Some slides for 10th Lecture, Algebra 1

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

9-10-2011

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 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 $x, y \in H$

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)

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

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

- Can we make G/H into a group?
- For $X, Y \in G$, Define the composition of subsets: $XY = \{xy; x \in X, y \in Y\}$
- Let G be the symmetric group and $H = \{e, a\}$. Compute $(bH)(cH)$. What does it mean?

$\circ$	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

Proposition 2.3.1

Let H be a subgroup of a group G. If $gH = Hg$ for every $g \in G$ then

$$(xH)(yH) = (xy)H,$$

for every $x, y \in G$.

Proof $(xH)(yH) \supset (xy)H$: (we do not need proposition hypothesis)

- Let $(xy)h \in (xy)H$.
- Then $(xy)h = (xe)(yh) \in (xH)(yH)$

Proof $(xH)(yH) \subset (xy)H$:

- Let $(xh_1)(yh_2) \in (xH)(yH)$
- Then, $(xh_1)(yh_2) = x((h_1 y)h_2)) = ??$

Proposition 2.3.1

Let H be a subgroup of a group G. If $gH = Hg$ for every $g \in G$ then
$$(xH)(yH) = (xy)H,$$
for every $x, y \in G$.

Proof: $(xH)(yH) \supset (xy)H$ (we do not need proposition hypothesis)

- Let $(xy)h \in (xy)H$.
- Then $(xy)h = (xe)(yh) \in (xH)(yH)$

Proof: $(xH)(yH) \subset (xy)H$

- Let $(xh_1)(yh_2) \in (xH)(yH)$
- Then, $(xh_1)(yh_2) = x((h_1y)h_2)) = x((yh_3)h_2) = (xy)(h_3h_2)$ for some $h_3 \in H$ since $Hy = yH$.

A subgroup N of group G is called normal if

$$gNg^{-1} = \{gng^{-1} : n \in N\} = N,$$

for every $g \in G$.

Exercise 13: A normal subgroup N of G satisfies $gN = Ng$ for every $g \in G$. So we have two equivalent conditions for normality

Corollary 2.3.3

Let N be a normal subgroup of the group G. Then the composition of subsets makes G/N into a group and

$$(g_1N)(g_2N) = (g_1g_2)N,$$

for $g_1N, g_2N \in G/N$.

Corollary 2.3.3

Let N be a normal subgroup of the group G. Then the composition of subsets makes G/N into a group and

$$(g_1 N)(g_2 N) = (g_1 g_2)N,$$

for $g_1 N, g_n \in G/N$.

Proof:

- Proposition 2.3.1 $\Rightarrow (g_1 N)(g_2 N) = (g_1 g_2)N$
- Composition of subsets is associative
- Neutral element: $eN = N$
- Inverse element: $(gN)^{-1} = g^{-1}N$

Let N be a normal subgroup of G. The group G/N is called a quotient group.

Exercise 2.14: A subgroup of an abelian group is normal.

Exercise 2.17: Consider a group G such that every subgroup in it is normal. Is G abelian?

Lemma 2.3.6

Let H and K, where H is normal, be subgroups of a group. Then HK is a subgroup of G.

Proof:

- $e \in HK$
- $x \in H, y \in K$: $(xy)^{-1} = (y^{-1}x^{-1}y)y^{-1} \in HK$
- $x, x' \in H, y, y' \in K$: $(xy)(x'y') = (x(yx'y^{-1}))yy' \in HK$

Quotient group of the integers

Prime residue classes: $[a] = a + n\mathbb{Z}$ with $\gcd(a, n) = 1$.

Let $n > 0$.

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[a] \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$$

with $[a][b] = [ab]$ is a group of order $\varphi(n)$.

- $[a] = [b]$ and $\gcd(a, n) = 1 \Rightarrow \gcd(b, n) = 1$.
- $\gcd(a, n) = 1, \gcd(b, n) = 1 \Rightarrow \gcd(ab, n) = 1$.
- Neutral: $[1]$
- Inverse?: using extended Euclidean algorithm.
  $\lambda a + \mu n = 1 \Rightarrow [1] = [\lambda a + \mu n] = [\lambda a]$