12/3/2018

Ορισμός: Τάξη ενός στοιχείου $a \in G$ λέγεται ο μικρότερος φυσικός αριθμός n (αν υπάρχει), τέτοιος ώστε:

$$a^n = 1,$$

και συμβολίζουμε $ord(a) = n$. Αν δεν υπάρχει τέτοιος φυσικός αριθμός, λέμε ότι το a έχει άπειρη τάξη. $(ord(a) = \infty)$

Παραδείγματα: • Το $[5]_8 \in U(\mathbb{Z}_8)$ έχει:

$ord([5]_8) = 2$, καθώς $([5]_8)^2 = [25]_8 = [1]_8$

• Το $[4]_8 \in \mathbb{Z}_8$ έχει:

$ord([4]_8) = 2$, καθώς $[4]_8^2 = 2 \cdot [4]_8 = [8]_8 = [0]_8$ (e_8)

• Το $7 \in \mathbb{Z}$, έχει, προφανώς: $ord(7) = \infty$

Θεώρημα: Έστω $a \in G$ και $a^n = 1 \Longrightarrow ord(a) \mid n$

Παρατήρηση: Έστω $a \in G$ και $ord(a) = n$

Έχω: $1, a, a^2, a^3, \ldots, a^{n-2}, a^{n-1}$

$1 = a^n$, $a = a^{n+1}$, $a^2 = a^{n+2}$, $a^3 = a^{n+3}$

• Τα στοιχεία $1, a, \dots, a^{n-1}$ είναι διαφορετικά μεταξύ τους.

↳ Έστω: $1, a, a^2, \dots \boxed{a^i}, \dots \boxed{a^j}, \dots, a^{n-1}$, με $0 \le i < j \le n-1$

• Έχω: $a^i = a^j \Rightarrow a^{i-1} = a^{j-1} \Rightarrow$

$\Rightarrow \boxed{1 = a^{j-i}}$, με $1 \le j-i \le j \le n$

↳ Άτοπο, καθώς $\boxed{\text{ord}(a) = n}$.

Πρόταση Έστω $a \in G$. Τότε η τάξη του a ισούται με την τάξη της υποομάδας $\langle a \rangle$, που παράγεται από το a. Δηλαδή:

$$\boxed{\text{ord}(a) = |\langle a \rangle|}$$ ← Πλήθος στοιχείων της ομάδας $\langle a \rangle$

Θεώρημα Αν $\text{ord}(a) = n$, τότε:

$$\boxed{\text{ord}(a^s) = \frac{n}{(s,n)}}$$

• Απόδειξη: Έστω: $\text{ord}(a^s) = m$. Έχω ότι:

$$(a^s)^{n/(s,n)} = a^{\frac{s \cdot n}{(s,n)}} = (a^n)^{s/(s,n)} \xrightarrow{\text{ord}(a)=n,\ a^n = 1} 1$$

• Συνεπώς, $\text{ord}(a^s) \mid n/(s,n) \Rightarrow \boxed{m \mid n/(s,n)}$

• Έστω : $\text{ord}(\alpha^s) = u \Longrightarrow (\alpha^s)^u = 1 \Rightarrow$

$\Rightarrow \alpha^{s \cdot u} = 1 \xrightarrow{\text{ord}(\alpha)=u} u \mid s \cdot u \Rightarrow$

$\Rightarrow \boxed{\frac{u}{(s,u)} \mid \frac{s}{(s,u)} \cdot u}$ (1)

• Προφανώς, $\left(\frac{u}{(s,u)}, \frac{s}{(s,u)}\right) = 1$

• Άρα, από (1): $\boxed{\frac{u}{(s,u)} \mid u}$ (Άρα $\frac{u}{(s,u)}$ και $\frac{s}{(s,u)}$ είναι πρώτοι μεταξύ τους)

▶ Παράδειγμα $U(Z_7) = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$

• Προφανώς: $\boxed{\text{ord}([3]_7) = 6}$, διότι:

$\rightarrow [3^6]_7 = [3^3]_7 \cdot [3^3]_7 = [-1]_7 \cdot [-1]_7 = \boxed{[1]_7}$

• Άρα: $\boxed{|\langle 3 \rangle| = 6}$

• Από, αυτό έπεται ότι το $[3]_7$ είναι γεννήτορας της $U(Z_7)$, καθώς παράγει όλα τα στοιχεία της!

• Προφανώς, η $U(Z_7)$ είναι κυκλική ομάδα, διότι:

$$\boxed{U(Z_7) = \langle 3 \rangle}$$

⚠ Έστω $[b]_4$ γεννήτορας της ομάδας $U(Z_7)$.

Συνεπώς: $\boxed{\text{ord}([b]_4) = 6}$ και $\boxed{[b] = [3^k]_7}$ $\Bigg\} \Longrightarrow$

$\Longrightarrow \text{ord}([3]^k) = 6 \Longrightarrow \frac{\text{ord}([3]_7)}{(k, \text{ord}([3]_7))} = 6 \Leftrightarrow$

$\Longrightarrow 6 \cdot \frac{6}{(k, \text{ord}([3]_7))} \Longrightarrow (k, 6) = 1 \Rightarrow \boxed{k = 5}$

• Άρα: $\boxed{U(Z_7) = \langle [3]_7 \rangle = \langle [5]_7 \rangle}$

Άσκηση Βρείτε όλες τις υποομάδες της $U(Z_7)$

• Η $U(Z_7)$ είναι κυκλική ομάδα $\Longrightarrow$ Κάθε υποομάδα κυκλικής ομάδας, είναι κυκλική!

• Άρα, αν $H \leq U(Z_7)$, τότε $H = \langle a \rangle$, με $a \in U(Z_7)$

• Έχω: • $\langle [1]_7 \rangle = \{[1]_7\}$

• $\langle [2]_7 \rangle = \{[2], [4], [1]\}$

• $\langle [3]_7 \rangle = U(Z_7)$ (γεννήτορας)

• $\langle [4]_7 \rangle = \{[2], [4], [1]\} = \langle [2]_7 \rangle$ (Κοινά [2] & [4] στη παραπάνω)

• $\langle [3] \rangle = U(Z_7) = \langle 5 \rangle$ και: $\langle [6] \rangle = \{[1], [6]\}$

• Άρα η $U(Z_4)$ έχει 4 υποομάδες!

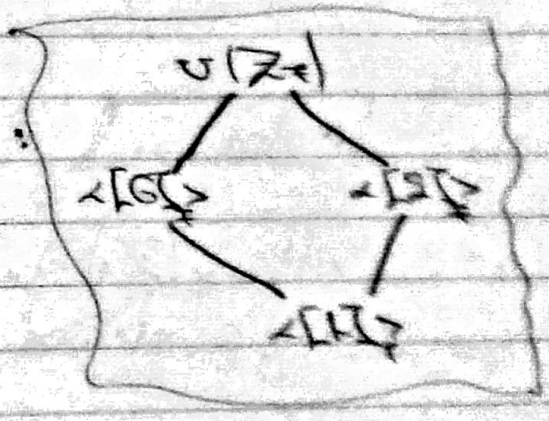
Δ Για κάθε διαιρέτη του 4 (εδώ $4=6$) μοναδική υποομάδα τάξης ίσης με έναν από τους διαιρέτες του 4!

▸ Διάγραμμα Hasse της ομάδας G_6

• Αν $H_1' \leq H_1$ και $H_1 \leq H_2$, τότε:

▸ Παράδειγμα

Το διάγραμμα Hasse της $U(Z_4)$:



▸ Παρατήρηση

Έστω $b \in G$ και $H \leq G$, αν $b \in H \Longrightarrow \langle b \rangle \leq H$

▸ Απόδειξη. ($\longleftarrow$) $\langle b \rangle \leq H \Rightarrow b \in H$

($\longrightarrow$) $b \in H \Rightarrow$ • Για $n=0$: $b^0 = 1 \in H$ (αφού H: υποομάδα)

• Για $n>0$: $b^n = \underbrace{b.b.\ldots b}_{n\text{: φορές}} \in H$

• Για $n<0$: $b^n = \underbrace{b^{-1}.b^{-1}.\ldots.b^{-1}}_{-n\text{: φορές}} \in H$ (Το αντίστροφο $\in H$)

• Άρα, για $\boxed{b \in H \iff \langle b \rangle \leq H}$

▸Θεώρημα Έστω α: γεννήτορας της κυκλικής ομάδας G, με $|G|=\nu$. Τότε, όλοι οι γεννήτορες της ομάδας G, είναι της μορφής α^s, με:

$$|s,\nu|=1 \quad \text{και} \quad 1 \leq s \leq \nu-1.$$

• Άρα, το πλήθος των γεννητόρων μιας κυκλικής ομάδας G, τάξης ν, είναι: $\varphi(\nu)$

▸ Απόδειξη: $\boxed{\Leftarrow}$ Έστω: $1 \leq s \leq \nu-1$ & $|s,\nu|=1$

$$\Longrightarrow \text{τ.σ}(\alpha^s) = \frac{\nu}{|s,\nu|} = \frac{\nu}{1} \Rightarrow \boxed{\text{τ.σ}(\alpha^s)=\nu}$$

• Άρα: $|\langle \alpha^s \rangle| = \nu$ και $\langle \alpha^s \rangle \subseteq G$ $\Rightarrow \boxed{\langle \alpha^s \rangle = G}$

↳ Το α^s γεννήτορας της G

$\boxed{\Rightarrow}$

• Έστω b: γεννήτορας της $G \Rightarrow G = \langle b \rangle \Rightarrow \boxed{\text{τ.σ}|b|=\nu}$

• Παρατηρώ: $b \in G = \langle \alpha^s \rangle \Rightarrow \boxed{b=\alpha^s}$, με $\boxed{1 \leq s \leq \nu-1}$

• Επίσης: $\nu = \text{τ.σ}(H) = \text{τ.σ}(\alpha^s) = \frac{\nu}{|s,\nu|} \Rightarrow \boxed{|s,\nu|=1}$

Αποδείχθη!!!

Θεώρημα · Έστω : $G = \langle a \rangle$, κυκλική ομάδα τάξης n

· Έστω : $H \leq G$. Τότε $|H| = d$, όπου $d \mid n$

· Για κάθε $d \mid n$, η G έχει ακριβώς μία υποομάδα τάξης d.

· **Απόδειξη** : Έστω : $H \leq G = \langle a \rangle \Rightarrow$

$\Rightarrow H$: κυκλική $\Rightarrow \boxed{H = \langle b \rangle} \Rightarrow b \in G = \langle a \rangle \Rightarrow$

$\Rightarrow \boxed{b = a^s \text{, για κάποιο } s} \Rightarrow$

$\Rightarrow |H| = |\langle b \rangle| = |\langle a^s \rangle| = \text{ord}|a^s| = \boxed{\frac{n}{(s,n)}}$ (1)

· Έστω : $|H| = d \overset{(1)}{\Longrightarrow} d = \frac{n}{(s,n)} \Rightarrow n = d \cdot (s,n) \Rightarrow$

$\Rightarrow \boxed{d \mid n}$

· Έστω $d \mid n$. Ορίζουμε $H = \langle a^{n/d} \rangle$ όπου $|H| = d$

· Έχω : $|H| = |\langle a^{n/d} \rangle| = \text{ord}|a^{n/d}| = \frac{n}{(\frac{n}{d}, n)} = \frac{n}{\frac{n}{d}} \Rightarrow$

$\Rightarrow \boxed{|H| = d}$

· Έστω : H_1 : μία ομάδα τάξης d, όπου $H_1 = H$

· Έχω : $H_1 \leq G = \langle a \rangle \Rightarrow H_1$: κυκλική $\Rightarrow \boxed{H_1 = \langle b \rangle}$

· Όμως : $b \in G = \langle a \rangle \Rightarrow \boxed{b = a^s}$

• Έχω, δοθέν, ότι: $H = \langle a^{4/d} \rangle$, $|H| = d$

• Υποθέτουμε, ότι: $|H_1| = d$ και χωρίζουμε ότι:

$H_1 = \langle a^s \rangle$, έχω:

• $d = |H_1| = \text{ord}(a^s) = \frac{4}{(s,4)} \Rightarrow (s,4) = 4/d \Rightarrow$

$\Rightarrow 4/d \mid s \Rightarrow \boxed{s = l \cdot \frac{4}{d}}$.

• Έχω: $H_1 = \langle a^s \rangle = \langle a^{4l/d} \rangle = \langle (a^{4/d})^l \rangle \Rightarrow$

$\Rightarrow a^s \in \langle a^{4/d} \rangle = H \Rightarrow \boxed{H_1 = \langle a^s \rangle < H}$.

• Καθώς: $|H_1| = d = |H|$ και δύο πλήθος στοιχείων,

έχουμε ότι: $\boxed{H_1 = H}$ Αντίφαση!!!

▶ **Άσκηση** Βρείτε όλες τις υποομάδες της $\mathbb{Z}_{12}$ και σχεδιάστε το διάγραμμα Hasse της $\mathbb{Z}_{12}$.

▶ **Λύση**: Έχω: $\mathbb{Z}_{12} = \{[0], [1], \ldots, [11]\}_{12}$

• Προφανώς: $\langle [1] \rangle = \{[11], [2], \ldots, [11], [0]\} = \mathbb{Z}_{12}$.

• Άρα, η $\mathbb{Z}_{12}$ είναι κυκλική!!!

• Η $\mathbb{Z}_{12}$ έχει 4 γεννήτορες, καθώς: $\varphi(12) = 4$

• Οι γεννήτορες του $\mathbb{Z}_{12}$ είναι οι εκφυλισμένοι 4:

$\longrightarrow [1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}$

• Η $\mathbb{Z}_{12} = \langle [1]_{12} \rangle$ είναι κυκλική τάξης 12, άρα έχει τόσες υποομάδες, όσοι οι φυσικοί διαιρέτες του 12.

• $1 | 12 \Rightarrow H_1 = \langle [0] \rangle$

$2 | 12 \Rightarrow H_2 = \langle [6] \rangle = \{[0], [6]\}$

$3 | 12 \Rightarrow H_3 = \langle [4] \rangle = \{[0], [4], [8]\}$

$4 | 12 \Rightarrow H_4 = \langle [3] \rangle = \{[0], [3], [6], [9]\}$

$6 | 12 \Rightarrow H_5 = \langle [2] \rangle = \{[0], [2], [4], [6], [8], [10]\}$.

$12 | 12 \Rightarrow H_6 = \langle [1] \rangle = \mathbb{Z}_{12}$.

• Διαγράμμα Hasse της $\mathbb{Z}_{12}$: