Abstract Algebra, Lecture 5

Permutations

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

Summary

Summary

Summary

Definition

Let X be a set. Then the *symmetric group* on X is the group of all bijections

$$f : X \to X$$

with functional composition as operation. It is denoted by S_X.

Theorem

If X, Y are sets, and $\phi : X \to Y$ is a bijection, then the maps

$$S_X \ni f \mapsto \phi \circ f \circ \phi^{-1} \in S_Y$$
$$S_y \ni g \mapsto \phi^{-1} \circ g \circ \phi \in S_X$$

are each other's inverses; thus, they are bijections. Furthermore, these assignments respect the group operations of S_x and S_y, showing these two groups to be isomorphic. We say that f and $\tilde{f} = \phi \circ f \circ \phi^{-1}$ are conjugate.

The following commutative diagram illustrates conjugation:

$$\begin{array}{ccc} X & \xrightarrow{f} & X \\ \big\downarrow \phi & & \big\downarrow \phi \\ Y & \xrightarrow{\tilde{f}} & Y \end{array}$$

Definition

For any positive integer n, we let $[n] = \{1, 2, \ldots, n\}$. We define the symmetric group on n letters as $S_n = S_{[n]}$.

Lemma

If X is a set with n elements, then $S_X \simeq S_n$.

Proof.

Number the elements in X to get a bijection $\phi : [n] \to X$. Then the desired isomorphism is the conjugation

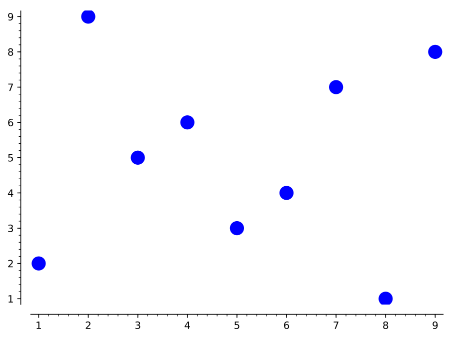
$$S_X \ni f \mapsto \phi^{-1} \circ f \circ \phi \in S_n$$

□

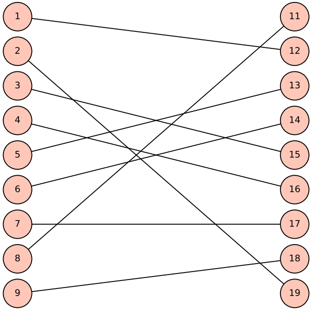
Representations of permutations

- Let $\sigma \in S_n$
- Since $\sigma : [n] \to [n]$, we can consider its graph, a subset of $[n]^2$
- Can represent σ in *two-row notation* as $\begin{array}{c|c|c|c} 1 & 2 & \cdots & n \\ \hline \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{array}$
- One-row notation is $[\sigma(1), \sigma(2), \cdots, \sigma(n)]$
- The associated bipartite graph has vertex set two copies of $[n]$, a left and a right set, and an edge from i on the left to $\sigma(i)$ on the right
- The associated directed graph has vertex set $[i]$ and a directed edge from i to $\sigma(i)$

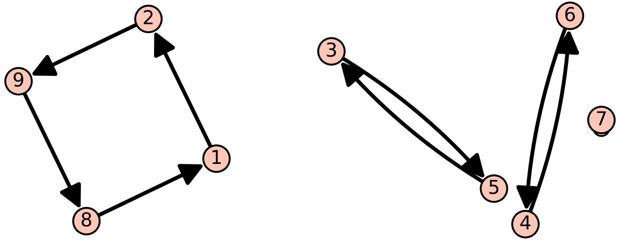
Example

- $\sigma = [2, 9, 5, 6, 3, 4, 7, 1, 8]$
- 

Example

- $\sigma = [2, 9, 5, 6, 3, 4, 7, 1, 8]$
- 

Example

- $\sigma = [2, 9, 5, 6, 3, 4, 7, 1, 8]$
- 

- To understand the multiplication, the following representation is useful
- The associated linear map is the map $F_\sigma : V \to V$, where V is the free vector space (over $\mathbb{Q}$ or whatever) with basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$, and with $F_\sigma(\mathbf{e}_i) = \mathbf{e}_{\sigma(i)}$
- The associated permutation matrix M_σ is the matrix of the aforementioned map w.r.t. the natural ordered basis (the matrix acts on column vectors from the left)
- If τ is another permutation in S_n then

$$F_{\sigma\tau} = F_\sigma \circ F_\tau$$
$$M_{\sigma\tau} = M_\sigma M_\tau$$

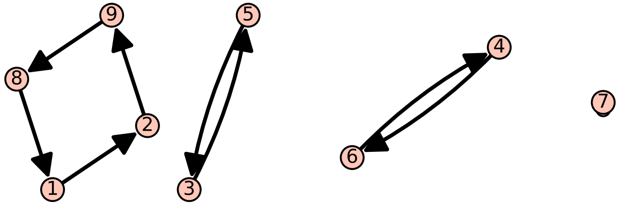
Example

- $\sigma = [2, 9, 5, 6, 3, 4, 7, 1, 8]$
- $M_\sigma = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$

- In the directed graph each vertex has in-degree one and out-degree one
- Hence the digraph decomposes into directed cycles
- The *cycle notation* of σ is obtained by listing the elements of each cycles, as

$$(a_1, \ldots, a_{\ell_1})(a_{\ell_1+1}, \ldots, a_{\ell_2}) \cdots ()$$

  where, in each cycle, $\sigma(a_v) = a_{v+1}$
- The *cycle type* of σ is the numerical partition of n given by the cycle lengths. It can be encoded in various ways; we'll usually write it as a (non-strictly) decreasing sequence $(c_1, c_2, \ldots, c_k)$ of cycle lengths.

- $\sigma = [2, 9, 5, 6, 3, 4, 7, 1, 8]$
- 

- $\sigma = (1, 2, 9, 8)(3, 5)(4, 6)(7)$
- Cycle type is $9 = 4 + 2 + 2 + 1$, written as $(4, 2, 2, 1)$.

Theorem

$\sigma, \tau \in S_n$ are conjugate if and only if they have the same cycle type.

Proof.

Order the cycles in order of decreasing length, breaking ties arbitrarily. Let ϕ be the bijection that associates the elements in correspoding cycles (in cyclic order, picking a starting element in each cycle howsoever). Conjugate using ϕ. □

Note that in this case we have that $X = Y = [n]$, and that $\phi \in S_n$, as well.

Example

$$\sigma = (1,2,9,8)(3,5)(4,6)(7)$$
$$\tau = (2,3,4,5)(6,7)(8,9)(1)$$

are conjugate, for instance using $\phi =$

1	2	3	4	5	6	7	8	9
2	3	6	8	7	9	1	5	4

Check that

$$\tau = \phi\sigma\phi^{-1},$$

or is it

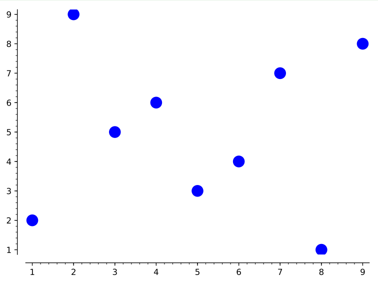
$$\tau = \phi^{-1}\sigma\phi?$$

Definition

Let $S_n \ni \sigma = [\sigma(1), \ldots, \sigma(n)]$.

- A descent is an index $1 \leq i < n$ such that $\sigma(i) > \sigma(i+1)$. We use $\mathtt{Des}(\sigma) \subseteq [n-1]$ for the set of descents, and $\mathtt{des}(\sigma)$ for the number of descents. The major index $\mathtt{maj}(\sigma)$ is the sum of the elements in the descent set.
- An inversion is a pair of indices $1 \leq i < j \leq n$ such that $\sigma(i) > \sigma(j)$. We use $\mathtt{Inv}(\sigma) \subseteq [n]^2$ for the set of inversions, and $\mathtt{inv}(\sigma)$ for the number of inversions.
- There are many, many more permutation statistics. Their enumeration is a huge topic in algebra and combinatorics!

Example

- $\sigma = [2, 9, 5, 6, 3, 4, 7, 1, 8]$
  

- Descent set is $2, 4, 7$
- Inversion set is $(2, 3), (2, 4), (2, 5), (2, 6), (2, 7), (2, 8), (2, 9), (4, 5), (4, 6), (4, 8), (6, 8), (7, 8)$. There are thus 12 inversions.

Left versus right

- We (I, Judson, Svensson) write $f(x)$ for a function
- Furthermore, $(g \circ f)(x) = g(f(x))$
- Arguments enter from the right, and gets transported leftwards
- In particular, if $f, g \in S_n$, then $fg \in S_n$ is the bijection "first apply g, then apply f to the result"
- Other authors prefer to write $(x)f$ or just xf.
- Then fg means "first apply f, then apply g to the result"
- In particular, SAGE (and GAP) uses this convention
- Do not become confused!

Definition

- A k-cycle is a permutation whose cycle type has a single cycle of length k, and possibly a bunch of cycles of length one.
- For instance, $(1, 2, 3)(4)(5) \in S_5$ is a 3-cycle.
- A transposition is another name for a 2-cycle.
- An involution is a permutation whose square is the identity
- The disjoint cycle factorization is the factorization of the permutation into cycles as given by the cycle notation
- For instance, if $f = (1, 2, 3)(4, 5, 6) \in S_6$ then we can write $f = gh$ with $g = (1, 2, 3)(4)(5)(6)$ and $h = (4, 5, 6)(1)(2)(3)$
- It is common and convenient to omit the cycles of length one.

Lemma

- *Disjoint cycles commute*
- *Transpositions are involutions*
- *Involutions are products of disjoint transpositions, hence have cycle type* $(2, 2, 2, \ldots, 2, 1, \ldots, 1)$.
- *A* k*-cycle has order* k.
- *The order of a permutation is the l.c.m. of the sizes of its cycles*

Example

If $\sigma = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)$ then its powers have cycle structure as follows:

```
0 ()
1 (1,2,3,4,5,6,7,8,9,10,11,12)
2 (1,3,5,7,9,11)(2,4,6,8,10,12)
3 (1,4,7,10)(2,5,8,11)(3,6,9,12)
4 (1,5,9)(2,6,10)(3,7,11)(4,8,12)
5 (1,6,11,4,9,2,7,12,5,10,3,8)
6 (1,7)(2,8)(3,9)(4,10)(5,11)(6,12)
7 (1,8,3,10,5,12,7,2,9,4,11,6)
8 (1,9,5)(2,10,6)(3,11,7)(4,12,8)
9 (1,10,7,4)(2,11,8,5)(3,12,9,6)
10 (1,11,9,7,5,3)(2,12,10,8,6,4)
11 (1,12,11,10,9,8,7,6,5,4,3,2)
12 ()
```

In general, the k-th power of an m-cycle consists of $(m/\gcd(k, m))$-cycles, and $\gcd(k, m)$ such cycles.

Example

Non-disjoint cycles need not commute:

$$(1,2)(1,3) = (1,3,2)$$
$$(1,3)(1,2) = (1,2,3)$$

Example

Let $\sigma = (1,2,3,4)(5,6,7)(8,9,10)$. Then $o(\sigma) = \mathrm{lcm}(4,3,3) = 12$, and its powers are

```
0 ()
1 (1,2,3,4)(5,6,7)(8,9,10)
2 (1,3)(2,4)(5,7,6)(8,10,9)
3 (1,4,3,2)
4 (5,6,7)(8,9,10)
5 (1,2,3,4)(5,7,6)(8,10,9)
6 (1,3)(2,4)
7 (1,4,3,2)(5,6,7)(8,9,10)
8 (5,7,6)(8,10,9)
9 (1,2,3,4)
10 (1,3)(2,4)(5,6,7)(8,9,10)
11 (1,4,3,2)(5,7,6)(8,10,9)
12 ()
```

Lemma

Any k-cycle can be written as a product of transpositions.

Thus, since every permutation is the product of disjoint cycles, the transpositions generate S_n.

Proof.

It is enough to note that

$$(1, 2, 3, \ldots, k) = (1, 2) \cdots (k-2, k-1)(k-1, k)$$

□

Example

$(1,2)(2,3)(3,4) = (1,2,3,4)$

Lemma

Every transposition is the product of an odd number of adjacent transpositions, i.e. transpositions of the form $(j, j+1)$

So S_n is generated by adjacent transpositions.

Proof.

Enough to note that

$$(1, k-1)(k-1, k)(1, k-1) = (1, k)$$

□

Example

$(1,4) = (1,3)(3,4)(1,3) = (1,2)(2,3)(1,2)(3,4)(1,2)(2,3)(1,2)$

Lemma

S_n is generated by $\{(1,2),(1,2,3,\dots,n)\}$

So, while not cyclic, S_n has a generating set with just two elements.

Proof.

Enough to note that

$$(j+1,j+2) = (1,2,3,\dots,n)^j(1,2)(1,2,3,\dots,n)^{-j}$$

□

Example

$$(1,2,3,4)^2(1,2)(1,2,3,4)^{-2} = (1)(2)(3,4)$$

S_2

Example

S_2 is cyclic:

$*$	$()$	$(1,2)$
$()$	$()$	$(1,2)$
$(1,2)$	$(1,2)$	$()$

S_3

Example

S_3 is the smallest non-abelian group:

$*$	$()$	$(1,3,2)$	$(1,2,3)$	$(2,3)$	$(1,3)$	$(1,2)$
$()$	$()$	$(1,3,2)$	$(1,2,3)$	$(2,3)$	$(1,3)$	$(1,2)$
$(1,3,2)$	$(1,3,2)$	$(1,2,3)$	$()$	$(1,2)$	$(2,3)$	$(1,3)$
$(1,2,3)$	$(1,2,3)$	$()$	$(1,3,2)$	$(1,3)$	$(1,2)$	$(2,3)$
$(2,3)$	$(2,3)$	$(1,3)$	$(1,2)$	$()$	$(1,3,2)$	$(1,2,3)$
$(1,3)$	$(1,3)$	$(1,2)$	$(2,3)$	$(1,2,3)$	$()$	$(1,3,2)$
$(1,2)$	$(1,2)$	$(2,3)$	$(1,3)$	$(1,3,2)$	$(1,2,3)$	$()$

S_4

Example

S_4 has $4! = 24$ elements, with the following orders:

()	1	(3,4)	2
(1,3)(2,4)	2	(1,3,2,4)	4
(1,4)(2,3)	2	(1,4,2,3)	4
(1,2)(3,4)	2	(1,2)	2
(2,3,4)	3	(2,3)	2
(1,3,2)	3	(1,3,4,2)	4
(1,4,3)	3	(1,4)	2
(1,2,4)	3	(1,2,4,3)	4
(2,4,3)	3	(2,4)	2
(1,3,4)	3	(1,3)	2
(1,4,2)	3	(1,4,3,2)	4
(1,2,3)	3	(1,2,3,4)	4

Definition

The sign of a permutation $\sigma \in S_n$ is

$$\mathrm{sgn}(\sigma) = (-1)^{\mathrm{inv}(\sigma)}.$$

Permutations with sign $+1$ are even, the rest are odd.

Lemma

$\mathrm{sgn}((i, i+1)) = -1$.

Proof.

We have that $\mathrm{Inv}((i, i+1)) = \{(i, i+1)\}$. □

Lemma

Any transposition is odd.

Proof.

If $\tau = (a, b)$ with $a < b$ then $\mathrm{Inv}(\tau)$ contains

- (a, c) for $a < c < b$,
- (c, b) for $a < c < b$, and
- (a, b).

This is an odd number. □

The only hard proof today — proof skipped

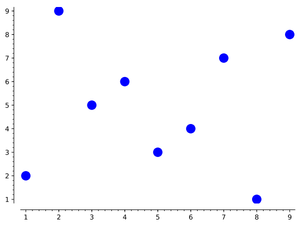
Theorem

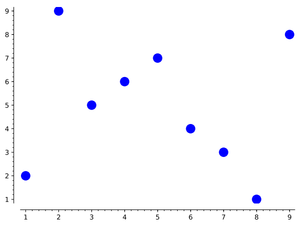
If $\sigma, \tau \in S_n$, and τ is a transposition, then $|\mathrm{inv}(\sigma) - \mathrm{inv}(\tau\sigma)|$ is odd.

Proof.

You absolutely, unequivocally, positively, have to read this proof in your textbook! (It is a case-by-case study, similar to the previous lemma) □

Example

1. $\sigma = [2, 9, 5, 6, 3, 4, 7, 1, 8]$
2. 

3. $(3, 7)\sigma = [2, 9, 5, 6, 7, 4, 3, 1, 8]$
4. 

New inversions: $(5, 6)$, $(5, 7)$, $(5, 8)$

Disappearing inversions: $(3, 5)$, $(4, 5)$

Net gain: $+1$ inversions

Corollary

Let $\sigma \in S_n$. Then, if

$$\sigma = \prod_{j=1}^{m} \tau_j$$

is a factorization of σ as a product of transpositions, then

$$(-1)^m = \operatorname{sgn}(\sigma),$$

that is, m is odd if σ is an odd permutation, and even if σ is even.

Corollary

If $\sigma, \gamma \in S_n$, then

$$\mathrm{sgn}(\sigma\gamma) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\gamma).$$

Proof.

Write σ and γ as a product of transpositions. □

Corollary

The determinant of M_σ is the sign of σ.

Proof.

It is true for transpositions. □

Definition

Let E^n be the n-dimensional Euclidean space, with the standard inner product. A linear isometry is a linear map $F : E^n \to E^n$ preserving the inner product, i.e,

$$\langle F(\mathbf{u}), F(\mathbf{v}) \rangle = \langle \mathbf{u}, \mathbf{v} \rangle$$

for all vectors $\mathbf{u}, \mathbf{v} \in E^n$.

Clearly, F also preserves norms, and distances.

Definition

We denote the group of linear isometries of E^n by $\mathrm{LI}(E^n)$.

This is a subgroup of S_{E^n}, the group of all bijections on E^n.

Lemma

- *The matrix M of the linear isometry F satisfies $M * M^t = I$. It has either determinant $+1$, if F is orientation-preserving, or -1, if F is orientation-reversing.*
- *In the plane, the isometries are either the orientation-preserving rotations, with matrix*

$$\begin{pmatrix} \cos(\phi) & -\sin(\phi) \\ \sin(\phi) & \cos(\phi) \end{pmatrix}$$

  or reflections in a line through the origin with (unit) normal vector $\mathbf{w}$, given by

$$\mathbf{u} \mapsto \mathbf{u} - 2\langle \mathbf{u}, \mathbf{w} \rangle \mathbf{w}$$

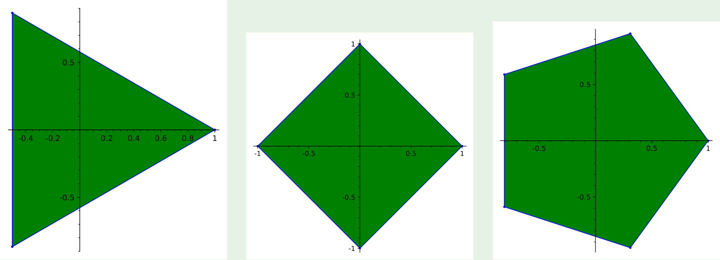
- *In E^3, there are orientation-preserving rotations, and orientation-reversing rotation-reflections*

Definition

Let, for $n \geq 3$, K_n be the regular n-gon in E^2, realized as the convex hull of its set of vertices

$$V_n = \{ (\cos(2k\pi/n), \sin(2k\pi/n)) | 0 \leq k < n \}$$

Example



Definition

The Dihedral group D_n is the group of symmetries of K_n, i.e.

$$D_n = \{ F \in \mathrm{LI}(E^n) | F(K_n) = K_n \}$$

Theorem

An element of D_n must restrict to a bijection on V_n. Two different elements of D_n induce different permutations of V_n. Thus

$$D_n = \{ F \in \mathrm{LI}(E^n) | F(V_n) = V_n \} \simeq G \leq S_{V_n} \simeq S_n$$

In general, not every permutation of the vertices can be extended to a linear isometry preserving K_n.

Theorem

D_n has $2n$ elements; n rotations and n reflections.

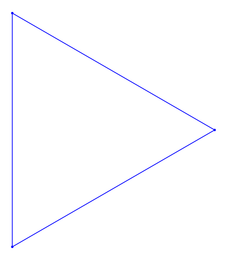
Proof.

Imagine cutting out K_n from the plane and then putting it back, filling the hole. You either flip the cut-out, or you don't. □

We will label the vertices counter-clockwise, starting with $(1, 0)$ as vertex number 1.

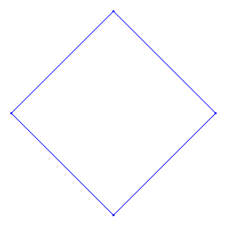
Example

Any permutation of the vertices of the triangle K_3 can be obtained by a rotation or a reflection. Thus $D_3 \simeq S_3$.



Example

Since adjacent vertices of K_4 must remain adjacent after a symmetry, the permutation $(2,3)$ is impossible.



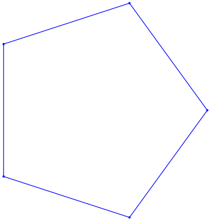
In fact, D_4 has multiplication table

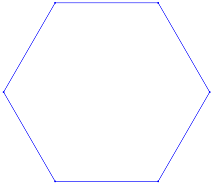
$*$	$()$	$(1,3)(2,4)$	$(1,4,3,2)$	$(1,2,3,4)$	$(2,4)$	$(1,3)$	$(1,4)(2,3)$	$(1,2)(3,4)$
$()$	$()$	$(1,3)(2,4)$	$(1,4,3,2)$	$(1,2,3,4)$	$(2,4)$	$(1,3)$	$(1,4)(2,3)$	$(1,2)(3,4)$
$(1,3)(2,4)$	$(1,3)(2,4)$	$()$	$(1,2,3,4)$	$(1,4,3,2)$	$(1,3)$	$(2,4)$	$(1,2)(3,4)$	$(1,4)(2,3)$
$(1,4,3,2)$	$(1,4,3,2)$	$(1,2,3,4)$	$(1,3)(2,4)$	$()$	$(1,2)(3,4)$	$(1,4)(2,3)$	$(2,4)$	$(1,3)$
$(1,2,3,4)$	$(1,2,3,4)$	$(1,4,3,2)$	$()$	$(1,3)(2,4)$	$(1,4)(2,3)$	$(1,2)(3,4)$	$(1,3)$	$(2,4)$
$(2,4)$	$(2,4)$	$(1,3)$	$(1,4)(2,3)$	$(1,2)(3,4)$	$()$	$(1,3)(2,4)$	$(1,4,3,2)$	$(1,2,3,4)$
$(1,3)$	$(1,3)$	$(2,4)$	$(1,2)(3,4)$	$(1,4)(2,3)$	$(1,3)(2,4)$	$()$	$(1,2,3,4)$	$(1,4,3,2)$
$(1,4)(2,3)$	$(1,4)(2,3)$	$(1,2)(3,4)$	$(1,3)$	$(2,4)$	$(1,2,3,4)$	$(1,4,3,2)$	$()$	$(1,3)(2,4)$
$(1,2)(3,4)$	$(1,2)(3,4)$	$(1,4)(2,3)$	$(2,4)$	$(1,3)$	$(1,4,3,2)$	$(1,2,3,4)$	$(1,3)(2,4)$	$()$

Theorem

Let $r \in D_n$ denote rotation by $2\pi/n$ radians counter-clockwise, and let s denote reflection in the x-axis.

1. *r induces the permutation $(1,2,\ldots,n)$. It has order n.*
2. *s induces $(1)(2,n-1)\cdots((n+1)/2\rfloor,(n+3)/2)$ if n is odd, and $(1)(2,n-1)\cdots(n/2,n/2+2)((n+1)/2)$ if n is even. It has order two.*





Theorem (Contd)

3 *If n is odd, then the reflection in the line through the vertex k can be given as*

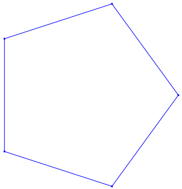
$$r^{k-1}sr^{1-k}$$

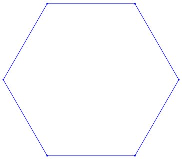
If n is even, then the reflection in the line through the opposite vertices k and $(n+1)/2+(k-1)$ is given by

$$r^{k-1}sr^{1-k},$$

whereas the reflection in the line through the midpoint between k and $k+1$ is given by

$$(k,k+1)(k-1,k+2)\cdots$$





Theorem (Contd)

4 *All rotations commute*

4 *The product of two reflections is a rotation (which?)*

4 *Regardless of the parity of n, the following relation hold:*

$$srs = r^{-1}$$

4 $D_n = \langle r, s \rangle$*, and all relations can be derived from*

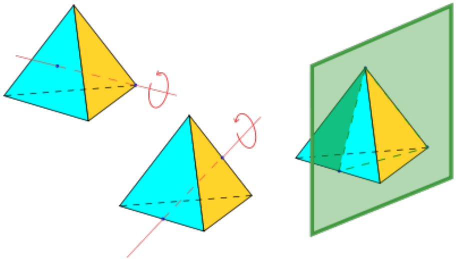
$$r^n = s^2 = srsr = 1$$

4 *Thus, the elements of* D_n *can be listed as* $s^a r^b$ *with* $0 \leq a \leq 1$, $0 \leq b < n$

Theorem

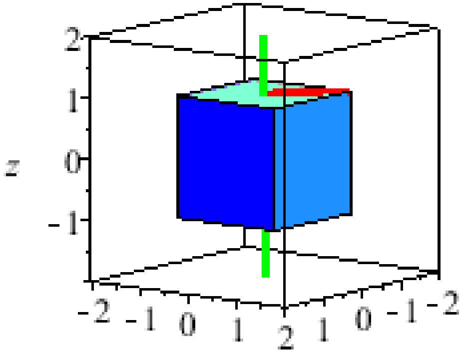
Let G be the group of symmetries of the regular tetrahedron. Then G has $4 * 3 = 12$ rotations, and equally many rotation-reflections. Thus G has 24 elements in total; since G permutes the four vertices of the tetrahedron, and $4! = 24$, we must have that $G \simeq S_4$. The subgroup of rotations correspond to even permutations.

From Wikipedia:



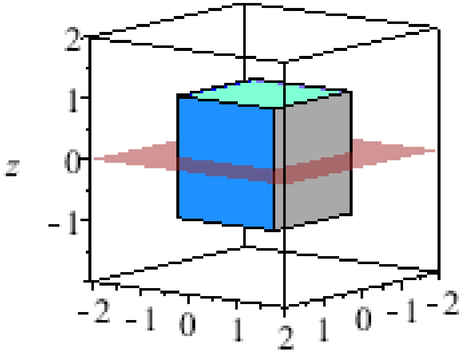
Theorem

The symmetry group of the cube has 48 elements, of which half are rotations. The subgroup of rotations is isomorphic to S_4.



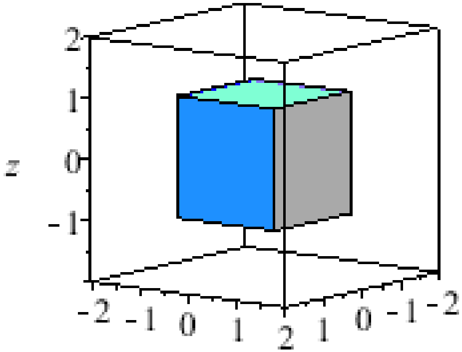
Theorem

The symmetry group of the cube has 48 elements, of which half are rotations. The subgroup of rotations is isomorphic to S_4.



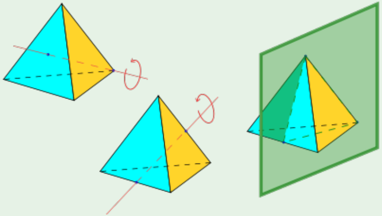
Theorem

The symmetry group of the cube has 48 elements, of which half are rotations. The subgroup of rotations is isomorphic to S_4.



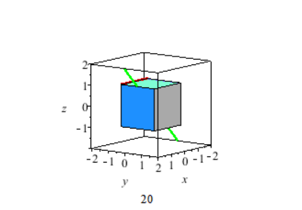
Example

Consider again the symmetries of the tetrahedron



- Any symmetry permutes the vertices. For instance, the first rotation induces $(1, 2, 3)(4)$, labeling the vertices on the blue triangle first.
- The same rotation induces $(a, b, c)(d, e, f)$ on the edges

Example



- The rotations of the cube acts on the four space diagonals, and each possible permutation of space diagonals can be so obtained. This is one way of showing that the rotations form a group isomorphic to S_4
- The full isomorphism group of the cube has 48 elements.
- Thus there is a pair of different symmetries that permutes the space diagonals in the same way!
- In fact, the antipodal map $z \mapsto -z$ fixes the space diagonals, just like the identity map $z \mapsto z$.

- There is a canonical way of representing group elements as permutations, so that
  1. Different group elements yields different permutations
  2. Products of group elements correspond to products of their induced permutations
- The name of this magnificent construction is...
- Cayley's left regular representation!!!!!
- Works even for infinite groups!
- Is intuitive and straightforward — once learned, will never be forgotten!
- Just make sure not to confuse left and right...

- There is a canonical way of representing group elements as permutations, so that
  1. Different group elements yields different permutations
  2. Products of group elements correspond to products of their induced permutations
- The name of this magnificent construction is...
- Cayley's left regular representation!!!!!
- Works even for infinite groups!
- Is intuitive and straightforward — once learned, will never be forgotten!
- Just make sure not to confuse left and right...

- There is a canonical way of representing group elements as permutations, so that
  1. Different group elements yields different permutations
  2. Products of group elements correspond to products of their induced permutations
- The name of this magnificent construction is...
- Cayley's left regular representation!!!!!
- Works even for infinite groups!
- Is intuitive and straightforward — once learned, will never be forgotten!
- Just make sure not to confuse left and right...

- There is a canonical way of representing group elements as permutations, so that
  1. Different group elements yields different permutations
  2. Products of group elements correspond to products of their induced permutations
- The name of this magnificent construction is...
- Cayley's left regular representation!!!!!
- Works even for infinite groups!
- Is intuitive and straightforward — once learned, will never be forgotten!
- Just make sure not to confuse left and right...

- There is a canonical way of representing group elements as permutations, so that
  1. Different group elements yields different permutations
  2. Products of group elements correspond to products of their induced permutations
- The name of this magnificent construction is...
- Cayley's left regular representation!!!!!
- Works even for infinite groups!
- Is intuitive and straightforward — once learned, will never be forgotten!
- Just make sure not to confuse left and right...

- There is a canonical way of representing group elements as permutations, so that
  1. Different group elements yields different permutations
  2. Products of group elements correspond to products of their induced permutations
- The name of this magnificent construction is...
- Cayley's left regular representation!!!!!
- Works even for infinite groups!
- Is intuitive and straightforward — once learned, will never be forgotten!
- Just make sure not to confuse left and right...

Injective homomorphisms

Definition

Let G, H be group. A map $\phi : G \to H$ is a *homomorphism* if for all $x, y \in G$,

$$\phi(xy) = \phi(x)\phi(y)$$

Lemma

$\phi(1) = 1$, and $\phi(g^{-1}) = \phi(g)^{-1}$.

Proof.

Take $x \in G$. Then $\phi(x) = \phi(1x) = \phi(1)\phi(x)$, so $\phi(1)$ acts as the identity.
Consider $\phi(gg^{-1})$. On one hand, $gg^{-1} = 1$, and we have shown that $\phi(1) = 1$. On the other hand, $\phi(gg^{-1}) = \phi(g)\phi(g^{-1})$. Hence $\phi(g^{-1})$ acts as the inverse of $\phi(g)$. □

Lemma

- $\phi(G) \leq H$.
- $\phi^{-1}(H) \leq G$, *and is trivial iff* ϕ *is injective.*
- *If* ϕ *is an injective homomorphism, then* $\phi(G) \simeq G$.
- *If* $G \leq H$ *then the inclusion is an injective homomorphism.*

Example

The exponential map

$$\mathbb{Z} \ni k \mapsto \exp(ki) \in \mathfrak{T}$$

is a homomorphism, by the functional equation of the complex exponential function. It is injective, since

$$\exp(ki) = 1 \iff \frac{k}{2\pi} \in \mathbb{Z} \iff k = 0$$

The image is the cyclic subgroup of $\mathfrak{T}$ generated by $\exp(i)$; this subgroup is infinite cyclic. The kernel is trivial.

Theorem (Cayley)

Let G be a group. Then there is a set X, and a subgroup $H \leq S_X$, such that $G \simeq H$.

Proof

1. Take any $g \in G$
2. Define $v_g : G \to G$ as left multiplication by g, so $v_g(x) = gx$
3. From lemma "Linear equations in group have unique soln" follows that v_g is a bijection (not an isomorphism though, does not respect multiplication).
4. So $v_g \in S_G$

Proof (contd)

5. $v_{gh}(x) = (gh) * x = g * (h * x) = v_g(v_h(x)) = (v_g \circ v_h)(x)$
6. So $G \ni g \mapsto v_g \in S_G$ respects multiplication
7. Furthermore, $g_1 \neq g_2 \implies v_{g_1} \neq v_{g_2}$ (evaluate at 1)
8. So $G \ni g \mapsto v_g \in S_G$ is an injective homomorphism.
9. Call its image H; this is a subgroup of S_X, with $X = G$.
10. Furthermore $G \simeq H$.

Example

Let G be Klein's Viergruppe, in its guise

*	I	S	T	R
I	I	S	T	R
S	S	I	R	T
T	T	R	I	S
R	R	T	S	I

Then left multiplication by the various group elements induce the folowing permutations (read the rows in the multiplication table):

$$I \longrightarrow (I)(S)(T)(R)$$
$$S \longrightarrow (I,S)(T,R)$$
$$T \longrightarrow (I,T)(S,R)$$
$$R \longrightarrow (I,R)(S,T)$$

These four permutations form a subgroup of $S_{\{I,S,T,R\}} \simeq S_4$ which is isomorphic to G.

Example

Let $G = S_3$, and label the elements as a through f, inte the order $[, (1,3,2), (1,2,3), (2,3), (1,3), (1,2)]$. The multiplication table is then

$*$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	f	d	e
c	c	a	b	e	f	d
d	d	e	f	a	b	c
e	e	f	d	c	a	b
f	f	d	e	b	c	a

The group elements induce the permutations

$$(), (bca)(dfe), (acb)(def), (ad)(be)(cf), (ae)(bf)(cd), (af)(bd)(ce)$$

which form a subgroup of $S_{\{a,b,c,d,e,f\}} \simeq S_6$