Notions on groups

L. Chupin

Pôle de Mathématiques, INSA de Lyon

November 30, 2008

Summary

1. Definition and first properties

2. Some finite groups

Definition 1

A group is a set, G, together with an operation $\perp$ that combines any two elements a and b to form another element denoted $a \perp b$. To qualify as a group, the set and operation, $(G, \perp)$, must satisfy four requirements known as the group axioms:

1. For all a, b in G, the result of the operation $a \perp b$ is also in G;
2. For all a, b and c in G, the equation $(a \perp b) \perp c = a \perp (b \perp c)$ holds;
3. There exists an element e in G (called the identity element), such that for all elements a in G, the equation $e \perp a = a \perp e = a$ holds;
4. For each a in G, there exists an element b in G such that $a \perp b = b \perp a = e$, where e is the identity element.

Example 2

- The group of integers $\mathbb{Z}$ under addition, denoted $(\mathbb{Z}, +)$ is one of the most familiar groups. The integers, with the operation of multiplication instead of addition, $(\mathbb{Z}, \times)$ do not form a group.
- The set of non zero real numbers, $\mathbb{R}^*$ with the operation of multiplication $\times$, is a group.
- The set of rotations leaving unchanged an equilateral triangle $\{\mathrm{id}, \mathrm{r}_1, \mathrm{r}_2\}$ with the operation of composition $\circ$ is a group.

◇ The identity operation leaving everything unchanged is denoted id;

◇ Rotations of the triangle by 120° right and 240° right are denoted by r_1 and r_2 respectively.

Two important consequences of the group axioms are given by the following proposition:

PROPOSITION 1

Let $(G, \perp)$ *be a group.*

1. *There exists only one identity element.*
2. *For each a in G there exists only one inverse element.*

Proposition 1

Let $(G, \perp)$ be a group.

1. *There exists only one identity element.*
2. *For each a in G there exists only one inverse element.*

– Proof –

To prove the uniqueness of an identity element, suppose that e_1 and e_2 are two identity elements. Then

$$e_1 = e_1 \perp e_2 \quad \text{and} \quad e_2 = e_1 \perp e_2.$$

Consequently, $e_1 = e_2$ that implies the uniqueness of the inverse element (usually denoted by e).

Proposition 1

Let $(G, \perp)$ be a group.

1. *There exists only one identity element.*
2. *For each a in G there exists only one inverse element.*

– Proof –

To prove the uniqueness of an inverse element of a, suppose that a has two inverses, denoted b and c. Then

$$b = b \perp e = b \perp (a \perp c) = (b \perp a) \perp c = e \perp c = c.$$

Hence the two extremal terms b and c are connected by a chain of equalities, so they agree. In other words there is only one inverse element of a.

Summary

1 Definition and first properties

2 Some finite groups

Definition 3

A group is called finite if it has a finite number of elements.

Example 4

- The group $(\{\mathrm{id}, \mathrm{r}_1, \mathrm{r}_2\}, \circ)$ (discussed above) is a finite group with 3 elements.
- The group $(\mathbb{Z}, +)$ is not a finite group.

For finite group, we can draw the "group table" which lists the results of all operations possible.

Example 5

The set $\{1; -1\}$ whith the multiplication $\times$ is a group. Its table is given by

$\times$	1	-1
1		
-1		

Definition 3

A group is called finite if it has a finite number of elements.

Example 4

- The group $(\{\mathrm{id}, \mathrm{r}_1, \mathrm{r}_2\}, \circ)$ (discussed above) is a finite group with 3 elements.
- The group $(\mathbb{Z}, +)$ is not a finite group.

For finite group, we can draw the "group table" which lists the results of all operations possible.

Example 5

The set $\{1; -1\}$ whith the multiplication $\times$ is a group. Its table is given by

$\times$	1	-1
1		
-1		

Definition 3

A group is called finite if it has a finite number of elements.

Example 4

- The group $(\{\mathrm{id}, \mathrm{r}_1, \mathrm{r}_2\}, \circ)$ (discussed above) is a finite group with 3 elements.
- The group $(\mathbb{Z}, +)$ is not a finite group.

For finite group, we can draw the "group table" which lists the results of all operations possible.

Example 5

The set $\{1; -1\}$ whith the multiplication $\times$ is a group. Its table is given by

$\times$	1	-1
1	1	-1
-1	-1	1

Towards a classification

Mathematicians often strive for a complete classification (or list) of a mathematical notion. In the context of finite groups, this aim quickly leads to difficult and profound mathematics.

Moreover it is relatively easy to prove that there exists only one structure of group with 2 elements, or with 3 elements:

$\perp$	e	a
e		
a		

$\perp$	e	a	b
e			
a			
b			

Towards a classification

Mathematicians often strive for a complete classification (or list) of a mathematical notion. In the context of finite groups, this aim quickly leads to difficult and profound mathematics.

Moreover it is relatively easy to prove that there exists only one structure of group with 2 elements, or with 3 elements:

$\perp$	e	a
e	e	a
a	a	

$\perp$	e	a	b
e			
a			
b			

Towards a classification

Mathematicians often strive for a complete classification (or list) of a mathematical notion. In the context of finite groups, this aim quickly leads to difficult and profound mathematics.

Moreover it is relatively easy to prove that there exists only one structure of group with 2 elements, or with 3 elements:

$\perp$	e	a
e	e	a
a	a	e

$\perp$	e	a	b
e			
a			
b			

Towards a classification

Mathematicians often strive for a complete classification (or list) of a mathematical notion. In the context of finite groups, this aim quickly leads to difficult and profound mathematics.

Moreover it is relatively easy to prove that there exists only one structure of group with 2 elements, or with 3 elements:

$\perp$	e	a
e	e	a
a	a	e

$\perp$	e	a	b
e	e	a	b
a	a		
b	b		

Towards a classification

Mathematicians often strive for a complete classification (or list) of a mathematical notion. In the context of finite groups, this aim quickly leads to difficult and profound mathematics.

Moreover it is relatively easy to prove that there exists only one structure of group with 2 elements, or with 3 elements:

$\perp$	e	a
e	e	a
a	a	e

$\perp$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

They respectively correspond to $(\{1;-1\},\times)$ and $(\{\mathrm{id},\mathrm{r}_1,\mathrm{r}_2\},\circ)$.

Exercise

Let $(G, \perp)$ be a group with 4 elements. We denote by e its identity element.

1. Draw its table in the case where $a \perp a = e$ for any a in G.
2. In the other case, assume that there exists an element a in G such that $a \perp a \neq e$.
   a) Show that e, a and $a \perp a$ are three different elements.
   b) Draw the table of such a group.
3. Consider the two following groups

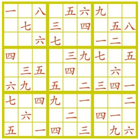
$$G_1 = \{\mathrm{id}, \mathrm{r}_a, \mathrm{r}_b, \mathrm{r}_c\} \quad \text{and} \quad G_2 = \{\mathrm{id}, \mathrm{s}_a, \mathrm{s}_b, \mathrm{s}_c\},$$

   endowed with the composition law $\circ$,
   where r_a, r_b and r_c respectively correspond to rotations of the square by 90° right, 180° right, and 270° right,
   and where s_a, s_b, s_c respectively correspond to reflections with respect to the two diagonals of the square, and with respect to the center of the square.
   a) Evaluate $r_a \circ r_a$ and $s_a \circ s_a$.
   b) Give the table of these two groups.

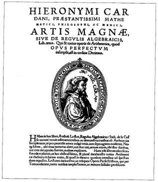
Examples of applications

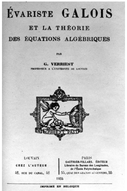
- Cryptography, combinatorics...

- Games : Sudoku, RubiXcub...



- Polynomial resolutions: $\mathcal{P}(X) = 0$





• • •