Some slides for 18th Lecture, Algebra 1

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

6-11-2012

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 $\mathbb{Z}/N\mathbb{Z}$.
-

$$N = \sum_{g \in G} 1 = \sum_{d|N} \sum_{g \in G, \mathrm{ord}(g) = d} 1 \overbrace{=}^{\textit{Prop. } 2.7.4(3)} \sum_{d|N} \varphi(d)$$

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 $n_1, \ldots, n_t \in \mathbb{Z} \setminus \{0\}$ 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

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

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

$$\begin{aligned} \pi_{n_i\mathbb{Z}} : \mathbb{Z} &\rightarrow \mathbb{Z}/n_i\mathbb{Z} \\ x &\mapsto [x] \end{aligned}$$

then the map

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

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 $n_1, \ldots, n_r \in \mathbb{Z}$ 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 $\mathbb{Z}/N\mathbb{Z}$.