07/04/17.

Θεώρημα: Έστω $G=\langle\alpha\rangle$ άπειρη κυκλική ομάδα δηλ. $o(\alpha)=\infty$.

(1) Αν $\kappa,\lambda\in\mathbb{Z}$ τότε $\langle\alpha^\kappa\rangle\subseteq\langle\alpha^\lambda\rangle\Leftrightarrow\lambda|\kappa$
Ισοδύναμα αν $\kappa,\lambda\in\mathbb{N}$ τότε $\langle\alpha^\kappa\rangle=\langle\alpha^\lambda\rangle\Rightarrow\lambda=\kappa$

(2) Οι υποομάδες της G είναι οι εξής:
$\langle e\rangle=\{e\}$, $G=\langle\alpha\rangle$, $\langle\alpha^2\rangle$, $\langle\alpha^3\rangle$, ..., $\langle\alpha^n\rangle$, ...

(3) Η G έχει ακριβώς 2 γεννήτορες: α, α^{-1}

(4) Η απεικόνιση $f:\mathbb{Z}\to G$, $f(\kappa)=\alpha^\kappa$ είναι ένας ισομορφισμός ομάδων

(5) Δυο άπειρες κυκλικές ομάδες είναι ισόμορφες.

Απόδειξη: (1) Έστω ότι $\langle\alpha^\kappa\rangle\subseteq\langle\alpha^\lambda\rangle$. Τότε $\alpha^\kappa\in\langle\alpha^\kappa\rangle\subseteq\langle\alpha^\lambda\rangle$
άρα $\alpha^\kappa\in\langle\alpha^\lambda\rangle\Rightarrow\exists m\in\mathbb{Z}:\alpha^\kappa=(\alpha^\lambda)^m=\alpha^{\lambda m}\Rightarrow$
$\Rightarrow\alpha^{\kappa-\lambda m}=e$. Επειδή $o(\alpha)=\infty\Rightarrow\nexists r\in\mathbb{N}:\alpha^r=e$ άρα αναγκαστικά $\kappa=\lambda m\Rightarrow\lambda|\kappa$
Αντίστροφα, αν $\lambda|\kappa\Rightarrow\kappa=\lambda m$ για κάποιο $m\in\mathbb{Z}$ και τότε:
$\alpha^\kappa=\alpha^{\lambda m}=(\alpha^\lambda)^m\in\langle\alpha^\lambda\rangle\overset{(*)}{\Rightarrow}\langle\alpha^\kappa\rangle\subseteq\langle\alpha^\lambda\rangle$
(*) Αν $x\in H\leq G\Rightarrow\langle x\rangle\leq H$
Άρα $\langle\alpha^\kappa\rangle\subseteq\langle\alpha^\lambda\rangle\Leftrightarrow\lambda|\kappa$.
Έστω $\kappa,\lambda\in\mathbb{N}$ και $\langle\alpha^\lambda\rangle=\langle\alpha^\kappa\rangle$, τότε
$\left.\begin{matrix}\langle\alpha^\kappa\rangle\subseteq\langle\alpha^\lambda\rangle\Rightarrow\lambda|\kappa\\ \langle\alpha^\lambda\rangle\subseteq\langle\alpha^\kappa\rangle\Rightarrow\kappa|\lambda\end{matrix}\right\}\overset{\kappa,\lambda\in\mathbb{N}}{\Longrightarrow}\boxed{\kappa=\lambda}$. Δηλαδή $\langle\alpha^\kappa\rangle=\langle\alpha^\lambda\rangle\Leftrightarrow$
$\Leftrightarrow\kappa=\lambda$, $\forall\kappa,\lambda\in\mathbb{N}$

(2) Προκύπτει άμεσα από (1) διότι γνωρίζουμε οι υποομάδες της G είναι οι $\langle\alpha^\kappa\rangle$, όπου $\kappa\in\mathbb{N}\cup\{0\}$ και από το (1) έχουμε ότι οι παραπάνω υποομάδες είναι ανά δύο διαφορετικές.

(3) Έστω X γεννήτορας της G. Τότε $G=\langle\alpha\rangle=\langle x\rangle$
Αφού $x\in G\to x=\alpha^\kappa$, $\kappa\in\mathbb{Z}$. Τότε $\alpha\in\langle\alpha\rangle=\langle x\rangle=\langle\alpha^\kappa\rangle\Rightarrow$

$\Rightarrow \exists w \in \mathbb{Z}: \alpha = (\alpha^k)^w \Rightarrow \alpha = \alpha^{kw} \Rightarrow \alpha^{1-kw} = e \xrightarrow{o(\alpha)=\infty}$

$\Rightarrow 1-kw=0 \Rightarrow 1=kw \xrightarrow{k,w\in\mathbb{Z}} k,w = \pm 1 \Rightarrow x = x^{\pm 1} \Rightarrow$

$\Rightarrow x=\alpha$ ή $x=\alpha^{-1}$. Άρα οι γεννήτορες της G είναι οι α, α^{-1}

(Αν $G=\langle\alpha\rangle = \{\alpha^n \in G, | n\in\mathbb{Z}\} = \{\alpha^{-n} \in G | n\in\mathbb{Z}\} = \{(\alpha^{-1})^n \in G | n\in\mathbb{Z}\} =$
$= \langle\alpha^{-1}\rangle$, $\forall G$: κυκλική)

④ $\forall k,\lambda \in \mathbb{Z}: f(k+\lambda) = \alpha^{k+\lambda} = \alpha^k \cdot \alpha^\lambda = f(k)\cdot f(\lambda)$ (άρα είναι το αθροίσμα στο χωρίο των εικόνων στην G άρα καλά ορισμένη)

$f(k)=f(\lambda) \Rightarrow \alpha^k = \alpha^\lambda \Rightarrow \alpha^{k-\lambda} = e \xrightarrow{o(\alpha)=\infty} k-\lambda=0 \Rightarrow k=\lambda \Rightarrow f: 1-1$

$\forall x \in G: \exists k\in\mathbb{Z}: x=\alpha^k \Rightarrow f(k)=\alpha^k = x \Rightarrow f:$ επί

Άρα η f είναι ισομορφισμός ομάδων.

⑤ Έστω G_1, G_2: άπειρες κυκλικές ομάδες. Τότε από το ④ έπεται ότι: η G_1 είναι ισόμορφη με την $(\mathbb{Z},+)$ και } $\Rightarrow$
επίσης η G_2 είναι ισόμορφη με την $(\mathbb{Z},+)$

$\Rightarrow$ οι G_1, G_2 είναι ανάμεσα τους ισόμορφες (λογικά).

(συνθετικά αν f,g ισομορφισμοί $\Rightarrow f\circ g$: ισομορφισμός).

Η προσθετική ομάδα των ακεραίων $(\mathbb{Z},+)$ είναι άπειρη κυκλική ομάδα $\mathbb{Z}=\langle 1\rangle$. Τότε $\langle n\rangle := n\mathbb{Z}$, $\forall n\in\mathbb{Z}$

Οι μόνοι γεννήτορες της $(\mathbb{Z},+)$ είναι οι: $1, -1$.

$\forall n,m\in\mathbb{Z}: \underset{\parallel}{\langle n\rangle} \subseteq \underset{\parallel}{\langle m\rangle} \Leftrightarrow m|n$
$n\mathbb{Z}$ $m\mathbb{Z}$

Άρα $n\mathbb{Z}=m\mathbb{Z} \Leftrightarrow n|m$, $n,m\in\mathbb{N}$.

Οι υποομάδες της $(\mathbb{Z},+)$ είναι οι εξής: $\langle 0\rangle=\{0\}$, $\langle 1\rangle=\mathbb{Z}$, $\underset{\parallel}{\langle 2\rangle}, \ldots, \underset{\parallel}{\langle n\rangle}, \ldots$
$2\mathbb{Z}$ $n\mathbb{Z}$

$(\mathbb{C}^*,\cdot)$ δεν είναι άπειρη κυκλική διότι αν ήταν θα ήταν ισόμορφη με την $(\mathbb{Z},+)$ και άρα θα είχαμε ότι $|\mathbb{Z}|=|\mathbb{C}^*|$ ΑΤΟΠΟ.

Όμοια οι ομάδες $(\mathbb{C},+)$, $(\mathbb{R},+)$, $(\mathbb{R}^*,\cdot)$ δεν είναι κυκλικές (άπειρες)

Έστω $z \in \mathbb{C}^*$ και θεωρούμε την κυκλική ομάδα $\langle z \rangle \leq (\mathbb{C}^*, \cdot)$

Τότε $\langle z \rangle$: πεπερασμένη $\Leftrightarrow o(z) = |\langle z \rangle| < \infty \Leftrightarrow$
$\Leftrightarrow \exists n \in \mathbb{N}: z^n = 1 \Leftrightarrow \exists n \in \mathbb{N}: z \in U_n$

Άρα $\langle z \rangle$ πεπερασμένη κυκλική $\Leftrightarrow z \in U_n$ για κάποιο $n \in \mathbb{Z}$.

Όμως αν $z \in U_n$ τότε $z^n = 1 \Rightarrow |z^n| = 1 \Rightarrow |z|^n = 1 \Rightarrow$
$\Rightarrow |z| = 1$.

Έχει για παράδειγμα $\langle 1+i \rangle$: άπειρη διότι $|1+i| = \sqrt{2} \neq 1$

Θεώρημα: Έστω $(G, \cdot)$ ομάδα και $\alpha \in G$ με $o(\alpha) < \infty$.
Τότε:

(1) $o(\alpha^k) < \infty$ και $o(\alpha^k) = \dfrac{o(\alpha)}{(k, o(\alpha))}$

(2) $o(\alpha) = o(\alpha^{-1})$ και $\forall k \in \mathbb{Z}: o(\alpha^k) = \dfrac{o(\alpha)}{(|k|, o(\alpha))}$

(3) $\forall k \in \mathbb{N}: o(\alpha) = o(\alpha^k) \Leftrightarrow (k, o(\alpha)) = 1$.

(4) $\forall k \in \mathbb{N}: o(\alpha^k) = \dfrac{o(\alpha)}{k} \Leftrightarrow k \mid o(\alpha)$.

Απόδειξη: (1) Έστω $o(\alpha) < \infty$. Τότε $\alpha^n = e$ και άρα
$(\alpha^k)^n = \alpha^{kn} = (\alpha^n)^k = e^k = e \Rightarrow o(\alpha^k) < \infty$.

Έστω $m = o(\alpha^k)$ και $d := (k, o(\alpha)) = (k, n)$

Άρα αρκεί να δείξω $m = \dfrac{n}{d} = n'$

Είναι $d = (k, n) \Rightarrow \begin{matrix} d \mid k \\ d \mid n \end{matrix} \Rightarrow \begin{cases} k = dk' \\ n = dn' \end{cases}$ (*) για κάποιους $k', n' \in \mathbb{N}$ και $(n', k') = 1$.

- $(\alpha^k)^{\frac{n}{d}} = \alpha^{k\frac{n}{d}} = \alpha^{n\frac{k}{d}} = e^{\frac{k}{d}} = e \Rightarrow \boxed{o(\alpha^k) = m \mid \frac{n}{d}}$ (1)

- $o(\alpha^k) = m \Rightarrow (\alpha^k)^m = e \Rightarrow \alpha^{km} = e \Rightarrow o(\alpha) = n \mid km \overset{(*)}{\Rightarrow}$
$\Rightarrow dn' \mid dk'm \Rightarrow n' \mid k'm \overset{\text{ΛΗΜΜΑ Euclid}}{\underset{(n', k') = 1}{\Rightarrow}} n' \mid m \Rightarrow \boxed{\frac{n}{d} \mid m}$ (2)

Από (1), (2) $\Rightarrow o(\alpha^k) = m = \dfrac{o(\alpha)}{(k, o(\alpha))}$

(2) Γνωρίζουμε ότι: $o(\alpha) = o(\alpha^{-1}) \to o(\alpha^k) = o(\alpha^{-k}), \forall k \in \mathbb{Z} \Rightarrow$

$\Rightarrow$ { αν $k<0 \Rightarrow o(\alpha^k) = o(\alpha^{-k}) \overset{(1)}{=} \frac{o(\alpha)}{(-k, o(\alpha))}$

{ αντίστοιχα για $k>0$.

(3), (4) Άμεσες συνέπειες του (1). $\Longleftrightarrow$

Έστω $G = \langle \alpha \rangle$ κυκλική ομάδα πεπ/μης τάξης $n \Rightarrow o(\alpha) = n$

Τότε $G = \{e, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$.

Το $x \in G$ είναι γεννήτορας $\Leftrightarrow G = \langle \alpha \rangle = \langle x \rangle$. Αν το x: γεννήτορας τότε $\langle x \rangle = \langle \alpha \rangle \Rightarrow \underbrace{|\langle x \rangle|}_{o(x)} = |\langle \alpha \rangle| = |G| = n$.

Όμως $x \in G \Rightarrow x = \alpha^k$, $k = 1, 2, \dots, n-1$. Τότε $o(\alpha^k) = n = o(\alpha) \Rightarrow$

$\Rightarrow \frac{n}{(k,n)} = n \Rightarrow (k,n) = 1$.

Αντίστροφα, αν $(k,n)=1$, δ.δ. ο α^k: γεννήτορας της G.

Τότε από (1) του θεωρήματος: $o(\alpha^k) = \frac{o(\alpha)}{(k, o(\alpha))} = \frac{n}{(k,n)} = n \Rightarrow$

$\Rightarrow |\langle \alpha^k \rangle| = n = |G|$

Άρα $\left.\begin{matrix} \langle \alpha^k \rangle \leq G \\ |\langle \alpha^k \rangle| = |G| \end{matrix}\right\} \Rightarrow \langle \alpha^k \rangle = G \Rightarrow \alpha^k$: γεννήτορας της G.

Άρα $\forall k = 1, \dots, n-1$: α^k: γεννήτορας της $G \to (k,n) = 1$.

Άρα οι γεννήτορες της G με τάξη n είναι $\varphi(n)$ σε πλήθος όπου φ: συνάρτηση Euler ($\forall n \in \mathbb{N}: \varphi(n) = \left|\{k \in \mathbb{N} \mid \begin{matrix} 1 \leq k \leq n \\ (k,n)=1 \end{matrix}\}\right|$ και $\varphi(n)$: άρτιος $\Leftrightarrow n \geq 3$ και $\varphi(1) = 1$, $\varphi(2) = 1$.

Το πλήθος των γεννητόρων μιας άπειρης κυκλικής και μιας πεπερασμένης κυκλικής τάξης ≥ 3 είναι άρτιο.

$\Longleftrightarrow$

(*) **Θεώρημα**: Έστω $G=\langle\alpha\rangle$: πεπερασμένη κυκλική ομάδα τάξης n. Τότε $o(\alpha)=n$ και $G=\{e,\alpha,\dots,\alpha^{n-1}\}$.

(1) Το στοιχείο α^k, $k=1,\dots,n$ είναι γεννήτορας της G $\Leftrightarrow$ $(k,n)=1$, και το πλήθος των γεννητόρων της G είναι $\varphi(n)$.

(2) Οι υποομάδες της G είναι οι εξής: $\langle\alpha^{d_1}\rangle,\langle\alpha^{d_2}\rangle,\dots,\langle\alpha^{d_{\tau(n)}}\rangle$, όπου $d_1,\dots,d_{\tau(n)}$ θετικοί διαιρέτες του n.

(3) Η τάξη κάθε υποομάδας της G διαιρεί την τάξη της G και για κάθε διαιρέτη d της τάξης της G, υπάρχει ακριβώς μία υποομάδα H της G με τάξη $|H|=d$.

(4) Η απεικόνιση $f:\mathbb{Z}_n\to G$, $f([k]_n)=\alpha^k$ είναι ισομορφισμός ομάδων

(5) Δύο πεπερασμένες κυκλικές ομάδες είναι ισόμορφες $\Leftrightarrow$ έχουν την ίδια τάξη.

Απόδειξη: (1) Αποδείχθηκε προηγουμένως.

(2) Έστω $H\le G$. Επειδή υποομάδες κυκλικών ομάδων είναι κυκλικές $\Rightarrow H$: κυκλική και άρα $\exists m=1,\dots,n$ τέτοιο ώστε $H=\langle\alpha^m\rangle$. [Αν $H\le G$: κυκλική, $G=\langle\alpha\rangle\Rightarrow H=\langle\alpha^k\rangle$ όπου $k=\min\{m\in\mathbb{N}\mid\alpha^m\in H\}$.]: Έστω $k=\min\{r\in\mathbb{N}\mid\alpha^r\in H\}$ Τότε $H=\langle\alpha^m\rangle=\langle\alpha^k\rangle$. Ισχυρίζομαι: $k\mid n=o(\alpha)$. Έστω $d=(k,n)\Rightarrow\exists x,y\in\mathbb{Z}: d=kx+ny$. Τότε: $\alpha^d=\alpha^{kx+ny}=\alpha^{kx}\cdot\alpha^{ny}=(\alpha^k)^x\cdot(\alpha^n)^y\overset{o(\alpha)=n}{=}(\alpha^k)^x\cdot e^y=(\alpha^k)^x\in H$. Όμως $d\mid k\Rightarrow d\ge k=\min\{r\in\mathbb{N}\mid\alpha^r\in H\}$ και $\alpha^d\in H$. Άρα $\boxed{k=d}=(k,n)$ και άρα $k\mid n$.

Άρα οι υποομάδες της G είναι οι εξής: $\langle\alpha^d\rangle$, $\forall d\mid n$.

Έστω $k\mid n$, $\lambda\mid n$ όπου $k,\lambda\in\mathbb{N}$ και έστω ότι $\langle\alpha^k\rangle\subseteq\langle\alpha^\lambda\rangle$ Τότε $\alpha^k\in\langle\alpha^k\rangle\subseteq\langle\alpha^\lambda\rangle\Rightarrow\exists m\in\mathbb{N}:\alpha^k=(\alpha^\lambda)^m\Rightarrow$ $\Rightarrow\alpha^k=\alpha^{\lambda m}\Rightarrow\alpha^{k-\lambda m}=e\Rightarrow o(\alpha)=n\mid\lambda-k$ Θα έχουμε $\lambda\mid n\Rightarrow\lambda\mid k-\lambda m$. Όμως $\lambda\mid\lambda m\Rightarrow\lambda\mid k$. Αντίστροφα, αν $\lambda\mid k\Rightarrow k=\lambda m$, για κάποιο $m\in\mathbb{Z}$ και τότε $\alpha^k=\alpha^{\lambda m}=$

$= (\alpha^\lambda)^{\frac{k}{\lambda}} \in \langle \alpha^\lambda \rangle \Rightarrow \langle \alpha^k \rangle \subseteq \langle \alpha^\lambda \rangle$

Άρα αν $k, \lambda \in \mathbb{N}$ και $\lambda | n \Rightarrow \langle \alpha^k \rangle \subseteq \langle \alpha^\lambda \rangle \Leftrightarrow \lambda | k$

Ισχύει αν $k, \lambda \in \mathbb{N}$ τ.ω. $k | n$ και $\lambda | n \Rightarrow \langle \alpha^k \rangle = \langle \alpha^\lambda \rangle \Leftrightarrow k = \lambda$.

Άρα οι $\tau(n)$ διαφορετικές υποομάδες της G είναι:

$\langle \alpha^{d_1} \rangle, \dots, \langle \alpha^{d_{\tau(n)}} \rangle$, με $d_1, \dots, d_{\tau(n)}$: φυσικοί διαιρέτες του n.

(3) Η τάξη των υποομάδων αυτών είναι:

$$|\langle \alpha^{d_i} \rangle| = o(\alpha^{d_i}) = \frac{o(\alpha)}{(d_i, o(\alpha))} = \frac{n}{(d_i, n)} = \frac{n}{d_i}, \quad i = 1, \dots, \tau(n)$$

Καθώς το d διατρέχει τους θετικούς διαιρέτες του n, το n/d διατρέχει επίσης τους $1, \dots, n$ αλλά με διαφορετική σειρά

Από τα παραπάνω έπεται ότι η τάξη κάθε υποομάδας H διαιρεί την τάξη της ομάδας και επιπλέον $\forall d | n = |G|$, υπάρχει ακριβώς μία υποομάδα H με τάξη d η οποία είναι η $H = \langle \alpha^{\frac{n}{d}} \rangle$.

(4) Έστω $[k]_n = [\lambda]_n \Rightarrow k \equiv \lambda \bmod n \Rightarrow n | k - \lambda \Rightarrow$

$\Rightarrow k - \lambda = n \cdot x \quad x \in \mathbb{Z} \Rightarrow k = \lambda + nx$

Τότε $\alpha^k = \alpha^{\lambda + nx} = \alpha^\lambda \cdot \alpha^{nx} = \alpha^\lambda (\alpha^n)^x \overset{o(\alpha)=n}{=} \alpha^\lambda \cdot e^x = \alpha^\lambda$

- Άρα f: καλά ορισμένη.

$f([k]_n + [\lambda]_n) = f([k+\lambda]_n) = \alpha^{k+\lambda} = \alpha^k \cdot \alpha^\lambda = f([k]_n) \cdot f([\lambda]_n)$

άρα f: ομομορφισμός.

- $f([k]_n) = f([\lambda]_n) \Leftrightarrow \alpha^k = \alpha^\lambda \Leftrightarrow \alpha^{k-\lambda} = e \Leftrightarrow o(\alpha) = n | k - \lambda \Leftrightarrow$

$\Leftrightarrow k \equiv \lambda \bmod n$. Άρα f : 1-1.

- $\forall x \in G \Rightarrow \exists k = 1, \dots, n-1 : x = \alpha^k$. Τότε $f([k]_n) = \alpha^k = x \Rightarrow f$: επί.

Άρα f ισομορφισμός ομάδων.

(5) Αν G_1, G_2 κυκλικές και $|G_1| = n = |G_2| \Rightarrow$ G_1 ισόμορφη $\mathbb{Z}_n$, G_2 -||- $(\mathbb{Z}_n, +)$ και άρα G_1 ισόμορφη με G_2. Αντίστροφα, αν G_1, G_2 ισόμορφες θα έχουν προφανώς ίδια τάξη.