Some slides for 16th Lecture, Algebra 1

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

30-10-2012

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

$$\begin{array}{rccc} f_g : \mathbb{Z} & \to & G \\ n & \mapsto & g^n \end{array}$$

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

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

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 $|G| = [G : H]|H|$

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

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

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

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

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

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

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

For $g \in G$, $\langle g \rangle = f_g(\mathbb{Z}) = \{g^n : n \in \mathbb{Z}\}$. Hence, $\langle g \rangle \subset G$

A cyclic group is a group G containing an element g such that $G = \langle g \rangle$.
Such a g is called a generator of G and we say that G is generated by g.

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

What is $Ker(f_g)$?
How are the subgroups of $(\mathbb{Z}, +)$?

Group isomorphism Theorem (Theorem 2.5.1):

$$\mathbb{Z}/n_g\mathbb{Z} \to \langle g \rangle = G$$

for some unique natural number $n_g \geq 0$.

Proposition 2.7.2

A group G of prime order $|G| = p$ is isomorphic to the cyclic group $\mathbb{Z}/p\mathbb{Z}$

Proof:

- Let $g \in G$ with $g \neq e$
- $H = f_b(\mathbb{Z}) \subset G$ and it has more than one element
- By Lagrange's Theorem, $|H|$ divides $p = |G|$
- Then $|H| = |G|$ and therefore $H = G$ (since $H \subset G$)
- Thus, $f_g : \mathbb{Z} \to G$ is a surjective morphism.
- $\ker(f_g) = p\mathbb{Z}$ ($\mathrm{ord}(p)$ divides $|G|$)
- Apply Theorem 2.5.1-Isomorphism theorem

Example

- $[a] = a + 12\mathbb{Z}$
- $\mathbb{Z}/12\mathbb{Z} = \{[0], [1], [2], \ldots, [10], [11]\}$

Table for $\mathrm{ord}([a])$:

[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]
1	12	6	4	3	12	2	12	3	4	6	12

- For a divisor d of 12. There is a unique subgroup of order d, the subgroup generated by $[12/d]$
- There are $\varphi(d)$ elements of order d (d divisor of 12)

d	0	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(d)$	0	1	1	2	2	4	2	6	4	6	4	10	4

Proposition 2.7.4

Let G be a cyclic group

- Every subgroup of G is cyclic
- Suppose that G is finite and that d is a divisor in $|G|$. Then G contains a unique subgroup H or order d.
- There are $\varphi(d)$ elements of order d in G. These are the generators of H.

Proof: Every subgroup of G is cyclic. If $|G|$ is infinite:

- Then $G \cong \mathbb{Z}$
- The subgroups of G are $d\mathbb{Z}$, with $d \in \mathbb{N}$. They are cyclic and generated by d.

Proof: Every subgroup of G is cyclic. If $|G| = N > 0$ is finite:

- Let $G = \{[0], [1], \ldots [N-1]\}$ and $H \subset G$ a subgroup
- If $H \neq \{0\}$ consider smallest $d > 0$, s.t. $[d] \in H$
- Euclid's trick: If $[n] \in H$ then $[n - qd] = [r] \in H$ for $n = qd + r$, $0 \leq r < d$.
- But, since d is minimal: $r = 0$ and $H = \langle [d] \rangle$

Proof: Suppose that G is finite and that d is a divisor in $|G|$. Then G contains a unique subgroup H or order d.

- Let $m = N/d$, then $[m]$ is an element of order d in G.
- If $[n]$ is another element of order d then $[dn] = [0]$
- Then $N|nd$ and $m|n$. That is, an element of order d is a multiple of $[m]$
- But by (1), subgroups are cyclic. Hence, $H = \langle [m] \rangle$ is the only subgroup of order d

Proof there are $\varphi(d)$ elements of order d in G. These are the generators of H:

- H unique subgroup of order d, the elements of order d in G must be in one-to-one correspondence with the generators of H.
- $H = \{[0], [1], \ldots, [d-1]\}$ since $H \cong \mathbb{Z}/d\mathbb{Z}$

The $\varphi(d)$ elements of order d in $\mathbb{Z}/N\mathbb{Z}$ are

$$\{[k\frac{N}{d}] : 0 \leq k < d, \gcd(k, d) = 1\}$$