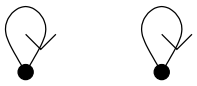
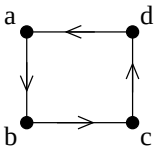
Mouse icon in page 788 extra examples

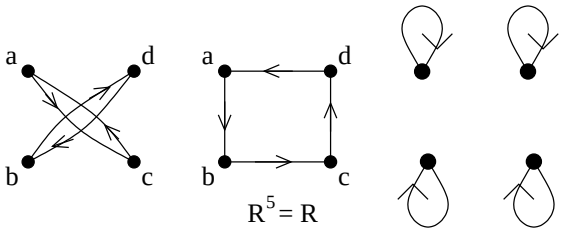
1. Construct a monoid using the operation max which has no zero and an infinite carrier.
   Solution: Let $N = \{0, 1, 2, \dots\}$
   $$\max(a, b) = \begin{cases} b & \text{if } b > a \\ a & \text{if } b \leq a \end{cases}$$
   This has no zero element and an infinite carrier.

2. For each of the following digraphs, let R be the binary relation represented by the digraph and let $S = \{R^n | n \in I+\}$ be the carrier of the algebra in which composition of relations is the binary operation. In each case determine whether the algebra can be presented as a semigroup, monoid or group and state the cardinality of the carrier.

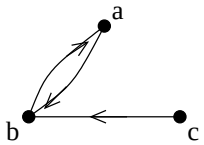
   (a)  $R = R^2 = R^3 \dots$ group with one element

   (b) 

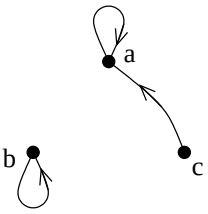
   R^2, R^3, R^4 are given by

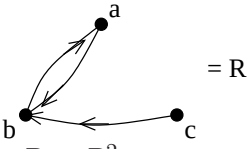
   

   This can be represented by a group with 4 elements. R^4 is the identity.

   (c) 

   = R

R^2 is given by 

R^3 is given by 

= R

The table is

	R	R^2
R	R^2	R
R^2	R	R^2

group with R^2 as the identity.

3. State necessary and sufficient condition on a binary relation R so that the set $\{R^n | n \in I+\}$ can be made the carrier of a monoid using the operation of composition.

   The algebra $< R^n, \circ >$ is a monoid if and only if $R^k R^j = R^j$ for all positive j. R^k is the identity. i.e., $R^k R = R$ or $R^{k+1} = R$. The necessary and sufficient condition is that there exists a k such that $R^{k+1} = R$. It is not necessary that $R^k = R^0$ as seen by (c) of the previous example.

4. Consider the group G of 2×2 matrices with rational entries and non zero determinant. Let H be the subset of G consisting of matrices whose upper right entry is 0. Then show that H is a subgroup of G but not a normal subgroup.

   Solution: The operation is matrix multiplication

$$\begin{bmatrix} a & 0 \\ b & c \end{bmatrix} \begin{bmatrix} a' & 0 \\ b' & c' \end{bmatrix} = \begin{bmatrix} aa' & 0 \\ ba' + cb' & cc' \end{bmatrix}$$

   Hence if we take $A, B \in H$, $AB \in H$ closure is proved. Matrix multiplication is associative. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ the identity $\in H$. Inverse of $\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$ is $\begin{bmatrix} \frac{1}{a} & 0 \\ -\frac{b}{ac} & \frac{1}{c} \end{bmatrix} \in H$. Hence H is a subgroup of G.

   If H is a normal subgroup for any a in G aha^{-1} should be in H for $h \in H$.

$aH = Ha$ if H is a normal subgroup.
so $ah = b = h'a$ for $h' \in H$
$aha^{-1} = h' \in H$. Also $a^{-1}ha \in H$
Take $a = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$, $h = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$
$a^{-1}ha = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} -1 & -4 \\ 1 & 3 \end{pmatrix} \notin H.$
Hence H is not a normal subgroup.

5. Let H be a normal subgroup of G. Then the cosets of H in G form a group under coset multiplication defined by

$$(aH)(bH) = abH$$

Solution: $(aH)(bH) = a(Hb)H = a(bH)H = abHH = abH$.
Closure is proved.
$(aH)((bH)(cH)) = abcH$
$= ((aH)(bH))(cH)$
Inverse of aH is $a^{-1}H$
H is the identity.

Permutation Groups

Mouse icon in page 789 extra examples

1. If $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$
   $f^{-1} = \begin{pmatrix} 5 & 3 & 2 & 1 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$

2. Show that S_3 is non abelian.
   S_3 can be given by the table given in page 790.
   If we look at it as the variations of a triangle by rotating about 120°, 240° and reflecting about a_1A, a_2B and a_3C as given in p. 790 and if we represent the original position of the triangle as C and rotations as r_1 and r_2 and reflections by $f_1 f_2 f_3$ respectively the table can be given by

	e	r_1	r_2	f_1	f_2	f_3
e	e	r_1	r_2	f_1	f_2	f_3
r_1	r_1	r_2	e	f_3	f_1	f_2
r_2	r_2	e	r_1	f_2	f_3	f_1
f_1	f_1	f_2	f_3	e	r_1	r_2
f_2	f_2	f_3	f_1	r_2	e	r_1
f_3	f_3	f_1	f_2	r_1	r_2	e

   It can be seen that $r_1 f_3 = f_2$

   $$f_3 r_1 = f_1$$

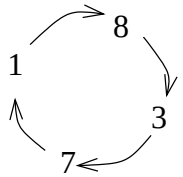
   Hence S_3 is not abelian.
   This is the smallest non abelian group. There is only one nonisomorphic group of order 2, 3 and 5 and they are cyclic. There are 2 nonisomorphic groups of order 4 and both are abelian. S_3 having 6 elements is the smallest nonabelian group. But all its proper subgroups are abelian, in fact cyclic.
   $\{e\}$, $\{e, r_1, r_2\}$, $\{e, f_1\}$, $\{e, f_2\}$, $\{e, f_3\}$ are the proper subgroups.
   For $k \geq 3$ S_k is of order $k!$.
   This is because with n elements we can have $k!$ permutations. All of

them are non abelian. This can be shown as follows:
Let $p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & k \\ 2 & 3 & 1 & 4 & 5 & 6 & \dots & k \end{pmatrix}$
$p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & k \\ 1 & 3 & 4 & 2 & 5 & 6 & \dots & k \end{pmatrix}$
Then $p_1.p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & k \\ 2 & 1 & 4 & 3 & 5 & 6 & \dots & k \end{pmatrix}$
$p_2.p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & k \\ 3 & 4 & & & 5 & 6 & \dots & k \end{pmatrix}$
So $p_1.p_2 \neq p_2.p_1$
Hence S_k is not abelian.

Cyclic Notation for Permutations
Another way of describing a permutation is by means of cycles. Consider $f \in S_8$.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 7 & 6 & 5 & 4 & 1 & 3 \end{pmatrix}$$

Consider the images of 1 when f is applied repeatedly. The images $f(1), f^2(1), f^3(1), \dots$ are 8, 3, 7, 1, 8, 3, 7, ... If $j \geq 1$ and $f^j(1)$ is an element of



then $f^{j+1}(1)$ is the next element in the indicated direction. The numbers 1, 8, 3, 7 make up a cycle of length 4. The above figure illustrates how the cycle can be represented. It canbe also represented as (8, 3, 7, 1) or (3, 7, 1, 8) or (7, 1, 8, 3) or (1, 8, 3, 7). Though as a figure it is more easy to understand the second way of representation is the one which is usually used. The last number in the list has as its image the first number. The other cycles in f are (2), (4, 6) and (5). We can express f as a product of disjoint cycles.

$$f = (1, 8, 3, 7)(2)(4, 6)(5)$$

$$\text{or } f = (1, 8, 3, 7)(4, 6)$$

The absence of 2 and 5 implies that $f(2) = 2$ and $f(5) = 5$.
Disjoint cycles: We say that two cycles are disjoint if no number appears in both cycles. We can easily see that in the representation of a permutation by cycles, we get only disjoint cycles. Disjoint cycles can be written in any order. f can also be written as

$$f = (4, 6)(1, 8, 3, 7)$$

Let us now see how to deal with composition of permutations in this new representation.
Suppose f is as above and g is given by

$$g = (1, 5, 6)(8, 3, 7, 4)$$

To calculate fg, we start with simple concatenation
$fg = (1, 8, 3, 7)(4, 6)(1, 5, 6)(8, 3, 7, 4)$ - I.
Now we want to express fg as a product of disjoint cycles as f and g were individually written. We will start with the cycle that contains 1. The four cycles in I are read from right to left. The first cycle does not contain 1. Thus we move to the second. The image of 1 under the cycle is 5. Now move on to the next cycle in I, looking for 5. It does not appear. The fourth cycle also does not contain 5. So $fg(1) = 5$. At this point we have $fg = (1, 5, \dots)$. Repeat the steps to find $fg(5)$ which is seen to be 4. $fg(4)$ is similarly found as 4. $fg(3)$ is 1 and now we have a cycle $(1, 5, 4, 3)$. Similarly we find another cycle $(6, 8, 7)$, (2) is a cycle and need not be written. So fg can be written as $(1, 5, 4, 3)$ $(6, 8, 7)$ as product of disjoint cycles.
Similarly we find
(1, 2, 3, 4) (1, 2, 3, 4) = (1, 3) (2, 4)
(1, 4) (1, 3) (1, 2) = (1, 2, 3, 4)
It should be noted that the cyclic notation does not indicate the set which is being permuted. The examples above could be in S_5 where the image of 5 is 5. This ambiguity is usually overcome by making the context clear.

A cycle of length 2 is called a transposition (1, 2) (4, 5) are transpositions (1, 5, 4) is not. It can be seen that every cycle of length greater than 2 can be expressed as a product of transpositions.
(1, 5, 4) can be represented as (1, 4) (1, 5) $(a_1, \dots, a_k)$ canbe expressed as

$(a_1, a_k)(a_1, a_{k-1}) \dots (a_1, a_3)(a_1, a_2)$.
The order is important here. It cannot be changed. Even and odd permutations are defined in p. 794. It is also seen that every permutation in a finite set can be expressed as the product of an even number of transpositions or an odd number of transpositions but not both. This is seen as follows. Every permutation is expressed as disjoint cycles omitting the cycles having only one element. If the length of the cycle is ≥ 3, each cycle is written as a product of transpositions. Hence every permutation is represented as a product of transpositions. If the number of transpositions is odd, it is called an odd permutation. If it is even it is called an even permutations.

Let $n \geq 2$. The set of even permutations in S_n is a proper subgroup of S_n called the alternating group on $\{1, \dots, n\}$ denoted as A_n. The order of A_n is $\frac{n!}{2}$.

This can be seen as follows:
Let A_n denote the set of even permutations of S_n and let B_n denote the set of odd permutation of S_n. If $f, g \in A_n$ we can write fg as $s_1 \dots s_p t_1 \dots t_q$ where s_i's and t_j's denote transposition.
Since p is even and q is even $p + q$ is even and so $fg \in A_n$. Since A_n is a finite set, by theorem. By Theorem 1 in p. 785, it is enough to prove closure alone. A_n is a subgroup of S_n. To show that the order of A_n is $n!/2$, we consider the following mapping $\theta : A_n \to B_n$. Let $t = (1, 2)$, $\theta(h) = ht$.

It can be easily seen that θ is an injection because if
$\theta(h) = \theta(h')$
$ht = h't$
$htt' = h'tt'$ so $h = h'$.

To show θ is a surjection. Let h in B_n be the image of an element g in A_n.
$\theta(g) = h$.
Specifically $g = ht$
$\theta(ht) = (ht)t$

$= h(tt)$

$= hi$

$= h$

Since θ is a bijection $\#A_n = \#B_n = \frac{n!}{2}$.

The sliding-tile puzzle explained in Example 8 of section 2.2 illustrates the use of even and odd permutations.

Mouse icon in page 824 Extra Examples

1. Find the group code given by the generator matrix $\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$
   Find the encoding scheme $e : B^3 \to B^6$. Draw the coset table. How will you decode 000011, 001111, 001110?
   Solution.

   $e(000) = 000000$ $\quad$ $e(100) = 100110$
   $e(001) = 001101$ $\quad$ $e(101) = 101011$
   $e(010) = 010011$ $\quad$ $e(110) = 110101$
   $e(011) = 011110$ $\quad$ $e(111) = 111000$

   Coset table is

000000	100110	010011	001101	110101	101011	011110	111000
000001	100111	010010	001100	110100	101010	011110	111000
000010	100100	010001	001111	110111	101001	011100	111010
000100	100010	010111	001001	110001	101111	011010	111100
001000	101110	011011	000101	111101	100011	010110	110000
010000	110110	000011	011101	100101	111011	001110	101000
100000	000110	110011	101101	010101	001011	111110	011000
100001	000111	110010	101100	010100	001010	111111	011001

   Encoding matrix is $E = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$ $\quad a^i E = b^i$

   (a) $d(000011)$: This is located in the 3^{rd} column, 6^{th} row. Coset leader is 010000
   $000011 \oplus 010000 = 010011$
   $d(010011) = 010$.

   (b) Similarly $d(001111) = 001$

   (c) $d(001110) = 011$

2. A code C is said to be equivalent to a code C^*, when there is a distance preserving bijections between the code words of C and those of C^*. Given an encoding (generator) matrix G for a code, show that any (a) permutations of the rows of G (b) permutations of the columns of G, or (c) addition of a scalar multiple of a row of G to another row will result in the new matrix G^* for a code which is equivalent to a code generated by G.

   (a) We shall consider a $(3, 6)$ code. The result can be extended to any (m, n) code. The generator matrix is of size 3×6. Let us consider row 1, row 2, row 3 of this matrix. The eight code words are obtained as 000000, row 1, row 2, row 3, row 1 $\oplus$ row 2, row 1 $\oplus$ row 3, row 2 $\oplus$ row 3, row 1 $\oplus$ row 2 $\oplus$ row 3. If we permute the rows still we get the same codewords. Hence G^* generates the same set of codewords.

   (b) The weight of a code word is the number of 1's in the code word. If we permute the columns the number of 1's in each row remains the same. Let us consider the permutation as sequence of transpositions. Suppose the i^{th} column and j^{th} column are interchanged. We are considering row p and row q. Now p_i and p_j will be exchanged. q_i and q_j will be exchanged. If a codeword is represented by row $p\oplus$ row q. This has as the i^{th} element $p_i \oplus q_i$ and as the j^{th} element $p_j \oplus q_j$. In the new codeword in c^* obtained by interchanging i^{th} and j^{th} column, the codeword represented by row $p\oplus$ row q will have the i^{th} and j^{th} element interchanged. It will have $p_j \oplus q_j$ as the i^{th} bit and $p_i \oplus q_i$ as the j^{th} bit. Thus we see that the number of 1's in the codeword is not affected i.e., the weights are maintained.

   (c) If a scalar multiple of one row of G is added to another row of G. If the scalar is 0 no change is obtained. Without loss of generality assume that row 2 is added to row 1 (scalar is 1 in this case).
   row 1 in G is now replaced by row 1 $\oplus$ row 2. So the code words are 000000, row 1 $\oplus$ row 2, row 2, row 3, row 1 $\oplus$ row 2 $\oplus$ row 2, row 1 $\oplus$ row 2 $\oplus$ row 3, row 2 $\oplus$ row 3, row 1 $\oplus$ row 2 $\oplus$ row 2 $\oplus$ row 3 respectively. They are equal to 000000, row 1 $\oplus$ row 2, row 2, row 3, row1, row 1 $\oplus$ row 2 $\oplus$ row 3, row 2 $\oplus$ row 3, row 1 $\oplus$ row 3. Thus the set of codewords in C^* is the same as in C.

Hence there is a proper bijection from C to C^*, and the weight of the code is maintained.