Some slides for 17th Lecture, Algebra 1

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

1-11-2012

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

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

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

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
- $\mathrm{Ker}(\pi) \cong M \cap N = \{e\}$
- 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

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

then the map

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

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 $n \in \mathrm{Ker}(\varphi)$, 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 $\mathrm{Ker}(\varphi) \subset N\mathbb{Z}$
- It is clear that $N\mathbb{Z} \subset \mathrm{Ker}(\varphi)$ (is it?). Hence, $\mathrm{Ker}(\varphi) = N\mathbb{Z}$
- 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 $\mathbb{Z}/N\mathbb{Z}$.

- $X = \{1, 2, 3\}$
- G bijective maps $X \to X$.
- Composition: composition of maps

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

For instance:

$$\begin{array}{rcl} c : \{1,2,3\} & \to & \{1,2,3\} \\ 1 & \mapsto & 3 \\ 2 & \mapsto & 2 \\ 3 & \mapsto & 1 \end{array}$$

- The same construction makes sense for a set with n elements. For instance $M_n = \{1, \ldots, n\}$.
- We have S_n: bijective maps $M_n \to M_n$.
- S_n is a group with the composition of maps and order $|S_n| = n!$
- $\sigma \in S_n$ is a bijection and denoted by

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

We know that S_3 is not abelian. Easily we see that S_n is not abelian. However: Are there some permutations in S_n that commute?, that is

$$\sigma\tau = \tau\sigma$$

Let $\sigma \in S_n$. We define M_σ

$$M_\sigma = \{x \in M_n : \sigma(x) \neq x\}$$

We say that $\sigma, \tau \in S_n$ are disjoint if $M_\sigma \cap M_\tau = \emptyset$.

Proposition 2.9.2

Let $\sigma, \tau \in S_n$ be disjoint permutations in S_n. Then $\sigma\tau = \tau\sigma$

Proof:

- We shall see that $\sigma(\tau(x)) = \tau(\sigma(x))$, for all $x \in M_n$.
- If $x \notin M_\sigma \cup M_\tau$, then $\sigma(x) = x$ and $\tau(x) = x$, so the equality holds.
- If $x \in M_\sigma$, then $\sigma(x) \neq x$ but $\sigma(x) \in M_\sigma$ (because $\sigma(x)$ cannot be invariant by σ).
- Hence, $\tau(\sigma(x)) = \sigma(x)$ and $\sigma(\tau(x)) = \sigma(x)$.
- Do the same for $x \in M_\tau$

A **k-cycle** is a permutation $\sigma \in S_n$ such that for k (different) elements $x_1, \dots, x_k \in M_n$,

$$\sigma(x_1) = x_2, \;\; \sigma(x_2) = x_3, \;\; , \dots \sigma(x_{k-1}) = x_k, \;\; \sigma(x_k) = x_1$$

and $\sigma(x) = x$ if $x \notin \{x_1, \dots, x_k\}$.

We denote it by $\sigma = (x_1 x_2 \dots x_k)$

The k-cycle σ can be represented in k ways:

$$\begin{array}{c} (x_1 x_2 \dots x_{k-1} x_k), \\ (x_2 x_3 \dots x_k x_1), \\ \vdots \\ (x_k x_1 \dots x_{k-2} x_{k-1}) \end{array}$$

- What is M_σ?
- What is the order of a k-cycle in S_n?

- 1-cycle: identity map
- 2-cycle: trasposition. σ transposition: σ^{-1}?
- Simple trasposition: a transposition $s_i = (i \;\; i+1)$

Proposition 2.9.5

Let $\sigma \in S_n$ be written as a product of disjoint cycles $\sigma_1 \cdots \sigma_r$. Then the order of σ is the least common multiple of the orders of the cycles $\sigma_1, \ldots, \sigma_r$

Proof:

- $\sigma^n = \sigma_1^n \cdots \sigma_r^n$
- Then if $\sigma^n = e$, then n is divisible by order of the cycles (prop 2.6.3)
- Hence $m = \mathrm{lcm}(\mathrm{ord}(\sigma_1), \ldots, \mathrm{ord}(\sigma_r)) \leq \mathrm{ord}(\sigma)$
- But $\sigma_i^m = e$ for every i and the result holds.

Proposition 2.9.6

Every permutation $\sigma \in S_n$ is a product of unique disjoint cycles.

Proof existence, by induction on $|M_\sigma|$:

- If $|M_\sigma| = 0$, then σ is the identity map and it is the product of disjoint 1-cycles
- Assume that $|M_\sigma| \geq 0$. Pick $x \in M_\sigma$. Then $x \neq \sigma(x)$.
- Consider $x, \sigma(x), \sigma^2(x), \ldots$ and stop when you find a repeated element
- The repeated element should be equal to x (if $\sigma^N(x) = \sigma^n(x) \Rightarrow \sigma^{N-n} = x$). Define the cycle $\tau = (x_1 \ldots x_k)$ by
  $x_1 = x, \;\; x_2 = \sigma(x_1), \ldots, x_k = \sigma(x_{k-1}), \;\; x_1 = \sigma(x_k)$
- $M_{\sigma\tau^{-1}} = M_\sigma \setminus \{x_1, \ldots, x_k\}$
- Apply induction hypothesis to $\sigma\tau^{-1}$, so $\sigma\tau^{-1} = \tau_1 \ldots \tau_r$ product of disjoint cycles
- Then $\sigma = \tau_1 \ldots \tau_r \tau$ and since τ is disjoint from $\tau_1, \ldots, \tau_r$ the result holds

Proof uniqueness:

- Let $\sigma = \sigma_1 \ldots \sigma_r$ product of disjoint cycles
- Then $M_\sigma = M_{\sigma_1} \cup \ldots \cup M_{\sigma_r}$ and $M_{\sigma_i} \cap M_{\sigma_j} = \emptyset$ for $i \neq j$.
- Thus, if $x \in M_\sigma$ it only belongs to a unique M_{σ_j} and then $\sigma_j = (x\sigma(x)\ldots)$ (by the previous proof). So the cycles are unique.

Lemma 2.9.8

Suppose that $\tau = (i_1 i_2 \dots i_k)$ is a k-cycle and σ a permutation in S_n. Then

$$\sigma(i_1 i_2 \dots i_k)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\dots\sigma(i_k))$$

Proof:

- Let $J = \{\sigma(i_1), \dots, \sigma(i_k)\}$
- Check both sides of the equality give the same values for $i \in J$
- Both sides of the equality are the identity map for $i \notin J$

Bubble sort