# Some slides for 8th Lecture, Algebra 1

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

28-09-2011

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 $s \in G$, $e \circ s = s \circ e = e$.
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 $G$.

A subgroup of a group $G$ is a non-empty subset $H \subset G$ such that the composition of $G$ makes it into a group. That is $H$ is a subgroup of $G$ if and only if

1. $e \in H$
2. $x^{-1} \in H$ for every $x \in H$
3. $xy \in H$, for every $x, y \in H$

In $S_3$: $\{e, a\}$ and $\{e, f, d\}$ are subgroups. How do we see it?

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

$(\mathbb{Z}, +)$ is a group. Application of division with remainder:

**Proposition 2.2.3**

Let $H$ be a subgroup of $(\mathbb{Z}, +)$. Then

$$H = d\mathbb{Z} = \{dn : n \in \mathbb{Z}\}$$

for a unique number $d \in \mathbb{N}$.

- If $H = \{0\}$, then set $d = 0$.

Proof $d\mathbb{Z} \subset H$:

- For $H \neq \{0\}$, $\mathbb{N} \cap H$ contains a smallest number $d > 0$
- Then, $-d \in H$
- Also, $d + \cdots + d \in H$ and $(-d) + \cdots + (-d) \in H$

Proof $H \subset d\mathbb{Z}$:

- Let $m \in H$, division: $m = qd + r$, with $0 \leq r < d$
- $m, d \in H \Rightarrow -qd \in H$ and $r = m - qd \in H$
- But $d$ was the first element, then $r = 0$ and $m = qd$

Let $H$ be a subgroup of $G$ and $g \in G$. Then the subset

$$gH = \{gh : h \in H\} \subset G$$

is called a left coset of $H$.
The subset

$$Hg = \{hg : h \in H\} \subset G$$

is called a right coset of $H$.
(coset=sideklasse)

Notation:

- $G/H$: The set of left cosets of $H$
- $H\backslash G$: The set of right cosets of $H$

## Lemma 2.2.6

Let $H$ be a subgroup of a group $G$ and let $x, y \in G$. Then

1. $x \in xH$
2. $xH = yH \Leftrightarrow x^{-1}y \in H$
3. If $xH \neq yH$ then $xH \cap yH = \emptyset$
4. The map $\varphi : H \to xH$ given by $\varphi(h) = xh$ is bijective.

Proof (1):

- $x = xe$ ($e \in H$), hence $x \in xH$

Proof (2):

- If $xH = yH$ then $xh = ye = y$ for some $h \in H$. Then $x^{-1}y = h \in H$.
- If $x^{-1}y = h \in H$ then $y = xh$. Then, $yH \subset xH$.
- Since $x = yh^{-1}$ we get $xH \subset yH$.

Proof (3): If $xH \neq yH$ then $xH \cap yH = \emptyset$

- Let $z \in xH \cap yH$, then $z = xh_1 = yh_2$ for some $h_1, h_2 \in H$.
- Then, $x^{-1}y \in H$ and $xH = yH$ by (2).

Proof (4): The map $\varphi : H \to xH$ given by $\varphi(h) = xh$ is bijective.

- $\varphi$ is multiplication by $x$, then it is bijective.
- It is just the restriction to $H$

## Corollary 2.2.7

Let $H$ be a subgroup of $G$. Then

$$G = \bigcup_{g \in G} gH,$$

and if $g_1 H \neq g_2 H$ then $g_1 H \cap g_2 H = \emptyset$.

Proof:
Think in (1) and (3) of previous lemma:

- $x \in xH$
- If $xH \neq yH$ then $xH \cap yH = \emptyset$

## Theorem 2.2.8 Lagrange

If $H \subset G$ is a subgroup of a finite group $G$ then

$$|G| = |G/H||H|$$

The order of a subgroup divides the order of the group

Proof:

- Let $gH$ be a coset in $G/H$.
- We know that there is a bijection between $gH$ and $H$. Then $|gH| = |H|$.
- $G$ is disjoint union of cosets, hence $|G|$ is equal to the number of cosets times $|H|$

The number of cosets $|G/H|$ is called the index of $H$ in $G$ and denoted by $[G : H]$.