Module 23: Groups, Rings and Fields

- Groups, Rings, Fields are Fundamental elements of abstract algebra.
- Combine two elements of set, to obtain a third element of set.

Groups:

- A group G, denoted by [G, ●]
- Set of elements with a binary operation denoted by ● that associates to each ordered pair (a,b) of elements in G, an element (a ● b) in G, such that following axioms are obeyed.
- (A1) Closure: If a and b belong to G, then a ● b is also in G.
- (A2) Associative : a ● (b ● c) = (a ● b) ● c for all a,b,c in G.
- (A3) Identity element: element e in G such that a ● e = e ● a = a for all a in G
- (A4) Inverse Element : For each a in G, there is an element a’ in G such that a ● a’= a’ ● a = e

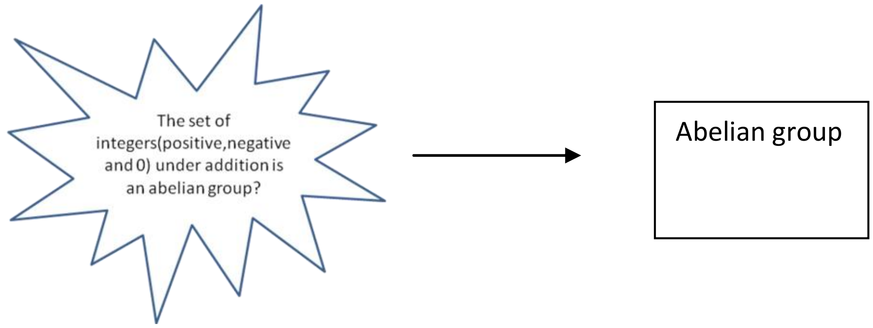
Finite Group

- If a group has finite number of elements, it is referred as a finite Group.
- Number of elements in the group is called the order of the group.
- A group with infinite number of elements is called infinite group.

Abelian group

- A group is abelian if follows the following axiom in addition to (A1) to (A4)

  (A5) commutative : a ● b = b ● a for all a,b in G.



The set of integers(positive,negative and 0) under addition follow all axioms

(A1) Closure: adding two positive integers is positive integer, two negative integers is negative integers, positive and negative may end up in positive or negative integer.

5+2 = 7

-2+3=1

-3+-3=-6

(A2)Associative: 3+(4+5)=(3+4)+5

-2+(-5+-6)=(-2+-5)+-6

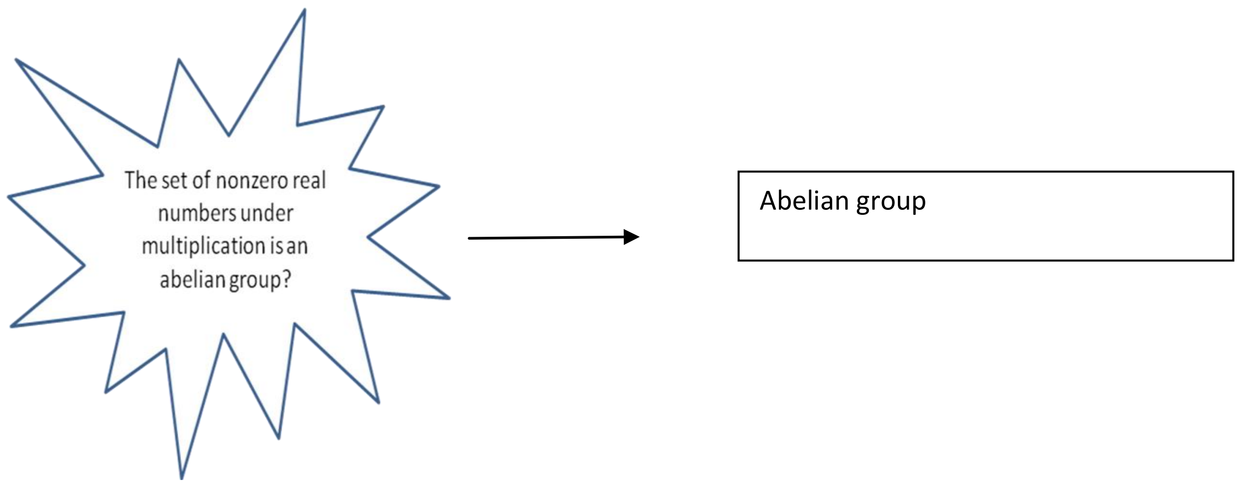
(A3)Identity element: 5+0=0+5=5

-3+0=0+-3=-3

(A4) Inverse element : 5+(-5)=0

(A5) Commutative : 5 + -7 = -7+5

* For group operation addition, the identity element is 0, inverse element of a is –a. subtraction is defined as a-b = a+(-b).

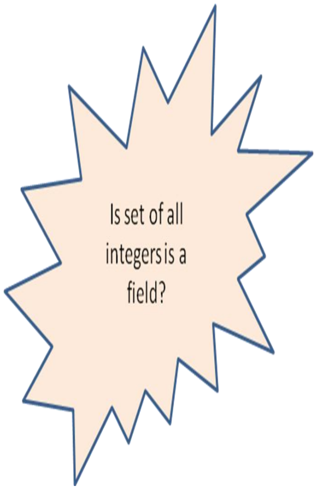


Cyclic group

- a^4= axaxaxa
- a^0=e(as identity element)
- a^{-n}=(a')n where a' is the inverse element of a within the group.
- A group G is cyclic if every element of G is a power a^k (k is an integer) of a fixed element aεG. The element a is said to generate the group G or to be a generator of G. A cyclic group is always abelian and may be finite or infinite.
- The additive group of integers is an infinite cyclic group generated by the element 1.
- Powers are interpreted as addition so that nth power of 1.
- $1^1+2^1+3^1+$ ….

<u>Rings:</u>

- A ring R, denoted by {R, +, x} is a set of elements with two binary operations(addition and multiplication) such that all axioms are followed for all a,b,c in R .
- (A1-A5) - R satisfies A1 through A5 for addition so R is an abelian group with respect to addition.
- (M1) Closure under multiplication - ab is in R if a and b belong to R.
- (M2) Associativity of multiplication – a(bc)=(ab)c for all a,b,c in R.
- (M3) distributive laws –



1. a(b+c) = ab+ac for all a,b,c in R.
2. (a+b)c = ac+bc for all a,b,c in R.

* Ring can do addition, multiplication and subtraction. Subtraction is [a-b=a+(-b)].

- A set of integer numbers(positive, negative and 0) is a ring, with respect to addition and multiplication.
- The set of all matrices is a ring.
- Ring is commutative If following axiom is satisfied.

(M4) commutative(multiplication): ab=ba for all a,b, in R.

Integral domain:

- Integral domain is a commutative ring if following axioms are satisfied.

  (M5) Multiplicative identity – the element 1 in R such that a1=1a=a for all a in R.

  (M6)No zero divisor – if a,b in R and ab=0 then either a=0 or b=0.

- Let S be the set of integers positive, negative and 0 under operation of addition and multiplication, S is an integral domain.

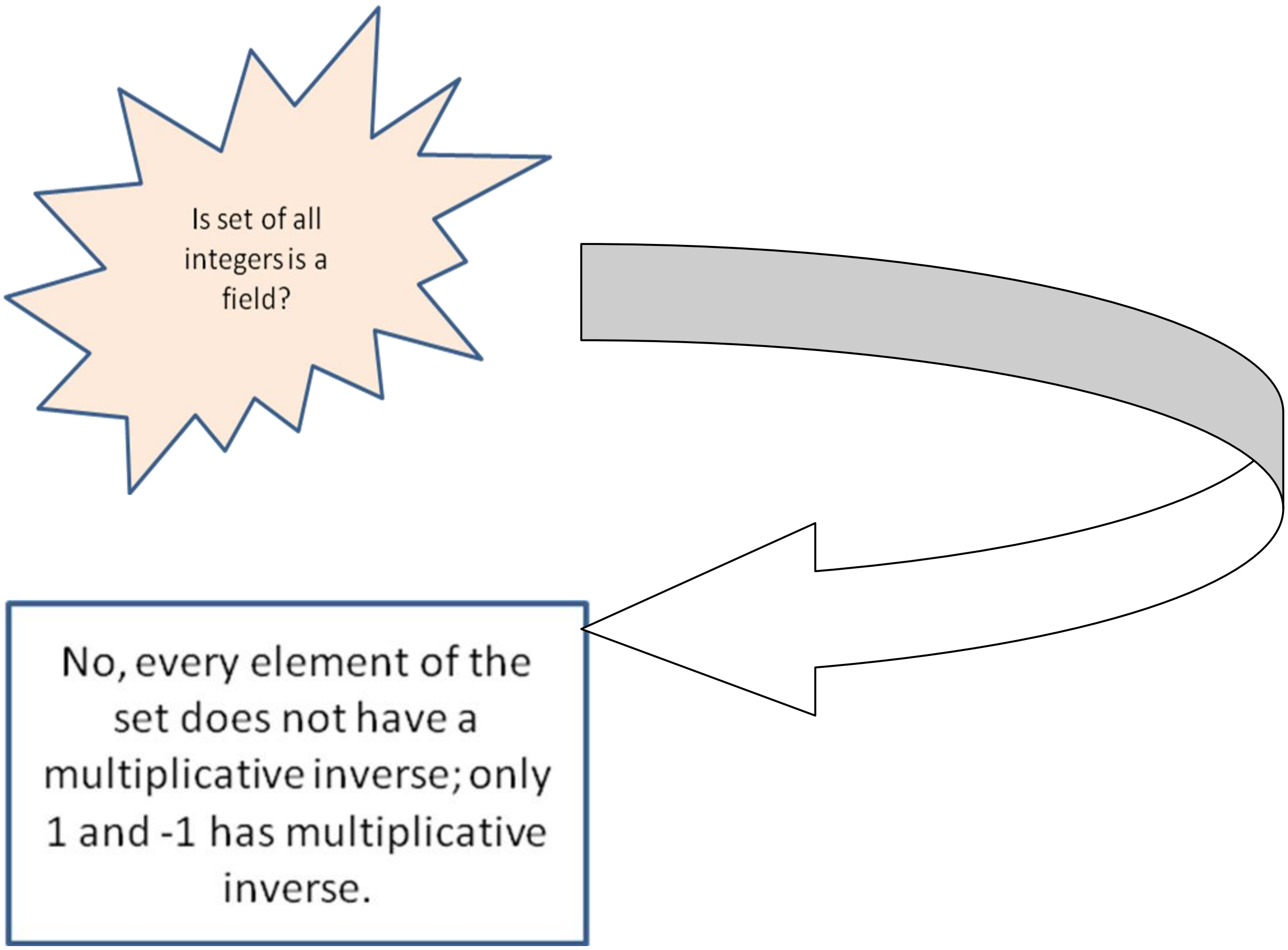
Fields:

- A field F denoted by [F, +,x] is set of elements with two binary operations, called addition and multiplication, such that all a,b,c in F follows following axioms.

(A1-M6) : F is an integral domain if F satisfies axioms A1 through A5 and M1 through M6.

(M7) Multiplicative inverse : For each a in F, except 0 , there is an element a^{-1} in F such that aa^{-1} in F such that $aa^{-1}=(a^{-1})a=1$

- In Field, addition, subtraction, multiplication and division results in the same set.
- Division is defined as $a/b=a(b^{-1})$
- All rational, real and complex numbers are field.



<u>Finite Fields of the Form GF(p)</u>

- Finite fields are important in cryptography
- Order of a finite field that is number of elements in the field must be a power of a prime p^n, where n is a positive integer.

<u>GF(p^n)</u>

- Finite field of order p^n is GF(p^n).
- GF stands for Galois field, in the honor of mathematician who studied this for the first time.

- Two special cases exist.
  1. n=1, finite field GF(p)
  2. n>1

Finite fields of Order p

- For a given prime p, finite field of order p, Gf(p) as the set Zp of integers {0,1…p-1} together with the arithmetic operations modulo p.
- Zp is a commutative ring, with the arithmetic operations modulo p.
- Any integer in Zp has multiplicative inverse if and only if that integer is relatively prime to p.
- If p is prime, then all nonzero integers in Zp are relatively prime to p so for all elements multiplicative inverse exist.

GF(2) – addition is equivalent to XOR and multiplication is equivalent to logical AND.

+	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	1

Finding the multiplicative inverse in GF(p)

- if a and b are relatively prime, then b has a multiplicative inverse modulo a.
- For positive integer b<a there exists b^{-1}<a such that bb^{-1}=1 mod a.

  if by mod a=1 then y=b^{-1}

Addition modulo 5 GF(5)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplicative modulo 5 GF(5)

X	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2

4	0	4	3	2	1

additive and multiplicative inverse modulo 5.

w	-w	w^{-1}
0	0	-
1	4	1
2	3	3
3	2	2
4	1	4

Finite Fields of the form GF(p)

> Finite fields are used in cryptography. The number of elements in the field must be power of prime p^n, where n is a positive integer.

The finite field of order p^n is written as $GF(p^n)$; GF stands for Galois field. For n=1, the finite field is GF(p)

- For a given prime p, finite field of order p, GF(p), as the set of Z_p of integers [0,1,…,p-1} together with the arithmetic operations modulo p.
- An integer in Z_p has a multiplicative inverse, if and only if that integer is relatively prime to p.
- If p is prime, then all nonzero integers in Z_p are relatively prime to p and therefore there exists a multiplicative inverse for all nonzero integers in Z_p.

Multiplicative inverse(w^{-1})	For each $w \varepsilon Z_p$, $w \neq 0$, there exist a $z \varepsilon Z_p$ such that $wxz \equiv 1 (\text{mod } p)$.

GF(p) has following properties

- GF(p) consists of p elements
- The binary operations + and x are defined over set. The operations of addition, subtraction, multiplication and division can be performed without leaving the set. Each element of the set other than 0 has a multiplicative inverse.