Some slides for 8th Lecture, Algebra

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

7-10-2010

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?

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 of N of G satisfies $gN = Ng$ for every $g \in G$.

For $X, Y \in G$, Define the composition of subsets:

$$XY = \{xy; x \in X, y \in Y\}$$

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 $g_1N, g_n \in G/N$.

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

Let G and K be groups. A map $f : G \to K$ is called a group homomorphism if

$$f(xy) = f(x)f(y)$$

for every $x, y \in G$.

The kernel of a group homomorphism $f : G \to K$ is

$$\mathrm{Ker}(f) = \{g \in G : f(g) = e\}$$

The image of f is

$$f(G) = \{f(g) : g \in G\}$$

A bijective group homomorphism is called a group isomorphism.
We write $G \cong K$ and say G and K are isomorphic.

Proposition 2.4.9

Let $f : G \to K$ be a group homomorphism.

1. The image $f(G) \subset K$ is a subgroup of K
2. The kernel $\mathrm{Ker}(f) \subset G$ is a normal subgroup of G.
3. f is injective if and only if $\mathrm{Ker}(f) = \{e\}$

Proof: (1)

- $e \in f(G)$?: $f(e) = f(ee) = f(e)f(e) \Rightarrow f(e) = e$
- $f(x)^{-1} \in f(G)$?: Yes, $f(x)^{-1} = f(x^{-1})$. For $x \in G$,

$$e = f(e) = f(xx^{-1}) = f(x)f(x^{-1})$$

$$e = f(e) = f(x^{-1}x) = f(x^{-1})f(x)$$

- $f(x)f(y) \in f(G)$?: For $x, y \in G$, $f(x)f(y) = f(xy)$

Proof: (2), $\mathrm{Ker}(f)$ is a subgroup

- $e \in \mathrm{Ker}(f)$?: $f(e) = e$
- $x^{-1} \in \mathrm{Ker}(f)$?: For $x \in \mathrm{Ker}(f)$, $e = f(x) = f(x)^{-1} = f(x^{-1})$
- $xy \in \mathrm{Ker}(f)$?: For $x, y \in \mathrm{Ker}(f)$, $f(xy) = f(x)f(y) = ee = e$

Proof: (2), the subgroup $N = \mathrm{Ker}(f)$ is a normal subgroup. $N = gNg^{-1}, \forall g \in G$.

- $gNg^{-1} \subset N$: For $x \in N$, $f((gx)g^{-1}) = (f(g)f(x))f(g^{-1}) = f(g)f(g)^{-1} = e$.
- $gNg^{-1} \supset N$: Consider the previous statement for g^{-1}: $g^{-1}Ng \subset N$. Then $Ng \subset gN$ and $N \subset gNg^{-1}$.

Proof: (3) f is injective $\Leftrightarrow \mathrm{Ker}(f) = \{e\}$

- $\Rightarrow$): For f injective, $Ker(f) = e$ since $f(e) = e$.
- $\Leftarrow$): For $\mathrm{Ker}(f) = \{e\}$ and $f(x) = f(y)$,

$$e = f(y)^{-1} f(x) = f(y^{-1}) f(x) = f(y^{-1} x)$$

Then, $y^{-1}x \in \mathrm{Ker}(f)$, and therefore $y^{-1}x = e$ and $x = y$.

To think: The previous result tells us that the kernel of any homomorphism is a normal subgroup. Is the converse true?

Theorem 2.5.1-The isomorphism theorem

Let G and K be groups and $f : G \longrightarrow K$ a group homomorphism and $N = \mathrm{Ker}(f)$. Then

$$\begin{array}{rcl} \tilde{f} : G/N & \longrightarrow & f(G) \\ gN & \longmapsto & f(g) \end{array}$$

is a well defined map and a group isomorphism

How do we understand G/N? Finding a group K, a surjective morphism $f : G \longrightarrow K$ such that $N = \mathrm{Ker}(f)$

Theorem 2.5.1

Let G and K be groups and $f : G \to K$ a group homomorphism and $N = \mathrm{Ker}(f)$. Then

$$\begin{array}{rcl} \tilde{f} : G/N & \to & f(G) \\ gN & \mapsto & f(g) \end{array}$$

is a well defined map and a group isomorphism

Proof: well defined and injective. For $x, y \in G$:

- $f(x) = f(y) \Leftrightarrow$
- $f(y)^{-1} f(x) = e \Leftrightarrow$
- $f(y^{-1}) f(x) = e \Leftrightarrow$
- $f(y^{-1}x) = e \Leftrightarrow$
- $y^{-1}x \in N \Leftrightarrow$
- $xN = yN$

Theorem 2.5.1

Let G and K be groups and $f : G \to K$ a group homomorphism and $N = \mathrm{Ker}(f)$. Then

$$\begin{array}{rcl} \tilde{f} : G/N & \to & f(G) \\ gN & \mapsto & f(g) \end{array}$$

is a well defined map and a group isomorphism

Proof: $\tilde{f}$ is a group homorphism

$$\tilde{f}((g_1N)(g_2N)) = \tilde{f}((g_1g_2)N) = f(g_1g_2) = f(g_1)f(g_2) = \tilde{f}(g_1N)\tilde{f}(g_2N$$

Proof: $\tilde{f}$ is surjective
f is surjective onto $f(G)$

Examples

For $g \in G$:

- $g^0 = e$
- $g^n = g^{n-1} g$ for $n > 0$
- $g^n = (g^{-1})^{-n}$ for $n < 0$

Proposition 2.6.1

Let G be group and $g \in G$. The map

$$\begin{array}{rcl} f_g : \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & g^n \end{array}$$

is a group homomorphism from $(\mathbb{Z}, +)$ to G.

- Notation: $\langle g \rangle = f_g(\mathbb{Z}) = \{g^n : n \in \mathbb{Z}\}$
- Exercise 2.26: $\langle g \rangle$ is an abelian group
- $\mathrm{ord} = |\langle g \rangle|$ is called order of g

- Order of e?
- Order of a?
- Order of f?

$\circ$	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

Examples

$$\begin{array}{rcl} f_g : \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & g^n \end{array}$$

Proof Proposition 2.6.1: (f_g is a group homomorphism)
By definition of g^n, $n \in \mathbb{Z}$:

- $f_{g^{-1}}(-m) = f_g(m)$, for every $g \in G$, $m \in \mathbb{Z}$.
- $f_g(m+1) = f_g(m)f_g(1)$, for every $g \in G$, $m \geq 0$.
- $f_g(m-1) = f_g(m)f_g(-1)$, for every $g \in G$, $m \geq 0$

Hence,

- $f_g(m+1) = f_g(m)f_g(1)$ for every $g \in G$, $m \in \mathbb{Z}$
- $f_g(m+n) = f_g(m)f_g(n)$ for every $g \in G$, $m \in \mathbb{Z}$, $n \geq 0$
- If $n < 0$: $f_g(m+n) = f_{g^{-1}}(-m+(-n)) =$
  $f_{g^{-1}}(-m)f_{g^{-1}}(-n) = f_g(m)f_g(n)$

Proposition 2.6.3

Let G be a finite group and let $g \in G$.

1. $\mathrm{ord}(g)$ divides $|G|$
2. $g^{|G|} = e$
3. If $g^n = e$ for some $n > 0$ then $\mathrm{ord}(g)$ divides n

If $H \subset G$ is a subgroup of a finite group G then $|G| = [G:H]|H|$

$$\begin{array}{rcl} f_g : \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & g^n \end{array}$$

Proof: $\mathrm{ord}(g)$ divides $|G|$

- Let $H = \langle g \rangle$. Then $|H| = \mathrm{ord}(g)$.
- Apply Lagrange's theorem.

Proof: $g^{|G|} = e$

- $g^{|G|} = g^{\mathrm{ord}(g)[G:H]} = \left(g^{\mathrm{ord}(g)}\right)^{[G:H]} = e^{[G:H]} = e$

proof: If $g^n = e$ for some $n > 0$ then $\mathrm{ord}(g)$ divides n

- If $g^n = e$, $n \in \mathrm{Ker}(f_g) = \mathrm{ord}(g)\mathbb{Z}$
- Thus $\mathrm{ord}(g)|n$