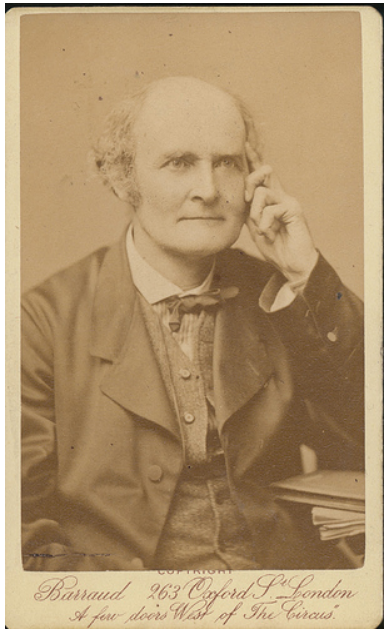
Cayley-Sudoku Tables

Michael Ward
with
Jennifer Carmichael WOU ‘06
Keith Schloeman WOU ’07

April 8, 2010

Outline

Arthur Cayley 1821-1895



Distinguished student at Cambridge. Graduated 1842. Barrister in London 1849-1863. Sadleirian Professor of Pure Mathematics at Cambridge 1863. Collected works in 13 volumes contain over 900 papers, including . . .

The First Paper on Abstract Group Theory

ON THE THEORY OF GROUPS, AS DEPENDING UPON THE SYMBOLIC EQUATION $\theta^n = 1$

Arthur Cayley

Philosophical Magazine, VOL. VII (1854)

Cayley's Definition of an Abstract Finite Group

A set of symbols,

$$1, \alpha, \beta, \ldots$$

all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a *group*[1].

Cayley's Definition of a Group

A set of symbols,

$$1, \alpha, \beta, \ldots$$

all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a *group*[1].

Notes and hidden assumptions

Cayley's Definition of a Group

A set of symbols,

$$1, \alpha, \beta, \ldots$$

all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a *group*[1].

Notes and hidden assumptions

- "product" refers to the result of some operation, which need not be multiplication

Cayley's Definition of a Group

A set of symbols,

$$1,\ \alpha,\ \beta, \ldots$$

all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a *group*[1].

Notes and hidden assumptions

- "product" refers to the result of some operation, which need not be multiplication
- The set is understood to be finite.

Cayley's Definition of a Group

A set of symbols,

$$1,\ \alpha,\ \beta, \ldots$$

all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a *group*[1].

Notes and hidden assumptions

- "product" refers to the result of some operation, which need not be multiplication
- The set is understood to be finite.
- Cayley is saying for any symbols (=elements) x, y in the set, xy is also in the set. We call that *closure*.

Cayley's Definition of a Group

A set of symbols,

$$1, \alpha, \beta, \ldots$$

all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a *group*[1].

Notes and hidden assumptions

- "product" refers to the result of some operation, which need not be multiplication
- The set is understood to be finite.
- Cayley is saying for any symbols (=elements) x, y in the set, xy is also in the set. We call that *closure*.
- 1 is meant to be an *identity* for the operation, meaning $1y = y = y1$ for any element y.

Cayley's Definition of a Group

A set of symbols,

$$1, \alpha, \beta, \ldots$$

all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a *group*[1].

Notes and hidden assumptions (continued)

Cayley's Definition of a Group

A set of symbols,

$$1,\ \alpha,\ \beta, \ldots$$

all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a *group*[1].

Notes and hidden assumptions (continued)

- In the preamble, Cayley makes it clear that the operation is meant to be associative, that is, for all elements x, y, z in the set, $(xy)z = x(yz)$.

Cayley's Definition of a Group

A set of symbols,

$$1,\ \alpha,\ \beta, \ldots$$

all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a *group*[1].

Notes and hidden assumptions (continued)

- In the preamble, Cayley makes it clear that the operation is meant to be associative, that is, for all elements x, y, z in the set, $(xy)z = x(yz)$.
- Cayley also requires cancelation: "...if $\theta = \phi$, then, whatever the symbols α, β may be, $\alpha\theta\beta = \alpha\phi\beta$, and conversely." From which it follows that there are *inverses*, that is, for any element x, there exists an element x' such that $xx' = 1 = x'x$.

Cayley continues . . .

It follows that if the entire group is multiplied by any one of the symbols, either as further or nearer factor, the effect is simply to reproduce the group; or what is the same thing, that if the symbols of the group are multiplied together so as to form a table, thus:

Further factors

Nearer factors	1	α	β	..
1	1	α	β	..
α	α	α^2	$\beta\alpha$	
β	β	$\alpha\beta$	β^2	
	:			

that as well each line as each column of the square will contain all the symbols 1, α, β, ...

- The table thus described by Cayley is now called the *Cayley Table* of the group.

- The table thus described by Cayley is now called the *Cayley Table* of the group.
- Cayley claims that it has 2/3 of the properties of a Sudoku-like table, that is, each symbol occurs (exactly) once in each row and exactly once in each column. Such a table is called a *Latin Square*.

- The table thus described by Cayley is now called the *Cayley Table* of the group.
- Cayley claims that it has 2/3 of the properties of a Sudoku-like table, that is, each symbol occurs (exactly) once in each row and exactly once in each column. Such a table is called a *Latin Square*.
- The convention nowadays is to have the row label as on the left ("further factor") and the column label on the right ("nearer factor").

	1	α	β	$\dots$
1	1	α	β	$\dots$
α	α	α^2	$\alpha\beta$	$\dots$
β	β	$\beta\alpha$	β^2	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Summary

1. A *group* is a set with an operation. The operation must be closed and associative. There must be an identity. Each element must have an inverse.

Summary

1. A *group* is a set with an operation. The operation must be closed and associative. There must be an identity. Each element must have an inverse.
2. Each group has a Cayley table in which each element occurs exactly once in each row and once in each column.

An Example of a Group

Set: $\mathbb{Z}_9 := \{1,2,3,4,5,6,7,8,9\}$

Operation: Addition mod 9, denoted $+_9$

- For every $x, y \in \mathbb{Z}_9$,
  $x +_9 y := x + y \bmod 9 := \bmod(x + y, 9)$

An Example of a Group

Set: $\mathbb{Z}_9 := \{1,2,3,4,5,6,7,8,9\}$

Operation: Addition mod 9, denoted $+_9$

- For every $x, y \in \mathbb{Z}_9$,
  $x +_9 y := x + y \bmod 9 := \bmod(x + y, 9)$
- $:=$ the remainder when $x + y$ is divided by 9 *Exception! Today only, write 9 when the remainder is 0.*

An Example of a Group

Set: $\mathbb{Z}_9 := \{1,2,3,4,5,6,7,8,9\}$

Operation: Addition mod 9, denoted $+_9$

- For every $x, y \in \mathbb{Z}_9$,
  $x +_9 y := x + y \bmod 9 := \bmod(x + y, 9)$
- $:=$ the remainder when $x + y$ is divided by 9 *Exception! Today only, write 9 when the remainder is 0.*
- Examples:

An Example of a Group

Set: $\mathbb{Z}_9 := \{1,2,3,4,5,6,7,8,9\}$

Operation: Addition mod 9, denoted $+_9$

- For every $x, y \in \mathbb{Z}_9$,
  $x +_9 y := x + y \bmod 9 := \bmod(x+y, 9)$
- $:=$ the remainder when $x+y$ is divided by 9 *Exception! Today only, write 9 when the remainder is 0.*
- Examples:
  - $3 +_9 8 := 3 + 8 \bmod 9 := \bmod(3+8, 9) = 2$

An Example of a Group

Set: $\mathbb{Z}_9 := \{1,2,3,4,5,6,7,8,9\}$

Operation: Addition mod 9, denoted $+_9$

- For every $x, y \in \mathbb{Z}_9$,
  $x +_9 y := x + y \bmod 9 := \bmod(x+y, 9)$
- $:=$ the remainder when $x+y$ is divided by 9 *Exception! Today only, write 9 when the remainder is 0.*
- Examples:
  - $3 +_9 8 := 3 + 8 \bmod 9 := \bmod(3+8, 9) = 2$
  - $3 +_9 6 = 9$

An Example of a Group

Set: $\mathbb{Z}_9 := \{1,2,3,4,5,6,7,8,9\}$

Operation: Addition mod 9, denoted $+_9$

- For every $x, y \in \mathbb{Z}_9$,
  $x +_9 y := x + y \bmod 9 := \bmod(x+y, 9)$
- $:=$ the remainder when $x+y$ is divided by 9 *Exception! Today only, write 9 when the remainder is 0.*
- Examples:
  - $3 +_9 8 := 3 + 8 \bmod 9 := \bmod(3+8, 9) = 2$
  - $3 +_9 6 = 9$
- For kids, it's "clock arithmetic" on a clock with 9 hours.

An Example of a Group

Set: $\mathbb{Z}_9 := \{1,2,3,4,5,6,7,8,9\}$

Operation: Addition mod 9, denoted $+_9$

- For every $x, y \in \mathbb{Z}_9$,
  $x +_9 y := x + y \bmod 9 := \bmod(x + y, 9)$
- $:=$ the remainder when $x + y$ is divided by 9 *Exception! Today only, write 9 when the remainder is 0.*
- Examples:
  - $3 +_9 8 := 3 + 8 \bmod 9 := \bmod(3 + 8, 9) = 2$
  - $3 +_9 6 = 9$
- For kids, it's "clock arithmetic" on a clock with 9 hours.
- Closure is clear. 9 is the identity. Inverses are easy to spot. Trust me on associativity. $\therefore$ it is a group.

Cayley Table of $\mathbb{Z}_9$ with operation $+_9$

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

(Unorthodox) Cayley Table of $\mathbb{Z}_9$ with operation $+_9$

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

Hold that thought . . .

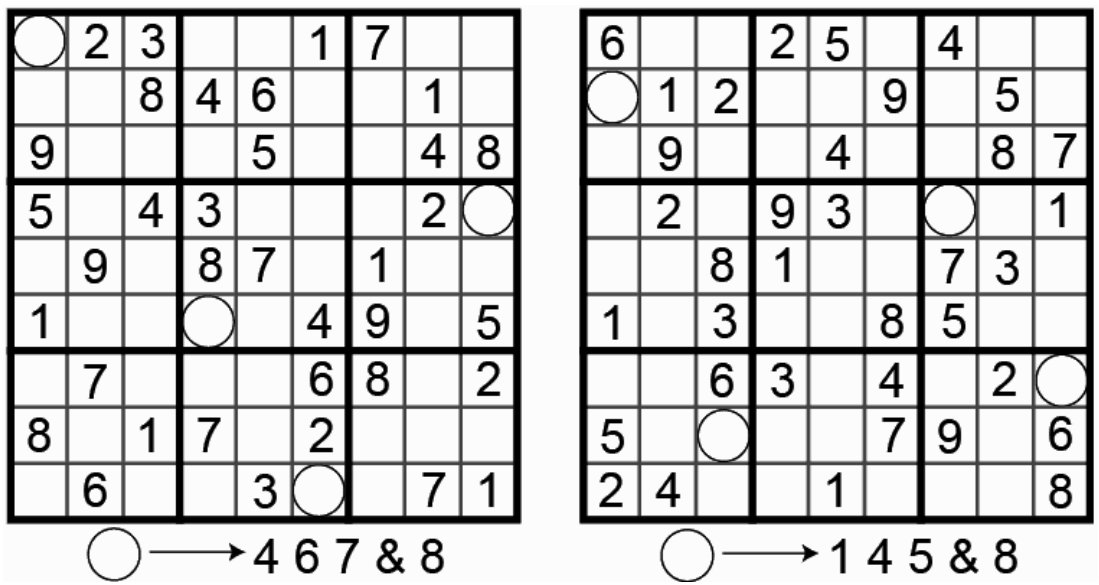
Whence Sudoku?

According to Ed Pegg, Jr. (MAA website),

> *In the May 1979 issue of Dell Pencil Puzzles & Word Games (issue #16), page 6, something amazing appeared:* ***Number Place****. Here are the original instructions: "In this puzzle, your job is to place a number into every empty box so that each row across, each column down, and each small 9-box square within the large square (there are 9 of these) will contain each number from 1 through 9. Remember that no number may appear more than once in any row across, any column down, or within any small 9-box square; this will help you solve the puzzle . . .*

Whence Sudoku?

. . . The numbers in circles below the diagram will give you a head start–each of these four numbers goes into one of the circle boxes in the diagram (not necessarily in the order given)."



The first Number Place puzzles. (*Dell Pencil Puzzles & Word Games* #16, page 6, 1979-05)

Whence Sudoku?

- Pegg cites personal communication with Will Shortz (*NY Times* crossword puzzle editor and "star" of the movie *Wordplay*), who found the puzzle was invented by 74 year old architect Howard Garns (circa 1905-1989).

Whence Sudoku?

- Pegg cites personal communication with Will Shortz (*NY Times* crossword puzzle editor and "star" of the movie *Wordplay*), who found the puzzle was invented by 74 year old architect Howard Garns (circa 1905-1989).
- The speaker first saw a Sudoku puzzle in the possession of Professor Sam Hall, Willamette U, July 2005.

Drum roll, please.

Divide the Cayley table of $\mathbb{Z}_9$ into nine 3 by 3 blocks, like a Sudoku puzzle.

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

Tah-dah! A Cayley-Sudoku Table

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

It is a Cayley table (so every group element appears exactly once in each row and in each column) and it is also a Sudoku table because it is divided into blocks in which each group element appears exactly once.

Every Cayley table has two of the three of the properties of a Sudoku table; only the subdivision of the table into blocks that contain each element exactly once is in doubt. When and how can a Cayley table be arranged in such a way as to satisfy the additional requirements of being a Sudoku table?

Examine our Cayley-Sudoku table of $\mathbb{Z}_9$ for clues.

Column Labels

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

The set of the first three column labels $\{9,3,6\}$ is also a group under $+_9$. That makes it a *subgroup* of $\mathbb{Z}_9$.

Column Labels

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

Add 1 to each of the elements of the subgroup: $9 +_9 1 = 1$, $3 +_9 1 = 4$, $6 +_9 1 = 7$, those are the next three column labels. The resulting set is called a *right coset* of the subgroup, it is denoted $\{9,3,6\} +_9 1$.

Column Labels

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

Now consider the right coset $\{9,3,6\} +_9 2 = \{9 +_9 2, 3 +_9 2, 6 +_9 2\} = \{2,5,8\}$. The elements of that coset are the final three column labels.

Column Labels

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

Observation 1: The columns in each block of the Cayley-Sudoku table are labeled with elements of the right cosets of a subgroup.

Row Labels

Left cosets of the subgroup are also of interest.

$9 +_9 \{9,3,6\} = \{9 +_9 9, 9 +_9 3, 9 +_9 6\} = \{9,3,6\}$

$1 +_9 \{9,3,6\} = \{1 +_9 9, 1 +_9 3, 1 +_9 6\} = \{1,4,7\}$

$2 +_9 \{9,3,6\} = \{2 +_9 9, 2 +_9 3, 2 +_9 6\} = \{2,5,8\}$

Notice that left and right cosets partition the group into disjoint subsets.

Row Labels

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

$9 +_9 \{9,3,6\} = \{9 +_9 9, 9 +_9 3, 9 +_9 6\} = \{9,3,6\}$

$1 +_9 \{9,3,6\} = \{1 +_9 9, 1 +_9 3, 1 +_9 6\} = \{1,4,7\}$

$2 +_9 \{9,3,6\} = \{2 +_9 9, 2 +_9 3, 2 +_9 6\} = \{2,5,8\}$

Row Labels

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

Observation 2: The rows in each block of the Cayley-Sudoku table are each labeled with a *complete set of left coset representatives*, that is, a *left transversal*.

Keith's Construction of a Cayley-Sudoku Table

Let G with operation $\star$ be a finite group. Assume H is a subgroup of G having order k and the number of distinct cosets is n (so that $|G| = nk$[1]). If $H \star g_1, H \star g_2, \ldots, H \star g_n$ are the n distinct right cosets of H in G, then arranging the Cayley table of G with columns labeled by the cosets $H \star g_1, H \star g_2, \ldots, H \star g_n$ and the rows labeled by sets $T_1, T_2, \ldots, T_k$ (as in the table) yields a Cayley-Sudoku table of G with blocks of dimension $n \times k$ if and only if $T_1, T_2, \ldots, T_k$ partition G into complete sets of left coset representatives of H in G.

	$H \star g_1$	$H \star g_2$	$\ldots$	$H \star g_n$
T_1				
T_2				
$\vdots$				
T_k				

[1] Lagrange's Theorem!

Another Example of a Group

D_4 = the set of symmetries of a square under the operation of composition of functions.

Eight Symmetries

Another Example of a Group

D_4 = the set of symmetries of a square under the operation of composition of functions.

Eight Symmetries

- Rotations about the center (counterclockwise):
  $R_0, R_{90}, R_{180}, R_{270}$

Another Example of a Group

D_4 = the set of symmetries of a square under the operation of composition of functions.

Eight Symmetries

- Rotations about the center (counterclockwise): $R_0, R_{90}, R_{180}, R_{270}$
- Reflections across lines through the center: H (horizontal), V (vertical), D and F (diagonal)
  (Yikes! H here is a reflection not a subgroup.)

Right cosets of the subgroup $\{R_0, H\}$ will label the columns.

1. $\{R_0, H\} \circ R_0 := \{R_0 \circ R_0, H \circ R_0\} = \{R_0, H\}$
2. $\{R_0, H\} \circ R_{90} := \{R_0 \circ R_{90}, H \circ R_{90}\} = \{R_{90}, D\}$
3. $\{R_0, H\} \circ R_{180} := \{R_0 \circ R_{180}, H \circ R_{180}\} = \{R_{180}, V\}$
4. $\{R_0, H\} \circ R_{270} := \{R_0 \circ R_{270}, H \circ R_{270}\} = \{R_{270}, F\}$

Complete sets of left coset representatives of $\{R_0, H\}$ will label the rows.

1. $R_0 \circ \{R_0, H\} := \{R_0 \circ R_0, R_0 \circ H\} = \{R_0, H\}$
2. $R_{90} \circ \{R_0, H\} := \{R_{90} \circ R_0, R_{90} \circ H\} = \{R_{90}, F\}$
3. $R_{180} \circ \{R_0, H\} := \{R_{180} \circ R_0, R_{180} \circ H\} = \{R_{180}, V\}$
4. $R_{270} \circ \{R_0, H\} := \{R_{270} \circ R_0, R_{270} \circ H\} = \{R_{270}, D\}$

These sets do the trick:
$T_1 := \{R_0, R_{90}, R_{180}, R_{270}\}$ and $T_2 := \{H, D, V, F\}$

(Notice the left and right cosets are not the same.)

Keith's Construction Applied to D_4

	R_0	H	R_{90}	D	R_{180}	V	R_{270}	F
R_0	R_0	H	R_{90}	D	R_{180}	V	R_{270}	F
R_{90}	R_{90}	F	R_{180}	H	R_{270}	D	R_0	V
R_{180}	R_{180}	V	R_{270}	F	R_0	H	R_{90}	D
R_{270}	R_{270}	D	R_0	V	R_{90}	F	R_{180}	H
H	H	R_0	D	R_{90}	V	R_{180}	F	R_{270}
V	V	R_{180}	F	R_{270}	H	R_0	D	R_{90}
D	D	R_{270}	V	R_0	F	R_{90}	H	R_{180}
F	F	R_{90}	H	R_{180}	D	R_{270}	V	R_0

Why Keith's Construction Works

Look at one block in our $\mathbb{Z}_9$ Cayley-Sudoku Table.

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

Why is each group element in it exactly once?

Why Keith's Construction Works

Deconstruct the block. Recall the column label set $\{1,4,7\}$ is the right coset $\{9,3,6\} +_9 1 := \{9 +_9 1, 3 +_9 1, 6 +_9 1\}$.

	9	3	6	$9 +_9 1$	$3 +_9 1$	$6 +_9 1$	2	5	8
3				$3 +_9 (9 +_9 1)$	$3 +_9 (3 +_9 1)$	$3 +_9 (6 +_9 1)$			
4				$4 +_9 (9 +_9 1)$	$4 +_9 (3 +_9 1)$	$4 +_9 (6 +_9 1)$			
5				$5 +_9 (9 +_9 1)$	$5 +_9 (3 +_9 1)$	$4 +_9 (6 +_9 1)$			

Apply the associative property.

	9	3	6	$9 +_9 1$	$3 +_9 1$	$6 +_9 1$	2	5	8
3				$(3 +_9 9) +_9 1$	$(3 +_9 3) +_9 1$	$(3 +_9 6) +_9 1$			
4				$(4 +_9 9) +_9 1$	$(4 +_9 3) +_9 1$	$(4 +_9 6) +_9 1$			
5				$(5 +_9 9) +_9 1$	$(5 +_9 3) +_9 1$	$(4 +_9 6) +_9 1$			

Recall row labels = complete set of left coset reps.

	9	3	6	$9 +_9 1$		$3 +_9 1$		$6 +_9 1$		2	5	8
3				$(3 +_9 9) +_9 1$		$(3 +_9 3) +_9 1$		$(3 +_9 6) +_9 1$				
4				$(4 +_9 9) +_9 1$		$(4 +_9 3) +_9 1$		$(4 +_9 6) +_9 1$				
5				$(5 +_9 9) +_9 1$		$(5 +_9 3) +_9 1$		$(5 +_9 6) +_9 1$				

$3 +_9 \{9,3,6\} = \{3 +_9 9, 3 +_9 3, 3 +_9 6\} = \{3,6,9\}$

$4 +_9 \{9,3,6\} = \{4 +_9 9, 4 +_9 3, 4 +_9 6\} = \{4,7,1\}$

$5 +_9 \{9,3,6\} = \{5 +_9 9, 5 +_9 3, 5 +_9 6\} = \{5,8,2\}$

Substitute.

	9	3	6	$9+_9 1$	$3+_9 1$	$6+_9 1$	2	5	8
3				$3+_9 1$	$6+_9 1$	$9+_9 1$			
4				$4+_9 1$	$7+_9 1$	$1+_9 1$			
5				$5+_9 1$	$8+_9 1$	$2+_9 1$			

Cayley tells us that adding 1 to the group elements gives the group elements back. Elegant!

"Christmas Eve" Construction of a Cayley-Sudoku Table

	$t_1 \star H$	$t_2 \star H$	$\ldots$	$t_n \star H$
L_1				
L_2				
$\vdots$				
L_k				

In order for the above to be a Cayley-Sudoku table, the sets $L_1, L_2, \ldots, L_k$ labeling the rows must be complete sets of left coset representatives for H and (usually) several other subgroups at once!

(Namely, for the subgroups $g^{-1} \star H \star g$ for all $g \in G$, where $g^{-1} \star H \star g := \{g^{-1} \star h \star g : h \in H\}$.)

Use the subgroup $\{R_0, H\}$.
Left cosets of $\{R_0, H\}$ will label the columns.

1. $R_0 \circ \{R_0, H\} := \{R_0 \circ R_0, R_0 \circ H\} = \{R_0, H\}$
2. $R_{90} \circ \{R_0, H\} := \{R_{90} \circ R_0, R_{90} \circ H\} = \{R_{90}, F\}$
3. $R_{180} \circ \{R_0, H\} := \{R_{180} \circ R_0, R_{180} \circ H\} = \{R_{180}, V\}$
4. $R_{270} \circ \{R_0, H\} := \{R_{270} \circ R_0, R_{270} \circ H\} = \{R_{270}, D\}$

Rows must be labeled with complete sets of left coset representatives for $\{R_0, H\}$ and for the subgroup $\{R_0, V\}$ (i.e. $R_{90}^{-1} \circ \{R_0, V\} \circ R_{90}$).

1. $R_0 \circ \{R_0, V\} := \{R_0 \circ R_0, R_0 \circ v\} = \{R_0, V\}$
2. $R_{90} \circ \{R_0, V\} := \{R_{90} \circ R_0, R_{90} \circ V\} = \{R_{90}, D\}$
3. $R_{180} \circ \{R_0, V\} := \{R_{180} \circ R_0, R_{180} \circ V\} = \{R_{180}, H\}$
4. $R_{270} \circ \{R_0, V\} := \{R_{270} \circ R_0, R_{270} \circ V\} = \{R_{270}, F\}$

These sets do the trick:
$L_1 := \{R_0, R_{90}, R_{180}, R_{270}\}$ and $L_2 := \{H, V, D, F\}$

Christmas Eve Construction Applied to D_4

	R_0	H	R_{90}	F	R_{180}	V	R_{270}	D
R_0	R_0	H	R_{90}	F	R_{180}	V	R_{270}	D
R_{90}	R_{90}	F	R_{180}	V	R_{270}	D	R_0	H
R_{180}	R_{180}	V	R_{270}	D	R_0	H	R_{90}	F
R_{270}	R_{270}	D	R_0	H	R_{90}	F	R_{180}	V
H	H	R_0	D	R_{270}	V	R_{180}	F	R_{90}
V	V	R_{180}	F	R_{90}	H	R_0	D	R_{270}
D	D	R_{270}	V	R_{180}	F	R_{90}	H	R_0
F	F	R_{90}	H	R_0	D	R_{270}	V	R_{180}

Question: Under what conditions on H can G be partitioned into complete sets of left coset representatives of all the required subgroups (i.e. of $g^{-1} \star H \star g$ for all $g \in G$)?

From group theory

Question: Under what conditions on H can G be partitioned into complete sets of left coset representatives of all the required subgroups (i.e. of $g^{-1} \star H \star g$ for all $g \in G$)?

From group theory

- Only one subgroup–Easy, but it's just Keith's Construction (H a *normal* subgroup in this case)

Question: Under what conditions on H can G be partitioned into complete sets of left coset representatives of all the required subgroups (i.e. of $g^{-1} \star H \star g$ for all $g \in G$)?

From group theory

- Only one subgroup–Easy, but it's just Keith's Construction (H a *normal* subgroup in this case)
- Can be done whenever H has a *complement* (i.e. $\exists$ a subgroup T of G such that $G = TH := \{t \star h : t \in T, h \in H\}$ and $T \cap H =$ identity).

From combinatorics

From combinatorics

- Two subgroups (as in the example)–Can be done as a corollary to a general combinatorial theorem ("Arranged Marriage Theorem" = Hall's Marriage Theorem for two families)

From combinatorics

- Two subgroups (as in the example)–Can be done as a corollary to a general combinatorial theorem ("Arranged Marriage Theorem" = Hall's Marriage Theorem for two families)
- Three or more subgroups–No general combinatorial theorem? In general, NP-complete?

Cayley-Sudoku Puzzles

Given a partially completed Cayley-Sudoku Table of an unknown group (and not assuming it was made by one of the given constructions), complete the table so that each group element appears exactly once in each row, in each column, and in each designated block.

Hints

- The usual Sudoku techniques.

Cayley-Sudoku Puzzles

Given a partially completed Cayley-Sudoku Table of an unknown group (and not assuming it was made by one of the given constructions), complete the table so that each group element appears exactly once in each row, in each column, and in each designated block.

Hints

- The usual Sudoku techniques.
- Look for the identity.

Cayley-Sudoku Puzzles

Given a partially completed Cayley-Sudoku Table of an unknown group (and not assuming it was made by one of the given constructions), complete the table so that each group element appears exactly once in each row, in each column, and in each designated block.

Hints

- The usual Sudoku techniques.
- Look for the identity.
- If you find $x \cdot y =$ identity, then you also know $x \cdot y =$ identity.

Cayley-Sudoku Puzzles

Given a partially completed Cayley-Sudoku Table of an unknown group (and not assuming it was made by one of the given constructions), complete the table so that each group element appears exactly once in each row, in each column, and in each designated block.

Hints

- The usual Sudoku techniques.
- Look for the identity.
- If you find $x \cdot y =$ identity, then you also know $x \cdot y =$ identity.
- In the given puzzle, the group is not $\mathbb{Z}_8$. The puzzle can be done without knowing the actual group.

Concluding Remarks

1. For another construction (extending a Cayley-Sudoku table of a subgroup to a table for the big group) and more open questions see Cosets and Cayley-Sudoku Tables, *Mathematics Magazine* Vol. 83, April 2010, pp. 130-139.

Concluding Remarks

1. For another construction (extending a Cayley-Sudoku table of a subgroup to a table for the big group) and more open questions see Cosets and Cayley-Sudoku Tables, *Mathematics Magazine* Vol. 83, April 2010, pp. 130-139.
2. THANK YOU!!

Appendix: Keith's Construction Applied to A_4

	(1)	(12)(34)	(13)(24)	(14)(23)	(123)	(243)	(142)	(134)	(132)	(143)	(234)	(124)
(1)	(1)	(12)(34)	(13)(24)	(14)(23)	(123)	(243)	(142)	(134)	(132)	(143)	(234)	(124)
(13)(24)	(13)(24)	(14)(23)	(1)	(12)(34)	(142)	(134)	(123)	(243)	(234)	(124)	(132)	(143)
(123)	(123)	(134)	(243)	(142)	(132)	(124)	(143)	(234)	(1)	(14)(23)	(12)(34)	(13)(24)
(243)	(243)	(142)	(123)	(134)	(143)	(234)	(132)	(124)	(12)(34)	(13)(24)	(1)	(14)(23)
(132)	(132)	(234)	(124)	(143)	(1)	(13)(24)	(14)(23)	(12)(34)	(123)	(142)	(134)	(243)
(143)	(143)	(124)	(234)	(132)	(12)(34)	(14)(23)	(13)(24)	(1)	(243)	(134)	(142)	(123)
(12)(34)	(12)(34)	(1)	(14)(23)	(13)(24)	(243)	(123)	(134)	(142)	(143)	(132)	(124)	(234)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	(1)	(134)	(142)	(243)	(123)	(124)	(234)	(143)	(132)
(134)	(134)	(123)	(142)	(243)	(124)	(132)	(234)	(143)	(14)(23)	(1)	(13)(24)	(12)(34)
(142)	(142)	(243)	(134)	(123)	(234)	(143)	(124)	(132)	(13)(24)	(12)(34)	(14)(23)	(1)
(234)	(234)	(132)	(143)	(124)	(13)(24)	(1)	(12)(34)	(14)(23)	(142)	(123)	(243)	(134)
(124)	(124)	(143)	(132)	(234)	(14)(23)	(12)(34)	(1)	(13)(24)	(134)	(243)	(123)	(142)

The columns in each 6×2 block are labeled with the elements of the subgroup $\{(1), (12)(34)\}$ in A_4, the group of even permutations on four symbols. The rows in each block are labeled with complete sets of left coset representatives.

In this case the right and left cosets are not the same.

Example: $\{(1), (12)(34)\}(123) = \{(123), (243)\}$ while $(123)\{(1), (12)(34)\} = \{(123), (134)\}$.

Appendix 1 Partial Proof of K's Construction

An arbitrary block of the table, indexed by $T_h = \{t_1, t_2, \ldots, t_n\}$ and $H \star g_i$, is the given the following table.

	$H \star g_i$
t_1	$t_1 \star H \star g_i$
t_2	$t_2 \star H \star g_i$
$\vdots$	$\vdots$
t_n	$t_n \star H \star g_i$

1. Elements in the block:
   $B := (t_1 \star H \star g_i) \cup (t_2 \star H \star g_i) \cup \ldots \cup (t_n \star H \star g_i)$

Appendix 1 Partial Proof of K's Construction

An arbitrary block of the table, indexed by $T_h = \{t_1, t_2, \ldots, t_n\}$ and $H \star g_i$, is the given the following table.

	$H \star g_i$
t_1	$t_1 \star H \star g_i$
t_2	$t_2 \star H \star g_i$
$\vdots$	$\vdots$
t_n	$t_n \star H \star g_i$

1. Elements in the block:
   $B := (t_1 \star H \star g_i) \cup (t_2 \star H \star g_i) \cup \ldots \cup (t_n \star H \star g_i)$
2. Easy to show using associativity:
   $B = (t_1 \star H \cup t_2 \star H \cup \ldots \cup t_n \star H) \star g_i$

Appendix 1 Partial Proof of K's Construction

An arbitrary block of the table, indexed by $T_h = \{t_1, t_2, \ldots, t_n\}$ and $H \star g_i$, is the given the following table.

	$H \star g_i$
t_1	$t_1 \star H \star g_i$
t_2	$t_2 \star H \star g_i$
$\vdots$	$\vdots$
t_n	$t_n \star H \star g_i$

1. Elements in the block:
   $B := (t_1 \star H \star g_i) \cup (t_2 \star H \star g_i) \cup \ldots \cup (t_n \star H \star g_i)$
2. Easy to show using associativity:
   $B = (t_1 \star H \cup t_2 \star H \cup \ldots \cup t_n \star H) \star g_i$
3. When T_h is a complete set of left coset representatives, then
   $t_1 \star H \cup t_2 \star H \cup \ldots \cup t_n \star H = G$.

Appendix 1 Partial Proof of K's Construction

An arbitrary block of the table, indexed by $T_h = \{t_1, t_2, \ldots, t_n\}$ and $H \star g_i$, is the given the following table.

	$H \star g_i$
t_1	$t_1 \star H \star g_i$
t_2	$t_2 \star H \star g_i$
$\vdots$	$\vdots$
t_n	$t_n \star H \star g_i$

1. Elements in the block:
   $B := (t_1 \star H \star g_i) \cup (t_2 \star H \star g_i) \cup \ldots \cup (t_n \star H \star g_i)$
2. Easy to show using associativity:
   $B = (t_1 \star H \cup t_2 \star H \cup \ldots \cup t_n \star H) \star g_i$
3. When T_h is a complete set of left coset representatives, then
   $t_1 \star H \cup t_2 \star H \cup \ldots \cup t_n \star H = G$.
4. By Cayley, $B = G \star g_i = G$.

	$H \star g_i$
t_1	$t_1 \star H \star g_i$
t_2	$t_2 \star H \star g_i$
$\vdots$	$\vdots$
t_n	$t_n \star H \star g_i$

We just saw that each element of the group is in the above block.

1. Number of entries in block $B \equiv$ number of elements in G

	$H \star g_i$
t_1	$t_1 \star H \star g_i$
t_2	$t_2 \star H \star g_i$
$\vdots$	$\vdots$
t_n	$t_n \star H \star g_i$

We just saw that each element of the group is in the above block.

1. Number of entries in block $B \equiv$ number of elements in G
2. $\therefore$ every element of G appears exactly once.