb{Z}_{25}$, $\mathbb{Z}_{27}$, $\mathbb{Z}_{28}$, $\mathbb{Z}_{32}$, and $\mathbb{Z}_{36}$ are also part of the nontrivial gang!

Nilpotent Elements (mod $n > 9$ Table A)

Nilpotent Elements (mod $n > 9$ Table B)

Zero Element Motivation

- What if a semigroup $(S, *)$ does not have a 'zero element'? Can we do anything about it?

Adding Zero Element to a Semigroup

Definition 1.2

Let $(S, *)$ be a semigroup without a zero element. We define the set $S^0 = S \cup \{\mathbf{0}\}$. We can construct a binary operation $\hat{*}$ on S^0 as follows:

1. $a \hat{*} b = a * b$ for all $a, b \in S$.
2. $x \hat{*} \mathbf{0} = \mathbf{0} \hat{*} x = \mathbf{0}$ for all $x \in S^0$.

- With $\hat{*}$ define above, $(S^0, \hat{*})$ forms a semigroup structure right?
- In particular, $\mathbf{0}$ is nilpotent right?

Homework Challenge 4

Consider the semigroups $(\mathbb{Z}_3, +)$, $(\mathbb{Z}_4, +)$, $(\mathbb{Z}_5, +)$. Try construct the tables for $(\mathbb{Z}_3^0, \hat{+})$, $(\mathbb{Z}_4^0, \hat{+})$ and $(\mathbb{Z}_5^0, \hat{+})$!

Nilpotent Semigroup

Definition 1.3

Let $(S, *)$ be a semigroup with a zero element $\boldsymbol{z}$. We say $(S, *)$ is a nilpotent semigroup if all the elements of S are nilpotent i.e. for all $a \in S$ there exists some $n \in \mathbb{N}$ such that $a^n = \boldsymbol{z}$.

- Can you find a nontrivial example of nilpotent semigroup?

Hint: Consider starting your hunt with matrices!

Lecture 04 starts here

Inverse Semigroup

Definition 1.0

Let $(S, *)$ be a semigroup and $x \in S$. Then x is said to be invertible if there exists some $\tilde{x} \in S$ such that $x * \tilde{x} * x = x$ and $\tilde{x} * x * \tilde{x} = \tilde{x}$.

- The element $\tilde{x}$ is as you can guess is called an inverse for x!

Definition 1.1

A semigroup $(S, *)$ is called 'inverse semigroup' if for every $x \in S$ there is a unique $\tilde{x} \in S$ such that $x * \tilde{x} * x = x$ and $\tilde{x} * x * \tilde{x} = \tilde{x}$.

- When dealing with inverse semigroups, the notation x^{-1} is used to denote the inverse of $x \in S$ instead of $\tilde{x}$!

Homework Challenge 1

Let $(S_1, *_1)$ and $(S_2, *_2)$ be inverse semigroups. Now suppose that a map $f : S_1 \longrightarrow S_2$ is a homomorphism.

- Is it true that $f(x^{-1}) \in S_2$ is the inverse of $f(x) \in S_2$ for all $x \in S_1$?

Semigroup Identity Element

Definition 1.2

Let $(S, *)$ be a semigroup. An element $\boldsymbol{e} \in S$ is called:

1. A left identity if $\boldsymbol{e} * x = x$ for all $x \in S$.
2. A right identity if $x * \boldsymbol{e} = x$ for all $x \in S$.
3. A two sided identity if $\boldsymbol{e} * x = x * \boldsymbol{e} = x$ for all $x \in S$.

- For our purposes, we are only interested in semigroups with two sided identity elements!

Spoiler alert: A semigroup with a two sided identity is called a monoid!

Homework Challenge 2

Let $(S, *)$ be a semigroup with a two sided identity element $\boldsymbol{e} \in S$.

- Is it true that $\boldsymbol{e}$ is unique i.e. if $\boldsymbol{e}_1$ and $\boldsymbol{e}_2$ are two sided elements then $\boldsymbol{e}_1 = \boldsymbol{e}_2$?

Homework Challenge 3

Let $(S_1, *_1)$ and $(S_2, *_2)$ be semigroups with two sided identity elements $\boldsymbol{e}_1$ and $\boldsymbol{e}_2$ respectively. Now suppose that a map $f : S_1 \longrightarrow S_2$ is a homomorphism.

- Is it true that $f(\boldsymbol{e}_1) = \boldsymbol{e}_2$?

Identity Element Examples

- Let $(S, *) = (\mathbb{R}, \times)$. Then 1 is an identity element right? Is it two sided identity?
- Let $\mathbb{R}^*$ denote the set of nonzero reals i.e $\mathbb{R}^*$ is the set of reals excluding zero. We can construct a binary operation $*$ on $\mathbb{R}^*$ as $a * b = |a|b$ for all $a, b \in \mathbb{R}^*$ where $|.|$ denotes the absolute value of reals.
  1. $(\mathbb{R}^*, *)$ forms a semigroup right?
  2. It's clear that 1 is a left identity? What about -1?
  3. Does $(\mathbb{R}^*, *)$ contain a right identity?
- Is $(\mathbb{R}^*, *)$ as constructed above an abelian semigroup?

Question: What if a semigroup doesn't have any identity? Can we invent one?!

Adding an Identity to a Semigroup

Definition 1.3

Let $(S, *)$ be a semigroup without an identity. We first define the set $S^1 = S \cup \{\mathbf{1}\}$. Then we can construct a binary operation $\hat{*}$ on S^1 as follows:

1. $a \hat{*} b = a * b$ for all $a, b \in S$.
2. $x \hat{*} \mathbf{1} = \mathbf{1} \hat{*} x = x$ for all $x \in S^1$.

- With $\hat{*}$ define above, $(S^1, \hat{*})$ forms a semigroup structure with a two-sided identity $\mathbf{1}$.

Monoid Structure

Definition 1.4

A monoid is a triple $(M, *, \boldsymbol{e})$ such that $(M, *)$ is a semigroup and $\boldsymbol{e} \in M$ is a two-sided identity in the semigroup $(M, *)$.

Question: Is $\boldsymbol{e}$ in a monoid unique i.e. if $\boldsymbol{e}$ and $\tilde{\boldsymbol{e}}$ are two-sided identities then $\boldsymbol{e} = \tilde{\boldsymbol{e}}$?

Definition 1.5

Let $(M, *, \boldsymbol{e})$ be a monoid and $N \subseteq M$. If $(N, *, \boldsymbol{e}_N)$ is a monoid then we call it a submonoid.

- Is it true that we must have $\boldsymbol{e}_N = \boldsymbol{e}$?

Homework Challenge 4

Let $(M_1, *_1, \boldsymbol{e}_1)$ and $(M_2, *_2, \boldsymbol{e}_2)$ be monoids. Now let $\phi : M_1 \longrightarrow M_2$ be a homomorphism.

- Is it true that we must have $\phi(\boldsymbol{e}_1) = \boldsymbol{e}_2$?

Monoid Homomorphism Kernel

Definition 1.5

Let $(M_1, *_1, \boldsymbol{e}_1)$ and $(M_2, *_2, \boldsymbol{e}_2)$ be monoids. Now let $\phi : M_1 \longrightarrow M_2$ be a homomorphism. The set $ker(\phi) = \{x \in M_1 \mid \phi(x) = \boldsymbol{e}_2\}$ is called the kernel of the homomorphism ϕ.

- Obviously $ker(\phi)$ cannot be empty right?

Homework Challenge 5

Let $(M_1, *_1, \boldsymbol{e}_1)$ and $(M_2, *_2, \boldsymbol{e}_2)$ be monoids. Now let $\phi : M_1 \longrightarrow M_2$ be a homomorphism.

1. Is it true that $ker(\phi)$ is a submonoid of $(M_1, *_1, \boldsymbol{e}_1)$?
2. Is it true that ϕ is an isomorphism iff $ker(\phi) = \{\boldsymbol{e}_1\}$?

Monoid Inverse Elements

Definition 1.0

Let $(M, *, \boldsymbol{e})$ be a monoid and $x \in M$. An element $x^{-1} \in M$ is called:

1. A left inverse of x if $x^{-1} * x = \boldsymbol{e}$.
2. A right inverse if $x * x^{-1} = \boldsymbol{e}$.
3. A two-sided inverse (or group inverse) if $x^{-1} * x = x * x^{-1} = \boldsymbol{e}$.

- Obviously, x^{-1} doesn't necessarily exist for all $x \in M$.

Simple Concrete Examples:

1. Consider the monoid $(\mathbb{R}, \times, 1)$. Then any nonzero element $a \in \mathbb{R}$ has a group inverse $a^{-1} = \frac{1}{a}$ right?
2. Consider now the monoid $(\mathbb{R}, +, 0)$. Then any element $a \in \mathbb{R}$ has a group inverse $a^{-1} = -a$ right?

Inverse Element Examples

Challenge 1

Let $(M, *, \boldsymbol{e})$ be a monoid and $x \in M$. Now suppose that $x^{-1} \in M$ is a group inverse. Is is true that x^{-1} is unique i.e. if x_1^{-1} and x_2^{-1} are two group inverses of x then $x_1^{-1} = x_2^{-1}$?

- Consider the monoid $(\mathbb{R}, \times, 1)$. Then any nonzero element $a \in \mathbb{R}$ has a group inverse $a^{-1} = \frac{1}{a}$ right?
- Consider now the monoid $(\mathbb{R}, +, 0)$. Then any element $a \in \mathbb{R}$ has a group inverse $a^{-1} = -a$ right?
- Let $\mathbb{R}^*$ denote the set of nonzero reals i.e $\mathbb{R}^*$ is the set of reals excluding zero. We can construct a binary operation $*$ on $\mathbb{R}^*$ as $a * b = |a|b$ for all $a, b \in \mathbb{R}^*$ where $|.|$ denotes the absolute value of reals.
    1. Does $(\mathbb{R}^*, *, 1)$ form a monoid? What about $(\mathbb{R}^*, *, -1)$?

Question: What if a semigroup doesn't have any identity? Can we invent one?!

Fundamental Theorem of Algebra (FTA)

$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ with $a_i \in \mathbb{C}$ and $a_n \neq 0$ has at least one root in $\mathbb{C}$.

- Equivalently every polynomial of degree n with real or complex coefficients has exactly n complex roots, counting multiplicity.
- Interestingly, most versions of the FTA proof including the original rely on methods from other branches of mathematics such as Analysis! This led to a healthy debate over the years whether it should be called 'Fundamental Theorem of Algebra'! There are now of course other more algebraic methods that prove FTA, for example Galois theory.
- When we can find the solutions for $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ with rational coefficients using only rational numbers and the operations of addition, subtraction, division, multiplication and nth roots, we say that p(x) is solvable by radicals.

The Genesis of Group Theory (B)

- Consider the second degree polynomial $p(x) = a_2x^2 + a_1x + a_0$ with $a_i \in \mathbb{C}$. Then the polynomial equation $p(x) = 0$ can be solved by radicals as we all learned in basic school via the quadratic formula!
- The third degree polynomial equation $p(x) = a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ and the fourth degree polynomial equation $p(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ can also be solved by radicals.

Big Question 1:

Can $p(x) = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ also be solved by radicals? Or even better, can a general polynomial equation $p(x) = a_nx^n + a_{n-}x^{n-1} + \ldots + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ be solved by radicals for any $n \geq 5$?

- Note that the question is whether $p(x) = 0$ can be solved by radicals, not whether $p(x) = 0$ can be solved by other means.

The Genesis of Group Theory (C)

The answer to 'Big Question 1'

The famous Abel–Ruffini theorem (aka Abel's impossibility theorem) shows that not all polynomial of degrees ≥ 5 can be solved by radicals!

- An example of a polynomial equation that cannot be solved by radicals is $x^5 - x - 1 = 0$.
- An example of a polynomial that can be solved by radicals is $x^5 + 15x + 12 = 0$.

Big Question 2

Is there a way to decide whether a polynomial equation $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0$ is solvable by radicals for any $n \geq 5$?

The Genesis of Group Theory (D)

The answer to 'Big Question 2'

Évariste Galois hacked a positive answer in his seminal work that gave birth to a subbranch of abstract algebra now known as 'Galois Theory'!

- In a nutshell, given a polynomial of degree $n \geq 5$, $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$. To find out if the polynomial equation $p(x) = 0$ is solvable by radicals, we do the following:

1. We compute a special group $Gal(p(x))$ for the polynomial aka Galois group of $p(x)$.
2. We check if the Galois group $Gal(p(x))$ is 'solvable' in the group theoretic sense. If $Gal(p(x))$ is solvable then $p(x) = 0$ is solvable by radicals! Otherwise it's not solvable by radicals!

Galois Theory Impact

- Galois theory is nowadays used in many applied topics like Cryptography e.g. Advanced Encryption Standard (AES).
- Sophus Lie took inspiration from Galois Theory and pursued creating a similar theory for differential equations! This led to the creation of what we now know as 'Differential Galois Theory'!
- Differential Galois Theory led to the creation of Lie Groups. In a nutshell, Lie groups are for differential equations what Galois groups are for polynomial equations!

The Group Structure

Definition 1.1

A group is a triple $(G, *, \boldsymbol{e})$ satisfying the following:

1. $(G, *, \boldsymbol{e})$ is a monoid.
2. For every $g \in G$ there exists a group inverse $g^{-1} \in G$ i.e. $g * g^{-1} = g^{-1} * g = \boldsymbol{e}$.

- From now on, we'll just write G to denote an abstract group instead of $(G, *, \boldsymbol{e})$. We'll also abbreviate $g_1 * g_2$ as $g_1 g_2$.
- Given a group G, it's cardinality (number of elements) is called the order of G and it's usually denoted $|G|$.
- When $|G| = p$ for some prime number p, then G is called a $p-$ group.
- A group G is commutative (or abelian) if $g_1 g_2 = g_2 g_1$ for all $g_1, g_2 \in G$. Otherwise, it's called noncommutative (or nonabelian).

Group Examples

Example 1

Let A be a non-empty set and let $G = \{f : A \longrightarrow A \mid f \text{ is a bijection } \}$. Now suppose that $*$ is the composition $\circ$ of maps in G.

- Is G a group under $\circ$? If yes, is it abelian or non-abelian?

Example 2

Let G be the set $M_n(\mathbb{C})$ of $n \times n$ matrices with complex entries and let the operation $*$ be the ordinary matrix multiplication.

- Is $M_n(\mathbb{C})$ a group under matrix multiplication? Is it abelian or non-abelian? What about under matrix addition?

Example 3

Let G be the set $GL(n, \mathbb{C})$ of invertible $n \times n$ matrices with complex entries and let the operation $*$ be still the ordinary matrix multiplication.

- Is $GL(n, \mathbb{C})$ a group under matrix multiplication?

Group Element Exponentiation

Definition 1.2

Let G be a group and $g \in G$. Then for $k \in \mathbb{Z}$, we define the following:

1. $g^0 = \boldsymbol{e}$.
2. $g^k = gg \dots gg$ for $k > 0$.
3. $g^{-k} = g^{-1}g^{-1} \dots g^{-1}g^{-1}$ for $k < 0$. $k-$ times

- The notion of exponentiation above will lead us to the important notion of a 'cyclic group' that we'll define in the next lecture!
- Cyclic groups are very important in applied topics such as Cryptography e.g. the Diffie-Hellman Key Exchange Protocol.

Challenge 2

Let G be a group and $g \in G$. Then for $k_1, k_2 \in \mathbb{Z}$, prove the following :

1. $g^{k_1}g^{k_2} = g^{k_1+k_2}$ for all $g \in G$.
2. $(g^{k_1})^{k_2} = g^{k_1 k_2}$ for all $g \in G$.

Lecture 06 Starts

Group Exponentiation Recap

Definition 1.0

Let G be a group, $g \in G$ and $k \in \mathbb{Z}$. We can now make the following definitions:

1. For $k = 0$, we define $g^0 = \boldsymbol{e}$.
2. For $k > 0$, we define $g^k = gg \ldots gg$ i.e. we apply the binary operation on g $k-$ times.
3. For $k < 0$, we define $g^k = (g^{-1})^{|k|} = g^{-1}g^{-1} \ldots g^{-1}g^{-1}$ i.e we apply the binary operation on g^{-1} $|k|-$ times.

Exponentiation Properties

Let G be a group and $g \in G$. Then for $k_1, k_2 \in \mathbb{Z}$, prove the following :

1. $g^{k_1}g^{k_2} = g^{k_1+k_2}$ for all $g \in G$.
2. $(g^{k_1})^{k_2} = g^{k_1k_2}$ for all $g \in G$.

Challenge 1

Let G be a group and $g_1, g_2 \in G$. Is it true that if $g_1 g_2 = g_2 g_1$ then $(g_1 g_2)^k = g_1^k g_2^k$ for all $k \in \mathbb{Z}$?

Additive Notation Comment

Convention

Let G be a an additive group such as $(\mathbb{Z}, +)$ with an identity called zero 0. Then for each $g \in G$ and $k \in \mathbb{Z}$, the exponentiation as g^k as defined previously coincides with notion of 'multiple' written kg:

1. For $k = 0$, $g^k = 0$ coincides with $0g = 0$.
2. For $k > 0$, $g^k = g + g + g + \ldots + g + g$ coincides with kg
3. For $k < 0$, we define $g^k = (-g) + (-g) + \ldots (-g)$ which coincides with $k(-g)$.

- Hence, for additive groups like $(\mathbb{Z}, +)$, we'll write kg instead of g^k!

$|k| - times$

The Order of an Element in a Group

Definition 1.1

Let G be a group and $g \in G$. Then order of g in G is the smallest positive integer $n \in \mathbb{Z}^+$ such that $g^n = \boldsymbol{e}$. We write $|g| = n$ to denote that n is the order of g.

- If there is no such $n \in \mathbb{Z}^+$, by convention we say g has infinite order and we write $|g| = \infty$.
- The group identity $\boldsymbol{e}$ has order 1 right? Is it the only element of order 1 in G?
- Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with the binary operation $+$ defined by the following table (mod 4 addition):
  Question: What is the order of the elements 1 i.e. what is the smallest $n \in \mathbb{Z}^+$ such that $n1 = 0$? What about the order of 3?

Challenge 2

Is the order $|g| = n \in \mathbb{Z}^+$ of $g \in G$ unique i.e. if $n_1 = |g|$ and $n_2 = |g|$ then $n_1 = n_2$?

Side note on Idempotent Elements

1. Recall that in the semigroup section, we defined an element $g \in G$ to be idempotent if $g^2 = g$. Now, taking into the group structure in G, is it true that the only idempotent element in G is the identity $\boldsymbol{e}$?

For the Folks in Quantum Computing

Tricky Challenge 1

Let $G = U(2)$, where $U(2)$ is the unitary group of operators acting on the Hilbert space $\mathbb{C}^2$.

- Now consider the single qubit gates $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ and $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

1. What is the order (as per definition 1.1) of X, Y and Z gates as elements of the group $U(2)$? What about the Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$?
2. Are all the unitary operators in $U(2)$ of the same order as the gates above? If not, can you find examples of unitary operators in $U(2)$ of the same order as the gates above?

The Subgroup Structure

Definition 1.2

Let G be a group and $H \subseteq G$. H is a subgroup of G if it forms a group structure under the same binary operation as G.

- Indeed, $H \subseteq G$ is a subgroup iff the following hold:

1. $\boldsymbol{e} \in H$.
2. $h_1 h_2 \in H$ for all $h_1, h_2 \in H$.
3. $h^{-1} \in H$ for all $h \in H$.

- Obviously, G and $\{\boldsymbol{e}\}$ are trivially subgroup!
- We'll write $H \leq G$ to denote the fact that H is a subgroup of G. In particular, when H is a proper subset i.e. $H \neq G$, then we write $H < G$.

Challenge 3

Let $H_1 \leq G$ and $H_2 \leq G$.Is it true that $H_1 \cap H_2 \leq G$? Is $H_1 \cup H_2 \leq G$ also necessarily true?

Special Subgroup Structures

Definition 1.3

Let G be group and $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$.

- It's relatively easy to prove that $Z(G) \leq G$! It's also easy to see that $Z(G) = G$ iff G is abelian right?
- In the literature, $Z(G)$ is called the 'centre' of G.

Definition 1.4

Let $H \leq G$ and $C(H) = \{g \in G \mid gh = hg \text{ for all } h \in H\}$.

- $C(H)$ is a subgroup called the 'centraliser' of H in G.

For the Folks in Quantum Computing

Tricky Challenge 2

Let $G = U(2)$, where $U(2)$ is the unitary group of operators acting on the Hilbert space $\mathbb{C}^2$ and let $H = SU(2)$ (the special unitary group) of $U(2)$.

1. Try identify at least 3 concrete elements of the centre $U(2)$ i.e. 3 elements of $Z(U(2))$.
2. Try identify at least 4 concrete elements of the centraliser of $SU(2)$ i.e. 4 elements of $C(SU(2))$.
3. Is any of the single qubit gates X, Y, Z and H in the centre of $U(2)$?
4. Is any of the single qubit gates X, Y, Z and H in the centraliser of $SU(2)$?

The Cyclic Subgroup Structure

Definition 1.5

Let G be a group and for $g \in G$, we define $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$.

- $\langle g \rangle$ is called the 'cyclic subgroup' generated by the element $g \in G$.
- Interestingly, $\langle g \rangle$ is the smallest subgroup of G containing g!
- Also, if $|g| = n$ then $\langle g \rangle = \{\boldsymbol{e}, g, g^2, \ldots g^{n-1}\}$.

Challenge 4

Is it true that $\langle g \rangle = \langle g^{-1} \rangle$ for all $g \in G$? Is it also true that $\langle g \rangle$ is always abelian regardless whether G is abelian or not?

Simple examples:

- Consider the group structure of the integers $\mathbb{Z}$ under ordinary addition. Then the cyclic subgroup generated by the integer 2 is $\langle 2 \rangle = \{2k \mid k \in \mathbb{Z}\} = 2\mathbb{Z}$.
- Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under mod 4 addition. Then the cyclic subgroup generated by 1 is $\langle 1 \rangle = \{1, 2, 3, 0\}$? What about $\langle 3 \rangle$?

For the Folks in Quantum Computing

Tricky Challenge 3

Let $G = U(2)$, where $U(2)$ is the unitary group of operators acting on the Hilbert space $\mathbb{C}^2$. For each of the single qubit gates X, Y, Z and H, identify the following subgroups:

1. $\langle X \rangle$
2. $\langle Y \rangle$
3. $\langle Z \rangle$
4. $\langle H \rangle$

The Cyclic Group Structure

Definition 1.6

A group G is cyclic if there exists some $g \in G$ such that $G = \langle g \rangle$.

- We say g generates the group G or that g is a generator of G.

Simple concrete examples:

- $G = \mathbb{Z}$ be the additive group of the integers. This is a cyclic group! Now, which of the following integers is a generator for $\mathbb{Z}$?
  1. 0 i.e. is $\langle 0 \rangle = \mathbb{Z}$?
  2. 1 i.e. is $\langle 1 \rangle = \mathbb{Z}$?
  3. 2 i.e. is $\langle 2 \rangle = \mathbb{Z}$?
  4. -1 i.e. is $\langle -1 \rangle = \mathbb{Z}$?
- Consider $G = 2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ under the addition of integers. This is a cyclic group of course! As we have seen, the integer 2 is its generator i.e. $2\mathbb{Z} = \langle 2 \rangle$.
- Interestingly, $2\mathbb{Z}$ is a subgroup of the cyclic group $\mathbb{Z}$. This motivates the following question: **Is every subgroup of a cyclic group cyclic?**

Challenge 5

Under the normal addition, can any of the following sets be a cyclic group?

1. The set of rationals $\mathbb{Q}$
2. The set of the reals $\mathbb{R}$
3. The set of complex numbers $\mathbb{C}$

Lecture 07

Cyclic Group Structure Recap

Definition 1.0

A group G is cyclic if $G = \langle g \rangle$ for some $g \in G$.

- We say g generates the group G or that g is a generator of G.

Simple concrete examples:

- Let $G = \mathbb{Z}$ be the additive group of the integers. This is a cyclic group generated by the integers 1 and -1 i.e. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
- Consider $G = 2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ under the addition of integers. This is a cyclic group generated by the integer 2 i.e. $2\mathbb{Z} = \langle 2 \rangle$.
  Interestingly, $2\mathbb{Z}$ is a subgroup of the cyclic group $\mathbb{Z}$.
  Question: Is every subgroup H of a cyclic group G also cyclic?
- Consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ under mod 6 addition. This is a cyclic group with 1 and 5 as generators i.e. $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$.

- Interestingly, $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ under mod 7 addition has $1, 2, 3, 4, 5, 6$ as generators i.e. $\mathbb{Z}_7 = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 6 \rangle$.

- Have you notice that 1 has been a generator for all the examples above right? Indeed 1 is always a generator for $\mathbb{Z}n$!

- The example above also motivates the following natural question:

Question: Given a cyclic group G, how many generators are there?

Some Properties of Cyclic Groups

Theorem 1.0

Let G be a group and $H \leq G$. If G is cyclic then H is also cyclic.

- So all the subgroups of $\mathbb{Z}$ are cyclic and the same for $\mathbb{Z}_n$.

Alert: It is possible that a group G is not cyclic, but it contains subgroups that are cyclic! An example is the dihedral group D_{2n}.

Theorem 1.1

Let G be a cyclic group of order $|G| = \infty$ i.e. G is an infinite group. Then G is isomorphic to the cyclic group of the integers $\mathbb{Z}$.

- Hence, infinite cyclic groups are all abelian.
- Also, infinite cyclic groups have at most two generators right?

Theorem 1.2

Let G be a cyclic group of finite order $|G| = n$ i.e. G is a finite group with n elements. Then G is isomorphic to the cyclic group $\mathbb{Z}_n$.

- The above implies that finite cyclic groups are abelian too. Hence, cyclic groups are all abelian!

Note: You're recommended to try prove the theorems yourself! Happy to provide a pdf of the proof provided you tried to proved it yourself!

Mod n Comments

Notation Awareness

We have been using the notation $\mathbb{Z}_n$ as abbreviation for the set of integers mod n. In many books, the quotient notation $\mathbb{Z}/n\mathbb{Z}$ is used instead.

- Another thing you've notice is that $\mathbb{Z}_n$ as a whole forms a group structure under addition only, not under multiplication right?
- As a side note, $\mathbb{Z}_n$ forms a ring structure with unit under mod n addition and multiplication.

Question: Can we find a subset $\mathbb{Z}_n^* \subset \mathbb{Z}_n$ such that $\mathbb{Z}_n^*$ is a group under mod n multiplication?

- For example, consider $\mathbb{Z}_3 = \{0, 1, 2\}$ under mod 3 multiplication table given below:

Does the subset $\mathbb{Z}_3^* = \{1, 2\}$ form a group under the multiplication above? If yes, is it a cyclic group?

Multiplicative Groups (mod 4 Example)

- Let consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under mod 4 multiplication table given below:

Does the subset $\mathbb{Z}_4^* = \{1, 3\}$ form a group under the multiplication above? If yes, is it a cyclic group?

Multiplicative Groups (mod 5 Example)

- Let consider $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ under mod 5 multiplication table given below:

Does the subset $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ form a group under the multiplication above? If yes, is it a cyclic group?

Multiplicative Groups (mod 6 Example)

- Let consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ under mod 6 multiplication table given below:

Does the subset $\mathbb{Z}_6^* = \{1, 5\}$ form a group under the multiplication above? If yes, is it a cyclic group?

Multiplicative Groups (mod 7 Example)

- Let consider $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ under mod 7 multiplication table given below:

Does the subset $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ form a group under the multiplication above? If yes, is it a cyclic group?

The Multiplicative Group of Units mod n

Definition 1.1

For $\mathbb{Z}_n$, we define $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid a \text{ has a multiplicative inverse } \}$.

- A more formal definition of the above is $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid gcd(a, n) = 1\}$ where $gcd(a, n)$ denotes the greater common divisor of a and n.
- Another simple way to describe $\mathbb{Z}_n^*$ is as the set of numbers that are coprimes to n.
- It's already clear that $\mathbb{Z}_n^*$ forms a group under mod n multiplication?

Challenge 1

Identify all the group elements of $\mathbb{Z}_9^*, \mathbb{Z}_{12}^*, \mathbb{Z}_{14}^*, \mathbb{Z}_{18}^*, \mathbb{Z}_{20}^*, \mathbb{Z}_{24}^*$, $\mathbb{Z}_{32}^*$, $\mathbb{Z}_{34}^*$, $\mathbb{Z}_{36}^*$ and $\mathbb{Z}_{38}^*$.

Euler's phi function

Definition 1.2

For a positive integer n, we define Euler's phi function as $\phi(n) = |\mathbb{Z}_n^*|$ i.e. $\phi(n)$ is the number of elements in $\mathbb{Z}_n^*$.

- Hence, by definition we have $\phi(6) = 2$ whereas $\phi(7) = 6$.
- $\phi(n)$ is also often called 'Euler's totient function'.
- If $n = p_1^{k_1} p_2^{k_2} \dots p_j^{k_i}$ where $p_1, p_2, \dots p_j$ are prime numbers and $k_1, k_2, \dots k_i$ are positive numbers. Then we have the following beautiful formula to compute $\phi(n)$:

$$\phi(n) = n\,(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_j}).$$

Important note: $\phi(n)$ gives us the number of generators in finite cyclic groups! For example, the number of generators in $\mathbb{Z}_7$ is 6 because $\phi(7) = 6$.

Challenge 2

Compute $\phi(12)$, $\phi(14)$, $\phi(18)$, $\phi(20)$, $\phi(24)$, $\phi(32)$, $\phi(34)$ and $\phi(38)$.

Challenge 3

Let $n_1, n_2 \in \mathbb{Z}^+$. Is it true that $\phi(n_1 n_2) = \phi(n_1)\phi(n_2)$ iff $gcd(n_1, n_2) = 1$?

Cryptography Mini School I (Focus on Symmetric Cryptography)

Symmetric Cryptography Systems

Definition 1.0

A symmetric cryptographic scheme is a 5-tupple $(\mathcal{K}, \mathcal{M}, \mathcal{C}, e, d)$ such that the following conditions hold:

1. $\mathcal{K}$ is a non-empty set called the keyspace.
2. $\mathcal{M}$ is a non-empty set called the message space.
3. $\mathcal{C}$ is a non-empty set called ciphertext space.
4. $e : \mathcal{K} \times \mathcal{M} \longrightarrow \mathcal{C}$ and $d : \mathcal{K} \times \mathcal{C} \longrightarrow \mathcal{M}$ are maps satisfying $d(k, e(k, m)) = m$ for all $k \in \mathcal{K}$ and $m \in \mathcal{M}$.

- Hence, informally, the map e (encryption algorithm) takes a key $k \in \mathcal{K}$ and a message $m \in \mathcal{M}$ to produce a ciphertext $e(k, m) \in \mathcal{C}$.
- Whereas the map d (decryption algorithm) takes the key $k \in \mathcal{K}$ and the produced ciphertext $e(k, m) \in \mathcal{C}$ to reproduce the message $d(k, e(k, m)) = m \in \mathcal{M}$.
- When the key $k \in \mathcal{K}$ is fixed, then the notation e_k is used to denote the encryption map e and d_k to denote the decryption map d such that:

1. The encryption map $e(k, m)$ is abbreviated as $e_k(m)$.

2. The decryption map $d(k, e(k, m))$ is abbreviated as $d_k(e(m))$.

Desired Properties of a Symmetric Cryptosystem

1. When $k \in \mathcal{K}$ and $m \in \mathcal{M}$ are known, computing the map $e_k(m) \in \mathcal{C}$ shouldn't be hard i.e. applying the encryption algorithm should be easy.
2. Likewise, when $e_k(m) \in \mathcal{C}$ and $k \in \mathcal{K}$ are known, computing $d_k(e_k(m)) = m \in \mathcal{M}$ shouldn't be hard i.e. appying the decryption algorithm should be easy.
3. Let $c_1 = e_k(m_1), c_2 = e_k(m_2), \ldots, c_j = e_k(m_j)$. Then without the knowledge of the encryption key k, it should be computationally hard to find $d_k(c_j)$.