Abstract Algebra

- **OUTLINE**
  - **Basic Terms/Definitions**
    - Binary operation
    - Commutativity/Associativity
  - **Groups and related concepts**
    - Groupoid
    - Semigroup / commutative semigroup / subsemigroup
      - Identity element
    - Monoid / submonoid
      - Inverse element
    - Group / abelian group
    - Some finite groups
  - **Cyclic Groups**

Abstract Algebra

- **BINARY OPERATION** on a set A
  a function *f* that maps each and every ordered pair (a,b) $\in$ A $\times$ A to an element of A.
  - That is
- *NOTATION*:
  binary operations $\Rightarrow$
  element assigned to (a,b) $\Rightarrow$.
  In other words, .
- ***Examples***:
  - Binary operations defined on R :

Abstract Algebra

- ***Examples***:
  Let A = Z^+
  - Define **a*b = min(a,b)**.
    Examples:
  - Define **a*b = a**
    Examples:
  - Define **a*b = max(a,b) + 1**
    Examples:

Abstract Algebra

- **Remarks:**
  The binary operation * (on the set A) should be defined in such a way so that the following are satisfied:
  - ______________________ is assigned to the each ordered pair (a,b) $\in$ A$\times$A
  - the element assigned to (a,b) must be an element of A. In other words, a*b $\in$ A or ________________________ __________.

Abstract Algebra

- A set A is said to be **closed under the operation *** if it has the following property:
  - *if a and b are elements of the set A, then* _______
- ***Examples:***
  Determine if the given functions are binary operations defined over the given set A:
  - *Let A = Q, and* ***a*b = a/b***
  - *Let A =* Q^+*, and* ***a*b = a/b***
  - *Let A =* $Z^{\oplus}$*, and* ***a*b = a-b***
  - *Let A = Z, and* ***a*b = c*** *such that c < a and c < b*
  - *Let A = set of matrices, and * ≡ matrix addition.*

Abstract Algebra

- **Remarks:**
  If A = {a_1, a_2, … , a_n} is a *finite set*, we can define a binary operation on A thru means of a table, as follows:

*	a_1	a_2	…	a_j	…	a_n
a_1	a_1*a_1	a_1*a_2	…	a_1*a_j	…	a_1*a_n
a_2	a_2*a_1	a_2*a_2	…	a_2*a_j	…	a_2*a_n
:	:	:	…	:	…	:
a_i	a_i*a_1	a_i*a_2	…	a_i*a_j	…	a_i*a_n
:	:	:	…	:	…	:
a_n	a_n*a_1	a_n*a2	…	a_n*a_j	…	a_n*a_n

Abstract Algebra

- ***Example*:**

  Multiplication table: where a*b=a·b on Z^+::

×	1	2	3	4	5	...
1	1	2	3	4	5	
2	2	4	6	8	10	
3	3	6	9	12	15	
4	4	8	12	16	20	
5	5	10	15	20	25	
:	:	:	:	:	:	

Abstract Algebra

- ***Example*:**

  Truth table for **a*b = a $\wedge$ b** on **A={T, F}** is

$\wedge$	T	F
T		
F		

- ***Example*:**

  Construct the table for **a*b = |a-b|** on **A = {0,1,2}**

	0	1	2
0			
1			
2			

Abstract Algebra

- ***Example:***

  Suppose we define * on the set **A={a,b,c}** as follows

	a	b	c
a	a	c	a
b	b	c	a
c	c	a	b

  Using the table above, compute for the following:
  - **b*c**
  - **(a*c)*b**
  - **a*(b*c)**

Abstract Algebra

- **Properties of Binary Operations**
  - A binary operation on a set A is **commutative** if __________ for all elements a and b in A.
  - A binary operation on a set A is **associative** if _________________ for all elements a and b in A.
  - ***Examples:***

    Determine whether each of the following binary operations are commutative and/or associative.
    - Define **a*b = a – b** on **A = Z**
    - Define **a*b = min(a,b)**

Abstract Algebra

- ***Examples:***

  Determine whether each of the following binary operations are commutative and/or associative.
  - Define **a*b = a**
  - Define **a*b = min(a,b) + 1**
  - Define **a*b = |a – b|** for A = {0,1,2}

Abstract Algebra

- ***Examples:***

  Determine whether each of the following binary operations are commutative and/or associative.
  - **a*b** as defined by the table on the set A = {a,b,c}:

	a	b	c
a	a	c	a
b	b	c	a
c	c	a	b

- **Remark:**

  The binary operation * on the set A is commutative iff its corresponding table is ________________________________ ________ in the table.

Groupoids, etc.

- **GROUPOID (G,*)**
  - Nonempty set G together with *binary operation* * defined on G

Examples:
Are the following groupoids or not?
- **(Z^+,*)** where **a*b = min(a,b)**
- **(Z^+,-)** (ordinary subtraction)
- **(Q^+,/)** (ordinary division)
- **(A,*)** where A = {0,1,2} and **a*b = |a-b|**

Groupoids, etc.

- **SEMIGROUP (S,*)**
  - Nonempty set S together with an ________________ __________ defined on the set S.
- **COMMUTATIVE SEMIGROUP (S,*)**
  - Semigroup (S,*) where * is a ____________________.

Examples:
Are the following (commutative) semigroups or not?
- **(Z,+)**
- **(Z^+,*)** where **a*b = a**
- **(Z,-)**

Groupoids, etc.

- **SUBSEMIGROUP of a semigroup (S,*)**
  - (T,*) if T is closed under * given that T $\subseteq$ S

Remarks:
- Note that associativity holds for any subset of a semigroup so that the subsemigroup (T,*) is ______________.
- Also, (S,*) is a subsemigroup of itself.

Examples:
Consider the semigroup **(Z,*)** where **a*b = |a – b|**. Are the following subsemigroups of (Z,*)?
- **(T,*)** where **T = {0, 1, 2}**
- **(T,*)** where **T = Z^-**
- **(T,*)** where **T = $Z^\oplus$**

Groupoids, etc.

- **IDENTITY ELEMENT e**
  - Element **e** in a semigroup if _____________ for all elements a $\in$ A.

Examples:
What is the identity element of each of the following semigroups?
- **(Z, +)**
- **(Z^+, +)**
- **(A, *)** on **A = {a, b, c}** where * is defined by the table

	a	**b**	**c**
a	c	a	b
b	a	b	c
c	b	c	a

Groupoids, etc.

- ***Examples:***
  What is the identity element of **(Q, *)** where **a*b = -(a·b)?**
  Solution:

Groupoids, etc.

- **Theorem.** If a semigroup (S,*) has an identity element, that element is unique.
  Proof:

Groupoids, etc.

- **MONOID (M,*)**
  - A semigroup (M,*) that ____________________.

Examples:
Are the following semigroups also monoids?
- **(Z, +)**
- **(Z^+, +)**
- **(A, *)** on **A = {a, b, c}** where * is defined by the table

	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

Groupoids, etc.

- **SUBMONOID of a monoid (M,*)**
  - (T,*) where $T \subseteq M$ *and* $T \neq \emptyset$ and such that
    - T is closed under the operation *
    - ____________________ is also in T

Examples:
Are the following submonoids of **(Z,+)**?
- **(T,*)** where **T = {0, 1, 2}**
- **(T,*)** where **T = Z^+**
- **(T,*)** where **T = $Z^\oplus$**

Groupoids, etc.

- **INVERSE ELEMENT of element *a***
  - Element **a'** in a monoid if ______________ for every element $a \in M$.

Examples:
What are the inverse elements in each of the following monoids?
- **($Q^\oplus$, +)**
- **(Z, +)**
- **(A, *)** on **A = {a, b, c}** where * is defined by the table

	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

Groupoids, etc.

- ***Examples:***
  What is the inverse element of **(Q, *)** where **a*b = -(a·b)?**
  Solution:

Groupoids, etc.

- **GROUP (G,*)**
  - A monoid (G,*) with identity element e that also ______ ________________ *f*or each element a in G.
- **ABELIAN GROUP (G,*)**
  - A group (G,*) where * is also ____________.

Examples:
Are the following monoids also (abelian) groups?
- **(Z, +)**
- **($Z^\oplus$, +)**
- **(Z, ·)** (ordinary multiplication)

Groupoids, etc.

- **SUBGROUP of a group (G,*)**
  - (H,*) where $H \subseteq G$ *and* $H \neq \emptyset$ and such that
    - H is closed under the binary operation *
    - Identity element e in G is also in H
    - If for every element a in H, there exists ___________ also in H

Examples:
- Is **(Q^+,·)** a subgroup of the group **(R^+,·)**?
- Is **(Z,+)** a subgroup of the group **(Q,+)**?
- Is **(Z^+,·)** a subgroup of the group **(R^+,·)**?

Groupoids, etc.

- Let (H,*) be a subgroup of (G,*) with identity element e.
  - If H=G then (H,*) is an ____________________ of (G,*). Otherwise (H,*) is a **proper subgroup**.
  - If H={e} then (H,*) is known as the **trivial subgroup** of (G.*). Otherwise, (H,*) is a ____________________.

Examples:
- Is **(Q^+,·)** a proper subgroup of the group **(R^+,·)**?
- What is the trivial subgroup of **(R^+,·)**?

Groupoids, etc.

- ***Examples:***
  Consider the group structure $\mathbf{Z_4}$ = (A,*) where A = {0, 1, 2, 3} and * is defined as follows:

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

  - Give an improper subgroup of $\mathbf{Z_4}$.
  - Give a trivial subgroup of $\mathbf{Z_4}$.
  - Give a (nontrivial) proper subgroup of $\mathbf{Z_4}$.

Groupoids, etc.

- **FINITE GROUPS**
  If (G,*) is a finite group, then the **order of G**, denoted by **|G|** is the ______________________.

Examples:
- The group (A,*) where A={e}, e being the identity element, is a group of order one(1).
- How would you fill in the table of each of the following finite groups (G,*)? (*where e is the identity element*)
  - Finite group of **order one(1)** where **G = {e}**
  - Finite group of **order two(2)** where **G = {e, a}**
  - Finite group of **order three(3)** where **G = {e, a, b}**

Groupoids, etc.

- **SUMMARY**

	Binary	Assoc	e	a'
Groupoid	✔			
Semigroup	✔	✔		
Monoid	✔	✔	✔	
Group	✔	✔	✔	✔

Cyclic Groups

- **POWER of an element a**
  Given group (S,*) with identity element e and n ∈ Z
  - The powers of element a are defined as:
    - $\mathbf{a^0 = e}$
    - $\mathbf{a^1 = a}$ and $\mathbf{a^{-1} = a'}$
    - $\mathbf{a^n = a^{n-1}*a}$ for n ≥ 2 and _____________ for n ≤ -2
  - NOTE: Also, $\mathbf{a^{-n} = (a^{-1})^n}$
  - *Essentially*: $\mathbf{a^n} = \underbrace{\mathbf{a*a*a* \dots *a}}_{n \text{ terms}}$

$$\mathbf{a^{-n}} = \underbrace{\mathbf{a^{-1}*a^{-1}*a^{-1}* \dots *a^{-1}}}_{n \text{ terms}}$$

Cyclic Groups

- ***Example:***
  Consider the group **(Q^+, ·)**. Note that
  -
  -
  -
  -
- ***Example:***
  Consider the group **(Z,+)**. Note that
  -
  -
  -
  -

Cyclic Groups

- ***Example*:**

  Consider the group ({1, 2},*) where * is defined as

	1	**2**
1	2	1
2	1	2

  Note that
  -
  -

  What is $\mathbf{1^4}$?
  -

Cyclic Groups

- ***Example*:**

  Consider the group ({1, 2},*) where * is defined as

	1	**2**
1	2	1
2	1	2

  Note that
  -
  -

  What is $\mathbf{1^{-3}}$?
  -

Cyclic Groups

- ***Example:***
  - Consider the group **(Q^+, *)** where **a*b = 2ab**.
    - $\mathbf{a^0}$ =
    - $\mathbf{a^1}$ = and $\mathbf{a^{-1}}$ =
    - What is 1^4?
    - What is $\mathbf{1^{-3}}$?

Cyclic Groups

- **THEOREM**

  Given group (G,*) and $a \in$ G
  - (H,*) where $\mathbf{H = \{a^n \mid n \in Z\}}$ is
    - a subgroup of (G,*)
    - the smallest subgroup of G ____________

***Example*:**

Consider the group (Z,+). Find the elements of the sets below:
- $H_1 = \{2^n \mid n \in Z\}$
- $H_2 = \{5^n \mid n \in Z\}$
- $H_3 = \{10^n \mid n \in Z\}$

Cyclic Groups

- ***Example:***

  Consider the group structure Z_4 = (A,*) where A = {0, 1, 2, 3} and * is defined as follows:

	0	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

  Find the elements of the sets below:
  - $H_1 = \{0^n \mid n \in Z\}$
  - $H_2 = \{2^n \mid n \in Z\}$

Cyclic Groups

- **CYCLIC SUBGROUP of (G,*) generated by a $\in$ G**

  <a> = ___________________________

***Examples*:**
- Recall (Z,+). We had previously defined the cyclic subgroups
  - **<2> = (H_1,+)** where $H_1 = \{\mathbf{2}^n \mid n \in Z\}$
  - **<5> = (H_2,+)** where $H_2 = \{\mathbf{5}^n \mid n \in Z\}$
  - **<10> = (H_3,+)** where $H_3 = \{\mathbf{10}^n \mid n \in Z\}$
- Recall Z_4 . We had previously defined the cyclic subgroups
  - **<0> = (H_1,+)** where $H_1 = \{\mathbf{0}^n \mid n \in Z\}$
  - **<2> = (H_2,+)** where $H_2 = \{\mathbf{2}^n \mid n \in Z\}$

Cyclic Groups

- **CYCLIC GROUPS**
  - ***a* generates G** and ***a* is a generator for G**
    if <a> = ____________________
  - (G,*) is a **cyclic group** if ∃ a ∈ G which generates G.

Examples:
- Are the following cyclic groups? If so, what element(s) generates the group?
  - Z_4
  - (Z,+)