$\Rightarrow$ $ex = a^{-1}b$ (By existence of Inverse)

$\Rightarrow$ $x = a^{-1}b$ (By existence of Identity)

But by closure axiom:

$$a^{-1}b \in G \therefore x \in G$$

$\therefore$ $ax = b$ has a solution in G.

Let if possible $ax = b$ have two solutions x_1, x_2.

i.e. $ax_1 = b$ and $ax_2 = b$.

$$ax_1 = ax_2.$$

$\Rightarrow \boxed{x_1 = x_2}$ (By left cancellation law)

Thus, solution is unique.

Similarly,

$ya = b$

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

$\Rightarrow$ $(a^{-1}a)y = a^{-1}b$ (By Associative Property)

$\Rightarrow$ $ey = a^{-1}b$ (By existence of Inverse)

Now let a be an arbitrary element in G and $b = e$, so that the equation $ya = b$ becomes $ya = e$.

But solution of this equation is unique in G. Let C $\Re$ G be the solution.

$\therefore$ $Ca = e$. Hence C is left inverse of a in G.

Thus left identity exists and each element has its left inverse. Hence G is a graph.

Theories II. Prove that a finite set G with an associative multiplicatively denoted binary composition is a group if right and left cancellation laws hold good in G, *i.e.*,

$$ax = bx \Rightarrow a = b \text{ and } xa = xb \Rightarrow a = b.$$

Proof: Let $G = \{a_1, a_2, a_3, ..., a_b, ..., a_n\}$, where all the n elements in G are distinct. Let n be any one element of G. Consider the n 'Products'.

$$a_1a_r, a_2a_r^2, ..., a_ba_{rb}$$

All these 'Products' are distinct, for it possible, let

$$a_pa_r = a_qa_r \text{ where } a_pa_q \in G$$

But, by right cancellation $a_pa_r = a_qa_r \Rightarrow a_p = a_q$.

But by hypothesis $a_p \neq a_q$. Hence all products are distinct.

Also by closure product $a_1\ a_r,\ a_2\ a_{rw}$ .... $a_nn_{rb} \in G$. Hence these are the n elements of G, order of elements have may be different from that given in G above.

Thus, the equation $xa_n = a_1$ has a unique solution in G, *i.e.*, the equation $xa = b$, where $a, b \in G$ has a unique solution in G.

Similarly, by applying left cancellation law, we can prove that $ay = b$, where $ab \in G$ has a unique solution in G. Maximum operation is associative. Hence by 1st theorem, G is a group.

Example 27: Prove that if $a, b \in$ graph G, then $(ab)^2 = a^2b^2$ iff G is abelian.

Solution:

Let G be abelian and $a, b \in G$

$\therefore$ $(ab)^2 = (ab)(ab)$

$= a(ba)b$ by G_2.

$= a(ab)b$ $\quad \therefore$ G is abelian, *i.e.* $ab = ba$.

$= (ab)(bb)$ by G_2.

$= a^2b^2$ Hence proved.

Converse: Let $a, b \in G$ and $(ab)^2 = a^2b^2$

Now $(ab)^2 = a^2b^2 \Rightarrow (ab)(ab) = (aa)b^2$

$\Rightarrow$ $a(ba)b = a(ab^2)$

$\Rightarrow$ $bab = ab^2$ by left cancellation law

$\Rightarrow$ $(ba)b = (ab)b$

$\Rightarrow$ $ba = ab.$ by right cancellation law

$\Rightarrow$ G is abelian

Example 28: If G a group such that $(ab)^3 = a^3 b^3$ for three consecutive integers M, $a, b \in G$, prove that G is abelian.

Solution:

Let M, M + 1, M + 2 be three consecutive integers :

Hence we are given that

$$(ab)^M = a^M b^M \quad \ldots(1)$$

$$(ab)^{M+1} = a^{M+1} b^{M+1} \quad \ldots(2)$$

$$(ab)^{M+2} = a^{M+2} b^{M+2} \quad \ldots(3)$$

Now $(ab)^{M+2} = a^{M+2} b^{M+2} \Rightarrow (ab)^{M+1}(ab) = (a^{M+1} a)(b^{M+1} b)$

$\Rightarrow$ $(a^{M+1} b^{M+1})(ab) = a^{M+1}(ab^{M+1} b)$ by (2) and G_2

$\Rightarrow$ $a^{M+1}(b^{M+1} ab) = a^{M+1}(ab^{M+1} b)$ by G_2

$\Rightarrow$ $b^{M+1} ab = ab^{M+1} b$ by left cancellation law

$\Rightarrow$ $(b^{M+1} a)b = (ab^{M+1})b$ by G_2

$\Rightarrow$ $b^{M+1} a = ab^{M+1}$ by right cancellation law

$\Rightarrow$ $a^M (b^{M+1} a) = a^M (ab^{M+1})$ by operating a^M on both sides.

$\Rightarrow$ $(a^M b^M) (b a) = a^{M+1} b^{M+1}$ by G_2

$\Rightarrow$ $(a^M b^M) (ba) = (ab)^{M+1}$ by (2)

$\Rightarrow$ $(ab)^M (ba) = (ab)^M (ab)$ by G_2 and (2)

$\Rightarrow$ $ba = ab$ by left cancellation law

$\Rightarrow$ G is abelian Hence proved

5.9 SUBGROUPS AND SUBGROUP TESTS

A *subgroup* of a group G is a subset of G which is a subgroup in its own right (with the same group operation).

There are two subgroup tests, resembling the two subring tests:

5.9.1 Proposition (First Subgroup Test)

A non-empty subset H of a group G is a subgroup of G if, for any h, k $\in$ H, *we have hk* $\in$ H *and* $h^{-1} \in$ H.

Proof: We have to show that H satisfies the group axioms. The conditions of the test show that it is closed under composition (G0) and inverses (G3). The associative law (G1) holds in H because it holds for all elements of G. We have only to prove (G2), the identity axiom.

We are given that H is non-empty, so choose $h \in$ H. Then by assumption, $h^{-1} \in$ H, and then (choosing $k = h^{-1}$) I = $hh^{-1} \in$ H.

5.9.2 Second Subgroup Test

We can reduce the number of things to be checked from two to one proposition: A non-empty subset H of a group G is a subgroup of G if, for any $h, k \in$ H, we have $hk^{-1} \in$ H.

Proof: Choosing $k = h$, we see that I = $hh^{-1} \in$ H.. Now using I and h in place of h and k, we see that $h^{-1} = 1h^{-1} \in$ H. Finally, given $h, k \in$ H, we know that $k^{-1} \in$ H, so $hk = h(k^{-1})^{-1} \in$ H. So the conditions of the First Subgroup test hold.

Example 29:

Look back to the Cayley tables in the last chapter, in the first case, $\{e, y\}$ is a subgroup. In the second case. $\{e, a\}$, $\{e, b\}$ and $\{e, e\}$ are all subgroups.

5.10 CYCLIC GROUPS

If g is an element of a group G, we define the powers g^n of G (for $n \in \mathbb{Z}$) as follows: if n is positive, then g^n is the product of n factors g; $g^0 = -l$; and $g^{-n} = (g^{-1})^n$. The usual laws of exponents hold: $g^{m+n} = g^m.g^n$ and $g^{mn} = (g^m)^n$.

A *cyclic group* is a group C which consists of all the powers (positive and negative) of a single element. If C consists of all the powers of g, then we write C = (g), and say that C is *generated by g*.

Proposition: A cyclic group is Abelian.

Proof: Let C = (g), Take two elements of C, say g^m and g^n. Then,

$$g^m \cdot g^n = g^{m+n} = g^n \cdot g^m$$

Let C = (g). Recall the order of g the smallest positive integer n such that $g^n = 1$ (if such n exists - otherwise the order is infinite).

Proposition: Lef g be an element of the group G. Then the set of all powers (positive and negative) of g forms a cyclic subgroup of G. Its order is equal to the order of g.

Proof: Let $C = \{g^n : n \in Z\}$. We apply the Second Subgroup test: if $g^m, g^n \in C$, then, $(g^m)(g^n)^{-1} = g^{m-n} \in C$. So C is a subgroup.

If g has infinite order, then no positive power of g is equal to 1. It follows that all the powers g^n for $n \in \mathbb{Z}$ are different elements. (For if $g^m = g^n$, with $m > n$, then $g^{n-m} = 1$.) So C is infinite.

Suppose that g has finite order n. We claim that any power of g is equal to one of the elements $g^0 = 1$, $g^1 = g \ldots g^{n-1}$. Take any power g^m. Using the division algorithm in Z, write $m = nq + r$, where $0 \leq r \leq n - 1$. Then

$$g^m = g^{nq+r} = (g^n)^q \cdot g^r = 1 \cdot g^r = g^r$$

Furthermore, the elements $1, g \ldots g^{n-1}$ are all different: for if $g^r = g^s$, with $0 \leq r < s \leq n - 1$, then $g^{s-r} = 1$, and $0 < s - r < n$, contradicting the fact that n is the order of g (the smallest exponent i such that $g^i = 1$).

5.11 HOMOMORPHISMS

An isomorphism between groups has two properties: it is a bijection; and it preserves the group operation. If we relax the first property but keep the second, we obtain a homomorphism. Just as for rings, we say that a function $q : G_1 \to G_2$ is

- a *homomorphism* if it satisfies

  $(gh)\theta = (g\theta)(h\theta)$; ...(5.1)
- a monomorphism if it satisfies (5.1) and is one-to-one;
- an epimorphism if it satisfies (5.1) and is onto;
- an isomorphism if it satisfies (5.1) and is one-to-one and onto.

We have the following lemma, proved in much the same way as for rings:

Lemma: Let $\theta : G_1 \to G_2$ be a homomorphism. Then $1\theta = 1$; $(g^{-1})\theta = (g\theta)^{-1}$; and $(gh^{-1})\theta = (g\theta)(h\theta)^{-1}$, for all $g, h \in G_1$.

Now, if $\theta : G_1 \to G_2$ is a homomorphism, we define the *image* of θ to be the subset

$\{x \in G_2 : x = g\theta$ for some $g \in G_1\}$ of G_2, and the *kernel* of θ to be the subset $\{g \in G_1 : g\theta = 1\}$ of G_1.

Proposition: Let θ: $G_1 \to G_2$ be a homomorphism.

(*a*) $\mathrm{Im}(\theta)$ *is a subgroup of* G_2.

(*b*) $\mathrm{Ker}(\theta)$ *is a subgroup of* G_1.

Proof: We use the Second Subgroup Test in each case.

(*a*) Take $x, y \in Im(\theta)$, say $x = g\theta$ and $y = h\theta$ for $g, h \in G_1$. Then $xy^{-1} = (gh^{-1})\theta \in Im(\theta)$, by the Lemma.

(*b*) Take $g, h \in \text{Ker}(\theta)$. Then $g\theta = h\theta = 1$, so $(gh^{-1})\theta = 1^{-1} I = 1$, so $gh^{-1} \in \text{Ker}(\theta)$.

Example 30: Colour the elements 1, (1, 2, 3) and (1, 3, 2) red, and the elements (1, 2), (2, 3) and (1, 3) blue. We see that the Cayley table has the "simplified form"

.	red	blue
red	red	blue
blue	blue	red

This is a group of order 2, and the map θ taking 1, (1, 2, 3) and (1, 3, 2) to red and (1, 2), (2, 3) and (1, 3) to blue is a homomorphism. Its kernel is the subgroup {1, (1, 2, 3), (1, 3, 2)}.

5.12 PERMUTATION GROUP

A permutation group is a group G whose elements are permutations of a given set M, and whose group operation is the composition of permutations in *G* (which are thought of as bijective functions from the set *M* to itself); the relationship is often written as *(G, M)*. Note that the group of *all* permutations of a set is the symmetric group; the term *permutation group* is usually restricted to mean a subgroup of the symmetric group. The symmetric group of *n* elements is denoted by S_n; if M is any finite or infinite set, then the group of all permutations of M is often written as Sym(M). The application of a permutation group to the elements being permuted is called its group action; it has applications in both the study of symmetries, combinatorics and many other branches of Mathematics, Physics and Chemistry.

Closure properties: As a subgroup of a symmetric group, all that is necessary for a permutation group to satisfy the group axioms is that it contain the identity permutation, the inverse permutation of each permutation it contains, and be closed under composition of its permutations. A general property of finite groups implies that a finite subset of a symmetric group is again a group if and only if it is closed under the group operation.

Examples: Permutations are often written in *cyclic form, e.g.* during cycle index computations, so that given the set M= {1, 2, 3, 4}, a permutation *g* of M with $g(1) = 2$, $g(2) = 4$, $g(4) = 1$ and $g(3) = 3$ will be written as (1, 2, 4)(3), or more commonly, (1, 2, 4) since 3 is left unchanged; if the objects are denoted by a single letter or digit, commas are also dispensed with, and we have a notation such as (1 2 4).

Consider the following set *G* of permutations of the set M = {1, 2, 3, 4}:

1. $e = (1)(2)(3)(4)$

   This is the identity, the trivial permutation which fixes each element.

2. $a = (1\ 2)(3)(4) = (1\ 2)$

   This permutation interchanges 1 and 2, and fixes 3 and 4.

3. $b = (1)(2)(3\ 4) = (3\ 4)$

   Like the previous one, but exchanging 3 and 4, and fixing the others.

4. $ab = (1\ 2)(3\ 4)$

This permutation, which is the composition of the previous two exchanges simultaneously 1 with 2, and 3 with 4.

G forms a group, since $aa = bb = e$, $ba = ab$, and $baba = e$. So (G,M) forms a permutation group.

The Rubik's Cube puzzle is another example of a permutation group. The underlying set being permuted is the coloured subcubes of the whole cube. Each of the rotations of the faces of the cube is a permutation of the positions and orientations of the subcubes. Taken together, the rotations form a generating set, which in turn generates a group by composition of these rotations. The axioms of a group are easily seen to be satisfied; to invert any sequence of rotations, simply perform their opposites, in reverse order.

The group of permutations on the Rubik's Cube does not form a complete symmetric group of the 20 corner and face cubelets; there are some final cube positions which cannot be achieved through the legal manipulations of the cube. More generally, *every* group G is isomorphic to a permutation group by virtue of its regular action on G as a set; this is the content of Cayley's theorem.

5.13 COSETS AND LAGRANGE'S THEOREM

5.13.1 Cosets

Given any subgroup H of a group G we can construct a partition of G into "cosets" of H, just as we did for rings. But for groups, things are a bit more complicated.

Because the group operation may not be commutative, we have to define two different sorts of cosets.

Let H be a subgroup of a group G. Define a relation $\sim_r$ on G by the rule $x \sim_r y$ if and only if $yx^{-1} \in H$

We claim that $\sim_r$ is an equivalence relation:

Reflexive: For any $x \in G$, we have $xx^{-1} = 1 \in H$, so $x \sim_r x$,

Symmetric: Suppose that $x \sim_r y$, so that $h = yx^{-1} \in H$. Then $h^{-1} = (yx^{-1})^{-1} = xy^{-1} \in H$, so $y \sim_r x$.

Transitive: Suppose that $x \sim_r y$ and $y \sim_r z$, so that $h = yx^{-1} \in H$ and $k = zy^{-1} \in H$.

Then, $kh = (zy^{-1})(yx^{-1}) = zx^{-1} \in H$, so $x \sim_r z$.

The equivalence classes of this equivalence relation are called the *right cosets* of H in G.

A right coset is a set of elements of the form $Hx = \{hx : h \in H\}$, for some fixed element $X \in G$ called the "coset representative". For,

$y \in Hx \Leftrightarrow y = hx$ for some $h \in H \leftrightarrow yx^{-1} \in H \Leftrightarrow x \sim_r y$.

We summarise all this as follows:

Proposition: *If H is a subgroup of the of the group G, then G is partitioned into right cosets of H in G, sets of the form* $Hx = \{hx : h \in H\}$.

In a similar way, the relation $\sim r$ defined on G by the rule, $x \sim r\ y$ if and only $x^{-1}\ y \in H$ is an equivalence relation on G, and its equivalence classes are the *left cosets of* H in G, the sets of the form $xH = \{xh : h \in H\}$.

If G is an abelian group, the left and right cosets of any subgroup coincide, since $Hx = \{hx : h \in H\} = \{xh : h \in H\} = xH$.

This is not true in general:

Example 31: Let G be the symmetric group S_3, and let H be the subgroup {1, (1,2)} consisting of all permutations fixing the point 3. The right cosets of H in G are

H1 = {1, (1, 2)},

H(1, 3) = {(1, 3), (1, 2, 3)}

H (2, 3) = {(2, 3), (1, 3, 2)}

while the left cosets are:

1H = {1, (1, 2)},

(1, 3) H = {(1, 3), (1, 3, 2)}

(2, 3) H = {(2, 3), (1, 3, 2)}

We see that, as expected, both right and left cosets partition G, but the two partitions are not the same. But each partition divides G into three sets of size 2.

5.13.2 Theorem (Lagrange's Theorem)

Lagrange's Theorem states a very important relation between the orders of a finite group and any subgroup.

Let H be a subgroup of a finite group G. Then the order of H divides the order of G.

Proof: We already know from the last section that the group G is partitioned into the right cosets of H. We show that every right coset Hg contains the same number of elements as H.

To prove this, we construct a bijection f from H to Hg. The bijection is defined in the obvious way: ϕ maps h to hg.

- ***ϕ is one-to-one:*** suppose that $\phi(h_1) = (\phi)\ h_2$, that is, $h_{1g} = h_{2g}$. Cancelling the *g* (by the cancellation law, or by multiplying by *g*–1, we get $h_1 = h_2$.
- ***ϕ is onto:*** by definition, every element in the coset Hg has the form hg for some $h \in H$, that is, it is $\phi(h)$.

So, ϕ is a bijection, and $\{Hg\} = |H|$.

Now, if m is the number of right cosets of H in G, then $m|H| = |G|$, so $|H|$ divides $|G|$.

Remarks: We see that $|G|/|H|$ is the number of right cosets of H in G. This number is called the index, of H in G.

We could have used left cosets instead, and we see that $|G|/|H|$ is also the number of left cosets. So these numbers are the same. In fact, there is another reason for this.

Exercise: Show that the set of all inverses of the elements in the right coset Hg form the left coset $g^{-1}H$. So there is a bijection between the set of right cosets and the set of left cosets of H.

In the example of preceding section, we had a group S_3 with a subgroup having three right cosets and three left cosets: that is, a subgroup with index 3.

Corollary: Let g be an element of the finite group G. Then the order of g divides the order of G.

Proof: Remember, first, that the word "order" here has two quite different meanings: the order of a group is the number of elements it has: while the order of an element is the smallest n such thai $g^n = 1$.

However, we also saw that if the element g has order m, then the set $\{1, g, g^2, ..., g^{m-1}\}$ is a cyclic subgroup of G having order m. So, by Lagrange's Theorem m divides the order of G.

Example: Let $G = S_3$. Then the order of G is 6. The element (1) (2, 3) has order 2, while the element (1, 3, 2) has order 3.

5.14 NORMAL SUBGROUPS

A normal subgroup is a special kind of subgroup of a group. As we know subgroup H has right and left cosets, which may not be the same. We say that H is a *normal subgroup* of G if the right and left cosets of H in G are the same; that is, if $Hx = xH$ for any $x \in G$.

There are several equivalent ways of saying the same thing. We define $x^{-1} Hx = \{x^{-1} hx : h \in H\}$for any element $x \in G$.

Proposition: Let H be a subgroup of G. Then be following are equivalent:

(*a*) H is a normal subgroup, that is, $Hx = xH$ for all $x \in G$;

(*b*) $x^{-1} Hx = H$ for all $x \in G$:

(*c*) $x^{-1} hx \in H$, for all $x \in G$ and $h \in H$.

Proof: If $Hx = xH$, then $x^{-1} Hx = x^{-1} xH = H$ and conversely. So (*a*) and (*b*) are equivalent.

If (*b*) holds then every element $x^{-1} hx$ belongs to $x^{-1} Hx$ and so to H, so (*c*) holds. Conversely, suppose that (*c*) holds. Then every element, of $x^{-1} Hx$ belongs to H, and we have to prove the reverse inclusion. So take $h \in H$. Putting $y = x^{-1}$, we have $k = y^{-1} hy = xhx^{-1} \in H$, so $h \in x^{-1} Hx$, finishing the proof.

Now the important thing about normal subgroups is that, like ideals, they are kernels of homomorphisms.

Proposition

Let $\theta: G_1 \rightarrow G_2$ be a homomorphism. Then Ker (θ) is a normal subgroup of G_2.

Proof: Let $H = \text{Ker}(\theta)$. Suppose that $h \in H$ and $x \in G$. Then

$(x^{-1} hx)\theta = (x^{-1})\theta \cdot h\theta \cdot x\theta = (x\theta)^{-1} \cdot 1 \cdot x\theta = 1,$

so $x^{-1} hx \in \ker(\theta) = H$. By part (c) of the preceding; proposition H is a normal subgroup of G.

There are a couple of situations in which we can guarantee that a subgroup is normal.

Proposition:

(a) If G is Abelian then every subgroup H of G is normal.

(b) If H has index 2 in G, then H is normal in G.

Proof: (*a*) If G is Abelian. then $xH = Hx$ for all $X \in G$.

(*b*) Recall that this means that H has exactly two cosets (left or right) in G. One of these cosets is H itself; the other must consist of all the other elements of G that is, G/H. This is the case whether we are looking at left or right cosets. So the left and right cosets are the same.

Remark: We saw in the last section an example of a group S_3 with a non-normal subgroup having index 3 (that is, just three cosets). So we cannot improve this theorem from 2 to 3.

In our example in the last section, the subgroup {1, (1, 2, 3), (1, 3, 2)} of S_3 has index 2, and so is normal, in S_3 this also follows from the fact that it is the kernel of a homomorphism.

For the record, here is a normal Subgroup test:

Proposition (Normal subgroup test): *A non-empty subset H of a group G is a normal subgroup of G if he following hold:*

(*a*) *for any* $h, k \in H$, *we have* $hk^{-1} \in H$;

(*b*) *for any* $h \in H$ *and* $x \in G$, *we have* $x^{-1} hx \in H$.

Proof: (*a*) is the condition of the second subgroup test, and we saw that (*b*) is a condition for a subgroup to be normal.

5.15 RINGS

A ring can be thought of as a generalization of the integers, $\mathbb{Z}$. We can add and multiply elements of a ring, and we are interested in such questions as factorization into primes, construction of "modular arithmetic", and so on'.

Our first class of structures is *rings.* A ring has two operations: the first is called *addition* and is denoted by + (with infix notation); the second is called *multiplication,* and is usually denoted by juxtaposition (but sometimes by with infix notation).

In order to be a ring, the structure must satisfy certain rules called *axioms.* We divide these into three part. The name of the ring is R.

We define a ring to be a set R with two binary operations satisfying the following axioms:

(i) ***Axioms for Addition***

(A0) (*Closure law*) For any $a, b \in R$, we have $a + b \in R$.

(A1) (*Associative law*) For any $a, b, c \in R$, we have $(a + b) + c = a + (b + c)$.

(A2) (*Identity law*) There is an element $0 \in R$ with the property that $a + 0 = 0 + a = a$ for all $a \in R$. (The element 0 is called the *zero element* of R.)

(A3) (*Inverse law*) For any element $a \in R$, there is an element $b \in R$ satisfying $a + b = b + a = 0$. (We denote this element b by $-a$, and call it the *additive inverse* or *negative* of a.)

(A4) *(Commutative law)* For any $a, b \in R$, we have $a + b = b + a$.

(ii) ***Axioms for Multiplication***

(M0) *(Closure law)* For any $a, b \in R$, we have $ab \in R$.

(Ml) *(Associative law)* For any $a, b, c \in R$, we have $(ab)c = a(bc)$.

(iii) ***Mixed Axiom***

(D) (*Distributive laws*) For any $a, b, c \in R$, we have $(a + b)c = ac + bc$ and $c(a + b) = ca + cb$.

Remark 1. The closure laws (A0) and (M0) are not strictly necessary. If + is a binary operation, then it is a function from $R \times R$ to R, and so certainly $a + b$ is an element of R for all $a, b \in R$. We keep these laws in our list as a reminder.

Remark 2. The zero element 0 denoted by (A2) and the negative $-a$ denoted by (A3) are not claimed to be unique by the axioms. We will see later on that there is only one zero element in a ring, and that each element has only one negative.

Axioms (M0) and (M1) parallel (A0) and (A1). Notice that we do not require multiplicative analogues of the other additive axioms. But there will obviously be some rings in which they hold. We state them here for reference.

Further multiplicative properties

(M2) (*Identity law*) There is an element $1 \in R$ such that $a1 = 1a = a$ for all $a \in R$. (The element 1 is called the *identity element* of R).

(M3) (*Inverse law*) For any $a \in R$, if $a \neq 0$, then there exists an element $b \in R$ such that $ab = ba = 1$. (We denote this element b by a^{-1}, and call it the *multiplicative inverse* of a.)

(M4) (*Commutative law*) For all $a,b \in R$, we have $ab = ba$.

A ring which satisfies (M2) is called a *ring with identity;* a ring which satisfies (M2) and (M3) is called a *division ring;* and a ring which satisfies (M4) is called a *commutative ring.* (Note that the term "commutative ring" refers to the fact that the multiplication is commutative; the addition in a ring is always commutative!) A ring which satisfies all three further properties (that is, a commutative division ring) is called *a field.*

5.15.1 Examples of Rings

The integers

The most important example of a ring is the set $\mathbb{Z}$ of integers, with the usual addition and multiplication. The various properties should be familiar to you; we will simply accept that they hold. $\mathbb{Z}$ is a commutative ring with identity. It is not a division ring because there is no *integer* b satisfying $2b = 1$. This ring will be our prototype for several things in the course.

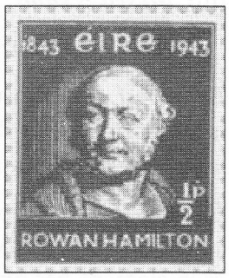
Note that the set $\mathbb{N}$ of natural numbers, or non-negative integers, is not a ring, since it fails the inverse law for addition. (There is no non-negative integer b such that $2 + b = 0$).

Other number systems

Several other familiar number systems, namely the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$, are fields. Again, these properties are assumed to be familiar to you.

The quaternions

There do exist division rings in which the multiplication is not commutative, that is, which are not fields, but they are not so easy to find. The simplest example is the ring *of quaternions,* discovered by Hamilton in 1843.



On 16 October 1843 (a Monday), Hamilton was walking in along the Royal Canal with his wife to preside at a Council meeting of the Royal Irish Academy. Although his wife talked to him now and again Hamilton hardly heard, for the discovery of the quaternions, the first noncommutative [ring] to be studied, was taking shape in his mind. He could not resist the impulse to carve the formulae for the quaternions in the stone of Broom'e Bridge (or Brougham Bridge as he called it) as he and his wife passed it.

Instead of adding just one element i to the real numbers, Hamilton added three. That is, a *quaternion* is an object of the form $a + bi + cj + d$k, where

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

It can be shown that all the axioms (A0)-(A4), (M0)-(M3) and (D) are satisfied.

For example, if a, b, c, d are not all zero, then we have

$$(a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k})\left(\frac{a - b\mathrm{i} - c\mathrm{j} - d\mathrm{k}}{a^2 + b^2 + c^2 + d^2}\right) = 1$$

The ring of quaternions is denoted by $\mathbb{H}$, to commemorate Hamilton.

Matrix Rings

We briefly denned addition and multiplication for matrices in the last chapter. The formulae for addition and multiplication of $n \times n$ matrices, namely

$$(\mathrm{A} + \mathrm{B})_{ij} = \mathrm{A}_{ij} + \mathrm{B}_{ij}, \ (\mathrm{AB})_{ij} = \sum_{k=1}^{n} \mathrm{A}_{ik}\mathrm{B}_{kj}$$

just depend on the fact that we can add and multiply the entries. In principle these can be extended to any system in which addition and multiplication are possible. However, there is a problem with multiplication, because of the $\sum_{k=1}^{n}$, which tells us to add up n terms. In general we can only add two things at a time, since addition is a binary operation, so we have to make the convention that, for example, $a + b + c$ means $(a + b) + c$, $a + b + c + d$ means $(a + b + c) + d$, and so on. We will return to this point in the next subsection.

Proposition: Let R be a ring. Then the set M_n (R) of n × n matrices over R, with addition and multiplication defined in the usual way, is a ring. If R has an identity, then M_n(R) has an identity; but it is not in general a commutative ring or a division ring.

We will look at the proof later, once we have considered addition of n terms.

Polynomial Rings

In much the same way, the usual rules for addition of polynomials,

$$\left(\Sigma a_i x^i\right)+\left(\Sigma b_i x^i\right)=\Sigma(a_i+b_i)x^i, \left(\Sigma a_i x^i\right)+\left(\Sigma b_i x^i\right)=\Sigma d_i x^i$$

where

$$d_i = \sum_{k=0}^{i} a_k b_{i-k}$$

can be extended to polynomials with coefficients in any algebraic structure in which addition and multiplication are defined. As for matrices, we have to be able to add an arbitrary number of terms to make sense of the definition of multiplication.

Rings of Sets

The idea of forming a ring from operations on sets is due to George Boole, who published in 1854 *An investigation into the Laws of Thought, on Which are founded the Mathematical Theories of Logic and Probabilities.* Boole approached logic in a new way reducing it to algebra, in much the same way as Descartes had reduced geometry to algebra.

The familiar set operations of union and intersection satisfy some but not all of the ring axioms. They are both commutative and associative, and satisfy the distributive laws both ways round; but they do not satisfy the identity and inverse laws for addition.

Boole's algebra of sets works as follows. Let P (A), the *power set* of A, be the set of all subsets of the set A. Now we define addition and multiplication on to P (A) be the operations of symmetric difference and intersection respectively:

$$x + y = x \Delta y, xy = x \cap y$$

A ring satisfying the further condition that $xx = x$ for all x is called a *Boolean ring.*

Zero Rings

Suppose that we have any set R with a binary operation + satisfying the additive axioms (A0)-(A4). (We will see later in the course that such a structure is called an abelian group.) Then we can make R into a ring by defining $xy = 0$ for all $x, y \in R$. This is not a very exciting rule for multiplication, but it is easy to check that all remaining axioms are satisfied.

A ring in which all products are zero is called a zero ring. It is commutative, but doesn't have an identity (if $|R| > 1$).

Direct Sum

Let R and S be any two rings. Then we define the direct sum R ⊕ S as follows. As a set, R ⊕ S is just the cartesian product R × S. The operations are given by the rules

$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$, $(r_1, s_1)(r_2, s_2) = (r_1r_2, s_1s_2)$.

(Note that in the ordered pair $(r_1 + r_2, s_1 + s_1)$, the first + denotes addition in R, and the second + is addition in S.)

Modular Arithmetic

Let $\mathbb{Z}_n$ denote the set of all congruence classes modulo n, where n is a positive integer. We saw in the first chapter that there are n congruence classes; $\mathbb{Z}_n$ so is a set with n elements:

$\mathbb{Z}_n = \{[0]_n, [1]_n, ..., [n-1]_n\}$

Define addition and multiplication on $\mathbb{Z}_n$ by the rules

$[a]_n + [b]_n = [a + b]_n$, $[a]_n [b]_n = [ab]_n$

There is an important job to do here: we have to show that these definitions do not depend on our choice of representatives of the equivalence classes.

Proposition: For any positive integer n, $\mathbb{Z}_n$, is a commutative ring with identity. It is a field if and only if n is a prime number.

Here, for example, are the addition and multiplication tables of the ring $\mathbb{Z}_5$. We simplify the notation by writing x instead of $[x]_5$.

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

.	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Note, for example, that $2^{-1} = 3$ in this ring.

Rings of Functions

The sum and product of continuous real functions are continuous. So there is a ring $C(\mathbb{R})$ of continuous functions from $\mathbb{R}$ to $\mathbb{R}$, with

$$(f + g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)\, g(x)$$

There are several related rings, such as $C^1(\mathbb{R})$ (the ring of differentiable functions), $C_0(\mathbb{R})$ (the ring of continuous functions satisfying $f(x) \to 0$ as $x \to \pm\infty$), and $C([a, b])$ (the ring of continuous functions on the interval $[a, b]$. All these rings are commutative, and all except $C_0(\mathbb{R})$ have an identity (the constant function with value 1).

These rings are the subject-matter of Functional Analysis.

5.15.2 Properties of Rings

Matrix Rings

The definition of the product of two $n \times n$ matrices now makes sense: AB = D, where

$$D_{ij} = \sum_{k=1}^{n} A_{ik}B_{kj}$$

So we are in the position to prove Proposition on page 113.

A complete proof of this proposition involves verifying all the ring axioms. The arguments are somewhat repetitive; I will give proofs of two of the axioms.

Axiom (A2): Let 0 be the zero element of the ring R, and let O be the zero matrix in $M_n(R)$, satisfying $O_{ij} = 0$ for all i, j. Then O is the zero element of $M_n(R)$: for, given any matrix A,

$$(O + A)_{ij} = O_{ij} + A_{ij} = 0 + A_{ij} = A_{ij}, \quad (A + O)_{ij} = A_{ij} + O_{ij} = A_{ij} + 0 = A_{ij}$$

using the properties of $0 \in R$. So O + A = A + O = A.

Axiom (D): the (i, j) entry of A(B + C) is

$$\sum_{k=1}^{n} A_{ik}(B+C)_{kj} = \sum_{k=1}^{n} A_{ik}B_{kj} + A_{ik}C_{kj}$$

by the distributive law in R; and the (i, j) entry of AB + AC is

$$\sum_{k=1}^{n} A_{ik}B_{kj} + \sum_{k=1}^{n} A_{ik}C_{kj}$$

Why are these two expressions the same? Let us consider the case $n = 2$. The first expression is

$$A_{i_1}B_{1j} + A_{i_1}C_{1j} + A_{i_2}B_{2j} + A_{i_2}C_{2j}$$

while the second is

$$A_{i_1}B_{1j} + A_{i_2}B_{2j} + A_{i_1}C_{1j} + A_{i_2}C_{2j}$$

Now the commutative law for addition allows us to swap the second and third terms of the sum; so the two expressions are equal. Hence A(B + C) = AB + AC for any matrices A, B, C. For $n > 2$, things are similar, but the rearrangement required is a bit more complicated.

The proof of the other distributive law is similar.

Observe what happens in this proof: we use properties of the ring R to deduce properties of M_n (R). To prove the distributive law for $M_n(R)$, we needed the distributive law and the associative and commutative laws for addition in R. Similar things happen for the other axioms.

Polynomial Rings

What exactly is a polynomial? We deferred this question before, but now is the time to face it.

A polynomial Saixi is completely determined by the sequence of its coefficients $a_0, a_1, \ldots$. These have the property that only a finite number of terms in the sequence are non-zero, but we cannot say in advance how many. So we make the following definition:

A polynomial over a ring R is an infinite sequence

$$(a_i)_{i \geq 0} = (a_0, a_1, \ldots)$$

of elements of R, having the property that only finitely many terms are non-zero; that is, there exists an n such that $a_i = 0$ for all $i > n$. If an is the last non-zero term, we say that the degree of the polynomial is n. (Note that, according to this definition, the all-zero sequence does not have a degree.) Now the rules for addition and multiplication are

$$(a_i) + (b_i) = (c_i) \text{ where } c_i = a_i + b_i,$$

$$(a_i) + (b_i) = (d_i) \text{ where } d_i = \sum_{j=0}^{i} a_j b_{i-j}$$

Again, the sum in the definition of multiplication, we think of the polynomial $(a_i)_{i \geq 0}$ of degree n as what we usually write as $\sum_{i=0}^{n} a_i x^i$; the rules we gave agree with the usual ones.

Asserting that the set of polynomials over a ring R is a ring. As for matrices, we have to check all the axioms, which involves a certain amount of tedium. The zero polynomial required by (A2) is the all-zero sequence. Here is a proof of (Ml). You will see that it involves careful work with dummy subscripts!

We have to prove the associative law for multiplication. So suppose that $f = (a_i)$, $g = (b_i)$ and $h = (c_i)$. Then the ith term of f_g is and so $\sum_{j=0}^{i} a_i b_{i-j}$ tne ith term of $(fg)h$ is

$$\sum_{k=0}^{i} \left(\sum_{j=0}^{k} a_j b_{k-j} \right) c_{i-k}$$

Similarly the ith term of f(gh) is

$$\sum_{s=0}^{i} a_s \left(\sum_{t=0}^{i-s} b_t c_{i-s-t} \right)$$

Each term on both sides has the form apbc,cr, where $p, q, r \geq 0$ and $p + q + r = i$. (In the first expression, $p = j, q = k - j, r = i - k$; in the second, $p = s, q = t, r = i - s - t$.) So the two expressions contain the same terms in a different order. By the associative and commutative laws for addition, they are equal.

Check Your Progress

1. Define normal subgroup.
2. What is permutation group?
3. Define ring.

5.16 LET US SUM UP

Arithmetic operations combine two elements of the set of real numbers to give another element of the same set. Such operations are called 'binary operations or binary compositions'. A non-empty set together with one or more binary operations defined on the set is called a Algebraic Structure or Mathematical Structure.

Or we can say an algebraic structure is a set together with closed operation defined over the set.

A *subgroup* of a group G is a subset of G which is a subgroup in its own right (with the same group operation).

A *cyclic group* is a group C which consists of all the powers (positive and negative) of a single element.

Lagrange's Theorem states a very important relation between the orders of a finite group and any subgroup.

A normal subgroup is a special kind of subgroup of a group. Any subgroup H has right and left cosets, which may not be the same. We say that H is a *normal subgroup* of G if the right and left cosets of H in G are the same. A permutation group is a group G whose elements are permutations of a given set M, and whose group operation is the composition of permutations in G (which are thought of as bijective functions from the set *M* to itself).

5.17 KEYWORDS

Commutative: If binary operation on a set S is such that then operation is called Commutative.

Finite Group: If a group consists of a finite number of elements, it is called a finite group.

Infinite Group: If a group contains an infinite number of elements, it is called an infinite group.

Abelian Group or Commutative Group: It is addition to group axioms, operation is also commutative, it is called Abelian Group or Commutative Group.

Cosets: Given any subgroup H of a group G we can construct a partition of G into "cosets" of H.

Homomorphisms: An isomorphism between groups has two properties: it is a bijection; and it preserves the group operation. If we relax the first property but keep the second, we obtain a homomorphism.

Ring: A ring has two operations: the first is called *addition* and is denoted by + (with infix notation); the second is called *multiplication.*

5.18 QUESTIONS FOR DISCUSSION

1. If in group G, $a, b \in G$ and operation is denoted multiplicatively, then prove that:
   (a) $aa = a \Rightarrow a = e$,
   (b) $a^{-1}b^{-1} = b^{-1}a^{-1}$ if $ab = ba$
   (c) $a^{-1}b = b^{a^{-1}}$ if $ab = ba$
2. Prove that a group G with composition denoted. Multiplicatively is an abelian group, if.
   (a) each element is its own inverse.
   (b) $b^{-1}a^{-1}ba = e, \forall\ a, b \in G$
   (c) it has only form elements.
3. When G is abelian group, prove that $\forall\ a, b \in G, (ab)^n = a^n b^n, n \in G$.
4. Let S be the totality of the pairs (a, b) such that $a, b \in R$ and $a \neq 0$. If composition $\not>$ in S is defined by $(a, b) \not> (c, d) = (ac, bc, + d)$ verify that (S, *) is a group.

5. Prove that a non-compensative group has at least six elements.
6. If corresponding to any element $a \in$ group G, there is an element O_a which satisfies a condition. $a + O_a = a$ and $O_a + a = a$, then show that it is necessary that $O_a = 0$ where O is additive identity of G.
7. Is the mathematical system $(Q, \div,)$ a group when Q is the set of all rational numbers and $\div$, is ordinary division?
8. Show that in a group with even number of elements there is at least one element besides identity which is its own inverse.
9. Show that the additive group of integers is a subrgoup of the additive group of national numbers.
10. Show that with respect to addition the set of all even integers is a sub-group of set of all integers.
11. Prove that the integral multiples of 5 form subgroup of additive group of integers.
12. Show that if a commutative group of order 6 contains an element of orders 3, then it is cyclic.
13. Shows that additive groups.

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

    and $G' = \{..., -6, -4, -2, 0, 2, 4, 6, ...\}$ are isomorphic.
14. Prove that multiplicative group $G = \{1, -1, i, -i\}$ is isomorphic to the group G′ of residue classes modulo 4 under additive composition of residue classes.
15. If G be the additive group of all integers and $G' = \{2m : m \in I, I \text{ is the set of integers}\}$ be a multiplicative group, show that G is isomorphic to G′.
16. If R is the additive group of real numbers and R^+, the multiplicative group of all positive real numbers, prove that the map $f: R \to R^+$ defined by $f(x) = e^x$ is an isomorphism.
17. Prove that the multiplicative group $G = \{1, \omega, \omega^2\}$ is isomorphic to the additive group G′ of residue classes (mod 3), where $\omega^3 = 1$.
18. Show that any two cyclic group of the same order are isomorphic.

Check Your Progress: Modal Answers

1. A normal subgroup is a special kind of subgroup of a group. As we know subgroup H has right and left cosets, which may not be the same. We say that H is a *normal subgroup* of G if the right and left cosets of H in G are the same; that is, if $Hx = xH$ for any $x \in G$.
2. A permutation group is a group G whose elements are permutations of a given set M, and whose group operation is the composition of permutations in *G* (which are thought of as bijective functions from the set *M* to itself); the relationship is often written as *(G, M)*. Note that the group of *all* permutations of a set is the symmetric group; the term *permutation group* is usually restricted to mean a subgroup of the symmetric group.
3. Our first class of structures is *rings*. A ring has two operations: the first is called *addition* and is denoted by + (with infix notation); the second is called *multiplication*, and is usually denoted by juxtaposition (but sometimes by with infix notation).

5.19 SUGGESTED READINGS

Anuranjan Misra, *Discrete Mathematics*, Acme Learning pvt ltd.

Richard Johnsonbaugh, *Discrete Mathematics*, Prentice Hall

V. K. Balakrishnan, *Introductory Discrete Mathematics*, Courier Dover Publications,

R. C. Penner, *Discrete Mathematics: Proof Techniques and Mathematical Structures*, World Scientific, 1999

Mike Piff, *Discrete Mathematics: An Introduction for Software* Engineers, Cambridge University Press, 1991

LESSON

6

MATRIX AND DETERMINANTS

CONTENTS

6.0 AIMS AND OBJECTIVES

After studying this lesson, you will be able to:

- Understand concept of matrix and discuss its manipulations
- Discuss determinants and its properties
- Discuss canonical forms of a matrix
- Understand Cayley-Hamiltonian theorm
- Discuss characteristic polynomial

6.1 INTRODUCTION

A matrix (plural matrices, or less commonly matrixes) is a rectangular array of numbers. The horizontal and vertical lines in a matrix are called *rows* and *columns*, respectively. Matrix manipulations include square matrix, unit matrix, etc.

Determinant of a matrix A is defined by the following formula:

$$\det(A) = \sum_{(i_1 i_2 \cdots i_n)} \pm a_{i1}\, a_{i2} \cdots a_{in}$$

6.2 MATRIX

In mathematics, a matrix is a rectangular array of numbers, such as

$$\begin{bmatrix} 1 & 9 & 13 \\ 20 & 55 & 4 \end{bmatrix}.$$

An item in a matrix is called an entry or an element. The example has entries 1, 9, 13, 20, 55, and 4. Entries are often denoted by a variable with two subscripts, as shown on the right. Matrices of the same size can be added and subtracted entry wise and matrices of compatible sizes can be multiplied. These operations have many of the properties of ordinary arithmetic, except that matrix multiplication is not commutative, that is, AB and BA are not equal in general.

A *matrix* is a rectangular arrangement of numbers. *For example,*

$$\mathbf{A} = \begin{bmatrix} 9 & 8 & 6 \\ 1 & 2 & 7 \\ 4 & 9 & 2 \\ 6 & 0 & 5 \end{bmatrix}.$$

An alternative notation uses large parentheses instead of box brackets:

$$\mathbf{A} = \begin{pmatrix} 9 & 8 & 6 \\ 1 & 2 & 7 \\ 4 & 9 & 2 \\ 6 & 0 & 5 \end{pmatrix}.$$

The horizontal and vertical lines in a matrix are called *rows* and *columns*, respectively. The numbers in the matrix are called its *entries* or its *elements*. To specify a matrix's size, a matrix with m rows and n

columns is called an m-by-n matrix or $m \times n$ matrix, while m and n are called its *dimensions*. The above is a 4-by-3 matrix.

A matrix with one row (a $1 \times n$ matrix) is called a row vector, and a matrix with one column (an $m \times 1$ matrix) is called a column vector. Any row or column of a matrix determines a row or column vector, obtained by removing all other rows respectively columns from the matrix. For example, the row vector for the third row of the above matrix A is [4 9 2].

When a row or column of a matrix is interpreted as a value, this refers to the corresponding row or column vector. For instance one may say that two different rows of a matrix are equal, meaning they determine the same row vector. In some cases the value of a row or column should be interpreted just as a sequence of values (an element of R^n if entries are real numbers) rather than as a matrix, for instance when saying that the rows of a matrix are equal to the corresponding columns of its transpose matrix.

6.3 MATRIX MANIPULATIONS

6.3.1 Square Matrix

It is a matrix which has the same number of rows and columns. An n-by-n matrix is known as a square matrix of order n. Any two square matrices of the same order can be added and multiplied. A square matrix A is called invertible or non-singular if there exists a matrix B such that

$$AB = I_n.$$

This is equivalent to $BA = I_n$. Moreover, if B exists, it is unique and is called the inverse matrix of A, denoted A^{-1}.

The entries $A_{i,j}$ form the main diagonal of a matrix. The trace, tr(A) of a square matrix A is the sum of its diagonal entries. While, as mentioned above, matrix multiplication is not commutative, the trace of the product of two matrices is independent of the order of the factors: tr(AB) = tr(BA).

If all entries outside the main diagonal are zero, A is called a diagonal matrix. If only all entries above (below) the main diagonal are zero, A is called a lower triangular matrix (upper triangular matrix, respectively). For example, if n = 3, they look like

$$\begin{bmatrix} d_{11} & 0 & 0 \\ 0 & d_{22} & 0 \\ 0 & 0 & d_{33} \end{bmatrix} \text{(diagonal)}, \quad \begin{bmatrix} l_{11} & 0 & 0 \\ l_{21} & l_{22} & 0 \\ l_{31} & l_{32} & l_{33} \end{bmatrix} \text{(lower) and} \quad \begin{bmatrix} u_{11} & u_{12} & u_{13} \\ 0 & u_{22} & u_{23} \\ 0 & 0 & u_{33} \end{bmatrix} \text{(upper triangular matrix).}$$

6.3.2 Unit Matrix

In linear algebra, the identity matrix or unit matrix of size n is the n-by-n square matrix with ones on the main diagonal and zeros elsewhere. It is denoted by I_n, or simply by I if the size is immaterial or can be trivially determined by the context. (In some fields, such as quantum mechanics, the identity matrix is denoted by a boldface one, 1; otherwise it is identical to I.)

$$I_1 = [1],\ I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ \cdots,\ I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

Some mathematics books use U and E to represent the Identity Matrix (meaning "Unit Matrix" and "Elementary Matrix", or from the German "Einheitsmatrix", respectively), although I is considered more universal.

The important property of matrix multiplication of identity matrix is that for m-by-n A

$I_m A = AI_n = A.$

In particular, the identity matrix serves as the unit of the ring of all n-by-n matrices, and as the identity element of the general linear group GL (n) consisting of all invertible n-by-n matrices. (The identity matrix itself is invertible, being its own inverse.)

6.3.3 Zero/Null Matrix

In mathematics, particularly linear algebra, a zero matrix is a matrix with all its entries being zero. Some examples of zero matrices are

$$0_{1,1} = [0],\ 0_{2,2} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},\ 0_{2,3} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

The set of $m \times n$ matrices with entries in a ring K forms a ring $K_{m,n}$. The zero matrix $K_{m,n}$ in $K_{m,n}$ is the matrix with all entries equal to 0_K, where 0_K is the additive identity in K.

$$0_{K_{m,n}} = \begin{bmatrix} 0_K & 0_K & \cdots & 0_K \\ 0_K & 0_K & \cdots & 0_K \\ \vdots & \vdots & & \vdots \\ 0_K & 0_K & \cdots & 0_K \end{bmatrix}_{m \times n}$$

The zero matrix is the additive identity in $K_{m,n}$. That is, for all $A \in K_{m,n}$, it satisfies

$0_{Km,n} + A = A + 0_{m,n} = A.$

There is exactly one zero matrix of any given size $m \times n$ having entries in a given ring, so when the context is clear one often refers to *the* zero matrix. In general the zero element of a ring is unique and typically denoted as 0 without any subscript indicating the parent ring. Hence the examples above represent zero matrices over any ring.

6.3.4 Matrix Addition

In mathematics, matrix addition is the operation of adding two matrices by adding the corresponding entries together. However, there is another operation which could also be considered as a kind of addition for matrices.

Entrywise sum

The usual matrix addition is defined for two matrices of the same dimensions. The sum of two *m*-by-*n* matrices *A* and *B*, denoted by *A* + *B*, is again an *m*-by-*n* matrix computed by adding corresponding elements. For example:

$$\begin{bmatrix} 1 & 3 \\ 1 & 0 \\ 1 & 2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 7 & 5 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1+0 & 3+0 \\ 1+7 & 0+5 \\ 1+2 & 2+1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 8 & 5 \\ 3 & 3 \end{bmatrix}$$

We can also subtract one matrix from another, as long as they have the same dimensions. *A* - *B* is computed by subtracting corresponding elements of *A* and *B*, and has the same dimensions as *A* and *B*. For example:

$$\begin{bmatrix} 1 & 3 \\ 1 & 0 \\ 1 & 2 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 7 & 5 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1-0 & 3-0 \\ 1-7 & 0-5 \\ 1-2 & 2-1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ -6 & -5 \\ -1 & 1 \end{bmatrix}$$

6.3.5 Matrix Multiplication

Multiplication of two matrices is defined only if the number of columns of the left matrix is the same as the number of rows of the right matrix. If A is an *m*-by-*n* matrix and B is an *n*-by-*p* matrix, then their *matrix product* AB is the *m*-by-*p* matrix whose entries are given by dot-product of the corresponding row of A and the corresponding column of B:

$$[\mathbf{AB}]_{i,j} = A_{i,1}B_{1,j} + A_{i,2}B_{2,j} + \cdots + A_{i,n}B_{n,j} = \sum_{r=1}^{n} A_{i,r}B_{r,j},$$

Where $1 \le i \le m$ and $1 \le j \le p$.For example (the underlined entry 1 in the product is calculated as the product $1 \cdot 1 + 0 \cdot 1 + 2 \cdot 0 = 1$):

$$\begin{bmatrix} \underline{1} & \underline{0} & \underline{2} \\ -1 & 3 & 1 \end{bmatrix} \times \begin{bmatrix} 3 & \underline{1} \\ 2 & \underline{1} \\ 1 & \underline{0} \end{bmatrix} = \begin{bmatrix} 5 & \underline{1} \\ 4 & 2 \end{bmatrix}.$$

Matrix multiplication satisfies the rules (AB) C = A (BC) (associativity), and (A+B) C = AC+BC as well as C (A+B) = CA+CB (left and right distributivity), whenever the size of the matrices is such that the various products are defined. The product AB may be defined without BA being defined, namely if A and B are *m*-by-*n* and *n*-by-*k* matrices, respectively, and $m \neq k$. Even if both products are defined, they need not be equal, i.e. generally one has AB ≠ BA, i.e., matrix multiplication is not commutative, in marked contrast to (rational, real, or complex) numbers whose product is independent of the order of the factors. An example of two matrices not commuting with each other is:

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 3 \end{bmatrix},$$

Whereas

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 0 & 0 \end{bmatrix}.$$

The identity matrix I_n of size n is the n-by-n matrix in which all the elements on the main diagonal are equal to 1 and all other elements are equal to 0, e.g.

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

It is called identity matrix because multiplication with it leaves a matrix unchanged: $MI_n = I_mM = M$ for any m-by-n matrix M.

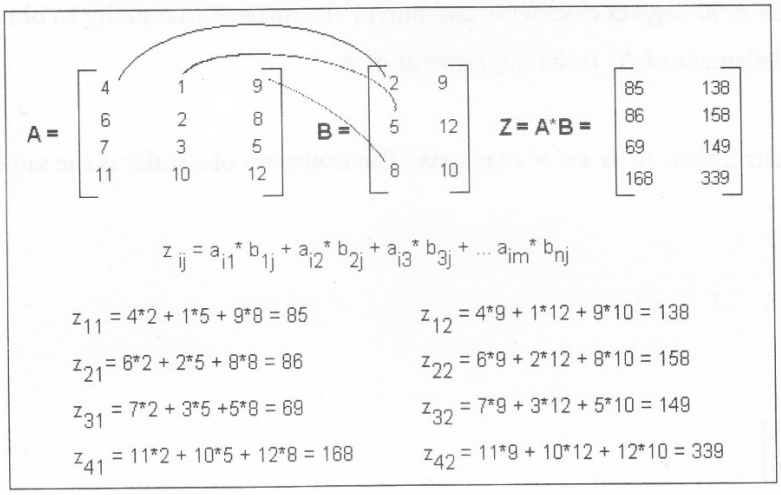
Consider another example of multiplication of Matrices:

Consider two matrices A and B with the following characteristics: the number of columns in A equals the number of rows in B. These are conformable with respect to one another, and they can be multiplied together to form a new matrix Z.

The expression

$z_{ij} = a_{i1} * b_{1j} + a_{i2} * b_{2j} + a_{i3} * b_{3j} + \ldots a_{im} * b_{nj}$

means "add the products obtained by multiplying elements in each i row of matrix A by elements in each j column of matrix B". Figure below illustrates what we mean by this statement.



Note: A * B and B * A will different results!!!

Scalar Multiplication

The matrix obtained by multiplying every element of a matrix A by a scalar λ is called the scalar multiple of A by λ.

$$A = \begin{vmatrix} 2 & 3 & 5 \\ 6 & 7 & 8 \end{vmatrix}_{2 \times 3}$$

For example:

$$\text{Thus,} = \begin{bmatrix} 4 & 6 & 10 \\ 12 & 14 & 16 \end{bmatrix}_{2 \times 3}$$

Properties of Scalar Multiplication

All the laws of ordinary algebra hold for the addition or subtraction of matrices and their multiplication by scalars.

(i) If A and B be two matrices of the same order and if k be a scalar, then

$k(A + B) = kA + kB$

(ii) If k_1 and k_2 are two scalars and if A is a matrix, then

$(k_1 + k_2)A = k_1A + k_2A$ and $k_1(k_2A) = k_2(k_1A)$

6.3.6 Transposition of Matrix

In linear algebra, the transpose of a matrix A is another matrix A^T (also written A', A^{tr} or ${}^tA$) created by any one of the following equivalent actions:

- write the rows of A as the columns of A^T
- write the columns of A as the rows of A^T
- reflect A by its main diagonal (which starts from the top left) to obtain A^T
- visually rotate A 90 degrees clockwise, and mirror the image horizontally to obtain A^T

Formally, the (i,j) element of A^T is the (j,i) element of A.

$[A^T]_{ij} = [A]_{ji}$

If A is a $m \times n$ matrix then A^T is a $n \times m$ matrix. The transpose of a scalar is the same scalar.

Examples

$$[1 \quad 2]^T = \begin{bmatrix} 1 \\ 2 \end{bmatrix}.$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}^T = \begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix}.$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}^T = \begin{bmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{bmatrix}.$$

Properties

For matrices A, B and scalar *c* we have the following properties of transpose:

$(A^T)^T = A$

Taking the transpose is an involution (self inverse).

$(A + B)^T = A^T + B^T$

The transpose respects addition.

$(AB)^T = B^T A^T$

Note that the order of the factors reverses. From this one can deduce that a square matrix A is invertible if and only if A^T is invertible, and in this case we have $(A^{-1})^T = (A^T)^{-1}$. It is relatively easy to

extend this result to the general case of multiple matrices, where we find that $(ABC...XYZ)^T = Z^TY^TX^T...C^TB^TA^T$.

$(cA)^T = cA^T$

The transpose of a scalar is the same scalar. Together with this, this states that the transpose is a linear map from the space of $m \times n$ matrices to the space of all $n \times m$ matrices.

$\text{Det}(A^T) = \det(A)$

The determinant of a square matrix is the same as that of its transpose.

The dot product of two column vectors a and b can be computed as

$a \cdot b = a^T b,$

which is written as $a_i b^i$ in Einstein notation.

If A has only real entries, then A^TA is a positive-semide finite matrix.

$(A^T)^{-1} = (A^{-1})^T$

The transpose of an invertible matrix is also invertible, and its inverse is the transpose of the inverse of the original matrix. The notation A^{-T} is often used to represent either of these equivalent expressions.

If A is a square matrix, then its eigenvalues are equal to the eigenvalues of its transpose.

Special Transpose Matrices

A square matrix whose transpose is equal to itself is called a symmetric matrix; that is, A is symmetric if

$A^T = A.$

A square matrix whose transpose is also its inverse is called an orthogonal matrix; that is, G is orthogonal if

$GG^T = G^TG = I_n$, the identity matrix, i.e. $G^T = G^{-1}$.

A square matrix whose transpose is equal to its negative is called skew-symmetric matrix; that is, A is skew-symmetric if

$A^T = -A.$

The conjugate transpose of the complex matrix A, written as A^*, is obtained by taking the transpose of A and the complex conjugate of each entry:

$A^* = \overline{(A)}^T = \overline{\left(A^T\right)}.$

6.3.7 Inverted Matrices

In linear algebra an *n*-by-*n* (square) matrix A is called invertible or nonsingular or nondegenerate, if there exists an *n*-by-*n* matrix B such that,

$AB = BA = I_n$

Where, I_n denotes the *n*-by-*n* identity matrix and the multiplication used is ordinary matrix multiplication. If this is the case, then the matrix B is uniquely determined by A and is called the *inverse* of A, denoted by A^{-1}. It follows from the theory of matrices that if

$AB = I$

for *square* matrices A and B, then also

$BA = I.$

Non-square matrices (m-by-n matrices for which $m \neq n$) do not have an inverse. However, in some cases such a matrix may have a left inverse or right inverse. If A is m-by-n and the rank of A is equal to n, then A has a left inverse: an n-by-m matrix B such that BA = I. If A has rank m, then it has a right inverse: an n-by-m matrix B such that AB = I.

A square matrix that is not invertible is called singular or degenerate. A square matrix is singular if and only if its determinant is 0. Singular matrices are rare in the sense that if you pick a random square matrix, it will almost surely not be singular.

While the most common case is that of matrices over the real or complex numbers, all these definitions can be given for matrices over any commutative ring. However, in this case the condition for a square matrix to be invertible is that its determinant is invertible in the ring, which in general is a much stricter requirement than being nonzero.

Matrix inversion is the process of finding the matrix B that satisfies the prior equation for a given invertible matrix A.

The following properties hold for an invertible matrix A:

$(A^{-1})^{-1} = A$

$(kA)^{-1} = k^{-1} A^{-1}$

for nonzero scalar k

$(A^T)^{-1} = (A^{-1})^T$

For any invertible n×n matrices A and B $(AB)^{-1} = B^{-1} A^{-1}$. More generally, if A1,...,Ak are invertible n×n matrices, then $(A_1 A_2 \cdots A_k)^{-1} = A_k^{-1} A_{k-1}^{-1} \cdots A_1^{-1}$

$\det(A^{-1}) = \det(A)^{-1}$

A matrix that is its own inverse, i.e. $A = A^{-1}$ and $A^2 = I$, is called an involution.

For matrices , DIVISION property of algebra , did not exist but Indirectly Matrices supports this with its INVERSE terminology.

Note: 1 may be called the Universal identity because multiplying something by 1 doesn't change its value.

This terminology and these facts are very important for matrices. If you are given a matrix equation like $AX = C$, where you are given A and C and are told to figure out X, you would like to "divide off" the matrix A. But you can't do division with matrices. On the other hand, what if you could find the inverse of A, something similar to finding the reciprocal fraction above? The inverse of A, written as

"A^{-1}" and pronounced "A inverse", would allow you to cancel off the A from the matrix equation and then solve for X.

$$\begin{aligned} AX &= C \\ A^{-1}AX &= A^{-1}C \\ IX &= A^{-1}C \\ X &= A^{-1}C \end{aligned}$$

How did "$A^{-1}AX$" on the left-hand side of the equation turn into "X"? Think back to the nature of inverses for regular numbers. If you have a number (such as 3/2) and its inverse (in this case, 2/3) and you multiply them, you get 1. And 1 is the identity, so called because $1x = x$ for any number x. It works the same way for matrices. If you multiply a matrix (such as A) and its inverse (in this case, A^{-1}), you get the identity matrix I. And the point of the identity matrix is that $IX = X$ for any matrix X (meaning "any matrix of the correct size", of course).

Example :

$$A = \begin{bmatrix} 1 & 1 & 2 \\ 2 & 1 & 2 \\ 1 & 1 & 1 \end{bmatrix} \quad B = \begin{bmatrix} -1 & 1 & 0 \\ 0 & -1 & 2 \\ 1 & 0 & -1 \end{bmatrix}$$

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

In this case B is called the inverse of A. We write $B = A^{-1}$.

6.4 DETERMINANTS

If A $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, we define the determinant of A, (also denoted by det A,) to be the scalar

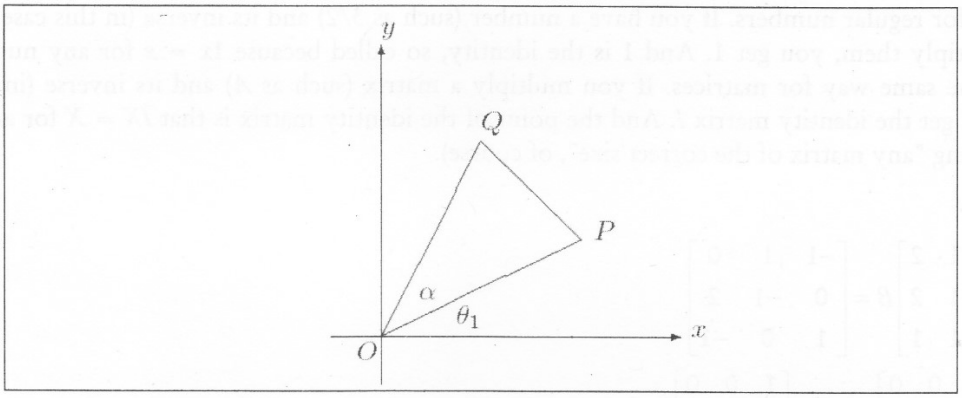
$$\det A = a_{11}a_{22} - a_{12}a_{21}.$$

The notation $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ is also used for the determinant of A.

If A is a real matrix, there is a geometrical interpretation of det A. If P = (x_1, y_1) and Q = (x_2, y_2) are points in the plane, forming a triangle with the origin O = (0, 0), then apart from sign, $\frac{1}{2}\begin{bmatrix} x_1 & y_1 \\ x_2 & y_2 \end{bmatrix}$ is the area of the triangle OPQ. For, using polar coordinates, let $x_1 = r_1 \cos\theta_1$ and $y_1 = r_1 \sin\theta_1$, where $r_1 = OP$ and θ_1 is the angle made by the ray $\overrightarrow{OP}$ with the positive x-axis. Then triangle OPQ has area, $\frac{1}{2}OP \cdot OP \sin\alpha$, where $\alpha = \angle POQ$. If the triangle OPQ has anti-clockwise orientation, then the ray $\overrightarrow{OP}$ makes angle $\theta_2 = \theta_1 + \alpha$ with the positive x-axis.

Also $x_2 = r_2 \cos\theta_2$ and $y_2 = r_2 \sin\theta_2$. Hence

$$\begin{aligned}
\text{Area } OPQ &= \frac{1}{2} OP \cdot OQ \sin\alpha \\
&= \frac{1}{2} OP \cdot OQ \sin(\theta_2 - \theta_1) \\
&= \frac{1}{2} OP \cdot OQ (\sin\theta_2 \cos\theta_1 - \cos\theta_2 \sin\theta_1) \\
&= \frac{1}{2} (OQ \sin\theta_2 \cdot OP \cos\theta_1 - OQ \cos\theta_2 \cdot OP \sin\theta_1)
\end{aligned}$$



Area of Triangle OPQ

$$= \frac{1}{2}(y_2 x_1 - x_2 y_1)$$

$$= \frac{1}{2}\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}.$$

Similarly, if triangle OPQ has clockwise orientation, then its area equals $-\frac{1}{2}\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}$.

For a general triangle $P_1P_2P_3$, with $P_i = (x_i, y_i)$, $i = 1, 2, 3$, we can take P_1 as the origin. Then the above formula gives

$$\frac{1}{2}\begin{vmatrix} x_2 - x_1 & y_2 - y_1 \\ x_3 - x_1 & y_3 - y_1 \end{vmatrix} \quad \text{or} \quad -\frac{1}{2}\begin{vmatrix} x_2 - x_1 & y_2 - y_1 \\ x_3 - x_1 & y_3 - y_1 \end{vmatrix},$$

according as vertices $P_1P_2P_3$ are anti-clockwise or clockwise oriented.

We now give a recursive definition of the determinant of an $n \times n$ matrix $A = [a_{ij}]$, $n \geq 3$.

6.4.1 Definition

Let $M_{ij}(A)$ (or simply M_{ij} if there is no ambiguity) denote the determinant of the $(n-1) \times (n-1)$ submatrix of A formed by deleting the i^{-th} row and j^{-th} column of A. ($M_{ij}(A)$ is called the (i, j) minor of A.)

Assume that the determinant function has been defined for matrices of size(n−− 1)×× (n−− 1). Then det A is defined by the so-called first-row Laplace expansion:

$$\begin{aligned}\det A &= a_{11}M_{11}(A) - a_{12}M_{12}(A) + \ldots + (-1)^{1+n}M_{1n}(A)\\ &= \sum_{j=1}^{n}(-1)^{1+j}a_{1j}M_{1j}(A).\end{aligned}$$

For example, if $A = [a_{ij}]$ is a 3×3 matrix, the Laplace expansion gives

$$\begin{aligned}&\det A = a_{11}M_{11}(A) - a_{12}M_{12}(A) + a_{13}M_{13}(A)\\ &= a_{11}\begin{vmatrix} a_{22} & a_{23}\\ a_{32} & a_{33}\end{vmatrix} - a_{12}\begin{vmatrix} a_{21} & a_{23}\\ a_{31} & a_{33}\end{vmatrix} + a_{13}\begin{vmatrix} a_{21} & a_{22}\\ a_{31} & a_{32}\end{vmatrix}\\ &= a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31})\\ &= a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}.\end{aligned}$$

Example: If $P_1P_2P_3$ is a triangle with $P_i = (x_i, y_i)$, $i = 1, 2, 3$, then the area of triangle $P_1P_2P_3$ is

$$\frac{1}{2}\begin{vmatrix} x_1 & y_1 & 1\\ x_2 & y_2 & 1\\ x_3 & y_3 & 1\end{vmatrix} \quad \text{or} \quad -\frac{1}{2}\begin{vmatrix} x_1 & y_1 & 1\\ x_2 & y_2 & 1\\ x_3 & y_3 & 1\end{vmatrix},$$

According as the orientation of $P_1P_2P_3$ is anticlockwise or clockwise.

As according to the definition of 3×3 determinants, we have

$$\begin{aligned}\frac{1}{2}\begin{vmatrix} x_1 & y_1 & 1\\ x_2 & y_2 & 1\\ x_3 & y_3 & 1\end{vmatrix} &= \frac{1}{2}\left(x_1\begin{vmatrix} y_2 & 1\\ y_3 & 1\end{vmatrix} - y_1\begin{vmatrix} x_2 & 1\\ x_3 & 1\end{vmatrix} + \begin{vmatrix} x_2 & y_2\\ x_3 & y_3\end{vmatrix}\right)\\ &= \frac{1}{2}\begin{vmatrix} x_2 - x_1 & y_2 - y_1\\ x_3 - x_1 & y_3 - y_1\end{vmatrix}.\end{aligned}$$

Properties of determinants that follows immediately from the definition are the following:

6.4.2 Properties of Determinants

1. Rows and columns can be interchanged without affecting the value of a determinant. That is:
   $|\mathbf{A}| = |\mathbf{A}^T|$
2. If two rows (or columns) are interchanged the sign of the determinant is changed. For example:
   $$\begin{vmatrix} 3 & 4\\ 1 & -2\end{vmatrix} = -\begin{vmatrix} 1 & -2\\ 3 & 4\end{vmatrix}$$
3. If a row (or column) is changed by adding to or subtracting from its element the corresponding elements of any other row (or column) the determinant remains unaltered. For example:
   $$\begin{vmatrix} 3 & 4\\ 1 & -2\end{vmatrix} = \begin{vmatrix} 3+1 & 4-2\\ 1 & -2\end{vmatrix} = \begin{vmatrix} 4 & 2\\ 1 & -2\end{vmatrix} = -10$$

4. If the elements in any row (or column) have a common factor α then the determinant equals the determinant of the corresponding matrix in which $\alpha = 1$, multiplied by α. For example:

$$\begin{vmatrix} 6 & 8 \\ 1 & -2 \end{vmatrix} = 2 \begin{vmatrix} 3 & 4 \\ 1 & -2 \end{vmatrix} = 2 \times (-10) = -20.$$

5. When at least one row (or column) of a matrix is a linear combination of the other rows (or columns) the determinant is zero. Conversely, if the determinant is zero, then at least one row and one column are linearly dependent on the other rows and columns, respectively. For example, consider

$$\begin{vmatrix} 3 & 2 & 1 \\ 1 & 2 & -1 \\ 2 & -1 & 3 \end{vmatrix}$$

This determinant is zero because the first column is a linear combination of the second and third columns:

column 1 = column 2 + column 3

Similarly there is a linear dependence between the rows which is given by the relation.

Row 1 = 7/8 row 2 + 4/5 row 3

6. The determinant of an upper triangular or lower triangular matrix is the product of the main diagonal entries. For example,

$$\begin{vmatrix} 3 & 2 & 1 \\ 0 & 2 & -1 \\ 0 & 0 & 4 \end{vmatrix} = 3 \times 2 \times 4 = 24$$

This rule is easily verified from the definition because all terms vanish except $j_1 = 1, j_2 = 2, \ldots j_n = n$, which is the product of the main diagonal entries. Diagonal matrices are a particular case of this rule.

7. The determinant of the product of two square matrices is the product of the individual determinants:

$|\mathbf{AB}| = |\mathbf{A}|\,|\mathbf{B}|$

This rule can be generalized to any number of factors. One immediate application is to matrix powers: $|\mathbf{A}^2| = |\mathbf{A}|\,|\mathbf{A}| = |\mathbf{A}|^2$, and more generally $|\mathbf{A}^n| = |\mathbf{A}|^n$ for integer n.

8. The determinant of the transpose of a matrix is the same as that of the original matrix:

$|\mathrm{A}^{\mathrm{T}}| = |\mathrm{A}|$

6.4.3 Theorems of Determinants

The following theorems can be proved by straights-forward inductions on the size of the matrix.

Theorem1: A matrix and its transpose have equal determinants; that is

$$\text{Det } \mathrm{A}^{\mathrm{t}} = \text{det A}.$$

Definitions

Adjoint: If $A = [a_{i,j}]$ is an ${}^{n}X_{n}$ matrix, the adjoint of A, denoted by adj A, is the transpose of the matrix of co-factors.

Hence, adj $A = \begin{vmatrix} C_{11} & C_{21} & .... & C_{n1} \\ C_{12} & C_{22} & .... & C_{n2} \\ \vdots & & & \vdots \\ C_{1n} & C_{2n} & .... & C_{nn} \end{vmatrix}$

Theorem 2: Let A be an nXn matrix.

Then, A (adj A) = (det A) In = (adj A) A.

Proof:

$$(A \text{ adj } A)_{ik} = \sum_{j=1}^{n} a_{ij} (\text{adj } A)_{jk}$$

$$= \sum_{j=1}^{n} a_{ij} C_{kj} (A)$$

$$= S_{ik} \det A$$

$$= ((\det A) I_n) ik .....$$

Hence, A (adj A) = (det A) I_n.

Corollary formula for the inverse; If det $A \neq 0$, then A is non-singular and

$$A^{-1} = \frac{1}{\det A} \text{ adj } A.$$

Theorem 3: The determinant is a linear function of each row and column.

E.g. 1. $\begin{vmatrix} a_{11} + a'_{11} & a_{12} + a'_{12} & a_{13} + a'_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} a'_{11} & a'_{12} & a'_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$

2. $\begin{vmatrix} ta_{11} & ta_{12} & ta_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = t \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$

Corollary: If a multiple of a row is added to another row, the value of the determinant is unchanged. Similarly for columns.

Proof: We illustrate with a 3×3 example, but the proof is really quite general.

$$\begin{vmatrix} a_{11} + ta_{21} & a_{12} + ta_{22} & a_{13} + ta_{23} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} + \begin{vmatrix} ta_{21} & ta_{22} & ta_{23} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

$$= \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} + t \begin{vmatrix} a_{21} & a_{22} & a_{23} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

$$= \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} + t \times O$$

$$= \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

Theorem 4: Let A be an n × n matrix.

Then, (i) A is non-singular if and if det A ≠ O

(ii) A is singular if and only if det A = O;

(iii) the homogeneous system AX = O has a non-trivial solution if and only if det A = O.

Theorem 5: Cramer's Rule

The system of 'n' linear equations in 'n' unknowns x_1 ...., x_n.

$a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = b_1$

.....

.....

$A_{n1}x_1 + a_{n2}x_2 + ... + a_{nn}x_n = b_n$

has a unique solution if $\Delta = \det [a_{ij}] \neq O$, namely

$$x_1 = \frac{\Delta_1}{\Delta}, x_2 = \frac{\Delta_2}{\Delta}, ..., x_n = \frac{\Delta_n}{\Delta}$$

where Δ_i is the determinant of the matrix formed by replacing the i-th column of the co-efficient matrix. A by the entries b_1, b_2, ..., b_n.....

Proof: Suppose the coefficient determinant $\Delta \neq 0$.

Then, by corollary, A^{-1} exists and is given by $A^{-1} = \frac{1}{\Delta}$ adj A and the system has the unique solution.

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = A^{-1} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = \frac{1}{\Delta} \begin{bmatrix} C_{11} & C_{21} & \dots & C_{n1} \\ C_{12} & C_{22} & \dots & C_{n2} \\ \vdots & & & \vdots \\ C_{1n} & C_{2n} & \dots & C_{nn} \end{bmatrix}$$

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = \frac{1}{\Delta} \begin{bmatrix} b_1C_{11} + b_2C_{21} + \dots + b_nC_{n1} \\ b_2C_{12} + b_2C_{22} + \dots + b_nC_{n2} \\ \vdots \quad\quad\quad\quad \vdots \\ b_nC_{1n} + b_2C_{2n} + \dots + b_nC_{nn} \end{bmatrix}$$

However, the i-th component of the last vector is the expansion of Δ_i along column i, Hence

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \frac{1}{\Delta} \begin{bmatrix} \Delta_1 \\ \Delta_2 \\ \vdots \\ \Delta_n \end{bmatrix} = \begin{bmatrix} \Delta_1 / \Delta \\ \Delta_2 / \Delta \\ \vdots \\ \Delta_n / \Delta \end{bmatrix}$$

6.5 CANONICAL FORMS OF A MATRIX

6.5.1 Jordan Canonical Form

The Jordan canonical form is also known as classical canonical form. It is basically a type of block matrix where each block contains Jordan blocks with differing constants λ_i. In particular, it is a block matrix of the form given below:

$$\begin{vmatrix} \lambda_1 & 1 & 0 & \cdots & 0 & & & & & \\ 0 & \lambda_1 & 1 & \ddots & 0 & & & & & \\ 0 & 0 & \lambda_1 & \ddots & 0 & & & & & \\ \vdots & \ddots & \ddots & \ddots & 1 & & & & & \\ 0 & 0 & 0 & \cdots & \lambda_1 & & & & & \\ & & & & & \ddots & & & & \\ & & & & & & \lambda_k & 1 & 0 & \cdots & 0 \\ & & & & & & 0 & \lambda_k & 1 & \ddots & 0 \\ & & & & & & 0 & 0 & \lambda k & \ddots & 0 \\ & & & & & & \vdots & \ddots & \ddots & \ddots & 1 \\ & & & & & & 0 & 0 & 0 & \cdots & \lambda_k \end{vmatrix}$$

6.5.2 Rational Canonical Form

The rational canonical form is a special one which shows the extent to which the minimal polynomial characterizes a matrix.

Any square matrix T has a canonical form and there is no need to extend the field of its coefficients. If the entries of T are rational numbers, then so are the entries of its rational canonical form consists of the similar entries.

6.6 CAYLEY-HAMILTONIAN THEORM

Let us consider

$$A = \begin{vmatrix} a_{11} - x & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} - x & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m2} & a_{m2} & \cdots & a_{mm} - x \end{vmatrix} \quad (1)$$

$$= x^m + c_{m-1}x^{m-1} + \cdots + c_0. \quad (2)$$

then

$$A^m + c_{m-1}A^{m-1} + \cdots + c_0 I = 0 \tag{3}$$

where I is the identity matrix. Cayley verified this identity for m=2 and 3 and stated that it was true for all m. For m=2, it gives the following:

$$\begin{vmatrix} a-x & b \\ c & d-x \end{vmatrix} = (a-x)(d-x) - bc \tag{4}$$

$$= x^2 - (a+d)x + (ad - bc) \tag{5}$$

$$\equiv x^2 + c_1 x + c_2 \tag{6}$$

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{7}$$

$$A^2 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{8}$$

$$= \begin{bmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{bmatrix} \tag{9}$$

$$-(a+d)A = \begin{bmatrix} -a^2 - ad & -ab - bd \\ -ac - dc & -ad - d^2 \end{bmatrix} \tag{10}$$

$$(ad - bc)I = \begin{bmatrix} ad - bc & 0 \\ 0 & ad - bc \end{bmatrix}, \tag{11}$$

so

$$A^2 - (a+d)A + (ad - bc)I = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}. \tag{12}$$

The Cayley-Hamilton theorem states that an $n \times n$ matrix A is annihilated by its characteristic polynomial det (x 1=A), which is monic of degree n. Characteristic polynomial is discussed below.

6.7 CHARACTERISTIC POLYNOMIAL

The left-hand side of the characteristic equation is considered as characteristic polynomial. Consider the following equation:

$$\text{Det } (A - \lambda I) = 0, \tag{1}$$

Here A is a square matrix and I is the identity matrix . Both are of identical dimensions. The characteristic polynomial is allowed to be calculated recursively without divisions. The characteristic polynomial of a matrix m may be computed as Characteristic Polynomial[m, x].

6.8 SOLVED EXAMPLES

1. The matrix $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 8 & 8 & 9 \end{bmatrix}$ is non-singular. For

$$\det A = \begin{vmatrix} 5 & 6 \\ 8 & 9 \end{vmatrix} - 2 \begin{vmatrix} 4 & 6 \\ 8 & 9 \end{vmatrix} + 3 \begin{vmatrix} 4 & 5 \\ 8 & 8 \end{vmatrix}$$

$$= -3 + 24 - 24$$

$$= -3 \neq 0$$

Also,

$$A^{-1} = \frac{1}{-3} \begin{bmatrix} C_{11} & C_{21} & C_{31} \\ C_{12} & C_{22} & C_{32} \\ C_{13} & C_{23} & C_{33} \end{bmatrix}$$

$$= -\frac{1}{3} \begin{bmatrix} \begin{vmatrix} 5 & 6 \\ 8 & 9 \end{vmatrix} & -\begin{vmatrix} 2 & 3 \\ 8 & 9 \end{vmatrix} & \begin{vmatrix} 2 & 3 \\ 5 & 6 \end{vmatrix} \\ -\begin{vmatrix} 4 & 6 \\ 8 & 9 \end{vmatrix} & \begin{vmatrix} 1 & 3 \\ 8 & 9 \end{vmatrix} & -\begin{vmatrix} 1 & 3 \\ 4 & 6 \end{vmatrix} \\ \begin{vmatrix} 4 & 5 \\ 8 & 8 \end{vmatrix} & -\begin{vmatrix} 1 & 2 \\ 8 & 8 \end{vmatrix} & \begin{vmatrix} 1 & 2 \\ 4 & 5 \end{vmatrix} \end{bmatrix}$$

$$= -\frac{1}{3} \begin{bmatrix} -3 & 6 & -3 \\ 12 & -15 & 6 \\ -8 & 8 & -3 \end{bmatrix}$$

2. Evaluate the determinant $\begin{vmatrix} 1 & 1 & 2 & 1 \\ 3 & 1 & 4 & 5 \\ 7 & 6 & 1 & 2 \\ 1 & 1 & 3 & 4 \end{vmatrix}$

Solution: $\begin{vmatrix} 1 & 1 & 2 & 1 \\ 3 & 1 & 4 & 5 \\ 7 & 6 & 1 & 2 \\ 1 & 1 & 3 & 4 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 2 & 1 \\ 0 & -2 & -2 & 2 \\ 0 & -1 & -13 & -5 \\ 0 & 0 & 0 & 3 \end{vmatrix}$

$$= -2 \begin{vmatrix} 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & -1 \\ 0 & -1 & -13 & -5 \\ 0 & 0 & 1 & 3 \end{vmatrix} = -2 \begin{vmatrix} 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & -12 & -6 \\ 1 & 0 & 1 & 3 \end{vmatrix}$$

$$= 2\begin{vmatrix} 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & -12 & -6 \end{vmatrix} = 2\begin{vmatrix} 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 30 \end{vmatrix} = 60$$

3. Vander-monde determinant: Prove that,

$$\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix} = (b-a)\,(c-a)\,(c-b)$$

Solution: Subtracting column 1 from columns 2 and 3, then expanding along row 1, gives

$$= \begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ a & b-a & c-a \\ a^2 & b^2-a^2 & c^2-a^2 \end{vmatrix} = \begin{vmatrix} b-a & c-a \\ b^2-a^2 & c^2-a^2 \end{vmatrix}$$

$$= (b-a)\,(c-a)\begin{vmatrix} 1 & 1 \\ b+a & c+a \end{vmatrix}$$

$$= (b-a)\,(c-a)\,(c-b)$$

Remarks: (i) $\det(E_{ij}\,A) = -\det A$,

(ii) $\det(E_i(t)A) = t \det A$, if $t \neq 0$,

(iii) $\det(E_{ij}(t)A) = \det A$

4. Find the rational numbers 'a' for which the following homogenous system has a non-trivial solution and solve the system for these values of a:

$$x - 2y + 3z = 0$$

$$ax + 3y + 2z = 0$$

$$6x + y + az = 0$$

Solution: The coefficient determinant of the system is,

$$\Delta = \begin{vmatrix} 1 & -2 & 3 \\ a & 3 & 2 \\ 6 & 1 & a \end{vmatrix} = \begin{vmatrix} 1 & -2 & 3 \\ 0 & 3+2a & 2-3a \\ 0 & 13 & a-18 \end{vmatrix}$$

$$= \begin{vmatrix} 3+2a & 2-3a \\ 13 & a-18 \end{vmatrix} = (3 + 2a)\,(a - 18) - 13\,(2 - 3a)$$

$$= 2a^2 + 6a - 80 = 2(a + 8)\,(a - 5)$$

So, $\Delta = 0 \leftrightarrow a = -8$ or $a = 5$ and these values of 'a' are the only values for which the given homogenous system has a non-trivial solution.

If $a = -8$, the coefficient matrix has reduced row-echelon form equal to

$$\begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{bmatrix}$$

and, so the complete solution is $x = z$, $y = 2z$, with z arbitrary. If $a = 5$, the coefficient matrix has reduced row-echelon form equal to:

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

and, so the complete solution is $x = -'z'$, $'y' = 'z'$, with 'z' arbitrary.

5. Find the values of 't' for which the following system is consistent and solve the system in each case:

$$x + y = 1$$

$$tx + y = t$$

$$(1 + t)x + 2y = 3$$

Solution: Suppose that the given system has a solution (x_0, y_0). Then the following homogeneous system:

$$x + y + z = 0$$

$$tx + y + tz = 0$$

$$(1 + t)x + 2y + 3z = 0$$

will have a non-trivial solution:

$$x = x_0, y = y_0, z = -1$$

Hence, the coefficient determinant Δ is zero. However,

$$\Delta = \begin{vmatrix} 1 & 1 & 1 \\ t & 1 & t \\ 1+t & 2 & 3 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ t & 1-t & 0 \\ 1+t & 1-t & 2-t \end{vmatrix} = \begin{vmatrix} 1-t & 0 \\ 1-t & 2-t \end{vmatrix}$$

$$= (1 - t)(2 - t)$$

Hence, $t = 1$ or $t = 2$. If $t = 1$, the given system becomes

$$x + y = 1$$

$$x + y = 1$$

$$2x + 2y = 3$$

which is clearly inconsistent. If $t = 2$, the given system becomes,

$$x + y = 1$$

$$2x + y = 2$$

$$3x + 2y = 3$$

which has the unique solution $x = 1, y = 0$ ....

Check Your Progress

Find the inverse of the following matrix.

$$\begin{bmatrix} 1 & 3 & 3 \\ 1 & 4 & 3 \\ 1 & 3 & 4 \end{bmatrix}$$

6.9 LET US SUM UP

In mathematics, a matrix (plural matrices, or less commonly matrixes) is a rectangular array of numbers. The horizontal and vertical lines in a matrix are called *rows* and *columns*, respectively. The numbers in the matrix are called its *entries* or its *elements* has the same number of rows and columns. An n-by-n matrix is known as a square matrix of order n. In linear algebra, the identity matrix or unit matrix of size n is the n-by-n square matrix with ones on the main diagonal and zeros elsewhere. Matrix addition is the operation of adding two matrices by adding the corresponding entries together. *Multiplication* of two matrices is defined only if the number of columns of the left matrix is the same as the number of rows of the right matrix. The Jordan canonical form is also known as classical canonical form which is basically a type of block matrix. The left-hand side of the characteristic equation is considered as characteristic polynomial.

6.10 KEYWORDS

Matrix: A matrix (plural matrices, or less commonly matrixes) is a rectangular array of numbers

Identity Matrix: Unit matrix of size n is the n-by-n square matrix with ones on the main diagonal and zeros elsewhere.

Characteristic Polynomial: The left-hand side of the characteristic equation is considered as characteristic polynomial.

6.11 QUESTIONS FOR DISUSSION

1. What is matrix? Discuss matrix addition and multiplication with examples.
2. Discuss transportation of matrices.
3. What is inverted matrix. Give example.
4. Define determinant. Discuss the properties of determinants.
5. What is Cayley-Hamiltonian theorm?

Check Your Progress: Modal Answers

1. First, I write down the entries the matrix A, but I write them in a double-wide matrix:

$$\left[\begin{array}{ccc|c} 1 & 3 & 3 & \\ 1 & 4 & 3 & \\ 1 & 3 & 4 & \end{array}\right]$$

In the other half of the double-wide, I write the identity matrix:

$$\left[\begin{array}{ccc|ccc} 1 & 3 & 3 & 1 & 0 & 0 \\ 1 & 4 & 3 & 0 & 1 & 0 \\ 1 & 3 & 4 & 0 & 0 & 1 \end{array}\right]$$

Now I'll do matrix row operations to convert the left-hand side of the double-wide into the identity. (As always with row operations, there is no one "right" way to do this. What follows are just the steps that happened to occur to me. Your calculations could easily look quite different.)

$$\left[\begin{array}{ccc|ccc} 1 & 3 & 3 & 1 & 0 & 0 \\ 1 & 4 & 3 & 0 & 1 & 0 \\ 1 & 3 & 4 & 0 & 0 & 1 \end{array}\right] \begin{array}{l} \xrightarrow{-R_1+R_2} \\ \xrightarrow{-R_1+R_3} \end{array} \left[\begin{array}{ccc|ccc} 1 & 3 & 3 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 1 \end{array}\right]$$

$$\xrightarrow{-3R_2+R_1} \left[\begin{array}{ccc|ccc} 1 & 0 & 3 & 4 & -3 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 1 \end{array}\right]$$

$$\xrightarrow{-3R_3+R_1} \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 7 & -3 & -3 \\ 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 1 \end{array}\right]$$

Now that the left-hand side of the double-wide contains the identity, the right-hand side contains the inverse. That is, the inverse matrix is the following:

$$\begin{bmatrix} 7 & -3 & -3 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}$$

Note that we can confirm that this matrix is the inverse of A by multiplying the two matrices and confirming that we get the identity:

$$\begin{bmatrix} 7 & -3 & -3 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 3 & 3 \\ 1 & 4 & 3 \\ 1 & 3 & 4 \end{bmatrix}$$

$$= \begin{bmatrix} 7\cdot1-3\cdot1-3\cdot1 & 7\cdot3-3\cdot4-3\cdot3 & 7\cdot3-3\cdot3-3\cdot4 \\ -1\cdot1+1\cdot1+0\cdot1 & -1\cdot3+1\cdot4+0\cdot3 & -1\cdot3+1\cdot3+0\cdot4 \\ -1\cdot1+0\cdot1+1\cdot1 & -1\cdot3+0\cdot4+1\cdot3 & -1\cdot3+0\cdot3+1\cdot4 \end{bmatrix}$$

$$= \begin{bmatrix} 7-3-3 & 21-12-9 & 21-9-12 \\ -1+1+0 & -3+4+0 & -3+3+0 \\ -1+0+1 & -3+0+3 & -3+0+4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$