Some slides for 7th Lecture, Algebra

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

26-09-2011

A composition on a set G is a map

$$\begin{array}{rcl} \circ : G \times G & \rightarrow & G \\ (g,h) & \mapsto & \circ(g,h) = g \circ h = gh \end{array}$$

A pair $(G, \circ)$ consisting of a set G and a composition $\circ : G \times G \rightarrow G$ is a group if it satisfies:

1. The composition is associative: for every $s_1, s_2, s_3 \in G$

$$s_1 \circ (s_2 \circ s_3) = (s_1 \circ s_2) \circ s_3$$

2. There is a neutral element $e \in G$: for every $s \in G$

$$e \circ s = s \circ e = s$$

3. For every $s \in G$ there is an inverse element $t \in G$ such that

$$s \circ t = t \circ s = e$$

A pair $(G, \circ)$ consisting of a set G and a composition $\circ : G \times G \to G$ is a group if it satisfies:

1. The composition is associative: for every $s_1, s_2, s_3 \in G$, $s_1 \circ (s_2 \circ s_3) = (s_1 \circ s_2) \circ s_3$.
2. There is a neutral element $e \in G$: for every $s \in G$, $e \circ s = s \circ e = s$.
3. For every $s \in G$ there is an inverse element $t \in G$ such that $s \circ t = t \circ s = e$.

A group is called abelian or commutative if for every $g, h \in G$:

$$g \circ h = h \circ g$$

The number of elements $\mid G \mid = \#G$ in G is called the order of G.

Examples

- For $a, n \in \mathbb{Z}$ consider:

$$a + n\mathbb{Z} = \{a + nx : n \in \mathbb{Z}\}$$

- When is $a + n\mathbb{Z} = b + m\mathbb{Z}$?

Proposition 2.1.2

Let $a, b, c \in \mathbb{Z}$. Then $a + c\mathbb{Z} = b + c\mathbb{Z}$ if and only if $a \equiv b (\mathrm{mod}\ c)$.
Also, $(a + c\mathbb{Z}) \cap (b + c\mathbb{Z}) = \emptyset$ if and if $a \not\equiv b (\mathrm{mod}\ c)$.

$a + c\mathbb{Z} = b + c\mathbb{Z} \Rightarrow a \equiv b \pmod{c}$.

- Let $m \in a + c\mathbb{Z} = b + c\mathbb{Z}$.
- Then exists $x, y \in \mathbb{Z}$ s.t. $m = a + cx = b + cy$
- Hence $a - b = c(y - x) \Rightarrow a \equiv b \pmod{c}$

$a \equiv b \pmod{c} \Rightarrow a + c\mathbb{Z} = b + c\mathbb{Z}$.

- $a = b + cx$, for $x \in \mathbb{Z}$
- Then $a + c\mathbb{Z} = b + cx + c\mathbb{Z} = b + c\mathbb{Z}$, since $cx + c\mathbb{Z} = c\mathbb{Z}$

$(a + c\mathbb{Z}) \cap (b + c\mathbb{Z}) \neq \emptyset \Rightarrow a \equiv b \pmod{c}$

- There is $m, x, y \in \mathbb{Z}$ such that $m = a + cx = b + cy$
- $a - b = c(y - x)$, then $a \equiv b \pmod{c}$

- By previous proposition $a + c\mathbb{Z} = b + c\mathbb{Z}$ if and only if $a \equiv b \pmod{c}$.
- But $a + c\mathbb{Z} = b + c\mathbb{Z}$ if and only if $[a]_c = [b]_c$.

So we can have more notation:

- Denote by $[x] = x + c\mathbb{Z}$.
- Denote by $\mathbb{Z}/c\mathbb{Z} = \{[0], [1], \ldots, [c-1]\}$

We have a set $\mathbb{Z}/c\mathbb{Z}$, can we define a composition on it to get a group?

For $[x], [y] \in \mathbb{Z}/c\mathbb{Z}$

$$[x] + [y] = [x + y]$$

- Is this composition well defined?

$(\mathbb{Z}/c\mathbb{Z}, +)$ is an abelian group:

- Associativity: holds using the associativity of $(\mathbb{Z}, +)$
- Neutral element: subset $[0] = 0\mathbb{Z} = c\mathbb{Z}$
- The inverse element of $[x]$ is $[-x]$
- Abelian: $[x] + [y] = [x + y] = [y + x] = [y] + [x]$

What is $(\mathbb{Z}/0\mathbb{Z}, +)$?
What is $x + 0\mathbb{Z}$?

Composition table for a finite group

Associativity in $(G, \circ)$

What is $g_1 \circ g_2 \circ g_3$?, for $g_1, g_2, g_3 \in G$

Easy case: (set of maps from a set X to itself, composition of maps)

A non-abelian group

- $X = \{1, 2, 3\}$
- G bijective maps $X \to X$.
- Composition: composition of maps

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$\circ$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	f	d	c	b
b	b	d	e	f	a	c
c	c	f	d	e	b	a
d	d	b	c	a	f	e
f	f	c	a	b	e	d

- The neutral element is unique:

$$e = ee' = e'$$

- For $g \in G$ there is only one inverse: $gh = hg = h'g = gh' = e$, we have

$$h' = eh' = (hg)h' = h(gh') = he = h$$

Let g be an element of a group. We denote by g^{-1} the unique inverse of g.

Inverse in a non-commutative group: $(ab)^{-1} = b^{-1}a^{-1}$:

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a(ea^{-1}) = aa^{-1} = e$$

Multiplication by $g \in G$ is bijective