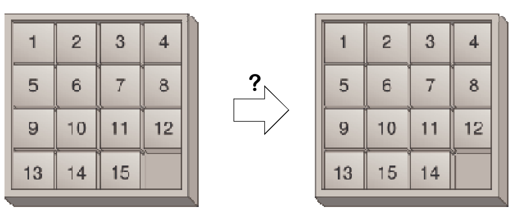
15-251

Some ~~Great~~ Theoretical Ideas ~~in~~ for Computer Science

Group Theory II

Lecture 19 (March 25, 2008)

The 15 Puzzle



Permutations

A permutation of a set X is a bijection $\alpha : X \to X$

We denote the set of all permutations of $X = \{1,2,\ldots,n\}$ by S_n

$|S_n| = n!$

Notation:

$\alpha = \begin{bmatrix} 1\ 2\ 3\ 4\ 5 \\ 4\ 3\ 2\ 1\ 5 \end{bmatrix}$ means $\alpha(1)=2$, $\alpha(2)=3$, …, $\alpha(5)=5$

Composition

Define the operation "•" on S_n to mean the composition of two permutations

As shorthand, we will write $\alpha\bullet\beta$ as $\alpha\beta$

To compute $\alpha\beta$, first apply β and then α:
$\alpha\beta(i) = \alpha(\beta(i))$

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

This permutation "fixes 2"

$$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

Groups

A group G is a pair $(S, \blacklozenge)$, where S is a set and $\blacklozenge$ is a binary operation on S such that:

1. $\blacklozenge$ is associative
2. (Identity) There exists an element $e \in S$ such that:
   $e \blacklozenge a = a \blacklozenge e = a$, for all $a \in S$
3. (Inverses) For every $a \in S$ there is $b \in S$ such that: $a \blacklozenge b = b \blacklozenge a = e$

If $\blacklozenge$ is commutative, then G is called a commutative group

$(S_n, \bullet)$ is a Group

Is • associative on S_n? YES!

Is there an identity? YES: The identity function

$$\begin{bmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{bmatrix}$$

Does every element have an inverse? YES!

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{bmatrix}$$

Is the group commutative? No!

Cycles

Let $i_1, i_2, \ldots, i_r$ be distinct integers between 1 and n. Define $(i_1\ i_2 \ldots i_r)$ to be the permutation α that fixes the remaining n-r integers and for which:

$$\alpha(i_1) = i_2,\ \alpha(i_2) = i_3,\ \ldots,\ \alpha(i_{r-1}) = i_r,\ \alpha(i_r) = i_1$$

$$(1\ 2\ 3\ 4) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$$

$$(1\ 5\ 3\ 4\ 2) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{bmatrix}$$

Examples

$$(1\ 5\ 2)(2\ 4\ 3) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{bmatrix}$$

$$(1\ 2\ 3)(4\ 5) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{bmatrix}$$

Two cycles are disjoint if every x moved by one is fixed by the other

$(i_1\ i_2 \ldots i_r)$ is called a cycle or an r-cycle

Express α as the product of disjoint cycles

Follow 1

Follow 2

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{bmatrix}$$

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

Theorem: Every permutation can be uniquely factored into the product of disjoint cycles

Express β as the product of disjoint cycles

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 3 & 2 & 4 & 6 & 1 & 8 & 9 & 5 \end{bmatrix}$$

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

Definition: A transposition is a 2-cycle

Express (1 2 3 4 5 6) as the product of transpositions (no necessarily disjoint):

(1 2 3 4 5 6) = (1 6)(1 5)(1 4)(1 3)(1 2)

Theorem: Every permutation can be factored as the product of transpositions

Is it unique? No!

(1 3)(1 2) = (1 2 3)

(1 3)(4 2)(1 2)(1 4) = (1 2 3)

But the parity is unique!

There are many ways to factor a permutation into transpositions

But, every factorization into transpositions has the same parity of the number of transpositions

Definition:

A permutation is even if it can be factored into an even number of transpositions

A permutation is odd if it can be factored into an odd number of transpositions

Examples

$\begin{bmatrix} 1\,2\,3 \\ 1\,2\,3 \end{bmatrix}$ = (1) is an even permutation

$\begin{bmatrix} 1\,2\,3 \\ 2\,3\,1 \end{bmatrix}$ = (1 2 3) = (1 3)(1 2) is an even permutation

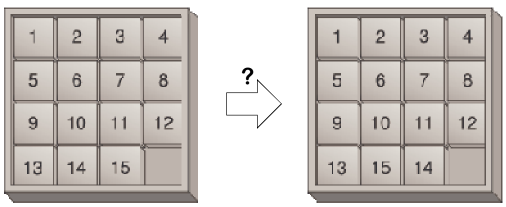
$\begin{bmatrix} 1\,2\,3 \\ 3\,2\,1 \end{bmatrix}$ = (1 3) is an odd permutation

Generators

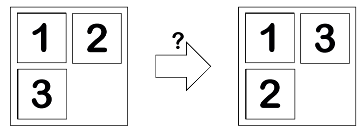
A set $T \subseteq S$ is said to generate the group $G = (S, \blacklozenge)$ if every element of S can be expressed as a finite product of elements in T

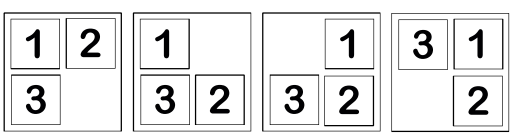
The set T = { (x y) | (x y) is a transposition in S_n} generates S_n

The 15 Puzzle



Let's Start Simpler





$\begin{bmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{bmatrix}$ $\begin{bmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{bmatrix}$ $\begin{bmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{bmatrix}$ $\begin{bmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{bmatrix}$

Notation: We will read the numbers in this order:

$$\begin{array}{ccc}1 & \longrightarrow & 2\\ & & \downarrow\\ 4 & \longleftarrow & 3\end{array}$$

and we will ignore the blank

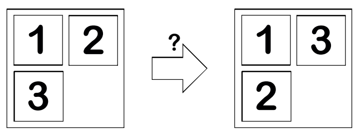
Reachable Permutations

$$\begin{bmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{bmatrix} = (1)$$

$$\begin{bmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{bmatrix} = (1\ 3)(1\ 2)$$

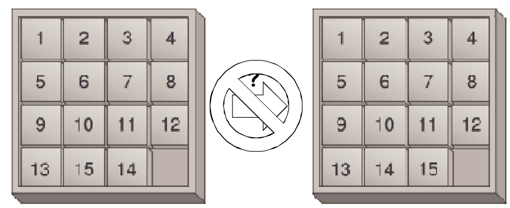
$$\begin{bmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{bmatrix} = (1\ 2)(1\ 3)$$

They are all even!!!



No, because $\begin{bmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{bmatrix}$ is an odd permutation

The 15 Puzzle



Similarly, it is possible to prove that only even permutations are possible in the 15 puzzle

Definition: The order of an element a of G is the smallest positive integer n such that $a^n = e$

(1 2 3)(1 2 3)(1 2 3) = (1)

What is the order of an r-cycle? r

Subgroups

Let G = (S, ♦) be a group. A non-empty subset H of G is a subgroup of G if:

1. $s \in H \Rightarrow s^{-1} \in H$
2. $s,t \in H \Rightarrow s \blacklozenge t \in H$

Theorem: If H is a subgroup of G, then e (the identity of G) is in H

Proof:

Let $h \in H$

Then $h^{-1} \in H$

Therefore $e = h \blacklozenge h^{-1} \in H$

Examples

Is { (1) } a subgroup of S_n? Yes

Is { (1), (1 2 3) } a subgroup of S_3?

No because $(1\ 2\ 3)^2$ is not in it

Is { 0, 3 } a subgroup of Z_6? Yes

Lagrange's Theorem

If H is a subgroup of G then |H| divides |G|

Proof: For $t \in G$, look at the set $Ht = \{ ht \mid h \in H\}$

Fact 1: if $a,b \in G$, then Ha and Hb are either identical or disjoint

Proof of Fact 1: Let $x \in Ha \cap Hb$.

Then $ha = x = kb$ where $h,k \in H$

So $k^{-1}h = ba^{-1} \in H$ and $(ba^{-1})^{-1} = ab^{-1} \in H$

Then Ha = Hb because:

If $x \in Hb$ then $x = jb$ ($j \in H$) so $x = jba^{-1}a \in Ha$

If $x \in Ha$ then $x = ja$ ($j \in H$) so $x = jab^{-1}b \in Hb$

Lagrange's Theorem

If H is a subgroup of G then |H| divides |G|

Proof: For $t \in G$, look at the set $Ht = \{ ht \mid h \in H\}$

Fact 1: if $a,b \in G$, then Ha and Hb are either identical or disjoint

Fact 2: if $a \in G$, then |Ha| = |H|

Proof of Fact 2: The function $f(s) = sa$ is a bijection from H to Ha

From Fact 1 and Fact 2, we see that G can be partitioned into sets of size |H|

For p prime, what are all the subgroups of Z_p?

By Lagrange's Theorem, the order of any subgroup of Z_p must divide p. Therefore, the only subgroups must have size 1 or p:

{0} and Z_p are the only subgroups of Z_p

S_2 =

•	(1)	(1 2)
(1)	(1)	(1 2)
(1 2)	(1 2)	(1)

Z_2 =

+	0	1
0	0	1
1	1	0

Are S_3 and Z_6 Isomorphic?

S_3	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1)	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	(1)	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	(1)	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	(1)	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	(1)
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	(1)	(1 2 3)

Here's What You Need to Know…

Permutations

Notation
Compositions
Cycles
Transpositions

Group Theory

Subgroups
LaGrange's Theorem
Isomorphisms