UNIT - 1

Defn binary operation :-

Let G be a set. A binary operation on G is a function that assigns each ordered pair of element of G.

Note :

The binary operations are ordinary addition substraction, Multication of integers.

Division of integer is not a binary operation on the integer.

Defn group :-

G is a group under this operation (usually called multiplication) if the following three properties are statisfied.

1. Associativity :

(a, b, c).

$(ab)c = a(bc)$ for all a, b, c in set

2. Identity :

There is an element 'e' in G such that $ae = ea = a$ for all 'a' in G

3. Inverse :

For each element a in G

There is an element 'b' in G

such that $ab = ba = e$.

Note :

If 'a' is an inverse of 'b' then

'b' is an inverse of 'a'.

Group is Abelian :

If a group has the property that

$ab = ba$ for every pair of elements

'a' and 'b' we say the group is abelian.

EX : 1

The set of integer I the set of rational no Q, and set of real no. R are all group under ordinary addition. In each case the identity is '0' and the inverse of 'a' is '-a'.

EX : 2

The set of integers under the ordinary multiplication is not a group. Since the number 1 is the identity Inverse property fails.

Eg: There is no integer b such that

Ex:3.

The subset $\{1, -1, i, -i\}$ of the complex number is a group under complex multiplication

Note that '-1' is the own inverse whereas the inverse of 'i' is '-i' and vice versa.

Ex:4

The set $\mathbb{Q}$ of positive rationals is a group under ordinary multiplication.

The inverse of any 'a' is $1/a = a$

Ex:5

The set 'S' of positive irrational numbers together with 1 under multiplication is not a group $\sqrt{2} \cdot \sqrt{2} = 2$, so S is not closed under multiplication.

Note:

Any pair of elements can be combined without going outside the set is called closure.

Ex:6 A rectangular array of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is called 2×2 matrix. The set of all 2×2 matrices with real entries is a group under component wise addition. That is.

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix}$$

The identity is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and the inverse of

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$

Ex:7 The set $Z_n = (0, 1 \cdots n-1)$ for $n \geq 1$ is a group under addition modulo n. For any $j > 0$ in Z_n the inverse of j is $n-j$. This group is usually reffered to as the group of integers modulo n.

$n = 9$ the inverse of 2 is 7.

As we have seen the real numbers the 2×2 matrices with real entries and the integral modulo n are all grps under the appropriate addition. But what about multiplication? In each case the existence of some elements that do not having inverses prevents the set

from being a group under the usual multiplication. However we can form a group in each case by simply throwing out the rascals. Examples 8, 9, 11. illustrate this.

Ex:8 The set R^* of nonzero real numbers is a group under ordinary multiplication. The identity is 1. The inverse of a is $1/a$.

Ex:9 The determinant of 2×2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is the number $ad-bc$. If A is a 2×2 matrix. $\det A$ denotes the determinant of A. The set

$$GL(2,R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a,b,c,d \in R, ad-bc \neq 0 \right\}$$

of 2×2 matrices with real entries and nonzero determinant is a non-Abelian group under the operation.

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$$

The first step in verifying that this set is a group is to show that the product of two matrices with nonzero determinant also have nonzero determinant. This follows from the fact that for any pair of 2×2 matrices A and B $\det(AB) = (\det A)(\det B)$.

Associativity can be verified by direct (but cumbersome) calculations. The identity is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ the inverse of

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

$$\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$

(Explaining the requirement that $ad-bc \neq 0$)

This very important non-abelian group is called the general linear group 2x2 matrices over R.

EX:10 The set 2x2 matrices with real numbers entries is not a group under the operation defined in EX:9. Inverses do not exist when the determinant is 0. Now that we have shown how to make subsets of the real numbers and subsets of the set 2x2 matrices into multiplication groups we next consider the Integer under multiplication modulo n.

EX:11 (L. Euler 1761).

By EX:13 in chapter 0 an integer a has a multiplicative inverse modulo n if and only if a and n are relatively prime. So for each $n>1$, we defn $U(n)$ to be the set of all +ve integers less than n, and relatively prime to n. Then U(n) is a group under multiplication modulo n. (we leave as an ex the proof that this set is closed under this operation)

For $n=10$, we have $U(10) = \{1, 3, 7, 9\}$. The cayley table for $U(10)$ is

mod 10	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

(Recall that $ab \bmod n$ is the unique integer r with the property $a \cdot b = nq + r$ where $0 \leq r \leq n$ and $a \cdot b$ is ordinary multiplication). In the case that n is a prime $U(n) = \{1, 2 \cdots n-1\}$.

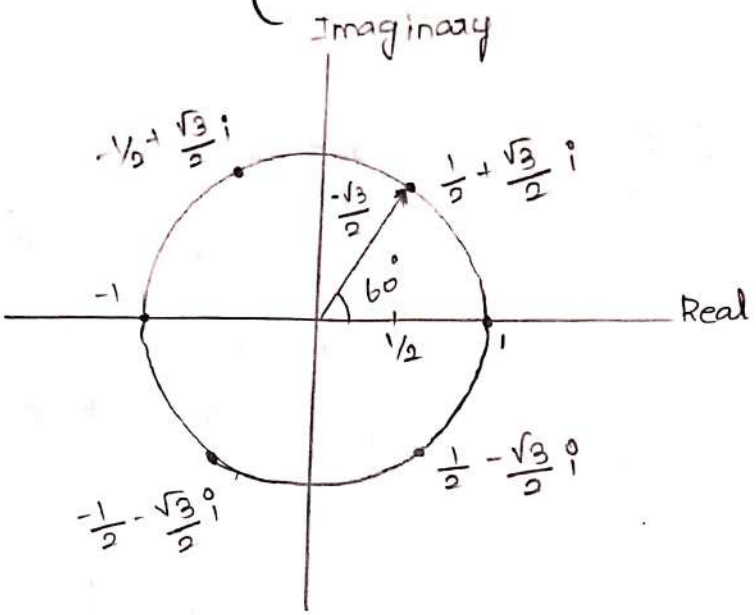
In this classic book Lehrbuch der algebra, published in 1899. Henrich weber gave an extensive treatment of the groups $U(n)$ and described them as the most important exples of finite abelian groups.

Ex: 12. The set $\{0, 1, 2, 3\}$ is not a group under multiplication modulo 4. Although 1 and 3 have inverses, the element 0 and 2 do not.

Ex: 13. The set of integers under subtraction is not a group since the operation is not associative

With the examples given this far as a guide it is wise for the reader to pause here and think of his or her own examples. study respectively

Ex:14 For all integers $n \geq 1$ the set of complex roots of unity $\left\{ \cos \frac{k \cdot 360^\circ}{n} + i \sin \frac{k \cdot 360^\circ}{n} \;\middle|\; k = 0, 1, 2 \cdots n-1 \right\}$



(ii) (complex zeros of $x^n - 1$) is a group under multiplication (see demoivre's thm - Ex : 8 in chapter 0). compare this gp with one in Ex 3.

The complex number $a+bi$ can be represented geometrically as the point (a, b) in a plane co-ordinatized by a horizontal real axis and a vertical i(or imaginary) axis. The distance from the point $a+bi$ to the origin is $\sqrt{a^2+b^2}$ and is often denoted by $|a+bi|$. For any angle θ the line segment joining the complex number $\cos\theta + i\sin\theta$ and the origin forms an angle of θ with the positive real axis. Thus the six complex zeros of $x^6 = 1$ are located at point

around the circle of radius 1, 60° apart.

EX:15 The $R^n = \{(a_1, a_2 \ldots a_n) \mid a_1, a_2 \ldots a_n \in R\}$ is a group under componentwise addition

[ie $(a_1, a_2 \ldots a_n) + (b_1, b_2, \ldots b_n) = (a_1+b_1, a_2+b_2 \ldots a_n+b_n)$]

EX:16 For a fixed point (a, b) in R^2 defn $T_{a,b}$: $R^2 \to R^2$ by $(x, y) \mapsto (x+a, y+b)$ Then $T(R^2) = \{T_{a,b} \mid a, b \in R\}$ is a group under function composition. Straight forward calculations show that $T_{a,b} T_{c,d} = T_{a+b+c+d}$ From this formula we may observe that $T(R)^2$ is closed. $T_{0,0}$ is the identity the inverse of $T_{a,b}$ is $T_{-a,-b}$, and $T(R^2)$ is abelian. Function composition is always associative. The element of $T(R^2)$ are called translations.

EX:17 The set of all 2x2 matrices with determinant 1 with entries from Q (rationals) R (reals) C (complex numbers) or Z_p (p a prime) is a non-Abelian group under matrix multiplication: This group is called the special linear group of 2x2 matrices over Q, R, C or Z_p respectively. If the entries are from F where F is any of the above, we denote the group by $SL(2, F)$. For this group $SL(2, F)$ formula given in the eg 9 for the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. when the matrix

entries are from Z_p. we use modular arithmetic to compute determinants, matrix product and inverse

Illustrate the case $SL(2, Z_5)$. consider the element

$$A = \begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix} \Rightarrow \det A = |A| = |12 - 16| = |-4| = 4$$

$$= |\text{mod } 5| \text{ and the inverse}$$

of the matrix A is $\begin{bmatrix} 4 & -4 \\ 4 & 3 \end{bmatrix} = \frac{1}{|A|} \text{adj } A$.

$$\begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix} \text{ note that,}$$

$$\begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix} \begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 16 & 15 \\ 20 & 16 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

where the arithmetic is done with modulo 5.

Ex: 18.

let F be any of Q, R, C or Z_p | p is prime

The group $GL(2, F)$ of all 2×2 matrices with nonzero determination and F is a non-abelian grp under matrix multiplication From Eg 17 when F is Z_p modulo p arithmetic is used to calculate the determinants, the matrix products and inverses. The formula given in Eg 4 for the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ remains valid for elements for $GL(2, Z_p)$ provided we interpret division by $ad - bc$ as multiplication by

the inverse of $ad-bc$ modulo p. For example in $GL(2, Z_p)$ consider $\begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix}$. Then the determinant $ad-bc$ is $12-30 = |-18|$ and modulo 7 and the inverse of 3 is 5 (since $35 = 1 \bmod 7$). So the inverse of $\begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix}$ is

$$\begin{bmatrix} 3\cdot 5 & 2\cdot 5 \\ 4\cdot 5 & 4\cdot 5 \end{bmatrix} = \begin{bmatrix} 15 & 10 \\ 5 & 20 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 6 \end{bmatrix}$$ we should know that $\begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 5 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is

$$= \begin{bmatrix} 4+25 & 12+30 \\ 6+15 & 18+18 \end{bmatrix} = \begin{bmatrix} 29 & 42 \\ 21 & 36 \end{bmatrix}$$

Ex:19.

The set $\{1, 2 \ldots n-1\}$ is a group under multiplication modulo n if and only if n is prime.

⇒ An Integer is defined as a number that can be written without a fractions component.

Eg: 21, 0, -20 are integers while 9.7 and $\sqrt{2}$ are not.

⇒ A Rational number is a number that can be expressed as the quotient p/q of two integers a numerator p and nonzero determinant q since q may be equal to 1. every integer is a rational number.

⇒ Irrational Number is a real number that cannot be written as a simple fraction.

Another clue is that the decimal goes on for ever without repeating π is a famous irrational number $\pi = \frac{22}{7} = 3.14285714285714\ldots$

⇒ The real number inclined all the rational numbers such as the integer -5 and the fraction $\frac{4}{3}$, and all irrational numbers such as $\sqrt{2}$.

Note:

componentwise addition means add a_1+a_2, d_1+d_2 etc...

Modulo N of a no means when you divide the number x, After dividing the no whatever remainder you get is called modulo.

(Eg) Modules of N of a number 2 is 1

Multiplication modulo n of A and B is $(A \neq B) \bmod n$.

Addition modulo of A and B is $(A+B) \bmod n$

Two integers are relatively prime (or coprime) if there is no integer greater than one that divides them both that is their greatest

common divisor 1 and 4 are relatively prime is respect to each other.

Ex:10.

mod 4	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Note: complex zeros of $x^b - 1$ is a group under multiplication degree b.

$\therefore$ b zeros of $x^b - 1$

$$x^b - 1 = (x^3)^2 - 1^2$$

$$= (x^3 - 1)(x^3 + 1)$$

1, -1 are at roots.

$$x^3 - 1 = (x-1)(x^2 + x + 1)$$

$$x^2 + x + 1 = \frac{-1 \pm \sqrt{1-4}}{2}$$

$$= \frac{-1 \pm i\sqrt{3}}{2}$$

$$x^3 + 1 = (x+1)(x^2 - x + 1)$$

$$(x^2 + x + 1) = \frac{1 \pm \sqrt{1-4}}{2}$$

$$= 1 \pm i\sqrt{3}/2$$

$1, -1, -1+i\sqrt{3}/2, -1-i\sqrt{3}/2, 1+i\sqrt{3}/2, \frac{1-i\sqrt{3}}{2}$ are

Zeros of $x^b - 1$

$x \left\{ 1, -1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}, \frac{1+i\sqrt{3}}{2}, 1-i\sqrt{3}/2 \right\}$ is a group under multiplication Inverse of $\frac{1+i\sqrt{3}}{2}$ is $1+i\sqrt{3}/2$

$\left(\frac{1+i\sqrt{3}}{2}\right)\left(\frac{1-i\sqrt{3}}{2}\right) = 1$ so $x^6 = 1$ is a group under multiplication.

Elementary properties of Groups :-

Thm : 2.1 suppose ~~both~~ uniqueness of the identity.

In a group G there is only one Identity element

proof : suppose both e and e' are identities of G, then

1. $ae = a$ for all a in G and
2. $e'a = a$ for all a in G.

The choice of $a = e'$ in (1) and $a = e$ in (2) yields $e'e = e$ & $e'e = e$. Thus e and e' are both equal to ee' and so are equal to any other.

Because of the thm, we may unambiguously speak of the identity of a group, and denote it by "e" (because the German for identity is Einheit)

Thm : 2.2 cancellation.

In a group G the right and left cancellation laws hold, then is $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.

proof : suppose $ba = ca$ let a' be an inverse of a. Then multiplying on the right by 'a' gives $(ba)a' = (ca)a'$. Associativity yields $b(aa') = c(aa')$

The be = ce and therefore b = c as desired. similarly one can prove that ab = ac implies b = c by multiplying by a' on the left.

A consequence of the cancellation property is the fact that in a cayley take for a group, each group element occurs exactly once in each row and column] (see Ex: 24) Another consequence in the cancellation propeaty is the uniqueness of inreases.

Thm: 2.3 Uniqueness of Inreases:

For each element a in a group G, there is a unique element b in G such that $ab = ba = e$.

Proof: suppose b and c are both inverses of a Then $ab = e$ and $ac = e$ so that $ab = ac$ Now cancel $a \Rightarrow b = c$ $\therefore$ b is the inreases of c.

As was the case with the identity element it is reasonable in view of thm 2.3 to speak of inreise of an element g of a group. and in fact we may unambiguosly denote it by g^{-1}. This notation is suggested by that used for ordinary real numbers under multiplication. similarly when is the integer, g^n is used to denote the

Product

$$\underbrace{gg\cdots g}_{n \text{ factors}}.$$

we define $g^0 = e$ when n is negative we define $g^n = (g^{-1})^{-n}$ (for example $g^{-3} = (g^{-1})^3$). With this notation the familiar laws of exponential hold for groups that is for all integers m and n be any group element g. we have $g^m \cdot g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$. Although the way one manipulates the group expression $g^m g^n$ and $(g^m)^n$ coincides with the laws of exponents for real numbers, the laws of exponents fails to hold for expressions involving two group elements. Thus for groups in general, $(ab)^n \neq a^n b^n$ (see EX 15).

Also one must be careful with this notation when dealing with a specific group whose binary operation is addition and is denoted by "+". In this case, the defn and group properties expressed in multiplication notation must be translated to additive notation. For ex, the inverse of g is written as $-g$. likewise for example $g3$ means $g+g+g$ and is usually written as $3g$ whereas g^{-3} means $(-g)+(-g)+(-g)$ and is written as $-3g$. when additive notation

Finite group ; subgroups

Defn: order of a group

The number of element of a group (finite or infinite) is called order . we will use |G| to denote the order of G.

Thus the group $\mathbb{Z}$ of integers under addition has infinite whereas the group $U(10) = \{1, 3, 7, 9\}$ under multiplication and 10 has order 4.

Defn: order of an element :

The order of an element g in a group G is the smallest +ve integer n such that $g^n = e$ (In additive notation this would has 0) . If no such integer exists, we say g has finite order . The order of an element g is denoted by $|g|$.

So to find the order of a group element g you need only one sequence of product $g, g^2, g^3 \ldots$ until you reach the identity the 1st time. The exponent of this product (or co-eff if the notation is addition) is the order of g . If the Identity never appears in the sequence then g has Infinite order

Ex:1

Consider $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication modulo 15. To find the order of 7, we compute the sequence $7^1 = 7, 7^2 = 4, 7^3 = 13, 7^4 = 1$. So $|7| = 4$. To find the order of 11, we compute $11^1 = 11, 11^2 = 1$ so $|11| = 2$. similar computation, show that $|1| = 1$, $|2| = 4$, $|4| = 2$, $|8| = 4$, $|13| = 4$, $|14| = 2$

[Here is a trick that makes these calculation easier. Rather than computation the sequence $13^1, 13^2, 13^3, 13^4$ we may observe that $13 = -2$ modulo 15 (since $13 + 2 = 0 \mod 15$). so that

$[13^2 = (-2)^2 = 4, 13^3 = -2 \cdot 4 = -8, 13^4 = (-2)(-8) = 1]$

where, $13^4 = (-8)(-2) = -16$, using mod 15 we get

Ex:2

Consider Z_{10} under addition modulo 10. since $1 \cdot 2 = 2$, $2 \cdot 2 = 4$, $3 \cdot 2 = 6$, $4 \cdot 2 = 8$, $5 \cdot 2 = 0$, we know that $|2| = 5$ similar computations show that

$|0| = 1$, $|7| = 10$, $|5| = 2$, $|6| = 5$.

Ex:3

Consider Z under ordinary addition. Here every non zero element has infinite order, since the sequence $a, 2a, 3a \cdots$ never includes 0 when $a \neq 0$. Note: The group of complex no is $\{i, -1, 1, -i\}$ is a subset of a group $\{\cos\frac{k \cdot 360}{n} + i \sin\frac{k \cdot 360}{n}\}$ $k = 0, 1, \ldots$ for n equal to any multiple of 4.

Defn: subgroup

If a subset H of a group G is itself a group under the operation of G, we say H is a subgroup of G.

We use the notation $H \leq G$ to mean H is a subgroup of G. If we want to indicate that H is a subgroup of G, but not equal to G itself, we write $H < G$. such a subgroup is called a proper subgroup. The subgroup $\{e\}$ is called a nontrivial subgroup of G.

Notice that $\mathbb{Z}_n$ under addition modulo n is not a subgroup of $\mathbb{Z}$ under addition since addition modulo n is not the operation of $\mathbb{Z}$.

Eg:

(i) Find the order of group of element g,

The sequence of product $g, g^2, g^3, \ldots$.

$\therefore g^2 \neq e$. g has infinite order.

(ii) let G be the group in which $(ab)^m = a^m b^m$ for three consective integers and for all $a, b \in G$. The G is abelian.

soln: let $a, b \in G$

let $(ab)^m = a^m b^m$, $(ab)^{m+1} = a^{m+1} b^{m+1}$ and

$(ab)^{m+2} = b^{m+2} b^{m+2}$.

Now $(ab)^{m+1} = a^{m+1} b^{m+1}$.

(ie) $(ab)^m ab = (a^m a)(b^m b)$.

$\Rightarrow (a^m b^m) ab = (a^m a)(b^m b)$.

$b^m a = ab^m$ (by cancellation law).

IIIly $(ab)^{m+2} = a^{m+2} b^{m+2}$.

$\Rightarrow (ab)^{\overline{m+1}+1} = a^{\overline{m+1}+1} b^{\overline{m+1}+1}$

$\Rightarrow b^{m+1} a = ab^{m+1}$

$\Rightarrow bm\ ba = a b^m b$.

$= b^m ab$ by (1)

$\Rightarrow b \cdot a = a \cdot b$ (by cancellation law)

$\therefore G$ is abelian.

(iii) consider $(\mathbb{R}^*, 0)$ form the sequence of the element $2, 2^2, 2^3 \ldots 2^n$.

In this case there is no +ve integers n. such that $2^n = 1$ and (2) (order 2) contains infinite no. of elements.

Subgroup test:

when determing whether or not a subset 'H' of a group which is a subgroup of G one need not directly verify the group. The simple three results provide simple tests that suffers to show that H groups is the subgroup of G.

Thm 3.1 ONE STEP SUBGROUP Test.

let G be a group and if a non-empty subset of G. If ab^{-1} is in H, whenever

a and b are in H is a subgroup of G. (In additive notation if a-b is in H whenever a and b are in H, then H is a subgroup of G).

Proof: Since the operation of H is the same as that of G, it is clear that this operation is associative. Next, we show that e is in H. Since H is nonempty we may pickup some x in H then letting $a = x$ and $b = x$ in the hypothesis, we have $e = xx' = ab^{-1}$ is in H. To verify that x^{-1} is in H whenever x is in H, all we need to do is to choose $a = e$ and $b = x$ in the statement of the thm. Finally the proof will be complete we show that H is closed, that is if x, y belong to H, we most show that xy is in H also well we have already show that y^{-1} is in H whenever y is H, so letting $a = x$ and $b = y^{-1}$ we have $xy = x(y^{-1})^{-1} = ab^{-1}$ is in H.

one-step subgroup test, contains of actually four step involved in applying the thm.

(1) Identify the property P that distinguishes the element of H, That is identity a defining condition

(2) Prove that identity has property P (This verifies it is non-empty).

(3) Assume that 2 element a and b have property P.

(4) Use the assumption that a and b has property P to show that ab^{-1} has property P.

This is illustrated in the below Examples.

Ex: 4 :

let G be the abelian group with identity e The $H = \{x \in G \mid x^2 = e\}$ is a subgroup of G, Here, the defining property of H is the condition $x^2 = e$ so, we first note that $e^2 = e$, so that H is nonempty Now we assume that a and b belong to H. This mean that $a^2 = e$ and $b^2 = e$. Finally we must show that $(ab^{-1})^2 = e$,

since G i, Abelian $(ab^{-1})^2 = ab^{-1}ab^{-1} = a^2(b^2)^{-1}$.

$xec^{-1} = e$. therefore ab^{-1} belongs to H and by the one step - subgroup test H is a subgroup of G.

In many instance a subgroup will consist of all elements that have a particular form then the property p is that the elements have the particular form.

Ex: 5

let G be a abelian group under multiplication with identity e. Then $H = \{x^2 \mid x \in G\}$ is a subgroup of G. (In words, H is the set of all squares in G. since $e^2 = e$, the identity has the correct form next, we write two elements of H in the correct form, say a^2 and b^2. we must Show that $a^2(b^2)^{-1}$ also has the correct form

(ie) $a^2(b^2)^{-1}$ is the square of some element since G is abelian, we may write $a^2(b^2)^{-1}$ as $(ab^{-1})^2$ which is the correct form thus H is the subgroup of G.

Thm 3.2 Two Step subgroup test.

Statement:

Let G be a group and let H be a non-empty subset of G. If ab is in H whenever a and b are in H (H is closed order the operation, H is closed under a inverses. a^{-1} is in H whenever a is in H. Then H is a subgroup of G).

Proof:-

By the thm 3.1 (one step subgroup test), it suffices to show that $a,b \in H$ implies $ab^{-1} \in H$. so we suppose that $a,b \in H$. since H is closed under taking inverses, we also have $b^{-1} \in H$. Thus $ab^{-1} \in H$ by closure under multiplication.

when applying the 2-step subgroup test we proceed exactly as in the case of the one-step subgroup test except we use the assumption that a and b have property p to prove that ab has the property p and that a^{-1} has the property p.

Ex:6

Let G be an abelian group then $H = \{x \in G \mid |x| \text{ is finite}\}$ is a subgroup of G. since $e^1 = e$ $H \neq 0$. To apply the two step subgroup test we assume that a and b belongs to H and prove that ab and a^{-1} belongs to H. Let $|a| = m$.

and $|b| = n$. Then because G is abelian we have $(ab)^{mn} = (a^m)^n (b^n)^m = e^n e^m = e$. Thus ab has finite order moreover, $(a^{-1})^m = (a^m)^{-1} = e^{-1} = e$ shows a^{-1} has finite order.

EX:7

Let G be an abelian group and H and K be subgroups of G. Then $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G. First note that $e = e$ belongs to HK because e is in both H and K. Now suppose that a and b are in HK. Then by defn of H There are element $h_1, h_2 \in H$ and $k_1, k_2 \in K$ such that $a = b_1 k_1$ and $b = h_2 k_2$. We must prove that $ab \in HK$ and $a^{-1} \in HK$. Observe that G is abelian and H and K are subgroup of G we have $ab = h_1 k_1, h_2 k_2 = (h_1 h_2)(k_1 k_2) \in HK$. likewise $a^{-1}(h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} = h_1^{-1} k_1^{-1} \in HK$.

To prove that a subset of a group is not a subgroup, there are three posible ways.

(1) Show that the identity is not in the set

(2) Exhibit an element of the set whose Inverse is not in the set.

(3) Exhibit two element of the set whose product is not in the set.

EX: 8

Let G be the group of non-zero real no's under multiplication $H = \{x \in G / x = 1$ or x is irrational$\}$ and $K = \{x \in G / x \geq 1\}$. Then H is not a subgroup of G. Since $\sqrt{2} \in H$ but $\sqrt{2} \cdot \sqrt{2} = 2 \notin H$

Also K is not a subgroup, since $2 \in K$ but $2^{-1} \notin K$.

Thm : 3.3 Finite subgroup test.

Statement :

Let H be a non-empty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.

Proof :-

In view of thm 3.2 (Two step subgroup test) we need only to prove that $a^{-1} \in H$ whenever $a \in H$

If $a = e$, $a \neq e$ then $a^{-1} = a$ and we are done.

If $a \neq e$ consider the sequence $a, a^2, a^3 \ldots$ By closure all of these element belongs to H. Since H is finite, not of all these element are distinct say $a^i = a^j$ and $i > j$, then $a^{i-j} = e$, since $a \neq e$ $i - j > 1$. Thus, $aa^{i-j-1} = a^{i-j} = e$ and therefore $a^{i-j-1} = a^{-1}$

But $i - j - 1 \geq 1$ implies $a^{i-j-1} \in H$ and hence the thm is proved.

Examples of subgroup :

For any element a from a group, we let $\langle a \rangle$ denote the set $\{a^n / n \in I\}$. In particular the exponents of a includes all negative integers as well as 0 and the +ve integers (a^0 is defined as the identity). This can be proved in the next thm.

Thm 3.4 : $\langle a \rangle$ is a subgroup.

Statement :

Let G be a group and let a be any element of G, Then $\langle a \rangle$ is a subgroup of G.

Proof :

Since $a \in \langle a \rangle$, $\langle a \rangle$ is non-empty.

Let $a^n, a^m \in \langle a \rangle$ Then

$a^n (a^m)^{-1} = a^{n-m} \in \langle a \rangle$ so by one step subgroup test WKT, $\langle a \rangle$ is a subgroup of G.

The subgroup $\langle a \rangle$ is called the cyclic subgroup of G generated by a. In the case that $G = \langle a \rangle$ we say that G is cyclic and a is Generator of G. (A cyclic group have many generators) Notice that although the list $\ldots a^{-2}, a^{-1}, a^0, a^1, a^2 \ldots$ has infinity many entries, the set $\{a^n / n \in I\}$ might have only finitely many elements. Also note that since $a^i a^j = a^{i+j} = a^j a^i$ every

EX:9

In $U(10)$, $\langle 3 \rangle = \{3, 9, 7, 1\} = U(10)$

for $3^1 = 3$, $3^2 = 9$, $3^3 = 7$, $3^4 = 1$, $3^5 = 3^4 \cdot 3 = 1 \cdot 3$, $3^6 = 3^4 \cdot 3^2 = 9$ ... $3^{-1} = 7$ (since $3 \cdot 7 = 1$), $3^{-2} = 9$, $3^{-3} = 3$, $3^{-4} = 1$, $3^{-5} = 3^{-4} \cdot 3^{-1} = 1 \cdot 7$, $3^{-6} = 3^{-4} \cdot 3^{-2} = 1 \cdot 9 = 9$, ...

(7 is the inverse of 3).

EX:10

In $Z10$, $\langle 2 \rangle = \{2, 4, 6, 8, 10\}$ Remember an means na when the operation is addition.

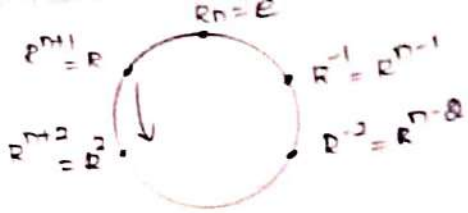
EX:11

In I, $\langle -1 \rangle = I$ Here each entry in the list .... $-2(-1)$, $(-1)(-1)$, $0(-1)$, $1(-1)$, $2(-1)$ --- represents a distinct group of elements.

Examples 12:- In D_n the divided group of order $2n$, let R denote a notation of 360 In degrees Then,

$R^n = R360^\circ = e$, $R^{n+1} = R$, $R^{n+2} = R^2$ ....

IIIly $R^{-1} = R^{n-1}$, $R^{-2} = R^{n-2}$, so that $\langle R \rangle = \{e, R \cdots R^{n-1}\}$ we see then that the proves of the R "cyclic bank" periodically with period n. Visually, raising R to Successive positive power e is the same as moving counterclockwise around the following circle one needs at a time, Whereas raising R to Successive negative powers is the some as moving around the circle Clockwise one nods at a time.



Defn : centre of a group

The centre $Z(G)$ of a group G is the subset of element in G that commute with every element of G. In symbol. $Z(G) = \{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}$

The notation $Z(G)$ comes from the German word for centre is zentrum.

Thm 3.5 centre is a subgroup.

Statement :

The centre of a group G is a subgroup of G.

Proof :

we shall use thm (3.8) [two step subgroup test] to prove that result clearly $e \in Z(G)$, so $Z(G)$ is non-empty, Now suppose $a, b \in Z(G)$. Then $(ab)x = a(bx)$ $= a(xb) = (ax)b$ for all x in G and therefore $ab \in Z(G)$.

Next assume that $a \in Z(G)$. Then we have $ax = xa$ for all x in G what we want $\{a^{-1}x = xa^{-1}\}$ for all x in G. Informally all we need to obtain the 2nd example from the first one is simultaneously to bring the a^{-1}s accross the equal signs.

$$a\overleftarrow{x} = \overrightarrow{xa}$$

becomes $xa^{-1} = a^{-1}x$.

Note that the group need not to be commulatives the a on the left corner across as a^{-1} on the left and the a on the right comes across as a^{-1} on the right - Formally the desired eqns can be obtained from the original one by multiplying it on the left and right by a^{-1} like so,

$$a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$$

$$(a^{-1}a)xa^{-1} = a^{-1}x(aa^{-1})$$

$$exa^{-1} = a^{-1}xe.$$

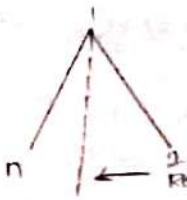
$$xa^{-1} = a^{-1}x$$

This show that $a^{-1} \in Z(G)$ whenever a's.

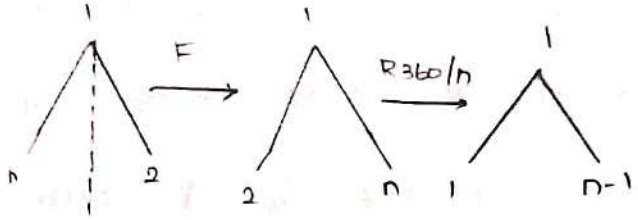
EX: 14 FOR $n \geq 3$

$$Z(D_n) = \begin{cases} \{R_0, R_{180}\} & \text{when } n \text{ is even} \\ \{R_n\} & \text{when } n \text{ is odd.} \end{cases}$$

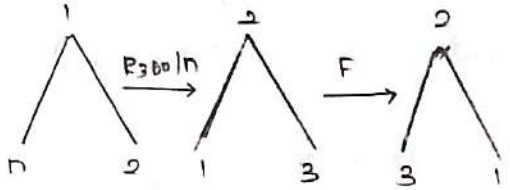
we begin by s.T $Z(D_n)$ cannot contains reflection If its a reflection. There are two possible causes for the reflection axis f.F Either this axis passes through a vertex of n-gon or it joins the midpoints of two opposite sides of n-gon. let's assume first that the axis passes through a vertex label then gon as shown below.



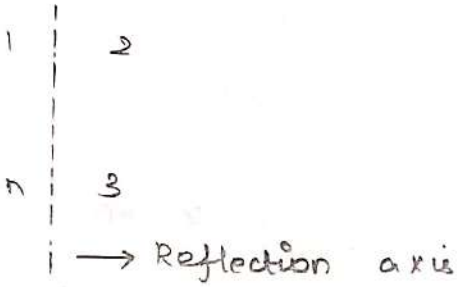
Now $R_{360/n} F$ gives.



whereas $R_{360/n}$ gives.



Thus $R_{360/n} F$ sends vertex 1 to n whereas $FR_{360/n}$ sends vertex 1 to vertex 2, since $n=3$ we have $R_{360/n} F \neq FR_{360/n}$ so that F is not in the centre of D_n A similar arguement on the following diagram rules at reflections that join midpoints of opposite sides (This cases arises when n is even).



we have proved then no reflections is in the centre of D_n. Next consider a rotation $R = R_{k \cdot 360/n}$ $(1 \leq k < n)$ in D_n let's assume that $0 < k \cdot 360/n < 180$ lable the n-gon as shown in the following fig and let F denotes reflectives across the axis passing through vertex 1.

Now FR sends vertex 1 to vertex 2 on the rightside of the reflection axis whereas RF sends vertex 1 to a vertex on the left side of the reflection axis. Thus $FR \neq RF$. A similar argument shows that $FR \neq RF$ when $180^\circ < K\ 360^\circ/n < 360^\circ$. This proves that R_0 and R_{180} are the only possible elements in the centre of D_n series when $n \in S$ odd, D_n has no 180° rotation, and when n is even R_{180} indeed commute with every members of D_n.

Note:

Although an element from an non-abelian group need not necessary commute with every element of the group, there are always some elements with which it will commute. For example every element a commute with all powers of a.

Defn: centralizer of a in G.

Let a be a fixed element of a group G. The centralized of a in G, $C(a)$ is the set of all elements in G that commutes with 'a' In symbol

$$C(a) = \{g \in G / ga = ag\}.$$

Ex: 15.

In D_4 we have the following centralizers

$$C(R_0) = D_4 = C(R_{180}),$$

$$C(R_{90}) = \{R_0, R_{90}, R_{180}, R_{270}\} = C\{R_{270}\},$$

$$C(H) = \{R_0, H, R_{180}, V\} = C(V),$$

$$C(D) = \{R_0, D, R_{180}, D'\} = C(D')$$

C(a) is a subgroup.

For each a in a group G, the centralizer of a is a subgroup of G.

Proof: A proof similar to thm 3.5 (centre of a subgroup)

Note that every element of 'a' of a group G ≥ (G) ≤ C(a)

Also observe that G is a abelian if and only if

$C(a) = G$ for all a in G.

Defn:

let G be a group let $a \in G$, then

$N = \{a^n \mid n \in Z\}$ is a subgroup of G. H is called the cyclic subgroup of G generated by a and its denoted by $\langle a \rangle$.

Proof:

Show that centralizer of a (ie) C(a) is a subgroup of G.

Soln:

clearly $ea = ae = a$.

Hence $e \in C(a)$ so that C(a) is not abelian group

Now let $x, y \in C(a)$ Thus $ax = xa$ and $ay = ya$

Now $ay = ya$

$y^{-1}(ay)y^{-1} = y^{-1}(ya)y^{-1}$

$y^{-1}a(yy^{-1}) = (y^{-1}y)ay^{-1}$

$y^{-1}ae = eay^{-1}$

$\Rightarrow y^{-1}a = ay^{-1}$

Hence $a(xy)^{-1} = (ax)y^{-1}$

$= (xa)\,y^{-1}$

$= x(ay^{-1})$

$= x(y^{-1}a)$

$= (xy^{-1})a$

Hence xy^{-1} commutes with a therefore $xy^{-1} \in C(a)$ and hence $C(a)$ is the subgroup of G.

cyclic group :-

Note :

(i) If G is a cyclic group generated by an element a, then every element of G is of the form a^n for some $n \in I$.

(ii) For any element a from a group, we let $\langle a \rangle$ denote the set $\{a^n \mid n \in I\}$

In particular observe that the exponent of a include of all -ve integers as well as 0 and the +ve integer (a^0 is defined to be the identity)

(iii) In case $G = \langle a \rangle$ we say G is cyclic and a is generator of G.

Defn order of a group :-

The number of element of a group (Infinite or finite) is called its order $|G|$ to denote the order of G.

Defn order of an element :

The order of an element g in a group G is the smallest positive integers n such that $g^n = e$ (In additive notation $ng = 0$) If no such integer exist s, we say g has infinite order. The order of an element g is denoted by $|g|$.

So it to find the order of a group element g, you need only compute the sequence of products $g, g^2, g^3 \ldots$ until you reach the Identity for the first time.

Defn: The division Algorithm for all positive integers a and b where $b \neq 0$ $a = qb + r$ is $a/b = q + r/b$.

'a' divided by b gives a quotient and remainder.

The quotient q and remainder r are $0 \leq r < |b|$.

Ex :

Use the division algorithm to find the quotient and remainders when $a = 158$, $b = 17$

$$a = qb + r$$

$$158 = 9 \times 17 + 5$$

so $q = 9$ $r = 5$

Note $qa = qb$

we say b divides a.

Properties of cyclic group :-

Recall from chapter 3 that a group G is called cyclic. If there is an element a in G such that $G = \{a^n \mid n \in \mathbb{Z}\}$ such an element a is called a generator of G.

The introduced notation in the previous chapter we may indicate that G is a cyclic group generated by a writing

$$G = \langle a \rangle .$$

Ex:1 The set of integers $\mathbb{Z}$ under ordinary addition is cyclic. Both 1 and -1 are generators when the operation is addition I^n is interpreted as

$$\underbrace{1+1+\cdots+1}_{n \text{ terms}}$$

when n is +ve integer and as

$$\underbrace{(-1)+(-1)+\cdots+(-1)}_{|n| \text{ terms}}$$

when n is (-)ve.

Ex:2 The set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ for $n \geq 1$ is a cyclic group under addition modulo n again 1 and $-1 = n-1$ are generators (depending on which n we are given)

Ex:3 $Z_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$ ·To verify for instance that $Z_n = \langle 3 \rangle$ note that $\langle 3 \rangle = \{3, (3+3) \bmod 8, (3+3+3) \bmod 8\}$ is the set $\{3, 6, 9, 4, 7, 2, 5, 0\} = Z_8$

Thus 3 is a generator of Z_8 on the other hand 2 is not a generator since $\langle 2 \rangle = \{0, 2, 4, 6\} \neq Z_8$.

Ex:4 $U(10) = \{1, 3, 7, 9\} = \{3^0, 3^1, 3^2, 3^3\} = \langle 3 \rangle$

Also $\{1, 3, 7, 9\} = \{7^0, 7^3, 7^1, 7^2\} = \langle 7 \rangle$ so both 3 and 7 are generators for $U(10)$.

Quite often in mathematics a "nonexample" is as helpful in understanding a concept as an example. With regard to cyclic group, $U(8)$ serves this purpose; that is $U(8)$ is not a cyclic group ·How we can verify this? well note that $U(8) = \{1, 3, 5, 7\}$ But.

$\langle 1 \rangle = \{1\}$

$\langle 3 \rangle = \{3, 1\}$

$\langle 5 \rangle = \{5, 1\}$

$\langle 7 \rangle = \{7, 1\}$

So that $U(8) \neq \langle a \rangle$ for any a in $U(8)$ with these examples under our belts. we should now be ready to tackle cyclic group in an abstract way and state their key properties.

Thm 4] criterion for $a^i = a^j$.

Let G be a group, let a belong to G. If a has infinite order then all distinct powers of a are distinct group elements. If a has finite order say n then $\langle a \rangle = \{e, a, a^2 \ldots a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i-j$.

Proof:

If a has infinite order there is no non-zero n such that a^n is the identity since $a^i = a^j$ implies $a^{i-j} = e$ we must have $i-j = 0$ and the first statement of the thm is proved.

Now assume that $|a| = n$. we will prove that $\langle a \rangle = \{e, a \ldots a^{n-1}\}$ certainly the elements $e, a \ldots a^{n-1}$ are distinct. For if $a^i = a^j$ with $0 \leq j < i < n-1$ then $a^{i-j} = e$ But this contradicts that fact that n is the least +ve integer such that a^n is the identity.

Now suppose that a^k is an arbitrary member of $\langle a \rangle$ By the division algorithm there exist integers q and r such that

$$k = qn + r \text{ with } 0 \leq r < n$$

Then $a^k = a^{qn+r} = a^{qn} a^r = (a^n)^q . a^r = e a^r = a^r$,

so that $a^k \in \{e, a, a^2 \ldots a^{n-1}\}$. This proves that

divides $i-j$. we begin by observing $a^i = a^j$ implies $a^{i-j} = e$

Again by the division algorithm, there are integers q and r such that

$$i-j = qn+r \quad \text{with} \quad 0 \leq r < n.$$

Then $a^{i-j} = a^{qn+r}$ and therefore $e = ea^r = a^r$ since n is the least +ve integer such that q^n is the identity we must have $r=0$ so that n divides $i-j$

(ie) $i-j = qn$

conversely if n divides $i-j = a^{nq} = e^q = e$ so that $a^i = a^j$.

Collary: $a^k = e$ Implies that $|a|$ divides k.

let G be a group and let a be an element of order n in G. If $a^k = e$ then n divides k.

Proof :-

since $a^k = e = a^0$ wkt by thm 4.1 that n divides $k-0$

By 4.1 In the finite case is that it says that multiplication in $\langle a \rangle$ is essentially done by addition modulo n. That is if $(i+j) \bmod n = k$ then $a^i \cdot a^j = a^k$

Thus no matter what group G is or how the element a is chosen multiplication in $\langle a \rangle$ works the same as addition in $\mathbb{Z}_n$ whenever $|a| = n$ (11/4)

if a has infinite order, then multiplication in $\langle a \rangle$ works the same as addition in $\mathbb{Z}$. since $a^i \, a^j = a^{i+j}$ and no modular arithmetic is done.

Thm 4.2 Generators of cyclic group :-

Let $G = \langle a \rangle$ be a cyclic group of order n Then $G = \langle a^k \rangle$ if and only if $\gcd(k, n) = 1$.

Proof :

If $\gcd(k, n) = 1$, we may write $1 = ku + nv$ for some integers u and v, then $a = a^{ku+nv}$.

Thus a belongs to $\langle a^k \rangle$ and therefore all powers of a belongs to $\langle a^k \rangle$ so $G = \langle a^k \rangle$ and a^k is a generator of G.

Now suppose that $\gcd(k, n) = d > 1$ write $k = td$, $n = sd$ then $\langle a^k \rangle^s = (a^{td})^s = (a^{sd})^t = (a^n)^t = e$, so that $|a^k| \leq s < n$. This show that a^k is not a generator of G.

Taking $G = I_n$ and $a = 1$ in thm 4.2 we have the following useful result.

Ex:1 2 is the generator of I_5^* (Multiplication group) iff $\gcd(2, 5) = 1$.

$I_5^* = \{2, 4, 3, 1\}$ (ie) $2^1 = 2 \pmod 5$

$= \{2^1, 2^2, 2^3, 2^4\}$ $2^2 = 4 \pmod 5$

$2^3 = 3 \pmod 5$

$2^4 = 1 \pmod 5$

hence each element of this group is of the form a^k for some integer k. It follows that the

group I_5 is cyclic with generator 2.

Also $I5 = \{3^1, 3^2, 3^3, 3^4\}$

$= \{3, 4, 2, 1\}$

3 is a generator of I_5.

8) Find the number of generators of the cyclic group of order 8.

let G be a cyclic group of order 8, and let a be a generator of G. Then $a^8 = e$ and we may write $G = \{e, a, a^2, a^3, a^4, a^5, a^6, a^7\}$. we have seen that a^m is also a generator iff m and n are relatively prime to 8. Now the integer 1, 3, 5, 7 are relatively prime to 8. hence all the generators of G are a, a^3, a^5, a^7 which are four in number.

nm 4:3 Fundamental theorem of cyclic group:

Every subgroup of a cyclic group is cyclic moreover if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; for each +ve divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k namely $\langle a^{n/k} \rangle$.

Proof:

let $G = \langle a \rangle$

suppose H is a subgroup of G

If $H = \{e\}$ then clearly H is cyclic

Now claim H > an element a^t form, t is +ve,

Since $G = \langle a \rangle$

when $\forall a^t \in H$, $t < 0$ then $a^{-t} \in H$ and $-t$ is +ve

Thus claim is verified.

Now let $a^m \in H$, m is +ve integer

By closure $\langle a^m \rangle \subseteq H$

Next claim that $H = \langle a^m \rangle$

It suffices to prove that let 'b' be an arbitary number of H.

To S.T 'b' is in $\langle a^m \rangle$

Since $b \in G_1 = \langle a \rangle$

we have $b = a^k$ for some k.

Apply the division algorithm to k and m such that $k = mq + r$ where $0 \leq r < m$ (q, r are integers) then

$a^k = a^{mq+r} = a^{mq} \cdot a^r$

$\Rightarrow a^r = a^{-mq} \cdot a^k$.

$a^{-mq} = (a^m)^{-q} \in H$ [since $a^k = b \in H$]

Also $a^r \in H$ $0 \leq r < m$ but m is least +ve integer thus $a^{-mq}\, a^k = e$.

Therefore $b = a^k = a^{mq} = (a^m)^q \in \langle a^m \rangle$

This proves that every subgroup of a cyclic group is cyclic.

Next suppose $|\langle a\rangle| = n$ H is any subgroup of $\langle a\rangle$

Already shown $\exists\ H = \langle a^m\rangle$ for some m since $(a^m)^n = (a^n)^m = e^m = e$ From corollary "$a^k = e \Rightarrow |a|$ divides n" That $|a^m|$ is a divisor of n. Thus $|H| = |a^m|$ is a divisor of n.

Finally, let k be any divisor of n clearly $(a^{n/k})^k = a^n$

$$(a^{n/k})^k = a^n = e .$$

and $(a^{n/k})^t \neq e$ for any +ve $t < k$,

$\therefore \langle a^{n/k}\rangle$ has order k.

Next show that $\langle a^{n/k}\rangle$ is the only subgroup of order k.

writing $n = mq + r$ where $0 \leq r < m$

$$e = a^n = a^{mq+r} = a^{mq} \cdot a^r \ \&o\ a^r = \bar{a}^{(mq)} = (a^m)^{-q} \in H$$

Thus $r = 0$ (since m is least +ve integer) and

$n = mq$.

$$\text{so } k = |H| = |\langle a^m\rangle| = |\langle (a^m)^{n/m}\rangle| .$$

It follows that $m = n/k$.

and $H = \langle a^m\rangle = \langle a^{n/k}\rangle$.

$\therefore$ If $\langle a\rangle$ has order 30 and 30 divides k, then $\langle a^{30/k}\rangle$ is the unique subgroup of order k.

<u>soln:</u> From thm A·3 subgroups of $\langle a\rangle$ are of the form $\langle a^m\rangle$ where m is a divisor of 30 If k

is a divisor of 30, then subgroup of order k is

$\langle a^{30/k} \rangle$ list of subgroup of $\langle a \rangle$ is

$\langle a \rangle = \{e, a, a^2 \ldots a^{29}\}$ order 30

$\langle a^2 \rangle = \{e, a^2, a^4 \ldots a^{28}\}$ order 15.

$\langle a^3 \rangle = \{e, a^3, e^6 \ldots a^{27}\}$ order 10.

$\langle a^5 \rangle = \{e, a^5, a^{10} \ldots a^{25}\}$ order 6.

$\langle a^6 \rangle = \{e, a^6, a^{12} \ldots a^{24}\}$ order 5

$\langle a^{10} \rangle = \{e, a^{10}, a^{20}\}$ order 3.

$\langle a^{15} \rangle = \{e, a^{15}\}$ order 2.

$\langle a^{30} \rangle = \{e\}$. order 1.

corollary:

subgroups of $\mathbb{Z}_n$.

For each +ve divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order of k Moreover these are the only subgroup of $\mathbb{Z}_n$.

Theorem:

Prove that any cyclic group is abelian.

Proof:

Let $G = \langle a \rangle$ be a cyclic group let $x, y \in$

Thus $x = a^r$ and $y = a^s$ for $r, s \in \mathbb{Z}$

Hence $xy = a^r a^s = a^{r+s}$

$= a^{s+r} = a^s \cdot a^r = yx$

G is abelian.

Theorem :

If H is a subgroup of group G prove that

$aH = bH \Rightarrow a^{-1}b \in H$.

$aH = bH \Leftrightarrow a^{-1}(aH) = a^{-1}(bH)$

$\Leftrightarrow (a^{-1}a)H = H$

$\Leftrightarrow a^{-1}b \in H$.

Let G be a cyclic group of order 6. How many of its element generate G?

Soln:

$G = \{1, a, a^2, a^3, a^4, a^5\}$

$O(G) = 6 \Rightarrow a^6 = 1$ iff $\gcd(a, 6) = 1$.

Here the only generators of G are a and a^5.

∴ The number of generators of a cyclic group of order 6 is 2.

UNIT-4

Rings

Introduction to Rings:

Definition Ring.

A ring R is a set with two binary operations, addition (denoted by a+b) and multiplication (denoted by ab) such that for all a, b, c in R which satisfy the following axioms is called a Ring.

(i) $a+b = b+a$ (R, +) is an ab abelian group

(ii) $(a+b)+c = a+(b+c)$ '·' is an associative binary operation.

(iii) There is an element 0 in R such that $a+0=a$

(iv) There is an element $-a$ in R such that $a+(-a)=0$

(v) $a(bc)$, $(ab)c$

(vi) $a.(b+c) = ab+ac$ and $(b+c)a$, $ba+ca$

Note: 1

a Ring is an abelian under addition, also having an associative multiplication that is left and right distributive over addition.

$a(b+c) = (a+b).c$

Note: 2

The $(I, \cdot)$ has multiplication need not be commutative

Even of a ring has a multiplication identity same elements of the ring may not have multiplication inverses.

For example, The Ring $(Z, +)$ has as a multiplicative identity. and all the elements of Z except 1 and -1 do not have multiplication inverse.

Note: 3

When a ring other than $\{0\}$ has an identity under multiplication then it called ring has a unity (or) identity.

Note: 4

A non zero elements of a commutative ring with unity need not have multiplicative inverse. when it does, that it is a unit of the ring. Thus a is unit of a^{-1} exists.

Definition: divides or factors.

If a and b belong to a commutative ring R and a is non zero, we say that a divides b & (or that a is a is (factor of b) and write a/b. if there exists an element c in R.

$b = a\ell$

If a does not divide b.

write $a \nmid b$.

Examples of Rings :-

Example : 1

The set $\mathbb{Z}$ of integers under ordinary addition and multiplication ring with unity 1. The units of $\mathbb{Z}$ are 1 and -1.

Example : 2

The set $\mathbb{Z}_n = \{0, 1, 2 \cdots n-1\}$ under addition and multiplication modulo n is an commutative ring with unity 1.

Example : 3

The set $\mathbb{Z}[x]$ of all polynomials in the variable x with integer co-efficients under ordinary addition and multiplication is a commutative ring with unity $f(x) = 1$

Example : 4

The set $M_2(\mathbb{Z})$ of 2×2 matrices with integer entries is a non-commutative ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

Example : 5

The set $2\mathbb{Z}$ of even integers under ordinary addition and multiplication is a commutative ring without unity.

Example:6

The set of all continuous real valued functions of a real variable whose group pass through the point $(1,0)$ is a commutative ring without unity under the operations of point wise addition and multiplication

(i.e) The operation $(f+g)a = f(a) + g(a)$

and $(f \cdot g)a = f(a) \cdot g(a)$

Example:7

Let $R_1, R_2 \cdots R_n$ be rings. we can use there to construct a new ring as follows.

Let

$$R_1 \oplus R_2 \oplus \cdots \oplus R_n = \{(a_1, a_2 \cdots a_n) / a_i \in R\}$$

and perform componentwise addition and multiplication

(i) define

$$(a_1, a_2 \cdots, a_n) + (b_1, b_2 \cdots b_n)$$

$$= (a_1 + b_1, a_2 + b_2, \cdots a_n + b_n)$$

$$\text{and } (a_1, a_2 \cdots a_n)(b_1, b_2 \cdots b_n)$$

$$= a_1 b_1, a_2 b_2 \cdots a_n b_n.$$

This ring is called the direct ring of $R_1, R_2 \cdots R_n$.

Properties of Rings:

Theorem: - 1

Rules of multiplication Let a, b and c belong to a ring then

(i) $a0 = 0a = 0$

(2) $a(-b) \cdot (-a)b = -(ab)$

(3) $(-a)(-b) = ab$

(4) $a(b-c) = ab - ac$

and $(b-c)a = ba - ca$

Further more if R has a unity element then

(5) $(-1)a = -a$

(6) $(-1)(-1) = 1$

Proof:

(i) $a0 = a(0+0) = a \cdot 0 + a \cdot 0$

$\therefore a0 = 0$ (by cancellation law in $R,+$)

Illy $0a = (0+0)a$

$= 0a + 0a$

$= 0$

(ii) $a(-b) + ab = a(-b+b)$

$= a(0) = 0$

$a(-b) = -(ab)$

Illy $(-a)b + ab = (-a+a)b = 0$

$(-a)b = -ab$

(iii) by (ii) $(-a)(b) = -[a(-b)]$

$= -[-ab]$

$= ab$

(iv) $a(b-c) = a[b+(-c)]$

$= ab + a(-c)$

$= ab - ac$

Also by $(b-c)a = [b+(-c)]a$

$= ba + (-c)a$

$= ba - ca$

(v) $(-1)a = (-1)a + a + -a$

$= (-1)a + (1)a + -a$

$= (-1+1)a - a$

$= 0 - a$

$= -a$

(vi) We known that -

$-1(0) = 0$

We can write $(-1)0 = (-1)[-1+1]$

Then using distributive property

$= (-1)(-1) + (-1)(1)$

We know that $(-1)(1) = -1$

$0 = (-1)(-1) + (-1)$

$= (-1)(-1) - 1$

$\therefore (-1)(-1) = 1$

Theorem : 12.2

Uniqueness of the unity and Inverse

Of a ring has a unity, it is unique. If a ring element has an inverse, it is unique.

solution:

Let R be a ring with identity ① suppose $a, b \in R$ both satisfy the property of being Unity.

That is for each $r \in R$.

$$ar = ra = r$$

and $$br = rb = r$$

In particular, choosing $r = b$ and using the first equation, we have

$$ab = ba = b$$

$$\Rightarrow ab = b$$

where as choosing $r = a$ and using the second equation. we have

$$ba = ab = a$$

$$\Rightarrow ab = a$$

Thus $b = a$ and so if there is unity of R, it is unique.

We denote such a unity by 1

Let $s \in R$ and suppose $a, b \in R$ both satisfy the properties of being multiplicative inverses of s.

that is

$ra = ar = 1$ and $rb = br = 1$ we want to show that $x = y$

using the equation from the definitions $ar \cdot 1 = br$

But r has a multiplication inverse, namely a. so, multiply each side of a in is equation by a

$$ara = bra$$

By the fact That $ra = 1$ and using associativity, we get the chain of equations.

$$a = a \cdot 1 = a(ra) = ara = bra$$
$$= b(ra)$$
$$= b(1) = b$$

Thus $a = b$ and the multiplication inverse of r is unique.

Definition: Sub ring.

A sub set S of a Ring R is a subring of R if S is itself a ring with the operation of R.

Theorem: 12.3

Subring Test.

A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication that is, if a-b and ab are in S whenever a and b are in S

Proof: Supose S is a subring of R

Then $0_R \in S$ and there is always a solution in S to the equation $a+x=0_R$

In fact, that means solution is unique.

So we can denote it uniquely

$-a \in S$

now we angle agree as follows,

if $a, b \in S$, then $-b \in S$

Hence $a+(-b) \in S$ (since a subring is closed under addition)

Hence $a-b \in S$ (by the definition of subraction)

Since S is a subring it is also closed under multiplication.

We conclude that S must be closed under both subtraction and multiplication

$\Leftarrow$

By hypothesis b, S is closed under

multiplication

To show that S is a subring of R we must show

(i) $0_R \in S$

(ii) Every equation $a + x = 0_R$ has a solution in S

(iii) S is closed under additions

If $a - b \in S$ for all $a, b \in S$ then certainly $0_R \in S$ since $a - a = 0_R$

Since $0_R \in S$, Then for any $a \in S$, $-a \in S$

Since $0_R - a = -a$, must be in S

This is turn implies that the equation $a + x = 0_R$ always has solution in S Also the fact $a \in S \Rightarrow -a \in S$ implies that If $a, b \in S$, then

$a - b \in S$, and so

$a - (b) = a + b \in S$

Then S is closed under addition

Theorem: 3.10

For x, y in R

Proof:-

(i) $x(-y) = -(xy)$

The result is equivalent saying that $x(-y)$ is the negative of xy.

Example: 9

$\{0, 2, 4\}$ is a subring of the ring Z_6. the integers modulo 6

1. Chose under addition

these are all even number in Z_6.

The sum of two even numbers in even. the sum of and we take its remainder need 6, we still get an even number denote under addition

(a) Zero Elements.

$$0+2=2$$
$$0+3=3$$
$$0+6=6$$

(8) Existism of negative

$$-2=4 \quad , -4=2 \quad ,$$

Closed under negative

b) closed under multiplication

$$6 \cdot 0 = 0$$
$$6 \cdot 2 = 12 = 0$$
$$6 \cdot 4 = 24 = 0$$
$$6 \cdot 6 = 36 = 0$$

Example: 8

$\{0\}$ and R are subrings of any ring R. $\{0\}$ is called the trivial subring of R

Example: 9

$\{0, 2, 4\}$ is a subring of the ring Z_6, the integers modulo 6

Example: 10

For each positive integer n, the set

$$nZ = \{0, \pm n, \pm 2n, \pm 3n, \cdots\}$$

is a subring of the integers Z.

Example 11.

The set of Gaussian integers

$$Z[i] = \{a + bi \mid a, b \in Z\}$$

is a subring of the complex numbers C.

Example: 12

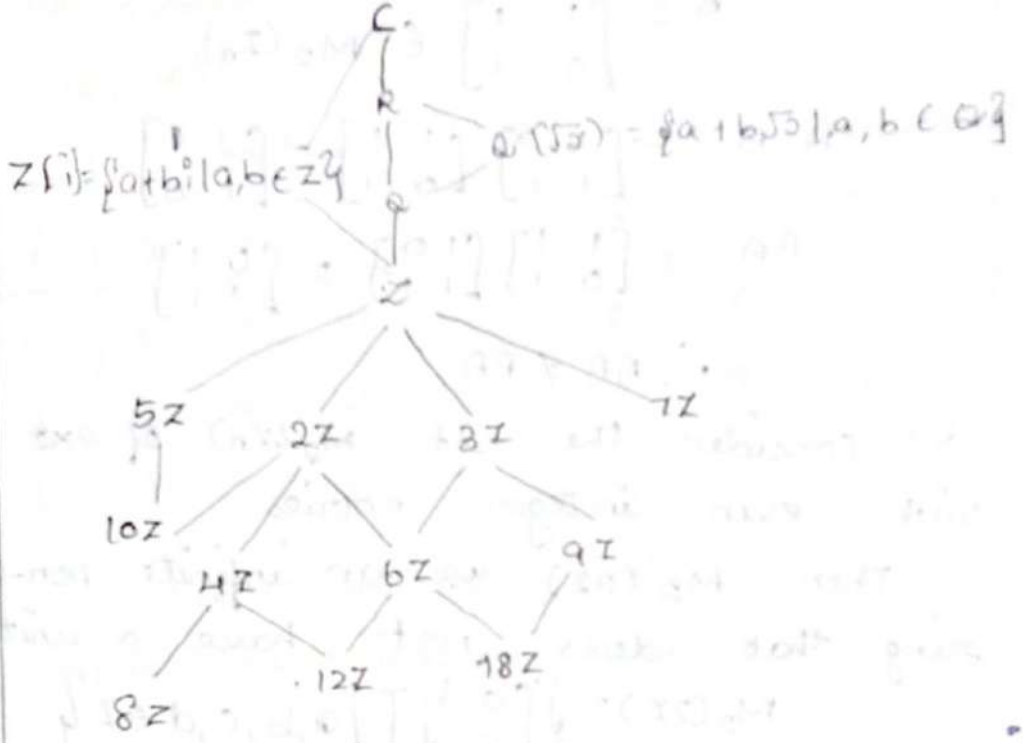
Let R be the ring of all real-valued functions of a single real variable under pointwise addition and multiplication. The subset S of R of functions whose graphs pass through the origin forms a subring of R.

Example: 13

The set $\left\{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in Z\right\}$ of diagonal matrices is a subring of the ring of all 2×2 matrices over Z.

We can picture the relationship between a ring and its various subrings by way of a subring lattice diagram. In such a diagram, any ring is a

subring of all the rings that it is connected by one or more upward lines Figure 10.1 shows the relationship among some of the rings we have already discussed.



In the next several chapters, we will see that many of the fundamental concepts of group theory can be naturally extended to rings. In particular, we will introduce ring homomorphisms and factor rings.

EXERCISE

1) Give an examples of a finite, non-commutative ring, Give an example of an infinite non-commutative ring that does not have a unity.

(i) For any field $n>1$, consider the ring $M_2(Z_n)$ of 2×2 matrices with entries from Z_n.

Then $M_2(Z_n)$ is a finite non-commutative ring $M_2(Z_n) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in Z_n \right\}$

Let us take $n=2$, then

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in M_2(Z_n)$$

$$B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in M_2(Z_n)$$

$$AB = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

$$BA = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

$\therefore AB \neq BA$

(ii) Consider the set $M_2(Z_n)$ of 2×2 matrices with even integer entries.

Then $M_2(2Z)$ is an infinite non-commutative ring that does not have a unity.

$$M_2(2Z) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in Z \right\}$$

$$A = \begin{bmatrix} 2 & 0 \\ 2 & 0 \end{bmatrix} \in M_2(Z_n)$$

$$B = \begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix} \in M_2(Z_n)$$

$$AB = \begin{bmatrix} 2 & 0 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 4 \\ 4 & 8 \end{bmatrix}$$

$$BA = \begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 8 & 4 \\ 4 & 4 \end{bmatrix}$$

$AB \neq BA$

If possible let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be the unity of $M_2(2Z)$

Then we have

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

This gives that

$$2a = 2 \Rightarrow a = 1$$

which contradicts that a is an even integer.

Hence $M_2(2\mathbb{Z})$ does not have any unity.

2) The set $\{0, 2, 4\}$ under addition and multiplication modulo 6 has a unity. Find it.

under addition:

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

under multiplication

•	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

under addition, unity = 0

under multiplication, unity = 4

3) Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. prove that $\mathbb{Z}[\sqrt{2}]$ is a ring under the ordinary addition and multiplication of real numbers.

Let $a+b\sqrt{2}$ and $c+d\sqrt{2} \in R$

$R = \mathbb{Z}[\sqrt{2}]$

$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd) + (cb+ad)\sqrt{2} \in R$

$\therefore R$ is a ring with usual addition and multiplication.

4) Show by the example that for any fixed non zero elements a and b in a ring, The equation $ax = b$ can have more than one solution. How does this compare with groups?

Consider the ring Z_4

Let $a = b = 2$

Then $2(1) = 2$ and $2(3) = 2$

So $2x = 2$

$2x = 2$ has two solutions

This is in contrast to groups where there is only one solution, $x = a^{-1}b$.

5) Prove that a ring can han at most one unity.

Let R be the ring with unity.

suppose $\beta_1, \beta_2 \in R$ both satisfies the properties of being unity.

Then $\forall \alpha \in R$

(i) $\alpha\beta_1 = \beta_1\alpha = \alpha$

(ii) $\alpha\beta_2 = \beta_2\alpha = \alpha$

Hence from (i) and (ii)

$$\alpha\beta_1 = \alpha\beta_2 \Rightarrow \alpha\beta_1 - \alpha\beta_2 = 0$$

$$\alpha(\beta_1 - \beta_2) = 0$$

$\therefore \alpha = 0$ and $\beta_1 - \beta_2 = 0$

If $\alpha = 0$, $\alpha(\beta_1 - \beta_2) = 0 \; (\beta_1 - \beta_2) = 0$

If $\alpha \neq 0$ $\alpha(\beta_1 - \beta_2) \neq \beta_1 - \beta_2 = 0$

$$\beta_1 = \beta_2$$

Hence, A ring can have at most one unity

6) Find an integer n that shows that rings Z_n need not have the following properties that the ring of integers has

a) $a^2 = a$ implies $a = 0$ or $a = 1$

(b) $ab = 0$ implies $a = 0$ or $b = 0$

(c) $ab = ac$ and $a \neq 0$ imply $b = c$

Is the n you found prime?

Let $n = 10$, Hence $Z_n = Z_{10}$

(a) $a^2 = a$ implies $a = 0$ or 1

$Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Let $a = 5$, $a^2 = 5^2$

mod $10 = 25$, mod $10 = 5$

Here, $a^2 = a$

but $5 \neq 0$ and $5 \neq 1$

(b) $ab = 0$ implies $a = 0$ or $b = 0$

Let $a = 5$ and $b = 2$

$ab = 5 \cdot 2$

mod $10 = 10$

mod $10 = 0$

Hence, $ab = 0$

but $5 \neq 0$ and $2 \neq 0$

(c) $ab = ac$ $a \neq 0$ imply $b = c$

Let $a = 2$, $b = 6$ and $c = 1$

$ab = 2 \cdot 6$, mod $10 = 12$, mod $10 = 2$

$ac = 2 \cdot 1$, mod $10 = 2$.

Hence, $ab = ac$ and $a \neq 0$

but $b \neq c$

$\therefore n$ that I have found is not prime

7) show that the three properties in the previous question are valid for Z_p, where p is prime

(a) prove that $a^2 = a$ implies $a = 0$ or $a = 1$

let p be prime.

$a^2 = a$ where $a \in Z_n$

$a^2 - a = 0$

so, $p \mid (a^2 - a) \Rightarrow p \mid a(a-1)$

then $p \mid a$ or $p \mid a-1$

If $p \mid a$, $a < p$

$a = 0$

If $p \mid a-1$, $a - 1 = 0$

$a = 1$

$\therefore a = 0$ and $a = 1$

(b) prove that $ab = 0$ implies $a = 0$ or $b = 0$

Let p be prime.

$ab = 0$ where $a, b \in Z_n$

then $p \mid ab$

$p \mid a$ or $p \mid b$

If $p \mid a$, $a < p$

$a = 0$

If $p \mid b$, $b < p$

$b = 0$

$\therefore a = 0$ or $b = 0$

7) prove that $ab = ac$ and $a \neq 0$ implies $b = c$

Let p be prime

$ab = ac$ where $a, b, c \in Z_N$ and $a \neq 0$

then $ab - ac = 0$

$a(b-c) = 0$

so, $p / a(b-c)$

since $a \neq 0$, $a < p$

$b - c = 0$

$b = c$

$\therefore b = c$

8) show that a ring is commutative if it has the property that $ab = ca$ implies $b = c$ when $a \neq 0$

We need to show that

if $x, y \in$ then $xy = yx$

Let $a = x$

$b = yx$

$c = xy$

$ab = x(yx) = (xy)x = ca$

By the hypothesis,

$b = c$ (or) $xy = yx$

when $a \neq 0$, $b = c$

9) show that a ring that is cyclic under addition is commutative.

$(R, +)$ is a cyclic group

Let $R = \langle x \rangle$; $a, b \in R$

$a = mx$

$b = nx$. where $m, n \in \mathbb{Z}$

Now $ab = mx \cdot nx$

$= (x + x + \cdots + x)(x + x + \cdots + x)$
(m times, n times)

$= mn x^2$

$= nm x^2 = nx mx$

$= ba$

$\therefore ab = ba$

Hence R is a commutative ring.

12) Given an example of non-commutative ring that has 16 elements.

The set of all 2×2 matrices with entries from a field F of 2 elements.

The ring has $2^4 = 16$ elements

$\begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \end{bmatrix}$

$\begin{bmatrix} 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \end{bmatrix}$

But, $\begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \end{bmatrix}$

$\begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \end{bmatrix}$.

$\therefore$ This is a non-commutative ring.

13) Describe all the subrings of the ring of integers.

I is a cyclic group under addition we also know that the subgroup of a cyclic group is also a cyclic group.

$(ma)(nb) + (|m|a)(nb) = ((m+|m|)a)nb = 0$

so that $(ma)(nb) = -(|m|n)(ab) = (mn)(ab)$

If m is positive

Thus A subgroup of $(I, +)$ is of the form, $\langle m \rangle = \{n \cdot m \mid n \in x\}$

$\therefore \langle m \rangle = mx$ is also a subring of I.

14) Show that if m are integers and a and b are elements from a ring; then $(ma)(nb) = (mn)(ab)$

If m or n is zero, Then both sides equal If $m, n \in N$, then

$$\underbrace{(a+a+\cdots+a)}_{m}\underbrace{(b+b+\cdots+b)}_{n} = \underbrace{(ab+\cdots+ab)}_{mn} = (mn)(ab)$$

If m is negative and n is positive.

$(ma)(nb) + (|m|a)(nb) = [|m|n](ab) = (mn)(ab)$

If $(ma)(nb) + (|m|a)(nb) = ((m+|m|)a)nb = 0$

so that $(ma)(nb) = -(|m|n)(ab) = (mn)(ab)$

If m is positive and n is negative,

$(ma)(nb) + (ma)(|n|b) = ma((n+|n|))b = 0$

so that $(ma)(nb) = -(m|n|)ab = (mn)(ab)$

$\therefore (ma)(nb) = (mn)(ab)$

If m, n are negative,

$(ma)(nb) = (-|m|a)(-|n|b) = |mn|ab$

$= (mn)(ab)$

16) Let a and b belong to a ring R and let m be an integer. Prove that $m \cdot (ab) = (m \cdot a)b = a(m$

To prove this statement we must consider 3 cases: $m = 0$, m is negative and m is positive

Case-1: m=0

$m.(ab) = 0(ab) = 0$

$(m.a)b = (0.a)b = 0$

$a(m.b) = a(0.b) = 0$

$\therefore m.(ab) = (m.a)b = a(m.b)$

Case-2: $m < 0$

$m.(ab) = -(ab) + [-(ab)] + \cdots + [-(ab)]$

$= (-a)b + (-a)b + \cdots + (-a)b$

$= \{(a) + (-a) + \cdots + (-a)\}b$

$m.(ab) = (m.a)b$

III by $m.(ab) = a(m.b)$

Case-3: $m > 0$

$m.(ab) = (ab) + (ab) + \cdots + (ab)$

$= (a)b + (a)b + \cdots + (a)b$

$= \{(a) + (a) + \cdots + (a)\}b$

$m.(ab) = (m.a)b$

III by $m.(ab) = a(m.b)$

Since all three cases are met, we say that $m.(ab) = (m.a)b = a(m.b)$ for all integers.

17) prove that the intersection of only collection of subrings of a ring R is a subring of R.

Let A, B be two subrings of R

Let $a, b \in A \cap B$

Then $a, b \in A$ and B

since A and B are subrings $a-b$ and $ab \in$ A and B

$\therefore a-b$ and $ab \in A \cap B$

$\therefore A \cap B$ is subring of R

18) Let a belong to a ring R. Let $S = \{x \in R \mid ax = 0\}$ show that S is a subring of R.

First we must show that S is non-empty $[S \neq \emptyset]$

Let $S = \{x \in R \mid ax = 0\}$

By theorem 12.1,

$$a0 = 0$$

$\therefore 0 \in S$ and $S \neq \emptyset$

Suppose that there exists an arbitrary $x, y \in S$.

Then $ax = ay = 0$

For S to be subring of R, it must be closed under subtraction and multiplication

By theorem 12.1,

$$a(x - y) = ax - ay$$

Both x and y are arbitrary in S,

$$ax - ay = 0 - 0 = 0$$

This is closed under subtraction and $x - y \in S$

By associativity,

$$a(xy) = (ax)y = 0y = 0$$

Hence, it is closed under multiplication and $xy \in S$.

$\therefore$ S is a subring of R.

19) Let R be a ring the center of R is the set $\{x \in R \mid ax = xa$ for all a in $R\}$. Prove that the centre of a ring is a subring.

Clearly 0 is the center since $0x = 0 = x0$ for all $x \in R$. Hence, the center is non-empty.

Let a and b be elements of the center of R.

Then, $(a-b)x = ax - bx = xa - xb = x(a-b)$

So $a-b$ is in the center

III by $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$

so ab is in the center

∴ the center of a ring is a subring

20) Describe the elements of $M_2(\mathbb{Z})$ that have multiplicative inverses.

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an element of $M_2(\mathbb{Z})$

then A has multiplicative inverse if it has non-zero determinant so $ad - bc \neq 0$

The inverse is only in $M_2(\mathbb{Z})$ if $\frac{1}{\det(A)}$ is in $(\mathbb{Z})$.

Thus the determinant of A must be ± 1

Thus the elements with multiplicative inverse are $\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} | ad - bc = \pm 1\}$

29) Let R be a group with unity and let $U(R)$ denote the set of units of R. prove that $U(R)$ is a group under multiplication.

(i) $1 \in U(R)$ so $U(R)$ is non-empty

(ii) Let $a, b \in U(R)$

then a and b have multiplicative inverse in R, a^{-1} and b^{-1} respectively.

Then $(ab)(b^{-1}a^{-1}) = a[b(b^{-1})]a^{-1} = a(1)a^{-1} = aa^{-1} = 1$

III by $(b^{-1}a^{-1})(ab) = 1$

This proves that $b^{-1}a^{-1}$ is the multiplicative inverses i.e of ab.

Hence ab is in U(R)

(iii) If $a \in U(R)$ then obviously its inverse is also invertible and hence in U(R)

From the above,

U(R) is a group under multiplication of R.

22) Determine $U(Z[i])$

An element $x+yi \in I$, the invertible if there exists $a+bi \in I$ such that

$(x+yi)(a+bi) = 1$

consider this equation in the bigger ring C. Then the multiplicative inverse of $x+yi$ would be $\left(\frac{1}{x+yi} = \frac{x-yi}{x^2+y^2}\right)$

$$\frac{1}{x+yi} = \frac{1}{x+yi} \times \frac{x-yi}{x-yi} = \frac{x-yi}{x^2+y^2}$$

$$= \frac{x}{x^2+y^2} - \frac{y}{x^2+y^2} i$$

solutions has integer components, if $\frac{x}{x^2+y^2}$ and $\frac{y}{x^2+y^2} \in C$. both integers.

This happens only when $x^2+y^2=1$

So possibilities are:

$x=1, y=0$, $x=-1, y=0$, $x=0, y=1$ and $x=0, y=-1$.

So invertible elements in Z_i are $\pm 1, \pm i$.

24. If $R_1, R_2, \cdots, R_n$ are commutative rings with unity, show that $U(R_1 \oplus R_2 \oplus \cdots \oplus R_n) = U(R_1) \oplus U(R_2) \oplus \cdots \oplus U(R_n)$

Let 1 denote the unity element in each of the rings R.

So $(1, 1, \ldots 1)$ is the unity element in $R_1 \oplus R_2 \oplus \cdots \oplus R_n$, since if $(a_1, a_2, \cdots a_n)$

$\in R_1 \oplus R_2 \oplus \cdots \oplus R_n$,

&

$$(a_1, a_2, \cdots a_n)(1,1,\cdots,1) = (a_1 \cdot 1, a_2 \cdot 1, \cdots a_n \cdot 1)$$
$$= (a_1, a_2, \cdots, a_n)$$

and

$$(1,1,\cdots,1)(a_1, a_2, \cdots a_n) = (1 \cdot a_1, 1 \cdot a_2, \cdots 1 \cdot a_n)$$
$$= (a_1, a_2, \cdots a_n)$$

Suppose that $(u_1, u_2 \cdots u_n) \in U(R_1 \oplus R_2 \oplus \cdots \oplus R_n)$

Then since the elements unit in the ring $R_1 \oplus R_2 \oplus \cdots \oplus R_n$, this means that there exists an element

$$(x_1, x_2, \cdots, x_n) \in R_1 \oplus R_2 \oplus \cdots \oplus R_n$$

$$(u_1, u_2 \cdots u_n)(x_1, x_2, \cdots, x_n) = (1, 1 \cdots, 1)$$

By definition of multiplication in direct sum of rings,

$$(u_1, u_2, \cdots, u_n)(x_1, x_2, \cdots, x_n) = (u_1 x_1, u_2 x_2, \cdots, u_n x_n)$$
$$= (1, 1, \cdots 1)$$

So, for each i, $1 \leq i \leq n$

$$u_i x_i = 1 = x_i u_i$$

$\therefore x_i \in R_i$ and x_i is the multiplicative inverse of u_i

$$\therefore u_i \in U(R_i)$$

$$(u_1, u_2, \cdots, u_n) \in U(R_1) \oplus U(R_2) \oplus \cdots \oplus U(R_n)$$

$$\therefore U(R_1 \oplus R_2 \oplus \cdots \oplus R_n) \subseteq U(R_1) \oplus U(R_2) \oplus \cdots \oplus U(R_n)$$

To prove the direction containment, suppose that $(y_1, y_2, \cdots y_n) \in U(R_1) \oplus U(R_2) \oplus \cdots \oplus U(R_n)$

This means $y_i \in U(R_i)$. So there exist a $w_i \in R_i$

$$y_i w_i = 1 = w_i y_i$$

$$\therefore (w_1, w_2, \cdots, w_n) \in R_1 \oplus R_2 \oplus \cdots \oplus R_n$$

$$(y_1, y_2, \cdots, y_n)(w_1, w_2, \cdots, w_n) = (y_1 w_1, y_2 w_2, \cdots, y_n w_n)$$

and

$$= (1, 1, \cdots, 1)$$

$(w_1, w_2, \cdots, w_n)(y_1, y_2, \cdots y_n) = (w_1 y_1, w_2 y_2, \cdots, w_n y_n)$

$= (1, 1, \cdots, 1)$

$\therefore w_i$ is the multiplicative inverse of y_i, $y_i \in R_i$

Thus, $(y_1, y_2, \cdots, y_n) \in U(R_1) \oplus U(R_2) \oplus \cdots \oplus U(R_n)$.

$U(R_1) \oplus U(R_2) \oplus \cdots \oplus U(R_n) \leq U(R_1 \oplus R_2 \oplus \cdots \oplus R_n)$

$\therefore U(R_1 \oplus R_2 \oplus \cdots \oplus R_n) = U(R_1) \oplus U(R_2) \oplus \cdots \oplus U(R_n)$

24) Show that a unit of a ring divides every element of the ring.

Let a be a unit in a ring R.

Let x be any element in R.

Then, $x = aa^{-1}x = a(a^{-1}x)$

$a^{-1}x$ also in R.

Hence a divides x.

28) In Z_6, show that $4 | 2$; in Z_8 show that $3 | 7$; in Z_{15} show that $9 | 12$.

We know that $4 | 2$ in Z_6 if there exists $x \in Z_6$ such that $4x = 2$ in Z_6

$4 \cdot 2 = 8 = 2$ in Z_6

111 by

$3 \cdot 5 = 15 = 7$ in Z_8

$9 \cdot 3 = 27 = 12$ in Z_{15}

29) Suppose that a and b belong to a commutative ring R, a is a unit of R and $b^2 = 0$, show that $a+b$ is a unit of R.

Let $ax = 1$

Ring R is a commutative, which implies that

$a^2x^2 = (ax)^2 = (1)^2 = 1$

Now we will prove that a^{th} is unit of R

$(a+b)(a-b) = a^2 - ab + ba - b^2 = a^2 - ab + ab - b^2$

$= a^2 - b^2 = a^2 - 0 = a^2$

This implies that

$(a+b)((a-b)x^2) = 1$

Hence, $a+b \in U(R)$

80) Suppose that there is an integer $n > 1$ such that $a^n = a$ for all element a of some ring. If m is a positive integer and $a^m = 0$ for some a, show that $a = 0$

If $m = n$, then $a = a^n = a^m = 0$

If $n > m$,

$a = a^n = a^m a^{n-m} = 0 \cdot a^{n-m} = 0$

If $n < m$,

$1 < n, m$. So there is an element α such that $n^\alpha > m$

$a^{n^\alpha} = a^{n^\alpha - m} a^m = a^{n^\alpha - m} 0 = 0$

we conclude that it is enough to show that $a^{n^\alpha} = a$, this is easily accomplished by induction on α.

If $\alpha = 1$, Then we are done by hypothesis

So suppose that $\alpha > 1$,

Then $a^{n^\alpha} = (a^{n^{\alpha-1}})^n = (a)^n = a$ by the induction hypotheses. this completes the proof.

81) Give an example of ring elements a and b with the properties that $ab = 0$ but $ba \neq 0$.

Let $R = M_2(I)$

$$a = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$$b = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$ab = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = 0$$

$$ba = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq 0$$

$\therefore ab = 0$ but $ba \neq 0$

82) Let n be an integer greater than 1. In a ring in which $x^n = x$ for all x, show that $ab = 0$ implies $ba = 0$

$$ba = bx^n$$

$$= b \underbrace{ab\,ab \ldots ab}_{(n-1)\text{ terms}} a$$

$$ba = 0$$

$\therefore ab = 0$

84) Let m and n be positive integers and let k be the least common multiple of m and n. Show that $mI \cap nI = kI$.

Let m and n be positive integers

Let k be the least common multiple of m and n.

$kI \subseteq nI$

$kI \subseteq mI$

$\therefore n \mid k$ and $m \mid k$ [$\because aI \subseteq bI$ if and only if $b \mid a$]

So k is a common multiple

$nZ \cap mZ = kI$

35) Explain every subgroup of Z_n under addition is also a subring of Z_n.

Let S is a subring of D.

$\therefore 0 \in S$

$a, b \in S \Rightarrow a-b \in S$ and $ab \in S$

$(S, +)$ is a subgroup

If $S \subseteq R$.

(i) $0 \in S$

(ii) $\forall a, b \in S$, $a-b \in S$

(iii) $\forall a, b \in S$, $ab \in S$

Clearly $S \neq \phi$

By (i),

$(S, +) \subseteq (R, +)$

since S is closed under multiplication by (iii)

$(S, +, \cdot)$ is a subring of $(R, +, \cdot)$

36) Is I_6 is subring of I_{12}?

$I_6 = \{0, 1, 2, 3, 4, 5\}$ is not a subring of I_{12}. since it is closed under addition mod 12 : $5+5=0$ in I_{12} and $10 \notin I_6$.

37) Suppose that R is a ring with unity 1 and a is an element of R such that $a^2 = 1$

Let $S = \{ara \mid r \in R\}$

prove that S is a subring of D. Does S contain 1?

Let ar_1a and $ar_2a \in S$

subring test

(i) $ar_1a - ar_2a = a(r_1 - r_2)a \in S$

(ii) $ar_1a\,ar_2a = ar_1r_2a \in S$

Thus, S is a subring and contains one because,

$a\,1a = a^2 = 1$

10) Let $R = \left\{\begin{bmatrix} a & a \\ b & b \end{bmatrix} \mid a, b \in Z\right\}$, prove or disprove that R is a subring of $M_2(Z)$.

It is clear that $R \subseteq M_2(Z)$ since R contains the zero matrix

$\therefore$ R is non-empty.

Let $A = \begin{bmatrix} a & a \\ b & b \end{bmatrix}$, $C = \begin{bmatrix} c & c \\ d & d \end{bmatrix}$ be matrices in R

$$A - B = \begin{bmatrix} a-c & a-c \\ b-d & b-d \end{bmatrix} \in R$$

since the integers are closed under subtraction additionally,

$$AC = \begin{bmatrix} ac+ad & ac+ad \\ bc+bd & bc+bd \end{bmatrix}$$

$ac+ad$ and $bc+bd \in Z$

$AC \in R$

Since C is closed under subtraction and multiplication.

R is a subring.

11) Let $R = Z \oplus Z \oplus Z$ and $S = \{(a,b,c) \in R \mid a+b=c\}$ prove or disprove that S is a subring of R.

S is contained in R and S is non-empty let $x = (a,b,c)$ and $y = (d,f,g) \in S$. $x - y = (a,b,c) - (d,f,g) = (a-d, b-f, c-g)$

$x, y \in S$

$a+b=c$ and $d+f=g$

Now, $(a-d)+(b-f)=(a+b)-(d+f)=c-g$ so $x-y \in S$

Now, consider the condition for,

$xy=(ad, bf, cg)$

$e.g. \quad =(a+b)(d+f)=ad+bf+af+bd$

So xy is in S only if $af+bd=0$

By the above,

$\therefore S$ is not a subring of R.

H3) Show that $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subring of $\mathbb{Z}$.

The set $2\mathbb{Z} \cup 3\mathbb{Z}$ consis of integer multiples of 2 and integer multiples of 3.

In order to be a ring,

the set is must be closed under addition and multiplication.

However, $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$

but $2+3 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$

$\therefore 2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subring of $\mathbb{Z}$.

H5) Determine the smallest subring of $\mathbb{Q}$ contains $\frac{1}{2}$, (That is, Find the subring S with the property that S containing $\frac{1}{2}$ then T contains S)

The smallest subgroup $\mathbb{Q}$ which contains $\frac{1}{2}$ is cyclic group $\langle \frac{1}{2} \rangle = \left\{ \frac{m}{2} \mid m \in \mathbb{Z} \right\}$

But any subring containg $\frac{1}{2}$ must also contain elements $\frac{1}{2^n}$, for $n \in \mathbb{N}$.

Thus, the smallest subring of $\mathbb{Q}$ containing $\frac{1}{2}$ is set,

$$\left\{\frac{m}{2^n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\right\}$$

47) Let R be a ring, prove that $a^2 - b^2 = (a+b)(a-b)$ for all a, b in R if and only if R is commutative.

$$a^2 - b^2 = (a+b)(a-b)$$

$$(a+b)(a-b) = (a+b)a - (a+b)b$$

$$= aa + ba - ab - bb$$

$$= aa + ab - ab - b^2$$

$(a+b)(a-b) = a^2 - b^2$ if R is commutative.

48) Suppose that R is a ring that $a^2 = a$ for all a in R, show that R is commutative (Note: such a ring is called a Boolean ring)

Let R be a ring such that $a^2 = a$ for all $a \in R$.

we notice that $a+b = (a+b)^2 = a^2 + b^2 + ab + ba$

Thus $ab + ba = 0$

or $ab = -ba$

$-ba = (-ba)^2 = (ba)^2 = ba$

so $ab = ba$ and

R is commutative.

49) Given an example of a Boolean ring with four elements. Give an example of an infinite Boolean ring.

Let $B = \mathbb{Z}_2 = \{0, 1\}$

such that $0 + 0 = 0$

Then B is Boolean ring with 2 elements, and B⊕B is a Boolean ring with 4 elements. Let $R = B^{\infty} = \{(a_1, a_2, \cdots) \mid a_i \in B$ for each $i\}$. Then R Boolean ring with infinitely many elements

50) Give an example of a subset of a ring that is a subgroup under addition but not a subring.

Let $R = C$

$S = \{ix : x \in R\}$

$0 \in S$ and $a - b \in S$, $\forall a, b \in S$

But $i, i = -1 \notin S$

∴ It is not a subring.

Integer Domains

Definition - Zero-divisors:

A zero-divisor is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$

Definition: Integer Domain

An integral domain is a commutative ring with unity and no zero-divisors.

Example:-

(1) The integers Z are an integral domain.

(2) The Gaussian integers $Z[i] = \{a + bi \mid a, b \in Z\}$ is an integral domain.

5) The ring $Z[x]$ of polynomials with integral domain.

4) $Z[\sqrt{3}] = \{a+b\sqrt{3} \mid a, b \in Z\}$ is an integral domain.

5) For p prime, Z_p is an integral domain. The proof for this is in the corollary to Theorem 13.2, which follows later. For n not prime, the ring Z_n is not an integral domain.

6) $M_2(Z)$ is not an integral domain since

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

7) $Z \oplus Z$ is not an integral domain since $(1,0)(0,1) = (0,0)$.

Theorem :- 13.1

Let D be an integral domain with $a, b, c \in D$. If $a \neq 0$ and $ab = ac$, then $b = c$.

Proof :-

$$ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0$$

Since $a \neq 0$, $b - c = 0 \Rightarrow b = c$.

Fields :-

Definition :

A field is a commutative ring with identity in which every nonzero element is a unit.

Corollary :-

A field is an integral domain

Proof:-

Suppose $a \neq 0$ and $ab = 0$. Since $a \neq 0, a^{-1}$ exists and

$$a^{-1}ab = a^{-1}0 \Rightarrow 1b = 0 \Rightarrow b = 0$$

∴ Thus we have an integral domain.

NOTE:

One can think of ab^{-1} as $\frac{a}{b}$ in the same way we think of $a + (-b) = a - b$.

In a field, addition, subtraction, multiplication, and division (except by 0) are closed.

Example:- $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are fields.

Theorem: 13.2

A finite integral domain D is a field.

Proof:-

Let $a \in D, a \neq 0$. If $a = 1, a^{-1} = 1$ and a is a unit, so suppose $a \neq 1$.

Consider the following sequence of elements of D: $a, a^2, a^3, \ldots$ since D is finite, $\exists\, i, j \in \mathbb{N}$ with $i > j$ and $a^i = a^j$.

By cancellation, $a^{i-j} = 1$. Since $a \neq 1$, $i - j > 1$

$\Rightarrow a^{i-j-1} = a^{-1}$, Thus a is a unit. Since a was arbitrary, D is a field.

Corollary

For p prime, $\mathbb{Z}_p$ is a field

Proof:

Suppose $a, b \in \mathbb{Z}_p$, and $ab = 0$ then $ab = pk$ for some $k \in \mathbb{Z}$. By Euclid's Lemma, $p|a$ or $p|b \Rightarrow a \equiv 0 \bmod p$ or $b \equiv 0 \bmod p \Rightarrow a = 0$ or $b = 0$. Thus $\mathbb{Z}_p$ is an integral domain, and so is also a field by Theorem 13.2.

EXAMPLE:

Let $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$. That $\mathbb{Q}[\sqrt{3}]$ is a commutative ring with identity is fairly clear. Suppose $a + b\sqrt{3} \neq 0$ then $a - b\sqrt{3} \neq 0$ also since $a \neq 0$ or $b \neq 0$ with $a + b\sqrt{3}$ viewed as an element of the superset $\mathbb{R}$,

$$(a+b\sqrt{3})^{-1} = \frac{1}{a+b\sqrt{3}} = \frac{1}{a+b\sqrt{3}} \cdot \frac{a-b\sqrt{3}}{a-b\sqrt{3}} =$$

$$\frac{a-b\sqrt{3}}{a^2-3b^2} = \frac{a}{a^2-3b^2} - \frac{b}{a^2-3b^2}\sqrt{3} \in \mathbb{Q}[\sqrt{3}].$$

Thus $a + b\sqrt{3}$ is a unit and $\mathbb{Q}[\sqrt{3}]$ a field.

EXAMPLE:

$\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\} = \{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$, $i^2 = -1$, the ring of Gaussian integers modulo 3 is a field, with the multiplication table for the nonzero

elements below.

	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
1	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
2	2	1	$2i$	$2+2i$	$1+2i$	i	$2+i$	$1+i$
i	i	$2i$	2	$2+i$	$2+2i$	1	$1+i$	$1+2i$
$1+i$	$1+i$	$2+2i$	$2+i$	$2i$	1	$1+2i$	2	i
$2+i$	$2+i$	$1+2i$	$2+2i$	1	i	$1+i$	$2i$	2
$2i$	$2i$	i	1	$1+2i$	$1+i$	2	$2+2i$	$2+i$
$1+2i$	$1+2i$	$2+i$	$1+i$	2	$2i$	$2+2i$	i	1
$2+2i$	$2+2i$	$1+i$	$1+2i$	i	2	$2+i$	1	$2i$

NOTE :-

For any $x \in I_3[i]$, $3x = x+x+x = 0 \bmod 3$.

In the subring $\{0, 4, 8, 12\}$ of Z_{12},

$4x = x+x+x+x = 0$

Characteristic of a Ring:

Definition :-

The characteristic of a ring R is the least positive integer n such that $nx = 0$ for all $x \in R$. If no such integer n exists, we say R has characteristic 0. The characteristic of R is denoted as Char R.

EXAMPLE :-

I has characteristic 0. I_n has characteristic n, and char $Z_2[x] = 2$ an infinite, ring with a non zero characteristic.

THEOREM: 13·3

Let R be a ring with unit 1. If 1 has infinite order under addition, then char R = 0. If 1 has order n under addition, then char R = n.

PROOF:-

If |1| = ∞, n ≠ n·1 = 0, so char R = 0

suppose |1| = n. Then n·1 = 0 and n is the least positive integer with this property Then, for all x ∈ R,

$$n \cdot x = \underbrace{x + x + \cdots + x}_{n \text{ terms}} = \underbrace{1x + 1x + \cdots + 1x}_{n \text{ terms}} = \underbrace{(1 + 1 + \cdots + 1)}_{n \text{ terms}} x$$

$$= 0x = 0$$

Thus char R = n.

LEMMA:-

If m, n ∈ Z and a, b ∈ R, a ring, then $(m \cdot a)(n \cdot b) = (mn) \cdot (ab)$.

Proof:-

For m, n > 0,

$$(m \cdot a)(n \cdot b) = \underbrace{(a + a + \cdots + a)}_{m \text{ terms}} \underbrace{(b + b + \cdots + b)}_{n \text{ terms}} =$$

$$\underbrace{(ab + ab + \cdots + ab)}_{mn \text{ terms}} = (mn) \cdot (ab)$$

The other cases are similar.

THEOREM: 13·4

If D is an integral domain, then char D = 0 or char D is prime.

Proof:-

Suppose the additive order of 1 is

finite. Suppose $|1| = n$ and $n = st$ with $1 \le s, t \le n$. Then, by the Lemma, $a = n \cdot 1 = (st) \cdot (1) = (s \cdot 1)(t \cdot 1)$. Thus $s \cdot 1 = 0$ or $t \cdot 1 = 0$.

Since n is the least positive integer such that $n \cdot 1 = 0$, $s = n$ or $t = n$. Thus, n is prime.

NOTE:-

In high school algebra, we learned to solve polynomial equations like $x^2 - 5x + 6 = 0$ by first factoring the left side to get $(x-3)(x-2) = 0$ and then setting each factor equal to 0 to get $x - 3 = 0$ and $x - 2 = 0$, and thus $x = 3$ and $x = 2$ as the solution set.

But suppose we try to solve the same equation in Z_{12}. We do get 2 and 3 as solutions just as above. But now $x = 6$ is also a solution that we cannot find by factoring.

$$(6-3)(6-2) = 3 \cdot 4 = 12 = 0 \bmod 12.$$

The issue is that Z_{12} is not an integral domain. We can be sure that the factoring method gives us all the solutions of a polynomial equation only if we know we are working in an integral domain.

Following is a table of some of the rings and their properties.

Summary of Rings and their properties:-

Ring	Form of Element	Unity	commutative	Integral Domain	Field	Characteristic
$\mathbb{Z}$	k	1	Yes	Yes	No	0
Z_n, n composite	k	1	Yes	No	No	n
Z_p, p prime	k	1	Yes	Yes	Yes	p
$\mathbb{Z}[x]$	$a_n x^n + \cdots + a_1 x + a_0$	$f(x) = 1$	Yes	Yes	No	0
$n\mathbb{Z}$, $n > 1$	nk	None	Yes	No	No	0
$M_2(\mathbb{Z})$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	No	No	No	0
$M_2(2\mathbb{Z})$	$\begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix}$	None	No	No	No	0
$\mathbb{Z}[i]$	$a+bi$	1	Yes	Yes	No	0
$Z_3[i]$	$a+bi$; $a,b \in Z_3$	1	Yes	Yes	Yes	3
$\mathbb{Z}[\sqrt{2}]$	$a+b\sqrt{2}$; $a,b \in \mathbb{Z}$	1	Yes	Yes	No	0
$\mathbb{Q}[\sqrt{2}]$	$a+b\sqrt{2}$; $a,b \in \mathbb{Q}$	1	Yes	Yes	Yes	0
$\mathbb{Z} \oplus \mathbb{Z}$	(a,b)	$(1,1)$	Yes	No	No	0

section 14. Ideals and Factor Rings.

Definition: Ideal

A subring A of a ring R is called (two-sided) an ideal of R if for every $r \in R$ and every $a \in A$ both ra and ar are in A.

A subring A of a ring R is an ideal of R if A "absorbs" elements from R that is, if $rA \subseteq A$ and $Ar \subseteq A$ for all $r \in R$.

An ideal A of R is called a proper ideal of R if A is a proper subset of R.

Theorem 14.1 (Ideal Test)

A nonempty subset A of a ring R is an ideal of R if

1. $a - b \in A$ whenever $a, b \in A$
2. ra and ar are in A whenever $a \in A$ and $r \in R$.

Example: 1

For any ring R {0} and R are ideals of R. The ideal {0} is called the trivial ideal.

Example: 2 For any positive integer n, the set $nZ = \{0, \pm n, \pm 2n, \ldots\}$ is an ideal of Z.

Example: 3

Let R be commutative ring with unity and let $a \in R$. The $\langle a \rangle = \{ra / r \in R\}$ is an ideal of R called the principal ideal generated by a. ~~the assumption that R is commutative is necessary~~

Example: 4.

Let R[x] denote the set of all polynomials with real co-efficient and let A denote the subset of all polynomials with Constant term 0. Then A is an ideal of R[x] and $A = \langle x \rangle$.

Example: 5

Let R be a commutative ring with unity and let $a_1, a_2 \ldots a_n$ belong to R. Then $I = \langle a_1, a_2 \ldots a_n \rangle = \{r_1a_1 + r_2a_2 + \ldots + r_na_n\}$ $= r_i \in R$ is an ideal

of R called the ideal $\langle a_1, a_2 \cdots a_n \rangle$.

Example : 6.

Let $Z[x]$ denote the ring of all polynomials with ~~even~~ Constant ~~term~~ integer co-efficients and let I be the subset of $Z[x]$ of all polynomials with even constant term. Then I is an ideal of $Z[x]$ and $I = \langle x, 2 \rangle$.

Example : 7

Let R be the ring of all real valued functions of real variable. The subset S of all differentiable functions is a subring of R.

FACTOR Rings

Let R be a ring and let A be an ideal of R. Since R is a group under addition and A is a normal subgroup of R, we may form the factor group

$R/A = \{r + A / r \in R\}$.

Theorem 14.2. Existence of Factor Rings.

Let R be a ring and let A be a subring of R. The set of cosets $\{r+A \mid r \in R\}$ is a ring under the operation $(s+A)+(t+A) = s+t+A$ and $(s+A)(t+A) = st+A$ if and only if A is an ideal of R.

Proof:

Let us suppose that A is an ideal and let $s+A = s'+A$ and $t+A = t'+A$

Then we must show that

$$st+A = s't'+A.$$

By definition, $s = s'+a$ and $t = t'+b$.

where a and b belong to A. Then

$$st = (s'+a)(t'+b)$$

$$= s't'+s'b+at'+ab.$$

Adding both side by A.

$$st+A = s't'+at'+s'b+ab+A$$

$$= s't'+A.$$

since A absorbs the last three summands of the middle expression.

$\therefore$ multiplication is well defined when A is an ideal.

On the other hand, suppose that A is a subring of R

ie) not an ideal of R.

Then there exist element $a \in A$ and $r \in R$

$\Rightarrow ar \notin A$ or $ra \notin A$. (say $ar \notin A$).

Consider the elements

$a+A = 0+A$ and $r+A$.

clearly, $(a+A)(r+A) = ar+A$

but $(0+A)(r+A) = 0 \cdot r + A = A$

$(\because ar+A \neq A)$.

$\therefore$ Multiplication is not well defined

$\therefore$ The set of cosets is not ring.

Example: 8

$Z/4Z = \{0+4Z, 1+4Z, 2+4Z, 3+4Z\}$.

To see how to add and multiply,

consider $2+4Z$ and $3+4Z$.

$(2+4Z)+(3+4Z) = 5+4Z = 1+4+4Z = 1+4Z$

$(2+4Z)(3+4Z) = 6+4Z$

$= 2+4+4Z$

$= 2+4Z$.

Prime Ideals and Maximal Ideals.

Definition: Prime Ideal, Maximal Ideal.

* A proper ideal A of a commutative ring R is said to be prime ideal of R if $a, b \in R$ and $ab \in A$

$\Rightarrow a \in A$ (or) $b \in A$.

* A proper ideal A of R is said to be a maximal ideal of R. if, whenever B is an ideal of R such

$\Rightarrow A \subseteq B \subseteq R$

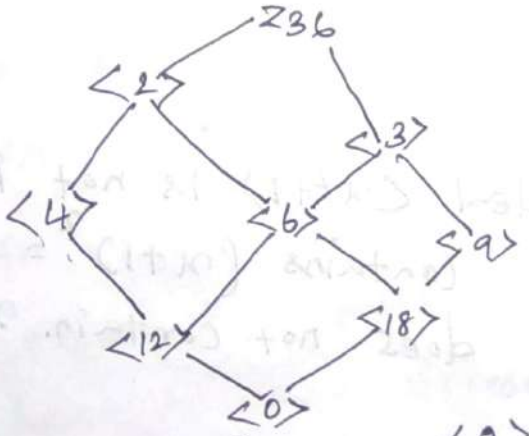
Then $B = A$ (or) $B = R$.

Example: 13

Let n be a positive integer. Then in the ring of integers, the ideal $n\mathbb{Z}$ is prime if and only if n is prime.

Example: 14.

The lattice of ideals of $\mathbb{Z}_{36}$



In this figure $\langle 2 \rangle$ and $\langle 3 \rangle$ are maximal ideals.

Example : 15

The ideal $\langle x^2+1 \rangle$ is maximal in $R[x]$

To see this, assume that A is an ideal of $R[x]$ that properly contains $\langle x^2+1 \rangle$. We will P.T $A = R[x]$. (∵ A contains some non-zero real number c.)

~~Then $1 = (1/c)c \in A$~~

Let $f(x) \in A$, but $f(x) \notin \langle x^2+1 \rangle$. Then

$$f(x) = q(x)(x^2+1) + r(x).$$

where $r(x) \neq 0$ and degree $r(x) < 2$.

It follows that $r(x) = ax+b$.

where a and b are not both 0 and

$$ax+b = r(x)$$
$$= f(x) - q(x)(x^2+1) \in A.$$

Thus,

$a^2x^2 - b^2 = (ax+b)(ax-b) \in A$ and $\{a^2(x^2+1)\} \in$

So, $0 \neq a^2+b^2 = (a^2x^2+a^2) - (a^2x^2-b^2) \in A.$

Example : 16

The ideal $\langle x^2+1 \rangle$ is not Prime in $Z_2[x]$ since it contains $(x+1)^2 = x^2+2x+1$ $= x^2+1$ but does not contain $x+1$.

Theorem 14.3

R/A is an Integral domain if and only if A is Prime.

Statement:

Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is an integral domain if and only if A is prime.

Proof:

Suppose that R/A is an integral domain and $ab \in A$. Then

$$(a+A)(b+A) = ab+A$$
$$= A.$$

Then R/A is zero elements. So either $a+A = A$ (or) $b+A = A$.

ie) $a \in A$ (or) $b \in A$.

Hence A is prime.

On the other hand, we first observe that R/A is a commutative ring with unity for any proper ideal A.

To show that when A is prime, R/A has no zero-divisors.

suppose that A is prime and

$(a+A)(b+A) = 0+A$

$= A.$

Then $ab \in A$ and $\therefore a \in A$ (or) $b \in A$.

$\therefore a+A$ (or) $b+A$ is the zero coset in R/A.

Hence the proof.

Theorem 14.4 R/A is a field if and only if A is maximal.

Statement:

Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is a field iff and only if A maximal.

Proof:

suppose that R/A is a field and B is an ideal of R.

Let $b \in B$ but $b \notin A$.

Then $b+A$ is nm2ero element of R/A.

Then their exist an element $c+A$

$\ni (b+A)(c+A) = 1+A$. (Multiplicative identity R/A).

since $b \in B$, we have $bc \in B$, because

$$\Rightarrow 1+A = (b+A)(c+A) = bc+A$$

$$\therefore 1+A = bc+A$$

$$\Rightarrow 1-bc \in A \subset B \quad (\because bc \in B)$$

$$\therefore 1 = (1-bc) + bc \in B.$$

$\therefore B = R$ ($\because B$ is an ideal in R)

hence A is maximal.

On the other hand,

suppose that A is maximal and let $b \in R$ but $b \notin A$.

To show that $b+A$ has a multiplicative inverse.

Consider $B = \{br+a / r \in R, a \in A\}$.

This is an ideal of $R \subset A$.

since A is Maximal.

$\therefore B = R$.

Thus $1 \in B$ say, $1 = bc + a'$

where $a' \in A$. Then

$$1+A = bc+a'+A$$

$$= bc+A$$

$$1+A = (b+A)(c+A)$$

Example 17

The ideal $\langle x \rangle$ is a Prime ideal in $\mathbb{Z}[x]$ but not a maximal ideal in $\mathbb{Z}[x]$.

To verify this,

we begin with the observation that

$$\langle x \rangle = \{ f(x) \in \mathbb{Z}[x] / f(0) = 0 \}.$$

Thus, if $g(x)h(x) \in \langle x \rangle$.

Then $g(0)h(0) = 0$. $\{ \because g(0) \& h(0)$ integers$\}$.

we have $g(0) = 0$ (or) $h(0) = 0$.

To see that $\langle x \rangle$ is not maximal. simply note that $\langle x \rangle \subset \langle x, 2 \rangle \subset \mathbb{Z}[x]$.