Ex:→ How many errors can be corrected by (3,4) parity check code?

Sol":→ Since the distance between any two code words in (3,4) parity check code is two, so according to the minimum distance decoding criterion, it can correct zero errors. i.e. it can't correct any errors.

Group codes:→

A class of block codes is known as group codes.

A subset G of A is called a group code if $(G, \oplus)$ is a subgroup of $(A, \oplus)$, where A is the set of binary sequences of length n.

Now let us see how the distance of G is equal to the minimum weight of the nonzero words in G. This results makes it much easier to compute the distance of a group code since it is no longer necessary to compute the distance between every pair of distinct words in G exhaustively.

Suppose x is a non-zero word in G.

Since $w(x) = d(x, 0)$

& since 0 is in G, we have

$$w(x) \geq \min_{y,z \in G} [d(y,z)] \quad \text{---(1)}$$

On the other hand for any $y, z \in G$.

Since $d(y,z) = w(y \oplus z)$

& since $(y \oplus z) \in G$

we have

$$d(y,z) \geq \min_{\substack{x \in G \\ x \neq 0}} [w(x)] \quad \text{---(2)}$$

From (1) we obtain

$$\min_{\substack{x \in G \\ x \neq 0}} [w(x)] \geq \min_{y,z \in G} [d(y,z)] \quad \text{---(3)}$$

From (2) we obtain

$$\min_{y,z \in G} [d(y,z)] \geq \min_{\substack{x \in G \\ x \neq 0}} [w(x)] \quad \text{---(4)}$$

Combining (3) & (4) we obtain

$$\min_{\substack{x \in G \\ x \neq 0}} [w(x)] = \min_{y,z \in G} [d(y,z)]$$

~~let G~~

Let $(G, \oplus)$ be a group code.

Let y be a received word.

Since $d(x_i, y) = w(x_i \oplus y)$,

the weights of the words in the coset $G \oplus y$ are the distances between the codewords in G & y.

Let e denote the word of smallest weight in $G \oplus y$.

Let $e = x_j \oplus y$ where $x_j \in G$.

According to minimum distance decoding criterion, $e \oplus y = x_j$ is the transmitted codeword.

Since this argument is valid for all y in the coset $G \oplus y$, our decoding procedure can be stated as:

(1) Determine all cosets of G.

(2) For each coset, pick the word of the smallest weight, which we shall refer to as the leader of the coset.

(3) For a received word y, $e \oplus y$ is the transmitted word, where e is the leader of the coset containing y.

Ex:- let code $C = \{1100110, 0011010, 0001001\}$.

Find the error correction & error detection capabilities of the code C.

Sol^n:- Since $d_{min}(C) = 3$,

we have $t+1 = 3 \Rightarrow t = 2$.

Hence C can ~~correct~~ detect upto two errors.

And according to minimum distance decoding criterion. Code C can correct upto $2k+1 = 3$

$\Rightarrow k = 1$ error.

Here C can correct one error.

Isomorphism of groups

A mapping f of G into G' is said to be an isomorphic mapping of G into G' if

(i) f is one-to-one

i.e. distinct elements in G have distinct f-images in G'.

(ii) $f(ab) = f(a)f(b)$

$\forall\ a, b \in G$.

i.e. the image of the product is the product of the images.

If f is an isomorphic mapping of a group G onto G', then f is also called an isomorphism of G into G'.

If G is isomorphic to the group G' symbolically we write

$$G \cong G'.$$

Note: (1) If G is isomorphic to G', there may exist more than one isomorphism of G onto G'.

There may be many one-one onto funct^n from G to G'.

But if $\exists$ at least one funct^n f which is one-one, onto & also preserves compositions, then G will be isomorphic to G'.

(2) If the group G is finite, then G can be isomorphic to G' only if G' is also finite & the number of elements in G equal to the number of elements in G'. Otherwise there will exist no mapping f from G to G' which is one-one as well as onto.

Ex:→ Show that the additive group of integers

$$G = \{\cdots -3, -2, -1, 0, 1, 2, 3 \cdots\}$$

is isomorphic to the additive group.

$$G' = \{\cdots -3m, -2m, -1m, 0, 1m, 2m, 3m \cdots\}$$

where m is any fixed integer not equal to zero.

Soln:→ If $x \in G$, then $mx \in G'$

Let $f : G \to G'$ be defined by

$$f(x) = mx \quad \forall x \in G.$$

If is one-to-one.

As: Let $x_1, x_2 \in G$ Then

$$f(x_1) = f(x_2)$$

$$\Rightarrow mx_1 = mx_2$$

$$\Rightarrow x_1 = x_2$$

$\therefore$ f is one-to one.

Suppose y is any element of G'.

Then obviously $y/m \in G$

Also $f(y/m) = m(y/m) = y$

Thus $y \in G'$.

$\Rightarrow \exists\ y/m \in G$ s.t. $f(y/m) = y$.

$\therefore$ Each element of G' is the f-image of some element of G.

Hence f is onto.

Again if x_1 & x_2 are any two elements of G, then

$$f(x_1 + x_2) = m(x_1 + x_2)$$

$$= mx_1 + mx_2 \quad [\text{By distributive law of integers}]$$

$$= f(x_1) + f(x_2)$$

Thus f preserves compositions in G & G'.

Therefore f is an isomorphic mapping of G onto G'.

Hence G is isomorphic to G'.

Homomorphism of groups

A mapping f from a group G into group G' is said to be a homomorphism of G into G' if

$$f(ab) = f(a)f(b) \quad \forall a, b \in G.$$

Normal subgroup :→

Let G be an abelian group. H be any subgroup of G. If x is any element of G, then Hx is a right coset of H in G & xH is a left coset of H in G.

Also G is abelian.

Therefore. $Hx = xH \quad \forall x \in G$.

A subgroup H of a group G is said to be a normal subgroup of G if for every $x \in G$ & for every $h \in H$,

$$xhx^{-1} \in H.$$

$$\Rightarrow xHx^{-1} \subseteq H \quad \forall x \in G.$$

We have $x \in G \Rightarrow x^{-1} \in G$

$\therefore$ H is a normal subgroup of G iff $x^{-1}h(x^{-1})^{-1}$

i.e. $x^{-1}hx \in H \quad \forall x \in G, \forall h \in H.$

Theorem-1 :→

A subgroup H of a group G is normal iff $xHx^{-1} = H \quad \forall x \in G$.

If → only If part

Let H be a normal subgroup of G.

Then $xHx^{-1} \subseteq H \quad \forall x \in G$

Also $x \in G \Rightarrow x^{-1} \in G$

Therefore we have

$$x^{-1}H(x^{-1})^{-1} \subseteq H \quad \forall x \in G.$$

$$\Rightarrow x^{-1}Hx \subseteq H \quad \forall x \in G$$

$$\Rightarrow x(x^{-1}Hx)x^{-1} \subseteq xHx^{-1} \quad \forall x \in G.$$

$$\Rightarrow H \subseteq xHx^{-1} \quad \forall x \in G. \qquad (1)$$

If part

Let $xHx^{-1} = H \quad \forall x \in G$.

Then $xHx^{-1} \subseteq H \quad \forall x \in G$.

Therefore H is a normal subgroup of G.

Theorem-2 :→

A subgroup H of a group G is a normal subgroup of G iff each left coset of H in G is a right coset of H in G.

If :→

Then let H be a normal subgroup of G

$$xHx^{-1} = H \quad \forall\, x \in G$$

$$\Rightarrow (xHx^{-1})\,x = Hx \quad \forall\, x \in G$$

$$\Rightarrow xH = Hx \quad \forall\, x \in G$$

$\Rightarrow$ Each left coset xH is the right coset Hx

Conversely suppose that each left coset of H in G is a right coset of H in G.

Let x be any element of G.

Then $xH = Hy$ for some $y \in G$.

Since $e \in H$, $\therefore xe = x \in xH$

$\therefore x \in Hy$ $\quad [\because Hy = Hx]$

But $x \in Hy \Rightarrow Hx = Hy$

$\therefore Hx = xH$ $\quad [\because Hy = xH]$

Thus we have

$$xH = Hx \quad \forall\, x \in G$$

$$\Rightarrow xHx^{-1} = Hxx^{-1} \quad \forall\, x \in G.$$

$$\Rightarrow xHx^{-1} = H \quad \forall\, x \in G$$

$\Rightarrow H$ is a normal subgroup of G

Thus H is a normal subgroup of G

$\Leftrightarrow xH = Hx \quad \forall\, x \in G.$

Theorem-3 :→

A subgroup H of a group G is a normal subgroup of G iff the product of two right cosets of H in G is again a right coset of H in G.

Pf :→ Let H be a normal subgroup of a group G.

Let $a, b \in G$

Then Ha & Hb are two right cosets of H in G.

We have $(Ha)(Hb) = H(aH)b$

$= H(Ha)b$

$= HHab = Hab$

$[\because H$ is normal $\Rightarrow Ha = aH]$

$[\because HH = H]$

Since $a \in G$, $b \in G \Rightarrow ab \in G$,

therefore Hab is also a right coset of H in G.

Thus the product of the right cosets Ha & Hb is the right coset Hab.

Converse

Let H be a subgroup of G such that the product of two right cosets of H in G is again a right coset of H in G.

Let $x \in G$.

Then $x^{-1} \in G$.

Therefore

Hx & Hx^{-1} are two right cosets of H in G.

Consequently, by hypothesis $HxHx^{-1}$ is also a right coset of H in G.

Since $e \in H$,

therefore $exex^{-1} = e$

is an element of the right coset $HxHx^{-1}$.

But H itself is a right coset of H in G & $e \in H$.

Also if two right cosets have one element common they must be identical.

Therefore we must have

$$HxHx^{-1} = H \quad \forall\ x \in G$$

$$\Rightarrow h_1 x h x^{-1} \in H \quad \forall\ x \in G \ \& \ \forall\ h_1, h \in H$$

$$\Rightarrow h_1^{-1}(h_1 x h x^{-1}) \in h_1^{-1} H$$

$$\forall\ x \in G \ \& \ \forall\ h_1, h \in H$$

$$\Rightarrow x h x^{-1} \in H \quad \forall\ x \in G \ \& \ \forall\ h \in H$$

$$\left[\because h_1^{-1} H = H \text{ as } h_1^{-1} \in H \text{ since } h_1 \in H\right].$$

$\Rightarrow H$ is a normal subgroup of G.

Ex → Show that every subgroup of an abelian group is normal.

Sol^{n} → Let G is an abelian group & H be a subgroup of G.

Let $x \in G$ & $h \in H$

we have $xhx^{-1} = xx^{-1}h$ [$\because$ G is abelian $\Rightarrow x^{-1}h = hx^{-1}$]

$= eh = h \in H$

Thus $x \in G$, $h \in H$

$\Rightarrow xhx^{-1} \in H$.

Hence H is normal in G.

RINGS

Suppose R is a non-empty set equipped with two binary operations called addition & multiplication & denoted by $+$ & $\cdot$ respectively i.e. $\forall\ a, b \in R$.

we have $a+b \in R$

& $a \cdot b \in R$

Then this algebraic structure $(R, +, \cdot)$ is called a Ring, if the following postulates are satisfied.

(1) Addition is associative

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

$\forall\ a, b \in R$

(2) Addition is commutative.

i.e. $a+b = b+a \quad \forall\ a, b \in R$

(3) $\exists$ an element denoted by 0 in R such that

$0+a = a \quad \forall\ a \in R$

$= a+0$

(4) To each element $a \in R$

$\exists$ an element $-a \in R$

s.t. $(-a)+a = 0 = a+(-a)$.

(5) Multiplication is associative.

i.e. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

$\forall\ a, b, c \in R$.

(6) Multiplication is distributive w.r.t. addition

i.e. $\forall\ a, b, c \in R$

$a \cdot (b+c) = a \cdot b + a \cdot c$ [Right distributive law]

& $(a+b) \cdot c = a \cdot c + b \cdot c$

[left distributive law]

Ring with unity →

If in a ring there exist an element denoted by 1 such that $1 \cdot a = a = a \cdot 1 \quad \forall\ a \in R$.

then R is called a ring with unit element. The element $1 \in R$ is called the unit element of the ring.

Commutative ring :→

If in a ring R, the multiplication composition is also commutative

i.e. if we have $a \cdot b = b \cdot a \quad \forall\ a, b \in R$

then R is called a commutative ring.

Elementary properties of a Ring.

Theorem :→ If R is a ring and $a, b, c \in R$

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

Pf :→ $a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0$

Now applying Right cancellation law we have

$\Rightarrow 0 = a \cdot 0$

Similarly, we have

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

$$= 0 \cdot a + 0 \cdot a$$

$\therefore \Rightarrow 0 = 0 \cdot a$ [Applying left cancellation law]

Hence $a \cdot 0 = 0 \cdot a = 0$.

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

Pf :- We have $a \cdot 0 = 0$

$\Rightarrow a(-b+b) = 0$

$\Rightarrow a(-b) + a \cdot b = 0$ [Using left distributive law]

$\Rightarrow a(-b) = -ab$ [since in a ring $a+b=0 \Rightarrow a = -b$]

Similarly we have

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

$\Rightarrow (-a)b + ab = 0$ [Right distributive law]

$\Rightarrow (-a)b = -ab$.

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

Pf :- We have

$(-a)(-b) = -[(-a)b]$ [Using (ii)]

$= -(-ab)$

$= ab$

Since R is a group.

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

Pf → we have

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

$= ab + a(-c)$ [Left dist. law]

$= ab + [-(ac)]$

$= ab - ac.$

(v) $(b-a)c = bc - ac$

Pf →

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

$= bc + (-a)c$ [Right dist. law]

$= bc + (-ac)$

$= bc - ac$

Note → The set R consisting of a single element 0 with two binary operations defined by $0+0=0$ & $0 \cdot 0 = 0$ is a ring.

This ring is called the null ring or the zero ring.

Ex → Show that the set I of all integers is a ring with respect to addition & multiplication of integers as the two ring composition.

Pf →

In the set I of integers for $a, b, c \in I$ we observe that

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

(2) $a+b = b+a \quad \forall\, a, b \in I$

(3) $\exists\ 0 \in I$ s.t.
$a+0 = 0+a = a \quad \forall\, a \in R$

(4) To each element a in R $\exists$ an element $-a \in R$
s.t. $(-a)+a = a+(-a) = 0$

(5) $a(bc) = (ab)c \quad \forall\ a, b, c \in R$

(6) $a\cdot(b+c) = a\cdot b + a\cdot c$
& $(b+c)\cdot a = b\cdot a + c\cdot a$.

$\forall\, a, b, c \in I$

Hence I is a ring.

This ring is called the ring of Integers.

Note :→ Similarly, we can show the following

(1) The set $2I$ of all even integers is a commutative ring without unity, the addition & multiplication of integers being the two ring compositions.

(2) The set Q of all rational numbers is a commutative ring with unity,

the addition & multiplication of rational numbers being the two ring compositions.

(3) The set R of all real numbers is a commutative ring with unity, the addition & multiplication of real numbers being the two ring Composition.

(4) The set C of all complex numbers is a commutative ring with unity the addition & multiplication of complex numbers being the two ring compositions.

Example :→

The set M of all nxn matrices with their elements as real numbers is a non-commutative ring with unity, with respect to addition & multiplication of matrices as the two ring composition.

Sol^{n} :→ We know that the sum & the product of two nxn matrices with their elements as real numbers are again nxn matrices with their elements as real numbers. Therefore M is closed w.r.t. addition & multiplication of matrices.

Further we can observe that

(i) $A+(B+C)=(A+B)+C$

$\forall\ A, B, C \in M$,

Since the addition of matrices is commutative.

(ii) $A+B=B+A \quad \forall\ A, B \in M$

Since the addition of matrices is commutative.

(iii) If 0 is the null matrix of the type $n \times n$, then $0 \in M$ & we have

$0+A=A \quad \forall\ A \in M$

(iv) To each matrix $A \in M$ $\exists$ $-A \in M$ such that

$-A+A=0$ (null matrix)

(v) $(AB)C=A(BC) \quad \forall\ A, B, C \in M$

Since multiplication of matrices is associative.

(vi) $A(B+C)=AB+AC$

& $(B+C)A=BA+CA \quad \forall\ A, B, C \in M$

Since matrix multiplication is distributive w.r.t. matrix addition.

Hence M is a ring with respect to the given composition.

Since multiplication of matrices is not in general commutative, therefore the ring is non-commutative ring.

Finally if I be the unit matrix of type $n \times n$, then $I \in M$ & we have $IA = A = AI$ $\forall A \in M$.

Therefore the matrix I is the multiplicative identity.

Thus the ring is with unity & the matrix I is the unit element of the ring.

Zero-divisor def^n →

A non-zero element of a ring R is called a zero divisor or divisor of zero if $\exists$ an element $b \neq 0 \in R$ such that either $ab = 0$ or $ba = 0$

Ex → Suppose M is a ring of all 2×2 matrices with their elements as integers, the addition & multiplication of matrices being the two ring compositions, then M is a ring with zero divisors.

Integral Domain

A ring is called an integral domain if it is (i) commutative,
(ii) has unit element,
(iii) is without zero divisors.

Field → A ring R with at least two elements is called a field if it is (i) commutative, (ii) has unity, (iii) is such that each non-zero element possesses multiplicative inverse.

For example, the ring of rational numbers $(\mathbb{Q}, +, \cdot)$ is a field since it is a commutative ring with unity & each non-zero element is invertible.

The rings of real numbers & complex numbers are also examples of fields.

Division Ring or Skew field :->

A ring R with at least two elements is called a division Ring or a skew field if it has

(i) unity,

(ii) is such that each non-zero element possesses multiplicative inverse.

Thus a commutative division ring is a field.

Theorem -> Every field is an integral domain.

Pf :- Since a field F is a commutative ring with unity, therefore in order to show that every field is an integral domain we should show that a field has no zero divisors.

Let $a, b \in F$ with $a \neq 0$ s.t. $ab = 0$

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

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

$\Rightarrow 1 \cdot b = 0$

$\Rightarrow b = 0$

Similarly let $ab = 0 \Rightarrow (ab)b^{-1} = 0b^{-1}$

$[\because b \neq 0]$ $\Rightarrow a(bb^{-1}) = 0$

$\Rightarrow a \cdot 1 = 0 \Rightarrow a = 0$

Thus in a field $ab=0 \Rightarrow a=0$ or $b=0$.
Therefore a field has no zero divisors.
Therefore every field is an integral domain.
But the converse is not true, i.e. every integral domain is not a field.

For example the ring of integers is an integral domain & it is not a field.
The only invertible elements of the ring of integers are 1 & -1.

Note:- For a field unity & zero are distinct elements. i.e. $1 \neq 0$
let ~~$a \neq 0$~~ $a \in F$ (Field) $a \neq 0$.
Then a^{-1} exists.
For $a^{-1}=0 \Rightarrow a a^{-1} = a \cdot 0$
$\Rightarrow 1 = 0$
$\Rightarrow a1 = a \cdot 0 \Rightarrow a = 0$
which is a contradiction.
Now a field has no zero divisors.
Therefore $1 = a^{-1}a \neq 0$.

*. The non-zero elements of a field forms an abelian group with respect to multiplication.

Theorem :-
A field (Skew field) has no zero divisors.

Pf:- Let D be a skew field.
Then D is a ring with unit element & each non-zero element of D possesses multiplicative inverse.

Let $a, b \in D$ with $a \neq 0$
such that $ab = 0$

Since $a \neq 0$, a^{-1} exists & we have

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

Similarly, let $ab = 0$ with $b \neq 0$

Since $b \neq 0$, b^{-1} exists & we have

$$ab = 0 \Rightarrow (ab)b^{-1} = 0b^{-1}$$
$$\Rightarrow a(bb^{-1}) = 0$$
$$\Rightarrow a \cdot 1 = 0$$
$$\Rightarrow a = 0$$

Therefore a skew field has no zero divisors.

Theorem :→ A finite commutative ring without zero divisors is a field.

OR · Every finite integral domain is a field.

Pf :→ Let D be a finite commutative ring without zero divisors having n elements $a_1, a_2 \cdots a_n$.

In order to prove D is a field we must have $1 \in D$ s.t.

$$1 \cdot a = a \quad \forall a \in D.$$

Also we should show that for every element $a \neq 0 \in D$ $\exists$ an element $b \in D$ s.t. $ba = 1$.

Let $a \neq 0 \in D$.

Consider the n products

$aa_1, aa_2 \ldots aa_n$

All these are elements of D.

Also they are all distinct.

For suppose that $aa_i = aa_j$ for $i \neq j$.

Then $a(a_i - a_j) = 0$ ——— (1)

Since D is without zero divisors & $a \neq 0$ therefore from (1)

$a_i - a_j = 0$

$\Rightarrow a_i = a_j$, contradicting $i \neq j$.

$\therefore aa_1, aa_2 \ldots aa_n$ are all the n distinct elements of D placed in some order.

So one of these elements will be equal to a.

Thus $\exists$ an element, say $c \in D$ s.t.

$ac = a = ca$ [$\because D$ is commutative]

We shall show that this element c is the multiplicative identity of D.

Let $y \in D$

Then for some $x \in D$,

we shall have $ax = y = xa$

Now $cy = c(ax)$ [$\because ax = y$]

$= (ca)x$

$= ax$ [$\because ca = a$]

$= y$ [$\because ax = y$]

$= yc$

Thus $cy = y = yc \quad \forall y \in D$.

$\therefore$ c is the unit element of the ring D.
& let us denote it by 1.

Now $1 \in D$

& Out of n products

$aa_1, aa_2 \cdots aa_n$, one will be equal to 1.

Thus $\exists$ an element say $b \in D$

such that

$ab = 1 = ba$

$\therefore$ b is the multiplicative inverse of the non-zero element $a \in D$

Thus every non-zero element of D is invertible.

Hence D is a field.

Subrings :→

Let R be a ring. A non-empty subset S of the set R is said to be a subring of R if S is closed with respect to the operations of addition & multiplication on R & S itself is a ring for these operations.

If S is a subring of a ring R, it is obvious that S is a subgroup of the additive group of R.

→ i.e. (i) $a+b \in S$ for $a, b \in S$

(ii) $0 - a \in S$ for $a \in S$

(iii) $a.b \in S$ for $ab \in S$

If R is any ring then $\{0\}$ & R itself are always subrings of R.
These are known as improper subrings of R.
Other subrings if any, of R are called proper subrings of R.

If A is a ring & B_i is an arbitrary collection of subrings of A, then B_i is a subring of A.

If A is a ring & B is a subset of A then, the intersection of all subrings of A that contains B, is a subring of A, it is called the subring generated by B.

Example:→ let R → set of all real numbers
Q → set of all rational numbers.

As $Q \subseteq R$ & R is a ring.
wrt. '+' & '.'
Q is closed under operation '+'.
For every element $q \in Q$,

$$-q \in Q.$$

Q is also closed under multiplication
i.e. for $a, b \in Q \Rightarrow a.b \in Q$.
Hence Q is a subring of R.