MEI Innovators in Mathematics Education

Mathematics in Education and Industry

50 years at the forefront of Mathematics Education

Members only an introduction to groups

Sue de Pomerai
MEI (FMSP Deputy rogramme Leader)

Latin squares

A **Latin square** is an $n \times n$ table filled with n different symbols in such a way that each symbol occurs exactly once in each row and exactly once in each column.

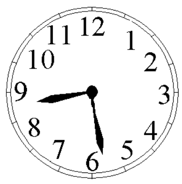
1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

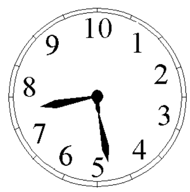
1	2	3	4
2	4	1	3
3	1	4	2
4	3	2	1

The great Swiss mathematician Leonhard Euler introduced the idea of latin squares in 1783. He used Latin characters as symbols, hence the name.

Uses:
error correcting codes
Experimental design

Clock arithmetic





9 + 4 = 1 (mod 12)   9 + 4 = 3 (mod 10)

The number X (mod Y) is the remainder when X is divided by Y.

Binary operations

Most operations take two elements of a set and combine them to give a definite result; such a rule of combination is called a **binary operation.**

Modular arithmetic

What are the similarities and differences?

+	0	1	2	3	4
0					
1			3		0
2					1
3					
4					3

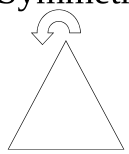
X	0	1	2	3	4
0					
1			2		
2					3
3					
4					

Modular arithmetic – mod 5

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

X_5	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Symmetry: equilateral triangle

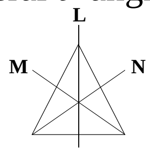


Rotations

I 0º (or 360º)

R_1 120º anticlockwise

R_2 240º anticlockwise



Reflections

L reflection in line L

M reflection in line M

N reflection in line N

Groups

	first						
	*	I	R_1	R_2	L	M	N
second	I			R_2			
	R_1						
	R_2			R_1	N		
	L				I		
	M		L				
	N					R_1	

Groups

	first						
	*	I	R_1	R_2	L	M	N
second	I	I	R_1	R_2	L	M	N
	R_1	R_1	R_2	I	M	N	L
	R_2	R_2	I	R_1	N	L	M
	L	L	N	M	I	R_2	R_1
	M	M	L	N	R_1	I	R_2
	N	N	M	L	R_2	R_1	I

Group axioms

A group (G, *) is a non empty set G with a binary operation * such that

- * is closed in G
  a*b $\in$G for all a,b $\in$G
- There is an identity element *e* $\in$G such that a*e = e*a = a for all a $\in$G
- Inverses: for all *a* $\in$G, there is an element a^{-1} such that $a * a^{-1} = e$
- Associativity:
  a(b*c) = (a*b)*c* for all *a,b,c* $\in$G

Groups

	first						
	*	I	R_1	R_2	L	M	N
second	I	I	R_1	R_2	L	M	N
	R_1	R_1	R_2	I	M	N	L
	R_2	R_2	I	R_1	N	L	M
	L	L	N	M	I	R_2	R_1
	M	M	L	N	R_1	I	R_2
	N	N	M	L	R_2	R_1	I

	first			
second	*	I	R_1	R_2
	I	I	R_1	R_2
	R_1	R_1	R_2	I
	R_2	R_2	I	R_1

There is one subgroup

MEI Innovators in Mathematics Education — Mathematics in Education and Industry

Is it a group?

All integers under subtraction

No – subtraction is not associative

3 – (6 – 2) = -1
(3 – 6) – 2 = -5

MEI Innovators in Mathematics Education — Mathematics in Education and Industry

Is it a group?

{1, 10} under multiplication modulo 11

X_{11}	1	10
1	1	10
10	10	1

yes

MEI Innovators in Mathematics Education — Mathematics in Education and Industry

Is it a group?

All irrational numbers under multiplication

No – it is not closed

$\sqrt{2}$ X $\sqrt{2}$ = 2, which is rational

MEI Innovators in Mathematics Education — Mathematics in Education and Industry

The missing axiom

Commutativity:

$a * b = b * a$ for all $a, b, \in G$

Is $+_5$ commutative? Yes

Is X_5 commutative? Yes

Is * commutative? No

Groups that are also commutative are called Abelian groups after the Norwegian mathematician Neils Abel

MEI Innovators in Mathematics Education — Mathematics in Education and Industry

A bit of history

- The theory of groups started early in nineteenth century in connection with the solutions of algebraic equations.
- Originally a group was the set of all permutations of the roots of an algebraic equation which has the property that combination of any two of these permutations again belongs to the set.
- Later the idea was generalized to the concept of an abstract group. An abstract group is essentially the study of a set with an operation defined on it.
- Group theory has many useful applications both within and outside mathematics.
- Groups arise in a number of apparently unconnected subjects. In fact they appear in crystallography and quantum mechanics in geometry and topology, in analysis and algebra and even in biology.

A bit of history

Euler, Gauss, LaGrange, Ruffini, Abel Cauchy, Klein, Cayley

Evariste Galois

Born: 25 Oct 1811 in Bourg La Reine (near Paris), France
Died: 31 May 1832 in Paris, France

Finding Moonshine

Marcus du Sautoy

PLUS Maths

- http://plus.maths.org/issue48/package/index.html#intro
- A package of readings and resources for teachers
- http://www-history.mcs.st-andrews.ac.uk
- Find out abut your favourite mathematicians

example

Consider the set *S* = {1, 3, 4, 9, 10, 12} on which the operation * is defined as multiplication modulo 13.

(a) Write down the Cayley table for *S* under *.

(b) Assuming multiplication modulo 13 is associative, show that (*S* , *) is a commutative group.

(c) State the order of each element.

(d) Find all the subgroups of (*S*, *)

answer

Consider the set *S* = {1, 3, 4, 9, 10, 12} on which the operation * is defined as multiplication modulo 13.
(a) Write down the Cayley table for *S* under *.

*	1	3	4	9	10	12
1	1	3	4	9	10	12
3	3	9	12	1	4	10
4	4	12	3	10	1	9
9	9	1	10	3	12	4
10	10	4	1	12	9	3
12	12	10	9	4	3	1

(b) Assuming multiplication modulo 13 is associative, show that (*S* , *) is a commutative group.

(b)
The set is closed under *
1 is the identity element
Every element has an inverse because 1 is on each row.

Self inverses

$1^{-1}=1$

$12^{-1}=12$

inverse pairs

$3^{-1}=9$

$4^{-1}=12$

$9^{-1}=3$

$12^{-1}=4$

* is associative (assumed) and commutative since multiplication modulo 13 is associative and commutative

MEI Innovators in Mathematics Education — Mathematics in Education and Industry

(c) State the order of each element.

(c) 1 is of order 1
12 is of order 2
3 and 9 are of order 3

4 and 10 are of order 6

*	1	3	4	9	10	12
1	1	3	4	9	10	12
3	3	9	12	1	4	10
4	4	12	3	10	1	9
9	9	1	10	3	12	4
10	10	4	1	12	9	3
12	12	10	9	4	3	1

MEI Innovators in Mathematics Education — Mathematics in Education and Industry

Find all the subgroups of (S, *)

(d) Subgroups must have order 1, 2, 3, 6 (Lagrange's theorem)

Order 1
{1}

Order 2
{1, 12}

Order 3
{1, 3, 9}

Order 6
{1, 3, 4, 9, 10, 12}

*	1	3	4	9	10	12
1	1	3	4	9	10	12
3	3	9	12	1	4	10
4	4	12	3	10	1	9
9	9	1	10	3	12	4
10	10	4	1	12	9	3
12	12	10	9	4	3	1

MEI Innovators in Mathematics Education — Mathematics in Education and Industry

Here is the ultimate Sudoku variation — Binary Sudoku:

1	

There are 10 possible boards, each more exciting than the last.

0	1
1	0

(of course, that's the binary number 10)

Group Theory

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

Latin squares

A **Latin square** is an *n* × *n* table filled with *n* different symbols in such a way that each symbol (element) occurs exactly once in each row and exactly once in each column.

Consider the this latin square; it is of order 4 below and is constructed by cyclically permuting the symbols in the first row for subsequent rows.

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

Binary operations

Most operations take two elements of a set and combine them to give a definite result; such a rule of combination is called a binary operation.

Modular arithmetic – complete these tables for addition and multiplication in modulo 5.

+	**0**	**1**	**2**	**3**	**4**
0					
1			3		0
2					1
3					
4					3

X	**0**	**1**	**2**	**3**	**4**
0					
1			2		
2					3
3					
4					

The number X (mod Y) is the remainder when X is divided by Y.

- **What are the differences in structure between the two tables?**

Calculate the values of 3^0, 3^1, 3^2, 3^3, 3^4, 3^5 in modulo 5. What do you notice?

TFM3 Group Theory

Groups

In abstract algebra, a **group** (G, *) is a non empty set G with a binary operation * which satisfies these axioms

- Closure: $a*b \in G$ for all $a,b \in G \Rightarrow$ * is closed in G
- Identity: there is an element $e \in G$ such that $a*e = e*a = a$ for all $a \in G$
- Inverses: for all $a \in G$, there is an element a^{-1} such that $a*a^{-1} = e$
- Associativity: $a*(b*c) = (a*b)*c$ for all $a,b,c \in G$

Which of the following form groups? Justify your answer

- **All integers under subtraction**
- **{1, 10} under multiplication modulo 11**
- **All irrational numbers under multiplication**

Many of the structures investigated in mathematics turn out to be groups. These include familiar number systems, such as the integers, the rational numbers the real numbers, and the complex numbers under addition, as well as the non-zero rationals, reals, and complex numbers, under multiplication. Group theory allows for the properties of such structures to be investigated in a general settings so it has extensive applications in mathematics, science, and engineering. Group theory provides an important tool for studying symmetry and is useful in fields such as relativity, quantum mechanics, and particle physics. Furthermore, the ability to represent geometric transformations finds applications in chemistry, computer graphics, and other fields.

http://en.wikipedia.org/wiki/Latin_square
http://mathworld.wolfram.com/LatinSquare.html
http://www.cut-the-knot.org/arithmetic/latin.shtml
http://www.princeton.edu/~matalive/VirtualClassroom/v0.1/html/lab1/lab1_3.html

Sudoku Joke

Here is the ultimate sudoku variation—Binary Sudoku:

1	

And here is the solution:

0	1
1	0

There are 10 possible boards, each more exciting than the other (of course, that's the binary number 10).