Some slides for 15th (and 16th) Lecture, Algebra 1

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

9-11-2011

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

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

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 $\operatorname{ord}([a])$:

[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

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

Corollary 2.7.6

Let N be a positive integer. Then

$$\sum_{d|N} \varphi(d) = N,$$

(the sum is over the divisors of N)

Proof:

- Let G be the cyclic group $\mathbb{Z}/N\mathbb{Z}$.
- $$N = \sum_{g\in G} 1 = \sum_{d|N} \sum_{g\in G, \mathrm{ord}(g)=d} 1 \overbrace{=}^{Prop.\ 2.7.4(3)} \sum_{d|N} \varphi(d)$$

Revisiting Euler's theorem proof

Theorem 1.7.2 (Euler)

Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ relative prime. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Proof:

- List the numbers (lower than n) relative prime to n:

$$0 < a_1 < \cdots < a_{\varphi(n)} < n$$

Claim: $\{[aa_1]_n, \ldots, [aa_{\varphi(n)}]_n\} = \{a_1, \ldots, a_{\varphi(n)}\}$

- $[aa_i]_n = [aa_j]_n \Rightarrow n \mid a(a_i - a_j) \Rightarrow n \mid (a_i - a_j) \Rightarrow i = j$.
- $\gcd(n, aa_i) = 1 \Rightarrow \gcd(n, [aa_i]_n) = 1$

Revisiting Euler's theorem proof

- Hence $[aa_1]_n \cdots [aa_{\varphi(n)}]_n = a_1 \cdots a_{\varphi(n)}$
- Then $aa_1 \cdots aa_{\varphi(n)} \equiv a_1 \cdots a_{\varphi(n)} \pmod{n}$, but $aa_1 \cdots aa_{\varphi(n)} = a^{\varphi(n)} a_1 \cdots a_{\varphi(n)}$.
- That is, $n \mid a_1 \cdots a_{\varphi(n)}(a^{\varphi(n)} - 1)$.
- By corollary 1.5.10, $n \mid (a^{\varphi(n)} - 1)$.
- That is, $a^{\varphi(n)} \equiv 1 \pmod{n}$

New proof for Euler's theorem

Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ relative prime. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Proof:

- Consider $G = (\mathbb{Z}/n\mathbb{Z})^*$ with order $\varphi(n)$
- Since $gcd(a, n) = 1$, $[a] \in G$
- Prop. 2.6.3 (2) is $g^{|G|} = e$, hence:

$$[a]^{|G|} = [a]^{\varphi(n)} = [1]$$

- Hence, $a^{\varphi(n)} \equiv 1 \pmod{n}$

Revisiting Chinese reamainder theorem

Theorem 1.6.4-The Chinese remainder theorem

Let $N = n_1 \cdots n_t$, with $n_1, \dots, n_t \in \mathbb{Z} \setminus \{0\}$ and $\gcd(n_i, n_j) = 1$, for $i \neq j$. Consider the system

$$\begin{cases} X \equiv a_1 \pmod{n_1} \\ X \equiv a_2 \pmod{n_2} \\ \quad \vdots \\ X \equiv a_t \pmod{n_t} \end{cases}$$

With $a_i \in \mathbb{Z}$. Then

1. The system has a solution $X \in \mathbb{Z}$.
2. If $X, Y \in \mathbb{Z}$ are solutions of the system then $X \equiv Y \pmod{N}$. If X is a solution of the system and $X \equiv Y \pmod{N}$ then Y is a solution of the system.

Revisiting the remainder map

Suppose that $N = n_1 \cdots n_t$, where $n_1, \ldots, n_t \in \mathbb{N} \setminus \{0\}$ and $\gcd(n_i, n_j) = 1$ if $i \neq j$. Then the remainder map

$$r : \mathbb{Z}/N :\to \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t$$

is bijective

We should define the product of groups to extend the Chinese remainder theorem:

If $G_1, G_2, \ldots, G_n$ are groups then the product

$$G = G_1 \times \cdots \times G_n = \{(g_1, \ldots, g_n) : g_i \in G_i \forall i\}$$

has the natural composition

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

G is a group called product group:

- Associative: because each component is associative
- Neutral element: $(e_1, \ldots, e_n)$
- Inverse $g = (g_1, \ldots, g_n)$: $g^{-1} = (g_1^{-1}, \ldots, g_n^{-1})$.

If we have group homomorphisms $\varphi : H \to G_i$, for $i = 1, \ldots, n$. We have a group homomorphism:

$$\begin{array}{rcl} \varphi : H & \to & G = G_1 \times \cdots \times G_n \\ g & \mapsto & (\varphi_1(g), \ldots, \varphi_n(g)) \end{array}$$

Lemma 2.8.1

Let M, N be normal subgroups of a group G with $M \cap N = \{e\}$. Then MN is a subgroup of G and

$$\begin{array}{rcl} \pi : M \times N & \rightarrow & MN \\ (x, y) & \mapsto & xy \end{array}$$

is an isomorphism.

Proof: By lemma 2.3.6, MN is a subgroup.

Lemma 2.3.6

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

Lemma 2.8.1

Let M, N be normal subgroups of a group G with $M \cap N = \{e\}$. Then MN is a subgroup of G and

$$\begin{array}{rcl} \pi : M \times N & \to & MN \\ (x, y) & \mapsto & xy \end{array}$$

is an isomorphism.

Proof: π homomorphism. $(xy)(x'y') = (xx')(yy')$?

- $(xy)(x'y') = (xx')(x'^{-1}yx'y^{-1})(yy')$
- But $x'^{-1}yx'y^{-1} \in M \cap N = \{e\}$, since M, N are normal.

Proof: π isomorphism

- $\pi(M \times N) = MN$, it is surjective
- $\ker(\pi) \cong M \cap N = \{e\}$
- Apply ismorphism theorem

Proposition 2.8.2-Group version of Chinese remainder theorem

Let $n_1, \dots, n_r \in \mathbb{Z}$ be pairwise relative prime integers and let $N = n_1 \cdots n_r$. If φ_i denotes the canonical group homomorphism

$$\begin{array}{rcl} \pi_{n_i\mathbb{Z}} : \mathbb{Z} & \to & \mathbb{Z}/n_i\mathbb{Z} \\ x & \mapsto & [x] \end{array}$$

then the map

$$\begin{array}{rcl} \tilde{\varphi} : \mathbb{Z}/N\mathbb{Z} & \to & \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \\ x + N\mathbb{Z} & \mapsto & (\varphi_1(x), \dots, \varphi_r(x)) \end{array}$$

is a group isomomorphism.

Proof:

- We know φ is a group homomorphism. Why?

$$\begin{array}{rcl}\varphi : \mathbb{Z} & \to & \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \\ x & \mapsto & (\varphi_1(x), \ldots, \varphi_r(x))\end{array}$$

- If $n \in \ker(\varphi)$, then $n_1|n, \ldots, n_r|n$.
- Since $n_1, \ldots, n_r$ are relative prime, $N = n_1 \cdots n_r|n$. So $\ker(\varphi) \subset N\mathbb{Z}$
- It is clear that $N\mathbb{Z} \subset \ker(\varphi)$ (is it?). Hence, $\ker(\varphi) = N\mathbb{Z}$
- By isomorphism theorem and since the map is surjective (why?), we have that $\tilde{\varphi}$ is an isomorphism

$$\begin{array}{rcl}\tilde{\varphi} : \mathbb{Z}/N\mathbb{Z} & \to & \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \\ x + N\mathbb{Z} & \mapsto & (\varphi_1(x), \ldots, \varphi_r(x))\end{array}$$

(it is surjective because $\mathbb{Z}/N\mathbb{Z}$ and $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ have the same order)

Let's think about cyclic groups and this theorem

To remember it:

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.

For $n_1, \dots, n_r \in \mathbb{Z}$ pairwise relative prime integers and $N = n_1 \cdots n_r$. We have

$$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

is a cyclic group isomorphic to $\mathbb{Z}/N\mathbb{Z}$.