Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Τμήμα Μαθηματικών

Ηλεκτρονική Τάξη: http://eclass.uoa.gr

Σημειώσεις Φοιτητών

Εαρινό Εξάμηνο 2013-2014

Μάθημα:

834. Θεωρία Ομάδων

Διδάσκοντες: Ο. Ταλέλλη & Δ. Δεριζιώτης

Ευχαριστούμε για τις σημειώσεις τον Toxus

ΘΕΩΡΙΑ ΟΜΑΔΩΝ

(ακαδ. έτος 2013-14, εαρ. εξάμ.)

Μάθημα 1° **(Τετάρτη, 16/4/2014)**

[*Υπενθυμίσεις από τη Βασική Άλγεβρα*]:

- **Ορισμός ομάδας**:

Ομάδα $\langle G,* \rangle$ ονομάζεται ένα σύνολο G, εφοδιασμένο με μία (διμελή) πράξη $*: GxG \to G$ τέτοια ώστε να ικανοποιούνται τα ακόλουθα αξιώματα:

i. Η πράξη $*$ είναι προσεταιριστική.

ii. Υπάρχει (μοναδικό) στοιχείο $e \in G: e*a = a*e = a,\ \forall a \in G$. Το στοιχείο e ονομάζεται ταυτοτικό στοιχείο της $\langle G,* \rangle$.

iii. Για κάθε $a \in G$ υπάρχει (μοναδικό) στοιχείο $a^{-1} \in G: a^{-1}*a = a*a^{-1} = e$. Το στοιχείο a^{-1} ονομάζεται αντίστροφο στοιχείο του a στη $\langle G,* \rangle$.

- **Παρατήρηση:**

1. Η μοναδικότητα του ταυτοτικού και του αντιστρόφου στοιχείου μπορεί να αποδειχθεί, δεν αποτελεί δηλαδή μέρος του αξιωματικού ορισμού της έννοιας της ομάδας.

- **Παραδείγματα**:

1. Η ομάδα $\left\langle S(X) = \left\{ f : X \underset{\text{επί}}{\overset{1\text{-}1}{\to}} X \right\}, \circ \right\rangle$ των μεταθέσεων ενός συνόλου X με πράξη την σύνθεση. Εάν $|X| = n \in \mathbb{N}$, τότε η ομάδα αυτή είναι ισόμορφη με τη συμμετρική ομάδα S_n (γράφουμε $\langle S(X), \circ \rangle \simeq S_n$).
2. Η γενική γραμμική ομάδα $GL_n(K)$ των nxn αντιστρέψιμων πινάκων με στοιχεία από ένα σώμα K, με πράξη τον πολλαπλασιασμό πινάκων. Δηλαδή $GL_n(K) = \langle A \in M_n(K) \,|\, |A| \neq 0, \bullet \rangle$.
3. Η ειδική γραμμική ομάδα $SL_n(K)$ των nxn αντιστρέψιμων πινάκων με στοιχεία από ένα σώμα K και οι οποίοι έχουν ορίζουσα ίση με τη μονάδα, με πράξη τον πολλαπλασιασμό πινάκων. Δηλαδή $SL_n(K) = \langle A \in M_n(K) \,|\, |A| = 1, \bullet \rangle$. Η $SL_n(K)$ είναι υποομάδα της $GL_n(K)$ (γράφουμε $SL_n(K) \leq GL_n(K)$).

- ***Ορισμός υποομάδας*:**

Έστω $\langle G,* \rangle$ μία ομάδα και $H \subseteq G$. Εάν το σύνολο H είναι κλειστό ως προς την πράξη $*$ και αν, επιπλέον, εφοδιασμένο με την (επαγόμενη) πράξη $*$ αποτελεί ομάδα, τότε η ομάδα $\langle H,* \rangle$ ονομάζεται υποομάδα της $\langle G,* \rangle$ και γράφουμε $H \leq G$.

- **Παρατηρήσεις:**

1. Ισχύει η ακόλουθη ισοδυναμία: $H \leq G \Leftrightarrow \forall h_1, h_2 \in H \Rightarrow h_1 * h_2^{-1} \in H$.
2. Εάν $H \leq G$ και e το ταυτοτικό στοιχείο της G, τότε $e \in H$ και μάλιστα το e είναι το ταυτοτικό στοιχείο της H.
3. Ισχύει ότι $G \leq G$ και εάν $H \leq G$, με $H \neq G$, τότε η H ονομάζεται γνήσια υποομάδα της G.
4. Εάν e είναι το ταυτοτικό στοιχείο της $\langle G,* \rangle$, τότε το μονοσύνολο $\{e\}$ εφοδιασμένο με την πράξη $*$ αποτελεί την υποομάδα $\{e\} \leq G$. Η υποομάδα $\{e\}$ είναι η τετριμμένη υποομάδα της G.

- **Βασικά είδη ομάδων:**

1. Κάθε ομάδα με πεπερασμένο πλήθος στοιχείων ονομάζεται πεπερασμένη. Διαφορετικά, ονομάζεται άπειρη ομάδα. Το πλήθος των στοιχείων μίας ομάδας ονομάζεται τάξη της ομάδας.
2. Έστω $\langle G,* \rangle$ μία ομάδα. Εάν $a * b = b * a,\ \forall a,b \in G$, τότε η ομάδα G λέγεται αβελιανή ή μεταθετική ομάδα.
3. Έστω $\langle G,* \rangle$ μία ομάδα και $g \in G$ τυχόν στοιχείο της. Τότε η υποομάδα της G που παράγεται από το g είναι η $\langle g \rangle = \{g^n \mid n \in \mathbb{N}\}$, όπου $g^n = g * g * \ldots * g$ (n φορές). Η $\langle g \rangle$ ονομάζεται κυκλική ομάδα και λέμε ότι το g είναι ο γεννήτορας της $\langle g \rangle$. Προφανώς κάθε κυκλική ομάδα είναι αβελιανή.
4. Έστω $\langle g \rangle$ μία κυκλική ομάδα. Τότε, εάν η $\langle g \rangle$ είναι άπειρη, ισχύει ότι $\langle g \rangle \simeq \langle 1 \rangle = \langle \mathbb{Z}, + \rangle = \{z \mid z \in \mathbb{Z}\}$, δηλαδή κάθε άπειρη κυκλική ομάδα είναι ισόμορφη με την προσθετική ομάδα των ακεραίων. Από την άλλη μεριά, εάν η $\langle g \rangle$ είναι πεπερασμένη με $|\langle g \rangle| = n \in \mathbb{N}$, ισχύει ότι $\langle g \rangle \simeq \langle 1 (\mathrm{mod} n) \rangle = \langle \mathbb{Z}_n, + \rangle = \{k (\mathrm{mod} n) \mid k = 0,1,2,\ldots,n-1\}$, δηλαδή κάθε πεπερασμένη κυκλική ομάδα $\langle g \rangle$ είναι ισόμορφη την προσθετική ομάδα των ακεραίων modulo $|\langle g \rangle|$.

- ***Ορισμός συμπλόκου*:**

Έστω $\langle G,* \rangle$ μία ομάδα, $a \in G$ και $H \leq G$. Το υποσύνολο $aH = \{a * h \mid h \in H\}$ λέγεται το αριστερό σύμπλοκο της H που περιέχει το a. Αντίστοιχα, το

υποσύνολο $Ha = \{h * a \mid h \in H\}$ λέγεται το δεξιό σύμπλοκο της H που περιέχει το a.

- **Παρατηρήσεις:**

1. Για κάθε αριστερό σύμπλοκο aH μπορούμε να ορίσουμε την 1-1 και επί απεικόνιση $\phi : H \to aH$ με $\phi(h) = ah$. Ομοίως μπορούμε να ορίσουμε την 1-1 και επί απεικόνιση $\phi' : H \to Ha$ με $\phi(h) = ha$, για κάθε δεξιό σύμπλοκο Ha. Αυτό αποδεικνύει ότι, εάν περιοριστούμε σε πεπερασμένες ομάδες, έπεται ότι $|H| = |aH| = |Ha|$.
2. Έστω $H \leq G$. Τα αριστερά (ομοίως τα δεξιά) σύμπλοκα της υποομάδας H αποτελούν μία διαμέριση της G. Συνδυάζοντας τις δύο παρατηρήσεις οδηγούμαστε στο ακόλουθο Θεώρημα.

- ***Θεώρημα Lagrange*:**

Έστω $\langle G, * \rangle$ μία πεπερασμένη ομάδα και $H \leq G$. Τότε $|H| \,|\, |G|$.

- ***Ορισμός δείκτη υποομάδας*:**

Έστω $H \leq G$. Το πλήθος των αριστερών συμπλόκων της H στην G ονομάζεται δείκτης $|G : H|$ της H στην G.

- **Παρατηρήσεις:**

1. $|G| = |G : H| \cdot |H|$.
2. Υπάρχει 1-1 και επί απεικόνιση από το σύνολο των αριστερών συμπλόκων της $H \leq G$ στο σύνολο των δεξιών συμπλόκων της H, $gH \to Hg^{-1} \quad \forall g \in G$. Επομένως το πλήθος των αριστερών συμπλόκων της H στην G είναι ίσο προς το πλήθος των δεξιών συμπλόκων της H στην G.

- ***Ορισμός ομομορφισμού ομάδων*:**

Έστω $\langle G, * \rangle$, $\langle G', \bullet \rangle$ δύο ομάδες. Μία απεικόνιση $\phi : G \to G'$ λέγεται ομομορφισμός, εάν $\phi(a * b) = \phi(a) \bullet \phi(b) \quad \forall a, b \in G$.

- **Παρατηρήσεις:**

1. Ας υποθέσουμε ότι υπάρχει μία ομάδα $\langle G, * \rangle$, την οποία θέλουμε να μελετήσουμε. Η μελέτη γίνεται μέσω της σύγκρισης της ομάδας αυτής $\langle G, * \rangle$ με μία άλλη ομάδα $\langle G', \bullet \rangle$, την οποία έχουμε ήδη μελετήσει. Η σύγκριση επιτυγχάνεται ακριβώς μέσω ενός ομομορφισμού $\phi : G \to G'$, που είναι μία απεικόνιση η οποία επιπλέον διατηρεί τις ιδιότητες της πράξης $*$.

2. Εάν ο ομομορφισμός είναι 1-1, τότε λέγεται μονομορφισμός. Εάν είναι επί, τότε λέγεται επιμορφισμός. Εάν είναι 1-1 και επί, τότε λέγεται ισομορφισμός.
3. Κάθε ομομορφισμός $\phi : G \to G$ λέγεται ενδομορφισμός. Εάν επιπλέον ένας ενδομορφισμός είναι 1-1 και επί, τότε λέγεται αυτομορφισμός της ομάδας G.
4. Έστω $\phi : G \to G'$ ένας ομομορφισμός ομάδων. Για την εικόνα $\phi(G) = \{\phi(g) \mid g \in G\}$ και τον πυρήνα $\ker\phi = \{g \in G \mid \phi(g) = e_{G'}\}$ ισχύουν ότι $\phi(G) \leq G'$ και $\ker\phi \leq G$. Ειδικότερα $\ker\phi \lhd G$, δηλαδή ο πυρήνας $\ker\phi$ είναι κανονική υποομάδα της G (βλ. παρακάτω).
5. Έστω $\phi : G \to G'$ ένας ομομορφισμός ομάδων. Ο ϕ είναι ισομορφισμός αν και μόνο αν $\ker\phi = \{e_G\}$, δηλαδή ο ϕ είναι ισομορφισμός αν και μόνο αν ο πυρήνας είναι η τετριμμένη υποομάδα της G.

- ***Ορισμός κανονικής υποομάδας*:**

Έστω $\langle G, * \rangle$ μία ομάδα και $H \leq G$. Τότε η H λέγεται κανονική υποομάδα της G εάν τα αριστερά και δεξιά της σύμπλοκα συμπίπτουν. Γράφουμε $H \lhd G$ και ισχύουν οι ακόλουθες ισοδυναμίες:

$$H \lhd G \;\Leftrightarrow\; gH = Hg,\ \forall g \in G \;\Leftrightarrow\; gHg^{-1} = H,\ \forall g \in G.$$

- ***Ορισμός ομάδας-πηλίκο*:**

Έστω $\langle G, * \rangle$ μία ομάδα και $H \lhd G$. Τότε στο σύνολο $G/H = \{gH \mid g \in G\}$ η πράξη $(aH)(bH) = (a * b)H$ είναι καλά ορισμένη. Επομένως το σύνολο G/H εφοδιασμένο με την παραπάνω πράξη αποτελεί ομάδα, που ονομάζεται ομάδα-πηλίκο της G ως προς την H.

- **Παρατηρήσεις:**

1. Ταυτοτικό στοιχείο της ομάδας-πηλίκο G/H είναι η ομάδα H.
2. Το αντίστροφο στοιχείο του gH της ομάδας-πηλίκο G/H είναι το $g^{-1}H$.

- **1° Θεώρημα ισομορφισμών:**

Έστω $\phi : G \to G'$ ένας ομομορφισμός ομάδων. Τότε $G/\ker\phi \simeq \phi(G)$, με $g\ker\phi \to \phi(g)$.

- **Παρατήρηση:**

1. Αντίστροφα, εάν $H \lhd G$, τότε ο ομομορφισμός $\phi : G \to G/H$ με $\phi(g) = gH$ ονομάζεται φυσικός (ή κανονικός) επιμορφισμός. Προφανώς $\ker\phi = H$.

- **Λήμμα:**

Έστω G μία ομάδα και H, N δύο υποομάδες της G. Τότε το σύνολο $HN = \{hn \mid h \in H,\ n \in N\}$ δεν είναι αναγκαστικά ομάδα. Μάλιστα, $HN \subseteq \langle H,N \rangle$, όπου με $\langle H,N \rangle$ συμβολίζουμε την ελάχιστη υποομάδα της G που περιέχει τις H και N.

Ωστόσο, εάν $N \lhd G$, τότε ισχύει ότι $HN = NH = \langle H,N \rangle$, δηλαδή στην περίπτωση αυτή η HN (και προφανώς η NH) είναι υποομάδα της G. Εάν επιπλέον $H \lhd G$, τότε $HN = NH = \langle H,N \rangle \lhd G$. Δηλαδή αν $N \lhd G$ και $H \lhd G$, τότε $HN \lhd G$.

- **2ο Θεώρημα ισομορφισμών:**

Έστω G μία ομάδα, $H \leq G$ και $N \lhd G$. Τότε $(HN)/N \simeq H/(H \cap N)$.

- **3ο Θεώρημα ισομορφισμών:**

Έστω G μία ομάδα, $H \lhd G$, $N \lhd G$ και $N \leq H$. Τότε $G/H \simeq (G/N)/(H/N)$.

- **Θεώρημα της αντιστοιχίας:**

Έστω G μία ομάδα και $N \lhd G$. Τότε κάθε υποομάδα της ομάδας-πηλίκο G/N είναι της μορφής H/N, όπου $N \leq H \leq G$. Επιπλέον, κάθε κανονική υποομάδα της ομάδας-πηλίκο G/N είναι της μορφής K/N, όπου $N \leq K \lhd G$, και παράλληλα $G/K \simeq (G/N)/(K/N)$.

- **Θεώρημα του Cayley:**

Έστω G μία πεπερασμένη ομάδα τάξης n. Τότε η G είναι ισόμορφη με μία ομάδα μεταθέσεων, που είναι υποομάδα της S_n. Δηλαδή υπάρχει ομάδα G' τέτοια ώστε $G \simeq G' \leq S_n$.

- **Παρατήρηση:**

1. Έστω G μία πεπερασμένη ομάδα <u>περιττής</u> τάξης n. Τότε υπάρχει ομάδα G' τέτοια ώστε $G \simeq G' \leq A_n$.

- ***Ορισμός απλής ομάδας***:

Μία ομάδα λέγεται απλή εάν δεν έχει γνήσιες μη-τετριμμένες κανονικές υποομάδες.

- **Παρατηρήσεις:**

1. Εάν G είναι μία απλή ομάδα και $H \lhd G$, τότε $H = G$ ή $H = \{e_G\}$.
2. Η εναλλάσσουσα ομάδα A_n των άρτιων μεταθέσεων είναι απλή για $n = 3$ και $n \geq 5$.
3. Για $n = 3$ και $n \geq 5$, οι κανονικές υποομάδες της S_n είναι οι S_n, A_n και $\{e\}$.

4. Οι κανονικές υποομάδες της S_4 είναι οι S_4, A_4, $K_4 = V$ (ομάδα του Klein) και $\{e\}$.

- **Ορισμός κέντρου ομάδας**:

Κέντρο $Z(G)$ μίας ομάδας $\langle G,* \rangle$ είναι το σύνολο των στοιχείων της G που αντιμετατίθενται με κάθε άλλο στοιχείο της G. Δηλαδή $Z(G) = \{z \in G \mid z*g = g*z \ \forall g \in G\}$.

- **Παρατηρήσεις:**

1. $Z(G) \lhd G$.
2. $Z(S_n) = \{e\}$, για $n \geq 3$.
3. Έστω ομάδα G. Ισχύει το εξής κριτήριο: Η G είναι αβελιανή αν και μόνο αν η $G/Z(G)$ είναι κυκλική.

- **Η διεδρική ομάδα**:

Για $n \geq 3$, η D_n είναι η ομάδα συμμετριών ενός κανονικού n-γώνου. Η D_n αποτελείται από n στροφές (γύρω από το κέντρο του) και n ανακλάσεις (ως προς τις ευθείες που διέρχονται από μία κορυφή και το κέντρο του). Συνεπώς $|D_n| = 2n$. Οι n στροφές αποτελούν κυκλική υποομάδα της D_n και κάθε ανάκλαση έχει τάξη 2.

Εάν $r \in D_n$ είναι η στροφή κατά $2\pi/n$ και $s \in D_n$ είναι μία ανάκλαση, τότε $|r| = n, |s| = 2$ και $srs = r^{-1}$. Έτσι λοιπόν:

$$D_n = \{\langle r,s \rangle \mid |r| = n, \ |s| = 2, \ srs = r^{-1}\}.$$

Ακόμη, εάν θέσουμε $r = ts$, τότε ισοδύναμα:

$$D_n = \{\langle t,s \rangle \mid |t| = |s| = 2, \ |ts| = |st| = n\}.$$

[*Στα επόμενα μαθήματα –συνήθως- θα παραλείπεται το σύμβολο της πράξης μίας ομάδας, δηλαδή για τυχόντα στοιχεία* $a,b \in \langle G,* \rangle$ *θα γράφουμε* $ab \in G$ *και θα εννοείται ότι* $ab \equiv a*b$.]

Μάθημα 2ο (Πέμπτη, 24/4/2014)

[*Εισαγωγή στην έννοια της δράσης ομάδας*]:

- **Ορισμός δράσης ομάδας σε σύνολο**:

Έστω X ένα –μη κενό- σύνολο και G μία ομάδα. Δράση της G πάνω στο σύνολο X ονομάζεται μία απεικόνιση $*: G\times X \to X$, τέτοια ώστε να ικανοποιούνται τα εξής:

i. $e*x = x,\ \forall x \in X$.

ii. $(g_1 g_2)*x = g_1*(g_2*x),\ \forall x \in X$ και $\forall g_1, g_2 \in G$.

- **Παρατηρήσεις:**

1. Το X θα λέμε τότε ότι είναι ένα G-σύνολο.
2. Συνήθως θα παραλείπεται το σύμβολο $*$ της δράσης, και θα γράφουμε gx αντί του $g*x$.
3. Κάθε αριστερή δράση gx επάγει δεξιά δράση xg^{-1} (και αντίστροφα). Πράγματι, για τις δύο ιδιότητες της δεξιάς δράσης θα είχαμε $xe = x$, $(g_1 g_2)*x = x(g_1 g_2)^{-1} = x\left(g_2^{-1} g_1^{-1}\right) = \left(xg_2^{-1}\right)g_1^{-1} = g_1*\left(xg_2^{-1}\right) = g_1*(g_2*x)$.
4. Έστω η δράση μίας ομάδας G σε ένα σύνολο X. Τότε η δράση αυτή επάγει έναν ομομορφισμό $\phi: G \to S(X)$. Πράγματι, εάν η G δρα επί του X, τότε $\forall g \in G$ η απεικόνιση $\rho_g: X \to X$, $x \to gx$ είναι 1-1 και επί, δηλαδή ορίζει μία μετάθεση των στοιχείων του συνόλου X. Η ρ_g είναι 1-1, αφού $\forall x_1, x_2 \in X$ έχουμε ότι $gx_1 = gx_2 \Rightarrow \Rightarrow g^{-1}(gx_1) = g^{-1}(gx_2) \Rightarrow \left(g^{-1}g\right)x_1 = \left(g^{-1}g\right)x_2 \Rightarrow x_1 = x_2$. Η ρ_g είναι επίσης επί, αφού $\forall x \in X$ έχουμε ότι $g\left(g^{-1}x\right) = x$. Ακόμη, $\rho_{g_1 g_2}(x) = (g_1 g_2)x = g_1(g_2 x) = \rho_{g_1}\left(\rho_{g_2}(x)\right)$, δηλαδή $\rho_{g_1 g_2} = \rho_{g_1} \circ \rho_{g_2}$ και συνεπώς ο ϕ είναι όντως ομομορφισμός.
5. Εάν ο παραπάνω ομομορφισμός ϕ είναι μονομορφισμός, δηλαδή εάν $\ker\phi = 1$, τότε η δράση λέγεται <u>τέλεια δράση</u>. Με άλλα λόγια, μία δράση είναι τέλεια όταν $g*x = x,\ \forall x \in X \Leftrightarrow g = e$ ή ισοδύναμα $g_1*x = g_2*x,\ \forall x \in X \Leftrightarrow g_1 = g_2$.

- **Παραδείγματα**:

1. Έστω μία ομάδα G. Θεωρούμε τη δράση $*: G\times G \to G$, $g*x \to gx$, δηλαδή τη δράση της G στον εαυτό της με αριστερό πολλαπλασιασμό. Τότε ο επαγόμενος ομομορφισμός $\phi: G \to S(G)$ είναι μονομορφισμός, αφού $gx = x,\ \forall x \in G \Leftrightarrow g = e$ (δηλαδή η δράση είναι τέλεια). Από το 1ο Θεώρημα ισομορφισμών έπεται τότε ότι η G είναι ισόμορφη με μία ομάδα

μεταθέσεων, δηλαδή $G \simeq G' \leq S_{|G|}$. Ουσιαστικά, η παραπάνω δράση αποτελεί την απόδειξη του Θεωρήματος του Cayley (ότι κάθε ομάδα G είναι ισόμορφη με μία ομάδα μεταθέσεων).

2. Η συμμετρική ομάδα S_n δρά επί του συνόλου $X = \{1,2,...,n\}$ με φυσικό τρόπο.
3. Η ομάδα $G = (\mathbb{R}^n, +)$ δρα επί του $\mathbb{R}^n$ με τη δράση $* : G x \mathbb{R}^n \to \mathbb{R}^n$, $v * x \to v + x$.
4. Η γενική γραμμική ομάδα $GL_n(F)$ δρα επί του F^n με τον αριστερό πολλαπλασιασμό πίνακα επί διάνυσμα, $A * x \to Ax$.
5. Έστω $F[x_1, x_2, ..., x_n]$ ένας δακτύλιος πολυωνύμων. Η S_n δρά επί του $F[x_1, x_2, ..., x_n]$ έτσι ώστε για κάθε πολυώνυμο $f \in F[x_1, x_2, ..., x_n]$, $\sigma * f(x_1, x_2, ..., x_n) \to f\left(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, ..., x_{\sigma^{-1}(n)}\right)$.
6. Έστω V ένας F-διανυσματικός χώρος, $\dim V = n$ και $\{v_1, v_2, ..., v_n\}$ μία βάση του. Τότε $\forall v \in V \quad v = \sum_{i=1}^{n} \lambda_i v_i$, $\lambda_i \in F$ και η S_n δρα επί του V, $\sigma * v = \sigma * \left(\sum_{i=1}^{n} \lambda_i v_i \right) \to \sum_{i=1}^{n} \lambda_i v_{\sigma(i)}$.
7. Έστω μία ομάδα G. Θεωρούμε τη δράση $* : GxG \to G$, $g * x \to gxg^{-1}$. Η δράση αυτή λέγεται <u>δράση συζυγίας</u>.

Μάθημα 3ο (Τετάρτη, 30/4/2014)

[*Τροχιές, σταθεροποιούσες ομάδες, εξίσωση κλάσεων*]:

- **Παρατήρηση:**

1. Έστω X ένα G-σύνολο. Τότε, εάν $x,y \in X$, ορίζουμε $x \sim y \Leftrightarrow \exists g \in G$ τέτοιο ώστε $gx = y$. Η σχέση $\sim$ ορίζει μία σχέση ισοδυναμίας.

- **Ορισμός τροχιάς**:

Έστω X ένα G-σύνολο. Οι κλάσεις ισοδυναμίας που ορίζονται από τη σχέση $\sim$ της προηγούμενης παρατήρησης ονομάζονται τροχιές στο X υπό την G. Η τροχιά T_x (κλάση ισοδυναμίας) που περιέχει κάποιο $x \in X$ λέγεται τροχιά του x.

- **Παρατηρήσεις:**

1. Ουσιαστικά $T_x = \{gx \mid g \in G\}$.
2. Η τροχιά T_x είναι το μικρότερο υποσύνολο του X που περιέχει το x και παραμένει αναλλοίωτο από τη δράση της G, δηλαδή $\forall y \in T_x$ και $\forall g \in G$ ισχύει ότι $gy \in T_x$.
3. Αφού κάθε σχέση ισοδυναμίας σε ένα σύνολο ορίζει μία διαμέριση του συνόλου αυτού, έπεται ότι $X = \dot{\bigcup}_{x \in X} T_x$.
4. Θεωρούμε το σύνολο $\mathrm{Stab}(x) \equiv G(x) \equiv G_x = \{g \in G \mid gx = x\}$, για κάποιο $x \in X$. Τότε $G_x \leq G$ και η G_x ονομάζεται <u>σταθεροποιούσα ομάδα</u> (σταθεροποιητής) του x. Η G_x είναι πράγματι υποομάδα της G, αφού $e \in G_x$, αν $g_1, g_2 \in G \Rightarrow (g_1 g_2)x = g_1(g_2 x) = g_1 x = x \Rightarrow g_1 g_2 \in G$ και αν $g \in G \Rightarrow gx = x \Rightarrow g^{-1}(gx) = g^{-1}x \Rightarrow (g^{-1}g)x = g^{-1}x \Rightarrow g^{-1}x = x \Rightarrow g^{-1} \in G_x$.
5. Στην περίπτωση της δράσης με συζυγία, η σταθεροποιούσα ομάδα του x ονομάζεται <u>κεντροποιούσα ομάδα</u> (κεντροποιητής) του x και συμβολίζεται με $C_G(x)$. Επίσης, η τροχιά T_x ονομάζεται <u>κλάση συζυγίας</u> και αν $x \sim y \Leftrightarrow T_x = T_y$, τότε τα x και y είναι συζυγή.
6. Θεωρούμε την εξής δράση μίας ομάδας G στο σύνολο των υποομάδων της: $*: GxX \to X$, $gH \to g^{-1}Hg$, όπου $X = \{H \mid H \leq G\}$. Τότε η σταθεροποιούσα ομάδα της $H \leq G$ ονομάζεται <u>κανονικοποιούσα ομάδα</u> (κανονικοποιητής) της H και συμβολίζεται με $N_G(H)$. Ισχύει ότι $H \lhd N_G(H) \leq G$ και μάλιστα η $N_G(H)$ είναι η μεγαλύτερη υποομάδα της G στην οποία η H είναι κανονική.

- **Θεώρημα:**

Έστω X ένα G-σύνολο και $x \in X$. Τότε $|T_x| = |G : G_x|$.

Απόδειξη:

Υπάρχει αμφιμονοσήμαντη αντιστοιχία από την τροχιά του x στα αριστερά σύμπλοκα της G_x στη G, $\phi : T_x \to G/G_x$, $gx \to gG_x$.

- **Παραδείγματα**:

1. Θεωρούμε τη δράση της S_3 στο $X = \{1,2,3,4,5\}$. Τότε $T_1 = T_2 = T_3 = \{1,2,3\}$, $T_4 = \{4\}$ και $T_5 = \{5\}$.
2. Θεωρούμε τη δράση $* : S_3 x S_3 \to S_3$, $gx \to g^{-1}xg$. Τότε $T_e = \{e\}$, $T_{(12)} = T_{(13)} = T_{(23)} = \{(12),(13),(23)\}$ και $T_{(123)} = T_{(132)} = \{(123),(132)\}$, καθώς ουσιαστικά κάθε τροχιά αποτελείται από συζυγείς μεταθέσεις – δηλαδή μεταθέσεις που έχουν τον ίδιο τύπο.
3. Έστω $H \leq G$. Θεωρούμε τη δράση $* : GxG/H \to G/H$, $g * xH \to gxH$, Τότε $T_{xH} = \{gxH \mid g \in G\} = G/H$. Ο επαγόμενος ομομορφισμός $\phi : G \to S(G/H)$ έχει πυρήνα ίσο με $\ker\phi = \{g \in G \mid \phi(g) = e\} = \{g \in G \mid gxH = xH \ \forall x \in G\} =$ $= \{g \in G \mid x^{-1}gx \in H \ \forall x \in G\} = \{g \in G \mid g \in x^{-1}Hx \ \forall x \in G\} = \bigcap_{x \in G} x^{-1}Hx \lhd G$.

   Μάλιστα, η $\bigcap_{x \in G} x^{-1}Hx$ είναι η μεγαλύτερη κανονική υποομάδα της G που περιέχεται στην H.

- **Θεώρημα:**

Έστω G μια ομάδα και H υποομάδα της G πεπερασμένου δείκτη $|G : H| = \delta_H$. Τότε, υπάρχει κανονική υποομάδα K της G πεπερασμένου δείκτη $|G : K| = \delta_K$, η οποία περιέχεται στην H και είναι τέτοια ώστε $\delta_H \mid \delta_K$ και $\delta_K \mid \delta_H!$.

Απόδειξη:

Θεωρούμε τον ομομορφισμό του προηγούμενου παραδείγματος 3. Τότε έχουμε το ζητούμενο για $K = \bigcap_{x \in G} x^{-1}Hx$. Πράγματι $\bigcap_{x \in G} x^{-1}Hx \leq H$ και $\bigcap_{x \in G} x^{-1}Hx \lhd G$. Τότε, από το Θεώρημα του Lagrange έπεται ότι $|G : K| = |G : H| \cdot |H : K| \Rightarrow \delta_K = \delta_H \cdot |H : K|$ $\Rightarrow \delta_H \mid \delta_K$, ενώ $G/K \simeq \phi(G) \leq S(G/H) \simeq S_{|G/H|} \equiv S_{\delta_H}$, δηλαδή $|G/K| \mid |S_{\delta_H}| \Rightarrow \delta_K \mid \delta_H!$.

- **Πόρισμα 1:**

Έστω G μια πεπερασμένη ομάδα και H γνήσια υποομάδα της G δείκτη $|G : H| = \delta_H$. Αν $|G| \nmid \delta_H!$, τότε η G δεν είναι απλή.

- **Πόρισμα 2:**

Έστω G μια πεπερασμένη ομάδα και p ο μικρότερος πρώτος αριθμός που διαιρεί την $|G|$. Αν υπάρχει $H \le G$ τέτοια ώστε $|G:H| = p$, τότε $H \lhd G$.

- **Παρατηρήσεις:**

1. Θεωρούμε τη δράση $*: GxX \to X$, $g * x \to gx$. Τότε $G_{gx} = g^{-1}G_x g \quad \forall g \in G$ και $\forall x \in X$.
2. Μία δράση $*: GxX \to X$ ονομάζεται <u>μεταβατική δράση</u> εάν υπάρχει μόνο μία τροχιά, δηλαδή εάν $x \sim y \Leftrightarrow \forall x, y \in X$. Τότε το σύνολο X λέγεται G-ομογενές σύνολο.
3. Εάν X είναι ένα G-ομογενές σύνολο, τότε υπάρχει $H \le G$ τέτοια ώστε να υπάρχει αμφιμονοσήμαντη απεικόνιση $\phi: G/H \to X$.
4. Έχουμε δείξει ότι $X = \dot{\bigcup_{x \in X}} T_x$ και ότι $|T_x| = |G:G_x|$. Δηλαδή $|X| = \sum_{x \in T} |G:G_x|$, όπου T είναι ένα σύνολο αντιπροσώπων των τροχιών της δράσης. Ιδιαιτέρως, εάν η G είναι πεπερασμένη ομάδα, τότε $|X| = \sum_{x \in T} \frac{|G|}{|G_x|}$.

- **Εφαρμογές:**

1. Έστω $X = \{1,2,\ldots,n\}$ και $B_m = \{P \subseteq X \,|\, |P| = m\}$. Θεωρούμε τη φυσική δράση της S_n στο σύνολο B_m. Η δράση αυτή είναι μεταβατική, αφού κάθε στοιχείο της B_m διατρέχει όλα τα άλλα υπό τη δράση της S_n. Δηλαδή $\forall x \in B_m$ υπάρχει μία τροχιά T_x και επομένως $|B_m| = \sum_{x \in T} \frac{|S_n|}{|G_x|} \Rightarrow |B_m| = \frac{|S_n|}{|G_x|}$, για τυχόν $x \in B_m$ (αφού όλα έχουν την ίδια τροχιά). Όμως $G_x = \{s \in S_n \,|\, s * x = x\}$, δηλαδή το G_x αποτελείται από όλες εκείνες τις μεταθέσεις που αφήνουν σταθερό το σύνολο $x \in B_m$. Το πλήθος αυτών των μεταθέσεων είναι $|G_x| = m!(n-m)!$, αφού κάθε τέτοια μετάθεση είτε μεταθέτει τα m στοιχεία του $x \in B_m$ (οπότε υπάρχουν $m!$ τέτοιες) είτε μεταθέτει τα $(n-m)$ στοιχεία του $X \setminus x$ (οπότε υπάρχουν $(n-m)!$ τέτοιες). Τελικά $|B_m| = \frac{|S_n|}{|G_x|} \Rightarrow |B_m| = \frac{n!}{m!(n-m)!}$.
2. Έστω G πεπερασμένη ομάδα και H, K υποομάδες της G. Θεωρούμε τη δράση της H στα αριστερά σύμπλοκα της K, G/K, $*: HxG/K \to G/K$, $h * gK \to hgK$. Έστω T_K η τροχιά του K. Τότε $T_K = \{hK \,|\, h \in H\} = HK$. Δηλαδή, στην ομάδα G/K η T_K διατρέχει όλα τα στοιχεία του HK, από το οποίο έπεται ότι $|T_K| = \frac{|HK|}{|K|}$. Ακόμη, $H_K = \{h \in H \,|\, hK = K\,|\} = \{h \in H \,|\, h \in K\,|\} = H \cap K$. Συνεπώς $|T_K| = |H:H_K| \Rightarrow |T_K| = \frac{|H|}{|H_K|} \Rightarrow \frac{|HK|}{|K|} = \frac{|H|}{|H \cap K|} \Rightarrow |HK| = \frac{|H| \cdot |K|}{|H \cap K|}$.

Μάθημα 4ο (Πέμπτη, 8/5/2014)

[*Εφαρμογές*]:

- **Παρατηρήσεις:**

1. Θεωρούμε τη δράση της G στο X, $*: GxX \to X$, $g*x \to gx$. Έχουμε πει ότι αν $x,y \in X$, ορίζουμε $x \sim y \Leftrightarrow \exists g \in G$ τέτοιο ώστε $gx = y$. Η σχέση $\sim$ ορίζει μία σχέση ισοδυναμίας. Πράγματι, έστω η τροχιά του $x \in X$, $T_x = \{gx \mid g \in G\}$. Ισχυρισμός: αν $x,y \in X$, τότε είτε $T_x = T_y$ είτε $T_x \cap T_y = \varnothing$. Πράγματι, εάν $T_x \cap T_y \neq \varnothing$ τότε $\exists z \in X$ τέτοιο ώστε $z \in T_x \cap T_y$. Δηλαδή $z \in T_x \Rightarrow \exists g_1 \in G : g_1 x = z$ και $z \in T_y \Rightarrow \exists g_2 \in G : g_2 y = z$. Τότε $g_1 x = z = g_2 y \Rightarrow$ $\Rightarrow g_1 x = g_2 y \Rightarrow x = g_1^{-1} g_2 y$. Επομένως αν $h \in T_x$ τότε $\exists g \in G : gx = h \Rightarrow$ $\Rightarrow \left(g g_1^{-1} g_2\right) y = h \Rightarrow h \in T_y$. Άρα $T_x \subseteq T_y$. Ομοίως δείχνουμε ότι $T_y \subseteq T_x$ και τελικά $T_x = T_y$. Επομένως ο ισχυρισμός είναι ορθός, το οποίο αποδεικνύει ότι όντως η σχέση $\sim$ ορίζει μία σχέση ισοδυναμίας, αφού οι τροχιές ορίζουν μία διαμέριση του συνόλου X. Οι τροχιές είναι επομένως οι κλάσεις της ισοδυναμίας αυτής.
2. Υπενθυμίζουμε ότι, εάν T είναι ένα σύνολο αντιπροσώπων των τροχιών της δράσης, τότε $|X| = \left|\dot{\bigcup_{x \in X}} T_x\right| = \sum_{x \in T} |T_x| = \sum_{x \in T} |G : G_x| = \sum_{x \in T} \frac{|G|}{|G_x|}$, όπου η τελευταία ισότητα ισχύει μόνο στην περίπτωση που η G είναι πεπερασμένη ομάδα. Η εξίσωση $X = \sum_{x \in T} \frac{|G|}{|G_x|}$ ονομάζεται εξίσωση κλάσεων.
3. Η πλέον χρήσιμη μορφή της εξίσωσης κλάσεων είναι η $|X| = |\mathrm{Fix}(X)| + \sum_{\substack{x \in T \\ x \notin \mathrm{Fix}(X)}} \frac{|G|}{|G_x|}$, όπου με $\mathrm{Fix}(X)$ έχουμε συμβολίσει τα $x \in X$ που παραμένουν σταθερά υπό τη δράση της G, δηλαδή $\mathrm{Fix}(X) \equiv X^G = \{x \in X \mid gx = x \ \forall g \in G\}$. Με άλλα λόγια, το σύνολο $\mathrm{Fix}(X)$ αποτελείται από εκείνα τα $x \in X$ που η τροχιά τους είναι μονοσύνολο, δηλαδή $\mathrm{Fix}(X) = \{x \in X \mid T_x = \{x\}\}$.
4. Ιδιαίτερα, αν θεωρήσουμε τη G να δρα στον εαυτό της με συζυγία, τότε $\mathrm{Fix}(G) = Z(G)$. Πράγματι, έχουμε ότι $\mathrm{Fix}(G) = \{x \in G \mid gxg^{-1} = x \ \forall g \in G\} =$ $= \{x \in G \mid gx = xg \ \forall g \in G\} = \{x \in G \mid x \in Z(G)\} = G \cap Z(G) = Z(G)$. Επομένως η εξίσωση κλάσεων στην περίπτωση αυτή λαμβάνει τη μορφή $|G| = |Z(G)| + \sum_{\substack{x \in T \\ x \notin Z(G)}} \frac{|G|}{|C_G(x)|}$, όπου $C_G(x)$ είναι ο κεντροποιητής του x, δηλαδή $C_G(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}$.

5. Ισχύει ότι $Z(G)=\bigcap_{x\in G} C_G(x)$.

- ***Ορισμοί*:**

1. Μία ομάδα G λέγεται p-ομάδα εάν $|G|=p^n$, για κάποιο $n\in\mathbb{N}$.
2. Μία δράση $*: GxX\to X$ λέγεται <u>ελεύθερη δράση</u>, αν δεν υπάρχουν $x\in X$ και $g\in G$, $g\neq e$, τέτοια ώστε $gx=x$. Με άλλα λόγια, εάν για κάποιο $x\in X$ ισχύει $gx=x$, τότε αναγκαστικά έπεται ότι $g=e$.

- **Εφαρμογές:**

1. Έστω G μία p-ομάδα. Τότε να δειχθεί ότι $Z(G)\neq\{e\}$.

   <u>Απάντηση:</u>
   Έχουμε ότι $\exists n\in\mathbb{N}: |G|=p^n$. Θεωρούμε την εξίσωση κλάσεων με τη δράση της G στον εαυτό της με συζυγία, δηλαδή την $|G|=|Z(G)|+\sum_{\substack{x\in T\\ x\notin Z(G)}}\frac{|G|}{|C_G(x)|}\Rightarrow |Z(G)|=|G|-\sum_{\substack{x\in T\\ x\notin Z(G)}}\frac{|G|}{|C_G(x)|}$. Όμως $\forall x\in G: x\notin Z(G)$, η $C_G(x)$ είναι γνήσια υποομάδα της G. Επομένως $|C_G(x)|=p^m$, $m<n$. Δηλαδή $\frac{|G|}{|C_G(x)|}=\frac{p^n}{p^m}=p^{n-m}\geq p$. Έχουμε λοιπόν ότι $p\,|\,|G|$, $p\,|\,\frac{|G|}{|C_G(x)|}$ $\forall x\in G: x\notin Z(G)\Rightarrow p\,|\,\sum_{\substack{x\in T\\ x\notin Z(G)}}\frac{|G|}{|C_G(x)|}$, και τελικά $p\,|\,|G|-\sum_{\substack{x\in T\\ x\notin Z(G)}}\frac{|G|}{|C_G(x)|}\Rightarrow p\,|\,|Z(G)|$.
   Έπεται ότι $p\leq|Z(G)|$. Ιδιαιτέρως $|Z(G)|>1\Rightarrow Z(G)\neq\{e\}$.

2. Έστω η ομάδα $G=(\mathbb{R},+)$ και η δράση της στο σύνολο $\mathbb{R}^2$, $\delta: G\times\mathbb{R}^2\to\mathbb{R}^2$. Εάν $\mathbf{v}\in\mathbb{R}^2$, $\theta\in G$, τότε $\theta\cdot\mathbf{v}\equiv$στροφή του $\mathbf{v}$ κατά γωνία θ αντίθετη των δεικτών του ρολογιού. Να δειχθεί ότι η δ είναι όντως δράση και να βρεθούν οι τροχιές και οι σταθεροποιητές.

   <u>Απάντηση:</u>
   Οι τροχιές είναι οι κύκλοι με κέντρο το $(0,0)$ και οι σταθεροποιητές είναι τα σύνολα $\{2k\pi,\ k\in\mathbb{Z}\}$.

3. Να δοθούν 3 παραδείγματα τέλειας δράσης και 3 παραδείγματα μη-τέλειας δράσης.
4. Να δοθούν 3 παραδείγματα μεταβατικής δράσης και 3 παραδείγματα μη-μεταβατικής δράσης.
5. Έστω $\delta: G\times X\to X$ μία μεταβατική και τέλεια δράση. Έπεται ότι υπάρχει 1-1 και επί απεικόνιση από την ομάδα G στο σύνολο X;

Απάντηση:

Εάν $\delta : G \times X \to X$ είναι μία μεταβατική και τέλεια δράση, δεν έπεται υποχρεωτικά ότι υπάρχει $f : G \xrightarrow[\text{επί}]{1\text{-}1} X$. Για παράδειγμα, εάν $G = S_3$, $X = \{1,2,3\}$ και δ η φυσική δράση της G στο σύνολο X, τότε η δ είναι μεταβατική και τέλεια. Ωστόσο δεν υπάρχει $f : S_3 \xrightarrow[\text{επί}]{1\text{-}1} X$, αφού $|S_3| = 6$ και $|X| = 3$.

Όμως, ισχύει ότι εάν $\delta : G \times X \to X$ είναι μία μεταβατική, τέλεια και *ελεύθερη* δράση, τότε υπάρχει $f : G \xrightarrow[\text{επί}]{1\text{-}1} X$.

6. Έστω δ η δράση της $GL_2(\mathbb{R})$ στο $\mathbb{R}^2$ με τον αριστερό πολλαπλασιασμό (πίνακας χ διάνυσμα). Να ελεγχθεί εάν η δράση είναι τέλεια/μεταβατική/ελεύθερη. Ακόμη, να βρεθούν οι τροχιές και οι σταθεροποιητές.

   Απάντηση:

   Οι τροχιές είναι το $\mathbb{R}^2$ και το μηδενικό διάνυσμα, αφού για κάθε μη-μηδενικά διανύσματα $a, b \in \mathbb{R}^2$ υπάρχει αντιστρέψιμος πίνακας $A \in GL_2(\mathbb{R})$, τέτοιος ώστε $A \cdot a = b \Leftrightarrow A^{-1} \cdot b = a$. Ο σταθεροποιητής (για ένα μη-μηδενικό διάνυσμα) είναι ο μοναδιαίος πίνακας.

7. Έστω πεπερασμένη ομάδα G τάξεως $|G| = n$, η οποία δρα ελεύθερα επί της G με τον αριστερό πολλαπλασιασμό. Άρα κάθε υποομάδα της G δρα ελεύθερα επί της G. Εάν λοιπόν $g \in G$, τότε η $H = \langle g \rangle$ δρα ελεύθερα επί της G. Ποιες είναι οι τροχιές και οι σταθεροποιούσες ομάδες της δράσεως αυτής;

   Απάντηση:

   Οι τροχιές είναι τα δεξιά σύμπλοκα της H και η σταθεροποιούσα ομάδα είναι το ταυτοτικό στοιχείο της H (που είναι και ταυτοτικό στοιχείο της G).

8. Στην προηγούμενη άσκηση, θεωρούμε την κανονική δράση αναπαράστασης μεταθέσεων του g, $\lambda_g : G \to G$, $h \to gh$, και θέτουμε $|H| = \delta \Rightarrow \frac{|G|}{|H|} = n/\delta$. Τότε τα δεξιά σύμπλοκα της H (που είναι και οι τροχιές της δράσης) ορίζουν μία διαμέριση της G και επομένως $|G| = \bigcup_{i=1}^{n/\delta} Hh_i$. Άρα το λ_g ορίζει μία μετάθεση της G και αναλύεται σε γινόμενο n/δ ξένων κύκλων. Να

δειχθεί ότι εάν ο δ είναι άρτιος και ο n/δ περιττός, τότε η G περιέχει μία κανονική υποομάδα δείκτου 2 (ιδιαίτερα, η G δεν είναι απλή).

<u>Απάντηση:</u>

Υπάρχει ομομορφισμός $sgn : S_n \to \{\pm 1\}$, όπου $\ker(sgn) = A_n$. Τότε $G \xrightarrow{L_g} S_n \xrightarrow{sgn} \{\pm 1\}$ και συνεπώς ορίζεται ο ομομορφισμός $(sgn \circ L_g) := \phi : G \to \{\pm 1\}$, όπου $L_g : G \to S_n$, $g \to \lambda_g$. Από το 1ο Θεώρημα ισομορφισμών έχουμε ότι $G/\ker\phi \simeq \phi(G) \leq Z_2$, δηλαδή $G/\ker\phi \simeq Z_2$ ή $G/\ker\phi \simeq \{1\}$. Δηλαδή $\ker\phi \lhd G$ και είτε $[G : \ker\phi] = 2$ είτε $[G : \ker\phi] = 1 \Leftrightarrow \ker\phi = G$. Αρκεί επομένως να δείξουμε ότι $[G : \ker\phi] \neq 1 \Leftrightarrow G/\ker\phi \neq \{1\}$. Καταλήγουμε ότι αρκεί να βρούμε κάποιο $g \in G$: το λ_g να αντιστοιχεί σε περιττή μετάθεση, αφού τότε $\phi(g) = -1 \Rightarrow \phi(G) = \{\pm 1\} \Rightarrow \phi(G) \simeq Z_2 \Rightarrow G/\ker\phi \simeq Z_2 \Rightarrow |G : \ker\phi| = 2$.

Εάν $\sigma \in S_n$ και η ανάλυση της σ σε ξένους κύκλους είναι $\sigma = \sigma_1\sigma_2 \cdots \sigma_s$, όπου s είναι το πλήθος των ξένων κύκλων *ίσου* μήκους, τότε $sgn(\sigma) = (-1)^{n-s}$. Πράγματι, $n - s = \sum_{i=1}^{s}(n_i - 1)$ και $(n_i - 1)$ είναι το πλήθος των αντιμεταθέσεων του i κύκλου μήκους $(n_i - 1)$, οπότε $\sum_{i=1}^{s}(n_i - 1)$ είναι το πλήθος των αντιμεταθέσεων της σ.

Στην περίπτωσή μας, αν περιοριστούμε στα $g \in H$, τότε η μετάθεση $\sigma \in S_n$ που αντιστοιχεί στη λ_g έχει κυκλική πάρασταση $\sigma = \sigma_1\sigma_2 \cdots \sigma_s$, όπου $s = n/\delta$, αφού κάθε ξένος κύκλος αντιστοιχεί σε μία τροχιά της δράσης, και κάθε ξένος κύκλος έχει μήκος δ. Δηλαδή $sgn(\sigma) = (-1)^{n-s} = (-1)^{n-n/\delta} = -1$, καθώς $n = \delta \cdot (n/\delta) \Rightarrow n$ άρτιος και n/δ περιττός, άρα $n - n/\delta$ περιττός. Επομένως η $\sigma \in S_n$ είναι περιττή μετάθεση και, σύμφωνα με την ανάλυση που έχει προηγηθεί, έπεται ότι $|G : \ker\phi| = 2$. Άρα ο $\ker\phi$ είναι -γνήσια- κανονική υποομάδα της G δείκτου 2. Ιδιαίτερα, η G δεν είναι απλή.

Μάθημα 5ο (Πέμπτη, 15/5/2014)

[*Εισαγωγή στα Θεωρήματα του Sylow*]:

- **Θεώρημα του Cauchy:**

Αν G είναι μια πεπερασμένη ομάδα, που η τάξη της διαιρείται από κάποιον πρώτο αριθμό p, τότε υπάρχει τουλάχιστον ένα στοιχείο της G που έχει τάξη p. Δηλαδή $p\,|\,|G| \Rightarrow \exists g \in G:\ |g| = p$.

1η Απόδειξη:

Εφαρμόζουμε επαγωγή στην τάξη της $|G| = n$. Έχουμε ότι $p\,|\,n \Rightarrow p \le n$. Αν $p = n$, τότε $\forall g \in G$ ισχύει ότι $|g| = p$.

Υποθέτουμε πρώτα ότι η G είναι αβελιανή. Θεωρούμε μια μέγιστη γνήσια υποομάδα N της G. Αφού η G είναι αβελιανή, έπεται ότι $N \lhd G$. Μπορούμε να θεωρήσουμε ότι η G δεν είναι κυκλική (αν ήταν κυκλική θα υπήρχε μοναδική υποομάδα της τάξης p, και κάθε στοιχείο της υποομάδας αυτής θα είχε τάξη p). Εάν $p\,|\,|N|$, τότε επαγωγικά το Θεώρημα ισχύει για την N, δηλαδή $\exists g \in N:\ |g| = p \Rightarrow \exists g \in G:\ |g| = p$. Εάν $p \not| |N|$, θεωρούμε ένα $g \in G - N$, οπότε $\langle x \rangle N = G$, καθώς $\langle x \rangle N = N \langle x \rangle$ (έχουμε υποθέσει ότι η G είναι αβελιανή) και συνεπώς η $\langle x \rangle N$ είναι υποομάδα της G που περιέχει γνήσια την μέγιστη υποομάδα N. Επομένως $|G| = |G:N| \cdot |N| \overset{p||G|}{\Rightarrow} p\,|\,|G:N| \cdot |N| \overset{p \not| |N|}{\Rightarrow} p\,|\,|G:N| \Rightarrow p\,|\,|G/N|$. Τότε από επαγωγή $\exists u \in G/N:\ |u| = p \Rightarrow \exists u \in G:\ |uN| = p \Rightarrow \exists u \in G:\ u^p \in N \Rightarrow$ $\Rightarrow \exists u \in G:\ u^p = y,\ y \in N \Rightarrow \exists u \in G:\ \left(u^p\right)^{|y|} = y^{|y|},\ y \in N \Rightarrow \exists u \in G:\ \left(u^{|y|}\right)^p = e$ και θέτοντας $u^{|y|} = g$ έχουμε ότι $\exists g \in G:\ g^p = e \Rightarrow \exists g \in G:\ |g| = p$.

Τώρα υποθέτουμε ότι η G δεν είναι αβελιανή. Θεωρούμε την εξίσωση κλάσεων: $|G| = |Z(G)| + \sum_{\substack{x \in T \\ x \notin Z(G)}} \frac{|G|}{|C_G(x)|}$. Εάν $p\,|\,|Z(G)|$ τότε $\exists g \in Z(G):\ |g| = p \Rightarrow$ $\Rightarrow \exists g \in G:\ |g| = p$, αφού η $Z(G)$ είναι αβελιανή. Εάν $p \not| |Z(G)|$, τότε από την εξίσωση κλάσεων $p \not| |G| - \sum_{\substack{x \in T \\ x \notin Z(G)}} \frac{|G|}{|C_G(x)|} \overset{p||G|}{\Rightarrow} p \not| \sum_{\substack{x \in T \\ x \notin Z(G)}} \frac{|G|}{|C_G(x)|}$, δηλαδή υπάρχει $x \in G$ τέτοιο ώστε $p \not| \frac{|G|}{|C_G(x)|} \overset{p||G|}{\Rightarrow} p\,|\,|C_G(x)|$ και από την επαγωγική υπόθεση $\exists g \in C_G(x):\ |g| = p \Rightarrow \exists g \in G:\ |g| = p$.

2η Απόδειξη (McKay):

Θεωρούμε το σύνολο $X=\left\{\left(g_1,g_2,...,g_p\right)\mid g_1,g_2,...,g_p\in G \text{ και } g_1g_2\cdots g_p=e\right\}$. Όμως: $g_1g_2\cdots g_p=e\Leftrightarrow g_p=\left(g_1g_2\cdots g_{p-1}\right)^{-1}$, το οποίο σημαίνει ότι τα πρώτα $p-1$ στοιχεία της ακολουθίας μπορούν να επιλεγούν αυθαίρετα, ενώ το τελευταίο προκύπτει με μοναδικό τρόπο. Έπεται λοιπόν ότι $|X|=|G|^{p-1}$. Παρατηρούμε επίσης ότι $g_2\cdots g_pg_1=g_1^{-1}\left(g_1g_2\cdots g_p\right)g_1=e\Rightarrow\left(g_2,...,g_p,g_1\right)\in X$. Αυτό ορίζει μία απεικόνιση $\sigma:X\to X$, $\left(g_1,g_2,...,g_p\right)\to\left(g_2,...,g_p,g_1\right)$. Συνεπώς έχουμε μία δράση της $\langle\sigma\rangle$ επί του X, όπου $\langle\sigma\rangle\simeq Z_p$.

Έστω τώρα $x=\left(g_1,g_2,...,g_p\right)\in X$. Τότε $Stab(x)\le\langle\sigma\rangle\simeq Z_p\Rightarrow$ $Stab(x)=\{e\}$ ή $Stab(x)=\langle\sigma\rangle$. Εάν $Stab(x)=\{e\}$, τότε $|T_x|=|\langle\sigma\rangle:\{e\}|=p$. Εάν $Stab(x)=\langle\sigma\rangle$, τότε $|T_x|=|\langle\sigma\rangle:\langle\sigma\rangle|=1$. Τελικά, από την εξίσωση κλάσεων έχουμε ότι $|G|^{p-1}=|X|=\sum_{x\in T}|T_x|=pr+s$ (για κάποια $r,s\in\mathbb{N}$), αφού $\forall x\in X$ είτε $|T_x|=1$ είτε $|T_x|=p$. Άρα $s=|G|^{p-1}-pr\overset{p\|G|}{\Rightarrow}p\mid s\Rightarrow s\ge p\Rightarrow s>1\Rightarrow$ $\exists x\in X:x\ne(e,e,...,e)$ και $|T_x|=1\Rightarrow x=(g,g,...,g)\in X\Rightarrow g^p=e\overset{g\ne e}{\Rightarrow}|g|=p$.

- **Θεώρημα του Sylow:**

Έστω G μια πεπερασμένη ομάδα τάξης $n=p^rm$, όπου p είναι ένας πρώτος αριθμός και $(p,m)=1$. Τότε:

i. Υπάρχει υποομάδα P της G τάξης p^r (μία τέτοια υποομάδα ονομάζεται Sylow p-υποομάδα της G).
ii. Όλες οι Sylow p-υποομάδες της G είναι συζυγείς.
iii. Κάθε p-υποομάδα της G περιέχεται σε μία Sylow p-υποομάδα της G.
iv. Αν n_p είναι το πλήθος των Sylow p-υποομάδων της G, τότε $n_p=1(\mathrm{mod}p)$ και $n_p\mid m$ (το σύνολο των Sylow p-υποομάδων της G συμβολίζεται με $Syl_p(G)$).

- **Παρατήρηση:**

1. Το i. αναφέρεται συχνά ως *1ο Θεώρημα του Sylow*, το iv. ως *2ο Θεώρημα του Sylow*, ενώ τα ii.-iii. αποτελούν το *3ο Θεώρημα του Sylow*.

1η Απόδειξη του i. :

Θεωρούμε την $GL_n\left(Z_p\right)$, η οποία περιέχει τους $n\times n$ αντιστρέψιμους πίνακες με στοιχεία από το σώμα Z_p. Σε κάθε αντιστρέψιμο πίνακα οι στήλες του είναι γραμμικά ανεξάρτητα διανύσματα. Επομένως, η πρώτη στήλη του πίνακα μπορεί να επιλεγεί με p^n-1 τρόπους (αποκλείεται το μηδενικό διάνυσμα), η

δεύτερη στήλη του πίνακα μπορεί να επιλεγεί με $p^n - p$ τρόπους (αποκλείονται τα πολλαπλάσια του διανύσματος της πρώτης στήλης) κ.ο.κ. Τελικά καταλήγουμε ότι $\left|GL_n\left(Z_p\right)\right| = p^{n(n-1)/2}\left(p^n-1\right)\left(p^{n-1}-1\right)\left(p^{n-2}-1\right)\cdots\left(p-1\right) \Rightarrow$ $\left|GL_n\left(Z_p\right)\right| = p^{n(n-1)/2}m$, όπου $(p,m)=1$. Επίσης, θεωρούμε την $U_n\left(Z_p\right) \le GL_n\left(Z_p\right)$, η οποία αποτελείται από τους άνω τριγωνικούς αντιστρέψιμους πίνακες, οι οποίοι έχουν μονάδα στη διαγώνιο. Τότε $\left|U_n\left(Z_p\right)\right| = p^{n(n-1)/2}$. Δηλαδή η $U_n\left(Z_p\right)$ είναι μία Sylow p-υποομάδα της $GL_n\left(Z_p\right)$.

Όμως η G εμφυτεύεται στην $S_{|G|}$, και η $S_{|G|}$ εμφυτεύεται στην $GL_n\left(Z_p\right)$, αφού κάθε μετάθεση αντιστοιχεί σε έναν πίνακα μετάθεσης. Άρα η G είναι ισόμορφη με μία υποομάδα της $GL_n\left(Z_p\right)$ και επιπλέον η $GL_n\left(Z_p\right)$ έχει μία Sylow p-υποομάδα. Το ακόλουθο Λήμμα αποδεικνύει ότι και η G έχει μία Sylow p-υποομάδα.

- **Λήμμα:**

Έστω G μια πεπερασμένη ομάδα και $H \le G$. Υποθέτουμε ότι η G έχει μία Sylow p-υποομάδα και ότι $p \mid |H|$. Τότε και η H έχει μία Sylow p-υποομάδα.

Απόδειξη:

Έστω P μία Sylow p-υποομάδα της G. Θεωρούμε το σύνολο $G/P = \{gP \mid g \in G\}$ και τη δράση της H στο G/P με αριστερό πολλαπλασιασμό $h * gP \to hgP$. Καθώς η P είναι μία Sylow p-υποομάδα της G, έπεται ότι $p \not| |G/P|$. Τότε, από την εξίσωση κλάσεων $|G/P| = \sum_{x \in T} |T_x|$, υπάρχει μία τροχιά O στην G/P με $p \not| |O|$. Έστω $gP \in O$ και $Stab(gP) = Q \le H$. Τότε $\forall q \in Q$ ισχύει $qgP = gP \Rightarrow g^{-1}qg \in P \Rightarrow$ $q \in gPg^{-1}$, δηλαδή $Q \subseteq gPg^{-1}$ και συνεπώς η Q είναι μία p-υποομάδα (αφού $\forall q \in Q \quad \exists p \in P: \quad q = gpg^{-1} \Rightarrow q^{|P|} = \left(gpg^{-1}\right)^{|P|} = gp^{|P|}g^{-1} = geg^{-1} = e$, δηλαδή $|q| \,||P| \Rightarrow p \,||q|$). Έχουμε τελικά ότι $p \not| |O| \Rightarrow p \not| |H:Q| \Rightarrow p \not| \frac{|H|}{|Q|} \overset{p||H|}{\Rightarrow}$ η Q είναι μία Sylow p-υποομάδα της H.

2η Απόδειξη του i. :

Εφαρμόζουμε επαγωγή στην τάξη της $|G| = n$.

Υποθέτουμε πρώτα ότι $p \mid |Z(G)|$. Τότε, από το Θεώρημα του Cauchy η $Z(G)$ έχει στοιχείο τάξης p, δηλαδή έχει υποομάδα τάξης p, έστω N. Προφανώς $N \lhd G$. Από επαγωγική υπόθεση η G/N έχει μία Sylow p-υποομάδα, έστω $\bar{P}$. Όμως $|G/N| = \frac{|G|}{|N|} = \frac{p^r m}{p} = p^{r-1}m$. Θεωρούμε το σύνολο $P = \left\{g \in G \mid gN \in \bar{P}\right\}$. Τότε

$P \le G$ και $N \lhd P$. Άρα υπάρχει επιμορφισμός $\phi : P \to \bar{P}$, $g \to gN$ με $\ker\phi = N$. Από το 1ο Θεώρημα ισομορφισμών έπεται ότι $P/N \simeq \bar{P} \Rightarrow |P/N| = |\bar{P}| \Rightarrow \frac{|P|}{|N|} = |\bar{P}| \Rightarrow$ $\frac{|P|}{p} = p^{r-1} \Rightarrow |P| = p^r$, δηλαδή η P είναι μία Sylow p-υποομάδα της G.

Τώρα υποθέτουμε ότι $p \not| |Z(G)|$. Από την εξίσωση κλάσεων $|G| = |Z(G)| + \sum_{\substack{x \in T \\ x \notin Z(G)}} \frac{|G|}{|C_G(x)|}$ συνεπάγεται ότι $p \not| \sum_{\substack{x \in T \\ x \notin Z(G)}} \frac{|G|}{|C_G(x)|}$, δηλαδή υπάρχει $x \in G$: $x \notin Z(G)$ με $p \not| \frac{|G|}{|C_G(x)|} \Rightarrow p \not| \frac{p^r m}{|C_G(x)|} \Rightarrow p^r \,|\, |C_G(x)|$. Καθώς η $C_G(x)$ είναι γνήσια υποομάδα της G (αφού $x \notin Z(G)$), έπεται από επαγωγική υπόθεση ότι η $C_G(x)$ έχει Sylow p-υποομάδα, έστω P'. Αφού $p^r \,|\, |C_G(x)|$, έπεται ότι $|P'| = p^r$. Αυτό σημαίνει όμως ότι η P' είναι Sylow p-υποομάδα της G.

Μάθημα 6° (Τετάρτη, 21/5/2014)

[*Συνέχεια στα Θεωρήματα του Sylow*]:

Απόδειξη των ii.-iii. :

Έστω P μία Sylow p-υποομάδα της G. Γενικότερα θα δείξουμε ότι αν $H \leq G$ με $|H| = p^k$, $k \leq n$, τότε υπάρχει μία Sylow p-υποομάδα της G, έστω P', τέτοια ώστε $H \leq P' = gPg^{-1}$ για κάποιο $g \in G$.

Παρατηρούμε ότι αν $H \leq N_G(P)$ τότε έπεται ότι $H \leq P$, αφού τότε θα ισχύει $hPh^{-1} = P$, $\forall h \in H$, δηλαδή $hP = Ph$, $\forall h \in H \Rightarrow HP = PH$, το οποίο σημαίνει πως $HP \leq G$ (υπενθυμίζουμε ότι $hp, h_1p_1 \in HP \Rightarrow hp(h_1p_1)^{-1} = hpp_1^{-1}h_1^{-1} \overset{HP=PH}{=} hph_2p_2 \overset{HP=PH}{=} (hh_3)\cdot(p_3p_2) \in HP$). Έχουμε δείξει ότι $|HP| = \dfrac{|H|\cdot|P|}{|H \cap P|}$, δηλαδή η HP είναι p-υποομάδα της G και $P \leq HP$. Αφού όμως η P είναι μία Sylow p-υποομάδα της G, έπεται ότι $P = HP$. Η ισότητα όμως $P = HP$ σημαίνει ότι $H \leq P$.

Θεωρούμε τη δράση της G με συζυγία στο σύνολο $X = \{H \mid H \leq G\}$, δηλαδή το σύνολο των υποομάδων της. Το σύνολο των Sylow p-υποομάδων της G, $Syl_p(G) \subseteq X$, είναι G-αναλλοίωτο. Πράγματι, έστω $P \in Syl_p(G)$, T_P η τροχιά του P και $\{gPg^{-1} \mid g \in G\}$ τα συζυγή του P. Ο κεντροποιητής $G(P)$ του P είναι η κανονικοποιούσα ομάδα του P, δηλαδή $G(P) = N_G(P) = \{g \in G \mid gPg^{-1} = P\}$. Τότε $|T_P| = |G : G(P)| = \dfrac{|G|}{|G(P)|} = \dfrac{|G|}{|N_G(P)|}$. Αφού $P \leq N_G(P)$ έπεται ότι $\dfrac{|G|}{|N_G(P)|} \mid m$, δηλαδή $|T_P| \mid m \Rightarrow |T_P| \neq 0 (\mathrm{mod} p)$.

Θεωρούμε τώρα το σύνολο T_P ως ένα H-σύνολο και, όπως προκύπτει από το επόμενο Λήμμα, έχουμε ότι $|T_P| = |T_P^H| (\mathrm{mod} p) \Rightarrow |T_P^H| \neq 0 (\mathrm{mod} p)$. Αυτό σημαίνει ότι υπάρχει μία συζυγής υποομάδα της P, $P' = gPg^{-1}$ για κάποιο $g \in G$, η οποία είναι H-αναλλοίωτη, δηλαδή $hP'h^{-1} = P'$, $\forall h \in H \Rightarrow H \leq N_G(P')$. Όπως δείξαμε προηγουμένως, έπεται ότι $H \leq P'$.

- Λήμμα:

Έστω G μια p-ομάδα, δηλαδή $|G| = p^n$ για κάποιο $n \in \mathbb{N}$, η οποία δρα σε ένα σύνολο X. Τότε $|X| = |X|^G (\mathrm{mod} p)$.

Απόδειξη:

Από την εξίσωση των κλάσεων έχουμε ότι $|X| = |X^G| + \sum_{\substack{x \in T \\ x \notin X^G}} |T(x)| \Rightarrow$

$|X| = |X^G| + \sum_{\substack{x \in T \\ x \notin X^G}} |G : G(x)| \Rightarrow |X| = |X^G| + \sum_{\substack{x \in T \\ x \notin X^G}} \frac{|G|}{|G(x)|}$. Όμως $\forall x \in G : x \notin X^G$ η $G(x)$ είναι γνήσια υποομάδα της G, δηλαδή $\frac{|G|}{|G(x)|} = 0(\mathrm{mod} p) \Rightarrow \sum_{\substack{x \in T \\ x \notin X^G}} \frac{|G|}{|G(x)|} = 0(\mathrm{mod} p)$.

Συνεπώς, παίρνοντας ισότητα modulo p στην εξίσωση κλάσεων προκύπτει πως $|X| = |X|^G (\mathrm{mod} p)$.

Απόδειξη του iv. :

Έχουμε αποδείξει ότι $n_p = |Syl_p(G)| = \frac{|G|}{|N_G(P)|} \mid m$. Πράγματι, $|G| = p^r m = |P| m$ και $|G| = |N_G(P)| \cdot |G : N_G(P)| = |N_G(P)| n_p$, άρα $|N_G(P)| n_p = |P| m \Rightarrow m = |N_G(P) : P| n_p \Rightarrow n_p \mid m$. Τώρα, έστω $P \in Syl_p(G)$. Τότε $|Syl_p(G)| = |Syl_p(G)^P| (\mathrm{mod} p)$. Όμως $Syl_p(G)^P = P$, δηλαδή $|Syl_p(G)^P| = 1$. Τελικά $n_p = |Syl_p(G)| \Rightarrow n_p = |Syl_p(G)| = |Syl_p(G)^P| (\mathrm{mod} p) \Rightarrow$ $n_p = 1 (\mathrm{mod} p) \Leftrightarrow p \mid n_p - 1$.

- **Θεώρημα:**

Έστω $P \in Syl_p(G)$, όπου G είναι μία πεπερασμένη ομάδα. Τότε $P \lhd G \Leftrightarrow n_p = 1$. Με άλλα λόγια, μία Sylow p-υποομάδα της G είναι κανονική υποομάδα της G αν και μόνο αν είναι η μοναδική Sylow p-υποομάδα της.

Απόδειξη:

Ισχύει ότι η G είναι ισόμορφη με το ευθύ γινόμενο των Sylow p-υποομάδων της αν και μόνο αν $n_p = 1$ για κάθε p.

Πράγματι, έστω $|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, όπου p_i πρώτοι αριθμοί και $n_i \in \mathbb{N}$. Εάν $n_{p_i} = 1 \ \forall p_i$, τότε υπάρχουν μοναδικές Sylow p-υποομάδες της G, έστω P_1, $P_2, \ldots, P_k$. Θεωρώ την απεικόνιση $\phi : P_1 \times P_2 \times \ldots \times P_k \to G$, $(g_1, g_2, \ldots, g_k) \to g_1 g_2 \cdots g_k$, όπου $g_i \in P_i$. Τότε μπορούμε να δείξουμε ότι ο ϕ είναι ισομορφισμός και συνεπώς $G \simeq P_1 \times P_2 \times \ldots \times P_k$. Όμως, καθώς $(|P_i|, |P_j|) = 1 \ \forall i, j \le k$ με $i \ne j$, έπεται ότι $P_i \lhd P_1 \times P_2 \times \ldots \times P_k \ \forall i \le k$, δηλαδή $P_i \lhd G$, $\forall i \le k$.

Για το αντίστροφο, έστω ότι ισχύει $P_i \lhd G, \forall i \le k$. Τότε $P_1 \times P_2 \times \ldots \times P_k \le G$, ενώ επιπλέον ισχύει ότι $|P_1 \times P_2 \times \ldots \times P_k| = |P_1| \cdot |P_2| \cdots |P_k| = |G|$. Από αυτό συμπεραίνουμε ότι $G \simeq P_1 \times P_2 \times \ldots \times P_k$. Είναι τώρα άμεσο ότι $n_{p_i} = 1$, $\forall p_i$.

- **Θεώρημα (χαρακτηρισμός κυκλικών ομάδων):**

Έστω G μία πεπερασμένη ομάδα. Τότε, η G είναι κυκλική αν και μόνο αν έχει το πολύ μία υποομάδα τάξης n, $\forall n \in \mathbb{N}$.

Απόδειξη:

Είναι γνωστό ότι εάν η G είναι μία κυκλική ομάδα, τότε έχει μοναδική υποομάδα για κάθε διαιρέτη της τάξης της. Συνεπώς αρκεί να αποδείξουμε το αντίστροφο.

Εξετάζουμε πρώτα την ειδική περίπτωση η G να είναι μια p-ομάδα, δηλαδή $|G| = p^n$ για κάποιο πρώτο αριθμό p, $n \in \mathbb{N}$ (Λήμμα).

Έστω τώρα $g \in G$ με την $|g|$ να είναι η μέγιστη δυνατή. Θα δείξουμε ότι $G = \langle g \rangle$. Θεωρούμε λοιπόν τυχόν $h \in G$. Αφού $|h| \,|\, |G| = p^n$, έπεται ότι $|h| = p^k$, $k \le n$. Για τον ίδιο λόγο ισχύει ότι $|g| = p^m$, $k \le m \le n$, αφού το g έχει τη μέγιστη δυνατή τάξη. Όμως τότε $|h| = p^k \,|\, p^m = |g|$. Αφού λοιπόν η $\langle g \rangle$ είναι κυκλική και $p^k \,|\, |\langle g \rangle|$, έπεται ότι η $\langle g \rangle$ έχει υποομάδα τάξης p^k, την οποία ονομάζουμε K. Όμως και η $\langle h \rangle \le G$ είναι τάξης p^k. Από υπόθεση όμως έχουμε ότι υπάρχει μία το πολύ υποομάδα της G με τάξη p^k. Δηλαδή $\langle h \rangle = K \le \langle g \rangle \Rightarrow h \in \langle g \rangle$. Δείξαμε ότι το τυχόν στοιχείο της G ανήκει στη $\langle g \rangle$, άρα $G = \langle g \rangle$.

Επιστρέφουμε τώρα στη γενική περίπτωση. Έχουμε ότι όλες οι Sylow p-υποομάδες της G έχουν την ίδια τάξη. Αφού όμως η G έχει το πολύ μία υποομάδα της τάξης αυτής, συμπεραίνουμε ότι υπάρχει μοναδική Sylow p-υποομάδα της G για κάθε πρώτο αριθμό p. Τότε όμως για κάθε Sylow p_i-υποομάδα της G, P_i, έχουμε ότι $P_i \lhd G$ και επομένως $G \simeq P_1 \times P_2 \times \ldots \times P_s$, εάν η $|G|$ έχει s διακεκριμένους πρώτους διαιρέτες. Από το Λήμμα παραπάνω έχουμε ότι η κάθε P_i είναι κυκλική ομάδα, αφού ως υποομάδες της G έχουν το πολύ μία υποομάδα δεδομένης τάξης. Καταλήγουμε ότι η G είναι ισόμορφη με το ευθύ γινόμενο κυκλικών ομάδων, οι τάξεις των οποίων, ανά δύο, έχουν μέγιστο κοινό διαιρέτη ίσο με τη μονάδα. Έπεται ότι η G είναι κυκλική ομάδα.

- **Εφαρμογές:**

1. Αν $\forall g \in G \,|\, g \neq e$ ισχύει ότι $|g| = k \in \mathbb{N}$, τότε να δειχθεί ότι $k = p$, για κάποιον πρώτο αριθμό p, και ότι $|G| = p^n$, $n \in \mathbb{N}$. (υπόδειξη: να χρησιμοποιήσετε το Θεώρημα του Cauchy).
2. Να δειχθεί ότι η τάξη ενός πεπερασμένου σώματος είναι μία δύναμη ενός πρώτου αριθμού.
3. Έστω G μία πεπερασμένη ομάδα και $k \in \mathbb{Z}$. Τότε η απεικόνιση $f : G \to G$, $x \to x^k$, είναι 1-1 και επί αν και μόνο αν $(k, |G|) = 1$.

4. Έστω $|G| = pq$, όπου p, q είναι πρώτοι αριθμοί με $p < q$. Εάν $q \neq 1(\mathrm{mod} p)$, τότε $G \simeq Z_{pq}$. Διαφορετικά η G είτε θα είναι κυκλική είτε θα είναι ισόμορφη με την ομάδα $\left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \mid x^p = 1(\mathrm{mod} p), x \in Z_q^*, y \in Z_q \right\}$.
5. Οι ομάδες A_5 και S_5 έχουν 10 υποομάδες τάξης 3 και 6 υποομάδες τάξης 5.
6. Για έναν πρώτο αριθμό p, κάθε στοιχείο της $GL_2(Z_p)$ τάξης p είναι συζυγές με έναν πίνακα της μορφής $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. Το πλήθος των Sylow p-υποομάδων της $GL_2(Z_p)$ είναι $n_p = p + 1$. Άρα το πλήθος των στοιχείων τάξης p είναι $p^2 - 1$.
7. Κάθε ομάδα τάξης p^2q, όπου p, q είναι πρώτοι αριθμοί με $p < q$ και $q \neq 1(\mathrm{mod} p)$, είναι αβελιανή (π.χ. $|G| = 45$, $|G| = 99$, $|G| = 175$).

Μάθημα 7ο (Πέμπτη, 22/5/2014)

[*Εφαρμογή*]:

- **Λύση εφαρμογής 4 (βλ. προηγούμενο μάθημα):**

Έστω $|G| = pq$, όπου p, q είναι πρώτοι αριθμοί με $p < q$. Εάν $q \neq 1(\mathrm{mod}p)$, τότε $G \simeq Z_{pq}$. Διαφορετικά η G είτε θα είναι κυκλική είτε θα είναι ισόμορφη με την ομάδα $\left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \mid x^p = 1(\mathrm{mod}q), x \in Z_q^*, y \in Z_q \right\}$.

Απάντηση:

Έχουμε ότι $|G| = pq$, p, q πρώτοι αριθμοί, $p < q$. Από το Θεώρημα του Cauchy προκύπτει ότι υπάρχουν $a,b \in G : a^p = b^q = e$. Δηλαδή $|\langle a \rangle| = p$ και $|\langle b \rangle| = q$. Αφού $\left(|\langle a \rangle|, |\langle b \rangle|\right) = 1$ έχουμε ότι $\langle a \rangle \cap \langle b \rangle = \{e\}$, καθώς $g \in \langle a \rangle \cap \langle b \rangle \Rightarrow |g| \mid |\langle a \rangle|$ και $|g| \mid |\langle b \rangle| \Rightarrow |g| \mid \left(|\langle a \rangle|, |\langle b \rangle|\right) = 1 \Rightarrow |g| = 1 \Rightarrow g = e$. Ακόμη, έχουμε δείξει ότι $|\langle a,b \rangle| = \dfrac{|\langle a \rangle| \cdot |\langle b \rangle|}{|\langle a \rangle \cap \langle b \rangle|} = |\langle a \rangle| \cdot |\langle b \rangle| \Rightarrow |\langle a,b \rangle| = pq = |G| \Rightarrow \langle a,b \rangle = G = \langle a \rangle \langle b \rangle$. Επιπλέον, η $\langle a \rangle$ είναι Sylow p-υποομάδα της G και η $\langle b \rangle$ είναι Sylow q-υποομάδα της G.

Υπενθύμιση: $|G : P| = |G : N_G(P)| \cdot |N_G(P) : P| = n_p \cdot |N_G(P) : P| \Rightarrow n_p = \dfrac{|G : P|}{|N_G(P) : P|}$ και $n_p \mid |G : P|$. Στη συγκεκριμένη περίπτωση έχουμε ότι $n_p \mid |G : \langle a \rangle| \Rightarrow n_p \mid q$ και $n_q \mid |G : \langle b \rangle| \Rightarrow n_q \mid p$. Επιπλέον, από το Θεώρημα του Sylow ισχύουν πως $n_p = 1(\mathrm{mod}p)$ και $n_q = 1(\mathrm{mod}q)$. Έτσι λοιπόν, έχουμε κατ' αρχάς ότι $n_q \mid p \Rightarrow n_q = 1$ ή $n_q = p$. Ακόμη, $n_q = 1(\mathrm{mod}q) \Rightarrow q \mid n_q - 1$. Εάν $n_q = p$, αυτό σημαίνει ότι $q \mid p - 1$, το οποίο είναι άτοπο αφού $p < q$. Έπεται ότι $n_q = 1 \Rightarrow \langle b \rangle \lhd G$. Από την άλλη, έχουμε $n_p \mid q \Rightarrow n_p = 1$ ή $n_p = q$. Διακρίνουμε τώρα περιπτώσεις:

Έστω $q \neq 1(\mathrm{mod}p)$. Τότε $p \not| q - 1 \Rightarrow n_p \neq q$. Συνεπώς $n_p = 1$. Τότε $\langle a \rangle \lhd G$ και $n_p = n_q = 1$, συνεπώς η G είναι ισόμορφη με το ευθύ γινόμενο των Sylow υποομάδων της. Δηλαδή $G \simeq \langle a \rangle \times \langle b \rangle \simeq \langle ab \rangle$, το οποίο σημαίνει ότι η G είναι κυκλική με $G \simeq Z_{pq}$.

Έστω τώρα $n_p = q$. Γνωρίζουμε ότι $\langle b \rangle \lhd G$, άρα $aba^{-1} \in \langle b \rangle \Rightarrow$ υπάρχει φυσικός $m \leq q$: $aba^{-1} = b^m$. Εάν $m = 1$, τότε $aba^{-1} = b \Rightarrow ab = ba \Rightarrow G = \langle a \rangle \langle b \rangle \simeq \langle a \rangle \times \langle b \rangle$, δηλαδή $\langle a \rangle \lhd G \Rightarrow n_p = 1$ - άτοπο. Επομένως $m \neq 1$. Επίσης, είναι $a^k b a^{-k} = a^{k-1} a b a^{-1} a^{-(k-1)} = a^{k-1} b^m a^{-(k-1)} = a^{k-2} a b^m a^{-1} a^{-(k-2)} = a^{k-2} \left(aba^{-1}\right)^m a^{-(k-2)} \Rightarrow$ $a^k b a^{-k} = a^{k-2} \left(b^m\right)^m a^{-(k-2)} = a^{k-2} b^{m^2} a^{-(k-2)} \Rightarrow \ldots \Rightarrow a^k b a^{-k} = b^{m^k}$. Για $k = p$ έχουμε

$a^p b a^{-p} = b^{m^p} \overset{a^p=e}{\Rightarrow} b^{m^p} = b \Rightarrow b^{m^p-1} = e$, δηλαδή $q \mid m^p - 1 \Rightarrow m^p = 1(\mathrm{mod}\, q)$, δηλαδή για την $\langle m \rangle \le Z_q^*$ ισχύει $|\langle m \rangle| = p$ (αφού $m \neq 1$). Ακόμη, $a^k b^l a^{-k} = b^{l \cdot m^k} \Rightarrow a^k b^l = b^{l \cdot m^k} a^k$. Συνεπώς $|G| = \langle a, b \rangle = \{ b^i a^j \mid i, j \in \mathbb{N} \}$. Θεωρούμε τώρα την ομάδα $H = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \mid x^p = 1(\mathrm{mod}\, q), x \in Z_q^*, y \in Z_q \right\}$. Η Z_q^* είναι κυκλική ομάδα τάξης $q-1$, όπου $p \mid q-1$. Είναι $|H| = pq$, αφού υπάρχουν p στοιχεία $x \in Z_q^*$ με $x^p = 1(\mathrm{mod}\, q)$ και q στοιχεία $y \in Z_q$. Η H δεν είναι κυκλική, αφού π.χ. ισχύει $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & 1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} x & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Η απεικόνιση $f : H \to G$, $\begin{pmatrix} m^j & i \\ 0 & 1 \end{pmatrix} \to b^i a^j$, όπου το m είναι γεννήτορας της κυκλικής υποομάδας -τάξεως p- $\langle m \rangle = \{ x^p = 1(\mathrm{mod}\, q), x \in Z_q^* \} \le Z_q^*$ (όπως έχει άλλωστε ήδη δειχθεί). Η f είναι ομομορφισμός αφού $\begin{pmatrix} m^{j_1} & i_1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} m^{j_2} & i_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} m^{j_1+j_2} & i_2 m^{j_1} + i_1 \\ 0 & 1 \end{pmatrix} \to b^{i_2 m^{j_1} + i_1} a^{j_1+j_2}$ $= b^{i_1} a^{j_1} b^{i_2} a^{j_2}$, λόγω της σχέσης $a^k b^l = b^{l \cdot m^k} a^k$. Ακόμη, είναι σαφές ότι η f είναι επί. Αφού $|G| = |H|$, έχουμε επιπλέον ότι η f είναι 1-1. Δηλαδή η f είναι ισομορφισμός. Έπεται ότι $G \simeq H$.

Μάθημα 8ο (Πέμπτη, 28/5/2014)

[*Εφαρμογές*]:

- **Εφαρμογές:**

1. Έστω $|G| = p^2 q$, όπου p, q είναι διακεκριμένοι πρώτοι αριθμοί. Τότε η G έχει μία κανονική Sylow p-υποομάδα ή μία κανονική Sylow q-υποομάδα.

   Απάντηση:
   Έχουμε ότι $|G| = p^2 q$ και p, q πρώτοι αριθμοί με $p \neq q$. Έστω ότι η G έχει n_p Sylow p-υποομάδες και n_q Sylow q-υποομάδες. Έστω ακόμη P μία Sylow p-υποομάδα της G και Q μία Sylow q-υποομάδα της G. Από το Θεώρημα του Sylow έχουμε ότι $n_p \,||G:P| \Rightarrow n_p \,|\, q \Rightarrow n_p = 1$ ή $n_p = q$.
   Εάν $n_p = 1$, τότε $P \lhd G$ και έχουμε τελειώσει, αφού έχουμε δείξει ότι η G έχει μία κανονική Sylow p-υποομάδα.
   Έστω τώρα $n_p = q$. Από το Θεώρημα του Sylow έχουμε ακόμη ότι $n_p = 1 (\mathrm{mod} p) \Rightarrow p \,|\, n_p - 1 \Rightarrow p \,|\, q - 1 \Rightarrow p < q$. Αντίστοιχα, έχουμε ότι $n_q \,||G:Q| \Rightarrow n_p \,|\, p^2 \Rightarrow n_q = 1$ ή $n_q = p$ ή $n_q = p^2$, και $n_q = 1 (\mathrm{mod} q) \Rightarrow q \,|\, n_q - 1$.
   Εάν $n_q = 1$ τότε $Q \lhd G$, δηλαδή η G έχει μία κανονική Sylow q-υποομάδα.
   Εάν $n_q \neq 1$, τότε κατ' αρχάς από τη σχέση $q \,|\, n_q - 1$ προκύπτει ότι $p < q < n_q \Rightarrow n_q \neq p$. Άρα πρέπει υποχρεωτικά $n_q = p^2$. Μετρούμε τώρα τα στοιχεία της που έχουν τάξη q. Κάθε Sylow q-υποομάδα της G είναι τάξης q, δηλαδή κυκλική, και έχει $q-1$ στοιχεία τάξης q. Αφού υπάρχουν n_q Sylow q-υποομάδες της G, οι οποίες ανά δύο έχουν τετριμμένη τομή, συμπεραίνουμε ότι υπάρχουν $n_q (q-1) = p^2 (q-1) = p^2 q - p^2$ στοιχεία τάξης q. Ακόμη, η G έχει $n_p = q \geq 2$ Sylow p-υποομάδες, οι οποίες έχουν p^2 στοιχεία η κάθε μία. Δηλαδή η G έχει τουλάχιστον 2 Sylow p-υποομάδες, οι οποίες έχουν το πολύ p κοινά στοιχεία. Δηλαδή η G έχει τουλάχιστον $p^2 + p^2 - p$ στοιχεία τάξης 1 ή p ή p^2. Συνολικά λοιπόν η G έχει τουλάχιστον $\left(p^2 q - p^2\right) + \left(p^2 + p^2 - p\right) = p^2 q + p^2 - p > p^2 q$ στοιχεία, που φυσικά είναι άτοπο.
   Επομένως υποχρεωτικά ισχύει είτε $n_p = 1$ είτε $n_q = 1$, δηλαδή η G είτε έχει μία κανονική Sylow p-υποομάδα είτε έχει μία κανονική Sylow q-υποομάδα.

2. Έστω $|G| = pqr$, όπου p, q, r είναι πρώτοι αριθμοί με $p < q < r$. Τότε η G έχει μία κανονική υποομάδα τάξεως r.

Απάντηση:

Όπως προηγουμένως, από το Θεώρημα του Sylow έχουμε ότι $n_r \mid pq \Rightarrow n_r = 1$ ή $n_r = p$ ή $n_r = q$ ή $n_r = pq$. Εάν $n_r = 1$, τότε η G έχει μία κανονική Sylow r-υποομάδα, η οποία έχει τάξη r.

Έστω τώρα $n_r \neq 1$. Από το Θεώρημα του Sylow έχουμε ακόμη ότι $n_r = 1 (\mathrm{mod} r) \Rightarrow r \mid n_r - 1 \Rightarrow r < n_r$. Επειδή όμως $p < q < r < n_r$, έπεται ότι $n_r > p$ και $n_r > q$, δηλαδή $n_r \neq p$ και $n_r \neq q$. Άρα $n_r = pq$. Η G λοιπόν έχει $n_r = pq$ Sylow r-υποομάδες, κάθε μία από τις οποίες έχει $r-1$ στοιχεία τάξης r. Δηλαδή η G έχει $pq(r-1) = pqr - pq$ στοιχεία τάξης r. Εάν υποθέσουμε ότι $n_p, n_q > 1$, καταλήγουμε ότι η G έχει τουλάχιστον $p(q-1) = pq - p$ στοιχεία τάξης q και $q(p-1) = pq - q$ στοιχεία τάξης p, δηλαδή ότι η G έχει τουλάχιστον $(pqr - pq) + (pq - p) + (pq - q) + 1 = pqr + (p-1)(q-1) > pqr = |G|$ στοιχεία, που είναι άτοπο. Άρα $n_p = 1$ ή $n_q = 1$, που σημαίνει ότι είτε η G έχει μία κανονική Sylow p-υποομάδα ή μία κανονική Sylow q-υποομάδα. Ας ονομάσουμε S την υποομάδα αυτή, δηλαδή $S \lhd G$. Τότε η $SR \leq G$ και $|SR| = \dfrac{|S| \cdot |R|}{|S \cap R|} = |S| \cdot |R| \Rightarrow |SR| = pr$ ή $|SR| = qr$. Φυσικά $S \lhd SR$ και η R είναι Sylow r-υποομάδα της SR. Στην SR, $n_r \mid p$ ή $n_r \mid q$ και $n_r = 1 (\mathrm{mod} r) \Rightarrow r \mid n_r - 1 \Rightarrow r < n_r$, συνεπώς $n_r = 1 \Rightarrow R \lhd SR$. Επομένως $SR \leq N_G(R) \leq G$ και $SR \leq N_G(R) \leq |G : SR| = |G : N_G(R)| \cdot |N_G(R) : SR|$, δηλαδή $|G : SR| = n_r |N_G(R) : SR| \Rightarrow n_r \mid |G : SR| \Rightarrow pq \mid |G : SR|$, το οποίο είναι άτοπο καθώς $|G : SR| = p$ ή $|G : SR| = q$.

Άρα $n_r = 1$, δηλαδή η G έχει μία κανονική υποομάδα τάξεως r.

3. Έστω $|G| = p^3 q$, όπου p, q πρώτοι αριθμοί. Τότε είτε η G έχει μία κανονική Sylow p-υποομάδα ή μία κανονική Sylow q-υποομάδα είτε $p = 2$, $q = 3$ και $|G| = 24$.

Απάντηση:

Εργαζόμαστε όπως στα παραπάνω. Από το Θεώρημα του Sylow έχουμε ότι $n_p \mid q \Rightarrow n_p = 1$ ή $n_p = q$. Εάν $n_p = 1$, τότε η G έχει μία κανονική Sylow p-υποομάδα.

Έστω τώρα $n_p = q$. Τότε $n_p = 1 (\mathrm{mod} p) \Rightarrow p \mid n_p - 1 \Rightarrow p \mid q - 1 \Rightarrow p < q$. Ακόμη, $n_q \mid p^3 \Rightarrow n_q = 1$ ή $n_q = p$ ή $n_q = p^2$ ή $n_q = p^3$ και $n_q = 1 (\mathrm{mod} q) \Rightarrow q \mid n_q - 1$. Εάν

$n_q = 1$, τότε η G έχει μία κανονική Sylow q-υποομάδα. Αν $n_q \neq 1$, τότε από τη $q \mid n_q - 1$ προκύπτει ότι $p < q < n_q$, άρα $n_q \neq p$. Εάν $n_q = p^3$, τότε η G έχει $p^3(q-1) = p^3q - p^3$ στοιχεία τάξης q και περισσότερα από p^3 στοιχεία διαφορετικής τάξης (αφού p^3 στοιχεία έχει μία Sylow p-υποομάδα, και έχουμε $n_p = q$ Sylow p-υποομάδες), άρα καταλήγουμε σε άτοπο.
Εάν $n_q = p^2$, τότε $q \mid n_q - 1 \Rightarrow q \mid p^2 - 1 \Rightarrow q \mid (p-1)(p+1) \Rightarrow$ $q \mid p-1$ ή $q \mid p+1$. Όμως $p < q$, άρα $q \nmid p-1$. Συνεπώς πρέπει $q \mid p+1 \Rightarrow p < q \leq p+1 \Rightarrow q = p+1$. Αυτό μπορεί να ισχύει μόνο όταν $p = 2$, $q = 3$ και $|G| = 24$.

4. Έστω $|G| = p^2$, όπου p πρώτος αριθμός. Τότε η G είναι αβελιανή ομάδα και είτε $G \simeq Z_{p^2}$ είτε $G \simeq Z_p \times Z_p$.

<u>Απάντηση:</u>
Θεωρούμε τη δράση συζυγίας της G στον εαυτό της. Τότε, γνωρίζουμε ότι $|G| = |\mathrm{Fix}(G)| (\mathrm{mod} p)$. Όμως $Z(G) = \mathrm{Fix}(G)$, δηλαδή $|G| = |Z(G)| (\mathrm{mod} p)$ $\Rightarrow p \mid |Z(G)| \Rightarrow$ $|Z(G)| = p$ ή $|Z(G)| = p^2$. Εάν $|Z(G)| = p^2$, τότε $G = Z(G)$, το οποίο σημαίνει ότι η G είναι αβελιανή.
Έστω (προς άτοπο) ότι $|Z(G)| = p$. Τότε $Z(G) \lhd G$ και $|G/Z(G)| = p$, δηλαδή η $G/Z(G)$ είναι κυκλική. Έστω $g \in G$: $g \notin Z(G)$. Τότε $C_G(g) \leq G$ και $C_G(g) \neq G$, αφού $g \notin Z(G)$. Ακόμη $|C_G(g)| > p$, αφού $g \in C_G(g)$ και $Z(G) \leq C_G(g)$. Άρα $|C_G(g)| = p^2 \Rightarrow C_G(g) = G$, το οποίο είναι άτοπο. Επομένως $|Z(G)| = p^2$ και η G είναι αβελιανή ομάδα.
Τώρα, αν η G έχει στοιχείο τάξης p^2, τότε αυτή είναι κυκλική και $G \simeq Z_{p^2}$.
Εάν η G δεν έχει στοιχείο τάξης p^2, τότε κάθε μη-ταυτοτικό στοιχείο της G έχει τάξη p. Δηλαδή η G έχει $p^2 - 1$ στοιχεία τάξης p. Τότε όμως $G \simeq Z_p \times Z_p$, αφού μπορούμε να βρούμε ισομορφισμό $f : G \to Z_p \times Z_p$.

5. Υπάρχουν 5 μη-ισόμορφες ομάδες G με $|G| = p^3$, όπου p πρώτος αριθμός.

<u>Απάντηση:</u>
Θεωρούμε τη δράση συζυγίας της G στον εαυτό της. Τότε, γνωρίζουμε ότι $|G| = |\mathrm{Fix}(G)| (\mathrm{mod} p)$. Όμως $Z(G) = \mathrm{Fix}(G)$, δηλαδή $|G| = |Z(G)| (\mathrm{mod} p)$ $\Rightarrow p \mid |Z(G)| \Rightarrow$ $|Z(G)| = p$ ή $|Z(G)| = p^2$ ή $|Z(G)| = p^3$.
Εάν $|Z(G)| = p^3$, τότε $G = Z(G)$ και η G είναι αβελιανή. Εάν υπάρχει στοιχείο τάξης p^3, τότε $G \simeq Z_{p^3}$. Έστω ότι δεν υπάρχει στοιχείο τάξης p^3 και ότι υπάρχει στοιχείο $g \in G$ τάξης p^2. Τότε $|\langle g \rangle| = p^2$, οπότε $\langle g \rangle \simeq Z_{p^2}$ και

$G/\langle g\rangle \simeq Z_p$, συνεπώς $G \simeq Z_{p^2} \times Z_p$, αφού $\langle g\rangle \lhd G$ και $G/\langle g\rangle \lhd G$. Τέλος, εάν όλα τα στοιχεία της G (πλην του ταυτοτικού) έχουν τάξη p, τότε $G \simeq Z_p \times Z_p \times Z_p$.

Εάν $|Z(G)| = p^2$ τότε $|G/Z(G)| = p$, δηλαδή η $G/Z(G)$ είναι κυκλική. Αυτό όμως σημαίνει ότι η G είναι αβελιανή – άτοπο.

Εάν $|Z(G)| = p$ τότε $|G/Z(G)| = p^2$, επομένως από την προηγούμενη άσκηση έπεται ότι $G/Z(G) \simeq Z_{p^2}$ ή $G/Z(G) \simeq Z_p \times Z_p$. Αν όμως $G/Z(G) \simeq Z_{p^2}$, τότε η $G/Z(G)$ είναι κυκλική, οπότε η G είναι αβελιανή – άτοπο. Άρα $G/Z(G) \simeq Z_p \times Z_p$.

Μάθημα 9ο (Πέμπτη, 29/5/2014)

[*Πεπερασμένες αβελιανές ομάδες, αυτομορφισμοί*]:

- **Θεμελιώδες Θεώρημα των πεπερασμένα παραγόμενων αβελιανών ομάδων:**

Κάθε πεπερασμένα παραγόμενη (πεπερασμένη) αβελιανή ομάδα G είναι ισόμορφη με ένα ευθύ γινόμενο κυκλικών ομάδων C_{n_i}, όπου n_i είναι μία δύναμη πρώτου αριθμού, δηλαδή $G \simeq C_{n_1} \times C_{n_2} \times \ldots \times C_{n_k}$.

Απόδειξη:

Έστω G μία πεπερασμένη αβελιανή ομάδα και $|G| = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$ η ανάλυση της τάξης της σε πρώτους παράγοντες. Γνωρίζουμε ότι κάθε υποομάδα της G είναι κανονική (αφού η G είναι αβελιανή). Επομένως και κάθε Sylow υποομάδα της G είναι κανονική. Αυτό όμως σημαίνει ότι, για κάθε p_i η G έχει μοναδική Sylow p_i-υποομάδα, έστω P_i, και $P_i \lhd G$. Έχουμε δείξει ότι τότε $G \simeq P_1 \times P_2 \times \ldots \times P_k$, δηλαδή κάθε πεπερασμένη αβελιανή ομάδα είναι ισόμορφη με το ευθύ γινόμενο των Sylow υποομάδων της (Λήμμα). Αρκεί λοιπόν να δείξουμε ότι κάθε Sylow p_i-υποομάδα της G είναι ισόμορφη με ένα ευθύ γινόμενο κυκλικών ομάδων. Όμως κάθε P_i είναι αβελιανή ομάδας τάξης $p_i^{n_i}$, δηλαδή κάθε P_i είναι αβελιανή p_i-ομάδα και το ζητούμενο έπεται από το ακόλουθο Θεώρημα.

- **Θεώρημα:**

Κάθε πεπερασμένη αβελιανή p-ομάδα G είναι ισόμορφη με ένα ευθύ γινόμενο κυκλικών ομάδων.

Απόδειξη:

Η απόδειξη προκύπτει άμεσα από τα επόμενα δύο Λήμματα, καθώς κάθε υποομάδα της G είναι επίσης πεπερασμένη αβελιανή p-ομάδα.

- **Λήμμα 1:**

Αν G είναι μία πεπερασμένη αβελιανή p-ομάδα που έχει μοναδική υποομάδα H τάξης p, τότε η G είναι κυκλική.

Απόδειξη:

Έστω $|G| = p^n$. Εφαρμόζουμε επαγωγή στο n. Για $n = 1$, $|G| = p$ οπότε προφανώς το ζητούμενο ισχύει για $H = G$. Έστω τώρα $n > 1$. Θεωρούμε τον ομομορφισμό

$\phi: G \to G$, $g \to g^p$. Τότε $K \equiv \ker\phi = \{g \in G \mid g^p = e\}$. Οπότε $H \le K \Rightarrow H = K$, αφού κάθε στοιχείο της H θα έχει τάξη p και επομένως θα περιέχεται στην K. Από το 1ο Θεώρημα ισομορφισμών έχουμε ότι $G/K \simeq \phi(G) \le G$. Όμως $K \neq \{e\} \Rightarrow \phi(G) \neq G$, δηλαδή η $\phi(G)$ είναι γνήσια υποομάδα της G. Από την υπόθεση και το Θεώρημα του Cauchy η $\phi(G)$ έχει μοναδική υποομάδα τάξης p (που είναι προφανώς η $H = K$), και από επαγωγική υπόθεση έπεται ότι η $\phi(G)$ είναι κυκλική. Δηλαδή η G/K είναι κυκλική, άρα $\exists g \in G: \; G/K = \langle gK \rangle$. Ισχυριζόμαστε ότι $G = \langle g \rangle$. Προς τούτο, αρκεί να δείξουμε επιπλέον ότι $K \le \langle g \rangle$, αφού τότε $h \in G \Rightarrow hK \in G/K \Rightarrow hK \in \langle gK \rangle \Rightarrow hK = g^m K \Rightarrow g^{-m}h \in K \Rightarrow$ $\Rightarrow g^{-m}h \in \langle g \rangle \Rightarrow g^{-m}h = g^l \Rightarrow h = g^{m+l} \Rightarrow h \in \langle g \rangle$. Αλλά, από το Θεώρημα του Cauchy η $\langle g \rangle$ έχει στοιχείο τάξης p, δηλαδή η $\langle g \rangle$ έχει υποομάδα τάξης p. Από την υπόθεση όμως αυτή είναι μοναδική και πρέπει να είναι η $H = K$. Άρα όντως $K \le \langle g \rangle$, συνεπώς $G = \langle g \rangle$. Δηλαδή η G είναι κυκλική.

- **Λήμμα 2:**

Αν G είναι μία πεπερασμένη αβελιανή p-ομάδα και C μία κυκλική υποομάδα της G μέγιστης τάξης, τότε $G = C \oplus H$, για κάποια $H \le G$.

<u>Απόδειξη:</u>

Εφαρμόζουμε επαγωγή στην $|G|$. Αν η G είναι κυκλική, τότε $C = G$ και $G = C \oplus \{e\}$. Έστω ότι G δεν είναι κυκλική. Από το Λήμμα 1 και το Θεώρημα του Cauchy έπεται ότι η G έχει περισσότερες από μία υποομάδες τάξης p. Η C όμως, ως κυκλική ομάδα, έχει μοναδική υποομάδα τάξης p. Επομένως υπάρχει $K \le G$ με $|K| = p$, η οποία δεν περιέχεται στην C. Είναι φανερό ότι $K \cap C = \{e\}$. Από το 2ο Θεώρημα ισομορφισμών έχουμε ότι $(C+K)/K \simeq C/(K \cap C)$, δηλαδή $C \simeq (C+K)/K$. Έστω τώρα $g \in G$. Η τάξη του gK διαιρεί την $|g| \le |C|$. Άρα η $(C+K)/K \simeq C$ έχει μέγιστη τάξη στην G/K. Από την επαγωγική υπόθεση λοιπόν, έχουμε ότι $G/K = (C+K)/K \oplus H/K$, για κάποια $H \le G$ (από το Θεώρημα της αντιστοιχίας). Προκύπτουν λοιπόν αφ' ενός ότι $G = (C+K) \oplus H$, και αφ' ετέρου ότι $(C+K)/K \cap H/K = K \Rightarrow (C+K) \cap H = \{e\} \Rightarrow C \cap H = \{e\}$, αφού $K \cap C = \{e\}$. Άρα $C + K = C \oplus K$ και $G = (C+K) \oplus H = (C \oplus K) \oplus H = C \oplus (K \oplus H) = C \oplus H \Rightarrow$ $G = C \oplus H$.

- **Πρόταση:**

Έστω F ένα σώμα και G πεπερασμένη ομάδα της πολλαπλασιαστικής ομάδας F^*. Τότε η G είναι κυκλική.

Απόδειξη:

Η G είναι προφανώς αβελιανή. Οπότε $G \simeq P_1 \times P_2 \times ... \times P_k$, όπου P_i είναι οι Sylow υποομάδες της G. Αρκεί να δείξουμε ότι κάθε P_i είναι κυκλική. Θεωρούμε λοιπόν μία Sylow p-υποομάδα της G, έστω P. Μπορούμε να υποθέσουμε ότι $|P| = p^n$. Τότε $P \simeq C_{p^{n_1}} \times C_{p^{n_2}} \times ... \times C_{p^{n_k}}$, όπου $n_1 \geq n_2 \geq ... \geq n_k$. Συνεπώς $p^{n_i} \mid p^{n_1}$, άρα για κάθε $h \in P$ έχουμε ότι $h^{p^{n_1}} = 1$. Δηλαδή κάθε στοιχείο της P είναι ρίζα της εξίσωσης $x^{p^{n_1}} - 1 = 0$. Καθώς το F είναι σώμα, υπάρχουν το πολύ p^{n_1} ρίζες της εξίσωσης $x^{p^{n_1}} - 1 = 0$. Άρα $|P| \leq p^{n_1}$. Έπεται ότι $P = C_{p^{n_1}}$.

- **Εφαρμογή:**

1. Η πολλαπλασιαστική ομάδα Z_n^* είναι κυκλική αν και μόνο αν $n = 2$ ή $n = 4$ ή $n = p^n$ ή $n = 2p^n$, όπου p ένας περιττός πρώτος αριθμός (δηλαδή $p \neq 2$).

- ***Ορισμός αυτομορφισμού*:**

Έστω G μία ομάδα. Ένας ισομορφισμός $\phi : G \to G$ λέγεται αυτομορφισμός. Το σύνολο των αυτομορφισμών της G αποτελεί ομάδα (με πράξη τη σύνθεση), την οποία συμβολίζουμε με $\mathrm{Aut}(G)$.

- **Παρατηρήσεις:**

1. Έστω $g \in G$. Ο αυτομορφισμός $i_g : G \to G$, $x \to gxg^{-1}$ ονομάζεται εσωτερικός αυτομορφισμός της G μέσω του g. Το σύνολο των εσωτερικών αυτομορφισμών της G συμβολίζεται με $\mathrm{Inn}(G)$. Ισχύει ότι η $\mathrm{Inn}(G)$ αποτελεί υποομάδα της $\mathrm{Aut}(G)$, και μάλιστα $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$, δηλαδή η $\mathrm{Inn}(G)$ είναι κανονική υποομάδα της $\mathrm{Aut}(G)$.
2. Έστω $N \lhd G$. Τότε $gNg^{-1} = N$, $\forall g \in G$. Δηλαδή $i_g(N) = N$, $\forall g \in G$. Παρατηρούμε λοιπόν ότι μία υποομάδα της G είναι κανονική αν και μόνο αν είναι αναλλοίωτη ως προς κάθε εσωτερικό αυτομορφισμό της.
3. Η απεικόνιση $\phi : G \to \mathrm{Inn}(G)$, $g \to i_g$ είναι ομομορφισμός με πυρήνα $\ker\phi = Z(G)$. Πράγματι, $\forall x \in G$ ισχύει $\phi(g_1g_2)(x) = i_{g_1g_2}(x) = g_1g_2x(g_1g_2)^{-1} = g_1g_2xg_2^{-1}g_1^{-1} = g_1i_{g_2}(x)g_1^{-1} = i_{g_1}\left(i_{g_2}(x)\right) = \left(i_{g_1} \circ i_{g_2}\right)(x) = \left(\phi(g_1) \circ \phi(g_2)\right)(x)$, δηλάδή $\phi(g_1g_2) = \phi(g_1) \circ \phi(g_2)$, ενώ ακόμη $\ker\phi = \left\{g \in G \mid \phi(g) = i_e\right\} = \left\{g \in G \mid i_g = i_e\right\} = \left\{g \in G \mid gxg^{-1} = x,\ \forall x \in G\right\}$, δηλαδή $\ker\phi = Z(G)$.

4. Ας εξετάσουμε τώρα την $Aut(Z_n)$. Έστω α ένας γεννήτορας της Z_n. Τότε $Z_n = \langle 1 \rangle$ και μία απεικόνιση $\phi : Z_n \to Z_n$ ορίζεται πλήρως από το $\phi(1)$. Η ϕ είναι αυτομορφισμός αν και μόνο αν το $\phi(1)$ είναι επίσης γεννήτορας της Z_n, δηλαδή αν και μόνο αν $\phi(1) = k$, όπου $(k,n) = 1$. Υπάρχουν λοιπόν $\phi(n)$ αυτομορφισμοί της Z_n, δηλαδή $|Aut(Z_n)| = \phi(n)$ και συγκεκριμένα το σύνολο των αυτομορφισμών της Z_n είναι $Aut(Z_n) = \{\phi_k : Z_n \to Z_n,\ 1 \to k \mid (k,n) = 1\}$. Επομένως $Aut(Z_n) \simeq Z_n^*$, καθώς υπάρχει ισομορφισμός $f : Aut(Z_n) \to Z_n^*$, $\phi_k \to k$, όπου $(k,n) = 1$.

Μάθημα 10ο (Τετάρτη, 4/6/2014)

[*Ευθέα και ημιευθέα γινόμενα ομάδων*]:

- **Ορισμός ευθέος γινομένου ομάδων**:

Έστω G μία ομάδα και $H_1,H_2,\ldots,H_n$ υποομάδες της. Τότε λέμε ότι η G είναι το ευθύ γινόμενο των υποομάδων της $H_1,H_2,\ldots,H_n$ και γράφουμε $G \simeq H_1 \times H_2 \times \cdots \times H_n$, εάν η απεικόνιση $H_1 \times H_2 \times \cdots \times H_n \to G$, $(h_1,h_2,\ldots,h_n) \to h_1h_2\cdots h_n$ είναι ισομορφισμός ομάδων.

Αυτό σημαίνει ότι κάθε $g \in G$ γράφεται κατά *μοναδικό* τρόπο ως $g = h_1h_2\cdots h_n$, όπου $h_i \in H_i$, και εάν $G \ni g' = h'_1h'_2\cdots h'_n$ τότε $gg' = (h_1h'_1)(h_2h'_2)\cdots(h_nh'_n)$.

- **Πρόταση 1:**

Έστω G μία ομάδα και $H_1,H_2 \le G$. Τότε $G \simeq H_1 \times H_2$ αν και μόνο αν ισχύουν τα ακόλουθα:

i. $H_1,H_2 \lhd G$,
ii. $G = H_1H_2$, και
iii. $H_1 \cap H_2 = \{e\}$.

- **Πρόταση 2:**

Έστω G μία ομάδα και $H_1,H_2 \le G$. Τότε $G \simeq H_1 \times H_2$ αν και μόνο αν ισχύουν τα ακόλουθα:

i. $G = H_1H_2$,
ii. $H_1 \cap H_2 = \{e\}$, και
iii. $h_1h_2 = h_2h_1 \quad \forall h_1 \in H_1, h_2 \in H_2$.

- **Πρόταση 3:**

Έστω G μία ομάδα και $H_1,H_2,\ldots,H_n \le G$. Τότε $G \simeq H_1 \times H_2 \times \cdots \times H_n$ αν και μόνο αν ισχύουν τα ακόλουθα:

i. $H_1,H_2,\ldots,H_n \lhd G$,
ii. $G = H_1H_2\cdots H_n$, και
iii. $H_j \cap \left(H_1H_2\cdots H_{j-1}H_{j+1}\cdots H_n\right) = \{e\} \quad \forall j \in \{1,2,\ldots,n\}$.

- **Παρατηρήσεις:**

1. Έστω G μία ομάδα, $g \in G$ και $i_g : G \to G$, $x \to gxg^{-1}$ ο επαγόμενος εσωτερικός αυτομορφισμός της G μέσω του g. Η απεικόνιση $f : G \to \mathrm{Aut}(G)$, $g \to i_g$ είναι ομομορφισμός, αφου $\forall x \in G$ έχουμε ότι

$f(ab)(x) = i_{ab}(x) = abx(ab)^{-1} = abxb^{-1}a^{-1} = ai_b(x)a^{-1} = i_a(i_b(x)) = i_{a\circ b}(x)$, δηλαδή $f(ab) = f(a)\circ f(b)$. Επιπλέον, ο πυρήνας της f είναι $\ker f = Z(G)$, αφού $i_g = e \Leftrightarrow g \in Z(G)$. Η εικόνα της f είναι προφανώς $f(G) = \mathrm{Inn}(G)$. Από το 1ο Θεώρημα ισομορφισμών έχουμε επομένως ότι $G/Z(G) \simeq \mathrm{Inn}(G)$.

2. Προκύπτει λοιπόν ότι $G \simeq \mathrm{Inn}(G) \Leftrightarrow Z(G) = \{e\}$. Επιπροσθέτως ισχύει ότι $G \simeq \mathrm{Aut}(G) \Leftrightarrow Z(G) = \{e\}$ και $\mathrm{Aut}(G) = \mathrm{Inn}(G)$.
3. Έστω τώρα G μία πεπερασμένη κυκλική ομάδα τάξης $|G| = n$. Γνωρίζουμε ότι $G \simeq Z_n$. Έχουμε ακόμη δείξει ότι $\mathrm{Aut}(Z_n) \simeq Z_n^*$.
4. Εάν p είναι ένας περιττός πρώτος αριθμός και $C_n \simeq Z_n$ η κυκλική ομάδα τάξης n (μοναδική ως προς ισομορφισμό), τότε από τη Θεωρία Αριθμών μπορεί να δειχθεί ότι $\mathrm{Aut}(Z_2) \simeq Z_2^* \simeq \{e\}$, $\mathrm{Aut}(Z_4) \simeq Z_4^* \simeq C_2$, $\mathrm{Aut}(Z_{2^n}) \simeq Z_{2^n}^* \simeq C_2 \times C_{2^{n-2}}$ (για $r > 2$) και $\mathrm{Aut}(Z_{p^n}) \simeq Z_{p^n}^* \simeq C_{p^{n-1}(p-1)}$.
5. Έχουμε επισημάνει ότι μία υποομάδα της G είναι κανονική αν και μόνο αν είναι αναλλοίωτη ως προς κάθε εσωτερικό αυτομορφισμό της. Ιδιαίτερα, αν η $H \le G$ είναι αναλλοίωτη ως προς κάθε αυτομορφισμό της G, τότε $H \lhd G$.
6. Η $Z(G)$ παραμένει αναλλοίωτη ως προς κάθε αυτομορφισμό της G, καθώς αν $a: G \to G$, $a \in \mathrm{Aut}(G)$, τότε $\forall x \in G$ και $\forall z \in Z(G)$ έπεται ότι $a(x)a(z) = a(xz) = a(zx) = a(z)a(x) \Rightarrow a(z) \in Z(G)$, δηλαδή $a(Z(G)) \subseteq Z(G)$ $\Rightarrow a(Z(G)) = Z(G)$. Αυτές οι υποομάδες της G ονομάζονται χαρακτηριστικές. Προφανώς κάθε χαρακτηριστική υποομάδα είναι και κανονική.

- **Ημιευθύ γινόμενο ομάδων – εισαγωγικά**:

Έστω G μία ομάδα. Η G είναι το ευθύ γινόμενο δύο υποομάδων αν και μόνο αν η G περιέχει δύο κανονικές υποομάδες N_1, N_2 με $N_1 \cap N_2 = \{e\}$ και $G = N_1N_2$. Μία γενίκευση του ευθέος γινομένου είναι το εσωτερικό ημιευθύ γινόμενο:
Λέμε ότι η G είναι ένα ημιευθύ γινόμενο μιας κανονικής υποομάδας N και μίας υποομάδας H, αν $G = NH$ και $N \cap H = \{e\}$.

- **Παρατηρήσεις:**

1. Έστω G ομάδα και $N, H \le G$. Οι N και H ονομάζονται συμπληρωματικές αν $G = HN = NH$ και $H \cap N = \{e\}$. Εάν επιπλέον μία από αυτές είναι κανονική στην G, τότε η G είναι το ημιευθύ γινόμενό τους.
2. Εάν η G είναι το ημιευθύ γινόμενο των $N \lhd G$ και $H \le G$, τότε $G/N \simeq H$. Πράγματι, από το 2ο Θεώρημα ισομορφισμών προκύπτει άμεσα ότι $G/N = HN/N \simeq H/(H \cap N) = H$, δηλαδή ότι $G/N \simeq H$.

3. Κάθε στοιχείο $g \in G$ γράφεται μοναδικά ως $g = nh$, $n \in N$, $h \in H$, αφού αν $nh = n'h'$ τότε $(n')^{-1} n = h'h^{-1} \in N \cap H = \{e\}$. Έχουμε λοιπόν κατασκευάσει μία 1-1 αντιστοιχία $G \overset{1-1}{\leftrightarrow} N \times H$. Άρα $|G| = |N| \cdot |H|$ και προφανώς $G = \langle N, H \rangle$.
4. Επειδή η N είναι κανονική στη G, κάθε στοιχείο $h \in H$ ορίζει τον αυτομορφισμό $n \to hnh^{-1}$ της N. Ουσιαστικά δηλαδή θεωρούμε τη δράση της G στη N με συζυγία, και συγκεκριμένα τον περιορισμό της δράσης συζυγίας στην H. Η απεικόνιση $H \to Aut(N)$, $h \to (n \to hnh^{-1})$ είναι ομομορφισμός: Γράφουμε $\phi_h : n \to hnh^{-1}$ και έχουμε $\phi_{h_1 h_2}(n) = h_1 h_2 n (h_1 h_2)^{-1} =$ $= \phi_{h_1}(\phi_{h_2}(n)) = (\phi_{h_1} \circ \phi_{h_2})(n)$. Άρα $\phi_{h_1 h_2} = \phi_{h_1} \circ \phi_{h_2}$.
5. Ο πολλαπλασιασμός στη G δίνεται ως εξής: $g_1, g_2 \in G$, $g_1 g_2 = (n_1 h_1)(n_2 h_2) =$ $= (n_1 h_1 n_2 h_1^{-1})(h_1 h_2) = (n_1 \phi_{h_1}(n_2))(h_1 h_2)$.

- **Ημιευθύ γινόμενο ομάδων - συνέχεια:**

Αν N και H είναι δύο ομάδες, τότε μπορούμε να κατασκευάσουμε ένα <u>εξωτερικό ημιευθύ γινόμενο</u> για κάθε ομομορφισμό $\phi : H \to Aut(N)$, ως εξής: Θεωρούμε το σύνολο $G = N \times H$ και ορίζουμε τον πολλαπλασιασμό στο G ως: $(n_1, h_1)(n_2, h_2) = (n_1 \phi_{h_1}(n_2), h_1 h_2)$, όπου $\phi_h = \phi(h)$, $h \in H$. Ως προς αυτόν τον πολλαπλασιασμό, το σύνολο G είναι ομάδα που την συμβολίζουμε με $\overline{G} = N \rtimes_\phi H$. Το ταυτοτικό στοιχείο της $\overline{G}$ είναι το (e_N, e_H) και το αντίστροφο του (n,h) είναι το $(\phi_{h^{-1}}(n^{-1}), h^{-1})$.

Το υποσύνολο $N' = N \times \{e_H\}$ είναι κανονική υποομάδα της $\overline{G}$ που είναι ισόμορφη με την N, και το υποσύνολο $H' = \{e_N\} \times H$ είναι υποομάδα της $\overline{G}$ που είναι ισόμορφη με την H. Πράγματι, έχουμε τους ισομορφισμούς $f_1 : N \to N'$, $n \to (n, e_H)$, και $f_2 : H \to H'$, $h \to (e_N, h)$. Είναι δε $G = N'H'$ και $N' \cap H' = \{(e_N, e_H)\}$. Άρα η G είναι το <u>εσωτερικό ημιευθύ γινόμενο</u> των N' και H'. Επίσης, ισχύει ότι $N'H' \simeq N \rtimes_\phi H$ και $(e_N, h)(n, e_H)(e_N, h^{-1}) = (\phi_h(n), h)(e_N, h^{-1}) = (\phi_h(n), e_H)$, δηλαδή ο ομομορφισμός ϕ που ορίζει το εξωτερικό ημιευθύ γινόμενο των N και H αναγνωρίζεται στο εσωτερικό ημιευθύ γινόμενο των N' και H' ως ο ομομορφισμός $\phi' : H' \to Aut(N')$, όπου $\phi'(e_N, h) : (n, e_H) \to (e_N, h)(n, e_H)(e_N, h^{-1})$.

Συνεπώς όταν ταυτίζουμε το εξωτερικό ημιευθύ γινόμενο $N \rtimes_\phi H$ με το εσωτερικό ημιευθύ γινόμενο N'H', μπορούμε να γράφουμε για το γινόμενο $(n_1, h_1)(n_2, h_2) = (n_1 h_1 n_2 h_1^{-1}, h_1 h_2)$.

- **Παρατηρήσεις:**

1. Αν η $\phi : H \to Aut(N)$ είναι τετριμμένος ομομορφισμός $\phi(h) = 1_N$, δηλαδή $\phi(h) : n \to n$, τότε $N \rtimes_\phi H \simeq N \times H$, $(n_1, h_1)(n_2, h_2) = (n_1 \phi_{h_1}(n_2), h_1 h_2) = (n_1 n_2, h_1 h_2)$.

2. Η υποομάδα $H' = \{e_N\} \times H$ είναι κανονική αν και μόνο αν ο $\phi : H \to Aut(N)$ είναι ο τετριμμένος ομομορφισμός. Πράγματι, αν υπάρχουν $h \in H$ και $n \in N$ με $\phi_h(n) \neq n$, τότε $(n, e_H)(e_N, h)(n, e_H)^{-1} = (n, e_H)(e_N, h)(n^{-1}, e_H) = (n, h)(n^{-1}, e_H) =$ $= (n\phi_h(n^{-1}), h) = (n\phi_h^{-1}(n), h) \notin H'$, δηλαδή η H' δεν είναι κανονική (άτοπο).
3. Αν ο $\phi : H \to Aut(N)$ δεν είναι τετριμμένος, τότε το $N \rtimes_\phi H$ δεν είναι αβελιανή ομάδα (ακόμα και αν οι N, H είναι αβελιανές). Πράγματι, έστω $\phi_h(n) \neq n$ για κάποια $h \in H$ και $n \in N$. Τότε $(n, e_H)(e_N, h) = (n, h)$ και $(e_N, h)(n, e_H) = (\phi_h(n), h)$, δηλαδή $(n, e_H)(e_N, h) = (n, h) \neq (\phi_h(n), h) = (e_N, h)(n, e_H)$ και συνεπώς η $N \rtimes_\phi H$ δεν είναι αβελιανή.

- **Ορισμός ημιευθέος γινομένου ομάδων**:

Έστω G μία ομάδα και $N, H \leq G$. Τότε λέμε ότι η G είναι το ημιευθύ γινόμενο των υποομάδων της N και H εάν $N \lhd G$ και $G/N \simeq H$. Τότε γράφουμε $G = N \rtimes H$ (ή $G = N \rtimes_\phi H$, όπου $\phi : H \to Aut(N)$ ο ομομορφισμός που ορίζει τη δράση της H στη N με εσωτερικούς αυτομορφισμούς).

- **Πρόταση 4:**

Έστω G μία ομάδα και $N, H \leq G$. Τότε $G = N \rtimes H$ αν και μόνο αν ισχύουν τα ακόλουθα:

i. $N \lhd G$,
ii. $G = HN = NH$, και
iii. $H \cap N = \{e\}$.

- **Εφαρμογές:**

1. Έστω G πεπερασμένη ομάδα τάξης $|G| = 21$. Να ταξινομήσετε ως προς ισομορφισμό τη G.

   <u>Απάντηση:</u>
   Έχουμε ότι $|G| = 21 = 3 \cdot 7$, η ανάλυση της $|G|$ σε πρώτους παράγοντες. Έστω n_3 και n_7 το πλήθος των Sylow 3-υποομάδων και των Sylow 7-υποομάδων της G, αντίστοιχα. Από το Θεώρημα του Sylow έχουμε ότι $n_7 \mid 3 \Rightarrow n_7 = 1$ ή $n_7 = 3$. Επιπλέον $n_7 = 1 (\mathrm{mod} 7)$, επομένως $n_7 = 1$. Δηλαδή η G έχει μοναδική Sylow 7-υποομάδα, έστω N. Προφανώς $N \lhd G$.
   Έστω τώρα H μία Sylow 3-υποομάδα της G. Τότε $H \cap N = \{e\}$. Επομένως $|HN| = \frac{|H| \cdot |N|}{|H \cap N|} = 3 \cdot 7 = 21 = |G| \Rightarrow G = HN$. Ακόμη, από το $2^{ο}$ Θεώρημα ισομορφισμών έχουμε ότι $G/N = HN/N \simeq H/(H \cap N) = H$, δηλαδή $G/N \simeq H$. Διαπιστώνουμε λοιπόν ότι $G = N \rtimes H$.

Στη συνέχεια αναζητούμε ομομορφισμό $\phi: H \to Aut(N)$. Όμως, έχουμε ότι $|N| = 7 \Rightarrow N \simeq Z_7$, από όπου έπεται ότι $Aut(N) \simeq C_6$. Έχουμε ότι $|\phi(H)| \mid |H| \Rightarrow |\phi(H)| \mid 3 \Rightarrow |\phi(H)| = 1$ ή $|\phi(H)| = 3$.

Εάν $|\phi(H)| = 1$ τότε $\phi(H) = \{e\}$, δηλαδή ο ϕ είναι τετριμμένος και επομένως το ημιευθύ γινόμενο είναι στην πραγματικότητα ευθύ, δηλαδή $G \simeq N \times H \simeq Z_7 \times Z_3 \Rightarrow G \simeq Z_3 \times Z_7$.

Έστω τώρα $|\phi(H)| = 3$. Θέτουμε $N = \langle n \rangle$ και θεωρούμε $a \in Aut(N)$ με $a(n) = n^3$. Τότε $a^2(n) = n^9 = n^2$, $a^3(n) = n^6$, άρα $|a| > 3 \Rightarrow |a| = 6$, δηλαδή $Aut(N) = \langle a \rangle$. Επομένως $\phi(H) = \langle a^2 \rangle$. Εάν θέσουμε $H = \langle h \rangle$, τότε $\phi(h) = a^2$ και $\phi(h^2) = a^4$. Τότε $G = N \rtimes_\phi H \Rightarrow G = \langle n \rangle \rtimes_\phi \langle h \rangle$, όπου $h \to \phi(h)$, $\phi(h)(n) = n^2$.

2. Θεωρούμε τις Z_n και $Z_2 = \langle a \rangle$. Να βρεθεί το $Z_n \rtimes_\phi Z_2$, όπου $\phi: Z_2 \to Aut(Z_n)$, $\phi(a)(x) = x^{-1} \ \forall x \in Z_n$.

<u>Απάντηση:</u>

Έχουμε ότι $(\phi(a)(x))^2 = 1 \Rightarrow (\phi(a))^2 = 1_{Z_n}$. Άρα $|\phi(a)| = 2 \Rightarrow \langle \phi(a) \rangle \simeq Z_2$. Επομένως ο ϕ δεν είναι τετριμμένος. Έπεται ότι η $Z_n \rtimes_\phi Z_2$ δεν είναι αβελιανή.

Έστω τώρα $Z_n = \langle b \rangle$. Τότε στην $Z_n \rtimes_\phi Z_2$ το $(b,1)$ έχει τάξη n και το $(1,a)$ έχει τάξη 2. Επίσης, έχουμε $(1,a)(b,1)(1,a)^{-1} = (1\phi(a)(b), a)(1,a^{-1}) =$
$= (b^{-1}, a)(1,a^{-1}) = (b^{-1}\phi(a)(1),1) = (b^{-1},1) = (b,1)^{-1}$.

Δηλαδή στην $Z_n \rtimes_\phi Z_2$ έχουμε τα στοιχεία $u = (b,1)$ και $v = (1,a)$, τα οποία ικανοποιούν τις συνθήκες $|u| = n$, $|v| = 2$ και $vuv^{-1} = u^{-1}$. Άρα υπάρχει ένας ομομορφισμός $D_n \to Z_n \rtimes_\phi Z_2$, που είναι επιμορφισμός αφού η $Z_n \rtimes_\phi Z_2$ παράγεται από τα στοιχεία u και v (υπενθυμίζουμε ότι η D_n είναι η διεδρική ομάδα τάξης 2n). Επειδή $|D_n| = |Z_n \rtimes_\phi Z_2| = 2n$, προκύπτει άμεσα ότι $Z_n \rtimes_\phi Z_2 \simeq D_n$.

3. Θεωρούμε την εναλλάσσουσα ομάδα A_4. Να γραφεί ως ημιευθύ γινόμενο δύο υποομάδων της.

<u>Απάντηση:</u>

Έστω η εναλλάσσουσα ομάδα A_4.

Η υποομάδα $V = \{e, (12)(34), (13)(24), (14)(23)\}$ (ομάδα του Klein) είναι κανονική στην A_4. Επίσης, η υποομάδα $H = \langle (123) \rangle$ έχει τάξη 3 και δεν

είναι κανονική στην A_4. Προφανώς $V \cap H = \{e\}$ και $A_4 = VH$, αφού $|VH| = \frac{|V| \cdot |H|}{|V \cap H|} = 12 = |A_4|$. Δηλαδή η A_4 είναι το ημιευθύ γινόμενο των V και H.

Μπορούμε να καθορίσουμε τον κατάλληλο ομομορφισμό $\phi : H \to Aut(V)$, προσδιορίζοντας το $\phi_{(123)} \equiv \phi(123)$. Έχουμε $(123)(12)(34)(123)^{-1} = (14)(23)$, $(123)(13)(24)(123)^{-1} = (12)(34)$ και $(123)(14)(23)(123)^{-1} = (13)(24)$. Ακόμη, ισχύει ότι $\phi_{(123)^2} = \phi^2_{(123)}$. Άρα ο ϕ καθορίζεται πλήρως.

4. Θεωρούμε την συμμετρική ομάδα S_4. Να γραφεί ως ημιευθύ γινόμενο δύο υποομάδων της.

<u>Απάντηση:</u>

Θεωρούμε τη συμμετρική ομάδα S_4 και την ομάδα του Klein $V \lhd S_4$. Έστω $H = \{\sigma \in S_4 \mid \sigma(4) = 4\} \simeq S_3$, $H \leq S_4$, η οποία έχει τάξη 6 και δεν είναι κανονική στην S_4. Ισχύει $V \cap H = \{e\}$ και $S_4 = VH$, αφού (όπως πριν) είναι $|VH| = \frac{|V| \cdot |H|}{|V \cap H|} = 24 = |S_4|$. Δηλαδή η S_4 είναι το ημιευθύ γινόμενο των V και H.

Για να καθορίσουμε τον κατάλληλο ομομορφισμό $\phi : H \to Aut(V)$, εργαζόμαστε ως εξής: Η υποομάδα V είναι ένας Z_2-χώρος, αφού είναι ισόμορφη με την $Z_2 \oplus Z_2$ και κάθε στοιχείο της $Aut(V)$ είναι ένας αντιστρέψιμος γραμμικός μετασχηματισμός. Επειδή $\dim_{Z_2} V = 2$, έχουμε ότι $Aut(V) \simeq GL_2(Z_2)$. Άρα ο ϕ μπορεί να θεωρηθεί ως ένας ομομορφισμός $S_3 \to GL_2(Z_2)$. Είναι δε $|GL_2(Z_2)| = 6$.

Έστω τώρα $u = (12)(34)$ και $v = (13)(24)$. Το σύνολο $\{u, v\}$ είναι μία βάση του V. Επίσης $H = \langle (123), (12) \rangle$ και $(123)(12)(34)(123)^{-1} = (14)(23) = uv$, $(123)(13)(24)(123)^{-1} = (12)(34) = u$. Δηλαδή η συζυγία με το (123) είναι ο γραμμικός μετασχηματισμός που αντιστοιχεί στον πίνακα $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Από την άλλη, $(12)(12)(34)(12)^{-1} = (12)(34) = u$ και $(12)(13)(24)(12)^{-1} = (14)(23) = uv$, δηλαδή η συζυγία με το (12) είναι ο γραμμικός μετασχηματισμός που αντιστοιχεί στον πίνακα $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

5. Θεωρούμε τις $Z_3 = \langle a \rangle$, $Z_4 = \langle b \rangle$ και τον ομομορφισμό $\phi : Z_4 \to Aut(Z_3)$, $b \to \phi(b)$, $\phi(b)(a) = a^{-1}$. Να δειχθεί ότι $Z_3 \rtimes_\phi Z_4 \simeq D_6$.

   <u>Απάντηση:</u>

   Θεωρούμε την $G = Z_3 \rtimes_\phi Z_4$. Τότε $|G| = 12 = 2^2 \cdot 3$. Επίσης $Z_3 \lhd G$, οπότε $n_3 = 1$, δηλαδή η Z_3 είναι η μοναδική Sylow 3-υποομάδα της G. Όμως η G δεν έχει κανονική Sylow 2-υποομάδα, καθώς τότε θα ήταν αβελιανή – άτοπο, αφού ο ϕ δεν είναι τετριμμένος.

   Δηλαδή η G είναι μία μη-αβελιανή ομάδα, τάξης 12. Επιπλέον $G \neq A_4$, καθώς η A_4 έχει κανονική Sylow 2-υποομάδα, την ομάδα του Klein V. Έπεται ότι $G \simeq D_6$, δηλαδή ότι $Z_3 \rtimes_\phi Z_4 \simeq D_6$.

   (παρατήρηση: ως προς ισομορφισμό, υπάρχουν 3 διαφορετικές ομάδες τάξης 12, οι οποίες είναι οι Z_{12}, D_6 και A_4).

6. Θεωρούμε τις $Z_5 = \langle a \rangle$, $Z_4 = \langle b \rangle$ και $\phi : Z_4 \to Aut(Z_5)$, $b \to \phi(b)$, $\phi(b)(a) = a^2$. Να βρεθεί το $Z_5 \rtimes_\phi Z_4$.

Μάθημα 11° (Τετάρτη, 11/6/2014)

[*Κανονικές σειρές ομάδων*]:

- **Ορισμός κανονικής σειράς ομάδας**:

Έστω G ομάδα. Μία κανονική σειρά της G είναι μία πεπερασμένη ακολουθία υποομάδων της G, έστω $G_0, G_1, \ldots, G_n$, τέτοια ώστε $G_i \lhd G_{i+1}$ $i = 0,1,\ldots,n-1$, και $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$.

- **Παρατηρήσεις:**

1. Οι υποομάδες G_i, $i = 0,1,\ldots,n$, λέγονται όροι της σειράς.
2. Τα πηλίκα G_i/G_{i-1}, $i = 1,2,\ldots,n$, λέγονται πηλίκα της σειράς.
3. Το πλήθος των μη-τετριμμένων πηλίκων της σειράς λέγεται μήκος της σειράς.

- **Παραδείγματα:**

1. $1 \lhd G$.
2. $1 \lhd A_n \lhd S_n$.
3. $1 \lhd \langle \rho \rangle \lhd D_\infty$.
4. $1 \lhd \langle \rho^2 \rangle \lhd \langle \rho \rangle \lhd D_\infty$.
5. $1 \lhd V \lhd A_4 \lhd S_4$.

- **Ορισμός ισοδύναμων σειρών**:

Δύο κανονικές σειρές μίας ομάδας G, έστω $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ (1) και $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$ (2), λέγονται ισοδύναμες εάν υπάρχει μία 1-1 και επί αντιστοιχία μεταξύ των συνόλων των πηλίκων της (1) και των πηλίκων της (2), έτσι ώστε αντίστοιχα πηλίκα να είναι ισόμορφα.

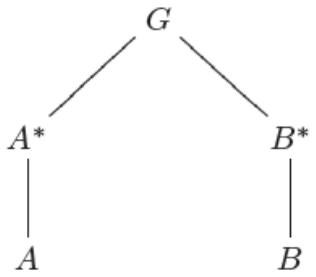
- **Παράδειγμα:**

1. Έστω $G = \langle x \rangle$, $|G| = 30 = 2 \cdot 3 \cdot 5$. Τότε δύο κανονικές σειρές της G είναι οι $1 = \langle x^{30} \rangle \lhd \langle x^{10} \rangle \lhd \langle x^5 \rangle \lhd \langle x \rangle = G$ (1) και $1 = \langle x^{30} \rangle \lhd \langle x^6 \rangle \lhd \langle x^2 \rangle \lhd \langle x \rangle = G$ (2). Οι δύο αυτές σειρές είναι ισόμορφες, αφού για τα πηλίκα της (1) ισχύουν $\langle x^{10} \rangle / \langle x^{30} \rangle \simeq \mathbb{Z}_3$, $\langle x^5 \rangle / \langle x^{10} \rangle \simeq \mathbb{Z}_2$ και $\langle x \rangle / \langle x^5 \rangle \simeq \mathbb{Z}_5$, ενώ για τα πηλίκα της (2) ισχύουν $\langle x^6 \rangle / \langle x^{30} \rangle \simeq \mathbb{Z}_5$, $\langle x^2 \rangle / \langle x^6 \rangle \simeq \mathbb{Z}_3$ και $\langle x \rangle / \langle x^2 \rangle \simeq \mathbb{Z}_2$.

- **Ορισμός επιλέπτυνσης σειράς**:

Έστω $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ (1) και $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$ (2) δύο κανονικές σειρές της G. Η (2) λέγεται επιλέπτυνση της (1), αν κάθε όρος της (1) είναι και όρος της (2).

- **Λήμμα του Zassenhaus**:



Έστω $A,B,A^*,B^* \leq G$ και $A \lhd A^*$, $B \lhd B^*$. Τότε $A(A^* \cap B) \lhd A(A^* \cap B^*)$, $B(A \cap B^*) \lhd B(A^* \cap B^*)$ και $A(A^* \cap B^*) \Big/ A(A^* \cap B) \simeq B(A^* \cap B^*) \Big/ B(A \cap B^*)$.

<u>Απόδειξη:</u>

Αφού $A \lhd A^* \Rightarrow A(A^* \cap B) = (A^* \cap B)A$, συνεπώς $A(A^* \cap B) \leq G$. Με όμοιο τρόπο μπορούμε να δείξουμε ότι και τα υπόλοιπα γινόμενα είναι υποομάδες της G.

Ακόμη, $\left.\begin{matrix} A \lhd A^* \Rightarrow A \cap B^* \lhd A^* \cap B^* \\ B \lhd B^* \Rightarrow A^* \cap B \lhd A^* \cap B^* \end{matrix}\right\} \Rightarrow (A \cap B^*)(A^* \cap B) \lhd A^* \cap B^*$.

Θεωρούμε τώρα την απεικόνιση $f : A(A^* \cap B^*) \to A^* \cap B^* \Big/ (A \cap B^*)(A^* \cap B)$,

$x = aw \to (A \cap B^*)(A^* \cap B)w$.

Η f είναι καλά ορισμένη, αφού αν $x = aw = a_1 w_1$, όπου $a, a_1 \in A$ και $w, w_1 \in A^* \cap B^*$, τότε $aw = a_1 w_1 \Rightarrow a_1^{-1} a = w_1 w^{-1} \in A \cap (A^* \cap B^*)$. Επομένως $f(aw) = (A \cap B^*)(A^* \cap B)w = (A \cap B^*)(A^* \cap B)a^{-1}a_1 w_1 = (A \cap B^*)(A^* \cap B)w_1 = f(a_1 w_1)$.

Επιπλέον, η f είναι ομομορφισμός, καθώς αν $x_1, x_2 \in A(A^* \cap B^*)$ με $x_1 = a_1 w_1$ και $x_2 = a_2 w_2$, τότε $x_1 x_2 = a_1 w_1 a_2 w_2 = a_1 w_1 a_2 w_1^{-1} w_1 w_2$. Όμως $w_1 a_2 w_1^{-1} = a' \in A$, αφού $A \lhd A^*$ και $w_1 \in A^* \cap B^* \Rightarrow w_1 \in A^*$. Έπεται ότι $f(x_1 x_2) = f(a_1 a' w_1 w_2) = = (A \cap B^*)(A^* \cap B)w_1 w_2 = f(x_1) f(x_2)$, δηλαδή η f είναι ομομορφισμός. Καθώς η f είναι προφανώς επί, από το 1ο Θεώρημα ισομορφισμών έχουμε ότι $A(A^* \cap B^*) \Big/ \ker f \simeq A^* \cap B^* \Big/ (A \cap B^*)(A^* \cap B)$.

Ακόμη, $\ker f = A(A^* \cap B^*) \cap A(A \cap B^*)(A^* \cap B) = A(A^* \cap B^*) \cap A(A^* \cap B) = A(A^* \cap B)$, όπου στην πρώτη ισότητα χρησιμοποιήσαμε το γεγονός ότι $A \cap B^* \subseteq A$ και στη

δεύτερη το γεγονός ότι $B \le B^*$. Δείξαμε λοιπόν ότι $\ker f = A(A^* \cap B)$, επομένως έχουμε $A(A^* \cap B) \lhd A(A^* \cap B^*)$ και $A(A^* \cap B^*)/A(A^* \cap B) \simeq A^* \cap B^*/(A \cap B^*)(A^* \cap B)$.
Ομοίως δείχνουμε τα άλλα ζητούμενα και η απόδειξη του Λήμματος είναι πλήρης.

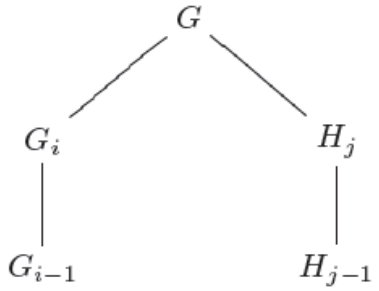
- **Παρατήρηση:**

1. Το Λήμμα του Zassenhaus αποτελεί γενίκευση του 2ου Θεωρήματος ισομορφισμών. Πράγματι, για $A = N$, $A^* = G$, $B = 1$ και $B^* = H$ έχουμε ότι $N, H \le G$, $N \lhd G \Rightarrow N \lhd HN$, $H \cap N \lhd H$ και $HN/N \simeq H/H \cap N$.

- **Θεώρημα του Schreier:**

Κάθε δύο κανονικές σειρές μίας ομάδας G έχουνε ισοδύναμες επιλεπτύνσεις.

Απόδειξη:
Έστω $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ (1) και $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_m = G$ (2) δύο κανονικές σειρές της G. Θα κατασκευάσουμε μία επιλέπτυνση της (1) παρεμβάλλοντας $m-1$ υποομάδες G_{ij}, $j = 1,\ldots,m-1$, μεταξύ της G_{i-1} και της G_i, για κάθε $i \in \{1,2,\ldots,n\}$, και μία επιλέπτυνση της (2) παρεμβάλλοντας $n-1$ υποομάδες H_{ij}, $i = 1,\ldots,n-1$, μεταξύ της H_{j-1} και της H_j, για κάθε $j \in \{1,2,\ldots,m\}$. Αυτές οι επιλεπτύνσεις θα έχουν $mn+1$ όρους, δηλαδή mn πηλίκα.



Ορίζουμε $G_{ij} = (G_i \cap H_j)G_{i-1}$, $j = 1,\ldots,m-1$, $\forall i \in \{1,2,\ldots,n\}$, και $H_{ij} = (H_j \cap G_i)H_{j-1}$, $i = 1,\ldots,n-1$, $\forall j \in \{1,2,\ldots,m\}$. Τότε, από το Λήμμα του Zassenhaus έχουμε ότι $G_{ij-1} \lhd G_{ij}$, $H_{i-1j} \lhd H_{ij}$ και $G_{ij}/G_{ij-1} \simeq H_{ij}/H_{i-1j}$, $\forall i \in \{1,2,\ldots,n\}$ και $\forall j \in \{1,2,\ldots,m\}$.

- **Ορισμός γνήσιας επιλέπτυνσης σειράς:**

Έστω $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ (1) κανονική σειρά της G. Μία επιλέπτυνση της (1) που έχει μήκος μεγαλύτερο από το μήκος της (1) ονομάζεται γνήσια επιλέπτυνση της (1).

- **Ορισμός συνθετικής σειράς**:

Έστω $1 = G_0 \lhd G_1 \lhd ... \lhd G_n = G$ (1) κανονική σειρά της G. Εάν $G_i \neq G_{i+1}$ $\forall i \in \{0,1,2,...,n-1\}$ και επιπλέον δεν υπάρχει γνήσια επιλέπτυνση της (1), τότε η (1) λέγεται συνθετική σειρά της G.

- **Παραδείγματα:**

1. Η $1 \lhd A_5$ είναι συνθετική σειρά της A_5.
2. Η $\mathbb{Z}$ δεν έχει συνθετική σειρά, αφού εάν $1 \lhd \langle x^k \rangle \lhd ... \lhd \langle x \rangle = \mathbb{Z}$ μία κανονική σειρά της $\mathbb{Z}$, τότε η $1 \lhd \langle x^{2k} \rangle \lhd \langle x^k \rangle \lhd ... \lhd \langle x \rangle = \mathbb{Z}$ είναι μία γνήσια επιλέπτυνσή της.

- **Θεώρημα των Jordan-Holder**:

Κάθε δύο συνθετικές σειρές μίας ομάδας G (εάν υπάρχουν) είναι ισοδύναμες.

Απόδειξη:

Άμεσο από το Θεώρημα του Schreier και τον ορισμό της συνθετικής σειράς.

- **Πρόταση**:

Μία κανονική σειρά $1 = G_0 \lhd G_1 \lhd ... \lhd G_n = G$ (1) είναι συνθετική αν και μόνο αν $\forall i \in \{0,1,2,...,n-1\}$ η G_{i+1}/G_i είναι απλή, μη-τετριμμένη ομάδα.

Απόδειξη:

Για το ευθύ, υποθέτουμε ότι η (1) είναι συνθετική σειρά. Τότε, $G_i \neq G_{i+1}$, δηλαδή η G_{i+1}/G_i είναι μη-τετριμμένη. Έστω τώρα ότι υπάρχει $i \in \{0,2,...,n-1\}$ τέτοιο ώστε η G_{i+1}/G_i να μην είναι απλή, δηλαδή ότι υπάρχει $1 \neq K \lhd G_{i+1}/G_i$ και $K \neq G_{i+1}/G_i$. Από το Θεώρημα της αντιστοιχίας $K = \Lambda/G_i$, όπου $G_i \lhd \Lambda \leq G_{i+1}$. Ακόμη, $1 \neq K \Rightarrow \Lambda \neq G_i$, $K \lhd G_{i+1}/G_i \Rightarrow \Lambda \lhd G_{i+1}$ και $K \neq G_{i+1}/G_i \Rightarrow \Lambda \neq G_{i+1}$. Από τα παραπάνω έπεται ότι η $1 = G_0 \lhd G_1 \lhd ... \lhd G_i \lhd \Lambda \lhd G_{i+1} \lhd ...G_n = G$ είναι μία γνήσια επιλέπτυνση της (1), το οποίο είναι άτοπο αφού η (1) είναι συνθετική σειρά.

Για το αντίστροφο, θεωρούμε μία κανονική σειρά $1 = G_0 \lhd G_1 \lhd ... \lhd G_n = G$ (1) για την οποία ισχύει ότι η G_{i+1}/G_i είναι απλή, μη-τετριμμένη ομάδα, $\forall i \in \{0,2,...,n-1\}$. Έστω ότι η (1) δεν είναι συνθετική σειρά. Τότε υπάρχει γνήσια επιλέπτυνση της (1), έστω $1 = G_0 \lhd G_1 \lhd ...G_i \lhd ... \lhd H \lhd G_{i+1} \lhd ...G_n = G$ (2), όπου H είναι η μεγαλύτερη υποομάδα που είναι όρος της (2) αλλά όχι της (1). Τότε $G_i \leq H \lhd G_{i+1}$, ενώ παράλληλα έχουμε ότι $G_i \lhd G_{i+1} \Rightarrow G_i \lhd H$. Αυτό όμως σημαίνει ότι $1 \neq H/G_i \lhd G_{i+1}/G_i$ και $H/G_i \neq G_{i+1}/G_i$. Ιδιαίτερα, η G_{i+1}/G_i δεν είναι απλή – άτοπο.

Μάθημα 12ο (Πέμπτη, 12/6/2014)

[*Συνέχεια στις κανονικές σειρές, επιλύσιμες ομάδες*]:

- **Πρόταση**:

Κάθε πεπερασμένη ομάδα G έχει συνθετική σειρά.

Απόδειξη:

Με επαγωγή στην $|G|$.

Εάν η G είναι απλή, τότε η $1 \lhd G$ είναι συνθετική σειρά της G.

Εάν η G δεν είναι απλή, τότε υπάρχει $H \leq G$ τέτοια ώστε $1 \neq H \lhd G$, $H \neq G \Rightarrow |H| < |G|$ και $|G/H| < |G|$. Από την υπόθεση της επαγωγής οι H και G/H έχουν συνθετική σειρά, έστω $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = H$, όπου οι H_{i+1}/H_i είναι απλές, και $1 = \Lambda_0 \lhd \Lambda_1 \lhd \ldots \lhd \Lambda_\rho = G/H$, όπου οι Λ_{i+1}/Λ_i είναι απλές. Από το Θεώρημα της αντιστοιχίας υπάρχουν $K_i \leq G$: $\Lambda_i = K_i/H$, με $K_i \lhd K_{i+1}$ αφού $\Lambda_i \lhd \Lambda_{i+1}$. Θεωρούμε τώρα την κανονική σειρά $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = H \lhd K_1 \lhd K_2 \lhd \ldots \lhd K_\rho = G$ (1). Παρατηρούμε ότι η $K_1/H \simeq {K_1/H}\big/{H/H} \simeq {\Lambda_1}\big/{\Lambda_0}$ και η $K_{i+1}/H \simeq {K_{i+1}/H}\big/{K_i/H} \simeq {\Lambda_{i+1}}\big/{\Lambda_i}$ είναι απλές ομάδες. Δηλαδή η (1) είναι συνθετική σειρά της G.

- **Παρατήρηση:**

1. Υπάρχουν άπειρες ομάδες που έχουν συνθετική σειρά. Για παράδειγμα, αν η G είναι μία άπειρη απλή ομάδα, τότε η $1 \lhd G$ είναι συνθετική σειρά της G.

- **Πρόταση**:

Έστω $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ (1) κανονική σειρά της G και $H \leq G$. Τότε, $H_i = H \cap G_i \Rightarrow H_i \lhd H_{i+1}$, δηλαδή η $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = H$ είναι κανονική σειρά της H και $H_{i+1}/H_i \simeq K_{i+1} \leq G_{i+1}/G_i$.

Απόδειξη:

Είναι $G_i \lhd G_{i+1} \Rightarrow H \cap G_i \lhd H \cap G_{i+1} \Rightarrow H_i \lhd H_{i+1}$ και $H_{i+1}/H_i = {H \cap G_{i+1}}\big/{H \cap G_i} = {H \cap G_{i+1}}\big/{(H \cap G_{i+1}) \cap G_i} \simeq {(H \cap G_{i+1})G_i}\big/{G_i} \leq {G_{i+1}}\big/{G_i}$, όπου η τελευταία ισότητα προκύπτει από το 2ο Θεώρημα ισομορφισμών.

- **Ορισμός επιλύσιμης σειράς και επιλύσιμης ομάδας**:

Έστω $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ (1) κανονική σειρά της G. Εάν η G_{i+1}/G_i είναι αβελιανή ομάδα $\forall i \in \{0,1,2,\ldots,n-1\}$, τότε η (1) λέγεται επιλύσιμη σειρά της G. Μία ομάδα λέγεται επιλύσιμη, εάν έχει επιλύσιμη σειρά.

- **Παραδείγματα:**

1. Κάθε αβελιανή ομάδα G είναι επιλύσιμη, αφού η $1 \lhd G$ είναι επιλύσιμη σειρά της.
2. Η διεδρική ομάδα $D_n = \langle \rho, \varepsilon \rangle$ είναι επιλύσιμη, αφού η $1 \lhd \langle \rho \rangle \lhd D_n$, είναι επιλύσιμη σειρά.
3. Η S_4 είναι επιλύσιμη, αφού η $1 \lhd V \lhd A_4 \lhd S_4$ είναι επιλύσιμη σειρά καθώς οι $V/1 \simeq V \simeq Z_2 \times Z_2$, $A_4/V \simeq Z_3$ και $S_4/A_4 \simeq Z_2$ είναι αβελιανές (υπενθυμίζουμε ότι $V = \{1,(12)(34),(13)(24),(14)(23)\}$).

- **Πρόταση**:

1. Επιλέπτυνση επιλύσιμης σειράς μίας ομάδας G, είναι επιλύσιμη σειρά της G.
2. Αν G είναι μία επιλύσιμη ομάδα, τότε κάθε συνθετική σειρά της G (αν έχει) είναι επιλύσιμη.
3. Μία απλή ομάδα είναι επιλύσιμη αν και μόνο αν έχει τάξη έναν πρώτο αριθμό.
4. Αν G είναι μία επιλύσιμη ομάδα και $H \leq G$, τότε η H είναι επιλύσιμη.
5. Αν G είναι μία επιλύσιμη ομάδα και $N \lhd G$, τότε η G/N είναι επιλύσιμη.
6. Αν G είναι μία ομάδα, $N \lhd G$ και οι N, G/N είναι επιλύσιμες, τότε η G είναι επιλύσιμη.
7. Μία πεπερασμένη ομάδα είναι επιλύσιμη αν και μόνο αν τα πηλίκα μίας συνθετικής της σειράς έχουν τάξη έναν πρώτο αριθμό.
8. Αν G, H είναι επιλύσιμες ομάδες, τότε η $G \times H$ είναι επιλύσιμη.

<u>Απόδειξη:</u>

1. Αφού η G είναι επιλύσιμη, τότε έχει επιλύσιμη σειρά. Έστω λοιπόν $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ (1) μία επιλύσιμη σειρά της G, δηλαδή οι G_{i+1}/G_i είναι αβελιανές. Θεωρούμε μία επιλέπτυνση της (1), έστω την $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_i \lhd \Lambda_1 \lhd \Lambda_2 \lhd G_{i+1} \lhd \ldots \lhd G_n = G$ (2). Τότε $\Lambda_1/G_i \leq G_{i+1}/G_i$, δηλαδή η Λ_1/G_i είναι αβελιανή ως υποομάδα αβελιανής ομάδας. Επίσης, από το $3^{ο}$ Θεώρημα ισομορφισμών $\Lambda_2/\Lambda_1 \simeq {\Lambda_2/G_i}\big/{\Lambda_1/G_i}$. Όμως $\Lambda_2/G_i \leq G_{i+1}/G_i$, δηλαδή η Λ_2/G_i είναι αβελιανή ως υποομάδα αβελιανής.

Έπεται ότι η Λ_2/Λ_1 είναι αβελιανή ως πηλίκο αβελιανής ομάδας. Συνεπώς η (2) είναι επιλύσιμη σειρά.

2. Άμεσο από το 1., το Θεώρημα του Schreier και τον ορισμό της συνθετικής σειράς.
3. Μία απλή ομάδα είναι επιλύσιμη αν και μόνο αν είναι αβελιανή. Όμως μία απλή και αβελιανή ομάδα έχει τάξη έναν πρώτο αριθμό (διαφορετικά θα είχε γνήσια μη-τετριμμένη υποομάδα, η οποία θα ήταν κανονική – ατοπο).
4. Αφού η G είναι επιλύσιμη, τότε έχει επιλύσιμη σειρά. Έστω λοιπόν $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ (1) μία επιλύσιμη σειρά της G, δηλαδή οι G_{i+1}/G_i είναι αβελιανές. Δείξαμε ότι η $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = H$ (2), όπου $H_i = H \cap G_i$, είναι κανονική σειρά της H, με $H_{i+1}/H_i \simeq K_{i+1} \leq G_{i+1}/G_i$. Άρα η H_{i+1}/H_i είναι αβελιανή ως ισόμορφη με υποομάδα αβελιανής ομάδας, συνεπως η (2) είναι επιλύσιμη σειρά της H. Δηλαδή η H είναι επιλύσιμη.
5. Έστω $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ (1) μία επιλύσιμη σειρά της G, δηλαδή οι G_{i+1}/G_i είναι αβελιανές, και $N \lhd G$. Παρατηρούμε ότι $G_iN \lhd G_{i+1}N$ και παίρνουμε την κανονική σειρά $1 = G_0N/N \lhd G_1N/N \lhd \ldots \lhd G_nN/N = G/N$ (2) της G/N. Τότε, από το 3ο Θεώρημα ισομορφισμών $\dfrac{G_{i+1}N/N}{G_1N/N} \simeq \dfrac{G_{i+1}N}{G_1N}$ και $\dfrac{G_{i+1}N}{G_iN} = \dfrac{G_{i+1}(G_iN)}{G_iN} \simeq$ (2ο Θεώρημα ισομορφισμών) $\simeq \dfrac{G_{i+1}}{G_{i+1} \cap G_iN} =$ $= \dfrac{G_{i+1}}{G_i(G_{i+1} \cap N)} \simeq \dfrac{G_{i+1}/G_i}{G_i(G_{i+1} \cap N)/G_i}$, επομένως η $\dfrac{G_{i+1}N/N}{G_1N/N}$ είναι αβελιανή ως πηλίκο της αβελιανής ομάδας G_{i+1}/G_i.
6. Έστω $1 = N_0 \lhd N_1 \lhd \ldots \lhd N_n = N$ (1) επιλύσιμη σειρά της N και $1 = \Lambda_0 \lhd \Lambda_1 \lhd \ldots \lhd \Lambda_n = G/N$ (2) επιλύσιμη σειρά της G/N. Τότε από το Θεώρημα της αντιστοιχίας $\Lambda_i = K_i/N$, με $K_i \lhd K_{i+1}$, για κάποια $K_i \leq G$, επομένως η $1 = N_0 \lhd N_1 \lhd \ldots \lhd N_n = N \lhd K_1 \lhd \ldots \lhd K_n = G$ είναι επιλύσιμη σειρά της G. Επομένως η G είναι επιλύσιμη.
7. Μία πεπερασμένη ομάδα G έχει πάντα συνθετική σειρά. Έστω ότι η G είναι επιλύσιμη. Τότε, έχει επιλύσιμη σειρά και υπάρχει συνθετική σειρά που είναι επιλέπτυνση αυτής της σειράς. Έπεται ότι η G έχει επιλύσιμη συνθετική σειρά. Τα πηλίκα της επιλύσιμης συνθετικής σειράς είναι απλές, αβελιανές ομάδες, επομένως έχουν τάξη έναν πρώτο αριθμό. Τώρα, μία συνθετική σειρά της G είναι ισοδύναμη με την επιλύσιμη συνθετική σειρά της, επομένως τα πηλίκα της είναι ισόμορφα με τα πηλίκα της επιλύσιμης συνθετικής σειράς της, επομένως τα πηλίκα της έχουν τάξη έναν πρώτο αριθμό. Αντίστροφα, αν η G έχει συνθετική σειρά της οποίας τα πηλίκα έχουν τάξη έναν πρώτο αριθμό, τότε τα πηλίκα αυτά είναι αβελιανές ομάδες. Επομένως η συνθετική αυτή σειρά της G είναι επιλύσιμη, συνεπώς η G είναι επιλύσιμη.

8. Έχουμε ότι $G \simeq G \times 1_H \lhd G \times H$ και $H \simeq {}^{G \times H}\!/_{G \times 1_H}$. Άρα, εάν θέσουμε $N = G \times 1_H$ έχουμε ότι $N \lhd G \times H$ και N, G/N επιλύσιμες ομάδες. Έπεται ότι η $G \times H$ είναι επιλύσιμη.

- **Πρόταση**:

Έστω G πεπερασμένη ομάδα και $|G| = p^m$ ή $|G| = p^m q$ ή $|G| = p^2 q^2$ ή $|G| = pqr$, όπου p,q,r πρώτοι αριθμοί. Τότε η G δεν είναι απλή, εκτός και αν η $|G|$ είναι πρώτος αριθμός.

<u>Απόδειξη:</u>

Εάν $|G| = p^m$ έχουμε δει ότι $Z(G) \neq 1$. Όμως $Z(G) \lhd G$ και συνεπώς η G δεν είναι απλή (εκτός αν $m = 1$). Επίσης, έχουμε δείξει ότι εάν $|G| = pqr$ τότε η G έχει κανονική Sylow υποομάδα, συνεπώς δεν είναι απλή. Οι περιπτώσεις $|G| = p^m q$ και $|G| = p^2 q^2$ θα αποδειχθούν αργότερα.

- **Πρόταση**:

Έστω G πεπερασμένη ομάδα και $|G| \in \{p^m,\ p^m q,\ p^2 q^2,\ pqr\}$, όπου p,q,r πρώτοι αριθμοί. Τότε η G είναι επιλύσιμη.

<u>Απόδειξη:</u>

Έστω $K \leq G$. Τότε $|K| \,|\, |G|$ και επομένως $|K| \in \{p^m,\ p^m q,\ p^2 q^2,\ pqr\}$. Εάν $\Lambda \lhd K$, τότε $|K/\Lambda| \,|\, |K| \Rightarrow |K/\Lambda| \in \{p^m,\ p^m q,\ p^2 q^2,\ pqr\}$. Έστω $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ (1) μία συνθετική σειρά της G. Τότε η G_{i+1}/G_i είναι απλή και από την προηγούμενη πρόταση έπεται ότι η $|G_{i+1}/G_i|$ είναι πρώτος αριθμός. Αυτό όμως σημαίνει ότι η G_{i+1}/G_i είναι κυκλική, άρα η G_{i+1}/G_i είναι αβελιανή. Δηλαδή η (1) είναι επιλύσιμη συνθετική σειρά της G. Έπεται ότι η G είναι επιλύσιμη.

- **Πρόταση**:

Έστω G πεπερασμένη ομάδα με $|G| = p^m q$, όπου p,q πρώτοι αριθμοί. Τότε η G δεν είναι απλή.

<u>Απόδειξη:</u>

Εάν $p = q$ τότε $|G| = p^{m+1}$, οπότε η G δεν είναι απλή.

Έστω $p \neq q$. Τότε $n_p \,|\, q \Rightarrow n_p = 1$ ή $n_p = q$. Εάν $n_p = 1$ τότε η G έχει κανονική Sylow p-υποομάδα, έστω P, με $|P| = p^m$ και $|G/P| = q$. Άρα η G δεν είναι απλή. Μάλιστα, $P \lhd G$ και P, G/P επιλύσιμες, απ' όπου έπεται ότι η G είναι επιλύσιμη.

Έστω τώρα $n_p = q$. Τότε, εάν $P_i \cap P_j = 1$ για κάθε δύο διαφορετικές Sylow p-υποομάδες P_i, P_j της G, υπάρχουν $q(p^m - 1)$ στοιχεία της G με τάξη μια δύναμη του p. Άρα υπάρχουν το πολύ q στοιχεία της G με άλλη τάξη. Συμπεραίνουμε ότι η G έχει το πολύ μία Sylow q-υποομάδα, έστω Q, η οποία θα είναι και κανονική. Ιδιαίτερα, η G δεν είναι απλή. Επιπλέον $Q \lhd G$ και $|Q| = q$, $|G/Q| = p^m$, δηλαδή οι Q, G/Q είναι επιλύσιμες, απ' όπου έπεται ότι η G είναι επιλύσιμη.

Έστω τώρα ότι υπάρχουν Sylow p-υποομάδες της G, οι οποίες δεν έχουν τετριμμένη τομή. Θέτουμε I την τομή δύο τέτοιων υποομάδων της G, όπου $|I|$ είναι η μέγιστη δυνατή. Τότε $I = P_1 \cap P_2$ για κάποιες P_1, P_2 Sylow p-υποομάδες της G. Όμως $\left.\begin{matrix} I \lneqq P_1 \Rightarrow I \lneqq N_{P_1}(I) = N_1 \\ I \lneqq P_2 \Rightarrow I \lneqq N_{P_2}(I) = N_2 \end{matrix}\right\} \Rightarrow I \lhd \langle N_1, N_2 \rangle = M$. Η M δεν είναι p-ομάδα, αφού τότε θα ήταν υποομάδα κάποιας Sylow p-υποομάδας P_a και $N_1 \le P_a \cap P_1$ με $|I| < |N_1|$ - άτοπο από επιλογή της I. Καθώς η M δεν είναι p-ομάδα και $M \le G$, συνεπάγεται ότι $q \,||M|$. Έστω K μία Sylow q-υποομάδα της M. Τότε $|P_1K| = \dfrac{|P_1| \cdot |K|}{|P_1 \cap K|} = \dfrac{p^m q}{1} = p^m q \Rightarrow G = P_1K$.

Δηλαδή, αν $g \in G$ τότε $g = p_1 k$, όπου $p_1 \in P_1$ και $k \in K$. Θεωρούμε την κανονική υποομάδα $\Lambda = \langle gIg^{-1} \,|\, g \in G \rangle \lhd G$. Όμως, $gIg^{-1} = p_1 kI(p_1 k)^{-1} = p_1 (kIk^{-1}) p_1^{-1}$ και καθώς $I \lhd K \le M$ έχουμε ότι $kIk^{-1} = I$, άρα $gIg^{-1} = p_1 I p_1^{-1}$. Καταλήγουμε πως $1 \lneqq I \le \Lambda = \{gIg^{-1} \,|\, g \in G\} = \{p_1 I p_1^{-1} \,|\, p_1 \in P_1\} \le P_1 \lneqq G$, δηλαδή $1 \lneqq \Lambda \lneqq G$ και $\Lambda \lhd G$. Επομένως η G δεν είναι απλή.

- **Παρατήρηση:**

1. Στην παραπάνω απόδειξη ισχυριστήκαμε ότι αν $I \lneqq P_1$, τότε $I \lneqq N_{P_1}(I)$. Αυτό έπεται από την πρόταση ότι εάν H είναι μία p-υποομάδα μίας πεπερασμένης ομάδας G και $p \,||G/H|$, τότε $H \lneqq N_G(H)$. Πράγματι, εάν θεωρήσουμε τη δράση της H στο σύνολο G/H, $* : Hx(G/H) \to G/H$, $h * xH \to hxH$, τότε η εξίσωση κλάσεων δίνει $|G/H| = |\mathrm{Fix}(G/H)| + \sum_{\substack{x \in T \\ x \notin \mathrm{Fix}(G/H)}} \dfrac{|H|}{|H_x|}$.

   Όμως $p \,||G/H|$ και $p \,| \sum_{\substack{x \in T \\ x \notin \mathrm{Fix}(G/H)}} \dfrac{|H|}{|H_x|}$, άρα $p \,|\mathrm{Fix}(G/H)|$. Επιπλέον, $\mathrm{Fix}(G/H) =$

   $= \{x \in G/H \,|\, T_x = x\} = \{xH \,|\, hxH = xH,\ \forall h \in H\} = \{xH \,|\, x^{-1}Hx = H\} = N_G(H)/H$.

   Δηλαδή $p \,|N_G(H)/H|$. Ιδιαιτέρως, $1 < |N_G(H)/H|$ άρα $H \lneqq N_G(H)$.

- **Εφαρμογή:**

1. Έστω G πεπερασμένη ομάδα με $p \mid |G|$ και P_1 μία Sylow p-υποομάδα της G, τέτοια ώστε $|P_1 : P \cap P_1| \geq p^k$ για κάθε Sylow p-υποομάδα της G, P, με $P \neq P_1$. Τότε να δείξετε ότι $n_p = 1 \left(\mathrm{mod} p^k\right)$. (υπόδειξη: θεωρείστε τη δράση της P_1 στο σύνολο $\Omega = \left\{K \mid K \text{ Sylow p-υποομάδα της } G\right\}$, $* : P_1 x \Omega \to \Omega$, $x * K = xKx^{-1}$).

Μάθημα 13° (Τετάρτη, 18/6/2014)

[*Εφαρμογές, η εναλλάσσουσα ομάδα* A_n]:

- **Πρόταση**:

Έστω G πεπερασμένη ομάδα με $|G| = p^2q^2$, όπου p,q πρώτοι αριθμοί. Τότε η G δεν είναι απλή.

Απόδειξη:

Εάν $p = q$ τότε $|G| = p^4$, οπότε η G δεν είναι απλή.

Έστω $p > q$. Τότε $n_p \mid q^2 \Rightarrow n_p = 1$ ή $n_p = q$ ή $n_p = q^2$. Επίσης $n_p = 1 (\mathrm{mod} p)$, άρα $n_p \neq q$, αφού για $n_p = q$ έχουμε ότι $q = 1(\mathrm{mod} p) \Rightarrow p \mid q-1 \Rightarrow p < q$ - άτοπο.

Εάν $n_p = 1$ τότε η G έχει κανονική Sylow p-υποομάδα, έστω P, με $|P| = p^2$. Άρα η G δεν είναι απλή.

Έστω τώρα $n_p = q^2$. Τότε, εάν $P_i \cap P_j = 1$ για κάθε δύο διαφορετικές Sylow p-υποομάδες P_i, P_j της G, υπάρχουν $q^2(p^2-1)$ στοιχεία της G με τάξη μια δύναμη του p. Άρα υπάρχουν το πολύ q^2 στοιχεία της G με άλλη τάξη. Συμπεραίνουμε ότι η G έχει το πολύ μία Sylow q-υποομάδα, έστω Q, η οποία θα είναι και κανονική. Ιδιαίτερα, η G δεν είναι απλή.

Εξετάζουμε τώρα την περίπτωση που $n_p = q^2$ και υπάρχουν Sylow p-υποομάδες της G, έστω P_1 και P_2, οι οποίες δεν έχουν τετριμμένη τομή. Θέτουμε $1 \neq I = P_1 \cap P_2$. Καθώς $|P_1| = |P_2| = p^2$, έπεται ότι οι P_1 και P_2 είναι αβελιανές. Συνεπώς $I \lhd P_1$, $I \lhd P_2 \Rightarrow 1 \neq I \lhd \langle P_1, P_2 \rangle = M$. Καθώς $|M| > |P_1| = p^2$, έχουμε ότι $|M| = p^2q$ ή $|M| = p^2q^2$. Εάν $|M| = p^2q^2$, τότε $M = G$ και επομένως $1 \neq I \lhd G$, δηλαδή η G δεν είναι απλή. Εάν $|M| = p^2q$, τότε $|G:M| = q$ και επομένως υπάρχει ομομορφισμός $\phi : G \to S_q$. Εάν $\ker\phi = 1$, τότε η G εμφυτεύεται στην S_q, δηλαδή $|G| = p^2q^2 \mid q! \Rightarrow p^2q \mid (q-1)!$, το οποίο είναι άτοπο. Άρα $1 \neq \ker\phi \lhd G$, επομενως η G δεν είναι απλή.

- **Εφαρμογή:**

1. Έστω G πεπερασμένη ομάδα με $|G| = 2^m p^n$, όπου p πρώτος αριθμός και $m = 1, 2, 3$ ή 4. Τότε η G είναι επιλύσιμη.

   Απάντηση:

   Εάν $p = 2$ τότε $|G| = 2^{m+n}$, οπότε η G είναι επιλύσιμη. Εξετάζουμε την περίπτωση $p \neq 2$.

Εάν $m=1$, τότε $|G|=2p^n \Rightarrow n_p \mid 2$ και $n_p=1(\mathrm{mod}p) \Rightarrow n_p=1$. Άρα η G έχει κανονική Sylow p-υποομάδα, έστω P, με $|P|=p^n$ και $|G/P|=|G:P|=2$. Επομένως $P \lhd G$ και P, G/P επιλύσιμες, άρα η G είναι επιλύσιμη.

Εάν $m=2$, τότε $|G|=4p^n$. Έστω P μία Sylow p-υποομάδα της G. Τότε $|G:P|=4$. Επομένως υπάρχει ομομορφισμός $\phi: G \to S_4$, με $\ker\phi \le P \Rightarrow |\ker\phi|=p^k$, άρα η $\ker\phi$ είναι επιλύσιμη. Ακόμα, $G/\ker\phi \le S_4$, άρα η $G/\ker\phi$ είναι επιλύσιμη ως υποομάδα επιλύσιμης ομάδας. Έχουμε λοιπόν $\ker\phi \lhd G$ και $\ker\phi$, $G/\ker\phi$ επιλύσιμες, άρα η G είναι επιλύσιμη.

Εάν $m=3$, τότε $|G|=8p^n$. Για $n=1$ είναι $|G|=8p=2^3p$, άρα η G είναι επιλύσιμη. Εξετάζουμε λοιπόν την περίπτωση $p \ne 2$ και $n \ge 2$. Από το Θεώρημα του Sylow είναι $n_p \mid 8$ και $n_p=1(\mathrm{mod}p) \Rightarrow p \mid n_p-1 \Rightarrow p<8$. Διακρίνουμε πάλι περιπτώσεις:

Εάν $n_p=1$ υπάρχει κανονική Sylow p-υποομάδα, έστω P, με $|P|=p^n$ και $|G/P|=|G:P|=8=2^3$. Δηλαδή $P \lhd G$ και P, G/P επιλύσιμες, άρα η G είναι επιλύσιμη.

Έστω $n_p \ne 1$ (θυμίζουμε ότι $n_p=|G:N_G(P)|$). Για $p=3$ έχουμε ότι $3 \mid n_3-1 \Rightarrow n_3=4$. Επομένως $|G:N_G(P)|=4$ και, όπως προηγουμένως, υπάρχει ομομορφισμός $\phi: G \to S_4$, με $\ker\phi \le N_G(P) \Rightarrow |\ker\phi| \mid 2\cdot 3^n$, άρα η $\ker\phi$ είναι επιλύσιμη. Ακόμα, $G/\ker\phi \le S_4$, άρα η $G/\ker\phi$ είναι επιλύσιμη ως υποομάδα επιλύσιμης ομάδας. Έχουμε λοιπόν $\ker\phi \lhd G$ και $\ker\phi$, $G/\ker\phi$ επιλύσιμες, άρα η G είναι επιλύσιμη.

Για $p=5$ έχουμε ότι $5 \mid n_5-1$ - άτοπο.

Για $p=7$ έχουμε ότι $7 \mid n_7-1 \Rightarrow n_7=8$. Εάν $P_i \cap P_j=1$ για κάθε δύο διαφορετικές Sylow 7-υποομάδες P_i, P_j της G, υπάρχουν $8(7^n-1)$ στοιχεία της G με τάξη μια δύναμη του 7. Άρα υπάρχουν το πολύ 8 στοιχεία της G με άλλη τάξη. Συμπεραίνουμε ότι η G έχει το πολύ μία Sylow 2-υποομάδα, έστω Q, η οποία θα είναι και κανονική, με $|Q|=2^3$ και $|G/Q|=|G:Q|=7^n$. Δηλαδή $Q \lhd G$ και Q, G/Q επιλύσιμες, άρα η G είναι επιλύσιμη.

Έστω τώρα ότι υπάρχουν Sylow 7-υποομάδες της G, έστω P_1 και P_2, με $1 \ne I = P_1 \cap P_2$ και $|I|$ η μέγιστη δυνατή. Τότε $|P_1 \cap P| \le |I|$ για κάθε Sylow 7-υποομάδα P της G, με $P \ne P_1$. Τότε $|P_1 : P \cap P_1| \ge |P_1 : I| = p^k$, για κάθε Sylow 7-υποομάδα P της G με $P \ne P_1$, συνεπώς $n_7=1(\mathrm{mod}7^k) \Rightarrow 8=1(\mathrm{mod}7^k) \Rightarrow 7^k \mid 7 \Rightarrow$

$\Rightarrow k=1$. Δηλαδή $|I|=7^{n-1}$. Τότε $\left.\begin{matrix} I \lneqq P_1 \Rightarrow I \lneqq N_{P_1}(I)=P_1 \\ I \lneqq P_2 \Rightarrow I \lneqq N_{P_2}(I)=P_2 \end{matrix}\right\} \Rightarrow I \lhd \langle P_1, P_2 \rangle = M$, όπου $|M|>7^n$. Άρα $|M|=2\cdot 7^n$ ή $|M|=4\cdot 7^n$ ή $|M|=8\cdot 7^n$.

Εάν $|M| = 2 \cdot 7^n$, τότε για $Q \leq M$ με $|Q| = 7^n$ έχουμε $Q \lhd M$, αφού $|M:Q| = 2$. Δηλαδή η M έχει μοναδική Sylow 7-υποομάδα. Άρα $P_1 \lhd M$ και $P_2 \lhd M$, από όπου έπεται ότι $P_1 = P_2$ - άτοπο.

Εάν $|M| = 4 \cdot 7^n$, τότε $|G:M| = 2 \Rightarrow M \lhd G$. Δηλαδή $1 \lhd I \lhd M \lhd G$. Ακόμη, $|G/M| = |G:M| = 2$ και $|M/I| = |M:I| = 4 \cdot 7 = 2^2 \cdot 7$. Συνεπώς, Δηλαδή $I \lhd M$ και I, M/I επιλύσιμες, άρα η M είναι επιλύσιμη. Ομοίως, $M \lhd G$ και M, G/M επιλύσιμες, άρα η G είναι επιλύσιμη.

Τέλος, εάν $|M| = 8 \cdot 7^n$, τότε $|G:M| = 1 \Rightarrow M = G$. Δηλαδή $I \lhd G$, με $|I| = 7^{n-1}$ και $|G/I| = |G:I| = 8 \cdot 7 = 2^3 \cdot 7$. Άρα $I \lhd G$ και I, G/I επιλύσιμες, άρα η G είναι επιλύσιμη.

- **Παρατήρηση:**

1. Εάν υπάρχει κανονική σειρά της G, έστω $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ και G_i/G_{i-1} είναι επιλύσιμη $\forall i$, τότε επαγωγικά μπορούμε να δείξουμε ότι η G είναι επιλύσιμη.

- **Θεώρημα του Burnside**:

Έστω G πεπερασμένη ομάδα με $|G| = p^m q^n$, όπου p,q πρώτοι αριθμοί. Τότε η G είναι επιλύσιμη.

- **Θεώρημα των Feit-Thompson**:

Έστω G πεπερασμένη ομάδα με $|G|$ περιττό αριθμό. Τότε η G είναι επιλύσιμη.

- **Πρόταση**:

Κάθε ελαχιστική (minimal) κανονική υποομάδα H μιας πεπερασμένης ομάδας G είναι της μορφής $H = \Theta \times \Theta \times \cdots \times \Theta$, όπου Θ απλή ομάδα.

<u>Απόδειξη:</u>

Με επαγωγή στην $|G|$.

Αν η G είναι απλή, τότε η πρόταση ισχύει για $H = \Theta = G$. Αν η G δεν είναι απλή και η H είναι απλή, τότε η πρόταση ισχύει για $H = \Theta$.

Έστω τώρα ότι η G και η H δεν είναι απλές, $1 \neq H \lneqq G$, $H \lhd G$. Έστω K ελαχιστική κανονική υποομάδα της H. Από επαγωγική υπόθεση έχουμε ότι $K = \Theta \times \Theta \times \cdots \times \Theta$, όπου Θ απλή ομάδα. Έστω ακόμα K_1, K_2,..., K_s οι συζυγείς της K στη G, όπου $s = |G : N_G(K)|$ και $K_i = g_i K g_i^{-1}$ για κάποιο $g_i \in G$. Τότε μπορεί να δειχθεί ότι $K_i \lhd H$, $1 \leq i \leq s$, και K_i ελαχιστική κανονική υποομάδα της H.

Πράγματι, $K_i = g_i K g_i^{-1} \leq g_i H g_i^{-1} = H$, αφού $H \lhd G$. Δηλαδή οι K_1, K_2,..., K_s είναι συζυγείς στην H. Έπεται ότι $K_i = h_i K h_i^{-1}$ για κάποιο $h_i \in H$. Έτσι, αν $h \in H$

έχουμε $hK_ih^{-1} = hh_iKh_i^{-1}h^{-1} = hh_iK(hh_i)^{-1} = K$, αφού $hh_i \in H$ και $K \lhd H$. Άρα $K_i \lhd H$. Επίσης K_i είναι ελαχιστική κανονική υποομάδα της H, αφού σε άλλη περίπτωση θα υπήρχε $\Lambda_i \lhd H$, $\Lambda_i \lneqq K_i$. Τότε όμως υπάρχει $h' \in H$ τέτοιο ώστε $\Lambda = h'\Lambda_i(h')^{-1} \lhd H$, $\Lambda \lneqq K$ - άτοπο από επιλογή της K.

Τότε $\langle K_1, K_2, \ldots, K_s\rangle = K_1K_2\cdots K_s \lhd G$ και $\langle K_1, K_2, \ldots, K_s\rangle = K_1K_2\cdots K_s \leq H$. Λόγω επιλογής της H είναι $\langle K_1, K_2, \ldots, K_s\rangle = K_1K_2\cdots K_s = H$. Άρα $H = K_1K_2\cdots K_s$. Επιλέγουμε K_1, K_2, ..., K_r τέτοια ώστε $K_1K_2\cdots K_r = K_1K_2\cdots K_s$ και $K_i \not\subset K_1K_2\cdots K_{i-1}$, $2 \leq i \leq r$. Τότε $K_i \cap K_1K_2\cdots K_{i-1} \lneqq K_i$, $K_i \cap K_1K_2\cdots K_{i-1} \lhd H$ και από την ελαχιστικότητα της K_i συνεπάγεται πως $K_i \cap K_1K_2\cdots K_{i-1} = 1$, $\forall i$. Επομένως $H = K_1 \times K_2 \times \cdots \times K_r$. Όμως από την ελαχιστικότητα της K_i έχουμε ότι $K_i = K = \Theta \times \Theta \times \cdots \times \Theta$, και το ζητούμενο έπεται.

- **Παρατηρήσεις:**

1. Αν $n \geq 3$, τότε η A_n παράγεται από 3-κύκλους. Πράγματι, αν $w \in A_n$ τότε η w είναι γινόμενο άρτιου πλήθους αντιμεταθέσεων. Όμως $(ab)(ac) = (acb)$ και $(ab)(cd) = (abc)(bcd)$.
2. Αν $n \geq 5$, τότε η A_n παράγεται από ζευγάρια ξένων αντιμεταθέσεων, δηλαδή από ζευγάρια της μορφής $(ab)(cd)$. Πράγματι, κάθε ζευγάρι της μορφής $(ab)(ac)$ γράφεται ως $(ab)(ac) = (ab)(de)(de)(ac)$.

Μάθημα 14ο (Πέμπτη, 19/6/2014)

[*Συνέχεια στην εναλλάσσουσα ομάδα A_n, παράγωγος σειρά ομάδας*]:

- **Θεώρημα:**

Έστω $n \geq 5$. Τότε:

i. Αν $1 \neq N \lhd S_n$ και $N \neq S_n$, τότε $N = A_n$.

ii. Η A_n είναι απλή ομάδα.

Απόδειξη του i. :

Έστω $1 \neq N \lhd S_n$ και $\sigma \in N$, $\sigma \neq 1$. Άρα υπάρχει $i : \sigma(i) \neq i$. Έστωσαν $j : j \neq i, \sigma(i)$, $\tau = (ij)$ και $\rho = \sigma\tau\sigma^{-1}\tau^{-1} \in N$, αφού $\sigma \in N$ και $N \lhd S_n \Rightarrow \tau\sigma^{-1}\tau^{-1} \in N$. Τότε $\rho \neq 1$. Πράγματι, εάν $\rho = 1$ τότε $\sigma\tau\sigma^{-1}\tau^{-1} = 1 \Rightarrow \sigma\tau = \tau\sigma \Rightarrow$ $\Rightarrow \sigma(\tau(i)) = \tau(\sigma(i)) \Rightarrow \sigma(j) = \sigma(i) \overset{\sigma \text{ 1-1}}{\Rightarrow} j = i$ - άτοπο.

Άρα $\rho \neq 1$ και $\rho = \sigma\tau\sigma^{-1}\tau^{-1} \in N$. Όμως η τ^{-1} είναι αντιμετάθεση ως αντίτροφη αντιμετάθεσης. Επίσης, η $\sigma\tau\sigma^{-1}$ είναι αντιμετάθεση ως συζυγής αντιμετάθεσης (υπενθυμίζουμε ότι οι συζυγείς μεταθέσεις έχουν τον ίδιο τύπο). Δηλαδή η ρ είναι γινόμενο 2 αντιμεταθέσεων. Έστω $\rho = (ab)(cd) \in N$. Αφού $\rho \in N$ και $N \lhd S_n$, έπεται ότι η N περιέχει όλες τις συζυγείς μεταθέσεις της ρ (κλάση συζυγίας της ρ), δηλαδή όλες τις μεταθέσεις που έχουν τον ίδιο τύπο με τη ρ. Διαπιστώνουμε λοιπόν ότι η N είτε περιέχει όλους τους 3-κύκλους είτε όλα τα ζευγάρια ξένων αντιμεταθέσεων, δηλαδή η N περιέχει ένα σύνολο γεννητόρων της A_n. Επομένως $A_n \leq N$. Όμως $|S_n : A_n| = |S_n : N| \cdot |N : A_n| \Rightarrow$ $\Rightarrow 2 = |S_n : N| \cdot |N : A_n| \Rightarrow |N : A_n| \mid 2 \Rightarrow |N : A_n| = 1$ ή $|N : A_n| = 2$. Εάν $|N : A_n| = 2$, τότε $|S_n : N| = 1 \Rightarrow N = S_n$ - άτοπο. Άρα $|N : A_n| = 1 \Rightarrow N = A_n$.

Απόδειξη του ii. :

Από το i. έχουμε ότι η A_n είναι ελαχιστική κανονική υποομάδα της S_n. Επομένως $A_n = \Theta \times \Theta \times \cdots \times \Theta$ (k φορές), όπου Θ απλή ομάδα. Όμως $|A_n| = \frac{n!}{2} \Rightarrow$ $2 \mid |A_n| \Rightarrow 2 \mid |\Theta|^k \Rightarrow 2 \mid |\Theta|$. Επομένως η Θ έχει στοιχείο τάξης 2 (βλ. παρατηρήσεις), δηλαδή υπάρχει $\rho \in \Theta : |\rho| = 2$. Έστω $\rho = \tau_1\tau_2 \cdots \tau_k$, όπου τ_i είναι αντιμεταθέσεις ξένες ανά δύο (και προφανώς αντιμετατίθενται). Τότε $\rho\tau_1 = \tau_1\rho \Rightarrow 1 \neq \rho = \tau_1\rho\tau_1^{-1} \Rightarrow \rho \in \Theta \cap \tau_1\Theta\tau_1^{-1}$. Όμως οι Θ, $\tau_1\Theta\tau_1^{-1}$ είναι κανονικές υποομάδες της A_n, που επιπλέον είναι απλές. Επομένως και η $\langle\rho\rangle \lhd A_n \Rightarrow \langle\rho\rangle \lhd \Theta$ - άτοπο. Έπεται ότι $\tau_1\Theta\tau_1^{-1} = \Theta$. Επιπλέον ισχύει ότι $a\Theta a^{-1} = \Theta \quad \forall a \in A_n$, αφού $\Theta \lhd A_n$. Έχουμε ακόμη $S_n / A_n = \langle \tau_1 A_n \rangle \Rightarrow S_n = \langle A_n, \tau_1 \rangle \Rightarrow$

$g\Theta g^{-1} = \Theta \quad \forall g \in S_n$, δηλαδή $\Theta \lhd S_n$ με $1 \neq \Theta \leq A_n$. Από το i. έχουμε ότι $A_n = \Theta \Rightarrow k = 1$ και A_n απλή.

- **Παρατηρήσεις:**

1. Αν G πεπερασμένη ομάδα με $2 \mid |G|$, τότε υπάρχει $a \in G : |a| = 2$. Πράγματι, έστω ότι η G δεν έχει στοιχείο τάξης 2. Τότε, αν $x \in G$ και $x \neq 1$, έχουμε ότι $x^2 \neq 1 \Leftrightarrow x \neq x^{-1}$. Άρα, τα στοιχεία της G πλην του ταυτοτικού, εμφανίζονται σε ζευγάρια. Αυτό σημαίνει ότι το πλήθος των στοιχείων της G, πλην του ταυτοτικού, είναι άρτιο. Τελικά, αν προσθέσουμε και το ταυτοτικό στοιχείο της G συμπεραίνουμε ότι η $|G|$ είναι περιττός αριθμός – άτοπο.
2. Για $n \geq 5$, η S_n δεν είναι επιλύσιμη, αφού η $1 \lhd A_n \lhd S_n$ είναι μία συνθετική σειρά της S_n, η οποία δεν είναι επιλύσιμη (αφού η A_n δεν είναι αβελιανή).

- **Εφαρμογές:**

1. Ποιες είναι οι κανονικές σειρές των S_3 και S_4;
2. Να δειχθεί ότι αν G απλή πεπερασμένη ομάδα, με $|G| = 60$, τότε $G \simeq A_5$ (υπόδειξη: δείξτε ότι δεν υπάρχει $K \leq G$ τέτοια ώστε $|G : K| = 4$ και ότι υπάρχει $K \leq G$ τέτοια ώστε $|G : K| = 5$).

- ***Ορισμός πλήρως αναλλοίωτης υποομάδας***:

Έστω G ομάδα και $A \leq G$. Η A λέγεται πλήρως αναλλοίωτη υποομάδα της G αν και μόνο αν για κάθε ενδομομορφισμό $f : G \to G$ ισχύει $f(A) \subseteq A$. Τότε γράφουμε $A \underset{\pi.\alpha.}{\leq} G$.

- ***Ορισμός χαρακτηριστικής υποομάδας***:

Έστω G ομάδα και $B \leq G$. Η B λέγεται χαρακτηριστική υποομάδα της G αν και μόνο αν για κάθε αυτομορφισμό $\rho : G \to G$ ισχύει $\rho(B) \subseteq B$ (μάλιστα ισχύει $\rho(B) = B$). Τότε γράφουμε $A \trianglelefteq G$.

- ***Ορισμός παραγώγου υποομάδας***:

Έστω G ομάδα. Τότε η $G' = [G,G] = \langle [g,h] \rangle, g,h \in G = \{ghg^{-1}h^{-1} \mid g,h \in G\}$ λέγεται παράγωγος υποομάδα της G.

- **Παρατηρήσεις:**

1. Αν $A \underset{\pi.\alpha.}{\leq} G$, τότε $A \trianglelefteq G$. Δηλαδή μία πλήρως αναλλοίωτη υποομάδα μίας ομάδας G είναι και χαρακτηριστική υποομάδα της G. Επίσης, μία χαρακτηριστική υποομάδα της G είναι κανονική υποομάδα της G.

2. Έστω $f: G \to G$ ομομορφισμός. Τότε $f\left(\left[g,h\right]\right) = f\left(ghg^{-1}h^{-1}\right) =$ $= f(g)f(h)f\left(g^{-1}\right)f\left(h^{-1}\right) = f(g)f(h)f(g)^{-1}f(h)^{-1} = \left[f(g),f(h)\right] \in G'$, δηλαδή $f(G') \le G'$, το οποίο σημαίνει ότι η G' είναι πλήρως αναλλοίωτη υποομάδα της G.
3. Έστω G ομάδα. Τότε $Z(G) \trianglelefteq G$, δηλαδή η $Z(G)$ είναι χαρακτηριστική υποομάδα της G.

- **Εφαρμογές:**

1. Να δειχθεί ότι $A \underset{\pi.\alpha.}{\le} B \underset{\pi.\alpha.}{\le} C \Rightarrow A \underset{\pi.\alpha.}{\le} C$.
2. Να δειχθεί ότι $A \trianglelefteq B \trianglelefteq C \Rightarrow A \trianglelefteq C$.
3. Να δειχθεί ότι $A \trianglelefteq B$ και $B \lhd C \Rightarrow A \lhd C$.
4. Να δειχθεί ότι κάθε υποομάδα κυκλικής ομάδας είναι πλήρως αναλλοίωτη.
5. Έστω $A,B \le G$ και $[A,B] = \left\langle [a,b] \right\rangle, a \in A, b \in B = \left\{ aba^{-1}b^{-1} \mid a \in A, b \in B \right\}$. Τότε να δειχθεί ότι $N \lhd G \Rightarrow [G,N] \le N$.
6. Να βρεθούν οι S_n', A_n' και D_n'.

- **Πρόταση:**

1. $G' = [G,G] \lhd G$ και η G/G' είναι αβελιανή.
2. Αν $N \lhd G$, τότε G/N αβελιανή $\Leftrightarrow G' \le N$.
3. Αν $A \le B$ και $B' \le A$, τότε $A \lhd B$.

<u>Απόδειξη:</u>

1. Έστω $k \in G$. Τότε, $\forall g,h \in G$ έχουμε $k\left[g,h\right]k^{-1} = kghg^{-1}h^{-1}k^{-1} = kghg^{-1}h^{-1}k^{-1} =$ $= \left(kgk^{-1}\right)\left(khk^{-1}\right)\left(kg^{-1}k^{-1}\right)\left(kh^{-1}k^{-1}\right) = \left(kgk^{-1}\right)\left(khk^{-1}\right)\left(kgk^{-1}\right)^{-1}\left(khk^{-1}\right)^{-1} \in G'$. Άρα $kG'k^{-1} \subseteq G'$, το οποίο σημαίνει ότι $G' \lhd G$. Άλλωστε έχουμε δείξει ότι η G' είναι πλήρως αναλλοίωτη υποομάδα της G, το οποίο σημαίνει ότι η G' είναι χαρακτηριστική υποομάδα της G, άρα είναι και κανονική υποομάδα της G. Ακόμη, G/G' αβελιανή $\Leftrightarrow (xG')(gG') = (gG')(xG')\ \forall x,g \in G \Leftrightarrow$ $\Leftrightarrow xgG' = gxG'\ \forall x,g \in G \Leftrightarrow x^{-1}g^{-1}xgG' = G'\ \forall x,g \in G \Leftrightarrow x^{-1}g^{-1}xg \in G'\ \forall x,g \in G$, το οποίο ισχύει από τον ορισμό της G'. Άρα όντως η G/G' είναι αβελιανή.
2. Έστω $N \lhd G$. Τότε G/N αβελιανή $\Leftrightarrow (xN)(gN) = (gN)(xN)\ \forall x,g \in G \Leftrightarrow$ $\Leftrightarrow xgN = gxN\ \forall x,g \in G \Leftrightarrow x^{-1}g^{-1}xgN = N\ \forall x,g \in G \Leftrightarrow x^{-1}g^{-1}xg \in N\ \forall x,g \in G \Leftrightarrow$ $\Leftrightarrow \left\{ xgx^{-1}g^{-1} \mid x,g \in G \right\} \in N \Leftrightarrow G' \le N$.
3. Έστω $A \le B$ και $B' \le A$. Έστω τώρα $a \in A$, $b \in B$. Τότε $bab^{-1}a^{-1} \in B' \le A \Rightarrow$ $\Rightarrow bab^{-1}a^{-1} \in A \overset{a^{-1} \in A}{\Rightarrow} bab^{-1} \in A$. Αφού το $a \in A$ ήταν τυχόν, έπεται ότι $bAb^{-1} \subseteq A$. Δηλαδή για το τυχόν $b \in B$ είναι $bAb^{-1} \subseteq A$, άρα $A \lhd B$.

- **Παρατηρήσεις:**

1. Η G/G' είναι αβελιανή.
2. Αν G/N αβελιανή τότε $G' \le N \Rightarrow G/N \simeq {G/G'}/{N/G'}$, δηλαδή κάθε ομάδα-πηλίκο μίας ομάδας G είναι ομάδα-πηλικό της G/G'.

- ***Ορισμός παραγώγου σειράς*:**

Έστω G ομάδα και $G^{(0)} = G$, $G^{(1)} = G' = [G,G]$, $G^{(2)} = [G',G'] = [G^{(1)},G^{(1)}]$ και γενικότερα $G^{(n)} = [G^{(n-1)},G^{(n-1)}]$. Τότε, παράγωγος σειρά της G ονομάζεται η σειρά $G = G^{(0)} \supseteq G' = G^{(1)} \supseteq G^{(2)} \supseteq \ldots \supseteq G^{(n-1)} \supseteq G^{(n)} \supseteq \ldots$.

- **Πρόταση:**

Αν G είναι μία επιλύσιμη ομάδα και $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ (1) μία επιλύσιμη σειρά της G, τότε $G^{(i)} \le G_{n-i}$ $\forall i$.

<u>Απόδειξη:</u>

Επαγωγικά: (για $i = 0$ ισχύει, αφού $G^{(0)} = G \le G = G_n$).

Για $i = 1$, θέλουμε να δείξουμε ότι $G^{(1)} = G' \le G_{n-1}$. Όμως η (1) είναι επιλύσιμη σειρά της G, άρα η $G_n/G_{n-1} = G/G_{n-1}$ είναι αβελιανή. Έπεται ότι $G' \le G_{n-1}$.

Για $i = k+1$, θέλουμε να δείξουμε ότι $G^{(k+1)} \le G_{n-(k+1)}$. Από την επαγωγική υπόθεση έχουμε ότι $G^{(k+1)} = [G^{(k)},G^{(k)}] \le [G_{n-k},G_{n-k}] = G^{(n-k+1)}$, δηλαδή $G^{(k+1)} \le G^{(n-k+1)}$. Όμως η G_{n-k}/G_{n-k-1} είναι αβελιανή και επομένως $G_{n-k}' \le G_{n-k-1} \Rightarrow$ $\Rightarrow [G_{n-k},G_{n-k}] \le G_{n-k-1} \Rightarrow G^{(n-k+1)} \le G_{n-k-1}$, άρα $G^{(k+1)} \le G^{(n-k+1)} \le G_{n-k-1} \Rightarrow G^{(k+1)} \le G_{n-(k+1)}$.

- **Παρατήρηση:**

1. Είδαμε ότι αν G είναι μία επιλύσιμη ομάδα, τότε η παράγωγος σειρά της G είναι μία επιλύσιμη σειρά της, η οποία έχει το μικρότερο δυνατό μήκος. Επιπλέον, υπάρχει επιλύσιμη σειρά της G που οι όροι της είναι πλήρως αναλλοίωτες υποομάδες της G.

- ***Ορισμός περιοδικής ομάδας*:**

Μία ομάδα G λέγεται περιοδική, εάν κάθε στοιχείο της G έχει πεπερασμένη τάξη.

- ***Ορισμός ελευθέρας στρέψης ομάδας (torsion free group)*:**

Μία ομάδα G λέγεται ελευθέρα στρέψης, εάν κάθε μη-τετριμμένο στοιχείο της G έχει άπειρη τάξη.

- **Εφαρμογές:**

1. Εάν $A,B \le G$, $N \lhd G$ τότε να δειχθεί ότι $[AN/N, BN/N] = {[A,B]N}/{N}$.
2. Εάν G είναι μία επιλύσιμη περιοδική ομάδα, τότε να δειχθεί ότι η G περιέχει κανονική αβελιανή p-ομάδα, για κάποιον πρώτο αριθμό p.
3. Έστω G ομάδα και $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ (1), $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$ (2) δύο κανονικές σειρές της, τέτοιες ώστε οι G_{i+1}/G_i και H_{i+1}/H_i να είναι κυκλικές. Να δειχθεί ότι το πλήθος των απείρων κυκλικών πηλίκων της (1) ισούται με το πλήθος των απείρων κυκλικών πηλίκων της (2).
4. Εάν $H \lhd G$, $K \lhd G$ και οι G/H, G/K είναι επιλύσιμες, τότε να δειχθεί ότι η ${G}/{H \cap K}$ είναι επίσης επιλύσιμη.
5. Να εξετασθεί αν μία ομάδα G τάξης 72, 84, 90, 300, 144 είναι επιλύσιμη.
6. Εάν G πεπερασμένη, μη-αβελιανή ομάδα με $|G| = p^3$, τότε να δείξετε ότι $G' = Z(G)$.

- **Θεώρημα του P. Hall:**

Αν G είναι μία επιλύσιμη ομάδα με $|G| = mn$, όπου $(m,n) = 1$, τότε:

i. Υπάρχει υποομάδα $A \le G$ τέτοια ώστε $|A| = m$.

ii. Αν $A,B \le G$ με $|A| = |B| = m$, τότε οι A και B είναι συζυγείς.

- **Θεώρημα των Schur-Zassenhaus:**

Αν G ομάδα με $A \lhd G$, όπου A αβελιανή ομάδα και $(A, G/A) = 1$, τότε υπάρχει $K \le G$ με $G = KA$ και $K \cap A = 1$ (δηλαδή η G είναι το ημιευθύ γινόμενο των A και K).

- **Θεώρημα:**

Μία πεπερασμένα παραγόμενη και επιλύσιμη ομάδα είναι πεπερασμένη.

- **Παρατηρήσεις:**

1. Το 1902 ο Burnside διατύπωσε την εικασία ότι μία πεπερασμένα παραγόμενη και περιοδική ομάδα είναι πεπερασμένη.
2. Το 1964 οι Golod-Shafarevich έδειξαν ότι η εικασία του Burnside ήταν λανθασμένη.
3. Το 1968 οι Adian-Norikov απέδειξαν ότι υπάρχει άπειρη ομάδα με πεπερασμένο εκθέτη n, αρκεί n περιττός και $n \ge 665$.
4. Το 1994 ο Zelmanof απέδειξε ότι μία προσεγγιστικά πεπερασμένα παραγόμενη ομάδα είναι πεπερασμένη.
5. $D_\infty = \langle \tau, \varepsilon \rangle$, $\langle \tau \rangle \simeq \mathbb{Z}$, $\varepsilon\tau\varepsilon^{-1} = \tau^{-1}$, $\varepsilon^2 = 1$. Εάν $x = \varepsilon$ και $y = \tau\varepsilon$, τότε $x^2 = \varepsilon^2 = 1$, $y^2 = (\tau\varepsilon)^2 = \tau\varepsilon\tau\varepsilon = \tau\tau^{-1} = 1$ και $xy = \varepsilon\tau\varepsilon = \tau^{-1}$. Επομένως το σύνολο των

στοιχείων πεπερασμένης ταξης της D_∞, έστω A, δεν είναι υποομάδα της, αφού $|\tau| = \infty \Rightarrow \tau \notin A$, ενώ $\tau = (xy)^{-1}$, δηλαδή $x, y \in A$ αλλά $(xy)^{-1} \notin A$.

6. Έστω G μία πεπερασμένα παραγόμενη ομάδα. Τότε, αν $H \leq G$ με $|G:H| < \infty$, τότε η H είναι επίσης πεπερασμένα παραγόμενη ομάδα.

Μάθημα 15ο (Τετάρτη, 25/6/2014)

[*Πεπερασμένα παραγόμενες ομάδες, Μηδενοδύναμες ομάδες*]:

- **Πρόταση**:

Έστω G πεπερασμένα παραγόμενη ομάδα και $H \leq G$ με $|G:H| < \infty$. Τότε και η H είναι πεπερασμένα παραγόμενη ομάδα.

- **Πρόταση**:

Αν G επιλύσιμη ομάδα, η οποία είναι πεπερασμένα παραγόμενη και περιοδική. Τότε η G είναι πεπερασμένη.

Απόδειξη:

Με επαγωγή στο μήκος της παραγώγου σειράς της G.

Αν το μήκος της παραγώγου σειράς είναι 1, τότε η G είναι αβελιανή. Τότε οι γεννήτορές της μετατίθενται και έπεται ότι η G είναι πεπερασμένη.

Έστω τώρα $G = G^{(0)} \supseteq G' = G^{(1)} \supseteq \ldots G^{(n)} \supseteq G^{(n+1)} = 1$ (1) είναι η παράγωγος σειρά της G. Τότε η παράγωγος σειρά της G' έχει μικρότερο μήκος, διαφορετικά η $G = 1$ (αφού η G είναι επιλύσιμη, βλ. εφαρμογή 3 παρακάτω). Επίσης, η G' είναι περιοδική ομάδα, ως υποομάδα περιοδικής ομάδας ($G' \leq G$). Ακόμη, η G είναι πεπερασμένα παραγόμενη $\Rightarrow$ η G/G' είναι πεπερασμένα παραγόμενη ομάδα, και η G είναι περιοδική $\Rightarrow$ η G/G' είναι περιοδική ομάδα. Δηλαδή η G/G' είναι πεπερασμένα παραγόμενη, περιοδική και επιλύσιμη (ως αβελιανή) ομάδα, άρα από επαγωγική υπόθεση έχουμε ότι η G/G' είναι πεπερασμένη. Δηλαδή $|G/G'| < \infty \Rightarrow |G:G'| < \infty$.

Έχουμε λοιπόν ότι η G είναι πεπερασμένα παραγόμενη ομάδα και $G' \leq G$ με $|G:G'| < \infty$. Από την προηγούμενη πρόταση έπεται ότι η G' είναι πεπερασμένα παραγόμενη ομάδα. Έχουμε τότε ότι η G' είναι επιλύσιμη ομάδα, η οποία είναι πεπερασμένα παραγόμενη και περιοδική. Από την επαγωγική υπόθεση έπεται ότι η G' είναι πεπερασμένη. Τελικά έχουμε ότι $|G| = |G:G'| \cdot |G'| < \infty$, αφού οι G/G' και G' είναι πεπερασμένες ομάδες. Άρα η G είναι πεπερασμένη.

- **Εφαρμογές:**

1. Έστω G πεπερασμένα παραγόμενη ομάδα. Τότε, αν $N \lhd G$ να δειχθεί ότι η G/N είναι πεπερασμένα παραγόμενη ομάδα.
2. Έστω $N \lhd G$ και N, G/N πεπερασμένα παραγόμενες ομάδες. Να δειχθεί ότι η G είναι πεπερασμένα παραγόμενη.
3. Αν G επιλύσιμη ομάδα και $G = G'$, τότε να δείξετε ότι $G = 1$.

- **Ορισμός κεντρικής σειράς ομάδας και μηδενοδύναμης ομάδας:**

Έστω G ομάδα. Μία κανονική σειρά $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ (1) της G λέγεται κεντρική σειρά της G, εάν $\forall i$ ισχύει $G_i \lhd G$ και $G_{i+1}/G_i \leq Z(G/G_i)$. Εάν μία ομάδα έχει μία κεντρική σειρά, τότε λέγεται μηδενοδύναμη ομάδα.

- **Παρατήρηση:**

1. Ισοδύναμα με τον παραπάνω ορισμό της κεντρικής σειράς μίας ομαδας G, μία κανονική σειρά $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ (1) της G λέγεται κεντρική σειρά της G, εάν $\forall i$ ισχύει $[G_{i+1}, G] \leq G_i$, όπου $[G_i, G] = \left\langle aga^{-1}g^{-1} \right\rangle \mid a \in G_i, g \in G$. Είναι $[G_{i+1}, G] \leq G_i \Leftrightarrow aga^{-1}g^{-1} \in G_i \ \forall a \in G_{i+1}, g \in G \Leftrightarrow G_iag = G_iga \ \forall a \in G_{i+1}, g \in G \Leftrightarrow$ $\Leftrightarrow G_i \lhd G$ και $G_iaG_ig = G_igG_ia \ \forall a \in G_{i+1}, g \in G \Leftrightarrow G_i \lhd G$ και $G_ia \in Z(G/G_i) \ \forall a \in G_{i+1}$ $\Leftrightarrow G_i \lhd G$ και $G_{i+1}/G_i \leq Z(G/G_i)$.

- **Παράδειγμα:**

1. Έστω G πεπερασμένη ομάδα με $|G| = p^k$, όπου p πρώτος αριθμός. Τότε η G είναι μηδενοδύναμη. Πράγματι, γνωρίζουμε ότι $J_1(G) = Z(G) \neq 1$. Τότε, είτε $J_1(G) = Z(G) = G$, οπότε η G είναι αβελιανή, είτε $J_1(G) = Z(G) \neq G \Rightarrow$ $G/J_1(G) \neq 1$, δηλαδή η $G/J_1(G)$ είναι p-ομάδα (και γνήσια υποομάδα της G), επομένως $Z(G/J_1(G)) \neq 1$. Θέτουμε τώρα $J_2(G)/J_1(G) = Z(G/J_1(G)) \neq 1$. Τότε $J_1(G) \lhd J_2(G)$ και αν $J_2(G) = G$ η $1 = J_0(G) \lhd J_1(G) \lhd J_2(G) = G$ είναι μία κεντρική σειρά της G. Αν $J_2(G) \neq G$, τότε η $G/J_2(G)$ είναι p-ομάδα και $Z(G/J_2(G)) \neq 1$. Ομοίως, θέτουμε $J_3(G)/J_2(G) = Z(G/J_2(G)) \neq 1$ και, συνεχίζοντας, παίρνουμε τη σειρά $1 = J_0(G) \underset{\neq}{\lhd} J_1(G) \underset{\neq}{\lhd} J_2(G) \underset{\neq}{\lhd} J_3(G) \underset{\neq}{\lhd} \ldots$. Καθώς η G είναι πεπερασμένη, υπάρχει $i \in \mathbb{N}$ με $J_{i-1}(G) \neq G$ και $J_i(G) = G$. Τότε η $1 = J_0(G) \underset{\neq}{\lhd} J_1(G) \underset{\neq}{\lhd} J_2(G) \underset{\neq}{\lhd} J_3(G) \underset{\neq}{\lhd} \ldots \underset{\neq}{\lhd} J_{i-1}(G) \underset{\neq}{\lhd} J_i(G) = G$ είναι μία κεντρική σειρά της G.

- **Παρατηρήσεις:**

1. Αν G μηδενοδύναμη ομάδα και $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ (1) μία κεντρική σειρά της με μη-τετριμμένα πηλίκα, δηλαδή $G_i \lhd G$ και $1 \neq G_{i+1}/G_i \leq Z(G/G_i)$, τότε $G_1/G_0 \leq Z(G/G_0) \Rightarrow 1 \neq G_1 \leq Z(G)$. Ιδιαίτερα $Z(G) \neq 1$. Δηλαδή κάθε μηδενοδύναμη ομάδα έχει μη-τετριμμένο κέντρο.
2. Από την προηγούμενη παρατήρηση έπεται ότι, για $n \geq 3$, η S_n δεν είναι μηδενοδύναμη ομάδα (αφού $Z(S_n) = 1$).
3. Αφού $G_{i+1}/G_i \leq Z(G/G_i)$ $\forall i$, έπεται ότι η G_{i+1}/G_i είναι αβελιανή ομάδα $\forall i$. Δηλαδή η (1) είναι επιλύσιμη σειρά της G. Άρα κάθε μηδενοδύναμη ομάδα είναι επιλύσιμη.

4. Το αντίστροφο δεν ισχύει. Για παράδειγμα, η S_3 είναι επιλύσιμη ομάδα, αλλά δεν είναι μηδενοδύναμη. Συνεπώς υπάρχουν επιλύσιμες ομάδες που δεν είναι μηδενοδύναμες.

- **Εφαρμογές:**

1. Εάν $A,B \le G$, $N \lhd G$ τότε να δειχθεί ότι $[AN/N, BN/N] = [A,B]N/N$.
2. Αν $G = A \times B$, $A_1, A_2 \le A$ και $B_1, B_2 \le B$, τότε να δειχθεί ότι $[A_1 \times B_1, A_2 \times B_2] = [A_1, A_2] \times [B_1, B_2]$.
3. Αν $A,B,C \le G$, $B \lhd G$, $C \lhd G$ και $A/B \le Z(G/B)$, τότε να δείξετε ότι $AC/BC \le Z(G/BC)$.

- **Πρόταση**:

1. Κάθε υποομάδα μηδενοδύναμης ομάδας είναι μηδενοδύναμη ομάδα.
2. Κάθε ομάδα-πηλίκο μηδενοδύναμης ομάδας είναι μηδενοδύναμη ομάδα.
3. Αν H,K είναι μηδενοδύναμες ομάδες, τότε η $H \times K$ είναι μηδενοδύναμη ομάδα.

<u>Απόδειξη:</u>

Έστω G μηδενοδύναμη ομάδα και $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ μία κεντρική σειρά της, δηλαδή $G_i \lhd G$ και $G_{i+1}/G_i \le Z(G/G_i)$ $\forall i$.

1. Έστω $H \le G$. Τότε η $1 = G_0 \cap H \le G_1 \cap H \le \ldots \le G_n \cap H = H$ είναι μία κεντρική σειρά της H, άρα η H είναι μηδενοδύναμη . Πράγματι, έχουμε $G_i \lhd G \Rightarrow G_i \cap H \lhd G \cap H = H$ και $[G_{i+1} \cap H, G \cap H] = [G_{i+1}, G] \cap H \le G_i \cap H$.
2. Έστω $N \lhd G$. Τότε η $1 = G_0N/N \le G_1N/N \le \ldots \le G_nN/N = G/N$ είναι μία κεντρική σειρά της G/N, αφού $G_i \lhd G \Rightarrow G_iN/N \lhd GN/N = G/N$ και $[G_{i+1}N/N, GN/N] = [G_{i+1}, G]N/N \le G_iN/N$.
3. Έστω H μηδενοδύναμη ομάδα και $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = H$ μία κεντρική σειρά της, K μηδενοδύναμη ομάδα και $1 = K_0 \lhd K_1 \lhd \ldots \lhd K_m = K$ μία κεντρική σειρά της. Τότε η $1 = H_0 \times K_0 \lhd H_1 \times K_1 \lhd \ldots \lhd H_s \times K_s = H \times K$, όπου $s = \max(m,n)$, είναι μία κεντρική σειρά της $H \times K$. Πράγματι, $H_i \lhd H$ και $K_i \lhd K \Rightarrow H_i \times K_i \lhd H \times K$ και $[H_{i+1} \times K_{i+1}, H \times K] = [H_{i+1}, H] \times [K_{i+1}, K] \le H_i \times K_i$.

- ***Ορισμός υποκανονικής υποομάδας:***

Έστω G ομάδα. Μία υποομάδα $H \le G$ λέγεται υποκανονική υποομάδα της G, αν υπάρχει μία σειρά της $H = H_0 \lhd H_1 \lhd \ldots \lhd H_k = G$.

- **Πρόταση**:

Έστω G μηδενοδύναμη ομάδα. Τότε:

1. Αν $H \leq G$ τότε η H είναι υποκανονική υποομάδα της G.
2. Αν $H \lneqq G$ τότε $H \lneqq N_G(H)$.

Απόδειξη:

1. Καθώς η G είναι μηδενοδύναμη ομάδα, τότε έχει μία κεντρική σειρά, έστω $1 = G_0 \lhd G_1 \lhd ... \lhd G_n = G$, δηλαδή $G_i \lhd G$ και $G_{i+1}/G_i \leq Z(G/G_i)$ $\forall i$. Τότε, $G_i \lhd G \Rightarrow HG_i \leq G$ και $H = HG_0 \leq HG_1 \leq ... \leq HG_i \leq HG_{i+1} \leq ... \leq HG_n = G$. Αρκεί λοιπόν να δείξω ότι $HG_i \lhd HG_{i+1}$ $\forall i$. Όμως $G_{i+1}/G_i \leq Z(G/G_i) \Rightarrow xG_iy_{i+1}G_i = y_{i+1}G_ixG_i$ $\forall x \in G, y_{i+1} \in G_{i+1} \Rightarrow xy_{i+1}G_i = y_{i+1}xG_i$ $\forall x \in G, y_{i+1} \in G_{i+1}$. Ακόμη, $HG_i \lhd HG_{i+1} \Leftrightarrow hg_{i+1}h_1g_i(hg_{i+1})^{-1} \in HG_i \Leftrightarrow hg_{i+1}h_1g_ig_{i+1}{}^{-1}h^{-1} \in HG_i \overset{G_i \lhd G}{\Leftrightarrow}$ $\overset{G_i \lhd G}{\Leftrightarrow} hg_{i+1}h_1g_{i+1}{}^{-1}g_i{}'h^{-1} \in HG_i \overset{xy_{i+1}G_i = y_{i+1}xG_i}{\Leftrightarrow} hg_{i+1}g_{i+1}{}^{-1}h_1g_i{}'h^{-1} \in HG_i \Leftrightarrow hh_1g_i{}'h^{-1} \in HG_i \overset{G_i \lhd G}{\Leftrightarrow}$ $\overset{G_i \lhd G}{\Leftrightarrow} hh_1h^{-1}g_i{}'' \in HG_i$, το οποίο ισχύει.
2. Αφού $H \lneqq G$ και G μηδενοδύναμη ομάδα, από το 1. έχουμε ότι η H είναι υποκανονική υποομάδα της G, δηλαδή υπάρχει $H = H_0 \lhd H_1 \lhd ... \lhd H_k = G$. Όμως $H \lneqq G$, άρα υπάρχει $m \in \mathbb{N} : H = H_m \lhd\!\!\!\!\neq H_{m+1} \Rightarrow H_{m+1} \leq N_G(H)$. Επομένως $H \lhd\!\!\!\!\neq H_{m+1} \leq N_G(H) \Rightarrow H \lneqq N_G(H)$.

- **Πρόταση**:

Έστω G πεπερασμένη ομάδα και P μία Sylow p-υποομάδα της G. Τότε, αν $N_G(P) \leq K \leq G$ έπεται ότι $N_G(K) = K$.

Απόδειξη:

Έχουμε προφανώς ότι $K \leq N_G(K)$. Για το αντίστροφο, έστω $x \in N_G(K)$. Τότε $xPx^{-1} \leq xKx^{-1} = K$, αφού $K \lhd N_G(K)$. Άρα οι P και xPx^{-1} είναι Sylow p-υποομάδες της K, δηλαδή είναι συζυγείς στην K. Επομένως υπάρχει $y \in K$: $yPy^{-1} = xPx^{-1} \Rightarrow x^{-1}yPy^{-1}x = P \Rightarrow x^{-1}yP(x^{-1}y)^{-1} = P \Rightarrow x^{-1}y \in N_G(P) \leq K$. Συνεπώς, $x^{-1}y \in K \Rightarrow x^{-1} \in K \Rightarrow x \in K$, αφού $y \in K$. Άρα $N_G(K) \leq K$ και το ζητούμενο έπεται.

- **Πρόταση**:

Έστω G πεπερασμένη ομάδα. Τότε, οι ακόλουθες προτάσεις είναι ισοδύναμες:

1. Η G είναι μηδενοδύναμη ομάδα.
2. Κάθε υποομάδα της G είναι υποκανονική.
3. Αν $H \lneqq G$ τότε $H \lneqq N_G(H)$.
4. Η G είναι το ευθύ γινόμενο των Sylow υποομάδων της.
5. Αν $m \mid |G|$, τότε υπάρχει $K \lhd G$ με $|K| = m$.

<u>Απόδειξη:</u>

1. $\Rightarrow$ 2.

   Έχει δειχθεί σε προηγούμενη πρόταση.

2. $\Rightarrow$ 3.

   Έχει δειχθεί σε προηγούμενη πρόταση.

3. $\Rightarrow$ 4.

   Πρώτα θα δείξουμε ότι αν $P \in Syl_p(G)$, τότε $P \lhd G$. Έχουμε ότι $P \leq N_G(P) \leq G$ και από την προηγούμενη πρόταση έπεται ότι $N_G(N_G(P)) = N_G(P)$. Τώρα, αν $N_G(P) \lneqq G$, τότε $N_G(P) \lneqq N_G(N_G(P))$ - άτοπο. Άρα $N_G(P) = G \Rightarrow P \lhd G$.

   Έστω λοιπόν $P_1, P_2, \ldots, P_k$ οι Sylow p_i-υποομάδες της G, όπου $p_i \mid |G|$. Τότε, αφού $P_i \lhd G$, είναι $\langle P_1, P_2, \ldots, P_k \rangle = P_1 P_2 \cdots P_k$ και $|P_1 P_2| = \frac{|P_1| \cdot |P_2|}{|P_1 \cap P_2|} = |P_1| \cdot |P_2|$. Επαγωγικά λοιπόν $|P_1 P_2 \cdots P_k| = |P_1| \cdot |P_2| \cdots |P_k| = |G|$ και $P_i \cap P_1 P_2 \cdots P_{i-1} P_{i+1} \cdots P_k = 1 \quad \forall i$, άρα $G = P_1 \times P_2 \times \cdots \times P_k$.

4. $\Rightarrow$ 5.

   Η συνεπαγωγή έπεται από την παρακάτω εφαρμογή και την υπενθύμιση που θα ακολουθήσει.

5. $\Rightarrow$ 4.

   Αν $|G| = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$, όπου $p_1, p_2, \ldots, p_k$ διακεκριμένοι πρώτοι αριθμοί, τότε οι Sylow υποομάδες της G είναι κανονικές στην G και συνεπώς η G είναι το ευθύ γινόμενο των Sylow υποομάδων της.

4. $\Rightarrow$ 1.

   Κάθε Sylow υποομάδα είναι μηδενοδύναμη ως p-ομάδα. Άρα και η G είναι μηδενοδύναμη, ως ευθύ γινόμενο πεπερασμένου πλήθους μηδενοδύναμων ομάδων.

- **Εφαρμογή:**

1. Εάν $|G| = p^k$, όπου p πρώτος αριθμός, τότε να δειχθεί ότι υπάρχει $K_i \lhd G$ με $|K_i| = p^i \quad \forall i \leq k$.

Μάθημα 16° (Πέμπτη, 26/6/2014)

[Ανωτέρα και κατωτέρα κεντρική σειρά ομάδας, εισαγωγή στο Θεώρημα δομής για πεπερασμένα παραγόμενες αβελιανές ομάδες]:

- **Υπενθύμιση:**

Έστω G ομάδα με $G = A \times B$, δηλαδή $A \lhd G$, $B \lhd G$, $G = AB$ και $A \cap B = 1$.
Τότε, αν $a \in A \leq G$ και $b \in B \leq G$, έπεται ότι $ab = ba$. Πράγματι, έχουμε ότι $A \lhd G \Rightarrow bab^{-1} \in A \Rightarrow bab^{-1}a^{-1} \in A$ και $B \lhd G \Rightarrow ab^{-1}a^{-1} \in B \Rightarrow bab^{-1}a^{-1} \in B$. Δηλαδή $bab^{-1}a^{-1} \in A$, $bab^{-1}a^{-1} \in B \Rightarrow bab^{-1}a^{-1} \in A \cap B = 1 \Rightarrow bab^{-1}a^{-1} = 1 \Rightarrow ab = ba$.
Επίσης, αν $N \lhd A$ έπεται ότι $N \lhd G$. Δηλαδή, αν μία υποομάδα είναι κανονική σε έναν παράγοντα, τότε είναι κανονική και σε όλη την ομάδα.

- **Παράδειγμα:**

1. Έστω $H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a,b,c \in \mathbb{Z} \right\} \leq GL(3,\mathbb{Z})$. Εύκολα βλέπουμε ότι $Z(H) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| b \in \mathbb{Z} \right\}$. Παρατηρούμε ότι υπάρχει επιμορφισμός $\phi : H \to \mathbb{Z} \times \mathbb{Z}$, $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \to (a,c)$, με $\ker\phi = Z(H)$. Επομένως $H/Z(H) \simeq \mathbb{Z} \times \mathbb{Z}$, δηλαδή η $H/Z(H)$ είναι αβελιανή ομάδα και συνεπώς $Z(H/Z(H)) = H/Z(H)$. Άρα η $1 \lhd Z(H) \lhd H$ είναι μία κεντρική σειρά της H, επομένως η H είναι μία άπειρη μηδενοδύναμη ομάδα.

- ***Ορισμός ανωτέρας κεντρικής σειράς ομάδας:***

Έστω G ομάδα. Ορίζουμε επαγωγικά μία ακολουθία υποομάδων της G ως εξής: $J_0(G) = 1$, $J_1(G) = Z(G/J_0(G)) = Z(G)$, $J_2(G)/J_1(G) = Z(G/J_1(G))$ και γενικά $J_{i+1}(G)/J_i(G) = Z(G/J_i(G))$. Τότε $J_i(G) \lhd G$ $\forall i$, και η ακολουθία $1 = J_0(G) \lhd J_1(G) \lhd \ldots \lhd J_i(G) \lhd J_{i+1}(G) \lhd \ldots$ (1) ονομάζεται ανωτέρα κεντρική σειρά της G.

- ***Ορισμός κατωτέρας κεντρικής σειράς ομάδας:***

Έστω G ομάδα. Ορίζουμε επαγωγικά μία ακολουθία υποομάδων της G ως εξής: $\gamma_1(G) = G$, $\gamma_2(G) = [\gamma_1(G), G] = [G,G] = G'$, $\gamma_3(G) = [\gamma_2(G), G] = [G', G]$ και γενικά $\gamma_{i+1}(G) = [\gamma_i(G), G]$. Τότε $\gamma_i(G) \lhd G$ $\forall i$, και η ακολουθία

$G = \gamma_1(G) \rhd \gamma_2(G) \rhd \ldots \rhd \gamma_i(G) \rhd \gamma_{i+1}(G) \rhd \ldots$ (2) ονομάζεται κατωτέρα κεντρική σειρά της G.

- **Παρατηρήσεις:**

1. Κάθε όρος $J_i(G)$ της ανωτέρας κεντρικής σειράς μίας ομάδας G, είναι χαρακτηριστική υποομάδα της G. Πράγματι, για $i=1$ έχουμε $J_1(G) = Z(G) \trianglelefteq G$. Αν $J_i(G) \trianglelefteq G$, τότε αρκεί να δείξουμε ότι $J_{i+1}(G) \trianglelefteq G$ και η απόδειξη με επαγωγή είναι πλήρης. Έστω $\alpha : G \to G$ αυτομορφισμός. Τότε $J_i(G) \trianglelefteq G \Rightarrow \alpha\big(J_i(G)\big) = J_i(G)$, επομένως ο α επάγει έναν αυτομορφισμό $\bar{\alpha} : G/J_i(G) \to G/J_i(G)$, $xJ_i(G) \to \alpha(x)J_i(G)$, αφού $\ker\bar{\alpha} = J_i(G)/J_i(G) = 1$, καθώς $\bar{\alpha}(x) \in 1 \Leftrightarrow \alpha(x) \in J_i(G) \Leftrightarrow \alpha \in J_i(G)$. Ακόμη, $Z\big(G/J_i(G)\big) \trianglelefteq G/J_i(G) \Rightarrow$ $\Rightarrow J_{i+1}(G)/J_i(G) \trianglelefteq G/J_i(G) \Rightarrow \bar{\alpha}\big(J_{i+1}(G)/J_i(G)\big) = J_{i+1}(G)/J_i(G)$, και επομένως $\forall x \in J_{i+1}(G)$ υπάρχει $y \in J_{i+1}(G)$: $\bar{\alpha}\big(x_{i+1}J_i(G)\big) = y_{i+1}J_i(G) \Rightarrow \alpha(x) = y \in J_{i+1}(G)$. Άρα $\alpha\big(J_{i+1}(G)\big) = J_{i+1}(G) \Rightarrow J_{i+1}(G) \trianglelefteq G$.
2. Κάθε όρος $\gamma_i(G)$ της κατωτέρας κεντρικής σειράς μίας ομάδας G, είναι πλήρως αναλλοίωτη υποομάδα της G. Πράγματι, για $i=2$ έχουμε $\gamma_2(G) = G' \underset{\pi.\alpha.}{\leq} G$. Αν $\gamma_i(G) \underset{\pi.\alpha.}{\leq} G$, τότε αρκεί να δείξουμε ότι $\gamma_{i+1}(G) \underset{\pi.\alpha.}{\leq} G$ και η απόδειξη με επαγωγή είναι πλήρης. Έστω $f : G \to G$ ενδομορφισμός. Τότε $\gamma_i(G) \underset{\pi.\alpha.}{\leq} G \Rightarrow f\big(\gamma_i(G)\big) = \gamma_i(G)$. Έχουμε ότι $\gamma_{i+1}(G) = \big[\gamma_i(G), G\big]$, δηλαδή $\gamma_{i+1}(G) = \big\langle x_i g x_i^{-1} g^{-1} \,|\, x_i \in \gamma_i(G), g \in G \big\rangle$. Όμως, ισχύει ότι $f\big(x_i g x_i^{-1} g^{-1}\big) =$ $= f(x_i) f(g) f(x_i)^{-1} f(g)^{-1} = y_i f(g) y_i^{-1} f(g)^{-1} \in \gamma_{i+1}(G)$ για κάποιο $y_i \in \gamma_i(G)$. Άρα $f\big(\gamma_{i+1}(G)\big) = \gamma_{i+1}(G) \Rightarrow \gamma_{i+1}(G) \underset{\pi.\alpha.}{\leq} G$.
3. Ακόμη, από την παραπάνω παρατήρηση έχουμε ότι $\gamma_{i+1}(G) = \big\langle x_i g x_i^{-1} g^{-1} \,|\, x_i \in \gamma_i(G), g \in G \big\rangle \leq \gamma_i(G)$, αφού $\gamma_i(G) \lhd G \Rightarrow g x_i^{-1} g^{-1} \in \gamma_i(G)$. Επίσης, $\gamma_{i+1}(G) = \big[\gamma_i(G), G\big] \Rightarrow \gamma_i(G)/\gamma_{i+1}(G) \leq Z\big(G/\gamma_{i+1}(G)\big)$.

- **Πρόταση**:

Έστω G μηδενοδύναμη ομάδα και $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ μία κεντρική σειρά της G. Τότε $\gamma_{n-i+1}(G) \leq G_i \leq J_i(G)$, δηλαδή η ανωτέρα και η κατωτέρα κεντρική σειρά της G είναι κεντρικές σειρές της G με το μικρότερο δυνατό μήκος.

<u>Απόδειξη:</u>

Εξετάζουμε πρώτα την πρόταση για την ανωτέρα κεντρική σειρά, δηλαδή πρέπει να δείξουμε ότι $G_i \leq J_i(G)$ $\forall i$. Για $i=0$ έχουμε ότι $G_0 = 1 \leq J_0(G)$, που προφανώς ισχύει. Εάν $G_i \leq J_i(G)$, τότε αρκεί να δείξουμε ότι $G_{i+1} \leq J_{i+1}(G)$ και η απόδειξη με επαγωγή είναι πλήρης. Όμως, καθώς $J_i(G) \lhd G$ (βλ. εφαρμογή 3

του μαθήματος 15) είναι $G_{i+1}/G_i \le Z(G/G_i) \Rightarrow {G_{i+1}J_i(G)}\big/{G_iJ_i(G)} \le Z\left({G}\big/{G_iJ_i(G)}\right) \overset{G_i \le J_i(G)}{\Rightarrow}$ $\overset{G_i \le J_i(G)}{\Rightarrow} {G_{i+1}J_i(G)}\big/{J_i(G)} \le Z\left({G}\big/{G_i}\right) \Rightarrow {G_{i+1}J_i(G)}\big/{J_i(G)} \le {J_{i+1}(G)}\big/{J_i(G)} \Rightarrow G_{i+1} \le J_{i+1}(G)$.

Στην συνέχεια εξετάζουμε την πρόταση για την κατωτέρα κεντρική σειρά, δηλαδή πρέπει να δείξουμε ότι $\gamma_{n-i+1}(G) \le G_i \ \forall i$. Θέτουμε $j = n-1$, οπότε η ζητούμενη σχέση γίνεται $\gamma_{j+1}(G) \le G_{n-j} \ \forall j$. Για $j = 0$ έχουμε ότι $\gamma_0(G) \le G_n = G$, που προφανώς ισχύει. Εάν $\gamma_{j+1}(G) \le G_{n-j}$, τότε αρκεί να δείξουμε ότι $\gamma_{j+2}(G) \le G_{n-(j+1)}$ και η απόδειξη με επαγωγή είναι πλήρης. Όμως $\gamma_{i+2}(G) = \left[\gamma_{i+1}(G), G\right] \le \left[G_{n-j}, G\right] \le G_{n-(j+1)} \Rightarrow \gamma_{i+2}(G) \le G_{n-(j+1)}$.

- **Παρατήρηση:**

1. Έστω G μηδενοδύναμη ομάδα με $\gamma_{i+1}(G) = 1 \Rightarrow \left[\gamma_i(G), G\right] = 1$ για κάποιο $i \in \mathbb{N}$. Για παράδειγμα, ας υποθέσουμε ότι $i = 2$, δηλαδή ότι $\gamma_3(G) = 1$. Τότε $\left[\gamma_2(G), G\right] = 1 \Rightarrow \left[\left[\gamma_1(G), G\right], G\right] = 1 \Rightarrow \left[\left[G, G\right], G\right] = 1$, δηλαδή $\left[\left[x, y\right], z\right] = 1$, $\forall x, y, z \in G$. Υπάρχει λοιπόν μία (μη-τετριμμένη) σχέση που χαρακτηρίζει την G.

- **Εφαρμογές:**

1. Έστω G πεπερασμένη μηδενοδύναμη ομάδα. Αν $a, b \in G$ και $\left(|a|, |b|\right) = 1$, τότε να δειχθεί ότι $ab = ba$.
2. Να βρεθεί η ανωτέρα κεντρική σειρά της Q_8 (ομάδα των quaternions). (υπόδειξη: $Q_8 \simeq \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix} \right\rangle \le GL(2, \mathbb{C})$ - να βρεθεί το $Z(Q_8)$).
3. Επιλέπτυνση κεντρικής σειράς είναι απαραίτητα κεντρική σειρά;
4. Έστω G ομάδα και $w \in J_2(G)$. Να δειχθεί ότι η απεικόνιση $\phi : G \to Z(G)$, $x \to [w, x]$, είναι ομομορφισμός και $G' \le \ker\phi$.
5. Έστω G ομάδα με $J_1(G) \ne J_2(G)$. Να δειχθεί ότι $G \ne G'$.

-Θεώρημα δομής για πεπερασμένα παραγόμενες αβελιανές ομάδες.

- **Πρόταση**:

Εάν $G = \langle x_1,...,x_n \rangle$ είναι μία πεπερασμένα παραγόμενη ομάδα, και $H \leq G$, τότε η H μπορεί να παραχθεί από n στοιχεία.

Απόδειξη:

Με επαγωγή στο n.

Για $n=1$ είναι $G = \langle x_1 \rangle$, δηλαδή η G είναι κυκλική και επομένως η $H \leq G$ είναι κυκλική, δηλαδή η H μπορεί να παραχθεί από 1 στοιχείο.

Για $n>1$, έστω $N = \langle x_1,...,x_{n-1} \rangle$. Τότε η $H \cap N \leq N$ μπορεί να παραχθεί από $n-1$ στοιχεία (από επαγωγική υπόθεση) και $H/H\cap N \simeq HN/N \leq G/N = \langle x_n N \rangle$, άρα η $H/H\cap N$ είναι κυκλική ομάδα ως υποομάδα κυκλικής ομάδας. Δηλαδή $H/H\cap N = \langle yH\cap N \rangle$, άρα η H μπορεί να παραχθεί από τα $n-1$ στοιχεία που παράγουν την $H\cap N$ και το y.

- ***Ορισμός***:

Εάν G πεπερασμένα παραγόμενη ομάδα. Ορίζουμε ως generating rank (και συμβολίζουμε με $g.r.(G)$) το ελάχιστο δυνατό πλήθος ενός συνόλου γεννητόρων της G.

- **Πρόταση**:

Έστω G ελευθέρα στρέψης, αβελιανή ομάδα με $g.r.(G) = n$. Τότε:

1. $G \simeq \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ (n φορές).
2. Αν $H \leq G$ με $|G:H| < \infty$, τότε $H \simeq G$.

Απόδειξη:

1. Με επαγωγή στο n.

   Για $n=1$ είναι $G = \langle a \rangle$, με $|a| = \infty$ (αφού η G είναι ελευθέρας στρέψης. Δηλαδή η G είναι άπειρη κυκλική ομάδα, συνεπώς $G \simeq \mathbb{Z}$.

   Για $n>1$, έστω $G = \langle x_1,...,x_n \rangle$. Θα δείξουμε ότι $G = \langle x_1 \rangle \times \cdots \times \langle x_n \rangle$, όπου προφανώς $\langle x_i \rangle \simeq \mathbb{Z}$ ως άπειρη κυκλική ομάδα. Έστω (προς άτοπο) ότι δεν ισχύει. Τότε $x_1^{a_1} \cdots x_n^{a_n} = 1$ για κάποια $a_1,...,a_n \in \mathbb{N}$, όχι όλα μηδέν. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $a_n \neq 0$. Τότε, αν $L = \langle x_1,...,x_{n-1} \rangle$, έπεται ότι $x_n^{a_n} \in L$. Καθώς $g.r.(L) = n-1$, από επαγωγική υπόθεση έχουμε ότι $L = \langle x_1 \rangle \times \cdots \times \langle x_{n-1} \rangle$. Επιπλέον, $m = |G:L| = |x_n| = a_n < \infty$. Θεωρούμε την απεικόνιση $\psi : G \to L$, $x \to x^m$. Η ψ είναι ομομορφισμός (αφού οι ομάδες είναι αβελιανές), με $\ker\psi = 1$ (αφού η G είναι ελευθέρα στρέψης).

Συνεπώς $G \simeq \psi(G) \leq L$, άρα από την προηγούμενη πρόταση προκύπτει ότι η G μπορεί να παραχθεί από $n-1$ στοιχεία – άτοπο.

2. Θέτουμε $m = |G:H| < \infty$. Καθώς $H \leq G$ και $g.r.(G) = n$, από προηγούμενη πρόταση έπεται ότι $g.r.(H) \leq n$. Έστω $g.r.(H) < n$. Όπως προηγουμένως, θεωρούμε την απεικόνιση $\phi : G \to H$, $x \to x^m$, η οποία είναι μονομορφισμός (βλ. απόδειξη της 1.). Άρα $G \simeq \phi(G) \leq H \Rightarrow g.r.(G) \leq g.r.(H) < n$ - άτοπο. Συνεπώς $g.r.(H) = n$, και από το 1. έχουμε ότι $H \simeq \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ (n φορές), δηλαδή $H \simeq G$.

Μάθημα 17ο (Τετάρτη, 2/7/2014)

[Ελεύθερες αβελιανές ομάδες, ολοκλήρωση του Θεωρήματος δομής για πεπερασμένα παραγόμενες αβελιανές ομάδες και των ιδιοτήτων των μηδενοδύναμων ομάδων]:

- **Ορισμός ελεύθερης αβελιανής ομάδας**:

Έστω A αβελιανή ομάδα και $X \subseteq A$. Η A λέγεται ελεύθερη αβελιανή ομάδα επί του X, αν για κάθε αβελιανή ομάδα B και για κάθε συνάρτηση $f: X \to B$ υπάρχει μοναδικός ομομορφισμός $\tilde{f}: A \to B$ με $\tilde{f}\big|_X = f$.

- **Παράδειγμα:**

1. Αν $A = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle$, όπου $\langle X_i \rangle \leq \mathbb{Z}$, τότε η A είναι ελεύθερη επί του $\{x_1, x_2, x_3\}$ - (εάν $A \simeq \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$, τότε η A είναι ελεύθερη επί του $x = 1$).

- **Πρόταση**:

Έστω $\phi: B \to A$ επιμορφισμός αβελιανών ομάδων, όπου $A = \langle X \rangle$ ελεύθερη αβελιανή επί του $X \subseteq A$. Τότε υπάρχει $K \leq B$ με $K \simeq A$ και $B \simeq K \times \ker\phi$.

Απόδειξη:

Αφού η ϕ είναι επί, υπάρχει απεικόνιση $\sigma: X \to B$ με $\phi \circ \sigma = 1$. Άρα, από τον ορισμό της ελεύθερης αβελιανής ομάδας, υπάρχει ομομορφισμός $\tilde{\sigma}: A \to B$ με $\tilde{\sigma}|_X = \sigma$. Επειδή $A = \langle X \rangle$ και $\phi \circ \tilde{\sigma}|_X = 1$, έπεται ότι $\phi \circ \tilde{\sigma} = 1_A$, δηλαδή η $\tilde{\sigma}$ είναι 1-1 και $\mathrm{im}\tilde{\sigma} = A$. Αν $b \in B$, τότε $\phi\left(b\tilde{\sigma}^{-1}\left(\phi(b)\right)\right) = \phi(b)\phi\left(\tilde{\sigma}\left(\phi^{-1}(b)\right)\right) =$ $= \phi(b)(\phi \circ \tilde{\sigma})\left(\phi^{-1}(b)\right) \overset{\phi\circ\tilde{\sigma}=1}{=} \phi(b)\phi^{-1}(b) = 1$, επομένως $b\tilde{\sigma}^{-1}\left(\phi(b)\right) \in \ker\phi \Rightarrow$ $\Rightarrow b \in \ker\phi\left(\tilde{\sigma}\left(\phi(b)\right)\right) \Rightarrow b \in \ker\phi \cdot \mathrm{im}\tilde{\sigma}$. Άρα $B \leq \ker\phi \cdot \mathrm{im}\tilde{\sigma} \leq B \Rightarrow B = \ker\phi \cdot \mathrm{im}\tilde{\sigma}$. Ακόμη, αν $w \in \ker\phi \cap \mathrm{im}\tilde{\sigma} \Rightarrow w = 1$, άρα $B = \mathrm{im}\tilde{\sigma} \times \ker\phi$, με $\mathrm{im}\tilde{\sigma} = A$.

- **Θεώρημα δομής για πεπερασμένα παραγόμενες αβελιανές ομάδες:**

Έστω A μία πεπερασμένα παραγόμενη αβελιανή ομάδα. Τότε $A \simeq C_1 \times \cdots \times C_k \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$, όπου C_i κυκλική ομάδα.

Απόδειξη:

Έστω A μία πεπερασμένα παραγόμενη αβελιανή ομάδα και $T_A = \{a \in A \,|\, |a| < \infty\}$. Τότε $T_A \leq A$ και η A/T_A δεν έχει μη-τετριμμένα στοιχεία πεπερασμένης τάξης. Επίσης, αφού η A είναι πεπερασμένα παραγόμενη αβελιανή ομάδα, έπεται ότι και η A/T_A είναι πεπερασμένα παραγόμενη αβελιανή ομάδα.

Θεωρούμε τον φυσικό επιμορφισμό $\pi : A \to A/T_A$, $x \to xT_A$. Καθώς η A/T_A είναι πεπερασμένα παραγόμενη αβελιανή, ελευθέρα στρέψης ομάδα, γνωρίζουμε ότι $A/T_A \simeq \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ (n φορές), όπου $n = g.r.(A/T_A)$. Συνεπώς η A/T_A είναι ελεύθερη αβελιανή και από προηγούμενη πρόταση $A \simeq K \times \ker\pi$, όπου $K \simeq A/T_A \simeq \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ (n φορές). Όμως $\ker\pi = T_A$, άρα $A \simeq T_A \times K$, όπου T_A είναι μία πεπερασμένα παραγόμενη αβελιανή και περιοδική ομάδα, συνεπώς η T_A είναι πεπερασμένη αβελιανή ομάδα. Επομένως η T_A ισούται με το ευθύ γινόμενο των Sylow p-υποομάδων της, και κάθε Sylow p-υποομάδα (ως p-ομάδα) γράφεται ως ευθύ γινόμενο κυκλικών ομάδων.

- **Πρόταση (transfer map)**:

Έστω G ομάδα και $H \le Z(G)$ με $|G:H| = n < \infty$. Τότε η απεικόνιση $\tau : G \to H$, $g \to g^n$, είναι ομομορφισμός.

- **Πρόταση (Schur)**:

Έστω G ομάδα και $|G:Z(G)| < \infty$. Τότε η G' είναι πεπερασμένη.

<u>Απόδειξη:</u>

Έστω $|G:Z(G)| = n$. Τότε $G = \{Z(G)x_1 \cup \ldots \cup Z(G)x_n\}$. Αν $a,b \in G$, τότε $a = wx_i$ και $b = w_1x_j$ για κάποια $w, w_1 \in Z(G)$. Άρα $aba^{-1}b^{-1} = wx_iw_1x_jx_i^{-1}w^{-1}x_j^{-1}w_1^{-1} = = x_ix_jx_i^{-1}x_j^{-1}$, δηλαδή $G' = \langle [a,b], a,b \in G \rangle = [x_i, x_j]$ και επομένως η G' είναι πεπερασμένα παραγόμενη. Ακόμη, $G'/G' \cap Z(G) \simeq G'Z(G)/Z(G) \le G/Z(G)$. Άρα $|G' : G' \cap Z(G)| < \infty$ και σε συνδυασμό με το γενονός ότι G' είναι πεπερασμένα παραγόμενη, έπεται ότι $G' \cap Z(G)$ είναι πεπερασμένα παραγόμενη αβελιανή ομάδα (αβελιανή ως υποομάδα του κέντρου $Z(G)$). Από την προηγούμενη πρόταση έπεται ότι η $\tau : G \to Z(G)$, $g \to g^n$, είναι ομομορφισμός με $G/\ker\tau \le Z(G)$. Δηλαδή η $G/\ker\tau$ είναι αβελιανή υποομάδα της G και επομένως $G' \le \ker\tau$. Έτσι αν $y \in G' \Rightarrow \tau(y) = 1 \Rightarrow y^n = 1$. Άρα κάθε στοιχείο της G' έχει πεπερασμένη τάξη, δηλαδή η $G' \cap Z(G)$ είναι πεπερασμένα παραγόμενη αβελιανή και περιοδική ομάδα. Έπεται ότι η $G' \cap Z(G)$ είναι πεπερασμένη. Τελικά $|G' : G' \cap Z(G)| < \infty$, $|G' \cap Z(G)| < \infty \Rightarrow$ η G' είναι πεπερασμένη.

- **Πρόταση**:

Αν G μηδενοδύναμη ομάδα και η $G_{ab} = G/G'$ είναι πεπερασμένη, τότε η G είναι πεπερασμένη.

Απόδειξη:

Με επαγωγή στην κλάση μηδενοδυναμίας c.

Για $c = 1$ η G είναι αβελιανή, άρα $G' = 1$ και η $G = G/1 = G/G' = G_{ab}$ είναι πεπερασμένη από υπόθεση.

Για $c > 1$, έστω $1 = G_0 \lhd G_1 \lhd ... \lhd G_n = G$ κεντρική σειρά της G. Τότε $G_1 \leq Z(G)$, G/G_1 μηδενοδύναμη με μικρότερη δυνατή κλάση ισοδυναμίας και $(G/G_1)' = G'G_1/G_1$. Άρα $(G/G_1)_{ab} = {}^{G/G_1}\!\big/_{G'G_1/G_1} \simeq {}^{G}\!\big/_{G'G_1}$. Παρατηρούμε ότι η απεικόνιση $G/G' \to G/G'G_1$, $xG' \to xG'G_1$, είναι επιμορφισμός, και η G/G' είναι πεπερασμένη. Επομένως και η $G/G'G_1$ είναι πεπερασμένη, δηλαδή η $(G/G_1)_{ab}$ είναι πεπερασμένη και από επαγωγική υπόθεση έχουμε ότι η G/G_1 είναι πεπερασμένη. Άρα $|G : G_1| < \infty$ και, καθώς $G_1 \leq Z(G)$, έχουμε ότι $|G : Z(G)| \leq |G : G_1| < \infty$. Από την πρόταση του Schur έπεται ότι η G' είναι πεπερασμένη. Από υπόθεση όμως ισχύει επιπλέον ότι $|G : G'| = |G/G'| < \infty$, άρα συμπεραίνουμε ότι η G είναι πεπερασμένη.

- **Πρόταση**:

Αν G μηδενοδύναμη ομάδα και $T_G = \{g \in G \mid |g| < \infty\}$, τότε η $T_G \leq G$.

Απόδειξη:

Αρκεί να δείξουμε ότι αν $x, y \in G$ έχουν πεπερασμένη τάξη, τότε και το $xy \in G$ έχει πεπερασμένη τάξη. Έστω $H = \langle x, y \rangle \leq G$. Τότε η H/H' είναι μία πεπερασμένα παραγόμενη αβελιανή ομάδα που παράγεται από δύο στοιχεία πεπερασμένης τάξης, τα xH' και yH'. Άρα είναι πεπερασμένη. Επίσης, η H είναι μηδενοδύναμη ως υποομάδα μηδενοδύναμης και από την προηγούμενη πρόταση η H είναι πεπερασμένη. Επομένως το $xy \in H$ έχει πεπερασμένη τάξη.

- **Πρόταση**:

Έστω G ομάδα ελευθέρα στρέψης, $H \leq G$ με $|G : H| < \infty$ και $H \simeq \mathbb{Z}$. Τότε $G \simeq \mathbb{Z}$.

Απόδειξη:

Υπάρχει $1 \neq N \leq H$, η οποία είναι κανονική υποομάδα της G. Προφανώς $1 \neq N \leq \mathbb{Z} \Rightarrow N \simeq \mathbb{Z}$, άρα χωρίς βλάβη της γενικότητας υποθέτουμε ότι $H \lhd G$. Έστω $g \in G$ με ${}^{\langle g \rangle}\!\big/_{\langle g \rangle \cap H} \simeq {}^{H\langle g \rangle}\!\big/_{H} \leq {}^{G}\!\big/_{H}$. Καθώς $\left|{}^{G}\!\big/_{H}\right| < \infty \Rightarrow |\langle g \rangle : \langle g \rangle \cap H| < \infty \Rightarrow$

$\Rightarrow \langle g\rangle \cap H \neq 1 \overset{H\simeq\mathbb{Z}}{\Rightarrow} |H:\langle g\rangle \cap H| < \infty \overset{|G:H|<\infty}{\Rightarrow} |G:\langle g\rangle \cap H| < \infty \Rightarrow |G:\langle g\rangle| < \infty$. Αφού η H είναι πεπερασμένα παραγόμενη ($H \simeq \mathbb{Z}$) και $|G:H| < \infty$, έπεται ότι και η G είναι πεπερασμένα παραγόμενη. Έστω $G = \langle X\rangle$, $|X| < \infty$. Τότε $\langle g\rangle \leq C_G(g) \Rightarrow$ $\Rightarrow |G:C_G(g)| < |G:\langle g\rangle| < \infty$, δηλαδή $|G:C_G(x)| < \infty \quad \forall x \in X$, άρα $\left|G:\bigcap_{x\in X} C_G(x)\right| < \infty$ (βλ. παρατήρηση). Όμως $\bigcap_{x\in X} C_G(x) = Z(G)$, συνεπώς $|G:Z(G)| < \infty$ και από την πρόταση του Schur έπεται ότι η G' είναι πεπερασμένη. Όμως η $G' \leq G$ είναι ακόμη ελευθέρα στρέψης, άρα $G' = 1$. Επομένως η G είναι αβελιανή και η $\sigma : G \to H$, $w \to w^n$ (όπου $n = |G:H|$) είναι ομομορφισμός. Όμως $\ker\sigma = 1$ (αφού η G είναι ελευθέρα στρέψης), δηλαδή η σ είναι μονομορφισμός, το οποίο σημαίνει πως $G \simeq \mathrm{im}\sigma \leq H \overset{H\leq G}{\Rightarrow} G \simeq H \Rightarrow G \simeq \mathbb{Z}$.

- **Παρατήρηση:**

1. Έστω G ομάδα, $A,B \leq G$ με $|G:A|, |G:B| < \infty$. Τότε $|G:A\cap B| < \infty$. Πράγματι,
$$|G:A\cap B| = \frac{|G|}{|A\cap B|} = \frac{|G|}{\frac{|A|\cdot|B|}{|AB|}} = \frac{|G|}{|A|}\cdot\frac{|AB|}{|A|} \leq \frac{|G|}{|A|}\cdot\frac{|G|}{|B|} = |G:A|\cdot|G:B| < \infty.$$

- **Εφαρμογή:**

1. Έστω G πεπερασμένα παραγόμενη ομάδα, δηλαδή $G = \langle X\rangle$, όπου $|X| < \infty$. Εάν η G έχει πεπερασμένο πλήθος συζυγών ομάδων, τότε να δειχθεί ότι η G είναι πεπερασμένη.