Chapter 8

Cayley Theorem and Puzzles

"As for everything else, so for a mathematical theory: beauty can be perceived but not explained."(Arthur Cayley)

We have seen that the symmetric group S_n of all the permutations of n objects has order $n!$, and that the dihedral group D_3 of symmetries of the equilateral triangle is isomorphic to S_3, while the cyclic group C_2 is isomorphic to S_2. We now wonder whether there are more connections between finite groups and the group S_n. There is in fact a very powerful one, known as Cayley Theorem:

Theorem 15. *Every finite group is isomorphic to a group of permutations (that is to some subgroup of S_n).*

This might be surprising but recall that given any finite group $G = \{g_1, g_2, \ldots, g_n\}$, every row of its Cayley table

	$g_1 = e$	g_2	g_3	$\cdots$	g_n
g_1					
g_2					
$\vdots$					
g_r	$g_r g_1$	$g_r g_2$	$g_r g_3$	$\cdots$	$g_r g_n$
$\vdots$					
g_n					

is simply a permutation of the elements of G ($g_r g_s \in \{g_1, g_2, \ldots, g_n\}$).

Groups and Permutation Groups

- We saw that $D_3=S_3$ and $C_2=S_2$.
- Is there any link in general between a given group G and groups of permutations?
- The answer is given by Cayley Theorem!

Cayley Theorem

Theorem Every finite group is isomorphic to a group of permutations.

This means a subgroup of some symmetric group.

One known link: for a group G, we can consider its multiplication (Cayley) table. Every row contains a permutation of the elements of the group.

Proof. Let $(G, \cdot)$ be a group. We shall exhibit a group of permutations $(\Sigma, \circ)$ that is isomorphic to G. We have seen that the Cayley table of $(G, \cdot)$ has rows that are permutations of $\{g_1, g_2, \ldots, g_n\}$, the elements of G. Therefore let us define

$$\Sigma = \{\sigma_g : G \to G,\ \sigma_g(x) = gx,\ \forall x \in G\}$$

for $g \in G$. In words we consider the permutation maps given by the rows of the Cayley table. We verify that Σ is a group under map composition.

1. To prove that Σ is closed under composition, we will to prove that

$$\sigma_{g_2} \circ \sigma_{g_1} = \sigma_{g_2 g_1},\ g_1 \in G,\ g_2 \in G.$$

   Indeed, for every $x \in G$,

$$\sigma_{g_2}(\sigma_{g_1}(x)) = \sigma_{g_2}(g_1 x) = g_2(g_1 x) = (g_2 g_1)x = \sigma_{g_2 g_1}(x) \in \Sigma$$

   since $g_2 g_1 \in G$.

2. Map composition is associative.

3. The identity element is $\sigma_e(x) = ex$, since

$$\sigma_g \circ \sigma_e = \sigma_{g \cdot e} = \sigma_g, \sigma_e \circ \sigma_g = \sigma_{e \cdot g} = \sigma_g.$$

4. The inverse. Consider g and g^{-1}, we have $gg^{-1} = g^{-1}g = e$. From

$$\sigma_{g_2} \circ \sigma_{g_1} = \sigma_{g_2 g_1}$$

   we have

$$\sigma_g \circ \sigma_{g^{-1}} = \sigma_e = \sigma_{g^{-1}} \circ \sigma_g.$$

Now we claim that $(G, \cdot)$ and $(\sum, \circ)$ are **isomorphic**, where the group isomorphism is given by

$$\phi : G \to \Sigma,\ g \mapsto \sigma_g.$$

Clearly if $\sigma_{g_1} = \sigma_{g_2}$ then $g_1 e = g_2 e \Rightarrow g_1 = g_2$. If $g_1 = g_2$, then $\sigma_{g_1} = \sigma_{g_2}$. Hence the map is one-to-one and onto, by construction!

Let us check that ϕ is a group homomorphism. If $g_1, g_2 \in G$,

$$\phi(g_1 g_2) = \sigma_{g_1 g_2} = \sigma_{g_1} \circ \sigma_{g_2} = \phi(g_1) \circ \phi(g_2),$$

and hence we are done, ϕ is an isomorphism between $(G, \cdot)$ and a permutation group! $\square$

Proof of Cayley Theorem (I)

- We need to find a group Σ of permutations isomorphic to G.
- Define $\Sigma=\{ \sigma_g : G \to G, \sigma_g(x)=gx , g \text{ in } G\}$

These are the permutations given by the rows of the Cayley table!

- The set Σ forms a group of permutations:
  - It is a set of permutations (bijections).
  - The identity is σ_1 since it maps x to x.
  - Associativity is that of map composition.
  - Closure: we have that $\sigma_{g1}\, \sigma_{g2} = \sigma_{g1g2}$.
  - Inverse: we have that $\sigma_g\, \sigma_{g^{(-1)}} = \sigma_1$.

Proof of Cayley Theorem (II)

- Left to prove: G and Σ are isomorphic.
- We define a group isomorphism $\phi: G \to \Sigma$, $\phi(g)=\sigma_g$.
  - The map ϕ is a bijection.
  - The map ϕ is a group homomorphism: $\phi(g_1g_2)=\phi(g_1)\, \phi(g_2)$.

    [Indeed: $\phi(g_1g_2)= \sigma_{g1g2} = \sigma_{g1}\, \sigma_{g2} =\phi(g_1)\, \phi(g_2)$.]

Now that we saw that all finite groups are subgroups of S_n, we can understand better why we could describe the symmetries of bounded shapes by the cyclic group C_n or the dihedral group D_n which can be mapped in a natural way to permutations of the vertex locations in the plane.

Example 30. Consider the group of integers modulo 3, whose Cayley table is

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

We have $\sigma_0(x) = x + 0$ corresponding to the permutation identity (). Then $\sigma_1(x) = x + 1$ corresponding to the permutation (123), $\sigma_2(x) = x + 2$ corresponding to (132).

Since we have a group homomorphism, addition in $G = \{\bar{0}, \bar{1}, \bar{2}\}$ corresponds to composition in $\Sigma = \{\sigma_0, \sigma_1, \sigma_2\}$. For example

$$\bar{1} + \bar{1} = \bar{2} \iff (123)(123) = (132).$$

We next illustrate how the techniques we learnt from group theory can be used to solve puzzles. We start with the **15 puzzle**. The goal is to obtain a configuration where the 14 and 15 have been switched.

Since this puzzle involves 16 numbers, we can look at it in terms of permutations of 16 elements.

Let us assume that when the game starts, the empty space is in position 16. Every move consists of switching the empty space 16 and some other piece. To switch 14 and 15, we need to obtain the permutation (14 15) as a product of transpositions, each involving the empty space 16. Now the permutation (14 15) has parity -1, while the product of transpositions will always have parity 1, since 16 must go back to its original position, and thus no matter which moves are done, the number of vertical moves are even, and the number of horizontal moves are even as well.

Example

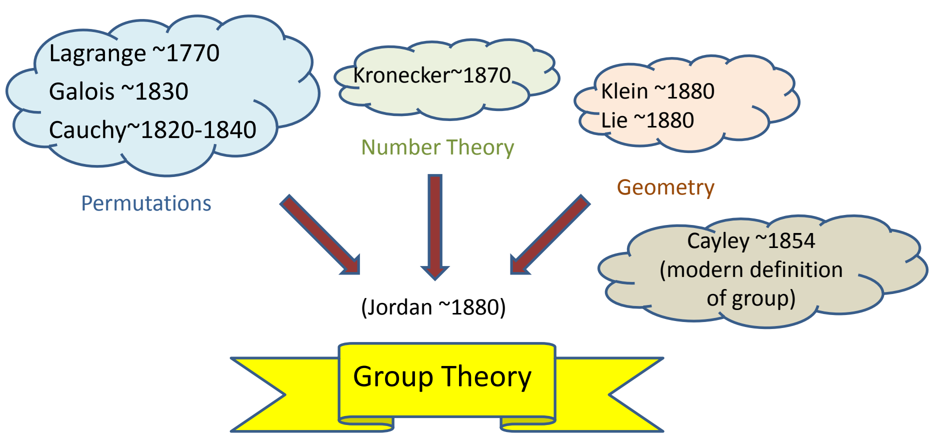
Take G={0,1,2} the group of integers mod 3.

	0	1	2	
0	0	1	2	()
1	1	2	0	(123)
2	2	0	1	(132)

- You can check the consistency of the operations! (homomorphism)
- For example: 1+1 =2 ↔ (123)(123)=(132)

This is a subgroup of S_3.

A Historical Point of View



[The symmetric group is complicated! Needs more tools.]

Some Applications

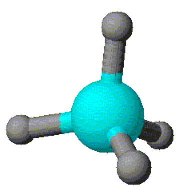
- Symmetries
- Cryptography
- Puzzles

Symmetries

One of the main focuses of this class

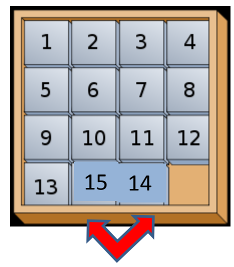
- Symmetries of finite planar shapes (cyclic and dihedral groups)
- Symmetries of some infinite planar shapes (Frieze groups, later!)

One could also study symmetries of 3-dimensional shapes!



A tetrahedral AB_4 molecule (ex. methane CH_4) with symmetric group A_4.

15 Puzzle



- 1870, New England
- 1890, price of 1000$ to who could solve it.

Impossibility of the 15 Puzzle (I)

Every move involves switching the empty space (say 16) and some other piece.

11	12		11				11		15	11		15	11
15			15	12		15	12			12		12	
		(12 16)			(11 16)			(15 16)			(12 16)		

Solving the puzzle means we can write:
$(14\ 15) = (a_n\ 16)(a_{n-1}\ 16) \ldots (a_2\ 16)(a_1\ 16)$

We next consider a **solitaire puzzle**. The goal of the game is to finish with a single stone in the middle of the board. This does not seem very easy! We might ask whether it would be easier to finish the game by having a single stone anywhere instead. To answer this question, we consider the Klein group, and label every position of the board with an element of the Klein group, such that two adjacent cells multiplied together give as result the label of the third cell (this is done by horizontally and vertically). The value of the board is given by multiplying all the group elements corresponding to board positions where a stone is. The key observation is that the value does not change when a move is made.

When the game starts, and only one stone is missing in the middle, the total value of the board is h (with the labeling shown on the slides). Since a move does not change the total value, we can only be left with a position containing an h. Since the board is unchanged under horizontal and vertical reflections, as well as under rotations by 90, 180, and 270 degrees, this further restricts the possible positions containing a valid h, and in fact, the easiest version is as hard as the original game!

Other applications of group theory can be found in the area of cryptography. We already saw Caesar cipher, and affine ciphers. We will see some more: (1) check digits and (2) the RSA cryptosystem.

Impossibility of the 15 Puzzle (II)

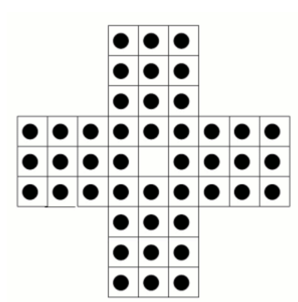
Solving the puzzle means we can write:
$(14\ 15) = (a_n\ 16)(a_{n-1}\ 16) \ldots (a_2\ 16)(a_1\ 16)$

parity = -1

parity = 1

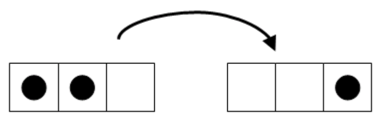
16 must return to its place, thus both number of horizontal and vertical moves are even!

Solitaire (I)



Solitaire (II)

- **A *move*** = pick up a marble, jump it horizontally or vertically (but *not* diagonally) over a single marble into a vacant hole, removing the marble that was jumped over.



- **A win** = finish with a single marble left in the central hole.
- Would it be **easier** if a win = finish with a single marble *anywhere*?

Solitaire (III)

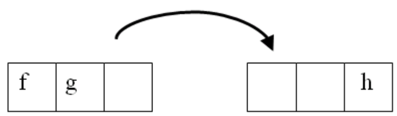
			f	g	h			
			g	h	f			
			h	f	g			
f	g	h	f	g	h	f	g	h
g	h	f	g	h	f	g	h	f
h	f	g	h	f	g	h	f	g
			f	g	h			
			g	h	f			
			h	f	g			

- G={1,f,g,h} = **Klein group**
- Label the board such that labels of two cells multiplied together give the label of the third cell.

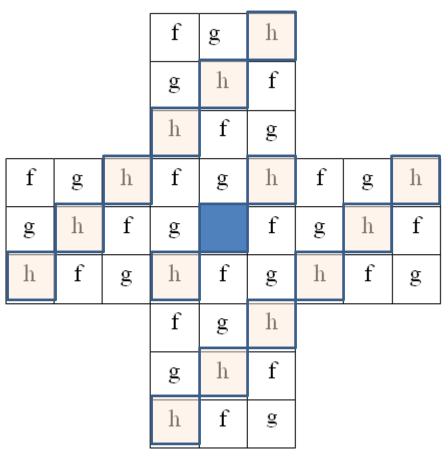
Binary operation of the Klein group

Solitaire (IV)

- ***total value*** of the board = the group element obtained by multiplying together the labels of *all* of the holes that have marbles in them.
- the total value *does not change when we make a move*!



Solitaire (V)



Total value =h

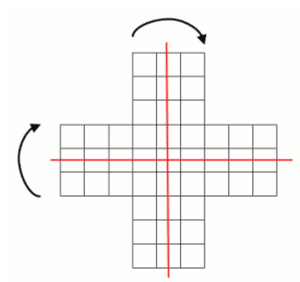
Total value= ?

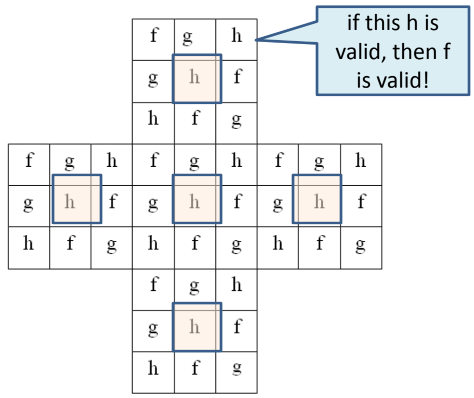
- $(fgh)^{15}$= fgh=e
- without h, we have fg=h.

Since a move does not change the total value, we can only be left with h!

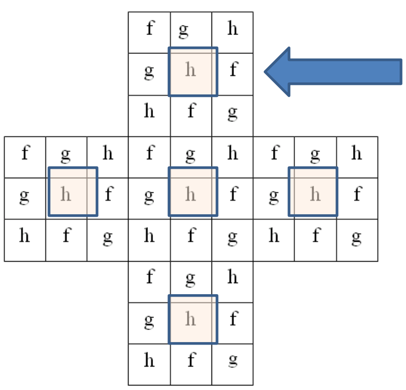
Solitaire (VI)

A Solitaire board is unchanged under reflection in the horizontal and vertical axes, and rotation through 90°, 180°, 270° and 360°.





Solitaire (VII)



If we can solve this position, then we can solve the middle one!

We just shown: the "easiest version" is as hard!!

Cryptography: Modular Arithmetic

Modular arithmetic (integers modulo n) enables

- Caesar's cipher $e_K: x \to e_K(x)=x+K \bmod 26, K=3$
- Affine ciphers

  $e_K: x \to e_K(x)=K_1x+K_2 \bmod 26, (K_1,26)=1, K=(K_1,K_2)$
- RSA cryptosystem

  $e_K: x \to e_K(x)=x^e \bmod n, K=(n,e)$

Cryptography: Discrete Log Problem

- "Regular" logarithm: $\log_a(b)$ is defined as the solution x of the equation $a^x = b$.
- Example: : $\log_2(8)=3$ since $2^3=8$.

- Discrete logarithm: let G be a finite cyclic group, take g and h in G, $\log_g(h)$ in G is defined as a solution x of the equation $g^x = h$.
- Example: $\log_3(13)=x$ in the group of invertible integers modulo 17 means that $3^x \equiv 13 \pmod{17}$, and x=4 is a solution.

Need to check this is a cyclic group!

This is useful in cryptography because solving the discrete log problem is hard!

Cryptography: Check Digit (I)

Take a message formed by a string of digits.

A **check digit** consists of a single digit, computed from the other digits, appended at the end of the message.

It is a form of redundancy to enable error detection.

We will look at the Check Digit introduced by J. Verhoeff in 1969, based on the dihedral group D_5.

Cryptography: Check Digit (II)

Multiplication table of D_5 with 0=do-nothing, 1-4=rotations, 5-9=reflections, *=binary operation in D_5.

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

Cryptography: Check Digit (III)

How does it work?Let σ be a permutation in S_{10}. To any string $a_1a_2\ldots\, a_{n-1}$ of digits, we append the check digit a_n so that

$\sigma(a_1)*\ \sigma^2(a_2)*\ \ldots *\sigma^{n-1}(a_{n-1})*\ \sigma^n(a_n)=0.$

Composition of the permutation σ

Binary operation of D_5

Single-digit errors are detected: if the digit a is replaced by b, then $\sigma^i(a)$ is replaced by $\sigma^i(b)$ ($\sigma^i(a)\neq\sigma^i(b)$ when $a\neq b$) thus the check digit is changed and an error is detected.

Cryptography: Check Digit (IV)

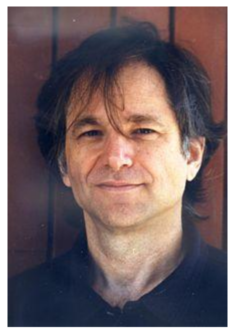
Example. Take $\sigma=(1,7,9)(2,5,10,4,6)$ and the digit 12345 (n-1=5).
[23456]

- $\sigma(2)=5$, $\sigma^2(3)=3$, $\sigma^3(4)=5$, $\sigma^4(5)=2$, $\sigma^5(6)=6$.
- $5*3*5*2*6*\ \sigma^6(a_6)=0 \Rightarrow 5*\ \sigma^6(a_6)=0 \Rightarrow \sigma^6(a_6)=\ 5$ and $a_6=2$.
- We get [234562] that is 123451.

Check digit 8 on a German banknote.

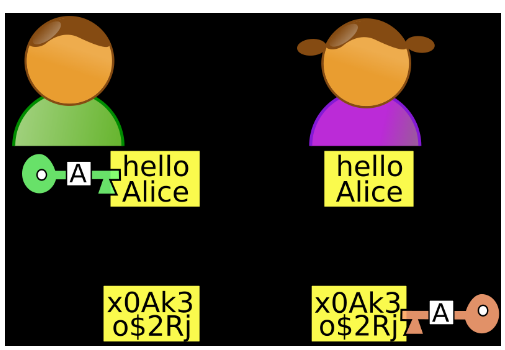
Application of Euler Theorem: RSA

RSA is an encryption scheme discovered by River, Shamir and Adleman (in 1978).

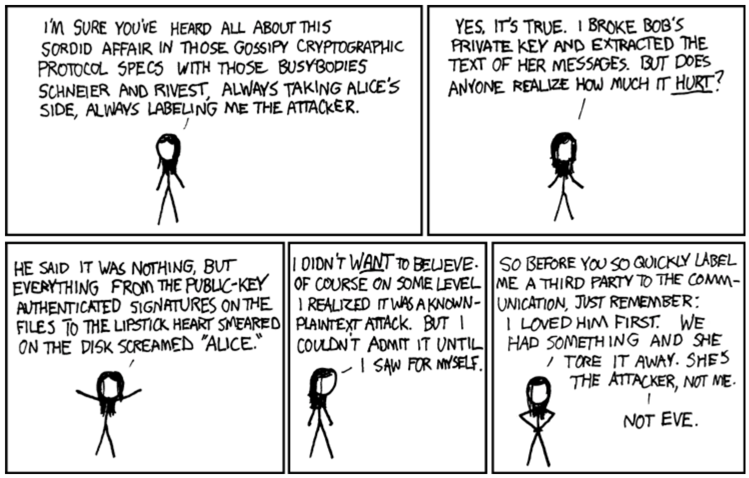


Alice and Bob Story

Alice and Bob want to exchange confidential data in the presence of an eavesdropper Eve.



Alice and Bob story by xkcd



RSA Protocol (I)

- Select two distinct large primes p and q ("large" means 100 digits ☺).
- Compute n=pq.
- The Euler totient function of n is $\varphi(n)$ = (p-1)(q-1).

This function counts the integers coprime to n.

- Pick an odd integer e such that e is coprime to $\varphi(n)$.
- Find d such that ed = 1 modulo $\varphi(n)$.

e exists because it is coprime to the Euler totient function!

Publish e and n as public keys, keep d private.

RSA Protocol (II)

- Alice: public key = (n,e), d is private.
- Bob sends m to Alice via the following encryption: c =m^e mod n.
- Alice decrypts: m = c^d mod n.

Why can Alice decrypt?

Step 1 c^d mod n = $(m^e)^d$ mod n.

Step 2 We have ed =1 +k $\varphi(n)$.

Step 3 Now $(m^e)^d$ mod n = $m^{1+k\varphi(n)}$ = m mod n when m is coprime to n.

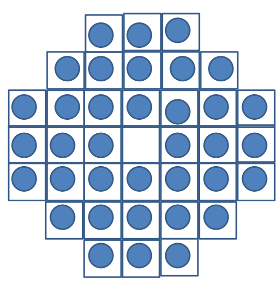
Exercises for Chapter 8

Exercise 40.

- Let G be the Klein group. Cayley's Theorem says that it is isomorphic to a subgroup of S_4. Identify this subgroup.
- Let G be the cyclic group C_4. Cayley's Theorem says that it is isomorphic to a subgroup of S_4. Identify this subgroup.

Exercise 41. Show that any rearrangement of pieces in the 15-puzzle starting from the standard configuration (pieces are ordered from 1 to 15, with the 16th position empty) which brings the empty space back to its original position must be an even permutation of the other 15 pieces.

Exercise 42. Has this following puzzle a solution? The rule of the game is



the same as the solitaire seen in class, and a win is a single marble in the middle of the board. If a win is a single marble anywhere in the board, is that any easier?